



Extreme Networks Extreme Management Center[®] *NAC Manager User Guide*

Copyright © 2016 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.,
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000



Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications

and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. **YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.**
4. LICENSE TYPES.
 - *Single User, Single Computer.* Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
 - *Client.* Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to

Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED

MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

- a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers.

This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

- b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme

of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.
10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
 - a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
 - b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in

accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
- NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.
- Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply

to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
15. GENERAL.
 - a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
 - b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
 - c. You represent that You have full right and/or authorization to enter into this Agreement.
 - d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.
 - e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
 - f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
 - g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
 - h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other

communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Table of Contents

Legal Notices	i
Trademarks	i
Support	i
Contact	i
Extreme Networks® Software License Agreement	ii
Table of Contents	x
Extreme Management Center® NAC Manager Help	1
NAC Manager Features	1
Document Version	2
NAC Manager Configuration Considerations	4
NAC Configuration Tables	4
General Considerations	8
Considerations When Implementing Policy Roles	12
ExtremeWireless Wireless Controller Configuration	13
DNS Proxy Functionality for Registration and Remediation	14
Basic Operation	14
Enabling DNS Proxy	15
Backup DNS Server	16
Troubleshooting	16
NAC Manager Concepts	17
Overview of NAC Manager	17
NAC Engines	18
Use Scenario	18
NAC VPN Deployment	21
NAC Manager Structure	22

NAC Configuration	23
Rule Components	24
NAC Profiles	25
AAA Configurations	25
Portal Configurations	25
Access Policies	26
Registration	28
How Registration Works	30
Assessment	30
Assessment Remediation	33
How Remediation Works	34
End-System Zones	35
End-System Zone Use Cases	36
Enforcing	37
Advanced Enforce Options	39
MAC Locking	40
Notifications	41
Automated Security Manager Blacklist	41
Mobile IAM	42
How to Set Up Registration	43
Extreme Access Control Gateway Configuration	44
Identifying Extreme Access Control Gateway Location	44
Third-Party URL Redirection Considerations	45
Defining the Unregistered Access Policy	45
Creating the Unregistered Access Policy	45
Configuring the Unregistered Extreme Access Control Profile	48

Configuring Policy-Based Routing	49
Configuring NAC Manager (for Extreme Access Control Gateways and Extreme Access Control Controllers)	52
Portal Configuration	54
Accessing the Portal Configuration	54
Network Settings	55
Administration	58
Administration Web Page Settings	59
Administrative Login Configuration	60
Look and Feel	63
Common Settings	67
Guest Registration	69
Registration Settings	71
Facebook Registration	73
Sponsorship	73
Guest Web Access	73
Secure Guest Access	77
Secure Access Settings	78
Sponsorship	80
Authenticated Registration	80
Authentication (Shared)	81
Web Page Customizations (Shared)	82
Redirection (Shared)	83
Registration Settings (Shared)	83
Authenticated Web Access	85
Authentication (Shared)	86

Web Page Customizations (Shared)	87
Redirection (Shared)	88
Web Access Settings	88
Assessment/Remediation	89
Web Page Settings	90
Remediation Attempt Limits	92
Remediation Links Subtab	93
Custom Remediation Actions Subtab	93
Portal Web Page URLs	94
Registration Administration	96
Devices	97
Users	99
Registered Users	99
Add Registered User	101
Local Users	103
Add Local User	104
Pre-Registration Portal	105
Screen Preview	106
Sponsored Registration	109
How to Configure Pre-Registration	110
Configuring Pre-Registration	110
Pre-Registering Guest Users	116
Pre-Registering a Single User	117
Pre-Registering Multiple Users	118
How to Set Up Assessment	123
Managing Your Assessment Servers	124

Adding External Assessment Servers	125
Creating Assessment Configurations	126
Enabling Assessment for NAC Profiles	129
NAC Assessment Phased Deployment Guide	131
Overview	132
Phased Deployment	132
How Assessments are Scored	133
Viewing Health Results	135
End User Notification	137
Web Portal Notification	137
Agent Notification	139
Phased Deployment	141
Informational Assessment	141
Warning Assessment	142
Quarantine Assessment	144
Agent-less Assessment	146
Agent-less Informational Assessment	146
Agent-less Warning Assessment	146
Agent-less Quarantine Assessment	147
Agent-Based Assessment	147
No Agent Detected	147
Agent-Based Informational Assessment	148
Agent-Based Warning Assessment	149
Agent-Based Quarantine Assessment	149
Combined Agent-less and Agent-Based Assessment	150
Combined Informational Assessment	150

Combined Warning Assessment	151
Combined Quarantine Assessment	151
Monitoring Assessment Results	152
Search by Assessment Results	152
Statistical Reports	154
Control Dashboard	156
Diagnostics and Troubleshooting	156
Analyze Health Results	156
End-System Events	156
Screen Preview	156
Extreme Access Control Engine Administration	157
Log Files	157
Disabling Assessment	158
Disable Assessment on the Engine	158
Disable Assessment in the NAC Profile	159
Change the Quarantine Policy	159
No Assessment End-System Group	160
Revert to Informational Assessment	162
How to Configure Assessment	163
Agent-less Assessment Configuration	164
Agent-less Informational Assessment	164
Agent-less Warning Assessment	169
Agent-less Quarantine Assessment	176
Agent-Based Assessment Configuration	182
Agent-Based Informational Assessment	182
Agent-Based Warning Assessment	188

Agent-Based Quarantine Assessment	194
Combined Assessment Configuration	199
Combined Informational Assessment	199
Combined Warning Assessment	202
Combined Quarantine Assessment	204
How to Deploy Agent-Based Assessment	208
Configuring Agent Deployment	208
Performing a Managed Deployment or Installation	212
Agent Icons and Notification Messages	213
Agent Information Messages	215
Client Timeout Message	215
Disabled Client Message	215
Upgrade Agent Message	215
Agent Remediation Message	216
Agent Diagnostics	217
Client Diagnostics Buttons	218
How to Create a Custom Scan for Agent-less Assessment	219
How to Change the Assessment Agent Adapter Password	226
How to Install the Assessment Agent Adapter on a Nessus Server	228
How to Set Up Assessment Remediation	231
Extreme Access Control Gateway Configuration	232
Identifying Extreme Access Control Gateway Location	232
Third-Party URL Redirection Considerations	233
Defining Assessment and Quarantine Policies	233
Configuring Policy-Based Routing	237

Configuring NAC Manager (for Extreme Access Control Gateways and Extreme Access Control Controllers)	240
How To Use NAC Manager	242
How to Change Extreme Access Control Engine Settings	243
Changing DNS, NTP, SSH, and SNMP Settings	243
Changing Hostname, Gateway, and Static Routes	244
How to Configure Communication Channels	247
Configuring Communication Channels	248
How to Configure Credential Delivery for Secure Guest Access	253
Configuration Steps	253
How Secure Guest Access Works	260
How to Configure End-System Zones	265
Preliminary Steps	266
Plan Your End-System Zones	266
Determine User Group Zone Authorization	266
Configuring Zones in NAC Manager	267
How to Configure LDAP for End Users and Hosts via Active Directory	269
How to Configure Load Balancing	275
ExtremeXOS/EOS Firmware Load Balancing	275
External Load Balancers	277
External Load Balancing Example	278
How to Configure Local RADIUS Termination at the Extreme Access Control Engine	280
LDAP Authentication	281
User Authentication Considerations	281
Active Directory	281
Other LDAP Servers	285

Local Authentication	286
User Password Considerations	286
Certificate Configuration	287
EAP-TLS Certificate Requirements	287
How to Configure Management Authentication	288
How to Configure PEAP Authentication via eDirectory	293
How to Configure PEAP Authentication via OpenLDAP	300
How to Configure Sponsorship for Guest Registration	302
How to Configure Verification for Guest Registration	306
Configuration Steps	306
How User Verification Works	313
How to Create a Rule	316
How to Deploy Extreme Access Control in an MSP or MSSP Environment	323
Configuring Extreme Management Center Behind a NAT Router	323
Defining Interface Services	324
How to Display End-System Registration and Group Information	325
How to Enable RADIUS Accounting	328
Considerations for Fixed Switching Devices	330
Considerations for ExtremeXOS Devices	331
NAC Enterprise Licensing	332
Enterprise Licenses	332
Applying an Enterprise License	333
Configuring End-System Capacity for an Extreme Access Control Engine	335
License Violations	337
Enterprise Assessment Licenses	337

Applying an Enterprise Assessment License	337
How to Implement Facebook Registration	340
Requirements	340
Creating a Facebook Application	341
NAC Portal Configuration	347
How Facebook Registration Works	349
Special Deployment Considerations	349
Networks using DNS Proxy	349
How to Initialize NAC Manager Database Components	351
How to Lock a MAC Address	352
Menu Bar	354
File Menu	354
Tools Menu	354
Applications Menu	357
Help Menu	357
Right-Click Menu Options	358
How to Set NAC Manager Options	363
Advanced Settings	363
Assessment Server	365
Data Persistence	367
Display	368
End-System Event Cache	369
Enforce Warning Settings	370
Setting Features Options	371
Setting Notification Engine Options	371
Policy Defaults	372

Port Wizard Defaults	373
Status Polling and Timeout	374
How to Set Up Access Policies and Policy Mappings	376
Setting Up Your Access Policies	377
Toolbar	384
How to Update Extreme Access Control Engine Server Certificates	387
Certificate Requirements	388
Replacing the Certificate	388
Verifying the Certificate	390
Verifying the Captive Portal Server Certificate	390
Use a Browser	390
Use OpenSSL	391
Verifying the Internal Communications Server Certificate	391
Use a Browser	391
Use OpenSSL	392
Generating a Server Private Key and Server Certificate	392
Generate a Server Private Key	393
Create a Certificate Signing Request	393
Submit the Request to a Certificate Authority	394
Verify the Contents of the Server Certificate	394
How to Use Device Type Profiling	395
Device Profiling Use Case	395
How to Verify RADIUS Configuration	403
NAC Manager Right-Panel Tabs	406
Appliance Groups Tab	407
Configuration Tab (Extreme Access Control Engine)	409

Configuration Tab	414
End-Systems Tab	417
End-Systems	418
Actions	422
End-System Events Tab	424
Health Result Summaries Tab	427
Health Result Details Tab	429
NAC Appliances Tab	433
Statistics Tab	436
End-System Info	436
States	436
Extended States	438
Reasons	440
End-System Status	440
Most Frequently Occurring Vulnerabilities	441
End-System NAC Profile Allocation	442
End-System Risk	444
Right-Click Menu Options	444
Switches Tab	446
NAC Manager Windows	451
AAA Configuration	452
Accessing the AAA Configuration	452
Basic AAA Configuration	453
Advanced AAA Configuration	454
Add/Edit Agent-Based Test Set Window	458
Agent Configuration	459

Test Cases	461
Default Test Cases	463
User-Defined Test Cases	464
Agent-Based Test Support per OS	465
Add/Edit Agent-less Test Set Window	467
Add/Edit Assessment Server Pool Window	474
Add/Edit Assessment Server Window	476
Add/Edit Device Type Group Window	478
Add/Edit End-System Group Window	481
Add/Edit IP Subnet Window	484
Primary/Secondary Gateway Router	485
Add/Edit Location Group Window	487
Add/Edit MAC Lock Window	489
Add/Edit Nessus Test Set Window	491
Add/Edit Other Test Set Window	495
Add/Edit Policy Mapping Window	497
Add/Edit Risk Level Configuration Window	500
Add/Edit Scoring Override Window	503
Add/Edit Scoring Override Configuration Window	506
Add/Edit Time Group Window	509
Add/Edit User Group Window	511
Add/Edit User to Authentication Mapping Window	513
Add Switches to NAC Appliance Group Window	517
Advanced Agent Configuration Window	522
Advanced Assessment Configuration Window	526
Advanced Configuration Window	527

NAC Configurations	527
Global and Appliance Settings	528
AAA Configurations Panel	529
Appliance Settings Panel	530
Assessment Panel	532
MAC to IP Mappings Panel	534
NAC Configuration Panel	536
Portal Configurations Panel	538
Web Site Configuration Panel	540
Advanced Location-Based Registration and Web Access	542
Advanced Switch Settings	547
Allowed Web Sites Window	549
Allowed URLs	549
Allowed Domains	550
Web Proxy Servers	552
Antivirus Editor	553
Extreme Access Control Engine Advanced Configuration Window	556
New/Edit Engine Settings Window	558
IP Resolution Tab	558
MAC Resolution Tab	563
Hostname/Username Resolution	565
Reauthentication Tab	567
Credentials Tab	571
Switch Configuration	571
Web Service Credentials	573
Access Control Admin Web Page	573

EAP-TLS Configuration	573
Miscellaneous Tab	574
Port Link Control	574
NetBIOS	575
Kerberos	576
Microsoft NAP	577
Device Type Detection Tab	578
Network Tab	580
Manage DNS Configuration	580
Manage NTP Configuration	581
Manage SSH Configuration	581
SNMP Configuration	583
Configuration Evaluation Tool	584
User Input	585
Configuration Results	585
Authorization Results Tab	585
Authentication Results Tab	586
Create NAC Appliance Window	587
Create/Edit Rule Window	589
Create/Edit Static Route Window	592
Create Virtual and Physical Network Configuration Window	593
Edit Action Overrides Window	595
Keyword Definitions	596
Edit Assessment Configuration Window	604
Edit Local Password Repository Window	608
Edit Notification Action Window	610

Conditions	612
Actions	613
Result	614
Edit Policy Mapping Configuration Window	616
Column Definitions	618
Edit Switches in NAC Appliance Group Window	621
Edit User Group Window	626
End-System Summary Window	628
Event Details Window	631
Event View	633
NAC Manager Events Tab	633
Logging of End-System Group Events	634
End-Systems Activity Tab	635
NAC Appliance Events Tab	638
Audit Events Tab	639
File Check Editor	642
Firewall Editor	644
Hotfix Check Editor	647
Import MAC Entries Window	650
Installed Program Check Editor	652
Interface Configuration Window	657
Interface Modes	658
Services	659
DHCP/Kerberos Snooping	660
Captive Portal HTTP Mirroring	660
Tagged VLANs	660

LDAP Policy Mapping Window	661
Manage Appliance Certificates Window	663
Appliance	664
AAA Configuration	666
Manage Assessment Server Pools Window	667
Manage Assessment Servers Window	669
Manage Assessment Settings Window	673
Assessment Configurations	673
Assessment Servers	675
Assessment Server Pools	678
Manage Custom Fields Window	681
Manage Data Center Fabric Window	685
Manage End-System Zones Window	687
Manage LDAP to Policy Mappings Window	689
Manage MAC Locks Window	691
Manage NAC Profiles Window	693
Manage Notifications Window	695
Manage Operating Systems Window	699
Manage RFC 3576 Configurations Window	700
Manage Risk Level Configurations Window	702
Manage Rule Groups Window	704
Manage Scoring Override Configurations Window	707
Manage Test Sets Window	709
Message Strings Editor	711
Minimum Agent Version Editor	714
NAC Configuration Window	716

Accessing the NAC Configuration	716
Features	717
NAC Configuration Rules	720
Accessing NAC Configuration Rules	720
Viewing Rules in the Table	720
Creating and Editing Rules	721
NAC Manager Options Window	724
Advanced Settings	724
Assessment Server	727
Data Persistence	729
Display	732
End-System Event Cache	735
Enforce Warning Settings	736
Features	737
Notification Engine	738
Policy Defaults	740
Port Wizard Defaults	742
Status Polling and Timeout	743
New/Edit Locale Window	746
New/Edit NAC Profile Window	748
Authorization	749
Assessment	751
Policy Mappings	752
New/Edit RFC 3576 Reauthentication Configuration Window	754
New/Edit Switch Reauthentication Configuration Window	757
Notification Advanced Settings Window	759

Operating System Editor	761
P2P Software Editor	763
Patch Auto Update Editor	766
Patch Update Last Run In Editor	769
Portal Configuration	771
Accessing the Portal Configuration	771
Network Settings	772
Administration	775
Administration Web Page Settings	776
Administrative Login Configuration	777
Look and Feel	780
Common Settings	784
Guest Registration	786
Registration Settings	788
Facebook Registration	790
Sponsorship	790
Guest Web Access	790
Secure Guest Access	794
Secure Access Settings	795
Sponsorship	797
Authenticated Registration	797
Authentication (Shared)	798
Web Page Customizations (Shared)	799
Redirection (Shared)	800
Registration Settings (Shared)	800
Authenticated Web Access	802

Authentication (Shared)	803
Web Page Customizations (Shared)	804
Redirection (Shared)	805
Web Access Settings	805
Assessment/Remediation	806
Web Page Settings	807
Remediation Attempt Limits	809
Remediation Links Subtab	810
Custom Remediation Actions Subtab	810
Portal Web Page URLs	811
Process State Check Editor	813
Registry Key Check Editor	816
Registry Key Check Editor	818
Registry Key Check Advanced Editor	821
Registry Key Test Cases	823
Remove End-Systems Window	824
Screen Saver Editor	826
Search for End-Systems Window	828
Search for End-Systems by Assessment Results Window	836
Send Message to End System Agents Window	837
Service State Check Editor	840
Static Route Configuration Window	843
Synchronize Appliances with Console Window	844
Import NAC (Extreme Access Control) Appliances From Console	845
Export NAC Appliances To Console	845
Update AAA Trusted Certificate Authorities Window	846

Update Captive Portal Server Certificate Window	848
Update Internal Communications Server Certificate Window	851
Update RADIUS Server Certificate Window	854
Updates Available Window	856
Extreme Access Control (NAC) Deployment Guide	858
Phased Rollout Strategy	859
Authentication Only	859
Assessment without Quarantine	860
Location-Based Assessment and/or Registration	860
Important Links in Extreme Access Control and Extreme Management Center	861
MAC and IP Resolution	863
MAC to IP Resolution	863
The MAC to IP Resolution Process	864
If IP Resolution Fails	868
Deployment Considerations	869
Diagnostics for IP Resolution	869
IP to MAC Resolution	870
The IP to MAC Resolution Process	871
Diagnostics for MAC Resolution	872
Agent-Based Assessment	873
Configure OS-Based Test Cases	873
Exclude End-Systems from Assessment Using MAC OUIs	877
Third-Party Device Considerations	880
Extreme Management Center Server Data Retention Tools	881
Extreme Access Control Capacity Option	881

Data Persistence Options	882
Age End-Systems	883
End-System Event Persistence	883
Health Result Persistence	884
Troubleshooting	884
Extreme Access Control Appliance	884
Appliance Command Line Diagnostics	884
Extreme Access Control Appliance Administration Web Page	886
Extreme Management Center Server	897
Generate Show Support	897
Monitoring	898
Extreme Management Center Server and Extreme Access Control Appliance Connectivity	901
SNMP	902
Web Services	902
JMS Connections	908
NAC Manager Reference Information	910
Microsoft® NAP Processing	911

Extreme Management Center[®] NAC Manager Help

NAC Manager provides secure, policy-based management for Extreme Networks Mobile IAM and Extreme Access Control solutions. It configures and manages Mobile IAM and Access Control gateways, provides user to device location mapping services, generates network endpoint audit reports and interfaces with other security management applications.

Contact your sales representative for information on obtaining a Extreme Management Center software license.

NAC Manager Features

NAC Configuration

The NAC Configuration lets you manage the end user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, time of day, and location. NAC Manager comes with a default NAC Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

Assessment/Remediation

NAC Manager supports agent-less or agent-based security posture assessment of endpoints. NAC Manager uses assessment servers to assess and audit connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail assessment can be dynamically quarantined with restrictive network access to prevent security threats from entering the network.

Assisted remediation is a process that informs end users when their end-systems are quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. Once the remediation steps are successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

End-System Monitoring

Monitor end-system events and view the health results from an end-system's latest assessment. Quickly view historical and last-known connection states for each end-system, and obtain information on security risks found on an end-system during an assessment.

Web-based Dashboard

The NAC Manager Dashboard feature provides three web-based views of end-system data including a selection of reports that provide an overview of end-system connection and assessment information along with detailed end-system event and health result information.

Registration

Registration forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. End users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations gains visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network.

Notifications

Notifications provide the ability for NAC Manager to notify administrators or helpdesk personnel of important information through email, trap, or syslog messages. These notifications help administrators understand what is going on in their Access Control system on a real-time basis. For example, NAC Manager can be configured to send a notification when a new end-system is learned on the network, when a MAC lock is violated, or when a new MAC address is registered on the network.

Leverages Automated Security Manager

Automated Security Manager (ASM) can be configured to notify NAC Manager in response to a real-time security threat from an end-system on the network. NAC Manager automatically adds the end-system's MAC address to the Blacklist end-system group, effectively putting the end-system in quarantine and preventing the end-system from accessing the network from any location.

Document Version

The following table displays the revision history for the NAC Manager Help documentation.

Date	Revision Number	Description
06-16	7.0 Revision -00	NetSight 6.4 release
07-15	6.3 Revision -00	NetSight 6.3 release
01-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9034984-01

NAC Manager Configuration Considerations

Review the following configuration considerations when installing and configuring NetSight NAC Manager.

- [NAC Configuration Tables](#)
- [General Considerations](#)
- [Considerations When Implementing Policy Roles](#)
- [IdentiFi Wireless Controller Configuration](#)
- [DNS Proxy Functionality for Registration and Remediation](#)

NAC Configuration Tables

The following tables provide valuable information to help guide you through the deployment of Extreme Networks NAC for your network. The first table displays suggested NAC configurations that should be used for different network deployment circumstances (e.g. type of end-systems on the network, network topology, authentication method deployed, etc.). The second table displays details and information for each of the different suggested NAC configurations. The information in the tables assumes that DHCP is deployed on the network.

Suggested NAC Configuration for Different Deployments

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- Policy Only (without changing of VLANs)	*	*	*	*	*	A
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Multiple	Microsoft XP SP1 with KB822596 installed ¹	802.1X ²	Yes	*	A

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Multiple	*	802.1X ²	Yes	*	B
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Multiple	*	802.1X ²	No	Yes	C
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Multiple	*	802.1X ²	No	No	D
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs) <i>[for Enterasys switch]</i>	Multiple	*	MAC Authentication	*	*	B
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs) <i>[for non-Enterasys switch]</i>	Multiple	*	MAC Authentication	*	Yes	C
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs) <i>[for non-Enterasys switch]</i>	Multiple	*	MAC Authentication	*	No	D

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Single	Microsoft or MAC OS	*	*	*	E
- VLAN only - Policy and VLAN - Policy Only (with changing of VLANs)	Single	Linux	*	*	*	F
Wireless Device	Multiple	*	*	*	*	G

* = Any value.

N/A = Not applicable.

¹For more information on this patch, see the following link: <http://support.microsoft.com/default.aspx?scid=kb;en-us;KB822596>

²When 802.1X is implemented to authenticate multiple users on a single switch port, the downstream device providing connectivity to the users must support the forwarding of EAP frames. Unintelligent devices such as repeaters and switches with newer firmware releases should forward EAP frames. However, some switches do not forward EAP frames therefore preventing the 802.1X authentication of multiple users on a single port.

NAC Configuration Details

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
A	Disabled	Disabled	*	No	N/A
NOTE: This is the simplest of configurations.					
B	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
NOTES: When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.					

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
C	Disabled	Enabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	<p>NOTES:</p> <p>When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. Furthermore, the end-system will continually reauthenticate to the network while it is being scanned.</p> <p>When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.</p>				
D	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	Set short reauthentication interval manually on edge switches (e.g. 2 min)
	<p>NOTE:</p> <p>This is not a very scalable configuration model, and therefore should not be implemented for a network with a large number of end-systems.</p>				
E	Enabled	Disabled	*	No	N/A
	<p>NOTE:</p> <p>End-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.</p>				
F	Enabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	<p>NOTES:</p> <p>End-system will be reauthenticated with link down/up execution and will automatically re-establish network connectivity via DHCP upon lease expiration of the IP address in the unauthenticated, Assessing, and Quarantine VLANs.</p> <p>When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.</p>				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
G	Disabled	*	*	*	RFC 3576 Reauthentication Enabled
NOTES: NAC Manager supports RFC 3576 which provides for forced reauthentication (Force Reauth) of end-systems connected to an RFC 3576-capable switch. RFC 3576 defines new RADIUS messaging that allows the NAC Gateway to send Disconnect or Change of Authorization (CoA) RADIUS messages to the authenticating switch or AP to force reauthentication on a currently authenticated end-system.					

* = Any value.
 N/A = Not applicable.

General Considerations

- Gateway RADIUS Attributes to Send - Send RFC 3580 Only Feature.** This feature (configured in the Add/Edit Switches to NAC Appliance Group window) lets you specify that a NAC Gateway will send a VLAN (instead of a policy) via RFC 3580-defined RADIUS Tunnel attributes to the RFC 3580-enabled switches in your network. Keep in mind the following considerations when configuring this feature:
 - Send RFC 3580 Only is not supported on Matrix E7 Devices.** Matrix E7 devices should not be configured with the "Gateway RADIUS Attributes to Send" parameter set to RFC 3580 Only.
 - Send RFC 3580 Only does not support end-systems with static IP addresses.** The Send RFC 3580 Only feature is not-supported for end-systems with static IP addresses. This is because end-systems transitioned between VLANs must be assigned an IP address on the appropriate subnet to maintain IP connectivity to the network, which is facilitated dynamically through DHCP.
 - Send RFC 3580 Only requires a particular DHCP configuration for Active/Default Role port mode.** When the Send RFC 3580 Only feature is configured, the Active/ Default Role port mode on network devices requires a particular DHCP configuration. The DHCP lease time for the pool of IP addresses that corresponds to the default role's VLAN must be short (e.g. less than 1 minute) because the Active/Default Role port mode allows end-systems to obtain IP addresses via the DHCP protocol before they are authenticated to a VLAN.

- **Switch management fails with Send RFC 3580 Only and certain Auth Access Types.** Switch management via TELNET/WebView will fail with the following configuration in the Add/Edit Switches to NAC Appliance Group window:
 - Auth Access Type = "Management Access" or "Any Access"
 - Gateway RADIUS Attributes to Send = "RFC 3580 Only"This is because switches check the "mgmt" attribute in the Filter-ID for Telnet management. To avoid this problem, set the Auth Access Type to "Network Access."
- **Enable Port Link Control Option.** Port link control is required if you are using VLAN only (RFC 3580) switches or if you are using policy with VLANs on policy-enabled switches. When an end-system is transitioned between VLANs with a new VLAN being assigned to a switch port, the end-system is required to obtain a new IP address for the assigned VLAN. To do this, the NAC Gateway links down the port (using the ifAdmin MIB), waits the configured amount of time, and then links up the port, causing the end-system to make a new DHCP request and get a new IP address.
 - **Port Link Control is not supported on authentication-enabled switch ports providing connectivity to multiple end-systems.** Port link control should not be enabled for switches that are authenticating multiple users per port. This is because when a NAC Gateway is configured to return only the VLAN RADIUS attribute, the gateway will link down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. This action will interrupt IP connectivity of other authenticated end-systems on the port. If the switch is an Enterasys switch, protection is automatically provided by reading the number of users currently on the port prior to linking down an port.
 - **Port Link Control is only supported on Windows XP or later.** Port link control is only supported for end-users that are authenticating from end-systems that are running Windows XP or later. This is because when a NAC Gateway is configured to return only the VLAN RADIUS attribute, the gateway will link down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. However, other systems such as NT workstations, do not release their DHCP IP address when the port is linked down. To account for this scenario, you can disable port link control, set the NAC Profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address

pools that correspond to the VLAN(s) associated to the Quarantine and Assessing access policies, as well as the default VLAN associated to the unauthenticated state of the port, to a low value (e.g. 1 minute). This will force an end-system to send DHCP Request messages every 30 seconds while it is unauthenticated, being assessed, and quarantined. Upon passing assessment, the end-system will be dynamically assigned an IP address on the production VLAN shortly after assessment is complete, establishing connectivity to the network on the production VLAN.

- **NAC Gateway DHCP Snooping:**

- **Option 1: Locate the NAC Gateway on the same subnet as the DHCP server.** If the NAC appliance is in the same subnet (relay router interface) as the end-system, it may be able to hear ACK responses from the DHCP server, allowing it to have more accurate DHCP entries. However, the NAC appliance will **not** be able to hear ACK responses if the relay router (or DHCP server) sends unicast ACK responses directly to the end-system.

Note: Whether the ACK response is sent using unicast or broadcast is normally determined by how the end-system requests the packet. If the end-system sends out a DHCP discover/request with a unicast bootp flag, then the DHCP server (or relay router) will send the ACK response using unicast. This is typically what happens. Sometimes, the end-system can request the DHCP discover/request with a broadcast bootp flag set. In this case, the end-system will get the ACK response with broadcast, and the NAC appliance will hear the ACK response if it is in the same broadcast domain.

The benefit of using option 1 over the helper-address implementation described in option 2, is that the helper-address implementation only gets the requests from the end-systems which may or may not have the correct IP address. When a NAC Gateway learns a MAC/IP address pair, it sends a message to all other NAC Gateways, so only one NAC Gateway needs to live on each subnet with a DHCP server on it, to leverage this technique.

- **Option 2: Add the NAC Gateway IP address as a helper address on default gateway routers.** To increase the accuracy of the MAP-to-IP resolution, the NAC Gateway listens for DHCP traffic on port 67 and saves the MAC/IP address pairs it learns. In order to receive DHCP traffic, the IP address of any NAC Gateway must be added as a helper address on default gateway routers on the network. Routers allow

multiple IP helper address entries, so the NAC Gateway's IP address can be added along with the actual DHCP server IP addresses. When a NAC Gateway learns a MAC/IP address pair, it sends a message to all other NAC Gateways, so only one NAC Gateway IP address needs to be added.

- **Configure RADIUS settings on 3rd-party switches.** You must manually configure the RADIUS settings on your third-party switches communicating to the NAC Gateway. In addition, make sure that the shared secret on the switches matches the shared secret you entered in the Switch Configuration section on the [Credentials tab of the Appliance Settings window](#) or the override shared secret entered in the [Advanced Switch Settings window](#). This is the shared secret the switches will use to communicate with NAC Gateways.
- **NAC Gateways should not be selected for ASM search.** The NAC Gateway should **not** be used as a search device in ASM. ASM should be configured to search other devices in the network for the IP-to-MAC-to-port bindings, such as gateway routers for IP-to-MAC bindings and access edge switches for MAC-to-port information.
- **Configuring Agent-based Assessment Test Sets with Hotfix Checks.** When configuring an Agent-based test set to perform multiple hotfix checks, make sure that the Monitoring Interval is set to at least 5 minutes, so that the assessment agent does not take a lot of CPU cycles trying to monitor these settings.
- **Supported Web Browsers for end-systems connecting through NAC.** The following web browsers are supported for end-systems connecting to the network through Extreme Networks NAC:
 - Microsoft Edge and Internet Explorer version 11
 - Mozilla Firefox 34 and later
 - Google Chrome 33.0 and later
- **RADIUS Configuration on E1 Devices.** The NAC appliance will open an SSH/Telnet session on the E1 device and enable RADIUS by running a script of CLI commands. CLI credentials for the device will be obtained from the device profile and must be configured in the

Authorization/Device Access tool.

- **RADIUS Authentication and Accounting Configuration on ExtremeXOS Devices.** NAC uses CLI access to perform RADIUS configuration operations on ExtremeXOS devices. CLI credentials for the device will be obtained from the device profile and must be configured in the Authorization/Device Access tool.
- **RADIUS Accounting Configuration on Fixed Switching Devices.** NAC uses CLI to configure RADIUS accounting on Enterasys fixed switching devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). CLI credentials for the device will be obtained from the device profile and must be configured in the Authorization/Device Access tool. This does not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP. For more information, see [How to Enable RADIUS Accounting](#).

Considerations When Implementing Policy Roles

This section describes the communication that takes place between NAC appliances and end-systems connecting to the network. This communication should be taken into account when defining and deploying policy roles and rules on your network. It is particularly critical because certain policy roles and rules may discard traffic that is necessary for communication between the end-system and the appliance. For example, in a Guest policy role, NetBIOS traffic is probably discarded, but doing so could impact the MAC to IP resolution process.

Review the following information and verify that the policy roles and rules deployed on your network will allow the required communication between end-systems and your NAC appliances.

IP resolution via NetBIOS

MAC Resolution via NetBIOS

NAC Appliance UDP Port 137 <==> End-System Port 137

Remediation and Registration

NAC Appliance (TCP or UDP) Port 80 <==> End-System Port (determined on the client) - HTTP

NAC Appliance (TCP or UDP) Port 443 <==> End-System Port (determined on the client) - HTTPS

NAC Agent Discovery via HTTP

NAC Appliance Port TCP 8080 <==> End-System Port (determined on the client)

NAC Agent Heartbeat via HTTPS

NAC Appliance Port TCP 8443 <==> End-System Port (determined on the client)

NAC Agent-less Assessment

All ports determined by the selected test set.

The following software is optional and may be installed with agent-less Assessment:

SAMBA add-on enabled

TCP Ports 149 and 195, and UDP Ports 137 and 138.

End-System Reachability Test (Assessment Configurations - does not apply to agent-based assessment)

ICMP Ping Test => ICMP Protocol (1), ICMP Type (8)

TCP Ping Test => Default TCP Ports: 21, 22, 23, 25, 79, 80, 111, 135, 139, 445, 497, 515, 548, 1025, 1028, 1029, 1917, 5000, 6000, 9100

ExtremeWireless Wireless Controller Configuration

- The NAS IP address used for the wireless controller should be either the management IP address or an IP address of one of its physical data ports, or all zeros to force NAC to use the source IP. If a logical IP address is used, then NAC will be unable to reauthenticate end-systems.
- If you have configured Assisted Remediation, you must perform the following steps if your network includes wireless controllers:
 - Enable the "ToS override for NAC" option configured through Wireless Manager in the Edit WLAN Service > Authentication Mode Configuration > Settings window.
 - If Policy Manager is **not** being used to configure policy on the wireless controller, use Wireless Manager to manually add the following rule to the VNS Quarantine, Assessing, and Unregistered filters to allow HTTP traffic to pass through (IN/OUT) the controller when end-systems are proxied to the Internet during remediation.
`0.0.0.0/0 tcp port 80 (Allow traffic In/Out)`

- If Policy Manager is being used to configure policy for the wireless controller, use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in your Quarantine, Assessing, and Unregistered policy roles. The rule would be a traffic classification type "IP TCP Port Destination" with the TCP type set to HTTP (80) and the Access Control set to "Permit Traffic." For more information, see the Help topic [How to Set Up Assessment Remediation](#).

DNS Proxy Functionality for Registration and Remediation

NAC Gateway appliances provide DNS proxy functionality for use in networks that are deploying registration and/or remediation, but cannot configure the policy-based routing that is required to redirect network traffic to the web portal. (See [How to Set Up Registration](#) or [How to Set Up Assessment Remediation](#) for more information on policy-based routing.) Using DNS proxy, any end-system that needs to be redirected to the remediation and registration web portal will have its DNS packets spoofed to direct all web page requests to the NAC Gateway appliance. This allows networks that do not have a router to deploy registration and remediation.

Basic Operation

To set up DNS proxy, the NAC appliance is configured as a secondary DNS server in the DHCP scope, in addition to the primary DNS server on the network. When an end-system is required to register or undergo remediation, access to the primary DNS server is blocked and the end-system sends its DNS requests to the DNS proxy on the NAC Gateway appliance.

The DNS proxy must determine whether to spoof the packet or forward the request to the primary DNS server. If the end-system is unregistered or quarantined, the DNS proxy will spoof the DNS packet and send back a DNS response to the end-system with the NAC appliance IP address. This will redirect the end-system traffic to the web portal where the end user can register or remediate. Once the end user has registered or remediated their end-system, their DNS requests will be forwarded to the primary DNS server.

For third-party devices, a dynamic ACL is configured to block access to the primary DNS server for end-systems undergoing registration or remediation. This will cause the DNS requests to be sent to the DNS proxy. The DNS proxy will determine whether spoofing is necessary or not by checking the state of the

end-system in the database. If the end-system is unregistered or quarantined, the DNS proxy will spoof the DNS packet.

To allow access to hosts or domains for any protocol other than http, you must add the host or domain to the list of [allowed web sites](#) configured in the Network Settings view of the NAC Edit Portal Configuration window. The DNS proxy will use this list of allowed domains to determine if the end-system is allowed access to the requested domain. This can be useful if you want to allow end-systems to perform specific functions such as anti-virus updates or software updates that run over TCP/UDP ports.

You can also define post authorization assessment behavior using DNS proxy. End-systems in the scan state will be granted access according to the [assessment settings](#) in your NAC profile.

- If an assessment policy is **not** defined, the user is allowed access while being scanned.
- If an assessment policy is defined for initial assessment only, the user is allowed access if they passed the last scan. If the first or last scan resulted in quarantine, the user is redirected to the NAC Gateway.
- If an assessment policy is defined for all assessments, the user is redirected to the NAC Gateway.

Enabling DNS Proxy

Use the following steps to enable DNS proxy:

1. Enable the distributed end-system cache on the NetSight Server. In NAC Manager, go to Tools > Options > Advanced Settings > [End-System Mobility option](#). When you enable this option, you must click the **Reload** button to reload the cache configuration on the NetSight server.
2. Enable Registration and/or Remediation via the [Edit NAC Configuration window](#) and enforce. Note that it is important to wait a couple of minutes after enabling or disabling registration and remediation for the DNS proxy to be notified of the enable/disable change, and to start or stop proxying DNS requests.
3. Uncomment the "#DNS_PROXY_ENABLE=true" in the config.properties file on the NAC appliance by deleting the # symbol at the beginning of the line.
4. Restart the NAC appliance using the `nacct1 restart` command.

5. Start the DNS Proxy process on the appliance using the `/opt/nac/server/dnsProxy.sh start` command.

Backup DNS Server

Because the DNS proxy forwards DNS requests to the primary DNS server, it is important to configure a backup DNS server on your network, in case the primary server is down. The DNS proxy polls the primary DNS server every minute. If the primary server is down, a backup DNS server is used. If both servers are down, all DNS requests forwarded by the DNS proxy will be dropped.

Troubleshooting

DNS proxy error messages are logged in the `/var/log/dnsProxy.log` file on the NAC appliance. You can enable diagnostics for DNS proxy by going to the NAC appliance administration web page and enabling the DNS Proxy diagnostic group to provide troubleshooting information. Launch the NAC appliance administration web page by right-clicking on the NAC appliance in the NAC Manager left-panel tree and selecting `WebView` or by using the following URL: `https://<NACApliancIP>:8443/Admin`. The default user name and password for access to this web page is "admin/Extreme@pp." Click on the `Diagnostics` page and then the `Server Diagnostics` page. View the output in the `/var/log/dnsProxy.log` file or on the `Log Files > Server Log` web page.

NAC Manager Concepts

This Help topic explains some of the concepts you'll need to understand in order to make the most effective use of NAC Manager.

Information on:

- [Overview of NAC Manager](#)
- [Extreme Access Control Engines](#)
 - [Use Scenario](#)
 - [NAC VPN Deployment](#)
- [NAC Manager Structure](#)
 - [NAC Configuration](#)
 - [Rule Components](#)
 - [NAC Profiles](#)
 - [AAA Configurations](#)
 - [Portal Configurations](#)
- [Access Policies](#)
- [Registration](#)
- [Assessment](#)
 - [Assessment Remediation](#)
- [End-System Zones](#)
- [Enforcing](#)
- [MAC Locking](#)
- [Notifications](#)
- [Automated Security Manager Blacklist](#)
- [Mobile IAM](#)

Overview of NAC Manager

Extreme Networks NAC is a centralized network access control solution that combines authentication, vulnerability assessment, and location services to authorize network access and determine the appropriate level of service for an end-system. The NAC solution ensures that only valid users and devices with

appropriate security postures at the proper location are granted access to your network. For end-systems which are not compliant with defined security guidelines, the NAC solution provides assisted remediation, allowing end users to perform self-service repair steps specific to the detected compliance violation.

NAC Manager is the management component in the Extreme Networks NAC solution. NAC Manager and NAC engines work in conjunction to implement network access control. NAC Manager provides one centralized interface for configuring the authentication, authorization, assessment, and remediation parameters for your Access Control engines. After these configurations are enforced, the Access Control engines can detect, authenticate, assess, authorize, and remediate end-systems connecting to the network according to those configuration specifications.

NAC Engines

The Access Control engine is required for all Extreme Networks NAC deployments. It provides the ability to detect, authenticate, and effect the authorization of end devices attempting to connect to the network. It also integrates with, or connects to, vulnerability assessment services to determine the security posture of end-systems connecting to the network. Once authentication and assessment are complete, the Access Control engine effects the authorization of devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results.

If authentication fails and/or the assessment results indicate a non-compliant end-system, the Access Control engine can either totally deny the end-system access to the network or quarantine the end-system with a highly restrictive set of network resources, depending on its configuration. The Access Control engine also provides the remediation functionality of the NAC solution by means of the remediation web server that runs on the engine. Remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations.

Use Scenario

The Access Control Gateway engine provides out-of-band network access control for networks where intelligent wired or wireless edge infrastructure

devices are deployed as the authorization point for connecting end-systems. End-systems are detected on the network through their RADIUS authentication interchange. Based on the assessment and authentication results for a connecting device, RADIUS attributes are added/modified during the authentication process to authorize the end-system on the authenticating edge switch. Therefore, the NAC Gateway may be positioned anywhere in the network topology with the only requirement being that IP connectivity between the authenticating edge switches and the NAC Gateways is operational.

It is important to note that if the wired edge of the network is non-intelligent (unmanaged switches and hubs) and is not capable of authenticating and authorizing locally connected end-systems, it is possible to augment the network topology to allow implementation of inline NAC with the NAC Gateway. This can be accomplished by adding an intelligent edge switch that possesses specialized authentication and authorization features. The Extreme Networks K-, S-, or N-Series switch is capable of authenticating and authorizing numerous end-systems connected on a single port through its Multi-User Authentication (MUA) functionality, and may be positioned upstream from non-intelligent edge devices to act as the intelligent edge on the network. In this configuration, the K-, S-, or N-Series switch acts as the intelligent edge switch on the network, although not physically located at the access edge.

For end-systems connected to EOS policy-enabled switches, a *policy role* is specified in NAC Manager (policy roles are defined and distributed to those switches on the [Control > Policy tab](#)) to authorize connecting end-systems with a particular level of network access. For end-systems connected to RFC 3580-compliant switches (Enterasys and third-party), a VLAN is specified in NAC Manager to authorize connecting end-systems with a particular level of network access, facilitated using dynamic VLAN assignment via Tunnel RADIUS attributes.

When a user or device attempts to connect to the network, the end-system is authenticated and assessed according to configurations defined in NAC Manager. NAC Manager uses the results of the authentication and assessment to determine if that device meets the requirements for a compliant end-system. If the results of the authentication and security assessment are positive, NAC Manager authorizes the end-system with network access by assigning a designated policy role or VLAN on the switch port to which the end-system is connected. If the result of the security assessment is negative, NAC will restrict network access by assigning the user or device to a Quarantine policy role or VLAN on the switch port until the end-system is remediated and brought into a compliant state. If the result of the authentication is negative, NAC can deny all

network access for the endpoint as an invalid device or user on the network, setting the switch port to the unauthenticated state.

Depending on the engine model, the Access Control Gateway provides either on-board (integrated) vulnerability assessment server functionality and/or the ability to connect to external assessment services, to determine the security posture of end-systems connecting to the network. (On-board assessment requires a separate license.)

The number of NAC Gateways you deploy on the network depends on the number of end-systems on the network. The following table displays the number of end-systems supported per NAC Gateway model. Use this table to help determine the number of gateways to deploy.

Model	Number of End-Systems Supported	Notes
IA-A-20	6000	Configured NAC Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	4500	Configured NAC Features: All features excluding Assessment.
	3000	Configured NAC Features: All features including Assessment.
IA-A-300	12000	Configured NAC Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	9000	Configured NAC Features: All features excluding Assessment.
	6000	Configured NAC Features: All features including Assessment.
IA-V	See Notes	The IA-V is included with the Extreme Management Center Advanced (NMS-ADV) license and is used in conjunction with a NAC Enterprise license (IA-ES-12K). For more information, see NAC Enterprise Licensing .
NAC-V-20	3000	The NAC-V-20 is a virtual engine and requires a NAC VM license in the Management Center Server. For more information, see the Suite-Wide Tools Server Information Window Help topic section on NAC VM license.
NAC-A-20	3000	
SNS-TAG-ITA	3000	
SNS-TAG-HPA	3000	
SNS-TAG-LPA	2000	

It is important to configure NAC Gateway redundancy for each switch. This is achieved by configuring two different Access Control Gateway engines as a primary and secondary gateway for each switch. When connection to the primary gateway engine is lost, the secondary gateway is used. Note that this configuration supports redundancy but not load-sharing, as the secondary gateway engine is only used in the event that the primary gateway becomes unreachable. To achieve redundancy with load-sharing for two NAC Gateways, it is suggested that one half of the switches connecting to the gateways are configured with "NAC Gateway A" as the primary and "NAC Gateway B" as the secondary, and the second half are configured with "NAC Gateway B" as the primary and "NAC Gateway A" as the secondary. In this way, NAC Gateways are configured in redundant active-active operation on the network.

NAC VPN Deployment

Extreme Networks NAC provides out-of-band support for VPN remote access with specific VPN concentrators (see the Release Notes for a list of supported VPN concentrators). Out-of-band VPN support provides visibility into who and what is accessing the network over VPN. If RADIUS accounting is used, you will have the additional ability to determine who was on the network at any given time. In the VPN remote access use scenario, the VPN concentrator acts as a termination point for remote access VPN tunnels into the enterprise network. In addition, the Extreme Networks Access Control Gateway engine is deployed to authenticate and authorize connecting end-systems on the network and implement network access control.

The process begins when the user's end-system successfully establishes a VPN tunnel with the VPN concentrator, and the VPN concentrator sends a RADIUS authentication request with the associated credentials to the Access Control Gateway. The Access Control Gateway proxies the authentication request to a backend authentication server (RADIUS or LDAP) to validate the identity of the end user/device or can authenticate with a local password repository within NAC. If authentication fails, the NAC Gateway can deny the end-system access to the network by sending a RADIUS access reject message to the VPN concentrator.

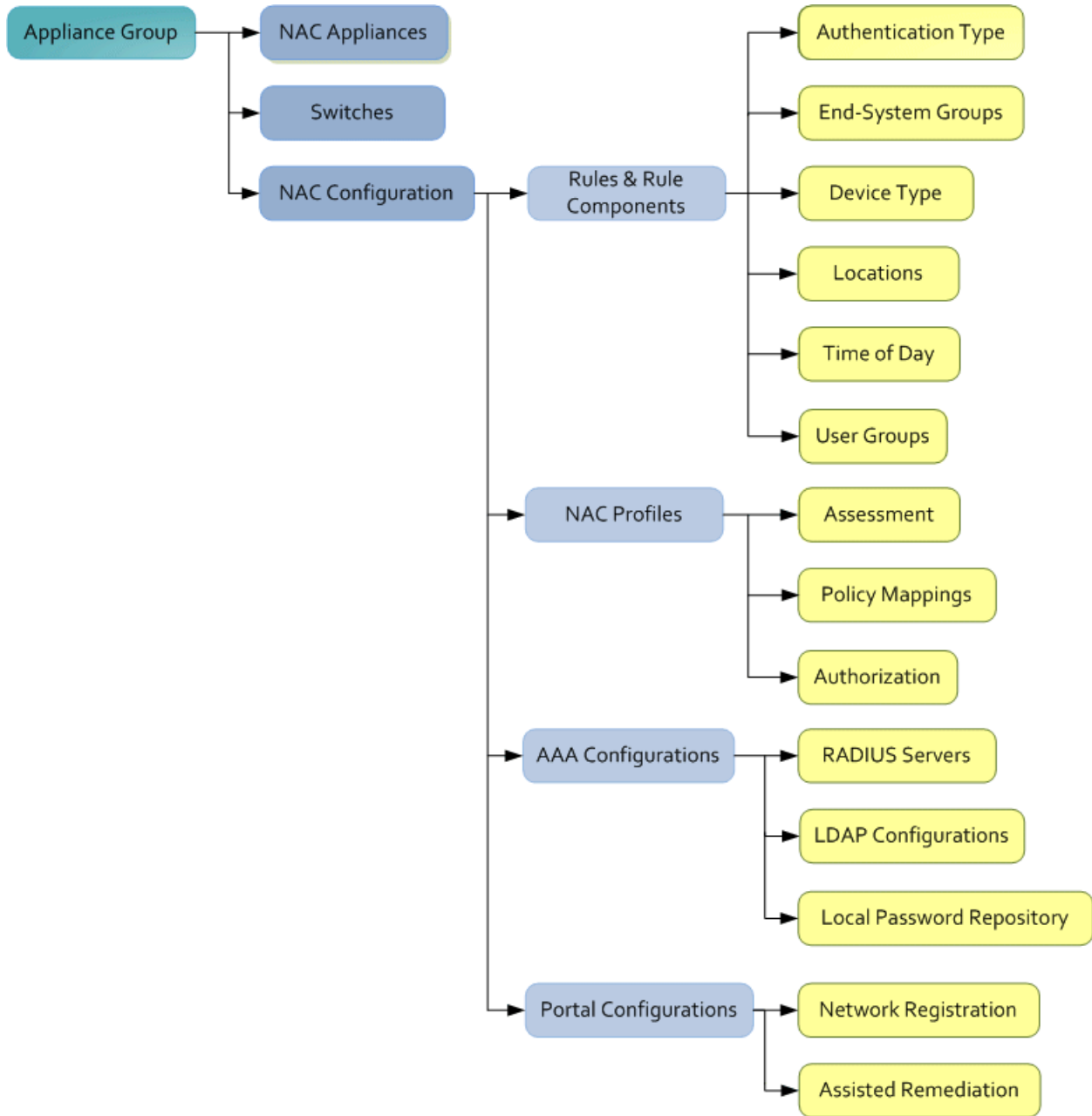
After the end-system is authenticated, the NAC Gateway requests an assessment of the end-system, if assessment is configured. Once authentication and assessment are complete, the NAC Gateway allocates the appropriate access control to the end-system based on authentication and/or assessment results. Access control can be implemented using one of two methods. With the first method, access control is applied directly at the VPN concentrator via

RADIUS response attributes, if the VPN concentrator supports this. For example, with a Cisco ASA security engine, this can be accomplished by using the filter-ID response attribute to specify the name of a valid ACL.

With the second method, an Extreme Networks K-Series, S-Series, or N-Series device is added between the VPN's internal port and the internal network as a Policy Enforcement Point (PEP). This allows the NAC Gateway to provide a more granular access control mechanism using IP to Policy Mappings. This method must be used if you are implementing remediation on your network. If the end-system fails assessment, the NAC Gateway can apply a Quarantine policy on the PEP to quarantine the end-system. When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that provides steps for the user to execute in order to achieve compliance. After executing the steps, the end user can reattempt network access and start the process again.

NAC Manager Structure

The following diagram shows the structure of NAC Manager components. At the top is the Engine Group, which is a "virtual container" that includes the Access Control engines, the switches in the network, and the NAC configuration that will be utilized. Most NAC deployments will have only one engine group configured for the network. And in that case, the "engine group" is the All Access Control Engines folder in the left-panel tree. However, an example of a network that may require separate engine groups would be a network in which there are remote offices that wish to have completely different NAC functionality than the main branch. These remote offices would need to have their own Access Control engines in a separate group. In this case, the separate engine groups are listed in the left-panel tree.



NAC Configuration

The NAC Configuration lets you manage the end user connection experience and control network access based on a variety of criteria. NAC Manager comes with a default NAC Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

The NAC Configuration determines what NAC Profile will be assigned to an end-system connecting to the network. It contains an ordered list of rules that are used by the configuration to assign a NAC Profile to a connecting end-system based on rule criteria. It also specifies the Default Profile which serves as a "catch-all" profile for any end-system that doesn't match one of the rules. By default, all end-systems will match the Default Profile.

When an end-system connects to the network, the rules are evaluated in a top-down fashion, similar to the way an ACL would be evaluated. End-systems that do not match any of the rules are assigned the Default Profile.

Rule Components

The rules defined in a NAC Configuration provide very granular control over how end-systems are treated as they come onto the network. The following criteria can be used to define the rules used in your NAC Configuration:

- Authentication Type - for example, 802.1X or MAC authentication.
- End-System Groups - allow you to group together devices that have similar network access requirements or restrictions. For example, a list of MAC addresses, IP addresses, or hostnames.
- Device Type - allow you to group together end-systems based on their device type. The device type can be an operating system family, an operating system, or a hardware type, such as Windows, Windows 7, Debian 3.0, and HP Printers.
- Locations - allow you to specify network access requirements or restrictions based on the network location where the end user is connecting. For example, a list of switches, wireless devices, switch ports, or SSIDs.
- Time of Day - allow you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, traditional work hours or weekend work hours.
- User Groups - allow you to group together end users having similar network access requirements or restrictions. For example, a list of usernames, an LDAP users group, or a RADIUS user group.

For more information, see the [Manage Rule Groups window](#).

NAC Profiles

NAC Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies that will be applied to end-systems for network authorization, depending on authentication and assessment results.

NAC Manager comes with ten system-defined NAC Profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

If desired, you can edit these profiles or you can define your own profiles to use for your NAC Configurations. For more information, see the [Manage NAC Profiles window](#).

AAA Configurations

The AAA Configuration defines the RADIUS servers, LDAP configurations, and Local Password Repository that provide the authentication and authorization services for all end-systems connecting to your Access Control engines. NAC Manager comes with a default Basic AAA Configuration that ships with each Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired. For more information, see the [Edit Basic AAA Configurations window](#).

Portal Configurations

If your network is implementing [Registration](#) or [Assisted Remediation](#), the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process. Access Control engines are shipped with a default Portal Configuration. You can use this default

configuration as is, or make changes to the default configuration, if desired. For more information, see the [Portal Configuration](#) Help topic.

Access Policies

Access policies define the authorization level that the NAC assigns to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies used in NAC Manager: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. In your NAC Profiles, these access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network. How access policies are implemented depends on whether your network utilizes Access Control Controller engines and/or Access Control Gateway engines.

For end-systems connected to EOS policy-enabled switches, Access Control Gateway engines inform the switch to assign a policy role to a connecting end-system, as specified by the access policy. These policy roles must be defined on the [Control > Policy tab](#) and enforced to the EOS policy-enabled switches in your network.

For end-systems connected to RFC 3580-enabled switches, policy roles are associated to a VLAN ID. This allows your NAC Gateways to send a VLAN ID instead of a policy role to those switches using Tunnel RADIUS attributes.

For Access Control Controller engines, authorization of the end-system is implemented locally on the Access Control Controller engine by assigning a policy role to the end-system, as specified by the access policy. In this scenario, all policy roles must be defined in the Access Control Controller policy configuration.

Here is a description of each NAC Manager access policy, and some guidelines for creating corresponding policy roles in Policy Manager.

Accept Policy: The Accept access policy is applied to an end-system when it has been authorized locally by the NAC Gateway and when an end-system has passed an assessment (if an assessment was required), or if the Accept policy has been configured to replace the Filter-ID information returned in the RADIUS authentication messages. For EOS policy-enabled switches, a corresponding policy role (created in Policy Manager) would allocate the appropriate set of network resources for the end-system depending on their role in the enterprise. For example, you might associate the Accept policy in NAC Manager to the "Enterprise User" role that is defined in the on the [Control > Policy tab](#)

demo.pmd file. For RFC 3580-compliant switches, the Accept access policy may be mapped to the Production VLAN. Access Control Controllers are shipped with a default policy configuration that includes an Enterprise User policy role.

Quarantine Policy: The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. For EOS policy-enabled switches, a corresponding Quarantine policy role (created in Policy Manager) should deny all traffic by default while permitting access to only required network resources such as basic network services (e.g. ARP, DHCP, and DNS) and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Quarantine access policy may be mapped to the Quarantine VLAN. Access Control Controllers are shipped with a default policy configuration that includes a Quarantine policy role.

Failsafe Policy: The Failsafe access policy is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place. For EOS policy-enabled switches, a corresponding policy role (created in Policy Manager) should allocate a nonrestrictive set of network resources to the connecting end-system so it can continue its connectivity on the network, even though an error occurred in the NAC Solution operation. For RFC 3580-compliant switches, the Failsafe access policy may be mapped to the Production VLAN. Access Control Controllers are shipped with a default policy configuration that includes a Failsafe policy role.

Assessment Policy: The Assessment access policy may be used to temporarily allocate a set of network resources to end-systems while they are being assessed. For EOS policy-enabled switches, a corresponding policy role (created in Policy Manager) should allocate the appropriate set of network resources needed by the Assessment server to successfully complete its end-system assessment, while restricting the end-system's access to the network.

Typically, the Assessment access policy allows access to basic network services (e.g. ARP, DHCP, and DNS), permits all IP communication to the Assessment servers so the assessment can be successfully completed (using destination IP address "Permit" classification rule), and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Assessment access policy may be mapped to the Quarantine VLAN. Access Control Controllers are shipped with a default policy configuration that includes an Assessing policy role.

It is not mandatory to assign the Assessment policy to a connecting end-system while it is being assessed. The policy role received from the RADIUS server or the Accept policy can be applied to the end-system, allowing the end-system immediate network access while the end-system assessment is occurring in the background. In this case, the policy role or Accept policy (or the associated VLAN for RFC 3580-compliant switches) must be configured to allow access to the appropriate network resources for communication with the Assessment servers.

NOTE: The Assessment server sends an ICMP Echo Request (a "ping") to the end-system before the server begins to test IP connectivity to the end-system. Therefore, the Assessment policy role, the router ACLs, and the end-system's personal firewall must allow this type of communication between end-systems and Assessment servers in order for the assessment to take place. If the Assessment server cannot verify IP connectivity, the Failsafe policy will be assigned to the end-system.

For more information, refer to the [How to Set Up Access Policies](#) Help topic.

Registration

The Extreme Networks NAC Solution provides support for Registration, a solution that forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network, without requiring the intervention of network operations. This means that end users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations has visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network without requiring the deployment of backend authentication and directory services to manage these users. This binding between user identity and machine is useful for auditing, compliance, accounting, and forensics purposes on the network.

End-system or user groups may be configured to exempt certain devices and users from having to register to the network, based on authentication type, MAC address, or user name. For example, a end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

The Registration solution has minimal impact on the end user's experience by initially redirecting guests, contractors, partners, students, or other pre-defined end users to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is

permitted access, and possibly assessed for security posture compliance checking, until the registration is administratively revoked.

Registration is supported on Access Control Gateway engines and/or Layer 2 Access Control Controller engines. (Registration is not supported on the Layer 3 Access Control Controller engines.) Registration provides flexibility in implementation by offering the following capabilities:

- Determine "valid" end users by prompting each end user for a username with additional information such as full name and e-mail address, or a username and password (e.g. e-mail address and student ID number) which can be validated against an existing database on the network.
- Allow end users to register to the network when approved by a "sponsor" who is an internal trusted user to the organization. This is referred to as "Sponsored Registration." With sponsored registration, end users are only allowed to register to the network when approved by a sponsor. Sponsorship can provide the end user with a higher level of access than just guest or web access and allows the sponsor to fine-tune the level of access for individual end users.
- Configure the introductory message for the Registration web page (displayed to end-systems before registering to the network) to state that the end user is agreeing to the Acceptable Use Policy for the network upon registering their device.
- Specify the maximum number of registered MAC addresses per user.
- Control areas on the network where Registration is enabled.
- Provide a web-based administrative interface served over HTTPS where registrations may be viewed, manually added, deleted, and modified by administrators and sponsors without requiring access to NAC Manager.

The Extreme Networks NAC Solution utilizes a Registration Web Server installed on the Access Control engine to provide this registration functionality to end-systems. Note that a Access Control engine may implement both assisted remediation and registration concurrently.

There are specific network configuration steps that must be performed when using Registration in your NAC Solution. In addition, you must configure Registration in NAC Manager. For more information, see [How to Set up Registration](#).

How Registration Works

Here is a description of how Registration works in the Extreme Networks NAC Solution:

- An unregistered end-system attempts to connect to the network and is assigned the unregistered access profile without being assessed by the Access Control engine. For example, if connected to a Layer 2 Access Control Controller, the end-system may be assigned to the "Unregistered" policy as defined in the Access Control Controller's default policy configuration. If connected to an EOS policy-enabled switch, the end-system may be assigned to the "Unregistered" policy as defined in on the [Control > Policy tab](#) and enforced to the policy-enabled switches. Or, if connected to an RFC 3580-compliant switch, the end-system may be assigned to the "Unregistered" VLAN.
- The user on the unregistered end-system opens up a web browser to any URL and is redirected to the Registration Web Page served by the Access Control engine.
- The end user registers its end-system on the network by entering information such as username, full name, e-mail, and possibly a password or sponsor's email address into the Registration Web Page, and clicking the "Complete Registration" button.
- The Registration Web Server assigns the end user to an end-system group based on the Registration Behavior configured in the NAC Configuration.
- The end-system is then automatically re-authenticated to the network by the Access Control engine. Upon re-authentication, the end-system is authenticated, assessed, and authorized as defined by the profile specified in the NAC Configuration for the newly registered system. If the profile specifies to assess the end-system, an assessment of the end-system will take place at this time.

Assessment

The Extreme Networks NAC Solution integrates with assessment services to determine the security posture of end-systems connecting to the network. It uses assessment servers to assess and audit connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail

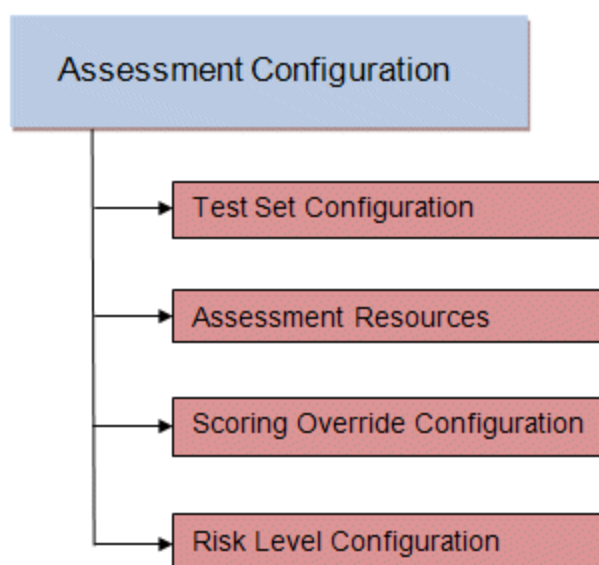
assessment can be dynamically quarantined with restrictive network access to prevent security threats from entering the network.

When an assessment is performed on an end-system, a *Health Result* is generated. For each health result, there may be several *Health Result Details*. A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 1 to 10, and based on this score, the health result is assigned a risk level. NAC Manager uses this risk level to determine whether or not the end-system will be quarantined.

In addition, assessment tests are assigned a *scoring mode* which determines whether the resulting health result detail is applied towards the quarantine decision, or is used only for informational or warning purposes. Informational health result details can be used to gather information about the security risks on your network, while warning health result details allow you to notify end users when they have security risks that should be remediated. Informational or warning health result details have scores, however these health result details do not impact the end-system's overall risk level.

NAC Manager lets you create multiple *assessment configurations* that can define different assessment requirements for end-systems. Assessment configurations define the following information:

- What assessment tests to run (determined by the selected test sets).
- What resources to use to run the tests (determined by the selected Assessment Resources).
- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).



Test sets let you define what type of assessment to execute, what parameters to pass to the assessment server, and which assessment server resources to use. NAC Manager provides three default test sets; one for each type of assessment agent that is either supplied or supported by NAC Manager. You can use these default test sets "as is" or edit them, if desired.

When you define your assessment server resources for a test set, you can specify to balance the assessment load between your all your assessment servers, or, you can specify an assessment server pool. For example, if you have four Nessus assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, in your test set configuration you can specify which server pool that test set should use.

You can use risk level and scoring override configurations to define how each assessment configuration will interpret an end-system's health results. The risk level configuration determines what risk level will be assigned to an end-system (high, medium, or low) based on the end-system's health result details score. The scoring override configuration lets you override the default score and scoring mode assigned to a particular assessment test ID.

Once you have defined your assessment configurations, they are available for selection when creating your NAC Profiles. In addition, NAC Manager provides a default assessment configuration that is already set up with default assessment parameters and is ready to use in your NAC Profiles.

Before beginning to configure assessment on your network, you should read through the following information presented in the NAC Manager online Help.

- [How to Set up Assessment](#) - Provides information on the steps that must be performed in NAC Manager prior to deploying assessment on your network, including managing your assessment servers and adding external assessment servers. It also includes basic information on how to use the default assessment configurations provided by NAC Manager, and enable assessment for your NAC Configuration.
- [NAC Assessment Phased Deployment Guide](#) - This guide describes the phased approach to introducing assessment into your NAC deployment using Informational, Warning, and Quarantine assessment. The guide also provides information on NAC Manager tools that can be used to monitor and evaluate assessment results, and diagnose and troubleshoot problems.
- [How to Configure Assessment](#) - Provides step-by-step instructions for configuring assessment using the phased approach described in the NAC Assessment Phased Deployment Guide. Instructions are provided for configuring phased assessment using agent-less or agent-based assessment, or a combination of both.
- [How to Deploy Agent-Based Assessment](#) - If you are deploying agent-based assessment, this Help topic provides the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.
- [How to Set Up Assessment Remediation](#) - Because Warning and Quarantine assessment provides end-system remediation, you must enable remediation for your NAC Configuration. This Help topic provides the specific steps that must be performed when setting up assisted remediation in your network.

Assessment Remediation

Remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. The process takes place when an end-system connects to the network and assessment is performed. End users whose systems fail assessment are notified that their systems have been quarantined,

and are instructed in how to perform self-service remediation specific to the detected compliance violation. Once the remediation steps have been successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

The Extreme Networks NAC Solution implements local Remediation Web Server functionality to provide web notification to end users indicating when their end-systems are quarantined and what remediation steps the end user must take. The Remediation Web Server is installed on the Access Control engine.

There are specific network configuration steps that must be performed when using assisted remediation in your NAC Solution. In addition, you must configure assisted remediation in NAC Manager. For more information, see [How to Set up Assessment Remediation](#) and [Portal Configuration](#) Help topics.

How Remediation Works

Here is a description of how assisted remediation works in the Extreme Networks NAC Solution:

- An end-system connects to the network (where assessment has been configured) and is authorized with the level of network access defined by the Assessment access policy configuration.
- The end-system is assessed by the assessment server for security threats and vulnerabilities.
- When the end-system opens a web browser to any web site, the HTTP traffic is redirected to the Access Control engine and a web page indicating that the end-system is currently being assessed is displayed.
- When the assessment is complete, the assessment server sends the results to the Access Control engine. If the end-system failed assessment, the end-system is authorized with the level of network access defined by the Quarantine access policy configuration.
- When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to the Access Control engine.
- The Access Control engine returns a web page formatted with self-service remediation information for the quarantined end-system. This web page indicates the reasons the end-system was quarantined and the remediation steps the end user must take.

- After taking the appropriate remediation steps, the end-user clicks a button on the web page and attempts to reconnect to the network. A re-assessment of the end-system is initiated. If the end-system is now compliant with network security policy, the Access Control engine authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the Quarantine access policy is again utilized to restrict the authorization level of the end-system and the process starts again.
- After a specified number of attempts and/or maximum time to remediate have expired, the end user may be redirected to a web page requiring them to contact the helpdesk for further assistance, and a notification is sent to the helpdesk system with information regarding the non-compliant end-system.

End-System Zones

NAC Manager end-system zones allow you to group end-systems into zones, and then limit a user's access to Management Center end-system information and configuration based on those zones.

End-system zones are configured and managed in NAC Manager, and are enforced for Management Center end-system information and configuration.

When an end-system authenticates to the network, NAC rules are used to assign a NAC profile and an end-system zone to the end-system. This allows you to use a variety of rule components (such as End-System Groups, Location Groups, and User Groups) to determine which zone an end-system should be assigned to.

You can create any number of end-system zones in your network. An end-system can only be assigned to one zone (but does not have to be assigned to a zone). You can view which zone an end-system is currently assigned to in the end-systems table in NAC Manager and Management Center.

A user's authorized zones are determined by their Management Center user group membership. User groups are created and configured in the Authorization/Device Access Tool (accessed from the Tool menu), and authorized zones are assigned to each user group in NAC Manager. For instructions, see [How to Configure End-System Zones](#).

In addition to using end-system zones, you can also limit a user's access to Management Center operations by assigning authorized rule groups. Whenever

a user initiates a change to a rule group, such as adding or removing an end-system to or from a group, a check is performed to verify that the user is authorized to change that rule group. Similar to end-system zones, a user's authorized rule groups are determined by their Management Center user group membership.

A third component that should be taken into consideration is the ability to limit user access to Management Center using authorization group capabilities. For example, you can assign a user group the OneView (Management Center) End-Systems Read Access capability to allow read-only access to Management Center end-system information, and use end-system zones to limit which end-systems can be viewed. You can assign a user group the OneView (Management Center) End-Systems Read/Write Access capability to allow the ability to modify rule groups, and use rule group authorization to limit which rule groups the user can perform these operations on.

Capabilities are assigned to user groups using the Authorization/Device Access Tool. The Management Center Administrator group is always assigned all capabilities.

For more information, see [How to Configure User Access to Extreme Management Center Applications and Authorization Group Capabilities in the Suite-Wide Tools Help](#).


End-System Zone Use Cases


Here are several network scenarios where using end-system zones could be beneficial.

- **A Service Provider with multiple tenants.** If a service provider serves multiple tenants and each tenant has a clearly delineated set of switches, user access can be configured to allow each tenant's IT staff to only view the end-systems connecting to their own switches.
- **A large enterprise with network administrator groups.** In a large enterprise where specific groups of network administrators are responsible for specific groups of switches on shared engines, user access can be configured so that each administrator can view reports and other information only for their switches and end-systems.
- **A large business segmented by business function.** In a large enterprise where division of control is not closely tied to switches or engines, user access can be configured so that administrators only have the ability to view and manage the appropriate end user groups.

In each of these scenarios, a restricted set of authorization group capabilities must be used to prevent users from viewing and accessing information that may not pertain to their area.

Enforcing

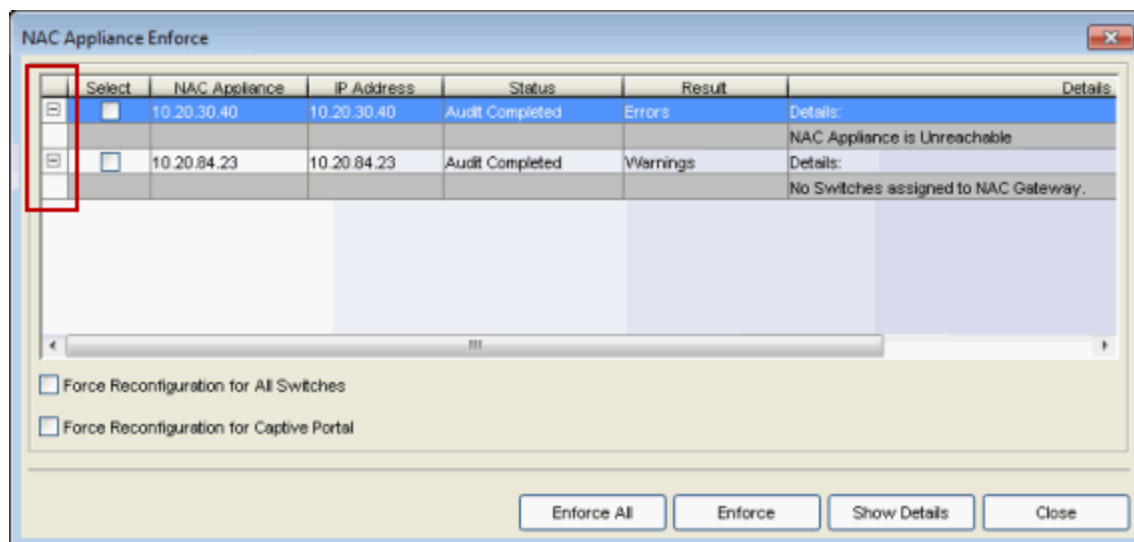
In NAC Manager, enforcing means writing NAC configuration information to one or more Access Control engines. Any time you add or make a change to the NAC Configuration, the engines need to be informed of the change through an enforce, otherwise the changes will not take effect. When an engine needs to be enforced, the Enforce icon  appears on that engine in the left-panel tree.

To enforce, use the Enforce All button in the toolbar  or the Tools > Enforce All menu option, both of which write the information to all the Access Control engines. You can enforce to an individual engine or engine group by right-clicking the engine or group in the left panel and choosing **Enforce** or **Enforce Group** from the menu.

TIP: For a preview of what will be enforced/updated on an individual engine, right-click the engine and choose **Enforce Preview** from the menu.

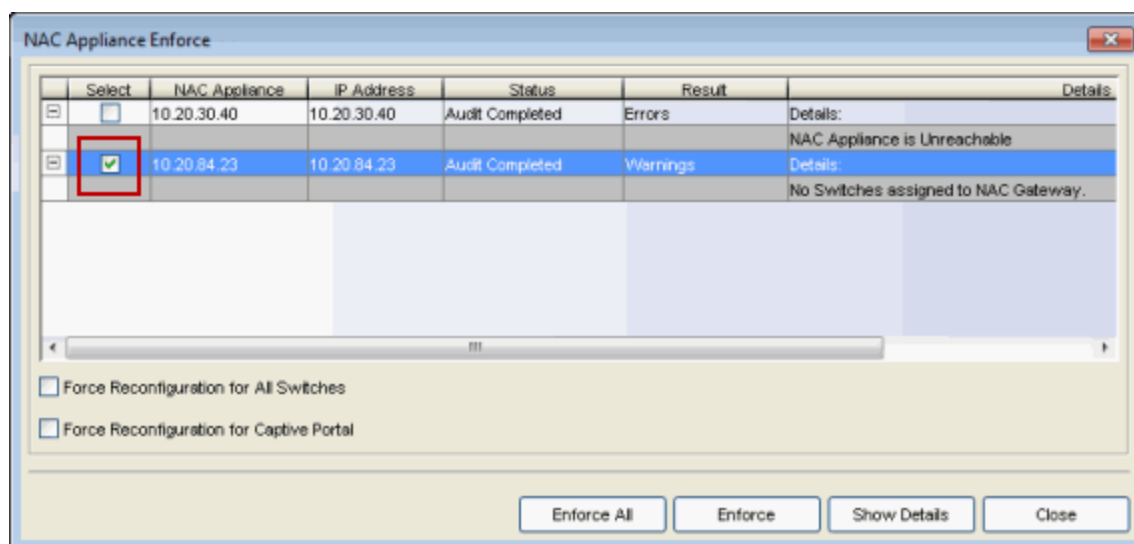
The enforce operation is performed in two stages: first an engine configuration audit is performed and then the actual enforce to engines is performed.

The configuration audit takes place automatically after you start the enforce operation. It looks for a wide-range of engine configuration problems including a review of the NAC Configuration, NAC Profile, rule configuration, AAA configuration, and portal configuration. The audit results are displayed in the Enforce window, allowing you to view any warning and error information. To see warning or error details, use the + icon in the left column to expand the Details information (as shown below) or click **Show Details** to open the information in a new window.



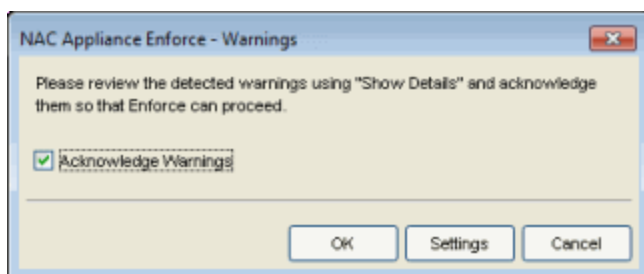
If you choose to correct any problems at this point, you must close the Audit Results window. When you have made your changes, click the **Enforce All** button to start the enforce operation and perform a new audit.

From the Enforce window, you can click the **Enforce All** button to enforce all engines, or use the checkboxes in the **Select** column to select some of the engines to enforce and click the **Enforce** button. In order for the enforce operation to be carried out, none of the selected engines can have an error associated with it. Even if one of the selected engine has passed the audit, it will not be enforced if other selected engines have errors.



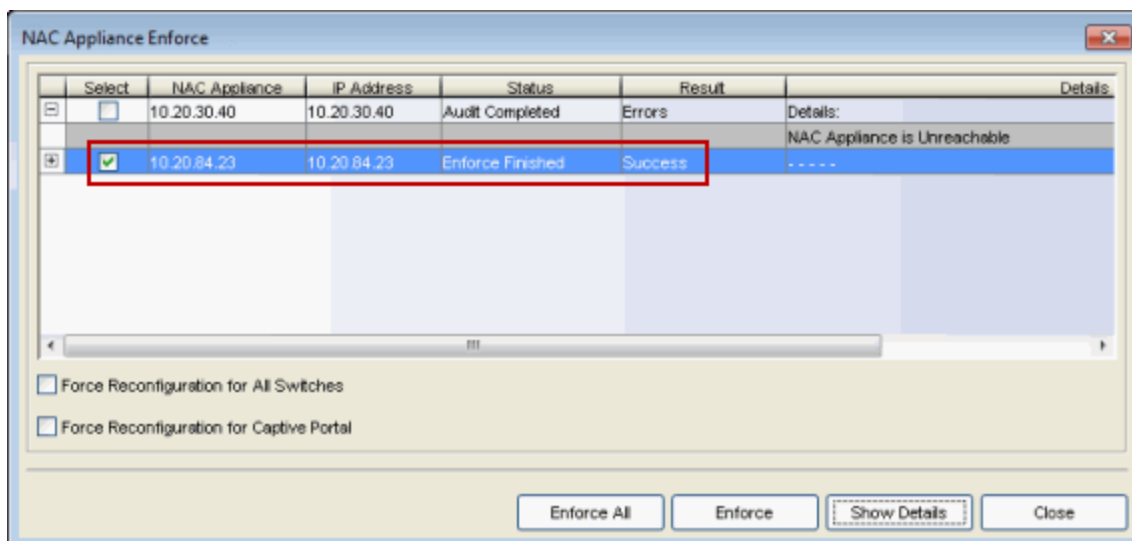
If none of the selected engines have errors, but a selected engine has a warning associated with it, you will be given the option to acknowledge the warning and

proceed with the enforce anyway. Once you acknowledge the warning and click OK, the enforce will be performed.



TIP: If there are warning messages that are regularly displayed during Enforce engine audits, you can use the [Enforce Warning Settings](#) (Tools > Options) to specify that these messages should be ignored and not be displayed.

The Enforce window will display the enforce operation status, as shown below.



Advanced Enforce Options

In the Enforce window, there are two Advanced enforce options available. The two options can be used for the following situations:

- **Force Reconfiguration for All Switches** - This option can be used if the switch RADIUS settings were manually changed via CLI or Policy Manager. Since NAC does not reconfigure the switches every time there is an enforce, selecting this option forces reconfiguration of RADIUS settings on all switches to ensure they are configured correctly.

- **Force Reconfiguration for Captive Portal** - During an enforce, captive portal settings are not enforced unless they have changed. You can use this option to force reconfiguration of the portal to ensure the state of the captive portal processes.

MAC Locking

MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different port or switch, it will be rejected or assigned a specific policy based on an action that you specify when you create the MAC Lock. You can view all your locked MAC addresses in the [MAC Locking](#) pane of the Advance Configuration tool, and access the [Add MAC Lock window](#) to set up your MAC Locks.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name will change and break the MAC Locking settings.

Here are some examples of ways to use MAC Locking:

- A university might lock end-users on a specific floor in a dormitory to a switch that services that floor.
- A printer, server, or other end-system could be allowed network access only when it is connected to a port specified by IT operations. This prevents security issues that could result if the device was moved to a different area of the network.
- A company could lock an IP phone to a specific port on a switch. This would allow exact identification of the phone's location in case an emergency (911) call was placed from the phone.

NOTE: For Access Control Controller Engines.

-- On Layer 3 Access Control Controllers, you should not use MAC Locking to lock a MAC address to the Access Control Controller PEP IP address **and** a port on the PEP. You can however, lock a MAC address to the PEP IP and **not** the port, which would restrict movement of the MAC address away from the Layer 3 Access Control Controller.

-- On Layer 2 Access Control Controllers, a MAC address can be locked to the Access Control Controller PEP IP address and port, or just the PEP IP address, but this will only control the movement of the end-system between the downstream ports on the PEP (IP address and port) and not the actual edge of the network.

-- On Layer 3 Access Control Controllers, there may be cases where NAC Manager cannot determine the MAC address of the connecting end-system (for example, DHCP is disabled and a firewall is enabled on the end-system, or the end-system is connecting through a VPN), and the MAC address for the end-system is displayed as "Unknown." In these cases, the MAC Locking feature is not supported.

Notifications

Notifications provide the ability for NAC Manager to notify administrators or helpdesk personnel of important information through email, Trap, or Syslog messages. These notifications help administrators understand what is going on in their NAC system on a real-time basis. For example, NAC Manager could be configured to send a notification when a new end-system is learned on the network, when a MAC lock is violated, or when a new MAC address is registered on the network. For more information, see the [Manage Notifications window](#).

Automated Security Manager Blacklist

Extreme Management Center Automated Security Manager (ASM) can be configured to notify NAC Manager in response to a real-time security threat from an end-system on the network. NAC Manager automatically adds the end-system's MAC address to the Blacklist end-system group, effectively putting the end-system in quarantine and preventing the end-system from accessing the network from any location. If ASM notifies NAC Manager that the security threat is no longer present, then NAC Manager removes the end-system from the Blacklist group and the end-system is dynamically re-authenticated to the network. Use ASM's Create/Edit Rule window (accessed from the Rule Definition view of the Automated Security Manager Configuration window) to configure the "Notify NAC" action.

You can view ASM blacklists under the End-System Group folder in the Advanced Configuration view, by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the Rule Components folder and the End-System Group folder, and click on Blacklist. An ASM blacklist entry will have a description of "ASM." In addition, NAC Manager generates a health result for the end-system when it is blacklisted by ASM. In the [Health Result Summaries table](#), the health result reason states "ASM Denied" and lists the Sender ID, Signature, and Sender Name. In the [Health Result Details table](#), one health result detail is generated with a Test Case ID of 200001, and a risk level of HIGH with a score of 10. All ASM Blacklist health result details will use the same Test Case ID of 200001.

Mobile IAM

Extreme Networks Mobile IAM (Identity and Access Management) is a comprehensive BYOD solution that provides total security, full IT control, and predictable network experience for all users. Mobile IAM provides the controls required to grant network access to BYOD devices, with the same fine-grained security controls that are applied to wired and wireless IT managed devices.

The Mobile IAM solution provides complete software for:

- identification all of the devices connected to their network
- access and inventory management
- context-based policy enforcement
- end-to-end management from a single, easy-to-use management application
- auditing and reporting

The Mobile IAM solution is delivered through a Access Control gateway engine and NetSight version 4.3, and configured in NAC Manager. The engine is available as a physical or virtual engine to best meet your deployment needs. The solution can also include installation and integration services that are sold separately.

Contact your Extreme Networks sales representative for more information about Mobile IAM.

How to Set Up Registration

The Extreme Networks Extreme Access Control Solution provides support for Registration which forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. Registration utilizes Registration Web Server functionality installed on a Access Control engine to allow end users to register their end-systems and automatically obtain network access without requiring the intervention of network operations. For more information on Registration and an overview of how it works, see the [Registration](#) section of the Concepts help file.

NOTE: For important information on [web browser requirements](#) for end-systems connecting through NAC Manager, refer to the NAC Configuration Considerations Help topic.

This Help topic describes the specific steps that must be performed when deploying Registration on your network. The steps vary depending on whether you are using Access Control Gateway engines and/or Layer 2 Access Control Controller engines on your network. (Registration is not supported on the Layer 3 Access Control Controller engines.)

For Access Control Gateway engines you must:

- Identify the location in your network topology for the Access Control Gateway installation.
- Define the access policy for authorizing unregistered end-systems.
- Configure policy-based routing on your network.
- Configure Registration parameters in NAC Manager.

For Layer 2 Access Control Controller engines you must:

- Configure Registration parameters in NAC Manager.

The Registration Web Server is pre-installed on the Access Control engine. For instructions on installing and configuring a Access Control engine, please refer to your engine Installation Guide.

NOTE: It is important to add a DNS entry from the Fully Qualified Domain Name (FQDN) of the Access Control engine (both Access Control Gateways and Access Control Controllers) into the DNS servers deployed on the network so that the device running NAC Manager is able to resolve queries to these DNS servers. Otherwise, a short delay occurs in returning the Registration web page to end users on the network.

Information and instructions on:

- [Extreme Access Control Gateway Configuration](#)
 - [Identifying Extreme Access Control Gateway Location](#)
 - [Third-Party Redirection Considerations](#)
 - [Defining the Unregistered Access Policy](#)
 - [Configuring Policy-Based Routing](#)
- [Configuring NAC Manager \(for Extreme Access Control Gateway and Extreme Access Control Controllers\)](#)

Extreme Access Control Gateway Configuration

Perform the following steps when you are deploying Registration in a network that utilizes Access Control Gateway engines. These steps are not necessary if you are utilizing only Access Control Controller engines on your network.

Identifying Extreme Access Control Gateway Location

Although several Access Control Gateways may be deployed on the entire network depending on the number of connecting end-systems, only one Access Control Gateway is required to serve as the Registration Web Server. The location of this Access Control Gateway is important for the implementation of web redirection for unregistered end-systems on the network. The Access Control Gateway serving as the Registration Web Server must be installed on a network segment directly connected to a router or routers that exist in the forwarding path of HTTP traffic from unregistered end-systems. This is because policy-based routing will be configured on this router or routers to redirect the web traffic sourced from unregistered end-systems to this Access Control Gateway. It is important to note that only the Access Control Gateway that you wish to serve as the Registration Web Server needs to be positioned in such a manner. All other Access Control Gateways may be positioned at any location on the network, with the only requirement being that access layer switches are able to communicate to the gateways.

Typically, the Access Control Gateway serving as the Registration Web Server is positioned on a network segment directly connected to the distribution layer routers on the enterprise network, so that any HTTP traffic sourced from unregistered end-systems that are connected to the network's access layer can be redirected to that Access Control Gateway. As an alternative, the Access Control Gateway may be positioned on a network segment directly connected

to the router providing connectivity to the Internet or internal web server farm. In this scenario, the HTTP traffic sourced from unregistered end-systems would be redirected to the Access Control Gateway before reaching the Internet or internal web servers.

Third-Party URL Redirection Considerations

If your environment incorporates third-party redirection (i.e., a Cisco Controller), configure the device to use the following the URL (or redirection ACL) to redirect HTTP traffic to the appropriate Captive Portal pages:

```
http://<GatewayIP>/static/index.jsp
```

Defining the Unregistered Access Policy

When you implement Registration, you assign the Unregistered Access Control Profile defined in NAC Manager as the Default Profile for all end-systems connected to the engine group. The Unregistered Access Control Profile specifies that end-systems is **not** assessed for security posture compliance (at this time) and authorizes end-systems on the network with the "Unregistered" access policy. With this configuration, end-systems are first forced to register to the network, and after successful registration, can be assessed for security posture compliance and subsequently quarantined or allowed network access.

Note that an end-system group may be configured to exempt certain devices from having to register to the network, based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Creating the Unregistered Access Policy

The Unregistered access policy must allow unregistered end-systems access to ARP, DHCP, DNS, and HTTP; particularly HTTP communication to the Access Control Gateway implementing the Registration Web Server functionality. For a network composed of EOS policy-enabled switches in the access layer, you must create the appropriate network access services and rules for the Unregistered *policy role* in Policy Manager to meet these requirements, and enforce those changes to the policy-enabled switches. For a network composed of RFC 3580-enabled switches, you must ensure appropriate network services are allowed for the VLAN(s) associated to the Unregistered access policy.

For EOS policy-enabled Access Layer Switches

When configuring the Unregistered policy role (using Policy Manager) for EOS policy-enabled switches, there are two configurations that are required:

- A rule must be added that permits HTTP traffic (i.e. TCP destination port equaling 80) on the network.
- The rule must specify a class of service action that rewrites the ToS value of the HTTP traffic to a value of 'y'. This value should match the decimal equivalent used in your policy-based routing that is used on the router.

If Assisted Remediation is already deployed with the Quarantine policy role appropriately configured for web redirection on EOS policy-enabled access layer switches, the simplest way to configure the Unregistered policy role in Policy Manager is to copy and paste the Quarantine policy role under the Roles tab in Policy Manager and rename this new policy role "Unregistered".

In addition, the Policy Manager Default Policy Domain includes an Unregistered role that is already configured with a service called Redirect Web Services, that includes an "Allow HTTP and Redirect" rule configured with the Access Control Web Redirect Class of Service.

Perform the following steps in Policy Manager to configure your Unregistered policy role.

NOTE: The Policy Manager Default Policy Domain includes a Access Control Web Redirect Class of Service that can be used. Make sure that the ToS rewrite value is set to the appropriate value for your network. If you already created a Class of Service with ToS rewrite functionality for Assisted Remediation, you may use that same Class of Service for Registration and start with step number 3 below.

1. In Policy Manager, use the Device Configuration Wizard to enable the Role-based Class of Service mode on your network devices.
2. Create a new Class of Service that implements the ToS rewrite functionality:
 - a. Open the Class of Service Configuration window (Edit > Class of Service Configuration).
 - b. Click the Create button and open the Create Class of Service window.
 - c. Enter a name for the class of service (e.g. "Web Redirection").
 - d. Select the 802.1p Priority checkbox and use the drop-down list to select the 802.1p priority to associate with the class of service.

- e. Select the Enable ToS/DSCP Marking checkbox and set the ToS Rewrite value to 'y' (hex).
 - f. Click **OK** to create the new Class of Service.
 3. Use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in your Unregistered policy role.
 - a. Select the service in the left-panel Roles/Services tab.
 - b. From the menu bar, select **Tools > Classification Rule Wizard**.
 - c. Enter a name for the rule (e.g. "Allow HTTP").
 - d. Set the rule status to Enabled.
 - e. Set the rule type to All Devices.
 - f. Set the traffic classification layer to Layer 4.
 - g. Set the traffic classification type to IP TCP Port Destination.
 - h. Set the well-known values to HTTP (80).
 - i. Do not enter an IP address value.
 - j. Review the traffic description summary.
 - k. For the Actions, select the CoS checkbox and the class of service you created in step 2 ("Web Redirection").
 - l. Select Permit Traffic for the Access Control.
 - m. Click **Finish** to complete the rule.
 4. Enforce these policy configurations to your network devices.

For RFC 3580-compliant Access Layer Switches

A VLAN must be identified to which unregistered end-systems will be assigned upon connecting to the network. This may or may not be the same VLAN assigned to end-systems when they are being assessed or quarantined. The VLAN must provision network services to an unregistered end-system that allow the end-system to open a web browser; specifically HTTP, DHCP, ARP, and DNS. Furthermore, it is required that IP connectivity between the end-system and the Access Control Gateway implementing the Registration Web Server functionality is operational.

The VLAN to which unregistered end-systems are assigned must be appropriately configured on all access layer switches where end-systems will be registering to the network. Access control lists may be configured at the default gateway router's interface for the unregistered VLAN to restrict particular types of traffic sourced from end-systems within this VLAN to other areas of the

network; withstanding the previously described provisioning requirements for this VLAN.

For Both EOS policy-enabled and RFC 3580-compliant Access Layer Switches

Now that you have defined the Unregistered policy role in Policy Manager for EOS policy-enabled switches and/or the VLAN assigned to unregistered end-systems for RFC 3580-compliant switches, you must associate this policy role to the appropriate VLAN in NAC Manager.

1. In NAC Manager, click on the Manage NAC Profiles button in the toolbar. The Manage NAC Profiles window opens.
2. Select the Unregistered Access Control Profile entry and click the **Edit** button. The Edit NAC Profile window opens.
3. Click the **Manage** button in the Policy Mappings section. The Edit Policy Mapping Configuration window opens.
4. Select the **Advanced** Radio button.
5. Select the Unregistered policy and click the **Edit** button. The Edit Policy Mapping window opens.
6. Use the drop-down list to select "Unregistered" as the Policy Role. (The drop-down list displays all the policy roles you have created and saved in your Policy Manager database.)
7. If only EOS policy-enabled switches are deployed in the access layer of the network, associate the Unregistered policy with the Default VLAN [1]. If RFC 3580-compliant access layer switches are deployed, associate the "Unregistered" policy with the Unregistered VLAN you will be using in your network, adding the VLAN using the **Add VLAN** button, if necessary.
8. Click **OK** to close all the open windows. Close the Manage NAC Profiles window.

Your NAC Manager Unregistered access policy is now configured to allow unregistered end-systems the ability to communicate to the Access Control Gateway serving as the Registration Web Server. In the next step, the authentication, authorization, and assessment of unregistered end-systems will be specified.

Configuring the Unregistered Extreme Access Control Profile

Now that you have created the Unregistered access policy, you can customize the Unregistered Access Control Profile. The Unregistered Access Control Profile is defined by default in NAC Manager to specify that an unregistered end-

system will **not** be assessed for security posture compliance and that it will be authorized on the network with the "Unregistered" policy. Therefore, unregistered end-systems will be immediately assigned to the "Unregistered" policy when connected to EOS policy-capable access layer switches and the "Unregistered" VLAN when connected to RFC 3580-compliant access layer switches, without being assessed. The authentication, assessment, and authorization settings of the Unregistered Access Control profile may be changed as required by your organization. Once you have configured the Unregistered Access Control Profile, it can be selected as the default profile for an engine group (as described in a later section) where end-systems will be required to register to the network.

To change the Unregistered Access Control Profile, use the following steps.

1. In NAC Manager, click on the Manage Access Control Profiles button in the toolbar. The Manage NAC Profiles window opens.
2. Select the Unregistered Access Control Profile entry and click the **Edit** button. The Edit NAC Profile window opens.
3. Select the desired authentication, assessment, and configuration settings.
4. Click **OK**.

Configuring Policy-Based Routing

As described above, the Access Control Gateway serving as the Registration Web Server must be located on a network segment directly connected to a router or routers that exist in the transmission path of all traffic from any end-system that is not registered. This is because policy-based routing (PBR) must be configured on the routers to redirect the web traffic sourced from unregistered end-systems to that Access Control Gateway.

If EOS policy-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with a ToS field of 'y' to the next-hop address of the Access Control Gateway serving as the Registration Web Server. If RFC 3580-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with the source IP address on the subnet(s)/VLAN(s) associated to the Unregistered access policy, to the next-hop address of the Access Control Gateway serving as the Registration Web Server.

In addition, if you are adding multiple Access Control Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well.

For EOS policy-enabled Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to a policy role on EOS policy-enabled switches that uses the "Allow HTTP" classification rule to assign HTTP traffic the "Web Redirection" class of service. This class of service rewrites the ToS field in the HTTP traffic to a value of 0x40 (or 64 base 10), equivalent to a DSCP value of 16. (The DSCP is the value defined in the six most significant bits of the 8-bit ToS field.) Furthermore, the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for EOS policy-enabled access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic with a DSCP of 16.
`access-list 102 permit tcp any any eq 80 dscp 16`
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the Access Control Gateway serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the Access Control Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple Access Control Gateways are serving as Registration Web Servers.
`route-map 101
match ip address 102
set next-hop xxx.xxx.xxx.xxx`
3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.
`ip policy route-map 101`

For RFC 3580-compliant Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for RFC 3580-compliant access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic sourced from subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24.
`access-list 102 permit tcp 10.1.10.0.0.0.0.255 any eq 80`

```
access-list 102 permit tcp 10.1.20.0.0.0.255 any eq 80
access-list 102 permit tcp 10.1.30.0.0.0.255 any eq 80
```

2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the Access Control Gateway serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the Access Control Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple Access Control Gateways are serving as Registration Web Servers.

```
route-map 101
match ip address 102
set next-hop xxx.xxx.xxx.xxx
```

3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.

```
ip policy route-map 101
```

Setting up Redundancy on Access Control Gateways

When adding multiple Access Control Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well. This is performed on the router in which policy-based routing is configured. Use the same commands described in the previous two sections except for the two following changes:

- In step 2, in addition to the single IP address set as the next-hop IP address, enter a list of IP addresses of the redundant Access Control Gateways. For example:

```
set next-hop xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
```

- In step 3, when adding the ip policy route-map to the router interface, specify an additional command called "ip policy pinger on". This command will attempt to ping the first IP address that is specified in the next-hop to determine its availability. If it is not available, the next IP in the list of next-hops is pinged and then used, if it is available.

For example:

```
ip policy route-map 101
ip policy pinger on
```


With policy-based routing and the Unregistered Access Control Profile configured, Registration settings can be specified and then enabled on the network, as described in the next section.

Configuring NAC Manager (for Extreme Access Control Gateways and Extreme Access Control Controllers)

Perform the following steps when you are deploying Registration in a network that utilizes Access Control Gateway engines and/or Layer 2 Access Control Controllers. (Registration is not supported on Layer 3 Access Control Controller engines.)

Use the portal configuration section of the [NAC Configuration window](#) (in NAC Manager) to configure parameters for the Registration web pages served from the Access Control engine. All Access Control engines are initially assigned a default portal configuration. You can use this window to view and edit the default configuration or create new configurations to use. Once you have defined your portal configuration, you must enforce the Access Control configuration to your engine(s).

Use the following steps to define your portal configuration and enforce it to the engine. These steps give you an overview of the required configuration. For more detailed information, see the [NAC Configuration Window](#) and [Portal Configuration](#) Help topics.

1. Verify that Registration/Web Access is enabled in the NAC Manager Features options accessed from Tools > Options in the NAC Manager menu bar.
2. Use the NAC Manager  toolbar button to open the NAC Configuration window.
3. In the left-panel tree, select the Features icon. Enable the registration, access, and assessment features you want for your network. For information on each available feature, see the [Features](#) section in the NAC Configuration Window Help topic.
4. In the left-panel tree, select the Portal icon. If needed, use the Portal Configuration drop-down menu in the right panel to select the configuration to configure or to create a new one.
5. Expand the Portal icon and select the portal configuration settings you want to edit:
 - a. Click on Network Settings to view network web page parameters. Click on Look and Feel to view the common web page parameters. These parameters are shared by both the Remediation and the Registration web pages. You can edit and change these parameters;

for a description of each parameter, see the [Network Settings](#) and [Look and Feel](#) sections of the Portal Configuration Help topic. Be aware that if you deploy both the assessment/remediation and registration features, any changes will affect the web pages for both features.

- b. Click on Common Settings where you can configure settings for the Registration web page. You can edit and change these parameters; for a description of each parameter, see the [Common Registration Settings](#) section of the Portal Configuration Help topic.
 - c. Click on Administration where you can configure settings for the registration administration web page and grant access to the page for administrators and sponsors. For information on this tab, see the [Administration](#) section of the Portal Configuration Help topic.
 - d. Depending on the registration, access, and assessment/remediation features you have selected for your network, there are additional views you can access where you can configure the settings and parameters for each type. For a description of each setting and parameter, see the [Portal Configuration](#) Help topic.
6. When you have finished making your changes to the portal configuration, click **Save** in the NAC Configuration window and then close the window.
 7. Enforce the Access Control configuration to the engine group.
 8. To exempt certain end-systems or end users from having to register to the network, you can configure end-system groups based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Registration is now enabled for all end-systems connecting to this engine group, with the exception of those end-systems and end users that have been exempted based on group membership.

Related Information

- [Registration Concepts](#)
- [Portal Configuration](#)
- [Registration Administration](#)

Portal Configuration


If your network is implementing [registration](#) or [assessment/remediation](#), you define the branding and behavior of the portal website used by the end user during the registration or assessment/remediation process using a Portal Configuration. Extreme Access Control engines ship with a default Portal Configuration. Use this default configuration as is, or make changes to the default configuration using this window.

This Help topic provides the following information for accessing and configuring the Portal Configuration:

- [Accessing the Portal Configuration](#)
- [Network Settings](#)
- [Administration](#)
- [Look and Feel](#)
- [Common Settings](#)
- [Guest Registration](#)
- [Guest Web Access](#)
- [Secure Guest Access](#)
- [Authenticated Registration](#)
- [Authenticated Web Access](#)
- [Assessment/Remediation](#)
- [Portal Web Page URLs](#)

Accessing the Portal Configuration

Use the following steps to access the Portal Configuration:

1. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
2. In the left-panel tree, select the Portal icon. If needed, use the Portal Configuration drop-down menu in the right panel to select the configuration to specify for your NAC Configuration, or to create a new one.

3. Expand the Portal icon and select the portal configuration settings you want to edit. Refer to the sections below for information on the different settings.

At the bottom of the window there is an **Appliance Portal Pages** button that displays a menu to let you quickly launch the following portal web pages:

- **Preview Web Page** — allows you to preview web pages that may be accessed by the end user during the assessment/remediation and registration process.
- **Registration Administration Page** — used by Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network. For more information, see [Registration Administration](#).
- **Registration Sponsor Page** — used by sponsors to view, delete, and add registered end-systems that they sponsor. For more information, see [Sponsored Registration](#).
- **Pre-Registration Page** — lets selected personnel register guest users in advance of an event, and print out a registration voucher that provides registration credentials. For more information, see [Pre-Registration Portal](#).
- **Self-Registration Page** — allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems). For more information, see [Enable Self-Registration Portal](#).

You can also launch these web pages using a URL. For a list of URLs for accessing commonly used portal web pages, see [Portal Web Page URLs](#).

Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment/Remediation and the Registration portal web pages.

The screenshot shows a configuration window titled "Network Web Page Settings". It contains the following fields and options:

- Allowed Web Sites: [change](#)
- Use Fully Qualified Domain Name:
- Use Mobile Captive Portal:
- Display Welcome Page:
- Redirect User Immediately: Test Image URL:
- Redirection: To URL:
- Portal HTTP Port:
- Portal HTTPS Port:
- Force Captive Portal HTTPS:

Allowed Web Sites

Click on the "change" link to open the [Allowed Web Sites window](#), where you can configure the web sites to which end users are allowed access during the assessment/remediation and registration process.

Use Fully Qualified Domain Name

Select this checkbox if you would like the URLs in the portal web pages to display the engine's hostname instead of IP address. When this is enabled, the user's browser performs a DNS lookup to find the IP address for the fully qualified hostname of the Extreme Access Control engine. Only enable this option if all Access Control engine hostnames are defined in DNS.

Use Mobile Captive Portal

Select this checkbox to allow end users using mobile devices to access the network via captive portal registration and remediation. In addition, it allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network using a mobile device. This feature is supported on the following mobile devices: iPod Touch, iPad, iPhone, Android Phone/Tablet/NetBook, and Windows phones.

Display Welcome Page

Select this checkbox to display the welcome page. If the checkbox is not selected, users bypass the welcome page and access the portal directly.

Redirect User Immediately

This option redirects end users to the specified test image URL as soon as they have network access. The redirect occurs regardless of where the end user is in the connection process. If the end-system's browser can reach the test image URL, then it assumes that the end user has network access and redirects the end user out of the captive portal. The test image URL should be an internal image on your own website that end users don't have access to until they're accepted. It is recommended that the test image URL is a link to an SSL site. The reason for this is that if the NAC Manager captive portal is configured for Force Captive Portal HTTPS, the browser does not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies, (typically the Unregistered, Assessing, and Quarantine policies), are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. In the event access to the test image is available, the user may experience the captive portal reverting to the "click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on the network.

Redirection

There are three Redirection options that specify where the end user is redirected following successful registration or remediation, when the end user is allowed on the network:

- **To URL** — This option lets you specify the URL for the web page to which the end user is redirected. This is also the connection URL that is displayed on the Guest User Voucher when using [Pre-Registration](#). This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."
- **Disabled** — This option disables redirection. The end user stays on the same web page, where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.

You can override this setting and specify different Redirection URLs for your remediation and registration configurations settings.

Portal HTTP Port

Specify which port the Extreme Management Center server and Access Control engine uses for HTTP web server traffic. Any change do not take effect on the Access Control engine until an Enforce is performed in NAC Manager.

Portal HTTPS Port

Specify which port the NetSight server and Access Control engine uses for HTTPS web server traffic. Any change do not take effect on the Access Control engine until an Enforce is performed in NAC Manager.

Force Captive Portal HTTPS

Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. It is recommended that this checkbox is enabled if [Authenticated Registration](#) is configured for the registration process. The default setting is unchecked, specifying to serve the captive portal web pages over HTTP.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network. The web page also provides access to the Pre-Registration Portal (if pre-registration is enabled) and the Screen Preview web page. For more information, see [Registration Administration](#).

The screenshot shows two main sections of a configuration page:

Administration Web Page Settings

- Welcome Message: [change](#)
- Force Administration HTTPS:
- Session Timeout (Minutes):
- Login Failure Image:
- Limit Sponsor's View To Own Users:
- LDAP Email Address Attribute Name:
- RADIUS Email Address Attribute Name:

Administrative Login Configuration

Controls portal access for administrators and sponsors.

Authentication	User Name, LDAP, or RADIUS User Gro.	Role Summary
Local Password Repository	Admin	Role Name: Admin Role - Capabili...
Local Password Repository	Sponsor	Role Name: Sponsor Role - Capabili...

Buttons on the right side of the table:

- Move Up...
- Move Down...
- Add...
- Delete
- Edit...
- Roles...

Administration Web Page Settings

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed to users when they log into the administration or sponsor portal. The default welcome message is "Registration System Administration."

Force Administration HTTPS

Select this checkbox to force the administration web page to be served securely over HTTPS (instead of HTTP) to administrators and sponsors on the network. It is recommended that this is enabled for security reasons.

Session Timeout (Minutes)

Use this field to specify how long an administrator can be inactive on the administration web page before getting automatically logged out. The default value is 10 minutes.

Login Failure Image

Select the image you would like displayed when the end user fails to correctly log in to the web page. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, click the configuration menu button to the right of the drop-down list and select Manage Images to open the Images window.

Limit Sponsor's View to Own Users

Select this checkbox if you want to limit a sponsor's view to only the users they have sponsored. This option is valid only if you configure LDAP or RADIUS authentication of your sponsors. If you select this checkbox, you must enter the LDAP or RADIUS email address attribute name so that a sponsor's login name can be matched to their email address, and only the registered users for that sponsor are displayed.

Administrative Login Configuration

Use this section to configure administrative user access to the Registration Administration web page, the Sponsor Administration web page, and the Pre-Registration Portal. (To see the URLs for these web pages, refer to [Portal Web Page URLs](#).)

Users authenticate to a local database or through an LDAP or RADIUS server and receive a role assignment based on their login. The assigned role determines their level of access to the portal web pages.

There are two default roles already configured:

- Admin Role — provides access to the administration page, sponsor page, and pre-registration portal. Allows the ability to add registered users and change user expiration, assign end users to all end-system and user groups, and view users from all engine groups.
- Sponsor Role — provides access to the sponsor page and pre-registration portal. Allows the ability to add registered users and change user expiration, assign end users to all end-system and user groups, and view users from all engine groups.

Use the default roles or create a new role. For example, create a role that defines access capabilities for administrative personnel that only accesses the Pre-Registration Portal, such as receptionists pre-registering guests to the network.

The table in this section lists the available login configurations, and lets you add, delete, and edit configurations. You can also add and modify the roles used to define access.

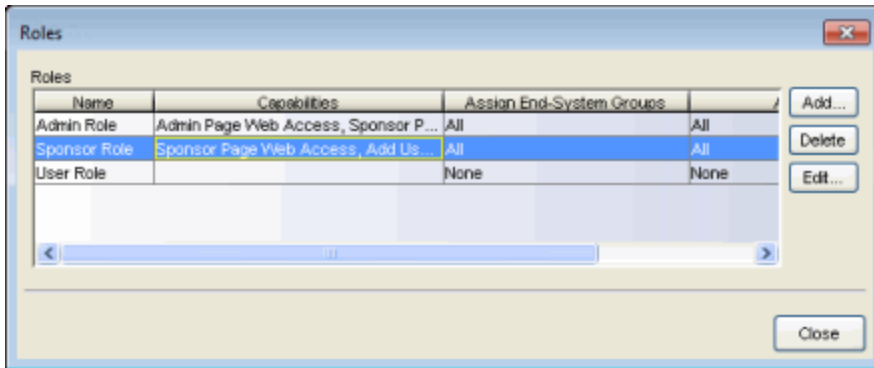
Use the following steps to add a new login configuration:

1. Click the **Add** button to open the Add Login Configuration window.

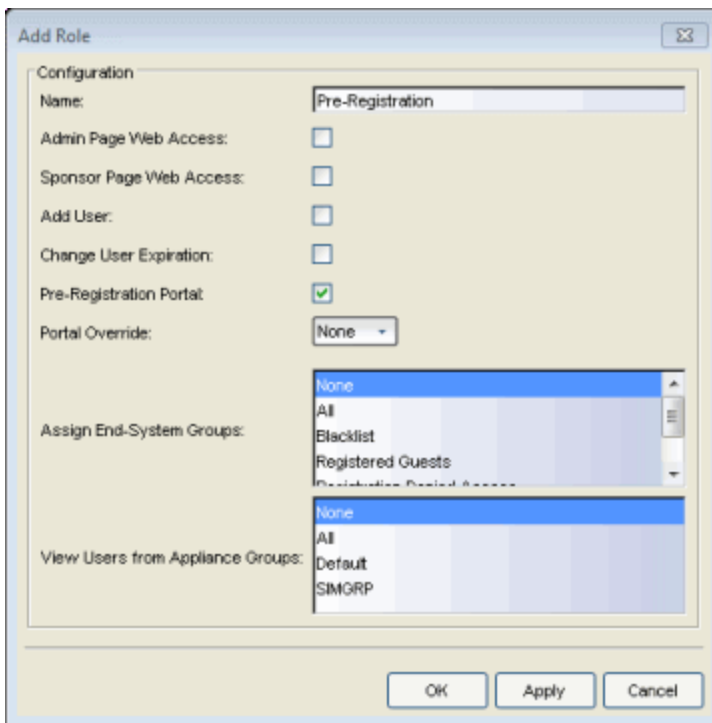
2. Define the configuration's authentication based on a local password repository user or user group, or an LDAP or RADIUS user group. Local repository users are configured through [AAA Configuration](#). You can add or edit user groups using the drop-down menu. User groups can also be defined in the [Manage Rule Groups window](#).
3. Select a role to assign to authenticated users.
4. Click **OK** to create the new login configuration in the Administrative Login Configuration table.
5. Use the **Move Up/Move Down** buttons to change the order of the configurations in the table list. This determines the precedence of the configurations, which is useful when you are using user groups and an end user falls into more than one group. For example, if a user is a member of both the Admin LDAP user group and the Sponsors LDAP user group in the LDAP server, list the Admin group first, otherwise the user never matches the Admin group and is never able to access the administration web page.
6. Use the **Edit** or **Delete** buttons to modify or remove a login configuration.

Use the following steps to modify or create a new Role.

1. Click the **Roles** button to open the Roles window that lists available roles and their capabilities, and allows you to add, edit, and delete roles.



- Click **Add** to open the Add Role window and enter a name for the new role. Click **Edit** to modify an existing role.



- Specify the role's access capabilities:
 - Select whether the role provides access to the Admin Page, Sponsor Page, or Pre-Registration Portal.
 - Select whether the role provides the ability to add registered users and change user expiration.
 - The Portal Override is used in environments where advanced location-based access is defined and allows you to specify the appropriate portal for the administrator logging in. For example, using two roles

with two different portal overrides, you can make sure that when an administrator from company ABC logs in, they see company ABC's portal, while an administrator from company XYZ sees company XYZ's portal.

- Select whether users are able to assign end users to all end-system and user groups (All), select groups, or no groups (None).
 - Select whether users are able to view users from all engine groups (All), select groups, or no groups (None).
4. Click **OK** to create or modify the role. You can now use the role in your login configurations.

Look and Feel

Use this panel to configure common web page settings that are shared by both the Assessment/Remediation and the Registration portal web pages.



The screenshot shows a configuration window titled "Common Web Page Settings". It contains the following settings:

Header:	change
Footer:	change
Helpdesk Information:	change
Images:	change
Colors:	change
Style Sheet:	change
Mobile Style Sheet:	change
Message Strings:	change
Default Locale:	English ▾
Supplemental Locales:	add
Display Locale Selector:	<input type="checkbox"/>
Display Powered By Logo:	<input checked="" type="checkbox"/>
Header Background Image:	Default ▾
Header Image:	None ▾
Favorites Icon:	Default ▾
Access Granted Image:	Default ▾
Error Image:	Default ▾
Busy Image:	Default ▾

Header

Click on the "change" link to open a window where you can configure the link for the header image displayed at the top of all portal web pages. By default, the header image is configured as the Extreme Networks logo

acting as a link to the Extreme Networks website. Text entered in this window can be formatted in HTML.

Footer

Click on the "change" link to open a window where you can configure the footer displayed at the bottom of all portal web pages. By default, the footer is configured with generalized information concerning an organization. Change the "example" text in this section to customize the footer to your own organization. Text entered in this window can be formatted in HTML.

Helpdesk Information

Click on the "change" link to open a window where you can configure the Helpdesk contact information that is provided to end users in various scenarios during the assessment/remediation and registration process (e.g. an end-system has exceeded the maximum number of remediation attempts). By default, this section is configured with generalized Helpdesk information, such as contact URL, email address, and phone number. Change the "example" text to customize the Helpdesk information for your own organization. Text entered in this window can be formatted in HTML. In addition, the entire contents of the Helpdesk Information section are stored in the variable "HELPDESK_INFO". By entering "HELPDESK_INFO" (without the quotation marks) in any section that accepts HTML in the Common Page Settings (or any other settings), all information configured in this section is displayed in place of "HELPDESK_INFO".

Images

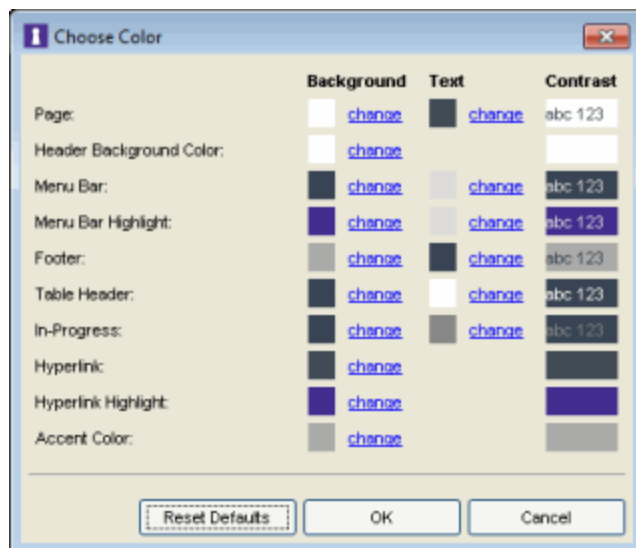
Click on the "change" link to open the Images window where you can specify the image files used in the portal web pages. All image files used for Assessment/Remediation and Registration portal web pages must be defined in this list. Once an image file is defined here, it is available for selection from the configuration drop-down menus (for example, when you configure the [Access Granted Image](#)), and may be referenced in the sections supporting HTML. The image files defined here are sent to the Access Control engine along with the web page configuration.

Use the **Add** button to select an image file to add to the list. You can select an image in the list and use the **Display Image** button to preview the image.

Colors

Click on the "change" link to open the Choose Color window, where you can define the colors used in the portal web pages:

- Page — Define the background color and the color of all primary text on the web pages.
- Header Background Color — Define the background color displayed behind the header image.
- Menu Bar — Define the background color and text color for the menu bar.
- Menu Bar Highlight — Define the background color and text color used for the menu bar highlights in the Administration pages.
- Footer — Define the background color and text color for the footer.
- Table Header — Define the background color and text color for the table column headers in the Administrative web pages.
- In-Progress — Define the background color and text color for task in-progress images.
- Hyperlink — Define the color used for hyperlinks on the web pages.
- Hyperlink Highlight — Define the color of a hyperlink when it is highlighted.
- Accent Color — Define the color used for accents on various parts of the web pages.



Style Sheet

Click on the "change" link to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the portal web pages.

Mobile Style Sheet

Click on the "change" link to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the mobile version of the portal web pages.


Message Strings

Click on the "change" link to open the [Message Strings Editor window](#) where you can edit the text and formatting of the various messages used on the portal web pages or replace them with message strings from another file. You can also use the Message Strings Editor to create a new message, if your portal configuration requires it. For example, you might want to add a welcome message to the Portal landing page. If you have defined supplemental locales (languages), you can edit those message strings here as well.

Default Locale

Select the locale (language) displayed to any captive portal user unless the client locale detected from their browser matches one of the defined supplemental locales. The list from which you select includes the current default locale and any supplemental locales defined.

Supplemental Locales

This field lists the locales (languages) presented as options to the user in the captive portal, in addition to the default locale. If no supplemental locales are defined, click the "add" link to open the Portal Locale Entries window, where you can define the locales to use. (In the Portal Local Entries window, click the  button and use the [New Locale window](#) to add a new locale.) If supplemental locales are defined, they are listed here as a link, which you can click to open the locale editor.

Display Locale Selector

Select this checkbox if you want a locale (language) selector to be displayed as a drop-down menu in the menu bar on the captive portal welcome and login pages. Use this option for a shared machine where the users of the machine may speak different languages. (On the mobile captive portal, the selector is displayed as a list of links at the bottom of the welcome screen.)

Display Powered by Logo

Select this checkbox to display the Extreme Networks logo at the bottom of all of your portal web pages.

Header Background Image

Select the background image you would like displayed behind the header image at the top of all portal web pages. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Header Image

Select the image displayed at the top of all portal web pages. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Favorites Icon

Select the image displayed as the Favorites icon in the web browser tabs. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Access Granted Image

Select the image displayed when the end user is granted access to the network either based on compliance with the network security policy or upon successful registration to the network. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Error Image

Select the image displayed when there is a communication error with the NetSight Server. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Busy Image

Select the progress bar image displayed to the end user when the web page is busy processing a request. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Common Settings

Use this tab to configure the common settings used by the different registration web pages.

The screenshot shows a configuration window titled "Registration Web Page Settings". It contains four settings:

- Title:** A text field with a blue "change" link next to it.
- Welcome Message:** A text field with a blue "change" link next to it.
- User Registration Success:** A text field with a blue "change" link next to it.
- Access Denied Image:** A drop-down menu currently showing "Default".

Below these settings is a section for "Survivable Registration" with an unchecked checkbox. The text below the checkbox reads: "This option will allow for a temporary Registration when communication to NAC Manager fails. During this time, any registrations will receive the Failsafe policy of the Unregistered NAC Profile. When communication is restored, the user will be put through the normal Registration process."

Title

Click on the "change" link to open a window where you can modify the text that appears in the title bar of the registration and web access page browser tabs. The default page title is "Enterprise Registration."

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed to users on the menu bar of any registration or web access page. The default welcome message is "Welcome to the Enterprise Network's Registration Center."

User Registration Success

Click the "change" link to open a window where you can edit the message displayed to the end user after successfully registering their end-system to the network.

Access Denied Image

Select the image you would like displayed when the end user has been denied access to the network. The drop-down menu displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Enable Survivable Registration

This feature provides temporary Registration for unregistered end-systems when the NetSight server is unreachable. If you select this checkbox, unregistered users that try to register while the NetSight server is

unreachable are redirected to the Registration web page. After entering the required information, users are assigned the Failsafe policy and allowed on the network. Once the connection to the NetSight server is reestablished, the users are reassigned the Unregistered policy and forced to re-register. If you enable Survivable Registration, make sure that the Failsafe policy provides the appropriate network services for unregistered users.

Guest Registration

Guest registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network. Guests are initially redirected to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

The end user's level of network access is determined by the settings specified here, and whether they are required to have a sponsor. With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

NOTE: If you configure both Guest Registration and [Authenticated Registration](#) for an area on your network, the end user is presented with a choice on the registration web page whether to authenticate or not.

The screenshot displays a configuration interface with the following sections:

- Web Page Customizations (Shared)**: Includes links for "Introduction Message" and "Customize Fields".
- Redirection (Shared)**: Features a "Redirection" dropdown menu set to "Use Network Settings Redirection" and a text input field containing "http://www.enterasys.com".
- Registration Settings**: Includes a "Verification Method" dropdown set to "Disabled" and a "Default Expiration" field set to "30" days.
- Facebook Registration**: A checkbox is unchecked. Below are input fields for "Facebook App ID" and "Facebook App Secret", and a "Show Secret" checkbox.
- Sponsorship**: Contains explanatory text about user assignment and access, and a "Sponsorship Mode" dropdown menu set to "None".

Introduction Message (Shared)

Click the "change" link to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the [Allowed Web Sites window](#) accessed from the [Network Settings](#). By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed

on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#). This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page to which the end user is redirected. Typically, this is the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User Verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see [How to Configure Verification for Guest Registration](#).

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user

must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by a sponsor.

Facebook Registration

Select the Facebook Registration checkbox if you are implementing guest registration using Facebook as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Facebook in order to complete the registration process. For more information, see [How to Implement Facebook Registration](#) for information regarding how to create a Facebook application. When you create an application, you are given a Facebook App ID and Facebook App Secret you enter here.

Sponsorship

Use this section to configure sponsorship for Guest Registration. Select the required Sponsorship Mode. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see [How to Configure Sponsorship for Guest Registration](#).

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Guest Web Access

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

End users are initially redirected to the captive portal when they first connect to the network. After the user enters the required information on the Guest Web Access login page (typically, their name and email address), they are allowed access on the network according to the assessment and authorization defined in the Guest Access profile.

Guest web access provides a single session, and no permanent end user records are stored. This provides increased network security, and also allows you to minimize the number of registration records stored in the NetSight database.

Implementing guest web access requires web redirection or DNS proxy.

Web Page Customizations (Shared)

Introduction Message: [change](#)

Customize Fields: [change](#)

Redirection (Shared)

Redirection: Use Network Settings Redirection

Web Access Settings

Verification Method: SMS Gateway or Email

SMS Gateway Email:

Message Strings: [change](#)

Verify Pin Characters: Alpha Numeric with No Vowels

Verify Pin Length:

Introduction Message (Shared)

Click the "change" link to open a window where you can edit the introductory message displayed to end users when gaining web access as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the [Allowed Web Sites window](#) accessed from the [Network Settings](#). By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Guest Web Access login page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#). This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Verification Method

User verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see [How to Configure Verification for Guest Registration](#).

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Guest Web Access login page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).

- **SMS Gateway** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).
- **SMS Text Message** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the **"SMS Text Message"** or the **"SMS Text or Email"** **Verification method:** click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to send an email to. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the **"SMS Gateway"** or **"SMS Gateway or Email"** **method:** enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Here are three scenarios where Secure Guest Access provides increased network security:

- An enterprise provides secure guest access for visitors. Guests self-register through the captive portal and receive connection credentials and instructions for the secure SSID via a text message on their mobile phone.
- A hospitality company provides guests with secure Internet access using pre-registration. A receptionist generates a voucher using the NAC Manager pre-registration portal. The voucher is handed to the guest, providing them with instructions and credentials for connecting directly to the secure SSID.
- An enterprise provides secure guest access with the option of elevated access through employee sponsors. Guests self-register through the captive portal and receive connection credentials and instructions via a text message. Sponsors approve guests for secure guest access. Later, sponsors can elevate guest access using the sponsorship portal.

Web Page Customizations (Shared)

Customize Fields: [change](#)

Secure Access Settings

Credential Delivery Method:

Service Providers: [change](#)

Message Strings: [change](#)

Default Expiration: (0=never)

Default Maximum Registered Devices:

Enable Pre-Registration Portal:

Generate Password Characters:

Generate Password Length:

Sponsorship

End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.

Sponsorship Mode:

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Secure Access Settings

Credential Delivery Method

Select the method used to send guests their credentials and access instructions for the secure SSID. For more information and complete instructions, see [How to Configure Credential Delivery for Secure Guest Access](#).

- **Captive Portal** — The credential information displayed on the Registration web page.
- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).
- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the "SMS Text Message" or the "SMS Text or Email" **Verification method**: click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to which to send an email. This email is then received by the service provider and converted

to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", modify the "secureGuestAccessEmailSentFromAddress" message string to be the appropriate email address for your company.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by the sponsor.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Enable Pre-Registration Portal

Use this checkbox to enable Pre-Registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users attending a company presentation, sales seminar, or a training session need network access. From the drop-down menu, select whether to pre-register a single user (to pre-register one user at time) or multiple users (when a larger group of users is pre-registering) or both. For more information, see [How to Configure Pre-Registration](#).

Generate Password Characters (Shared)

NAC Manager uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

NAC Manager uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Sponsorship

Use this section to configure sponsorship for Secure Guest Access registration. Select the Sponsorship Mode required. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see [How to Configure Sponsorship for Guest Registration](#).

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Authenticated Registration

Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

It is recommended that the [Force Captive Portal HTTPS](#) option is enabled if authenticated registration is required for security reasons.

NOTE: If you configure both [guest registration](#) and authenticated registration for an area on your network, the end user is presented with a choice on the registration web page whether to authenticate or not.

Authentication (Shared)	
AAA Configuration:	Default
Authentication To End-System Group:	Local change
Local Password Repository:	Default
Max Failed Logins:	<input type="checkbox"/>
Web Page Customizations (Shared)	
Login or Register Message:	change
Introduction Message:	change
Failed Authentication Message:	change
Customize Fields:	change
Redirection (Shared)	
Redirection:	Use Network Settings Redirection <input type="text" value="http://www.enterasys.com"/>
Registration Settings	
Default Maximum Registered Devices:	<input type="text" value="2"/>
Default Expiration:	<input type="text" value="30"/> <input type="text" value="Days"/> (0=never)
Delete Expired Users:	<input type="checkbox"/>
Delete Local Password Repository Users:	<input type="checkbox"/>
Enable Self Registration Portal:	<input type="checkbox"/>
Enable Pre-Registration Portal:	<input type="checkbox"/> <input type="text" value="Multi and Single User"/>
Generate Password Characters:	<input type="text" value="Alpha Numeric with No Vowels"/>
Generate Password Length:	<input type="text" value="8"/>


Authentication (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the NAC configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple NAC Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Click on the "change" link to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key  indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click on the Local Password Repository link to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this option if you want to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Web Page Customizations (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Login or Register Message

Click the "change" link to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the "change" link to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the "change" link to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page.

Redirection (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#).

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings (Shared)

The Generate Password Character and Generate Password Length settings are shared by Authenticated Registration and Secure Guest Access.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the registration list. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network. Individual registration expiration time can also be set by the administrator/sponsor through the Registration Administration web page.

Delete Expired Users

Specifies whether users should be deleted from the Registered users list in the Registration Administration web page when their registration expires. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network.

Delete Local Password Repository Users

If you have selected the Delete Expired Users option, then selecting this checkbox also deletes the expired user from the local password repository.

Enable Self Registration Portal

This checkbox allows an authenticated and registered user to be directed to a URL (provided by an administrator) to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. Once the additional devices have been registered, the student can access the network using those devices. The URL for the Self Registration web page is `https://<Access ControlEngineIP>/self_registration`. You can change the instructions displayed on this web page using the [Message Strings Editor](#) on the [Look and Feel Settings](#); select the selfRegIntro message string.

Enable Pre-Registration Portal

Use this checkbox to enable pre-registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session. From the drop-down menu, select whether you want to pre-register a single user (when you want to pre-register one user at a time) or multiple users (when you have a larger group of users to pre-register) or both. For more information, see [How to Configure Pre-Registration](#).

Generate Password Characters (Shared)

This option is available if you have enabled the Pre-Registration Portal. During the pre-registration process, NAC Manager can automatically generate the password that the guest user uses when connecting to the network. The password is generated according to the specification selected here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

This option is available if you have enabled the Pre-Registration Portal. During the pre-registration process, NAC Manager can automatically generate the password that the guest user uses when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Authenticated Web Access

Authenticated web access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy.

End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Implementing authenticated web access requires web redirection or DNS proxy.

The screenshot displays a web configuration interface with the following sections:

- Authentication (Shared)**
 - AAA Configuration: [basic](#)
 - Authentication To End-System Group: Local [change](#)
 - Local Password Repository: [Default](#)
 - Max Failed Logins:
- Web Page Customizations (Shared)**
 - Login or Register Message: [change](#)
 - Introduction Message: [change](#)
 - Failed Authentication Message: [change](#)
 - Customize Fields: [change](#)
- Redirection (Shared)**
 - Redirection: Use Network Settings Redirection ▾
- Web Access Settings**
 - Enable Agent-Based Login:


Authentication (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the NAC configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple NAC Configurations that are using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Click on the "change" link to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group is mapped to a user group, the icon for the end-system group changes to display a key  indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated web access.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click on the Local Password Repository link to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this option if you want to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Web Page Customizations (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Login or Register Message

Click the "change" link to open a window where you can edit the message displayed to the end user when they are logging in as an authenticated user. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the "change" link to open a window where you can edit the introductory message displayed to the end user when they are logging in as an authenticated user. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the "change" link to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Customize Fields

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed on the Authenticated Web Access login page.

Redirection (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#).

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page where the end user is redirected. Typically this is the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Web Access Settings

Enable Agent-Based Login

If this option is enabled, when the end user connects to the network with an agent installed, the login dialog is displayed in an agent window instead

forcing the user to go to the captive portal via a web browser. This allows you to provide authenticated web access without having to set up the captive portal. Agent-based login is useful for shared access end-systems running an agent because it prompts for a login dialog and also provides a logout option. Login credentials are limited to username/password and an Acceptable Use Policy is not displayed.

You can customize the messages in the Agent Login window using the [Message Strings Editor](#) available in the [Look and Feel Settings](#). Use the agentLoginMessage string to change the message. Any changes you make in the Message Strings Editor override the internationalized messages used in the Agent Login window.

Assessment/Remediation

Use this panel to configure settings for the Assessment/Remediation portal web page.

The screenshot shows a configuration window titled "Web Page Settings" with several sections:

- Web Page Settings:** Includes fields for Title, Welcome Message, Display Violations (set to "Description and Solution"), Do Not Allow Rescan, Allow Blacklist Remediation, Permanently Removed Message, Custom Agent Install Message, Redirection (set to "Use Network Settings Redirection" with URL "http://www.extremenetworks.com"), Access Denied Image, Image During Reattempt, and Agent Scan In Progress Image.
- Remediation Attempt Limits:** Includes checkboxes for "Limit Remediation Attempts" (set to 5) and "Limit Time for Remediation (min)" (set to 25).
- Remediation Links and Custom Remediation Actions:** A tabbed interface with "Remediation Links" selected. It contains a table with two entries:

Name	Link
MAC OS Update	http://www.apple.com/support/downloads
Microsoft Update	http://update.microsoft.com

Buttons for "Add...", "Delete", and "Edit..." are located to the right of the table.

Web Page Settings

Title

Click on the "change" link to open a window where you can modify the message displayed in the title bar of the Assessment/Remediation web pages. The default page title is "Enterprise Remediation."

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed in the banner at the top of the Assessment/Remediation web page. The default welcome message is "Welcome to the Enterprise Remediation Center."

Display Violations

Use this drop-down list to select an option for displaying assessment violation information to the end user:

- **None** — No violations are displayed to the web page. This option might be used for a Access Control engine that is serving web pages to guest users, when you do not want the guest users to attempt to remediate their end-system.
- **Description and Solution** — Both the description and solution are displayed for violations. This provides the end user with information concerning what violation was found and how to fix it. Providing complete information concerning the violation gives the end user the best chance of self-remediation, however, the technical details of the violation may result in end user confusion. Therefore, this configuration may be appropriate for scenarios where the user population of the network possesses more technical IT knowledge.
- **Description** — Only the description is displayed for violations. This provides the end user with information concerning what violation was found, but no information concerning how it can be fixed. This configuration may be appropriate for scenarios where the user population of the network does not possess technical IT knowledge and is not expected to self-remediate. It provides the Helpdesk personnel with technical information about the violation when the end user places a call to the Helpdesk.
- **Solution** — Only the solution is displayed for violations, allowing the end user to perform self-service remediation without knowing what the violation is. This configuration may be appropriate for scenarios where the user population on the network does not possess technical IT knowledge but is expected to self-remediate.

Do Not Allow Rescan

Select this checkbox if you do not want the end user to have the ability to initiate a rescan of their end-system when quarantined. When selected, the "Reattempt Network Access" button is removed from the Assessment/Remediation web page, and the user is not provided with any way to initiate a rescan on-demand for network access. The end user is forced to contact the Help Desk for assistance. You can edit the "Permanently Removed Message" which, by default, advises the end user to contact the Helpdesk to obtain access to the network. Note that the default configuration of the "Permanently Removed Message" references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Allow Blacklist Remediation

Select this checkbox if you want black-listed end users to have the ability to remediate their problem and attempt to reconnect to the network. When selected, a "Reattempt Network Access" button is added to the Blacklist web page, allowing end users to remove themselves from the blacklist and reauthenticate to the network.

Permanently Removed Message

Click on the "change" link to open a window where you can modify the message displayed when users can no longer self-remediate and must contact the Help Desk for assistance. Note that the default message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Custom Agent Install Message

Click on the "change" link to open a window where you can create a message containing additional agent install information to add to the default text on the Install Agent portal web page.

Redirection

There are four Redirection options that specify where the end user is redirected following successful remediation, when the end user is allowed on the network. The option selected here overrides the Redirection option specified in the [Network Settings](#) for Remediation only.

- **Use Network Settings Redirection** — Use the Redirection option specified in the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.

- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Access Denied Image

Select the image you would like displayed when the end user has been quarantined and denied access to the network. The drop-down menu displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Image During Reattempt

Select the image you would like displayed while the end-user is reattempting network access after they have repaired their system. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Agent Scan in Progress Image

Select the progress bar image you would like displayed while the end-user is being scanned. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Remediation Attempt Limits

Limit Remediation Attempts

Select this checkbox if you would like to limit the maximum number of times an end-user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the number of attempts allowed.

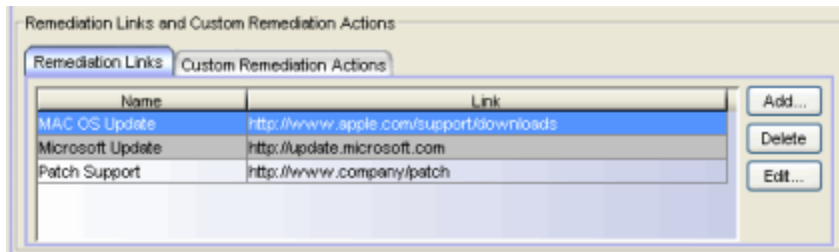
Limit Time for Remediation

Select this checkbox if you would like to limit the total interval of time an end user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the amount of time in minutes.

Remediation Links Subtab

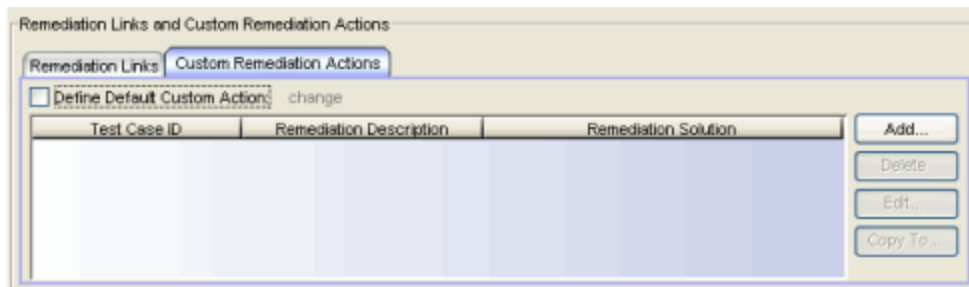
This tab lists the links displayed on the Assessment/Remediation web page for the end users to use to remediate their end-system violations. There are two default remediation links: Microsoft Support and MAC OS Support. Use this tab to add additional links such as an internal website for patches. Links must contain a valid protocol prefix (http://, https://, ftp://).

Click **Add** to open a window where you can define a new link's name and URL. Select a link and click **Edit** to edit the link's information.



Custom Remediation Actions Subtab

Use this tab to create your own custom remediation action for a particular violation to use in place of the remediation action provided by the assessment server.



Use the following steps to add a custom remediation action:

1. Click the **Add** button to open the Add Custom Remediation Action window.
2. Enter the Test Case ID for the particular violation being remediated by the custom action. You can identify the Test Case ID by looking in the Health Results Details subtab in the End-Systems tab.
3. Add a custom description of the violation (required) and an optional custom solution.

4. If you have multiple portal configurations and you would like to use this custom remediation action in all of your configurations, select the **Add to all Portal Configurations** option. This option overwrites any existing custom actions defined for the test case ID.
5. Click **OK**. Whenever the test case ID is listed as a violation on the web page, the custom violation description and solution you define is displayed instead of the remediation actions provided by the assessment server.

Back in the subtab, select the **Define Default Custom Action** checkbox if you would like to advise end users to contact the Helpdesk regarding additional security violations not explicitly listed with custom remediation actions. If this checkbox is selected, only the violations and associated custom remediation actions listed on this tab would be presented to the user, along with a message advising them to contact the Helpdesk for any other security violations not explicitly configured with a custom remediation action. Click the "change" link to edit this message.

To copy a custom action to another portal configuration, select the action in the table and click the **Copy To** button. A window opens where you can select the portal configurations where you want to copy the action, and whether you want it to overwrite any existing custom remediation actions already defined for that test case ID.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Appliance Portal Pages** button at the bottom of the NAC Configuration window.

Web Page	URL
<p>Preview Web Page Allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process.</p>	<p>https://<Access ControlEngineIP>/screen_preview</p>
<p>Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.</p>	<p>https://<Access ControlEngineIP>/administration</p>

Web Page	URL
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://<Access ControlEngineIP>/sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://<Access ControlEngineIP>/pre_ registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://<Access ControlEngineIP>/self_ registration

Related Information

For information on related help topics:

- [How to Set Up Assisted Remediation](#)
- [How to Set Up Registration](#)
- [How to Configure Verification for Guest Registration](#)

Registration Administration

Registration forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. Registration utilizes Registration Web Server functionality installed on a Extreme Access Control (Access Control) engine to allow end users to register their end-systems and automatically obtain network access without requiring the intervention of network operations.

In addition, the Registration Web Server provides a Registration Administration web page that allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network. The web page also provides access to the Pre-Registration Portal (if pre-registration is enabled) and the Screen Preview web page. This provides visibility and control into the registration system for administrators on the network without requiring the delegation of NAC Manager access for these users.

IT and Helpdesk administrators are granted access to the Registration Administration web page via NAC Manager, using the [Administration view](#) in the Edit Portal Configuration window. Once administrators are granted access, they can access the Registration Administration web page at `https://<Access Control Engine Name or IP address>/administration`. Administrators can also access the web page from the Registration Administration toolbar button or the **Tools > Registration Administration** menu option in NAC Manager.

NOTE: The Registration Administration web page cannot be accessed if the Enable Registration checkbox is deselected in the Edit NAC Configuration window.

The Registration Administration web page contains four tabs:

- [Devices](#)
- [Users](#)
- [Pre-Registration Portal](#)
- [Screen Preview](#)

Devices

The Devices web page contains a listing of all end-systems registering to the network. Use the **Display** drop-down menu to filter the end-systems according to state:

- Pending - If Required Sponsorship is configured for registration to the network, this state displays any devices waiting for sponsor approval.
- Approved - This state displays all end-systems successfully registered to the network.
- Suspended - This state displays end-systems whose registration expired, but are not deleted (as configured in the Edit Portal Configuration window, Authenticated Access). This gives administrators an opportunity to approve, deny, or edit the end-system's registration. Suspended end-systems are assigned the default profile.
- Denied - This state lists end-systems denied registration.

Use the buttons at the bottom of the page to approve, deny, edit, or delete the selected end-system.

Following is a sample Devices web page. See the field definitions below for more information.

Sample Devices Page

Registered Device Administration: All Devices

MAC Registration System Administration

Display: All Devices Filter Results:

User Name	MAC Address	Group	State	Sponsor	Description
user1	00:09:6B:53:16:38	Web Authenticated Users	Approved		

Displaying 1 - 1 of 1

Powered by
Extreme networks

Display

Use the Display drop-down menu to filter end-systems according to [registration state](#).

Filter Results

Use the Filter Results field to filter for specific entries in the list.

User Name

For unauthenticated registration, this is "Guest" followed by the MAC address with which the end-system originally connected. For authenticated registration, this is the actual user name with which the end user logged in. Click the link to open the Edit User web page where you can edit the end user's registration information. For example, you can change the end user's expiration time or user type. Click **Submit** to make the changes.

MAC Address

The device's MAC address with which the end-system originally connected, or a MAC address automatically discovered and registered by an assessment agent (for agent-based assessment). Click the link to open an Edit Device web page where you can make changes to the device registration information. For example, you can change the end-system group or add a description. Click **Submit** to make the changes.

Group

The end-system [registration state](#).

State

The end-system group to which device is assigned.

Sponsor

If sponsorship is configured for registration to the network, the email address of the sponsor assigned to approve registration.

Description

A description for the registration process.

Buttons

Select a device and use the buttons to approve, deny, edit, or delete the device.

Users

The Users web page contains two display options available from the **Display** drop-down menu in the upper left corner:

- [Registered Users](#) - displays a list of all registered users and lets you add, edit, or delete a registered user.
- [Local Users](#) - displays a list of user entries in Local Password Repositories and lets you add, edit, or delete users.

Registered Users

The Registered Users web page displays a list of all registered users in all states: Pending, Approved, Suspended, and Denied. Use the buttons at the bottom of the web page to add, edit, or delete a registered user. Use the Register New Device button to open the Devices page and add a device for the selected registered user. Use the Devices For User button to open the Devices page and display all the devices registered for the selected user.

Following is a sample Registered Users web page. See the field definitions below for more information.

Sample Registered Users Page

Registered User Administration: Registered Users

MAC Registration System Administration

Display: Registered Users Filter Results:

User Name	Device Count	Last Name	First Name	Sponsor	E-Mail Address	User Type	Max Registered Devices
badams	0	Adams	Brian			Web Authentication (Authenticated User)	Default: 2
ismith	0	Smith	John			Web Authentication (Authenticated User)	Default: 2
siones	0	Jones	Susan			Web Authentication (Authenticated User)	Default: 2

Displaying 1 - 3 of 3

Powered by

Filter Results

Use the Filter Results field to filter for specific entries in the list.

User Name

For unauthenticated registration, this is "Guest" followed by the MAC address with which the end-system originally connected. For authenticated registration, this is the actual user name with which the end user logged in. Click the link to open a page where you can edit the user's registration information.

Device Count

The number of devices registered to the selected user. Click the link to open the Devices page and see a listing of the registered devices.

Last Name

The end user's last name, if that field is visible and required on the Registration Web Page.

First Name

The end user's first name, if that field is visible and required on the Registration Web Page.

Sponsor

If sponsorship is configured for registration to the network, the email address of the sponsor assigned to approve registration.

E-Mail Address

The end user's e-mail address, if that field is visible and required on the Registration Web Page.

Max Registered Devices

Displays the number of devices the user is allowed to register to the network: either the Default number (which is the [Maximum Registered Devices](#) specified in the Authenticated Access view in the Edit Portal Configuration window) or an Override number specified when manually adding or editing the user on the Registration page.

Buttons

Click **Add** to open a page where you can [add a registered user](#). Select a user name and use the buttons to edit, or delete a user. Select a user and click **Register New Device** to register an additional device for that user. The maximum number of MAC addresses each user is allowed to register is determined by the [Maximum Registered Devices](#) specified in the Authenticated Access view in the Edit Portal Configuration window. Select a user and click **Devices For User** to open the Devices page and display all the devices registered for the selected user.

Add Registered User

Following is a sample web page where you can add a new registered user. Enter the end user registration information and then click Submit to register the user. See the field definitions below for more information.

Sample Add Registered User Page

The screenshot shows the 'MAC Registration System Administration' page. The page header includes the Extreme Networks logo and navigation tabs: Devices, Users, Pre-Registration Portal, Screen Preview, Mobile Screen Preview, and Logout admin. The main content area is titled 'Registered User Administration' and contains the following form fields:

- First Name: Susan
- Middle Name: Linn
- Last Name: Walton
- *User Name: swalton
- E-Mail Address: susan.walton@students.abd.edu
- Phone Number: (empty)
- Start Time: 02/21/2014 0:00:00
- Expires Time: 02/28/2014 0:00:00
- Sponsor: instructor@abc.edu
- User Type: Unauthenticated User
- Max Registered Devices (blank for default Authenticated User 2/Unauthenticated User 2): 2

Buttons for 'Submit' and 'Cancel' are located at the bottom of the form. The page is powered by Extreme Networks.

First Name

Enter the end user's first name, if desired.

Middle Name

Enter the end user's middle name, if desired.

Last Name

Enter the end user's last name, if desired.

User Name

Enter the end user's user name. This field is required.

E-Mail Address

Enter the end user's e-mail address, if desired.

Start Time

Use the calendar button to select a date when registration begins.

Expires Time

Use the calendar button to select a date when registration expires. This expiration time takes precedence over the Default Expiration value configured in the Edit Portal Configuration window, Authenticated Access. If you do not enter a value in this field (the field is blank), then the registration does not expire.

Sponsor

If sponsorship is configured for registration to the network, enter the email address of the sponsor assigned to approve registration.

User Type

Use the drop-down list to select the type of user: unauthenticated (guest registration) or authenticated (authenticated registration).

Max Registered Devices

Use this field to specify the maximum number of devices this user is allowed to register on the network. Leave the field blank to use the default [Maximum Registered Devices](#) specified in the Authenticated Access view in the Edit Portal Configuration window, or enter a value to override the default. Use this feature to allow your network administrators or help desk personnel to register more devices than the maximum count you specified for students or regular employees.

Local Users

The Local Users web page provides the ability to quickly add, edit, and delete users in a Local Password Repository without having to access the local repository through the NAC Manager AAA configuration. Local Password Repositories can be used to store credentials for authenticated registration and pre-registration, as well as for access to registration administration and sponsor administration web pages. NAC Manager supplies a default repository, or you can create additional repositories using the [Edit Basic AAA Configurations Window](#). Click **Add** to open a page where you can [add a local user](#) to a specified Local Password Repository.

Sample Local Users Page

Local User Administration: Local Users

MAC Registration System Administration

Display: Filter Results:

<input type="checkbox"/>	User Name	First Name	Last Name	Display Name	Password Repository	Description
<input type="checkbox"/>	Admin			Admin	Default	
<input type="checkbox"/>	PJohnson	Paul	Johnson	Paul Johnson	Default	abc.co sales
<input type="checkbox"/>	SSmith	Susan	Smith	Susan Smith	Default	abc.co technical
<input type="checkbox"/>	Sponsor			Sponsor	Default	

Displaying 1 - 4 of 4

Powered by

Add Local User

Following is a sample web page where you can add a user to a Local Password Repository. Enter the user name, password, and specify the password repository, then click **Submit** to add the user. The user entry displays on the Local User web page.

Sample Add Local User Page

The screenshot shows the 'Local User Administration: Local Users' page in the Extreme Networks management interface. The page title is 'MAC Registration System Administration'. It contains a form with the following fields:

- *User Name:
- First Name:
- Last Name:
- *Display Name:
- *Password:
- *Confirm Password:
- Description:

At the bottom of the form are 'Submit' and 'Cancel' buttons. The page footer includes the text 'Powered by' and the Extreme Networks logo.

Pre-Registration Portal

The Pre-Registration Portal web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials. Pre-registration must be enabled in the Edit Portal Configuration window for the page to be available. For more information on pre-registration, see [How to Configure Pre-Registration](#).

Sample Pre-Registration Portal Page

Pre-Registration Portal

Pre-Registration Instructions go here.

Single User	Multiple Users
*User Type: Secure Guest Access	*CSV File: Browse... No file selected.
*User Name:	Generate Passwords: <input type="checkbox"/>
*First Name:	Password Repository: From CSV File
*Last Name: admin	Upload
Generate Password: <input type="checkbox"/>	CSV Template With Password and Repository Fields
*Password: ●●●●●●●●	CSV Template Without Password and Repository Fields
*Confirm Password:	
*Expires Time: 03/23/2014 16:52:35	
Middle Name:	
*E-Mail Address:	
*Phone Number:	
*Mobile Service Provider: AT&T	
Pre-Register User	

Powered by Extreme Networks

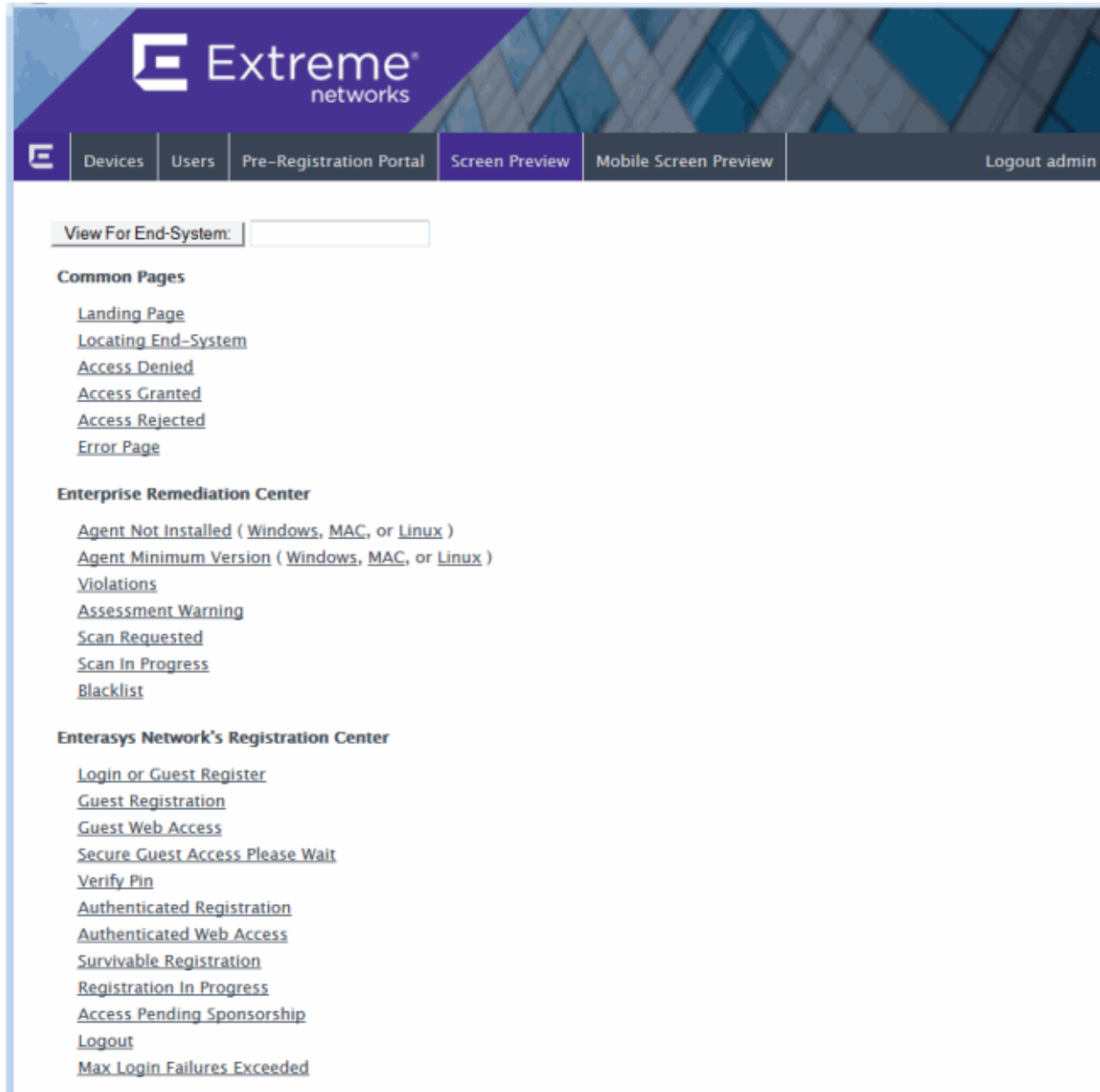
Screen Preview

The Screen Preview web page allows you to preview the web pages that may be accessed by the end user during the remediation and registration process. You can also access this web page using the Appliance Portal Pages button at the bottom of the [Edit Portal Configuration window](#).

A useful feature on this web page is View for End-System. You can enter an end user's IP address in the field and click View for End-System button to see the captive portal web page that the end user is looking at. Using this view, you can actually register or remediate the end-system, and change the end-system's

state. This is useful when attempting to help an end user that is having trouble on a web page.

Sample Screen Preview Page



The screenshot displays the Extreme Networks registration administration interface. The top navigation bar includes the Extreme Networks logo and the following tabs: Devices, Users, Pre-Registration Portal, Screen Preview (selected), Mobile Screen Preview, and Logout admin. Below the navigation bar, there is a search field labeled "View For End-System:". The main content area is organized into three sections:

- Common Pages**
 - [Landing Page](#)
 - [Locating End-System](#)
 - [Access Denied](#)
 - [Access Granted](#)
 - [Access Rejected](#)
 - [Error Page](#)
- Enterprise Remediation Center**
 - [Agent Not Installed \(Windows, MAC, or Linux \)](#)
 - [Agent Minimum Version \(Windows, MAC, or Linux \)](#)
 - [Violations](#)
 - [Assessment Warning](#)
 - [Scan Requested](#)
 - [Scan In Progress](#)
 - [Blacklist](#)
- Enterasys Network's Registration Center**
 - [Login or Guest Register](#)
 - [Guest Registration](#)
 - [Guest Web Access](#)
 - [Secure Guest Access Please Wait](#)
 - [Verify Pin](#)
 - [Authenticated Registration](#)
 - [Authenticated Web Access](#)
 - [Survivable Registration](#)
 - [Registration In Progress](#)
 - [Access Pending Sponsorship](#)
 - [Logout](#)
 - [Max Login Failures Exceeded](#)

Related Information

- [Registration Concepts](#)
- [How to Set Up Registration](#)

- [Sponsored Registration](#)
- [Edit Portal Configuration Window](#)

Sponsored Registration

Sponsored registration is configured in the Guest Registration and Secure Guest Access views in the [Edit Portal Configuration window](#). An admin\sponsor email address is specified, which is typically the network NAC administrator, for example "IT@CompanyA.com." This email address is always notified, in addition to any sponsor email address that is entered by the end user when they register to the network. Administrators can also specify a sponsor when manually registering an end user via the [Registration Administration web page](#).

When an end-system is registered to the network, it remains registered until it is administratively revoked. Because of this, it may be desirable to allow sponsors to view, delete, and add registered end-systems that they have or will sponsor. This is achieved by granting sponsor access to the Registration Administration web page (using the Administration view in the [Edit Portal Configuration window](#)). Administrators can also limit a sponsor's view to only their own sponsored end users, also from the Administration view.

The Sponsor Administration Page is served securely over HTTPS at `https://<NAC Gateway Name or IP address>/sponsor` and protected with a username and password login. For more information, see the Help topic on the [Registration Administration web page](#).

Related Information

- [How to Configure Sponsorship for Guest Registration](#)
- [Registration Concepts](#)
- [How to Set Up Registration](#)
- [Edit Portal Configuration Window](#)
- [Registration Administration](#)

How to Configure Pre-Registration

This Help topic describes how to configure and use NAC Manager's pre-registration feature as a part of Secure Guest Access or Authenticated Registration. With pre-registration, guest users can be registered in advance and given a username and password, allowing for a more streamlined and simple registration process when the guest user connects to the network. This can be particularly useful in scenarios where guest users will be attending a company presentation, sales seminar, or a training session.


Pre-registration allows IT to delegate control of the network registration process to less technical personnel such as company receptionists, administrative assistants, or training personnel. Using the pre-registration web portal, selected personnel can easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials. The guest user then follows the instructions on the voucher to connect to the corporate network.

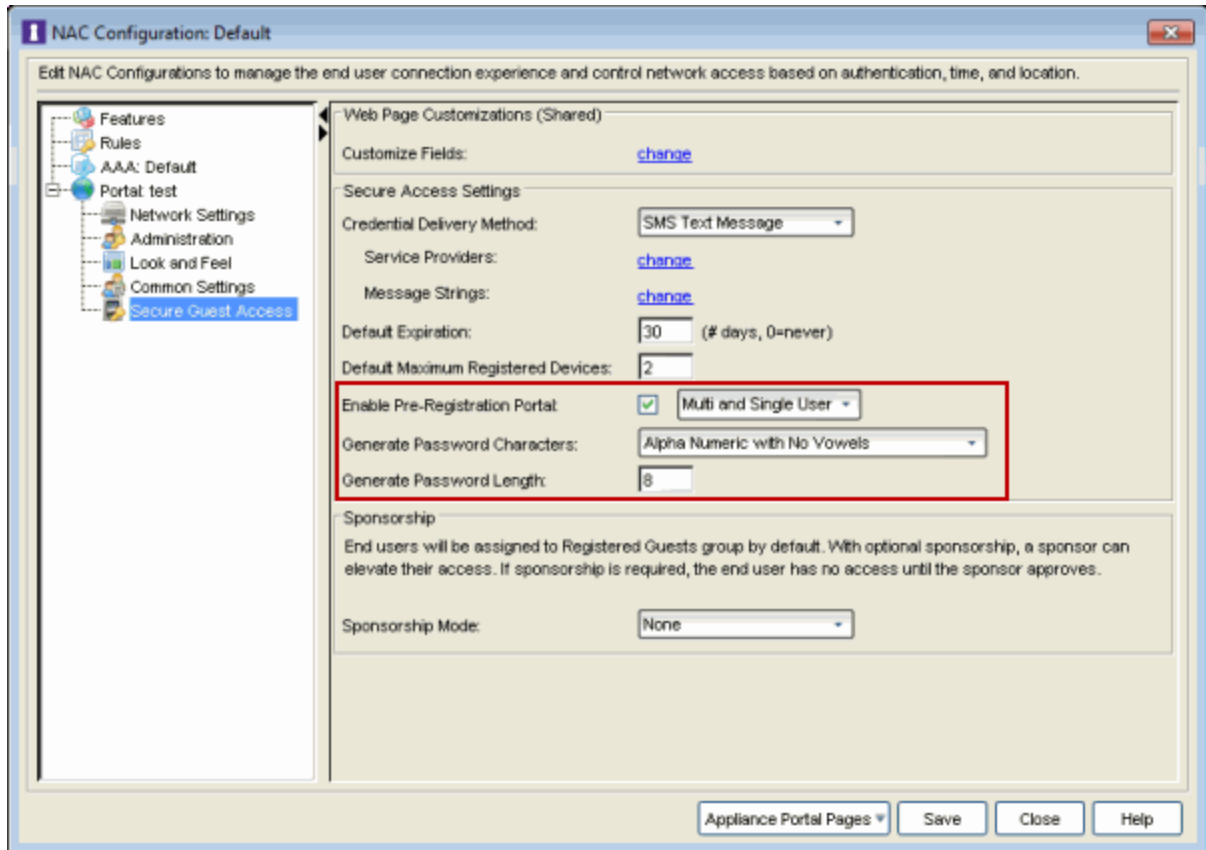
This topic includes information and instructions on:

- [Configuring Pre-Registration](#)
- [Pre-Registering Guest Users](#)
 - [Pre-Registering a Single User](#)
 - [Pre-Registering Multiple Users](#)

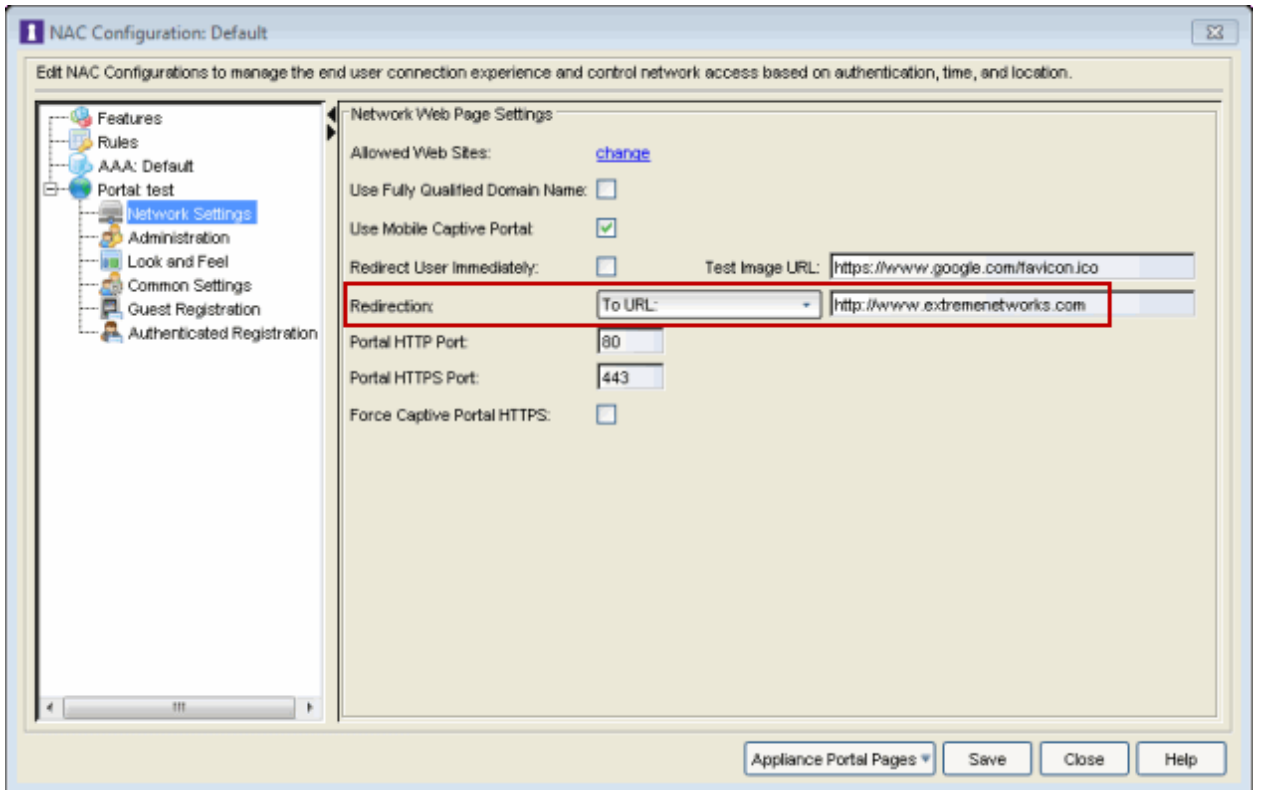
Configuring Pre-Registration

Following are instructions for configuring pre-registration in your portal configuration.

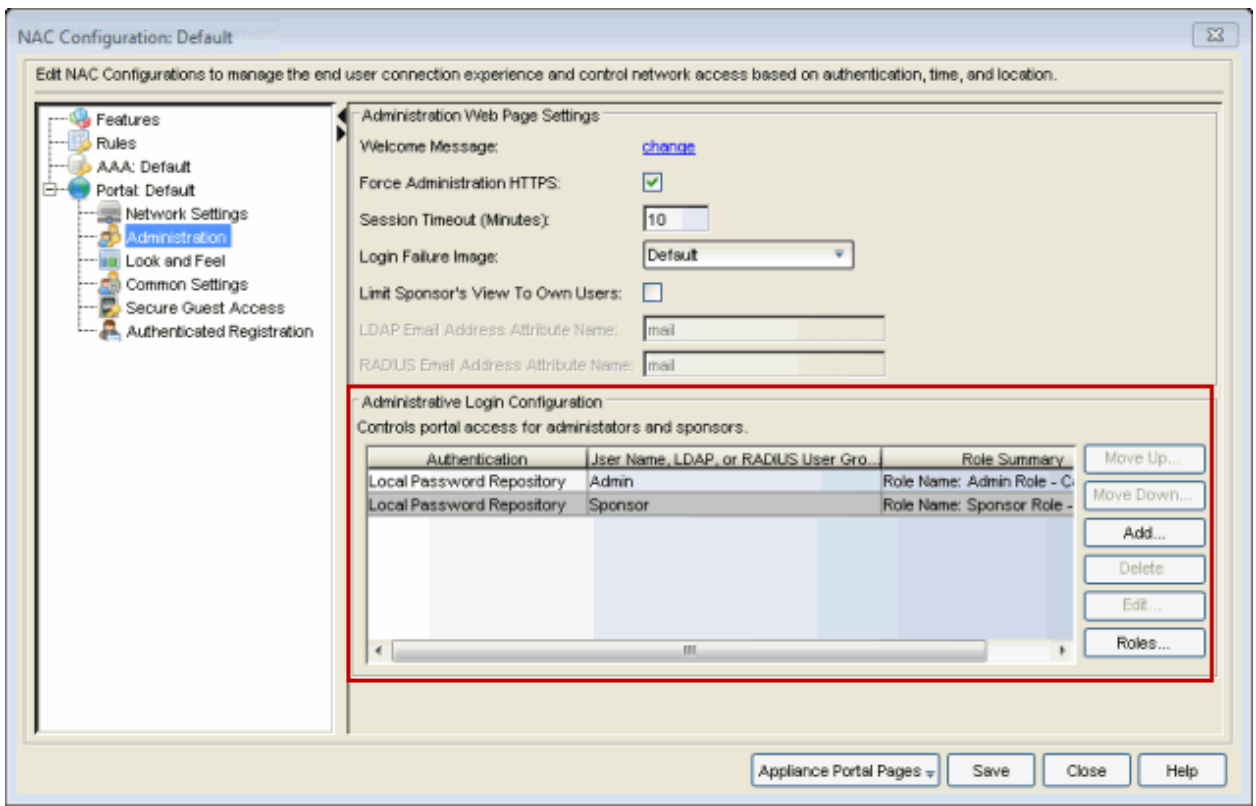
1. Use the NAC Manager  toolbar button to open the NAC Configuration window.
2. In the left-panel tree, expand the Portal icon and click on the [Secure Guest Access](#) view or the [Authenticated Registration](#) view (depending on the access type you are configuring).



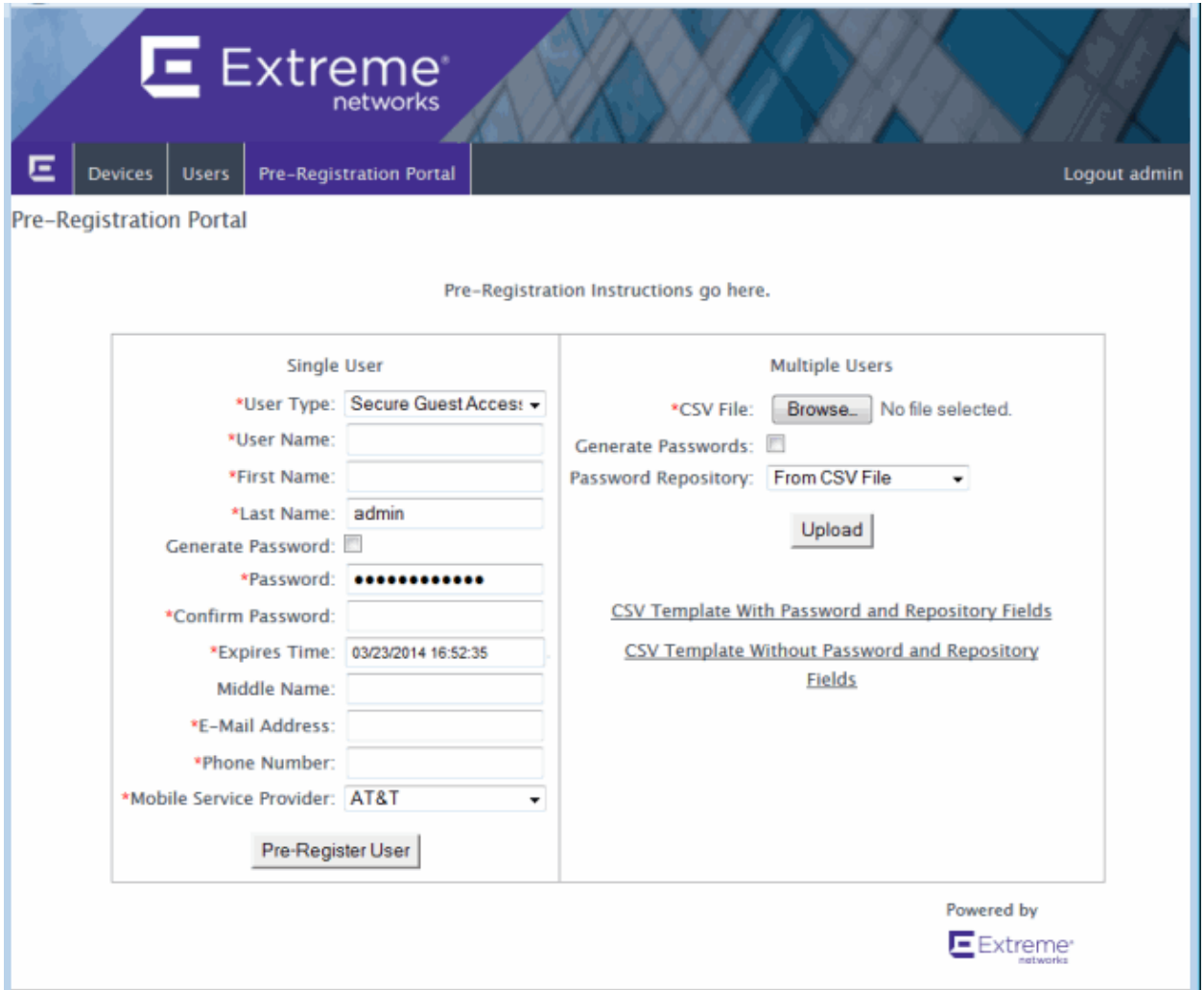
3. Select the **Enable Pre-Registration Portal** checkbox and specify whether personnel will be able to register a single user, multiple users, or both single and multiple users.
4. Set the **Generate Password Characters** and **Generate Password Length** options. NAC Manager will use these options when generating passwords for guest users to use when connecting to the network. These settings are shared by Authenticated Registration and Secure Guest Access. Changing it for one access type will also change it for the other.
5. For Authenticated Registration, click on the [Network Settings](#) view to configure the connection URL that will be specified on the Guest User Voucher (for example, www.ExtremeNetworks.com). Enter the URL in the **Redirection To URL** field. For Secure Guest Access, the Guest User Voucher will provide instructions for connecting directly to the secure SSID.



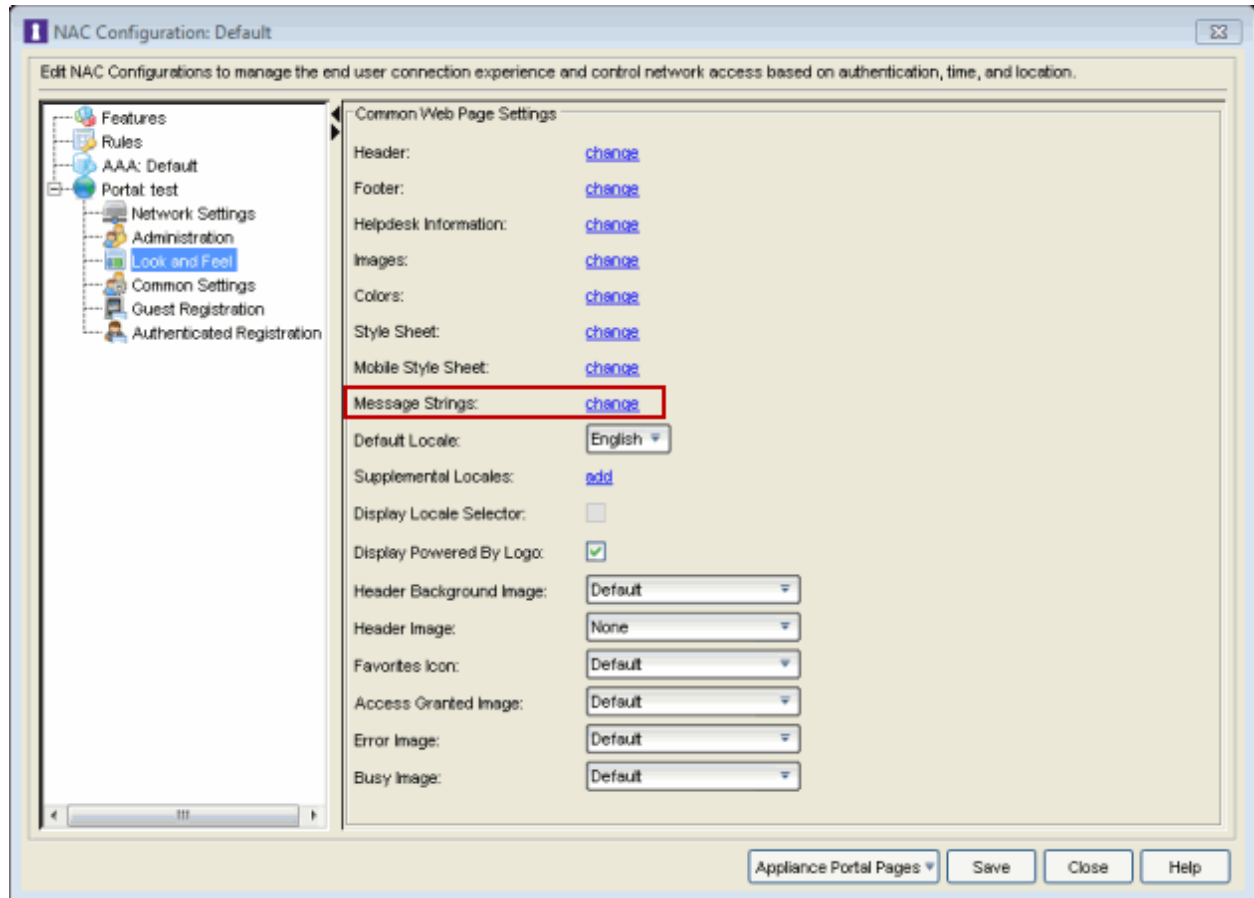
6. Click on the [Administration](#) view to configure administrative login privileges for the users that will have access to the Pre-Registration Portal. These users will then be able to log in to the Pre-Registration Portal and pre-register guests. For information on how to configure users, see [Administrative Login Configuration](#).



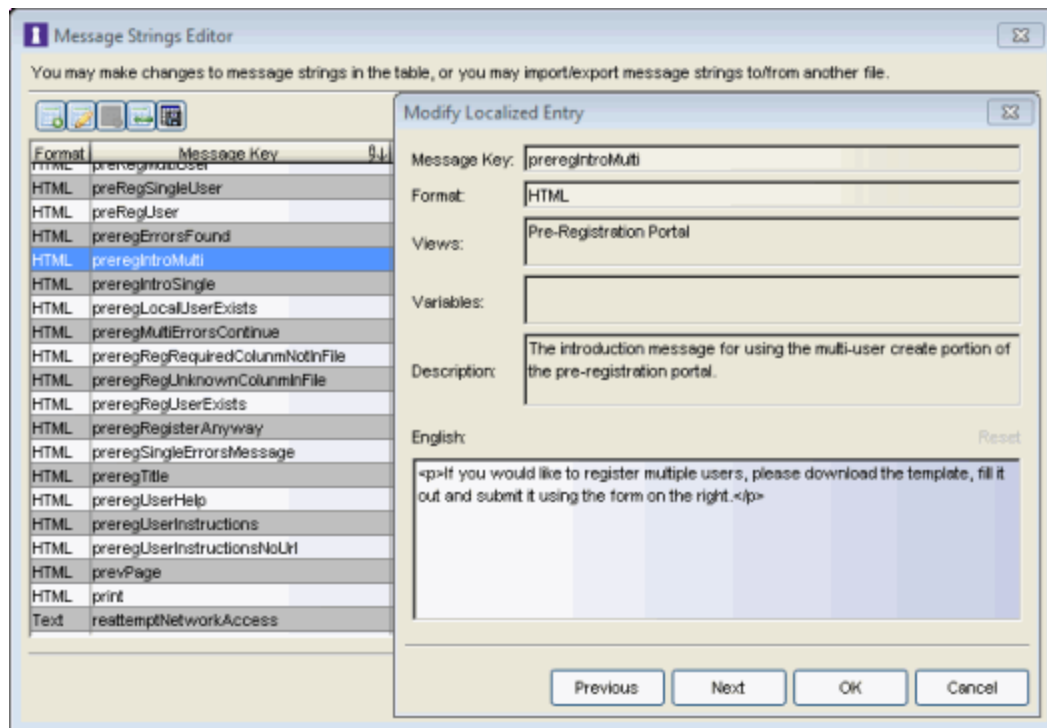
7. Click **Save** to save your changes. Enforce your NAC Configuration to your appliances.
8. Access the Pre-Registration Portal using the **Appliance Portal Pages** button at the bottom of the NAC Configuration window or by entering the following URL in a browser window:
https://<NACApplianceIP>/pre_registration



9. At the top of the portal web page you will see instructions for the people who will be performing the pre-registrations. To modify and edit these instructions:
 - a. In the NAC Configuration window, access the [Look and Feel](#) view.



- b. Click on the Message Strings "change" link. The Message Strings Editor window opens.
- c. Scroll down to the "preregIntroMulti" or "preregIntroSingle" message key and double-click that line. The Modify Localized Entry window opens.



- d. Enter any changes or modifications you wish to make to the instructions, and click **OK** to close the windows.
 - e. Enforce the changes to your appliances.
 - f. Refresh the browser window to see the new instructions in the Pre-Registration Portal.
10. The following sections provides information on how to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register).

Pre-Registering Guest Users

After you have configured pre-registration, provide the URL for the Pre-Registration Portal (`https://<NACApplianceIP>/pre_registration`) to the personnel who will be pre-registering guests. This may be network administrators or it may be personnel such as company receptionists, administrative assistants, or training personnel. (These users must be configured with [administrative login privileges](#) to access the web page).

The following sections provide steps for pre-registering single or multiple users in the Pre-Registration Portal.

Pre-Registering a Single User

Use the instructions in this section to pre-register a single end user using the Single User panel in the Pre-Registration Portal.

The screenshot shows a web form titled "Single User" for pre-registering a user. The form includes the following fields and values:

- *User Name:
- *First Name:
- *Last Name:
- Generate Password:
- *Password:
- *Confirm Password:
- *Expires Time:
- Middle Name:
- *E-Mail Address:
- *Phone Number:
- *Mobile Service Provider:

A "Pre-Register User" button is located at the bottom of the form.

1. Enter the information for the guest user you want to pre-register. Fields with a red asterisk are required.
 - User Name - Enter the user name that the guest user will use when connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames.
 - First Name/Last Name - Enter the guest user's first and last name. The name will be printed on the voucher along with their registration credentials.
 - Password/Confirm Password - Enter and confirm the password that the guest user will use when connecting to the network. Select the Generate Password checkbox if you want NAC Manager to automatically generate a password for you.
 - Password Repository - When you pre-register the user, their credentials are automatically added to the local password repository specified here. Local Password Repositories are configured in the [AAA Configuration](#) window. (You only see this field if you have multiple repositories.)

- Expires Time - Select a registration expiration date from the calendar. The time is automatically set to 0:00:00, which is midnight. You can enter a specific time, if desired.

NOTE: You can add additional fields to be displayed here using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view or Secure Guest Access view. However the Pre-Registration web page will always display the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher that will be printed out.

2. Click the **Pre-Register User** button to register the user. The user will be added to the local password repository and added to the Registration Administration web page.
3. A voucher (see [example](#) below) will be generated that provides registration instructions and the guest user's registration credentials. Print out this voucher to give to the guest user.

IMPORTANT: The voucher must be printed out immediately, as there is no way to go back and print out a voucher once you leave the web page. If you do not print out the voucher, the voucher will have to be created by hand. In the event that the "Generate Password" option was used, you will need to modify the guest user password using the registration administration page or local repository administration.

4. To register another user, you must re-access the Pre-Registration page by using the browser's back button or re-entering the URL.

Pre-Registering Multiple Users

Use the instructions in this section to pre-register multiple end users at one time using the Multiple Users panel in the Pre-Registration Portal. When pre-registering multiple users, create a CSV file to provide all the user credential information in table form. Then, upload the file to NAC Manager to perform the pre-registration.

Multiple Users

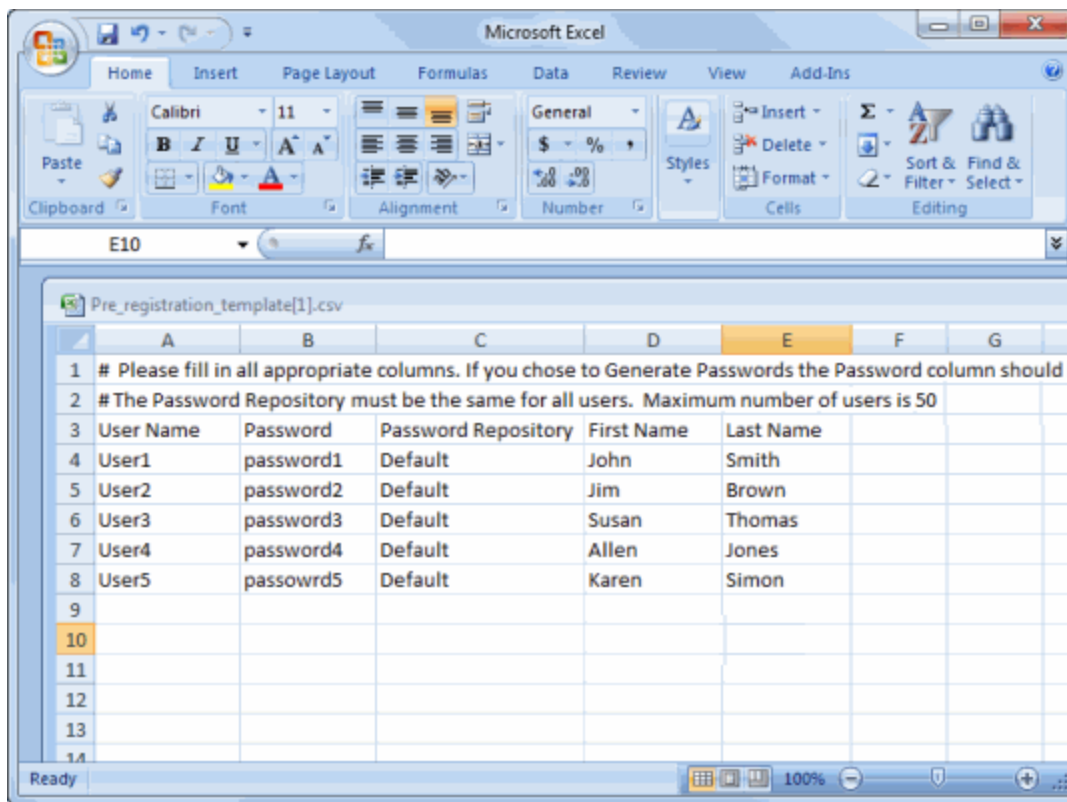
*CSV File: No file chosen

Generate Passwords:

Password Repository:

[CSV Template With Password and Repository Fields](#)
[CSV Template Without Password and Repository Fields](#)

1. Click the CSV Template link to open a template CSV file where you will create your list of guest users to pre-register. You can use a CSV template that includes password and password repository fields or not, depending on your network requirements. Do not change any of the column headings in the file.



Following is an explanation of the columns that need to be filled in for each user, depending on the template you selected.

- User Name - Enter the username that the guest user will use when connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames. (If you do try to pre-register existing usernames along with new usernames, you will be notified of the error and given the option to continue registering the new names.)
- Password - Enter the password that the guest user will use when connecting to the network. If you want NAC Manager to automatically generate end user passwords, leave the password column blank and select the Generate Passwords checkbox on the Multiple Users panel.
- Password Repository - When you pre-register the user, their credentials will automatically be added to the local password repository specified here. Local Password Repositories are configured in the [AAA Configuration](#) window. If you are using the Default repository, you can use the Password Repository drop-down list (in the Multiple Users section) to select Default, and then you don't have to enter the Password Repository for each entry.
- First Name/Last Name - Enter the guest user's first and last name. The name will be printed on the voucher along with their registration credentials.

NOTE: You can add additional columns to be included in the template using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view and Secure Guest Access view. However the template will always display the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher that will be printed out.

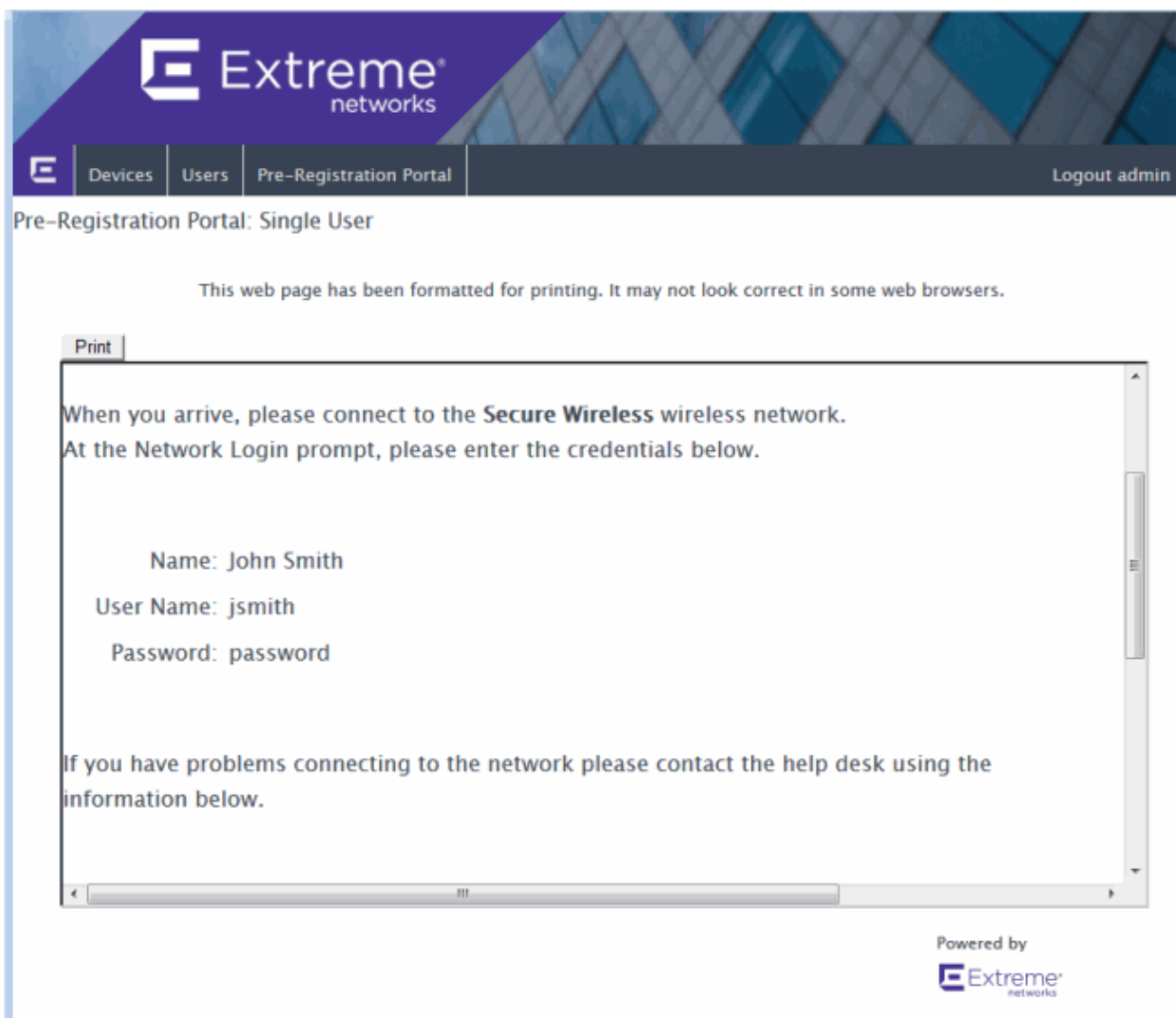
2. When you have finished entering the guest user information, save and close the file.
3. Back in the Multiple Users panel, enter the path and filename for the CSV file by using the **Browse** button to browse to the file on your system.
4. If your CSV file includes a Password Repository, use the Password Repository drop-down list to specify whether to use the default repository or the repository specified in the file.
5. Click the **Upload** button. Users will be added to the local password repository and to the Registration Administration web page.

- Individual vouchers (see an [example](#) below) will be generated that provide registration instructions and the guest user's registration credentials for each guest user. Print out these vouchers to give to the guest users.

IMPORTANT: Vouchers must be printed out immediately, as there is no way to go back and print out a voucher once you leave the web page. If you do not print out the vouchers, the vouchers will have to be created by hand. In the event that the "Generate Password" option was used, you will need to modify the guest user passwords using the registration administration page or local repository administration.

- To register another user, you must re-access the Pre-Registration Portal by using the browser's back button or re-entering the URL.

Sample Guest User Voucher



Related Information

- [Portal Configuration](#)
- [How to Set Up Registration](#)

How to Set Up Assessment

NAC Manager utilizes assessment servers to determine the security compliance of end-systems connecting to the network. Assessment servers assess connecting end-systems and provide details about the end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining security compliance. End-systems that fail assessment can then be quarantined with restricted network access to prevent security threats from entering the network. For more information on assessment and an overview of how it works, see the [Assessment](#) section of the Concepts help file.

The NAC solution requires the use of either on-board (integrated) assessment server functionality or the ability to connect to external assessment servers, in order to execute end-system assessment. Refer to the NAC Design Guide for information on determining the number of assessment servers and their location in the network, and configuring assessment server software.

In NAC Manager, you will need to configure the external assessment servers that will perform the end-system assessments in your network. Once you have configured your assessment servers, they can be added to an assessment server pool and participate in assessment server load-balancing.

NAC Manager uses *assessment configurations* to define the different assessment requirements for end-systems. They define how to score assessment results (determined by the selected Risk Level and Scoring Override configurations), and what assessment tests to run (determined by the selected test sets). NAC Manager provides default assessment configurations ready for you to use "as is" or allows you to create custom assessment configurations for your specific network requirements.

When you create a NAC Profile, you will select an assessment configuration that defines the assessment requirements for the end-systems using that profile.

This Help topic describes the steps that must be performed in NAC Manager when deploying assessment on your network, beginning with managing your assessment servers.


NOTES: -- Prior to configuring assessment, you must enable the Assessment/Remediation for End-Systems option in the NAC Manager Features options accessed from Tools > Options in the NAC Manager menu bar.
-- If you are configuring Agent-based assessment, you will need to perform the steps outlined in the [How to Deploy Agent-Based Assessment](#) Help topic in addition to the steps described here.

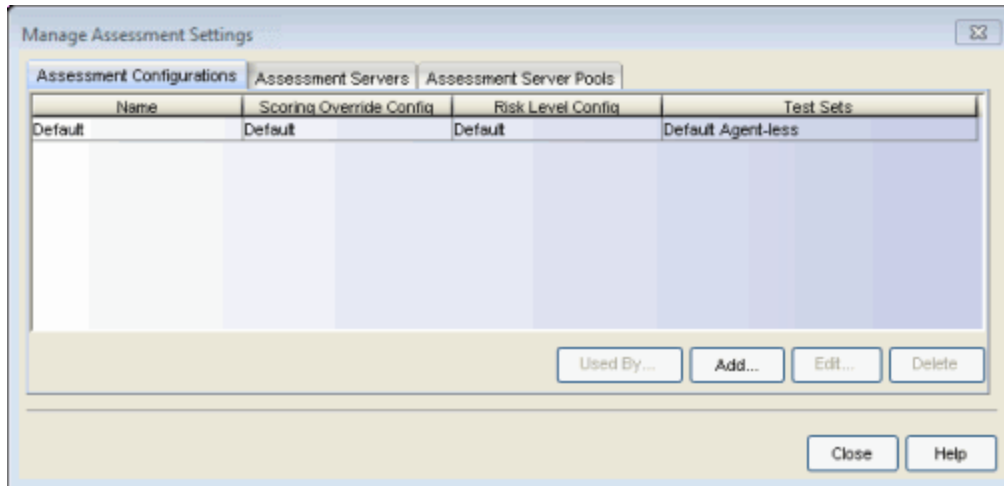
Information and instructions on:

- [Managing Your Assessment Servers](#)
- [Adding External Assessment Servers](#)
- [Creating Assessment Configurations](#)
 - [Scoring Override Configuration](#)
 - [Risk-Level Configuration](#)
 - [Test Sets](#)
- [Enabling Assessment for NAC Profiles](#)

Managing Your Assessment Servers

The Manage Assessment Settings window is the main window used to manage and configure your assessment servers.

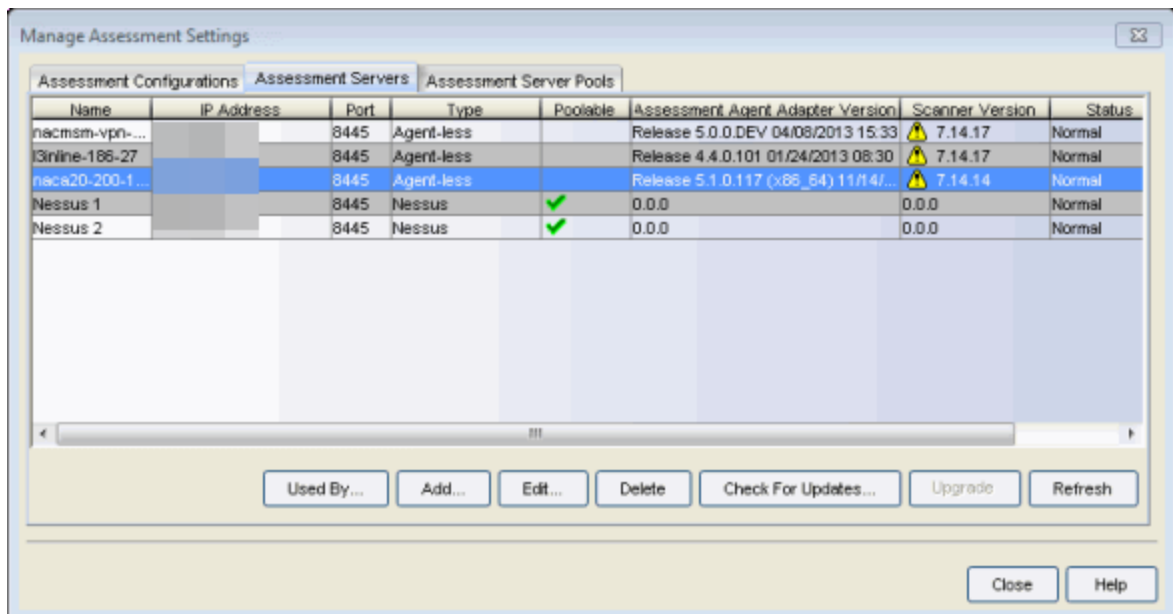
1. In NAC Manager, select **Tools > Management and Configuration > Assessment Settings** from the menu bar or click the Manage Assessment Settings toolbar button  to open the Manage Assessment Settings window.



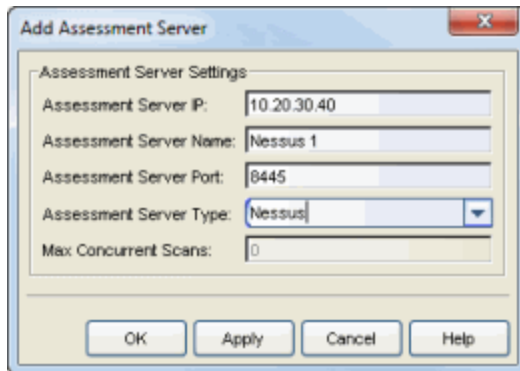
Adding External Assessment Servers

If you are using external assessment servers, the first step in setting up assessment in NAC Manager is to add your external assessment servers to the Manage Assessment Settings window. Once you have added your assessment servers, they can participate in assessment server load-balancing, and be used in an assessment server pool, if desired.

1. From the Manage Assessment Settings window, select the Assessment Servers tab.



2. Click **Add** to open the Add Assessment Server window.



Refer to the [Add Assessment Server window](#) Help topic for information on adding Assessment Servers. Click **OK**. The added assessment server will be listed in the tab.

3. Click back to the Assessment Configurations tab and proceed to creating assessment configurations.

Creating Assessment Configurations

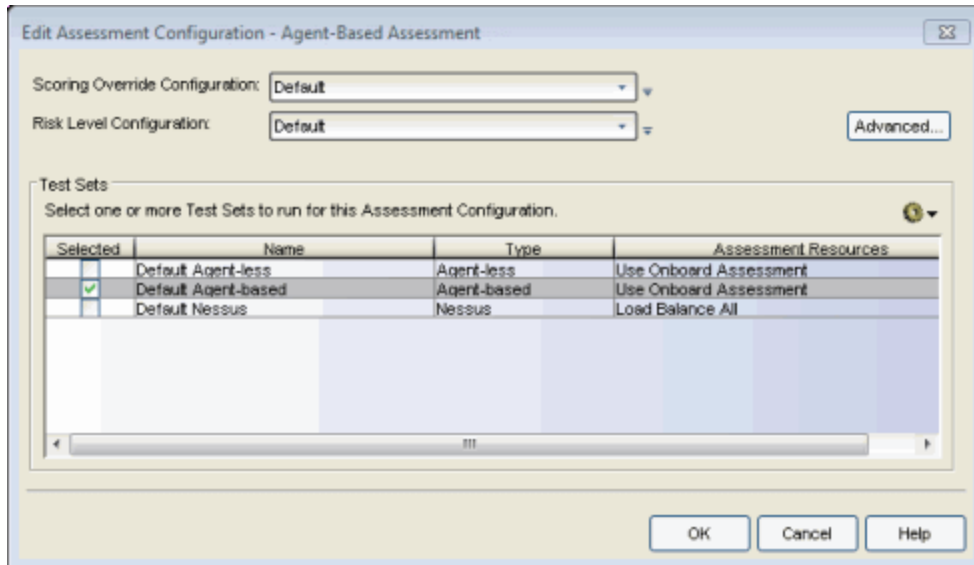
The next step in setting up assessment in NAC Manager is to create your assessment configurations. Assessment configurations define the different assessment requirements for end-systems connecting to your network. When you create a NAC Profile, you will select an assessment configuration that defines the assessment requirements for the end-systems using that profile.

It is recommended that you introduce assessment on your network using the phased deployment described in the [NAC Assessment Phased Deployment Guide](#). A phased approach minimizes disruptions to your enterprise, introduces end users to remediation procedures gradually, and increases your understanding of the strengths and weaknesses in the network.

However, while the phased deployment is the recommended approach, NAC Manager does provide a default assessment configuration that is already set up with default assessment parameters and is ready to use in your NAC Profiles.

The following steps discuss how to access the default assessment configuration and edit it, if desired. (For more information on the phased assessment deployment, see the [NAC Assessment Phased Deployment Guide](#) and [How to Configure Assessment](#).)

1. From the [Manage Assessment Settings window](#), select the Assessment Configurations tab. Select the Default configuration and click **Edit** to open the Edit Assessment Configuration window.



2. The window displays the assessment parameters configured in the Default configuration, and allows you to edit the assessment parameters, if desired.
 - a. **Scoring Override Configuration:**

Scoring overrides let you override the scoring mode and test result scores for a particular assessment test. The default scoring override configuration provided by NAC Manager specifies no overrides, but can be edited to contain overrides, if desired.


Scoring overrides let you create overrides to the test scoring system and assign a higher or lower score to specific assessment tests. For example, Nessus assessment checks to see if Limewire is installed on an end-system, and assigns a low risk score of "2" for that test result if it is found. Using a scoring override, you can assign a high risk score of "10" to that result instead of "2".

Scoring overrides also allow you to override the [scoring mode](#) for specific assessment tests. For example, you may set a test set scoring mode of "Informational Only" and then configure a scoring override so that a specific test counts towards a quarantine decision ("Apply Score"). Or, you may select a test set scoring mode of "Apply Score"


(quarantine), and then create a scoring override that sets specific tests to be "Warning."

To edit the default configuration, click the configuration menu button  to the right of the field and select **Edit**. For more information, refer to the [Add/Edit Scoring Override Configuration Window](#) Help topic.

b. **Risk Level Configuration:**

Risk level configurations determine how assessment results are classified into one of three risk levels: high risk, medium risk, or low risk. To edit the default risk level configuration, click the configuration menu button  to the right of the field and select **Edit**. For more information, refer to the [Add/Edit Risk Level Configuration window](#) Help topic.

c. **Test Sets:**

Select one or more test sets for the assessment configuration to run. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use. NAC Manager provides three default test sets and also lets you create new custom test sets. To create a new test set, use the configuration menu button  in the test set section to select the type of test set you want to add. For instructions on creating a new test set, refer to the following Help topics:

- [Add Agent-based Test Set](#)
- [Add Agent-less Test Set](#)
- [Add Nessus Test Set](#)
- [Add Other Test Set](#)

If you select multiple agent-based test sets, the first test set you select is called the Master test set. A Master test set includes the Agent Configuration settings, the Advanced Settings, and all the specified test cases. Each subsequent agent-based test set that you select for the configuration will be a "supporting" test set. For supporting test sets, only the "Application" test cases will be used; all other

configuration values will be ignored. In the list of Test Sets, Master test sets have a "(Master)" designation after them.

For example, you might want to use multiple agent-based test sets if you are managing multiple networks, and you have a unique agent-based test set for each network as well as secondary test sets for specific application tests that all the networks would use. In the assessment configuration for each network, you would select the unique test set as the Master test set and then select any number of secondary test sets to be included in the configuration as well.




If the Master test set is deselected, then a new master is automatically selected. If this is not the specific test set that you would like to have as Master, then you must deselect all test sets, select the desired Master test set first, and then select the additional supporting test sets.

d. Click **OK** to save your changes.

3. Proceed to enabling assessment for your NAC profiles.

Enabling Assessment for NAC Profiles

After you have created your assessment configuration, you must enable assessment for the NAC Profiles used by the rules in your NAC Configuration and specify the assessment configuration to use.

1. In NAC Manager, click the Manage NAC Profiles button  on the toolbar to open the [Manage NAC Profiles window](#).
2. Select a NAC Profile and click the Edit Profile button .
3. In the [Edit NAC Profile window](#), check the **Enable Assessment** checkbox, and select the desired assessment configuration.
4. Click **OK** to close the window.
5. You must enforce the updated NAC Configuration to your NAC appliances. Click the Enforce button  in the NAC Manager toolbar.

Related Information

- [Edit Assessment Configuration Window](#)
- [How to Deploy Agent-Based Assessment](#)
- [How to Set Up Assessment Remediation](#)

NAC Assessment Phased Deployment Guide

The NAC Assessment Deployment Guide describes a phased approach to introducing assessment into your Extreme Access Control deployment. A phased approach minimizes disruptions to your enterprise, introduces end users to remediation procedures gradually, and increases your understanding of the strengths and weaknesses in the network. While the phased approach described in this document is not required, it is the recommended way to approach implementing assessment in your network.

The guide also provides information on NAC Manager tools used to monitor and evaluate assessment results and provide data on overall network health. In addition, the guide includes a section with assessment diagnostic and troubleshooting information, including options for disabling assessment if the need should arise.

The following topics are discussed:

- [Overview](#)
 - [Phased Deployment](#)
 - [How Assessments are Scored](#)
 - [Viewing Health Results](#)
 - [End User Notification](#)
- [Phased Deployment](#)
 - [Informational Assessment](#)
 - [Warning Assessment](#)
 - [Quarantine Assessment](#)
- [Agent-less Assessment](#)
 - [Agent-less Informational Assessment](#)
 - [Agent-less Warning Assessment](#)
 - [Agent-less Quarantine Assessment](#)
- [Agent-Based Assessment](#)
 - [No Agent Detected](#)
 - [Agent-Based Informational Assessment](#)

- [Agent-Based Warning Assessment](#)
- [Agent-Based Quarantine Assessment](#)
- [Combined Agent-less and Agent-Based Assessment](#)
 - [Combined Informational Assessment](#)
 - [Combined Warning Assessment](#)
 - [Combined Quarantine Assessment](#)
- [Monitoring Assessment Results](#)
 - [Search by Assessment Results](#)
 - [Statistical Reports](#)
 - [Web Monitor Individual Reports](#)
- [Diagnostics and Troubleshooting](#)
 - [Analyze Health Results](#)
 - [End-System Events](#)
 - [Extreme Access Control Engine Administration](#)
 - [Log Files](#)
 - [Disabling Assessment](#)

Overview

This section provides an overview of the phased approach to assessment deployment and gives a brief introduction to the three phases. It also discusses concepts important to understanding how assessment works, such as how assessments are scored, where to view assessment results, and how end users are notified of assessment results.

Phased Deployment

The assessment phased deployment lets you introduce assessment into your Extreme Access Control deployment in three distinct phases, with each new phase increasing the overall security of your network. Each phase provides the groundwork for the next phase, allowing for a smooth transition to a stricter level of network security enforcement.

The three assessment phases are:

1. **Informational Assessment**

End-systems connecting to the network are assessed for security

compliance. The assessment results are reported, but no action is taken against end-systems with vulnerabilities. This allows you to use assessment as a data-gathering mechanism without end-systems being quarantined.

2. Warning Assessment

End-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are notified. End users are provided with the means to remediate their vulnerabilities and achieve compliance, however end-systems which are not compliant can still access the network.

3. Quarantine Assessment

End-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are quarantined. End users are provided with the means to remediate their vulnerabilities and achieve compliance. Only end-systems which are compliant can access the network.

This table provides a summary of the capabilities provided by each of the three assessment phases.

	Informational	Warning	Quarantine
End-systems are assessed.	√	√	√
Results are collected for analysis.	√	√	√
End users are notified of vulnerabilities.		√	√
End users are provided with remediation tools.		√	√
Network access is denied to non-compliant end-systems.			√

How Assessments are Scored

When an assessment is performed on an end-system, a **health result** is generated. For each health result, there may be several **health result details**. A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 0.0 (no risk) to 10.0 (high risk). The sum of all of the health result detail scores is the health result's **total score**. The greatest health result detail score is the health result's **top score**. These two values are measures of the end-system's over-all risk level. NAC

Manager uses this risk level to determine whether or not the end-system will be allowed on the network or denied access (quarantined).

In NAC Manager, assessment tests are assigned a **scoring mode** which determines whether the resulting health result detail is applied towards the quarantine decision, or is used only for informational or warning purposes. Informational health result details can be used to gather information about the security risks on your network, while warning health result details allow you to notify end users when they have security risks that should be remediated. Informational or warning health result details have scores, however these scores are not considered when calculating the total score or top score. Therefore, informational or warning health result details do not impact the end-system's overall risk level.

An end-system's **actual score** is the sum of all of the health results, including informational and warning results. It is what the total score would have been if all the health result details had been applied. The actual score lets you see what the impact to end-system would be if informational health results are applied towards the quarantine decision.

For example, let's say an assessment is performed on an end-system, producing the following four health result details:

Health Result Detail	Scoring Mode	Score
#1	Apply Score	1.0
#2	Apply Score	3.0
#3	Informational	2.0
#4	Warning	3.0

The health result summary for the end-system would be:

Total Score 4.0 (Health Result Detail #1 plus #2)
 Top Score 3.0 (Health Result Detail #2)
 Actual Score 9.0 (Total of all health result details)

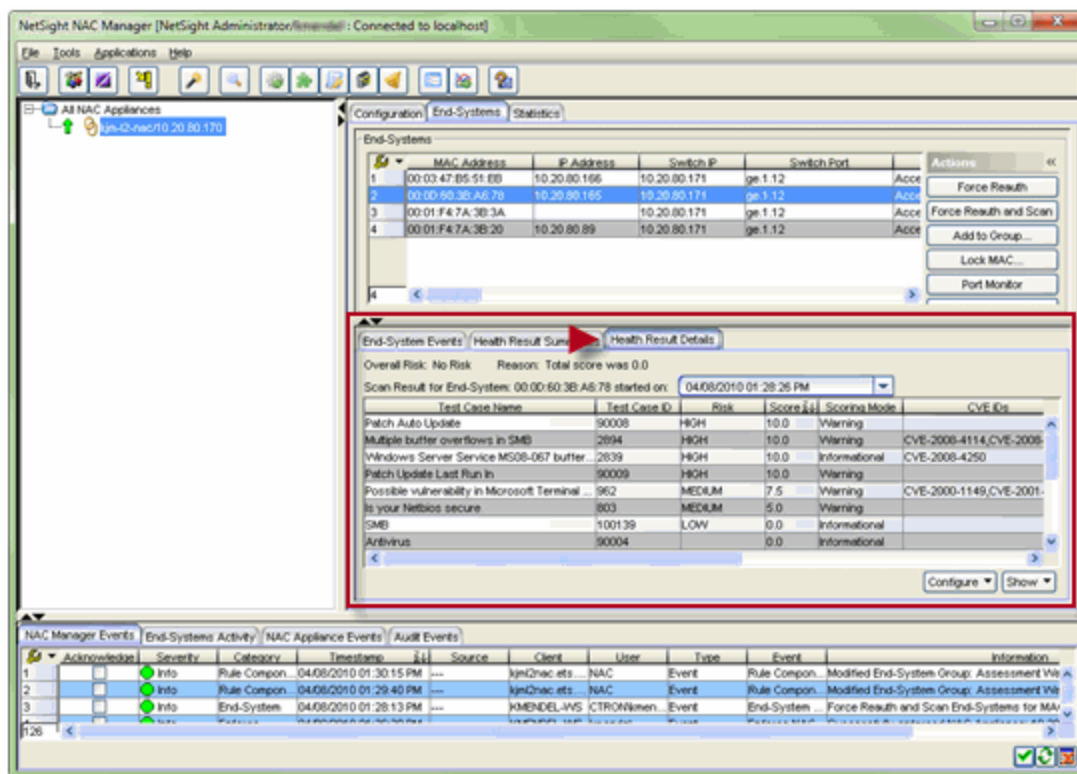
This table provides a summary of the capabilities provided by each of the three scoring modes.

	Informational	Warning	Apply Score
Health result is recorded.	✓	✓	✓
Contributes to total score and top score.			✓
Considered in the quarantine decision.			✓

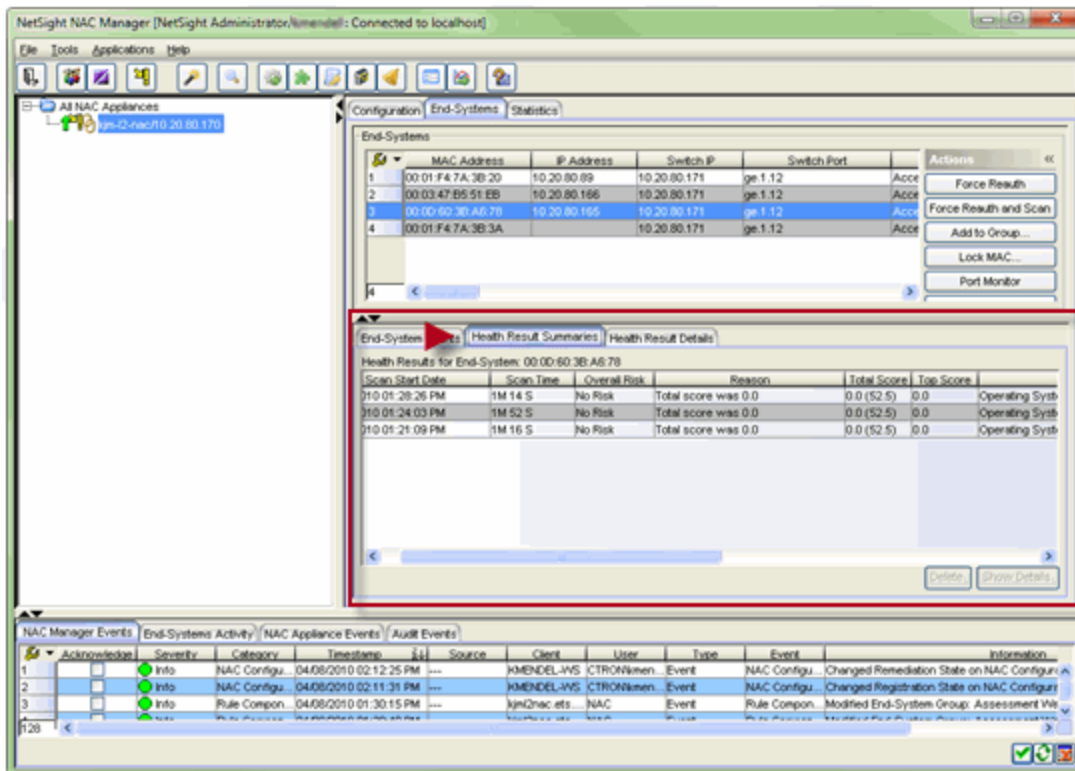
	Informational	Warning	Apply Score
End user is notified.		✓	✓
Contributes to actual score.	✓	✓	✓

Viewing Health Results

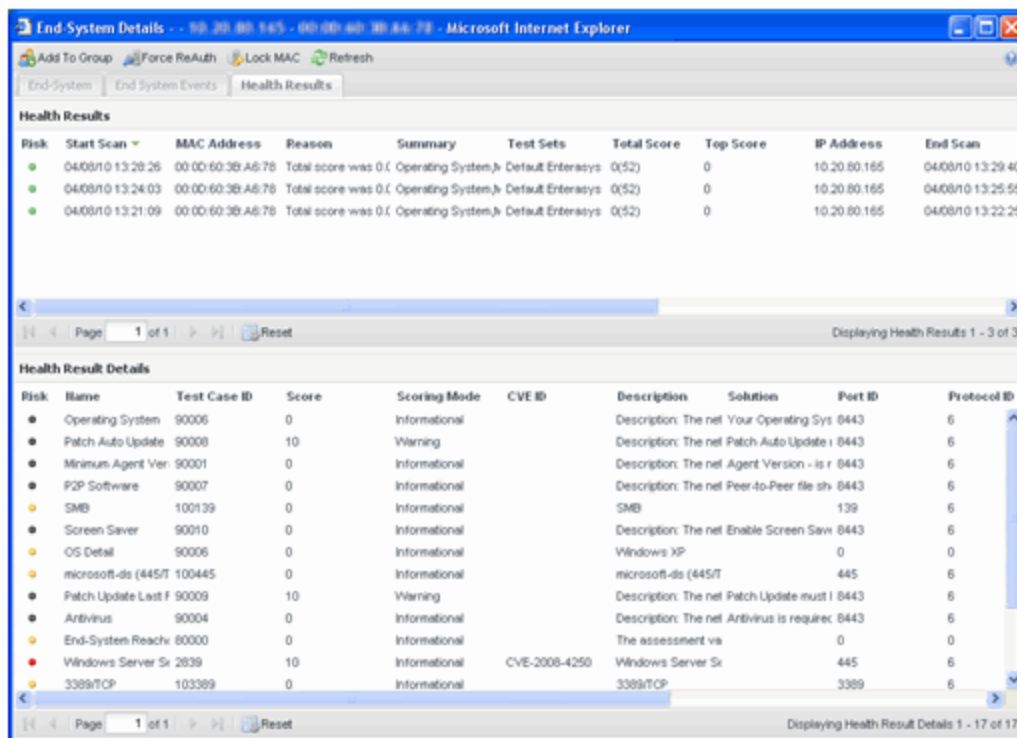
You can view health result summaries and health result details information several places in NAC Manager. In the [End-Systems tab](#), you can use the [Health Result Details tab](#) to view health result details for each end-system.



You can use the [Health Result Summaries tab](#) to view the total score and top score for each health result.



You can also access health result details and summary information in the [Health Results tab](#) of the End-Systems Details window.



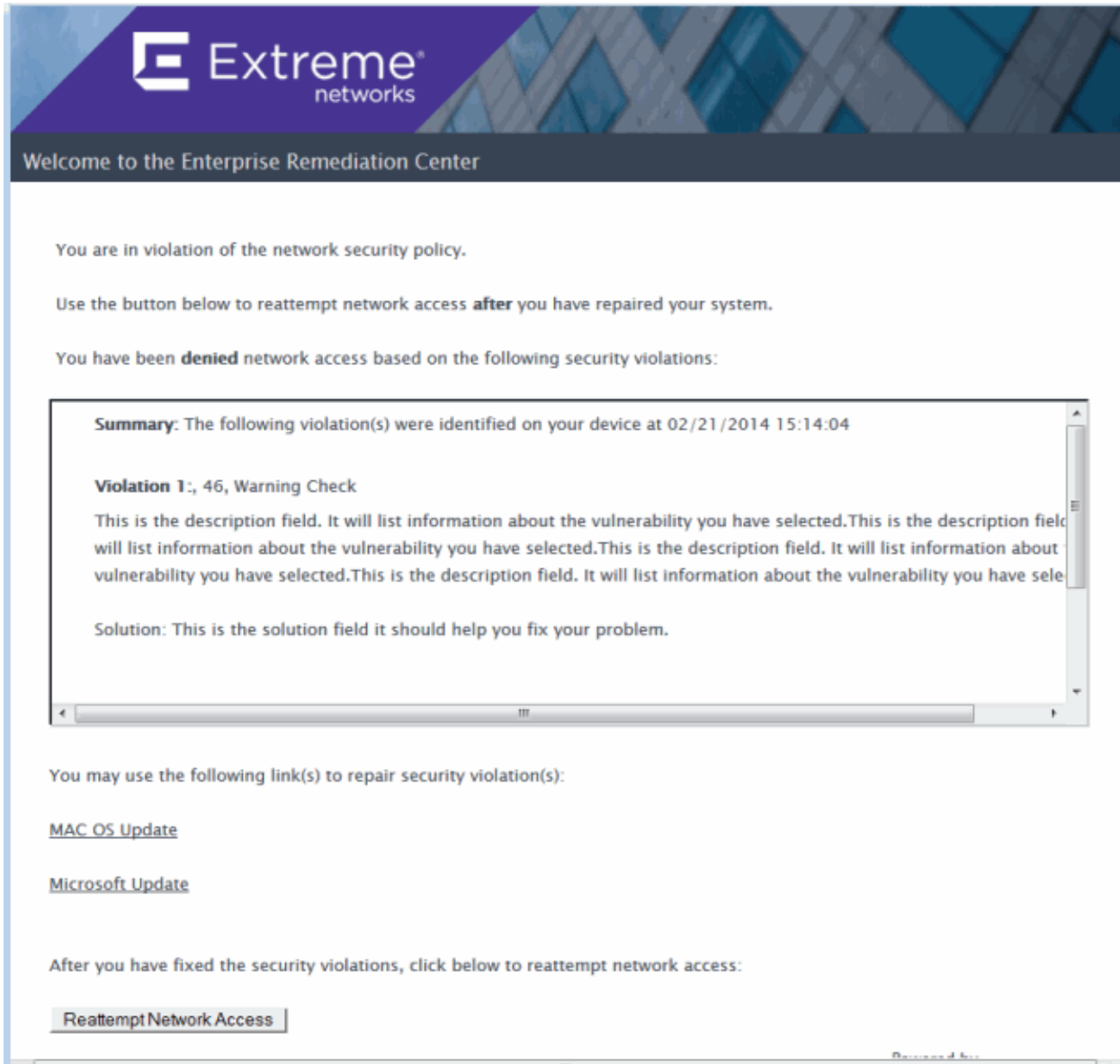
End User Notification

NAC Manager uses a web portal to notify end users of assessment violations and provide remediation information. The assessment notification can take the form of a quarantine notification or a warning notification, depending on the assessment configuration. If you are using agent-based assessment, the agent can be used to notify end users of assessment violations via a desktop notification instead of the web portal.

Web Portal Notification

Here is how quarantine and warning notifications are handled by the web portal:

Quarantine Notifications: If an end-system is quarantined due to its overall risk level, it cannot access the network and all web page requests are redirected to the web portal. Through the web portal, the end user is notified of the end-system's violations that have caused the quarantine. Remediation information is provided so that end users can clear the violations. When violations are cleared, and the end-system has passed another scan, the end-system can gain access to the network. In the image below, the web portal informs an end user of the end-system's security violations and presents remediation information so the end user can repair the violations and reattempt network access.



Warning Notifications: If an end-system has any health results that are warnings, all web requests are redirected to the web portal. Through the web portal, the end user is notified of the end-system's violations that have caused the warnings. Remediation information is provided so that the end user can repair the violations. The user only needs to acknowledge they have seen the warning notification. Once they do so, the end-system can gain access to the network. In the image below, the web portal informs an end user that they are in violation of network security policy, but is granted network access.

Extreme networks

Welcome to the Enterprise Remediation Center

You are in violation of the network security policy but will be granted to access the network.

Please repair the listed violations to secure your system.

Summary: The following violation(s) were identified on your device at 02/21/2014 15:18:32

Violation 1: 46, Warning Check

This is the description field. It will list information about the vulnerability you have selected. This is the description field. It will list information about the vulnerability you have selected. This is the description field. It will list information about the vulnerability you have selected. This is the description field. It will list information about the vulnerability you have selected.

Solution: This is the solution field it should help you fix your problem.

You may use the following link(s) to repair security violation(s):

[MAC OS Update](#)

[Microsoft Update](#)

After you have read the security violations, click below to acknowledge this warning:

Agent Notification

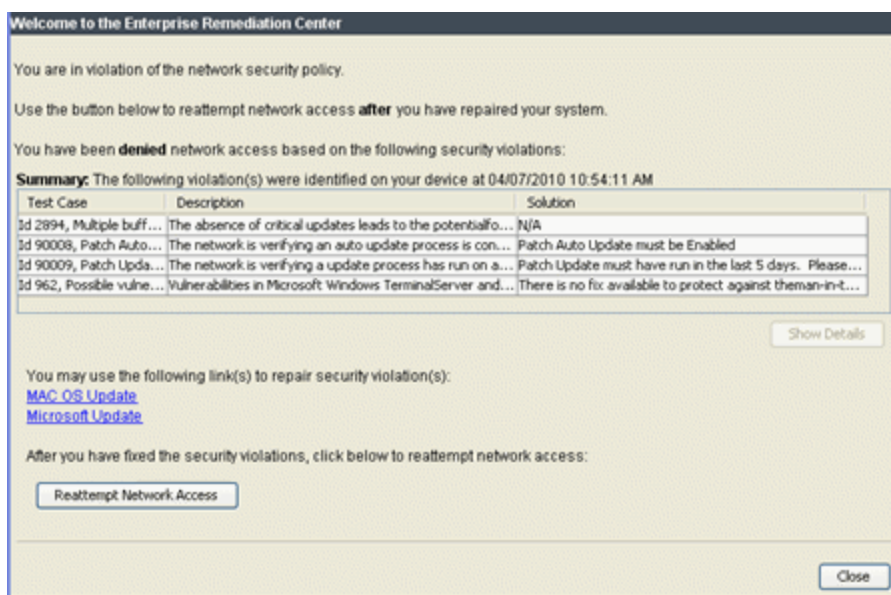
If your Extreme Access Control deployment uses agent-based assessment, the agent can be used to notify end users of assessment violations and provide remediation information. The information is displayed in an agent window on the desktop instead of the web portal remediation page. This allows remediation to take place with less hits to the portal remediation web server. (However, if the end user opens a browser window, they will still get the portal remediation web page.) You must have the Allow Agent Remediation option enabled in the [Advanced Agent Configuration window](#) and the Display Agent Notification Messages option enabled in the [Edit Agent-Based Test Set window](#) to use this

feature. For more information on agent notifications see [How to Deploy Agent-Based Assessment](#).

Here is how quarantine and warning notifications are handled by the agent:

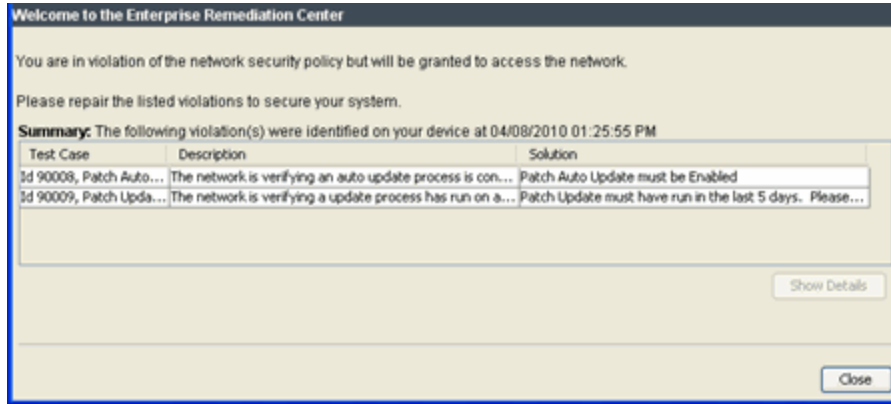
Quarantine Notifications: From a Quarantine Notification message or the agent icon, the end user can retrieve the list of violations that have caused the quarantine. Remediation information is provided so that end users can repair the violations. When violations are repaired and the end-system has passed another assessment, the end-system is allowed access to the network.

A sample agent remediation window for a Quarantine is shown below:



Warning Notifications: From a Warning Notification message or the agent icon, the end user can retrieve the list of violations that have caused the warnings. Remediation information is provided so that end users can repair the violations. The agent automatically acknowledges the warnings on behalf of the user, and the end-system immediately gains access to the network.

A sample agent remediation window for a Warning is shown below:



Phased Deployment

This section describes the three assessment phases and how they build on each other to provide a complete NAC assessment solution. The first phase implements informational assessment that provides a view into the security risks currently on your network. The second phase provides additional functionality allowing you to warn end users of security violations and provide remediation, while still allowing network access to all end users. The third phase provides the ability to quarantine non-compliant end-systems until they have remediated their violations. This phased approach allows you to derive value from the NAC assessment solution at each step along the way.

It is recommended that a new assessment configuration is created for each phase, rather than modifying the existing assessment configuration. This allows you to easily revert back to an earlier phase at any time by changing the assessment configuration that your NAC profile is using.

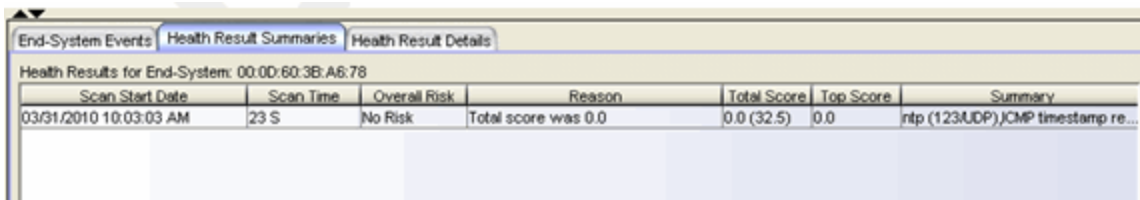
Informational Assessment

An Informational assessment will collect health results for the end-systems on your network, but will not use the health results to quarantine end-systems. This allows you to use assessment as a way to gather data about the security risks present on your network without denying end-systems access to the network. As data for end-systems is collected, you can use the NAC Manager search and reporting tools to gauge your overall network risk and identify frequently occurring vulnerabilities. See [Monitoring Assessment Results](#) for information on these tools.

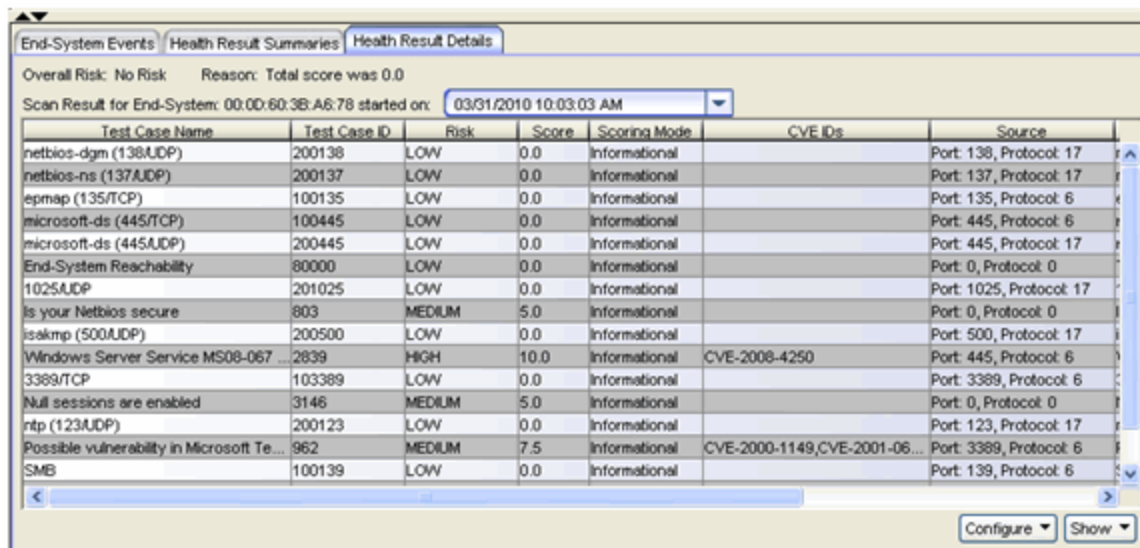
When you create an Informational assessment configuration, all health results are configured with an Informational scoring mode. End-systems connecting to the network will be assessed, and health results will be collected over time. All

end-systems will be considered to have no risk, and no end-systems will be quarantined.

The [Health Result Summaries tab](#) (shown below) will always show an overall risk of No Risk, a total score of 0.0, and a top score of 0.0. This is because all test results are considered informational and none are applied toward risk assessment. The actual score is shown in parentheses next to the total score, showing what the total score would have been if all the health result details had been applied towards risk assessment.



The [Health Result Details tab](#) (shown below) will show all the test results collected during an assessment and all the scores for each test. You may find low, medium, or high risk test results. The scoring mode will be Informational for all test results.



Warning Assessment

After you have collected Informational assessment results over a period of time, you can use NAC Manager’s search and reporting tools to identify the top vulnerabilities that end users need to address. If enough end users have the top vulnerabilities, it may not be feasible to quarantine all the end-systems with

these problems. A better strategy would be to warn end users that a problem was found with their end-system that needs to be addressed. Over time, as end users remediate their end-systems, the number of end-systems with the problem should diminish.

When you create a Warning assessment configuration, all health results that must be remediated will be configured with the Warning scoring mode, while all other health results will be configured with the Informational scoring mode. Like the Informational assessment configuration, all end-systems will be considered to have no risk, and no end-systems will be quarantined.

The [Health Result Details tab](#) (shown below) will show all the test results collected during an assessment and all the scores for each test. The scoring mode column will display whether the health result detail was informational or a warning.

Test Case Name	Test Case ID	Risk	Score	Scoring Mode	CVE IDs	Source
Patch Auto Update	90008	HIGH	10.0	Warning		Port: 8443, Protocol: 6
Minimum Agent Version	90001		0.0	Informational		Port: 8443, Protocol: 6
Patch Update Last Run In	90009	HIGH	10.0	Warning		Port: 8443, Protocol: 6
Antivirus	90004		0.0	Informational		Port: 8443, Protocol: 6
Screen Saver	90010		0.0	Informational		Port: 8443, Protocol: 6
Operating System	90006		0.0	Informational		Port: 8443, Protocol: 6
P2P Software	90007		0.0	Informational		Port: 8443, Protocol: 6
Firewall	90005	HIGH	10.0	Warning		Port: 8443, Protocol: 6

After assessment, users are warned of specific violations through the notification portal web page. When they acknowledge these notifications, they can continue accessing the network. If warnings are delivered to the desktop through the agent, the agent will present the violations and the remediation information on the desktop. The user does not need to use the web portal.

As users remediate their violations, the number of end-systems having violations will decrease, and new top vulnerabilities will be exposed. In addition, new tests can be added to the assessment configuration to provide more information on vulnerabilities. Warnings can be added for these new vulnerabilities as they are found, so that end users will remediate them. As this process continues, your overall network risk is reduced.

As an option, you can specify a time limit (called a Grace Period) for the end user to remediate their violations. If the end user does not correct the violations within

the specified time limit, they are quarantined. Once the end user remediates the problems, they are removed from quarantine and allowed access to the network.

Because Warning assessment provides end-system remediation, you must enable remediation in your [NAC Configuration](#) to activate the web portal, and configure the [Portal Configuration](#) correctly to allow remediation of the vulnerabilities that you are warning the user about. For example, be sure that the [Remediation Links](#) and [Custom Remediation Actions](#) subtabs in the [Assessment/Remediation](#) section are sufficient for remediating the vulnerabilities that are of concern.

Quarantine Assessment

With Warning assessment, your network continues to face risk because end-systems with vulnerabilities are still allowed access on the network while they work to remediate their violations. To take the next step in security, you can use a Quarantine assessment configuration that immediately quarantines end-systems that are assigned a high risk level. This means that all health result scores are applied to the determination of the end-system's overall risk level, and end-systems are quarantined based on that risk level.

Before creating a Quarantine assessment configuration, review the scores and risk levels of common vulnerabilities seen in your network, and the end-systems that score highest on actual score. This should provide you with a good idea of how many end-systems would be quarantined if a Quarantine assessment configuration is deployed, and which users would be affected. The default Risk Level Configuration specifies the following high risk criteria:

- Any end-systems with a high-risk vulnerability (score of 7.0 or more) will be quarantined. This includes any end-system failing an agent-based test (score 10.0).
- Any end-systems with an actual score of 20.0 or more will be quarantined.

If you determine that the number of end-systems that would be quarantined would be disruptive to your enterprise, then you can continue with the Warning assessment configuration. Consider increasing the number of warning vulnerabilities or enabling a [grace period](#) (or decreasing the grace period time if you already have a grace period in effect) in order to encourage more compliance.

When you create a Quarantine assessment configuration, all health results will be configured with the Apply Score mode. End-systems will be assessed for risk

on a scale of High Risk to No Risk, with High Risk end-systems being quarantined.

As an alternative, you can create scoring overrides for certain health results. For example, some health results can be made informational and other can continue to be warnings. This way, if there are specific vulnerabilities that you consider to be of no concern or that you wish to consider as warnings, you can still deploy a Quarantine assessment configuration and use scoring overrides to tailor how certain exceptions are handled.

Scoring overrides can also be used to adjust the scores of health results. For example, a vulnerability which scores 10 and is considered a high-risk can be changed to score 6 and be considered medium risk. This approach can be used if excluding the result altogether is not desired. Note that this affects how the vulnerability is categorized in searches and reports: if a vulnerability is rescored to be medium risk, it will appear as medium risk in all searches and reports as well.

The [Health Result Summaries tab](#) (shown below) will always show the overall risk, total score, and top score for the assessment. When every vulnerability found during assessment is applied to risk assessment, then the total score is always the same as the actual score, and the health result summary will display only a single score in the Total Score column. However, if end-systems have any vulnerabilities that are configured with scoring overrides as Informational or Warning, then the total score will be less than the actual score, and the actual score will be shown in parentheses next to the total score.

Scan Start Date	Scan Time	Overall Risk	Reason	Total Score	Top Score	Summary
04/02/2010 02:07:07 PM	31 S	High Risk	One health detail greater than or e...	37.5	10.0	ntp (123UDP),CMP timestamp re...
04/02/2010 01:54:47 PM	23 S	High Risk	One health detail greater than or e...	22.5 (32.5)	7.5	ntp (123UDP),CMP timestamp re...
04/02/2010 11:24:09 AM	25 S	No Risk	Total score was 0.0	0.0 (32.5)	0.0	ntp (123UDP),CMP timestamp re...

Over time, the Quarantine assessment configuration may need occasional adjustment. As high-risk vulnerabilities are discovered, you can use NAC Manager features such as scoring overrides to tailor how end-systems with these vulnerabilities should be treated: immediate remediation through quarantine, eventual remediation through assessment warnings, or no remediation. No remediation may be the proper choice:

- if a high-risk vulnerability poses no risk in your environment, due to the use of firewalls or other tools to defend your network. In this case, you may choose to ignore the vulnerability or change the score to 0.0.
- if the vulnerability is addressed by updates pushed out to end-systems by the network administrator, or if it otherwise requires an administrator to remediate. In this case, you may not want to quarantine end-systems until administrators have had sufficient time to update the end-system.

Because Quarantine assessment provides end-system remediation, you must enable remediation in your [NAC Configuration](#) to activate the web portal, and configure the [Edit Portal Configuration window](#) to allow remediation of the vulnerabilities for which a user is quarantined.

Agent-less Assessment

This section describes how to implement the three assessment phases for an assessment configuration using an agent-less test set. With agent-less assessment, the scoring mode used for all agent-less assessment tests is configured in the [Agent-less Test Set window](#). Scoring overrides are used to change the scoring mode for specific test cases.

Agent-less Informational Assessment

To create an Informational assessment configuration, set the scoring mode in the agent-less test set to Informational. The Scoring Override Configuration selected for the assessment configuration should have no scoring overrides configured. You may wish to initially use a lighter, less exhaustive set of tests, and then change to more exhaustive tests after some time has passed. This will allow you to begin by dealing with a smaller set of results, and after you have addressed these issues, you can expand the test set to include more vulnerabilities.

Agent-less Warning Assessment

To create a Warning assessment configuration, set the scoring mode in the agent-less test set to Informational and add scoring overrides to your Scoring Override Configuration for each test case that should be a warning.

Initially, configure Warning scoring overrides for your most frequent and severe vulnerabilities. Add additional scoring overrides for more vulnerabilities over time. You can easily add Warning scoring overrides from the **Health Result Details** tab, as you view the health results of an end-system.

At some point, you may wish to invert your assessment configuration and scoring overrides. Rather than having a base scoring mode of Informational with scoring overrides for Warnings, you can have a base scoring mode of Warning with scoring overrides for Informational. In other words, instead of specifically calling out which tests are warnings, you call out which tests aren't. (Tests that score 0.0 will not generate warnings.)

Agent-less Quarantine Assessment

To create a Quarantine assessment configuration, set the scoring mode in the agent-less test set to Apply Score. Create a new Scoring Override Configuration and add scoring overrides for any vulnerabilities that you wish to have as exceptions. You can configure these scoring overrides to be Informational or Warning, or you can change the score. You can easily add scoring overrides from the **Health Result Details** tab, as you view the health results of an end-system.

Agent-Based Assessment

This section describes how to implement the three assessment phases for an agent-based assessment configuration. With agent-based assessment, the scoring mode used for each test result is configured directly in the test case. Scoring overrides are not used, except to configure how the "No Agent Detected" health result is handled.

No Agent Detected

Agent-based assessment requires an agent to be installed and running on end-systems in order to assess their risk. If no agent is running at the time of assessment, this will result in a high-risk "No Agent Detected" health result, which will quarantine the end-system. This health result must be handled specially, because no useful assessment results can be collected unless agents are installed and running on end-systems.

There are several ways that the "No Agent Detected" result can be handled.

- Quarantine end-systems that are not running the agent. End-users are redirected to the portal web page where they must download and start the agent in order to gain access to the network. This is the default behavior; nothing needs to be configured.
- Warn end-systems that are not running the agent. End-users are redirected to the portal web page where they are notified that they should download

and start the agent soon. Once they acknowledge the warning they are allowed access to the network. To do this, add a Warning scoring override for Test ID 90000 to your Scoring Override Configuration.

- Do nothing to end-systems that are not running the agent. This method should be used if the agent is installed on end-systems by the network administrator and the end-user does not need to take any action. To do this, add an Informational scoring override for Test ID 90000 to your Scoring Override Configuration.

If the "No Agent Detected" result causes quarantine, users are redirected to the portal web page where they must install the agent in order to access the network. A link to install the agent is provided. Once the end user installs the agent, they will be rescanned. This will generate a new set of health result details for the end-system.

If the "No Agent Detected" result causes a warning, users are redirected to the portal web page where they are notified of their violation. Once they acknowledge the warning they can continue accessing the network. A link to install the agent is provided. When the end user installs the agent, they will be rescanned. This will generate a new set of health result details for the end-system.

Agent-Based Informational Assessment

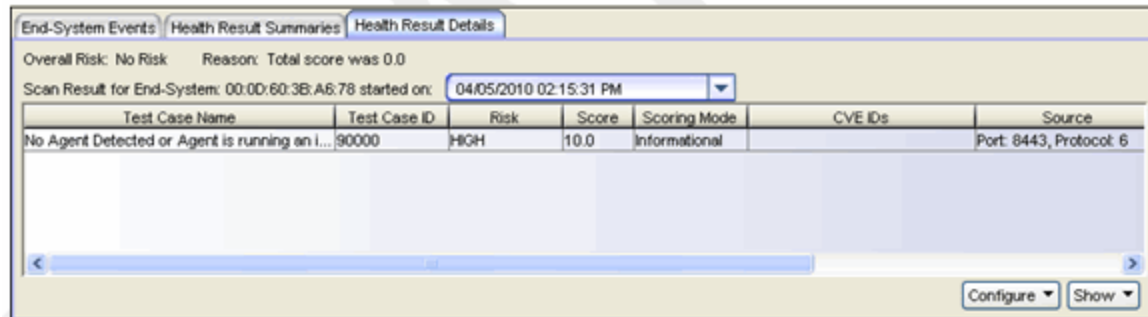
To create an Informational assessment configuration, configure all test cases defined in the agent-based test set to have a Test Status of Informational. You may wish to begin with a smaller list of tests, and then add more tests after some time has passed. This will allow you to deal with a smaller set of results, and after you have addressed these issues, you can expand the test set to include more tests.

There are two basic types of assessment results found during this phase: results from end-systems that are running the agent and results from end-systems that are not.

For end-systems that are running the agent, the **Health Result Details** tab shows all the tests run, and all their scores. You may find passing (score 0.0) or failing (score 10.0) test results. The scoring mode will be Informational for all of them.

End-Systems that are not running the agent will have a single "No Agent Detected" health result detail, as shown below. It may have a scoring mode of Applied (quarantine), Warning, or Informational, depending on your configuration. You can measure your network's overall compliance with running

the agent by searching for end-systems displaying this result (Test ID 90000). Use the search and reporting tools described in the [Monitoring Assessment Results](#) section.



Agent-Based Warning Assessment

To create a Warning assessment configuration, start by configuring all test cases defined in the agent-based test set to have a Test Status of Informational. Then, for each test case that should be a warning, change the Test Status to Warning.

Initially, configure Warning test cases for your most frequent and severe vulnerabilities. Then, configure more test cases to be Warning over time. You can easily change the test status for agent-based test cases from the **Health Result Details** tab, as you view the health results of an end-system.

When you move to an agent-based Warning assessment, you may want to change how the "No Agent Detected" health result is handled. See the [No Agent Detected](#) section for more information.

You may also want to use the agent to warn end users of assessment violations and provide remediation information. To do this, you must have the Allow Agent Remediation option enabled in the [Advanced Agent Configuration window](#) and the Display Agent Notification Messages option enabled in the [Edit Agent-Based Test Set window](#). For more information, see the [Agent Notification](#) section.

Agent-Based Quarantine Assessment

To create a Quarantine assessment configuration, configure all test cases defined in the agent-based test set to have a Test Status of Mandatory. You can make exceptions for individual tests that you wish to execute but exclude from risk assessment, by making those test cases Informational or Warning. You can

easily change the test status for agent-based test cases from the **Health Result Details** tab.

When you move to an agent-based Quarantine assessment, you may want to change how the "No Agent Detected" health result is handled. See the [No Agent Detected](#) section for more information.

You may also want to use the agent to display assessment violations and provide remediation information instead of the portal web pages. To do this, you must have the Allow Agent Remediation option enabled in the [Advanced Agent Configuration window](#) and the Display Agent Notification Messages option enabled in the [Edit Agent-Based Test Set window](#). For more information, see the [Agent Notification](#) section.

Combined Agent-less and Agent-Based Assessment

This section describes how to implement the three assessment phases for a combined agent-less and agent-based assessment configuration. A combined assessment includes both an agent-less test set and an agent-based test set in the assessment configuration. Each test set is configured independently. Assessment health results will contain both agent-less and agent-based results.

Combined Informational Assessment

To create a combined Informational assessment configuration, use the instructions for creating an [agent-less Informational assessment](#) and an [agent-based Informational assessment](#) as described above. You must also configure the ["No Agent Detected" health result](#), as described above.

There are two basic types of assessment results found during this phase: results from end-systems running the agent, and results from end-systems that aren't. For end-systems running the agent, the **Health Result Details** tab shows all the tests that were run, and all their scores. The scoring mode is Informational for all of them.

End-Systems not running the agent display results for agent-less tests, and also a "No Agent Detected" result, as shown below. The "No Agent Detected" result may have a scoring mode of Applied, Warning, or Informational, depending on your configuration. You can measure your network's overall compliance with running the agent by searching for end-systems displaying this result (Test ID 90000). Use the search and reporting tools described in the [Monitoring Assessment Results](#) section.

End-System Events | Health Result Summaries | **Health Result Details**

Overall Risk: High Risk Reason: One health detail greater than or equal to 7.0

Scan Result for End-System: 00:00:60:3B:A6:78 started on: 04/06/2010 04:32:02 PM

Test Case Name	Test Case ID	Risk	Score	Scoring Mode	CVE IDs	Source
OS Detail	90006	LOW	0.0	Informational		Port: 0, Protocol: 0
No Agent Detected or Agent is running an i...	90000	HIGH	10.0	Applied		Port: 8443, Protocol: 6
Windows Server Service MS08-067 buffer...	2839	HIGH	10.0	Informational	CVE-2008-4250	Port: 445, Protocol: 6
SMB	100139	LOW	0.0	Informational		Port: 139, Protocol: 6
End-System Reachability	80000	LOW	0.0	Informational		Port: 0, Protocol: 0
Is your Netbios secure	803	MEDIUM	5.0	Informational		Port: 0, Protocol: 0
Null sessions are enabled	3146	MEDIUM	5.0	Informational		Port: 0, Protocol: 0
3389/TCP	103389	LOW	0.0	Informational		Port: 3389, Protocol: 6
Possible vulnerability in Microsoft Terminal ...	962	MEDIUM	7.5	Informational	CVE-2000-1149,CVE-2001-06...	Port: 3389, Protocol: 6
microsoft-ds (445/TCP)	100445	LOW	0.0	Informational		Port: 445, Protocol: 6

Configure Show

If the "No Agent Detected" result causes a quarantine or a warning, the user is notified through the portal web page, where they can download an agent, as described in the [No Agent Detected](#) section above. When end-systems download, install, and start the agent, they will be rescanned. This will generate a new set of health results.

Combined Warning Assessment

To create a combined Warning assessment configuration, use the instructions for creating an [agent-less Warning assessment](#) and an [agent-based Warning assessment](#) as described above. You must also configure the ["No Agent Detected" health result](#), as described above.

When the user is redirected to the portal for notification, the list of violations presented will include warnings for both agent-less and agent-based results. Similarly, warnings for both agent-less and agent-based results can be delivered through [agent notification](#).

Combined Quarantine Assessment


To create a combined Quarantine assessment configuration, use the instructions for creating an [agent-less Quarantine assessment](#) and an [agent-based Quarantine assessment](#) as described above. You must also configure the ["No Agent Detected" health result](#), as described above.

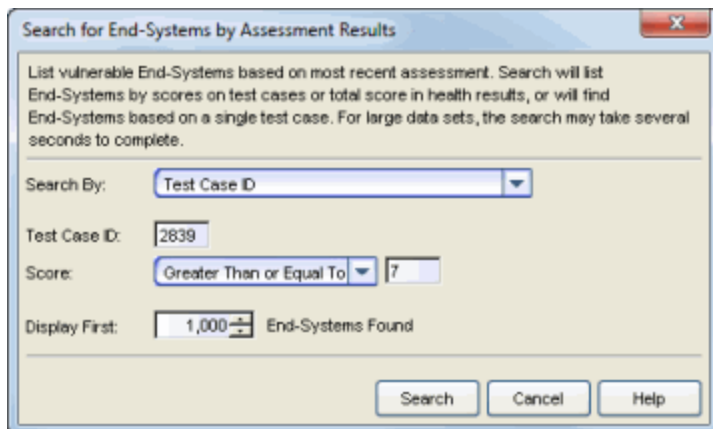
When the user is redirected to the portal for remediation, the list of violations presented will include both agent-less and agent-based results. Similarly, violations for both agent-less and agent-based results can be delivered through [agent notification](#).

Monitoring Assessment Results

This section describes how you can use NAC Manager's search functionality and statistical reports to help gauge your overall network security compliance and identify frequently occurring vulnerabilities. You can then use this information to modify your assessment configuration as needed.

Search by Assessment Results

You can access the NAC Manager assessment-related searches using the Tools > Search for End-Systems by Assessment Results menu option. In addition, the NAC [End-Systems View](#) provides the same search functionality, accessed from the Search for End-Systems by Assessment button .



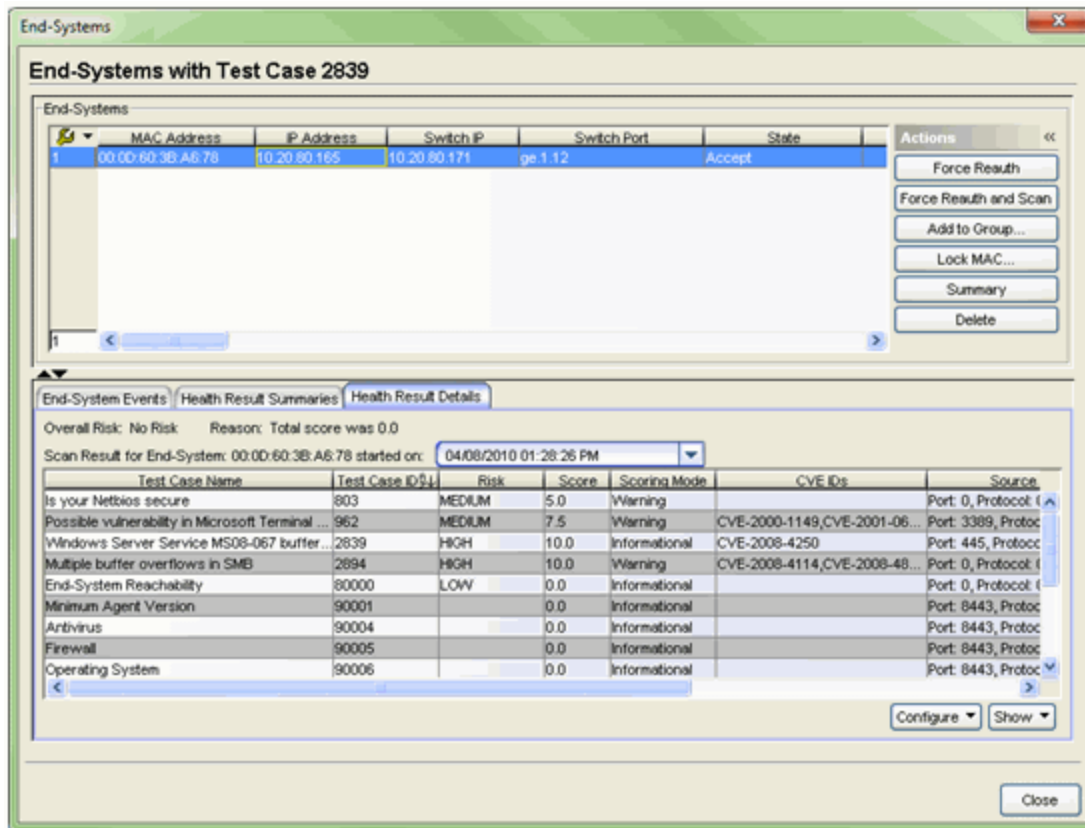
There are several search options provided. You can search by:

- **Highest Test Case Scores to Lowest** - Displays end-systems sorted according to their highest individual test case score (from the [Health Result Details tab](#)), listing the most vulnerable end-system with the highest score first. This search is only useful for Quarantine assessment because only applied scores count towards the high score.
- **Highest Total Health Result Scores to Lowest** - Displays end-systems sorted according to their total health result score (from the [Health Result Summaries tab](#)), listing the most vulnerable end-system with the highest total score first. This search is only useful for Quarantine assessment because only applied scores count towards the total score.
- **Highest Total Health Result Actual Scores to Lowest** - Displays end-systems sorted according to their actual health result score (from the [Health Result Summaries tab](#)), listing the most vulnerable end-system with

the highest actual score first. The actual score is what the total score would be if all the health details were included as part of the quarantine decision, including those marked Informational and Warning.

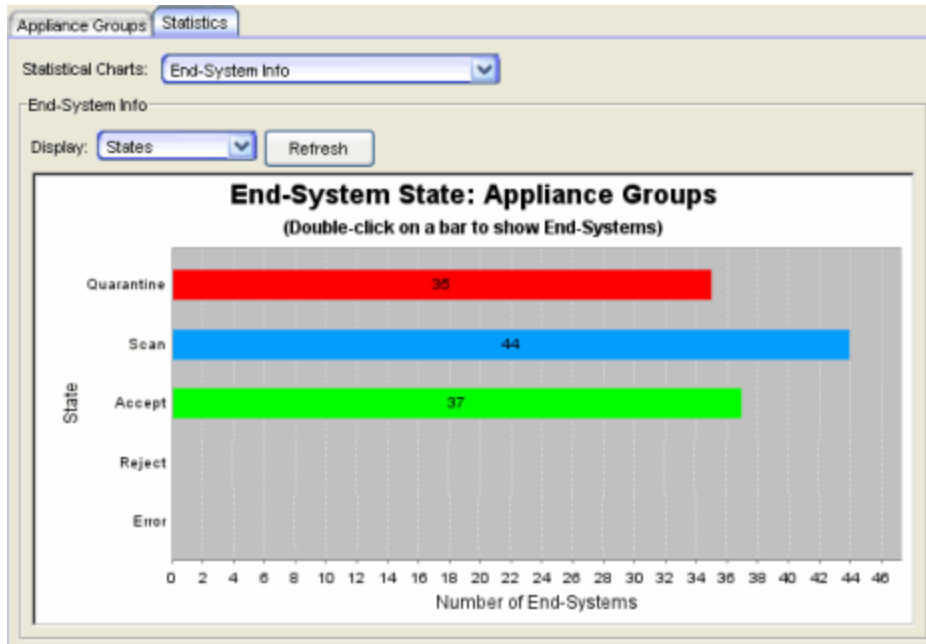
- **Selected Test Case** - Searches for end-systems where a specific agent-based test case and score are part of their latest assessment results. This search can be used with Informational, Warning, and Quarantine assessments, however it is not useful for agent-less health results. In the Score field, use a score criteria to find only end-systems that pass or fail the test or use Score Any to find all end-systems that have a test result, pass or fail. This search is particularly useful for finding end-systems which are not running the agent, by searching for the Test Case "Agent Status - ID: 90000."
- **Test Case ID** - Searches for end-systems where a specific test case ID and score are part of their latest assessment results. This search can be used with Informational, Warning, and Quarantine assessments. For agent-based tests, use a score criteria to find only end-systems that pass or fail the test or use Score Any to find all end-systems that have a test result, pass or fail.
- **Outstanding Warnings** - Searches for end-systems that have received warnings and have acknowledged them, but have not yet cleared them.
- **Unacknowledged Warnings** - Searches for end-systems that have received warnings and have not yet acknowledged them.

In order to display the most current data, searches are limited to information from the latest assessment results for each end-system. Search results are displayed in the **End-Systems** tab, presented as a separate window.



Statistical Reports

The right-panel **Statistics** tab presents end-system connection state statistics and vulnerability status information. For example, the End-System State chart (shown below) can show you the number of end-systems in the quarantine state.



The following statistical charts can provide valuable information with evaluating the overall network risk. For more information on each chart, see the [Statistics tab](#) Help topic.

- **End-System Info** - The States sub-option displays the number of end-systems in the quarantine state. Click on the red Quarantine bar to view the end-systems which are quarantined.
- **End-System Status** - This chart will show you the percentage of end-systems in quarantine. Click on the red Quarantine section to view the end-systems which are quarantined.
- **Most Frequently Occurring Vulnerabilities** - Use this report to see which agent-less vulnerabilities are most prevalent on your network. There are sub-options to display only High Risk, Medium Risk, or Low Risk vulnerabilities. You can click on each vulnerability that is found to see which end-systems are currently reporting that vulnerability. This is useful with Informational and Warning assessment, as well as Quarantine assessment.
- **End-System NAC Profile Allocation** - This chart will show any end-systems that are assigned the Notification NAC Profile. These are end-systems with unacknowledged notifications. Click on the Notification section to view the end-systems which have unacknowledged notifications.

Control Dashboard

The **Control** tab in Management Center provides reports on end-system connection and assessment. For more information on these reports, see the [Control tab](#) Help topic.

Diagnostics and Troubleshooting

This section describes the tools available in NAC Manager to help diagnose and troubleshoot problems that may occur during the assessment process.

Analyze Health Results

Problems with assessment can sometimes be resolved by examining the collected health results displayed in the Health Result Summaries and Health Result Details sub tabs in the [End-Systems tab](#). Looking through the health results, you can determine how often end-systems are assessed, which health results are causing an end-system to be quarantined, and which health results have changed over time. You can use the NAC Manager search and reporting tools to analyze health results across the entire network. See the [Monitoring Assessment Results](#) section for more information on these tools.

End-System Events

The End-System Events subtab in the [End-Systems tab](#) can often provide useful information about assessment. The tab displays events for each time an assessment is started and completed, showing when assessments have occurred, changes to the end-system after it was assessed, and whether any assessments are stuck or have been aborted.

Screen Preview

The [Registration Administration web page](#), available on each Extreme Access Control engine, provides a Screen Preview feature that allows you to view the Warning notification page for any end-system. In the Screen Preview web page, enter the end-system's IP address and click the View for End-System button to see the portal web page that the end user would see. Using this view you can actually help the end-system remediate their violations. You can access the Screen Preview web page at https://<Access Control Engine Name or IP address>/screen_preview.

Extreme Access Control Engine Administration

To access status and diagnostic information for a Extreme Access Control (Access Control) engine, launch the Access Control Engine administration web page by right-clicking on a Access Control engine in the left-panel tree and selecting WebView. (You can also access the administration web page using the following URL: `https://<Access ControlEngineIP>:8444/Admin.`) The default user name and password for access to this web page is "admin/Extreme@pp."

In the administration web page left-panel tree, expand the Status folder and the Log Files folder to view reports that provide assessment diagnostic information:

- Agent-Based - Displays information about the agent-based clients connected to NAC. Click the Show All button to display all connected agents.
- Assessment - Provides performance information related to NAC assessment.
- Captive Portal - Provides debug information for the web portal including statistics on the number of requests served and the interaction with Extreme Management Center.
- Agent Logs Tab - Displays the agent log files that have been retrieved from remote end-systems via the Client Diagnostics section on the **Agent-Based** tab page.

For more information, see the [Access Control Engine Administration Web Page section](#) of the NAC Deployment Guide.

Log Files

Extreme Access Control engine log files can also provide useful diagnostic information for assessment. You can enable diagnostics for assessment by going to the Access Control engine administration web page and enabling diagnostic groups that provide troubleshooting information. Launch the Access Control engine administration web page by right-clicking on the Access Control engine in the NAC Manager left-panel tree and selecting WebView or by using the following URL: `https://<Access ControlEngineIP>:8444/Admin.` The default user name and password for access to this web page is "admin/Extreme@pp."

Expand the Diagnostics folder in the left-panel tree and click on the Appliance/Server Diagnostics page. There are several useful diagnostic options to enable including:

- Assessment
- Assessment - Agent Based Connection Interaction
- Captive Portal - Authentication
- Captive Portal - Display
- Captive Portal - Processes and Configuration
- Captive Portal - Registration Administration
- Captive Portal - Registration and Remediation

View the debug information in the Access Control engine administration web page under the Log Files > **Server Log** tab or in /var/log/tag.log file on the Access Control engine. The assessment agent process has its own log file which can be found in /opt/nac/saint/logs/ on the Access Control engine.

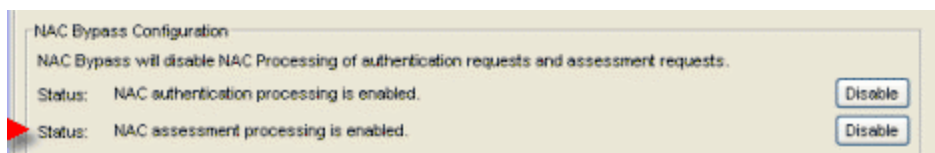
For more information, see the [Access Control Engine Administration Web Page section](#) of the NAC Deployment Guide.

Disabling Assessment

When diagnosing and troubleshooting assessment on your network, it may become prudent to disable assessment, especially if end users are experiencing problems arising from its use. In some cases, it may even be necessary to do so very quickly. There are a number of options available for disabling assessment, with different options being more appropriate at different times.

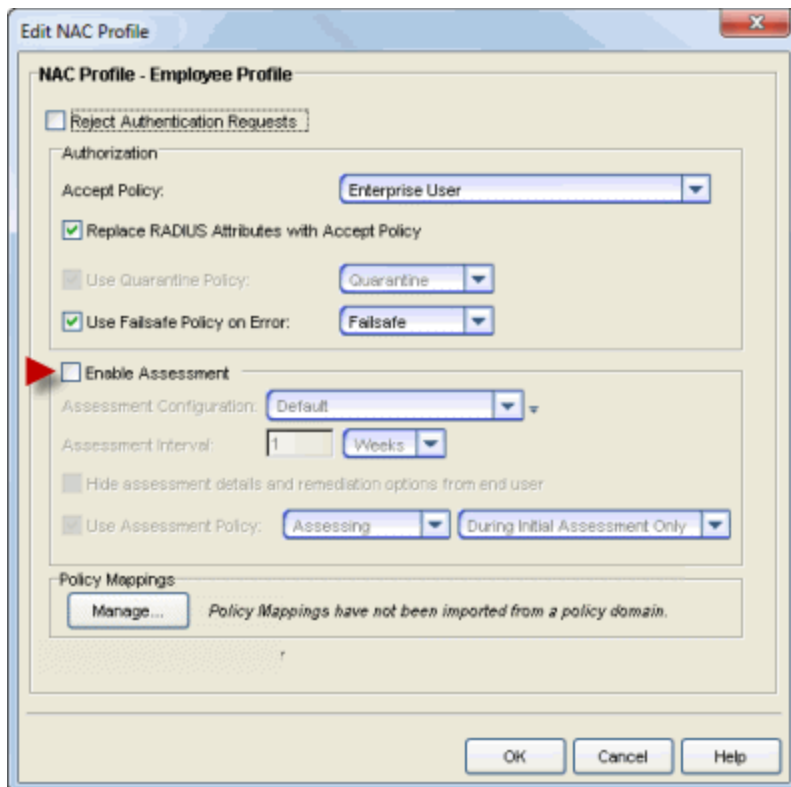
Disable Assessment on the Engine

In the NAC Manager right-panel [Appliance Configuration tab](#), the NAC Bypass Configuration section has a **Disable** button that allows you to very quickly disable assessment on the selected engine. For example, if there is a problem with an assessment configuration, the **Disable** button lets you remotely disable assessment functionality on the engine until the problem has been resolved. You can then use the **Enable** button to re-enable assessment functionality. When assessment is disabled, the Extreme Access Control engine name and IP address are displayed in red text in the left-panel tree indicating that the engine is in Bypass mode.



Disable Assessment in the NAC Profile

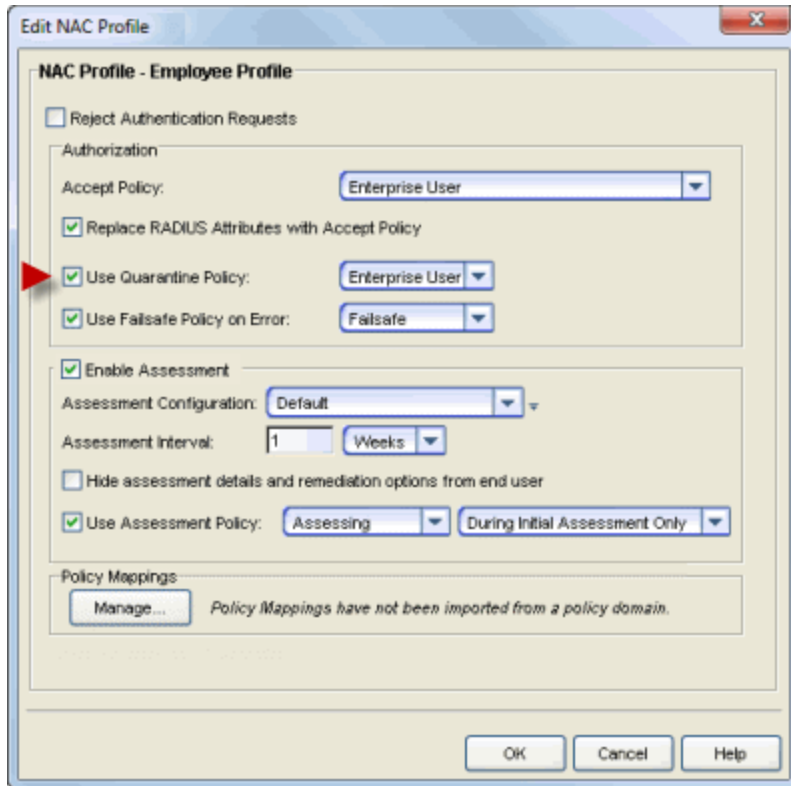
You can disable assessment for all end-systems that are assigned the same NAC Profile, by reconfiguring the NAC profile to disable assessment. To edit an existing profile, select a profile in the [Manage NAC Profiles window](#) and click the **Edit** button. In the Edit NAC Profile window, deselect the Enable Assessment option. This change must be enforced to your engines.



Change the Quarantine Policy

You can disable quarantine for all end-systems that are assigned the same NAC Profile, by reconfiguring the NAC profile to specify a Quarantine policy that allows network access, for example, the Enterprise User policy.

With this approach, end-systems assigned to that NAC profile are still assessed, and are still quarantined if determined to be high risk. However, being in quarantine will not affect the end user's ability to access the network, and end users will not be redirected to the portal web pages. (If you are using agent-based assessment and have [agent notification](#) enabled, the agent still reports to end-users that the end-system is quarantined.) End users already quarantined are not be affected by this change until they are re-assessed.

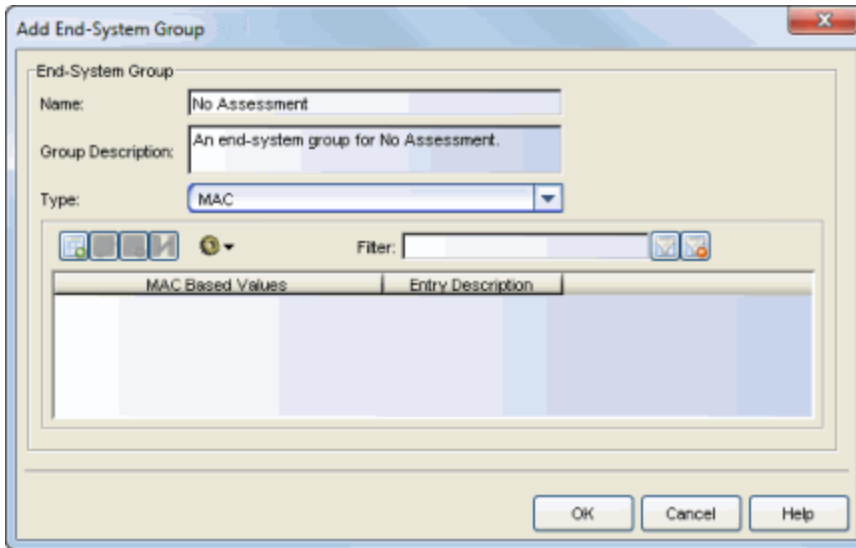


To edit an existing profile, select a profile in the [Manage NAC Profiles window](#) and click the **Edit** button, or use the **Default Profile** field in the [Edit NAC Configuration window](#). This change must be enforced to your engines.

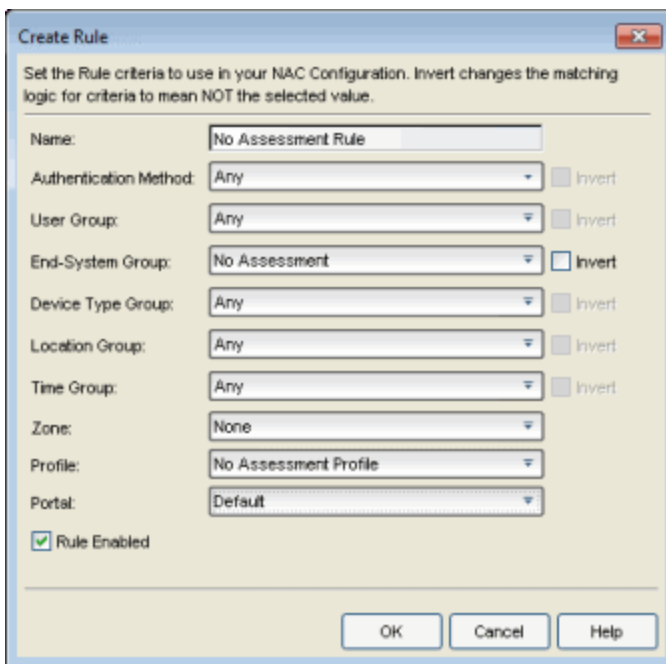
No Assessment End-System Group

This procedure allows you to disable assessment for certain end-systems by assigning them to an end-system group that uses a NAC Profile that does not have assessment enabled. You can create the end-system group in advance, so that it is ready to use when the need arises.

1. From the [Manage Rule Groups window](#), create an end-system group for No Assessment.



- From the [NAC Configuration Rules panel](#), create a custom rule that assigns end-systems in the No Assessment group to a NAC Profile that does not enable assessment.

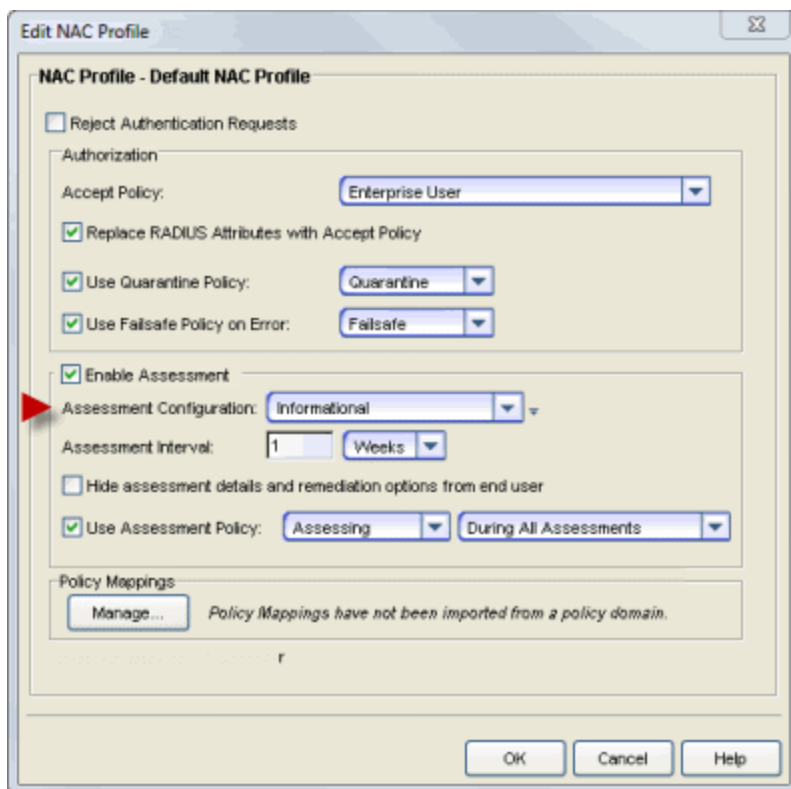


- Enforce these changes to your engines.

After you have created the end-system group, you can add an end-system to the group to disable assessment for that end-system. Remove them from the group to re-enable assessment. End-systems can be easily added and removed to and from end-system groups from the [End-Systems tab](#).

Revert to Informational Assessment

You can revert from a Warning assessment or Quarantine assessment configuration back to an Informational assessment configuration at any time by changing the assessment configuration assigned in a NAC Profile. End-systems assigned to that profile are still assessed, but the health results will not quarantine any end-systems. You may have preserved your Informational assessment configuration from earlier use or you can prepare an alternate Informational assessment configuration to use if necessary. You can change the assessment configuration in the [Edit NAC Profile window](#). You must enforce this change to your engines.



As an alternative, you can continue to use a Warning or Quarantine assessment configuration, and just change specific assessment tests to an Informational scoring mode. Agent-less test sets can be changed to Informational assessment by changing the Scoring Mode for the test set to Informational or by creating scoring overrides for specific tests. Agent-based test sets require changing the Test Status on the desired test cases to Informational.

How to Configure Assessment

This Help topic provides step-by-step instructions for configuring assessment using the phased approach described in the [NAC Assessment Phased Deployment Guide](#). The phased approach lets you introduce assessment into your NAC deployment in three distinct phases: Informational, Warning, and Quarantine. Using the phased approach you can minimize disruptions to your enterprise, introduce end users to remediation procedures gradually, and increase your understanding of the strengths and weaknesses in the network.

Instructions are provided for configuring phased assessment using agent-less or agent-based assessment, or a combination of both. You will need to use the instructions appropriate for your NAC deployment.

Before beginning the configuration procedures, you should read through the following information presented in the NAC Manager online Help.

- [Assessment Concepts](#) - A conceptual overview of assessment that introduces the terminology used in NAC assessment.
- [NAC Assessment Phased Deployment Guide](#) - This guide describes in detail the phased approach to introducing assessment into your NAC deployment using Informational, Warning, and Quarantine assessment. The guide also provides information on NAC Manager tools that can be used to monitor and evaluate assessment results, and diagnose and troubleshoot problems.
- [How to Set Up Assessment](#) - Provides information on the steps that must be performed in NAC Manager prior to deploying assessment on your network, including managing your assessment servers and adding external assessment servers. It also includes basic information on how to use the default assessment configurations provided by NAC Manager and enable assessment for your NAC Configuration.
- [How to Deploy Agent-Based Assessment](#) - If you are deploying agent-based assessment, this Help topic provides the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.

- [How to Set Up Assessment Remediation](#) - Because Warning and Quarantine assessment provides end-system remediation, you must enable remediation for your NAC Configuration. This Help topic provides the specific steps that must be performed when setting up assisted remediation in your network.

This topic includes information and instructions on:

- [Agent-less Assessment Configuration](#)
 - [Informational Assessment](#)
 - [Warning Assessment](#)
 - [Quarantine Assessment](#)
- [Agent-Based Assessment Configuration](#)
 - [Informational Assessment](#)
 - [Warning Assessment](#)
 - [Quarantine Assessment](#)
- [Combined Assessment Configuration](#)
 - [Informational Assessment](#)
 - [Warning Assessment](#)
 - [Quarantine Assessment](#)

Agent-less Assessment Configuration

This section presents instructions for creating assessment configurations for each of the three deployment phases, using an agent-less test set. A new assessment configuration is created for each phase, rather than modifying the existing assessment configuration. This allows you to easily revert back to an earlier phase at any time by changing the assessment configuration that your NAC profile is using.

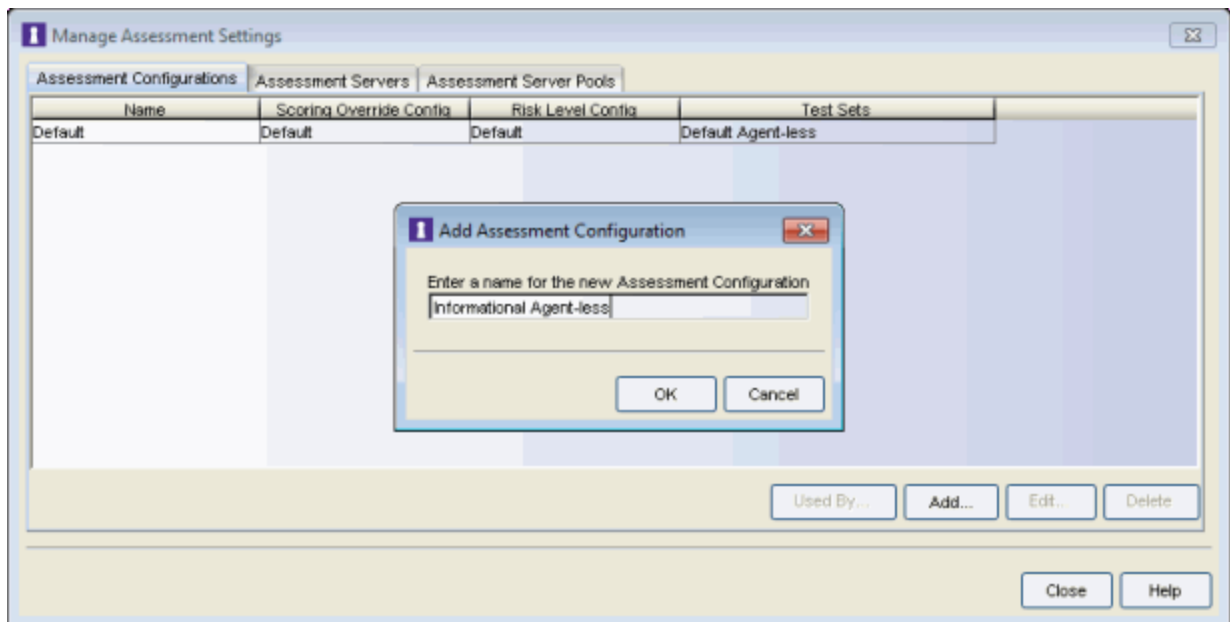
Agent-less Informational Assessment

Use the following steps to create and configure an agent-less Informational assessment configuration. With Informational assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, but no action is taken against end-systems with vulnerabilities. This allows you to use assessment as a data-gathering

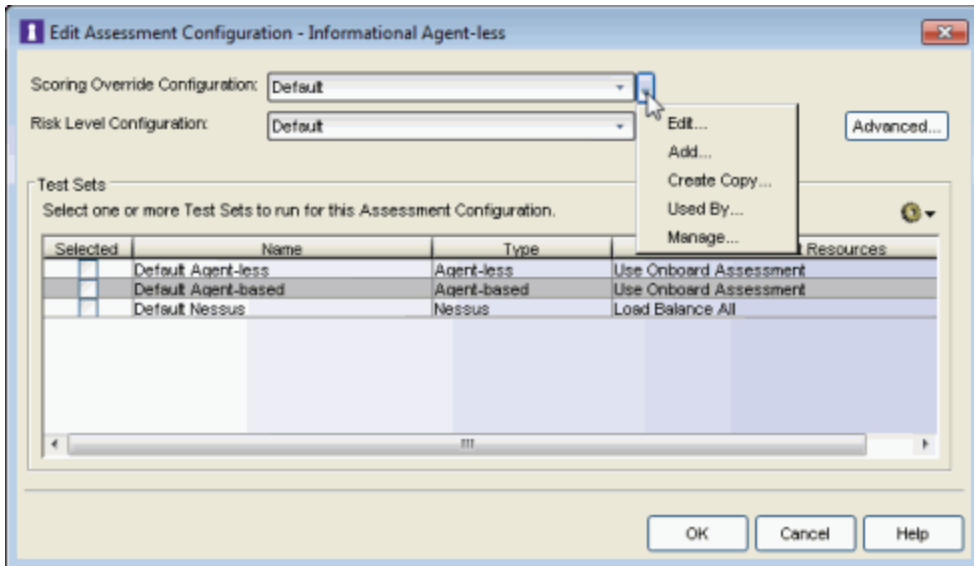
mechanism without end-systems being quarantined. For more information, see the [NAC Assessment Phased Deployment Guide](#).

When you create an agent-less Informational assessment configuration, all test results are configured with an Informational scoring mode. This means that test results are not counted towards a quarantine decision, and are used to provide information about overall network health.

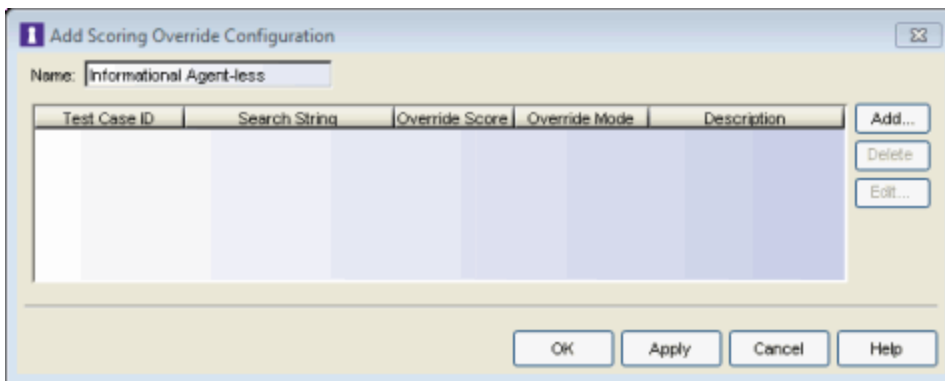
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Informational Agent-less."



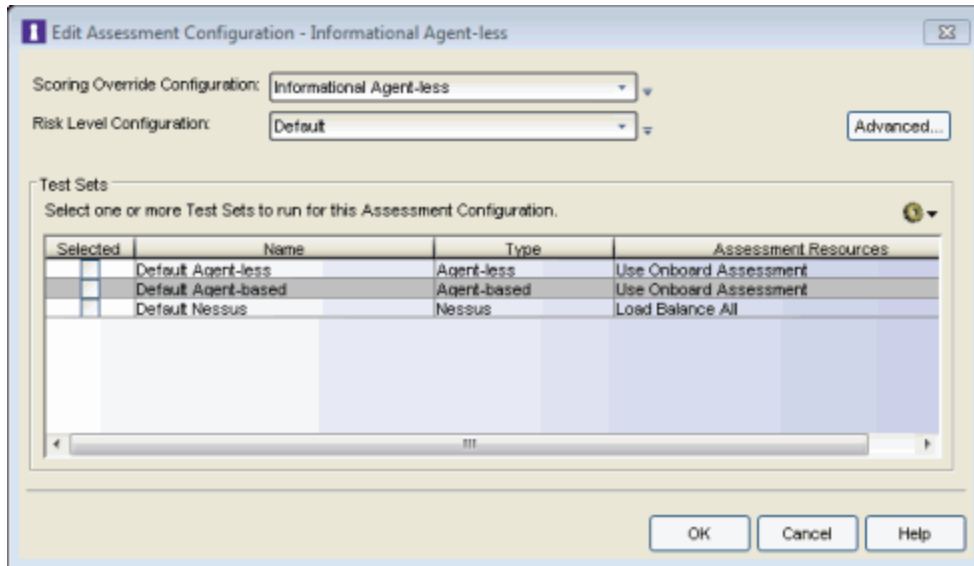
2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring override configuration called "Informational Agent-less."




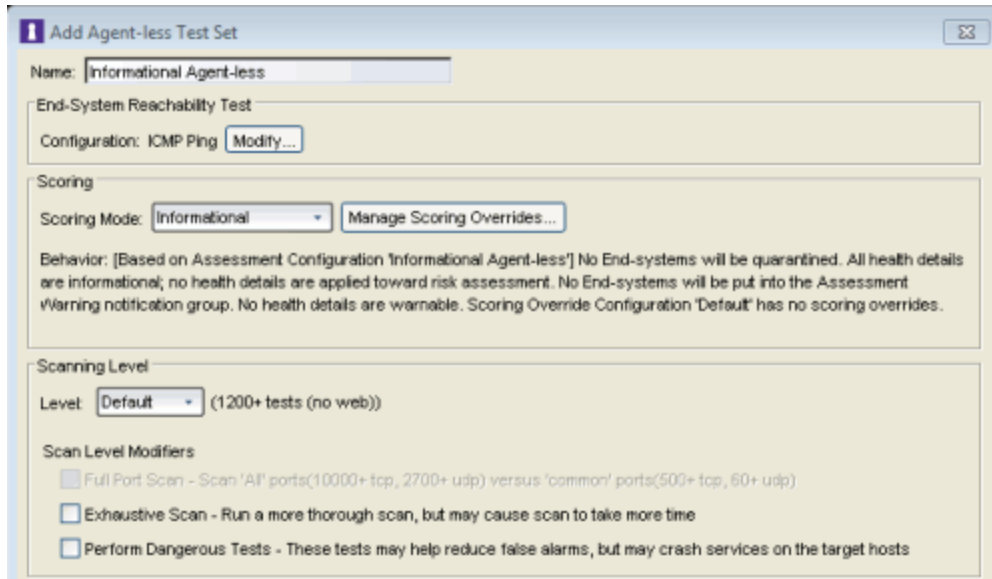
- Do not add any scoring overrides to the configuration at this time. Click **OK**.



- Back in the Edit Assessment Configuration window, verify that the Informational Agent-less scoring override configuration is selected.

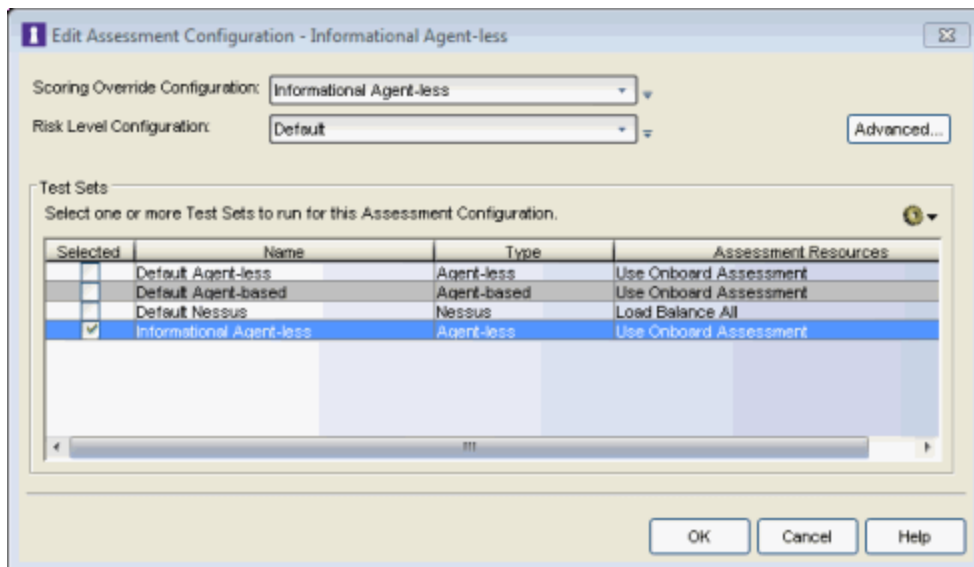


5. From the test sets Configuration Menu button  add a new agent-less test set named "Informational Agent-less." Configure the Informational Agent-less test set as follows:
 - a. Select the kinds of tests to perform.
 - b. Set the Scoring Mode to Informational.
 - c. Verify that the Informational scoring override configuration has no scoring overrides by reading through the Behavior description below the Scoring Mode field.

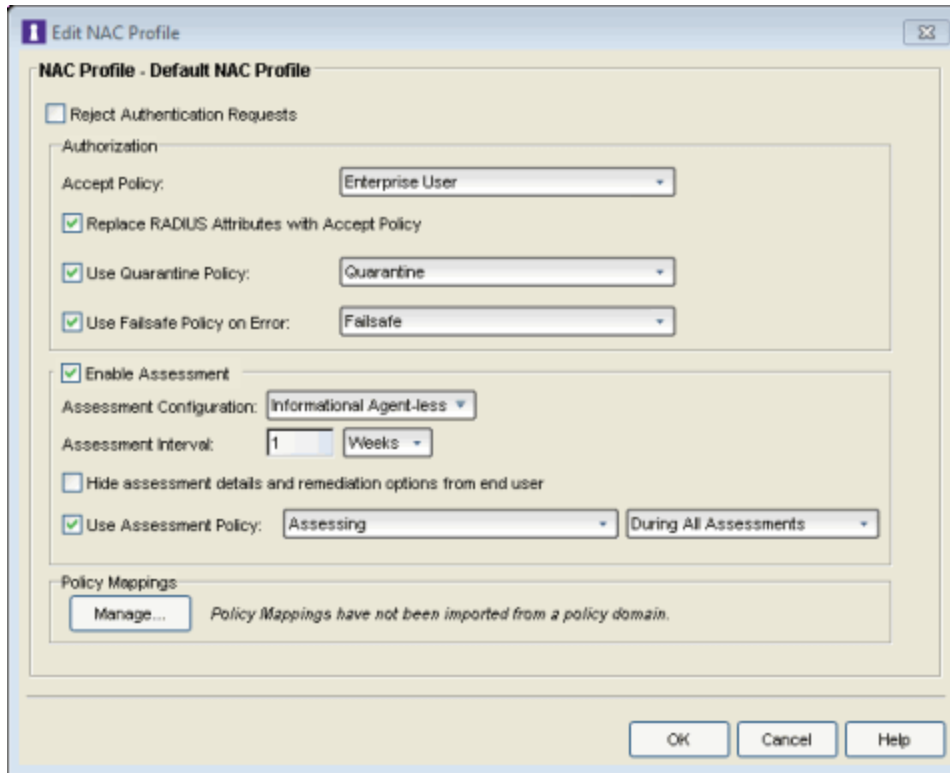


Click **OK** to close the window.

6. Back in the Edit Assessment Configuration window, verify that the Informational Agent-less test set is selected. Click **OK**.



7. Configure the Default NAC Profile to enable assessment and select the Informational Agent-less assessment configuration.



8. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Informational assessment. You can see assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

Agent-less Warning Assessment

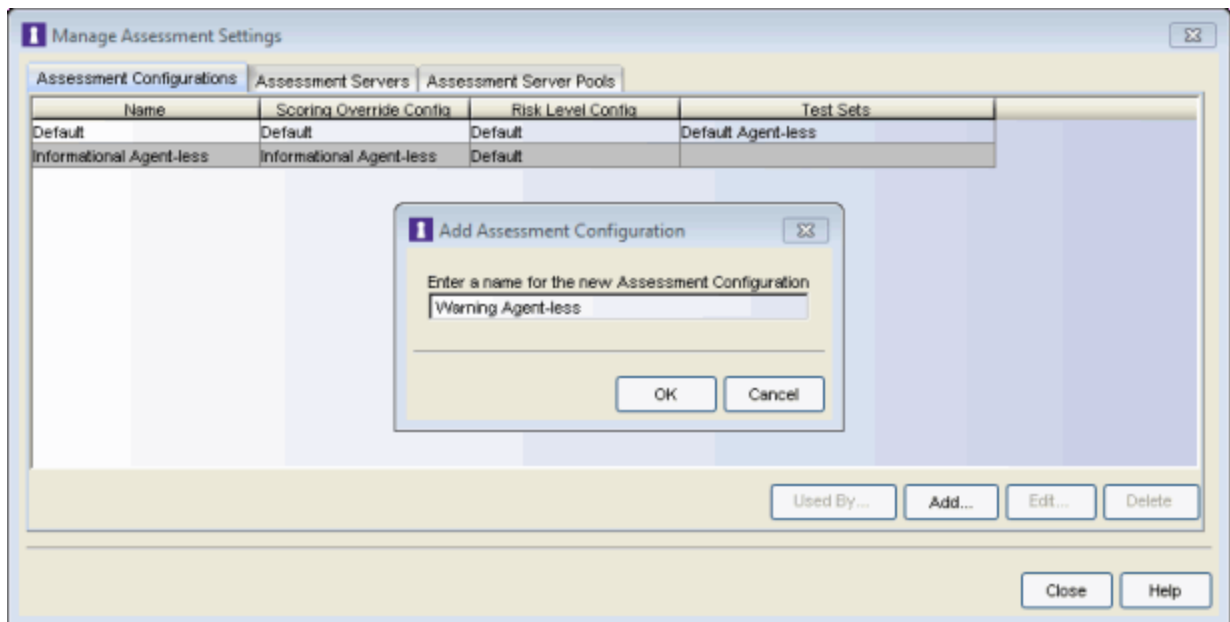
Use the following steps to create and configure an agent-less Warning assessment configuration. With Warning assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are notified. End users are provided with the means to remediate their vulnerabilities and achieve compliance, however end-systems which are not compliant can still access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

To create an agent-less Warning assessment configuration, the scoring mode in the agent-less test is set to Informational and scoring overrides are added to your scoring override configuration for each test case that should be a warning.

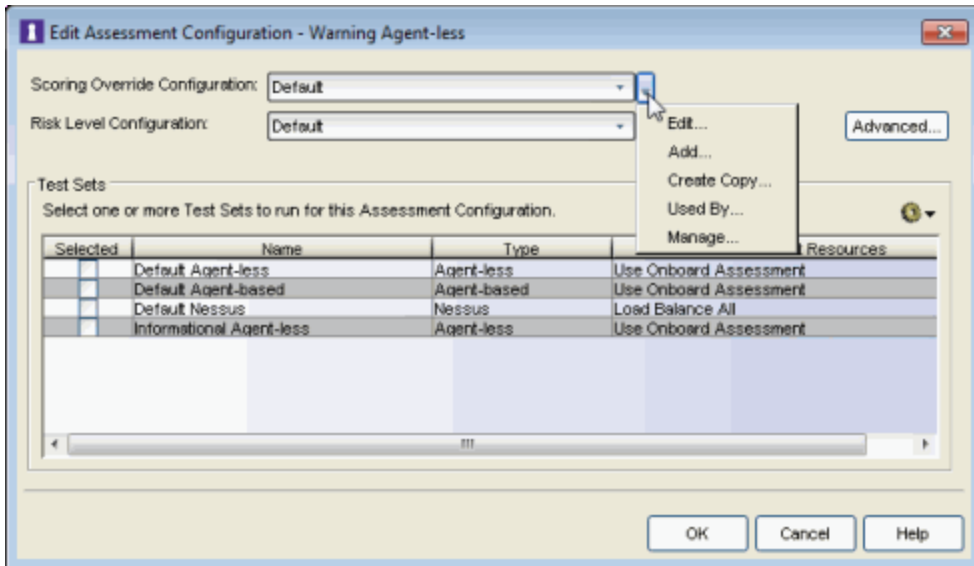
Like the Informational assessment configuration, all end-systems will be considered to have no risk, and no end-systems will be quarantined.

Initially, configure Warning scoring overrides for your most frequent and severe vulnerabilities. Add additional scoring overrides for more vulnerabilities over time. You can easily add Warning scoring overrides from the Health Result Details tab, as you view the health results of an end-system.

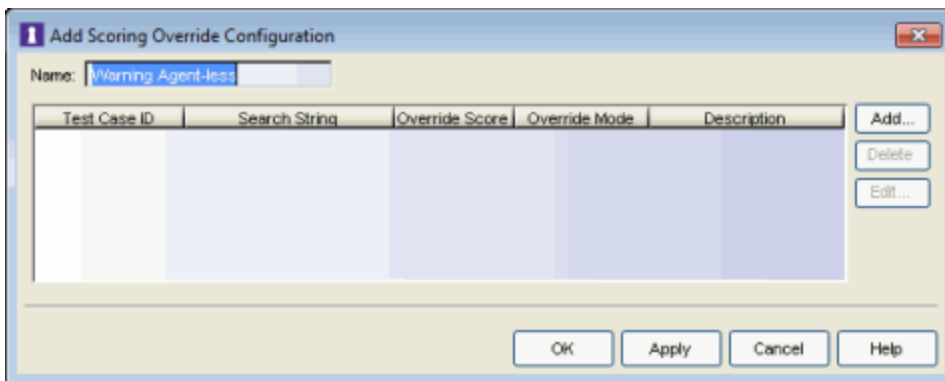
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Warning Agent-less."



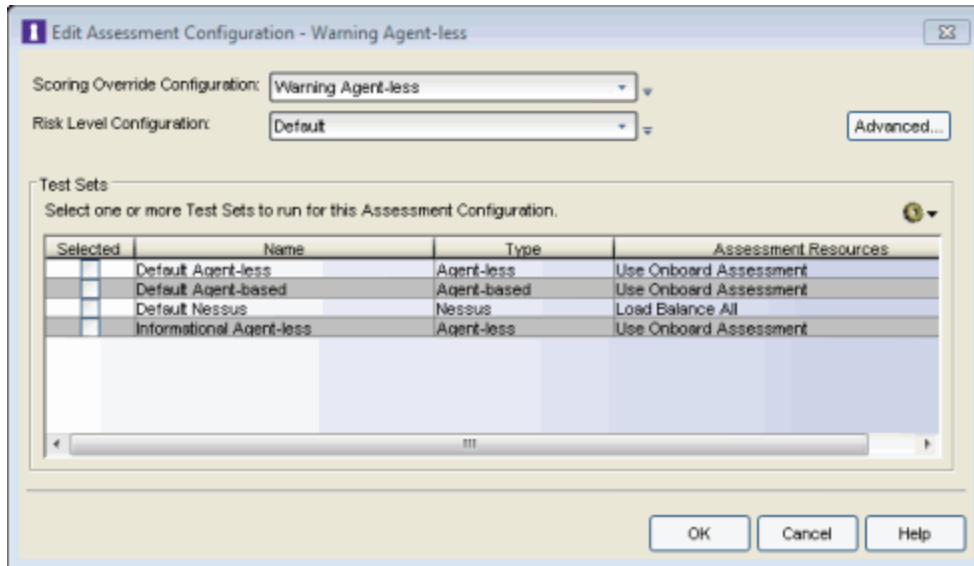
2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring override configuration called "Warning Agent-less."



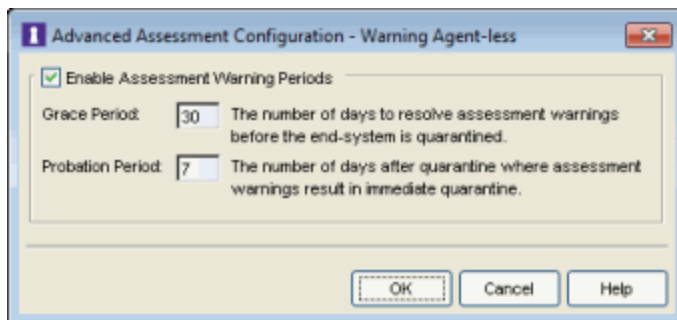
3. Do not add any scoring overrides to the configuration at this time. Click OK.




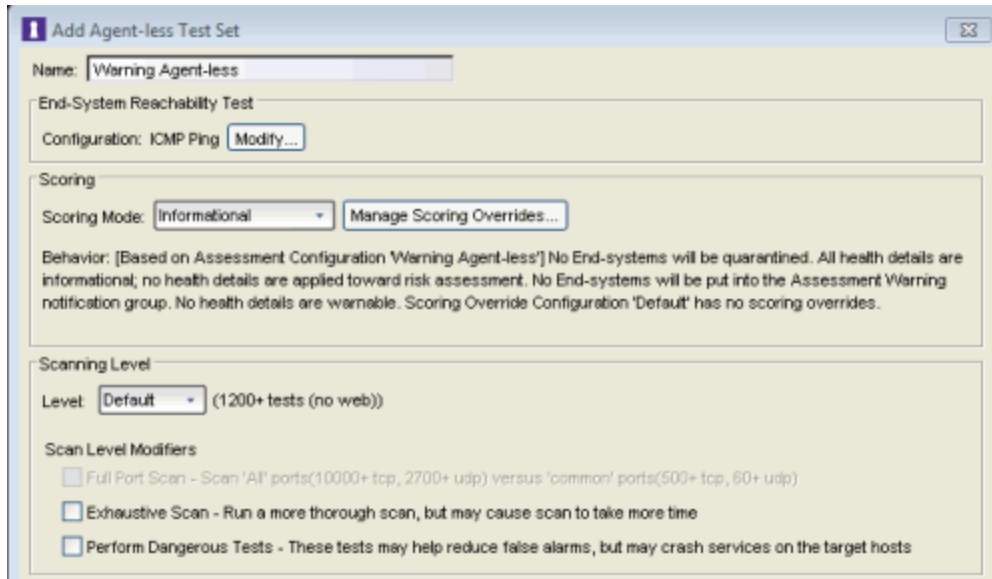
4. Back in the Edit Assessment Configuration window, verify that the Warning Agent-less scoring override configuration is selected.



5. Click the **Advanced** button to open the [Advanced Assessment Configuration window](#) where you can enable assessment warning periods. Set the number of Grace Period and Probation Period days to the desired values. Click **OK** to close the window.

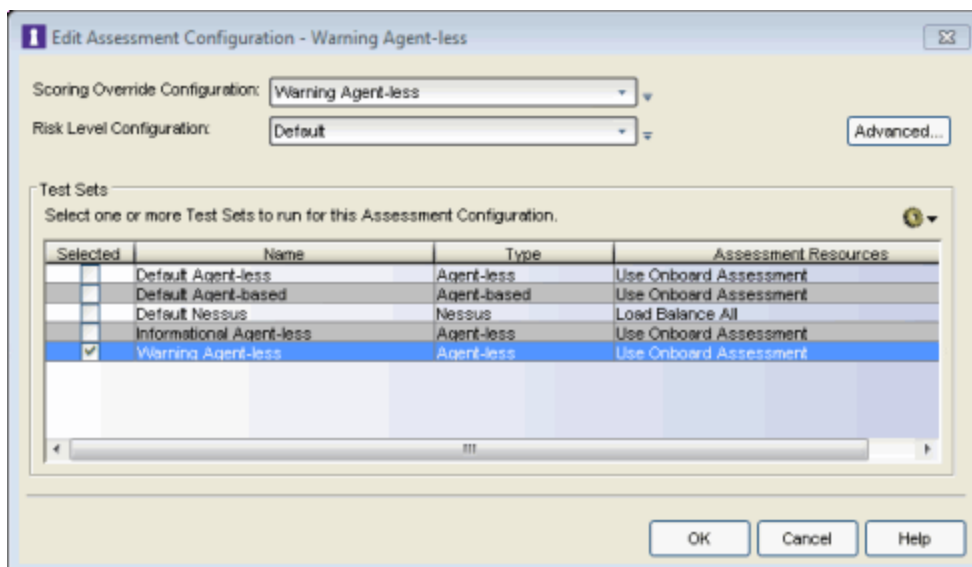


6. From the test sets Configuration Menu button  add a new agent-less test set named "Warning Agent-less." Configure the Warning agent-less test set as follows:
 - a. Select the kinds of tests to perform.
 - b. Set the Scoring Mode to Informational.



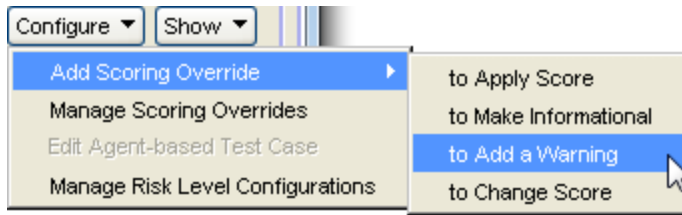
Click **OK** to close the window.

7. Back in the Edit Assessment Configuration window, select the Warning Agent-less test set to include in the configuration. Click **OK**.

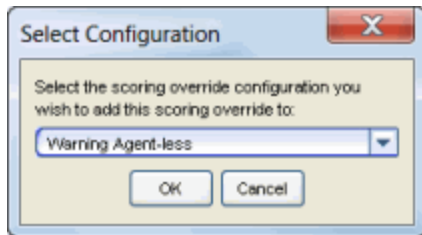


8. Use the following steps to add Warning scoring overrides from the [Health Result Details tab](#) (in the [End-Systems tab](#)), as you view the health results of an end-system.
 - a. Identify a health detail that represents a vulnerability you would like to add a Warning for.

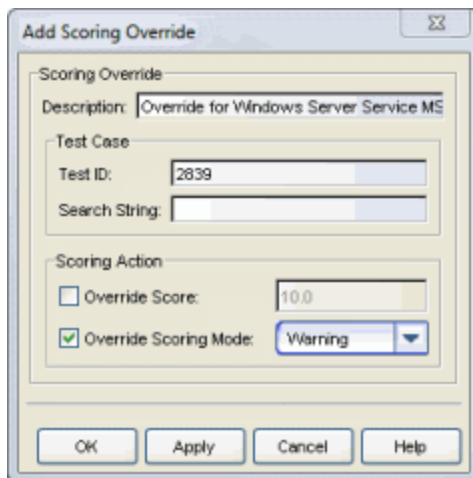
- b. With the target health detail selected in the Health Result Details tab, select **Configure > Add Scoring Override > to Add a Warning**.



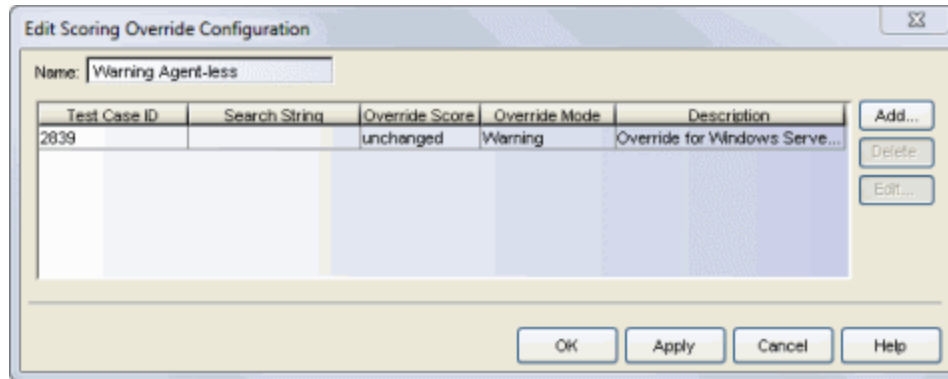
- c. Select the Warning Agent-less scoring override configuration. Click **OK**.



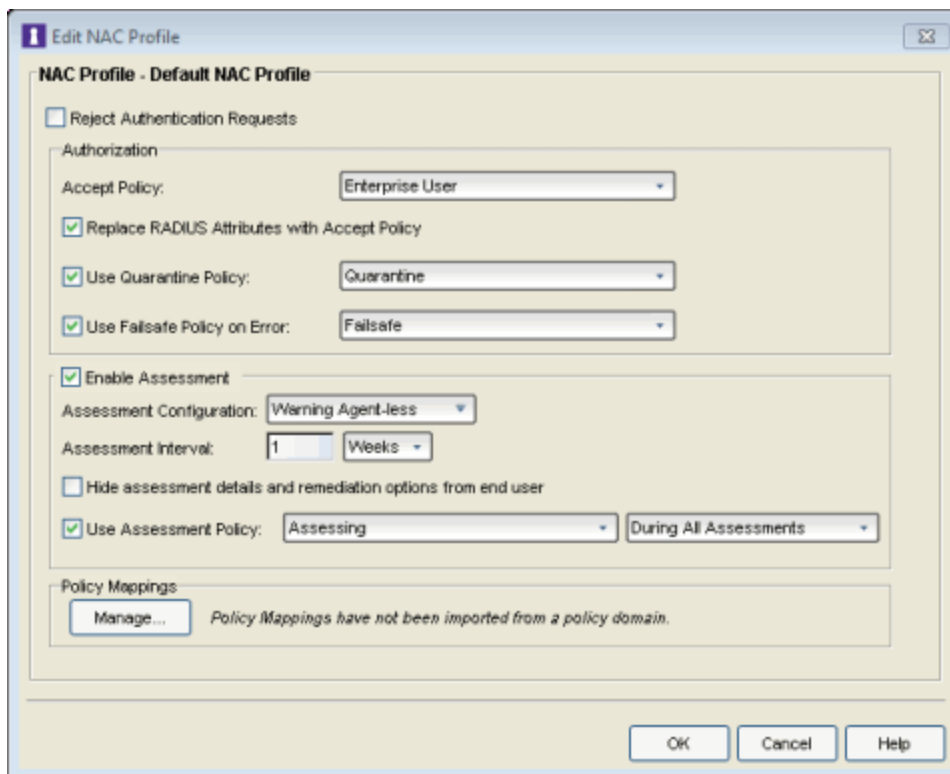
- d. Review the scoring override that will be created. No changes should be necessary. Click **OK**.



- e. Click **OK** to complete the scoring override. The Warning Agent-less scoring override configuration will be displayed with the new override. Click **OK** to save the scoring override configuration.



- f. Repeat steps **a** through **e** to create additional warning scoring overrides for other vulnerabilities, as needed.
9. Configure the Default NAC Profile to enable assessment and select the Warning Agent-less assessment configuration.



10. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Warning assessment. You can monitor the assessment results in the [End-Systems tab](#). For more

information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

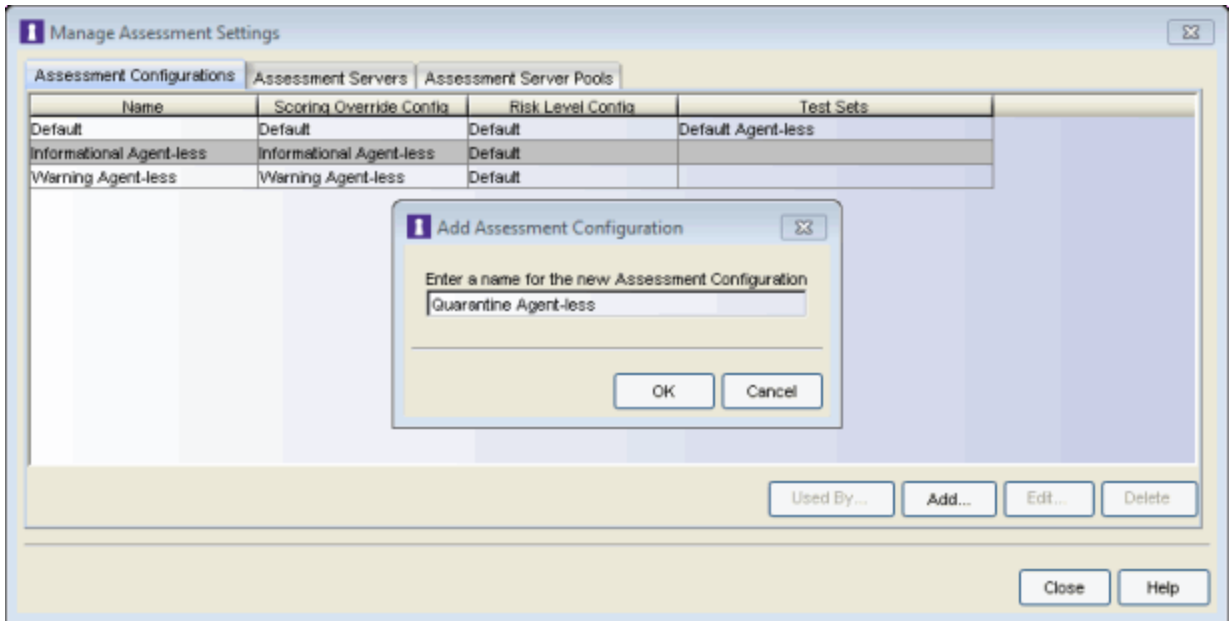
At some point, you may wish to invert your assessment configuration and scoring overrides. Rather than having a base scoring mode of Informational with scoring overrides for Warnings, you can have a base scoring mode of Warning with scoring overrides for Informational. In other words, instead of specifically calling out which tests are warnings, you call out which tests aren't. To do this, you will need to create a new scoring override configuration, and populate it with health result details marked as Informational by selecting the **Configure > Add Scoring Override > To Make Informational** menu option.

Agent-less Quarantine Assessment

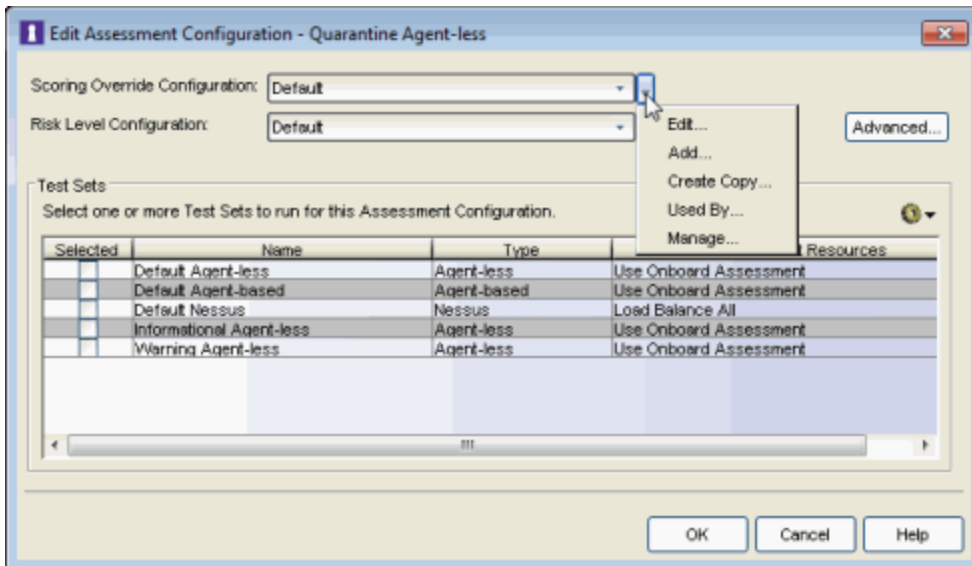
Use the following steps to create and configure an agent-less Quarantine assessment configuration. With Quarantine assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are quarantined. End users are provided with the means to remediate their vulnerabilities and achieve compliance. Only end-systems which are compliant can access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

When you create a Quarantine assessment configuration, all health results will be configured with the Apply Score mode. End-systems will be assessed for risk on a scale of High Risk to No Risk, with High Risk end-systems being quarantined. If desired, you can also create scoring overrides for certain health results, configuring some as informational and others as warnings. This way, if there are specific vulnerabilities that you consider to be of no concern or that you wish to consider as warnings, you can still deploy a Quarantine assessment configuration and use scoring overrides to tailor how certain exceptions are handled.

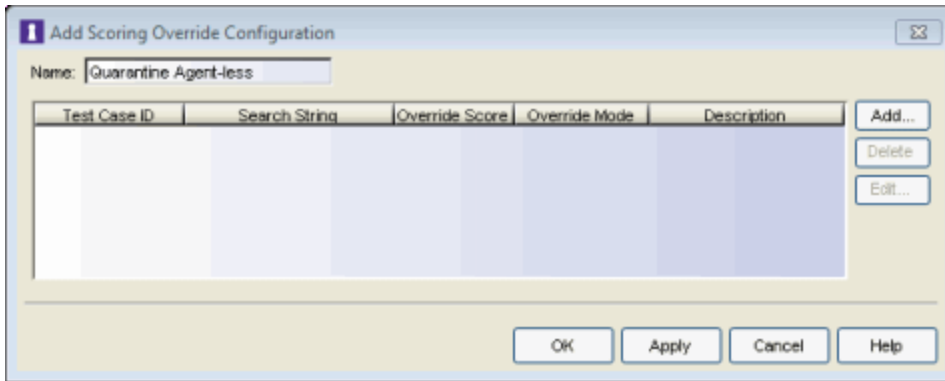
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Quarantine Agent-less."



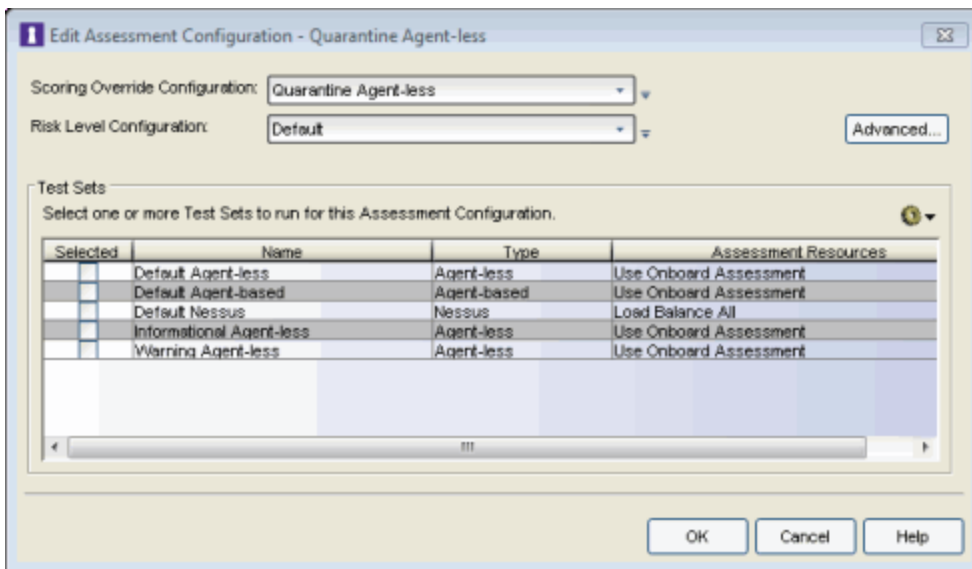
2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring override configuration called "Quarantine Agent-less."




3. Do not add any scoring overrides to the configuration at this time. Click **OK**.



4. Back in the Edit Assessment Configuration window, verify that the Quarantine Agent-less scoring override configuration is selected.



5. From the test sets Configuration Menu button  add a new agent-less test set named "Quarantine Agent-less." Configure the Quarantine agent-less test set as follows:
 - a. Select the kinds of tests to perform.
 - b. Verify that the Scoring Mode is set to Apply Score.

Add Agent-less Test Set

Name: Quarantine Agent-less

End-System Reachability Test
Configuration: ICMP Ping [Modify...](#)

Scoring
Scoring Mode: Apply Score [Manage Scoring Overrides...](#)

Behavior: [Based on Assessment Configuration 'Quarantine Agent-less'] End-systems can be quarantined. All health details are applied toward risk assessment. No End-systems will be put into the Assessment Warning notification group. No health details are warnable. Scoring Override Configuration 'Default' has no scoring overrides.

Scanning Level
Level: Default (1200+ tests (no web))

Scan Level Modifiers

Full Port Scan - Scan 'All' ports(10000+ tcp, 2700+ udp) versus 'common' ports(500+ tcp, 60+ udp)

Exhaustive Scan - Run a more thorough scan, but may cause scan to take more time

Perform Dangerous Tests - These tests may help reduce false alarms, but may crash services on the target hosts

Click **OK** to close the window.

6. Back in the Edit Assessment Configuration window, select the Quarantine Agent-less test set to include in the configuration. Click **OK**.

Edit Assessment Configuration - Quarantine Agent-less

Scoring Override Configuration: Quarantine Agent-less

Risk Level Configuration: Default [Advanced...](#)

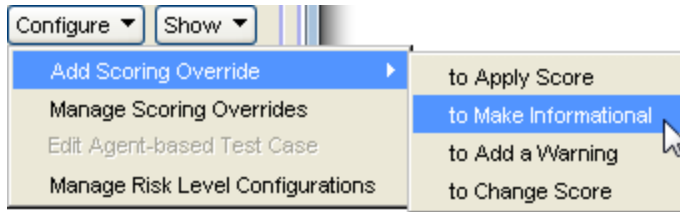
Test Sets
Select one or more Test Sets to run for this Assessment Configuration.

Selected	Name	Type	Assessment Resources
<input type="checkbox"/>	Default Agent-less	Agent-less	Use Onboard Assessment
<input type="checkbox"/>	Default Agent-based	Agent-based	Use Onboard Assessment
<input type="checkbox"/>	Default Nessus	Nessus	Load Balance All
<input type="checkbox"/>	Informational Agent-less	Agent-less	Use Onboard Assessment
<input checked="" type="checkbox"/>	Quarantine Agent-less	Agent-less	Use Onboard Assessment
<input type="checkbox"/>	Warning Agent-less	Agent-less	Use Onboard Assessment

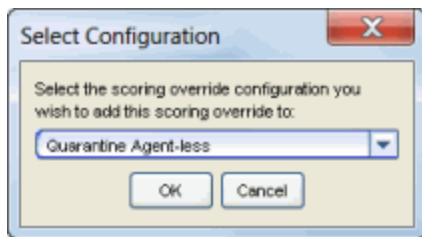
[OK](#) [Cancel](#) [Help](#)

7. Use the following steps to add scoring overrides from the [Health Result Details tab](#) (in the [End-Systems tab](#)), as you view the health results of an end-system.
 - a. Add scoring overrides for the vulnerabilities that should be informational. These are vulnerabilities that you still want to collect

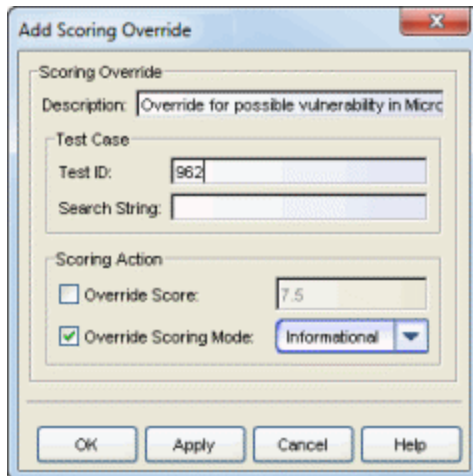
information about, but which should be excluded from risk level assessment. From the Health Result Details table, select **Configure > Add Scoring Override > to Make Informational**.



- b. Select the Quarantine Agent-less scoring override configuration. Click **OK**.



- c. Review the scoring override that will be created. No changes should be necessary. Click **OK**.



- d. Add scoring overrides for the vulnerabilities that should be warnings. These are vulnerabilities that you still want to collect information on and warn users about, but which should be excluded from risk level

- assessment. From the Health Result Details table, select **Configure > Add Scoring Override > to Add a Warning**.
- e. Add scoring overrides for the vulnerabilities that should be re-scored. These are vulnerabilities that should be included in risk level assessment, but with an altered risk level. From the Health Result Details table, select **Configure > Add Scoring Override > to Change Score**.
8. Configure the Default NAC Profile to enable assessment and select the Quarantine Agent-less assessment configuration.

The screenshot shows the 'Edit NAC Profile' dialog box for the 'Default NAC Profile'. The 'NAC Profile - Default NAC Profile' section contains the following settings:

- Reject Authentication Requests
- Authorization**
 - Accept Policy: Enterprise User
 - Replace RADIUS Attributes with Accept Policy
 - Use Quarantine Policy: Quarantine
 - Use Failsafe Policy on Error: Failsafe
- Enable Assessment**
 - Assessment Configuration: Quarantine Agent-less
 - Assessment Interval: 1 Weeks
 - Hide assessment details and remediation options from end user
 - Use Assessment Policy: Assessing During All Assessments
- Policy Mappings**
 - Manage... *Policy Mappings have not been imported from a policy domain.*

Buttons at the bottom: OK, Cancel, Help.

9. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Quarantine assessment. You can monitor the assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

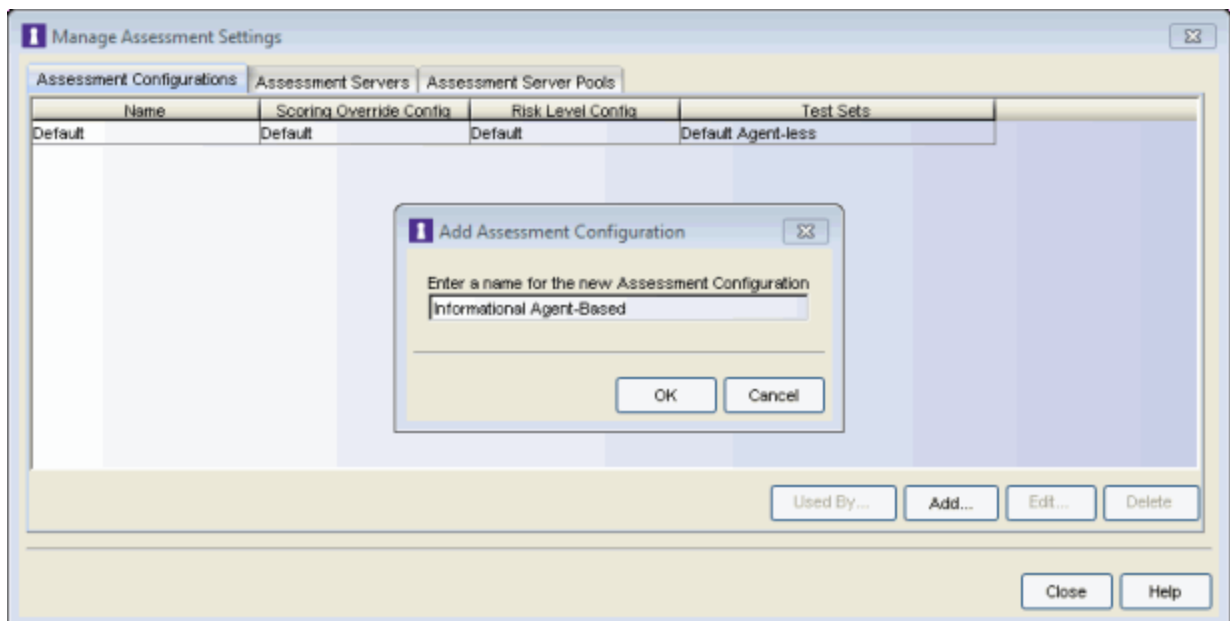
Agent-Based Assessment Configuration

This section presents instructions for creating assessment configurations for each of the three deployment phases, using an agent-based test set. A new assessment configuration is created for each phase, rather than modifying the existing assessment configuration. This allows you to easily revert back to an earlier phase at any time by changing the assessment configuration that your NAC profile is using.

Agent-Based Informational Assessment

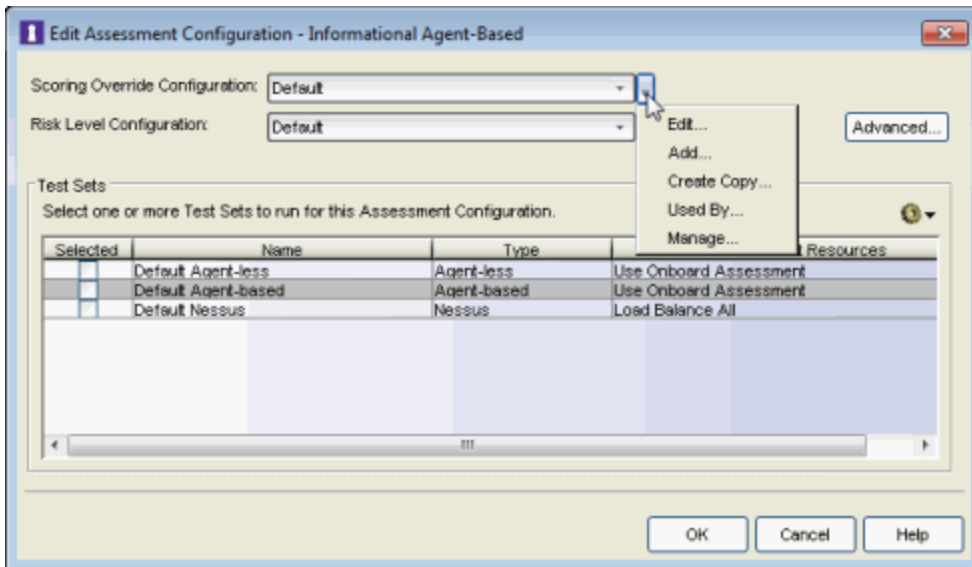
Use the following steps to create and configure an agent-based Informational assessment configuration. With Informational assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, but no action is taken against end-systems with vulnerabilities. This allows you to use assessment as a data-gathering mechanism without end-systems being quarantined. For more information, see the [NAC Assessment Phased Deployment Guide](#).

1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Informational Agent-Based."

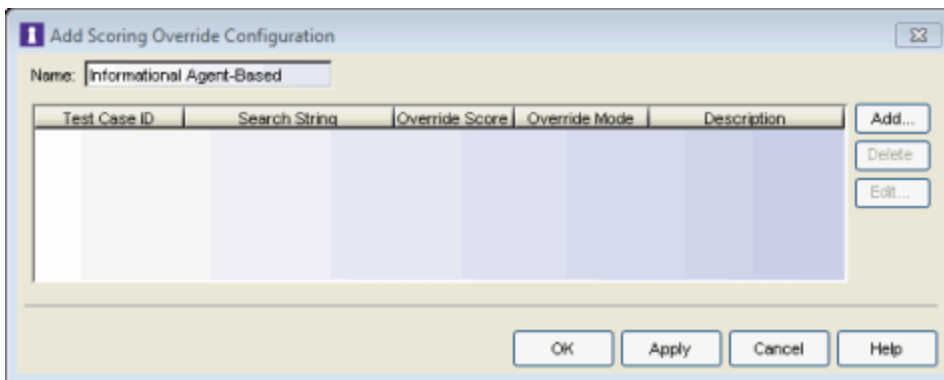


2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring

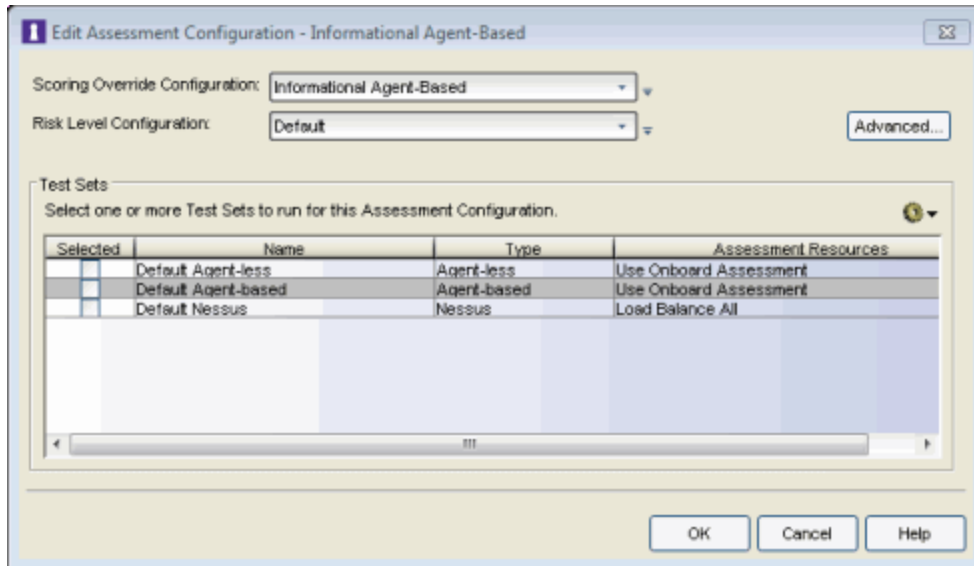
override configuration called "Informational Agent-Based."





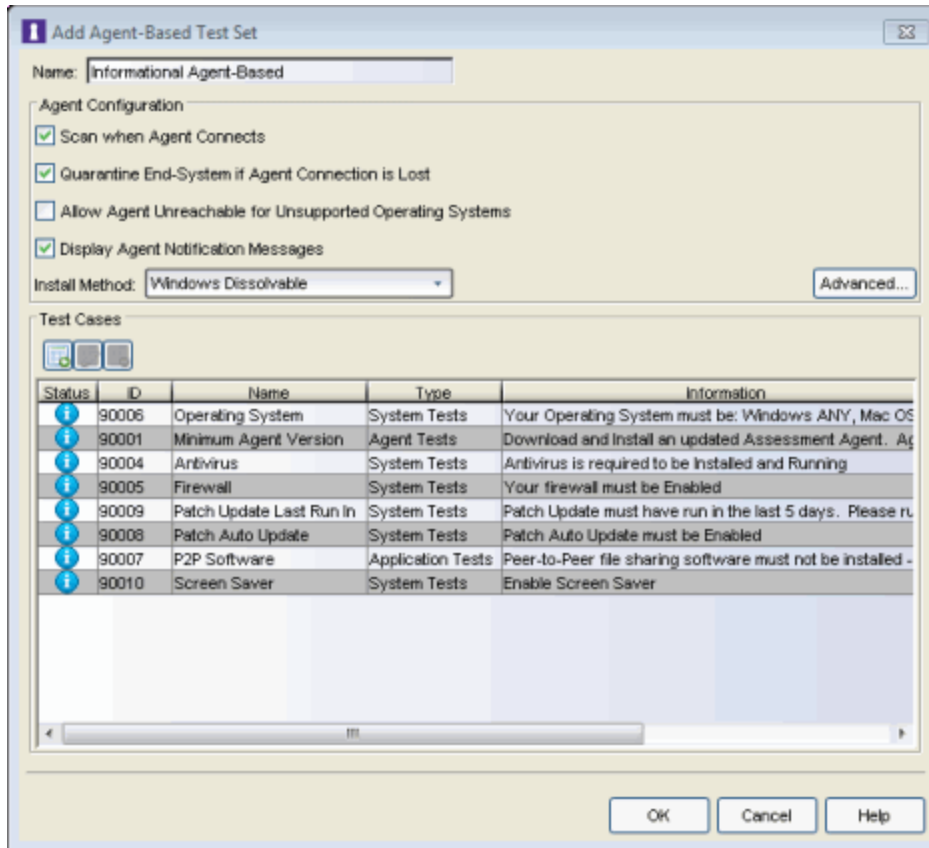
- Do not add any scoring overrides to the configuration at this time. Click **OK**.



- Back in the Edit Assessment Configuration window, verify that the Informational Agent-Based scoring override configuration is selected.

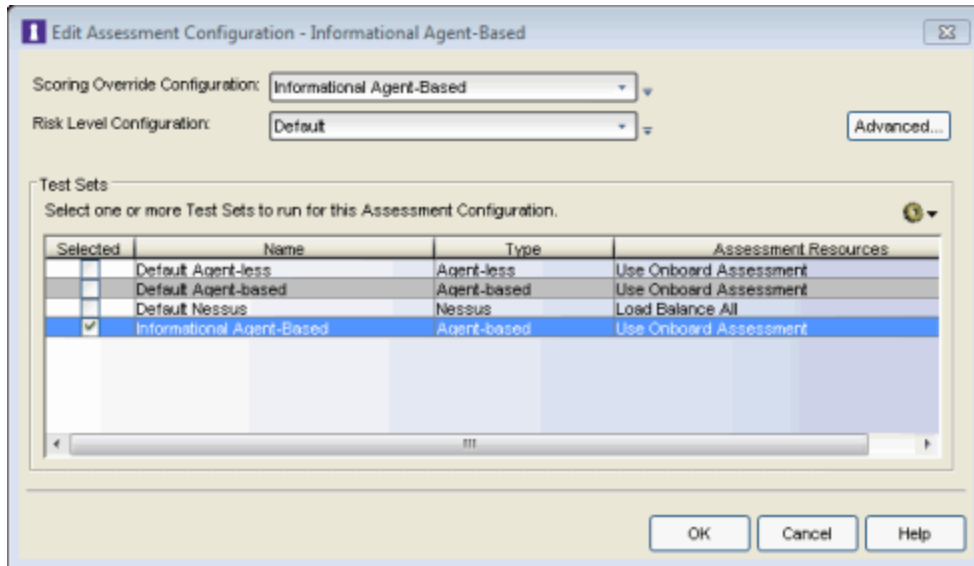


5. From the test sets Configuration Menu button  add a new Agent-Based Test Set named "Informational Agent-Based." Configure the test set as follows:
 - a. Set up the agent and choose the tests that will be executed.
 - b. Configure the test set to run entirely in an informational mode by setting the Test Status of every test case to Informational . This is done in the test case Editor, accessed by double-clicking on the test case or when creating a new test.

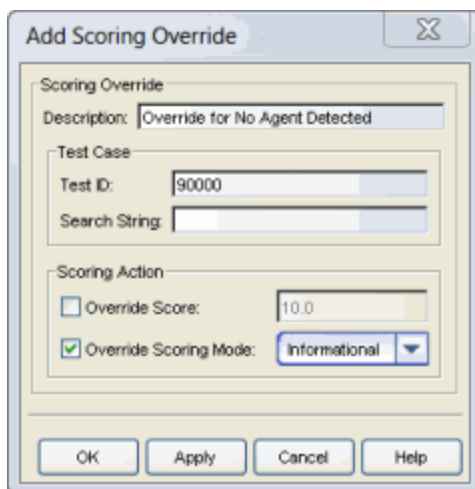


Click **OK** to close the window.

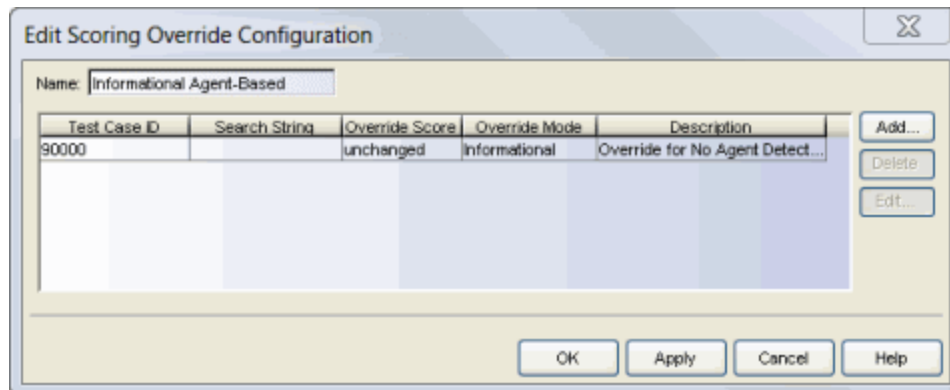
- Back in the Edit Assessment Configuration window, verify that the Informational Agent-Based test set is selected. Click **OK**.



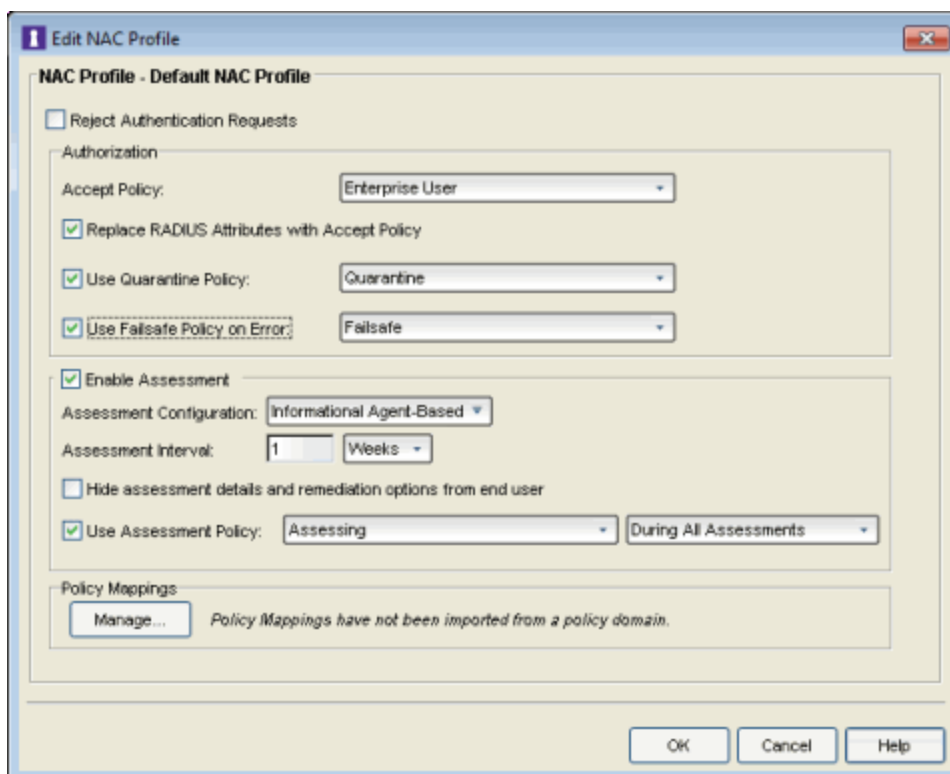
7. By default, the [No Agent Detected](#) test result score will be applied to risk assessment, and the end-system will be quarantined. If you choose to make this test result informational, you will need to set up a scoring override for Test ID 90000. This will be the only scoring override that will be configured.
 - a. Open the [Edit Scoring Override Configuration window](#) for the Informational Agent-Based scoring override configuration, using the Configuration Menu button in the Scoring Override Configuration field. Click **Add** to add the following scoring override to the configuration.



- b. Click **OK**. The scoring override will be added to the Informational Agent-Based scoring override configuration. Click **OK** to close the window.



8. Configure the Default NAC Profile to enable assessment and select the Informational Agent-Based assessment configuration.



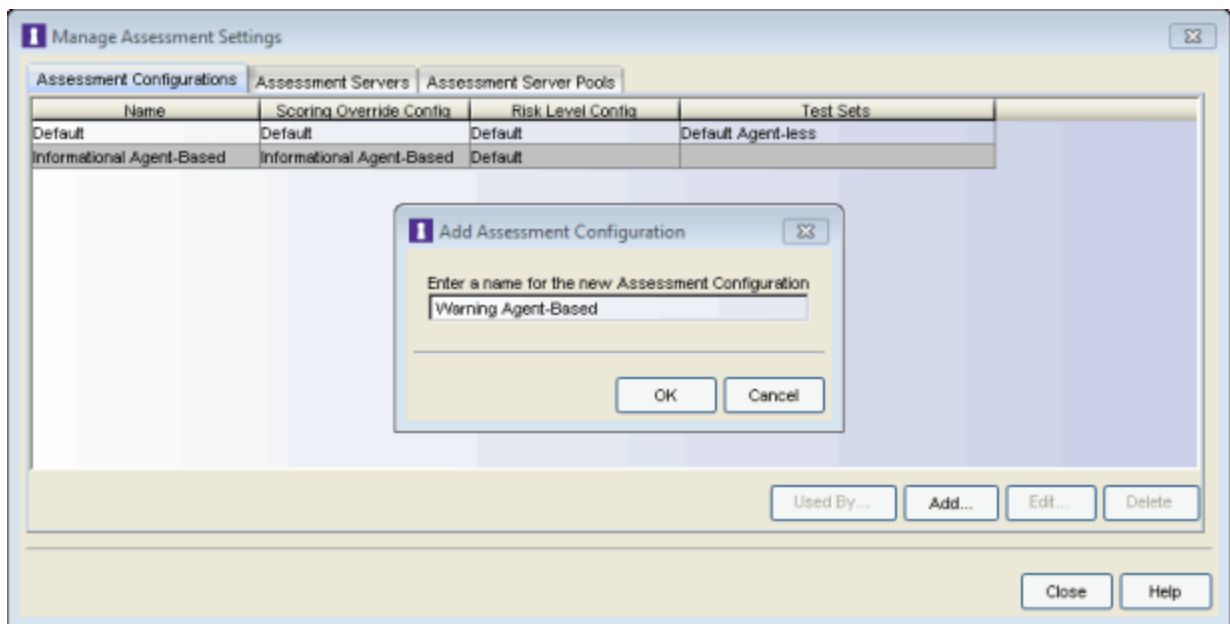
9. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Informational assessment. You can

see assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

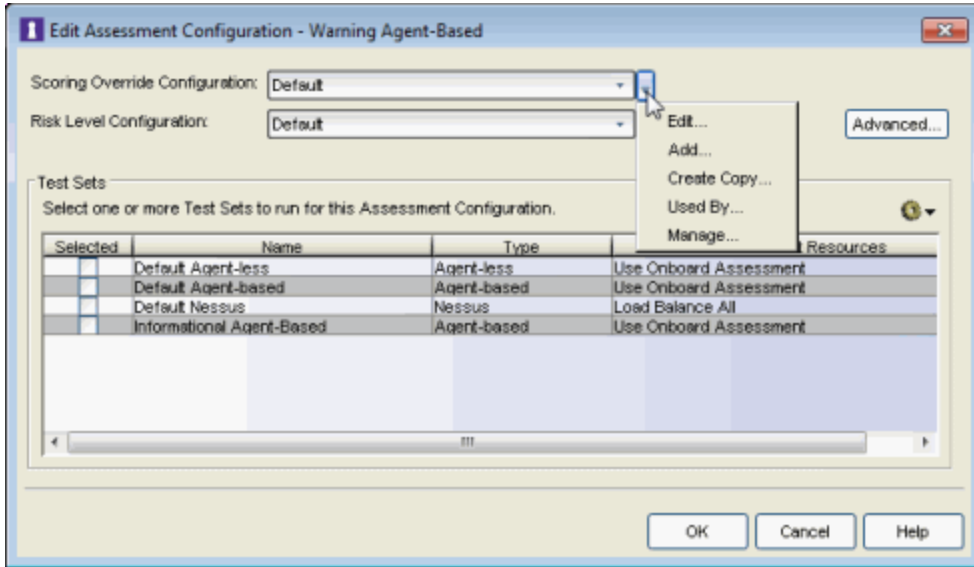
Agent-Based Warning Assessment

Use the following steps to create and configure an agent-based Warning assessment configuration. With Warning assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are notified. End users are provided with the means to remediate their vulnerabilities and achieve compliance, however end-systems which are not compliant can still access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

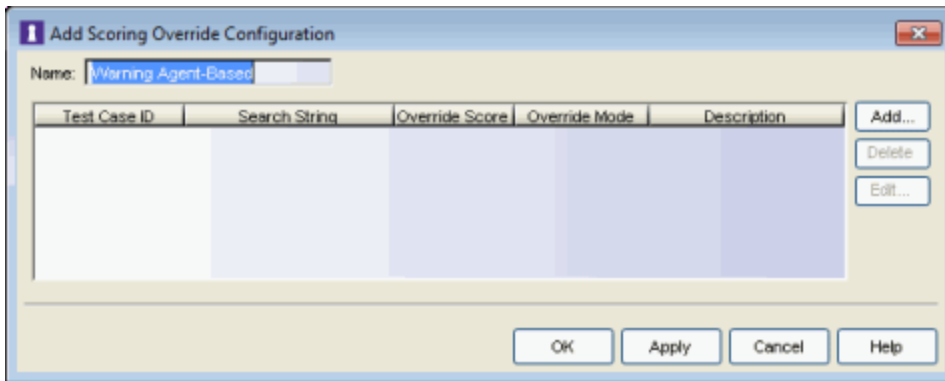
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Warning Agent-Based."



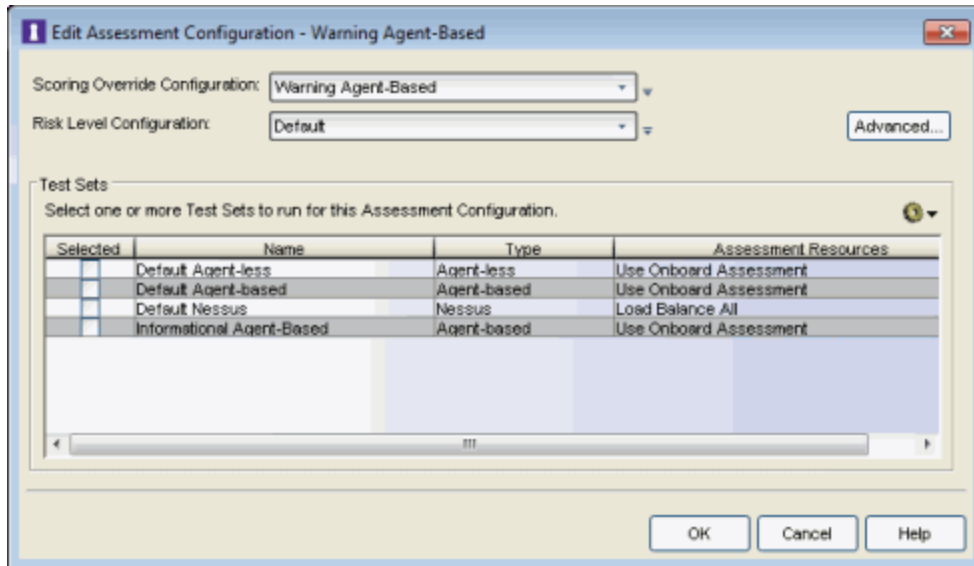
2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring override configuration called "Warning Agent-Based."



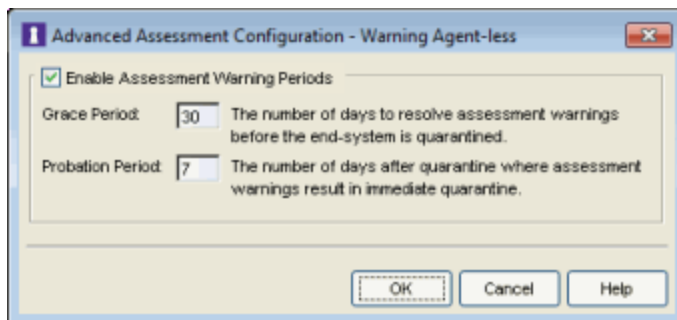
3. Do not add any scoring overrides to the configuration at this time. Click **OK**.





4. Back in the Edit Assessment Configuration window, verify that the Warning Agent-Based scoring override configuration is selected.

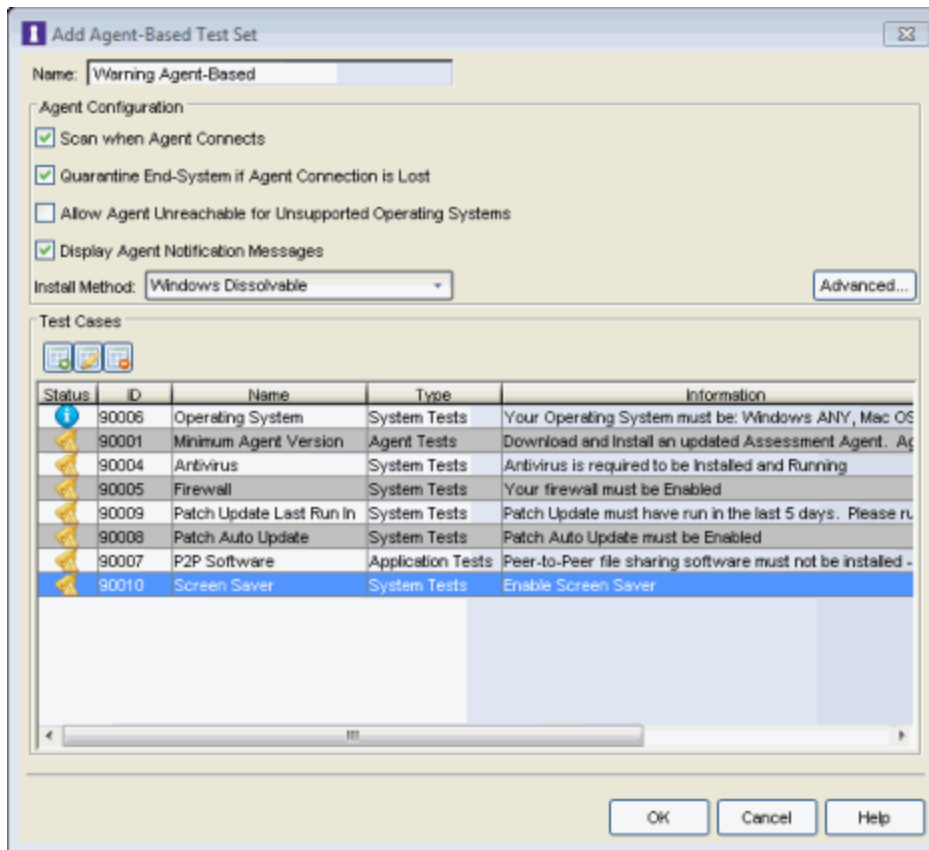


5. Click the **Advanced** button to open the [Advanced Assessment Configuration window](#) where you can enable Assessment Warning Periods. Set the number of Grace Period and Probation Period days to the desired values. Click **OK**.



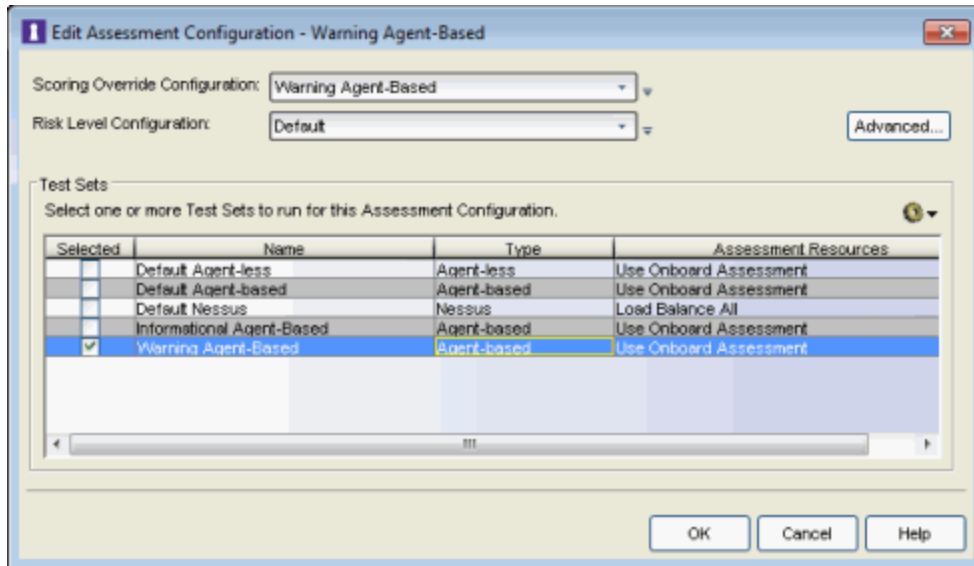
6. Back in the Edit Assessment Configuration window, from the test sets Configuration Menu button  add a new agent-based test set named "Warning Agent-Based." Configure the test set as follows:
 - a. Set up the agent and choose the tests that will be executed.
 - b. To use the [agent notification](#) feature (where the agent is used to notify end users of assessment violations), you must have the Display Agent Notification Messages option selected as well as the Advanced Agent Configuration option to Allow Remediation Through Agent selected.

- c. Configure each test case that you want to run in warning mode by setting the Test Status of that test case to Warning . This is done in the test case Editor, accessed by double-clicking on the test case or when creating a new test. All other tests should be configured to be Informational.

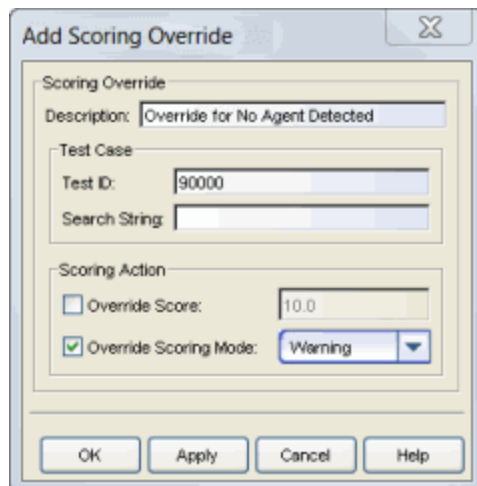


Click **OK** to close the window.

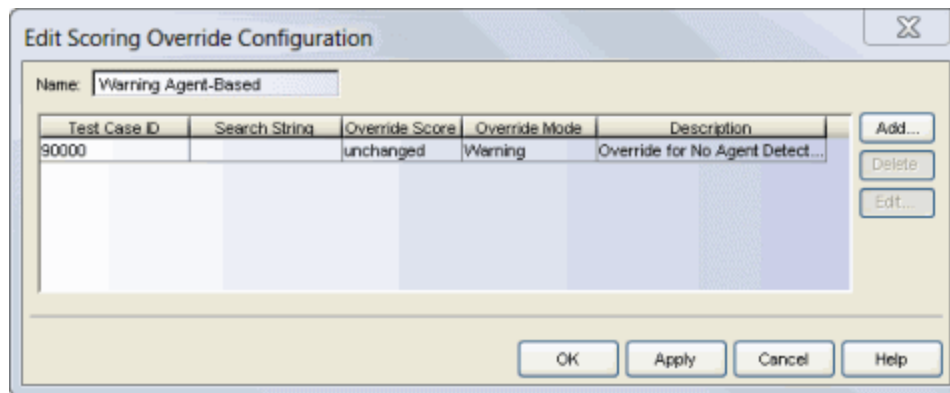
7. Back in the Edit Assessment Configuration window, select the Warning Agent-Based test set to include in the configuration. Click **OK**.



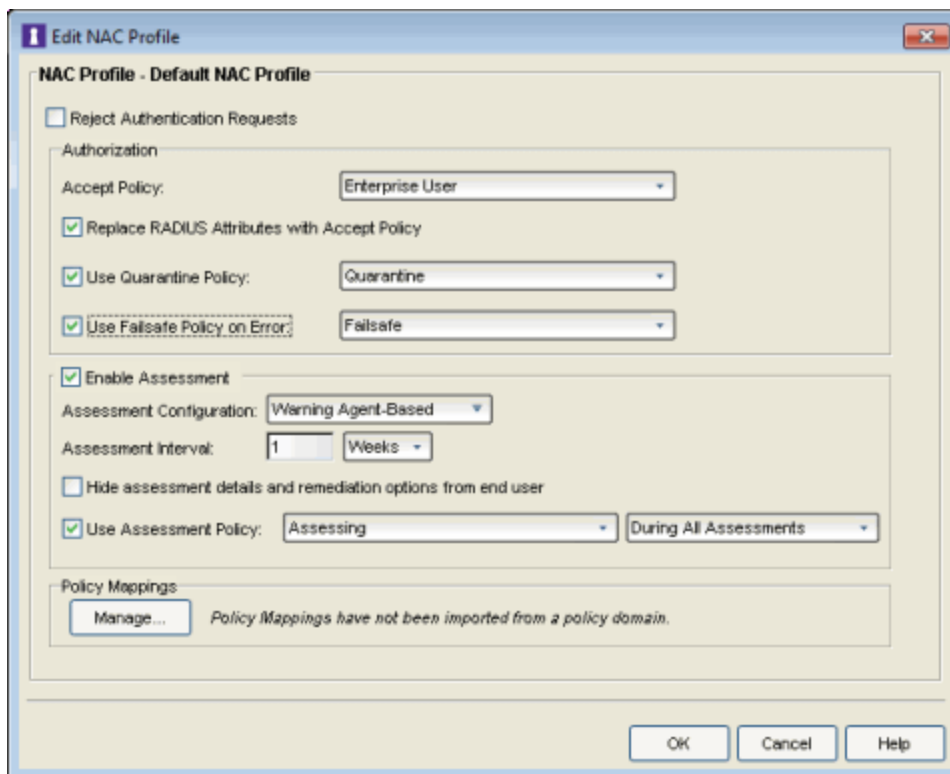
8. By default, the [No Agent Detected](#) test result score will be applied to risk assessment, and the end-system will be quarantined. If you choose to make this test result a warning, you will need to set up a scoring override for Test ID 90000. This will be the only scoring override that will be configured.
 - a. Open the [Edit Scoring Override Configuration window](#) for the Warning Agent-Based scoring override configuration, using the Configuration Menu button in the Scoring Override Configuration field. Click **Add** to add the following scoring override to the configuration.



- b. Click **OK**. The scoring override will be added to the Warning Agent-Based scoring override configuration. Click **OK** to close the window.



9. Configure the Default NAC Profile to enable assessment and select the Warning Agent-Based assessment configuration.



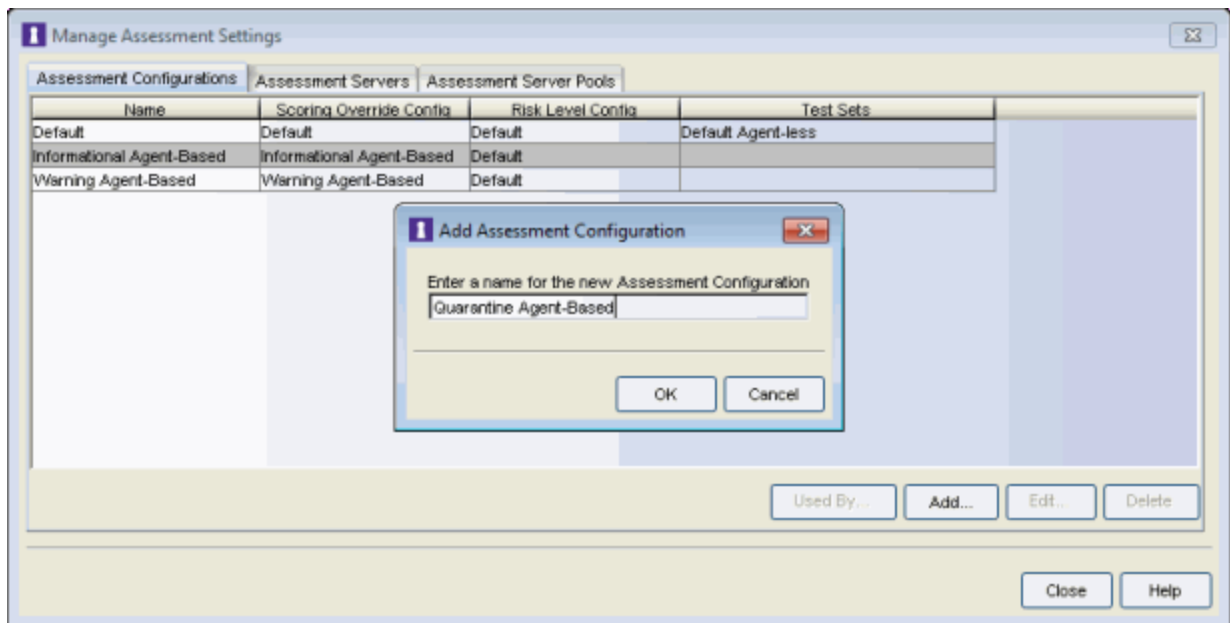
10. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Warning assessment. You can monitor the assessment results in the [End-Systems tab](#). For more

information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

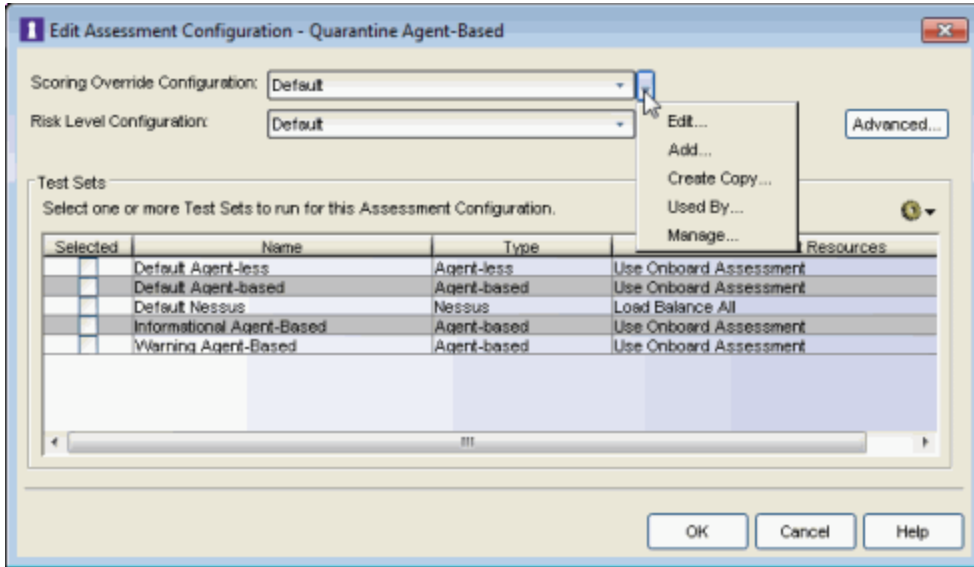
Agent-Based Quarantine Assessment

Use the following steps to create and configure an agent-based Quarantine assessment configuration. With Quarantine assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are quarantined. End users are provided with the means to remediate their vulnerabilities and achieve compliance. Only end-systems which are compliant can access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

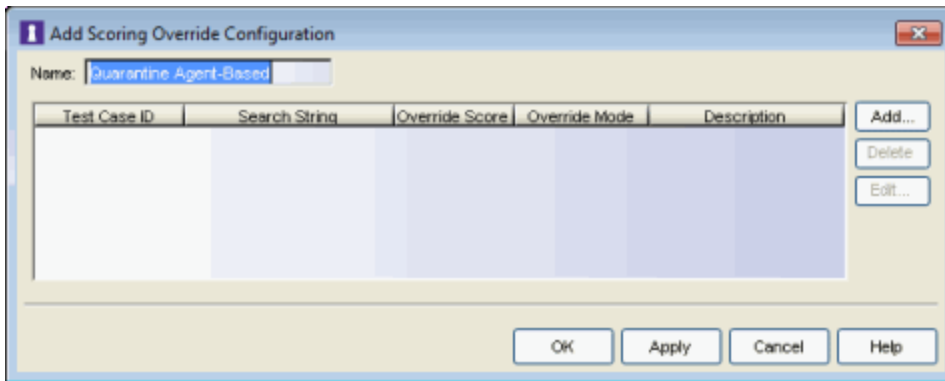
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Quarantine Agent-Based."



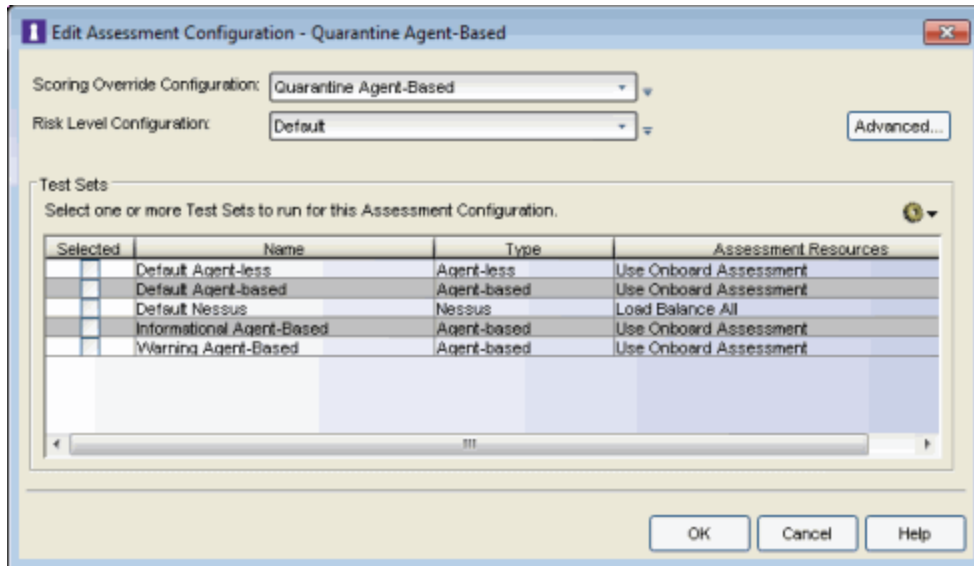
2. In the Edit Assessment Configuration window, use the Configuration Menu button in the Scoring Override Configuration field to add a new scoring override configuration called "Quarantine Agent-Based."





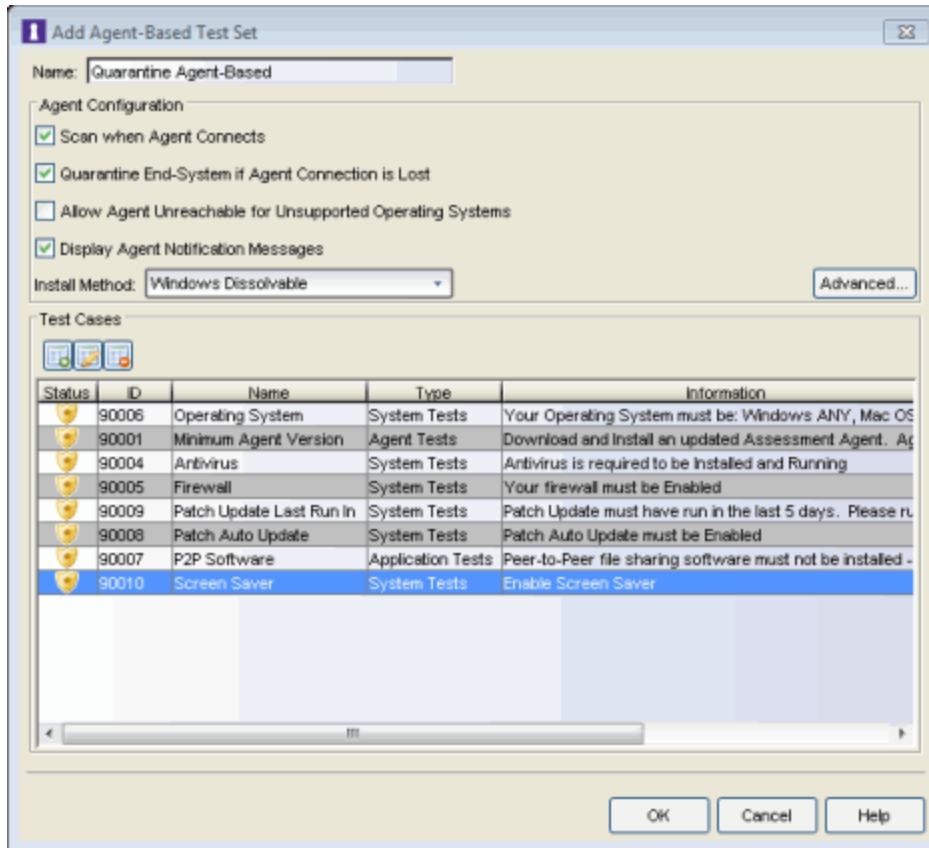
- Do not add any scoring overrides to the configuration at this time. Click OK.



- Back in the Edit Assessment Configuration window, verify that the Quarantine Agent-Based scoring override configuration is selected.

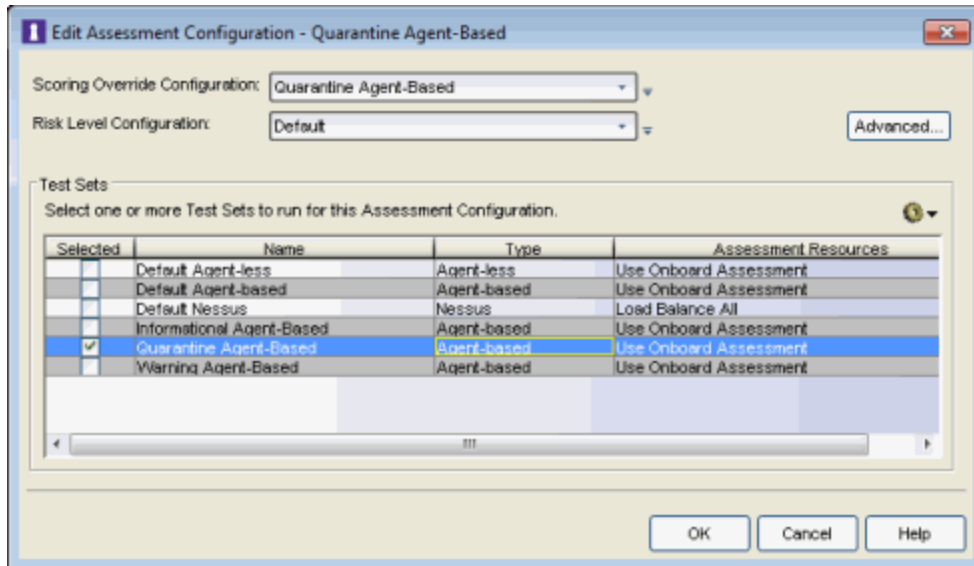


5. From the test sets Configuration Menu button  add a new agent-based test set named "Quarantine Agent-Based." Configure the test set as follows:
 - a. Set up the agent and choose the tests that will be executed.
 - b. To use the [agent notification](#) feature (where the agent is used to notify end users of assessment violations), you must have the Display Agent Notification Messages option selected as well as the Advanced Agent Configuration option to Allow Remediation Through Agent selected.
 - c. Configure each test case that you want included in the quarantine decision by setting the Test Status of that test case to Mandatory . This is done in the test case Editor, accessed by double-clicking on the test case or when creating a new test. Other tests can be configured as Informational or Warning.

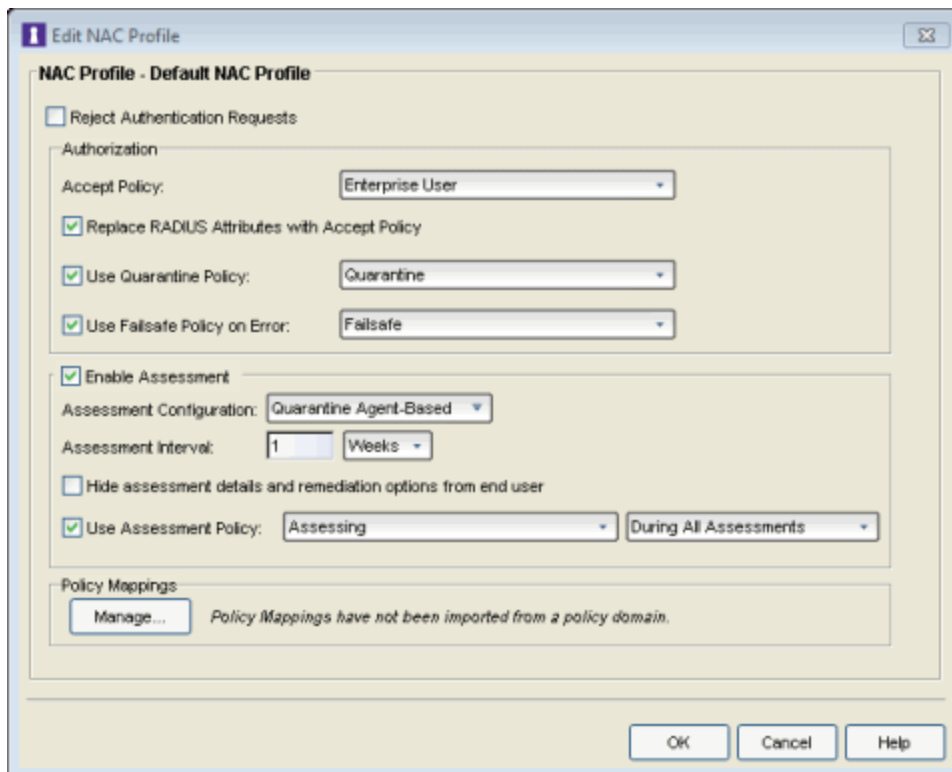


Click **OK** to close the window.

- Back in the Edit Assessment Configuration window, select the Quarantine Agent-Based test set to include in the configuration. Click **OK**.



- Configure the Default NAC Profile to enable assessment and select the Quarantine Agent-Based assessment configuration.



8. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Quarantine assessment. You can monitor the assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

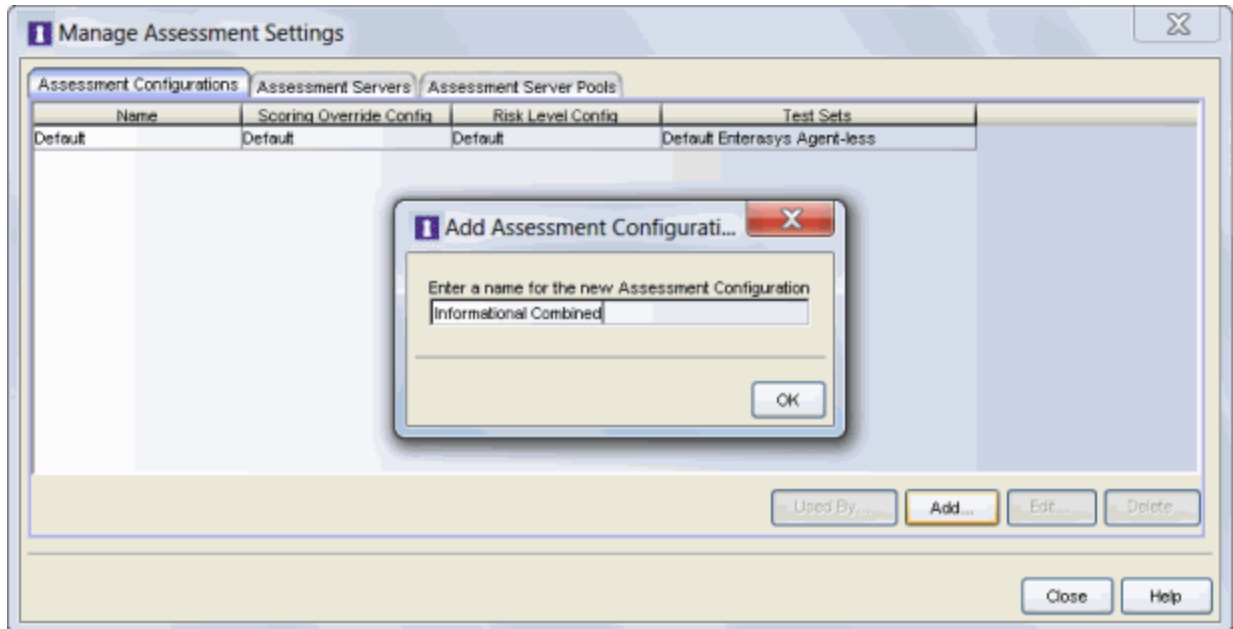
Combined Assessment Configuration

This section presents instructions for creating assessment configurations for each of the three deployment phases, using both an agent-less and an agent-based test set. A new assessment configuration is created for each phase, rather than modifying the existing assessment configuration. This allows you to easily revert back to an earlier phase at any time by changing the assessment configuration that your NAC profile is using.

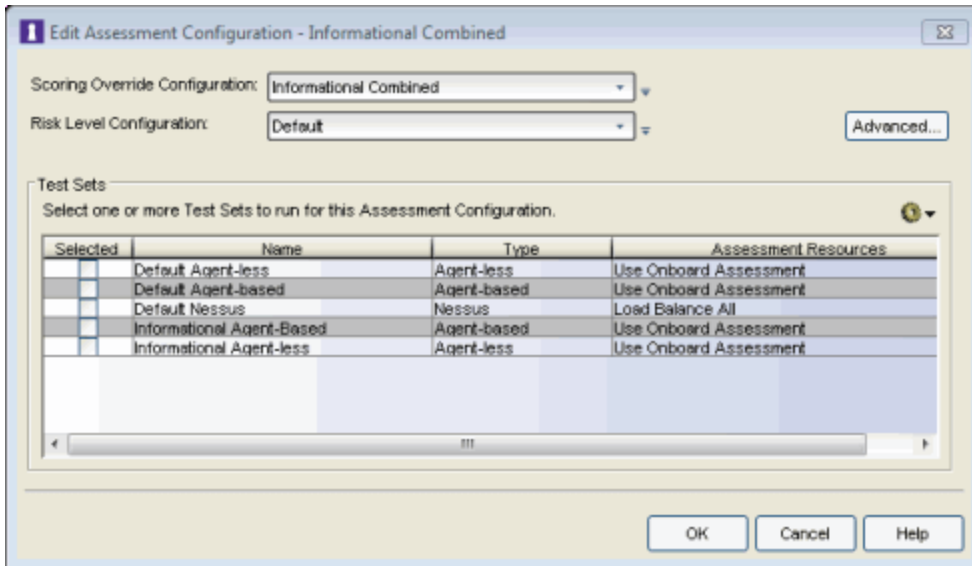
Combined Informational Assessment

Use the following steps to create and configure a combined Informational assessment configuration. With Informational assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, but no action is taken against end-systems with vulnerabilities. This allows you to use assessment as a data-gathering mechanism without end-systems being quarantined. For more information, see the [NAC Assessment Phased Deployment Guide](#).

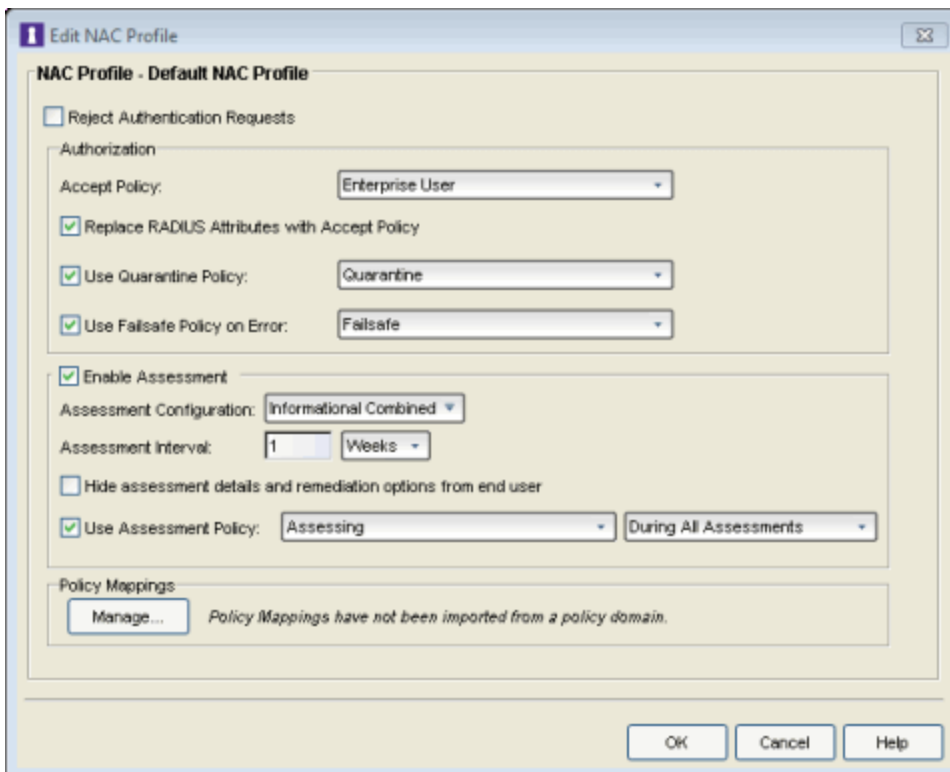
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Informational Combined."



2. Use [steps 2 through 4](#) in the [Agent-less Informational Assessment section](#) to create a scoring override configuration to use in your Combined assessment configuration. Name the scoring override configuration "Informational Combined."
3. Use [step 5](#) in the [Agent-less Informational Assessment section](#) to create an Informational agent-less test set to use in your Combined assessment configuration.
4. Use [step 5](#) in the [Agent-Based Informational Assessment section](#) to create an Informational agent-based test set to use in your Combined assessment configuration.
5. Use [step 7](#) in the [Agent-Based Informational Assessment section](#) to create a scoring override for the [No Agent Detected](#) health result if you would like the result to be informational. Note that you will need to add the scoring override to the Informational Combined scoring override configuration, instead of the Informational Agent-Based scoring override configuration as described in the step.
6. Back in the Edit Assessment Configuration window, select the Informational Agent-less and Agent-Based test sets to include in the configuration. Click **OK**.



- Configure the Default NAC Profile to enable assessment and select the Informational Combined assessment configuration.

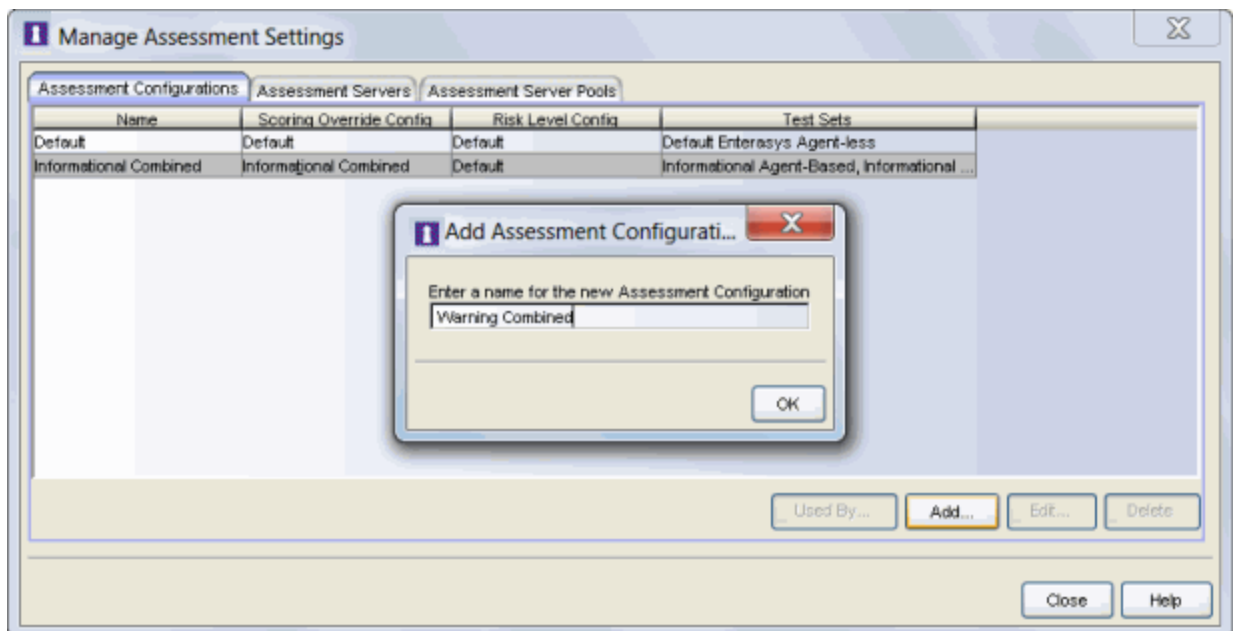


8. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Informational assessment. You can see assessment results in the [End-Systems](#) tab. For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

Combined Warning Assessment

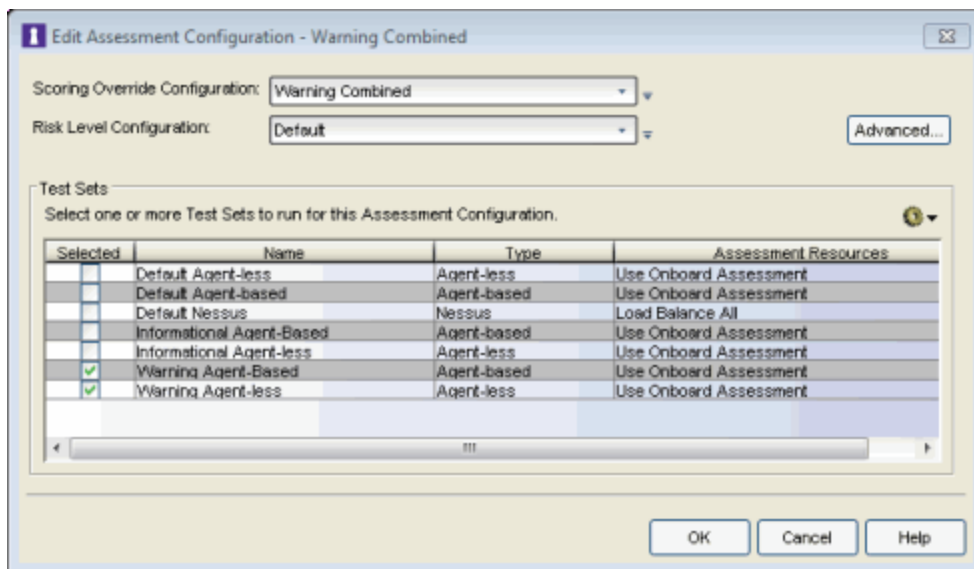
Use the following steps to create and configure a combined Warning assessment configuration. With Warning assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are notified. End users are provided with the means to remediate their vulnerabilities and achieve compliance, however end-systems which are not compliant can still access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Warning Combined."

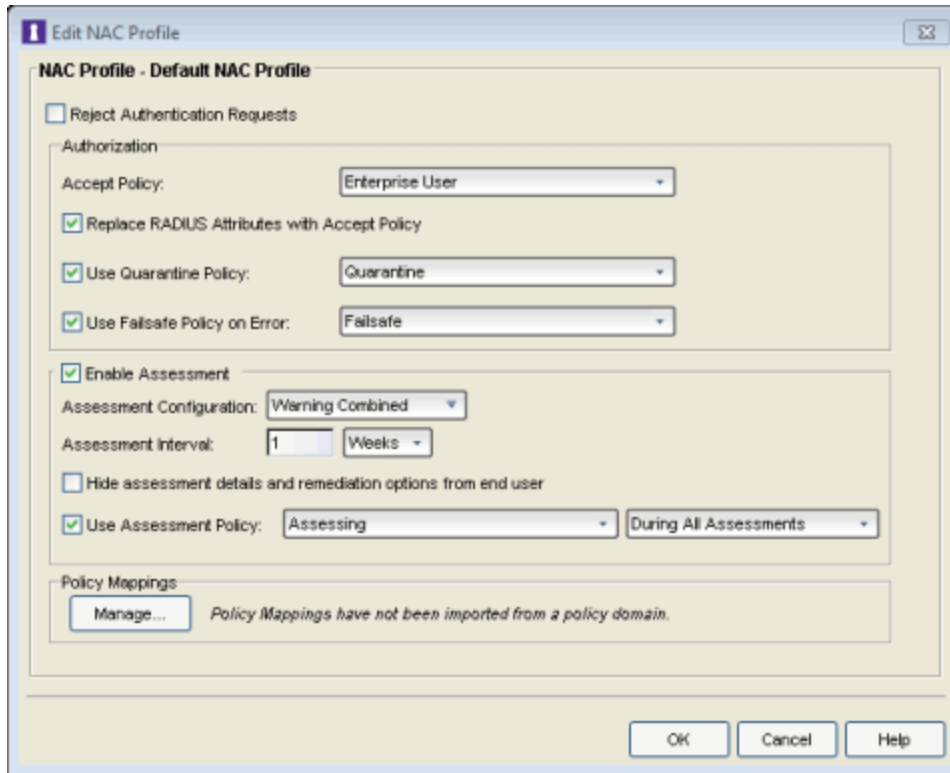


2. Use [steps 2 through 5](#) in the [Agent-less Warning Assessment section](#) above to create a scoring override configuration to use in your Combined assessment configuration. Name the scoring override configuration "Warning Combined."

3. Use [step 6](#) in the [Agent-less Warning Assessment section](#) above to create a Warning Agent-less test set to use in your Combined Assessment Configuration.
4. Use [step 6](#) in the [Agent-Based Warning Assessment section](#) above to create a Warning Agent-Based test set to use in your Combined Assessment Configuration.
5. Use [step 8](#) in the [Agent-Based Warning Assessment section](#) to create a scoring override for the [No Agent Detected](#) health result if you would like the result to be a warning. Note that you will need to add the scoring override to the Warning Combined scoring override configuration, instead of the Warning Agent-Based scoring override configuration as described in the step.
6. Back in the Edit Assessment Configuration window, select the Warning Agent-less and Agent-Based test sets to include in the configuration. Click OK.



7. Use [step 8](#) in the [Agent-less Warning Assessment section](#) to add Warning scoring overrides to your assessment configuration. Be sure to add the overrides to the Warning Combined scoring override configuration.
8. Configure the Default NAC Profile to enable assessment and select the Warning Combined assessment configuration.

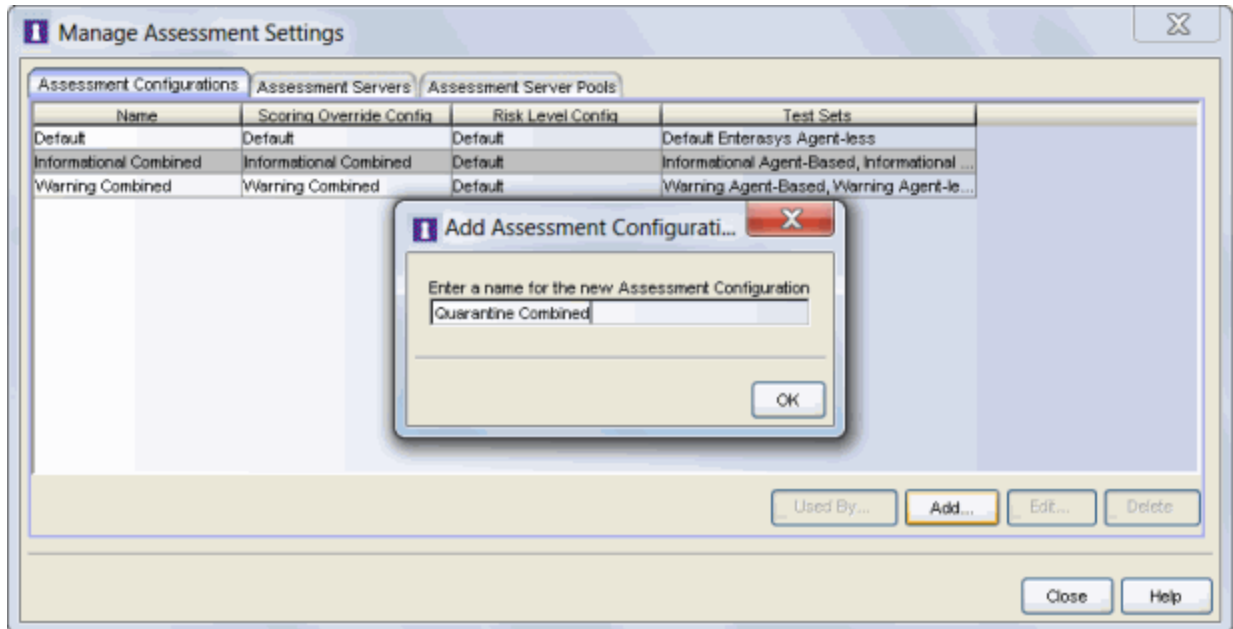


9. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Warning assessment. You can see assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

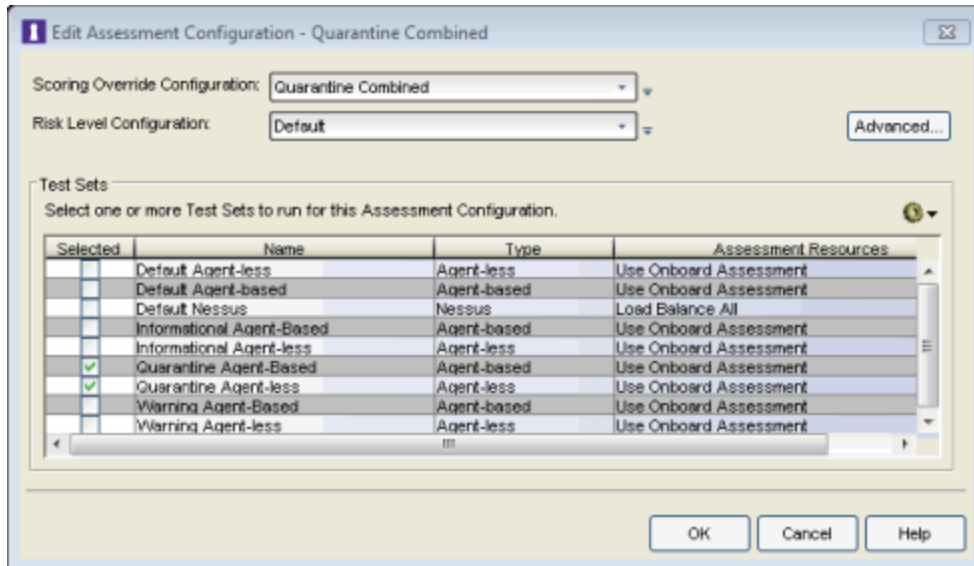
Combined Quarantine Assessment

Use the following steps to create and configure a combined Quarantine assessment configuration. With Quarantine assessment, end-systems connecting to the network are assessed for security compliance. The assessment results are reported, and end-systems with vulnerabilities are quarantined. End users are provided with the means to remediate their vulnerabilities and achieve compliance. Only end-systems which are compliant can access the network. For more information, see the [NAC Assessment Phased Deployment Guide](#).

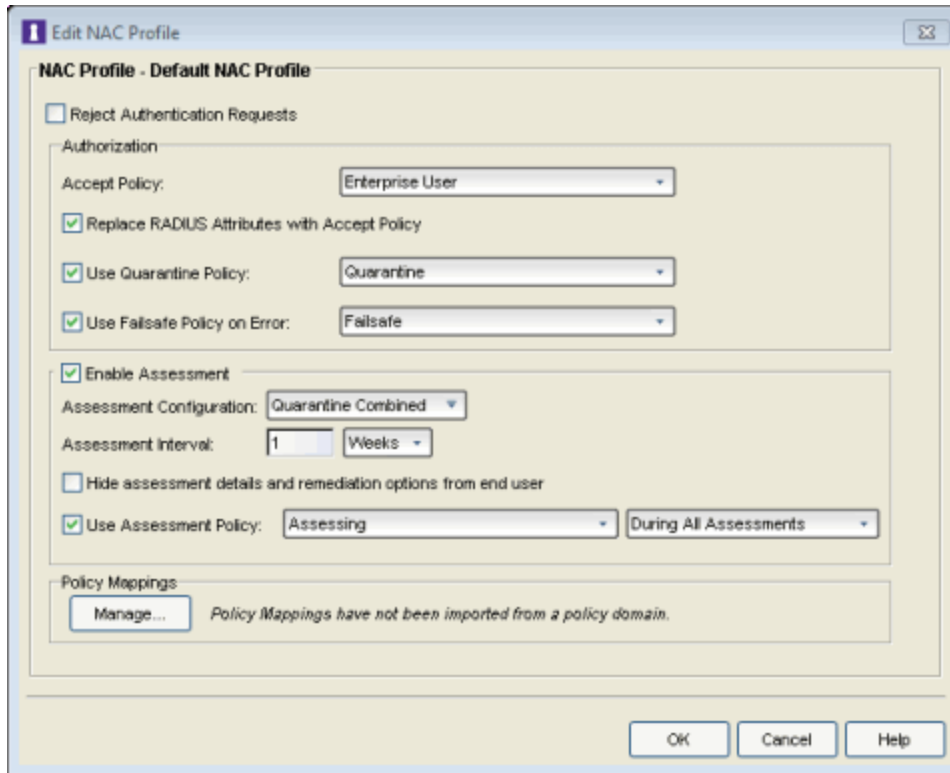
1. From the [Manage Assessment Settings window](#), click **Add** to create a new assessment configuration and name it "Quarantine Combined."



2. Use [steps 2 through 4](#) in the [Agent-less Quarantine Assessment section](#) to create a scoring override configuration to use in your Combined assessment configuration. Name the scoring override configuration "Quarantine Combined."
3. Use [step 5](#) in the [Agent-less Quarantine Assessment section](#) to create a Quarantine agent-less test set to use in your Combined assessment configuration.
4. Use [step 5](#) in the [Agent-Based Quarantine Assessment section](#) to create a Quarantine agent-based test set to use in your Combined assessment configuration.
5. Back in the Edit Assessment Configuration window, select the Quarantine Agent-less and Agent-Based test sets to include in the configuration. Click **OK**.



- Use [step 7](#) in the [Agent-less Quarantine Assessment section](#) to add scoring overrides to your assessment configuration. Be sure to add the overrides to the Quarantine Combined scoring override configuration.
- Configure the Default NAC Profile to enable assessment and select the Quarantine Combined assessment configuration.



8. Enforce the new configuration to your appliances. All appliances using the Default NAC Profile will now perform Quarantine assessment. You can see assessment results in the [End-Systems tab](#). For more information, see the [Viewing Health Results](#) section of the NAC Assessment Phased Deployment Guide.

Related Information

- [NAC Assessment Phased Deployment Guide](#)
- [How to Deploy Agent-Based Assessment](#)
- [How to Set Up Assessment Remediation](#)

How to Deploy Agent-Based Assessment

This Help topic describes the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.

Refer to [How to Set Up Assessment](#) for general information on setting up assessment on your network.

Instructions on:

- [Configuring Agent Deployment](#)
- [Performing a Managed Deployment or Installation](#)
- [Agent Icons and Notification Messages](#)
- [Agent Information Messages](#)
- [Agent Diagnostics](#)

Configuring Agent Deployment

The assessment agent is an integrated component of the Extreme Access Control Controller or Access Control Gateway engine and is downloaded by the end user from the Assessment/Remediation portal web page. When end users attempt to connect to the network, they are presented with the Assessment/Remediation web page, where they can download the agent and assessment can take place. NAC Manager automatically supplies the link to the appropriate engine on the Assessment/Remediation web page that is presented to the end user.

NOTES: -- The end user must have Write privileges for the `C:\Program Files` directory to install a persistent agent. A non-admin user by default does not have this permission.

-- Port 8080 must be open between the end-system and the Access Control engine for downloading the agent.

-- Port 8443 must be open between the end-system and the Access Control engine for secure communication.

These are the supported operating systems for end-systems connecting to the network through a Access Control deployment that is implementing agent-based assessment.

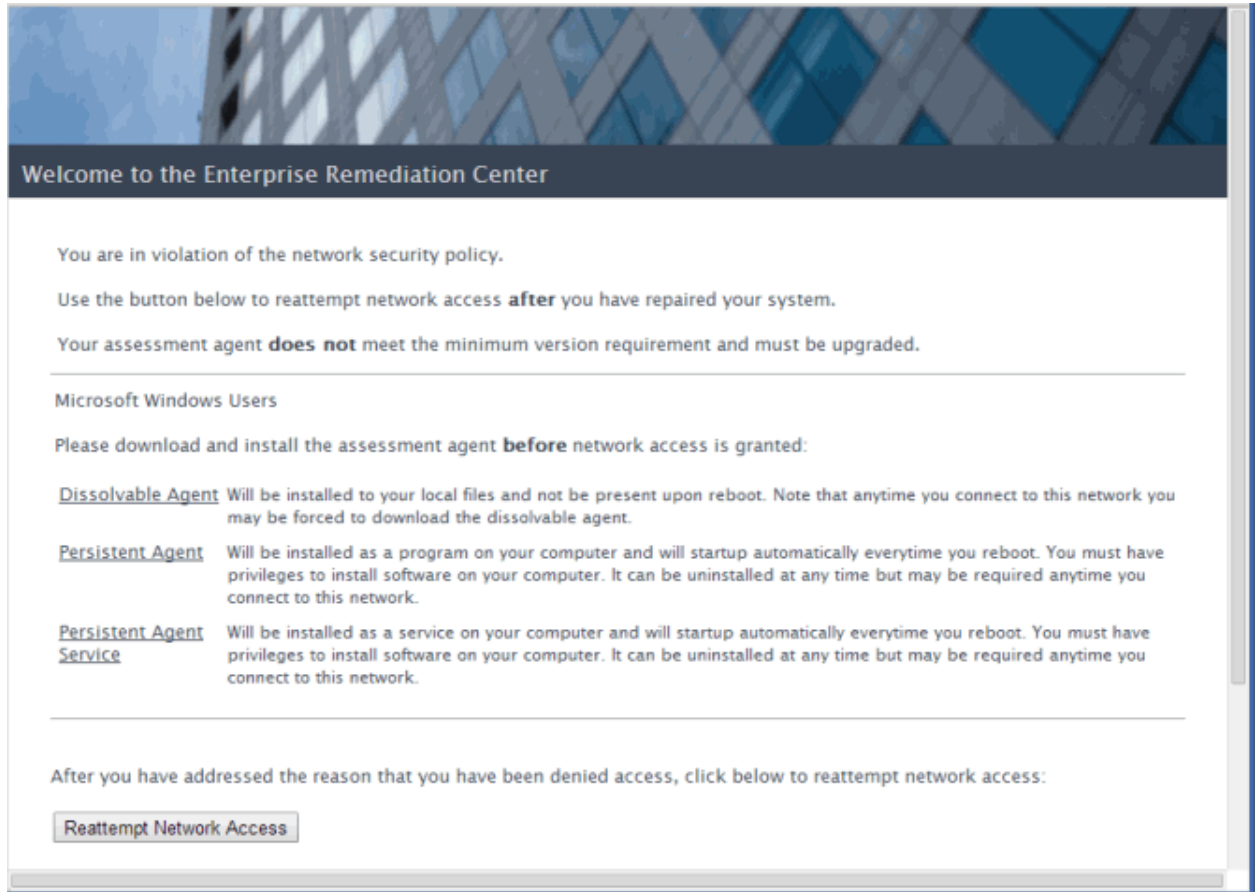
- Windows Vista
- Windows XP
- Windows 2008
- Windows 2003
- Windows 2000
- Windows 7
- Windows 8
- Windows 8.1
- Mac OS X - Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, Mavericks, Yosemite, and El Capitan

The end-system must support the following operating system disk space and memory requirements as provided by Microsoft® and Apple®:

- Windows Install: 80 MB of physical disk space for installation files; 40 MB of available memory (80 MB with Service Agent)
- Mac Install: 10 MB of physical disk space for installation files; 120 MB of real memory

Use the following steps to configure and deploy agent-based assessment in the network.

1. Configure assessment for your network using the instructions in [How to Set Up Assessment](#).
2. Configure remediation for your network using the instructions in [How to Set Up Assessment Remediation](#).
3. The end user connects to the network and receives an error message via the Assessment/Remediation web page that provides a link for downloading the agent.



4. The end user clicks on the link to download the agent. Depending on whether the agent is a dissolvable or persistent agent (as configured in the [Agent-Based Test Set](#)), the following actions take place.

For Dissolvable Agents:

- a. The agent is automatically installed to the user's `\Local Settings\Temp` directory.
- b. The agent process automatically starts and an [agent icon](#) is added to the Task Bar Notification area.
- c. The assessment automatically takes place.
- d. The end-system receives a [notification message](#) (if enabled in the [Agent-Based Test Set](#)) that tells them if they are quarantined, have assessment warnings, are in an error state, or are accepted. Users that are quarantined, have warnings, or are in an error state are directed to start the remediation process, while accepted end-systems are allowed access to the network.
If agent notification messages are disabled, end users that are

quarantined, have warnings, or are in an error state must follow the links on the Assessment/Remediation web page to start the remediation process. Accepted end users click the "Reattempt Network Access" button on the Assessment/Remediation web page (or open a new browser window) and are allowed network access.

- e. The agent dissolves after the end user logs out or reboots their system.

For Persistent/Service Agents:

- a. The agent is automatically installed to the `<install directory>\NetSight\NAC Agent` directory. The end user must have Write privileges to install in this directory.
- b. The agent process automatically starts and an [agent icon](#) is added to the Task Bar Notification area. In addition, a shortcut to the Agent is added to the Startup folder so that the agent starts automatically when the system reboots, and the service agent has a Windows service that starts automatically on machine start.
- c. The assessment automatically takes place.
- d. The end-system receives a [notification message](#) (if enabled in the [Agent-Based Test Set](#)) that tells them if they are quarantined, have assessment warnings, are in an error state, or accepted. Users that are quarantined, have warnings, or are in an error state are directed to start the remediation process, while accepted end-systems are allowed access to the network.

If agent notification messages are disabled, end users that are quarantined, have warnings, or are in an error state must follow the links on the Assessment/Remediation web page to start the remediation process. Accepted end users click the "Reattempt Network Access" button on the Assessment/Remediation web page (or open a new browser window) and are allowed network access.

- e. The agent can be uninstalled in two ways:
 - Using Add or Remove Programs in the Control Panel.
 - Right-clicking on the Windows Installer package and choosing Uninstall.

Performing a Managed Deployment or Installation

To perform a managed deployment or installation of the assessment agent in a Windows network environment, perform the following steps. The installer program (downloaded in step 1) varies depending on whether you are deploying a persistent assessment agent to each end-system or installing the agent as a Windows service on each end-system.

1. Download the appropriate Microsoft Installer program from your Access Control engine to your SMS (Systems Management Server) system using one of the following commands.

If deploying the assessment agent:

```
https://<Access  
Controlengineip>:8444/Admin/downloads/NacAgentInstall_  
<Access Controlengineip>.msi
```

If installing the assessment agent as a service:







```
https://<Access  
Controlengineip>:8444/Admin/downloads/NacAgentService_  
<Access Controlengineip>.msi
```

where <Access Controlengineip> is the IP address of a Access Control Gateway engine or the Access Control Engine IP of a Access Control Controller engine.

2. The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in the Web Service Credentials field on the [Credentials Tab](#) in the Appliance Settings window.
3. Use the installer program to deploy the agent to the end-systems in your network. The following operating systems are supported:
 - Windows 7
 - Windows Vista
 - Windows XP
 - Windows 2008
 - Windows 2003
 - Windows 2000

Agent Icons and Notification Messages

When the agent has been installed on an end-user's system, an agent icon appears in the end-system's Taskbar Notification area (on the lower right corner of the screen). The icon denotes the following states:

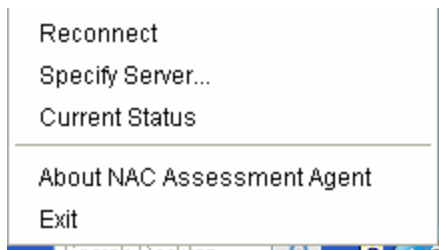
-  Connected - Indicates that the agent is connected, and the end user has passed assessment and been granted network access.
-  Disconnected - Indicates that the agent is disconnected.
-  Assessing - Indicates to the end user that they are being assessed.
-  Locked - Indicates that the machine is locked and the end user must log in through the agent.
-  Quarantined - Indicates to the end user that they are quarantined.
-  Warning - Indicates to the end user that they have assessment warnings. This icon displays until the user has a clean scan or is quarantined.

Once an assessment has taken place, the end user automatically receives a notification message if the Display Agent Notification Message option is enabled in the [Agent-Based Test Set](#). If this option is not selected, the end user must click on the agent icon to see the notification message.

The notification message tells them if they are quarantined, in an error state, have assessment warnings, or are accepted. From this message, the end user can click a link to start the remediation process.



If the end-user right-clicks on the agent icon, the agent system tray menu appears:



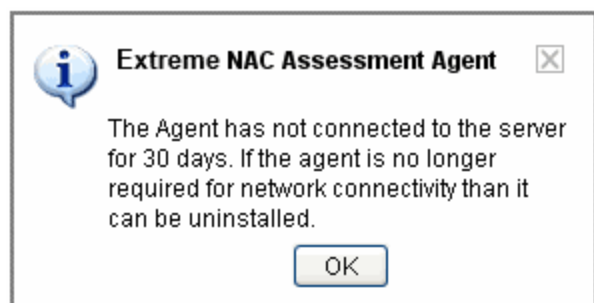
The menu displays the following options. You can hide the first three options using the Show Agent Menus option in the [Advanced Agent Configurations window](#).

- Reconnect - Causes the agent to disconnect from its current assessment server and attempt to reconnect to the default assessment server.
- Specify Server - Opens a window where the end user can change the default assessment server to which the agent attempts to connect.
- Current Status - Displays a popup showing the end-system's current assessment status.
- About NAC Assessment Agent - Displays a NAC splash screen with the agent version number.
- Exit - Exits the NAC Assessment Agent application.

Agent Information Messages

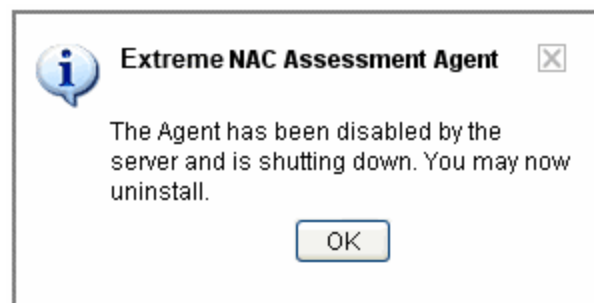
Client Timeout Message

The following message is displayed to end users if the agent has not connected to an assessment server in 30 days. (You can configure the number of days in the [Advanced Agent Configuration window](#).) When the end user clicks OK, the agent application exits. The end user needs to manually uninstall the agent application, if desired. If the end user restarts the agent application, NAC Manager gives them five minutes to connect to an assessment server or the message displays again.



Disabled Client Message

The following message displays to end users when the agent is disabled and the agent application is shutting down. When the end user clicks **OK**, the agent application exits. The end user needs to manually uninstall the agent application. If the end user restarts the agent application, the message displays again.



Upgrade Agent Message

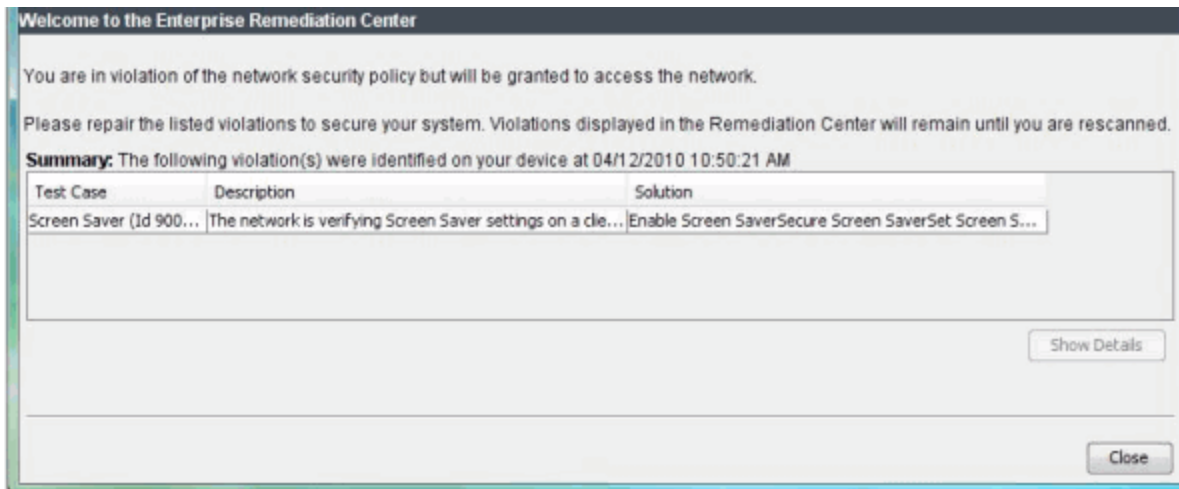
The following message displays to end users when they are granted access to the network (Accept state) and they are not running the current agent version.

The Notify End-Systems When Upgrade is Available option must be enabled in the [Advanced Agent Configuration window](#). When the user clicks on the link, it redirects them to an agent download web page on the web portal that provides links to their agent upgrade options.



Agent Remediation Message

If the Allow Agent Remediation option is enabled in the [Advanced Agent Configuration window](#), when the end user receives a Quarantine or Warning notification message and clicks the "Start Remediation" link, the remediation information is displayed in an agent window instead of the captive portal web browser. This allows remediation to take place with less hits to the captive portal remediation web server. However, if the end user opens a browser window, they are still directed to the captive portal remediation web page. A sample agent remediation window for a Warning is shown below:

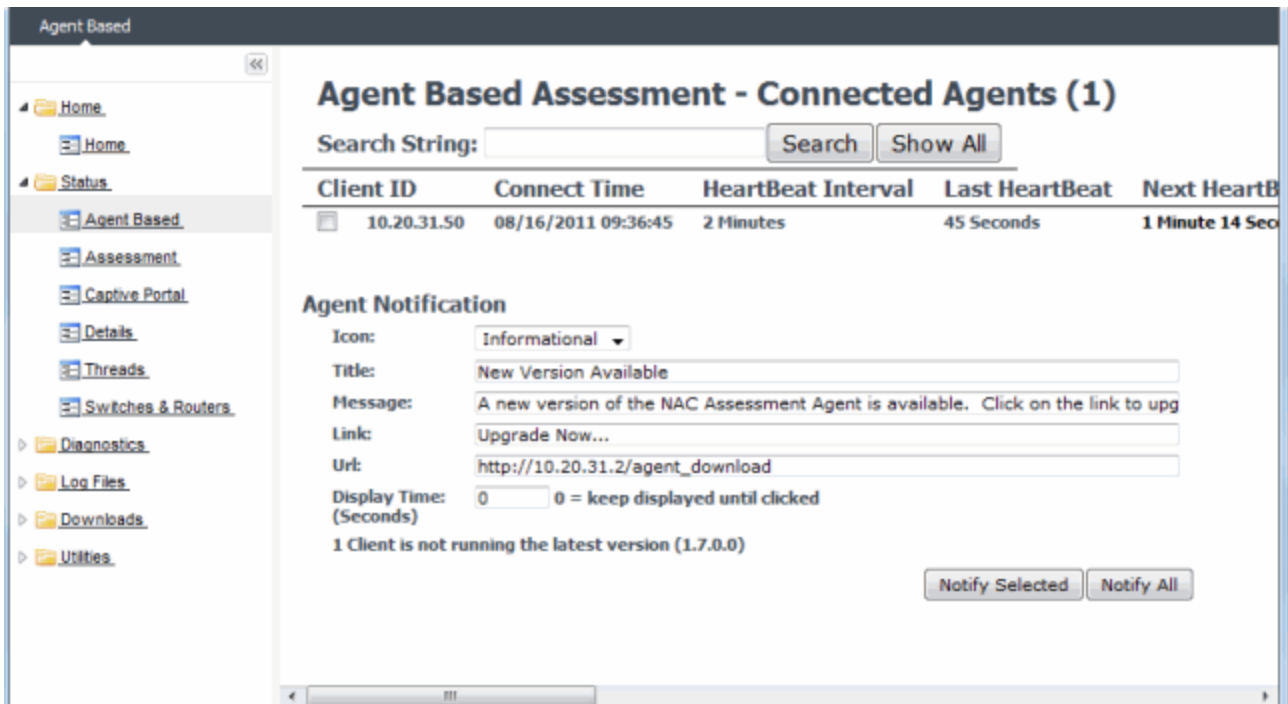


Agent Diagnostics

The NAC Appliance Administration web page lets you access status and diagnostic information for the selected Access Control engine, including agent connection status. Launch the web page by right-clicking on the Access Control engine in the left-panel tree and selecting WebView. The default user name and password for access to this web page is "admin/Extreme@pp." (The username and password can be changed in the Web Service Credentials field on the Credentials Tab in the [Edit Appliance Settings window](#).)

Expand the Status folder in the left-panel tree and select the Agent-Based report to view information and status on connected agents, as shown below. Click the Show All button to display all connected agents. Scroll to the right of the page to view buttons that allow you to perform client diagnostics (described [below](#)).

Use the Agent Notification section to notify end users if their agent version is not the latest version. You can use the default agent upgrade message or write a custom message to notify clients that their agent version is not the latest. When the message is complete, use the Notify Selected or Notify All button to send the [Upgrade Agent message](#) to selected clients or all clients. When the user clicks on the message, it redirects them to an agent download web page on the portal that provides links to their agent upgrade options.



The screenshot shows the 'Agent Based Assessment - Connected Agents (1)' page. The left sidebar contains a navigation tree with folders like Home, Status, Diagnostics, Log Files, Downloads, and Utilities. The main content area has a search string field and 'Search' and 'Show All' buttons. Below is a table of connected agents:

Client ID	Connect Time	HeartBeat Interval	Last HeartBeat	Next HeartBeat
10.20.31.50	08/16/2011 09:36:45	2 Minutes	45 Seconds	1 Minute 14 Sec

Below the table is the 'Agent Notification' section with the following fields:

- Icon: Informational
- Title: New Version Available
- Message: A new version of the NAC Assessment Agent is available. Click on the link to upg
- Link: Upgrade Now...
- Url: http://10.20.31.2/agent_download
- Display Time: 0 (Seconds) 0 = keep displayed until clicked

A status message at the bottom of the notification section reads: '1 Client is not running the latest version (1.7.0.0)'. At the bottom right, there are 'Notify Selected' and 'Notify All' buttons.

Client Diagnostics Buttons

Scroll to the right of the Agent-based report to view buttons that allow you to perform client diagnostics for each connected agent:

- **Diags On 30 Min** - Turns on agent-side diagnostics (debug) for 30 minutes. You can then use the Retrieve Log button to get the log file that was generated by the agent. This allows you to gather the debug information without having to go to the user's end-system.
- **Retrieve Log** - Retrieves the agent log file, and provides a link to the file for easy viewing.
- **Reconnect** - Causes the agent to disconnect from its current assessment server and attempt to reconnect to the default assessment server.
- **Disable Client** - Lets you disable the agent. The end user receives a [Disabled Client message](#) saying that the agent has been disabled and the agent application is shutting down. This is useful in situations where an end-system is no longer participating in the Access Control process, but the agent is still sending a heartbeat to the server.

Related Information

- [How to Set Up Assessment](#)
- [How to Set Up Assessment Remediation](#)

How to Create a Custom Scan for Agent-less Assessment

This Help topic describes how to create and use a custom Saint scan for networks that use on-board agent-less assessment. The custom scan feature is useful if you are already using Saint assessment and want to integrate existing custom scans into NAC Manager. It also allows you to create a custom scan with assessment criteria that requires only a limited number of port scans and tests.

To create a custom scan, you must connect to the Saint web site and use the Saint web interface to configure the scan. After you have created the scan, you will be able to add it to your agent-less test set configuration and use it for your end-system assessment.

Use the following steps to create a custom scan.

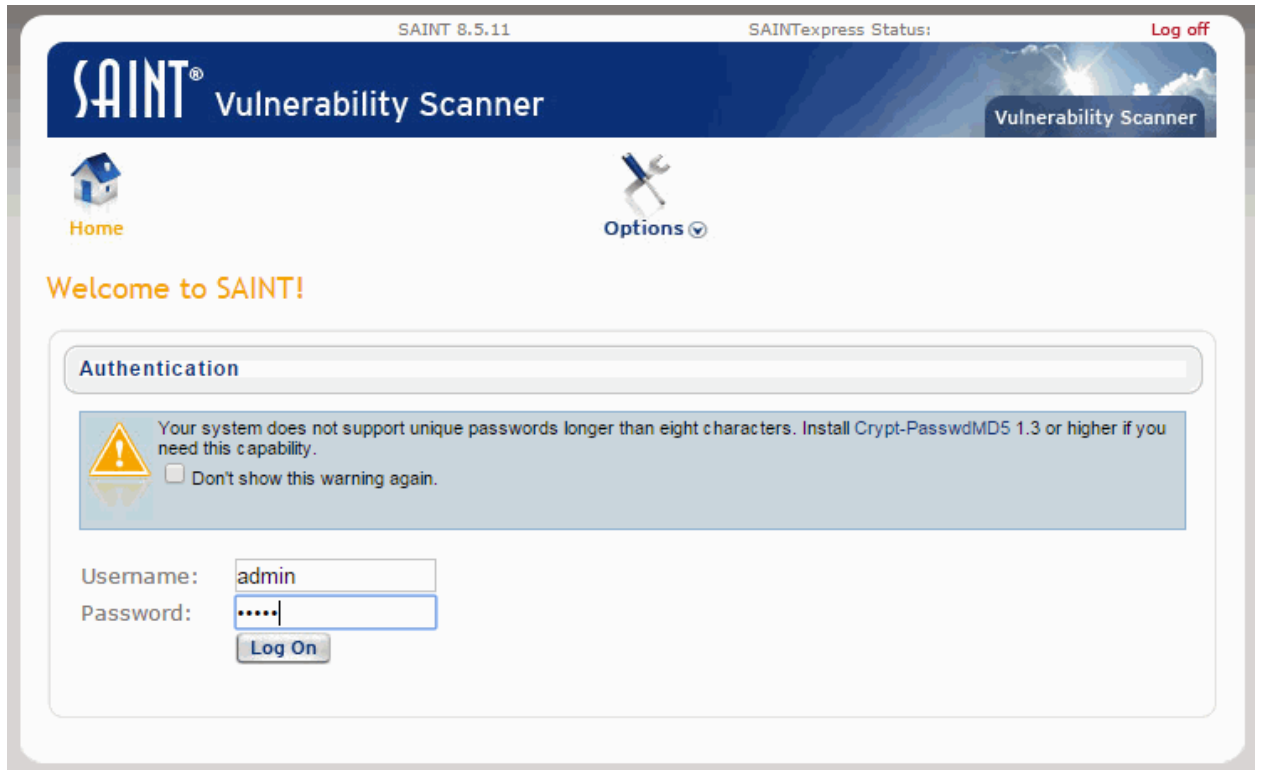
1. Connect a monitor and keyboard to your NAC appliance, or connect via SSH.
2. From the CLI, "cd" to the directory `/opt/nac/saint/saint`.
NOTE: On some NAC appliances the second `saint` directory will include a version number, for example `/opt/nac/saint/saint-8.5.11`.
3. Start the Saint web service by entering the following command line argument:

```
./custom_policy_editor.pl -r -h <ip>
```

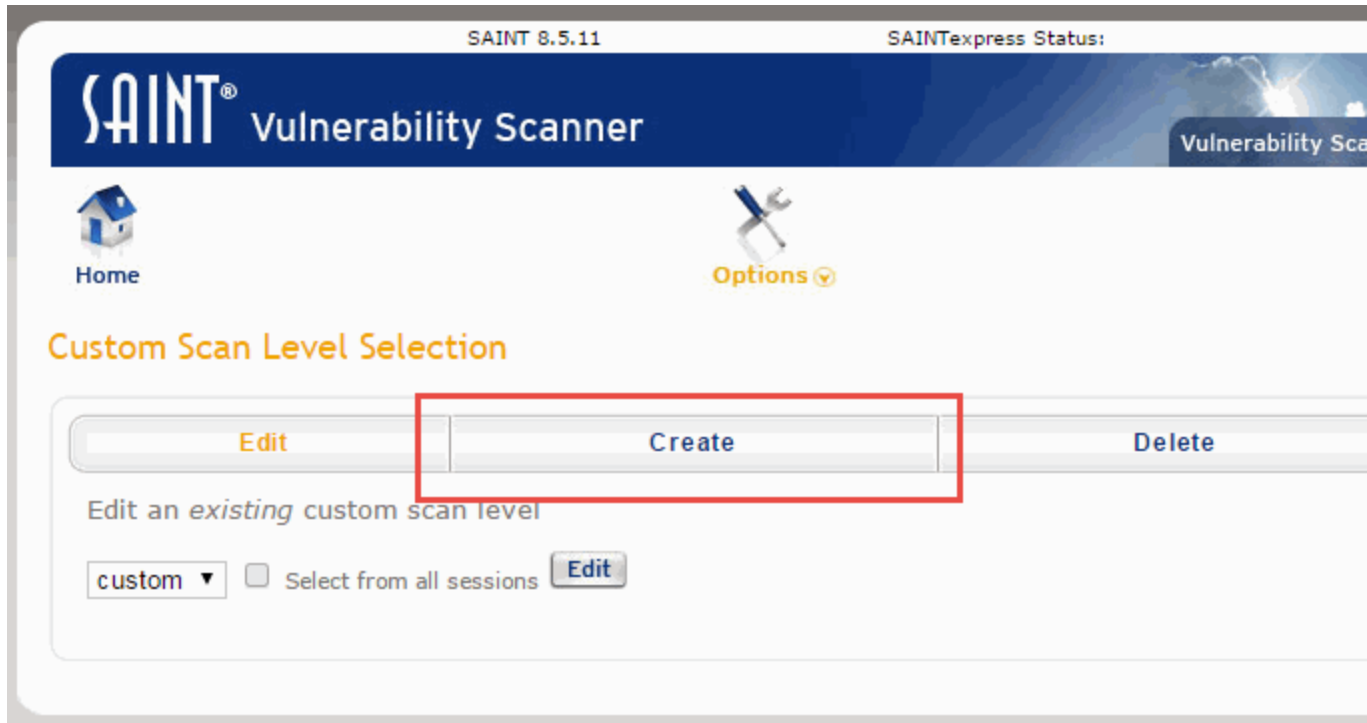
where `<ip>` is the IP address of the system that is going to connect to the Saint web service and configure the custom scan (for example, your laptop system).
NOTE: You cannot run `custom_policy_editor.pl` from any directory. You must "cd" to the directory `/opt/nac/saint/saint`.
4. During the web service startup, you are asked to create login user names and passwords for two accounts: `saint` and `admin`. The accounts are disabled by default, but they become enabled when you provide a password for them. After you complete the startup by providing the user names and passwords, you are ready to connect to the web service and configure your custom scan.
5. From the connecting system, connect to the Saint web service by entering the following URL in a web browser window:

```
http://<ip of NAC appliance>:1414
```

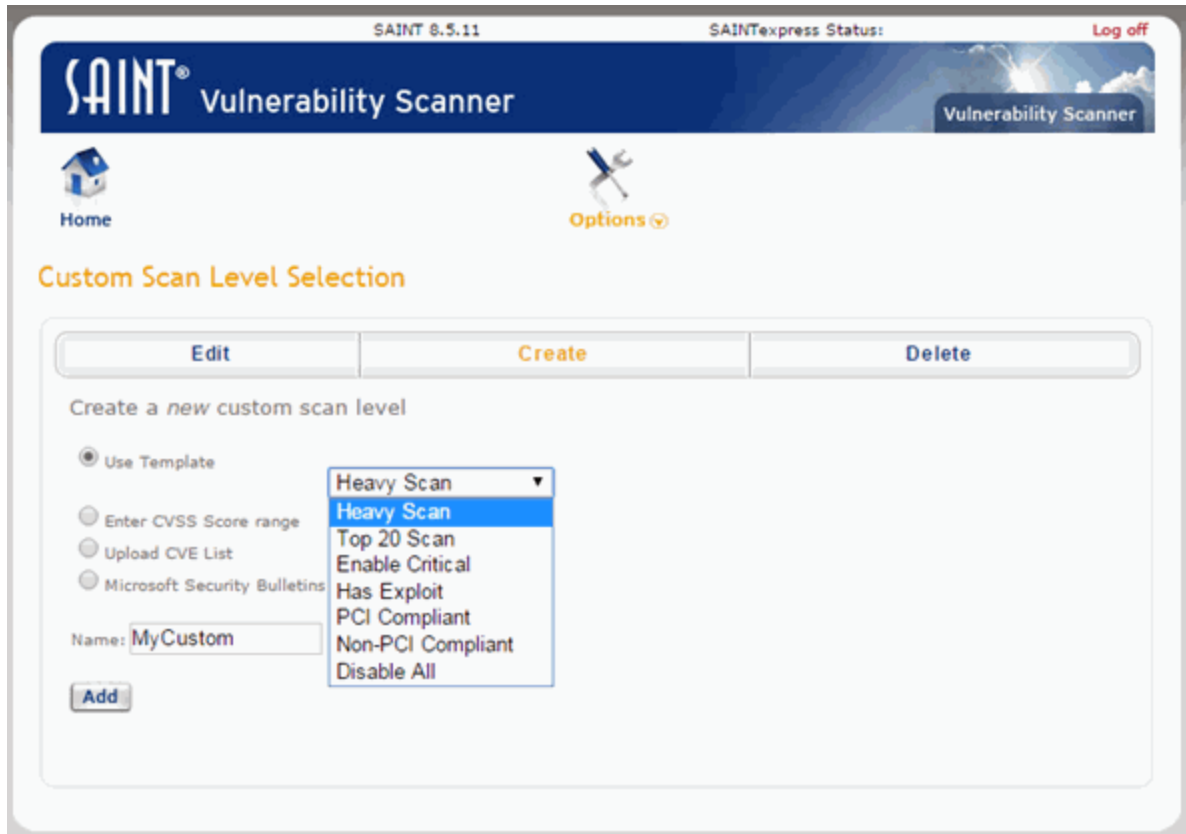

6. Login using the admin user name and password that you created during the web service startup. (The Welcome screen automatically displays the Saint username and password, so be sure to change it to the admin username and password.)



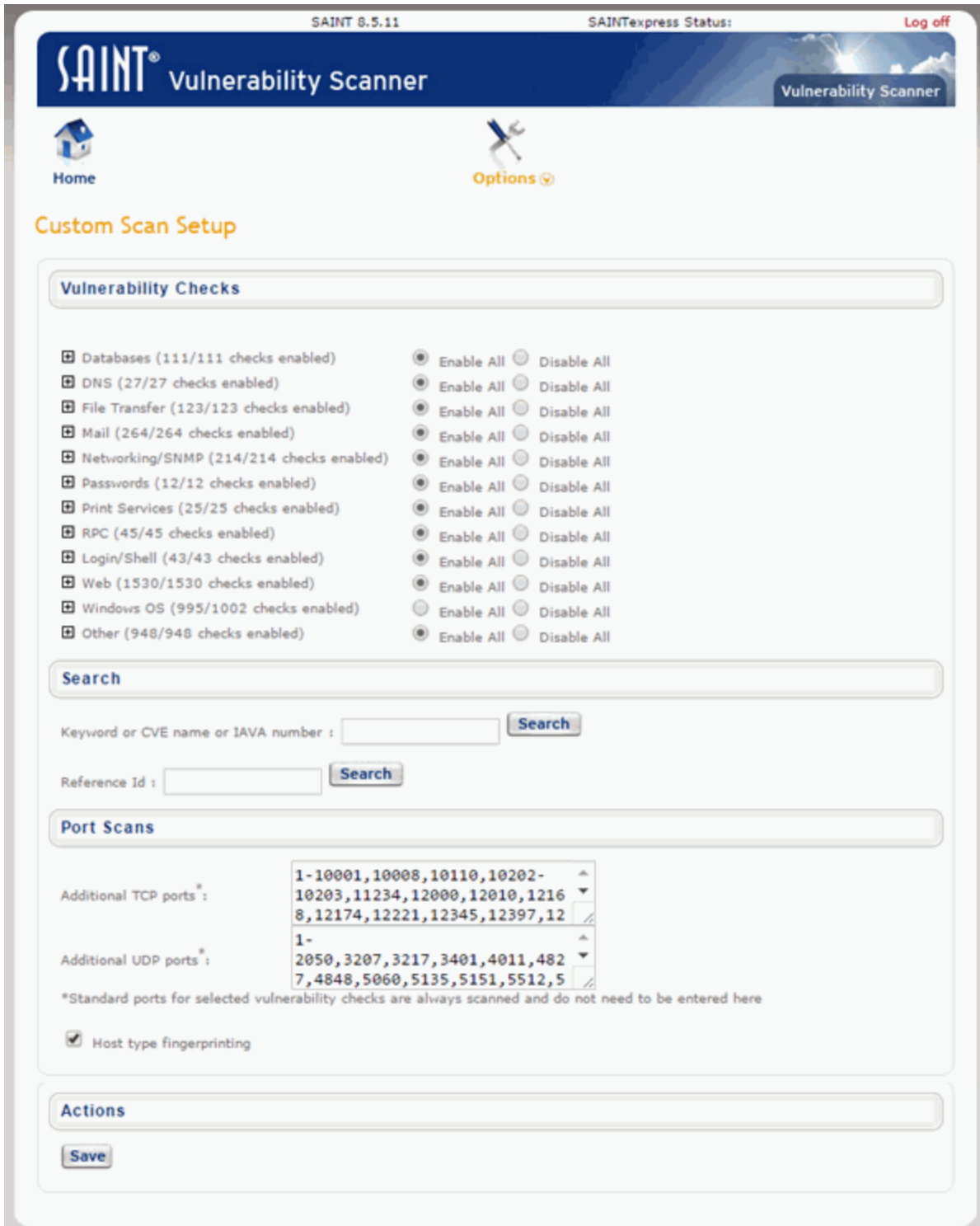
7. Click the Create option in the Custom Scan Level Selection screen once you have logged in.



8. Create a new scan by entering a name, choosing a template, and clicking the **Add** button.




9. Configure your custom scan by selecting the Vulnerability Checks, Port Scans, and other desired options in the Custom Scan Setup screen. Use the **Save** button at the bottom of the web page to save your scan (you may have to scroll down to see this button).



10. The custom scan has been created and you can close your web browser window.

11. Enter the name of the scan in your agent-less test set in NAC Manager.
 - a. From the NAC appliance command line, cd to the `/opt/nac/saint/saint/config/policy` directory to determine the name of the scan.

NOTE: On some NAC appliances the second `saint` directory will include a version number, for example `/opt/nac/saint/saint-8.5.11/config/policy`.
 - b. In the policy directory, there will be two files that contain the name of the scan as you entered it in the Saint web interface. For example, if you named the scan "MyCustom," you'll see the following two files in the directory: `saint_data_MyCustom.probe` and `saint_data_MyCustom.conf`. In this example, the scan name that you will enter into NAC Manager is `saint_data_MyCustom`. You can rename the scan if desired, as long as you rename both the `.probe` and `.conf` files. If you rename the scan, you will enter the new name into NAC Manager.
 - c. In NAC Manager, open the [Manage Assessment Settings window](#) (Tools > Manage Assessment Settings).
 - d. In the Assessment Configurations tab, select any configuration and click **Edit**. The [Edit Assessment Configuration window](#) opens.
 - e. In the Test Sets section of the window, you will see a list of all the test sets available for your assessment configurations. Select the agent-less test set that will be configured to use the custom scan, click the configuration menu button  and select **Edit**. (Select **Add Agent-less** if you need to create a new test set.)
 - f. In the Scanning Level section of the [Edit Agent-less Test Set window](#), select **Custom** from the drop-down list and enter the scan name as determined in step b. Click **OK**.
 - g. The agent-less test set with the custom scan can now be used in your assessment configurations.

Refer to [How to Set Up Assessment](#) for information on creating Assessment Configurations.

Related Information

- [How to Set Up Assessment](#)
- [Edit Assessment Configuration Window](#)
- [Manage Assessment Servers Window](#)

How to Change the Assessment Agent Adapter Password

This Help topic provides instructions for changing the password on the assessment agent adapter on your network assessment servers, including agent-less, Nessus, or a third-party assessment agent (an assessment agent that is not supplied or supported by NAC Manager). The assessment agent adapter enables communication between the NAC appliance and the assessment servers, and the password is used by the assessment agent adapter to authenticate NAC appliance assessment requests.

This password must match the password specified in the NAC Manager options as the [Assessment Agent Adapter Credentials](#) (Tools > Options > NAC Manager > Assessment Server > Assessment Agent Adapter Credentials). If you change the password on the assessment agent adapter, you will need to change assessment agent adapter credentials in the NAC Manager options as well, or connection between the appliance and assessment servers will be lost and assessments will not be performed.

To change the assessment agent adapter password:

1. Go to the install directory for the assessment agent adapter on the assessment server. This can be a Nessus server or the NAC appliance if you are using on-board agent-less assessment. On a NAC appliance, the install directory is `/opt/nac/saint`.
2. Run the `sha1.sh` script (on a NAC appliance, the script is located in `/opt/nac/saint/util`) using the new password as the argument. The script will produce a hash string that looks something like:
9ba2db465ff11b0bdfd188f7ee87b10fc3a145dc
3. Open the `users.properties` file (on a NAC appliance, the file is located in `/opt/nac/saint/users.properties`) and replace the existing hash string with the new one:
admin=<new string>
4. Restart the assessment agent adapter. On a NAC appliance, the command is `aglsctl restart`.

Related Information

For information on related tasks:

- [How to Install the Assessment Agent Adapter on a Nessus Server](#)
- [How to Set NAC Manager Options - Assessment Server](#)

For information on related windows:

- [Manage Assessment Servers Window](#)
- [NAC Manager Options - Assessment Server](#)

How to Install the Assessment Agent Adapter on a Nessus Server

This document provides instructions to install the Extreme Networks Assessment Agent Adapter software on a Nessus Server. The Assessment Agent Adapter is required for communication between the Extreme Access Control appliance and the Nessus server.

NOTE: As of NetSight Version 7.0, only Nessus Version 6 is officially supported.

1. Go to the Network Management Suite (NMS) Download web page to download the Assessment Agent Adapter:
<https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx>.
Select the version of Extreme Management Center you are using.
2. Scroll down to find the Extreme Access Control Tools section of the web page. The install file is named "Assessment Adapter (for 3rd party assessment integration)". Download the file and copy it to the Nessus server.
3. Open a shell and "cd" to the directory where you downloaded the install file.
4. Change the permissions on the install file by entering the following command at the shell prompt:

```
chmod 755 EXTRAssessmentServerAgentAdapter_  
x.x.x.x.bin
```
5. Run the install program by entering the following command at the shell prompt:

```
./EXTRAssessmentServerAgentAdapter_x.x.x.x.bin
```
6. The Introduction screen appears. Press **Enter**.
7. Enter Nessus as the agent type to install. Press **Enter**.
8. The Choose Install Folder screen appears where you can choose the installation folder or directory. Enter an absolute path or press **Enter** to accept the default installation folder /root/AssessmentAgent. The installer requires 100 MB of memory. If the installation folder does not have enough memory, you will see an error.

9. The Pre-Installation Summary screen appears. This screen shows you the locations you have chosen for the installation process and disk space requirements. Review this information to ensure its accuracy. Press **Enter**.
10. The Nessus Server Information screen appears. You must enter information in several fields in this screen.
11. Enter the port that the Nessus daemon is running on. The default value is 1241. Press **Enter**.
12. Enter the username that you created when you installed the Nessus server. Press **Enter**.
If you did not create a user when you installed the Nessus server, from a shell prompt, type:

```
cd /nessus installation directory/sbin
```

followed by

```
nessuscli adduser username
```

and follow the prompts to add a user to the application. Press **Enter**.
13. Enter the password for the Nessus user. Press **Enter**.
14. The SSL Server Information screen appears. Enter the port on which the HTTPS daemon is running. The default port number is 8445. Press **Enter**.
The Assessment Agent Adapter begins installing.
15. If you are upgrading to a newer version of the Assessment Agent Adapter, you are asked if you want to overwrite several files: launchAS.sh, bin/nessus_cmd, and version.txt. Enter the letter "y" to answer yes and press **Enter**.
16. The Installation Complete screen appears. The installation is complete and the Assessment Agent Adapter has been installed on the server.
17. Start the Assessment Agent Adapter as a background process by entering the following command at the shell prompt:

```
/assessment agent adapter installation  
directory/launchAS.sh &
```
18. Make sure that the Nessus daemon and the Assessment Agent Adapter are started each time the system is started, by adding this command into your rc.local script:

```
/assessment agent adapter installation  
directory/launchAS.sh &
```
19. To verify the Assessment Agent Adapter is running on the system, from the shell prompt enter:

```
netstat -an | grep port number
```

where port number is the port you entered that has the HTTPS daemon

running on it. The default value for this is 8445. You should see returned entries with ESTABLISHED or LISTEN in them.

20. To verify the Nessus application is running on the system, from the shell prompt enter:

```
ps -eaf | grep nessusd
```

You should see a return entry similar to: "nessusd: waiting for incoming connections." This is an indication that the Nessus process is running correctly on the system.

Related Information

For information on related tasks:

- [How to Change the Assessment Agent Adapter Password](#)
- [How to Set NAC Manager Options - Assessment Server](#)

For information on related windows:

- [Manage Assessment Settings Window](#)
- [Edit Assessment Configuration Window](#)

How to Set Up Assessment Remediation

Remediation utilizes Remediation Web Server functionality installed on a Extreme Access Control (Access Control) engine to notify end users when their systems are being assessed or have been quarantined due to network access policy non-compliance (identified during end-system security assessment). In addition, the web server notifies end users of the specific vulnerabilities identified during the end-system's assessment and the corresponding required remediation steps. Once the remediation steps have been successfully performed, reassessment of the end-system is performed and the appropriate network resources are allocated to the end-system. For more information on remediation and an overview of how it works, see the [Assisted Remediation](#) section of the Concepts help file.

This Help topic describes the specific steps that must be performed when setting up remediation in your network. The steps vary depending on whether you are using Access Control Gateway engines and/or Access Control Controller engines on your network.

For Access Control Gateway engines you must:

- Identify the location in your network topology for the Access Control Gateway installation.
- Redefine the Assessing and Quarantine policy roles created in Management Center Policy Manager for EOS policy-enabled switches.
- Configure policy-based routing on your network.
- Configure remediation values in NAC Manager.

For Access Control Controller engines you must:

- Configure remediation values in NAC Manager.

The Remediation Web Server is pre-installed on the Access Control engine. For instructions on installing and configuring the Access Control engine, please refer to your engine Installation Guide.

NOTE: It is important to add a DNS entry from the Fully Qualified Domain Name (FQDN) of the Access Control Gateway into the DNS servers deployed on the network so that the device running NAC Manager is able to resolve queries to these DNS servers. Otherwise, a short delay occurs in returning the Assessment/Remediation portal web page to end users on the network.

Instructions on:

- [Extreme Access Control Gateway Configuration](#)
 - [Identifying Access Control Gateway Location](#)
 - [Defining Assessment and Quarantine Policies](#)
 - [Configuring Policy-Based Routing](#)
- [Configuring NAC Manager \(for Access Control Gateway and Access Control Controllers\)](#)

Extreme Access Control Gateway Configuration

Perform the following steps when you are deploying remediation in a network that utilizes Extreme Access Control (Access Control) Gateway engines. These steps are not necessary if you are utilizing only Access Control Controller engines on your network.

Identifying Extreme Access Control Gateway Location

Although several Access Control Gateways may be deployed on the entire network depending on the number of connecting end-systems, only one Access Control Gateway is required to serve as the Registration Web Server. The location of the Access Control Gateway that is configured with Remediation Web Server functionality is important for the implementation of web redirection for end user notification of quarantined end-systems. The Access Control Gateway must be installed on a network segment directly connected to the router or routers that exist in the forwarding path of HTTP traffic from end-systems that may be quarantined. This is because policy-based routing will be configured on this router or routers to redirect the web traffic sourced from quarantined end-systems to the Access Control Gateway. It is important to note that only the Access Control Gateway that you wish to serve as the Registration Web Server needs to be positioned in such a manner. All other Access Control Gateways may be positioned at any location on the network, with the only requirement being that access layer switches are able to communicate to the gateways.

Typically, the Access Control Gateway with Remediation Web Server functionality is positioned on a network segment directly connected to the distribution layer routers on the enterprise network, so that any HTTP traffic sourced from quarantined end-systems that are connected to the network's access layer can be redirected to that Access Control Gateway. As an alternative, the Access Control Gateway may be positioned on a network segment directly

connected to the router providing connectivity to the Internet or internal web server farm. In this scenario, the HTTP traffic sourced from quarantined end-systems would be redirected to the Access Control Gateway before reaching the Internet or internal web servers.

Third-Party URL Redirection Considerations

If your environment incorporates third-party redirection (i.e., a Cisco Controller), configure the device to use the following the URL (or redirection ACL) to redirect HTTP traffic to the appropriate Captive Portal pages:

```
http://<GatewayIP>/static/index.jsp
```

Defining Assessment and Quarantine Policies

When you implement remediation, you must make sure the Assessment and Quarantine [access policies](#) defined in NAC Manager allow traffic to and from end-systems and the Remediation Web Server. For a network composed of EOS policy-enabled switches in the access layer, you must create the appropriate network access services and rules for the associated Assessing and Quarantine *policy roles* created in Policy Manager, and enforce those changes to the policy-enabled switches. For a network composed of RFC 3580-enabled switches, you must ensure appropriate network services are allowed for the VLANs associated to the Assessment and Quarantine access policies.

For EOS policy-enabled switches, there are two main changes that must be made to your Assessing and Quarantine policy roles when you deploy remediation:

- A rule must be added that allows HTTP traffic to pass between end-systems and the Remediation Web Server.
- The rule must specify a class of service action that rewrites the ToS value of the HTTP traffic to a value of 'y'. This value should match the decimal equivalent used in your policy-based routing that is used on the router.

For RFC 3580-compliant access layer switches, a VLAN must be identified to which end-systems will be assigned while being assessed and quarantined on the network. This may or may not be the same VLAN, and may or may not be identical to the VLAN used for unregistered end-systems. This VLAN must provision services on the network to an unregistered end-system that allows the device to open a web browser; specifically DHCP, ARP, and DNS, and allow IP connectivity to the Access Control Gateway implementing the Remediation Web Server.

NOTE: If quarantined end-users will be required to download remediation files via FTP, you will also need to add a rule that opens up ports 49152-65535. If you are concerned with security, you can configure your FTP server to use a smaller range of ports.

Furthermore, policy-based routing (PBR) must be configured on the router or routers that exist in the forwarding path of HTTP traffic sourced from quarantined end-systems where the Access Control Gateway is connected. This allows the routers to redirect the web traffic sourced from quarantined end-systems to the Access Control Gateway with Remediation Web Server functionality. For more information on this, see [Configuring Policy-Based Routing](#).

Once your Assessment and Quarantine access policies are defined to allow traffic between end-systems and the Remediation Web Server and your policy-based routing is implemented, the following communication can take place:

- When the end-system opens a web browser, the HTTP traffic is redirected to the Access Control Gateway implementing the Remediation Web Server functionality.
- The Access Control Gateway returns a web page indicating that the end-system is currently being scanned.
- If the end-system fails the scan, it is quarantined and the Access Control Gateway returns a web page indicating the reasons the end system was quarantined and the corresponding self-service remediation techniques.
- After taking the appropriate remediation steps, the end-user clicks a button on the web page and attempts to reconnect to the network.
- After a specified number of attempts to remediate have expired, the end user sees a web page requiring them to contact the helpdesk for further assistance.

For EOS policy-enabled Access Layer Switches

If EOS policy-enabled switches are deployed on the network, perform the following steps in Policy Manager to configure your Assessing and Quarantine policy roles to allow remediation.

NOTE: The Policy Manager Default Policy Domain includes a NAC Web Redirect Class of Service that can be used. Make sure that the ToS rewrite value is set to the appropriate value for your network.

1. Use the Device Configuration Wizard to enable the Role-based Class of Service mode on your network devices.
2. Create a new Class of Service that implements the ToS rewrite functionality:
 - a. Open the Class of Service Configuration window (Edit > Class of Service Configuration).
 - b. Click the Create button and open the Create Class of Service window.
 - c. Enter a name for the class of service (e.g. "Web Redirection").
 - d. Select the 802.1p Priority checkbox and use the drop-down list to select the 802.1p priority to associate with the class of service.
 - e. Select the Enable ToS/DSCP Marking checkbox and set the ToS Rewrite value to 'y' (hex).
 - f. Click **OK** to create the new Class of Service.
3. Use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in both your Quarantine and Assessing policy roles:
 - a. Select the service in the left-panel Services tab.
 - b. From the menu bar, select **Tools > Classification Rule Wizard**.
 - c. Enter a name for the rule (e.g. " Allow HTTP").
 - d. Set the rule status to Enabled.
 - e. Set the rule type to All Devices.
 - f. Set the traffic classification layer to Layer 4.
 - g. Set the traffic classification type to IP TCP Port Destination.
 - h. Set the well-known values to HTTP (80).
 - i. Do not enter an IP address value.
 - j. Review the traffic description summary.
 - k. For the Actions, select the CoS checkbox and the class of service you created in step 2 ("Web Redirection").
 - l. Select Permit Traffic for the Access Control.
 - m. Click **Finish** to complete the rule.
4. Enforce these changes to your network devices.

For RFC 3580-compliant Access Layer Switches

For RFC 3580-compliant access layer switches, the VLANs to which end-systems being assessed and quarantined are assigned must be appropriately configured on all access layer switches where end-systems may be assessed and quarantined on the network. The same VLAN may be used for end-systems being assessed and quarantined. Access control lists may be configured at the default gateway routers' interfaces for these VLANs to restrict particular types of traffic sourced from end-systems within these VLANs to other areas of the network; with respect to the previously described provisioning requirements for this VLAN.

For Both EOS policy-enabled and RFC 3580-compliant Access Layer Switches

Now that you have defined the Assessing and Quarantine policy roles in Policy Manager for EOS policy-capable switches and/or the VLANs assigned to end-systems being assessed and quarantined for RFC-3580-compliant switches, you must associate these policy roles to the Assessment and Quarantine access policies in NAC Manager.

1. In NAC Manager, click on the Manage NAC Profiles button in the toolbar. The Manage NAC Profiles window opens.
2. Select the Quarantine NAC Profile entry and click the **Edit** button. The Edit NAC Profile window opens.
3. Click the **Manage** button in the Policy Mappings section. The Edit Policy Mapping Configuration window opens.
4. Select the **Advanced** Radio button.
5. Select the Quarantine policy and click the **Edit** button. The Edit Policy Mapping window opens.
6. Use the drop-down list to select "Quarantine" as the Policy Role. (The drop-down list displays all the policy roles you have created and saved in your Policy Manager database.)
7. If only EOS policy-enabled switches are deployed in the access layer of the network, associate the Quarantine policy with the Default VLAN [1]. If RFC 3580-compliant access layer switches are deployed, associate the Quarantine policy with the Quarantine VLAN you will be using in your network, adding the VLAN using the **Add VLAN** button, if necessary.
8. Click **OK** to close the window.
9. In the Edit Policy Mapping Configuration window, select the row where the Assessing policy is configured and click **Edit selected mapping**.
10. Use the drop-down list to select "Assessing" as the Policy Role.

11. If only EOS policy-enabled switches are deployed in the access layer of the network, associate the Assessing policy with the Default VLAN [1]. If RFC 3580-compliant access layer switches are deployed in the network, associate the Assessing policy with the Assessing VLAN you will be using in your network, adding the VLAN using **Add VLAN**, if necessary. Click **OK**.
12. Click **OK** to close all the open windows. Close the Manage NAC Profiles window.

Your NAC Manager access policies are now configured to allow communication between the end-system and the Access Control Gateway implementing the Remediation Web Server functionality.

Configuring Policy-Based Routing

As described above, the Access Control Gateway with Remediation Web Server functionality must be located on a network segment directly connected to a router or routers that exist in the transmission path of all traffic from any end-systems that may be scanned or quarantined. This is because policy-based routing (PBR) must be configured on the routers to redirect the web traffic sourced from quarantined end-systems to the Access Control Gateway with Remediation Web Server functionality.

If EOS policy-enabled switches are deployed on the network, this is done by configuring an ACL to forward all HTTP traffic with a ToS field of 'y' to the next-hop address of the Access Control Gateway implementing the Remediation Web Server functionality. If RFC 3580-enabled switches are deployed on the network, this is done by configuring an ACL to forward all HTTP traffic with the source IP address on the subnet/VLAN associated to the Quarantine and/or Assessment access policies to the next-hop address of the Access Control Gateway implementing the Remediation Web Server functionality.

In addition, if you are adding multiple Access Control Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well.

For EOS policy-enabled Access Layer Switches

Let's consider an example where the Assessment and Quarantine access policies are associated to policy roles on EOS policy-enabled switches that use the "Allow HTTP" classification rule assigning HTTP traffic the "Web Redirection" class of service. This class of service rewrites the ToS field in the HTTP traffic to a value of 0x40 (or 64 base 10), equivalent to a DSCP value of 16. (The DSCP is the value defined in the six most significant bits of the 8-bit ToS field.) Furthermore,

the Assessment and Quarantine access policies are associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when remediation is deployed for EOS policy-enabled access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic with a DSCP of 16.
 `access-list 102 permit tcp any any eq 80 dscp 16`
 `access-list 102 permit tcp any any eq 8080 dscp 16`
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the Access Control Gateway implementing the Remediation Web Server functionality, where "xxx.xxx.xxx.xxx" is the IP addresses of the Access Control Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple Access Control Gateways are deployed with Remediation Web Server functionality.
 `route-map 101`
 `match ip address 102`
 `set next-hop xxx.xxx.xxx.xxx`
3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from end-systems being assessed and quarantined by entering the routed interface configuration prompt and executing the following command.
 `ip policy route-map 101`

For RFC 3580-compliant Access Layer Switches

Let's consider an example where the Assessment and Quarantine access policies are associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when remediation is deployed for RFC 3580-compliant access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic sourced from subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24.
 `access-list 102 permit tcp 10.1.10.0.0.0.255 any eq 80`
 `access-list 102 permit tcp 10.1.20.0.0.0.255 any eq 80`
 `access-list 102 permit tcp 10.1.30.0.0.0.255 any eq 80`
 `access-list 102 permit tcp 10.1.10.0.0.0.255 any eq 8080`

```
access-list 102 permit tcp 10.1.20.0.0.0.255 any eq 8080
access-list 102 permit tcp 10.1.30.0.0.0.255 any eq 8080
```

2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the Access Control Gateway implementing the Remediation Web Server functionality, where "xxx.xxx.xxx.xxx" is the IP addresses of the Access Control Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple Access Control Gateways are deployed with Remediation Web Server functionality.

```
route-map 101
match ip address 102
set next-hop xxx.xxx.xxx.xxx
```

3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from end-systems being assessed and quarantined by entering the routed interface configuration prompt and executing the following command.

```
ip policy route-map 101
```

Setting up Redundancy on Access Control Gateways

When adding multiple Access Control Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well. This is performed on the router in which policy-based routing is configured. Use the same commands described in the previous two sections except for the two following changes:

- In step 2, in addition to the single IP address set as the next-hop IP address, enter a list of IP addresses of the redundant Access Control Gateways. For example:
- In step 3, when adding the ip policy route-map to the router interface, specify an additional command called "ip policy pinger on". This command will attempt to ping the first IP address that is specified in the next-hop to determine its availability. If it is not available, the next IP in the list of next-hops will be pinged and then used, if it is available.

For example:

```
ip policy route-map 101
ip policy pinger on
```


With policy-based routing and the Assessment and Quarantine access policies defined, remediation settings can be specified, as described in the next section.

Configuring NAC Manager (for Extreme Access Control Gateways and Extreme Access Control Controllers)

Perform the following steps when you are deploying remediation in a network that utilizes Access Control Gateway engines and/or Access Control Controllers.

Use the portal configuration section of the [NAC Configuration window](#) (in NAC Manager) to configure parameters for the Assessment/Remediation portal web pages served from the Access Control engine. All Access Control engines are initially assigned a default portal configuration. You can use this window to view and edit the default configuration or create new configurations to use. Once you have defined your portal configuration, you must enforce the NAC configuration to your engine(s).

Use the following steps to define your portal configuration and enforce it to the engine. These steps give you an overview of the required configuration. For more detailed information, see the [NAC Configuration Window](#) and [Portal Configuration](#) Help topics.

1. Enable the Assessment/Remediation for End-Systems option in the NAC Manager Features options accessed from Tools > Options in the NAC Manager menu bar.
2. Use the NAC Manager  toolbar button to open the NAC Configuration window.
3. In the left-panel tree, select the Features icon. Enable the registration, access, and assessment/remediation features you want for your network. For information on each available feature, see the [Features](#) section in the NAC Configuration Window Help topic.
4. In the left-panel tree, select the Portal icon. If needed, use the Portal Configuration drop-down menu in the right panel to select the configuration to configure or to create a new one.
5. Expand the Portal icon and select the portal configuration settings you want to edit:
 - a. Click on Network Settings to view network web page parameters. Click on Look and Feel to view the common web page parameters. These parameters are shared by both the Assessment/Remediation and the Registration portal web pages. You can edit and change these parameters; for a description of each parameter, see the

[Network Settings](#) and [Look and Feel](#) sections of the Portal Configuration Help topic. Be aware that if you deploy both the assessment/remediation and registration features, any changes will affect the web pages for both features.

- b. Click on Administration where you can configure settings for the registration administration web page and grant access to the page for administrators and sponsors. For information on this tab, see the [Administration](#) section of the Portal Configuration Help topic.
 - c. Depending on the registration, access, and assessment/remediation features you have selected for your network, there are additional views you can access where you can configure the settings and parameters for each type. For a description of each setting and parameter, see the [Portal Configuration](#) Help topic.
 - d. Click on Assessment/Remediation to view the parameters for the Assessment/Remediation portal web pages. You can edit and change these parameters; for a description of each parameter, see the [Assessment/Remediation](#) section of the Portal Configuration Help topic.
6. When you have finished making your changes to the portal configuration, click **Save** in the NAC Configuration window and then close the window.
 7. Enforce the NAC configuration to the engine group.

Remediation is now enabled on the network. Whenever an end-system is assigned to the Assessment or Quarantine access policy, the web traffic from the end-system will be redirected to a web page stating information about the network resource provisioning restrictions.

Related Information

- [Registration](#)
- [Portal Configuration](#)

How To Use NAC Manager

The **How To** section contains Help topics that give you instructions for performing tasks in NAC Manager.

How to Change Extreme Access Control Engine Settings

You can use NAC Manager to change Extreme Access Control engine settings including DNS, NTP, SSH, and SNMP configuration. You can also use NAC Manager to change the engine hostname and default gateway, as well as configure static routes for advanced routing configuration.

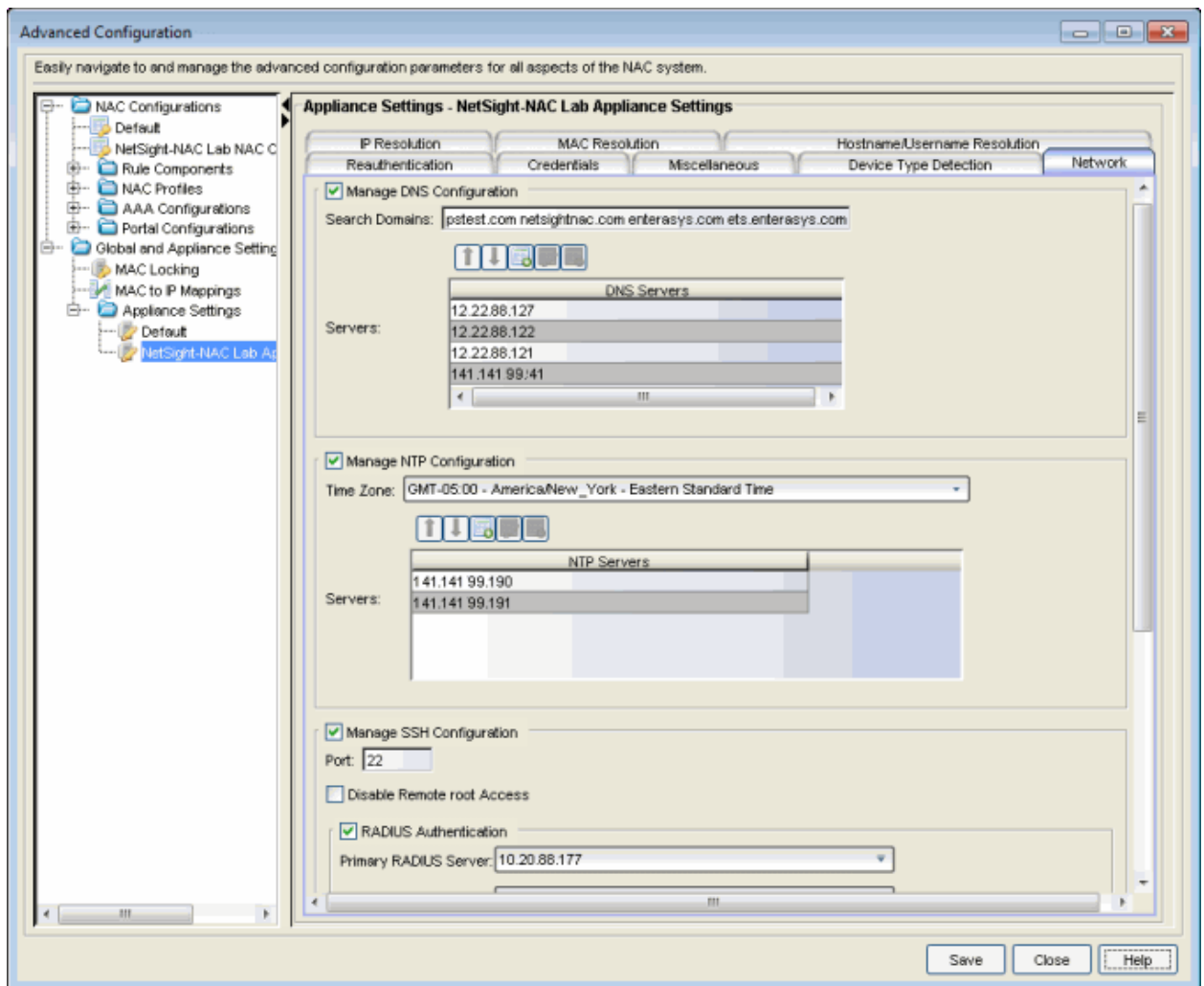
Changing DNS, NTP, SSH, and SNMP Settings

Use the **Network** tab in the NAC Manager Appliance Settings window to change:

- DNS Configuration - search domains and DNS servers
- NTP Configuration - time zone and NTP servers
- SSH Configuration - port number and RADIUS authentication
- SNMP Configuration - SNMP credentials for the engine

Use the following steps to access the Appliance Settings window:

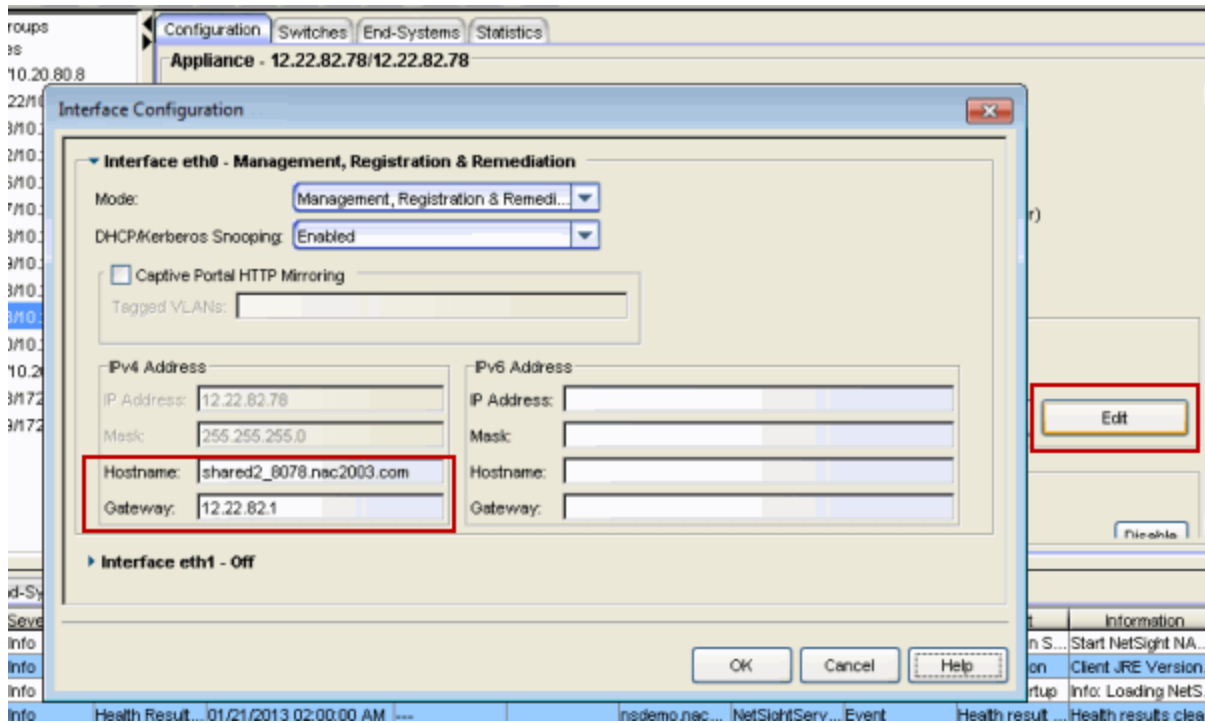
1. From the NAC Manager menu bar select Tools > Manage Advanced Configurations. The Advanced Configuration window opens.
2. In the left-panel tree, expand the Global and Appliance Settings folder and select Appliance Settings.
3. Click on the desired Appliance Settings (typically Default unless you configured a custom Appliance Settings).
4. Select the **Network** tab to change your engine configurations. For more information, see the [New/Edit Appliance Settings Window](#) topic in the NAC Manager online Help.



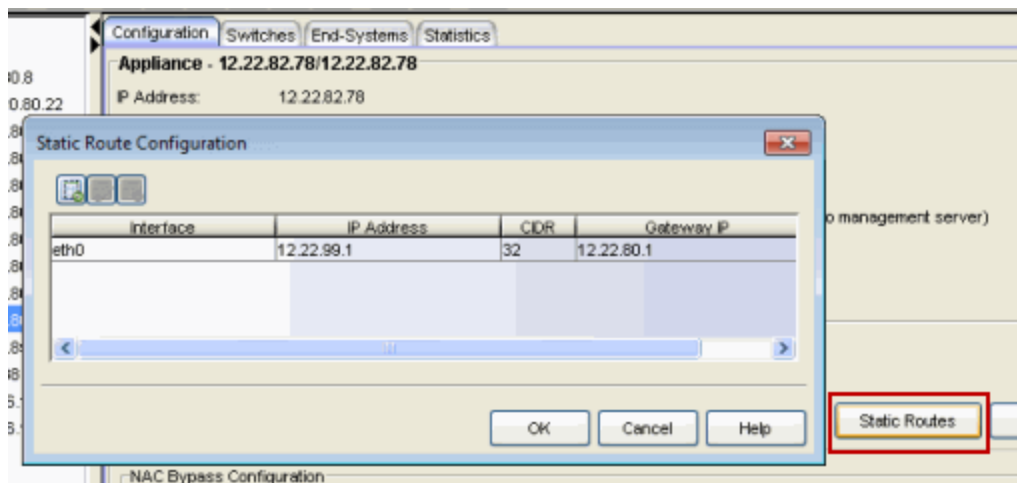
Changing Hostname, Gateway, and Static Routes

In NAC Manager, use the Interface Summary section of the **Configuration** tab for an engine to change the engine hostname, default gateway, and static routes.

1. Select the engine in the NAC Manager left-panel tree. Select the right-panel **Configuration** tab.
2. In the Interface Summary section, click **Edit** to open the Interface Configuration window where you can change the engine hostname and default gateway. For more information, see the [Interface Configuration Window](#) Help topic.



3. Back in the Interface Summary section, click **Static Routes** to open the Static Route Configuration window where you can add or edit the static routes used for advanced routing configuration. For more information, see the [Static Route Configuration Window](#) Help topic.



Related Information

- [New/Edit Appliance Settings Window](#)
- [Interface Configuration Window](#)
- [Static Route Configuration Window](#)

How to Configure Communication Channels

Communication channels allow you to create logical groupings of your Extreme Access Control appliance groups in order to segment data and limit network traffic between geographical or customer sensitive locations.

This is an advanced NAC Manager feature and is only appropriate in certain network scenarios. Here are two scenarios where using communication channels could be beneficial.

- **A large enterprise with remote offices.**
Sending unnecessary traffic over WAN resources can cause strain on the Extreme Management Center server and possibly increase data transmission costs. Communication channels allow you to limit network communications to each geographic location reducing the amount of data that is broadcast over the slower and more expensive WAN lines.
- **A Service Provider with multiple customers, clients, or organizations that do not share Extreme Access Control appliances.**
In this scenario, each service provider customer has their own Extreme Access Control appliance groups, and the data from one customer's appliance groups must not cross to another customer's appliance groups. The appliances may be located on the customer site or in the service provider's cloud. Communication channels can be created for each customer, to restrict data shared between customers and protect sensitive information.

Communication channels are not appropriate in scenarios where a service provider has multiple customer data located on the same appliance. In this type of scenario the Extreme Access Control appliance would need to be hosted in the cloud and physical access to the appliance would never be granted to the customer.

Communication channels are also not appropriate for large university networks where students and faculty move between different portions of the network, and thus move between Extreme Access Control appliances in different appliance groups. Because mobility is a requirement in this scenario, communication channels should not be implemented.

NOTES: In order to enable this feature, both the Extreme Management Center server and all the Extreme Access Control appliances must be running Extreme Management Center version 4.4 or higher. This feature is not supported if there are any appliances on the network running older versions.

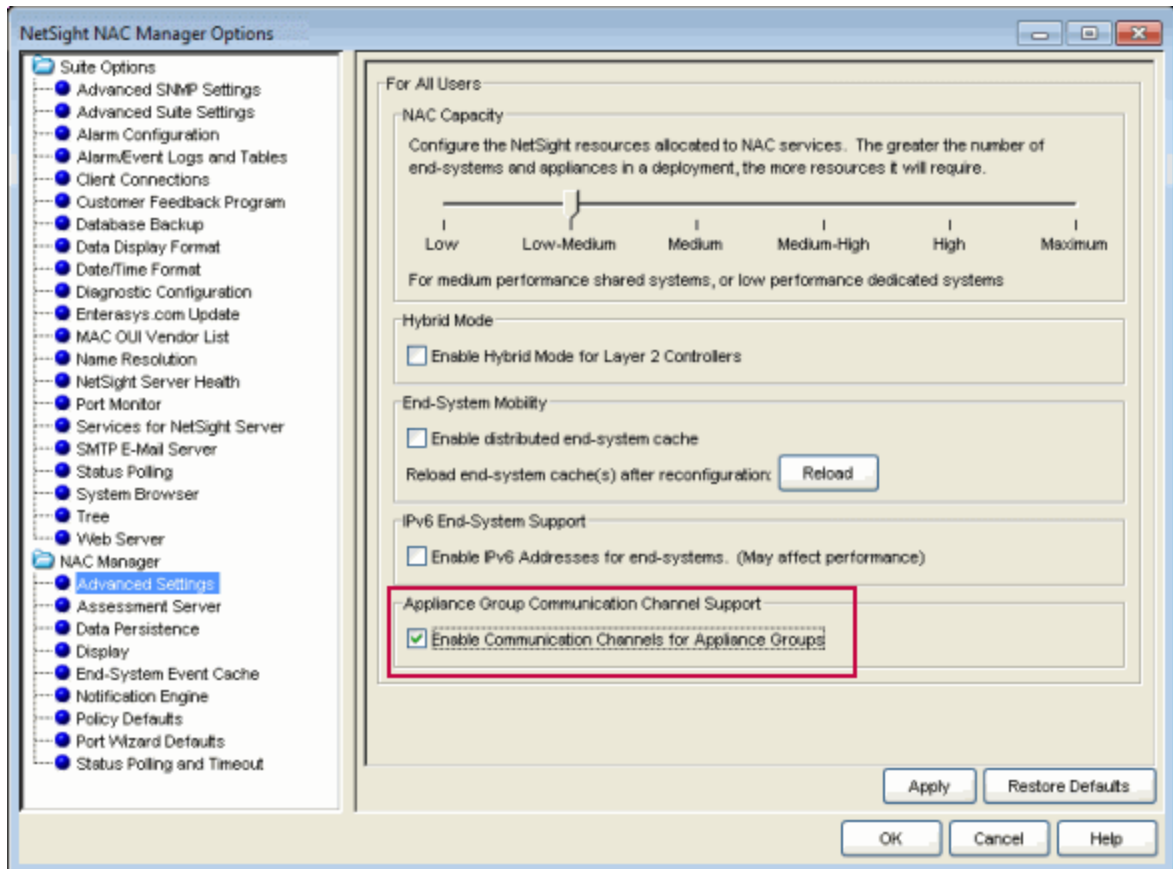
When enabling communication channels on a network that also uses Application Analytics, the communication channels must also be configured in Application Analytics. For more information, please see the [Enabling Extreme Access Control integration](#) section of the Application Analytics Application Data Collection help topic.


Configuring Communication Channels

Use the following steps in NAC Manager to configure communication channels for the appliance groups in your network. An appliance group can only have one communication channel, but multiple appliance groups can use the same communication channel.

1. Open the NAC Manager Options window (Tools > Options).

2. In the NAC Manager Advanced Settings options panel, select the **Enable Communication Channels for Appliance Groups** option.

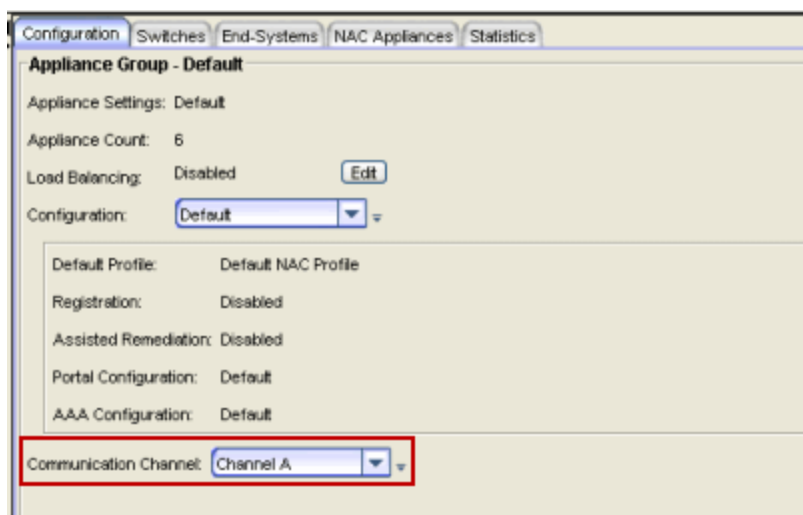


3. In the left panel tree, select an appliance group where you want to configure a communication channel. A communication channel configuration setting is displayed on the appliance group's right-panel Configuration tab. You can add new channels using the configuration menu button  to the right of the field. Any channels you create will be

available for all appliance groups.

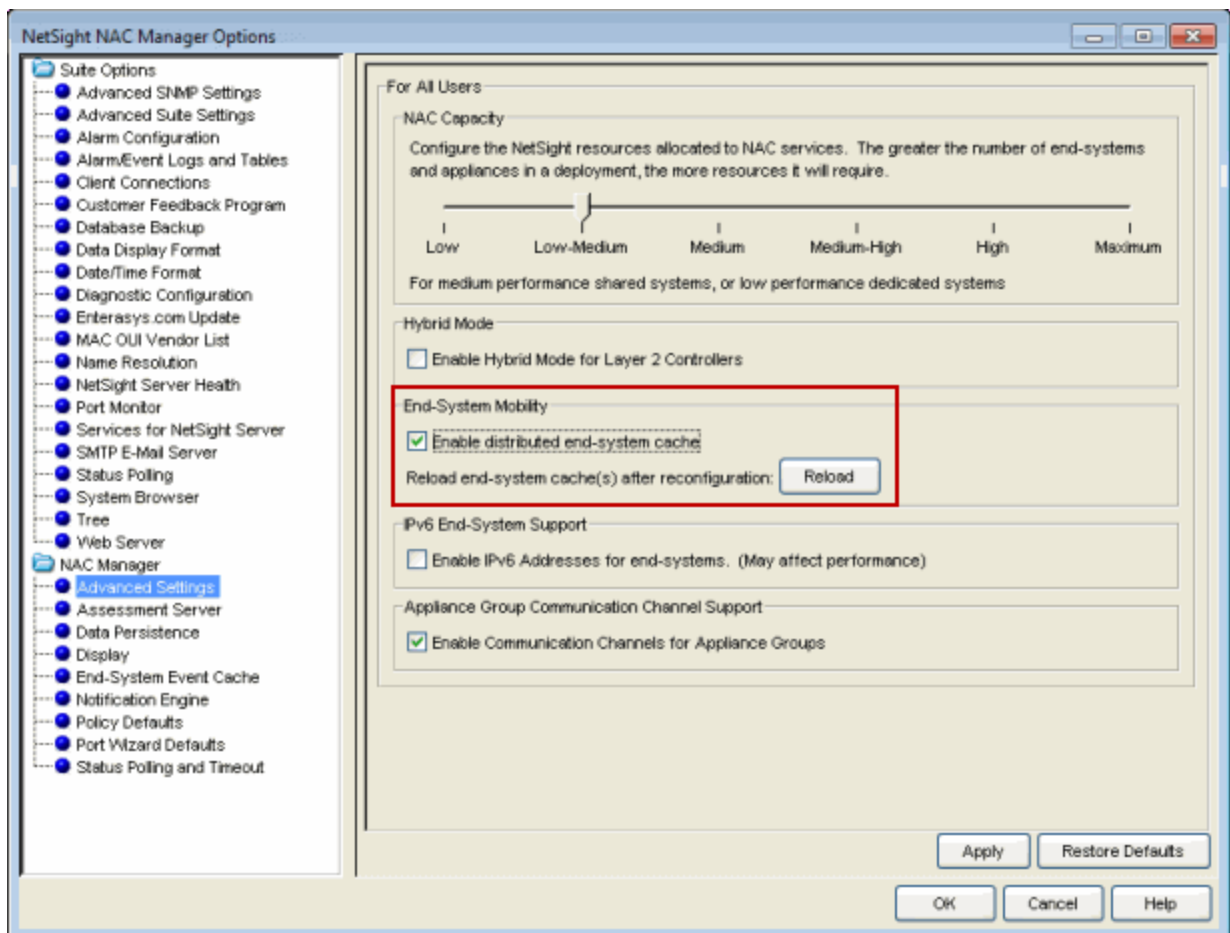


4. After you have created your communication channels, use the drop-down menu to select the appropriate communication channel for the appliance group. When you first enable communication channels, appliance groups will be members of the Default channel until you change the selection.



5. Repeat steps 3 and 4 to configure communication channels for all your appliance groups.

6. Click the **Enforce** toolbar button to enforce the new settings to your appliance groups. The communication channels are not active until you perform the enforce.
7. If you have enabled the Distributed End-Systems Cache option (Tools > Options > Advanced Settings), a new cache configuration must be reloaded on the Extreme Management Center server by pressing the **Reload** button in the options panel. This redistributes the end-system information to the new channels. The Reload operation may take some time and network communication may be temporarily disrupted.



Following the Enforce and Reload (if required), the traffic for each appliance group is restricted to its assigned communication channel. Disabling the Communication Channel option in the NAC Manager Options resets all channels for each appliance group back to Default.

Related Information

For information on related windows:

- [Options Window, Advanced Settings Options](#)

How to Configure Credential Delivery for Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Use the instructions in this Help topic to configure the method that will be used to send guests their credentials and access instructions for the secure SSID.

Configuration Steps

The Credential Delivery method is configured in your portal configuration. Depending on the method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

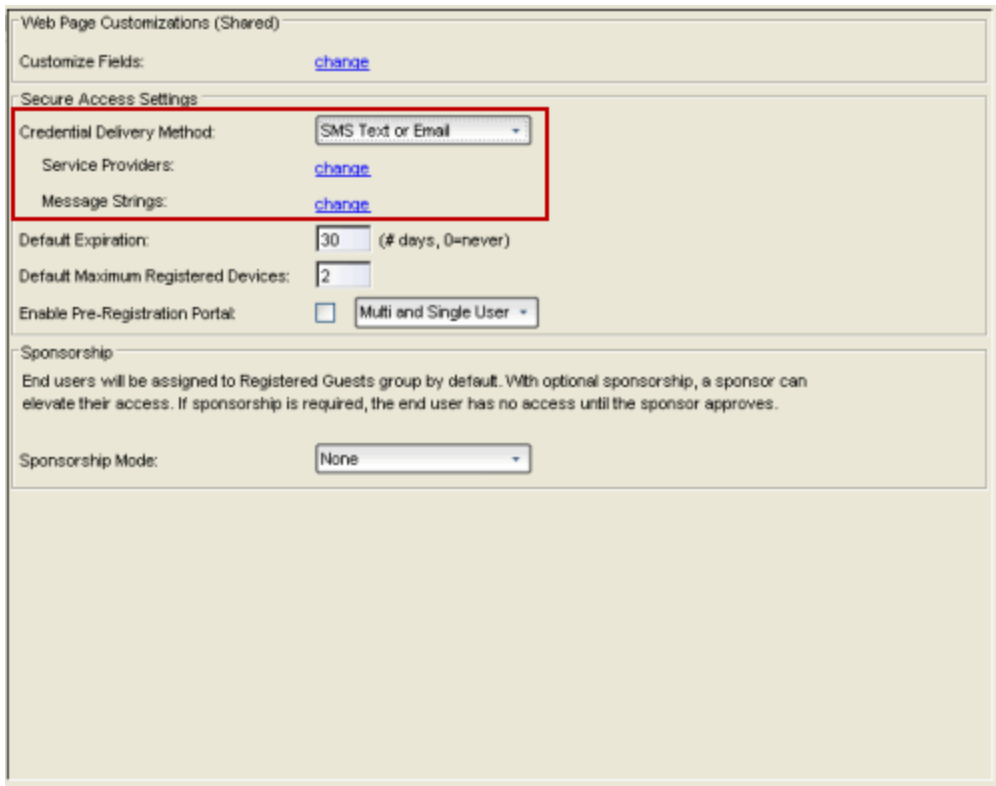
The following table provides a description of each credential delivery method and lists their custom field requirements.

User Verification Method	Description	Custom Field Requirement
Captive Portal	The credential information will be displayed on the Registration web page.	There are no Custom Field requirements.
Email	The end user must enter a valid email address on the Registration web page.	The Email Address Custom Field must be set to Required .
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to Required .

User Verification Method	Description	Custom Field Requirement
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to Visible .
SMS Text Message	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to Required .
SMS Text or Email	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to Visible .

Use the following steps to configure credential delivery for Secure Guest Access in your portal configuration.

1. In NAC Manager, [access the Portal Configuration](#). Click on the Secure Guest Access selection in the Portal Configuration tree. (If you don't see this selection, click Features in the tree and enable the Secure Guest Access feature.)
2. In the Secure Guest Access panel, use the drop-down menu to select the desired Credential Delivery Method (refer to the [table](#) above).



Web Page Customizations (Shared)

Customize Fields: [change](#)

Secure Access Settings

Credential Delivery Method: SMS Text or Email

Service Providers: [change](#)

Message Strings: [change](#)

Default Expiration: 30 (# days, 0=never)

Default Maximum Registered Devices: 2

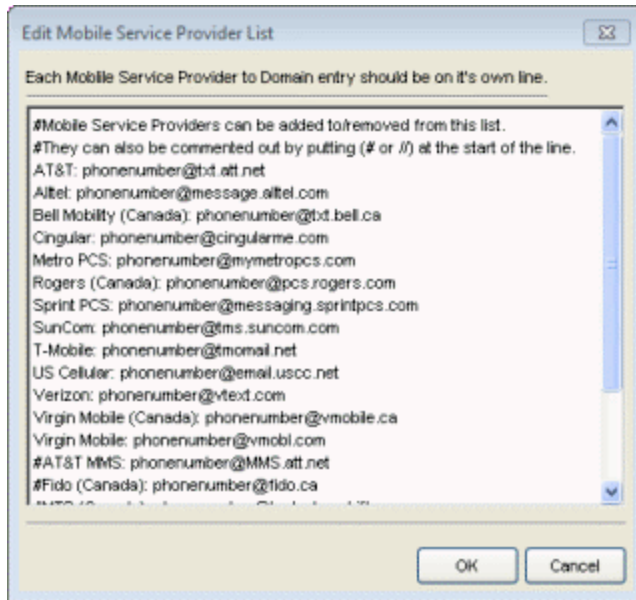
Enable Pre-Registration Portal: Multi and Single User

Sponsorship

End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.

Sponsorship Mode: None

3. If you selected the "SMS Text Message" or the "SMS Text or Email" Credential Delivery method, click the Service Providers "change" link to configure the list of mobile service providers from which end users can select on the Registration web page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.



You can comment out entries by preceding each line with either a # or // to allow temporary editing of the file without removing the text.

The list requires one service provider entry per line, using the following format: <Provider>;phonenumber@<specificdomain>.

When the end user registers, they will see only the <Provider> portion in the drop-down list of providers on the Registration web page.

Click **OK** to close the window.

4. If you have selected the "SMS Gateway" or "SMS Gateway or Email" method, enter the SMS Gateway Email address provided by the SMS Gateway provider.

Web Page Customizations (Shared)

Customize Fields: [change](#)

Secure Access Settings

Credential Delivery Method: SMS Gateway ▾

SMS Gateway Email:

Message Strings: [change](#)

Default Expiration: 30 (# days, 0=never)

Default Maximum Registered Devices: 2

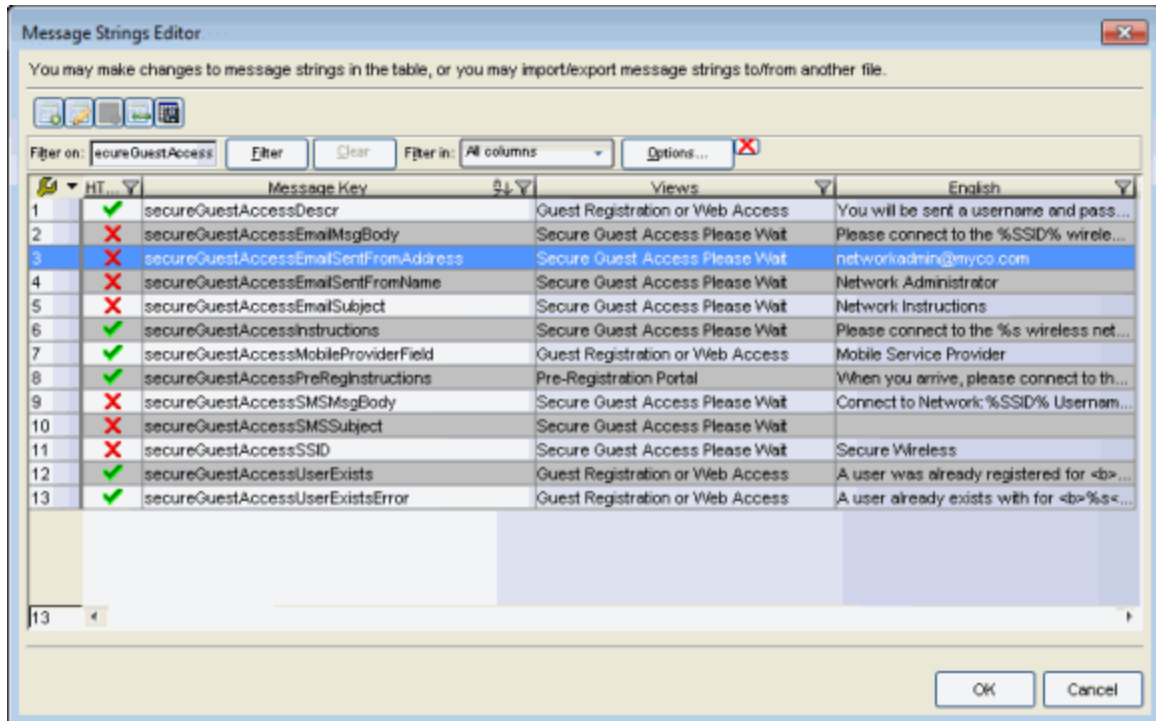
Enable Pre-Registration Portal: Multi and Single User ▾

Sponsorship

End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.

Sponsorship Mode: None ▾

5. For all methods, click on the Message Strings "change" link to open the [Message Strings Editor](#) where you can customize the text displayed on the Registration web page and the messages sent to the end user.



You will need to modify different message strings sent to the end user, depending on the delivery method or methods you selected. Double-click on the message to open a window where you can edit the message text.

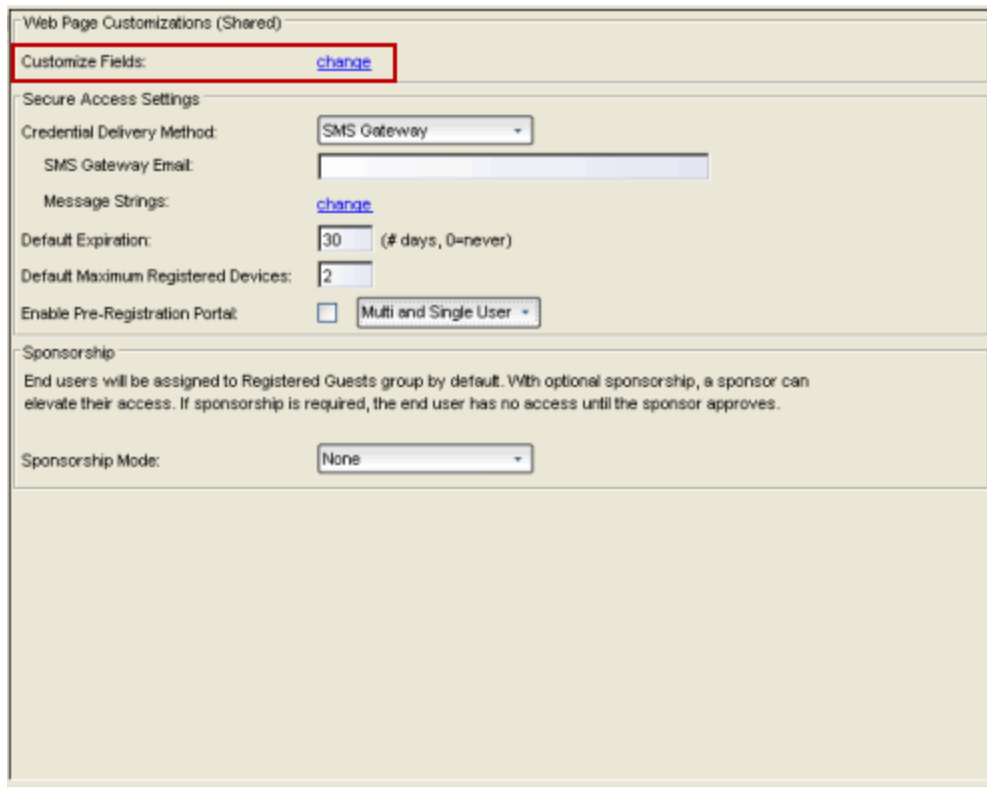
NOTE: When customizing message strings for text messaging (SMS Gateway or SMS Text Message) it is best to keep the message length as short as possible (under the maximum 160 characters limit). Some providers will break long messages into multiple messages and other providers will truncate the message, which could cause important information to be missing from the text message the guest receives.

- **Email** - This method uses the following strings:
 - secureGuestAccessEmailMsgBody - the default message shouldn't need to be changed.
 - secureGuestAccessEmailSentFromAddress - you will need to change the default message to the appropriate email address for your company.
 - secureGuestAccessEmailSentFromName - the default message shouldn't need to be changed.

- secureGuestAccessEmailSubject - the default message shouldn't need to be changed.
- **SMS Gateway** - Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone number.
 - secureGuestAccessSMSMsgBody
 - secureGuestAccessSMSSubject
- **SMS Text Message** - This method uses the following strings. The default messages shouldn't need to be changed.
 - secureGuestAccessSMSMsgBody
 - secureGuestAccessSMSSubject

Click **OK** to close the window.

6. In the Web Page Customizations (Shared) section, click the Customize Fields "change" link to open the Manage Custom Fields window.



The screenshot shows the 'Web Page Customizations (Shared)' window. At the top, there is a 'Customize Fields:' label with a blue 'change' link next to it, which is highlighted by a red rectangular box. Below this, the 'Secure Access Settings' section is visible, containing fields for 'Credential Delivery Method' (set to 'SMS Gateway'), 'SMS Gateway Email' (empty text box), 'Message Strings' (with a blue 'change' link), 'Default Expiration' (set to '30' days), 'Default Maximum Registered Devices' (set to '2'), and 'Enable Pre-Registration Portal' (checkbox) with a 'Multi and Single User' dropdown. The 'Sponsorship' section below contains explanatory text and a 'Sponsorship Mode' dropdown set to 'None'.

- Set the appropriate custom fields to display on the Registration web page, depending on the delivery method you selected (refer to the [table](#) above). If you do not set these fields, NAC will automatically set them for you based on your delivery method.

These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type will also change them for the others. For more information, see the [Manage Custom Fields Window](#).

Field	Visible	Required	Display String
First Name:	Visible	<input checked="" type="checkbox"/>	
Middle Name:	Visible	<input type="checkbox"/>	
Last Name:	Visible	<input checked="" type="checkbox"/>	
Email Address:	Visible	<input checked="" type="checkbox"/>	
Phone Number:	Visible	<input checked="" type="checkbox"/>	
1st Custom:	Not Visible	<input type="checkbox"/>	
2nd Custom:	Not Visible	<input type="checkbox"/>	
3rd Custom:	Not Visible	<input type="checkbox"/>	
4th Custom:	Not Visible	<input type="checkbox"/>	
5th Custom:	Not Visible	<input type="checkbox"/>	
Device Description:	Not Visible	<input type="checkbox"/>	

Acceptable Use Policy: Display [changes](#)

Note: Custom Display String fields are common between Unauthenticated and Authenticated Registration types. Modifying a Display String for one Registration type will affect the Display String in the other.

OK Cancel Help

Click **OK** to close the window.

- Back in the Portal Configuration, click **Save** to save your changes. Close the NAC Configuration window. Enforce the new portal configuration to your appliance(s). Credential delivery is now configured for your secure guest access.

How Secure Guest Access Works

When a guest attempts to access the network, the Registration web page asks for their email address and/or phone number, and any other required/configured information.

Welcome to the Enterprise Registration Center

You have been **denied** network access because this device is not registered to the network.

To obtain network access, you **must** complete registration using the form below

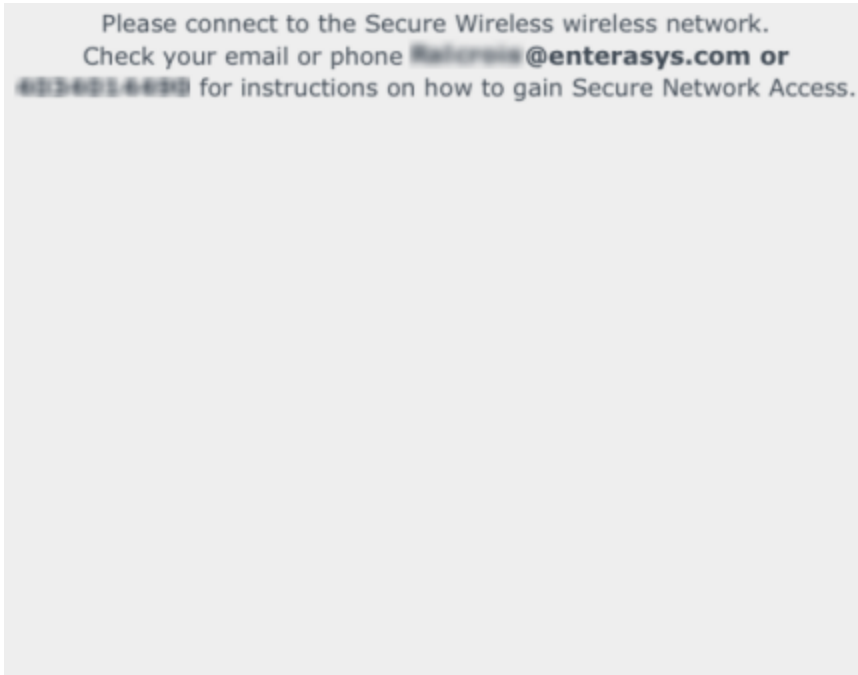
By registering to the network, you are **agreeing** to the terms and conditions explained in the [Enterprise Network and Computer Acceptable-Use Policy](#)

First Name*	
Middle Name	
Last Name*	
E-Mail Address*	
Phone Number*	
Mobile Service Provider*	AT&T ▼

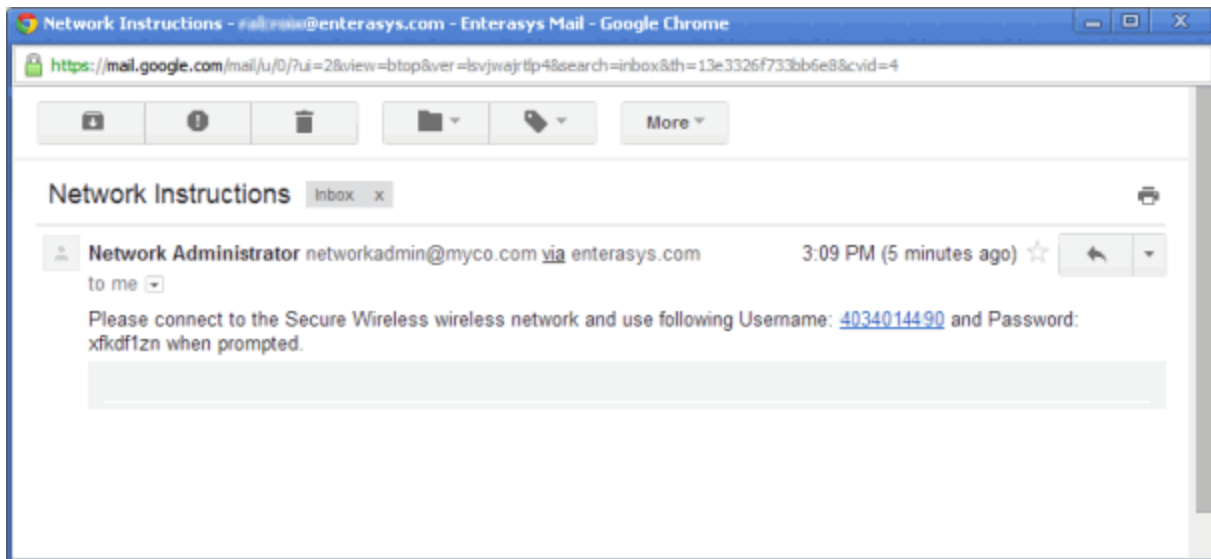
Complete Registration

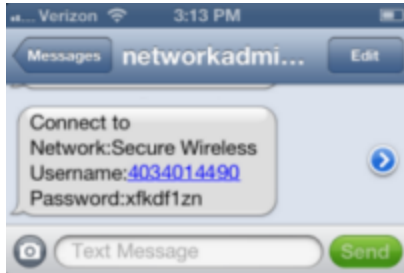
Please press the Complete Registration button only once.

When they click the **Complete Registration** button, they see the following screen that notifies them to check their email or phone for instructions on how to gain access to the network.

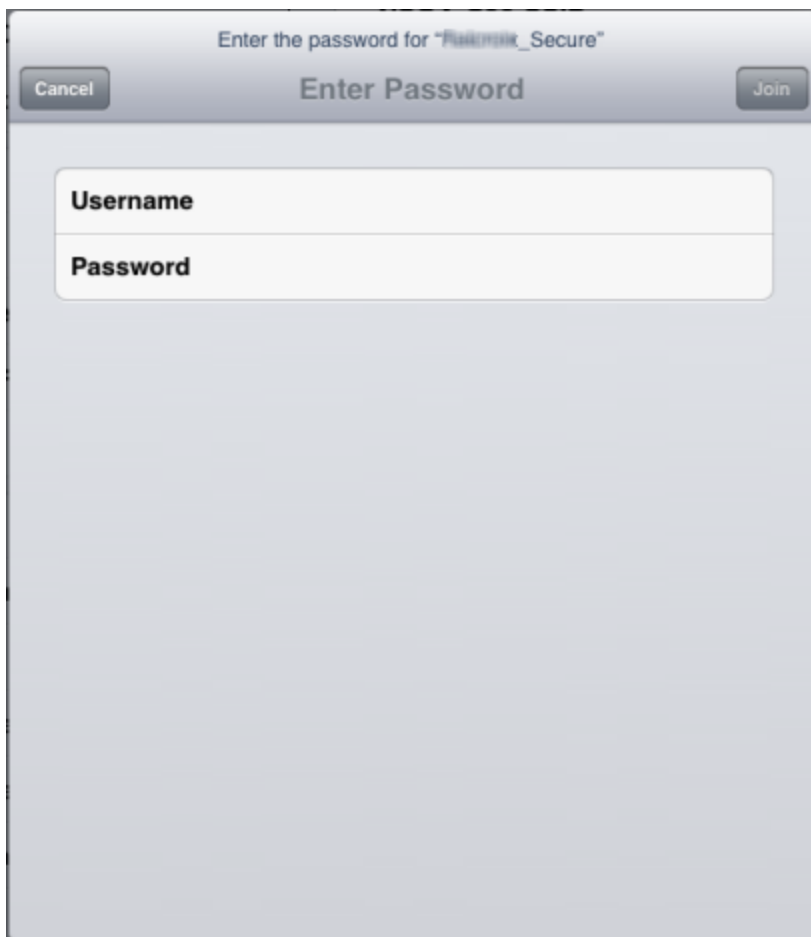


They are sent a username, password, and access instructions via an email or a phone text message.





When they connect to the Secure Wireless network, they will enter their username and password in this screen to gain access to the network.



Related Information

For information on related help topics:

- [Portal Configuration](#)

How to Configure End-System Zones

End-system zones allow you to limit a Extreme Management Center user's access to end-system information and configuration based on end-system zone membership. Users are only authorized to view or control a subset of end-systems, delimited by zones.

End-system zones are configured and managed in NAC Manager, and are enforced for Management Center end-system information and configuration.

When an end-system authenticates to the network, NAC rules are used to assign a NAC profile and a zone to the end-system. This allows you to use a variety of rule components (such as End-System Groups, Location Groups, and User Groups) to determine the zone to which an end-system should be assigned.

A user's zone access is determined by the authorized zones that are assigned to the user group of which they are a member. User groups are created and configured in the Authorization/Device Access Tool (accessed from the Tool menu), and authorized zones are assigned to each user group in NAC Manager.

When end-systems are filtered by zone, only authorized end-systems appear on the **Control** tab end-system views. Management Center users must have the appropriate capabilities to view end-system information or perform end-system operations, and then zone authorization lets them view and configure only a subset of end-systems based on zone.

NAC Manager also lets you use rule groups as a way to limit a Management Center user's access to rule group configuration operations in Management Center. Users are only authorized to view or make changes to a subset of rule groups. Whenever a user initiates a change to a rule group, such as adding or removing an end-system to or from a group, a check is performed to verify that the user is authorized to change that rule group.

NOTE: If you want to deny user access to Management Center end-system information (versus just limiting access), you must utilize authorization group capabilities (configured in the Authorization/Device Access Tool), independent of the zone configuration. For more information on configuring access to end-system information based on capabilities, see Management Center Access Requirements, specifically Use Case 4 and Use Case 5.

Preliminary Steps

Before you configure your end-system zones in NAC Manager, you should plan the authorized end-system zones and authorized rule groups for each of your Management Center user groups.

Plan Your End-System Zones

Create a worksheet that lists your end-system zones, the rules they will be associated with, and the NAC profile that will be assigned.

For example, the following table outlines the zones for an enterprise based on various business departments and their location.

Rule Name	Rule Summary	NAC Profile	Zone
Salem Sales	End-systems in Salem Sales	Sales Profile	Salem Zone
Salem Engineering	End-systems in Salem Engineering	Engineering Profile	Salem Zone
Salem Test Lab	End-systems in Salem Test Lab	Lab Profile	Salem Zone
New York Sales	End-systems in New York Sales	Sales Profile	New York Zone
New York Engineering	End-systems in New York Engineering	Engineering Profile	New York Zone
New York Test Lab	End-systems in New York Test Lab	Lab Profile	New York Zone
Registered Guests	End-Systems in Registered Guests	Guest Access	Guest Zone
Default Catch-all	End-systems in catch-all	Quarantine Access	

Determine User Group Zone Authorization

Create a worksheet that lists your user groups and their authorized zones and rule groups. Management Center users are assigned end-system zone and rule group authorization based on their user group membership. Before executing any end-system operation available in Management Center, the user's authorization to manage that end-system must be validated. Whenever a user initiates a change to a rule group, a check must be performed to determine if the user is authorized to change that rule group.

NOTES: Some operations modify several rule groups. For example, adding an end-system to one rule group may delete that end-system from another group. In this case, the user must be authorized to change both groups.



If an end-system has no zone, only unrestricted users can view it.


Continuing the example above, the user group authorization worksheet might look like this:

User Group	Authorized Zones	Authorized Rule Groups
Management Center Administrator	[unrestricted]	[unrestricted]
Salem Help Desk	Salem Zone, Guest Zone	Salem Sales, Salem Engineering, Salem Lab
New York Help Desk	New York Zone, Guest Zone	New York Sales, New York Engineering, New York Lab

Configuring Zones in NAC Manager

Use the following steps to configure your end-system zones in NAC Manager:

1. Configure the end-system zones for your Management Center user groups:
 - a. In NAC Manager, select Tools > Management and Configuration > End-System Zones.
 - b. In the [Manage End-System Zones window](#), select a Management Center user group in the list and then click the **Edit** button.
 - c. In the [Edit User Group window](#), use the **Select** buttons to configure the end-system zones that users in the group will be authorized to manage and the rule groups that they will be allowed to modify. You can also enter a list of end-system zones, if desired, instead of using the **Select** buttons.
 - d. Close the Edit User Group window to return to the Manage End-System Zones window.
 - e. Repeat these steps to configure all your user groups. Any changes made to a user group's capabilities do not take effect for the user until the next time they log in.
2. Associate your zones with the appropriate NAC rule.
 - a. In NAC Manager, use the  toolbar button to open the NAC Configuration window or use the **Edit** button in the [Configuration tab](#).
 - b. Click on the Rules icon in the left-panel tree.
 - c. In the right panel, click the  button and select Show Columns > Zone Column checkbox to add a Zone column to the rule list.
 - d. In the rule list, select one or more rules that you want to associate with a zone.

- e. Click the  button to open the Configure Rule Zone window.
 - f. Select a zone to associate with the rules. You may need to first add your zones using the New Zone button.
 - g. Click **OK**. The zone name appears in the Zone column in the rule list.
 - h. Perform these steps until all of your zones are associated with the appropriate rules.
-

Related Information

For information on concepts:

- [End-System Zones](#)



For information on related windows:

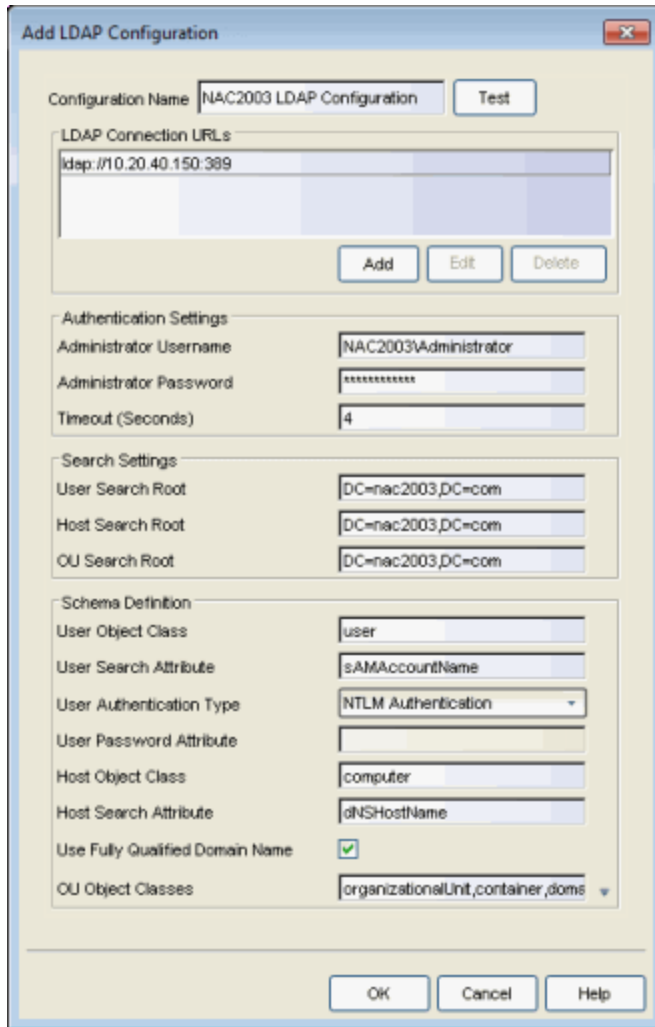
- [Manage End-System Zones Window](#)

How to Configure LDAP for End Users and Hosts via Active Directory

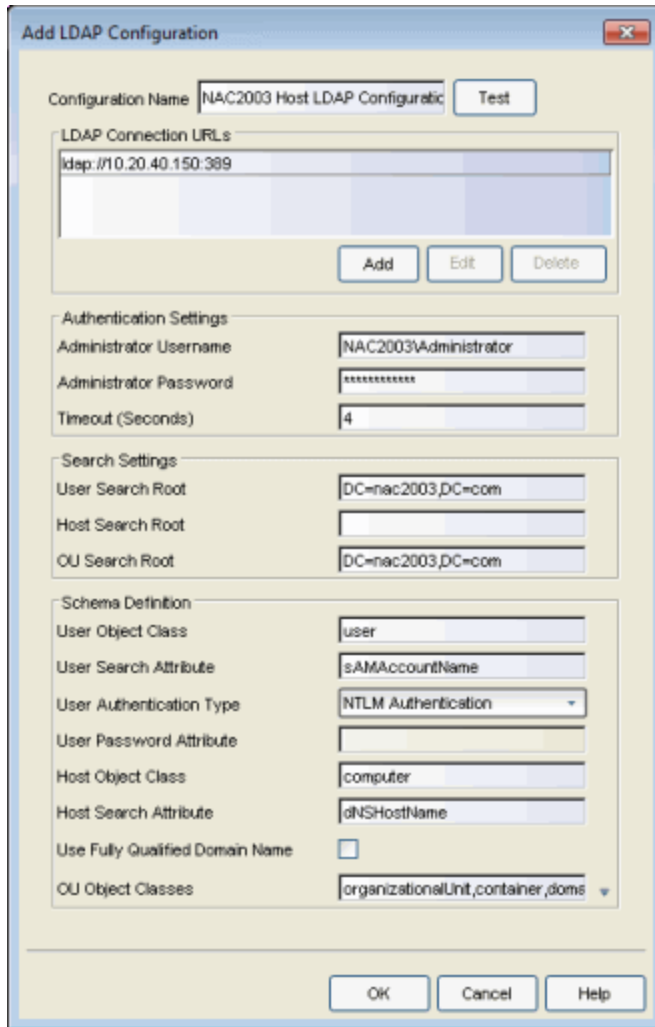
This Help topic provides instructions for creating LDAP configurations in NAC Manager that provide authentication and authorization for network end users and host machines via Active Directory.

In NAC Manager, you will need to create an Advanced AAA configuration that contains one mapping rule for your host machines and two mapping rules for your users. These mappings are the same except for their LDAP configuration. You will need to create two LDAP configurations: one for the hosts mapping and one for the users mapping. The LDAP configurations are identical except for the User Search Attribute. When you have completed these instructions, NAC Manager will use the new AAA configuration to authenticate both end users and host machines via your Active Directory server.

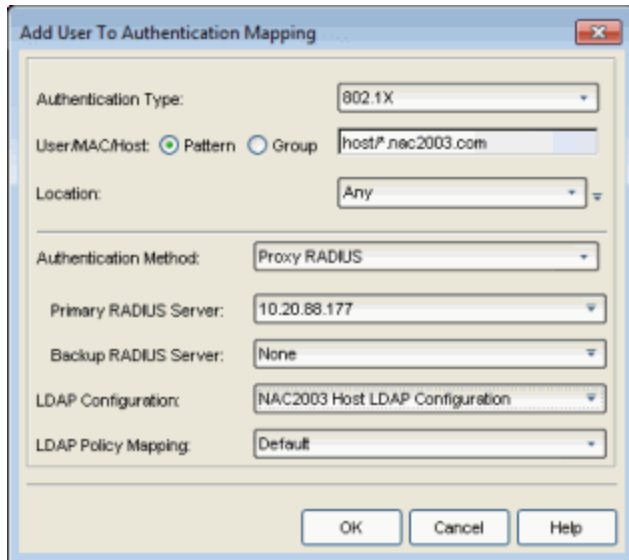
1. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
2. In the left-panel tree, select the AAA icon. The AAA Configuration is displayed in the right panel.
3. Use the AAA Configuration drop-down menu in the right panel create a new Advanced AAA Configuration or edit an existing Advanced AAA Configuration, if you already have one.
4. Click the Add New Mapping button  to open the [Add User to Authentication Mapping window](#).
5. Use the LDAP Configuration drop-down menu to select New and open the Add LDAP Configuration window.
6. Create an LDAP configuration for use with end users that authenticate to the network using the sample below as a guide. Click OK.



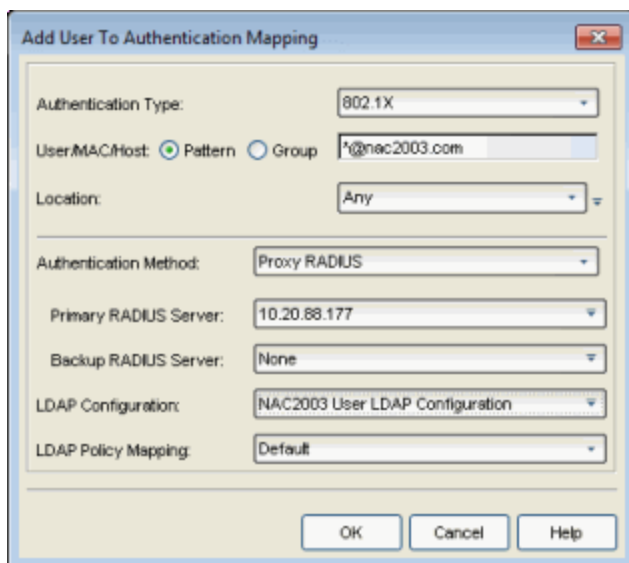
7. Back in the Add User to Authentication Mapping window, open the Add LDAP Configuration window again and add another LDAP configuration that will be used for host machines that authenticate to the network using the sample below as a guide. Note that the only difference between the two LDAP configurations is the User Search Attribute. Click OK.



8. In the Add User to Authentication Mapping window, create your first mapping rule to capture machine authentications using the sample below as a guide. In the example below, **host/*.nac2003.com** will capture the machine authentications for the NAC2003 active directory domain. Be sure to select the host LDAP Configuration that you created. Click OK.



9. Create your second mapping rule to capture end user authentications using the sample below as a guide. In the example below, `*@nac2003.com` will capture all users logging in to the NAC2003 active directory domain when they authenticate with their username in the format `<username>@<domain>`. Be sure to select the end user LDAP Configuration that you created. Click OK.



10. Create your third mapping rule to capture other end user authentications using the sample below as a guide. In the example below, `NAC2003*` will

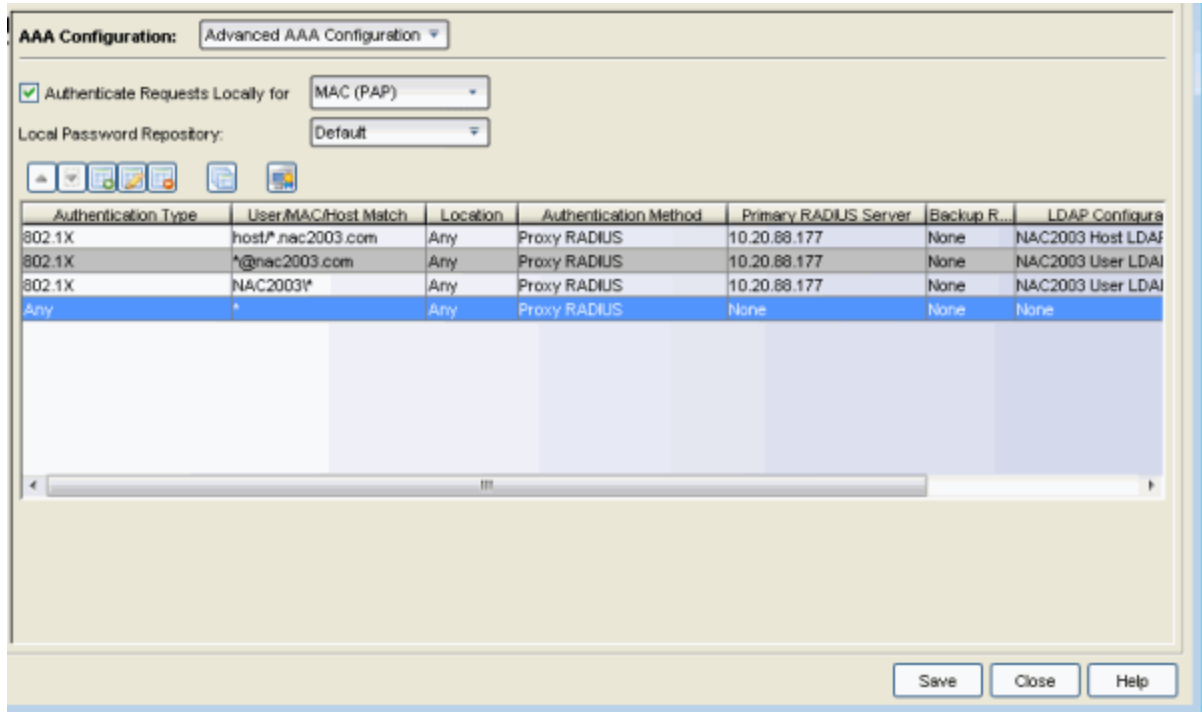
capture all users logging in to the NAC2003 active directory domain when they authenticate with their username in the format <domain>\<username>. Be sure to select the end user LDAP Configuration that you created. Click OK.

The screenshot shows a dialog box titled "Add User To Authentication Mapping". It contains the following fields and values:

- Authentication Type: 802.1X
- User/MAC/Host: Pattern Group, with the text "NAC2003*" in the adjacent field.
- Location: Any
- Authentication Method: Proxy RADIUS
- Primary RADIUS Server: 10.20.68.177
- Backup RADIUS Server: None
- LDAP Configuration: NAC2003 User LDAP Configuration
- LDAP Policy Mapping: Default

Buttons at the bottom: OK, Cancel, Help.

11. Back in the Advanced AAA Configuration, use the arrow buttons to make sure that the new mappings are listed above the "*" Any" mapping in the list of mappings. Your AAA configuration will now look like this. Click Save.



These instructions are complete. Now you can configure your [LDAP policy mappings](#) and/or [LDAP user groups](#) based on the attributes from either your host or user LDAP configurations.

Related Information

For information on related windows:

- [Add User to Authentication Mapping Window](#)
- [AAA Configuration Window](#)

How to Configure Load Balancing

This Help topic provides instructions for configuring load balancing in your NAC environment. Load balancing allows you to evenly distribute authentication requests and switch configuration ownership among your NAC gateway appliances. This can be useful in NAC deployments with a large number of switches, where manual delegation of switch resources would be cumbersome.

Load balancing is configured at the appliance group level. Once configured, all the NAC gateway appliances and switches in that group will participate in the load balancing process.

NAC Manager provides two different load balancing configuration options: either ExtremeXOS/EOS firmware on S-Series and K-Series devices, or utilizing external load balancers.

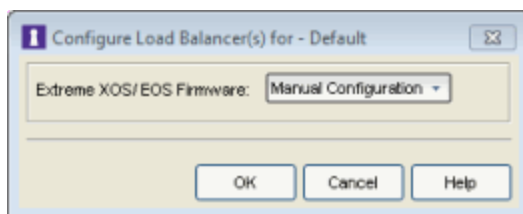
Instructions for:

- [ExtremeXOS/EOS Firmware Load Balancing](#)
- [External Load Balancers](#)

ExtremeXOS/EOS Firmware Load Balancing

Use the following steps to configure the native RADIUS load-balancing functionality on S-Series and K-Series switches.

1. Select an appliance group in the left-panel tree and click on the right-panel **Configuration** tab.
2. Click on the **Edit** button in the ExtremeXOS/EOS Firmware field. The **Configure Load Balancer(s)** window opens.



3. Select from the following four options:
 - **Manual Configuration** – Select this option if you have manually configured load balancing on your switches using the CLI. The Manual

Configuration option will leave the value as set on the device unchanged.

NOTE: If you are load balancing more than two NAC appliances, go to **Tools > Options > Display > Display Counts** and increase the number of NAC gateways a switch can be assigned to in the **Switches** tab.

- **Standard** – Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable.
- **Round Robin** – The round-robin RADIUS authentication algorithm spreads authentication requests evenly between available RADIUS servers, allowing large numbers of authentication requests to be evenly distributed across all RADIUS servers. This allows for a maximum authentication throughput for the number of RADIUS servers configured. Additionally, if a single server is down, incoming authentication sessions will be unaffected by the outage and will be distributed among the remaining available RADIUS servers.
- **Sticky Round Robin** – This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server should be used for any given authentication session once a session is initiated. In large-scale NAC deployments, this algorithm is used for switches that are authenticating more users than a NAC appliance supports. For example, a NAC deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three NAC appliances that support 3000 users each. In this scenario, the sticky round-robin algorithm allows the S-Series or K-Series device to spread the load across all three NAC appliances while using the same NAC appliance for all RADIUS transactions for a given session (MAC address).

4. Enforce all the appliances in the appliance group.

To disable load balancing, access the **Configuration** tab for an appliance group, and set the **Load Balancing** mode to **Standard**. Enforce all the appliances in the appliance group.

External Load Balancers

This section describes how to configure an ordered list of external load balancers that will be used to evenly distribute authentication load across multiple NAC appliances.

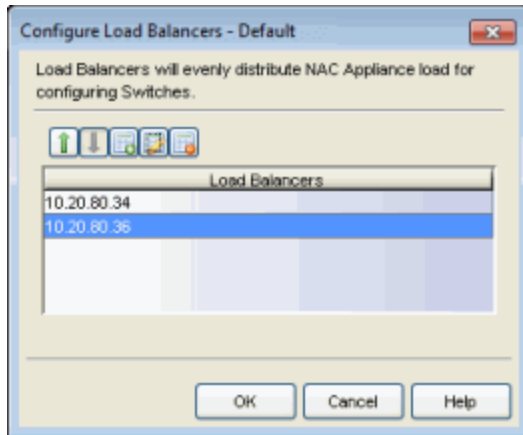
Typically, there is a primary and secondary (backup) load balancer configured to load balance the RADIUS requests for all the switches in an appliance group.



When an enforce is performed, the NetSight server assigns virtual IPs (VIPs) to the primary and secondary load balancers. Each switch in the appliance group will send authentication requests to the primary VIP, which will load balance authentication requests between the available NAC appliance gateways in the appliance group.

When a load balancer receives a RADIUS authentication request from a switch, it determines which appliance will service the request based on various criteria such as current appliance load, availability, and response time.

Use the following steps to configure load balancing:

1. Perform the following preliminary steps:
 - a. Verify that your NAC gateway appliances and switches (NAC RADIUS clients) are not on the same subnet. Appliances and switches cannot be on the same subnet for load balancing to work, as RADIUS access-request and response packets must traverse the load balancer for proper operation.
 - b. Configure your load balancers to load balance port 1812 for authentication and port 1813 for RADIUS accounting.
 - c. For 802.1x authentication, set the load balancers to **sticky** mode based on the source IP of the authentication request (the switch's IP address). This ensures that all RADIUS packets in the 802.1x authentication are sent to the same NAC appliance.
2. Select an appliance group in the left-panel tree and click on the right-panel **Configuration** tab.
3. Click on the **Edit** button in the **External Load Balancing** field. The **Configure Load Balancers** window opens.



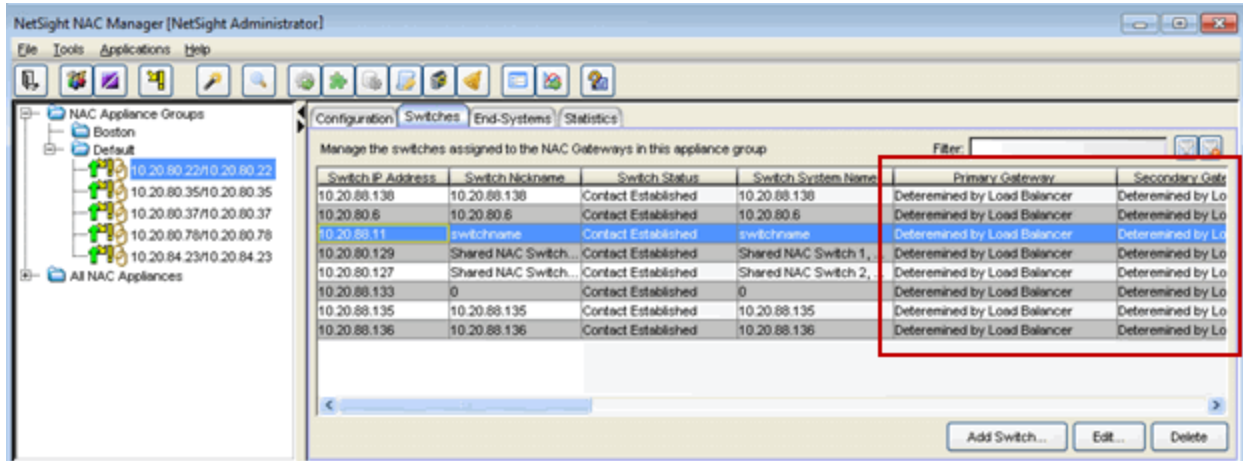
4. Use the toolbar icons to configure an ordered list of load balancers.
 - a. Click on  to open a window where you can add an IP address for a new load balancer. Click **OK**.
 - b. Add all of your RADIUS authentication and accounting load balance IPs to the list.
 - c. Use the up and down arrows  to configure load balancer precedence in the list. All switch traffic is sent to the first load balancer in the list, unless that load balancer is down. Then the traffic will be sent to the second load balancer in the list, and so on.
 - d. When your list is complete, click **OK** to close the **Configure Load Balancers** window.
 - e. Enforce all the appliances in the appliance group.

To disable load balancing, remove all the switches from the appliance group and then disable load balancing on the appliance group's **Configuration** tab.

External Load Balancing Example

This example demonstrates how load balancing works for an appliance group using one load balancer with the IP address of 10.22.70.1. The appliance group has five NAC gateway appliances and eight switches.

All switches in the appliance group will appear against each NAC gateway in the group, as shown in the **Switches** tab below. The primary, secondary, tertiary, and quaternary gateway columns in the **Switches** tab will indicate that the load balancer will determine the gateway.



At Enforce, the configuration for all eight switches is written to all five gateways. The table below shows how load balancing will be configured for all the gateways.

Switch IP	Primary Gateway	Secondary Gateway	Tertiary Gateway	Quaternary Gateway
10.20.88.127	10.20.80.22	10.20.80.35	10.20.80.37	10.20.80.78
10.20.88.129	10.20.80.35	10.20.80.37	10.20.80.78	10.20.80.23
10.20.88.6	10.20.80.37	10.20.80.78	10.20.80.23	10.20.80.22
10.20.88.11	10.20.80.78	10.20.80.23	10.20.80.22	10.20.80.35
10.20.88.133	10.20.80.23	10.20.80.22	10.20.80.35	10.20.80.37
10.20.88.135	10.20.80.22	10.20.80.35	10.20.80.37	10.20.80.78
10.20.88.136	10.20.80.35	10.20.80.37	10.20.80.78	10.20.80.23
10.20.88.138	10.20.80.37	10.20.80.78	10.20.80.23	10.20.80.22

How to Configure Local RADIUS Termination at the Extreme Access Control Engine

This Help topic provides information on how to configure authentication using the Extreme Access Control engine RADIUS server to locally terminate 802.1X EAP authentication requests. There are three methods that can be used to do this, depending on the protocol that is used:

- LDAP Authentication - Uses a backend Active Directory server or LDAP server, and RADIUS server and client certificates (if required) to authenticate users.
- Local Authentication - Uses a local password repository, and RADIUS server and client certificates (if required) to authenticate users.
- RADIUS Certificates only - Uses only RADIUS server and client certificates to authenticate users (no password is required).

The following chart lists the protocols that are supported for local RADIUS termination, and shows whether the protocol uses RADIUS certificates and/or passwords to authenticate users. If passwords are required, you can then decide whether to use LDAP or local authentication for password verification. The chart also lists the hash types supported by each protocol for user password encryption. Note that PEAP (TLS) is not supported for local RADIUS termination and is only supported in a proxy RADIUS configuration.

Protocol	RADIUS Certificates Required	Password Required	Supported Password Hash Types
PAP	No	Yes	PKCS5 Reversible, SHA1, NT Hash
CHAP	No	Yes	PKCS5 Reversible
MsCHAP	Yes	Yes	PKCS5 Reversible, NT Hash
PEAP (EAP-MsCHAPv2)	Yes	Yes	PKCS5 Reversible, NT Hash
EAP-TTLS	Yes	Yes	PKCS5 Reversible, SHA1, NT Hash
EAP-TLS	Yes	No	N/A
EAP-MD5	No	Yes	PKCS5 Reversible

Instructions on:

- [LDAP Authentication](#)
 - [User Authentication Considerations](#)

- [Local Authentication](#)
 - [User Password Considerations](#)
- [Certificate Configuration](#)
 - [EAP-TLS Certificate Requirements](#)

LDAP Authentication

LDAP authentication uses a backend Active Directory server or LDAP server defined in your AAA Configuration to authenticate users. Additionally, some protocols also require RADIUS server and client certificates to be used in conjunction with LDAP authentication (see [Certificate Configuration](#)).

Before configuring LDAP authentication, read through the User Authentication considerations described below.

User Authentication Considerations

If you are using LDAP authentication, the type of LDAP server you select depends on the protocol you are using. With Active Directory, NAC Manager provides a more feature-rich integration and supports a large number of protocols, while with other LDAP servers such as OpenLDAP, NAC Manager provides a more basic integration with limited protocol support.

Active Directory

Supported Protocols: PAP, MsCHAP, PEAP, EAP-MsCHAPV2, and EAP-TTLS with tunneled PAP.

PAP or EAP-TTLS with tunneled PAP protocols

During the authentication process, the Access Control engine sends an LDAP bind request to the Active Directory domain controller using the password retrieved from the end user's authentication request. Therefore, the LDAP protocol must be allowed between the Access Control engine and the Active Directory domain controller for the authentication process to take place.

MsCHAP, PEAP, and EAP-MsCHAPv2 protocols

These three protocols work with Active Directory (and not other LDAP servers) because they use NT Hash for password encryption, which is the same password hash type used by the Microsoft Active Directory domain controller.

Authentication requests are made by the Access Control engine sending an ntlm_auth request to the Active Directory domain controller. The Access Control engine attempts to join the Active Directory domain using the LDAP configuration and the administrator username and password. In your LDAP configuration, the administrator username used to connect to the LDAP server must be a member of the built-in Domain Administrator group or Account Operators group. (See the [Active Directory Permissions](#) section below.)

Additionally, the DNS configuration must be set up so that the Access Control engine can resolve the domain by name. To do this, you should configure the DNS server to be one of the domain controllers for that domain, and verify that the domain name is configured correctly on the Access Control engine. If users authenticate to multiple domains, you must also configure the domains to fully trust each other. Refer to the following Microsoft documentation for information on how to set up domain trusts:

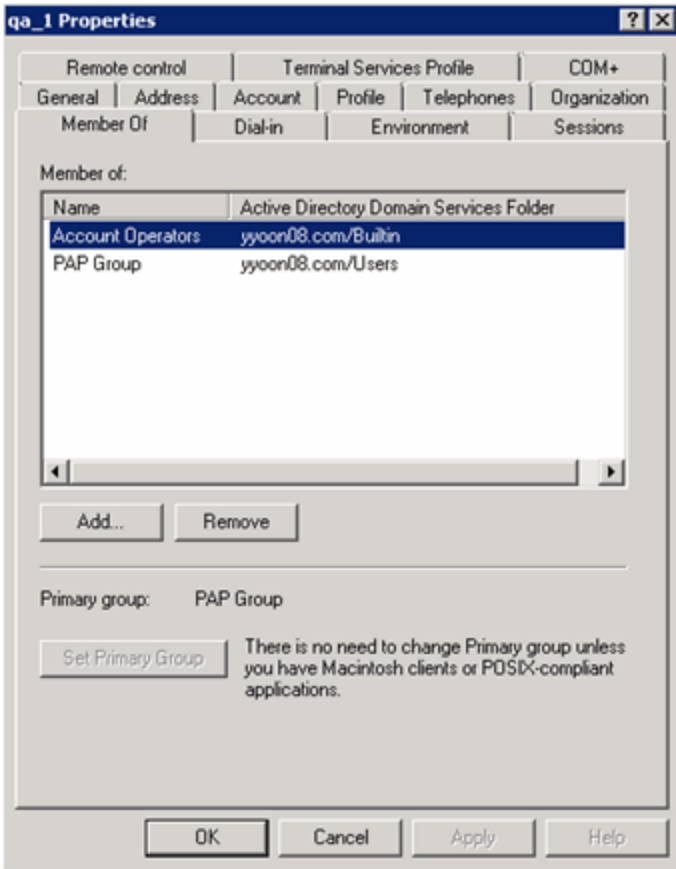
<https://technet.microsoft.com/en-us/library/cc740018%28WS.10%29.aspx>.

Note: These protocols do not work if the active directory domain server is set to only allow NTLMv2 authentication because these protocols do not use NTLMv2 and the hash passed to NAC Manager is rejected by the active directory server. Allowing only NTLMv2 authentication only works if NAC Manager proxies the 802.1x request to Microsoft IAS/NPS. Microsoft IAS/NPS allows this lower level of authentication because it is in a TLS session, which Microsoft believes makes it as secure as NTLMv2. For more information, see <https://technet.microsoft.com/en-us/library/cc772468.aspx>

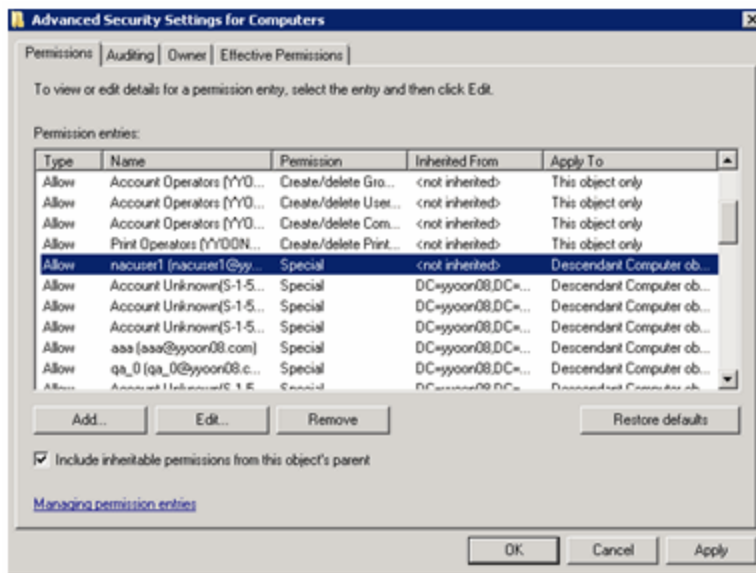
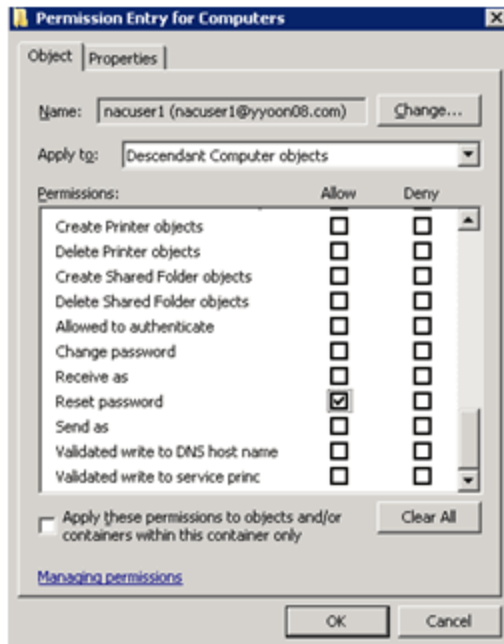
Active Directory Permissions

These instructions are valid for Windows 2008 and Windows 2012. You must configure the proper permissions in Active Directory to allow NAC Manager to do the local RADIUS termination and authenticate to the Active Directory Server. In your LDAP configuration, the administrator username used to connect to the LDAP server can be a member of the built-in Domain Administrator group or Account Operators group, or a Standard Domain User with Descendant Computer Objects ("Reset password" permissions only).

Example: Member of the built-in Account Operators group.



Example: Standard Domain User with Descendant Computer Objects



Active Directory with User Log On Restrictions

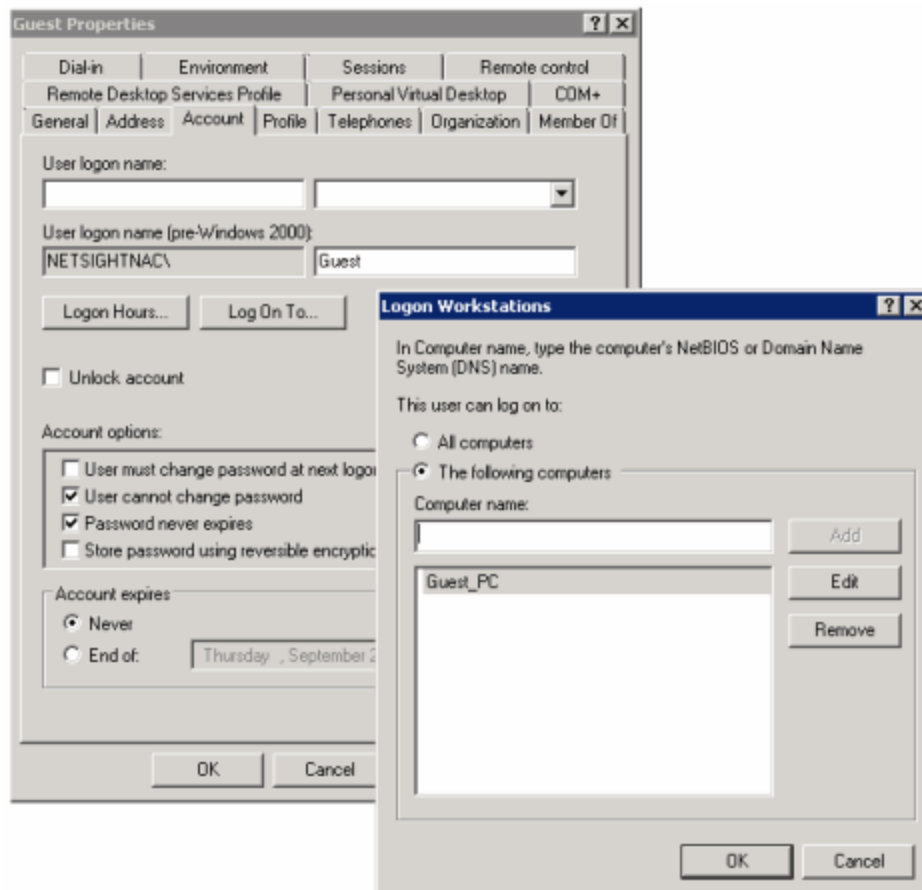
In Active Directory, it is possible to configure an option that restricts a user domain log on to specific computers. This configuration is enforced during the domain log on process.

In an Access Control environment where users authenticate using 802.1X and NAC Manager is configured to proxy RADIUS requests, no additional configuration is required. The 802.1X authentication process completes normally

and the determination of whether the user is allowed to log on to the domain from the specific computer is enforced at that time.

In an Access Control environment where NAC Manager is terminating 802.1X authentications locally, NAC Manager performs an NTLM authentication to authenticate the 802.1X session. This process simulates the domain log on process. Therefore, the incoming authentication request for the user appears to be coming from a computer (the Access Control engine) that the user is not allowed to log on to, and the authentication attempt is rejected.

The solution in this scenario is to add the Access Control engines to the list of computers the user is allowed to log on to. This allows the 802.1X authentication process to complete and successfully authenticate the user. The enforcement of whether the user is allowed to log on to the specific computer takes place during the domain log on process.



Other LDAP Servers

Supported Protocols: PEAP, PAP, and EAP-TTLS with tunneled PAP.

During the authentication process, the Access Control engine attempts an LDAP (S) bind with the LDAP server to authenticate the end user's credentials. Ensure that LDAP(S) between the Access Control engine and LDAP server is not blocked by an ACL or firewall.

For information, see: [How to Configure PEAP Authentication via eDirectory](#) and [How to Configure PEAP Authentication via OpenLDAP](#).

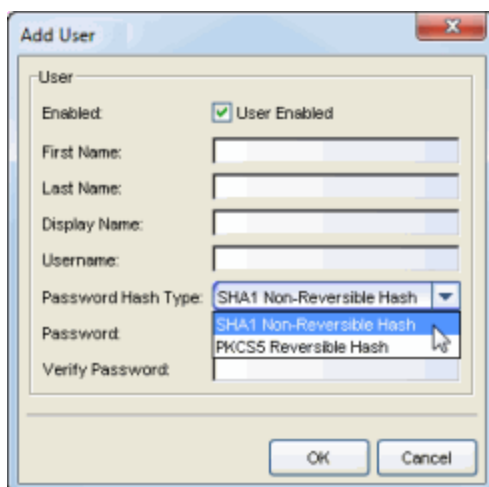
Local Authentication

Local authentication uses a local password repository defined in your AAA Configuration to authenticate users. Additionally, some protocols also require RADIUS server and client certificates to be used in conjunction with local authentication (see [Certificate Configuration](#)). Before configuring local authentication, read through the user password considerations described below.

User Password Considerations

When you add or edit a user in your local password repository, you can specify the password hash type used to encrypt the user's password in the Extreme Management Center and NAC Manager databases. Select from two supported hashing algorithms, depending on the protocol you are using:

- SHA 1 - a non-reversible hashing algorithm
Supported Protocols: PAP and EAP-TTLS with tunneled PAP
- PKCS5 - a reversible hashing algorithm
Supported Protocols: PAP, CHAP, MsCHAP, PEAP, EAP-MsCHAPV2, EAP-TTLS with tunneled PAP, and EAP-MD5



The screenshot shows a 'Add User' dialog box with the following fields and options:

- User Enabled:** User Enabled
- First Name:** [Empty text box]
- Last Name:** [Empty text box]
- Display Name:** [Empty text box]
- Username:** [Empty text box]
- Password Hash Type:** SHA1 Non-Reversible Hash (dropdown menu is open, showing options: SHA1 Non-Reversible Hash, PKCS5 Reversible Hash)
- Password:** [Empty text box]
- Verify Password:** [Empty text box]

Buttons: OK, Cancel

Certificate Configuration

If the protocol you are using requires RADIUS certificates for authentication (see the table above), review the certificate configuration information in this section.

During installation, Access Control generates a unique private key and server certificate for the NAC Manager RADIUS server. This certificate provides basic functionality while you are configuring and testing your NAC Manager deployment. To integrate with the certificate structure you already have on your network, update to a certificate generated by a Certificate Authority that your connecting end-systems are already configured to trust. For instructions, see the [Update RADIUS Server Certificate Window](#) Help topic.

In addition, configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted. For instructions see the [Update AAA Trusted Certificate Authorities Window](#) Help topic.

EAP-TLS Certificate Requirements

Server Certificate:

Enhanced Key Usage:
Server Authentication (1.3.6.1.5.5.7.3.1)

Key Usage:
Digital Signature, Key Encipherment

Client Certificate:

Enhanced Key Usage:
Client Authentication (1.3.6.1.5.5.7.3.2)

Key Usage:
Digital Signature, Key Encipherment



Related Information

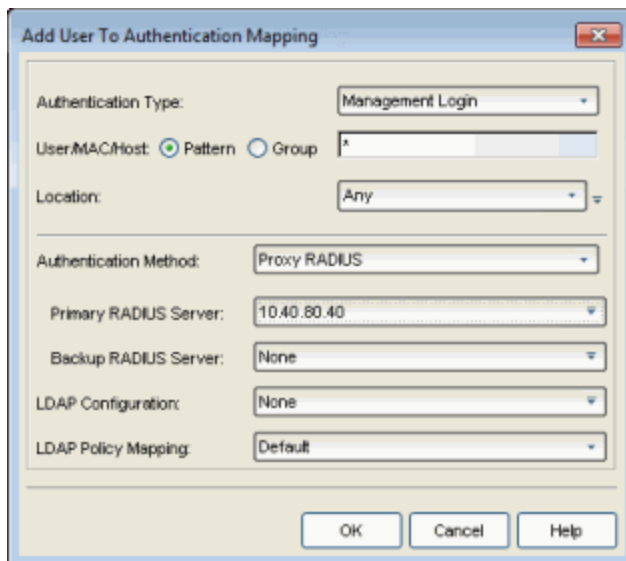
For information on related tasks:

- [Update RADIUS Server Certificate Window](#)
- [Update AAA Trusted Certificate Authorities Window](#)
- [Edit Basic AAA Configuration Window](#)

How to Configure Management Authentication

This Help topic describes how to configure authentication for management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet. To do this, you must create an Advanced AAA Configuration that includes a mapping for management authentication, as well as configure the authentication access type for each switch.

1. Create an Advanced AAA Configuration and add a mapping for management authentication.
 - a. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
 - b. In the left-panel tree, select the AAA icon. The AAA Configuration is displayed in the right panel.
 - c. Use the AAA Configuration drop-down menu in the right panel to create a new Advanced AAA Configuration or edit an existing Advanced AAA Configuration, if you already have one.
 - d. In the Advanced AAA Configuration, use the Add New Mapping button  to add a mapping that has the Authentication Type field set to Management Login. This authentication type can be used to authenticate users locally, or proxy them to specific RADIUS or LDAP servers, depending on the Authentication Method that you specify.



Add User To Authentication Mapping

Authentication Type: Management Login

User/MAC/Host: Pattern Group *

Location: Any

Authentication Method: Proxy RADIUS

Primary RADIUS Server: 10.40.60.40

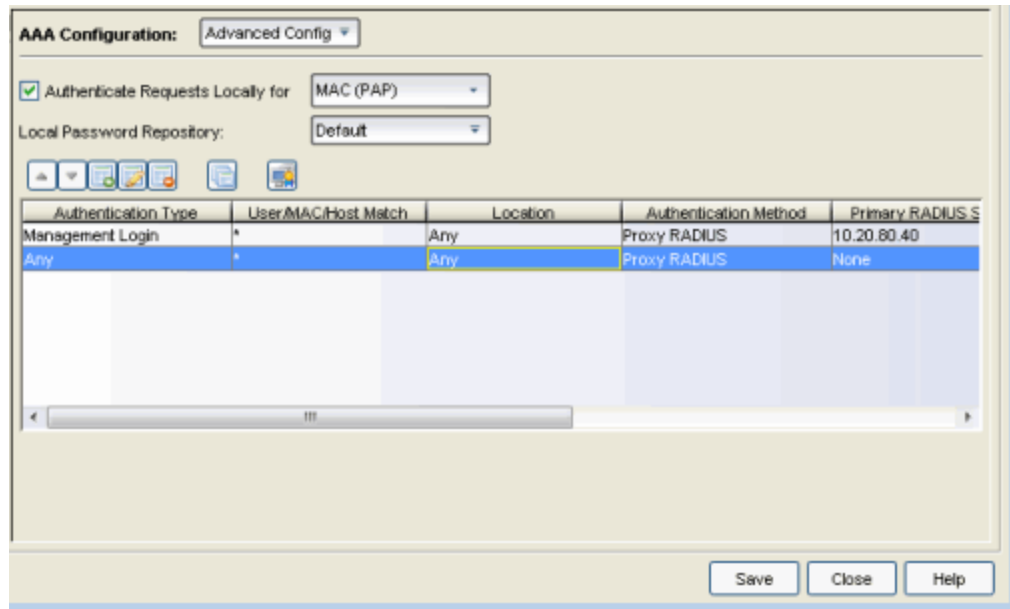
Backup RADIUS Server: None

LDAP Configuration: None

LDAP Policy Mapping: Default

OK Cancel Help

- e. Click **OK**. Back in the Advanced AAA Configuration, use the arrow buttons to make sure that the new mapping is listed above the "*" Any" mapping in the list of mappings.

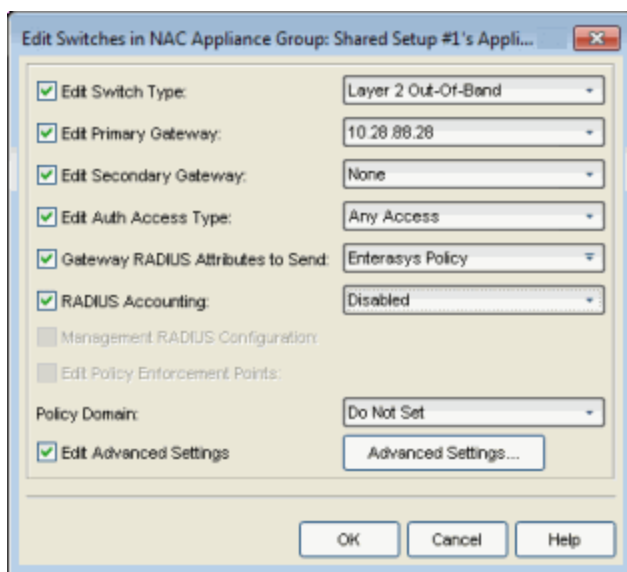


- f. Click **OK**. Back in the NAC Configuration window, assign the new Advanced AAA configuration to your NAC Configuration.
 - g. Enforce to your appliances.
2. Configure each switch to allow management requests.
 - a. In the [Switches tab](#), select the desired switch and click **Edit**.
 - b. In the [Edit Switches window](#), set the Auth. Access Type to either "Any Access" or "Management Access" to allow management requests.

WARNING: For ExtremeXOS devices only. NAC uses CLI access to perform configuration operations on ExtremeXOS devices.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. Make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator NAC Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that NAC will authenticate management login attempts against.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.


c. Make sure that the Gateway RADIUS Attributes to Send value is set to "Enterasys Policy".

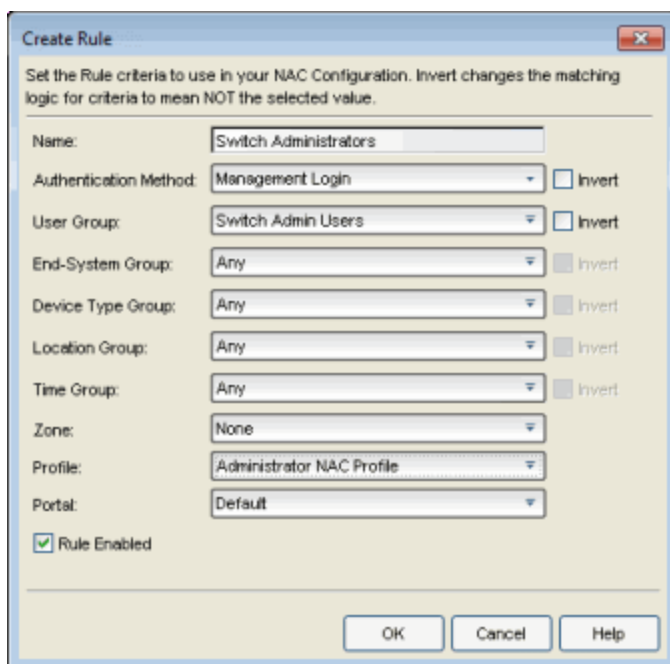


d. Click **OK**. Enforce to your appliances.

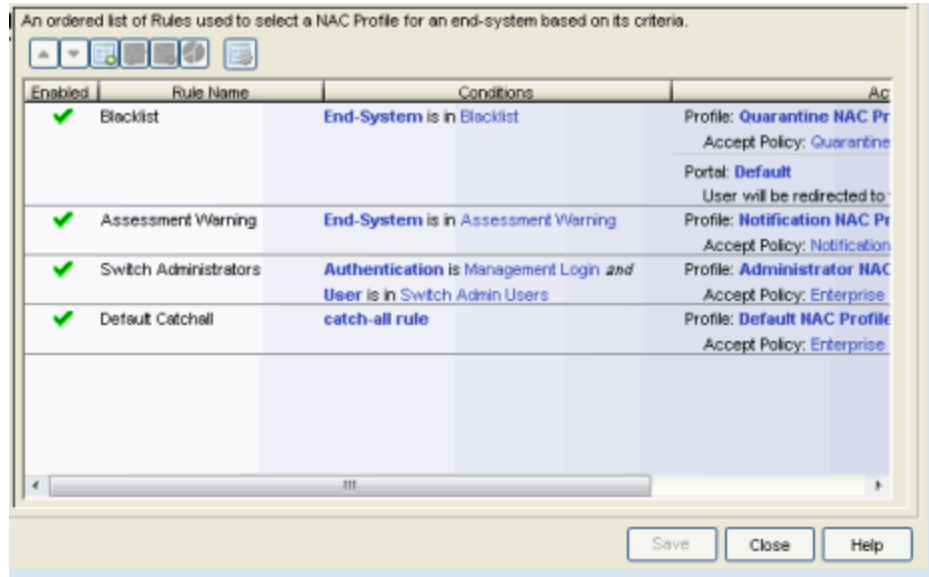
3. If you will be authenticating management requests locally or proxying them to an LDAP server, you must create a rule that assigns a profile where the Accept policy is set to a policy that has the management attribute configured. The management attribute determines the level of access the administrator will have to the switch: Administrator (Superuser) or Read-Only.

NOTE: If your authentication method is set to Proxy RADIUS (in your AAA configuration), you do not need to define a rule. Instead, the RADIUS server **must** be configured to return the filter ID with the management attribute already specified in it.

- a. Use the [Add/Edit User Group window](#) to create a User Group for your Switch Administrators. This group will specify those users that are allowed to login to and configure switches.
- b. In the NAC Configuration window Rules panel, click the Add New Rule button  to open the [Create Rule window](#).
- c. Create a rule that specifies the Switch Administrator users group that you created. Select a NAC profile that specifies an Accept Policy that defines either the Administrator (Superuser) or Read-Only management attribute, such as Enterprise User (Administrator) or Enterprise User (Read-Only Management). (You can also use a different policy that you have created, as long as the [management attribute](#) has been defined in the [Add/Edit Policy Mapping window](#).)



- d. Click **OK**. The rule appears in the rule list of your NAC Configuration.



e. Enforce to your appliances.

The switch administrators that you have defined will now be able to login to and configure the specified switches according to the defined level of access.

Related Information

- [AAA Configuration Window](#)
- [Edit Switches Window](#)
- [Edit Policy Mapping Window](#)

How to Configure PEAP Authentication via eDirectory

This Help topic provides instructions for configuring NAC to authenticate PEAP, MsCHAP, and MsCHAPv2 requests using Novell eDirectory.

To do this, you must create a RADIUS account and a Universal Password Policy on eDirectory. After eDirectory is configured, you can select the Populate Novell eDirectory Defaults for your NAC Manager LDAP configuration, and set the User Authentication Type to be Plain Text Password Lookup. Then, in your advanced AAA configuration, create an entry that uses this LDAP configuration. This will allow NAC to verify the user's password from the PEAP/MsCHAP/MsCHAPv2 request via eDirectory.

Use the following steps to create this configuration.

1. In Novell iManager, create an account that is permitted to authenticate to eDirectory and retrieve the user password information.
 - a. Create an admin user that the LDAP configuration in NAC Manager will use to connect and authenticate end-systems to the Novell eDirectory. In our example below, the username is radiusAdmin.

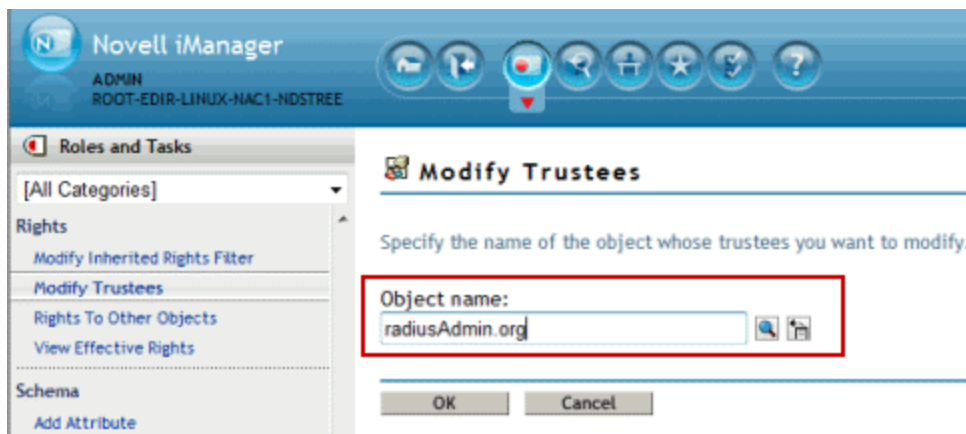


The screenshot shows the Novell iManager interface for creating a user. The top navigation bar includes the Novell iManager logo and the user's role: ADMIN, ROOT-EDIR-LINUX-NAC1-NDSTREE. A sidebar on the left lists 'Roles and Tasks' with categories like Schema, SNMP, and Users. The main area is titled 'Create User' and contains the following fields:

Username: *	<input type="text" value="radiusAdmin"/>
First name:	<input type="text"/>
Last name: *	<input type="text" value="NAC"/>
Full name:	<input type="text" value="NAC"/>
Context: *	<input type="text" value="org"/>  
Password:	<input type="password" value="....."/>
Retype password:	<input type="password" value="....."/>

Note: Failure to enter a password will allow the user to login without a password.

2. Assign the admin user trustee status and privileges to access the database.
 - a. On the Modify Trustees page, locate the admin user using the Search function.



- b. Add the admin user as a Trustee using the **Add Trustee** button on the right side of the Modify Trustees page.



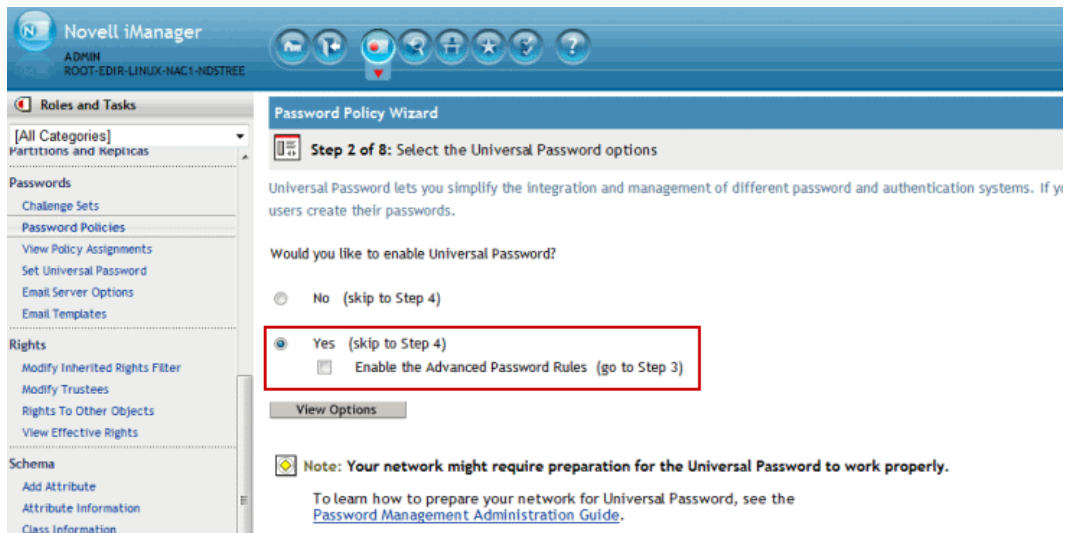
- c. Select the Assigned Rights link for the Trustee user and enable the Supervisor option defined for the All Attributes Rights Property.



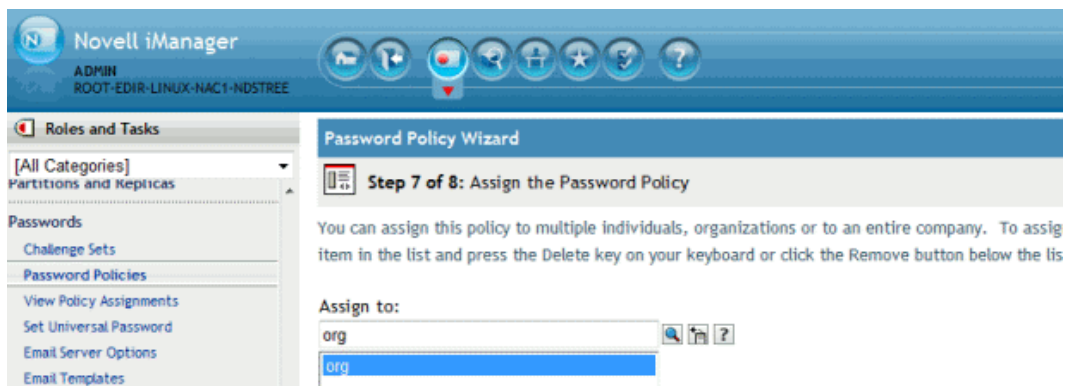
- 3. Establish a universal password policy to be assigned to the organization or specific unit within the organization.
 - a. Create a new Password Policy for the organization that will be used to enable universal passwords.



- b. Select the option to enable Universal Passwords and deselect the option Enable the Advanced Password Rules.



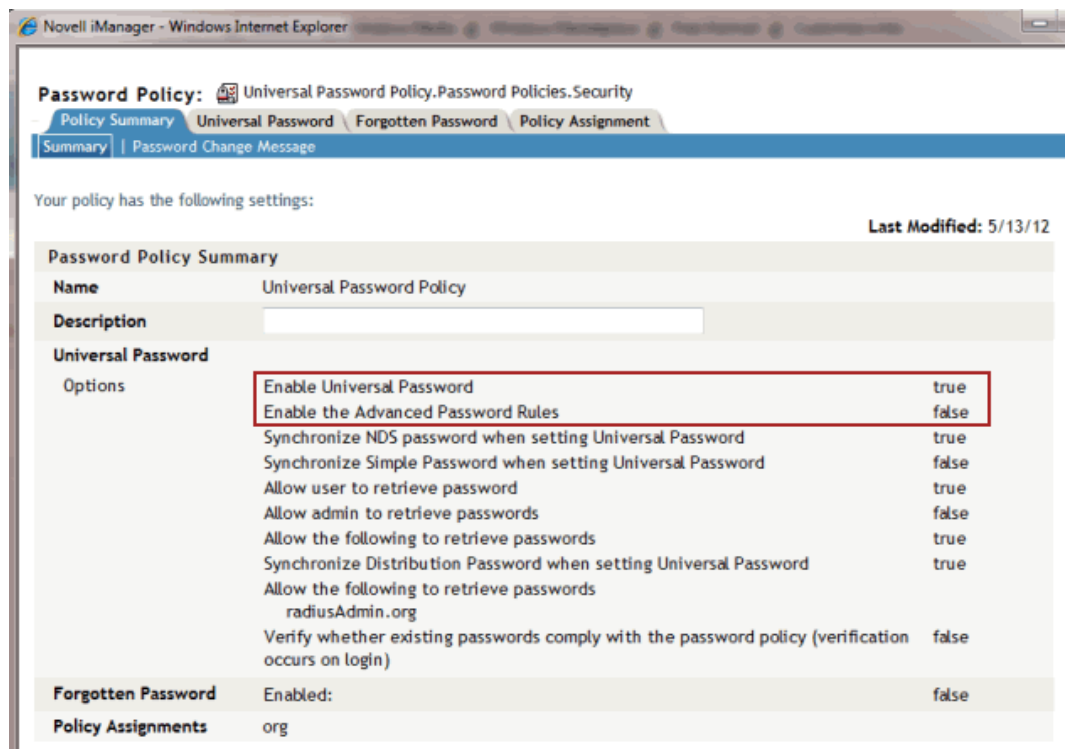
- c. Select the appropriate object in the Novell tree that the Universal Password Policy will be applied to.



The following screen shot shows a completed Universal Password Policy.

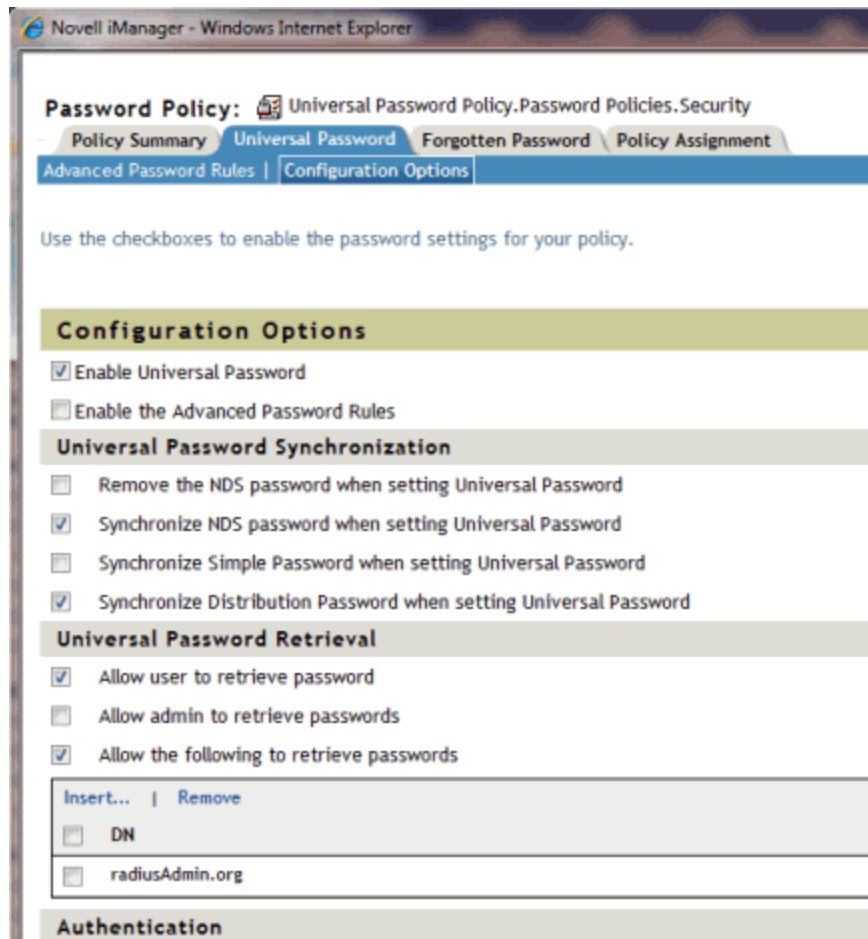


The following screen shot shows the Universal Policy Summary. Note that the Enable Universal Password option is set to true and the Enable the Advanced Password Rules option is set to false.



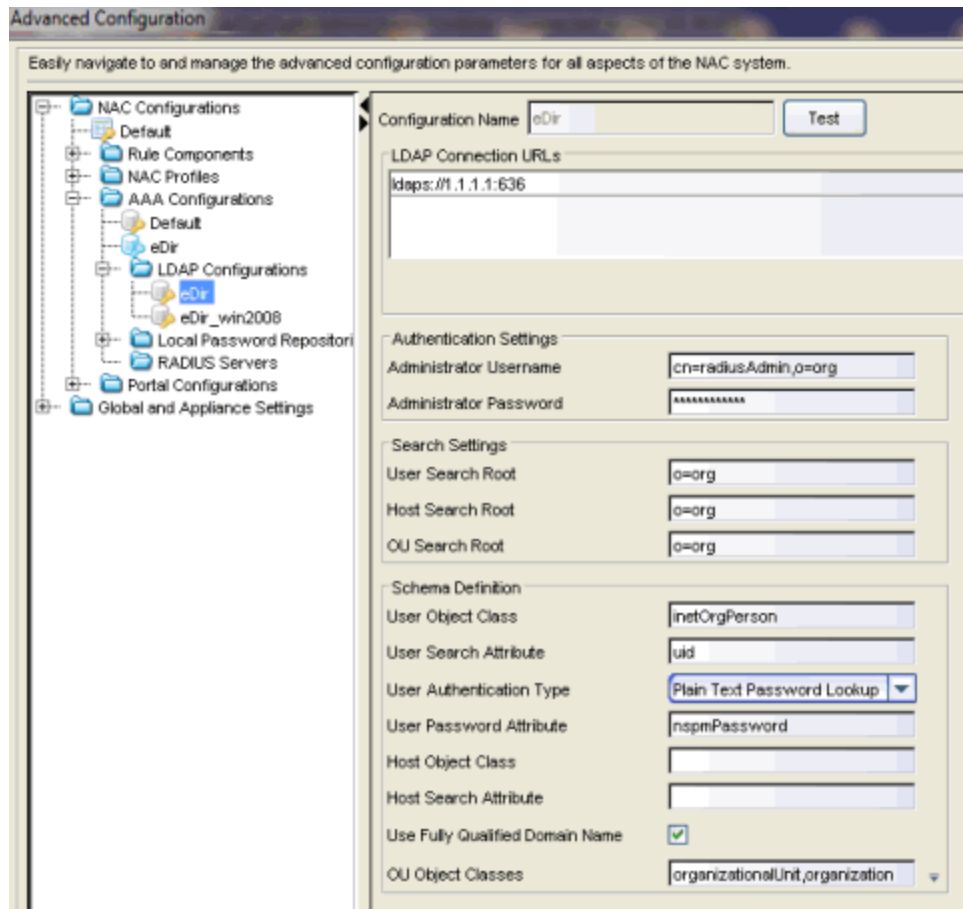
- d. The final step in defining the Universal Password Policy is to enable the option for the radiusAdmin user to retrieve users passwords from

the database.



4. In NAC Manager, create an LDAP configuration that defines access to Novell's eDirectory. The screen shot below shows an LDAP configuration used to authenticate 802.1x PEAP to eDirectory.
 - a. In the [Advanced Configuration window](#), right-click on the LDAP Configurations folder and select Add LDAP Configuration. The Add LDAP Configuration Window opens.
 - b. In the OU Object Classes field, use the configuration menu to select the Populate Novell eDirectory Defaults option.
 - c. Set the User Authentication Type to be Plain Text Password Lookup.

- d. Verify the User Password Attribute is nspmPassword.



- 5. In your Advanced AAA Configuration, add an entry that uses this LDAP configuration. The configuration will allow NAC to verify the user's

password from the PEAP/MsCHAP/MsCHAPv2 request.

The screenshot shows a dialog box titled "Add User To Authentication Mapping". It contains the following fields and settings:

- Authentication Type: Any
- User/MAC/Host: Pattern Group, NAC2003!
- Location: Any
- Authentication Method: LDAP Authentication
- LDAP Authentication Type: Plain Text Password Lookup
- Supported RADIUS Type: All authentication types.
- LDAP Configuration: NAC eDirectory
- LDAP Policy Mapping: Default

Buttons at the bottom: OK, Cancel, Help.

How to Configure PEAP Authentication via OpenLDAP

This Help topic provides instructions for configuring NAC to authenticate PEAP, MsCHAP, and MsCHAPv2 requests by checking the username and password using an OpenLDAP server.

In NAC Manager, create an LDAP configuration that defines access to OpenLDAP.

1. In the [Advanced Configuration window](#), right-click on the LDAP Configurations folder and select Add LDAP Configuration. The Add LDAP Configuration Window opens.
2. In the OU Object Classes field, use the configuration menu to select the Populate OpenLDAP Defaults option.
3. Configure the LDAP configuration to do a password lookup. There are three ways to do this:
 - Have the password encryption on the OpenLDAP server set to use clear text passwords. Then, in your LDAP configuration, set the User Authentication Type field to Plain Text Password Lookup and the User Password Attribute to userPassword (which is the default).
 - Use an NT Hashed password. These encryption types are not supported by OpenLDAP for user passwords, so you must modify your user password update script or web page to set the password for the user, create the desired hash of the password, and set a newly defined attribute to have that value. With this method, the LDAP configuration must use the User Authentication Type of NTHash Password Lookup. You will also need to configure the User Password Attribute to be the attribute you selected for storing the NT Hash or LM Hash of the password.
 - If your NAC deployment only requires authentication via captive portal Registration, then the User Authentication Type should be set to LDAP Bind for ease of deployment.
4. In your Advanced AAA Configuration, add an entry that uses this LDAP configuration (see the example screen shot below). The configuration will allow NAC to verify the user's password from the

PEAP/MsCHAP/MsCHAPv2 request.

The screenshot shows a dialog box titled "Add User To Authentication Mapping". The fields are as follows:

- Authentication Type: Any
- User/MAC/Host: Pattern Group, NAC2003!*
- Location: Any
- Authentication Method: LDAP Authentication
- LDAP Authentication Type: Plain Text Password Lookup
- Supported RADIUS Type: All authentication types.
- LDAP Configuration: NAC OpenLDAP
- LDAP Policy Mapping: Default


Buttons: OK, Cancel, Help

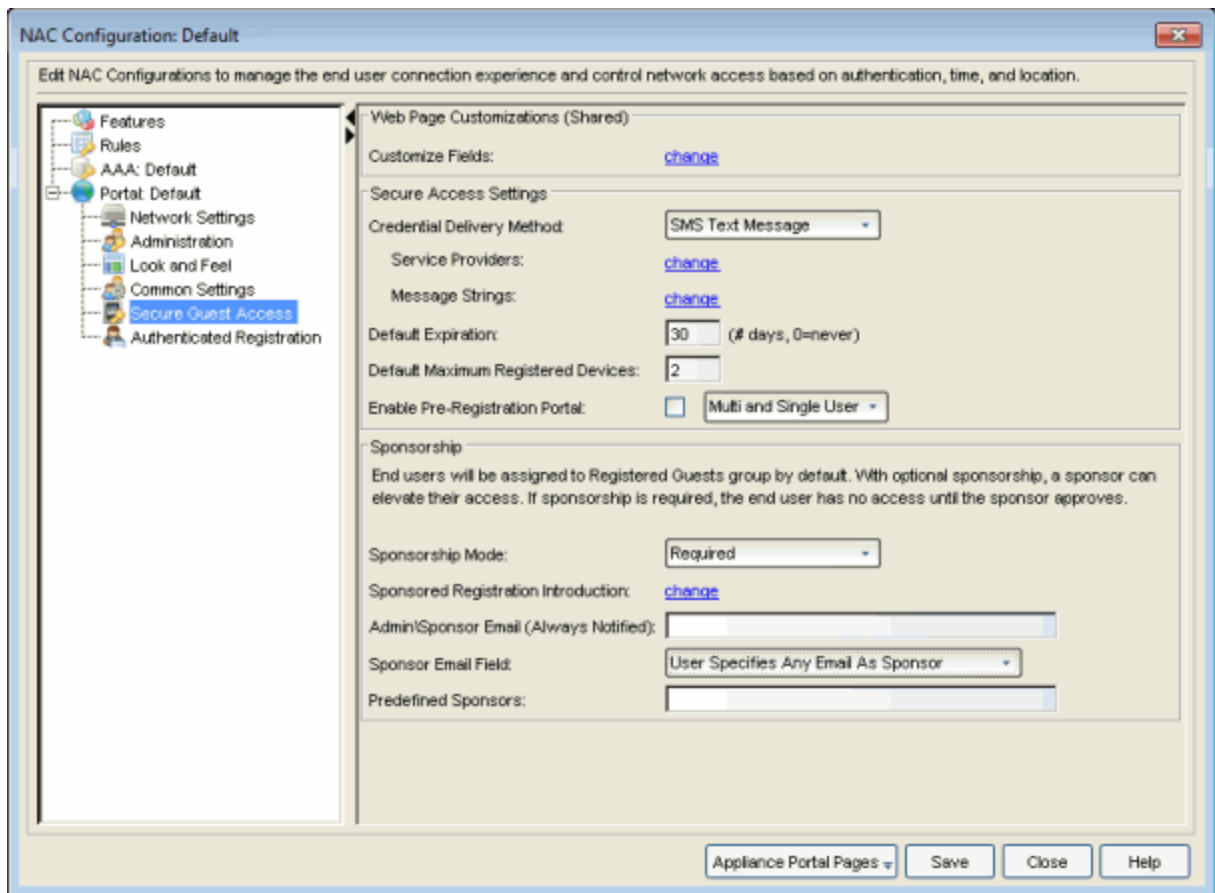
How to Configure Sponsorship for Guest Registration

This topic describes how to configure sponsorship for Guest Registration and Secure Guest Access. Sponsorship is configured as part of your portal configuration, and is accessed from the Guest Registration and Secure Guest Access views in the Portal section of the [NAC Configuration window](#).

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

To configure sponsorship:

1. Use the NAC Manager  toolbar button to open the NAC Configuration window.
2. In the left-panel tree, expand the Portal icon and click on the [Guest Registration](#) view or the [Secure Guest Access](#) view (depending on the access type you are configuring). The screenshot below shows the Secure Guest Access view.



3. In the Sponsorship section, select the **Sponsorship Mode** that will be required. Additional settings will be displayed when you select optional or required sponsorship.
 - **None** - Sponsorship is not required and the end user is assigned to the Registered Guests End-System Group.
 - **Optional** - The end user is assigned to the Registered Guests End-System Group until sponsored. At that time, the sponsor can assign elevated access, if desired.
 - **Required** - The end user has no access until the sponsor approves the registration. The end user is added to the Registration Pending Access end-system group and is presented the sponsorship pending page until approved.
4. **Sponsored Registration Introduction** - Click the "change" link to open a window where you can edit the introductory message displayed to the end user.

5. **Admin\Sponsor Email** - Enter the person or group to notify when an end user requests sponsorship, typically the network NAC administrator, for example "IT@CompanyA.com." This email address is always notified, in addition to the sponsor email address that is entered by the end user when they register to the network.
6. **Sponsor Email Field** - Select an option for the sponsor email field on the registration web page.
 - **Do Not Display** - The field will not be displayed, and the end user will not be required to enter a sponsor email address. In this case, only the admin\sponsor email address (defined above) will be notified when the end user registers.
 - **Display Predefined Sponsor List** - The end user must select a sponsor email from a list of predefined sponsors (defined below). The end user will see a drop-down list of sponsor email addresses and select the appropriate sponsor.
 - **User Specifies Any Email as Sponsor** - The end user can enter any email address as a sponsor's email address.
 - **User Must Specify Predefined Sponsor Email** - The end user must enter an email address that matches one of the predefined sponsors (defined below).
7. **Predefined Sponsors** - Enter one or more sponsor email addresses. If you have selected "Display Predefined Sponsor List" as your Sponsor Email Field option (above), these addresses will be presented to the end user as a drop-down list, allowing them to select a sponsor email address. If you have selected "User Must Specify Predefined Sponsor Email" as your Sponsor Email Field option, then the sponsor email address entered by the end user must match an email address listed here. Email addresses can be separated by semi-colons (;) or commas (,) for example, jdoe@CompanyA.com;smith@CompanyA.com. Because commas are accepted separators, they should not be used in actual email addresses.
8. In the NAC Configuration window, click **Save** to save your changes. You will need to enforce the new portal configuration to your appliance(s).

Related Information

For information on related help topics:

- [NAC Configuration Window](#)
- [Portal Configuration](#)

How to Configure Verification for Guest Registration

Guest registration requires end users to enter their name and contact information on a Registration web page in order to gain access to the network. However, in many cases, end users provide false names and contact information because they don't want their personal information to be used for other purposes. In those cases, network administrators do not have a way to contact the user in the event of an Acceptable Use Policy (AUP) violation or in the case of an emergency.

With verification, guest end users registering to the network are required to enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user.

Configuration Steps

The verification feature is supported for both Guest Registration and Guest Web Access, and is configured using the Verification Method options in your portal configuration. Depending on the verification method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

The following table provides a description of each verification method and lists their custom field requirements.

User Verification Method	Description	Custom Field Requirement
Email	The end user must enter a valid email address on the Registration web page or Guest Web Access login page.	The Email Address Custom Field must be set to Required .

User Verification Method	Description	Custom Field Requirement
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to Required .
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to Visible .
SMS Text Message	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to Required .
SMS Text or Email	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to Visible .

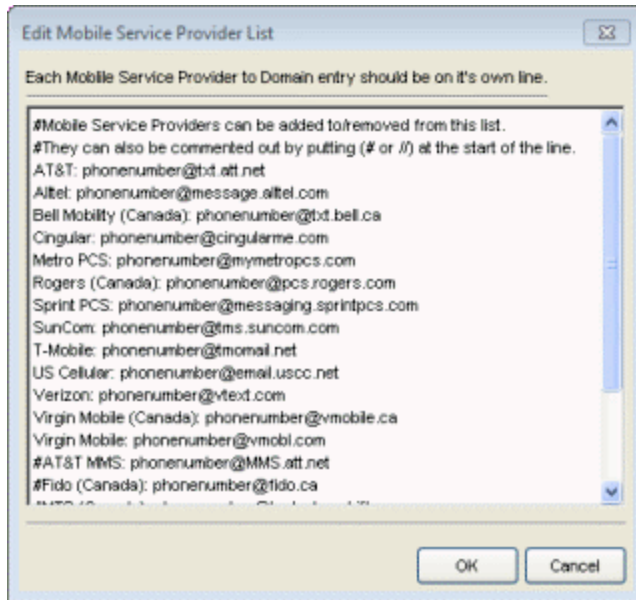
Use the following steps to configure verification in your portal configuration.

1. In NAC Manager, [access the Portal Configuration](#). Click on the Guest Registration or Guest Web Access selection in the Portal Configuration tree, depending on what access type your network is using. (If you don't see these selections, click Features in the tree and enable the appropriate feature.)
2. In the Guest Registration or Guest Web Access panel, use the drop-down menu to select the desired Verification Method (refer to the [table](#) above). The Guest Registration panel is shown below.

The screenshot displays a configuration interface for guest registration, organized into several sections:

- Web Page Customizations (Shared):** Includes links for "Introduction Message" and "Customize Fields", both labeled "change".
- Redirection (Shared):** Features a "Redirection" dropdown menu set to "Use Network Settings Redirection" and a text input field containing "http://www.enterasys.com".
- Registration Settings:** This section is highlighted with a red box and contains:
 - Verification Method:** A dropdown menu currently showing "SMS Text or Email".
 - Service Providers:** A link labeled "change".
 - Message Strings:** A link labeled "change".
 - Default Expiration:** A text input field with "30" and the label "(# days, 0=never)".
 - Enable Survivable Registration:** An unchecked checkbox.
- Sponsorship:** Includes a descriptive paragraph: "End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves." and a "Sponsorship Mode" dropdown menu set to "None".

3. If you selected the "SMS Text Message" or the "SMS Text or Email" User Verification method, click the Service Providers "change" link to configure the list of mobile service providers from which end users can select on the Registration web page or Guest Web Access login page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.



You can comment out entries by preceding each line with either a # or // to allow temporary editing of the file without removing the text.

The list requires one service provider entry per line, using the following format: <Provider>;phonenumber@<specificdomain>.

When the end user registers, they will see only the <Provider> portion in the drop-down list of providers on the Registration web page.

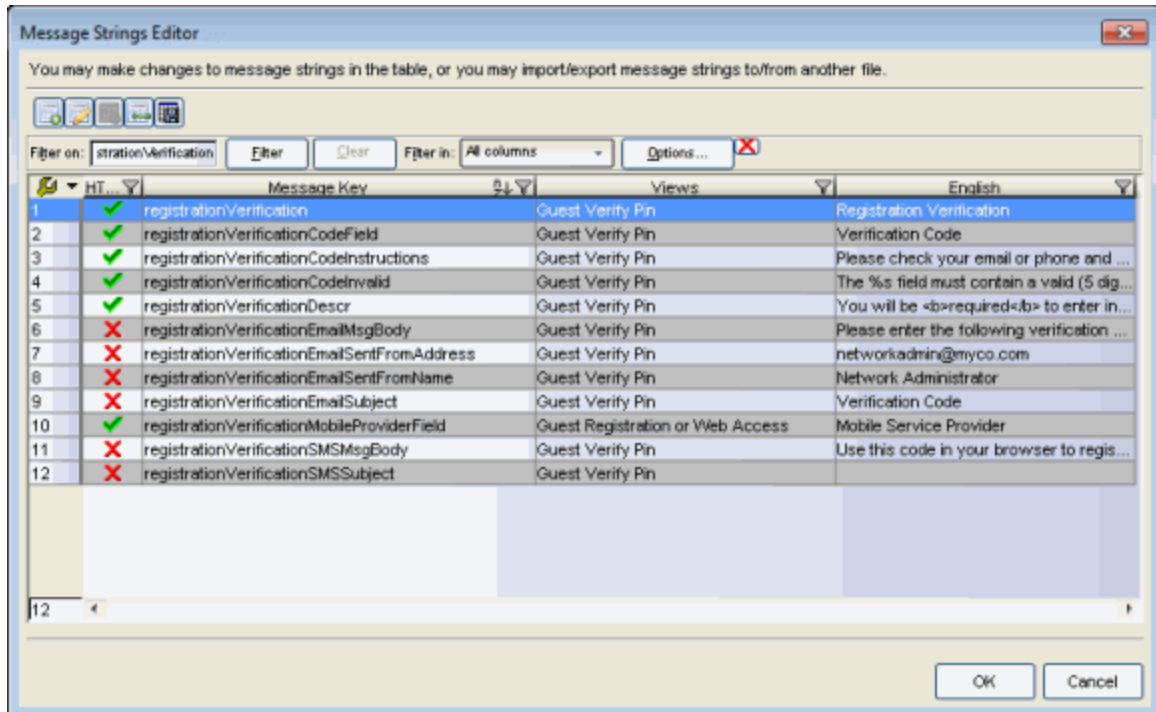
Click **OK** to close the window.

4. If you have selected the "SMS Gateway" or "SMS Gateway or Email" method, enter the SMS Gateway Email address provided by the SMS Gateway provider.

The screenshot shows a configuration page with several sections:

- Web Page Customizations (Shared)**
 - Introduction Message: [change](#)
 - Customize Fields: [change](#)
- Redirection (Shared)**
 - Redirection: Use Network Settings Redirection (dropdown) |
- Registration Settings** (highlighted with a red box)
 - Verification Method: SMS Gateway (dropdown)
 - SMS Gateway Email:
 - Message Strings: [change](#)
- Default Expiration:** 30 (# days, 0=never)
- Enable Survivable Registration:**
- Sponsorship**
 - End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.
 - Sponsorship Mode: None (dropdown)

5. For all methods, click on the Message Strings "change" link to open the [Message Strings Editor](#) where you can customize the text displayed on the Registration web page or Guest Web Access login page, and the messages sent to the end user.



You will need to modify different message strings sent to the end user, depending on the verification method or methods you selected. Double-click on the message to open a window where you can edit the message text.

- **Email** - This method uses the following strings:
 - registrationVerificationEmailMsgBody - the default message shouldn't need to be changed.
 - registrationVerificationEmailSentFromAddress - you will need to change the default message to the appropriate email address for your company.
 - registrationVerificationEmailSentFromName - the default message shouldn't need to be changed.
 - registrationVerificationEmailSubject - the default message shouldn't need to be changed.
- **SMS Gateway** - Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone

number.

- registrationVerificationSMSMsgBody
- registrationVerificationSMSSubject
- **SMS Text Message** - This method uses the following strings. The default messages shouldn't need to be changed.
 - registrationVerificationSMSMsgBody
 - registrationVerificationSMSSubject

Click **OK** to close the window.

6. In the Web Page Customizations (Shared) section, click the Customize Fields "change" link to open the Manage Custom Fields window.

The screenshot shows a configuration window titled "Web Page Customizations (Shared)". It is divided into several sections:

- Introduction Message:** Includes a "change" link.
- Customize Fields:** This section is highlighted with a red rectangular box and also has a "change" link.
- Redirection (Shared):** Features a "Redirection:" dropdown menu set to "Use Network Settings Redirection" and a text input field containing "http://www.enterasys.com".
- Registration Settings:** Contains a "Verification Method:" dropdown menu set to "SMS Gateway", an "SMS Gateway Email:" text input field, "Message Strings:" with a "change" link, a "Default Expiration:" spinner box set to "30" with the text "(# days, 0=never)", and an "Enable Survivable Registration:" checkbox which is currently unchecked.
- Sponsorship:** Includes a descriptive paragraph: "End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves." and a "Sponsorship Mode:" dropdown menu set to "None".

7. Set the appropriate custom fields to display on the Registration web page or Guest Web Access login page, depending on the verification method you selected (refer to the [table](#) above). When you save your portal changes, the correct configuration of the custom fields will be verified. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type will also change

them for the others. For more information, see the [Manage Custom Fields Window](#).

Field	Visible	Required	Display String
First Name:	Visible	<input checked="" type="checkbox"/>	
Middle Name:	Visible	<input type="checkbox"/>	
Last Name:	Visible	<input checked="" type="checkbox"/>	
Email Address:	Visible	<input checked="" type="checkbox"/>	
Phone Number:	Visible	<input checked="" type="checkbox"/>	
1st Custom:	Not Visible	<input type="checkbox"/>	
2nd Custom:	Not Visible	<input type="checkbox"/>	
3rd Custom:	Not Visible	<input type="checkbox"/>	
4th Custom:	Not Visible	<input type="checkbox"/>	
5th Custom:	Not Visible	<input type="checkbox"/>	
Device Description:	Not Visible	<input type="checkbox"/>	

Acceptable Use Policy: Display [change](#)

Note: Custom Display String fields are common between Unauthenticated and Authenticated Registration types. Modifying a Display String for one Registration type will affect the Display String in the other.

OK Cancel Help


Click **OK** to close the window.

- Back in the Portal Configuration, click **Save** to save your changes. Close the NAC Configuration window. Enforce the new portal configuration to your appliance(s). Verification is now configured for your guest registration.

How User Verification Works

When a guest attempts to access the network, the Registration web page or Guest Web Access login page asks for their email address and/or phone number and mobile service provider, along with their normal contact information.

Welcome to the Enterprise Registration Center



You have been **denied** network access because this device is not registered to the network.

To obtain network access, you **must** complete registration using the form below

By registering to the network, you are **agreeing** to the terms and conditions explained in the [Enterprise Network and Computer Acceptable-Use Policy](#)

You will be **required** to enter in a verification code that will be sent to your specified contact information.

Company's Acceptable Use Policy

Introduction

This Acceptable Use Policy (AUP) sets forth the principles that govern the use by customers of the Web-based products and services provided by Company. This AUP is designed to help protect our customers, and the Internet community, from irresponsible, abusive or illegal activities.

*First Name:

Middle Name:

*Last Name:

E-Mail Address:

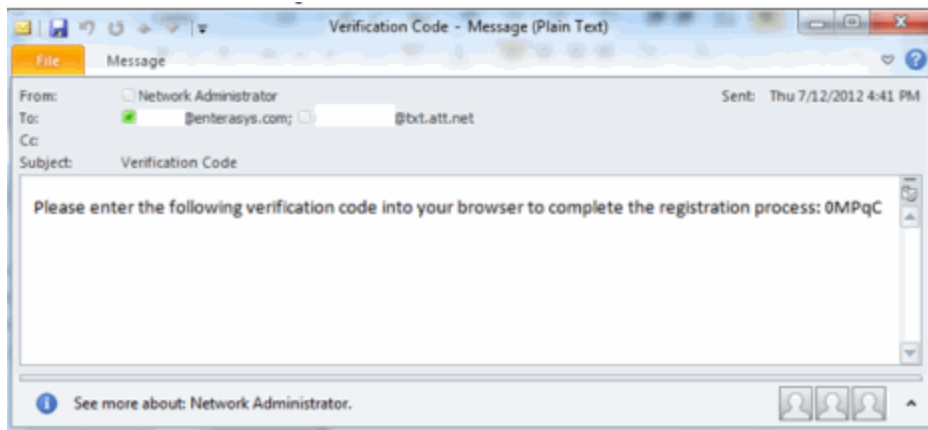
Phone Number:

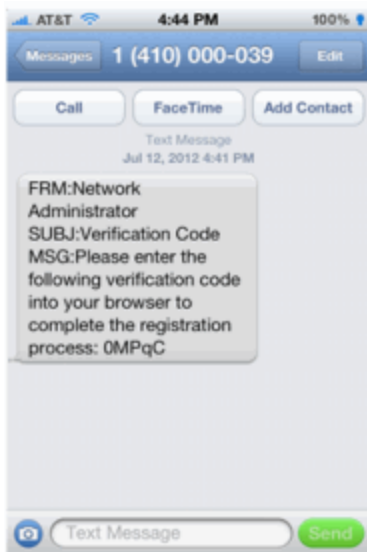
*Mobile Service Provider:

*I agree to the Acceptable Use Policy

Please press the Complete Registration button only once.


When they click the **Complete Registration** button, they are sent a verification code via an email or a phone text message.





The web page then prompts them for the code. When they enter the correct code that was generated for them and click the **Complete Registration** button, they are allowed access to the network. The verification code is valid for 15 minutes and cannot be reused once it is validated.

Welcome to the Enterprise Registration Center



Please check your email or phone and enter in the verification code that was sent to .

*Verification Code:

Complete Registration

Please press the Complete Registration button only once.

Related Information


For information on related help topics:

- [Portal Configuration](#)

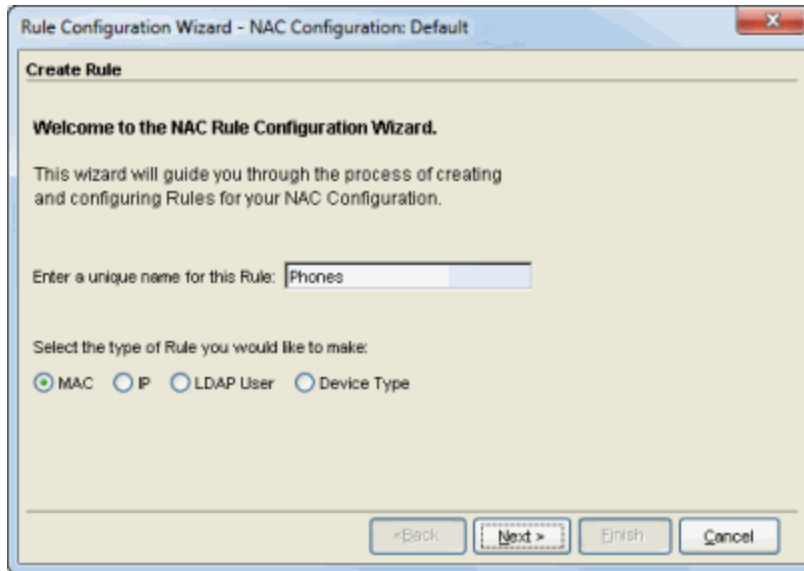
How to Create a Rule

A NAC Configuration contains rules that provide very granular control over how end-systems are treated as they come onto the network. When end-systems match a rule's criteria, they are assigned the NAC profile that is specified in the rule. To create rules, you can use the NAC Rule Configuration Wizard, which guides you through the process of creating and configuring rules for your NAC configuration, or you can create rules manually, using the [Create Rule window](#).

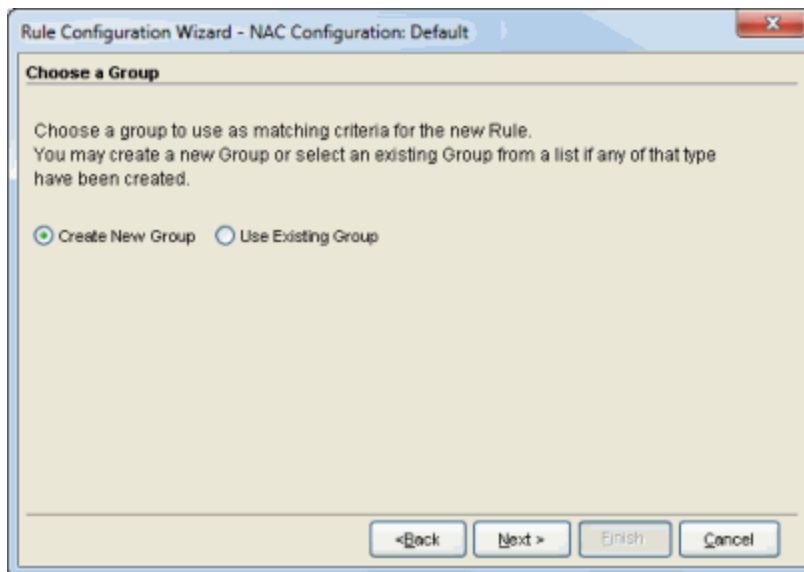
This Help topic describes how to use the NAC Rule Configuration wizard to create your rules.

1. Open the [Edit NAC Configuration window](#), and launch the wizard from the  button in the rules section.
2. In the **Create Rule** window, enter a name for the rule and select a rule type:
 - MAC - the rule will be based on a group of MAC addresses, MAC OUIs, or MAC Masks.
 - IP - the rule will be based on a group of IP addresses or subnets.
 - LDAP User - the rule will be based on a group of LDAP users imported from an LDAP Server, organized by Organization Unit (OU).
 - Device Type - the rule will be based on an operating system family, an operating system, or a hardware type, such as Windows, Windows 7, Debian 3.0, and HP Printers.

Click **Next**.



3. In the **Choose a Group** window, select a group to use as matching criteria for the new rule. To use an existing group, select the **Use Existing Group** radio button, select the group from the drop-down menu, and click **Next**. To create a new group, use the following instructions.



Create a New Group

- a. Select the **Create New Group** radio button and click **Next**.
- b. In the **Create a Group** window, enter a name and description for the group. Select **Add Entries to Group** to populate the group with entries to use for matching. Click **Next**.

The screenshot shows the 'Create a Group' window in the 'Rule Configuration Wizard - NAC Configuration: Default'. The window title is 'Rule Configuration Wizard - NAC Configuration: Default'. The main heading is 'Create a Group'. Below the heading, it says 'Create a new group to use as matching criteria for the Rule.' There are three input fields: 'Name' with the value 'Phones', 'Group Description' with the value 'The list of MAC OUIs for phones', and 'Add Entries to Group' which is checked. At the bottom, there are four buttons: '<Back', 'Next >', 'Finish', and 'Cancel'.

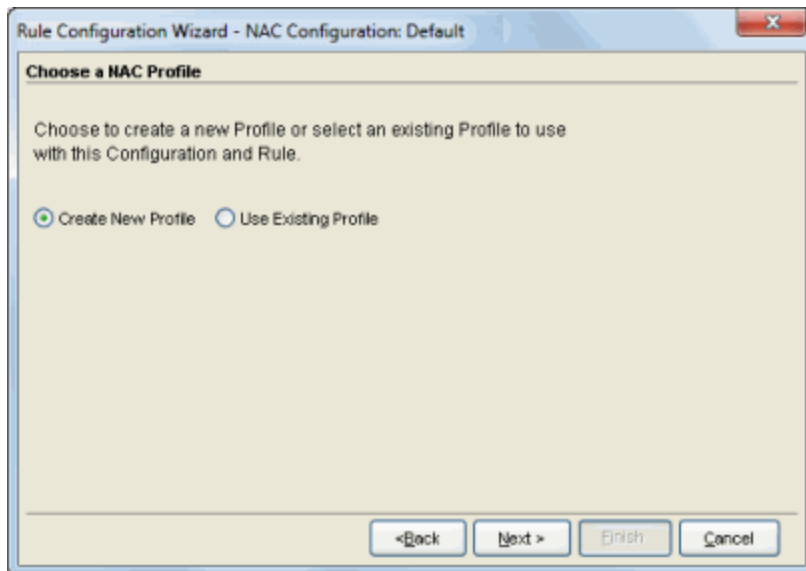
- c. In the **Add entries to the group** window, use the buttons to create a list of entries to use for matching criteria. Click **Next**.

The screenshot shows the 'Add entries to the group' window in the 'Rule Configuration Wizard - NAC Configuration: Default'. The window title is 'Rule Configuration Wizard - NAC Configuration: Default'. The main heading is 'Add entries to the group'. Below the heading, it says 'Populate a new group with entries to use for matching.' There is a section for 'End-System Group' with a filter field and a table of entries. The table has three columns: 'MAC Based Values', 'Entry Description', and 'Custom 1'. The entries are:

MAC Based Values	Entry Description	Custom 1
Siemens Enterprise Communications GmbH...	Siemens Phone MAC	
Cisco Systems (00:14:F2)	Cisco Phone MAC OUI	

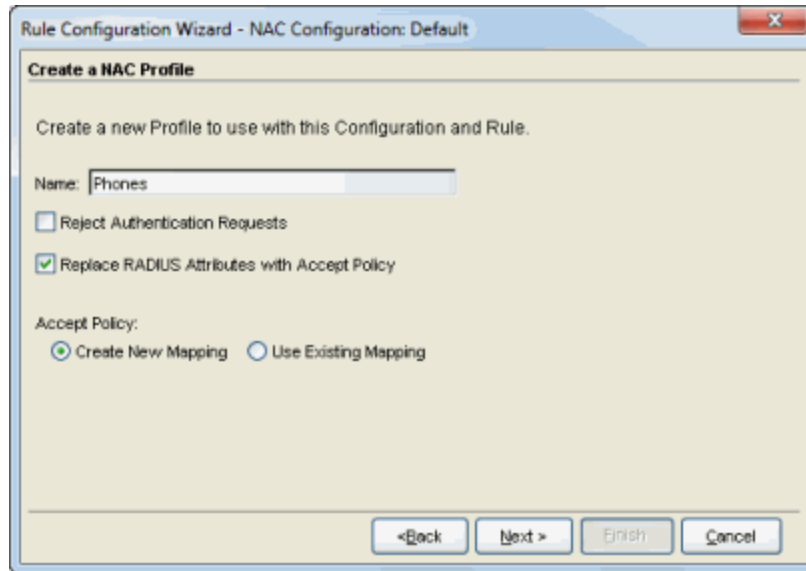
At the bottom, there are four buttons: '<Back', 'Next >', 'Finish', and 'Cancel'.

4. In the **Choose a NAC Profile** window, select a profile to assign to end-systems that match the rule's criteria. To use an existing profile, select the **Use Existing Profile** radio button, select the profile from the drop-down menu, and click **Next**. To create a new profile, use the following instructions.



Create a New Profile

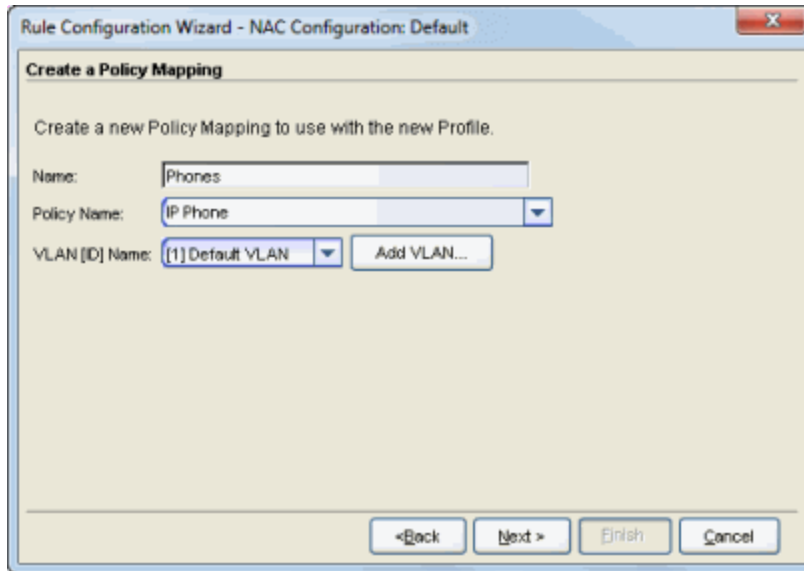
- a. Select the **Create New Profile** radio button and click **Next**.
- b. In the **Create a NAC Profile** window, enter a name for the profile and configure the following values.



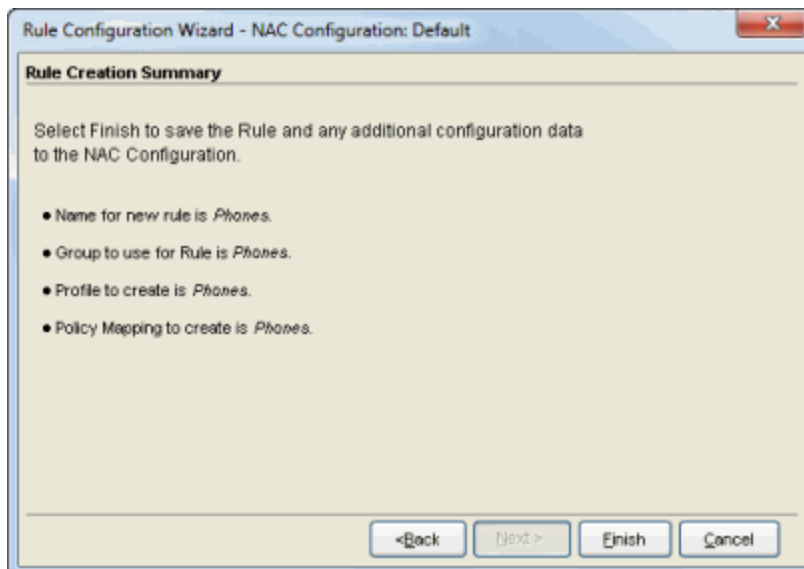
- **Reject Authentication Requests** - If you check this checkbox, all authentication requests from end-systems that match this rule will be rejected.
- **Replace RADIUS Attributes with Accept Policy** - When this option is checked, the attributes returned from the RADIUS server are replaced by the policy designated as the Accept policy.
- **Accept Policy** - Select the policy you want to map as the Accept policy for this NAC profile. NAC Manager provides ten policy names that are automatically associated with the Default VLAN [1]. You can select one of these existing mappings or add a new mapping.

Click **Next**.

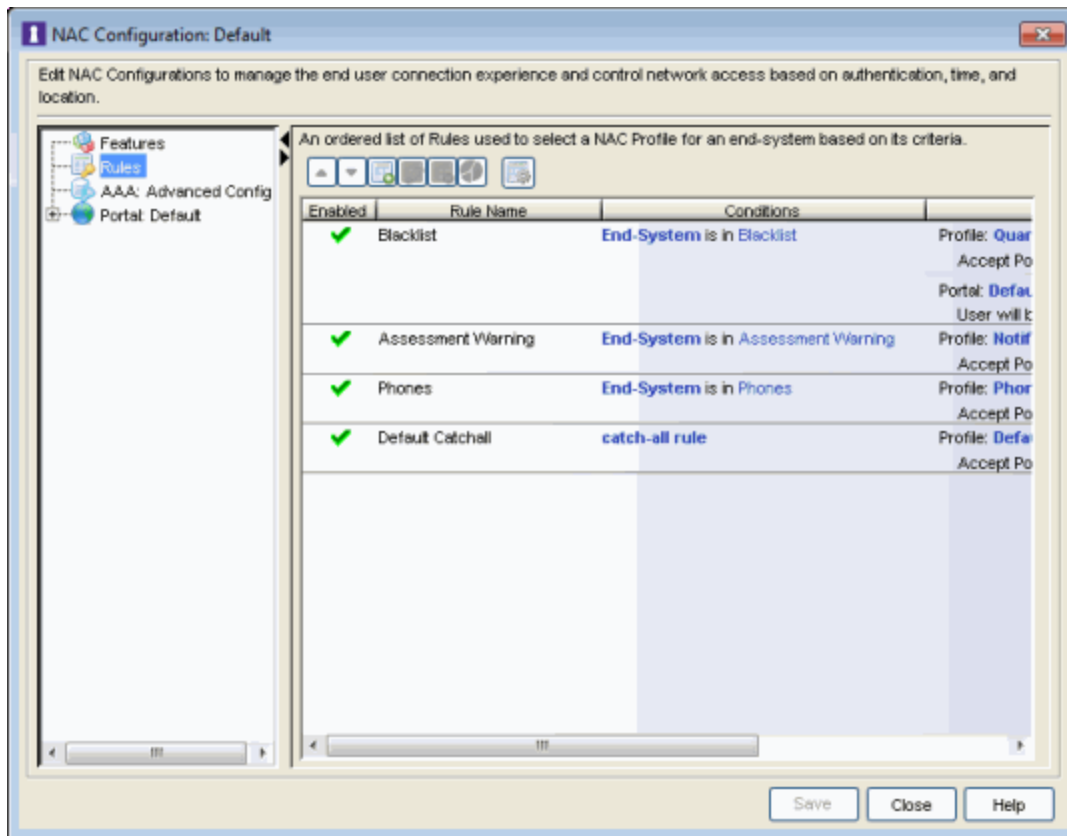
- c. If you are creating a new policy mapping, you will see the **Create a Policy Mapping** window where you can add a new policy. Enter a name for the policy mapping and configure its associated attributes. Refer to the [Add/Edit Policy Mapping Window](#) Help topic for information on the different attributes. Click **Next**.



5. In the **Rule Creation Summary** window, review your rule configuration and click **Finish**.



The rule is displayed in the rules section of the NAC Configuration.



Related Information

For information on related windows:

- [Create/Edit Rule Window](#)
- [Edit NAC Configuration Window](#)

How to Deploy Extreme Access Control in an MSP or MSSP Environment

This Help topic presents instructions for deploying Extreme Access Control (Access Control) within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment. It includes the following information:

- [Configuring Extreme Management Center Behind a NAT Router](#)
- [Defining Interface Services](#)

Configuring Extreme Management Center Behind a NAT Router

If the Extreme Management Center (Management Center) server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the `nat_config.text` file that defines the real IP address for the Management Center server. This allows the Management Center server to convert the NAT IP address received in the Access Control engine response to the real IP address used by the Management Center server.

NOTE: The text in the `nat_config.text` file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the Management Center server, add the following entry to the `<install directory>/appdata/nat_config.text` file.
`<NAT IP address>=<real IP address>`
2. Save the file.
3. Configure your Access Control engines to use the NAT IP address for the IP address of the Management Center server. For information on how to configure or change your engine settings, refer to your Access Control engine Installation Guide.

If you have remote Management Center clients connecting to the NAT IP address, perform the following additional steps.

1. On the Management Center (formerly NetSight) server, add the following text to the `<install directory>/appdata/NSJBoss.properties` file. In the


```
second to last line, specify the hostname of the Management Center server.  
# In order to connect to a NetSight server behind a NAT fi  
rewall or a  
# NetSight server with multiple interfaces you must define  
these two  
# variables on the NetSight server. The java.rmi.server.ho  
stname  
# should be the hostname  
(not the IP) if multiple IPs are being used  
# so that each client can resolve the hostname to the corr  
ect IP that  
# they want to use as the IP to connect to.  
java.rmi.server.hostname=<hostname of Management Center  
(NetSight) server>  
java.rmi.server.useLocalHostname=true
```

2. Save the file.
3. Add the Management Center server hostname to your DNS server.

Defining Interface Services

The advanced interface configuration mode available in NAC Manager allows you to define which services are provided by each of the Access Control engine's interfaces. This provides the very granular out-of-band management that is often required in MSP or MSSP environments.

For instructions, see the [Interface Configuration Window](#) Help topic.

Related Information

For information on related windows:

- [Interface Configuration Window](#)

How to Display End-System Registration and Group Information

This Help topic describes how to display registration and group membership information in the [End-Systems tab](#), the [Control tab End-Systems view](#), and the [Edit End-System Group window](#) for MAC-based groups. By enabling additional columns in these views, the following information can be displayed:

- **Registered User.** The registered username supplied by the end user during the registration process.
- **Registered Email.** The email address supplied by the end user during the registration process.
- **Sponsor.** The registered device's sponsor.
- **Custom registration information.** This is information supplied by the end user during the registration process. There are five custom fields that can be configured using the Customize Fields options in the [Edit Portal Configuration window](#).
- **Registered device description.** This is a device description supplied by the end user during the registration process. The Device Description Portal field can be configured using the Customize Fields options in the [Edit Portal Configuration window](#).
- **End-System Group Entry Descriptions.** These are the entry descriptions that are entered when adding a new entry to a MAC-based [end-system group](#). (These columns are not available in the Edit End-System Group window.)

Use the following steps to enable the display of this information:

- **To enable columns in the End-Systems tab:**
 - a. Right click on any row in the End-Systems table and select Table Tools > Settings. The Table Settings window opens.
 - b. In the Columns tab, scroll down and deselect the "Hide" checkbox for the columns you wish to display:
 - Registered User - the registered username.
 - Registered Email - the registered email address.
 - Sponsor - the registered device's sponsor.

- Registration 1-5 - the custom registration fields defined for the registration web page.
 - Registration Descr - the registered device description.
 - Group 1-3 - for end-system group entry descriptions, up to three groups per end-system.
- **To enable columns in the Control tab End-Systems view:**
 - a. Click on any column heading drop-down arrow and select the Columns option from the menu.
 - b. Scroll down the list and select the following columns:
 - Registered User - the registered username.
 - Registered Email - the registered email address.
 - Sponsor - the registered device's sponsor.
 - Registration 1-5 - the custom registration fields defined for the registration web page.
 - Registration Descr - the registered device description.
 - Group 1-3 - for end-system group entry descriptions, up to three groups per end-system.
- **To enable columns in the Edit End-System Group window (for MAC-based groups):**
 - a. Right click on any column heading in the entry table and select Table Tools > Settings. The Table Settings window opens.
 - b. In the Columns tab, deselect the "Hide" checkbox for the columns you wish to display:
 - Registered User - the registered username.
 - Registered Email - the registered email address.
 - Sponsor - the registered device's sponsor.
 - Registration 1-5 - the custom registration fields defined for the registration web page.
 - Registration Descr - the registered device description.

Related Information

- [End-Systems Tab](#)
- [End-Systems View](#)

How to Enable RADIUS Accounting

This Help topic describes how to use RADIUS accounting to provide real-time end-system connection status in NAC Manager. RADIUS accounting collects various end-system session data that NAC Manager uses to determine connection status for each end-system session. This can be useful for compliance purposes, allowing you to determine both when an end-system session started and when it was terminated.

RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. (For more information, see the [Auth. Access Type](#) section of the Add/Edit Switch Window Help topics.)

You must be running NAC Appliance version 4.0 or higher to take advantage of RADIUS accounting functionality in NAC.

For Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series), NAC uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on the switch. Before enabling RADIUS accounting on these devices, please read through [Considerations for Fixed Switching Devices](#) below.

NOTES: RADIUS accounting is not supported on the NAC Controller.

If RADIUS accounting is not desired, or if it is not supported on certain devices on your network, you can use the [Session Deactivate Timeout option](#) to provide more up-to-date information about which end-systems are still active on the network. This option is enabled on the Reauthentication Tab in the [Appliance Settings window](#).

Use the following steps to enable RADIUS accounting:

1. Enable RADIUS accounting on your switches and controllers using the instructions appropriate for your devices.

For Extreme Networks devices or ExtremeWireless Controller devices running firmware version 9.21.x.x or newer:

- a. **If you are editing an existing device:** In the right-panel **Switches** tab, select the devices you want to perform RADIUS accounting and click

the **Edit** button. The Edit Switches in NAC Appliance Group window opens.

If you are adding a new device: Click **Add** in the right-panel **Switches** tab and the Add Switches to NAC Appliance Group window opens.

NOTE: Wireless Controllers must be running in Strict mode to use RADIUS accounting.

- b. Set the RADIUS Accounting option to **Enabled**. Click **OK**.
- c. Enforce to your appliances.

For ExtremeWireless Controller devices running firmware versions older than 9.21.x.x:

- a. RADIUS accounting must be enabled manually on the controller using the ExtremeWireless Assistant or the device CLI (command line interface).
- b. Be sure to configure the NAC appliance IP address as the IP address of the RADIUS server. Refer to your wireless controller User Guide for instructions on enabling RADIUS accounting via the ExtremeWireless Assistant, or the CLI Reference Guide for the exact CLI command syntax to use.

For third-party switching devices:

- a. RADIUS accounting must be enabled manually on the device using the device CLI (command line interface).
 - b. Be sure to configure the NAC appliance IP address as the RADIUS accounting server. Refer to your device documentation for the exact command syntax.
2. If you are doing RADIUS accounting in a NAC environment where the primary RADIUS server is being used for redundancy in a single NAC appliance configuration (Basic AAA configuration only), then you must enable the Proxy RADIUS Accounting Requests option in the Edit RADIUS Server window.
- a. In the Edit Basic AAA Configurations window, use the Configuration Menu button in the Primary RADIUS Server field to open the Manage RADIUS Servers window.
 - b. Select the RADIUS Server and click **Edit**.

- c. Enable the Proxy RADIUS Accounting Requests option. Click **OK**.
- d. Enforce to your appliance.

With RADIUS accounting enabled, you will now see real-time connection status in the NAC Manager End-Systems tab and Dashboard.

Considerations for Fixed Switching Devices

NAC uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). Due to a limitation on the SNMP interface, the configuration can be read via SNMP, but must be written to the device via CLI. Before enabling RADIUS accounting on these devices, read through the following considerations.

NOTE: These considerations do not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP.

- The devices must be assigned a Device Access profile that provides Write access and includes CLI credentials for Telnet or SSH. Profiles and CLI credentials are configured using the Authorization/Device Access tool's Profile/Credentials tab.
- Before you enforce a new RADIUS server configuration to your fixed switching devices, you should verify that your CLI credentials are configured according to the settings in your new configuration. This is because the Enforce process first writes the RADIUS server configuration to the switch using SNMP, and then writes the RADIUS accounting configuration to the switch using Telnet or SSH. If CLI credentials are not configured according to the new RADIUS server configuration, then the RADIUS accounting configuration will not be written to the switches.

For example, by default you can Telnet to a fixed switching device using username=admin (with no password or a blank password). But, if you configure a new RADIUS configuration with an Auth Access Type (or Realm Type)=Any, then you may need to change the Device Access for the switches to use the IAS credentials, in order for NAC Manager to successfully write the RADIUS accounting information to the switches during Enforce.

Fixed switches only allow one accounting server to be configured. If a primary and secondary NAC gateway are configured for the switch, only the primary

gateway's accounting configuration will be written to the switch. If a secondary gateway is configured, a warning will be displayed.

Considerations for ExtremeXOS Devices

NAC uses CLI access to perform RADIUS accounting configuration operations on ExtremeXOS devices. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

Related Information

- [Add Switches to NAC Appliance Group Window](#)
- [Edit Switches in NAC Appliance Group Window](#)

NAC Enterprise Licensing

NAC Enterprise licensing allows deployment flexibility by providing end-system licensing on a system-wide basis regardless of the number of Extreme Access Control engines. For example, one IA-ES-12K Enterprise license supports 12,000 end-systems across all Access Control engines. The license limits the number of unique end-systems that can be authenticated in a day.

Enterprise licensing is enforced through Extreme Management Center. There are two license components to Enterprise licensing: the NAC Enterprise license and the NAC Enterprise Assessment license.

This Help topic includes the following information about the licenses:

- [Enterprise Licenses](#)
 - [Applying a Enterprise License](#)
 - [Configuring End-System Capacity for an Identity and Access appliance](#)
 - [License Violations](#)
- [Enterprise Assessment Licenses](#)
 - [Applying an Enterprise Assessment License](#)

Contact your sales representative for information on obtaining a NAC Enterprise or NAC Enterprise Assessment license.

Enterprise Licenses

The Enterprise license grants the number of end-systems that can be authenticated in the last 24-hour period.

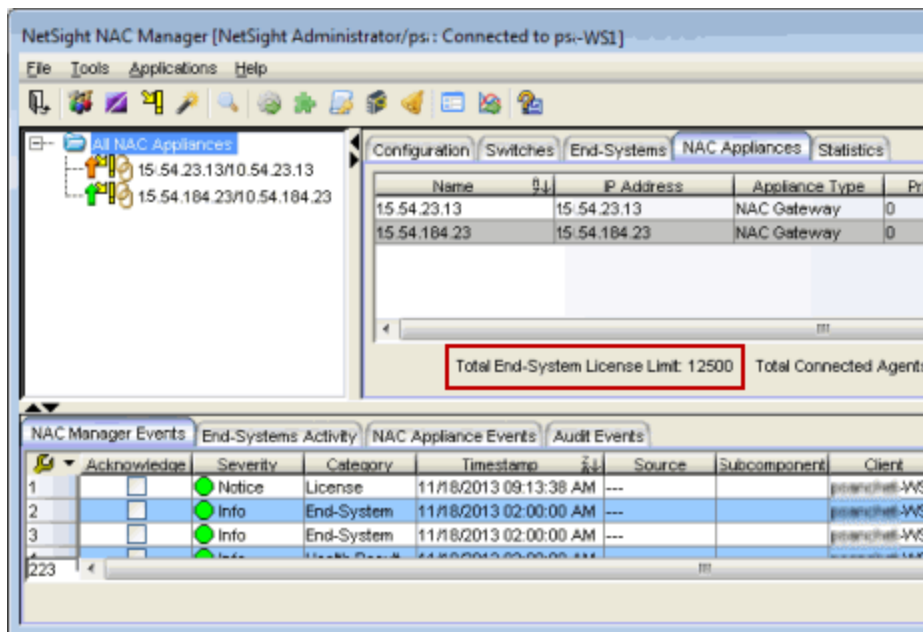
One IA-ES-12K license supports 12,000 end-systems across all Access Control engines.

One IA-ES-3K license supports 3,000 end-systems across all Access Control engines.

One IA-ES-1K license supports 1,000 end-systems across all Access Control engines.

The calculation is based on the number of end-systems granted by the Enterprise license plus the end-system limit for all NAC-A-20, NAC-V-20, and legacy Access Control engines, (including those running a pre-5.0 version). The

NAC Enterprise license can be aggregated by applying additional licenses. The respective end-system limits are dictated by the number of licenses applied. You can view the total end-system license limit for all engines in the [NAC Appliances](#) tab, as shown below.



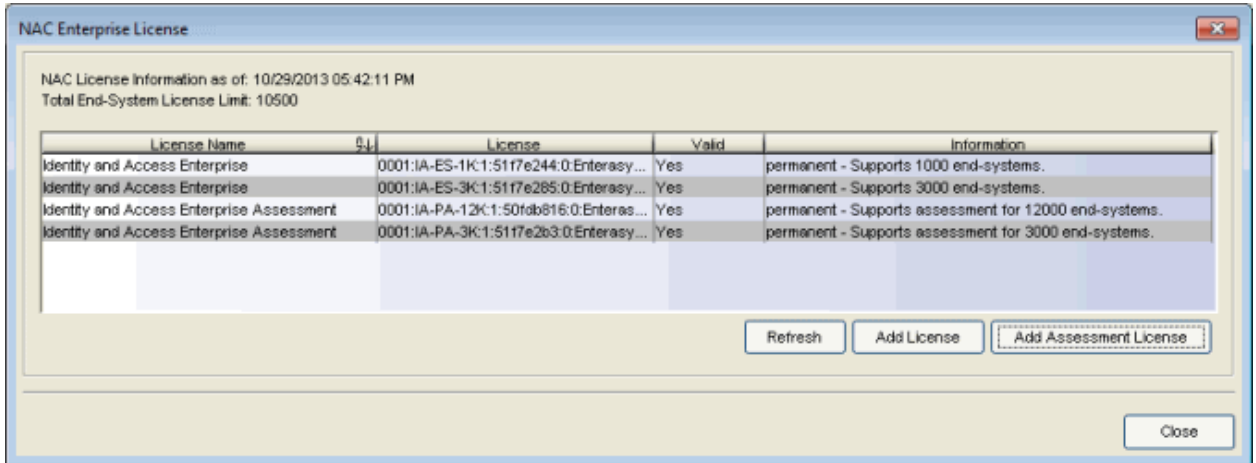
NOTE: The Extreme Management Center (NMS) license allows you to use a virtual Access Control engine, but does not display end-system information. The Management Center Advanced (NMS-ADV) license supports 500 end-systems on a virtual Access Control engine. This number is added to the end-system limit calculation if an Enterprise license or individual virtual engine is installed. (Note that any Access Control virtual engine running a pre-5.0 version still requires an Access Control VM license in the Management Center server.)

Applying an Enterprise License

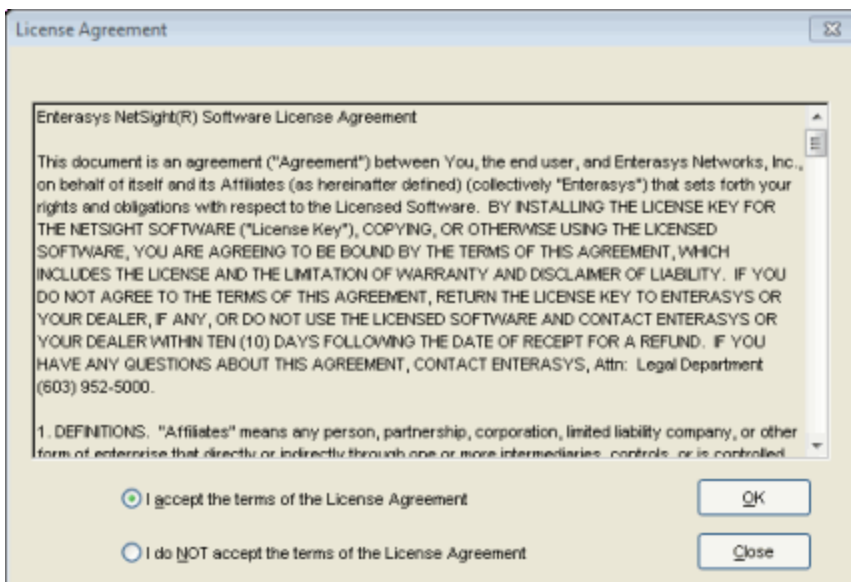
The NAC Enterprise license is applied and updated via NAC Manager. The license is applied to the Management Center server and pushed down to all Access Control engines managed by the server, including hardware Access Control engine.

Use the following steps to apply the license:

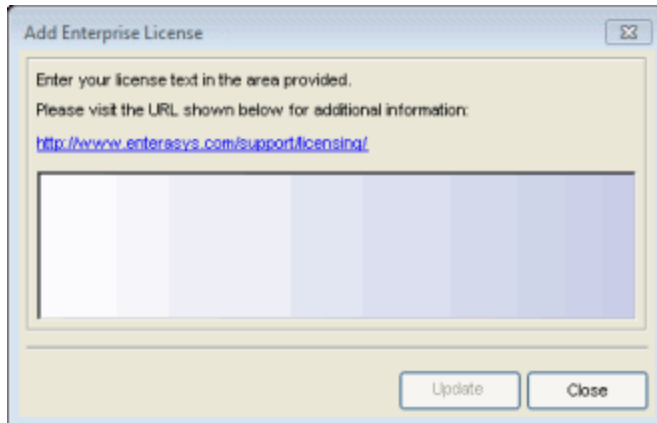
1. From the NAC Manager menu bar, select Tools > Update Enterprise License. The NAC Enterprise License window opens and lists all Enterprise and Enterprise Assessment licenses entered in the system.



2. Click the Add License button.
3. In the License Agreement screen, accept the terms of the agreement and click OK.



4. In the Add Enterprise License window, enter your license text and click Update.



5. Close the NAC Enterprise License window.

The update operation automatically pushes the license to all the Access Control engines running NetSight 5.0 and later. The Enterprise license also automatically gets pushed down to any new engines added to NAC Manager after the Enterprise license has been applied.

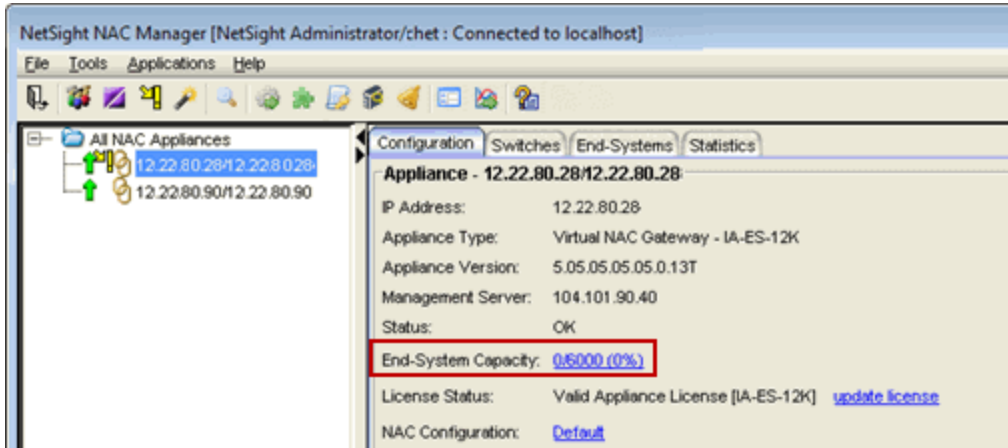
NOTES: While the license is being applied, the engine status in the NAC Manager tree stays orange until the Management Center server can confirm the license has been applied. This may take a few minutes.

If for some reason the license is not pushed to an engine, you can use the Update License link available in the License Status field on the engine [Configuration tab](#) to update the license on a particular engine.

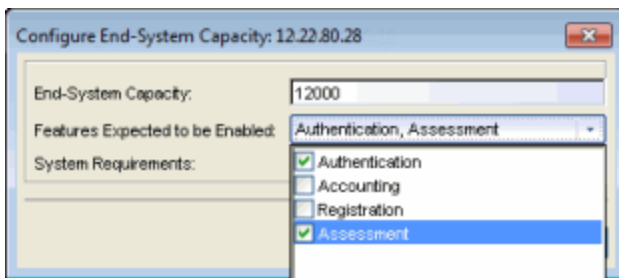
Configuring End-System Capacity for an Extreme Access Control Engine

You can configure the end-system capacity for an individual engine via NAC Manager. The default or configured Access Control engine capacity is used to tune the Access Control engine resources. If you do not configure the capacity using these steps, the capacity will be calculated according to the number of end-systems supported by the engine model.

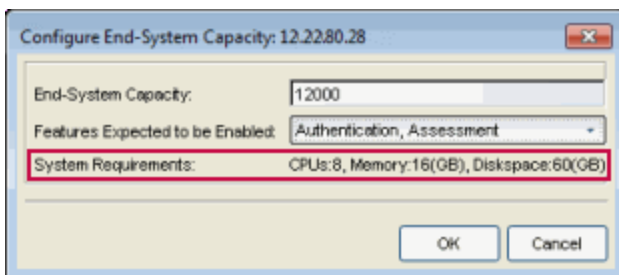
1. In the Access Control engine Configuration tab, click on the End-System Capacity link to open the Configure End-System Capacity window.



2. Enter the desired end-system capacity and specify the features expected to be enabled on the engine including Authentication, Accounting, Registration, and Assessment. Note that the number of end-systems supported on an engine is affected by the number of features that are enabled. Configuring the maximum capacity when all features are enabled may impact performance.



3. The window will then display the system requirements that are recommended for the specified capacity and feature set. Verify that the engine meets these system requirements or make adjustments, if necessary.



4. Click **OK** to set the capacity and close the window.
5. Enforce the engine.

License Violations

Extreme Management Center (Management Center) checks the number of end-systems on a Access Control system on a daily basis. Exceeding the license limit results in an event being logged in the NAC Manager Events log. As the length of the violations increases, progressively more severe actions are taken by Management Center.

If violations continue, a License Violation warning message displays when an administrator logs into a Management Center application. Next, additional warning messages display to all Management Center users logging in. For violations lasting a minimum of 60 days, Management Center does not record end-system data for those end-systems over the number allowed by the license. If a violation lasts a minimum of 120 days, all end-systems over the license limit bypass the Access Control rules engine and Management Center assigns the policy associated with the Default Catchall rule (configured by the administrator).

Enterprise Assessment Licenses

The Enterprise Assessment license limits the number of end-systems assessed across all Access Control engine managed by the Extreme Management Center (Management Center) server. The license count is determined by finding all unique end-systems that have an assessment result present. The limit is dictated by the number of Enterprise Assessment licenses purchased. One IA-PA-3K license supports 3,000 unique end-system assessments across all Access Control engine, while one IA-PA-12K license supports 12,000 end-system assessments across all Access Control engine.

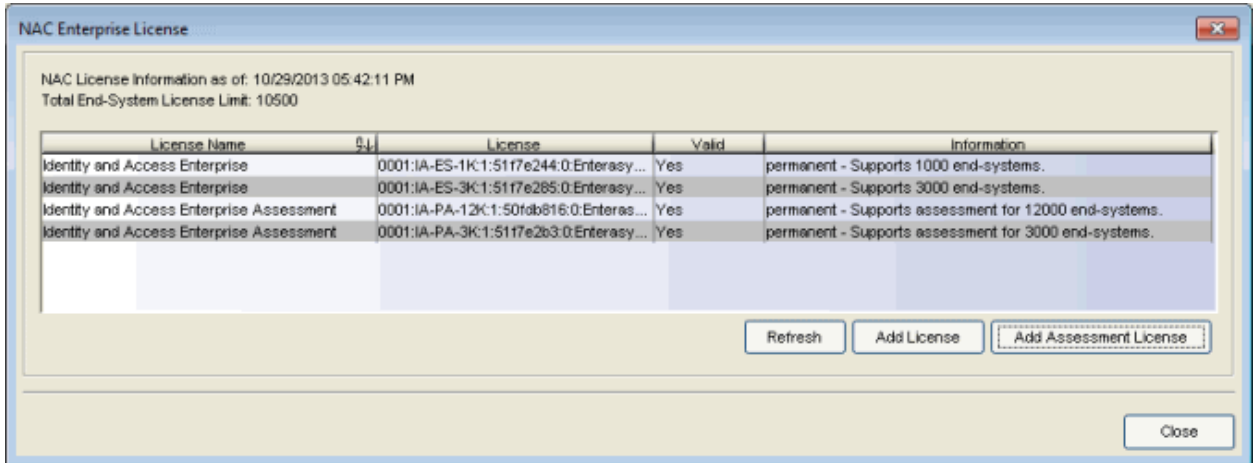
The NAC Enterprise Assessment license can be aggregated by applying additional licenses. The respective end-system limits are dictated by the number of licenses applied.

The limit is checked on a daily basis. If the limit is exceeded, an event is logged in the NAC Manager Events log.

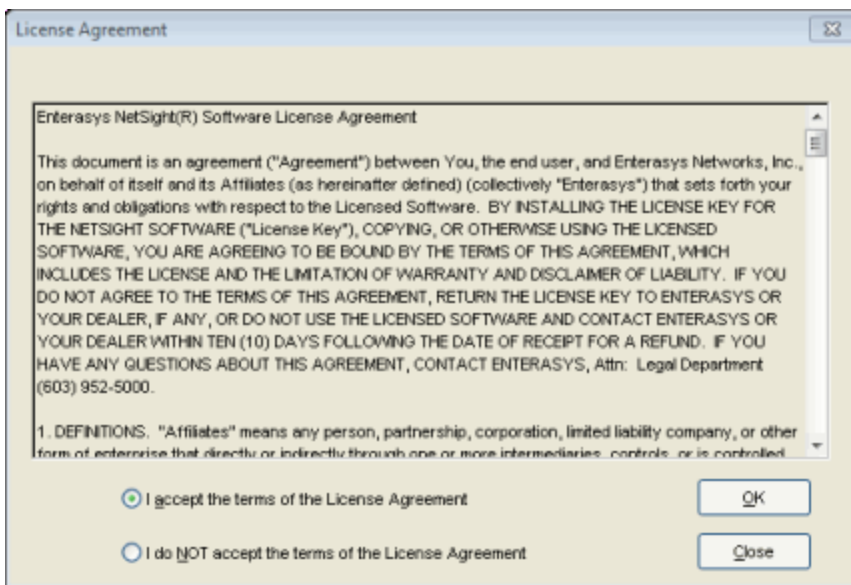
Applying an Enterprise Assessment License

The NAC Enterprise Assessment license is applied and updated via NAC Manager.

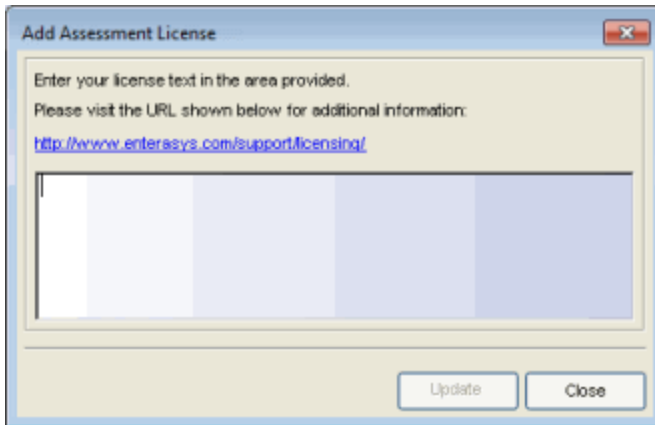
1. From the NAC Manager menu bar, select Tools > Update Enterprise License. The NAC Enterprise License window opens and lists all Enterprise and Enterprise Assessment licenses entered in the system.



2. Click the Add Assessment License button.
3. In the License Agreement screen, accept the terms of the agreement and click OK.



4. In the Add Assessment License window, enter your license text and click Update.



5. Close the NAC Enterprise License window.

The NAC Enterprise Assessment license is applied to the Management Center server. It does not get pushed to the Access Control engine.

How to Implement Facebook Registration

This Help topic describes the steps for implementing guest registration using Facebook as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Facebook in order to complete the registration process. If the end user selects the Facebook option, NAC uses OAuth to securely access the end user's Facebook account, obtain public end user data, and use that data to complete the registration process.

Guest Registration using Facebook has two main advantages:

- It provides NAC with a higher level of user information by obtaining information from the end user's Facebook account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. NAC retrieves the public information from the end user's Facebook account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- [Requirements for Facebook Registration](#)
- [Creating a Facebook Application](#)
- [NAC Portal Configuration for Facebook](#)
- [How Facebook Registration Works](#)
- [Special Deployment Considerations](#)
 - [Networks using DNS Proxy](#)

Requirements

These are the configuration requirements for Facebook Registration.

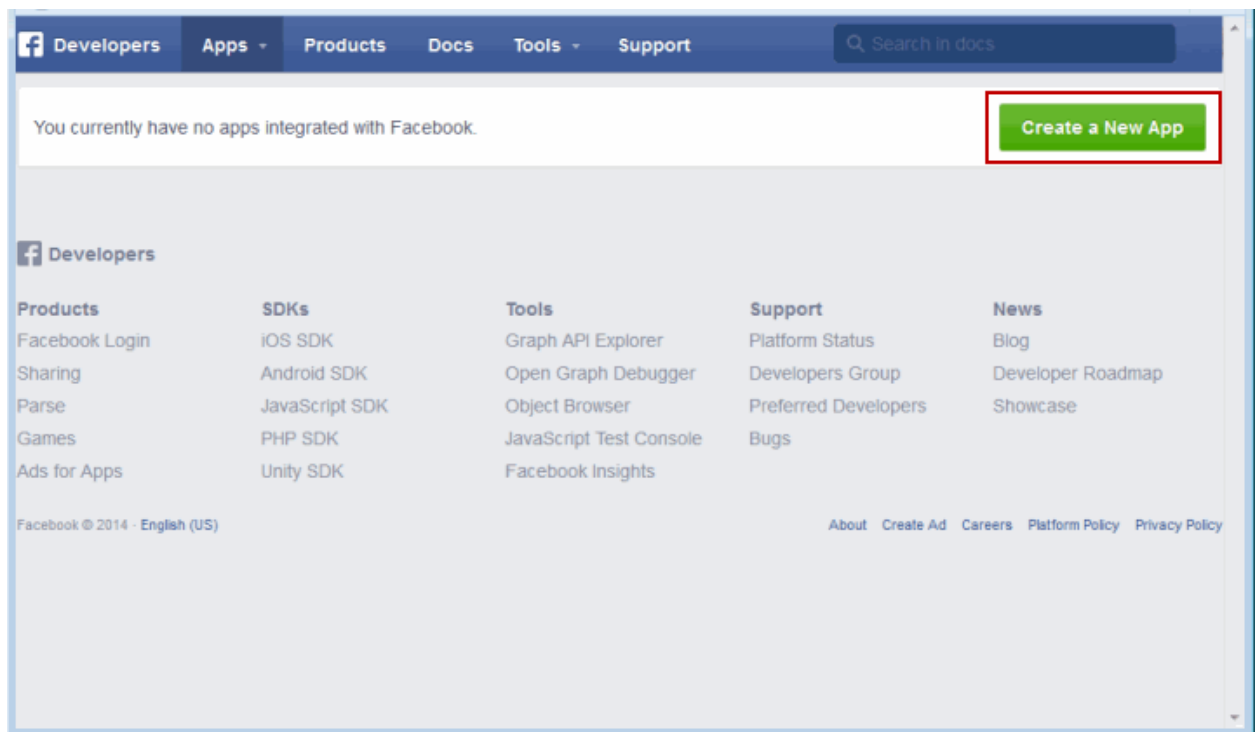
- The NAC Appliance must have Internet access in order to retrieve user information from Facebook.
- The NAC Unregistered access policy must allow access to the Facebook site (either allow all SSL or make allowances for Facebook servers).

- A Unique Facebook application must be created on the Facebook Developers page (see instructions below).
- The NAC Portal Configuration must have Facebook Registration enabled and include the Facebook Application ID and Secret (see instructions below).

Creating a Facebook Application

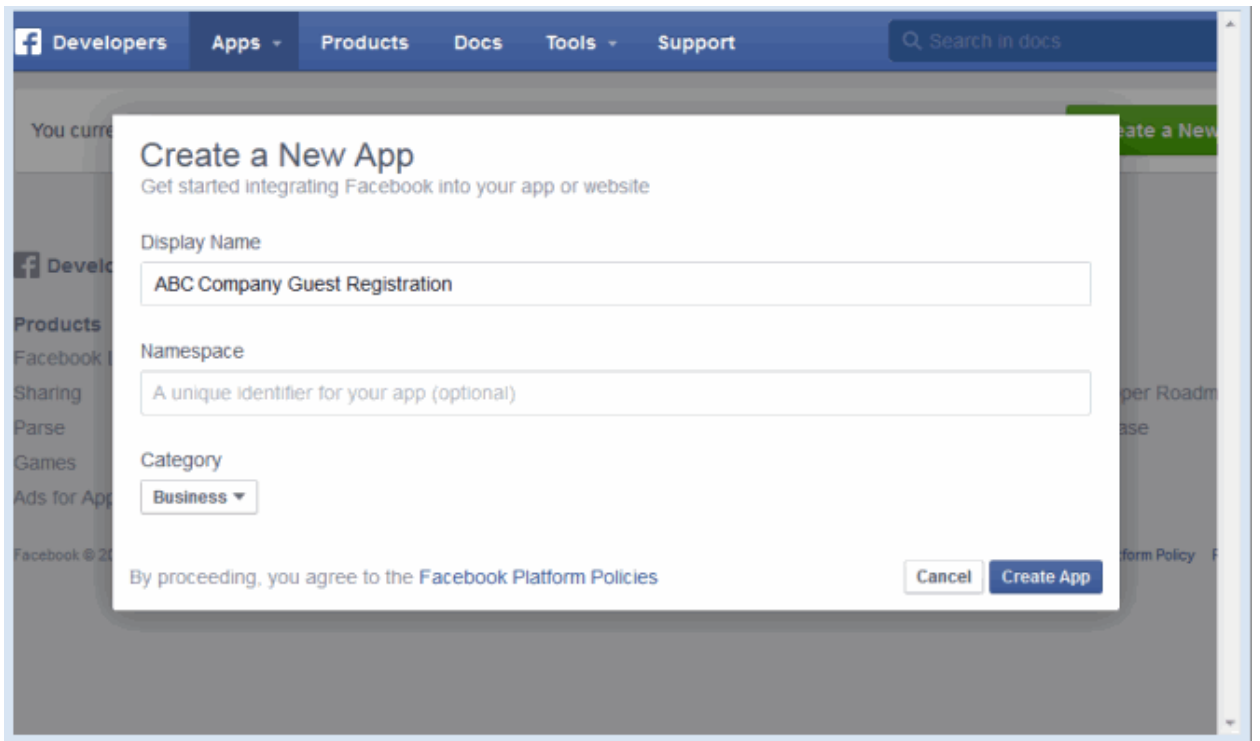
When implementing guest registration using Facebook, you must first create a Facebook application. This generates an Application ID and Application Secret that are required as part of the NAC OAuth process. Use the following steps to create a Facebook application.

1. Access the Facebook Developers page at <https://developers.facebook.com/apps/>. If you already have a Developers account you can log in, otherwise you must create a Developers account.
2. Once logged in, click the **Create New App** button to open the Create a New App dialogue.

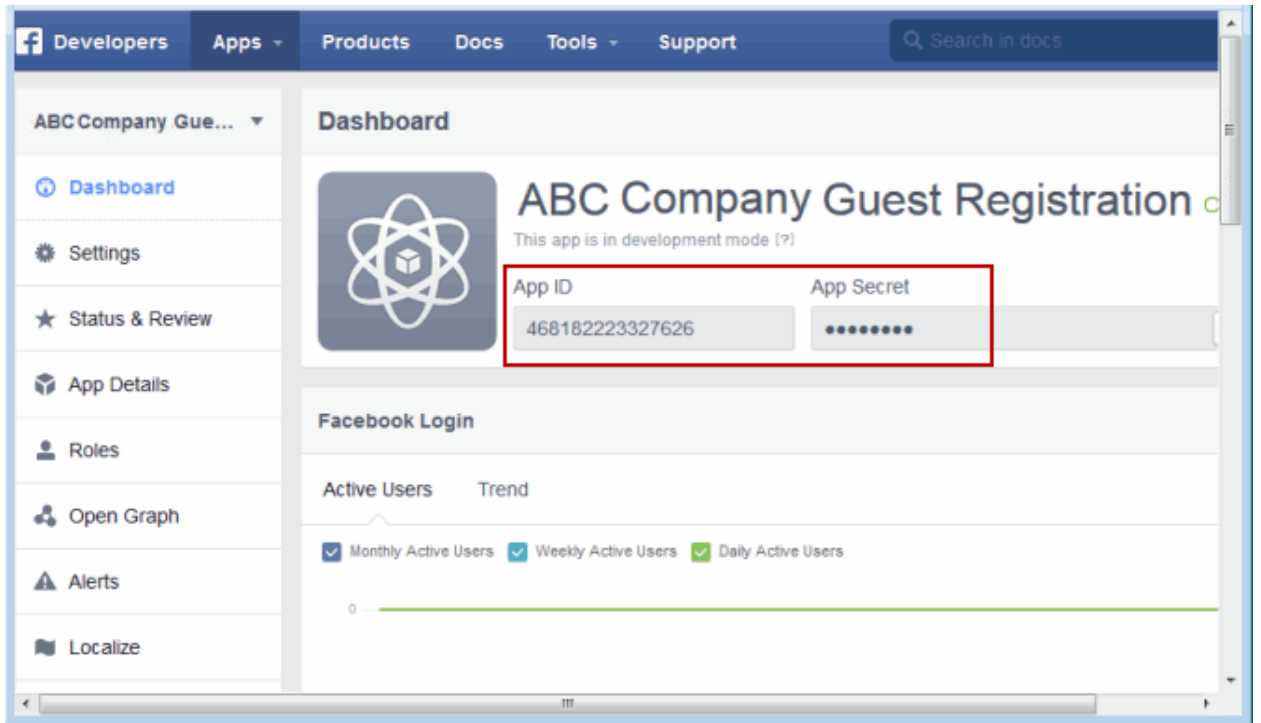


3. The Create a New App window opens. Enter a Display Name and select a category for your app. The Display Name is the name of the app that will be presented to the end-user when they grant NAC access to their Facebook

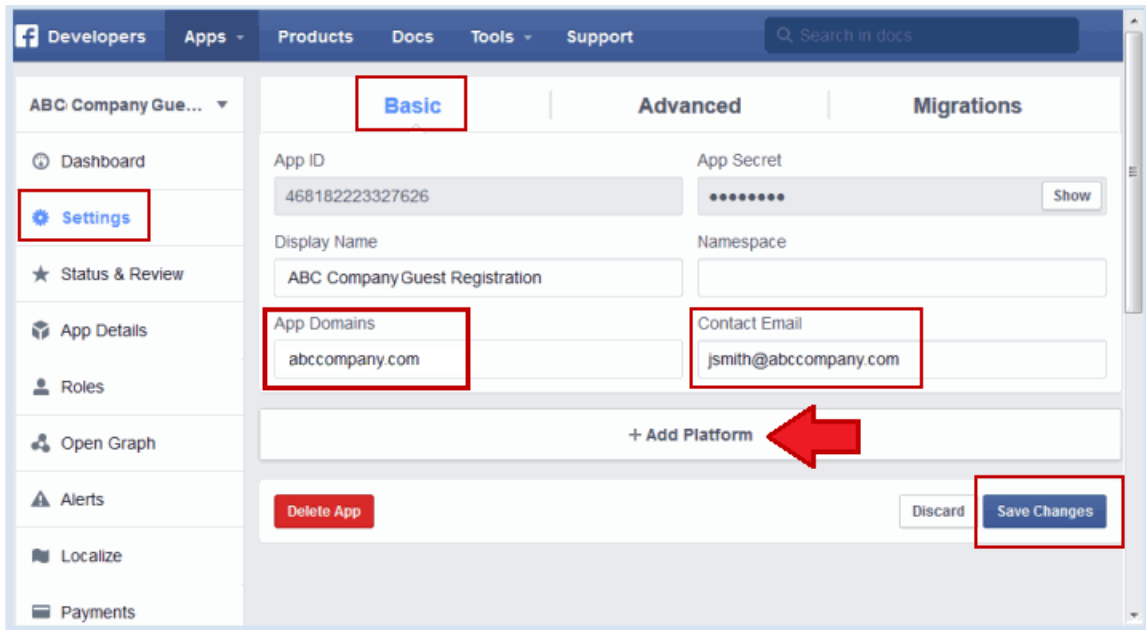
information and should clearly indicate what its purpose is, for example, Extreme Networks Guest Registration. Click **Create App**.



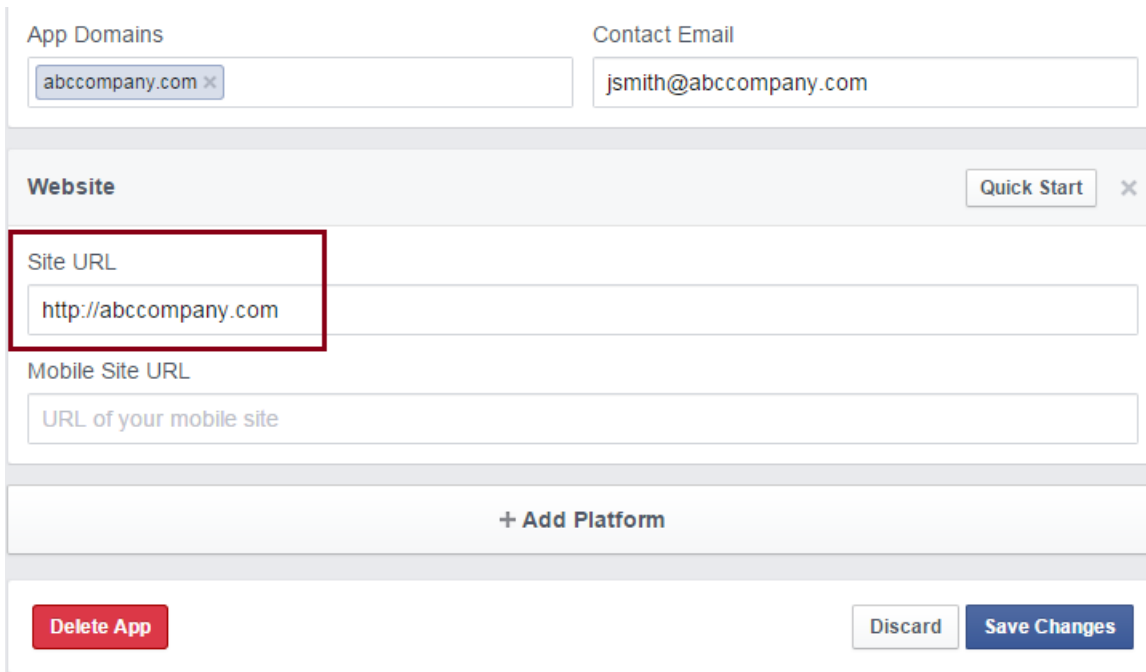
4. The Dashboard view opens and displays information about the new app including an App ID and an App Secret.



5. In the left panel, select **Settings**.
6. Enter in a valid domain name for the NAC Appliances in the **App Domains** field in the right-panel **Basic** tab. For example, if the NAC Appliance to which users are connecting is NACApliance.AbcCompany.com, enter "abccompany.com" in the **App Domain** field.



7. Enter a Contact Email.
8. Click Add Platform.
9. Select **Website** in the Add Platform options. The Platform window opens.

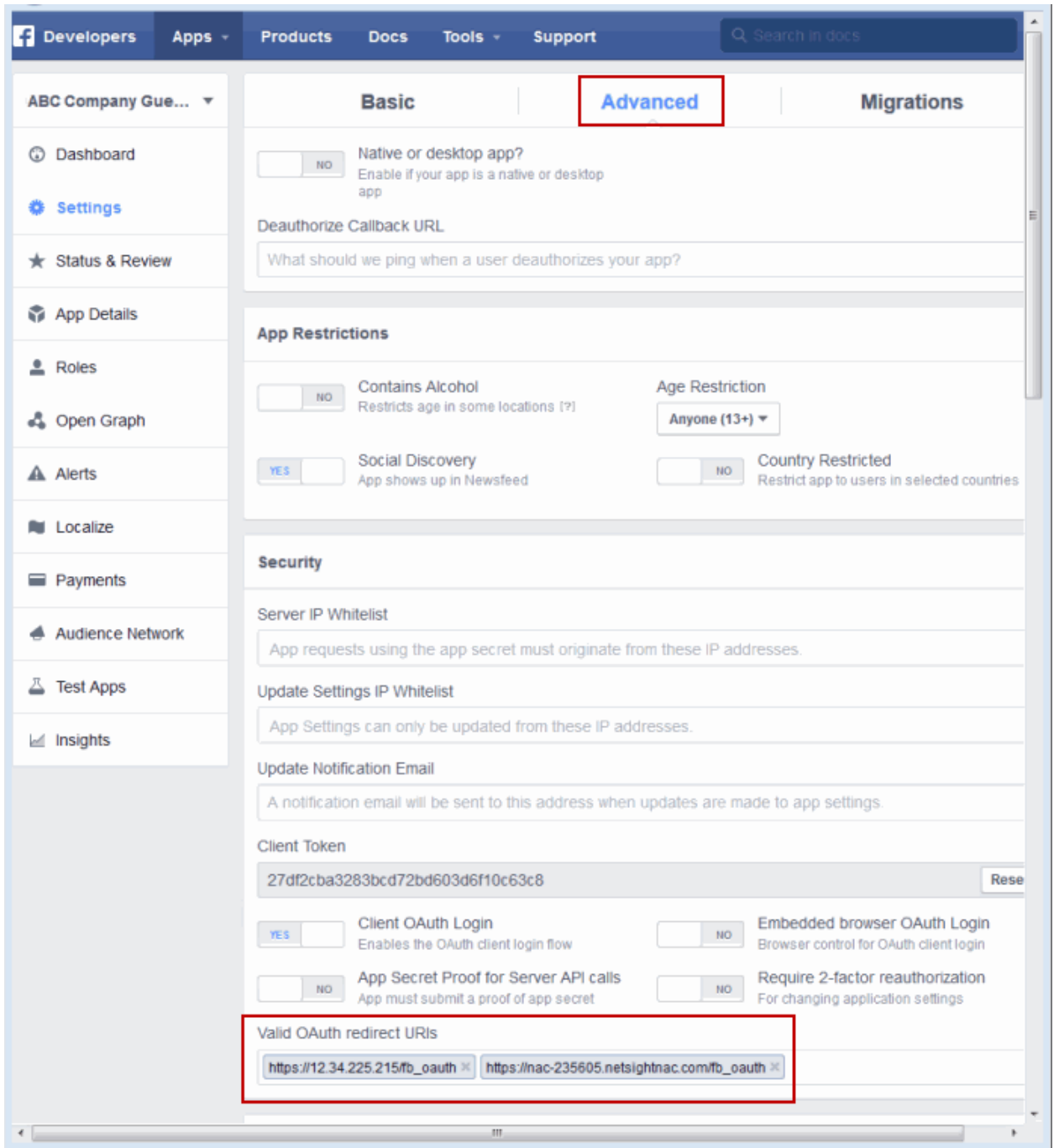


10. Enter the domain name you added in the **App Domain** field in step 5 in the **Site URL** field.
11. Click **Save Changes**.
12. In the **Advanced** tab, enter the Valid OAuth redirect URIs. A redirect URI is required to redirect the user back to the appliance with an Access Token that NAC uses to access the user account and retrieve the user data. The Redirection URI should be in the following format:

https:// <NAC appliance FQDN>/fb_oauth

A Redirection URI must be added for each NAC appliance where end users can register via Facebook.

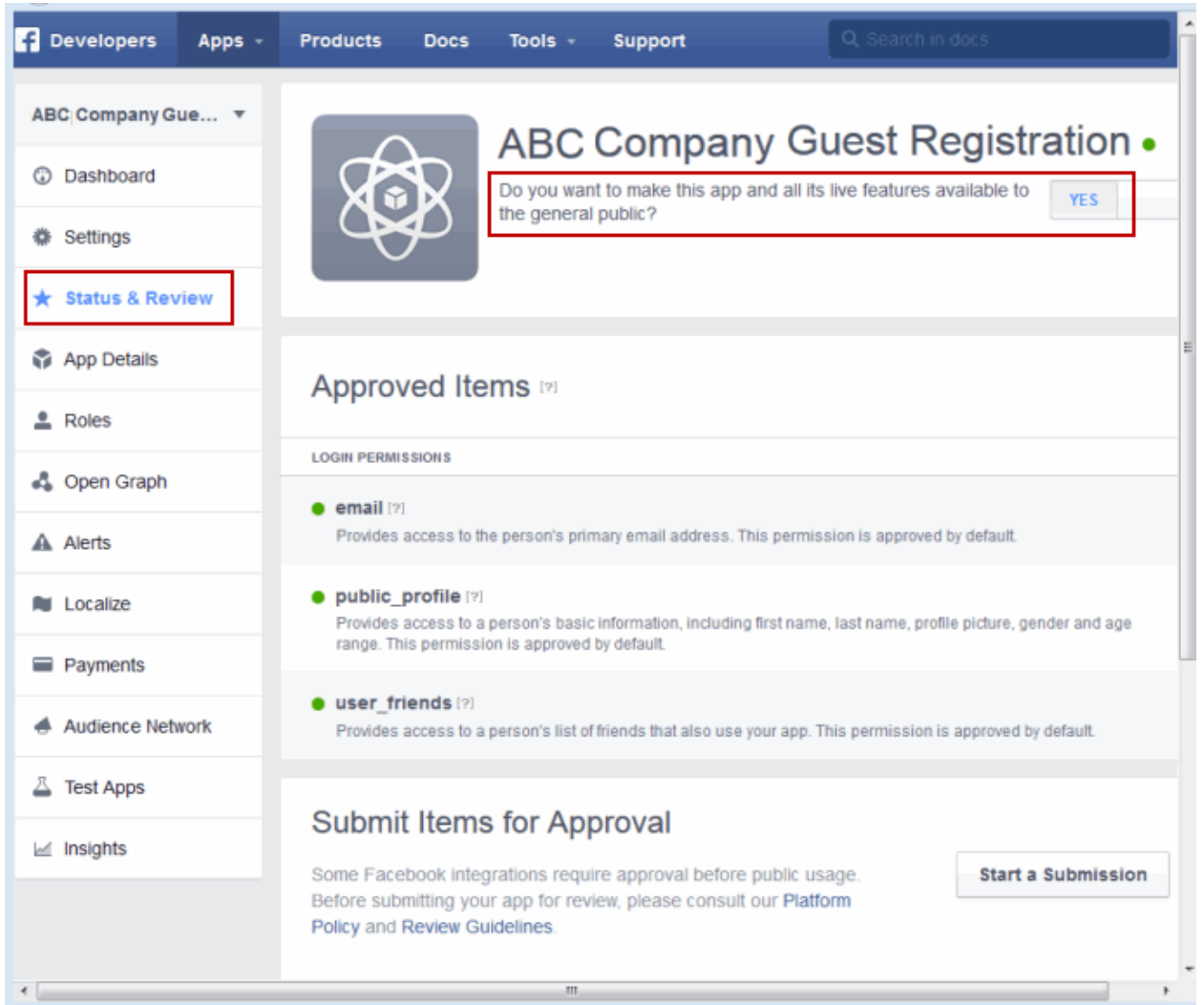
Scroll down and click **Save Changes**.



- In the left panel, select **Status & Review**. In the right-panel you will see a top section with the question "Do you want to make this app and all its live features available to the general public?" Select **Yes** and confirm your selection.

Under the Login Permissions section, you will see a list of default


permissions that provide access to end user data. (For more information on setting permissions, see <https://developers.facebook.com/docs/facebook-login/permissions#reference>.)

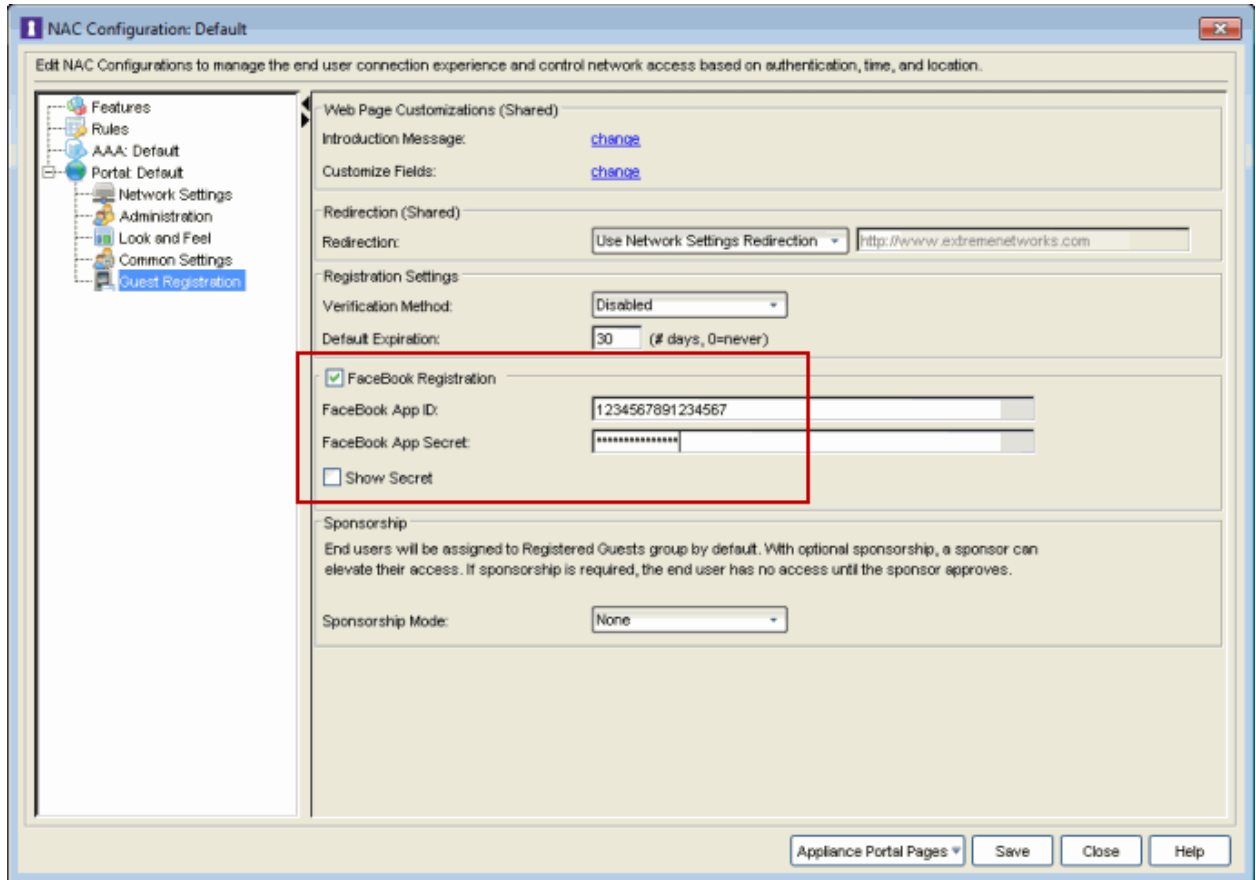


14. Your application is created and ready to use. You must now add the App ID and App Secret to your NAC portal configuration.

NAC Portal Configuration

The Application ID and Application Secret assigned during the creation of the Facebook application must be provided in the NAC Portal Configuration in order for the entire process to complete properly.

1. Use the NAC Manager  toolbar button to open the NAC Configuration window.
2. In the left-panel tree, expand the Portal icon and select Guest Registration.



3. In the Customize Fields section, click the "change" link to open the [Manage Custom Fields window](#) where you can change registration portal fields. Facebook registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal will verify that the AUP has been acknowledged before redirecting the user to Facebook.
4. Select the Facebook Registration checkbox.
5. Enter the Facebook App ID and Facebook App Secret.
6. Click **Save**. You will see some warnings messages stating that Verification Method and Sponsorship are not used for Facebook registration, and that an FDQN is required and will be enabled.
7. Enforce the new configuration to your appliances.

How Facebook Registration Works

Once you have configured Facebook registration using the steps above, the registration process will work like this:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to NAC's captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Facebook.
3. The end user is redirected to the Facebook login. If Acceptable Use Policy option is configured, the captive portal will verify that the AUP has been acknowledged before redirecting the user to Facebook.
4. Once logged in, the end user is presented with the information that NAC will receive from Facebook.
5. The end user grants NAC access to the Facebook information and is redirected back to NAC's captive portal where they see a "Registration in Progress" message.
6. Facebook provides the requested information to NAC, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Facebook" is added to the user name so that you can easily search for Facebook registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Facebook Registration.

Networks using DNS Proxy

Facebook Registration for networks redirecting HTTP traffic to the NAC captive portal using DNS Proxy requires additional configuration.

In order for Facebook Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Facebook web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the NAC appliance will resolve DNS queries for these components to the NAC appliance IP causing the page to not load properly.

As of July 26, 2014, you must add the following domains in order for Facebook registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

Facebook.com
fbstatic-a.akamaihd.net
fbcdn-profile-a.akamaihd.net
fbcdn-photos-c-a.akamaihd.net

Related Information

- [Portal Configuration](#)
- [How to Set Up Registration](#)

How to Initialize NAC Manager Database Components

NAC Manager provides a way for you to initialize only the NAC Manager components in the NetSight Database. The initialize operation removes **all** NAC Manager data elements from the database except default configurations (NAC, Portal, AAA, and appliance settings) or system-defined NAC Profiles. Default configurations and profiles will be restored to their original default parameters.

Using this operation instead of the Restore Initial Database function (accessed in the Server Information window) allows you to initialize your NAC Manager components while retaining your NetSight Console and other NetSight application data elements in the database.

NOTE: As a precaution, it is recommended that you make a backup of your NetSight Database prior to performing the initialize operation using the Backup Database window accessed from the Server Information window.

1. Make a backup of your database using the Backup Database window accessed from Database tab in the Server Information window (Tools > Server Information.)
2. Select **File > Database > Initialize NAC Manager Components** to begin the initialize operation. You will see a message asking if you want to delete all NAC Manager data in the server's database. Click **OK**.

How to Lock a MAC Address

MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different switch/port, it will be rejected or assigned a specific policy. Use the [Add/Edit MAC Lock window](#) to add a new locked MAC address or edit the settings for an existing locked MAC address. You can view all your locked MAC addresses in the [MAC Locking](#) panel of the Advanced Configuration tool.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name will change and break the MAC Locking settings.

NOTE: For NAC Controller Appliances.

- On Layer 3 NAC Controllers, you should not use MAC Locking to lock a MAC address to the NAC Controller PEP IP address **and** a port on the PEP. You can however, lock a MAC address to the PEP IP and **not** the port, which would restrict movement of the MAC address away from the Layer 3 NAC Controller.
 - On Layer 2 NAC Controllers, a MAC address can be locked to the NAC Controller PEP IP address and port, or just the PEP IP address, but this will only control the movement of the end-system between the downstream ports on the PEP (IP address and port) and not the actual edge of the network.
 - On Layer 3 NAC Controllers, there may be cases where NAC Manager cannot determine the MAC address of the connecting end-system (for example, DHCP is disabled and a firewall is enabled on the end-system, or the end-system is connecting through a VPN), and the MAC address for the end-system is displayed as "Unknown." In these cases, the MAC Locking feature is not supported.
-

To add a new locked MAC address:

- Open the Advanced Configuration tool (Tools > Management and Configuration > Advanced Configurations). In the left-panel tree, expand the Global and Appliance Settings folder and select MAC Locking. Click the **Add MAC Locking** button in the MAC Locking panel. (You can also add a locked MAC address from the [End-Systems tab](#).) The [Add MAC Lock window](#) opens.
- Enter the MAC address that you want to lock.

- Enter the IP address of the switch that you want to lock the MAC address to.
- Select the **Lock to Switch and Port** checkbox if you want to lock the MAC address to a specific port on the switch, and enter the port interface name.
- Select the action to take when this MAC address tries to authenticate on a different port and/or switch:
 - Reject - The authentication request is rejected.
 - Use Policy - Enter the policy that you want applied. This policy must exist in Policy Manager and be enforced to the switches in your network.
- Click **OK**.

To edit an existing locked MAC address:

- Open the Advanced Configuration tool (Tools > Manage Advanced Configurations). In the left-panel tree, expand the Global and Appliance Settings folder and select MAC Locking. In the MAC Locking panel, select the MAC address you want to edit, and click the **Edit MAC Locking** button. The [Edit MAC Lock window](#) opens.
- Make the desired changes.
- Click **OK**.

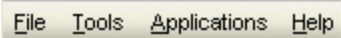
Related Information

For information on related tabs:

- [End-Systems tab](#)
- [MAC Locking](#)

Menu Bar

The menu bar on the main window provides access to NAC Manager functions. For information on menu options available from right-click menus, see [Right-Click Menu Options](#).



File Menu

File > Database > Initialize NAC Manager Components

Allows you to initialize all NAC Manager components in the Extreme Management Center database. This removes all NAC Manager data elements from the database. For more information, see [How to Initialize NAC Manager Database Components](#).

File > Database > Backup/Restore NAC Configuration

A database backup saves the active NAC Configuration to a specified location on the Management Center server workstation. If the server is remote, the configuration is saved to the default backup location. The backup saves all NAC Configuration data, but does not save end-system or health result data. Use the database restore to restore a saved NAC Configuration as the active configuration.

File > Generate Configuration Report (PDF)

Use this menu option to automatically generate a summary report of the NAC configuration information for your Extreme Access Control deployment. The report includes a summary of your Access Control engines, NAC configurations, NAC named lists, NAC profiles, AAA configurations, RADIUS servers, and engine details.

File > Exit

Exits the application.

Tools Menu

Tools > Setup Wizard

Opens the Initial Setup Wizard which assists you with first-time engine setup and configuration.

Tools > Authorization/Device Access

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in Management Center applications.

Tools > Server Information

Opens the Server Information window where you can view and configure certain Management Center Server functions, including management of client connections, locks, and licenses.

Tools > Synchronize with Console

Opens the [Synchronize Gateways with Console window](#) where you can synchronize the NAC Manager device database with Console's database.

Tools > Enforce All

Writes NAC configuration information to all Access Control engines.

Tools > End-System Operations > Search for End-Systems

Opens the [Search for End-Systems window](#) where you can search your NAC Manager database for end-systems that match the search criteria you select.

Tools > End-System Operations > Search for End-Systems by Assessment Results

Opens the [Search for End-Systems by Assessment Results window](#) where you can search your NAC Manager database for vulnerable end-systems based on their assessment results.

Tools > End-System Operations > Import End-System Information

Opens a window where you can select a file for importing end-system information. This allows you to create a file that lists up to four custom values per MAC address, and then import that file into NAC Manager so the custom values display in the [End-Systems tab](#) when the end-system connects. The information in the file must be listed in CSV format, one line per end-system:

02.0A.40.0B.01.44, value1, value2, value3, value4

Tools > End-System Operations > View End-System Counts

Opens a window where you can view the total number of current end-systems seen on each switch. Limit counts by specifying a time range, if desired.

Tools > End-System Operations > Remove End-Systems

Opens the [Remove End Systems window](#) where you can remove end-systems from the tables and charts in the [End-Systems tab](#) and the

[Statistics tab](#).

Tools > End-System Operations > Data Persistence

Opens a window where you can view estimated row counts for several tables displayed in NAC Manager. You can perform a one-time data cleanup for these tables or edit the [Data Persistence options](#).

Tools > Management and Configuration > NAC Configurations

Opens the [NAC Configuration window](#) where you can view and edit the selected NAC configuration.

Tools > Management and Configuration > Advanced Configurations

Opens the [Advanced Configuration window](#) that provides a central location to view and manage the configuration parameters for all aspects of your Access Control system.

Tools > Management and Configuration > Rule Groups

Opens the [Manage Rule Groups window](#) where you can view and edit the defined rule groups and also add new rule groups for use in your NAC configuration.

Tools > Management and Configuration > NAC Profiles

Opens the [Manage NAC Profiles window](#) where you can view and edit the seven system-defined NAC profiles that define the authorization and assessment requirements for the end-systems connecting to the network. You can also use the window to define new profiles.

Tools > Management and Configuration > Assessment Settings

Opens the [Manage Assessment Settings window](#) where you can manage and configure the assessment servers performing the end-system assessments in your network.

Tools > Management and Configuration > Notifications

Opens the [Manage Notifications window](#) where you can view created notifications, and enable, add, edit, and test specific notification rules.

Tools > Management and Configuration > MAC Locks

Opens the [Manage MAC Locks window](#) that displays information about all the MAC addresses that are locked. You can also add or delete locked MAC addresses, or import MAC locks from a file.

Tools > Management and Configuration > End-System Zones

Opens the [Manage End-Systems Zones window](#) where you can view and define the authorized end-system zones and authorized rule groups that are configured for your NetSight user groups.

Tools > Management and Configuration > Data Center Fabric

Opens the [Manage Data Center Fabric window](#). If your network uses the Data Center Manager (DCM) product, you can use this window to view a list of virtual/physical network configurations and how they map to the overall network and security configuration.

Tools > Registration Administration

Opens the Registration Administration web page where you can view registered devices and users, and manually add, delete, and modify users.

Tools > Identity and Access Dashboard

Opens the [Control tab](#) where you can access NAC Manager end-system data via Management Center.

Tools > Update Enterprise License

Allows you to apply a NAC Enterprise or Enterprise Assessment license to the Management Center server. For more information, see [NAC Enterprise Licensing](#).

Tools > Options

Opens the Options window where you can set suite-wide options and [NAC Manager options](#).

Applications Menu

Lets you launch other installed Management Center applications from NAC Manager. You can also customize the Applications menu to launch your own applications. For more information, see [How to Add Applications to the Applications Menu](#).

Help Menu

Help > Topics

Opens the NAC Manager Help system.

Help > NetSight Tips and Tutorials

Opens your system's Web browser and takes you to the Management Center Tips and Tutorials where you can access Flash tutorials on the Management Center suite of products.

Help > Release Notes

Displays the NAC Manager Release Notes for the current release.

Help > Support Center

Opens the Extreme Networks Support website.

Help > Check for Updates

Allows you to update NAC Manager with the latest software patches. For more information, see Setting Web Update Options.

Help > Check for Assessment Updates

Opens the Updates Available window that lists any assessment software updates that are available for updating your on-board agent-less assessment servers in your Access Control engines.

Help > Getting Started

Displays the Getting Started help topic that provides the basic steps you must perform to begin using NAC Manager in your network.

Help > About This Window

Displays detailed information about the currently selected right-panel tab. This menu option serves the same function as the **Help** button on the toolbar.

Help > About NAC Manager

Displays the NAC Manager version and copyright information.

Right-Click Menu Options

The following menu options are only available from right-click menus. They are listed in alphabetical order.

Add Appliance Group

Opens a window where you can create an engine group and select the NAC Configuration specifying the authentication and assessment (scanning) requirements for the end-systems connecting to that group. An engine group is a "virtual container" that includes the Access Control engines, the switches in the network, and the NAC configuration utilized. Most NAC deployments only use one engine group configured for the network and in that case, the "engine group" is the All NAC Appliances folder in the left-panel tree. However, an example of a network that may require separate engine groups is a network in which there are remote offices that want completely different Access Control functionality than the main branch. These remote offices need to have their own Access Control engines in a separate group. In this case, the separate engine groups are listed in the left-panel tree.

Add MAC Lock

Opens the [Add MAC Lock window](#) where you can lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch.

Appliance Group Properties

Opens the Appliance Property Editor. Please contact Extreme Networks Support for instructions on how to use this window.

Appliance Properties

Opens the Appliance Property Editor. Please contact Extreme Networks Support for instructions on how to use this window.

Appliance Settings

Opens the [Appliance Settings window](#) where you can access advanced configuration options for the selected engine or engine group.

Change Appliance Group

Lets you move an engine from one group to another.

Change Appliance Settings

Lets you change the engine settings for an engine group.

Clear Custom Information

Right-click on one or more end-system in the End-Systems tab and select this menu option to clear the custom information for those end-systems.

Delete Appliance

Lets you delete the selected engine from the [NAC Appliances tab](#).

Delete Appliance Group

Lets you delete the selected engine group from the [NAC Appliances tab](#).

Edit Appliance Settings

Opens the [Edit Appliance Settings window](#) that provides advanced configuration options for Access Control engines. NAC Manager comes with a default engine settings configuration. If desired, you can edit these default settings or you can define your own settings to use for your Access Control engines.

Edit Custom Information

Right-click on an end-system in the End-Systems tab and select this menu option to add or edit the custom information for that end-system.

Enforce

Lets you enforce to an individual Access Control engine.

Enforce Group

Lets you enforce to all the Access Control engines in a group.

Enforce Preview

Provides a preview of what is being enforced/updated on the engine.

Enforce Policy Manager Domain Configuration

For one or more switches in the **Switches** tab, this option lets you add or move a device to a Policy Manager domain and enforce the domain configuration to that device.

Launch CPU Utilization View

For one or more engines in the **NAC Appliance** tab, this option lets you open the Host Processor Load FlexView.

Launch Memory and Disk Space Utilization View

For one or more engines in the **NAC Appliance** tab, this option lets you open the Host Storage FlexView.

Launch MIB Tools

For a switch in the **Switches** tab, this option lets you launch the MIB Tools utility.

Launch Node Alias and Multi Auth View

For one or more switches in the **Switches** tab, this option lets you open the Node Alias and Multi Auth FlexView.

Launch RADIUS Client Information View

For one or more switches in the **Switches** tab, this option lets you open the RADIUS Client Information FlexView.

NAC Appliance Log

Displays the Access Control engine log, located at /var/log/tag.log on the engine. NAC Manager uses this log for informational, diagnostics, and error messages.

Override AAA Configuration

For a single engine, this option lets you override the AAA Configuration that is specified for the engine group.

Override Appliance Settings

For a single engine, this option lets you override the engine settings that are specified for the engine group.

Ping

Launches the Ping Device window and initiates a ping of the selected engine.

Ping End-System

Right-click on an end-system in the **End-Systems** tab and select Ping End-System to open a window where you can ping the end-system to determine if it can be contacted. View the results of the ping in the log in the window. Click **Clear** to enter another IP address or host name.

Policy > Port Configuration Wizard

For one or more switches in the **Switches** tab, this option accesses the Policy Manager Port Configuration Wizard. Select from pre-configured defaults for MAC, 802.1X, or MAC + 802.1X authentication, or select the complete wizard which leads you through all the steps required to configure a port or ports, including setting the port authentication configuration and default role. (If the devices are not in a domain or are in more than one domain, any role specific configuration, such as setting the default role, is disabled.)

Policy > Display Domains Associated with Switches

For one or more switches in the **Switches** tab, this menu option retrieves the Policy Manager domains associated with the switches and displays them in the Policy Domain column in the tab.

Policy > Set Domain

For one or more switches in the **Switches** tab, this option lets you assign the switch to a Policy Manager domain.

Policy > Verify Domain Policy Settings with Network

For one or more switches in the **Switches** tab, this menu option verifies that the roles in the assigned Policy Manager domain are enforced to the switch.

Policy > Enforce Domain Policy Settings with Network

For one or more switches in the **Switches** tab, this menu option enforces the roles in the assigned Policy Manager domain to the switch.

Poll Appliance(s)

If the Access Control engine icon is red, this menu option gives you a quick way to verify if the engine is back up.

SSH

Launches an SSH console session to the selected Access Control engine or switch.

Table Tools

Use the table options and tools to find, filter, sort, print, and export information in NAC Manager tables, and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body. For more information, see the Suite-Wide Tools Help topic on Table Tools.

Telnet

Launches a telnet session to the selected switch's Local Management.

Verify RADIUS Configuration

This right-click menu option is available when an Access Control Gateway or Layer 2 Access Control Controller engine is selected in the **NAC Appliance** tab. It is also available by selecting one or more switches in the **Switches** tab. The option lets you perform a [Verify RADIUS Configuration](#) operation.

View Selected

This right-click menu option is available when one or more end-systems are selected in the End-Systems table. It allows you to filter down to a smaller set of end-systems, by opening a new window that only displays the selected end-systems.

WebView

Launches the NAC Appliance Administration web page where you can access status and diagnostic information for the selected Access Control engine. The default user name and password for access to this web page is "admin/Extreme@pp." Change the username and password in the [Web Service Credentials](#) field on the Credentials Tab in the Edit Appliance Settings window.

How to Set NAC Manager Options

Use the Options window (**Tools > Options**) to set options for the NAC Manager application. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the NAC Manager folder in the tree to view all the different options you can set.

Instructions on setting the following NAC Manager options:

- [Advanced Settings](#)
- [Assessment Server](#)
- [Data Persistence](#)
- [Display](#)
- [End-System Event Cache](#)
- [Enforce Warning Settings](#)
- [Features](#)
- [Notification Engine](#)
- [Policy Defaults](#)
- [Port Wizard Defaults](#)
- [Status Polling and Timeout](#)

Advanced Settings

Use the [Advanced Settings view](#) to configure advanced settings for NAC Manager. These settings apply to all users on all clients.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Advanced Settings.
3. Use the **Capacity** option configure the NetSight resources allocated to end-system and configuration processing services. The greater the number of end-systems and appliances in your NAC deployment, the more resources it will require.

- Low - For low performance shared systems.
 - Low-Medium - For medium performance shared systems, or low performance dedicated systems
 - Medium - For medium performance shared systems, or medium performance dedicated systems.
 - Medium-High - For high performance shared systems, or medium performance dedicated systems.
 - High - For high performance dedicated systems.
 - Maximum - For extremely high performance dedicated systems.
4. Use the **Hybrid Mode** option to enable Hybrid Mode for Layer 2 Controllers. Hybrid Mode allows a Layer 2 NAC Controller appliance to act as a RADIUS proxy for switches, like a NAC Gateway appliance. Select this option to enable Hybrid Mode for your Layer 2 Controllers at a global level. When the option is selected, the Configuration tab for a Layer 2 Controller will display an option to enable Hybrid Mode for that specific controller. For more information, see the [Configuration tab](#) Help topic. Disabling Hybrid Mode at the global level when a controller has switches will have a similar effect to deleting a gateway: the switches will have the controller removed as a reference.
 5. The **Enable distributed end-system cache** option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling this option will improve NAC performance when discovering new end-systems as they connect, or when end-systems move from one place to another in the network.

To use the end-system cache feature, it must be enabled on both the NetSight Server (using this option) and on the NAC appliances that will be using the cache (using the [NAC Appliance Advanced Configuration window](#)).

When this feature is enabled, the NetSight Server and the NAC appliance exchange additional data each time end-system data is updated. This feature is **not** recommended unless there is sufficient network bandwidth for the additional data, a fast connection between the NetSight Server and the NAC appliance, and end-systems are adding or moving frequently.

When you enable or disable this option, you must click the **Reload** button to reload the cache configuration on the NetSight server.

The **Reload** button is also used if you have configured communication

channels for the appliance groups on your network. You must reload when you first configure your channels and also any time you change your channel configuration. Reload will redistribute the end-system information to the new channels.

CAUTION: The Reload operation may take some time and network communication may be temporarily disrupted.

6. The **Enable IPv6 Addresses for end-systems** option allows NAC to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your appliances before the new settings will take effect. In addition, end-systems will need to rediscover their IP addresses in order to reflect the change in the end-system table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system. Only end-systems that have a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems that have only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see NAC Manager IPv6 Support in the NetSight Configuration Considerations Help topic.
7. The **Enable Communication Channels for Appliance Groups** option allows you to create logical groupings of your NAC appliance groups in order to segment data and limit network traffic between geographical or customer sensitive locations. This is an advanced NAC Manager feature and is only appropriate in certain network scenarios. For more information and complete configuration instructions, see [How to Configure Communication Channels](#).
8. Click OK.

Assessment Server

Use the [Assessment Server view](#) to schedule updates to NAC assessment server software and provide assessment agent adapter credentials. The options apply to all users on all clients.

The Schedule Updates option pertains only to on-board agent-less assessment servers and allows you to schedule routine checks for assessment server software updates using the web update operation. The web update feature automatically recognizes when an updated version of NAC assessment server software is available and allows you to download the newer version to keep your software current. The update operation uses the Suite Web Update server and

proxy settings, which are configured in the Suite Options Web Update view. If your network is behind a firewall, you must specify the HTTP Proxy server being used.

NOTE: The web update feature will download any updated assessment server software but will not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button in the [Manage Assessment Settings](#) window with the Assessment Servers tab selected.

You should perform the Check for Assessment Updates and the Upgrade operation at least every two weeks to ensure that the assessment servers are running the latest scanner software that includes the most up-to-date virus definitions.

Because the on-board agent-less assessment license is subscription-based, the Upgrade operation must be performed at least once a month in order to upgrade the license. If the appliance is unable to contact the upgrade server, you should contact Extreme Networks Support so that a special license can be provided.

The assessment agent adapter credentials are used by the NAC appliance when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server that is not supplied or supported by NAC Manager). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. NAC Manager provides a default password that can be changed, if desired. However, if you change the password here, you will need to change the password on the assessment agent adapter as well, or connection between the appliance and assessment agent adapter will be lost and assessments will not be performed. For instructions, see [How to Change the Assessment Agent Adapter Password](#).

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Assessment Server Web Update.
3. To schedule updates to NAC assessment server software:
 - a. Use the drop-down list to select the desired frequency (**Daily**, **Weekly**, **Disabled**) for checking for updates. If you specify a Weekly check, use the drop-down list to select the day of the week you wish the check to be performed, and set the desired time. If you specify a Daily update, set the desired time.
 - b. Verify the web update server and proxy server settings in the Suite Options Web Update view.

4. Specify the assessment agent adapter credentials.
5. Click **OK**.

Data Persistence

Use the [Data Persistence view](#) to customize how NAC Manager will age-out or delete end-systems, end-system events, and end-system health results (assessment results) from the tables and charts in the [End-Systems tab](#) and the [Statistics tab](#). These settings apply to all users on all clients.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Data Persistence.
3. Set the time that you would like the Data Persistence Check to be performed each day.
4. In the **Age End-Systems** section, enter the number of days the Data Persistence Check will use as criteria for aging end-systems. Each day, when the Data Persistence check runs, it searches the database for end-systems that NAC Manager has not received an event for in the number of days specified (90 days by default). It will remove those end-systems from the tables in the [End-Systems tab](#).
5. If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check will also remove any MAC locks or group memberships associated with the end-systems being removed. The **Remove Associated Registration Data** checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.
6. In the **End-System Event Persistence** section, select the checkbox if you want NAC Manager to store non-critical end-system events, which are events caused by an end-system reauthenticating. End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes end-system events which are older than the number of days specified (90 days by default).
7. In the **End-System Information Events** section, select the checkbox if you want NAC Manager to generate an event when end-system information is modified.
8. In the **Transient End-Systems** section, configure the number of days to keep transient end-systems in the database before they will be deleted as

part of the nightly database cleanup task. The default value is 1 day. A value of 0 will disable the deletion of transient end-systems. Transient end-systems are end-systems that are Unregistered and have not been seen for the specified number of days. End-systems will not be deleted if they are part of an End-System group or there are MAC locks associated with them. Select the **Delete Rejected End-Systems** checkbox if you want end-systems in the Rejected state to be deleted as part of the cleanup. You can also delete transient end-systems using the Tools > End-System Operations > Data Persistence option.

9. In the **Health Result Persistence** section, specify how many health result (assessment results) summaries and details will be saved and displayed in the [End-Systems tab](#) for each end-system. By default, the Data Persistence check will save the last 30 health result summaries for each end-system along with detailed information for the last five health result summaries per end-system.

There are two additional options:

- You can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).
- You can specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are **not** saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results will be saved.

10. Click **OK**.

Display

Use the [Display view](#) to select different display options in NAC Manager. These settings apply only to the current user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Display.

3. Configure the following display options:
 - Specify how you want to display NAC appliance names in the left-panel tree. You can display the appliance's IP address, the name that was assigned when the appliance was created, or a combination of the name and IP address.
 - Limit the number of table rows displayed in the End-Systems Activity tab and NAC Appliances Events tab in the Event View.
 - Click the **Re-Show All** button to turn on the display of messages that have been turned off in individual message dialog box(es).
 - Click the **Reset All** button to reset all NAC Manager secondary windows to their default size and screen placement.
 - Show or hide the Welcome Panel that is displayed when you first open NAC Manager and the All NAC Appliances folder is selected in the left-panel tree.
 - Use the Custom End-System Information Labels section to specify new text for the Custom column headings in the [End-System table](#) on the End-Systems tab.
 - Use the End-System Table Performance option to display group membership data in the End-Systems tab. Deselecting this option removes the Groups column from the End-Systems table and allows the table data to display faster. The option will take effect when the table is loaded (e.g. when you click on the End-Systems tab and the table is displayed).
 - Increase the number of redundant NAC Gateways per switch in the [Add](#) or [Edit Switches in NAC Appliance Group](#) windows. By default, these windows allow you to configure two NAC Gateways per switch for redundancy. You can use this option to increase the number up to three or four gateways per switch.
4. Click **OK**.

End-System Event Cache

End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them in the [End-System Events tab](#). This cache allows NAC Manager to quickly retrieve and display end-system events without having to search through the database. Use the [End-System Event Cache view](#) to configure the amount of

resources used by the end-system event cache. This setting applies to all users on all clients.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select End-System Event Cache.
3. Specify the number of events to cache. Keep in mind that the more events you cache, the faster data is returned, but that caching uses more memory.
4. The End-System Event Cache also keeps a secondary cache of events by MAC address. This means that a particular end-system's events can be more quickly accessed in subsequent requests. Specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note that the secondary cache may includes events that are not in the main cache, but were retrieved by scanning the database outside the cache boundary.
5. Specify the time Extreme Management Center spends when searching for older events outside of the cache. (The search is initiated by using the **Search for Older Events** button in the [End-System Events tab](#).) The search is ended when the number of seconds entered is reached.
6. Click **OK**.

Enforce Warning Settings

Use the [Enforce Warning Settings view](#) to specify warning messages that you don't want displayed during the Enforce appliance audit.

When an appliance configuration audit is performed during an Enforce operation, warning messages may be displayed in the audit results listed in the Enforce window. If an appliance has a warning associated with it, you are given the option to acknowledge the warning and proceed with the enforce anyway.

These settings allow you to select specific warning messages that you do not want to have displayed in the audit results. This allows you to proceed with the Enforce without having to acknowledge the warning message. For example, you may have a NAC configuration that always results in one of these warning messages. By selecting that warning here, it will be ignored in future audit results and you will no longer have to acknowledge it before proceeding with the Enforce.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder and select Enforce Warning Settings. The Enforce Warning Settings view opens.
3. Select the checkbox in the Ignore column next to the warning messages that you don't want displayed.
4. Click **OK**.

Setting Features Options

Use the [Features view](#) to enable registration and web access configuration support, as well as assessment/remediation for end-system access support. If you are not using these features, you can disable them to remove sections that pertain only to those features from certain NAC Manager windows.

Setting Notification Engine Options

Use the [Notification Engine view](#) to define the default content contained in NAC Manager notification action messages. For example, with an email notification action, you can define the information contained in the email subject line and body. With a syslog or trap notification action, you can specify certain information that you want contained in the syslog or trap message. These settings apply to all users.

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For a complete list of available keywords for NAC Manager notifications, see the [Edit Action Overrides window](#) Help topic.

- \$type - the notification type.
- \$trigger - the notification trigger.
- \$conditions - a list of the conditions specified in the notification action.
- \$ipaddress - the IP address of the end-system that is the source of the event.
- \$macaddress - the MAC address of the end-system that is the source of the event.
- \$switchIP - the IP address of the switch where the end-system connected.
- \$switchPort - the port number on the switch where the end-system connected.

- \$username - the username provided by the end user upon connection to the network.
1. Select **Tools > Options** in the menu bar. The Options window opens.
 2. In the left-panel tree, expand the Suite folder and select Notification Engine. The Notification Engine view opens.
 3. Use the fields to define the default content contained in notification action messages. For a definition of each field, see the [Notification Engine view](#) Help topic.
 4. Click the **Advanced Settings** button to open the [Notification Advanced Settings window](#) where you can set parameters for the Action and Event queues processed by the Notification engine.
 5. Click **OK**.

Policy Defaults

Use the [Policy Defaults view](#) to specify a default policy role for each of the four [access policies](#). These default policy roles will be displayed as the first selection in the drop-down lists when you create a NAC profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" will be automatically displayed as the first selection in the Assessment Policy drop-down list in the [New NAC Profile window](#).

NAC Manager supplies seven policy role names to select from. You can add more policies in the [Edit Policy Mapping window](#), where you can also define policy to VLAN associations for RFC 3580-enabled switches. Once a policy has been added, it becomes available for selection in this view.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Policy Defaults.
3. Select the desired policies.
 - The **Assessment policy** is applied to an end-system while it is being assessed (scanned).
 - The **Accept policy** is applied to an end-system when an end-system has been authorized locally by the NAC Gateway and has passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option was used when the end-system authenticated.

- The **Quarantine policy** is applied to an end-system if the end-system fails an assessment.
 - The **Failsafe policy** is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and an assessment of the end-system could not take place.
4. Click **OK**.

Port Wizard Defaults

Use the [Port Wizard Defaults view](#) to define the default behavior for the MAC, 802.1X, or MAC + 802.1X authentication port configuration wizards. The wizards can be accessed by right-clicking one or more switches in the Switches tab and selecting Policy Manager Port Configuration Wizard. The options you define here will be used as the wizard defaults. These settings apply to all users on the client.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Port Wizard Defaults.
3. Select the **Port Mode - Unauthenticated Behavior**, which defines how the traffic of unauthenticated end users will be handled on the port.
 - **Default Role** - If the end user is unauthenticated, the port will implement its default role. You can select to use the current default role on the device or set a default role. If there is no default role specified, there will be no role on the port.
 - **Discard** - If the end user is unauthenticated, no traffic is allowed on the port.
4. Enable **Automatic Re-Authentication** if you want to set up the periodic automatic re-authentication of logged-in users on the port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information, to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes." Select the **Active** radio button to enable Automatic Re-Authentication. Specify the **Re-Authentication Frequency**, which determines how often (in seconds) the device checks the port to re-authenticate the logged in user.

5. Set the **Hold Time**, which is the amount of time (in seconds) authentication will remain timed out after the allowed number of authentication attempts has been exceeded.
6. Click **OK**.

Status Polling and Timeout

Use the [Status Polling and Timeout view](#) to specify polling and timeout options for NAC Appliances. These settings apply to all users on all clients.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the NAC Manager folder and select Status Polling and Timeout.
3. In the **NAC Appliance Enforce Timeout** section, specify the amount of time that NAC Manager waits for an enforce response from the appliance before determining that the NAC appliance is not responding. During an enforce, a NAC appliance responds every second to report that the enforce operation is either in-progress or complete. Typically, you should not need to increase this timeout value, unless you are experiencing network delays that require a longer timeout value.
4. In the **Status Polling** section, specify the **Polling Interval**, which is the frequency that NAC Manager will poll the NAC Appliances to determine appliance status.
5. When communicating with NAC appliances for status polling, the **Length of Timeout** specifies the amount of time NAC Manager waits before determining that contact has failed. If NAC Manager does not receive a response from an appliance in the defined amount of time, NAC Manager will consider the appliance to be "down" and the appliance icon will change from a green up-arrow to a red down-arrow in the left-panel tree. The appliance status refers to Messaging connectivity, not SNMP connectivity. This means that if the appliance is "down," NAC Manager will not be able to enforce a new configuration to it.
6. In the **NAC Inactivity Check** section, you can enable a check to verify end-system NAC activity is taking place on the network. If no end-system activity is detected, a NAC Inactivity event is sent to the NAC Manager Events view. You can use the Console Alarms Manager (in Console, Tools > Alarm/Event > Alarms Manager) to configure custom alarm criteria based on the NAC Inactivity event to create an alarm, if desired.
7. Click **OK**.

Related Information

For information on related windows:

- [Options Window, NAC Manager Options](#)

How to Set Up Access Policies and Policy Mappings

Access policies define the appropriate level of access to network resources allocated to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies defined in a NAC profile: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. When an end-system connects to the network, it will be assigned one of these access policies, as determined by the NAC profile assigned to the matching NAC rule and the end-system state.

In your NAC profiles, each access policy is associated to a *policy mapping* that defines exactly how an end-system's traffic will be handled when the access policy is applied.

A policy mapping specifies the policy role (created in Policy Manager) and other RADIUS attributes that will be included as part of a RADIUS response to a switch. The RADIUS attributes required by the switch are defined in the Gateway RADIUS Attributes to Send field configured in the [Edit Switch window](#). Policy mappings are configured in the [Edit Policy Mapping Configuration window](#).

How you set up your access policies depends on whether your network utilizes NAC Controller appliances and/or NAC Gateway appliances. In addition, if your network utilizes NAC Gateway appliances, your setup depends on whether your network contains EOS switches that support Policy, third-party switches that support RFC 3580, or switches that support RADIUS attributes that are defined manually.

For NAC Controllers:

If your network utilizes NAC L2/L3 controller appliances, the access policies specified in NAC profiles are mapped to policy roles that are defined in a default policy configuration already configured on the controller. It is recommended that you review this default policy configuration using the Policy Manager application. To do this, you must create a policy domain in Policy Manager specifically for the NAC Controller, assign the NAC Controller to the domain, then import the policy configuration from the device into Policy Manager (File > Import > Policy Configuration from Device). Review the policy roles and make any rule changes required for your environment. When you have finished

modifying the policy configuration, you must enforce it back to the NAC Controller.

For NAC Gateway Appliances:

If your network utilizes NAC Gateway appliances, the access policies specified in NAC profiles are mapped to policy roles that must be created and defined in NetSight Policy Manager and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, NAC Manager lets you associate your policy roles to a VLAN ID or VLAN Name using the Policy Mappings editor. This allows your NAC Gateway appliances to send the appropriate VLAN attribute instead of a policy role to those switches that are RFC 3580-enabled.

Policy mappings have a Location option that allows different VLAN IDs to be returned for a policy based on the location the authentication request originated from. This is useful in networks that may have a VoIP/voice VLAN that is defined on multiple switches, but that VLAN maps to a unique VLAN ID on each switch. (For more information, see the section on Location in the [Edit Policy Mapping Configuration Window](#) Help topic.)

NOTE: If you have RFC 3580-enabled switches in your network, be sure to verify that the DHCP Resolution Delay Time option is set correctly in your Appliance Settings (Tools > Manage Advanced Configurations> Global and Appliance Settings). This option specifies the number of seconds a NAC appliance will wait after an authentication completes before attempting to resolve the end-system's IP address. When modifying this delay, keep in mind that for RFC 3580 devices, the appliance will link down/up a port to force the end-system to get a new IP address when NAC determines that the VLAN has changed. If the delay time specified is less than the amount of time the end-system needs to renew its IP address, then the NAC appliance may resolve the end-system's IP address incorrectly (to the previously held IP), or additional delay may be introduced as the resolution process attempts to resolve the address based on the configured retry interval. This is a problem when either registration or assessment is enabled: the registration process may never complete or may take an unacceptable amount of time to complete, or the NAC appliance could attempt to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Setting Up Your Access Policies

Before you begin working with NAC Manager, use these steps to define the policy mapping criteria (policy roles, corresponding VLAN IDs, etc.) that will be

available for selection for each access policy.

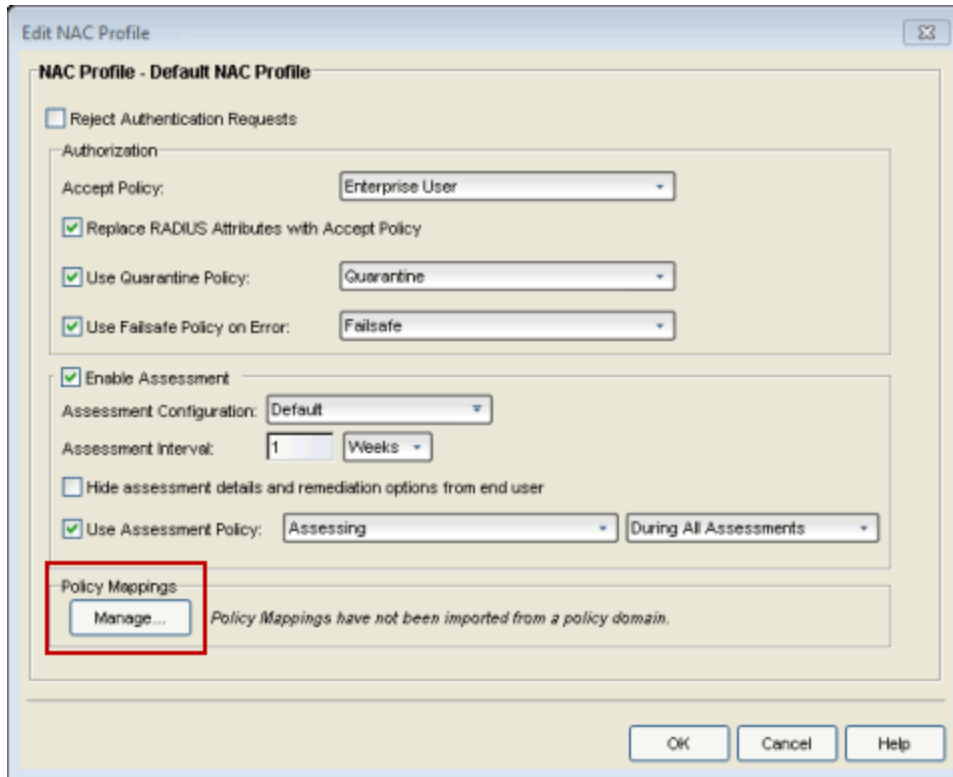
1. For each NAC profile, create a worksheet that lists the four NAC Manager access policies. For each access policy, associate a policy role (created in NetSight Policy Manager), and the policy role's corresponding VLAN ID, if you are using RFC 3580-enabled switches in your network. For a description of each NAC Manager access policy, and some guidelines for creating corresponding policy roles in Policy Manager, see the section on [Access Policies](#) in the Concepts file.

NOTE: If your network uses NAC Gateway appliances with only RFC 3580-enabled switches, instead of listing policy roles, simply create a list of policy names that correspond to the VLANs you will be using in your network. One tip is to use policy names that identify the corresponding VLAN name for ease of selection when you are creating your NAC profiles.

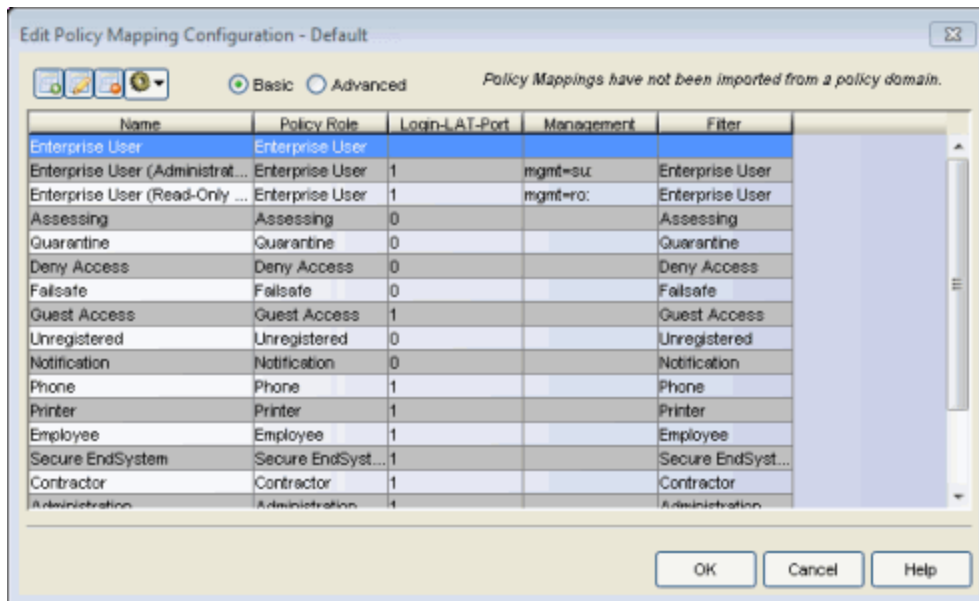
Here's an example of a worksheet for a NAC profile that contains both policy-enabled and RFC 3580 switches:

Access Policy	Policy Role	VLAN ID
Accept Policy	Enterprise User	[2] Enterprise User VLAN
Quarantine Policy	Quarantine	[4] Quarantine VLAN
Failsafe Policy	Failsafe	[5] Failsafe VLAN
Assessment Policy	Assessing - Strict	[6] Assessing - Strict VLAN

2. For NAC Controllers, use Policy Manager to verify that the policy configuration contains the required policy roles, and that the configuration has been enforced to the NAC Controller. See the [instructions](#) above.
3. For NAC Gateways, verify that each policy role listed on your worksheet has been created in NetSight Policy Manager and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, verify that your VLANs have been created on the switches in your network.
4. Define the policy mappings that map each NAC Manager access policy to the appropriate policy role as specified in your worksheet.
 - a. From the [New/Edit NAC Profile window](#), click the **Manage** button in the Policy Mappings section.



b. The [Edit Policy Mapping Configuration window](#) opens.

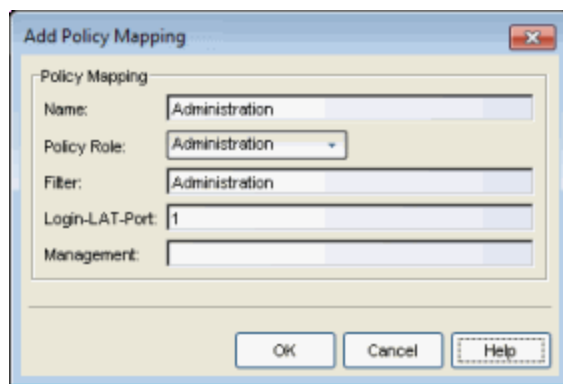


c. In the Edit Policy Mapping Configuration window, select between a Basic policy mapping and an Advanced policy mapping, depending on your network needs. Typically, the Basic policy mapping

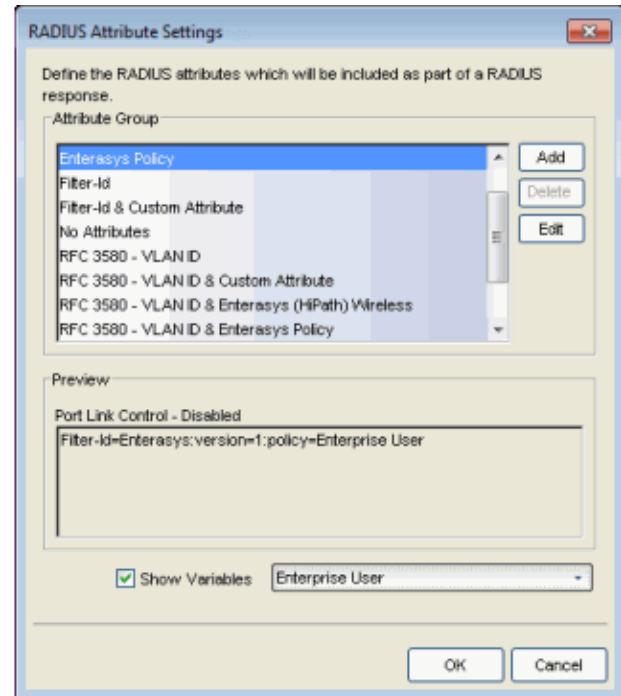
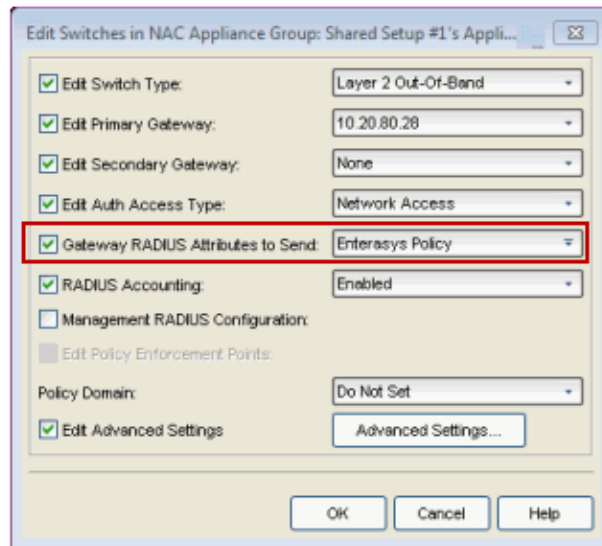
configuration is used unless your devices require customization or you will be using locations in your mappings.


You will see that NAC Manager provides a list of default policy mappings that you can use. Be aware that if you use one of the default mappings, you still need to verify that the policy role specified in the mapping is part of your NAC Controller policy configuration and/or is created and enforced to the policy-enabled switches in your network via Policy Manager.

- d. To add a new policy mapping, click the **Add new mapping** toolbar button to open the [Add Policy Mapping window](#).



For the new policy mapping, enter a mapping name and specify a policy role (created in Policy Manager) and other required RADIUS attributes that will be included in the RADIUS response to a switch. Click **OK** to add the mapping. Note that the required RADIUS attributes for your switches are defined in the Gateway RADIUS Attributes to Send field configured in the [Edit Switch window](#), as shown below.



- e. You can also use the configuration menu button  to access options for managing the import and export of mappings.
- Import from File** - Opens a window where you can select a file for importing policy mappings. In the file, policy mappings must be listed one mapping per line using the following format. (Fields in brackets < > are optional; all other fields are required.)
 Name, PolicyName, Location, VlanName, VlanId,
 <LoginLATGRoup>, <LoginLATPort>, <Management>, <Filter>,
 <Custom1>, <Custom2>, <Custom3>, <Custom4>, <Custom5>
 For example: Assessing, Assessing, Any, Default VLAN, 1,
 Assessing, 0, , Assessing
 For an explanation of the different fields, see the [Add Policy Mapping window](#) Help topic.
 - Import from Policy Manager Domains** - This operation creates new Policy Mappings in NAC Manager based on policy roles and corresponding VLANs imported from Policy Manager. It also updates VLAN information for the mappings if the mappings already exist in NAC. The import will remove mappings from NAC Manager if the policy no longer exists in Policy Manager

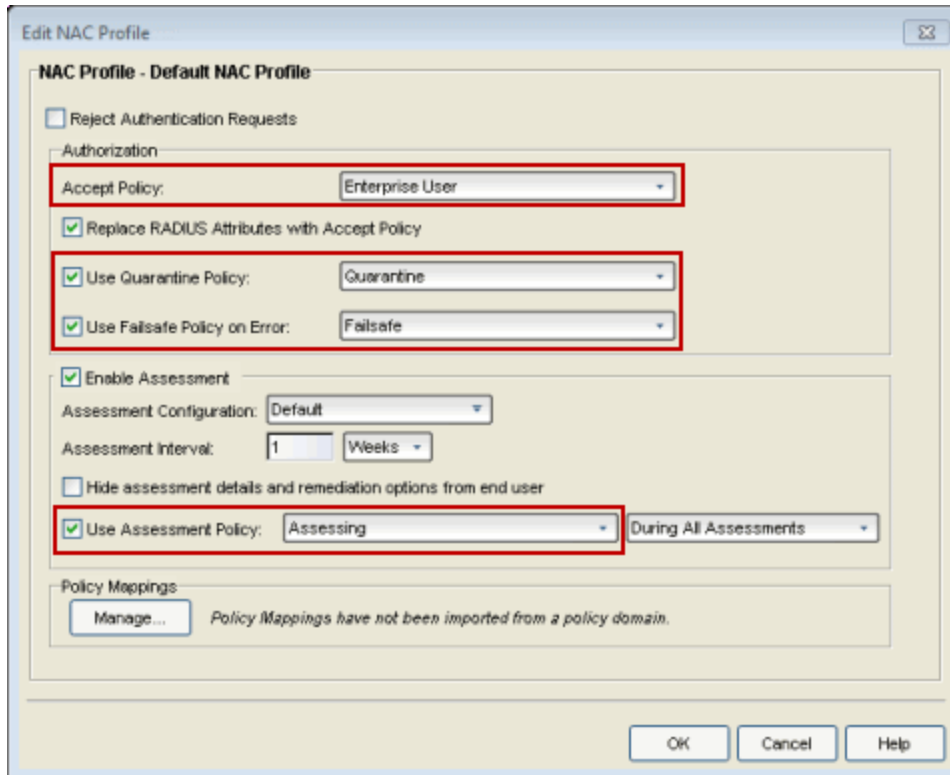
and is not being used by NAC Manager (via a NAC profile). If the policy is being used, the policy name will be cleared. This will result in an error notification on enforce of the NAC configuration to the NAC appliance.

This operation should not be used if policy mapping attributes are being managed outside of Policy Manager. An example would be a scenario in which RFC 3580-capable third-party devices participate in NAC, where default policy mapping names (Enterprise User, Accessing, etc.) have been updated to define VLAN information that is not configured in policy roles of the same name that exist in Policy Manager which is used to configure EOS switches. If this scenario exists, and the duplicate-named policy roles are imported, the existing VLAN information will be overwritten by the import.

- **Export to Policy Manager Domain** - This operation will export the selected policy mappings to a policy domain. It will verify that VLANs in the policy mappings exist in the policy domain. You can select an option to set the VLANs to forward as tagged and existing VLANs will be updated. The operation will also verify that policies referenced in NAC exist in the policy domain. Missing policies will be added as roles.
- **Clean Up Policies Missing from Policy Manager** - Opens a window that lists any policies that are not defined in Policy Manager, allowing you to remove mappings or clear policies from NAC Manager if the policy no longer exists in Policy Manager **and** is not being used by NAC Manager in a NAC profile. If the policy is being used in a NAC profile, only the policy name will be cleared. Do not select mappings for policies that are being managed outside of Policy Manager, for example, for third-party devices.

f. Click **OK** to close the Edit Policy Mapping Configuration window.

5. In your NAC profile, you will see your policy mappings available for selection when you define your Accept, Quarantine, Failsafe, or Assessment access policy.



Related Information

For information on related windows:

- [Edit Policy Mapping Configuration Window](#)
- [Add/Edit Policy Mapping window](#)
- [Access Policies, Concepts](#)

Toolbar

The toolbar on the main window provides easy access to certain NAC Manager functions.



Exit

Exits the NAC Manager application. This button serves the same function as the **File > Exit** menu option.



Authorization/Device Access

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in Extreme Management Center applications. This button serves the same function as the **Tools > Authorization/Device Access** menu option.



Server Information

Opens the Server Information window where you can view and configure certain Management Center Server functions, including management of client connections, locks, and licenses. This button serves the same function as the **Tools > Server Information** menu option.



Enforce All

Writes NAC configuration information to all Extreme Access Control engines. This button serves the same function as the **Tools > Enforce All** menu option.



Setup Wizard

Opens the Setup Wizard which assists you with first-time engine setup and configuration. This button serves the same function as the **Tools > Setup Wizard** menu option.



Search For End-Systems

Opens the [Search for End-Systems window](#) where you can search your NAC Manager database for end-systems that match the search criteria you select.



Manage NAC Configurations

Opens the [NAC Configuration window](#) where you can view and edit the selected NAC configuration. This button serves the same function as the **Tools > Management and Configuration > NAC Configurations** menu option.



Manage Rule Groups

Opens the [Manage Rule Groups window](#) where you can view and edit the defined rule groups and also add new rule groups for use in your NAC configuration. This button serves the same function as the **Tools > Management and Configuration > Rule Groups** menu option.



Manage NAC Profiles

Opens the [Manage NAC Profiles window](#) where you can view and edit the seven system-defined NAC profiles that define the authorization and assessment requirements for the end-systems connecting to the network. You can also use the window to define new profiles. This button serves the same function as the **Tools > Management and Configuration > NAC Profiles** menu option.



Manage Assessment Settings

Opens the [Manage Assessment Settings window](#) where you can manage and configure the assessment servers that perform the end-system assessments in your network. This button serves the same function as the **Tools > Management and Configuration > Assessment Settings** menu option.



Manage Notifications

Opens the [Manage Notifications window](#) where you can view created notifications, and enable, add, edit, and test specific notification rules. This button serves the same function as the **Tools > Management and Configuration > Notifications** menu option.



Registration Administration

Opens the Registration Administration web page where you can view registered devices and users, and manually add, delete, and modify users. This button serves the same function as the **Tools > Registration Administration** menu option.



Identity and Access Dashboard

Opens the [Control tab](#) where you can access NAC Manager end-system data via Management Center. This button serves the same function as the **Tools > Identity and Access Dashboard** menu option.



Help

Launches the NAC Manager Help, and displays detailed information about the currently selected right-panel tab. This button serves the same function as the **Help > About This Window** menu option.

How to Update Extreme Access Control Engine Server Certificates

This Help topic describes how to replace the following server certificates used by the Extreme Access Control engine:

- Captive Portal Server Certificate - Used for remediation and registration web pages on the Access Control engine.
- Internal Communications Server Certificate - Used for communication between the engine and the Extreme Management Center server, other Access Control engines, and Access Control assessment servers. It is also used for the Access Control administrative web pages.
- RADIUS Server Certificate - Sent to end-systems during certain forms of 802.1X authentication (EAP-TLS, PEAP, and EAP-TTLS).

NOTE: Management Center automatically generates alarms as the Access Control Engine Internal Communications Server Certificate, the Captive Server Portal Server Certificate, the RADIUS Server Certificate, the AAA Configuration Truststore, and the Access Control Engine Truststore approach their expiration date. Management Center generates a Notification alarm 30 days before expiring, a Warning alarm 7 days before expiring, and a Critical alarm when the certificate expires.

During installation, a new, unique private server key and server certificate is generated for each server. While these provide secure communication, there may be cases where you want to update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which NAC Manager must communicate. Additionally, you may want to use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages.

You need a server private key and server certificate to perform the certificate replacement. If you do not have these, this topic also includes procedures that can be used to generate them.

Some instructions in this Help topic use OpenSSL software to perform certain tasks. OpenSSL is available on the Management Center engine, the Access Control engine, or can be downloaded from <http://www.openssl.org>. After downloading and installing OpenSSL, add the OpenSSL tool to your path using the instructions in the Management Center and Access Control Secure

Communication Help topic section How to Add OpenSSL to Your Path. Other software tools can be used to perform these tasks, if desired.

Instructions on:

- [Certificate Requirements](#)
- [Replacing the Certificate](#)
- [Verifying the Certificate](#)
- [Generating a Server Private Key and Server Certificate](#)

Certificate Requirements

You need the RSA or DSA server private key (in PKCS #8 format) that was used to generate the server certificate. For "browser-friendly" certificates, the server certificate should identify the Access Control engine by its fully qualified host name. If you do not have the server private key and server certificate, refer to the [instructions for generating](#) them.

If your certificate authority (CA) provides additional intermediate certificates, you need to provide those as well. The intermediate certificates can be used in whatever format the CA provides them. They may be in individual files, in a bundle file, or even in the same file as the server certificate.

NOTE: if you need to convert your key file to a PKCS #8 format, use the following OpenSSL command where <server.key> is the original non-PKCS #8 formatted key file. (OpenSSL is available on Management Center and Access Control engines. The server.key file can be copied and converted on either engine.)

```
openssl pkcs8 -topk8 -in <server.key> -out server-pkcs8.key -nocrypt
```

Replacing the Certificate

The following steps assume that you have a replacement server private key and server certificate ready to use. If you do not, refer to the [Generating a Server Private Key and Server Certificate](#) section below. Be aware that the replacement operation stops communication on the server's secure ports for a small period of time (about 15 seconds).

NOTE: If the Captive Portal server certificate identifies the engine by a fully qualified host name, be sure the captive portal is configured with the Use Fully Qualified Domain Name option enabled in the Edit Captive Portal window, [Network Settings](#) view. Verify that end users are routed to the captive portal with the engine's fully qualified host name (the same name used on the certificate) instead of IP address in the portal URL and that there are no unexpected browser warnings. If the option is not enabled, then end users may get certificate warning messages in their browsers about the wrong server name. This happens because the IP address in the URL does not match the domain name in the server certificate.

NOTE: If you are updating the Internal Communications server certificate, be aware that other Management Center components may be affected by the change and stop trusting the server. Management Center clients and other servers must be configured to handle updated certificates using the client certificate trust mode and server certificate trust mode settings. Before updating the Internal Communications server certificate, be sure that the client and server trust modes are configured to trust the new certificate. For more information, see the Suite-Wide Tools Server Information Help topics Update Client Certificate Trust Mode window and Update Server Certificate Trust Mode window.

To replace the server private key and server certificate:

1. In NAC Manager, select the All NAC Appliances folder in the left-panel tree. In the right-panel [NAC Appliances tab](#), right-click on the desired engine and select Manage Appliance Certificates. The [Manage Appliance Certificates window](#) opens.
2. Click the **Update Certificate** button for the certificate you wish to replace. The Server Certificate window for that certificate opens.
3. If you are updating the Captive Portal server certificate or the Internal Communications server certificate, select the option to provision a private key and certificate from files. For the RADIUS server certificate, go to step 4.
4. In the Private Key section, provide a file containing the private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field.
5. In the Certificate Files section, use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

6. Click **OK**. You see a confirmation window listing your file information so that you can confirm that the information you have provided is correct. Click **Yes** to proceed with the certificate replacement. The private key and server certificate are updated in the engine configuration in the Management Center database.

NOTE: If there are Extreme Access Control (Access Control) engines or assessment servers on your network that are running NAC Manager version 4.0.0 or earlier, a warning displays stating that changing the certificate may interfere with communications between servers. Unless you have taken steps to ensure that installing the new certificate does not cause a communication problem, you should not continue with replacing the certificate.

7. Enforce the engine to deploy the new private key and server certificate. When enforced, the server's secure ports are offline for 15 seconds to reload the certificate:
 - Captive Portal Server Certificate - port 443.
 - Internal Communications Server Certificate - port 8444. Additionally, if the Agent-Based Assessment Server Certificate is configured to use the Internal Certificate, port 8443 is offline.

If you have replaced the RADIUS Server certificate, the RADIUS server on the engine is restarted to automatically to load the new certificate.

Verifying the Certificate

Once you have installed the new certificate, use the following steps to verify that the server is using the updated certificate.

Verifying the Captive Portal Server Certificate

Once the new server certificate is installed and the captive portal web server has restarted, use one of the following methods to verify that the server is now using the proper server certificate.

Use a Browser

1. Access the Registration Administration web page at `https://<Access Control Engine FQDN>/administration`. To eliminate browser warnings, verify that no browser warnings display when you access the web page.

2. Then, use your browser to view the certificate used:
 - Internet Explorer 7.0 or later: View > Security Report > View Certificates
 - Mozilla Firefox 3.5 or later: Tools > Page Info > Security > View Certificates

Use OpenSSL

1. Use OpenSSL to test the server connection with the following command:
`openssl s_client -connect <Access Control Engine Name or IP address>:443`
2. The output from this program includes a section titled "Certificate chain". This enumerates the certificates returned by the server. For each certificate, the Subject and the Issuer display. With multiple certificates, if the certificates are in the proper order, the issuer of each certificate matches the subject of the following certificate. Here is a sample output from the program:

```
Certificate chain
0 s:/O=mynac.enterprise.com/OU=Domain Control Validated/CN= mynac.enterprise.com
  i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
  repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
  repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
  i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
2 s:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
  i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
3 s:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
  i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
```

3. Close the program by typing Ctrl-C.

Verifying the Internal Communications Server Certificate

Once the new server certificate is installed, use one of the following methods to verify that the server is now using the proper server certificate.

Use a Browser

1. Access the Access Control Engine Administration web page at `https://<Access Control Engine FQDN>:8444/Admin/`. If your intention was to eliminate browser warnings, verify that no browser warnings are displayed when you access the web page.

2. Then, use your browser to view the certificate used:
 - Internet Explorer 7.0 or later: View > Security Report > View Certificates
 - Mozilla Firefox 3.5 or later: Tools > Page Info > Security > View Certificates

Use OpenSSL

1. Use OpenSSL to test the server connection with the following command:
`openssl s_client -connect <Access Control Engine Name or IP address>:8444`
2. The output from this program includes a section titled "Certificate chain". This enumerates the certificates returned by the server. For each certificate, the Subject and the Issuer are displayed. With multiple certificates, if the certificates are in the proper order, the issuer of each certificate matches the subject of the following certificate. Here is a sample output from the program:

```
Certificate chain
0 s:/O=mynac.enterprise.com/OU=Domain Control Validated/CN= mynac.enterprise.com
  i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
  repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
  repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
  i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
2 s:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
  i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
3 s:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
  i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
  Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
```

3. Close the program by typing Ctrl-C.

Generating a Server Private Key and Server Certificate

If you do not have a server private key and server certificate to use as a replacement, you can generate them using the instructions in the sections below. You need to:

1. Generate a server private key. Use OpenSSL to generate an RSA key.
2. Create a Certificate Signing Request.
3. Submit the request to a Certificate Authority or generate a self-signed certificate.
4. Verify the contents of the server certificate.

You can use the following steps regardless of whether you are using a commercial certificate authority or an in-house certificate authority.

Generate a Server Private Key

Use the following steps to generate an encrypted RSA private key.

1. Enter the following command to use OpenSSL to generate a password-encrypted PKCS #8 formatted server private key file. Use the key size and output file name you prefer. (If you are unsure of the key size, use 2048.)

```
openssl genrsa <key size> | openssl pkcs8 -topk8 -out <output file>
```

For example:

```
openssl genrsa 2048 | openssl pkcs8 -topk8 -out server.key
```

2. You are prompted for an Encryption Password. Be sure to make a note of the password that you enter. If the password is lost, generate a new server private key and a new server certificate.

Create a Certificate Signing Request

Use the following steps to create a Certificate Signing Request (CSR).

1. Enter the following command to generate a CSR file. Use the output file name you used in [step 1 above](#) as the input file, and specify the output file name you prefer:

```
openssl req -new -key <input file> -out <output file>
```

For example:

```
openssl req -new -key server.key -out server.csr
```

2. You are prompted for information that appears in the certificate. When you are prompted for a Common Name, specify the fully qualified host name of the Access Control engine. For example:

```
Common Name (eg, YOUR name) []:nac1.mycompany.com
```

If you are creating a client and/or server certificate CSR request for use with PEAP or EAP-TLS, you may need to add an extension to the command used to generate the CSR file. Server and client certificates require an extension in order to operate as intended. Verify with your certificate vendor whether they require that the extensions are part of the CSR or are included in the certificate when the

request is made. The following are command examples of the CSR request that include each of the extension options available.

- If the CSR is for the Access Control engine, the command must include:

```
openssl req -new -reqexts server_auth -key <input file> -out <output file>
```
- If the CSR is for a client, the command must include:

```
openssl req -new -reqexts client_auth -key <input file> -out <output file>
```
- If the CSR is for both the Access Control engine and client, the command must include:

```
openssl req -new -reqexts server_and_client_auth -key <input file> -out <output file>
```

Submit the Request to a Certificate Authority

The procedure for submitting a CSR to a Certificate Authority (CA) varies with the service used. Usually, it is done through a website using a commercial service such as VeriSign. You can also use an in-house CA, which generates certificates used internally by your enterprise. Provide information including the contents of the CSR and receive back one or more files containing the server certificate and possibly other certificates to be used in a chain.

Verify the Contents of the Server Certificate

It is important to verify that the new server certificate contains the data you supplied when creating the CSR. In particular, make sure the Common Name (CN) is the fully qualified host name of the Access Control engine.

Use OpenSSL to view the contents of the server certificate file `server.crt` using the following command:

```
openssl x509 -in server.crt -text -noout
```

How to Use Device Type Profiling

This Help topic describes how to set up device type profiling in your NAC Configuration using device type rule groups. Device type profiling lets you assign NAC profiles to end-systems based on operating system family, operating system, or hardware type. This allows you to use the end-system's device type to determine the end user's level of network access control and whether the end-system will be scanned. For more information on device type groups, see the [Add/Edit Device Type Group Window](#) Help topic.

NOTE: Assessment provides the most accurate determination of device type. If the initial device type determination is not based on assessment results, it may be less reliable. For that reason, device type rule groups should be based on broad families of device types.

Here are some examples of how device type profiling can be used to determine network access:

- When an end user with valid credentials logs in to the network on a registered iPad versus a registered Windows 7 machine, they receive a lower level of network access.
- When an end user registers a Windows machine using its MAC address, another user cannot spoof that MAC address using a Linux system. (Device profiling will not resolve this issue in environments with dual boot machines.)
- If an end user exports a certificate from a corporate PC to an iPad and successfully authenticates with 802.1x, the iPad is not allowed full network access.

Device Profiling Use Case

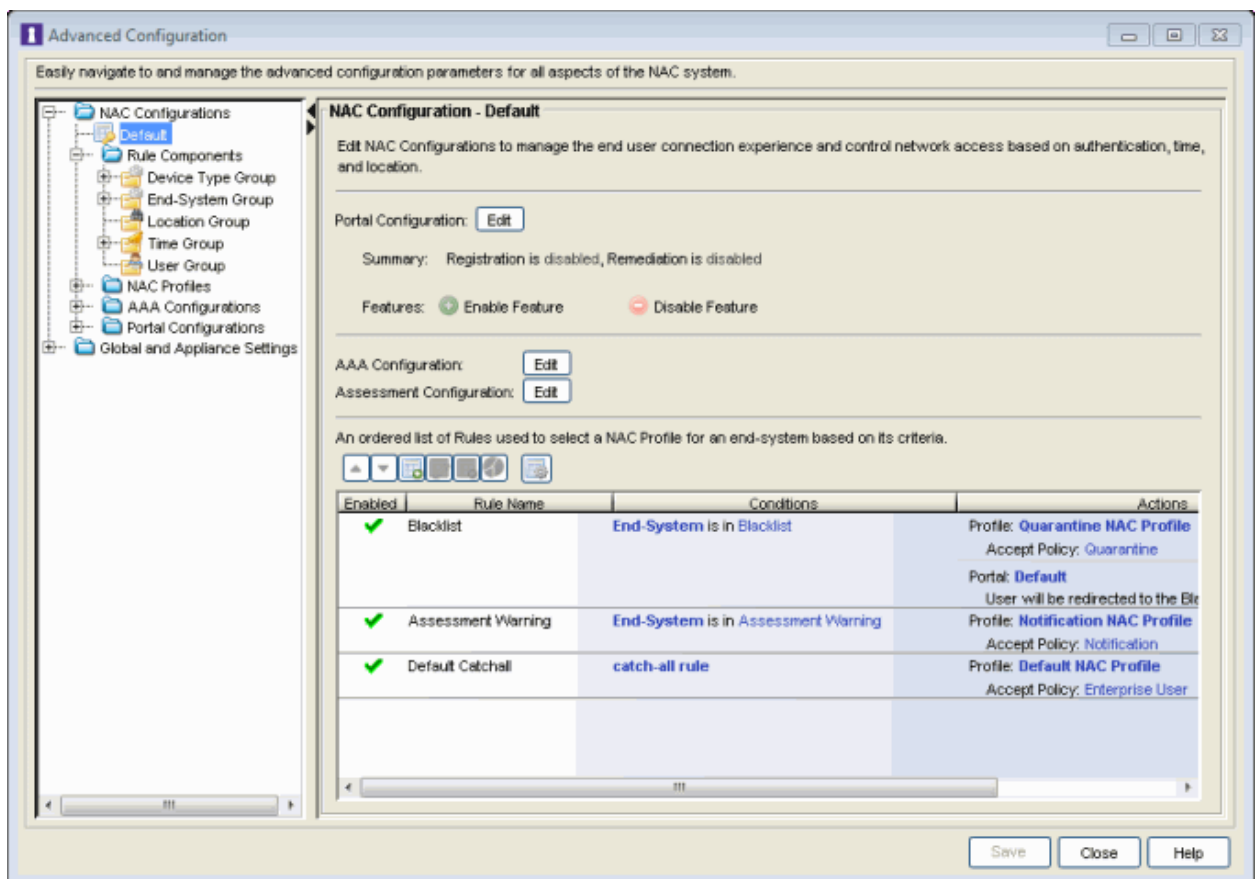
This section provides high-level instructions for configuring device type profiling for a sample use case. In this scenario, the network administrator has the following network access requirements:

- All Windows registered devices should be assigned the "Basic Profile."
- All Windows 7 registered devices should be assigned the "Windows7 Profile."

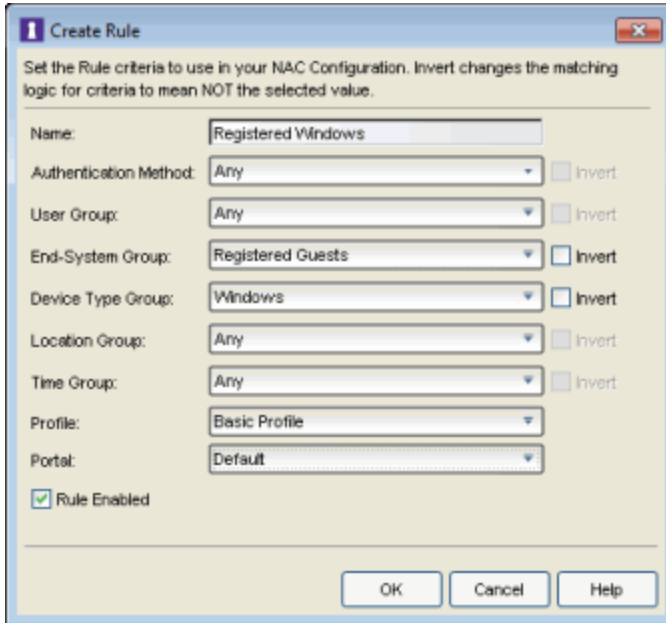
- All Linux registered devices should be assigned the "Basic Profile." In addition, a new Linux version called SuperLinux needs to be added to the Linux family device type.
- All HP Printers should be assigned the "HP Printer Profile."

To do this, you will need to create four rules in your NAC configuration that use device type as criteria for matching rules to end-systems authenticating to the network. The following instructions assume that you have already created your profiles: Basic Profile, Windows7 Profile, and HP Printer Profile.

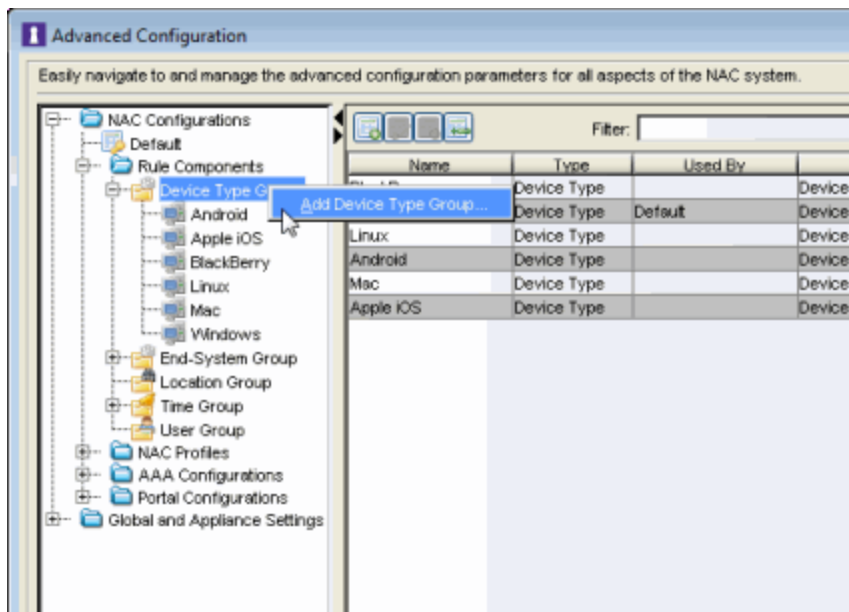
1. Open the Advanced Configuration window (Tools > Management and Configuration > Advanced Configurations).



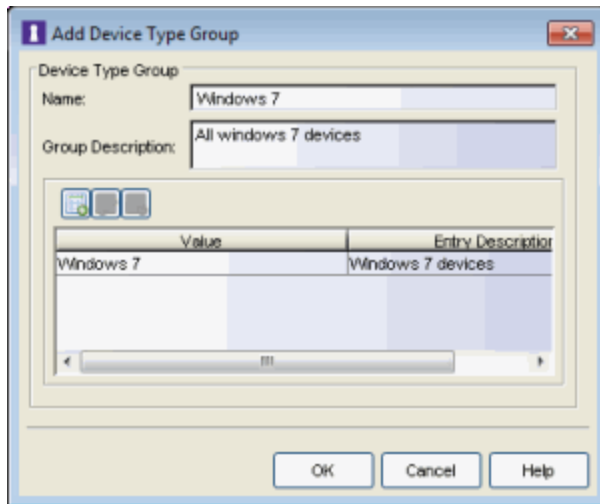
2. Create a rule that assigns the Basic Profile to all Windows registered devices.



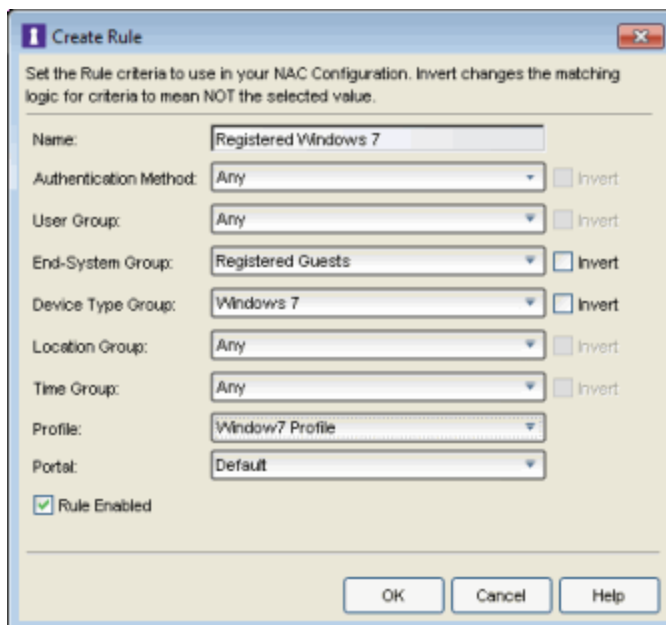
3. Create a rule that assigns the Windows7 Profile to all Windows 7 registered devices. To do this, you will need to create a new Windows 7 device type group.
 - a. From the Advanced Configuration window, open the Add Device Type Group window.



- b. Create the Windows 7 device type group.

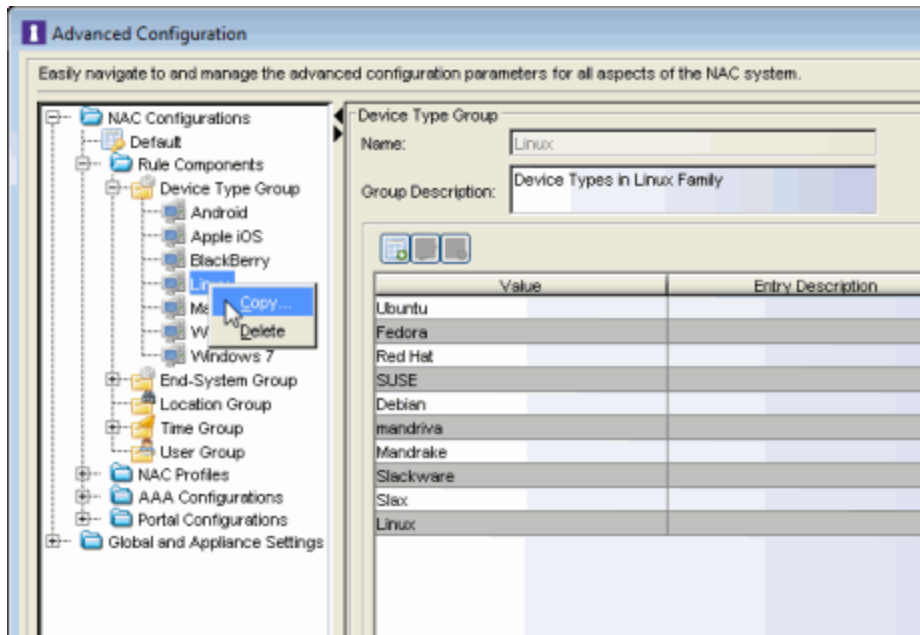


- c. You can then create the rule.

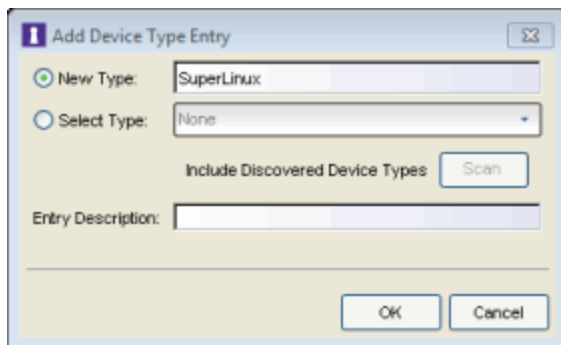


4. Create a rule that assigns the Basic Profile to all Linux registered devices and add the SuperLinux version to the Linux family device type. To do this, you will need to create a new Linux device type group that includes SuperLinux.

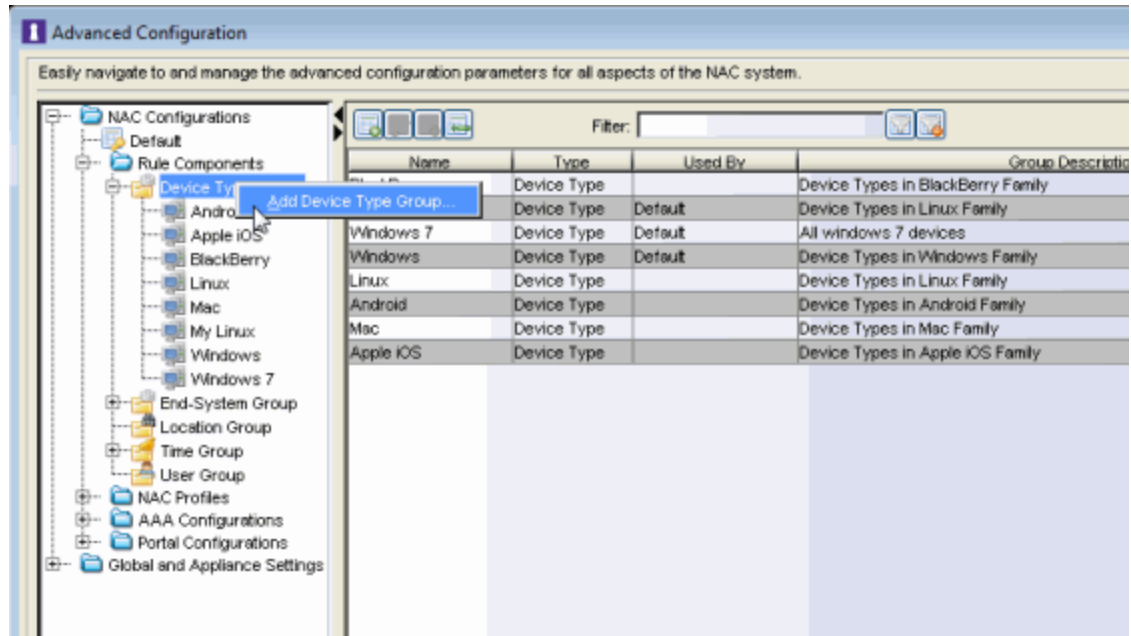
- a. Make a copy of the Linux device type group and name the new group My Linux.



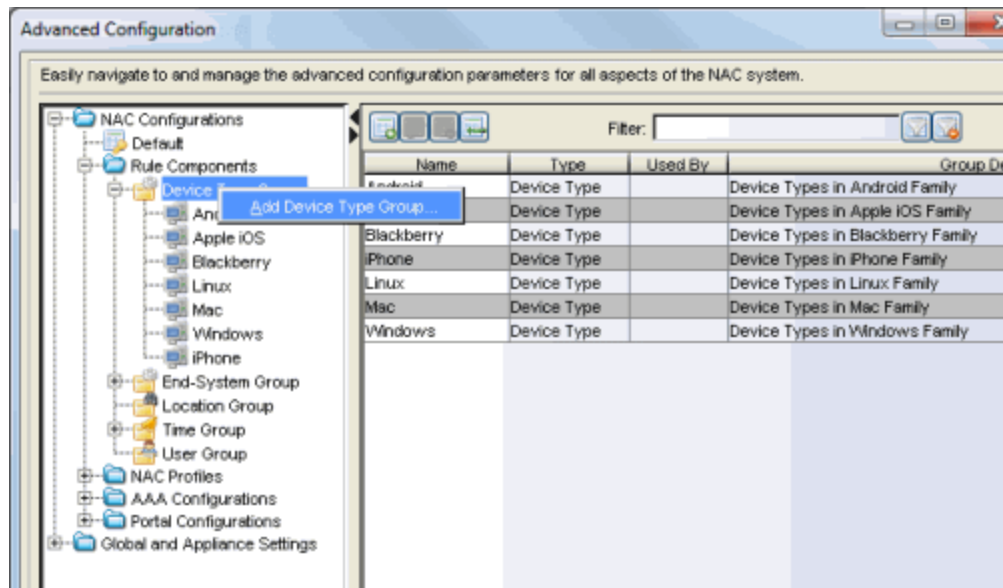
- b. Edit the My Linux device type group to include SuperLinux by adding a new device type entry.



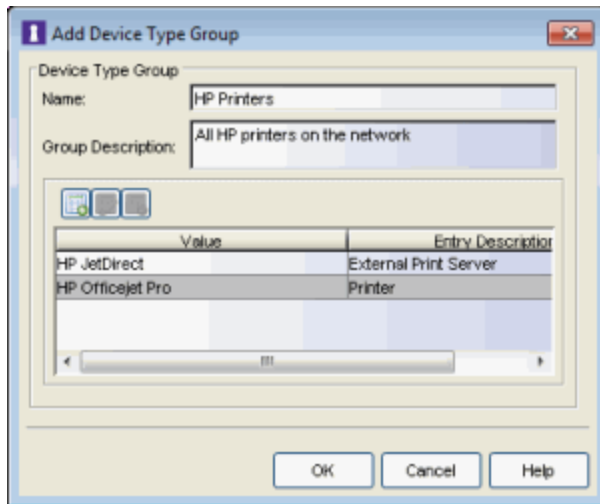
- c. You can now create the rule.



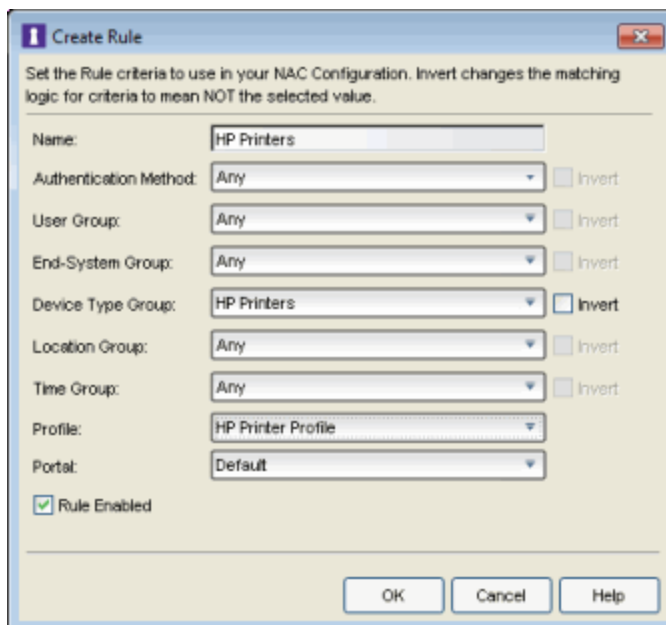
5. Create a rule that assigns the HP Printer Profile to all HP printers on the network. To do this, you will need to create a new HP Printers device type group.
 - a. From the Advanced Configuration window, open the Add Device Type Group window.



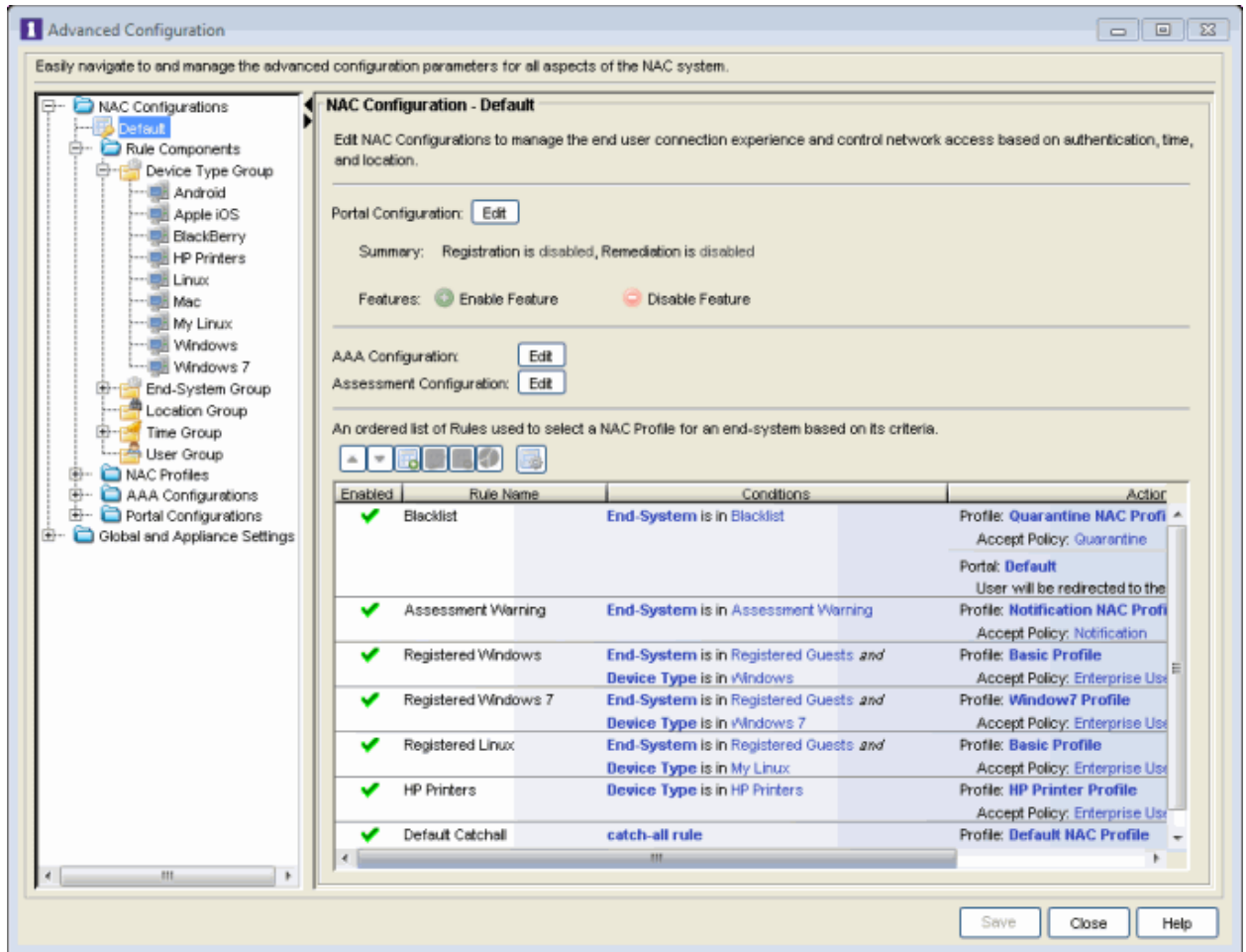
b. Create the HP Printers device type group.



c. You can then create the rule.



6. Your NAC Configuration now contains the following rules that will be used to determine network access and assessment requirements based on device type.



Related Information

- [Add/Edit Device Type Group Window](#)
- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

How to Verify RADIUS Configuration

This Help topic describes how to use the NAC Manager Verify RADIUS Configuration feature. The feature is available for NAC Gateway appliances and Layer 2 NAC Controllers, and can be used to alert you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network.

Switch RADIUS configurations can be modified independently of NAC; for example, they can be manually edited through the CLI, through Policy Manager, or by applying an archived switch configuration that was archived prior to the device being added to NAC. This can cause an authentication failure or a loss of visibility to the devices on the network. The Verify RADIUS Configuration tool can help you troubleshoot this problem.

For NAC Gateway appliances, the Verify RADIUS Configuration feature verifies the NAC Gateway's RADIUS configuration for each switch assigned to that appliance against the actual RADIUS configuration on the switch. The Verify feature compares the IP addresses and order of the primary and secondary gateways assigned to the switches, and the management RADIUS servers that are configured, if any. The feature also reports if SNMP connectivity cannot be established with the switch, or if RADIUS is disabled on the switch.

NOTE: The Verify feature will ignore any RADIUS servers on the switch that do not exist in the appliance RADIUS configuration. For example, if there are two management RADIUS servers configured on the switch, but only one is configured on the appliance, the Verify operation will ignore the extra server configured on the switch.

For Layer 2 NAC Controllers, the Verify RADIUS Configuration feature verifies that the NAC Controller Engine IP address and the redundant NAC Controller Engine IP address (if any) are configured as the RADIUS servers for the NAC Controller PEP. The Verify feature compares the IP addresses and order of the NAC Controller Engines assigned to the PEP. The feature also reports if SNMP connectivity cannot be established with the PEP, or if RADIUS is disabled on the PEP. If the Controller is in Hybrid Mode, the feature will verify both the PEP and the switches (if any).

Use the following steps to perform a Verify RADIUS Configuration operation:

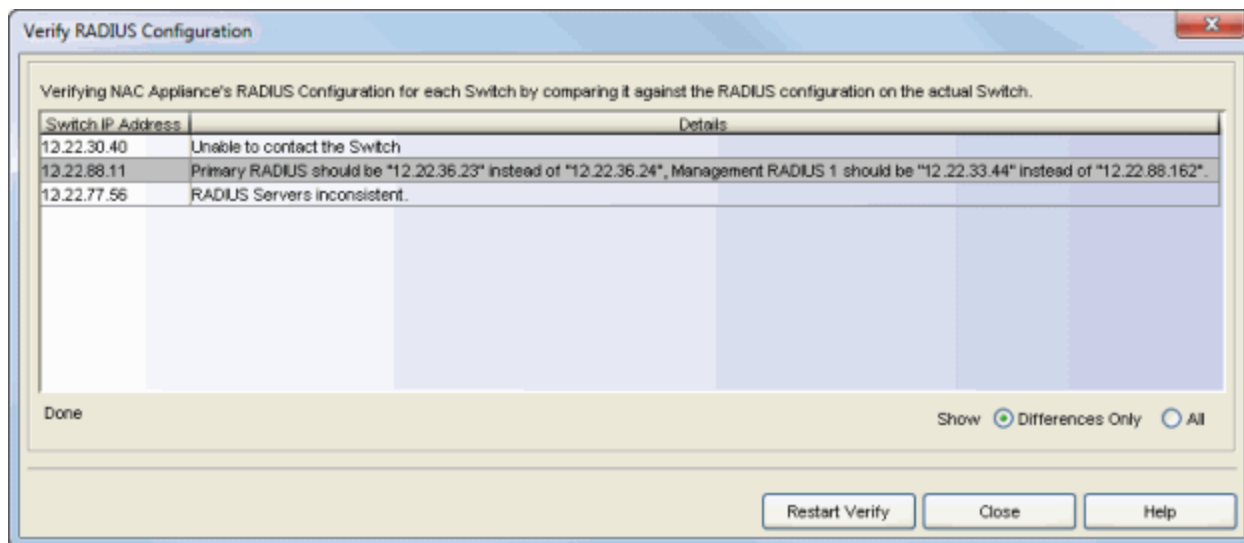
1. **For NAC Gateways:** To verify all the switches assigned to an appliance, right-click on a single appliance in the right-panel [NAC Appliances tab](#) and select Verify RADIUS Configuration from the menu. To verify select switches assigned to an appliance, right-click on one or more switches in the [Switches tab](#) for a single appliance, and select Verify RADIUS Configuration from the menu. A confirmation window opens; click **Yes** to continue with the Verify.

For Layer 2 NAC Controllers: Right-click on a single controller in the right-panel [NAC Appliances tab](#) and select Verify RADIUS Configuration from the menu. A confirmation window opens; click **Yes** to continue with the Verify.

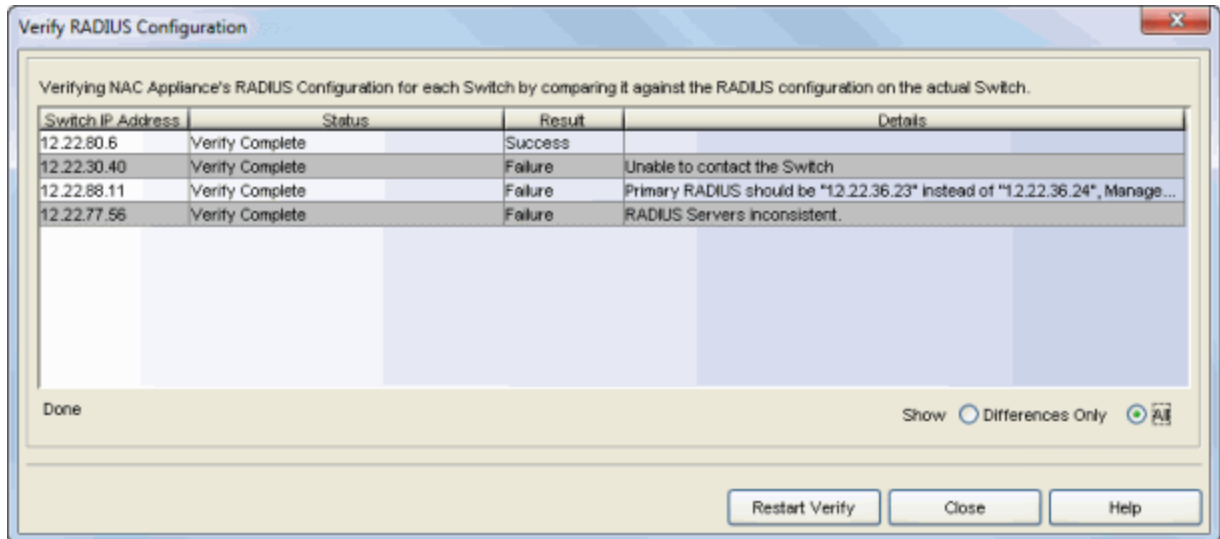
NOTE: While the Verify is running, you have the option to stop it, and then restart the Verify when you are ready.

2. The Verify RADIUS Configuration window opens, displaying the switches or PEP that failed verification or couldn't be contacted. The information in the Details section displays any problems reported by the Verify operation.

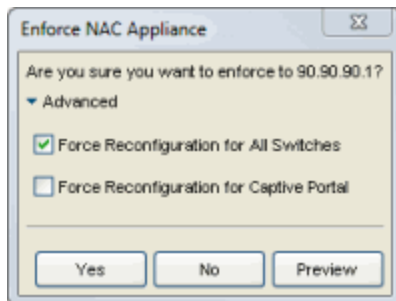
NOTE: For switches that support encrypted MIBs, only a minimal RADIUS configuration verification can be performed providing general information, such as "RADIUS Servers inconsistent."



You can use the radio buttons in the lower right corner of the window to select "Show All" to show all the switches/PEP that the Verify was performed against including those that passed verification.



- To sync up the appliance RADIUS Configuration, perform an enforce from NAC Manager to the NAC appliance with the Advanced option "Force Reconfiguration for All Switches" selected.



When enforcing to NAC Gateway appliances, the NAC Configuration is first written to the NAC Gateways and then the NAC Gateways will write the RADIUS configuration information to the switches. With NAC Controllers, the NAC Configuration is first written to the NAC Controller Engine and then the RADIUS configuration information is written to the NAC Controller PEP.

Related Information


- [Edit Switches in NAC Appliance Group Window](#)

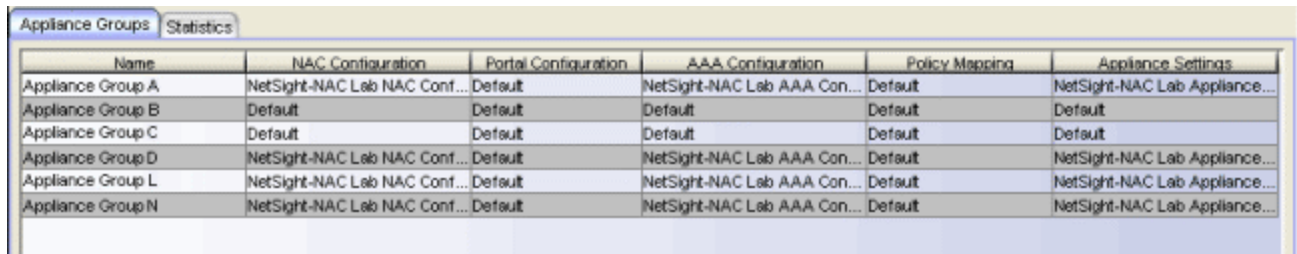
NAC Manager Right-Panel Tabs

The NAC Manager main window is divided into three panels: a left panel, a right panel, and a bottom panel. The right panel displays different tabs and information depending on the item selected in the left-panel tree. This section includes all the Help topics for the different right-panel tabs.

Appliance Groups Tab

The Appliance Groups tab displays in the right panel when you select the NAC Appliance Groups folder in the left panel. (The NAC Appliance Groups folder is only available if you create engine groups.) The tab displays a table of information about the engine groups in the folder.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Help topic on Table Tools.



Name	NAC Configuration	Portal Configuration	AAA Configuration	Policy Mapping	Appliance Settings
Appliance Group A	NetSight-NAC Lab NAC Conf...	Default	NetSight-NAC Lab AAA Con...	Default	NetSight-NAC Lab Appliance...
Appliance Group B	Default	Default	Default	Default	Default
Appliance Group C	Default	Default	Default	Default	Default
Appliance Group D	NetSight-NAC Lab NAC Conf...	Default	NetSight-NAC Lab AAA Con...	Default	NetSight-NAC Lab Appliance...
Appliance Group L	NetSight-NAC Lab NAC Conf...	Default	NetSight-NAC Lab AAA Con...	Default	NetSight-NAC Lab Appliance...
Appliance Group N	NetSight-NAC Lab NAC Conf...	Default	NetSight-NAC Lab AAA Con...	Default	NetSight-NAC Lab Appliance...

Name

The name of the engine group.

NAC Configuration

The NAC Configuration currently selected for this engine group.

Portal Configuration

If your network is implementing Registration or Assisted Remediation, the [Portal Configuration](#) that defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The AAA Configuration used by this engine group.

Policy Mapping

The Default policy mapping can be viewed in the Advanced Configuration tool (under NAC Profiles) or accessed from the Edit NAC Profile window.

Appliance Settings

The Appliance Settings configured for the group. Use the Edit Appliance Settings window to specify and configure engine settings.

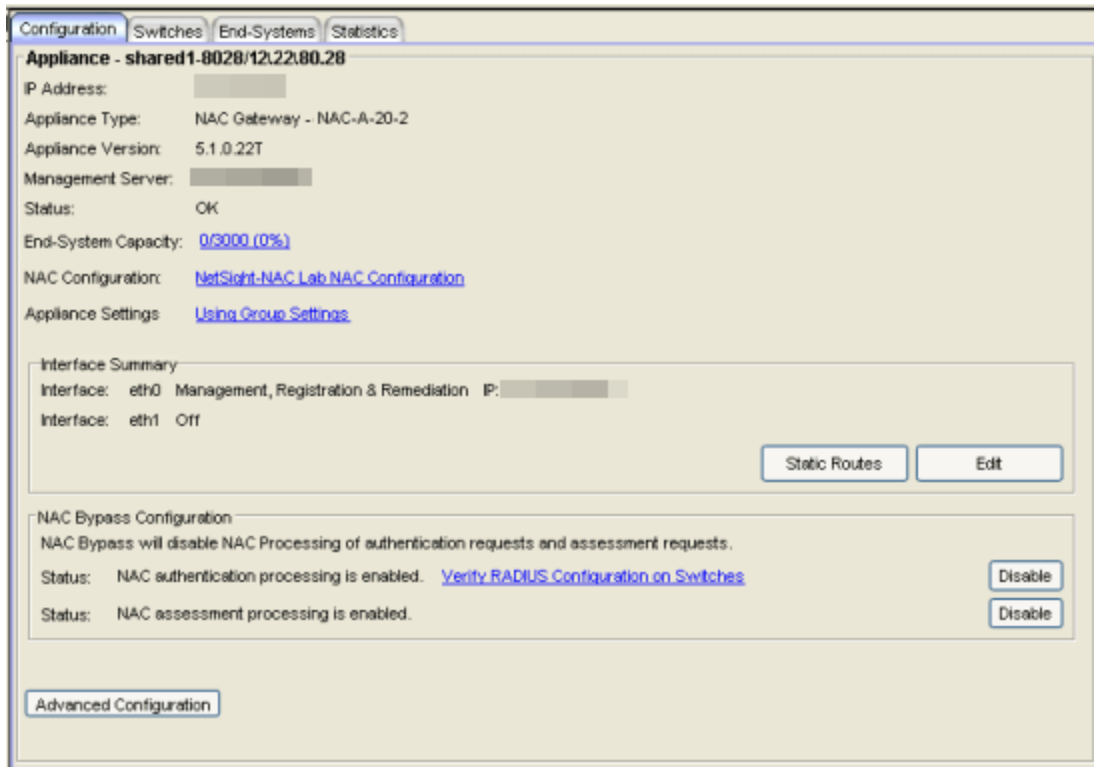
Related Information

For information on related windows:

- [Edit Portal Configuration Window](#)

Configuration Tab (Extreme Access Control Engine)

This tab provides information about a Extreme Access Control engine's configuration. The information changes depending on the type of engine selected in the left-panel tree. To access this tab, select an Access Control engine in the left-panel tree, then click the **Configuration** tab in the right panel.



General Information

This section displays general information about the Access Control engine, including its name, IP address, type (Access Control Gateway or Layer 2/Layer 3 Access Control Controller), the engine version, the IP address of the Extreme Management Center Management server, and the Access Control engine status.

End-System Capacity

This field lists the engine's current capacity, which is the number of end-systems that have authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the

engine.

Click the link to open a window where you can configure end-system capacity. Enter the desired end-system capacity and specify the features expected to be enabled on the engine including Authentication, Accounting, Registration, and Assessment. Note that the number of end-systems supported on an engine is affected by the number of features that are enabled. Configuring the maximum capacity when all features are enabled may impact performance. The window then displays the system requirements recommended for the specified capacity and feature set. Verify that the engine meets these system requirements or make adjustments, if necessary. Click **OK** to set the capacity and close the window. Enforce the engine.

NAC Configuration

Displays the NAC (Access Control) Configuration assigned to the engine. Click the NAC Configuration link to open the [Edit NAC Configuration window](#) where you can make changes to the configuration, if desired. The NAC Configuration determines what Access Control Profile is assigned to an end-system connecting to the network.

Appliance Settings

Click the Appliance Settings link to open the [Appliance Settings window](#) where you can access advanced configuration options for Access Control engines. The link indicates whether the engine is using Group Settings or has an engine settings override configured.

License Status

An Access Control virtual engine has an additional **License Status** field that displays whether the engine has a license allocated to it. For more information on virtual engine licensing, see the Suite-Wide Tools Server Information Window Help topic section on NAC VM license. The License Status field is also displayed if you are using a NAC Enterprise license. For more information, see [NAC Enterprise Licensing](#).

Interface Summary

Displays a summary of the current engine interface configuration. Click the **Static Routes** button to open the [Static Route Configuration window](#). Click the **Edit** button to open the [Interface Configuration window](#).

NAC Bypass Configuration

The NAC Bypass Configuration feature allows you to bypass NAC processing of authentication requests from end-systems connecting to the

network and also disable the Access Control assessment process. For Access Control authentication bypass, Access Control either configures the switch to authenticate directly to a RADIUS server to which Access Control is configured to proxy authentication requests, or it disables RADIUS authentication on the switch. This capability is useful for troubleshooting purposes. For example, if there is a problem with a Access Control Configuration, the **Disable** button lets you remotely disable NAC functionality until the problem is resolved. You can then use the **Enable** button to re-enable Access Control functionality on the engines. When Access Control authentication or assessment is disabled, the Access Control engine name and IP address display in red text in the left-panel tree indicating the engine is in Bypass mode.

For NAC Gateway engines, when you select the option to disable Access Control authentication processing, if proxy RADIUS servers are configured for authentication in a Basic AAA Configuration, the Access Control engine configures the switches to send RADIUS packets directly to the primary and secondary RADIUS servers (from the Basic AAA Configuration), instead of talking to the RADIUS proxy through the Access Control gateway. RADIUS authentication is not disabled on the switch, and end users still need to authenticate in order to connect to the network. The switches must be defined in the back-end proxy RADIUS server as RADIUS clients with the same shared secret used by the Access Control Gateway engines. If there are no proxy RADIUS servers configured in a Basic AAA Configuration, or if an Advanced AAA Configuration is used, RADIUS authentication on the switch is disabled when NAC authentication processing is disabled.

NOTES: If you have disabled Access Control authentication processing and then enforce with new switches, the new switches are configured to send RADIUS packets directly to the primary and secondary RADIUS servers. These switches are reconfigured to talk to the RADIUS proxy when you enable Access Control; a second enforce is not necessary.

Bypass is not an option for switches set to Manual RADIUS Configuration or ExtremeWireless controllers not configured for RADIUS strict mode.

For Access Control Controller engines, when you disable Access Control authentication, then the Access Control Controller does **not** send RADIUS packets directly to the RADIUS servers. Authentication **is** disabled on the Access Control Controller and end-systems do not need to authenticate to the network. Traffic from the end-systems bypass the Access Control

Controller and go directly onto the network.

The **Status** fields provide the current status of the Access Control authentication or assessment process. The authentication status field also includes a link to the Verify RADIUS Configuration on Switches feature. This feature is available for Access Control Gateway engines and Layer 2 Access Control Controllers, and can be used to alert you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network. For more information see [How to Verify RADIUS Configuration](#).

Controller PEP Settings

If the engine is a Layer 2 or Layer 3 Access Control Controller, this section displays the settings for the Access Control Controller Policy Enforcement Point (PEP). (This information is configured during the Access Control Controller Initialization procedure; for more information, refer to the Access Control Controller Hardware Installation Guide.) If a Redundant Controller has been configured, it is displayed here. Use the **Set Redundant Controller** button to specify or change the redundant controller, if desired.

Hybrid Mode

You must enable the global Hybrid Mode option in the [NAC Manager Advanced Settings option panel](#) in order to see this controller option for your Layer 2 Access Control Controllers. Once you have enabled the global Hybrid Mode option, you can enable or disable Hybrid Mode for each individual Layer 2 Controller here on the **Configuration** tab. Hybrid Mode allows a Layer 2 Controller to act as a RADIUS proxy for switches, like a Access Control Gateway engine. A [Switches tab](#) appears for the controller and the controller can now be used as a gateway. Like a gateway, an enforce must be performed for the switch configuration to take effect. Disabling Hybrid Mode when a controller has switches has a similar effect to deleting a gateway: the switches have the controller removed as a reference.

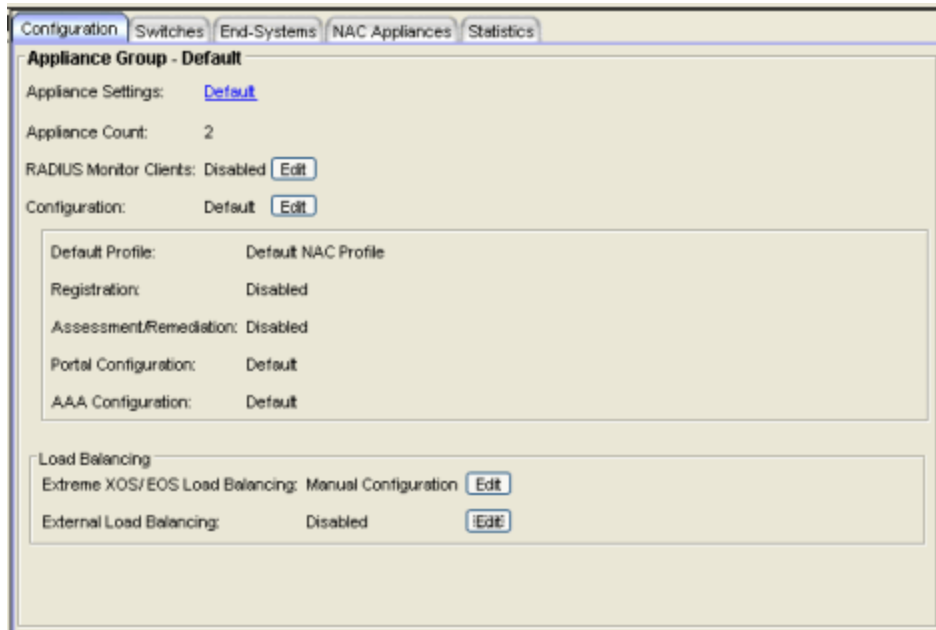
NOTE: A controller in Hybrid Mode functions exactly as a gateway when it comes to switches other than the Policy Enforcement Point (PEP). While Assessment/Remediation and Registration continues to work "out of the box" for the PEP end-systems, this is not the case for end-systems on the switches configured to use the controller as a gateway. You need to perform the Access Control Gateway configuration outlined in the [How to Set Up Assessment Remediation](#) and [How to Set Up Registration](#) Help topics.

Advanced Configuration Button

Opens the Access Control Appliance Advanced Configuration window where you can enable the distributed end-system cache option. This advanced option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. For more information, see the [Advanced Configuration](#) help topic.

Configuration Tab

This tab provides information about the [NAC Configuration](#) being used by your Extreme Access Control engines. To access this tab, select the All NAC Appliances folder or an Appliance Group folder in the left-panel tree, then click the **Configuration** tab in the right panel.



Appliance Settings

The engine settings configuration being used by your Access Control engines. Engine settings are configurable through the Advanced Configuration view, by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the Global and Appliance Settings folder.

Appliance Count

The number of engines under this folder.

RADIUS Monitor Clients

Displays whether RADIUS Monitor Clients are enabled for the Access Control engines in the folder. Click the **Edit** button to open the Configure RADIUS Monitor Clients window where you can configure RADIUS monitoring tools to monitor Access Control engine performance and availability. For more information, see Configure RADIUS Clients to Monitor NAC in the Monitor NAC Health section of the NAC Technical Reference.

Configuration

The name of the NAC Configuration being used by your Access Control engines. Click the **Edit** button to open the [Edit NAC Configuration window](#) where you can make changes to the configuration, if desired. The NAC Configuration determines what NAC Profile will be assigned to an end-system connecting to the network.

Default Profile

The name of the Default Profile specified in the NAC Configuration. The Default Profile serves as a "catch-all" profile for any end-system that doesn't match one of the rules listed in the NAC Configuration.

Registration

Whether a registration/web access feature is enabled or disabled for the NAC Configuration.

Assessment/Remediation

Whether the assessment/remediation feature is enabled or disabled for the NAC Configuration.

Portal Configuration

The name of the [Portal Configuration](#) specified in the NAC Configuration. If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The name of the [AAA Configuration](#) specified in the NAC Configuration.

Communication Channel

If your network has the Communication Channel feature enabled, you will see a menu where you can select a communication channel for the engine group. For more information, see [How to Configure Communication Channels](#). You will not see this field if the feature is not enabled.

Load Balancing


This section allows you to configure load balancing for the engine group. NAC Manager provides two different load balancing configuration options: either ExtremeXOS/EOS firmware on S-Series and K-Series devices, or utilizing external load balancers. Load balancing allows you to evenly distribute authentication requests and switch configuration ownership among your Access Control gateway engines. This can be useful in NAC Manager deployments with a large number of switches, where manual delegation of switch resources may be cumbersome.

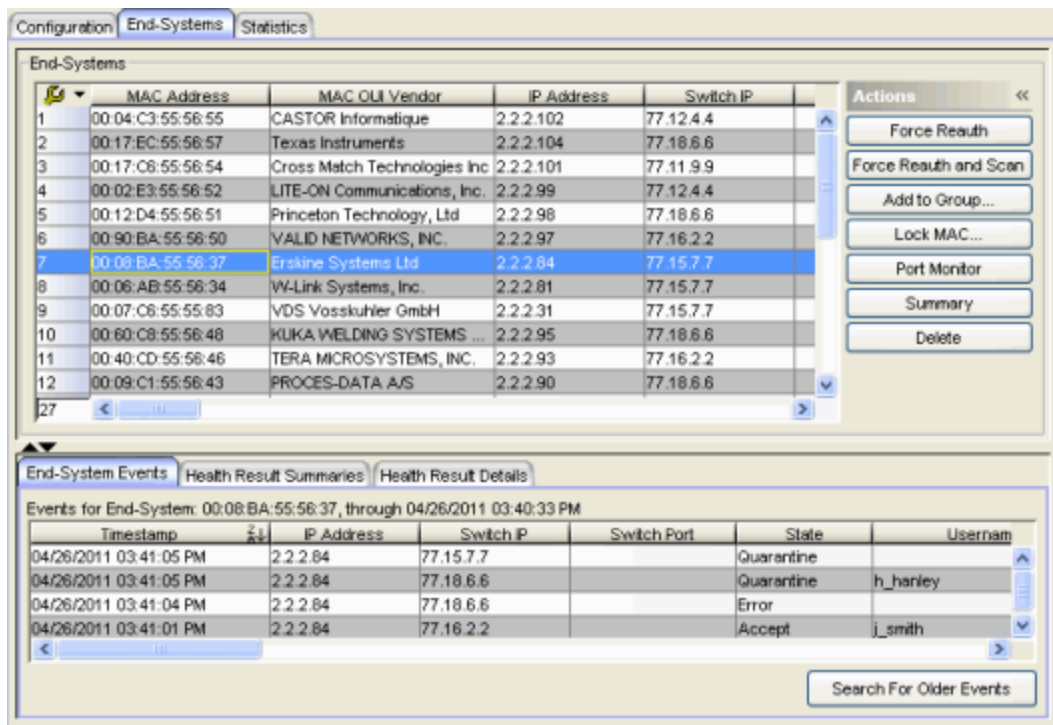
- **ExtremeXOS/EOS Firmware Load Balancing** – The default setting is **Manual Configuration**. Click the **Edit** button to open the **Configure Load Balancer(s)** window where you can select the load balancing algorithm as part of the RADIUS configuration on S-Series and K-Series devices. For more information, see the [How to Configure Load Balancing](#) Help topic.
- **External Load Balancer(s)** – The default setting is Disabled. Click the **Edit** button to open the **Configure Load Balancers** window where you can configure an ordered list of external load balancers that will be used to evenly distribute Access Control engine load. For more information, see the [How to Configure Load Balancing](#) Help topic.

End-Systems Tab

The End-Systems tab presents end-system connection information for a single Extreme Access Control engine, all Access Control engines, or all the engines in an engine group, depending on what you select in the left-panel tree. You can also monitor end-system events and view the health results from an end-system's assessment.

To access this tab, select a single Access Control engine, the All NAC Appliances folder, or an engine group in the left-panel tree, then click the End-Systems tab in the right panel.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see Table Tools.



The screenshot displays the 'End-Systems' tab in a network management interface. The top section shows a table of end-systems with columns for MAC Address, MAC OUI Vendor, IP Address, and Switch IP. The bottom section shows a table of end-system events for a specific MAC address, with columns for Timestamp, IP Address, Switch IP, Switch Port, State, and Username.

MAC Address	MAC OUI Vendor	IP Address	Switch IP
00:04:C3:55:56:55	CASTOR Informatique	2.2.2.102	77.12.4.4
00:17:EC:55:56:57	Texas Instruments	2.2.2.104	77.18.6.6
00:17:C6:55:56:54	Cross Match Technologies Inc	2.2.2.101	77.11.9.9
00:02:E3:55:56:52	LITE-ON Communications, Inc.	2.2.2.99	77.12.4.4
00:12:D4:55:56:51	Princeton Technology, Ltd	2.2.2.98	77.18.6.6
00:90:BA:55:56:50	VALID NETWORKS, INC.	2.2.2.97	77.16.2.2
00:08:BA:55:56:37	Erskine Systems Ltd	2.2.2.84	77.15.7.7
00:06:AB:55:56:34	W-Link Systems, Inc.	2.2.2.81	77.15.7.7
00:07:C6:55:55:83	VDS Vosskuhler GmbH	2.2.2.31	77.15.7.7
00:60:C8:55:56:48	KUKA WELDING SYSTEMS ...	2.2.2.95	77.18.6.6
00:40:CD:55:56:46	TERA MICROSYSTEMS, INC.	2.2.2.93	77.16.2.2
00:09:C1:55:56:43	PROCES-DATA A/S	2.2.2.90	77.18.6.6

Timestamp	IP Address	Switch IP	Switch Port	State	Username
04/26/2011 03:41:05 PM	2.2.2.84	77.15.7.7		Quarantine	
04/26/2011 03:41:05 PM	2.2.2.84	77.18.6.6		Quarantine	h_harley
04/26/2011 03:41:04 PM	2.2.2.84	77.18.6.6		Error	
04/26/2011 03:41:01 PM	2.2.2.84	77.16.2.2		Accept	j_smith

End-Systems

This table displays the last known connection state for each end-system attempting to connect.

MAC Address

The end-system's MAC address. MAC addresses can be displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix. You can specify how you want to display end-system MAC addresses in the [Options window Display view](#) (Tools > Options).

MAC OUI Vendor

The vendor associated with the MAC OUI.

IP Address

The end-system's IP address.

Switch IP

The IP address of the switch the end-system connected to. If the end-system is connected to a Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

Switch Port

The port alias (if defined) followed by the switch port number the end-system connected to. If the end-system is connected to a Layer 2 Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines this column is blank.

If you add or update the port alias on the switch, you must enforce the Access Control engine in order for the new information to be displayed in the End-Systems table.

If you don't want the port alias displayed, remove the PORT_DESCRIPTION_FORMAT variable from the /opt/nac/server/config/config.properties file. If this variable is removed, only the switch port number displays.

State

The end-system's connection state:

- Scan — The end-system is currently being scanned.
- Accept — The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.

- Quarantine — The end-system is quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled, or if the Session Deactivate Timeout option is enabled on the [Reauthentication tab](#) in Appliance Settings.
- Error — Indicates one of nine problems:
 - the MAC to IP resolution failed, if assessment is enabled
 - the MAC to IP resolution timed out, if assessment is enabled
 - all RADIUS servers are unreachable
 - the RADIUS request was non-compliant
 - all assessment servers are unavailable
 - the assessment server can't reach the end-system
 - no assessment servers are configured
 - the assessment server is not compatible with the current version of NAC Manager
 - the username and password configured in the [Assessment Server panel](#) of the NAC Manager options (Tools > Options > Assessment Server) are incorrect for the assessment server

Username

The username used to connect.

Hostname

The end-system's hostname.

Device Family

The hardware family or the operating system family for the end-system.

Device Type

The hardware type or the operating system type for the end-system.

Authentication Type

Identifies the latest authentication method used by the end-system to connect to the network. (For Layer 3 Access Control Controller engines,

this column lists "IP.") For a listing of all the authentication methods the end-system is using to authenticate, see the [All Authentication Types](#) column.

Authorization

The attributes returned by the RADIUS server for this end-system. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Profile

The name of the NAC profile that was assigned to the end-system when it connected to the network.

Risk

The overall risk level assigned to the end-system based on the health result of the scan:

- Red — High Risk
- Orange — Medium Risk
- Yellow — Low Risk
- Green — No Risk
- Gray — Unknown

Reason

Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Extended State

Provides [additional information](#) about the end-system's connection state.

State Description

This column provides more details about the end-system state.

Last Seen

The last time the end-system was seen by the Access Control engine.

First Seen

The first time the end-system was seen by the Access Control engine.

Last Scanned

The last time an assessment (scan) was performed on the end-system.

Last Scan Result

The last scan result assigned to the end-system: Scan, Accept, Quarantine, Reject, Error. This is the state that was assigned to the end-system as a result of the last completed scan. This typically matches the end-system [State](#) if scanning is currently enabled and was recently performed.

NAC Appliance/Source IP

The Access Control engine to which the end-system is connecting.

Appliance Group

This column only displays if you have multiple engine groups. It displays the engine group the Access Control engine was in when the end-system event was generated. For example, if the engine was in Appliance (Engine) Group A when an end-system connected, but then later the engine was moved to Appliance (Engine) Group B, this column still lists Appliance (Engine) Group A for that end-system's entry.

Switch Location

The physical location of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

All Authentication Types

This column displays all the authentication methods the end-system used to authenticate. The authentication types are listed in order of precedence from highest to lowest: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking. View details about each authentication session (such as the NAC profile assigned to the end-system for each authentication type) in the [End-System Events tab](#). You can also view authentication session information in the [End-System Summary window](#).

RFC3580 VLAN

For end-systems connected to RFC 3580-enabled switches, this is the RFC3580 VLAN ID assigned to the end-system.

Score

The total sum of the scores for all the health details that were included as part of the quarantine decision.

Top Score

The highest score received for a health detail in the health result.

Actual Score

The actual score is what the total score would be if all the health details including those marked Informational and Warning were included in the score.

Custom 1

Use this column to add additional information that you would like displayed. To add or edit custom information, right-click on the table entry and select Edit Custom Information. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, right-click in the table body and select Table Tools > Settings. In the Table Settings window, you can select to show these columns in the table. To clear the custom information, right-click on the table entry and select Clear Custom Information. You can change the text of the Custom column heading in the [Options window Display view](#) (Tools > Options).

Groups

Displays any end-system and/or user groups to which the end-system belongs.

Zone

Displays the end-system zone that the end-system is assigned to. For more information, see [End-System Zones](#) in the NAC Manager Concepts Help file.

Actions

TIP: These actions are also available from the right-click menu off an end-system entry in the table.

Force Reauth

Forces the selected end-system to re-authenticate. End-systems authenticated to a VPN device are disconnected from the VPN.

Force Reauth and Scan

Forces the selected end-system to re-authenticate and undergo an assessment (scan). (End-systems authenticated to a VPN device are disconnected from the VPN.) The assessment only takes place if scanning is enabled in the NAC profile assigned to the end-system.

Send Agent Message

Opens the [Send Message to End System Agents window](#), from which you can send a message to one or more systems running an assessment agent.

Add to Group

Lets you add the selected end-system to a specific end-system or user group. If the end-system is a registered device, it can be added to a registration group. After adding an end-system to a group, any rules created that involved that group apply to the end-system as well. Changes to end-system group membership do not require an enforce and are synchronized with engines immediately. Changes do not affect the end-system until the next authentication or assessment occurs.

Lock MAC

Opens the [Add MAC Lock window](#) where you can lock the MAC address of the selected end-system to a switch or switch and port.

Port Monitor

Opens the Port Monitor window where you can view detailed status information and statistics for the selected port.

Summary

Opens the [End-System Summary window](#) where you can view summary information for the end-system selected in the table.

Delete

Deletes the selected end-system entries from the table and also deletes the associated end-system events. You are given the option to delete any custom information, group assignment, MAC locks, and registration and web authentication associated with the end-systems.

The Force Delete of End-System option completely deletes the end-system from NAC Manager, regardless of whether the end-system reauthentication is successful when the delete is executed. The option is deselected by default. When deselected, it prevents possible synchronization conditions where the authentication session remains active on the switch even though the end-system is deleted from NAC Manager. These conditions can occur when there are underlying issues that prevent the end-system reauthentication from completing properly.

NOTES: The Delete operation does not remove an end-system from the Blacklist group. Blacklist is a special group that requires end-systems to be manually removed using the [Edit End-System Group window](#).

Deleting an end-system from the table also deletes the user's current authentication. If the user is connected to the network at the time of the delete, they are forced to re-authenticate.

End-System Events Tab

This tab displays historical connection information for the end-system selected in the table above. End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them here in this tab. This cache allows NAC Manager to quickly retrieve and display end-system events without having to search through the database. You can configure parameters for the event cache (such as the number of events to display) using the [End-System Event Cache options](#) in the NAC Manager Options view (Tools > Options).

NOTE: The End-System Events tab displays events up to the most recent delete event for the end-system, if one exists. If you want to see events that happened prior to the most recent delete event, use the Search for Older Events button.

Time Stamp	IP Address	Switch IP	Switch Port	State	Username
04/26/2011 03:41:05 PM	2.2.2.84	77.15.7.7		Quarantine	
04/26/2011 03:41:05 PM	2.2.2.84	77.18.6.6		Quarantine	h_harley
04/26/2011 03:41:04 PM	2.2.2.84	77.18.6.6		Error	
04/26/2011 03:41:01 PM	2.2.2.84	77.16.2.2		Accept	j_smith

Time Stamp

The date and time the end-system connected.

IP Address

The end-system's IP address.

Switch IP

The IP address of the switch the end-system connected to. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

Switch Nickname

The nickname defined for the switch to which the end-system is connected.

Switch Port

The switch port number to which the end-system is connected. If the end-system is connected to a Layer 2 Access Control Controller engine, this is

the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines this column is blank.

State

The end-system's connection state:

- Scan — The end-system was scanned.
- Accept — The end-system was granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine — The end-system was quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — This end-system session was disconnected, however other sessions for the end-system may still be active. For example, the end-system may have a disconnected session with an authentication type of 802.1X, but still have an active MAC authentication session. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled, or if the Session Deactivate Timeout option is enabled on the [Reauthentication tab](#) in Appliance Settings.
- Error — Indicates one of nine problems:
 - the MAC to IP resolution failed
 - the MAC to IP resolution timed out
 - all RADIUS servers are unreachable
 - the RADIUS request was non-compliant
 - all assessment servers are unavailable
 - the assessment server can't reach the end-system
 - no assessment servers are configured
 - the assessment server is not compatible with the current version of NAC Manager
 - the username and password configured in the [Assessment Server panel](#) of the NAC Manager options (Tools > Options > Assessment Server) are incorrect for the assessment server

Username

The username used to connect.

Hostname

The end-system's host name.

Device Family

The hardware family or the operating system family for the end-system.

Device Type

The hardware type or the operating system type for the end-system.

Authentication Type

Identifies the authentication method used by the end-system to connect to the network. For Layer 3 Access Control Controller engines, this column lists "IP."

Authorization

The attributes returned by the RADIUS server. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Profile

The name of the NAC profile assigned to the end-system when it connected to the network.

Reason

Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Extended State

Provides [additional information](#) about the end-system's connection state.

State Description

This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Switch Location

The physical location of the switch to which the end-system is connected. If the end-system is connected to a Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

Appliance Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Access Control engine was in when the end-system event was generated. For example, if the engine was in Appliance (Engine) Group A when an end-system connected, but then later the engine was moved to Appliance (Engine) Group B, this column would still list Appliance (Engine) Group A for that end-system's entry.

Zone

Displays the end-system zone that the end-system is assigned to. For more information, see [End-System Zones](#) in the NAC Manager Concepts Help file.

Search for Older Events

This button lets you search for older events stored in the database outside of the end-system events cache. The maximum search parameters for this extended search are configured in the [End-System Event Cache options](#) in the NAC Manager Options view (Tools > Options). The search is ended when any one of the parameters is reached.

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

Health Result Summaries Tab

This tab provides summary information on health results (assessment results) obtained for the end-system selected in the table above. You can specify the number of health result summaries displayed using the Health Result Persistence options in the [Data Persistence Option view](#).

Scan Start Date	Scan Time	Overall Risk	Reason	Total Score	Top Score	Summary	Test Set
06/09/2009 01:42:54 PM	0 S	No Risk	There was a health result above 7.0	64.4	1.4		
06/09/2009 01:42:54 PM	0 S	Low Risk	There was a health result above 7.0	46.1	4.4		
06/09/2009 01:42:54 PM	0 S	Medium Risk	There was a health result above 7.0	22.3	4.0		
06/09/2009 01:42:54 PM	0 S	No Risk	There was a health result above 7.0	45.1	7.7		
06/09/2009 01:42:54 PM	0 S	Low Risk	There was a health result above 7.0	54.2	6.2		

Scan Start Date

The date and time the assessment (scan) started.

Scan Time

The amount of time it took for the assessment (scan) to complete.

Overall Risk

The overall risk level assigned to the end-system based on the health result of the scan: High Risk, Medium Risk, Low Risk, or No Risk.

Reason

The reason the health result was placed into the specified risk level. This is based on the risk level configuration that was used for the assessment, for example, if there was one or more health result detail with a score greater than 7. If the end-system is NAP capable, then this is based on the values returned from NAP.

Total Score

The total sum of the scores for all the health details that were included as part of the quarantine decision, followed by the actual score in parenthesis. The actual score is what the total score would be if all the health details were included as part of the quarantine decision. It includes all scores, including those marked Informational and Warning. If the total score and the actual score are the same, only one score is shown.

Top Score

The highest score received for a health detail that was included as part of the quarantine decision. Scores that are marked as Informational or Warning are not considered.

Summary

A list of all the test cases that were run against the device during assessment. The test case name is listed, or if that is not available, the test case ID is listed.

Test Sets

The list of test sets that were run during assessment, for example, Default Nessus, Default Agent-less, and Default Agent-based. Test sets are defined as part of the assessment configuration. If the end-system is NAP capable, then this column displays Microsoft NAP indicating that NAP performed the assessment.

Total Details

The total number of health result details (vulnerabilities) detected during the assessment.

High Risk

The total number of high risk vulnerabilities detected during the assessment.

Medium Risk

The total number of medium risk vulnerabilities detected during the assessment.

Low Risk

The total number of low risk vulnerabilities detected during the assessment.

Warnings

The total number of health result details that are marked as Warnings.

Delete Button

Deletes the health results selected in the table.

Show Details Button

Opens the Health Results Details tab where you can view detailed information on the security risks found on the end-system during this particular assessment.

Health Result Details Tab

This tab lets you view health result details (assessment result details) for the end-system selected in the table above. The drop-down list at the top of the tab displays all the end-system's scan results listed by start date. Select the date for the particular scan result you wish to view. The tab presents detailed information on the security risks found on the end-system during that particular assessment (scan). You can specify the number of health result details displayed using the Health Result Persistence options in the [Data Persistence Option view](#).

TIP: Double-click on an individual entry in the table to view a description, result, and solution for the health result displayed in a separate window.

Test Case Name	Test Case ID	Risk	Score	Scoring Mode	CVE IDs	Source	Description
Warning Check5	45	MEDIUM	5.5	Applied	CVE-2065-0540BID	Port: 65, Protocol: 55	This is the descrip
DHCP	75	HIGH	8.1	Applied	CVE-2095-0550DLE	Port: 95, Protocol: 85	This is the descrip
Sendmail	78	HIGH	7.8	Applied	CVE-2098-0550DLE	Port: 98, Protocol: 88	This is the descrip
DHCP	75	HIGH	8.1	Applied	CVE-2095-0550DLE	Port: 95, Protocol: 85	This is the descrip

Test Case Name

This column lists the name of the test that is reported by the health result detail.

Test Case ID

The unique number assigned to the test case.

Risk

The risk level assigned to the problem found on the port:

- High (corresponds to a Hole)
- Medium (corresponds to a Warning)
- Low (corresponds to a Note)

Score

The score assigned to the test case. The score is a value between 0.0 and 10.0. In the case of agent-based test cases, the score is either 0.0 for a passed test, or 10.0 for a failed test, unless specifically overwritten by the scoring override configuration.

Scoring Mode

The scoring mode that was used at the time the test was performed.

- Applied — The score returned by this test was included as part of the quarantine decision.
- Informational — The score returned by this test was reported, but did not apply toward a quarantine decision.
- Warning — The score returned by this test was only used to provide end user assessment warnings via the Notification portal web page.

CVE IDs

The CVE (Common Vulnerability and Exposures) ID assigned to the security vulnerability or exposure. For more information on CVE IDs, refer to the following URL: <http://www.cve.mitre.org/>.

Source

The port on the end-system that the security risk was detected on followed by the well-known number (ID) assigned to the IP Protocol Type.

Description

This column lists information about the health result detail. Double-click on the entry in the table to open a Health Result Detail Description that displays a description, result, and solution for the health result. In addition, the Description window includes operating system information such as version and product type (when available). With this information, you have the flexibility to add scoring overrides for OS specific issues for any given Test Case, using the Regular expression functionality of the scoring

override. (For more information, see the [Add/Edit Scoring Override Configuration window](#).)

Remediation

For agent-based assessment, this column lists the results of remediation attempts: Success, Failed, or Not Attempted.

Type

A "type" is assigned to each security risk found on a port during an assessment, and is used to determine whether to Quarantine an end-system. Types are configurable on the assessment agent. There are three types:

- Hole — The port is vulnerable to attack.
- Warning — The port may be vulnerable to attack.
- Note — There may be a security risk on the port.

Configure Button

Use the Configure drop-down list to:

- [Add Scoring Override](#) — Create a scoring override for the selected test case.
- [Manage Scoring Override Configurations](#) — Open the Manage Scoring Override Configurations window where you can view and define the scoring override configurations used in your assessment configurations.
- Edit Agent-based Test Case — Open the Test Editor window for the selected agent-based test case.
- [Manage Risk Level Configurations](#) — Open the Manage Risk Level Configurations window where you can view and define the risk level configurations used in your assessment configurations.

TIP: The Configure and Show button menu options can also be accessed by right-clicking on a health result detail in the table.

Show Button

Use the Show drop-down list to:

- Show All End-Systems With Test Case ID — Open the End Systems tab as a separate window listing only those end-systems with the selected test case ID in their latest scan.

NOTE: If you select a vulnerability that does not list a CVE-ID (the column is empty), clicking this button launches a window that lists all end-systems that have *any* vulnerability without a CVE-ID.

- Show Description — Open a Health Result Detail Description window that displays information about the vulnerability. This window can also be displayed by double-clicking on any entry in the Health Result Details table.


Related Information

For information on related windows:

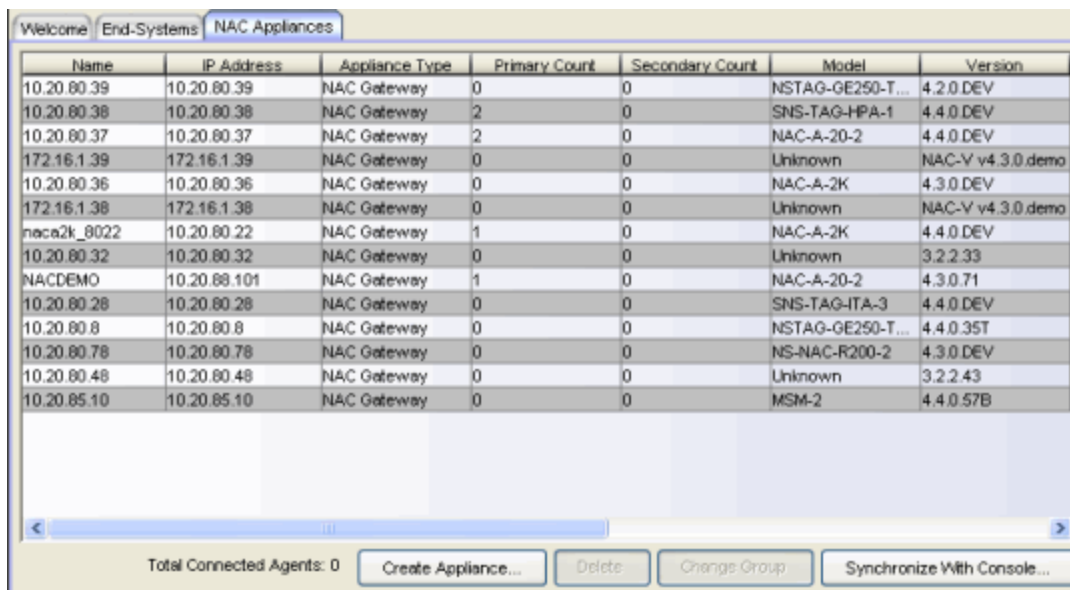
- [Add MAC Lock Window](#)
- [End-System Summary Window](#)

NAC Appliances Tab

The NAC Appliances tab is displayed in the right panel when you select the All NAC Appliances folder in the left panel. The tab is also available when selecting an engine group in the left panel. The tab displays a table of information about the engines in the folder or group. Right-click an engine for a menu of options.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you display the row count column). For more information, see Table Tools.

NOTE: The NAC Appliance administration web page allows you to access status and diagnostic information for an Extreme Access Control engine. Launch the administration web page by right-clicking on an Access Control engine in the left-panel tree and selecting WebView. You can also access the administration web page using the following URL: <https://<Access Control engine IP>:8444/Admin>. The default user name and password for access to this web page is "admin/Extreme@pp." Change the username and password in the Web Service Credentials field on the [Credentials Tab](#) in the Appliance Settings window.



The screenshot shows the NAC Appliances tab with a table of appliance information. The table has columns for Name, IP Address, Appliance Type, Primary Count, Secondary Count, Model, and Version. Below the table are buttons for 'Create Appliance...', 'Delete', 'Change Group', and 'Synchronize With Console...'. The status bar at the bottom indicates 'Total Connected Agents: 0'.

Name	IP Address	Appliance Type	Primary Count	Secondary Count	Model	Version
10.20.80.39	10.20.80.39	NAC Gateway	0	0	NSTAG-GE250-T...	4.2.0.DEV
10.20.80.38	10.20.80.38	NAC Gateway	2	0	SNS-TAG-HPA-1	4.4.0.DEV
10.20.80.37	10.20.80.37	NAC Gateway	2	0	NAC-A-20-2	4.4.0.DEV
172.16.1.39	172.16.1.39	NAC Gateway	0	0	Unknown	NAC-V v4.3.0.demo
10.20.80.36	10.20.80.36	NAC Gateway	0	0	NAC-A-2K	4.3.0.DEV
172.16.1.38	172.16.1.38	NAC Gateway	0	0	Unknown	NAC-V v4.3.0.demo
naca2k_8022	10.20.80.22	NAC Gateway	1	0	NAC-A-2K	4.4.0.DEV
10.20.80.32	10.20.80.32	NAC Gateway	0	0	Unknown	3.2.2.33
NACDEMO	10.20.88.101	NAC Gateway	1	0	NAC-A-20-2	4.3.0.71
10.20.80.28	10.20.80.28	NAC Gateway	0	0	SNS-TAG-ITA-3	4.4.0.DEV
10.20.80.8	10.20.80.8	NAC Gateway	0	0	NSTAG-GE250-T...	4.4.0.35T
10.20.80.78	10.20.80.78	NAC Gateway	0	0	NS-NAC-R200-2	4.3.0.DEV
10.20.80.48	10.20.80.48	NAC Gateway	0	0	Unknown	3.2.2.43
10.20.85.10	10.20.85.10	NAC Gateway	0	0	MSM-2	4.4.0.57B

Name

The name of the Access Control engine (assigned when the engine was created).

IP Address

The Access Control engine's IP address.

Appliance Type

The Access Control (NAC) engine type: NAC Gateway, NAC Layer 2 (L2) Controller, or NAC Layer 3 (L3) Controller.

Primary Count

The number of switches for which the Access Control engine is the primary engine.

Secondary Count

The number of switches for which the Access Control engine is the secondary engine.

Model

The Access Control engine's model number.

Version

The Access Control engine's version number.

CPU Load (0-100%)

The percentage of the engine's CPU currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

Memory Used

The amount of memory being used by the engine.

Memory Available

The amount of memory available to the engine.

Connected Agents

The number of assessment agents connected to the engine.

Capacity

The engine's current capacity, which is the number of end-systems authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Total End-System License Limit

The total end-system license limit for all engines.

Total Connected Agents

The total number of assessment agents connected to all engines.

Create Appliance Button

Opens the [Create NAC Appliance window](#) where you can create and configure a new engine.

Delete Button

Select an engine and click this button to delete the engine from NAC Manager's device database. When you perform the delete, you can also delete the engine from Console.

Change Group Button

Select one or more engines and click this button to open a window where you can choose a new engine group for the selected engines. When you click OK, the engines are automatically moved to the new group.

Synchronize with Console Button

Opens the [Synchronize Appliances with Console window](#) where you can import and export engines to and from Console.

Related Information

For information on related windows:

- [Create NAC Appliance Window](#)
- [Synchronize Appliances with Console Window](#)

Statistics Tab

This tab presents end-system connection state statistics and vulnerability status (security risks) for an Extreme Access Control engine, an engine group, or all the engine groups, depending on what you select in the left-panel tree. To access this tab, select an engine, an engine group, or the NAC Appliance Groups folder in the left-panel tree, then click the Statistics tab in the right panel.

Select the statistical information you want to view using the drop-down menu at the top of the tab. The following statistical information can be selected:

- [End-System Info](#)
- [End-System Status](#)
- [Most Frequently Occurring Vulnerabilities](#)
- [End-System NAC Profile Allocation](#)
- [End-System Risk](#)

End-System Info

This selection provides the last known end-system connection state information for the Access Control engine or engine group you select in the left-panel tree. The Display drop-down menu displays information on end-system connection [states](#), [extended states](#), and the [reasons](#) why the end-station is in the current state. The information is presented as a bar graph, with each bar representing a specific connection state or reason.

To clear an end-system from the chart, you must delete the end-system from the right-panel [End-Systems tab](#), or use the [Remove End-Systems window](#) to clear end-systems prior to and including a specified date.

TIPS: -- Double-click on a bar in the charts to open the End-Systems tab as a separate window listing only those end-systems with the selected connection state or reason.
-- Right-click on a chart to access [menu options](#) that let you print the chart, save the chart to a file, and zoom in on chart data.

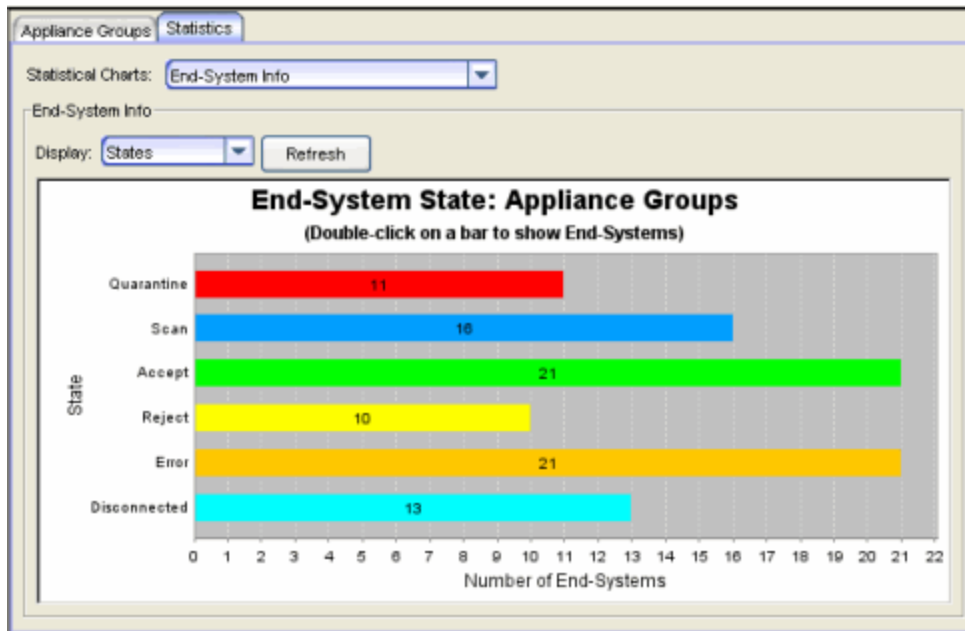
States

The States chart displays the last known connection state for each end-system attempting to connect. For example, if an end-system is currently being

scanned, it is in the Scan state. If the scan fails, the end-system is quarantined and is in the Quarantine state.

End-systems display one of the following connection states:

- Quarantine - The end-system is quarantined because the scanning test failed.
- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Reject - The end-system is rejected because the assigned NAC profile is set to Reject, the MAC Locking test failed, or the RADIUS server is reachable, but rejected the authentication request.
- Disconnected - All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches with RADIUS accounting enabled, or if the Session Deactivate Timeout option is enabled on the [Reauthentication tab](#) in Appliance Settings.
- Error - Indicates one of nine problems:
 - the MAC to IP resolution failed, if assessment is enabled
 - the MAC to IP resolution timed out, if assessment is enabled
 - all RADIUS servers are unreachable
 - the RADIUS request is non-compliant
 - all assessment servers are unavailable
 - the assessment server can't reach the end-system
 - no assessment servers are configured
 - the assessment server is not compatible with the current version of NAC Manager
 - the username and password configured in the [Assessment Server panel](#) of the NAC Manager options (Tools > Options > Assessment Server) are incorrect for the assessment server

Sample End-System Info - StatesExtended States

The Extended States chart provides additional information about the end-system connection states. The following five states provide information about the Error state, which results when scanning is required but a scan cannot be performed:

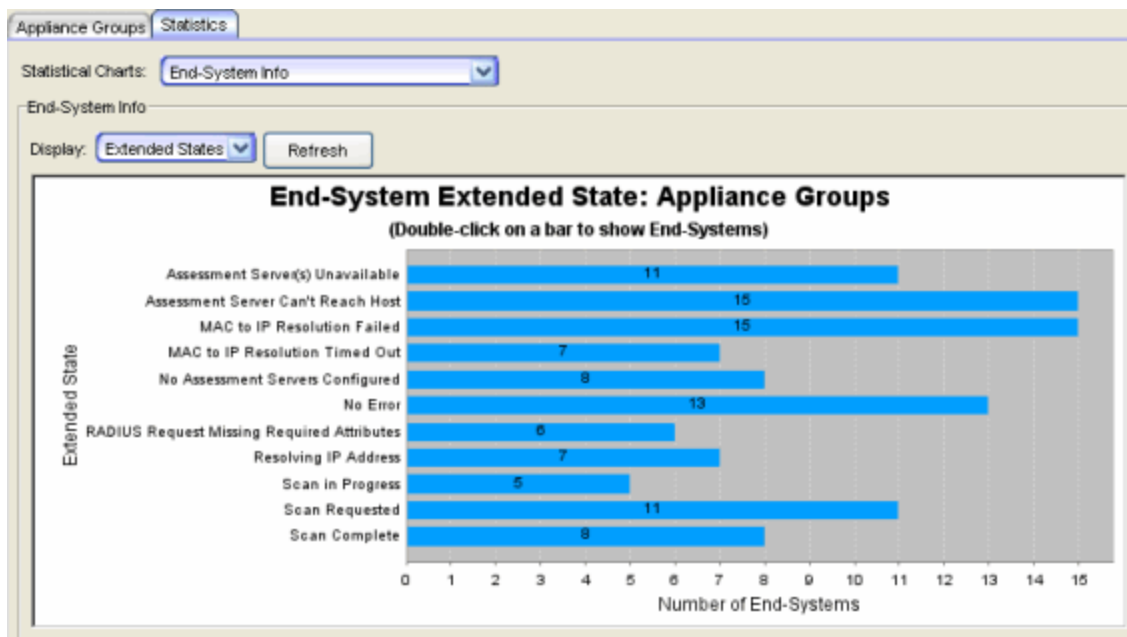
- Assessment Server(s) Unavailable - There are no Assessment servers available to perform a scan on the end-system. If an Assessment server responds to a scan request that it is too busy to perform a scan, the Access Control engine makes a scan request to the next Assessment server. If all your Assessment servers respond that they are too busy, an error is returned. In this case, you need to add more Assessment servers or increase the maximum number of scans your Assessment servers can perform at one time.
- Assessment Server Can't Reach Host - An error is returned because the Assessment server cannot reach the end-system to perform a scan. This may be caused by a routing problem; the Assessment server is not on the same subnet as the end-system. In addition, the Assessment server performs a "reachability" test on the end-system, which may fail because of a firewall on the end-system.
- MAC to IP Resolution Failed - The scan cannot be performed because the end-system's MAC address cannot be resolved to an IP address.

- MAC to IP Resolution Timed Out - The scan cannot be performed because the end-system's MAC address is not resolved to an IP address in the allowed time. (See the [IP Address Resolution Timeout option](#).)
- No Assessment Servers Configured - A scan is required for the end-system, but no Assessment servers are configured in NAC Manager. For more information, see the [Manage Assessment Servers window](#).

Other possible extended states are:

- No Error - End-system authentication and assessment completed without errors.
- RADIUS Request Missing Required Attributes - The attributes returned from the RADIUS server were not sufficient for processing.
- Resolving IP Address - MAC to IP Address Resolution is being performed for the end-system.
- Scan in Progress - Provides additional information for the Scan state; the end-system re-authenticated while a scan is in progress.
- Scan Requested - Provides additional information for the Scan state; a scan is requested for the end-system.
- Scan Complete - Provides additional information for the Scan state; a scan is completed for the end-system.

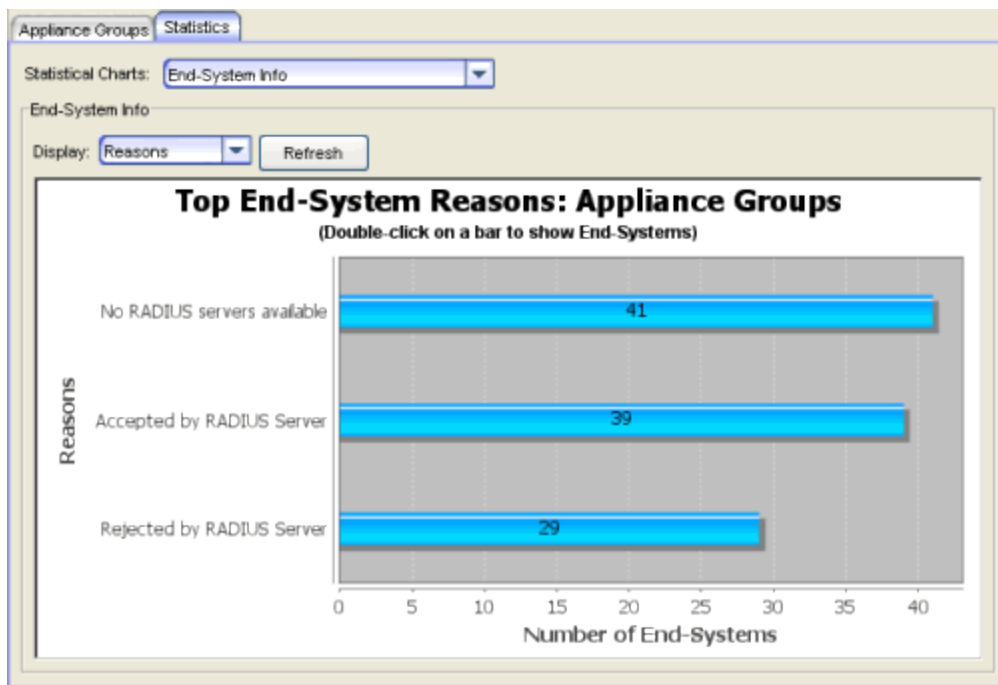
Sample End-System Info - Extended States



Reasons

This chart provides additional information about the reasons why the end-systems are in their particular connection states. It gives you an idea as to why a certain policy applies to an end-system or why the end-system is rejected.

Sample End-System Info - Reasons



End-System Status

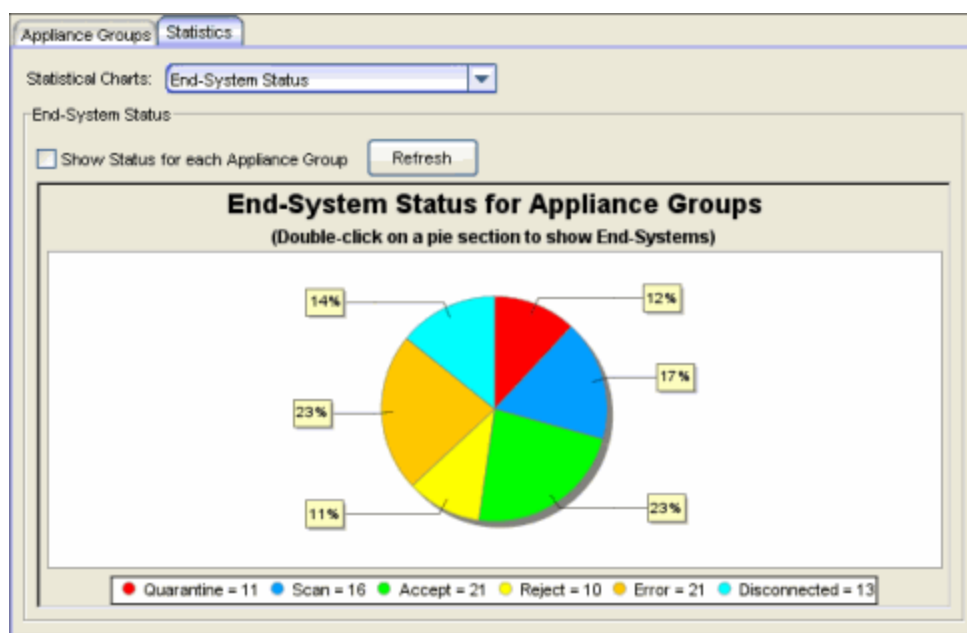
This chart presents the last known end-system connection states for the Access Control engine or engine group select in the left-panel tree. The information is presented as a pie chart, with each color-coded slice representing a specific [connection state](#). Holding the mouse pointer over a particular slice shows a *tool tip* that identifies the total number of end-systems with that particular state.

The chart displays the last known connection state for each end-system attempting to connect. For example, if an end-system is currently being scanned, it is represented as blue. Once the scan is complete, if the end-system goes to a Quarantine state, it is represented as red. To clear an end-system from the chart, you must delete the end-system from the right-panel [End-Systems tab](#), or use the [Remove End-Systems window](#) to clear end-systems prior to and including a specified date.

If you are viewing statistics for all engine groups, use the **Show Status for each Appliance Group** checkbox to display individual pie charts for each group. If you are viewing statistics for a single engine group, use the **Show Status for Each NAC Appliance** checkbox to display individual pie charts for each engine in the group.

TIPS: -- Double-click on a pie section to open the End-Systems tab as a separate window listing only those end-systems with the selected connection state.
 -- Right-click on the chart to access [menu options](#) that let you print the chart or save the chart to a file.

Sample End-System Status



Most Frequently Occurring Vulnerabilities

This chart displays the top ten agent-less vulnerabilities for the Access Control engine or engine group you select in the left-panel tree. The information is gathered from the latest end-system health results (scan results) and provides important information about the security risks found on the end-systems during the scan. The information is presented as a bar graph, with each bar representing a vulnerability identified by Test Case name and ID.

NOTE: Vulnerabilities with no Test Case IDs are grouped together and represented by a single bar in the chart (if there are enough of them).

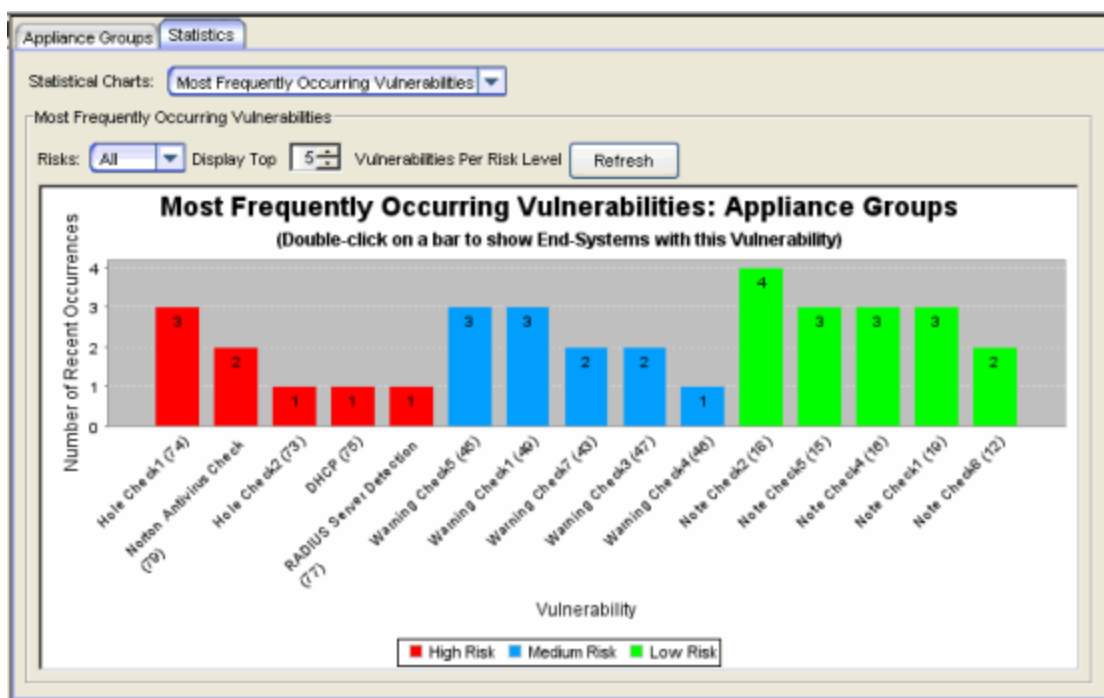
Each vulnerability is assigned a risk level:

- High (corresponds to a Hole - the port is vulnerable to attack)
- Medium (corresponds to a Warning - the port may be vulnerable to attack)
- Low (corresponds to a Note - there may be a security risk on the port)

Use the Risks drop-down menu to select whether to display all risk levels, or just the high, medium, or low risk level vulnerabilities. To get a good representation of all risk levels, you can use the spin box to adjust the number of vulnerabilities displayed for each risk level.

TIPS: -- Double-click on a bar to open the End-Systems tab as a separate window listing only those end-systems with the selected vulnerability and risk factor.
 -- Right-click on the bar graph to access [menu options](#) that let you print the chart or save the chart to a file. You can also use this menu to zoom in and out on the chart data.

Sample Most Frequently Occurring Vulnerabilities



End-System NAC Profile Allocation

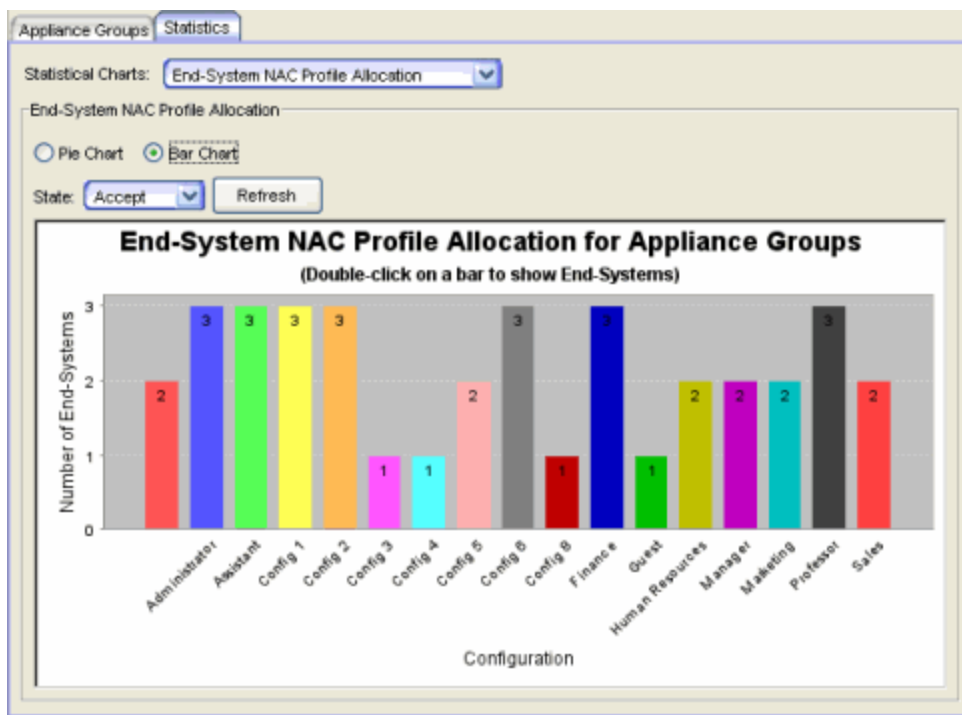
This chart displays the number and/or percentage of end-systems using a particular NAC profile. The statistics can be viewed as a pie chart or a bar chart, with each color-coded slice or bar representing the NAC profile being used. Holding the mouse pointer over a particular slice or bar shows a *tool tip* that

identifies the total number of end-systems using that particular configuration. Use the State drop-down menu to display the allocation information for any [connection state](#): Accept, Reject, Quarantine, Scan, Disconnected, or Error. The NAC profile displayed for Disconnected end-systems is the profile assigned to the end-systems in their previous state when still on the network. The NAC profile displayed for Rejected end-systems is the profile assigned if the end-system successfully connected to the network.

To clear an end-system from the chart, you must delete the end-system from the right-panel [End-Systems tab](#), or use the [Remove End-Systems window](#) to clear end-systems and end-system events prior to and including a specified date.

NOTE: There is a case where the chart may show statistics for two (or more) NAC profiles using the same profile name. If an end-system on an Access Control engine uses the Sales NAC profile. If you change the parameters on the Sales profile (but keep the same name) and another end-system on the same engine uses this revised profile, then the chart shows two separate bars or slices for the Sales profile.

Sample End-System Configuration Allocation

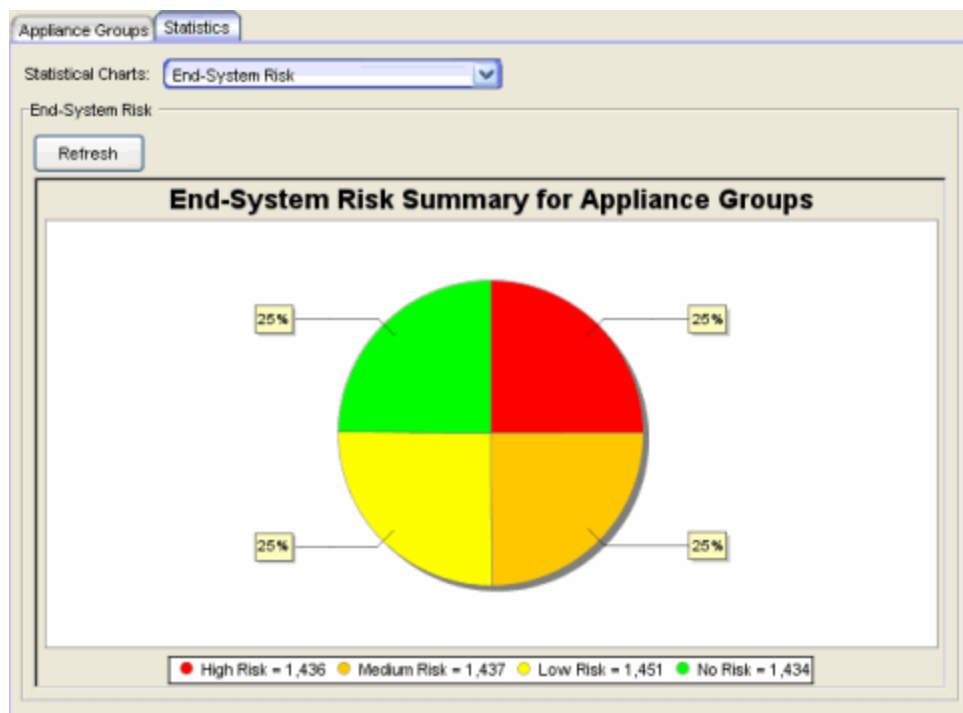


End-System Risk

This chart presents a summary of the overall end-system risk levels. The Risk Summary includes the last known health result risk level for each end-system attempting to connect. The information is presented as a pie chart, with each color-coded slice representing the percentage of the end-systems in each risk level. The legend below the graph displays the total number of end-systems with that particular risk level.

TIP: Right-click on the chart to access [menu options](#) that let you print the chart or save the chart to a file.

Sample End-System Risk Summary



Right-Click Menu Options

NAC Manager provides right-click menu options and tools that let you easily save, print, and zoom in on statistical charts. You can access these tools by right-clicking on a chart and selecting an option from the menu:

- **Save As** - lets you save the graph in .png format.
- **Print** - lets you print the graph.

- **Zoom In** - zoom in on one or both axes.
 - **Zoom Out** - zoom out on one or both axes.
 - **Auto Range** - set one or both axes back to the default range.
-

TIP: In bar charts, you can click and drag your mouse from left to right to zoom in on a specific section of the graph. Click and drag from right to left to zoom back out.

Related Information

For information on related windows:

- [End-Systems Tab](#)
- [Remove End-Systems Window](#)


Switches Tab

This tab provides information about the switches assigned to a Extreme Access Control Gateway engine or Access Control engine Group. To access this tab, select a gateway or engine group in the left-panel tree, then click the **Switches** tab in the right panel.

Right-click on one or more switch for a menu of options including launching the Node Alias and Multi Auth FlexView and the RADIUS Client Information FlexView.

If you are using Policy Manager, right-click on one or more switch and select from the following Policy options:

- **Port Configuration Wizard** - Accesses the Policy Manager Port Configuration Wizard. Select from pre-configured defaults for MAC, 802.1X, or MAC + 802.1X authentication, or select the complete wizard which leads you through all the steps required to configure a port or ports, including setting the port authentication configuration and default role. (If the devices are not in a domain or are in more than one domain, any role specific configuration, such as setting the default role, is disabled.)
- **Display Domains Associated with Switches** - Retrieves the Policy Manager domains associated with the switches and displays them in the Policy Domain column in the tab.
- **Set Domain** - Lets you assign the switch to a Policy Manager domain.
- **Verify Domain Policy Settings with Network** - Verify that the roles in the assigned Policy Manager domain have been enforced to the switch.
- **Enforce Domain Policy Settings with Network** - Enforce the roles in the assigned Policy Manager domain to the switch.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. Access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Help topic on .

Switch IP Address	Switch Nickname	Switch Status	Switch System Name	Primary Gateway	Secondary Gate
12.22.80.128	C3 80.128	Contact Established	12.22.80.128	12.22.80.37	12.22.80.38
12.22.80.10	N1 80.10	Contact Established	12.22.80.10	12.22.80.37	12.22.80.38

Filter

Use the Filter field to filter for a specific switch or switches based on a numeric value or text.

Switch IP Address

The switch's IP address.

Switch Nickname

The nickname assigned to the switch when it is added to the Extreme Management Center database.

Switch Status

The current operational status of the switch, based on the Management Center Console device poll. If the Console device poll did not update the status of a switch, and a Verify RADIUS Configuration operation is performed on that switch, the switch status in the **Switches** tab may differ from the switch status in the Verify RADIUS Configuration window.

Switch System Name

The assigned name of the device as stored in the device's sysName MIB object.

Primary Gateway

The name and IP address of the switch's primary Access Control Gateway. If load balancing has been configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

Secondary Gateway

The name and IP address of the switch's secondary Access Control Gateway. If load balancing is configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

Policy/VLAN

The RADIUS attributes included as part of the RADIUS response.

Policy Domain

The Policy Manager domain to which the switch is assigned (if any). Populate this field by right-clicking on a switch and selecting Policy > Display Domains Associated with Switches. This information does not automatically update if there are domain assignment changes. You need to re-select the menu option to update the domain information.

Auth Access Type

The type of authentication access allowed for this switch:

- **Any access** - the switch can authenticate users originating from any access type.
- **Management access** - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions.
- **Monitoring - RADIUS Accounting** - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. NAC Manager learns about these session via RADIUS accounting. This allows NAC Manager to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch.
- **Manual RADIUS Configuration** - RADIUS configuration is performed manually on the switch using Policy Manager or CLI.

Switch Type

Specifies the switch type: a switch that authenticates layer 2 traffic via RADIUS to an out-of-band Access Control gateway, or a VPN concentrator being used in a [NAC VPN deployment](#).

Switch Location

The physical location of the switch.

Switch Contact

The person responsible for the switch.

Switch Description

A description of the switch, which may include its manufacturer, model number, and firmware revision number.

Management RADIUS Servers

RADIUS servers used to authenticate requests for administrative access to the switch.

RADIUS Accounting

Displays whether RADIUS accounting is enabled or disabled on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time connection status in NAC Manager. For more information, see [How to Enable RADIUS Accounting](#). RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. For more information, see the [Auth. Access Type](#) section of the Add/Edit Switch Window Help topics.

IP Subnet for IP Resolution

Displays the IP subnet that the switch is using as an inclusive list for MAC to IP resolution. IP subnets are configured in the [Appliance Settings > IP Resolution tab](#). Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it is not discovered via DHCP. IP Subnets also contain an IP range Extreme Management Center uses to filter out secondary IP addresses not valid for the network. For more information on MAC to IP Resolution, see the [NAC Deployment Guide](#).

Policy Enforcement Points

If the switch is a VPN device (see Switch Type column), this column displays the Policy Enforcement Points that are being used to provide authorization for the connecting end-systems.

Add Switch

Opens the [Add Switches to NAC Appliance Group window](#), where you can select switches to add to the engine or engine group.

Edit

Select a switch and click this button to open the [Edit Switches in NAC Appliance Group window](#), where you can change the switch's primary and secondary Access Control Gateway (Gateway), and also edit other switch attributes, if desired.

Delete

Select a switch and click this button to delete the switch from NAC Manager's device database. The switch's primary gateway enforces its own primary RADIUS server as both the primary and secondary RADIUS servers on the switch.

Related Information

For information on related windows:

- [Add Switches to a NAC Appliance Group Window](#)
- [Edit Switches in NAC Appliance Group Window](#)

NAC Manager Windows

The **Windows** section contains Help topics describing NAC Manager windows and their field definitions.

AAA Configuration

The AAA Configuration defines the RADIUS and LDAP configurations that provide the authentication and authorization services to your Extreme Access Control engines. A AAA Configuration can be a basic or advanced configuration. Basic AAA Configurations define the authentication and authorization services for all end-systems connecting to your Extreme Access Control engines. Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings.


This Help topic provides the following information for accessing and configuring the AAA Configuration:

- [Accessing the AAA Configuration](#)
- [Basic AAA Configuration](#)
- [Advanced AAA Configuration](#)

NOTE: Users with a AAA configuration using NTLM authentication to a back-end active directory domain whose passwords expire are prompted via windows to change their domain password.

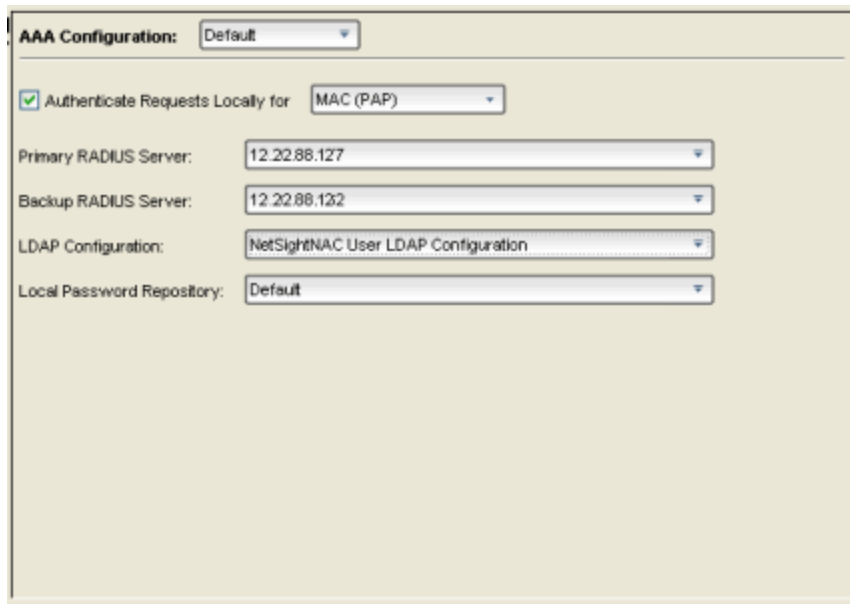
Accessing the AAA Configuration

Use the following steps to edit or change your AAA Configuration.

1. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
2. In the left-panel tree, select the AAA icon. The AAA Configuration is displayed in the right panel.
3. If needed, use the AAA Configuration drop-down menu in the right panel to select the configuration you want for your NAC Configuration, or to create a new one.
4. Use the fields in the right panel to edit or modify the configuration. The fields vary depending on whether you are editing a basic or advanced configuration. See the sections below for a description of each field and option in the panel.
5. Click **Save** to save your changes.

Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your Extreme Access Control (Access Control) engines.



The screenshot shows the 'AAA Configuration' web interface. At the top, there is a dropdown menu labeled 'AAA Configuration:' with 'Default' selected. Below this, there is a checked checkbox labeled 'Authenticate Requests Locally for' followed by a dropdown menu showing 'MAC (PAP)'. Underneath, there are four rows of configuration fields, each with a label and a dropdown menu: 'Primary RADIUS Server:' with '12.2288.127', 'Backup RADIUS Server:' with '12.2288.122', 'LDAP Configuration:' with 'NetSightNAC User LDAP Configuration', and 'Local Password Repository:' with 'Default'.

Authenticate Requests Locally

This option lets you specify that MAC authentication requests are handled locally by the Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems that are authorized locally.

Use the drop-down menu to select one or more MAC authentication types:

- MAC — includes MAC (PAP), MAC (CHAP), MAC (MsCHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) — this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) — this MAC authentication type requires a password, and the password must be the MAC address.

Primary/Backup RADIUS Servers

If your Access Control engines are configured to proxy RADIUS requests to a RADIUS server, use these fields to specify the primary and backup RADIUS servers to use. Use the drop-down menu to select a RADIUS server, add or edit a RADIUS server, or manage your RADIUS servers.

LDAP Configuration

Use this field to specify the LDAP configuration for the LDAP server on your network that you want to use in this AAA configuration. Use the drop-down menu to select an LDAP configuration, add or edit an LDAP configuration, or manage your LDAP configurations.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. NAC Manager supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down menu to select a repository, or add or [edit a repository](#).

Advanced AAA Configuration

Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings. Mappings can be based on:

- authentication type
- username/user group
- MAC address/end-system group
- hostname/hostname group
- location group
- authentication method
- RADIUS user group
- LDAP user group

NOTE: LDAP User Group is only available with an **Authentication Type** of **Registration**.

For example, in a higher education setting, you may want faculty members authenticating to one RADIUS server and students authenticating to another. You can also create mappings specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet.

Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of this, you might want to use the "Any" mapping (that is created automatically when you add a new advanced AAA configuration) as your last mapping in the list.

AAA Configuration: NetSight-NAC Lab AAA Configuration

Authenticate Requests Locally for: MAC (PAP)

Local Password Repository: Default

Join AD Domain: Auto Detect

Authentication Type	User/MAC/Host Match	Location	Authentication Method	Primary RADIUS Server	Backup RADIUS
Any	NAC2003 Users	Any	LDAP Authentication	None	None
Any	host/nac2003.com	Any	Proxy RADIUS	10.20.88.177	None
Any	NPSTEST Users	Any	LDAP Authentication	None	None
Any	host/npstest.com	Any	Proxy RADIUS	10.20.88.162	None
Any	NetSightNAC Users	Any	Proxy RADIUS	10.20.88.111	None
Any	host/netsightnac.com	Any	Proxy RADIUS	10.20.88.111	None
Any	*@devlab.com	Any	Proxy RADIUS	10.20.80.40	None
Any	*	Any	Local Authentication	None	None

Save Close Help

Authorize Authentication Requests Locally

This option lets you specify that MAC authentication requests will be handled locally by the Extreme Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems that are authorized locally.

Use the drop-down menu to specify a particular type of MAC authentication:

- MAC - includes MAC (PAP), MAC (CHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) - this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) - this MAC authentication type requires a password, and the password must be the MAC address.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. NAC Manager supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down menu to select a repository, or add or [edit a repository](#).

Join AD Domain

The Join AD Domain selection is only displayed if the AAA configuration has multiple mappings set to LDAP Authentication for an Active Directory domain, with different LDAP configurations specified. Specifying the domain to join is only necessary when multiple Active Directory domains are used but there is not a fully trusted relationship set up between all domains. If there is only a one-way trust set up between some domains you must choose the domain that can authenticate users from all the domains, which is determined by the configuration of a your Active Directory forest. Use the drop-down list to explicitly select which LDAP configuration of the Active Directory domain the Access Control engine joins in order to authenticate users to all Active Directory domains configured for that engine or select Auto Detect to let the Access Control engine determine the domain. Auto Detect starts at the first entry set to LDAP Authentication in the table and attempt to join that domain. If it cannot join that domain, it will go to the next entry that is set to LDAP Authentication and attempt to join that domain, and so on until one succeeds.

User to Authentication Mapping Table

This table lists mappings between groups of users and authentication configurations. The table displays the username to match along with the defined configuration parameters for that mapping. Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of

this, you might want to use an "Any" mapping as your last mapping in the list. Use the Mappings toolbar buttons to perform actions on the mappings.



Move Mappings Up/Down

Move mappings up and down in the list to determine mapping precedence. Mappings are listed in order of precedence from the top down.



Add New Mapping

Opens the [Add User to Authentication Mapping window](#) where you can define a new mapping.



Edit Mapping

Opens the [Edit User to Authentication Mapping window](#) where you can edit the selected mapping.



Delete Selected Mappings

Deletes any mappings selected in the table.



Manage LDAP Policy Mappings

Opens the [Manage LDAP to Policy Mappings window](#).



Manage AAA Trusted Certificate Authorities

Opens the [Update AAA Trusted Certificate Authorities window](#) where you can provide certificate authorities that are trusted to issue client certificates for 802.1x authentication (EAP-TLS, PEAP, or EAP-TTLS), as well as URLs for Certificate Revocation lists that can be used to check for revoked client certificates.

Related Information


For information on related windows:


- [Manage LDAP to Policy Mappings Window](#)
- [Add User to Authentication Mapping Window](#)

Add/Edit Agent-Based Test Set Window

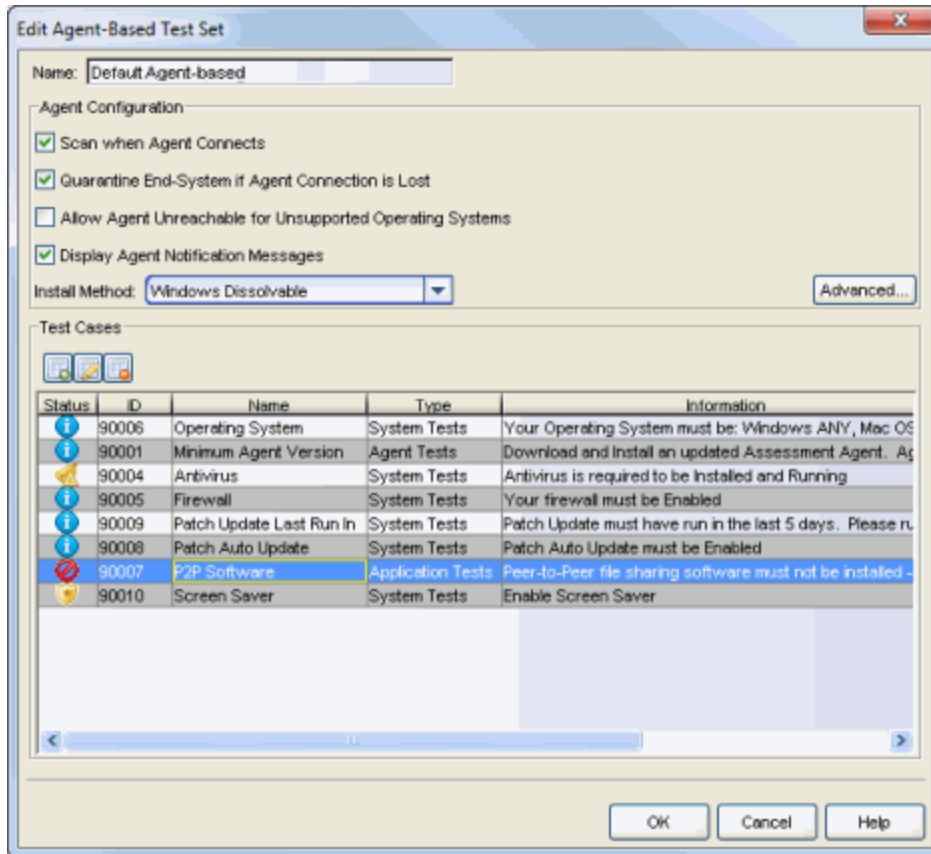
Use this window to add a new agent-based test set or edit an existing agent-based test set. In this window, you can configure the individual tests that you want the agent-based test set to perform. When you add a new test set, it becomes available for selection in the [Edit Assessment Configuration window](#).

Use the [Agent-Based Test Support per OS](#) tables (at the end of this topic) to determine which tests are supported on the various end-system operating systems.

To add an agent-based test set, click  (the configuration menu button in the Test Sets section of the [Edit Assessment Configuration window](#)) and select Add Agent-based. You can also click the Add button in the [Manage Test Sets window](#).

To edit an agent-based test set, from the [Edit Assessment Configuration window](#), click on the agent-based test set you want to edit, then click  (the configuration menu button in the Test Sets section), and select Edit. You can also click the Edit button in the [Manage Test Sets window](#).

NOTE: Changes made to the settings in this window are not effective until the end-system is rescanned.



Name

Enter a name for the test set.

Agent Configuration

Scan when Agent Connects

If this checkbox is selected, anytime the agent connects or reconnects, it will initiate a scan. If the checkbox is deselected, when the agent connects it will only initiate a scan if the end-system is quarantined or if the assessment interval has expired. Deselecting the checkbox reduces the number of scans taking place as end-systems connect and reconnect to the network. Note that the following checkbox must also be deselected to prevent the end-system from automatically being placed in the quarantine state when agent connection is lost.

Quarantine End-System if Agent Connection is Lost

If this checkbox is selected, an end-system is automatically placed in the quarantine state if connection to the agent is lost. This prevents end users from running the assessment agent to obtain network access, then

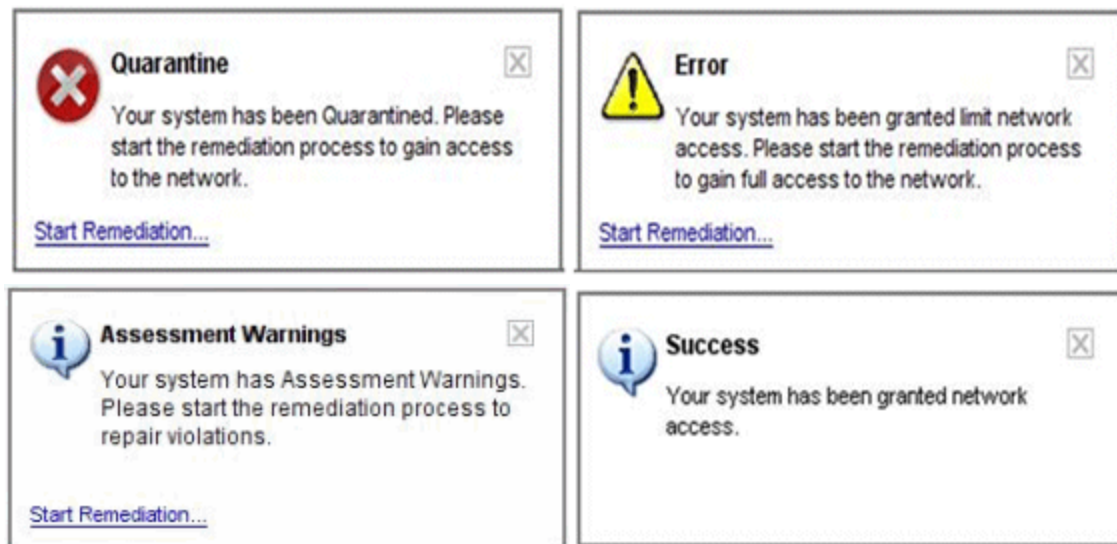
stopping the agent and changing their system settings in a manner that would normally fail assessment. Note that being placed in the quarantine state doesn't necessarily mean that the end user has been assigned a policy that prohibits network access.

Allow Agent Unreachable for Unsupported Operating Systems

If the end-system is running an unsupported operating system, the agent-based assessment will fail with an "Agent Unreachable" test result. If this checkbox is selected, the unsupported end-system will be allowed on the network where it can be assessed using on-board agent-less assessment or an external assessment server. See the How to Deploy Agent-Based Assessment Help topic for a list of [supported end user operating systems](#).

Display Agent Notification Messages

If this checkbox is selected, then once assessment has taken place, the end-system will receive a notification message that tells them if they are quarantined, in an error state, have assessment warnings, or are accepted:



Install Method

Specify the agent install method: persistent, dissolvable, or service.

- **Persistent** - A persistent agent will add itself to the startup group on Windows or the Login Items on the Mac, so that it will always restart with the system.

NOTE: For Windows users, the end user must have Write privileges for the `C:\Program Files` directory to install the persistent agent. A non-admin user by default does not have this permission.

- **Dissolvable** - A dissolvable agent will not automatically restart with the system and the end user will be directed to start the agent from a web page.
- **Service** - For Windows Persistent Service, the persistent agent will run as a service for all users and will continue to run when a user is logged out.

Advanced Button

Click this button to open the [Advanced Agent Configuration window](#) where you can configure advanced options for your agent-based test set.

Test Cases

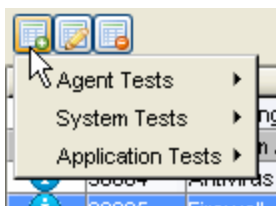
Use the Test Cases table to view and define the various tests that the test set will perform. The table displays information about each test case configured to run for this test set.

When you first open the Add Agent-Based Test Set window, the Test Cases table lists eight [default test cases](#). You can use these default test cases as is, edit them, or delete any tests you don't want performed (except the Operating System test). You can also add new [user-defined test cases](#) in addition to the default test cases. Use the Add New Test Cases button to access Editor windows where you can configure the different tests.

Status	ID	Name	Type	Information
	90006	Operating System	System Tests	Your Operating System must be: Windows ANY, Mac OS
	90001	Minimum Agent Version	Agent Tests	Download and install an updated Assessment Agent. Ag
	90004	Antivirus	System Tests	Antivirus is required to be installed and running
	90005	Firewall	System Tests	Your firewall must be enabled
	90009	Patch Update Last Run In	System Tests	Patch Update must have run in the last 5 days. Please ru
	90008	Patch Auto Update	System Tests	Patch Auto Update must be enabled
	90007	P2P Software	Application Tests	Peer-to-Peer file sharing software must not be installed.
	90010	Screen Saver	System Tests	Enable Screen Saver







Use these buttons to add, edit, or delete test cases listed in the table. Use the Add button to access Editor windows where you can create the different kinds of tests.



Status

Displays the status configured for each test. The status determines how the score returned by the assessment test will be used.

-  Disabled - The test does not run.
-  Informational - The test runs and test score results are reported, but are not applied toward a quarantine decision. No end-systems are quarantined. Auto-remediation is performed, if enabled.
-  Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation is performed, if enabled.
-  Mandatory - Test score results are included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation is performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

ID

Test cases are assigned a Test Case ID number when they are created. You can refer to these Test Case ID numbers when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Name

The name of the test case.

Type

The type of test case: Agent, System, or Application Test.

Information

Information about the test case requirements that have been configured.

Operating System(s)

The operating systems to which this test case applies. To view a table that lists which tests are supported on the various end-system operating systems, see [Agent-Based Test Support per OS](#).

Auto-Remediate

Certain test cases allow you to specify that NAC Manager attempts to auto-remediate any problems found by the test.

Default Test Cases

Following is a list of the default test cases that you can use for your test set. Default test cases are automatically assigned a Test Case ID number that cannot be changed. You can refer to these Test ID numbers when creating scoring overrides.

Operating System

This test checks to see if the operating system on the end-system matches a specified value. This is the only test that cannot be deleted or renamed. For more information, see the [Operating System Editor](#).

Minimum Agent Version

This test checks to see if the agent version on the end-system is the same as, or newer than, the specified version level. For more information, see the [Minimum Agent Version Editor](#).

Antivirus

This test checks to see if the state of the antivirus software matches the specified state. Windows requires the Windows Security Center for this test. For more information, see the [Antivirus Editor](#).

Firewall

This test checks to see if the end-system's firewall is enabled or disabled. Windows Security Center is required for this test. For more information, see the [Firewall Editor](#).

Patch Update Last Run In

This test checks to see if the last time a Windows patch update was run on the end-system falls within the specified time frame. This test relies on the Windows Update software program. For more information, see the [Patch Update Last Run In Editor](#).

Patch Auto Update

This test checks to see if Patch Auto Update is enabled or disabled on the end-system. This test relies on the Windows Update software program. For more information, see the [Patch Auto Update Editor](#).

P2P Software

This test checks to see if the specified file transfer software is installed or running on the end-system. For more information, see the [P2P Software Editor](#).

Screen Saver

This test checks to see if a screen saver is enabled, if the screen saver is secured (password protected), and the time before the screen saver starts. For more information, see the [Screen Saver Editor](#).

User-Defined Test Cases

Here is a list of user-defined tests that you can create and include in your agent-based test set. User-defined test cases are automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to these Test ID numbers when creating scoring overrides.

Hotfix Check

This test checks to see if a specific hotfix has been installed on the end-system. For more information, see the [Hotfix Check Editor](#).

File Check

This test checks to see if a specific file is on the end-system. For more information, see the [File Check Editor](#).

Process State Check

This test checks to see if a specific process is running on the end-system. For more information, see the [Process State Check Editor](#).

Registry Key Check

This test checks to see if the end-system has a specific Windows registry key. For more information, see the [Registry Key Check Editor](#).

Registry Key Check Advanced

This test checks to see if the end-system has one or more Windows registry keys. For more information, see the [Registry Key Check Advanced Editor](#).

Service State Check

This test checks to see if a specific service is installed and running on the end-system. For more information, see the [Service State Check Editor](#).

Installed Program Check

This test checks to see if a specific program is installed and running on the end-system. For more information, see the [Installed Program Check Editor](#).

NOTE: The Installed Program Check test case is supported with agent version 1.15.0.0 and later.

Agent-Based Test Support per OS

When configuring agent-based test sets, use the following tables to determine which tests are supported on the various end-system operating systems.

OS Test Support

Operating System	Antivirus	Screen Saver	Patch Update Last Run	Patch Auto Update	Firewall
Windows 10	X	X	-	X	X
Windows 8.1	X	X	X	X	X
Windows 8	X	X	X	X	X
Windows 7	X	X	X	X	X
Windows Vista SP1	X	X	X	X	X
Windows XP SP2/SP3	X	X	X	X	X
Windows XP SP1	X	X	X	X	-
Windows 2008	X	X	X	X	X
Windows 2003 SP2	X	X	X	X	-
Windows 2000 SP4	X	X	X	X	-
Mac OS X Tiger	X ¹	X	-	X	X
Mac OS X Leopard	X ¹	X	-	X	X
Mac OS X Snow Leopard	X ¹	X	-	X	X
Mac OS X Lion	X ¹	X	-	X	X
Mac OS X Mountain Lion	X ¹	X	-	-	X
Mac OS X Mavericks	X ¹	X	-	-	X
Mac OS X Yosemite	X ¹	X	-	-	X
Mac OS X El Capitan	X ¹	X	-	-	X

¹Supports Norton AntiVirus, McAfee Virex, Sophos Anti-Virus, ClamX AV 2, and Symantec 10 and 11.

OS Test Support

Operating System	P2P Software	Registry Key Check	Service State Check	Process State Check	Hotfix State Check	File Check
Windows 10	X	X	X	X	X	X
Windows 8.1	X	X	X	X	X	X
Windows 8	X	X	X	X	X	X
Windows 7	X	X	X	X	X	X
Windows Vista SP1	X	X	X	X	X	X
Windows XP SP2/SP3	X	X	X	X	X	X
Windows XP SP1	X	X	X	X	X	X

Operating System	P2P Software	Registry Key Check	Service State Check	Process State Check	Hotfix State Check	File Check
Windows 2008	X	X	X	X	X	X
Windows 2003 SP2	X	X	X	X	X	X
Windows 2000 SP4	X	X	X	X	X	X
Mac OS X Tiger	X ¹	-	-	X	-	X
Mac OS X Leopard	X ¹	-	-	X	-	X
Mac OS X Snow Leopard	X ¹	-	-	X	-	X
Mac OS X Lion	X ¹	-	-	X	-	X
Mac OS X Mountain Lion	X ¹	-	-	X	-	X
Mac OS X Mavericks	X ¹	-	-	X	-	X


¹No eMule.


Related Information

- [How to Deploy Agent-Based Assessment](#)
- [Edit Assessment Configuration Window](#)
- [Manage Test Sets Window](#)

Add/Edit Agent-less Test Set Window

Use this window to add a new agent-less test set or edit an existing agent-less test set. In the test set you can define certain assessment parameters, such as scanning level and scoring mode, and specify which assessment resources to use. When you add a new test set, it becomes available for selection in the [Edit Assessment Configuration window](#).

To add an agent-less test set, click  (the configuration menu button in the Test Sets section of the [Edit Assessment Configuration window](#)) and select Add Agent-less. You can also click the Add button in the [Manage Test Sets window](#).

To edit an agent-less test set, from the [Edit Assessment Configuration window](#), click on the agent-less test set you want to edit, then click  (the configuration menu button in the Test Sets section), and select Edit. You can also click the Edit button in the [Manage Test Sets window](#).

Name

Enter a name for the test set.

End-System Reachability Test

Click the **Modify** button to open a window where you can select the type of end-system reachability test that will be used to verify that the end-system can be reached prior to and following assessment: ICMP Ping and/or TCP Ping with a list of ports. If neither test is selected, then there will be no test.

Running either or both tests allows NAC Manager to determine if an end-system is reachable prior to running an assessment. If the end-system is not reachable, the assessment will not be run and the end-system will receive the Failsafe policy. If the end-system is reachable, the assessment will be performed. Without reachability testing, if assessment is required and the

end-system is not reachable, the assessment may take significantly more time and you could see a "false positive" in the sense that the assessment would come back without errors, but only because the end-system could not be contacted to do an assessment. In this case, the end-system would be assigned the Accept policy and allowed on the network without an actual assessment taking place.

Another advantage to running end-system reachability tests is that the test is performed before **and** after an assessment. If test results are different, the end-system will be quarantined. For example, with a TCP Ping test that has 15 ports configured, if any of the ports differ before or after the assessment, the end-system is quarantined. With the ICMP Ping test, if the end-system passes the test before assessment, but fails the test after assessment, the end-system is quarantined.

NOTE: For ICMP Ping, how NAC Manager handles the timeout per ping attempt may differ depending on the operating system on which the Extreme Management Center server is running, however the total timeout period specified will be the same (e.g. 2 attempts * 5 timeouts = 10 seconds). For TCP Ping, the number of ping attempts is not specified because it is inherent in the TCP protocol.

Scoring

The Scoring Mode lets you decide how the score returned by an assessment test will be used:

- Apply Score - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.
- Informational - Test score results will be reported, but are not applied toward a quarantine decision. This allows you to use assessment as a data-gathering mechanism without end-systems being quarantined or warned.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification Portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.

Scoring overrides can be used to change the scoring mode for specific tests. For example, you may set a scoring mode of "Informational" and then configure scoring overrides to set specific tests to count towards a quarantine decision. Or, you may select a scoring mode of "Apply Score" (quarantine), and then create scoring overrides to set specific tests to be warnings. Use the Manage Scoring Overrides button to open the [Manage](#)

[Scoring Override Configurations window](#) where you can view and define your scoring overrides.

The text below the Scoring Mode selection describes the behavior that will result from the current scoring mode and any scoring override settings. Since a test set can be used in different assessment configurations, this description is based on the assessment configuration that is currently open.

Scanning Level

The agent-less assessment can be configured to assess end-systems at various levels of intensity. Light assessments will be faster but will not gather as much information as heavy assessments.

- **Light** - The assessment collects information from the DNS (Domain Name System), tries to identify the operating system, and tries to establish what RPC (Remote Procedure Call) services the end-system offers and what file systems it shares via the network.
- **Default** - This scanning level scans roughly 600 ports and performs around 1,200 tests.
- **Heavy** - At this level, the scan checks for services listening on any TCP port from 1 to 10,000, and any UDP port from 1 to 2,050, with the exception of WinNT ports which are known to cause certain software to crash when scanned. Any services detected will then be scanned for any known vulnerabilities. It performs roughly 2,750 tests.
- **Custom** - This scanning level lets you run a custom Saint scan. Enter the custom scan file. For information on creating a custom scan see [How to Create a Custom Scan for Agent-less Assessment](#).

Scan Level Modifiers

Depending on what scan level you select, you can select from the following options to modify scan performance:

- **Full Port Scan** - Scans all ports (10000+ tcp, 2700+ udp) versus common ports (500+ tcp, 60+ udp). Useful for detecting services running on either common ports or non-standard ports.
- **Exhaustive Scan** - Runs a more thorough scan, but may cause the scan to take more time. Examples include checking for default router passwords on non-standard telnet ports, checking for Web application vulnerabilities in non-standard directories, checking for proxy vulnerabilities on non-standard HTTP ports, and checking for Oracle and Sybase vulnerabilities on all unidentified ports.

- **Perform Dangerous Tests** - The assessment will include dangerous checks, in which certain vulnerability exploits are launched in order to confirm that the end-system is or is not vulnerable. These tests may help eliminate false alarms by verifying the existence of certain vulnerabilities, but can cause services on the end-systems to crash as a result. Another side-effect of dangerous tests is that successful detection of a vulnerability could cause other vulnerabilities to be missed. That is, if a test crashes a service on the end-system, then any further tests against that service will come up negative. End-systems should be re-scanned after the known vulnerabilities have been fixed in case there are other vulnerabilities that were missed because the service crashed. If this option is not selected, then the assessment will skip these dangerous tests, and will report a potential problem if there is a possibility that the vulnerability exists.

Authentication

In order to conduct the most thorough and accurate scan possible, the agent-less assessment gives you the option of authenticating to target end-systems. Authentication allows the assessment to access the registry, file attributes, or package lists on the remote target. There are two benefits to authentication. First, an authenticated scan is able to detect additional vulnerabilities, such as client vulnerabilities and missing hot fixes, which could not otherwise be detected by probing network services. Second, an authenticated scan is sometimes able to check for fixes whose presence could not otherwise be determined, thereby reducing false alarms. If you choose not to authenticate, the assessment will still conduct its full set of unprivileged vulnerability checks, omitting only those few which require authentication.

If you wish to run an authenticated assessment, enter a valid login and password in this section:

- **Windows Domain Administrator** - Do **not** enter the domain name in the login field. The agent-less assessment will automatically authenticate to the domain that the end-system is a member of. For example, if you are scanning Host1 and Host2, and Host1 and Host2 are members of Domain_A, then the assessment will authenticate with Domain_A. If you also scan Host3, and Host3 is a member of Domain_B, then the assessment will use the provided password to authenticate with Domain_B when scanning that target. If a target is not a member of a domain, the assessment will assume the given account is a local account on each target. To use a local account even

if the end-system is a member of a domain, specify the account name as "local:login", where login is the login name. Do not put a space after the colon.

CAUTION: The encrypted Windows authentication functions require the crypto library which comes with OpenSSL. If the OpenSSL libraries are missing or outdated on the scanning system, a warning message will appear when the assessment starts, and passwords will be sent over the network in clear text.

Keep in mind that the assessment's detection of Windows updates should be used as a baseline assessment only. The assessment detects Windows updates using simple checks for the presence of registry keys and file time stamps, which cannot always account for updates which have been incorrectly installed, uninstalled, rendered ineffective due to incorrect order of installation, or other unusual situations. For more thorough evaluation of Windows updates, it would be advisable to use one of several available patch management tools.

- **SSH Login** - For authentication to Linux, Unix, and Macintosh end-systems, any active user account on the system may be used. The SSH service must be running on the remote end-system in order for authentication to function.
- **SNMP Communities** - SNMP runs on routers and switches, as well as some printers, servers, and workstations. SNMP access is controlled using community strings and provides configuration information which could be used for improved host detection and vulnerability detection. Enter a comma-separated list of community strings that the assessment can use for SNMP access. It is not necessary to include default strings such as "public" and "private."

Test Set Assessment Resources

Define which assessment servers you want to have perform the assessments.

- **Use Onboard Assessment** - Use the onboard agent-less assessment server.
- **Load Balance All** - Balance the assessment load across all of the agent-less assessment servers on the network.
- **Use Assessment Server Pool** - As a more granular approach, you can specify an assessment server pool. For example, if you have four agent-less assessment servers, you can put server A and server B in

server pool 1, and server C and server D in server pool 2. Then, you can specify which server pool the configuration should use.

 Use the configuration menu button to:

- Add - Open the [Add Assessment Server Pool window](#) where you can add a new server pool.
- Edit - Open the [Edit Assessment Server Pool window](#) where you can edit the selected server pool.
- Used By - List all assessment test sets currently using the selected server pool.
- Manage - Open the [Manage Assessment Server Pools window](#) where you can view and define the assessment server pools that will be used in your assessment configurations.

Assessment Delay

This option allows you to delay the start of the assessment by the number of seconds specified.

Related Information

For information on related windows:

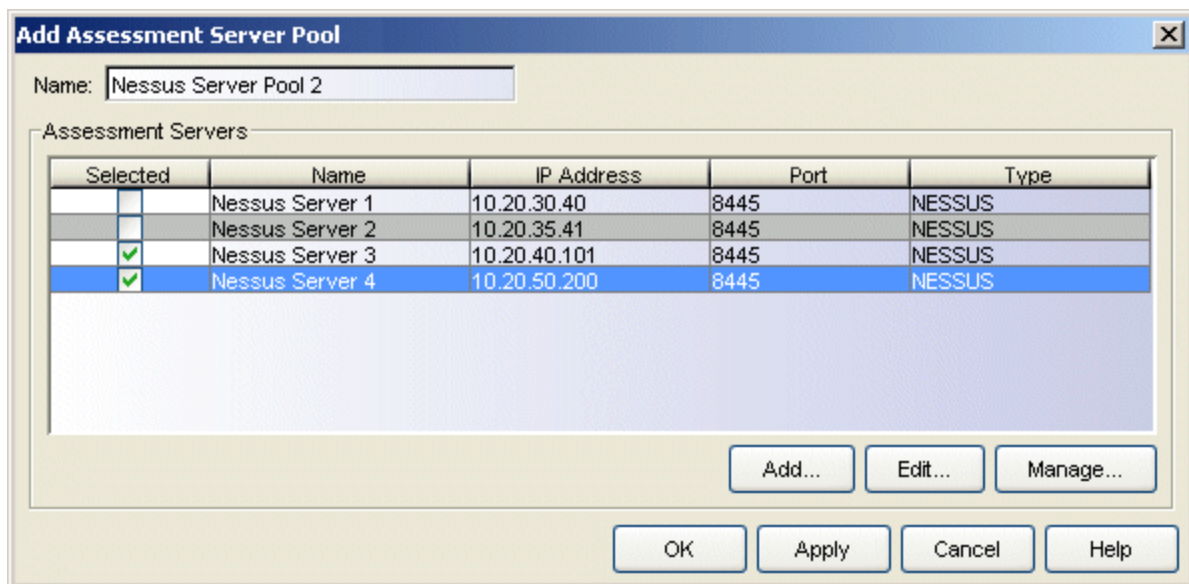
- [Edit Assessment Configuration Window](#)
- [Manage Test Sets Window](#)
- [Manage Assessment Server Pools Window](#)
- [Add/Edit Assessment Server Pool Window](#)

Add/Edit Assessment Server Pool Window

Use this window to create a new assessment server pool or edit an existing server pool.

To add an assessment server pool, click **Add** in the [Manage Assessment Server Pools window](#).

To edit an assessment server pool, select a server pool in the [Manage Assessment Server Pools window](#) and click **Edit**.



Name

Enter a name for the server pool.

Selected

Use this column to select the assessment servers you want in this pool.

Name

The name of the assessment server.

IP Address

The IP address of the assessment server.

Port

The port number on the assessment server to which the Extreme Access Control engine sends assessment requests.

Type

The assessment server type.

Add Button

Opens the [Add Assessment Server window](#) where you can add a new assessment server.

Edit Button

Opens the [Edit Assessment Server window](#) where you can edit the selected assessment server.

Manage Button

Opens the [Manage Assessment Servers window](#) where you can view and configure the assessment servers that will perform the end-system assessments in your network.

Related Information

For information on related windows:

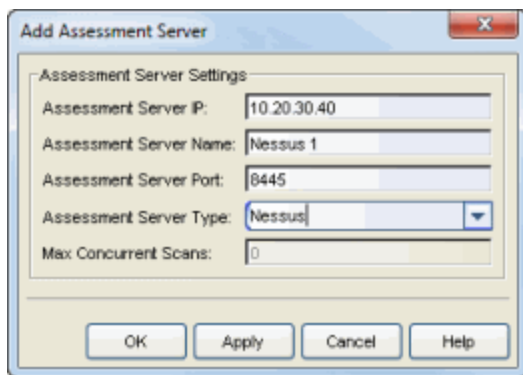
- [Manage Assessment Servers Window](#)
- [Edit Assessment Configuration Window](#)
- [Add/Edit Assessment Server Window](#)

Add/Edit Assessment Server Window

Use this window to add and configure a new assessment server or edit the settings for an existing assessment server. When you add an assessment server, it is added to the [Manage Assessment Settings window](#).

To add an assessment server, open the Manage Assessment Settings window (Tools > Manage Assessment Settings), select the Assessment Servers tab, and click the **Add** button.

To edit an assessment server, open the Manage Assessment Settings window (Tools > Manage Assessment Settings), select the Assessment Servers tab, and click the **Edit** button.



Assessment Server IP

The IP address of the assessment server.

Assessment Server Name

The name of the assessment server.

Assessment Server Port

The port number on the assessment server to which the Extreme Access Control engine sends scanning requests; the default port number is 8445.

Assessment Server Type

Use the drop-down menu to select the assessment server type (Agent-less or Nessus) or enter a third-party assessment agent (an assessment agent that is not supplied or supported by NAC Manager).

Max. Concurrent Scans

Enter the maximum number of scans that can be performed concurrently on this assessment server. For example, if the max is set to 50, and 1000

end-systems come online and need to be scanned, then only 50 scans occur concurrently. Each time a scan is completed a new one starts, but no more than 50 scans are performed at the same time. This is to prevent overwhelming the assessment server with assessment requests.

NOTE: The Max. Concurrent Scans value can only be set from the Edit Assessment Server window. This is because NAC Manager must be able to communicate with the server in order to set the value. So the server must first be added before the Max. Concurrent Scans value can be set.

Related Information

For information on related windows:

- [Manage Assessment Settings Window](#)

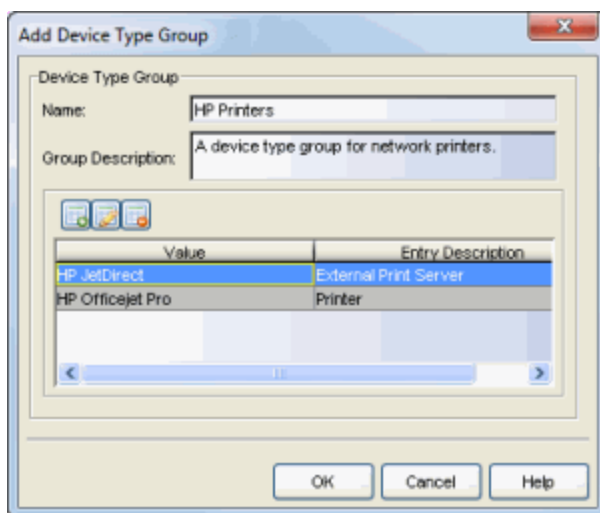
Add/Edit Device Type Group Window

There are nine system-defined operating system family device type groups that are automatically populated by NAC Manager: Android, Apple iOS, Blackberry, Chrome OS, Game Console, Linux, Mac, Windows, and Windows Mobile. You can view these system-defined groups and your other device type groups in the Manage Rule Groups window, by selecting **Tools > Manage Rule Groups** from the menu bar.

Device type groups are comprised of entries that NAC Manager uses to determine if an end-system's device type matches the group. Entries can be a specific device type or a wildcard, such as Windows 7 or win*. If an entry does not already contain a wildcard, NAC Manager creates a wildcard by adding an asterisk (*) to the beginning and end of the entry. For example, if the entry is **Gentoo**, the match pattern is ***Gentoo*** allowing a match for any end-system device type that contains Gentoo. This allows you to restrict the match to a very specific value that might include a version number or model number, or expand the match to include all versions and model numbers of a certain operating system or hardware family.

For more information on how to use device type groups, see [How to Use Device Type Profiling](#).

NOTE: Changes to rule groups do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a new name for the device type group. You cannot edit the name of a group.

Group Description

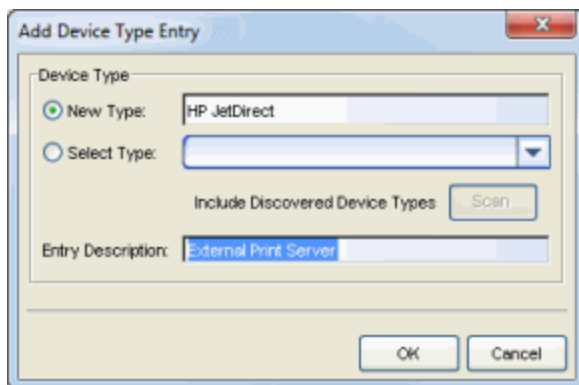
Enter a description of the device type group.



Use these buttons to add, edit, or delete device type entries in the group.

TIP: You can also copy and edit entries by right-clicking on an entry and selecting **Copy**. This allows you to quickly add group entries by copying a single entry in the table and editing the device type value.

Click the Add Item button to open the Add Device Type Entry window.



Use this window to add a new entry by entering a device type or a wildcard, such as Windows 7 or win*. Alternately, you can select a type from a list of entries that already appear in existing device type groups. This list allows you to multi-select entries, and each entry appears as a separate row in the table. The list also allows you to select "Unknown" that matches against any device that does not have an operating system name, either due to failed detection or because detection hasn't happened yet.

All entries selected from the list are assigned the same description. If you would like a separate description for each type, you need to add each entry individually.

In addition, there is an option to **Include Discovered Device Types** in the selection list, by performing a scan of the database to find all detected end-system device types from the end-system table. Using this scan you can

populate the list with the exact device types being seen on the network.
Note that this scan may take a few seconds to perform.

Related Information

For information on related windows:

- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

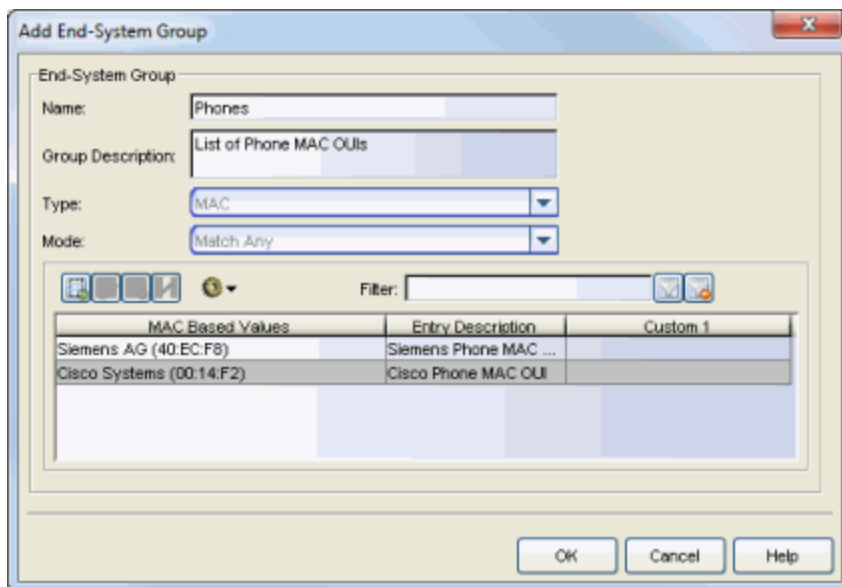
Add/Edit End-System Group Window

Use this window to add a new end-system group or edit an existing end-system group. End-system groups are rule components that allow you to group together devices having similar network access requirements or restrictions. You can access the Add/Edit End-System Group window from the [Manage Rule Groups window](#) or from the end-system group field in the [Create Rule window](#).

There are six system-defined end-system groups that are automatically populated by NAC Manager. The first is the Assessment Warning end-system group that includes end-systems that have assessment warnings and must acknowledge them before being granted access to the network. The second is the Blacklist end-system group that includes end-systems denied access to the network. The other four system-defined groups are populated as end-systems register through the Registration portal.

You can view and edit the system-defined groups and your other end-system groups in the Manage Rule Groups window, by selecting **Tools > Manage Rule Groups** from the menu bar.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a new name for the end-system group. You cannot edit the name of a group.

Group Description

Enter a description of the end-system group. If you are using Data Center Manager (DCM), the end-system group description contain the DCM specific settings as key/value pairs.

Type

Specify the criteria on which the end-system group is based:

- MAC - a list of MAC addresses, MAC OUI, or MAC Masks.
- IP - a list of IP addresses or subnets.
- Hostname - a list of hostnames: exact match or wild card (for example, *.extremenetworks.com).
- LDAP Host Group - a way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network. Note for the standard use with Active Directory, the Appliance Settings > Hostname Resolution must be configured to use DNS Hostname Resolution so NAC Manager can resolve the Fully Qualified Domain Name. In the LDAP configuration, you must also have the "Use Fully Qualified Domain Name" checkbox selected.

Mode

For LDAP Host Groups, the mode option lets you specify whether to match any or match all of the LDAP attributes listed below. You can also use "Exists" to just check to see if a host is present in LDAP.



Use these buttons to add, edit, or delete end-system entries in the group. The entries are displayed in the table below. Use the Move button to move a selected end-system entry to a different end-system group.

TIP: You can also copy and edit entries by right-clicking on an entry and selecting **Copy**. This allows you to quickly add group entries by copying a single entry in the table and editing the entry values.



Use the configuration menu button to either open a window where you can select MAC OUI vendors (if you are creating MAC entries) or open a window where you can select a file for importing entries.

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Custom 1

Use this column to add additional information that you would like displayed. To add or edit custom information, right-click on the table entry and select Edit Custom Information. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, right-click in the table body and select Table Tools > Settings. In the Table Settings window, you can select to show these columns in the table. To clear the custom information, right-click on the table entry and select Clear Custom Information. You can change the text of the Custom column heading in the [Options window Display view](#) (Tools > Options).

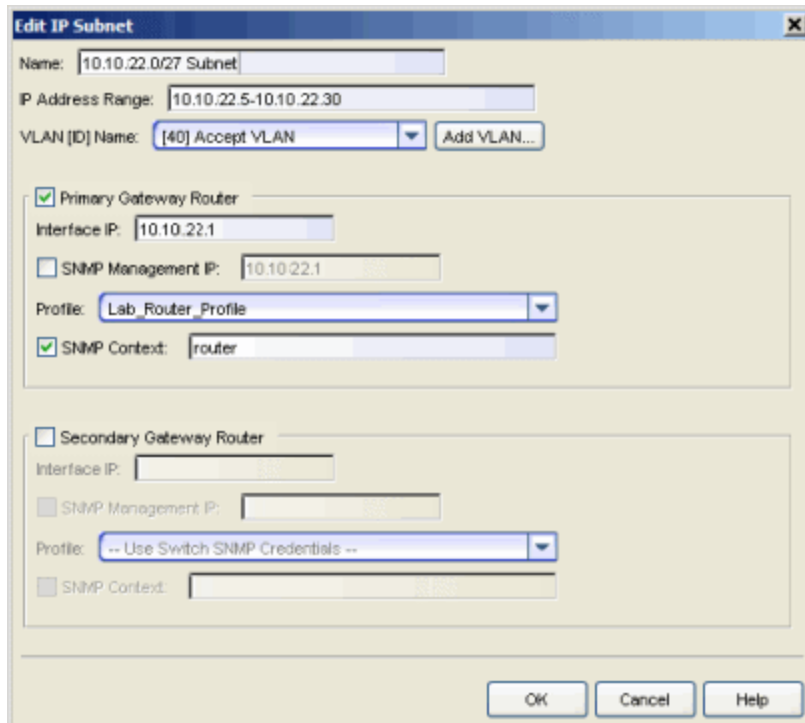
Related Information

For information on related windows:

- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

Add/Edit IP Subnet Window

Use this window to add or edit IP subnets used to assist in IP resolution. IP resolution resolves an end-system's MAC address to an IP address. You can access the Add/Edit IP Subnet window from the **IP Resolution** tab in the [Appliance Settings window](#).



Name

Enter a name for the IP subnet.

IP Address Range

Enter an IP address range for the subnet, which can be used to filter duplicate IPs.

VLAN [ID] Name

If a switch is using RFC 3580 (VLAN enforcement of access control), IP subnets can be defined for each VLAN to provide an IP range filter which can be used to filter the list of IPs discovered on the switch. Use the drop-down list to select the VLAN Name for the subnet. This list displays any VLANs defined in the legacy java Console application as well as any VLANs that are currently associated with a policy. Click **Add VLAN** to add a VLAN to the list.

Primary/Secondary Gateway Router

This section is used to provide gateway router configuration information for the following two scenarios:

- When using VRRP or HSRP, and you want NAC Manager to query the router for IP resolution if needed, NAC Manager needs to know the primary/secondary router relationship. This order of precedence can be defined in the IP subnet and ensures that NAC Manager queries the primary router first to get the most accurate data. Define the primary and secondary router in a VRRP or HSRP environment, because both routers send out a DHCP inform message, and it is likely that the Extreme Access Control Gateway gets the secondary router's message last, causing it to query the incorrect router.
- When using DHCP snooping, the router SNMP credentials are not the same for all routers. In this scenario, if you want NAC Manager to query the router for IP resolution, use the IP subnets to define the mapping between the relay router IPs and the correct SNMP credentials to use for them.

Select the checkbox for the primary and/or secondary gateway router and provide the following information. If you select both primary and secondary routers, a section for a tertiary gateway router is also provided.

Interface IP

Enter the IP address of the router interface that is for the subnet and/or VLAN being defined.

SNMP Management IP

If the router can only accept SNMP requests to one specific IP interface, select this checkbox and enter the SNMP Management IP address for the router.

Profile

If you have created a unique profile for this router, select it here. Otherwise, leave the profile set to "Use Default Router Profile" which is specified in the [IP Resolution tab](#) in the Add/Edit Appliance Settings window.

SNMP Context

When checked, you can specify an SNMP context that has been configured on a device. An SNMP context is a collection of MIB objects, often associated with a network entity. The SNMP context lets you access a subset of MIB objects related to that context.

Related Information

For information on related windows:

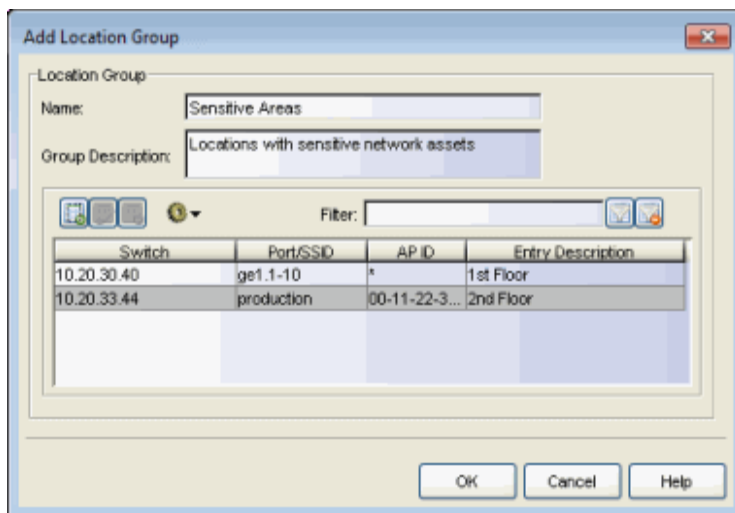
- [Appliance Settings Panel](#)
- [Add/Edit Appliance Settings Window](#)

Add/Edit Location Group Window

Use this window to add a new location group or edit an existing location group. Location Groups are rule components that allow you to specify network access requirements or restrictions based on the network location where the end user is connecting. For example, in an enterprise environment, an engineer logging on to the network from the corporate cafeteria could receive different network access than an engineer logging on from the engineering development area.

You can access the Add/Edit Location Group window from the [Manage Rule Groups window](#) or from the location group field in the [Create Rule window](#).

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new location group. You cannot edit the name of a group.

Group Description

Enter a description of the location group.



Use these buttons to add, edit, or delete entries in the group. The Add button opens the Add Location Entry window where you can use the tooltips for an explanation on what to enter in each field.

TIP: You can also copy and edit entries by right-clicking on an entry and selecting **Copy**. This allows you to quickly add group entries by copying a single entry in the table and editing the location values.



Use the configuration menu button to open a window where you can select a file for importing IP address locations. The files must be formatted as follows:

- IP addresses must be listed one per line.
- Lines starting with # or // are ignored.
- Lines are formatted with the following information: <IP address><interface><description>. The entry description is optional.
 - For wired interfaces, use a colon (:) between the IP address and interfaces, quotes (") around multiple interfaces, and a comma (,) between the interface and description. For example:
122.111.45.48:"fe.1.12, fe 1.13",My Wired
 - For wireless interfaces, use a semicolon (;) between the IP address and SSIDs, quotes (") around multiple SSIDs, a dollar sign (\$) between SSIDs and AP IDs, and a comma (,) between the interface and description. For example:
122.111.45.50;"my-SSID-AAA2,my-SSID-BBB3"\$Any,My Wireless
- Existing values with the same IP address are skipped.

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Related Information

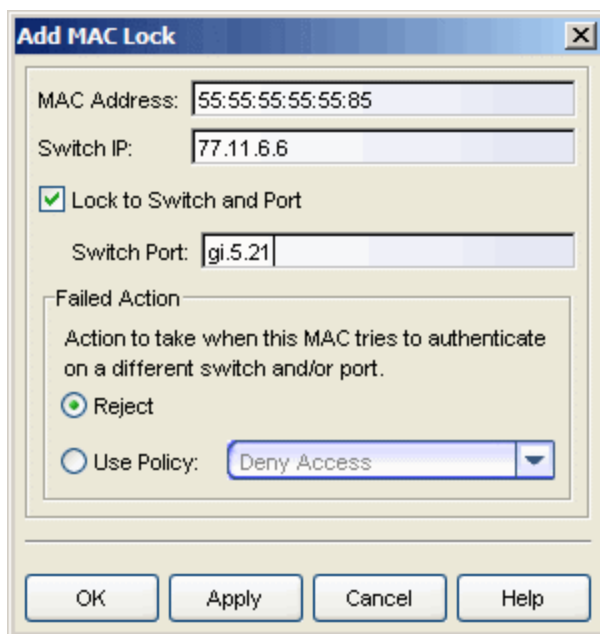
For information on related windows:

- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

Add/Edit MAC Lock Window

Use this window to add a new locked MAC address or edit the settings for an existing locked MAC address. MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different switch/port, it is rejected or assigned a specific policy. You can add or edit MAC locks from the [End-Systems tab](#). You can also view all your locked MAC addresses in the [Manage MAC Locks window](#) (Tools > Manage MAC Locks).

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name changes and breaks the MAC Locking settings.



The screenshot shows the 'Add MAC Lock' dialog box. The 'MAC Address' field contains '55:55:55:55:55:85'. The 'Switch IP' field contains '77.11.6.6'. The 'Lock to Switch and Port' checkbox is checked. The 'Switch Port' field contains 'gi.5.21'. Under the 'Failed Action' section, the 'Reject' radio button is selected, and the 'Use Policy' dropdown menu is set to 'Deny Access'. The dialog box has 'OK', 'Apply', 'Cancel', and 'Help' buttons at the bottom.

MAC Address

Enter the MAC address that you want to lock.

Switch IP

Enter the IP address of the switch to which you want to lock the MAC address.

Lock to Switch and Port

Select this checkbox if you want to lock the MAC address to a specific port on the switch, and enter the port interface name.

Failed Action

Select the action to take when this MAC address tries to authenticate on a different port and/or switch:

- Reject - The authentication request is rejected.
- Use Policy - Use the drop-down menu to select the policy that you want applied. This policy must exist in Policy Manager and be enforced to the switches in your network.


Related Information


For information on related windows:

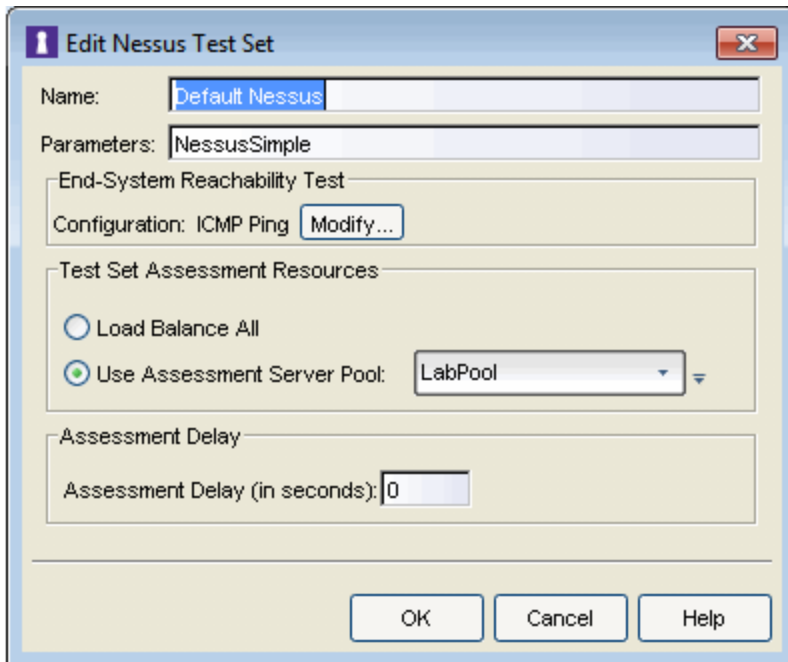
- [Manage MAC Locks Window](#)

Add/Edit Nessus Test Set Window

Use this window to add a new Nessus test set or edit an existing Nessus test set. Test sets let you define what type of assessment to execute (in this case, Nessus), what parameters to pass to the assessment server, and which resources to use. When you add a new test set, it becomes available for selection in the [Edit Assessment Configuration window](#).

To add a Nessus test set, click  (the configuration menu button in the Test Sets section of the [Edit Assessment Configuration window](#)) and select **Add Nessus**. You can also click the **Add** button in the [Manage Test Sets window](#).

To edit a Nessus test set, from the [Edit Assessment Configuration window](#), click on the Nessus test set you want to edit, then click  (the configuration menu button in the Test Sets section), and select **Edit**. You can also click the **Edit** button in the [Manage Test Sets window](#).



Name

Enter a name for the test set.

Parameters

Enter the scan policy name available in the Nessus **Policies** tab. For example, if you want to scan with the "NessusSimple" policy (as shown below), then you must enter the policy name **NessusSimple** in the field. This field is not optional and must provide a policy name.



End-System Reachability Test

Click the **Modify** button to open a window where you can select the type of end-system reachability test used to verify that the end-system can be reached prior to and following assessment: ICMP Ping and/or TCP Ping with a list of ports. If neither test is selected, then no test is run.

Running either or both tests allows NAC Manager to determine if an end-system is reachable prior to running an assessment. If the end-system is not reachable, the assessment is not run and the end-system receives the Failsafe policy. If the end-system is reachable, the assessment is performed. Without reachability testing, if assessment is required and the end-system is not reachable, the assessment may take significantly more time and you could see a "false positive" in the sense that the assessment would come back without errors, but only because the end-system could not be contacted to do an assessment. In this case, the end-system would be assigned the Accept policy and allowed on the network without an actual assessment taking place.

Another advantage to running end-system reachability tests is that the test is performed before **and** after an assessment. If test results are different, the end-system is quarantined. For example, with a TCP Ping test that has 15 ports configured, if any of the ports differ before or after the assessment, the end-system is quarantined. With the ICMP Ping test, if the end-system passes the test before assessment, but fails the test after assessment, the end-system is quarantined.

NOTE: For ICMP Ping, how NAC Manager handles the timeout per ping attempt may differ depending on the operating system on which Extreme Management Center server is running, however the total timeout period specified is the same (e.g. 2 attempts * 5 timeouts = 10 seconds). For TCP Ping, the number of ping attempts is not specified because it is inherent in the TCP protocol.

Test Set Assessment Resources

Define which assessment servers you want to have perform the assessments.

- **Load Balance All** - Balance the assessment load across all of the Nessus servers on the network.
- **Use Assessment Server Pool** - as a more granular approach, you can specify an assessment server pool. For example, if you have four Nessus assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, you can specify which server pool the configuration should use.



Use the configuration menu button to:

- Add - Open the [Add Assessment Server Pool window](#) where you can add a new server pool.
- Edit - Open the [Edit Assessment Server Pool window](#) where you can edit the selected server pool.
- Used By - List all assessment test sets currently using the selected server pool.
- Manage - Open the [Manage Assessment Server Pools window](#) where you can view and define the assessment server pools used in your assessment configurations.

Assessment Delay

This option allows you to delay the start of the assessment by the number of seconds specified.


Related Information


For information on related windows:

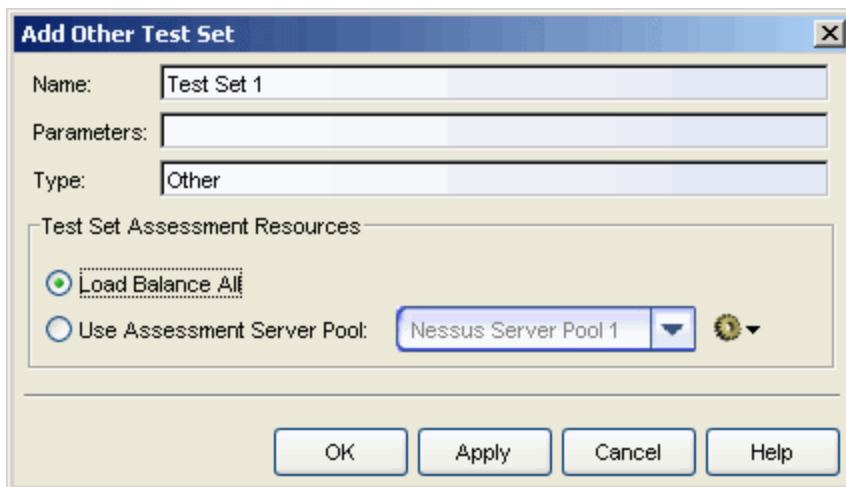
- [Edit Assessment Configuration Window](#)
- [Manage Test Sets Window](#)
- [Manage Assessment Server Pools Window](#)
- [Add/Edit Assessment Server Pool Window](#)

Add/Edit Other Test Set Window

Use this window to add a new test set for a third-party assessment agent (an assessment agent that is not supplied or supported by NAC Manager). You can also use this window to edit an existing "Other" test set. Test sets let you define what type of assessment to execute (in this case, the third-party assessment), what parameters to pass to the assessment server, and which resources to use. When you add a new test set, it becomes available for selection in the [Edit Assessment Configuration window](#).

To add an "Other" test set, click  (the configuration menu button in the Test Sets section of the [Edit Assessment Configuration window](#)) and select Add Other. You can also click the Add button in the [Manage Test Sets window](#).

To edit an "Other" test set, from the [Edit Assessment Configuration window](#), click on the test set you want to edit, then click  (the configuration menu button in the Test Sets section), and select Edit. You can also click the Edit button in the [Manage Test Sets window](#).



Name

Enter a name for the test set.

Parameters (optional)

Enter the parameters for the assessment server to use when performing the assessment. These parameters would be specific to the third-party assessment server you are using; refer to the third-party assessment server documentation for more information.

Type

Enter the type of third-party assessment server used in the test set.

Test Set Assessment Resources

Define which assessment servers you want to have perform the assessments.

- **Load Balance All** - Balance the assessment load across all of the third-party assessment servers of this type on the network.
- **Use Assessment Server Pool** - as a more granular approach, you can specify an assessment server pool. For example, if you have four third-party assessment servers of this type, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, you can specify which server pool the configuration should use.



Use the configuration menu button to:

- Add - Open the [Add Assessment Server Pool window](#) where you can add a new server pool.
 - Edit - Open the [Edit Assessment Server Pool window](#) where you can edit the selected server pool.
 - Used By - List all assessment test sets currently using the selected server pool.
 - Manage - Open the [Manage Assessment Server Pools window](#) where you can view and define the assessment server pools used in your assessment configurations.
-

Related Information

For information on related windows:

- [Edit Assessment Configuration Window](#)
- [Manage Test Sets Window](#)
- [Manage Assessment Server Pools Window](#)
- [Add/Edit Assessment Server Pool Window](#)

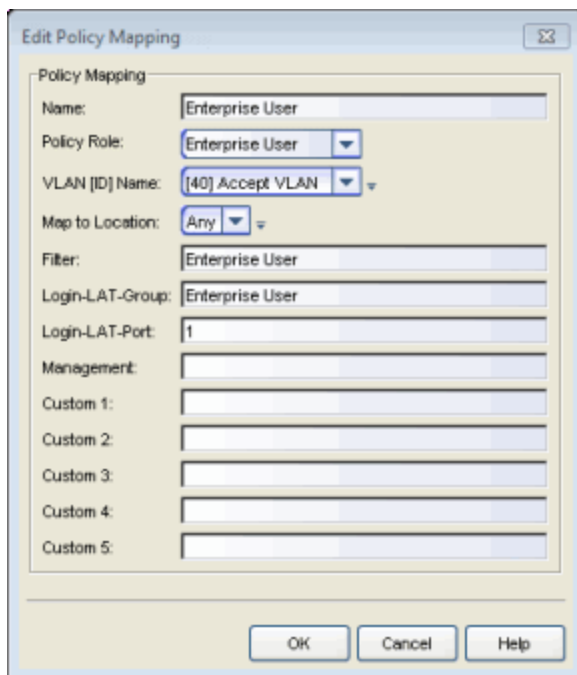
Add/Edit Policy Mapping Window

Use this window to add a new policy mapping or edit an existing policy mapping. A policy mapping specifies a policy role (created in Policy Manager) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch (as defined in the Gateway RADIUS Attributes to Send field configured in the [Edit Switch window](#)). For more information on configuring policy mappings, see [How to Set Up Access Policies and Policy Mappings](#).

Access this window by clicking the **Add** or **Edit** toolbar buttons in the [Edit Policy Mapping Configuration window](#).

The fields in this window vary depending on whether you are using a basic or advanced policy mapping configuration. For a definition of each field, see below.

Edit Policy Mapping - Advanced



The screenshot shows the 'Edit Policy Mapping' dialog box. It contains the following fields and controls:

- Name:** Text box containing 'Enterprise User'.
- Policy Role:** Drop-down menu showing 'Enterprise User'.
- VLAN [ID] Name:** Drop-down menu showing '[40] Accept VLAN'.
- Map to Location:** Drop-down menu showing 'Any'.
- Filter:** Text box containing 'Enterprise User'.
- Login-LAT-Group:** Text box containing 'Enterprise User'.
- Login-LAT-Port:** Text box containing '1'.
- Management:** Empty text box.
- Custom 1:** Empty text box.
- Custom 2:** Empty text box.
- Custom 3:** Empty text box.
- Custom 4:** Empty text box.
- Custom 5:** Empty text box.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Name

Enter a name for the policy mapping.


Policy Role

Use the drop-down menu to select a policy role, or enter a policy role in the field. The drop-down list displays any policy roles you have created and


saved in your Policy Manager database and/or all the policy roles contained in the Extreme Access Control Controller policy configuration. Roles from all your policy domains are listed; if there are duplicate names, only one is listed. The list is not case sensitive, so "Enterprise User" and "enterprise user" are considered duplicate policy names. All policy roles used in your mappings must be part of your Access Control Controller policy configuration and/or defined in Policy Manager and enforced to the EOS policy-enabled switches in your network.

NOTE: Entering a new policy role does **not** create a new role in Policy Manager.

VLAN [ID] Name

Use the drop-down list to select the appropriate VLAN associated with the policy. This list displays any VLANs that have been defined in the following legacy java applications: Console, Policy Manager, and NAC Manager. Click the configuration menu button  to the right of the field to add a VLAN to the list. VLANs that are added remain in the list only as long as they are being used in a mapping and they are **not** added to the Console database.

Map to Location

Allows you to specify a certain location for the mapping. You should first configure your locations using the Advanced Configuration view (Tools > Management and Configuration > Advanced Configurations > NAC Configurations > Rule Components > Location Group) or you can click the configuration menu button  to the right of the field to add a location group to the list. For more information on using the Location option in Policy Mappings, see the [Edit Policy Mapping Configuration Window](#) Help topic.

Filter

If your network devices require a custom Filter-Id, enter it here. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Wireless Controllers and other switches that support the Filter-Id attribute.

Login-LAT-Group

If your network devices require a Login-LAT-Group, enter it here.

Login-LAT-Port

If you have ExtremeWireless Wireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the authentication is fully authorized. A value of "1" indicates the

authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Extreme Access Control engine. This is used in conjunction with the Registration and Assessment features of NAC Manager.

Management

Enter a management attribute used to authenticate requests for administrative access to the selected switches, for example, "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator has to the switch: superuser, read/write, or read-only. Be sure to include the final colon (":") in the attribute, or the management access does not work.

Custom

If your network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session, you can define them in the five available Custom option fields.

Related Information


For information on related windows:


- [Edit Policy Mapping Configuration Window](#)

Add/Edit Risk Level Configuration Window

Use this window to add a new risk level configuration or edit the settings for an existing configuration. When you add a risk level configuration, it becomes available for selection in the [Edit Assessment Configuration window](#).

The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score. NAC Manager uses this risk level to determine whether or not the end-system is quarantined. You can create multiple risk level configurations to provide more granularity in determining end-system risk level.

To add a risk level configuration, click  (the configuration menu button next to the Risk Level Configuration field) in the [Edit Assessment Configuration window](#) and select Add. You can also click the Add button in the Manage Risk Level Configurations window.

To edit a risk level configuration, from the [Edit Assessment Configuration window](#), select the configuration you want to edit, click  (the configuration menu button next to the Risk Level Configuration field) and select Edit. You can also click the Edit button in the Manage Risk Level Configurations window.

Add Risk Level Configuration

Name:

Quarantine Risk Threshold
The quarantine risk threshold will quarantine End-Systems based upon the specified risk level
Quarantine Risk Threshold:

High Risk
End-Systems with a health result matching one or more of the following criteria will be classified into this risk level

- One or more health details with a score greater or equal to:
- 4 health details with scores greater or equal to:
- Health details with a sum of scores greater or equal to:

Medium Risk
End-Systems with a health result matching one or more of the following criteria will be classified into this risk level

- One or more health details with a score greater or equal to:
- 4 health details with scores greater or equal to:
- Health details with a sum of scores greater or equal to:

Low Risk
End-Systems will be classified as low risk if they have one or more health details with a score greater than 0 and do not fall into the high or medium risk levels.

Name

Enter a name for the configuration. You cannot change the name of the default risk level configuration.

Quarantine Risk Threshold

Select the quarantine risk threshold: high risk, medium risk, or low risk. This threshold sets the criteria that is used to determine whether or not an end-system is quarantined, based on the end-system's assessment results. The criteria for the three thresholds are defined in the sections below in this window. If you don't have any High or Medium risk level criteria defined, then all end-systems with a health result score greater than 0 would be classified as Low Risk.

High Risk

Specify the criteria used to determine whether an end-system is classified into the high risk level.

Medium Risk

Specify the criteria used to determine whether an end-system is classified into the medium risk level.

Low Risk

End-systems are classified as low risk if their health results contain one or more health details, and they do not fall into the high or medium risk levels.

Related Information

For information on related windows:

- [Edit Assessment Configuration Window](#)
- [Manage Risk Level Configurations Window](#)

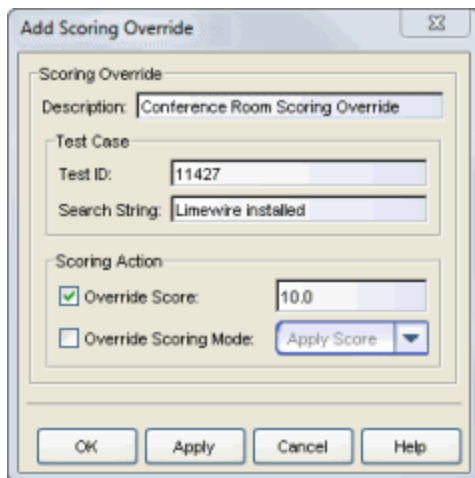
Add/Edit Scoring Override Window

Use this window to add a new scoring override or edit an existing scoring override. Scoring overrides let you create overrides to the test scoring system and assign a higher or lower score to specific assessment tests. For example, Nessus assessment checks to see if Limewire is installed on an end-system, and assigns a low risk score of "2" for that test result if it is found. Using a scoring override, you can assign a high risk score of "10" to that result instead of "2".

Scoring overrides also allow you to override the [scoring mode](#) for a specific assessment test. For example, you may set a scoring mode of "Informational Only" and then configure a scoring override so that a specific test counts towards a quarantine decision ("Apply Score"). Or, you may select a scoring mode of "Apply Score" (quarantine), and then create a scoring override that sets specific tests to be "Warning."

To add a scoring override, click the Add button in the [Add/Edit Scoring Override Configuration window](#). You can also add a scoring override by right-clicking a test case in the [Health Result Details tab](#) (in the End-Systems tab).

To edit a scoring override, select the override you want to edit in the Add/Edit Scoring Override Configuration window, and click the Edit button.



Description

A description of the individual scoring override.

Test ID

The test ID to which the scoring override is applied.

Search String

This search string is optional, and can be used in cases where the scoring override must match a test ID **and** a specific value in the health result detail description. If there is a match for the Test ID, then this search string is compared to the [health result detail description](#) to determine if the scoring override applies. You can view health result detail descriptions by double-clicking on an entry in the End-System Tab's [Health Result Details subtab](#). Use this description to create a search string for your scoring overrides. For example, the description includes operating system information such as version and product type (when available). With this information, you can add search strings for OS specific issues for any given Test Case.

NOTE: The search string is a Java Regular Expression and should be formatted accordingly. For more information, see <http://www.regular-expressions.info/java.html>.

Override Score

If you want to specify a new score for this test, select this checkbox and enter the new score that applies. Once you change the score, the original score is not retained in the health details.

Override Scoring Mode

If you want to specify a different scoring mode for this test, select this checkbox and use the drop-down menu to select a different mode.

- Apply Score - The score returned by this test is included as part of the quarantine decision.
- Informational - The score returned by this test is reported, but it is not applied toward a quarantine decision.
- Warning - The score returned by this test are only be used to provide end user assessment warnings via the Notification portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) has expired.

NOTE: You cannot override the scoring mode of agent-based tests.

Related Information

For information on related windows:

- [Edit Assessment Configuration Window](#)
- [Manage Scoring Override Configurations Window](#)

- [Add/Edit Scoring Override Configurations Window](#)


Add/Edit Scoring Override Configuration Window

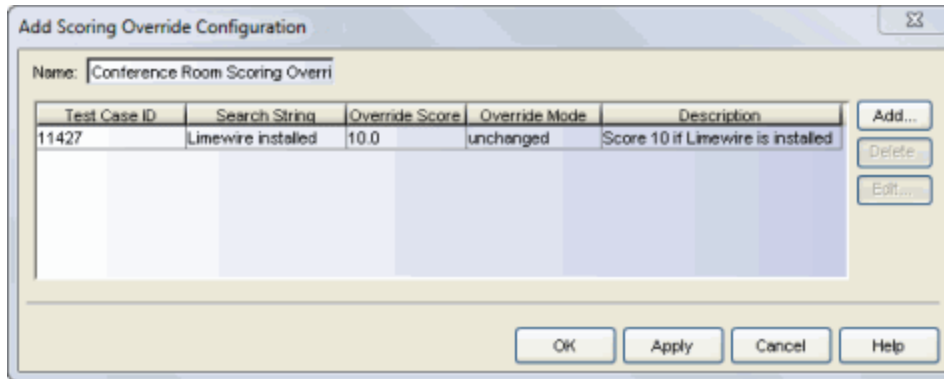
Use this window to add a new scoring override configuration and define the individual scoring overrides that make up the configuration. You can also use this window to edit an existing configuration. When you add a scoring override configuration, it becomes available for selection in the [Edit Assessment Configuration window](#).

Scoring overrides let you create overrides to the test scoring system and assign a higher or lower score to specific assessment tests. For example, Nessus assessment checks to see if Limewire is installed on an end-system, and assigns a low risk score of "2" for that test result if it is found. Using a scoring override, you can assign a high risk score of "10" to that result instead of "2".

Scoring overrides also allow you to override the [scoring mode](#) for specific assessment tests. For example, you may set a scoring mode of "Informational" and then configure a scoring override so that a specific test counts towards a quarantine decision ("Apply Score"). Or, you may select a scoring mode of "Apply Score" (quarantine), and then create a scoring override that sets specific tests to be "Warning."

To add a scoring override configuration, click  (the configuration menu button next to the Scoring Override Configuration field) in the [Edit Assessment Configuration window](#) and select Add. You can also click the Add button in the [Manage Scoring Override Configurations window](#).

To edit a scoring override configuration, from the [Edit Assessment Configuration window](#), select the configuration you want to edit, click  (the configuration menu button next to the Scoring Override Configuration field) and select Edit. You can also click the Edit button in the [Manage Scoring Override Configurations window](#).



Name

Enter a name for the configuration. You cannot change the name of the default scoring override configuration.

Test ID

The test ID to which the scoring override applies.

Search String

The search string is optional, and is used in cases where the scoring override must match a test ID **and** a specific value in the health result detail description. If there is a match for the Test ID, then this search string is compared to the [health result detail description](#) to determine if the scoring override applies.

Override Score

The test score applied for this specific test, or "unchanged" if the override doesn't change the score.

Override Mode

The scoring mode applied for this specific test.

- Unchanged - Use the [scoring mode](#) assigned for the test set where the scoring override is used.
- Apply Score - The score returned by this test is included as part of the quarantine decision.
- Informational - The score returned by this test is reported, but it is not applied toward a quarantine decision.
- Warning - The score returned by this test is only be used to provide end user assessment warnings via the Notification Portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) has expired.

Description

A description of the individual scoring override.

Add Button

Opens the [Add Scoring Override window](#) where you can define a new scoring override for the configuration.

Delete Button

Deletes the selected scoring override(s).

Edit Button

Opens the [Edit Scoring Override window](#) where you can edit the selected scoring override.

Related Information

For information on related windows:

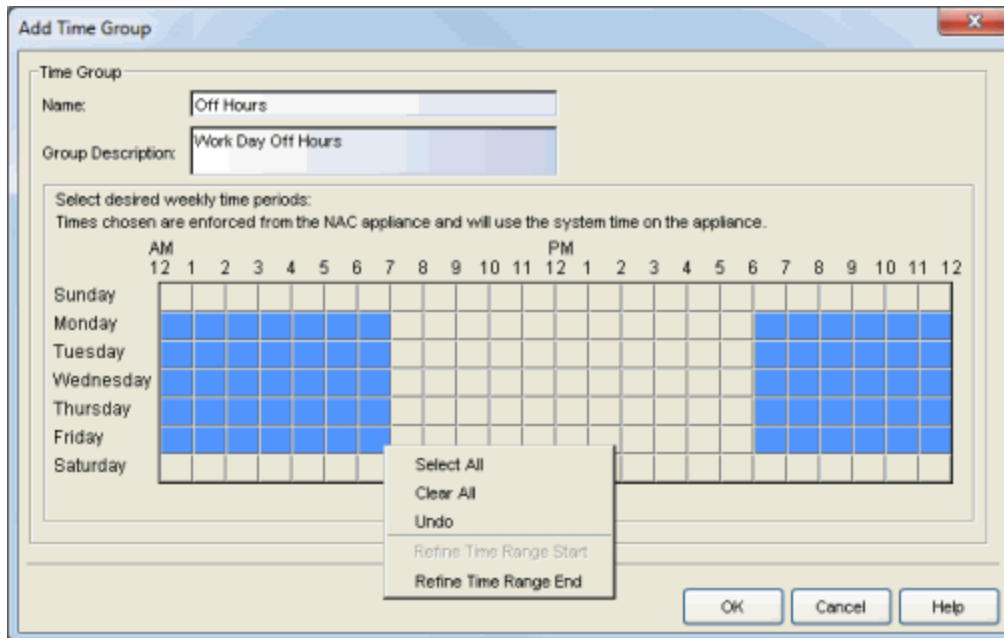
- [Edit Assessment Configuration Window](#)
- [Manage Scoring Override Configurations Window](#)

Add/Edit Time Group Window

Use this window to add a new time group or edit an existing time group. Time groups are rule components that allow you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, in an enterprise environment, an employee could be assigned different access privileges based on whether they log in during traditional work hours or after hours.

You can access the Add/Edit Time Group window from the [Manage Rule Groups window](#) or from the time group field in the [Create Rule window](#).

NOTE: Changes to rule components do not require an enforce. Changes automatically synchronize with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new time group. You cannot edit the name of an existing group. If you want to change the name, you must create a new time group with a new name and then delete the old time group.

Group Description

Enter a description of the time group. This description displays in the [Manage Rule Groups window](#).

Calendar

Use the calendar to select the desired weekly time periods. Click to select a specific day and time, or click and drag to quickly select a time sequence or series of days. For example, you can click on Monday at 8 AM and drag down to select that hour for Monday through Friday. The click and drag feature makes it easy to select an entire week or chunk of time with just one action. Right click on a selected square to access menu options that let you select all or clear all squares, and undo the last action. If a square is the first or last in a series, right click to access the Refine Time Range Start/End options that let you specify hourly increments for the start and end times.

Related Information

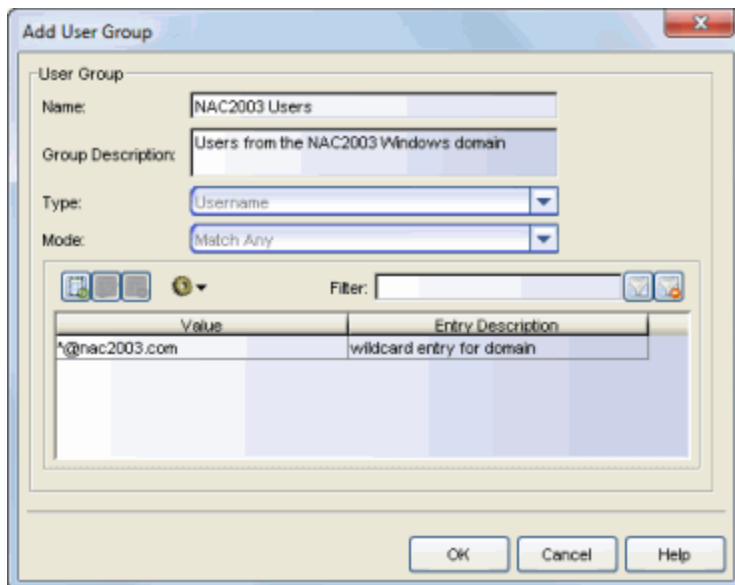
For information on related windows:

- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

Add/Edit User Group Window

Use this window to add a new user group or edit an existing user group. User groups are rule components that allow you to group together end users having similar network access requirements or restrictions. You can access the Add/Edit User Group window from the [Manage Rule Groups window](#) or from the user group field in the [Create Rule window](#).

NOTE: Changes to rule components do not require an enforce. Changes automatically synchronize with the engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new user group. You cannot edit the name of a group.

Group Description

Enter a description of the user group.

Type

Specify the criteria on which the user group is based:

- Username - a list of usernames which can be based on an exact match or a wild card.
- LDAP User Group - a list imported from an LDAP Server, organized by Organization Unit (OU), or a custom attribute lookup for any user

or MAC address if they match a AAA configuration entry that assigns the request a valid LDAP Configuration.

- RADIUS User Group - a list of attributes returned by the RADIUS server.

Mode

For LDAP and RADIUS user groups, the Mode option lets you select whether to match any or match all of the LDAP or RADIUS User Group entries (attribute names) listed below.

For LDAP User Groups, you can also select "Exists", since the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The "Exists" mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the Extreme Access Control engine for re-verification.



Use these buttons to add, edit, or delete entries in the group. The entries are displayed in the table below.

TIP: You can also copy and edit entries by right-clicking on an entry and selecting Copy. This allows you to quickly add group entries by copying a single entry in the table and editing the username value.



Use the configuration menu button to either open a window where you can select a file for importing usernames (if you are creating username entries) or open a window where you can configure an LDAP OU import (if you are creating an LDAP user group).

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Related Information

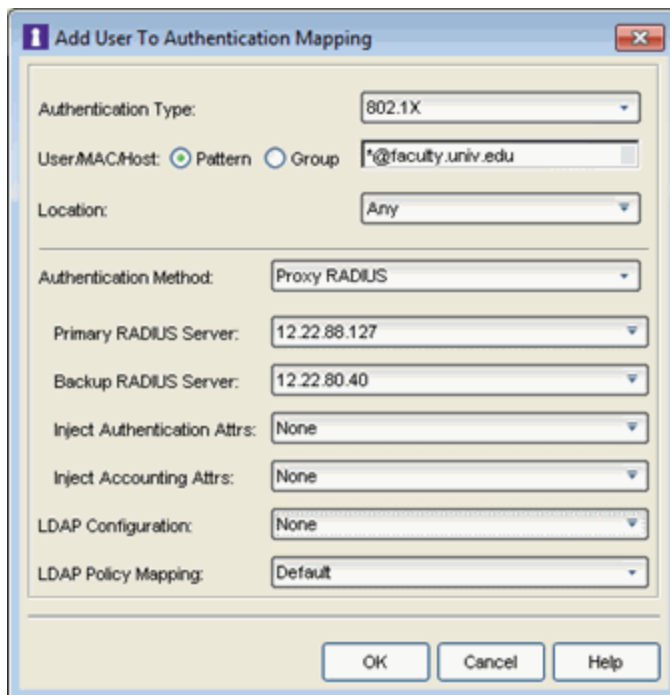
For information on related windows:

- [Create Rule Window](#)
- [Manage Rule Groups Window](#)

Add/Edit User to Authentication Mapping Window

This window lets you add or edit the user to authentication mappings that define your Advanced AAA configurations. You can access this window from the Add or Edit buttons in the [AAA Configuration window](#).

NOTE: You can also access AAA Configurations in the Advanced Configuration View, by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the AAA Configurations folder. Your configurations are listed below the folder.



Authentication Type

Select the authentication type that the end-system must match for this mapping. Note that individual types of 802.1X authentication are not available for selection because at this point in the authentication process, the fully qualified 802.1X authentication type cannot be determined. Select "Any" if you don't want to require an authentication match. Select **802.1X (TTLS-INNER-TUNNEL)** or **802.1X (PEAP-INNER-TUNNEL)** to authenticate via another RADIUS server using an inner tunnel to protect the authentication request.

The Management Login authentication type allows you to set up a mapping

specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet. This allows you to send management requests to a different authentication server than network access requests go to. This authentication type can be used to authenticate users locally, or proxy them to specific RADIUS or LDAP servers. Make sure that the Management Login mapping is listed above the "Any" mapping in the list of mappings in your Advanced AAA Configuration. In addition, you must set the Auth. Access Type to either "Management Access" or "Any Access" in the Add/Edit Switches window for this authentication type.

User/MAC/Host

Select the **Pattern** radio button and enter the username, MAC address, or hostname that the end-system must match for this mapping. Or, select the **Group** radio button and select a user group or end-system group from the drop-down list. If you enter a MAC address, you can use a colon (:) or a dash (-) as an address delimiter, but not a period (.).

Location

Select the [location group](#) that the end-system must match for this mapping, or select "Any" if you don't want to require a location match. You can also add a new location group or edit an existing one.

Authentication Method

Select the authentication method that the end-system must match for this mapping: Proxy RADIUS, LDAP Authentication, or Local Authentication.

Primary RADIUS Server - Use the drop-down menu to select the primary RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Backup RADIUS Server - Use the drop-down menu to select the backup RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Inject Authentication Attrs - Use the drop-down menu to select attributes to inject when proxying authentication requests to the back-end RADIUS servers. Select **Edit RADIUS Attribute Settings** within the drop-down menu to open the [RADIUS Attribute Settings window](#), which allows you to add or edit an attribute group.

Inject Accounting Attrs - Use the drop-down menu to select attributes to inject when proxying accounting requests to the back-end RADIUS servers. Select **Edit RADIUS Attribute Settings** within the drop-down menu to open

the [RADIUS Attribute Settings window](#), which allows you to add or edit an attribute group.

LDAP Authentication - If you select LDAP Authentication, specify the LDAP configuration for this mapping to use.

Local Authentication - If desired, select the option to configure a password for all authentications that match the mapping. This option could be used with MAC authentication where the password is not the MAC address. For example, you may have MAC (PAP) authentication configured for all your switches, with the exception of MAC (MsCHAP) authentication configured for a wireless controller. For the wireless controller, you would add a new AAA mapping with the authentication type set to MAC (MsCHAP), the location set to the wireless controller location group, and the authentication method set to Local Authentication with the password for all authentications set to the static password configured on the wireless controller.

LDAP Configuration

Use the drop-down list to select the LDAP configuration for the LDAP servers on your network that you want to use for this mapping. You can also add or edit an LDAP configuration, or manage your LDAP configurations. You must specify an LDAP configuration if you have selected LDAP Authentication as your authentication method. However, you might also specify an LDAP configuration if you use Proxy RADIUS to a Microsoft NPS server that is running on a domain controller. The domain controller is also an LDAP server that can do RADIUS requests and LDAP requests for users on that server.

LDAP Policy Mapping

Use the drop-down list to select the LDAP Policy Mapping for this mapping. You can also [add or edit an LDAP Policy Mapping](#) or open the [Manage LDAP to Policy Mappings window](#). If you have selected an LDAP configuration, this option allows you to use a different LDAP policy mapping. This is useful if the LDAP configuration uses user attribute values that overlap with another LDAP configuration. For example, in the case of multiple companies where company A's Sales department uses one policy, but company B's Sales department uses a different policy.

Related Information

For information on related windows:

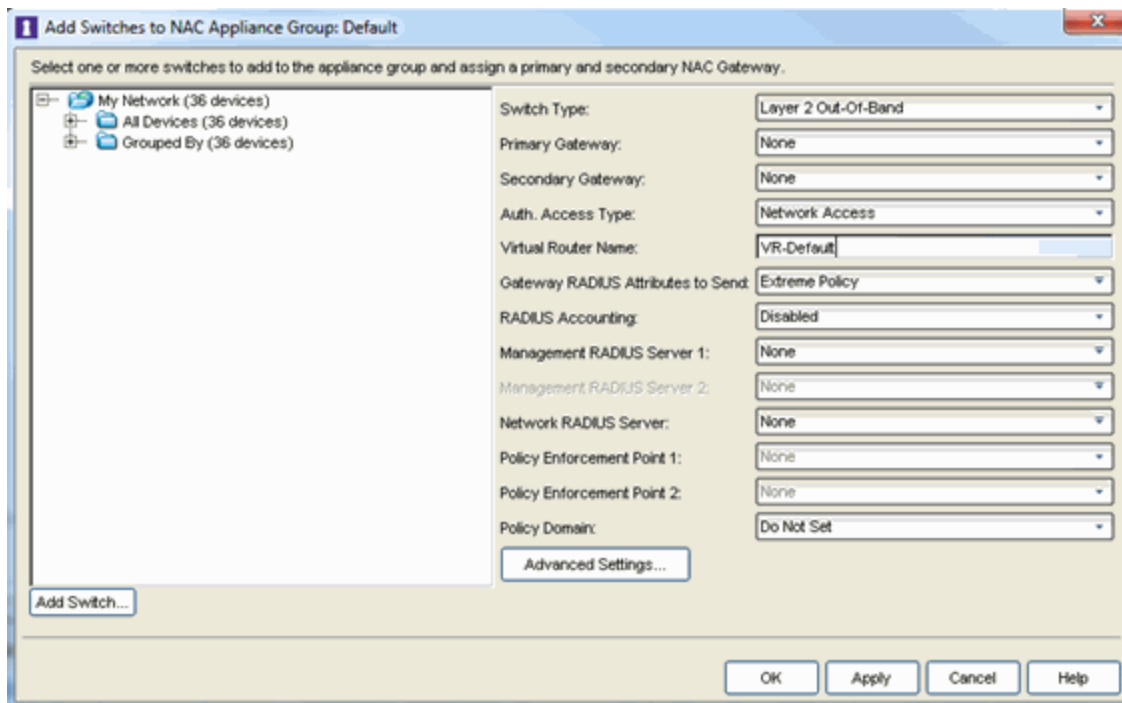
- [RADIUS Attribute Settings Window](#)
- [Manage LDAP to Policy Mappings Window](#)

Add Switches to NAC Appliance Group Window

Use this window to select switches to add to a gateway engine or engine group. The window allows you to select one or more switches from the Console device tree, and set the primary and secondary Extreme Access Control (Access Control) (formerly NAC) Gateways for the switches. It also lets you set other parameters including the authentication access type for the switches and the RADIUS attributes to send.

NOTE: If desired, you can set only the primary Access Control Gateway for the switches; NAC Manager does not require the secondary Access Control Gateway to be set. If only the primary Access Control Gateway is set, then by default that gateway uses its primary proxy RADIUS server as a secondary direct RADIUS server to the switch. This allows for redundancy without the requirement for a secondary Access Control Gateway. In this scenario, if contact with the Access Control Gateway fails, authentication traffic would bypass the Access Control gateway, but normal authentication continues in the network, and still provides some security. You can turn off this default behavior via a checkbox in the Switch Configuration section on the Credentials tab in the [Appliance Settings window](#).

You can access this window by selecting an engine or engine group and clicking the **Add Switch** button in the right-panel [Switches tab](#).



Console Device Tree

This area displays the Console device tree. Expand the tree and select the switches you want to add to the engine or engine group.

Add Switch

Opens the Add Device window where you can add a device to the Extreme Management Center (Management Center) database. The device displays in the My Network folder in the Console device tree.

Switch Type

Use the drop-down menu to select the type of switch you are adding:

- **Layer 2 Out-Of-Band** - A switch that performs authentication on layer 2 traffic via RADIUS to an out-of-band Access Control gateway.
- **Layer 2 Out-Of-Band Data Center** - A switch within a data center where virtualization and mobility are a factor. If an end-system changes location but does not move to a different Access Control engine, NAC Manager removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in NAC Manager, because only one authenticated session is allowed per end-system within NAC Manager.
- **Layer 2 RADIUS Only** - In this mode, NAC Manager does not require any information from the switch other than the end-system MAC address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the [Advanced Switch Settings window](#). IP resolution and reauthentication may not work in this mode.
- **VPN** - A VPN concentrator being used in a [NAC VPN deployment](#). In this case, you should specify one or more Policy Enforcement Points below. If you do not specify a Policy Enforcement Point, then NAC Manager is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down list to select the primary Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

Secondary Gateway

Use the drop-down list to select the secondary Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

NOTE: To configure additional redundant Access Control Gateways per switch (up to four), use the Display Counts option in the NAC [Display options panel](#) (Tools > (Tools > Options)).

Auth. Access Type

Use the drop-down list to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: For ExtremeXOS devices only. NAC Manager uses CLI access to perform configuration operations on ExtremeXOS devices.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. Make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator NAC Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that NAC Manager authenticates management login attempts against.
 - Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.
-
- **Any Access** - the switch can authenticate users originating from any access type.
 - **Management Access** - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
 - **Network Access** - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence is

displayed to provide the most accurate access control information for the user. The NAC Manager authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- **Monitoring - RADIUS Accounting** - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. NAC Manager learns about these session via RADIUS accounting. This allows NAC Manager to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence is displayed to provide the most accurate access control information for the user. The NAC Manager authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- **Manual RADIUS Configuration** - NAC Manager does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using Policy Manager or CLI.

Virtual Router Name

Enter the name of the Virtual Router. The default value for this field is **VR-Default**.

WARNING: For ExtremeXOS devices only. If Management Center has not detected and populated this field, enter the **Virtual Router Name** carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

Gateway RADIUS Attributes to Send

Use the drop-down menu to select the RADIUS attributes included as part of the RADIUS response from the Access Control engine to the switch. You can also select Edit RADIUS Attribute Settings from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes. If you define a new custom attribute, be sure to modify your policy mappings in the [Advanced Edit Policy Mapping view](#).

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time

connection status in NAC Manager. For more information, see [How to Enable RADIUS Accounting](#).

Management RADIUS Server 1 and 2

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in NAC Manager, or select **New** or **Manage** RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in NAC Manager, or select **New** or **Manage** RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device that you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then NAC Manager is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

Use this option to assign the switch to a Policy Manager domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

Advanced Settings

Click the **Advanced Settings** button to open the [Advanced Switch Settings window](#).

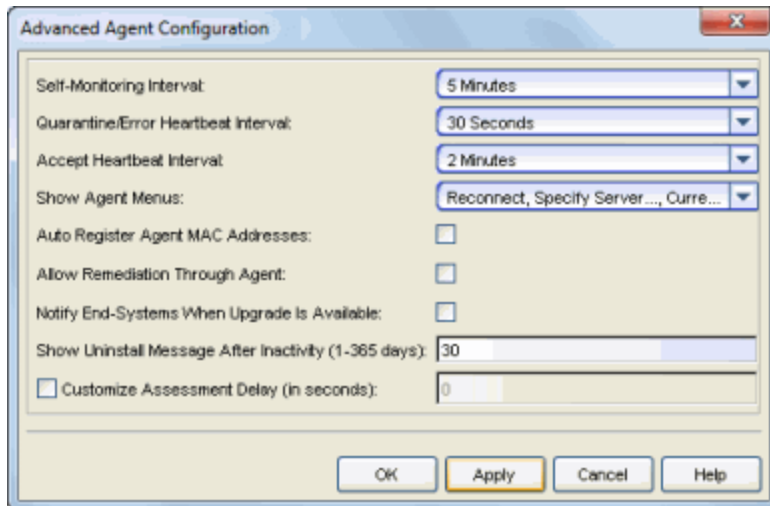
Related Information

For information on related windows:

- [Create NAC Appliance Window](#)
- [Edit Switches in Appliance Group Window](#)

Advanced Agent Configuration Window

Use this window to configure advanced options for an agent-based test set. Access these advanced options by clicking the **Advanced** button in the [Add/Edit Agent-Based Test Set window](#).



Self-Monitoring Interval

The self-monitoring interval specifies how frequently the agent performs mandatory tests.

Quarantine/Error Heartbeat Interval

The agent heartbeat is sent from the agent to the assessment server as a way for the agent to check with the assessment server for the next action or test. When end-systems are in a quarantine or error state, the heartbeat interval should be frequent enough to allow the remediation process to happen quickly. The default setting is 30 seconds.

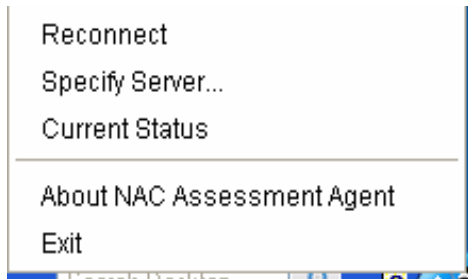
Accept Heartbeat Interval

The agent heartbeat is sent from the agent to the assessment server as a way for the agent to check with the assessment server if the scan interval has expired and it is time for the next action or test. When end-systems are in an accepted state, the heartbeat interval can be less frequent as a way to decrease network traffic. The default setting is 2 minutes.

Show Agent Menus

If the end user right-clicks on the agent icon, the agent system tray menu is displayed. Use this option to specify which menu options are included on

the menu.



The following menu options can be hidden from the end user, if desired:

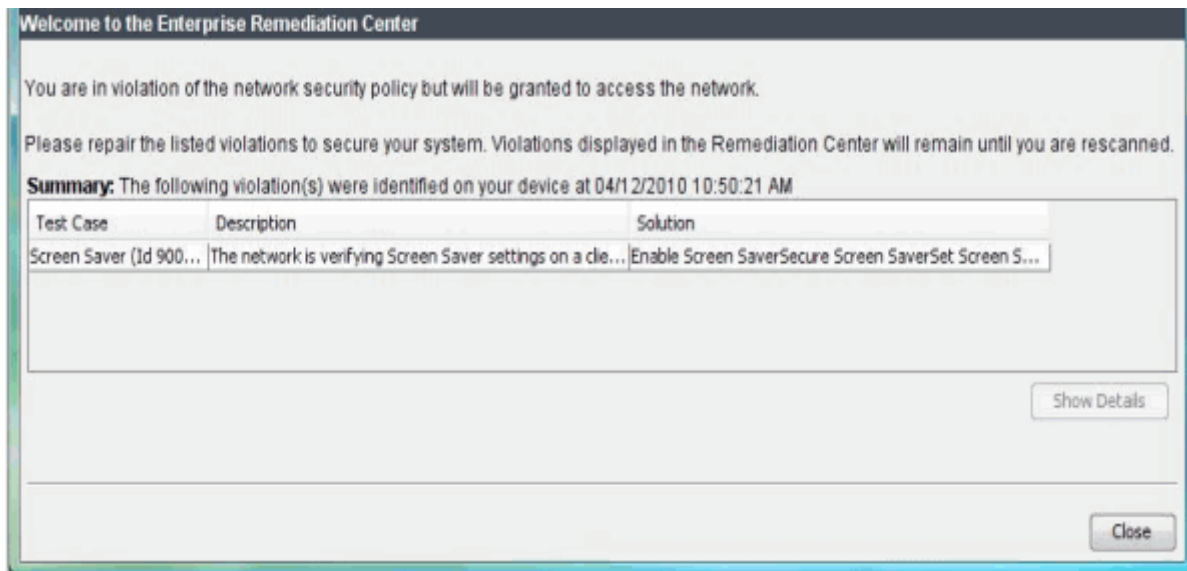
- Reconnect - Causes the agent to disconnect from its current assessment server and attempt to reconnect to the default assessment server.
- Specify Server - Opens a window where the end user can change the default assessment server to which the agent attempts to connect.
- Current Status - Displays a popup showing the end-system's current assessment status.

Auto Register Agent MAC Addresses

If an end-system is running the agent and registers to the network, NAC Manager automatically registers all of the end-system's other interfaces. For example, if an end user registers on the network using their Ethernet network card, but they also have a wireless card, NAC Manager automatically registers the wireless card's MAC address. That way, when the end user uses their wireless card, they won't get prompted to register that MAC address as well.

Allow Remediation Through Agent

If this option is enabled, when the end user receives a Quarantine or Warning notification message and clicks the "Start Remediation" link, the remediation information is displayed in an agent window instead of the captive portal web browser. This allows remediation to take place with less hits to the captive portal remediation web server. However, if the end user opens a browser window, they still connect to the captive portal remediation web page. A sample agent remediation window for a Warning is shown below:

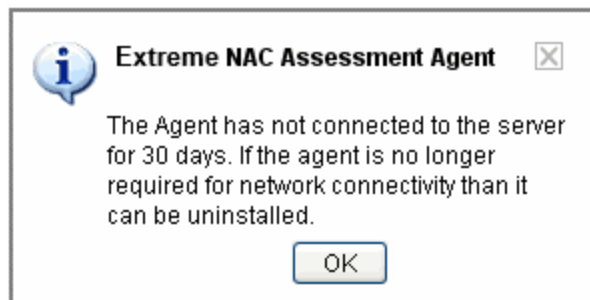


Notify End-Systems When Upgrade is Available

Enabling this option displays a popup window to the end user when they are granted access to the network (Accept state) if their agent version is not the latest version. When the user clicks on the popup, it redirects them to an agent download web page on the portal that provides links to their agent upgrade options.

Show Uninstall Message After Inactivity (1-365 Days)

The following message displays to end users if the agent has not connected to an assessment server in the number of days specified. When the end user clicks **OK**, the agent application exits. The end user needs to manually uninstall the agent application, if desired. If the end user restarts the agent application, they have five minutes to connect to an assessment server or the message re-displays.



Customize Assessment Delay

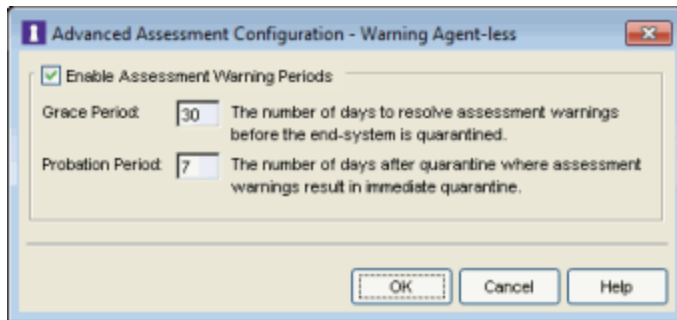
This option allows you to delay the start of the assessment by the number of seconds specified. This is useful with agent-based assessment as a way to provide additional time for an end-system to start up and allow the agent to connect to the assessment server. By specifying a delay time, the end-system could avoid being quarantined because the agent wasn't connected yet when the assessment began. When the checkbox is not selected, it defaults to either the Accept or Quarantine interval, whichever is higher. The delay is ignored if the agent is connected.

Related Information

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)
- [Edit Assessment Configuration Window](#)
- [Manage Test Sets Window](#)

Advanced Assessment Configuration Window

Use this window to enable and specify warning periods used with assessment warnings. Access these options by clicking the **Advanced** button in the [Edit Assessment Configuration window](#).



Grace Period

Specify the number of days the end user has to resolve the warning issues before the end-system is quarantined.

Probation Period

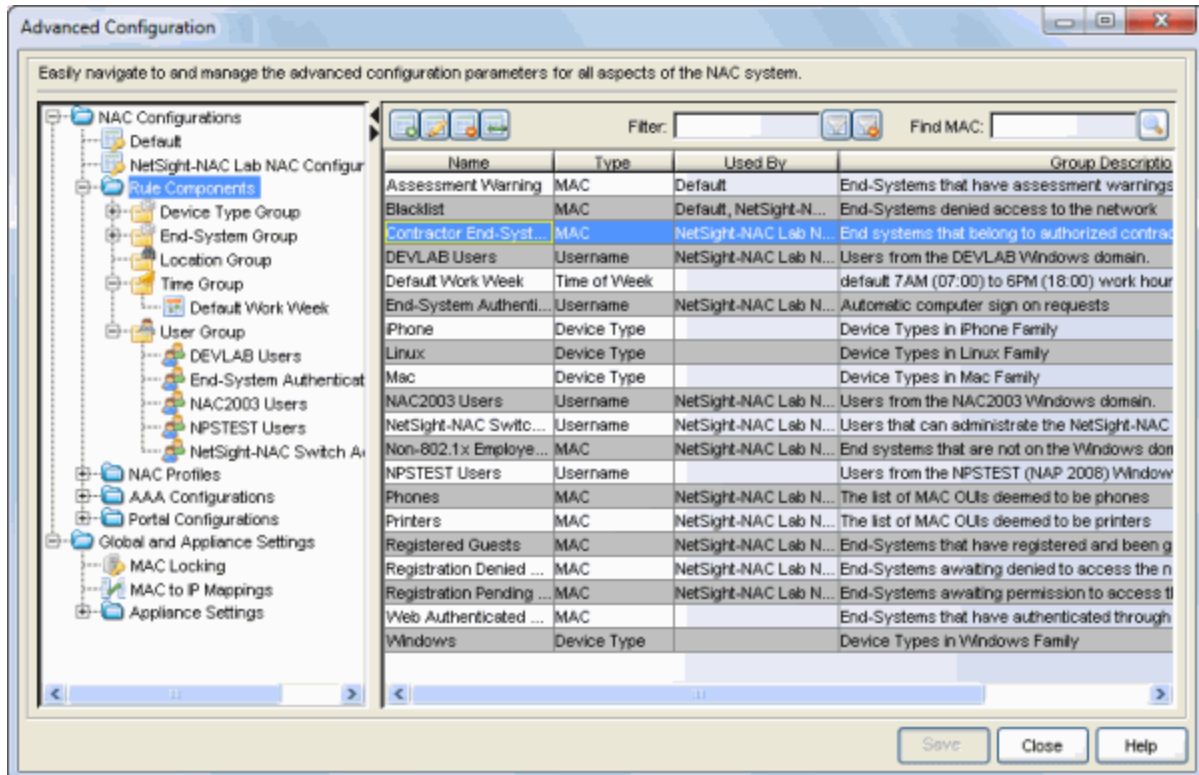
The number of days after an end user is quarantined that additional warnings result in immediate quarantine. This allows administrators to block repeat offenders by limiting their access to the network. Once the probation period passes, the end user receives assessment warnings again. Set the probation period to 0 to have no probation period.

Related Information

- [Edit Assessment Configuration Window](#)

Advanced Configuration Window

The Advanced Configuration window provides a central location to view and manage the configuration parameters for all aspects of your NAC system. You can access this window by selecting **Tools > Management and Configuration > Advanced Configurations** from the NAC Manager menu bar.



The left-panel tree provides access to the following NAC system components.

NAC Configurations

Each engine group uses one NAC configuration that contains an ordered list of rules used to determine which NAC profile is assigned to the end-systems connecting to the engines in that group. NAC configurations include the following components:

Rule Components

Rule components are used to define the criteria for the rules used in your NAC configuration.

NAC Profiles

NAC profiles specify the authorization and assessment requirements for the end-systems connecting to the network. The profile also specifies the security policies that will be applied to end-systems for network authorization, depending on authentication and assessment results.

AAA Configurations

AAA configurations define the RADIUS and LDAP configurations, and Local Password Repository that provide the authentication and authorization services to your Extreme Access Control engines.

Portal Configurations

If your network is implementing [Registration](#) or [Assisted Remediation](#), use the Portal Configuration to define the branding and behavior of the website used by the end user during the registration or remediation process.

Global and Appliance Settings

This section of the window allows you to configure the following NAC components:

MAC Locking

MAC locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch.

MAC to IP Mappings

MAC to IP mappings lets you create a table of MAC to IP address mappings for devices with statically assigned IP addresses. The MAC to IP mappings are sent to the Extreme Access Control (Access Control) engines in the configuration enforce. The Access Control engines uses this table to resolve IP addresses.

Appliance Settings

This folder lets you configure settings for IP, MAC, and Hostname/Username resolution. You can customize reauthentication behavior, OS detection using DHCP fingerprinting, and other settings for the Access Control engine.

AAA Configurations Panel

The AAA Configurations panel in the Advanced Configuration window provides a list of your AAA configurations and buttons to add, edit, or delete configurations. AAA configurations define the RADIUS and LDAP configurations that provide the authentication and authorization services to your Extreme Access Control engines.

You can access the Advanced Configurations window, by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the AAA Configurations folder. Your configurations are listed below the folder.

Easily navigate to and manage the advanced configuration parameters for all aspects of the NAC system.

Name	Type	Local MAC Authentication	Local Password Repository
Default	Basic	MAC (PAP)	Default
NetSight-NAC Lab A...	Advanced	MAC (PAP)	Default



Use these buttons to add, edit, or delete the AAA configurations. Click **Add** to add a new configuration to the table. Then select the configuration in the table and click **Edit** to open the Edit AAA Configurations window. Use the **Delete** button to remove any selected configuration(s).

Name

The name of the AAA Configuration.

Type

Whether the configuration is a [Basic configuration](#) or an [Advanced configuration](#).

Local MAC Authentication

Indicates whether MAC authentication requests are handled locally by the Extreme Access Control engine and the type of MAC authentication used.

Local Password Repository

The local password repository specified for this AAA configuration. NAC Manager supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.

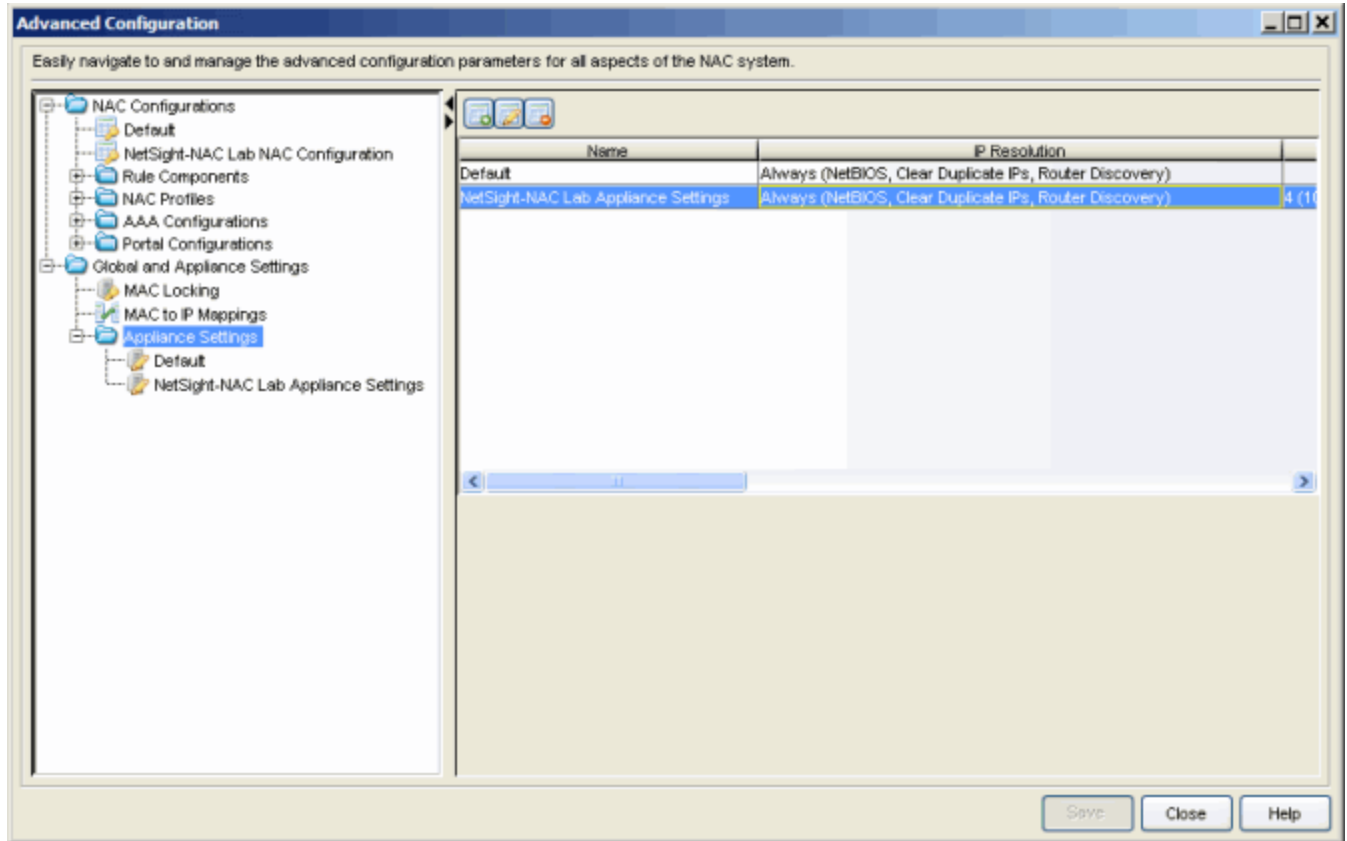
Related Information

- [AAA Configurations](#)

Appliance Settings Panel

The Appliance Settings panel in the Advanced Configuration window provides a list of your engine settings and buttons to add, edit, or delete settings. Engine settings provide advanced configuration options for Extreme Access Control engines. NAC Manager comes with a default engine settings configuration. If desired, you can edit these default settings or you can define your own settings to use for your Access Control engines. Any changes made in this panel are written immediately to the NAC Manager database.

To access the Appliance Settings panel, select **Tools > Management and Configuration > Advanced Configuration** from the menu bar to open the Advanced Configuration window. In the left-panel tree, expand the Global and Appliance Settings folder. If you expand the Appliance Settings folder you see the Default settings plus any other settings you have defined listed under the folder.



Use these buttons to add, edit, or delete the engine settings. Click **Add** to add a new engine settings to the table. To edit an engine settings, select the entry in the table and click Edit to open the [Edit Appliance Settings Window](#). Use the **Delete** button to remove any selected engine settings.

Name

The name of the engine settings configuration.

IP Resolution

The [IP resolution parameters](#) configured for your network engines.

IP Subnets

The [IP subnets](#) configured for your network engines.

MAC Resolution

The [MAC resolution parameters](#) configured for your network engines.

Hostname Resolution

The [hostname resolution parameters](#) configured for your network engines.

Username Resolution

The [username resolution parameters](#) configured for your network engines.

OS Name Resolution

The [operating system detection parameters](#) configured for your network engines.

Related Information

For information on related windows:

- [New/Edit Appliance Settings Window](#)

Assessment Panel

The Assessment panel in the Advanced Configuration window lets you view and edit all the assessment configurations that have been defined in NAC Manager. You can also see where each configuration is being used by a Extreme Access Control profile and add a new assessment configuration, if desired.

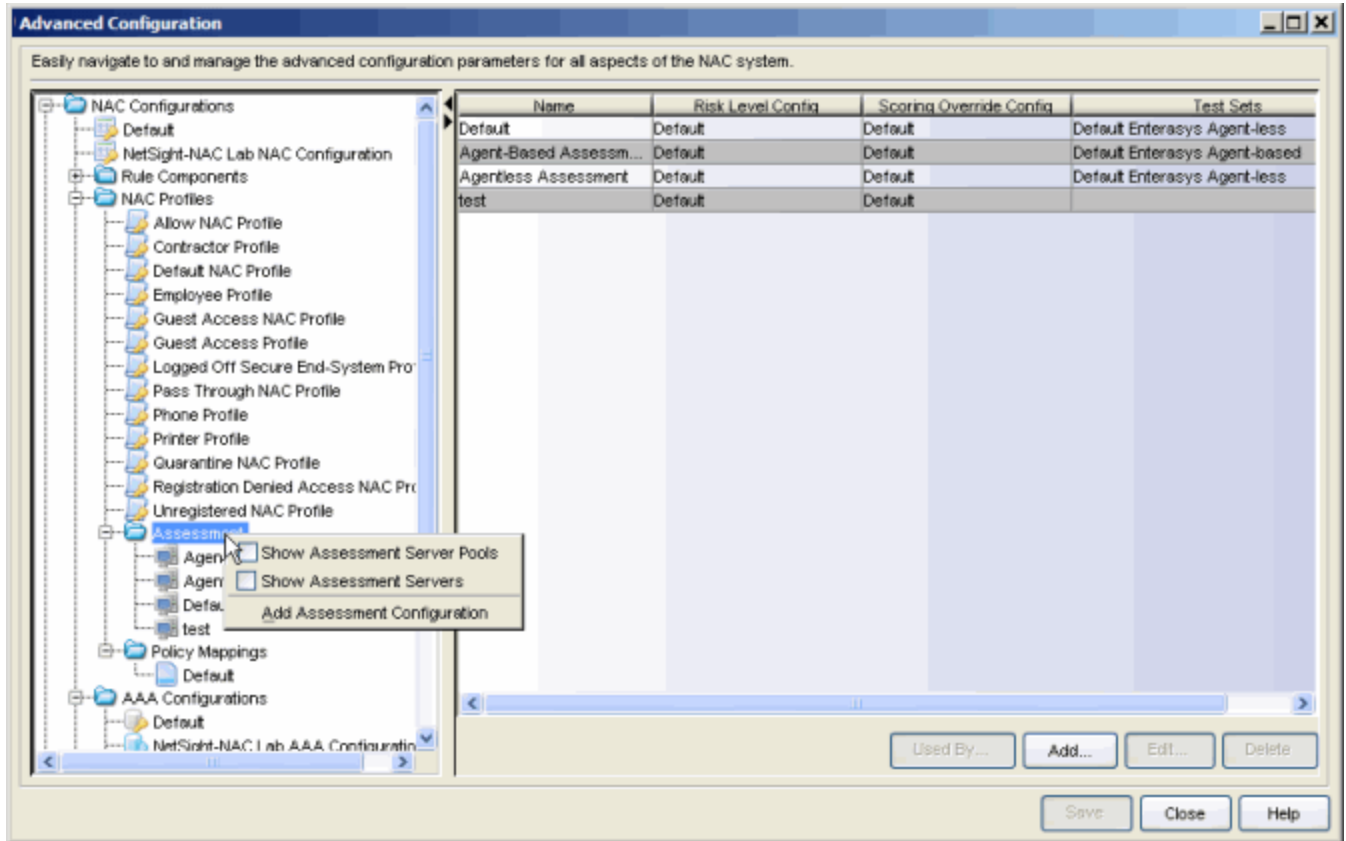
Assessment configurations define three basic categories of information:

- What assessment tests to run (determined by the selected test sets).
- What resources to use to run the tests (determined by the selected Assessment Resources).
- How to interpret the test results (determined by the selected Risk Level and Scoring Override configurations).

Once you have defined your assessment configurations, they are available for selection when creating your NAC (Extreme Access Control) Profiles.

To access the Assessment panel, select **Tools > Management and Configuration > Advanced Configuration** from the menu bar to open the Advanced Configuration window. In the left-panel tree, expand the NAC Profiles folder and select the Assessment folder. If you expand the Assessment folder you will see the Default assessment configuration plus any other configurations you have defined listed under the folder.

You can also display lists of your assessment servers and your assessment server pools by right-clicking on the Assessment folder and selecting the appropriate options (as shown below).



Name

The name of the assessment configuration.

Risk Level Configuration

The risk level configuration specified for this assessment configuration. The risk level configuration determines what risk level will be assigned to an end-system (high, medium, or low) based on the end-system's health result details score. It is specified when you create the assessment configuration.

Scoring Override Configuration

The scoring override configuration specified for this assessment configuration. The scoring override configuration lets you override the default scoring assigned by the assessment server to a particular assessment test ID. It is specified when you create the assessment configuration.

Test Sets

The test sets selected for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what

parameters to pass to the assessment server, and what assessment server resources to use.

Used By Button

Displays a list of assessment configurations in use by NAC (Extreme Access Control) profiles.

Add Button

Opens the [Edit Assessment Configurations window](#) where you can add a new assessment configuration.

Edit Button

Opens the [Edit Assessment Configurations window](#) where you can edit the selected assessment configuration.

Delete Button

Deletes the selected assessment configuration.

Related Information

For information on related windows:

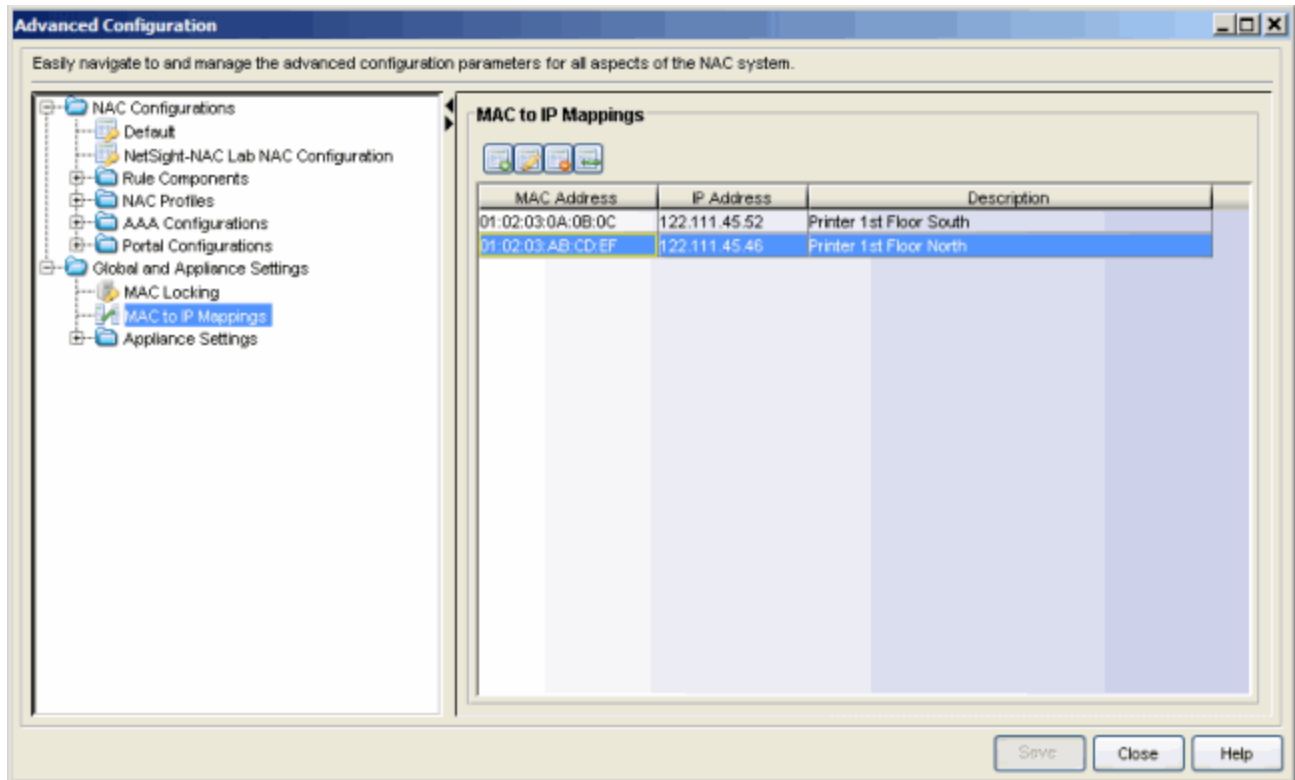
- [Manage Assessment Servers Window](#)
- [Manage Assessment Server Pools Window](#)
- [Manage Test Sets Window](#)

MAC to IP Mappings Panel

The MAC to IP Mappings panel in the Advanced Configuration window lets you add a table of MAC to IP address mappings for devices with statically assigned IP addresses. You can also [import](#) a file of MAC to IP mappings to the list. Any changes made in this panel are written immediately to the NAC Manager database.

The MAC to IP mappings are sent to the NAC appliances in the configuration enforce. The NAC appliances will use this table to resolve IP addresses.

To access this panel, open the Advanced Configuration window (**Tools > Management and Configuration > Advanced Configurations** from the menu bar) and expand the Global and Appliance Settings folder in the left-panel tree.



MAC Address

The MAC address mapped to the static IP address.

IP Address

The statically assigned IP address.

Description

A description of the mapping; for example, a description of the device with the statically assigned IP address.

Add Button

Opens the Add MAC to IP Mapping window where you can add a new mapping and description to the table.

Edit Button

Opens the Edit MAC to IP Mapping window where you can edit the IP address and description for a mapping.

Delete Button

Deletes the selected MAC to IP mapping.

Import Button

Use the **Import** button to import a file of MAC to IP mappings to the list. In the file, MAC to IP mappings must be listed in CSV format, with one mapping per line. For example:

02.0A.40.0B.01.44, 122.111.45.66, description of mapping

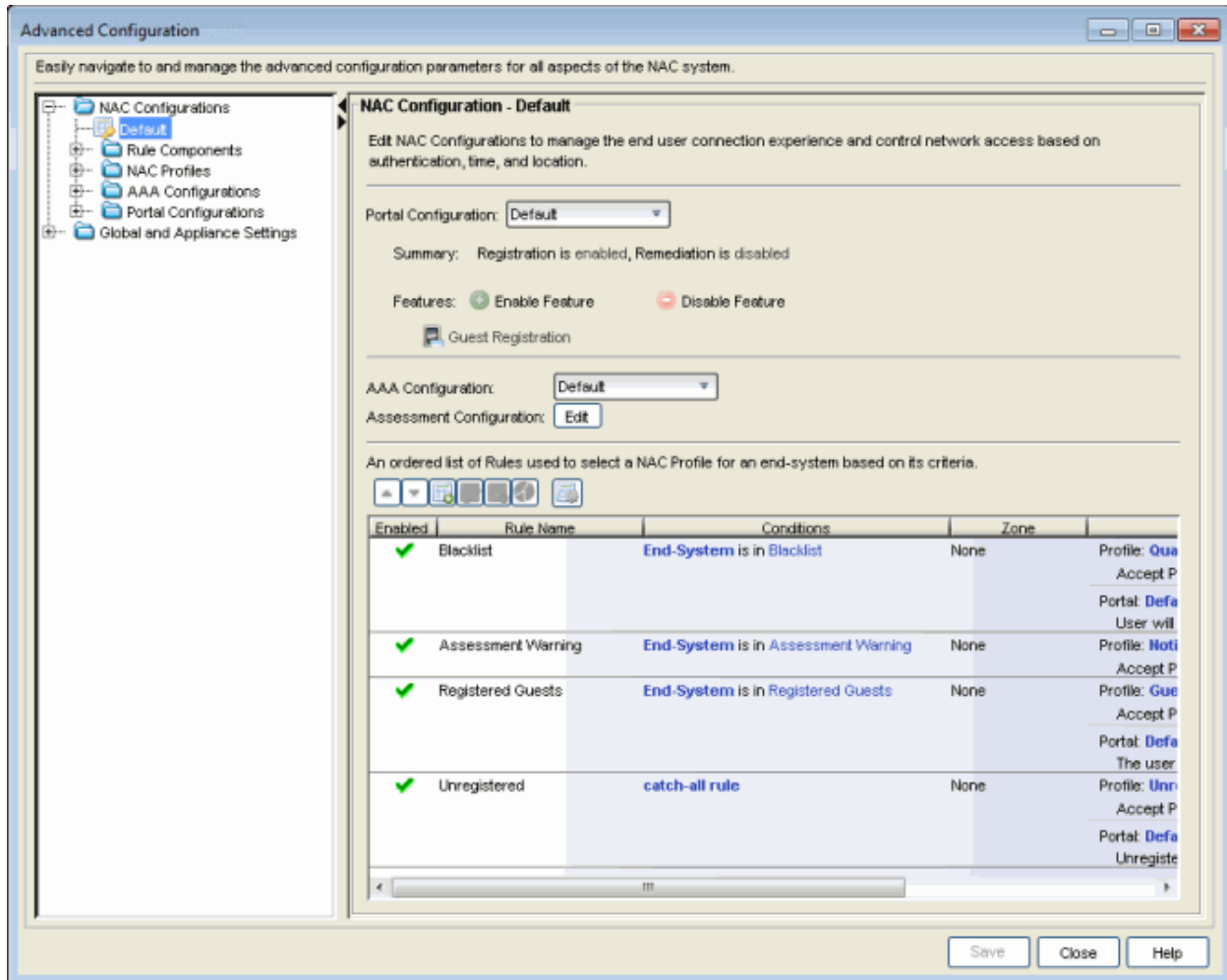
34.34.34.44.44.48, 122.111.45.48, description of mapping

MAC addresses can be delimited with colons (:), periods (.), or dashes (-), but they will be displayed in the table with colons. Lines starting with "#" or "/" will be ignored.

NAC Configuration Panel

The NAC Configuration panel in the Advanced Configuration window provides access to the various Extreme Access Control (Access Control) components included in a NAC Configuration.

You can access the Advanced Configuration window, by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the NAC Configurations folder. Your configurations are listed below the folder. You can also create a new NAC Configuration by right-clicking on the NAC Configurations folder and selecting Add new NAC Configuration.



Portal Configuration

If your network is implementing [Registration](#) or [Assisted Remediation](#), the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process. Use the drop-down menu to select and/or edit the Portal Configuration you want this NAC Configuration to use. Use the Enable Features button to enable or disable the registration, access, and assessment features you want available to users connecting to the network. Click on the feature's link to open the portal configuration page where you can configure the corresponding parameters.

AAA Configuration

The AAA Configuration defines the LDAP and RADIUS configuration which provides authentication and authorization services to the Access Control engines. Access Control engines are shipped with a default AAA configuration. Use the drop-down menu to select and/or edit the AAA

Configuration you want this NAC Configuration to use. For more information, see [AAA Configuration](#).

Assessment Configuration

Assessment configurations define the different assessment requirements for end-systems connecting to your network. If you have configured assessment for this NAC configuration (through either a profile used by one of the configuration rules or the default profile), use the Edit button to edit the Assessment Configuration. For more information, see [How to Configure Assessment](#).

Rules

The Rules table displays the rule name, whether the rule is enabled, and summary information about the rule. It also shows the NAC Profile assigned to any end-system that matches the rule and the portal redirection action, if applicable. Rules are listed in order of precedence. End-systems that do not match any of the listed rules are assigned the Default Catchall rule. Use the Rules toolbar buttons to create a new rule or perform actions on the rules. For more information, see [NAC Configuration Rules](#).

Related Information


- [Portal Configuration](#)
- [AAA Configuration](#)
- [NAC Configuration Rules](#)

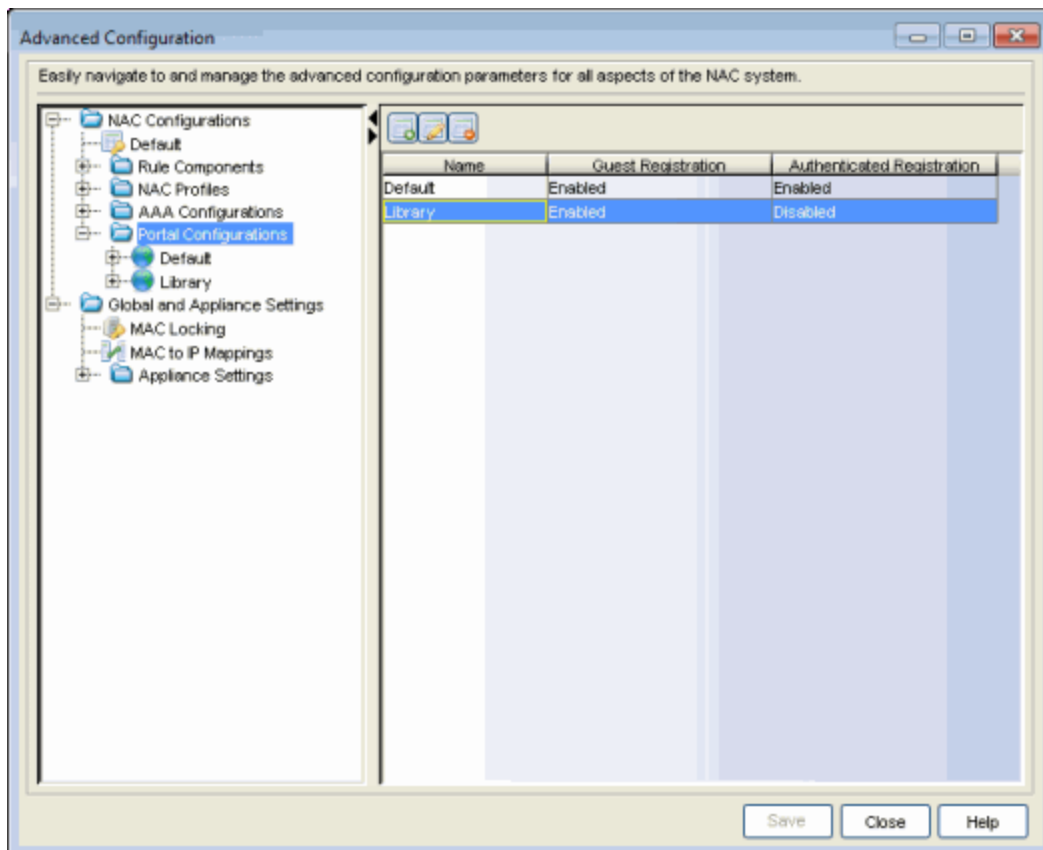
Portal Configurations Panel

The Portal Configurations panel in the Advanced Configuration window lets you view and edit all the portal configurations defined in NAC Manager. You can also add and configure a new portal configuration, if desired.

To access the Portal Configurations panel, select **Tools > Management and Configuration > Advanced Configuration** from the menu bar to open the Advanced Configuration window. In the left-panel tree, expand the NAC Configurations folder. If you expand the Portal Configurations folder you see the Default portal configuration plus any other configurations you have defined listed under the folder.

To add a new configuration, click on the  button in the toolbar. Enter a name for the configuration and click OK. The new configuration is added to the list.

To edit a configuration, select the configuration in the list and click the  button in the toolbar. The Edit Portal Configuration window opens where you can configure the portal's parameters.



Related Information

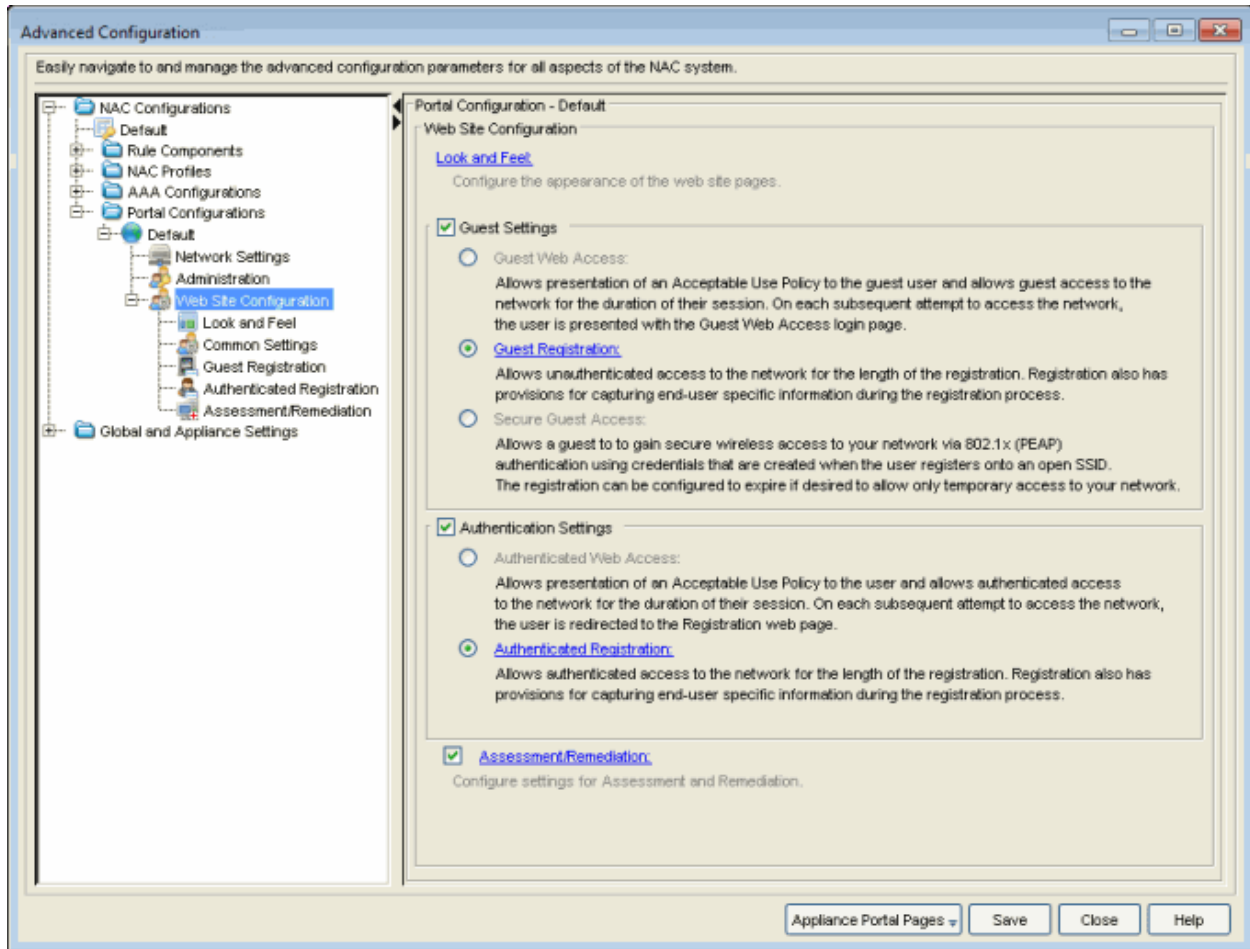
- [Portal Configuration](#)
- [AAA Configuration](#)
- [NAC Configuration Rules](#)

Web Site Configuration Panel

The Web Site Configuration panel in the Advanced Configuration window displays the different access types available for a portal configuration. It allows you to configure access types for a portal configuration that is not being used by a NAC Configuration. Read through the descriptions, and select the access types you want to configure. When a type is selected, a corresponding selection will become available for configuration in the Portal Configuration tree. You can also click on the link to access the configuration view for that access type.

NOTE: If the portal **is** being used by a NAC Configuration, you can enable captive portal access types directly in the NAC Configuration Features section. Be aware that changing the access types here in the Web Site Configuration panel will also change the access types configured in the NAC Configuration.

To access the Web Site Configuration panel, select **Tools > Management and Configuration > Advanced Configuration** from the menu bar to open the Advanced Configuration window. In the left-panel tree, expand the Portal Configurations folder.



Related Information


- [Portal Configuration](#)
- [NAC Configuration Panel](#)

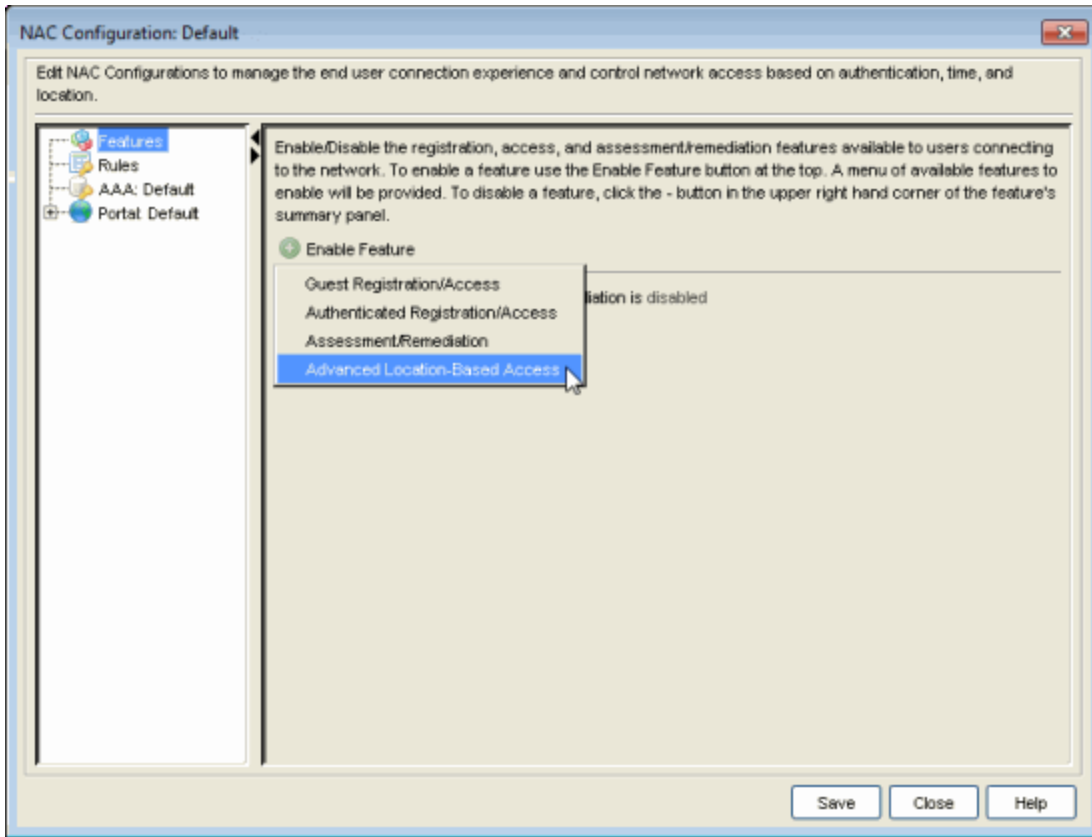
Advanced Location-Based Registration and Web Access

Advanced location-based registration and web access allows you to configure different access features for end users based on the location of a connecting end-system, as determined by the location groups you have defined for your network. (For more information on setting up location groups, see the [Add/Edit Location Group Window](#) Help topic.)

For example, with location-based registration, a company can have guest registration configured for their conference rooms and authenticated registration configured in offices, with different portal designs for each access method.

Use the following steps to define a location-based access configuration. The configuration specifies the access method and portal used by the end user to register or log in, and the access levels assigned to the end user following registration or login. You must define a separate access configuration for each location.

1. Click the NAC Manager  toolbar button to open the NAC Configuration window .
2. In the left-panel tree, select the **Features** icon. In the right panel, click the **Enable Feature** button and select Advanced Location-Based Access from the menu.



3. The Advanced Location-Based Registration & Web Access Behavior window opens.

Advanced Location Based Registration & Web Access Behavior

For the specified location conditions define an optional zone and the registration and web access features that will be displayed to a user of an unknown end-system when they enter the NAC Captive Portal. Then define the access level for users that will be achieved when they provide information about themselves and/or the device that is being registered.

Rule Conditions

Location: Library

Time: Any

Portal Welcome and Login Pages

Incoming IP Range: Library IP Subnet

End-System Zone Assignment: None

Portal: Library

Features: Enable Feature Disable Feature

Guest Web Access

Access Rules

Rule	End-System Group	NAC Profile
Registration Denied Access	Registration Denied Access	Registration Denied Access N...
Registered Guests	Registered Guests	Guest Access NAC Profile
Registration Pending Access	Registration Pending Access	Unregistered NAC Profile
Unregistered		Unregistered NAC Profile

OK Cancel

4. Configure the Rule Conditions that must be met in order for an end user to qualify for this location-based access.
 - a. In the Location drop-down box, select the desired location group from the list of existing groups. The location group defines the SSID, APs, switches, or ports that an end-system must connect to in order to meet the rule conditions. You can create a new location group or edit an existing group, if desired.
 - b. In the Time drop-down box, select the desired Time group from the list of existing groups. The time group defines the time period that an end-system must connect to in order to meet the rule conditions. You can create a new time group or edit an existing group, if desired.
5. The Portal Welcome and Login Pages are displayed when end users first attempt to connect to the network. In order to provide a custom experience for connecting end users, you can set all IP addresses for this location to

see the welcome and login pages as configured in the portal specified for this location. Otherwise, end users see the login page as defined by the default portal configuration. This option is useful for service providers with multiple tenants that want to have unique login pages for each tenant location.

- a. In the Incoming IP Range drop-down box, select an end-system group that contains the IP subnets for this location. You can create a new group or edit an existing group, if desired. If you select **None**, the default login page displays to end users.
6. Select the end-system zone assigned to any end user that matches the Rule Conditions. See [How to Configure End-System Zones](#) for more information about how to use and configure end-system zones in NAC Manager.
7. In the Portal section, use the drop-down menu to select the portal configuration you want to use for this location. You can also create a new portal configuration or edit an existing configuration, if desired.
8. Use the **Enable Feature** button to select the type of access you want to define for this location. Once you have enabled a feature, you can click on the feature link that appears below to open the Edit Portal Configuration window and edit the access feature parameters.
 - **Guest Registration** - Guest registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.
 - **Guest Web Access** - Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP). Guest web access provides a single session, and no permanent end user records are stored.
 - **Secure Guest Access** - Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text).
 - **Authenticated Registration** - Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

- **Authenticated Web Access** - Authenticated web access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy. End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored.
 - **Assisted Remediation** - Assisted remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations.
9. In the Access Rules section, define the access levels assigned to end users as they move through the registration or login process. As the end user registers or logs in through the portal, they transition through several rules. Each rule assigns the end user to an end-system group and NAC profile that specifies the access level for the end user while they are in that state. Use the drop-down menus to select the end-system group and NAC profile for each rule.
10. Click **OK**. The NAC Configuration Features panel lists the new location.
-

Related Information

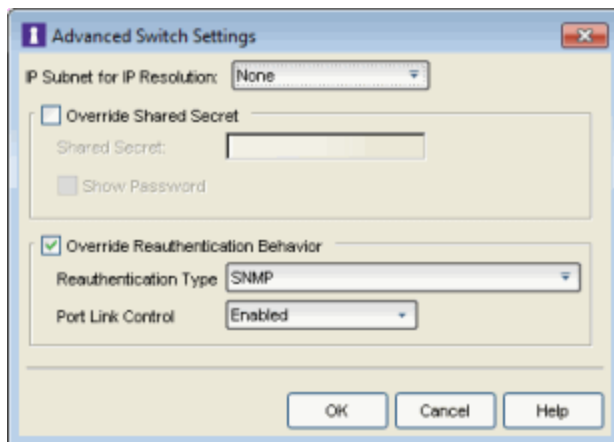
For information on related windows:

- [NAC Configuration Window](#)
- [Portal Configuration Window](#)
- [Add Location Group Window](#)
- [Add End-System Group Window](#)
- [Add Time Group Window](#)


Advanced Switch Settings

This window allows you to configure settings for switches that require a different configuration than your standard switch settings set in the Appliance Settings window for Extreme Access Control (formerly NAC) engines.

You can access the window from the [Add Switch to NAC Appliance Group window](#) or the [Edit Switch in NAC Appliance Group window](#).




IP Subnet for IP Resolution

Use the drop-down list to display a list of the IP subnets configured in the Appliance Settings window. Click the edit button  on the drop-down list to open the [IP Resolution tab of the Appliance Settings window](#) where you can add, edit, or delete IP subnets. If you select a subnet, the switch uses it as an inclusive list for MAC to IP resolution. Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it would not be discovered via DHCP. IP subnets also contain an IP range which can be used to filter out secondary IP addresses that are not valid for the network. For more information on MAC to IP Resolution, see the [NAC Deployment Guide](#).

Override Shared Secret

This option allows you to override the shared secret configured in the Switch Configuration section of the [Credentials tab of the Appliance Settings window](#). This is the shared secret the switch uses to communicate with the Extreme Access Control engine. Only use this option when the switch cannot use the standard shared secret you use for the rest of your devices. When the **Show Password** option is selected, the shared secret is shown in text.

Override Reauthentication Behavior

This option allows you to override the RFC 3576 reauthentication and port link control settings configured in the Switch Reauthentication Configuration section of the [Reauthentication tab of the Appliance Settings window](#). Use the drop-down list to display a list of the reauthentication types. Click the **Edit** button  on the drop-down menu to open the Appliance Settings window where you can add, edit, or delete reauthentication types.

Related Information

For information on related windows:

- [Edit Switches in NAC Appliance Group Window](#)
- [Add Switches to NAC Appliance Group Window](#)

Allowed Web Sites Window

Use this window to configure the web sites that end users are allowed to access during the NAC Assisted Remediation and Registration process. This window is configured as part of your portal configuration, and is accessed from the Network Settings section of the [Edit Portal Configuration window](#).

There are three subtabs in the window: [Allowed URLs](#), [Allowed Domains](#), and [Web Proxy Servers](#).

Allowed URLs

This tab lists the URLs that end-systems can access while the end-system is being assessed, when the end-system is quarantined, or when the end-system is not registered on the network. The Extreme Access Control engine proxies these HTTP connections to the allowed URLs as long as the engine is configured with an appropriate DNS server.

Any URLs that you may have referenced in the captive portal configuration must be entered into this tab so an end-system that is restricted access to the network is permitted to communicate to the URL. For example, a URL entered in the [Helpdesk Information](#) section should be entered here so a quarantined end-system may access the Helpdesk web site while quarantined.

Enter the URL you want to add to the list and click **Add**. URLs must be entered without "http://www". For example, if "http://www.apple.com" is an allowed website, then "apple.com" should be entered as the allowed URL.

You can use the **Import** button to import a file of URLs to the list. Files must be formatted to contain one URL per line. Lines starting with "#" or "/" are ignored.

NOTE: It is not necessary to enter URLs that are accessed over secure HTTP (HTTPS). To restrict access to these URLs, you must configure network policy to allow or disable HTTPS traffic all together or restrict it to specific IP ranges.

When an allowed URL is added, all web pages located within the directory are also allowed. For example, if apple.com is configured as an allowed URL, then HTTP connections for the following URLs are also permitted:

`www.apple.com/downloads`

`www.apple.com/downloads/macosex`

HTTP connections to URLs located on different hosts than that of the allowed URL entry are not permitted. These HTTP connections are redirected to the Assisted Remediation or MAC Registration web page. Using the same example, if apple.com is configured as an allowed URL, HTTP connections for the following URLs are not allowed:

```
store.apple.com
store.apple.com/download
```

Images on the web page may not be displayed properly if the images are served on a separate HTTP connection at a different URL. For example, the web page `http://www.apple.com/support/downloads/` contains images downloaded from `http://images.apple.com`. Therefore, if `apple.com/support/downloads/` is configured as an allowed URL, all of the text on the web page displays properly, but the images do not display on the web page unless `images.apple.com` is also entered as an Allowed URL.

Allowed Domains

This tab lists the domains to which end users can browse while the end-system is being assessed, the end-system is quarantined, or when the end-system is not registered on the network. The Extreme Access Control engine proxies these HTTP connections to the allowed domains as long as the engine is configured with an appropriate DNS server.

The higher-level domain information not explicitly specified in an allowed domain entry is also permitted for an end-system as well as any web pages served from within the domain. For example, if apple.com is configured as an allowed domain, then HTTP connections for the following URLs is also permitted:

```
www.apple.com
www.info.apple.com
store.apple.com
store.apple.com/info
images.apple.com
www.apple.com/software
apple.com/software
```

HTTP connections not matching the specified domain level information in an allowed domain entry is not permitted. These HTTP connections are redirected to the Assisted Remediation or Registration web page. Using the same example, if apple.com is configured as an allowed domain, HTTP connections for the following URLs are not allowed:

```
www.apple2.com
```

```
store.apple-chat.com
www.msn.com
```

If multiple allowed domain entries are configured with overlapping first-level and second-level domain information, then the allowed domain entry that is more specific takes precedence. For example, if `apple.com` and `store.apple.com` are configured as allowed domain entries, then the `apple.com` entry is effectively disabled. Therefore, HTTP connections for the following URLs are allowed:

```
store.apple.com
store.apple.com/info
www.store.apple.com/info
```

The following HTTP connections are not allowed:

```
www.apple.com
www.apple.com/support
images.apple.com
```

The following is a list of default allowed domains that are preconfigured for NAC remediation. These allowed domains are provided as part of the assisted remediation assessment functionality, which allows end-users limited Internet access to update patches, antivirus definitions, and to upgrade vulnerable software in order to comply with the network security policy. The Extreme Access Control engine proxies traffic to these allowed domains when an end user clicks on a remediation link presented on the violations page.

A default allowed domain should only be deleted if it is determined that a quarantined user should not be able to access it. In some cases, you may need to add additional URLs or domains. If a quarantined user selects a remediation link to resolve an issue and is redirected back to the remediation web page, the domain or URL needs to be added to provide access to that site.

adobe.com	akadns.net	akamai.com
akamai.net	altn.com	apache.org
apple.com	archives.neohapsis.com	asp.net
aws.amazon.com	bitdefender.com	bugzilla.org
ca.com	cdnetworks.com	cert.org
cisco.com	clamav.net	cve.mitre.org
debian.org	drupal.org	eset.com
eu.ntt.com	f-secure.com	gnu.org
godaddy.com	ibm.com	ipswitch.com

isc.org	kaspersky.com	lac.co.jp
level3.com	localmirror.com	kaspersky-labs.com
macromedia.com	mandriva.com	mcafee.com
microsoft.com	mozilla.org	mysql.com
netwiner.com	norton.com	novell.com
nsatc.net	openssl.org	oracle.com
osvdb.org	pandasecurityusa.com	php.net
phpuke.org	redhat.com	samba.org
secunia.com	securiteam.com	securityfocus.com
securitytracker.com	sendmail.org	sophos.com
sourceforge.net	squid-cache.org	sun.com
support.citrix.com	suse.com	suse.de
symantec.com	symantecliveupdate.com	techtarget.com
trendmicro.com	ubuntu.com	us-cert.gov
verisign.com	verisigninc.com	vmware.com
vupen.com	web.mit.edu	webroot.com
windows.com	windowsupdate.com	wireshark.org
xforce.iss.net	zerodayinitiative.com	zope.org

Web Proxy Servers

This tab is used to specify the web proxy server(s) deployed on the network. The Extreme Access Control (Access Control) engine proxies end-system Allowed URL and Allowed Domain HTTP traffic to the defined web proxy servers if the network utilizes proxy servers to access the Internet.

If multiple web proxy servers are configured, the Access Control engine round robins HTTP connections to the configured proxy servers. If the allowed web site is located with the Access Control engine's configured domain, the Access Control engine directly contacts the web site and not go through the configured web proxy servers.

Related Information

For information on related help topics:

- [Edit Portal Configuration Window](#)

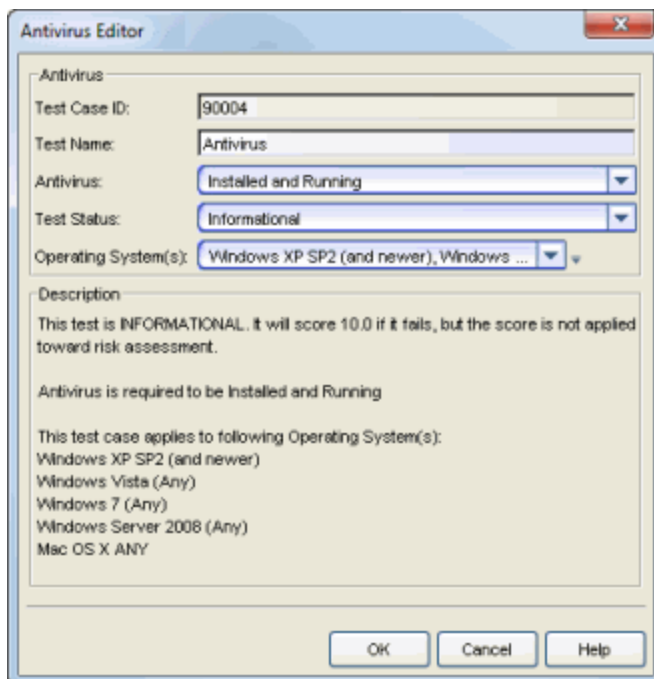
Antivirus Editor

This window lets you configure parameters for the Antivirus test case included in an [agent-based test set](#). This test checks to see if the state of the antivirus software on the end-system matches the Antivirus state specified here.

Windows requires the Windows Security Center for this test.

For the Mac operating system, NAC Manager supports the testing of the following antivirus software:

- McAfee 8.6
- McAfee 9.0
- McAfee 9.5
- Sophos 4.9
- Sophos 7.x
- Norton 11
- Symantec AV 10
- Symantec Endpoint 11
- ClamX AV 2.2.2



The screenshot shows the 'Antivirus Editor' dialog box. It contains the following fields and options:

- Test Case ID:** 90004
- Test Name:** Antivirus
- Antivirus:** Installed and Running (dropdown menu)
- Test Status:** Informational (dropdown menu)
- Operating System(s):** Windows XP SP2 (and newer), Windows ... (dropdown menu)

Description:

This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.

Antivirus is required to be Installed and Running

This test case applies to following Operating System(s):

- Windows XP SP2 (and newer)
- Windows Vista (Any)
- Windows 7 (Any)
- Windows Server 2008 (Any)
- Mac OS X ANY

Buttons: OK, Cancel, Help

Test Case ID

The Antivirus test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Antivirus

Use the drop-down list to select the antivirus state you want to test for.

Test Status


Use the Test Status drop-down menu to specify a status for this test. The status determines how the score returned by the assessment test is used.

- Disabled - The test is not run.
- Informational - The test is run and test score results are reported, but are not applied towards a quarantine decision. No end-systems are quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) is expired.
- Mandatory - Test score results are included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down menu to select the operating systems to which this test case applies. This menu is automatically populated with all the operating systems on which this test is performed. The Windows operating system requires the Windows Security Center to perform this test.

 Use the configuration menu button to open the Manage Operating Systems window, where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make are only reflected in the drop-down selection menu as long as they are supported by the test.

Description

A description of the test case parameters.

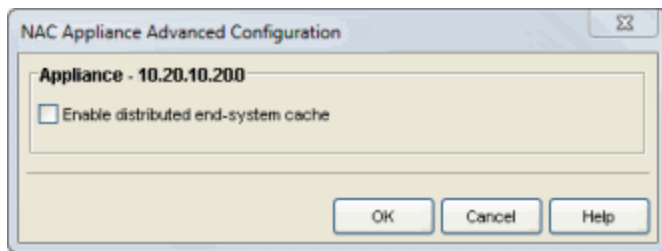
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Extreme Access Control Engine Advanced Configuration Window

Use this window to configure advanced options for the selected Extreme Access Control (Access Control) engine. Access these advanced options by clicking the **Advanced Configuration** button in the engine [Configuration tab](#).



Enable Distributed End-System Cache

This advanced option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling the distributed end-system cache improves Access Control performance when discovering new end-systems as they connect, or when end-systems move from one place to another in the network.

To use the end-system cache feature, it must be enabled on both the Extreme Management Center (Management Center) Server (using the NAC Manager options > Advanced Settings > [Enable distributed end-system cache option](#)) and on the Access Control engines using the cache (using the option in this window). Changing this option on an Access Control engine requires an enforce. The Access Control engine does not need to be restarted.

When this feature is enabled, the Management Center Server and the Extreme Access Control engine exchange additional data each time end-system data is updated. This feature is **not** recommended unless there is sufficient network bandwidth for the additional data, a fast connection between the Management Center Server and the Access Control engine, and end-systems are adding or moving frequently.

Related Information

- [NAC Manager Options](#)
- [Extreme Access Control Engine Configuration Tab](#)

New/Edit Engine Settings Window

Engine settings provide advanced configuration options for Extreme Access Control (Access Control) engines. NAC Manager comes with a default engine settings configuration. If desired, you can edit these default settings or you can define your own settings to use for your Access Control engines.

You can launch the New/Edit Engine Settings window from the [Engine Settings panel](#) in the Advanced Configuration window. **To create new engine settings**, click the **Add** button at the top of the panel. **To edit existing engine settings**, select the engine setting in the table and click the **Edit** button. The New or Edit Engine Settings window opens with the following tabs available for configuration:

- [IP Resolution Tab](#)
- [MAC Resolution Tab](#)
- [Hostname/Username Resolution Tab](#)
- [Reauthentication Tab](#)
- [Credentials Tab](#)
- [Miscellaneous Tab](#)
- [Device Type Detection Tab](#)
- [Network Tab](#)

NOTE: To access status and diagnostic information for a Access Control engine, launch the Access Control Engine administration web page by right-clicking on the Access Control engine in the left-panel tree and selecting WebView. You can also access the administration web page using the following URL: `https://<Access ControlEngineIP>:8444/Admin`. The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in the Web Service Credentials field on the [Credentials Tab](#) in the Engine Setting window.

IP Resolution Tab

The IP resolution tab is used to define how and when NAC Manager resolves an end-system's MAC address to an IP address for the end-system. These parameters are applicable for Extreme Access Control (Access Control)

Gateways and L2 Access Control Controllers, but not L3 Access Control Controllers.

Appliance Settings - NetSight-NAC Lab Appliance Settings

Credentials
 Miscellaneous
 Device Type Detection
 Network

IP Resolution
 Hostname/Username Resolution
 Reauthentication

Resolve IP Address:

IP Address Resolution Timeout (in seconds):

Allowed Retries On Failure: with Delay (in seconds):

DHCP Resolution Delay Time (in seconds):

Use DHCP Request IPs:

Rediscover IP on DHCP Request

Use Agent-based Assessment IPs:

Use RADIUS Accounting Packets

Clear Duplicate IPs on Switches:

Clear Duplicate IP Re-Read Delay (in seconds):

NetBIOS IP Filtering

Router IP Discovery

Clear Duplicate IPs on Routers:

Default Router Profile:

Default Router SNMP Context:

IP Subnets

Global IP Subnets

Subnet Name	VLAN ID	End System Ip Range
12.22.82.0/27 Subnet	[40] Accept VLAN	12.22.82.5-12.22.82.30
12.22.82.32/27 Subnet	[41] Quarantine VLAN	12.22.82.37-12.22.82.62
12.22.82.64/27 Subnet	[42] Unregistered VLAN	12.22.82.69-12.22.82.94
12.22.82.96/27 Subnet	[43] Guest and Assessing VLAN	12.22.82.101-12.22.82.126

Resolve IP Address

Specify when a Access Control engine resolves the IP address for end-systems:

- Always - (Default) Resolve the IP address for every end-system that NAC Manager sees.
- Only for Assessment - Resolve the IP address for end-systems that need to be assessed (scanned).

IP Address Resolution Timeout

Enter the maximum time a Access Control engine should spend trying to resolve an IP address from an end-system's MAC address before giving up and returning the Error state (MAC to IP Resolution Timed Out) for that end-system.

Allowed Retries on Failure

The number of attempts made to resolve the IP address after the first attempt fails. The default setting is 2 retries, which means that NAC Manager retries a timed-out request two times, making a total of three attempts to resolve the IP address. Enter the amount of delay time in seconds that NAC Manager waits before retrying to resolve the IP address.

DHCP Resolution Delay Time

The number of seconds a Access Control engine should wait after learning about an end-system before attempting to resolve the end-system's IP address. This delay is used to allow the end-system to negotiate its DHCP IP address. If Port Link Control is enabled, this delay is used after the Access Control engine links down/up the port to force the end-system to request a new IP address on the new VLAN.

NOTE: If the delay time specified here is less than the amount of time the end-system needs to renew its IP address, then the Access Control engine may resolve the end-system's IP address incorrectly. This is a problem when assessment is enabled and may cause the engine to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Use DHCP Request IPs

Specify when, if ever, an IP address learned from a DHCP request packet could be used when resolving an end-system's IP address. This option is applicable only for Access Control Gateways, since an inline Access Control Controller should always hear the DHCP response as well.

- Always - Always consider the IP address learned from a DHCP request for an end-system's IP, after all more reliable methods have been exhausted.
- Never - Never consider an IP address learned from a DHCP request when resolving an end-system's IP address. In a situation where the Access Control Gateway receives DHCP packets from both the client and server, the gateway uses this IP when these packets are received during the IP resolution process. With subsequent authentications for which there is no additional DHCP exchange, Access Control uses the

enabled resolution options to resolve the IP address but does not use any previously learned DHCP information to resolve the IP.

- For Non-VLAN Switches Only - (Default) Only consider IP addresses learned from DHCP request packets when the NAS switch the end-system was authenticated for does not use VLANs for access control. The IP addresses from request packets in a VLAN environment is always incorrect, because as an end-system transitions through VLANs, it always requests the IP from the previous VLAN.

Rediscover IP on DHCP Request

When this option is selected, NAC Manager re-runs IP resolution on an authenticated end-system if a DHCP request causes its IP address to change. In this instance, the Access Control policy applies to the new IP address and removed from the old IP address, and assessment scans and port resolution are not performed.

Use Agent-based Assessment IPs

Specify when, if ever, an IP address reported by a connected agent could be used when resolving an end-system's IP address. This process looks for the end-system's MAC address in the list of MAC addresses from known connected agents. If an agent is connected and heartbeats during the IP Resolution process, then NAC Manager uses the IP address of that agent.

- Always - Always consider the IP address reported by a connected agent for an end-system's IP, after all more reliable methods have been exhausted.
- Never - (Default) Never consider an IP address reported by a connected agent when resolving an end-system's IP address.
- For Non-VLAN Switches Only - Only consider IP addresses reported by a connected agent when the NAS switch the end-system was authenticated for does not use VLANs for access control.

Use RADIUS Accounting Packets

When this option is selected, if the Access Control engine receives a RADIUS accounting packet with a Framed-IP-Address in it, the engine skips IP resolution and use the IP address in the RADIUS accounting packet.

Clear Duplicate IPs on Switches

Select this option to have a Access Control engine clear out duplicate entries in the node alias and ARP tables of the NAS switch the end-system was authenticated for, if duplicates are found while trying to resolve the IP

address of an end-system. The Access Control engine then tries to re-read the IP address from the table to find the most recent entry.

Clear Duplicate IP Re-Read Delay

Specify the amount of time in seconds that a Access Control engine waits after clearing duplicate IPs on a switch or a router before re-reading the node alias or ARP tables.

NetBIOS IP Filtering

This option causes the Access Control engine to make NetBIOS requests to a list of IP addresses, if multiple IP addresses are found when trying to resolve the IP address of an end-system. See [NetBIOS Timeout](#) and [NetBIOS Timeout Retry Count](#) on the Miscellaneous tab.

Router IP Discovery

Selecting this option causes NAC Manager to make requests to an end-system's gateway router ARP table to try to resolve the IP address for an end-system, if the Access Control engine was unable to resolve the IP address by querying the NAS switch. The gateway router for an end-system can be discovered by the relay router field of a DHCP packet or by using the gateway router defined for an IP subnet for the VLAN an end-system is put into by NAC Manager. See [IP Subnets](#).

Clear Duplicate IPs on Routers

This option causes a Access Control engine to clear out duplicate entries in the ARP tables of an end-system's gateway router, if duplicates are found while trying to resolve the IP address of an end-system. The Access Control engine then tries to re-read the IP address from the table to find the most recent entry. See [Clear Duplicate IP Re-Read Delay](#).

Default Router Profile

The profile used to make SNMP requests to the gateway router for an end-system, if one is not defined for a specific router's interface IP address as part of an IP subnet. Use the **Edit** button to open the Profiles/Credentials tab in the Authorization/Device Access window where you can define authentication credentials and create the profiles that use those credentials.

Default Router SNMP Context

The SNMP context used when making requests to the router, if the credentials used for the router are SNMP v3 and the specific router's interface IP address has not been defined as part of an IP subnet.

IP Subnets

IP subnets are used to assist in IP resolution in the following three scenarios:

- If a switch is using RFC3580 (VLAN enforcement of access control), the process for determining an IP address is much more difficult. In this scenario, IP subnets can be defined for each VLAN to provide an IP range filter, which can be used to filter the list of IPs discovered on the switch. IP subnets also provide a way to specify a gateway router for the VLAN's subnet, which can be used for doing SNMP reads on a router if DHCP snooping did not capture the relay router.
- When VRRP or HSRP is used, and you want NAC Manager to query the router if needed, NAC Manager needs to know the primary/secondary router relationship. This order of precedence can be defined in the IP subnet and ensures that NAC Manager queries the primary router first to get the most accurate data. This is needed in a VRRP or HSRP environment, because both routers send out a DHCP inform message, and it is most likely that the Access Control Gateway gets the secondary router's message last causing it to query the incorrect router.
- When DHCP snooping is used, the router SNMP credentials are not the same for all routers. In this scenario, if you want NAC Manager to query the router for IP resolution, the IP subnets can be used to define the mapping between the relay router IPs and the correct SNMP credentials to use for them.

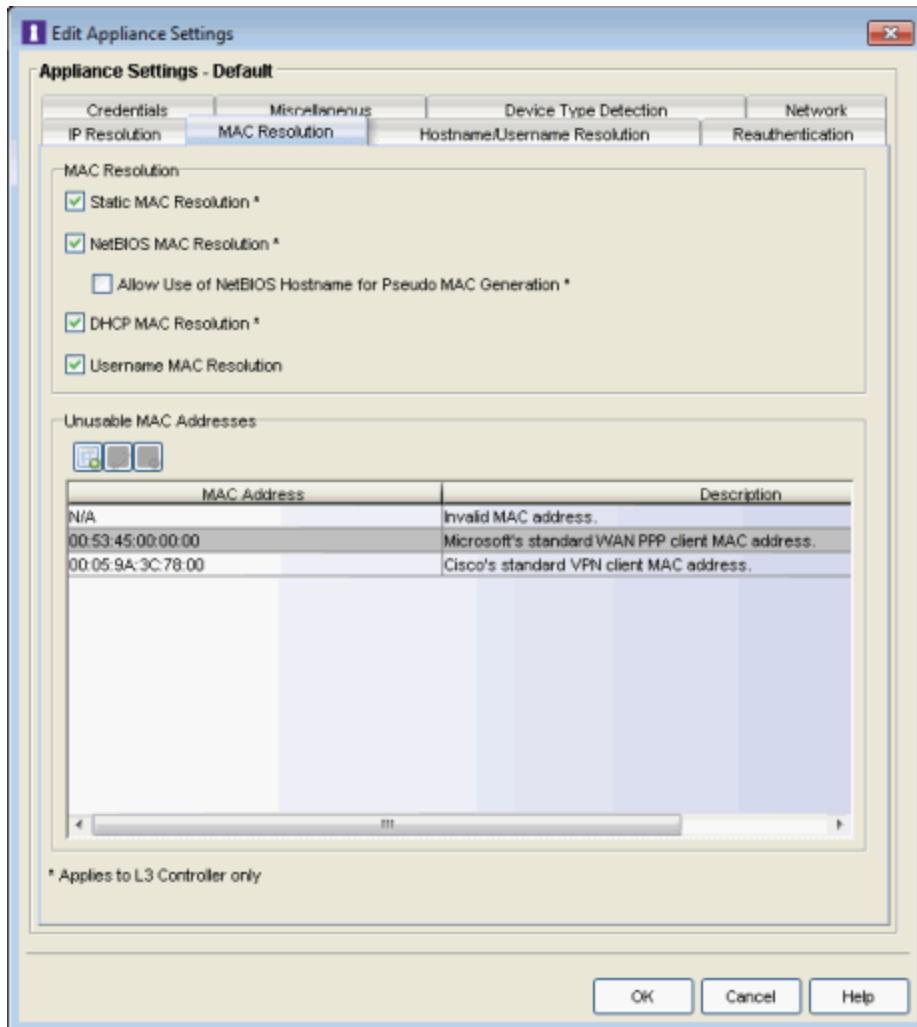
You can add, edit, or delete IP subnets using the toolbar buttons at the top of the table. There is also a File Import button that lets you import a file of IP subnets; see the File Import window for the file format that must be used.

The **Global IP subnets** option is used to create a global list of IP ranges used for the purpose of IP Resolution. The IP Resolution process ignores any IP address outside the configured ranges. The checkbox is disabled unless there is at least one subnet configured.

MAC Resolution Tab

The MAC resolution tab is used to define how and when NAC Manager resolves an end-system's IP address to a MAC address for that end-system. These parameters are applicable for L3 Extreme Access Control (Access Control)

Controllers only and this tab only displays if an L3 Controller is present on your network.



Static MAC Resolution

This option enables the reverse lookup for the Advanced Configuration > Global and Appliance Settings > [MAC to IP Mappings](#).

NetBIOS MAC Resolution

This option allows NAC Manager to perform NetBIOS requests to an end-system's IP address (heard by the L3 Access Control Controller), to resolve the end-system's MAC address. See [NetBIOS Timeout](#) and [NetBIOS Timeout Retry Count](#) on the Miscellaneous tab.

Allow Use of NetBIOS Hostname for Pseudo MAC Generation

This option allows NAC Manager to generate a pseudo MAC address for an end-system based on the end-system's hostname. This process is used if the MAC address discovered from the NetBIOS response is listed in the Unusable MAC Addresses table. The advantage to generating a pseudo MAC address is that it allows the end-system's events to be correlated to the end-system. The disadvantage is that users may name their end-systems with the same hostname, and then the algorithm used to generate the MAC address from a hostname is not guaranteed to generate unique hostnames for two different end-systems. See [Unusable MAC Addresses](#).

DHCP MAC Resolution

This option enables the reverse lookup into the DHCP table learned by DHCP snooping.

Username MAC Resolution

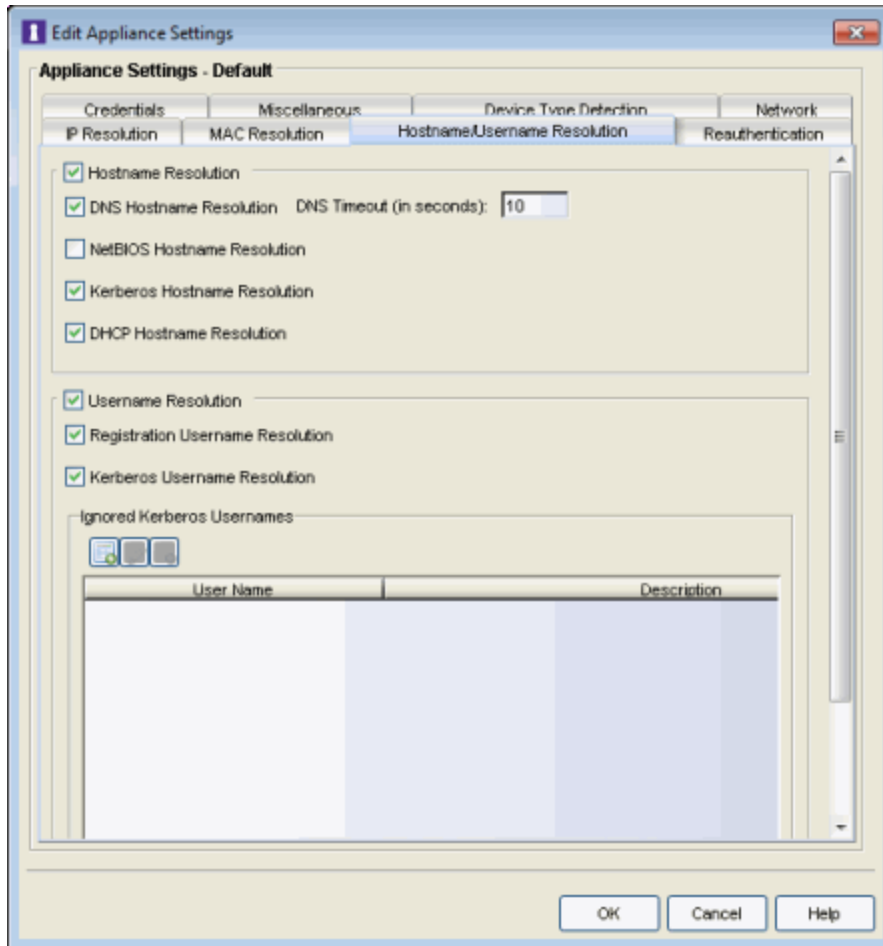
This option allows NAC Manager to generate a pseudo MAC address for an end-system based on the username used to log onto the network. This is mainly used with VPN requests where the username is known but the MAC address is not. Generating a pseudo MAC address from the username causes all the VPN logins from one user to show up as a single entry no matter what IP address they get. See [Unusable MAC Addresses](#).

Unusable MAC Addresses

This table is used to define well-known MAC addresses that are not real, and could be used by multiple end-systems. An example would be Microsoft's standard WAN PPP client MAC address, which is the MAC address of a Windows end-system's VPN interface, using the standard Microsoft VPN client. This MAC address is 00:53:45:00:00:00. You can add, edit, or delete entries using the toolbar buttons at the top of the table.

Hostname/Username Resolution

The tab is used to define how and when NAC Manager resolves an end-system's hostname and an end-system's username. These parameters are engine for Extreme Access Control (Access Control) Gateways, L2 Access Control Controllers, and L3 Access Control Controllers.



Hostname Resolution

Use this checkbox to enable or disable hostname resolution for Access Control engines. Hostname resolution is only performed for end-systems for which NAC Manager has an IP address.

DNS Hostname Resolution

This option allows the use of reverse DNS lookup on the Access Control engine to resolve an end-system's hostname. In order for this option to work, a valid DNS server IP address must have been specified when the Access Control engine was installed. Use the **DNS Timeout field** to specify the amount of time in seconds that the Access Control engine waits after making a reverse DNS lookup prior to giving up and moving on to the next hostname resolution mechanism.

NetBIOS Hostname Resolution

This option allows the Access Control engine to make a NetBIOS request to the end-system to query the end-system for its hostname. See [NetBIOS](#)

[Timeout](#) and [NetBIOS Timeout Retry Count](#) on the Miscellaneous tab.

Kerberos Hostname Resolution

This options allows the Access Control engine to do a lookup in the table of data learned from Kerberos snooping, to resolve the end-system's host name.

DHCP Hostname Resolution

This options allows the Access Control engine to do a lookup in the table of data learned from DHCP snooping, to resolve the end-system's host name.

Username Resolution

Use this checkbox to enable or disable username resolution, which allows the Access Control engine to try resolve the name of a user currently on an end-system when the username was not part of the authentication request. MAC authentication and L3 Access Control Controller authentication are the two cases where username resolution can currently be used.

Registration Username Resolution

This options cause NAC Manager to use the username used for authenticated registration or the user's full name for unauthenticated registration in the format: Last Name, First Name.

Kerberos Username Resolution

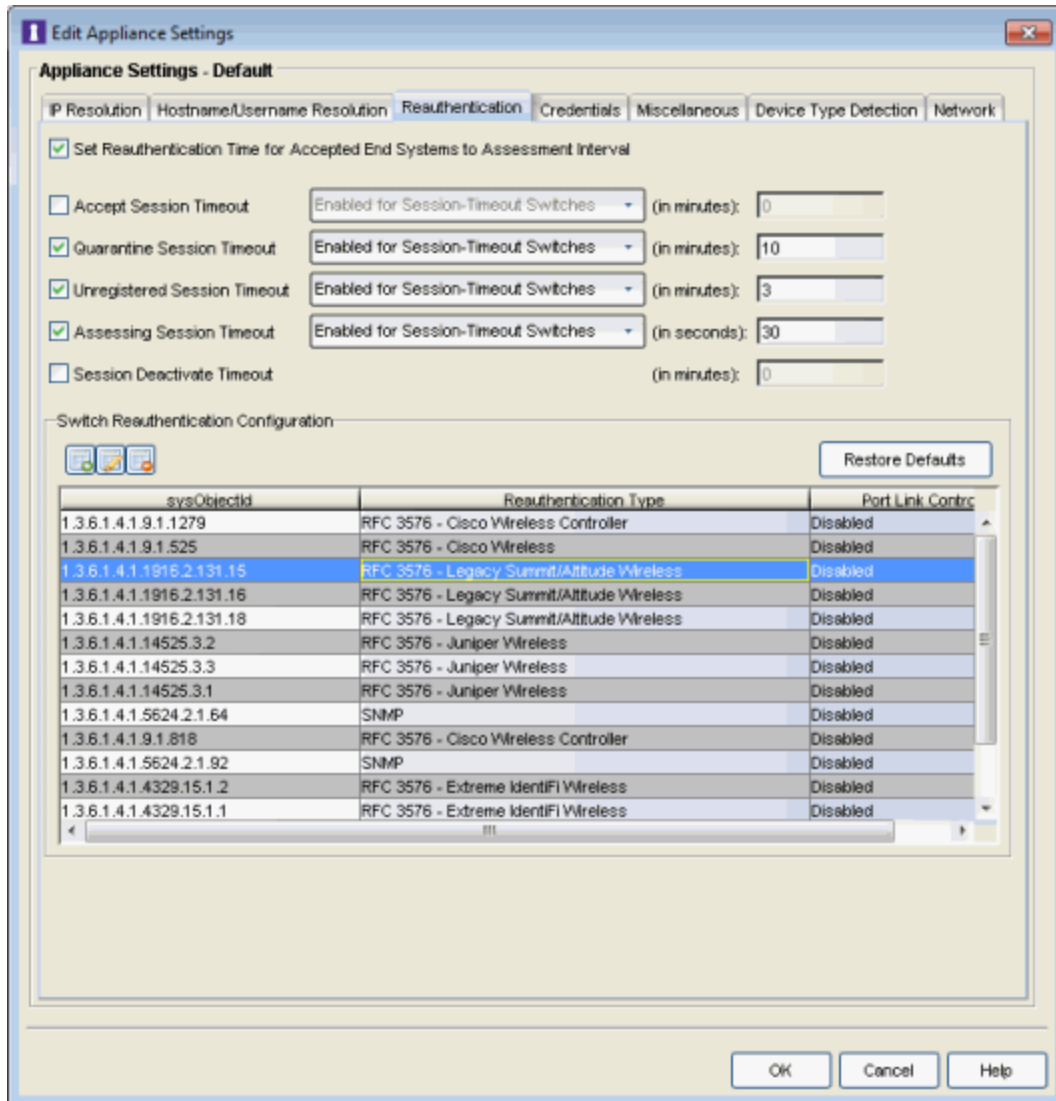
This options allows the Access Control engine to do a lookup in the table of data learned from Kerberos snooping, to resolve the name of the user currently logged into the end-system.

Ignored Kerberos Usernames

The table is used to define usernames for which Kerberos data is ignored. This is useful when applications running on an end-system use a global user over the Kerberos protocol to pass information for a program. Two known cases of this would be Sophos Anti-Virus software and the IBM Rational ClearCase source control system. You can add, edit, or delete entries using the toolbar buttons at the top of the table.

Reauthentication Tab

This tab is used to define global session-timeout behavior for L2 Access Control Controllers and Access Control Gateways, and how Access Control Gateways reauthenticates end-systems on various NAS switches. This tab is not applicable for L3 Access Control Controllers.



Set Reauthentication Time for Accepted End-Systems to Assessment Interval

This option allows the Access Control engine to set session-timeouts for accepted end-systems, causing the end-system to be reauthenticated the next time a scan needs to be performed. This option is required for networks using 802.1X authentication on wireless switches that do not support the IEEE 802.1X Port Reauthenticate MIB. It is also required for networks using MAC or Web-Based authentication on third-party switches. These switches do not have a mechanism to force re-authentication on end-systems when assessment is complete. This checkbox does not apply for Layer 3 Access Control Controller engines.

Accept Session Timeout

If enabled, this timeout applies to all end-systems that are accepted, but not considered by NAC Manager to be unregistered end-systems. If both this option and the "Set Reauthentication Time For Accepted End-Systems to Assessment Interval" option are enabled, Access Control uses the lower value. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout only applies to accepted end-systems authenticated for a NAS switch where NAC Manager cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any accepted end-system (not considered by NAC Manager to be unregistered) on any switch.

Quarantine Session Timeout

If enabled, this timeout applies to all end-systems quarantined by NAC Manager. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout is only applied to quarantined end-systems that were authenticated for a NAS switch where NAC Manager cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any quarantined end-system on any switch.

Unregistered Session Timeout

If enabled, this timeout applies to all end-systems determined to be unregistered by NAC Manager. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout only applies to unregistered end-systems authenticated for a NAS switch where NAC Manager cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any unregistered end-system on any switch.

Assessing Session Timeout

If enabled, this timeout applies to all end-systems being scanned by NAC Manager. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout applies to end-systems being assessed authenticated for a NAS switch where NAC Manager cannot reauthenticate sessions on

demand via SNMP or RFC3576.

- Enabled for All Switches - This option tells NAC Manager to apply the session timeout for end-systems being assessed on any switch.

Session Deactivate Timeout

This option can be used to provide more up-to-date information about which end-systems are still active on the network. When it is enabled, NAC Manager checks periodically to determine if an authentication request is received from an end-system within the specified time. If a user is still on the network, then the user is reauthenticated and a new event is generated stating the user is still active on the network. If the user is no longer on the network, the session is removed on the switch and the end-system is displayed in NAC Manager with the **Disconnected** state. (Note that when a user leaves the network within the period of time specified, NAC Manager does not display them as "**Disconnected** until the specified time has passed.) While this option does provide a more up-to-date list of active end-systems, RADIUS accounting should be used to provide real-time connection status. This option is useful when RADIUS accounting is not desired or is not supported on certain network devices.

NOTE: The timeout process could be off by approximately 60 seconds from the specified time, depending on when NAC Manager runs the check for authentication requests.

Switch Reauthentication Configuration

This table is used to configure the reauthentication method an Access Control engine uses on a switch. For example, you may want to add support for another wireless switch. In this case, you would add an entry for the new switch by clicking the Add button, entering the sysObjectId of the switch, and setting the Reauthentication Type to either RFC3576 (if the switch supports it) or Session Timeout. This table is also where you can disable port link control for switches by selecting the switch, clicking the Edit button, and setting the Port Link Control option to disabled.

If you've deleted or edited any of the default configurations, the **Restore Defaults** button restores them to their original state and add back any that are missing. Any custom entries you added are retained unless they have the same sysObjectId as a default configuration. Following a restore, you need to save the configurations.

Credentials Tab

Use this tab to configure various parameters for your network engines including switch configuration, web service credentials, and EAP-TLS configuration.

The screenshot shows the 'Edit Appliance Settings' window with the 'Credentials' tab selected. The window title is 'Edit Appliance Settings'. The main area is titled 'Appliance Settings - Default' and contains several sections:

- Switch Configuration:** Includes a 'Shared Secret' field, a 'Verify Shared Secret' field, a 'Show Shared Secrets' checkbox, 'RADIUS Timeout (in seconds):' set to 15, 'RADIUS Timeout Retry Count:' set to 3, and a checked checkbox for 'Use Primary RADIUS Server for Redundancy in Single NAC Appliance Configuration (Basic AAA configuration only)'.
- Web Service Credentials:** Includes a 'NAC Appliance Web Service Credentials' section with 'Username:' set to 'admin' and 'Password:' field, and a 'Show Password' checkbox.
- NAC Admin Web Page:** Includes a checkbox for 'Use NAC AAA Configuration for Admin Web Page authentication'.
- EAP-TLS Configuration:** Includes a 'Server Private Key Passphrase' field and a 'Show Passphrase' checkbox.

At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

Switch Configuration

Enter the shared secret that switches use when communicating with Extreme Access Control (Access Control) engines.

Shared Secret

A string of alpha-numeric characters used to encrypt and decrypt communications between the switch and the Access Control engine. The shared secret is shown as a string of asterisks.

Verify Shared Secret

Re-enter the shared secret you entered above.

Show Shared Secrets

When checked, the shared secret is shown in text. When unchecked, the shared secret is shown as a string of asterisks.

RADIUS Timeout

The amount of time (in seconds) that a switch waits before re-sending a RADIUS request to the Access Control engine. The default is 15 seconds and the maximum is 60 seconds. Note that the time specified should be long enough to allow the Access Control engine to receive a response from the RADIUS server.

NOTE: Although this option allows a maximum of 60 seconds, the actual maximum time allowed varies depending on the switch model. If a switch does not support the timeout value specified here, then the value is not set on the switch and an error message displays in the Access Control engine log. Check your switch documentation to verify supported values.

RADIUS Timeout Retry Count

The number of times the switch attempts to contact an Access Control engine with a RADIUS request, when an attempted contact fails. The default setting is 3 retries, which means that the switch retries a timed-out request three times, making a total of four attempts to contact the engine.

Use Primary RADIUS Server for Redundancy in Single Access Control Engine Configuration

If your Access Control deployment has only one Access Control Gateway engine, this option allows you to configure redundancy by using the primary RADIUS server as a backup when configuring the switches. This option would not apply to Access Control deployments using advanced AAA configurations with more than one set of RADIUS servers, or if you have configured primary and secondary Access Control Gateways.

Web Service Credentials

Access Control Engine Web Service Credentials

The credentials specified here provide access to the Access Control engine administration web page and the web services interface between the Extreme Management Center server and the Access Control engine. NAC Manager provides default credentials that can be changed, if desired. Changes to the credentials are propagated to the Access Control engines on Enforce.

Access Control Admin Web Page

By default, the Access Control engine administration web page (<https://<Access ControlEngineIP>:8444/Admin/>) uses the above Web Service Credentials for authentication. However, you can configure the web page to use the AAA Configuration assigned to that engine for authentication as well. This allows you to use LDAP or RADIUS authentication for the web page.

There are three steps for setting up the web page to use LDAP or RADIUS authentication:

1. Verify that the Access Control Configuration assigned to the engine has LDAP or RADIUS authentication configured in its AAA Configuration.
2. Create a local user account on the Access Control engine that matches the user name of the user logging in. Use the `useradd` command on the Access Control engine CLI to create the local user account.
3. Select the **Use Access Control AAA Configuration for Admin Web Page authentication** option here on the Credentials tab. Click **OK**. Enforce the change to the engine.

The Access Control engine begins using the AAA configuration for the administration web page authentication. Note that it may take the Linux operating system on the Access Control engine up to two minutes to recognize that the new user is valid.

EAP-TLS Configuration

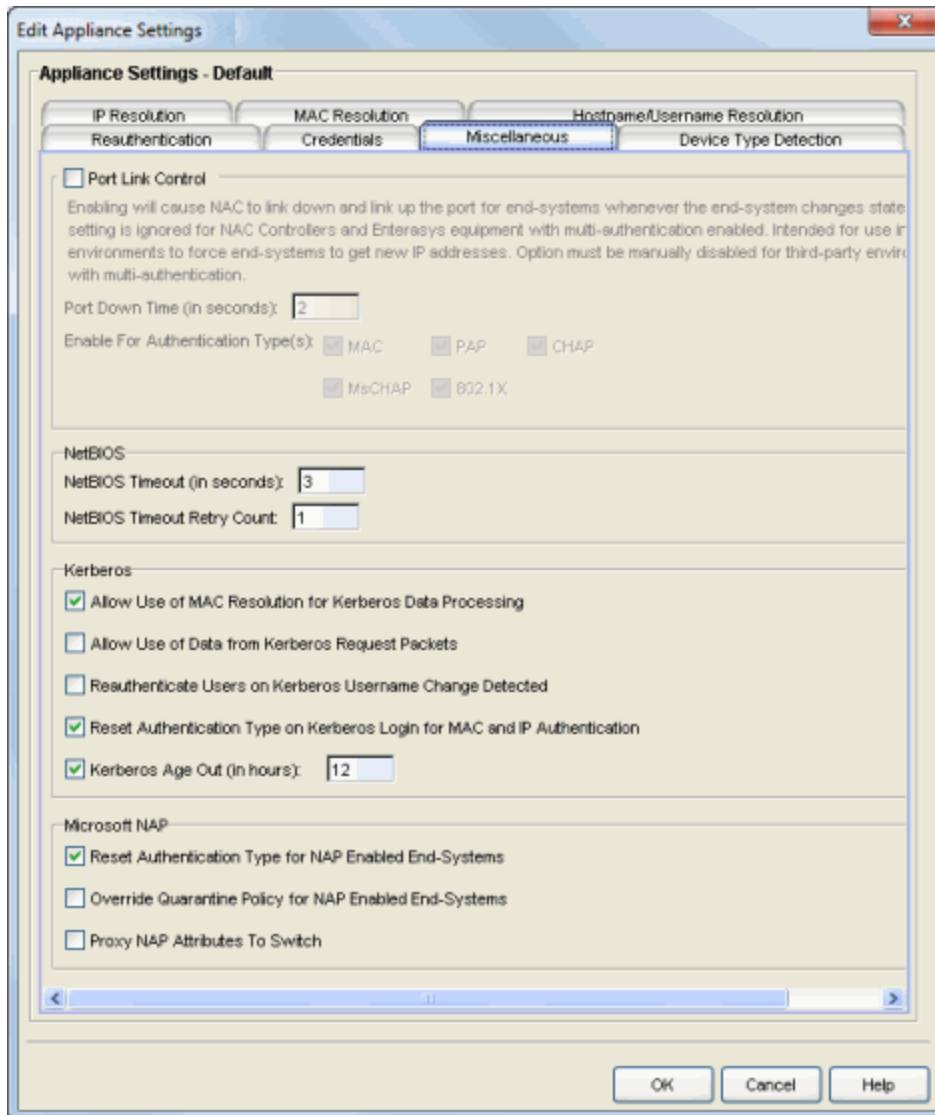
Server Private Key Passphrase

The Server Private Key Passphrase is used to encrypt the private key created during certificate request generation of server certificates for use by Access Control engines during Local EAP-TLS Authentication. The passphrase must be identical for all Access Control engines, and must be

configured properly, or Local EAP-TLS Authentication does not operate successfully.

Miscellaneous Tab

Use this tab to configure various parameters for your network engines including port link control, NetBIOS, Kerberos, and Microsoft NAP.



Port Link Control

Enable Port Link Control

Use this checkbox to enable or disable port link control. Port link control is required if you are using VLAN only (RFC 3580) switches or if you are

using policy with VLANs on EOS policy-enabled switches. When a VLAN is assigned to a switch port, the end-system needs to get a new IP address for the assigned VLAN. To do this, the Extreme Access Control (Access Control) engine links down the port, waits the configured amount of time, and then links up the port, causing the end-system to make a new DHCP request and get a new IP address.

Be aware that when multiple devices are connected to a switch port where authentication is enabled (such as an IP phone cascaded with a PC on a single port), port link down disconnects all devices. In this scenario, you may want to disable port link control, set the Access Control profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address pools that correspond to the VLAN(s) associated to the Quarantine and Assessment access policies to a low value (e.g. 1 minute).

This setting is ignored for Access Control Controllers and EOS equipment with multi-authentication enabled. The option must be manually disabled for third-party environments with multi-authentication.

In the **Port Down Time** field, enter the amount of time in seconds that the engine waits before linking up the port. The time must be sufficient to cause the end-system to make the DHCP request.

In the **Enable for Authentication Types** field, you can enable port link control for only specific authentication types, depending on the checkboxes you select. For example, you can disable port link control for 802.1x, but have it enabled for MAC authentication so that a port is only linked down when a MAC authentication session changes VLANs.

NetBIOS

This section controls the timeout and retries that a Access Control engine uses when making NetBIOS requests for IP resolution, MAC resolution, or hostname resolution.

NetBIOS Timeout

The amount of time in seconds that a Access Control engine waits for a response to a NetBIOS request to an end-system, before giving up on that request and retrying.

NetBIOS Timeout Retry Count

The number of times a Access Control engine retries making a NetBIOS request to an end-system, if the end-system does not respond.

Kerberos

Controls how a Access Control engine deals with data it receives from Kerberos snooping.

Allow Use of MAC Resolution for Kerberos Data Processing

When end-systems are behind a router, the Access Control engine uses MAC resolution to resolve an end-system's MAC address from its IP address. This is because when end-systems are behind a router (not in the local network), the Kerberos packets carry the MAC address of the router instead of the end-system. This option allows you to turn off the use of MAC resolution for Kerberos processing, if desired.

Allow Use of Data from Kerberos Request Packets

This option allows the use of data such as username and hostname, from Kerberos request packets. The data in the request packet is provided by the user, and is not guaranteed to be accurate, since it is not authenticated.

Reauthenticate Users on Kerberos Username Change Detected

This option causes the Access Control engine to reauthenticate a user if the username in the Kerberos packet changes.

Reset Authentication Type on Kerberos Login for MAC and IP Authentication

This option is supported for Access Control deployments with inline Access Control Controllers that can capture the end user login. When a user logs in via Kerberos, (for example, a user logs into a Windows domain,) the Access Control Controller resets the authentication type from MAC (for an L2 Access Control Controller) or IP (for an L3 Access Control Controller) to Kerberos. The Kerberos authentication type can then be used by rules to give elevated access to users that have successfully logged into a Windows domain.

Kerberos Age Out

This option provides a way to disable the aging out of Kerberos authentication data. This authentication data is used by NAC Manager to provide elevated access to end-systems. By default, the authentication data is automatically aged out every 12 hours. During that 12-hour period, any time the end-system reauthenticates with NAC Manager, the user would receive their elevated access privileges. After the 12 hours is exceeded and the authentication data is aged out, the end-system must log in again to get their elevated access. You can use this option to change the age out time or disable the aging altogether. For example, you might want to change the 12 hours to 8 hours, based on a shorter 8-hour workday.

WARNING: Keep in mind that disabling the age out would create a potential security hole. Elevated access is tied to the end-system, so if it isn't aged out, the elevated access is always available. For example, if a user leaves their laptop and someone logs them out and then logs in as a local user, that person continues to have the elevated access privileges of the original user. Also, a person could spoof someone else's MAC address and receive their elevated access, if the access isn't aged out.

Microsoft NAP

This section provides options related to Microsoft NAP for Windows.

Reset Authentication Type for NAP Enabled End-Systems

When this option is enabled, the Access Control engine resets the authentication type from 802.1x to MS NAP (Microsoft NAP), if the end-system authenticating is NAP-enabled (Windows XP SP2 or higher) and the 802.1x authentication request was proxied to a NAP-enabled server. The MS NAP (Microsoft NAP) authentication type can then be used by rules to assign a different Access Control profile. To configure NAC Manager to perform as it did in NAC Manager version 3.1.x, you can create a rule that maps the MS NAP (Microsoft NAP) authentication type to the Pass Through Access Control Profile. With this profile, NAC Manager does not assess the end-system, and uses the NAP determination of whether or not to quarantine a user.

Override Quarantine Policy for NAP Enabled End-Systems

This option allows NAC Manager to replace the quarantine policy for NAP-enabled end-systems, using the quarantine policy defined in the profile's Use Quarantine Policy field. Be aware that when this NAP option is enabled, the Use Quarantine Policy checkbox becomes active for all Access Control profiles, even if assessment is disabled. However, you can deselect the checkbox for an individual profile, in which case the policy from the RADIUS attributes is applied.

Proxy NAP Attributes to Switch

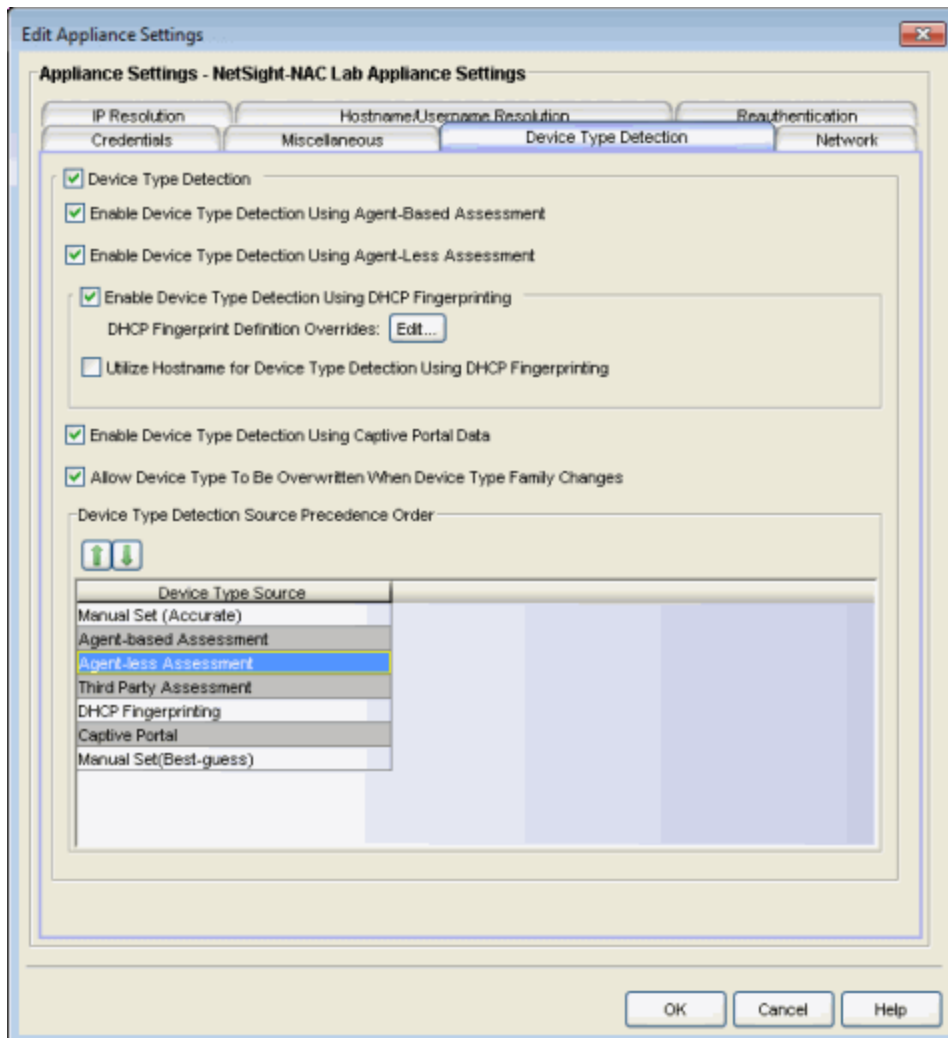
This option is disabled by default. When disabled, the following attributes are **not** proxied to the switch if they are present in the response from the backend RADIUS server:

- MS-Machine-Name
- MS-Extended-Quarantine-State
- MS-RNAP-Not-Quarantine-Capable
- MS-Quarantine-State

If the option is enabled, the attributes are proxied to the switch.

Device Type Detection Tab

The device type detection settings are advanced settings with complex requirements. Before editing these mappings, contact your Extreme Networks representative or Extreme Networks Support for information and assistance.



Device Type Detection

When the device type detection option is selected, NAC Manager determines the end-system's device type using the selected detection methods below. Device type can be an operating system family, an operating system, or a hardware type, such as a printer or a smartphone. NAC Manager uses the selected methods in the order configured in the [detection source precedence](#). When this option is deselected, all device type detection functionality on the Access Control engine is disabled.

Enable Device Type Detection Using Agent-Based Assessment

This option causes the Access Control engine to query connected agents for the end-system device type. This is the most accurate method of device type detection.

Enable Device Type Detection Using Agent-less Assessment

This option allows the Access Control engine to use the results of an agent-less scan to determine the end-system's device type.

Enable Device Type Detection Using DHCP Fingerprinting

This option enables passive device type detection by fingerprinting DHCP packets snooped from an end-system. The **Edit** button can be used to change the mapping of the DHCP packet properties to map to a different operating system or physical hardware type.

Utilize Hostname for Device Type Detection Using DHCP Fingerprinting

This option allows the end-system hostname to be used to fine-tune device type detection results using DHCP fingerprinting. With certain device types, if DHCP fingerprinting does not result in a unique device type match, the hostname can be used as one possible tie-breaker. For example, with Apple iOS devices, the hostname can be a good indicator of the device type.

Enable Device Type Detection Using Captive Portal Data

This option allows the Access Control engine to detect the end-system's device type by using the agent string returned from the end-system's browser. This is the least secure method for device type detection, since it can be faked by the end-system. However, this option should be enabled if you have configured agent-based assessment with the "Allow Agent Unreachable for Unsupported Operating Systems" option enabled, so that the operating system can be detected when the end-system gets the Remediation web page when it is quarantined.

Allow Device Type to be Overwritten When Device Type Family Changes

This option allows the device type to be changed by a lower precedence detection method, if the device type family has changed. This option is required if you are supporting dual boot systems and have configured agent-based assessment with the "Allow Agent Unreachable for Unsupported Operating Systems" option enabled. For example, let's say Microsoft Windows XP SP3 was detected by an agent running on a dual boot end-system. If the system is rebooted and switched to Red Hat Linux 4.4, and the end-system is quarantined for not running the agent, the device type detection using captive portal data (a lower precedence

method) would yield the device type family of Linux instead of Windows. The device type would be updated and would now pass the unsupported operating system test, and be allowed onto the network.

Device Type Detection Source Precedence Order

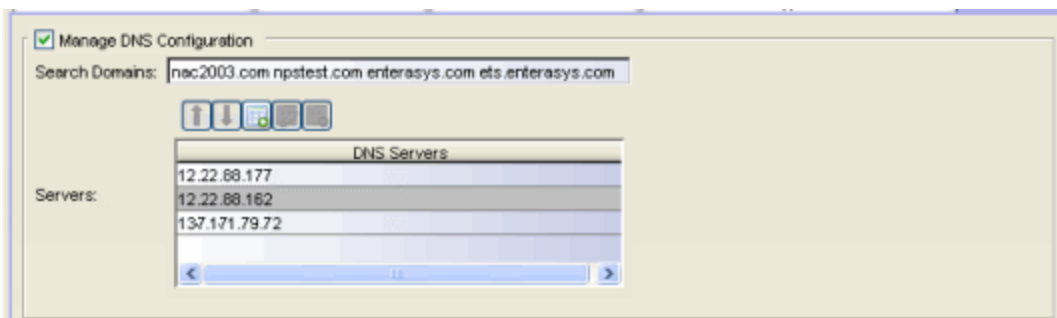
This list specifies the precedence for the source of information used to determine end-system device type, with the highest precedence listed first. Select an item in the list and use the Move Up and Move Down arrows to change its position in the list. Manual Set refers to device type information that has been hard-coded via Extreme Management Center Web Services. Typically, Manual Set (Accurate) has the highest precedence because the exact device type is known and the remaining sources of detection aren't needed, while Manual Set (Best-Guess) has the lowest precedence because it is a best-guess of the device type and should be used only when the other detection methods cannot provide a device type.

Network Tab

Use this tab to configure the following network services for the Extreme Access Control (Access Control) engine: DNS, NTP, SSH, and SNMP.

Manage DNS Configuration

Select the Manage DNS Configuration checkbox and enter a list of search domains and DNS servers.



Search Domains

A list of search domains used by the Access Control engine when doing lookups by hostname. When an attempt to resolve a hostname is made, these domain suffixes are appended to the hostname of the device. For example, if someone does a ping to server1, NAC Manager appends the search domains in an attempt to resolve the name: server1.domain1 server1.domain2, and so on.

DNS Servers

A list of DNS servers the Access Control engine sends DNS lookups to for name resolution. The list is used by both hostname resolution and by the DNS proxy. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage NTP Configuration

NTP (Network Time Protocol) configuration is important for protocols such as SNMPv3 and RFC3576 which incorporate playback protection. In addition, having accurate time configured on the Access Control engine is essential for event logging and troubleshooting. Select the Manage NTP Configuration checkbox, specify the appropriate time zone, and create a list of NTP servers.

NTP Servers	
139.191.79.190	
139.191.79.191	

Time Zone

Select the appropriate time zone. This allows NAC Manager to manage all date/time settings.

NTP Servers

A list of NTP servers. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage SSH Configuration

SSH configuration provides additional security features for the Access Control engine. Select the Manage SSH Configuration checkbox and provide the following SSH information.

The screenshot shows the 'New/Edit Engine Settings Window' with the following configuration options:

- Manage SSH Configuration
 - Port:
 - Disable Remote root Access
- RADIUS Authentication
 - Primary RADIUS Server:
 - Backup RADIUS Server:

Below the configuration options is a toolbar with three icons (add, delete, refresh) and a table of authorized users:

Username	Type	Administrative User
smith	RADIUS	no
superuser	Local	yes
reguser	Local	no

Port

The port field allows you to configure a custom port to be used when launching SSH to the engine. The standard default port number is 22.

Disable Remote root Access

Select this option to disable remote root access via SSH to the engine and force a user to first log in with a real user account and then su to root (or use sudo) to perform an action. When remote root access is allowed, there is no way to determine who is accessing the engine. With remote root access disabled, the `/var/log/message` file displays users who log in and su to root. The log messages look like these two examples:

```
sshd[19735]: Accepted password for <username> from
10.20.30.40 port 36777 ssh2
su[19762]: + pts/2 <username>-root
```

Enabling this option does not disable root access via the console. Do not disable root access unless you have configured RADIUS authentication or this disables remote access to the Access Control engine.

RADIUS Authentication

This option lets you specify a centralized RADIUS server to manage user login credentials for users that are authorized to log into the engine using SSH. Select a primary and backup RADIUS server to use, and use the table below to create a list of authorized RADIUS users.

Authorized Users Table

Use the toolbar buttons to create a list of users allowed to log in to the Access Control engine using SSH. You can add Local and RADIUS users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that only a root user would be able to run. For example, some commands that require

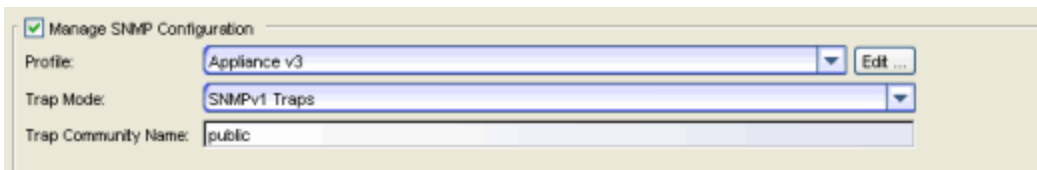
administrative rights to run would be:

```
sudo nacctl restart
sudo reboot
sudo nacdb
```

If a user is not granted administrative rights, they can log in, view files, and run some commands such a ping and ls.

SNMP Configuration

The SNMP configuration section allows you to deploy SNMP credentials for the Access Control engine. The credentials can include different read/write credentials, for example, the read credential can be "public" and the write credential can be "private". In addition, basic host traps can be enabled from the Access Control engine. Select the Manage SNMP Configuration checkbox and provide the following SSH information.



Profile

Use the drop-down menu to select a device access profile to use for the Access Control engine. Click the **Edit** button to open the in the Authorization/Device Access tool where you can create or edit a profile.

Trap Mode

Set the trap mode.

Trap Community Name


Supply the trap community name.

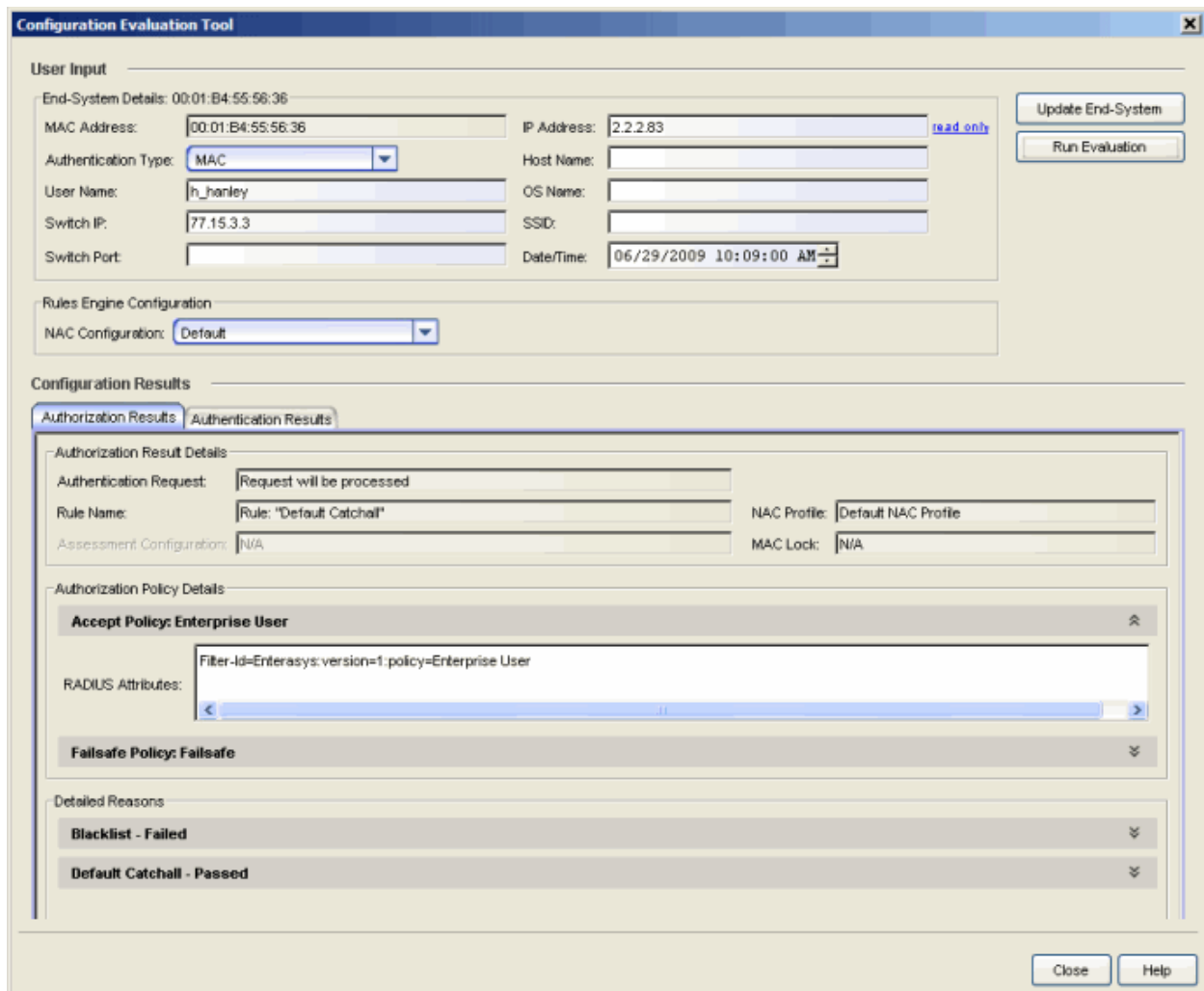
Related Information

For information on related windows:

- [Appliance Settings Panel](#)

Configuration Evaluation Tool

This tool is used to test the rules defined in your NAC Configuration in order to determine what behavior an end-system encounters when it is authenticated on a Extreme Access Control engine. To access this window, click the **Tools and Display Settings** button  above the Rules List in the [Edit NAC Configuration window](#), or right-click on an end-system in the [End-Systems tab](#), and select **Run Configuration Evaluation Tool** from the menu.



Configuration Evaluation Tool

User Input

End-System Details: 00:01:B4:55:56:36

MAC Address:	00:01:B4:55:56:36	IP Address:	2.2.2.83 <small>read only</small>
Authentication Type:	MAC	Host Name:	
User Name:	h_hanley	OS Name:	
Switch IP:	77.15.3.3	SSID:	
Switch Port:		Date/Time:	06/29/2009 10:09:00 AM

Update End-System
Run Evaluation

Rules Engine Configuration

NAC Configuration: Default

Configuration Results

Authorization Results | Authentication Results

Authorization Result Details

Authentication Request:	Request will be processed		
Rule Name:	Rule: "Default Catchall"	NAC Profile:	Default NAC Profile
Assessment Configuration:	N/A	MAC Lock:	N/A

Authorization Policy Details

Accept Policy: Enterprise User

RADIUS Attributes: Filter-Id=Enterasys; version=1; policy=Enterprise User

Failsafe Policy: Failsafe

Detailed Reasons

- Blacklist - Failed
- Default Catchall - Passed

Close Help

User Input

Use this section to configure the end-system data and select the NAC Configuration the evaluation. If you launch the window from the End-Systems tab, the End-System Details section pre-populates with the data from the selected end-system. You can change the data by using the **Edit** link in the upper-right corner of the section. The **Update End-System** button retrieves the most recent data from the end-system, if updated in NAC Manager.

Configuration Results

This section displays how the end-system is authenticated, assessed, and authorized according to the parameters and rules of the selected NAC Configuration. Note that the results does not factor in any RADIUS user attributes since the user's RADIUS request is not present at the time the evaluation is performed.

Authorization Results Tab

Authorization Result Details

- Authentication Request - Displays whether the Extreme Access Control engine processes the request, or reject the request based on a MAC Lock or a rule that assigns a NAC Profile configured to reject the user.
- Rule Name - The name of the rule that the end-system passed.
- NAC Profile - The NAC Profile assigned to the end-system by the rule.
- Assessment Configuration - The assessment configuration used by the NAC Profile, if any.
- MAC Lock - The MAC Lock assigned to the end-system, if any.

Authorization Policy Details

This section displays the RADIUS response attributes returned for end-systems in specific states. Possible states are Accept, Quarantine, Assessing, and Failsafe. Expand each state to view the RADIUS attributes. These are the RADIUS attributes returned for the switch IP that is listed in the End-System Details section.

Detailed Reasons

This section lists all the rules from the NAC Configuration that were evaluated during the end-system authentication. Rules are only evaluated

until one of them is passed. Each rule listing can be expanded to view why the end-system passed or failed that rule.

Authentication Results Tab

This tab displays which set of RADIUS servers and LDAP servers an end-system request would be processed by.

Authentication Result Details

- Rule Name - A description of the authentication type and user name expression used for the AAA entry that the Extreme Access Control engine uses to authenticate the end-system. For a Basic AAA Configuration, this is always: Authentication: Any, User Pattern "*".
- Authentication - For MAC authentication requests, this field displays whether the request is authenticated locally or proxied to the RADIUS server.
- LDAP Configuration - The LDAP configuration used to obtain any LDAP data for the end-system, if applicable.

Authentication RADIUS Server Details

This section lists the IP address, port, shared secret, timeout, and retries listed for all the RADIUS servers that can be used to authenticate the end-system request, if it needs to be proxied.

Detailed Reasons

This section is only applicable for an Advanced AAA Configuration. It lists why a request passed or failed the definition of each AAA entry.




Related Information

For information on related windows:

- [Edit NAC Configuration window](#)
- [End-Systems Tab](#)

Create NAC Appliance Window

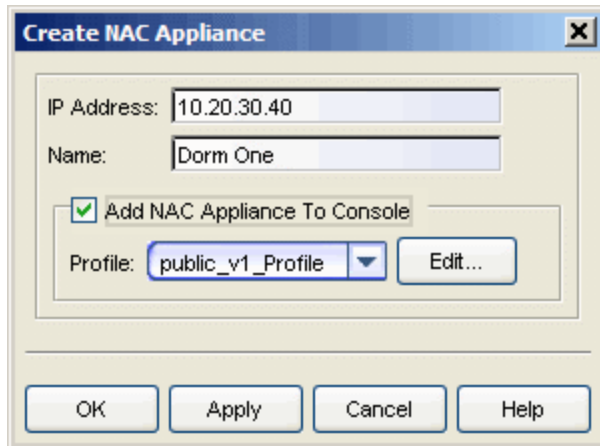
Use this window to add an Extreme Access Control engine to NAC Manager. When you add an engine, it is added to the All NAC Appliances folder in the left-panel tree. Engine icons listed in the tree display status arrows:

-  green up arrow - the engine is up and communicating with the Extreme Management Center (Management Center) server.
-  red down arrow - the engine is down and/or not communicating with the Management Center server.
-  orange up arrow - the orange arrow can mean one or more of the following:
 - the engine is up, but has lost communication with the Management Center server.
 - the engine version is not supported.
 - the engine is configured with the wrong management server.
 - the virtual engine is not licensed.

TIP: For assistance in diagnosing communication problems between an engine and the Management Center server, launch the engine's administration web page by right-clicking on the Access Control engine in the left-panel tree and selecting [WebView](#). On the administration web page, expand the Diagnostics folder in the left-panel tree, and select the Communication Diagnostics report to view communication status information and access diagnostic tools.

You can access this window by right-clicking the All NAC Appliances folder and selecting **Create NAC Appliances** from the menu, or by selecting the folder and clicking the **Create Appliance** button in the right-panel NAC Appliances tab.

NOTE: If you are adding an Access Control virtual engine, you need to provide an Access Control virtual engine license once it is communicating with the Management Center server.



IP Address

Enter the IP address of the engine you want to add.

Name

Enter a name for the engine. This name displays in the left-panel tree to help you identify the engine.

Add NAC Appliance to Console

Select this checkbox if you want to add the engine to the Console database so it displays in the Console tree. Use the drop-down menu to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.

Edit Button

Opens the Authentication/Device Access window where you can define SNMP profiles and credentials for your network devices.

Related Information


For information on related tabs:

- [NAC Appliances Tab](#)

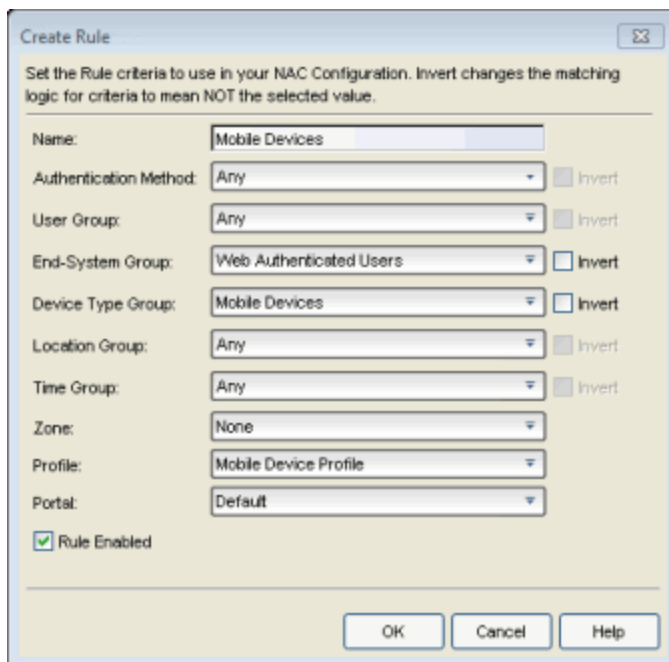
Create/Edit Rule Window

Use this window to add a new rule or edit an existing rule in a NAC configuration. End-systems that match the criteria selected for the rule are assigned the specified NAC profile.

To access this window:

1. Click the NAC Manager  toolbar button to open the NAC Configuration window.
2. In the left-panel tree, select the **Rules** icon. A table of rules for the NAC configuration displays in the right panel.
3. Click the **Add New Rule** button in the table toolbar to open the Create Rule window.
or
Select a rule in the table and click the **Edit Rule** button in the toolbar to open the Edit Rule window.

The image below shows a rule created to provide a different NAC profile for authenticated registered users on mobile devices. Descriptions of the different fields and options in the window are provided below.



Create Rule ✖

Set the Rule criteria to use in your NAC Configuration. Invert changes the matching logic for criteria to mean NOT the selected value.

Name:

Authentication Method: Invert

User Group: Invert

End-System Group: Invert

Device Type Group: Invert

Location Group: Invert

Time Group: Invert

Zone:

Profile:

Portal:

Rule Enabled

Name

Enter a name for a new rule or change the name of an existing rule, if desired.

NOTES: For the following rule criteria:

- If you select **Any**, then NAC Manager ignores the criteria during the rule match process.
 - If you select the **Invert** checkbox, NAC Manager considers the criteria a rule match if the end-system does **not** match the selected value.
-

Authentication Method

Select the authentication method that end-systems must match for this rule.

NOTE: For the following rule criteria, use the drop-down menu to select a value, add a new value, or edit an existing value. You can also use the Advanced Configuration view to edit Rule Components (device type, end-system, user, location, and time groups) by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the Rule Components folder.

User Group

Select the user group that the end user must be a member of to match this rule.

End-System Group

Select the end-system group that the end-system must be a member of to match this rule.

Device Type Group

Select the device type group that the end-system must be a member of to match this rule.

Location Group

Select the network location (switch and interface) that the end-system must originate from to match this rule.

Time Group

Select a time frame that the connection request must match for this rule.

Zone

You only see this field if you have displayed the Zone column in the NAC Configuration Rules table. Select the end-system zone assigned to any end-system matching this rule. See [End-System Zones](#) for more information.

Profile

Select the NAC profile assigned to any end-system matching this rule.

Portal

Select the portal configuration presented to any end-system matching this rule.

Rule Enabled

Select this checkbox to enable this rule in the NAC configuration.

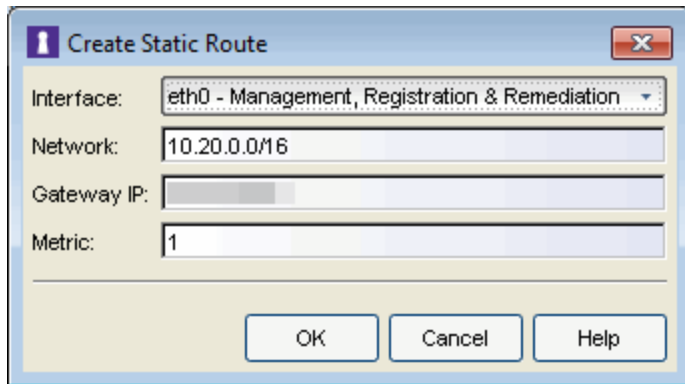
Related Information

For information on related windows:

- [NAC Configuration](#)

Create/Edit Static Route Window

Use this window to create or edit the static routes used for advanced routing configuration. This window is accessed from the toolbar buttons in the [Static Route Configuration window](#).



Interface

Select the Extreme Access Control engine interface used for the static route.

Network

Enter the IP address for the subnet or individual device whose traffic is assigned to the route. You can use the following formats:

- An IP address followed by the CIDR notation for a Class B subnet. For example, 10.20.0.0/16.
- An IP address followed by the full notation for a Class B subnet. For example, 10.20.0.0/255.255.0.0
- An IP address for a single device. If you enter an IP address without a notation, NAC Manager assumes it is a host IP address and assigns it a 32-bit mask.

Gateway IP

The IP address of the device where traffic matching the Network value is sent.

Metric

A number used to configure route precedence. The lower the number, the higher the precedence.

Create Virtual and Physical Network Configuration Window

If your network uses the Extreme Networks Data Center Manager product, you can use this window to create new virtual and physical network configurations. You can launch this window from the [Manage Data Center Fabric window](#).

The information you enter in this window is used to automatically create the following configuration components:

- **Policy Manager Role.** A role is created in Policy Manager within the appropriate domains (based on the switches associated with the NAC Configuration and the Policy Manager domains to which the switches belong) using the specified group name as the role name. Policy Manager verifies a VLAN exists and if necessary, it creates it using the specified VLAN ID. Forward is set as tagged/untagged for the VLAN according to the checkbox value.
- **Policy/VLAN mapping.** A new policy mapping is created using the specified group name, and the policy role and VLAN information.
- **NAC profile.** A NAC profile is created using the specified group name and the new access policy.
- **NAC End-System Group.** A new MAC end-system group is created using the specified group name. The settings configured in this window are saved in the new end-system group's description.
- **NAC Rule.** A new rule is created using the specified group name and the new MAC end-system group.

For more information and example configuration scenarios, see the NMS Data Center Manager User Guide (version 9034586-02), section 4.1, DCM Configuration in NAC Manager, available on the Network Management Suite (NMS) Documentation web page:<https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx>.

Create Virtual and Physical Network Configuration Window

Create Virtual and Physical Network Configuration

Using the Group Name, create an End-System Group, NAC Rule, NAC Profile, Policy Mapping, and the portgroup in the vSwitch if it does not exist.

Group Name: Mail Servers

Private VLAN: VLAN Type: promiscuous

Primary VLAN ID: 56 Secondary VLAN ID:

Forward as Tagged:

VMware vSwitch Group: None

XenServer Network Interface Card:

Enable vSwitch Configuration Synchronization

Enable Virtual Machine Approval Workflow

OK Cancel Help

Edit Action Overrides Window

This window lets you override the default content contained in a notification action message. For example, if you are creating an email notification action, you can customize the information contained in the email subject line and body. If you are creating a syslog or trap notification action, you can specify certain information you want contained in the syslog or trap message.

The default content that appears in the window (as shown below) is defined in the NAC Manager [Notification Engine options](#) (Tools > Options). Any overrides you define here only affects the specific notification action that you are editing.

The message content is configured as a template, with the content passed directly as typed, except for the variable information which is specified by \$keyword. The variable information (\$keyword) is replaced with information from the notification when the notification action is executed. See below for a list of available keywords, along with their definitions.

The Custom Arguments field is used to specify the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as \$keyword. A group of literals and variables can be combined into a single argument by using double quotes. The value "all" is a special value that tells Extreme Management Center to pass all variable values to the program as individual arguments.

To access this window, select the Override Content checkbox in the [Edit Notification Action window](#) and click the **Edit Content** button.

Keyword Definitions

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. These \$keywords are replaced with information from the notification when the notification action is executed.

Following is a list of available keywords for NAC Manager notifications, along with the value the returned keyword. The keywords are organized according to the notification type they pertain to (End-System, Registration, Health Result, User Group, or End-System Group), and can only be used when that specific type of notification action is being edited. The Default keywords can be used with any notification type.

Keyword	Returned Value
Default Keywords	
\$type	The notification type .
\$trigger	The notification trigger .
\$conditions	A list of the conditions specified in the notification action.
\$server	The Extreme Management Center server IP address.
End-System Keywords	
\$macAddress	The end-system's current MAC address.
\$oldmacAddress	The end-system's previous MAC address.

Keyword	Returned Value
\$ipAddress	The end-system's current IP address.
\$oldipAddress	The end-system's previous IP address.
\$username	The current username used to authenticate the end-system.
\$oldusername	The previous username used to authenticate the end-system.
\$hostname	The end-system's hostname.
\$oldhostName	The end-system's previous hostname.
\$operatingSystemName	The full operating system running on the end-system.
\$oldoperatingSystemName	The previous full operating system the end-system was running.
\$ESType	The end-system's current operating system family (for example, Windows, Mac, or Linux).
\$oldESType	The end-system's previous operating system family (for example, Windows, Mac, or Linux).
\$state	The end-system's current state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
\$oldstate	The end-system's previous state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
\$stateDescr	A description of the end-system's current state.
\$oldstateDescr	A description of the end-system's previous state.
\$extendedState	An extended description of the end-system's current state.
\$oldextendedState	An extended description of the end-system's previous state.
\$switchIP	The IP address of the switch the end-system is currently connected to.
\$oldswitchIP	The IP address of the switch the end-system was previously connected to.
\$switchLocation	The physical location of the switch the end-system is currently connected to (for example, the building/floor location).
\$oldswitchLocation	The physical location of the switch the end-system was previously connected to (for example, the building/floor location).

Keyword	Returned Value
\$switchPort	The ifIndex of the switch port the end-system is currently connected to.
\$oldswitchPort	The ifIndex of the switch port the end-system was previously connected to.
\$switchPortId	The name of the switch port the end-system is currently connected to (for example, ge.1.1).
\$oldswitchPortId	The name of the switch port the end-system was previously connected (for example, ge.1.1).
\$authType	The latest authentication method used by the end-system to connect to the network.
\$oldauthType	The previous authentication method used by the end-system to connect to the network.
\$allAuthTypes	A comma-separated list of authentication types currently used for this end-system in its current location. The list is only provided if there is more than one authentication type.
\$oldallauthTypes	A comma-separated list of authentication types previously used for this end-system in its current location. The list is only provided if there is more than one authentication type.
\$nacProfileName	The NAC profile currently assigned to the end-system.
\$oldnacProfileName	The NAC profile previously assigned to the end-system.
\$reason	The reasons why the end-system is assigned its current NAC profile or is in a particular state.
\$oldreason	The reasons why the end-system was assigned its previous NAC profile or is in a particular state.
\$policy	The access policy currently assigned to the end-system, if on a policy-based switch.
\$oldpolicy	The access policy previously assigned to the end-system, if on a policy-based switch.
\$firstSeentime	The first time the end-system was seen by the Extreme Access Control (Access Control) engine.
\$lastSeenTime	The last time the end-system was seen by the Access Control engine.
\$oldlastSeenTime	The previous last time the end-system was seen by the Access Control engine.
\$nacApplianceIp	The IP address of the Access Control engine on which the end-system authenticated.

Keyword	Returned Value
\$oldnacApplianceIp	The IP address of the previous Access Control engine on which the end-system authenticated.
\$nacapplianceGroupName	The engine group for the Access Control engine where the end-system was last heard.
\$oldnacApplianceGroupName	The previous engine group for the Access Control engine where the end-system was last heard.
\$lastScanTime	The last time a scan was performed on the end-system.
\$lastScanResultState	The resulting state of the last scan: ACCEPT, QUARANTINE, or empty.
\$ssid	The Service Set Identifier (SSID) of the wireless network the end-system is connected to.
\$oldssid	The Service Set Identifier (SSID) of the wireless network the end-system was previously connected to.
\$wirelessAp	The name of the Wireless Access Point (AP) to which the end-system is connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
\$oldwirelessAp	The name of the Wireless Access Point (AP) to which the end-system was previously connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
\$ifAlias	The ifAlias of the switch port to which the end-system is currently connected.
\$oldifAlias	The ifAlias of the switch port to which the end-system was previously connected.
\$ifDescription	The ifDescription of the switch port to which the end-system is currently connected.
\$oldifDescription	The ifDescription of the switch port to which the end-system was previously connected.
\$ifName	The ifName of the switch port to which the end-system is currently connected.
\$oldifName	The ifName of the switch port to which the end-system was previously connected.
\$custom1	The text from the Custom 1 end-system information column.

Keyword	Returned Value
\$custom2	The text from the Custom 2 end-system information column.
\$custom3	The text from the Custom 3 end-system information column.
\$custom4	The text from the Custom 4 end-system information column.
\$regName	The registered username supplied by the end user during the registration process.
\$regEmail	The email address supplied by the end user during the registration process.
\$regPhone	The phone number supplied by the end user during the registration process.
\$regData1	The text from the Custom 1 registration field supplied by the end user during the registration process.
\$regData2	The text from the Custom 2 registration field supplied by the end user during the registration process.
\$regData3	The text from the Custom 3 registration field supplied by the end user during the registration process.
\$regData4	The text from the Custom 4 registration field supplied by the end user during the registration process.
\$regData5	The text from the Custom 5 registration field supplied by the end user during the registration process.
\$regDeviceDescr	The device description supplied by the end user during the registration process.
\$regSponsor	The registered device's sponsor.
\$memberOfGroups	The current list of MAC end-system groups listed in the Groups end-system information column.
\$oldmemberOfGroups	The previous list of MAC end-system groups listed in the Groups end-system information column.
\$groupDescr1	The entry description that was entered when the end-system was added to a MAC-based end-system group.
\$groupDescr2	The entry description that was entered when the end-system was added to a MAC-based end-system group.
\$groupDescr3	The entry description that was entered when the end-system was added to a MAC-based end-system group.
Registration Keywords	

Keyword	Returned Value
\$category	The type of action that was performed, for example: Registered Device Added, Registered Device Updated, Registered User Added; Registered Device Removed, Registered User Removed.
\$time	The time the end-system registered to the network.
\$source	The MAC address of the registered device or the name of the registered user.
\$message	A message describing the action that was performed (for example, Added Registered Device for User: <username> - MacAddress: <MAC address>).
Health Result Keywords	
\$macAddress	The end-system's MAC address.
\$ipAddress	The end-system's IP address.
\$startScanDate	The date and time the scan started.
\$endScanDate	The date and time the scan ended.
\$hostUnreachable	Whether the host was unreachable before or after the scan was run: true or false.
\$testSets	A list of test sets that were run during assessment.
\$totalScore	The total sum of the scores for all the health details for the health result.
\$topScore	The highest score received for a health detail in the health result.
\$riskLevel	The risk level assigned to the end-system based on the health result.
\$riskLevelReason	The reason the health result was placed into the specified risk level.
\$assessmentSummary	A list of all the test cases that were run against the device during assessment.
\$statusDetail	A list of the vulnerabilities that were found during assessment.
\$assessmentServerIpAddress	The IP address of the assessment server that performed the scan.
\$assessmentServerName	The name of the assessment server that performed the scan.
User Group Keywords	
\$name	The name of the user group.

Keyword	Returned Value
\$createdBy	The name of the user that created the user group.
\$creationTime	The time and date the user group was created.
\$description	A description of the user group (if one was defined when the group was created).
\$added	A comma-separated list of user entries that were added to the group during the change.
\$removed	A comma-separated list of user entries that were removed from the group during the change.
\$lastModifiedTime	The last time the user group was modified.
\$oldlastModifiedTime	The previous last time the user group was modified.
\$lastModifiedBy	The name of the user who most recently edited the user group.
\$oldlastModifiedBy	The name of the user who had previously edited the user group.
\$revisionCounter	The current revision count (the number of changes that have been made) for the user group.
\$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the user group.
\$listtype	One of the following types: Username, LDAP User Group, RADIUS User Group.
End-System Group Keywords	
\$name	The name of the end-system group.
\$createdBy	The name of the user that created the end-system group.
\$creationTime	The time and date the end-system group was created.
\$description	A description of the end-system group (if one was defined when the group was created).
\$added	A comma-separated list of end-system entries that were added to the group during the change.
\$removed	A comma-separated list of end-system entries that were removed from the group during the change.
\$lastModifiedTime	The last time the end-system group was modified.
\$oldlastModifiedTime	The previous last time the end-system group was modified.
\$lastModifiedBy	The name of the user who most recently edited the end-system group.

Keyword	Returned Value
\$oldlastModifiedBy	The name of the user who had previously edited the end-system group.
\$revisionCounter	The current revision count (the number of changes that have been made) for the end-system group.
\$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the end-system group.
\$listtype	One of the following types: MAC, IP, Hostname.

Related Information

For information on related windows:

- [Edit Notification Action Window](#)
- [Manage Notifications Window](#)

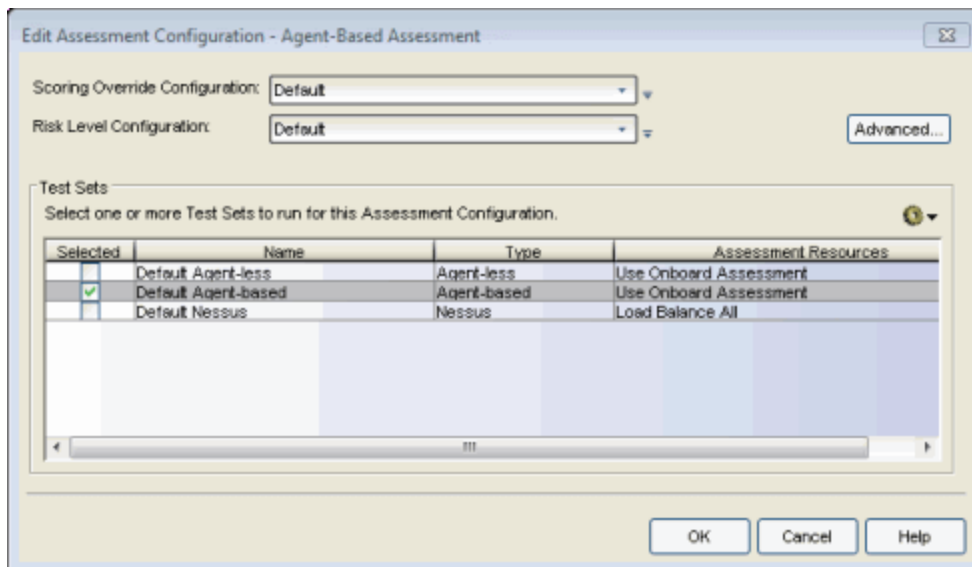
Edit Assessment Configuration Window

This window lets you view and configure the assessment configurations that define the assessment requirements for end-systems. Assessment configurations define the following information:

- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).
- What assessment tests to run (determined by the selected test sets).

Once you have defined your assessment configurations, they are available for selection when creating your NAC configurations.

To access this window, select **Tools > Management and Configuration > Assessment Settings** from the menu bar to open the [Manage Assessment Settings window](#). Select the Assessment Configurations tab. In the tab you can select an existing configuration and click **Edit** to open the Edit Assessment Configuration window, or you can click **Add** to add a new assessment configuration, and then open the Edit Assessment Configuration window.



Scoring Override Configuration

Use the drop-down list to select the scoring override configuration for this assessment configuration. Scoring overrides let you override the scoring mode and test result scores for a particular assessment test. The default scoring override configuration provided by NAC Manager specifies no

overrides, but can be edited to contain overrides, if desired.

 Use the configuration menu button to:

- Edit — Edit the currently selected scoring override configuration.
- Add — Add a new scoring override configuration.
- Create Copy — Create a copy of the currently selected scoring override configuration.
- Used By — Lists all assessment configurations currently using the selected scoring override configuration.
- Manage — Opens the [Manage Scoring Override Configurations window](#) where you can view details about all your scoring override configurations, and add, edit, or delete one or more of the configurations.

Risk Level Configuration

Use the drop-down list to select the risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

 Use the configuration menu button to:

- Edit — Edit the currently selected risk level configuration.
- Add — Add a new risk level configuration.
- Create Copy — Create a copy of the currently selected risk level configuration.
- Used By — Lists all assessment configurations currently using the selected risk level configuration.
- Manage — Opens the [Manage Risk Level Configurations window](#) where you can view details about all your risk level configurations, and add, edit, or delete one or more of the configurations.

Advanced Button

Use the Advanced button to access the [Advanced Assessment Configuration window](#) where you can enable assessment warning periods. Warning periods let you specify a grace period and probation period used for assessment warnings.

- Grace Period — specify the number of days the end user has to resolve the warning issues before the end-system is quarantined.

- Probation Period — The number of days after an end user is quarantined that additional warnings result in immediate quarantine. This allows administrators to block repeat offenders by limiting their access to the network. Once the probation period has passed, the end user can again receive assessment warnings. Setting the probation period to 0 is the same as having no probation period.

Test Sets

Select one or more test sets to run for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

If you select multiple agent-based test sets, the first test set you select is called the Master test set. A Master test set includes the Agent Configuration settings, the Advanced Settings, and all the specified test cases. Each subsequent agent-based test set you select for the configuration is a "supporting" test set. For supporting test sets, only the "Application" test cases are used; all other configuration values are ignored. In the list of Test Sets, Master test sets have a "(Master)" designation after them.

For example, you might want to use multiple agent-based test sets if you are managing multiple networks, and you have a unique agent-based test set for each network as well as secondary test sets for specific application tests that all the networks would use. In the assessment configuration for each network, you would select the unique test set as the Master test set and then select any number of secondary test sets to be included in the configuration as well.

If the Master test set is deselected, then a new master is automatically selected. If this is not the specific test set that you would like to have as Master, then you must deselect all test sets, select the desire Master test set first, and then select the additional supporting test sets.



Use the configuration menu button to:

- Add — Add a new test set:
 - [Agent-based](#)
 - [Agent-less](#)

- [Nessus](#)
 - [Other](#)
 - Edit — Edit the currently selected test set.
 - Create Copy — Create a copy of the currently selected test set.
 - Used By — List all assessment configurations currently using the selected test set.
 - Manage Test Sets — Opens the [Manage Test Sets window](#) where you can view details about all your test sets, and add, edit, or delete one or more of the test sets.
 - Delete — Deletes the currently selected test set.
 - Manage Assessment Server Pools — Opens the [Manage Assessment Server Pools window](#) where you can view and define the assessment server pools to be used by the test sets.
 - Manage Assessment Servers — Opens the [Manage Assessment Servers window](#) where you can view and configure the Assessment servers that perform the end-system assessments in your network.
-

Related Information

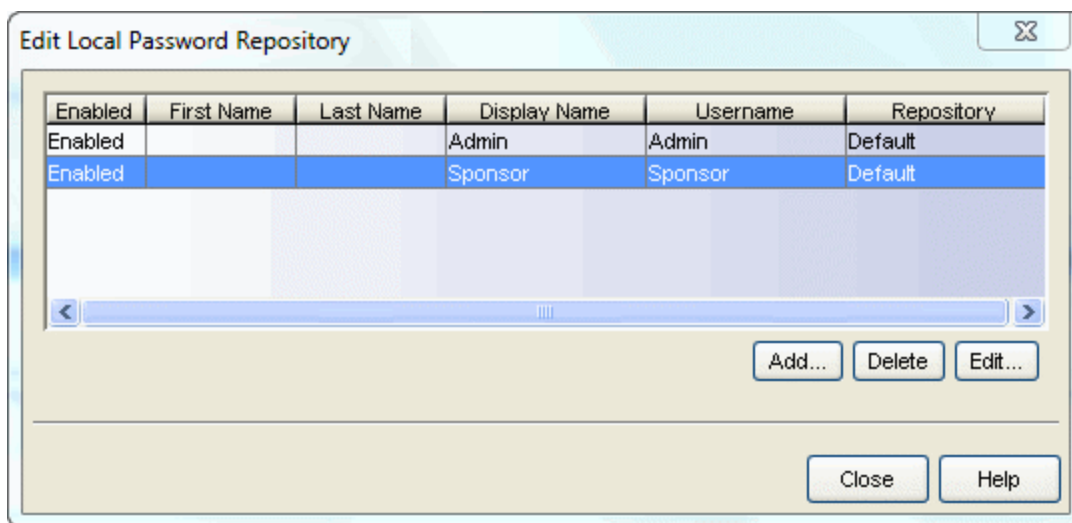
For information on related windows:

- [Manage Assessment Servers Window](#)

Edit Local Password Repository Window

Use this window to edit the user entries in a Local Password Repository. NAC Manager supplies a default repository used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.

You can access this window from the Local Password Repository menu button in the Edit Basic AAA Configuration window.



Enabled

Displays whether the user is enabled or disabled. If a user is disabled, they are not able to log in. This feature is useful if you want to enable a user only at certain times, such as when they are on-site. You can enable or disable a user by editing the user entry (select the entry and click the **Edit** button).

First Name

The user's first name (for administrative information only).

Last Name

The user's last name (for administrative information only).

Display Name

The display name is used on the voucher for pre-registration in the captive portal.

User Name

The user's login user name.

Repository

The name of the Local Password Repository of which the user is a member.

Add Button

Opens the Add User window where you can define a new user and password for the Repository.

Delete Button

Deletes the selected user entry. You cannot delete a user that is referenced by an Administrative Login Configuration (as configured in the Edit Portal Configuration Window > Administration).

Edit Button

Opens the Edit User window where you can edit the selected user entry.

Related Information

For information on related windows:

- [Basic AAA Configuration Window](#)

Edit Notification Action Window

The Edit Notification Action window lets you edit an existing notification or create a new one. In the window you can enable or disable the notification, specify the notification type and trigger, define the required conditions, and configure the actions that occur when the notification is activated. At the bottom of the window you can read a summary description of the notification's properties.

To create a new notification, click the **Add** button in the [Manage Notifications window](#). To edit a notification, select a notification in the Manage Notifications window table and click the **Edit** button.

The screenshot shows the 'Edit Notification Action' window for the notification 'NetSight event Report Blacklisted End-System has been quarantined'. The window is titled 'Edit Notification Action: NetSight event Report Blacklisted End-System has been quarantined' and contains the following sections:

- Enable Notification:**
- Name:** NetSight event Report Blacklisted End-System has been quarantined
- Notes:** Send email when a Blacklisted End-System is quarantined.
- Type:** End-System
- Trigger:** Quarantine
- Conditions:**
 - Appliances: None
 - End-System Group: Blacklist
 - User Group: (empty)
 - Time Group: Default Work Week
 - NAC Profile: Administrator NAC Profile
 - Location Group: (empty)
 - Device Type Group: Android
- Actions:**
 - Email: Helpdesk (with 'Edit Email Lists ...' button)
 - Syslog Server(s): (empty)
 - Trap Server: (empty)
 - Credential: default_snmp_v3
 - Isaac Service: (empty)
 - Program: (empty) (with 'Select ...' button)
 - Working Directory: (empty) (with 'Select ...' button)
 - Override Content: (with 'Edit Content ...' button)
- Result:** Quarantine End-System matches Blacklist Action Send E-Mail to Helpdesk Override Content

Buttons at the bottom: OK, Cancel, Help

Enable Notification

Select the checkbox to enable the notification. When a notification is enabled, then the defined action takes place when the trigger occurs and the conditions are met.

Name

Enter a name for the notification.

Notes

Enter notes for the notification that describe the notification action or other notification details. This information is displayed in the [Manage Notifications window](#).

Type

The notification type defines the source of the event that activates the notification. Use the drop-down menu to select one of the following notification types:

- End-System Group
- End-System
- User Group
- Health Result
- Registration

Trigger

Triggers allow you to determine when a notification action occurs based on filtering for a specific event. Use the drop-down menu to select the event for which you want to filter. The list of triggers changes according to the notification type you have selected. Selecting "Any" or "Any Change" means that no filtering occurs.

- End-System Group - the actions are performed when entries in the group are added or removed. "Any Change" would include added, removed, and modified.
- End-System - the actions are performed based on:
 - an end-system being added, deleted, or moved
 - an end-system state or a state change
 - an authentication type or device type change
 - a custom field change
 - whether the end-system is registered

- an end-system IP address change. An event is generated when an end-system is added with a static IP, the end-system IP changes after IP resolution, or the end-system IP changes due to DHCP rediscover.
- when an end-system is added to a MAC-based end-system group. Note that a notification is not generated if the end-system is already a member of three end-system groups and is added to an additional group, unless the option "Remove from Current Group Assignments" is enabled when the end-system is added to the group.
- certain errors occurring
- User Group - the actions occur when entries in the group are added or removed. "Any Change" would include added, removed, and modified.
- Health Result - the actions occur based on the risk level of a health result.
- Registration - the actions occur when a registered user or device is added, removed, or updated.

Conditions

This section lets you define additional conditions that, in addition to the trigger, determines when actions occur. Conditions can be used to limit the scope of events that trigger a notification action. The list of conditions changes according to the notification type you have selected.

Appliances

Filter end-system notifications based on the engines you select here. Only end-systems being managed by the selected engines trigger the notification actions.

User Group

Select a user group to use as a filter for the User Group notification type. When the end-system is a member of this user group, then the notification actions are performed. If you don't select this checkbox and specify a group, then the notification is sent if any user group is matched.

NAC Profile

End-System events are filtered based on the NAC profile assigned to the end-system. Use the drop-down menu to select the desired profile.

End-System Group

Select an end-system group to use as a filter for the End-System Group notification type. When the end-system is a member of this end-system group, then the notification actions are performed. If you don't select this checkbox and specify a group, then the notification is sent if any end-system group is matched.

Time Group

Specify a time group to use as a filter for the End-System, Health Result, and Registration notification types. When the day and time that the end-system (the source of the event) connects to the network matches the time group, then the notification actions are performed.


Location Group

Specify a location group to use as a filter for the End-System, Health Result, and Registration notification types. When the location where the end-system (the source of the event) connects to the network matches the location group, then the notification actions are performed.

Device Type Group

Specify a device type group to use as a filter for the End-System, Health Result, and Registration notification types. When the end-system's device type matches the device type group, then the notification actions are performed.

Actions

Use the checkboxes to specify the actions you want to take place when a notification is triggered and the conditions are met. You can test a notification by clicking the Test Action button . (A notification must be saved before it can be tested.)

Email

Select this checkbox if you want an email sent if the notification is triggered. Use the drop-down menu to select one of your pre-defined email lists. If no lists have been defined, the menu is empty and you can click the **Edit Email Lists** button to define a list.

Syslog Server(s)

Select this checkbox if you want to create a syslog message if the notification is triggered. Enter the IP address or hostname for each syslog server where the message is sent. Multiple syslog servers can be listed, separated by either a comma or a space.

Trap Server

Select this checkbox if you want to send an SNMP trap if the notification is triggered. Enter the IP address for a trap receiver where the trap is sent. Valid trap receivers are systems running an SNMP Trap Service. From the Credential drop-down menu, select the appropriate SNMP credential used when sending the trap to the trap receiver. Credentials are defined in the **Profiles/Credentials** tab in the Authorization/Device Access window (Tools > Authorization/Device Access).

isaac Service

Select this checkbox if you want to send a message to the isaac service if the notification is triggered. The default notification message is sent, or you can customize the message using the Override Content window. When you create the notification, it is seen as a notification in the Notifications panel in isaac. Then, when the notification is triggered, a message is sent to isaac, and isaac forwards out the notification to alert isaac users.

Program

Select this checkbox to specify a custom program or script run on the Extreme Management Center Server if the notification is triggered. In the Program field, enter the name of the program or use the **Select** button to open a file browser window and choose a program. In the Working Directory field, enter the path to the directory from which to open the program or use the **Select** button to open a file browser window and choose a directory. Any path references within your program that are not absolute paths are relative to the working directory.

Override Content

Select this checkbox if you want to override the default content contained in the action message. The default content is defined in the NAC Manager Notification Engine options (Tools > Options). Use the **Edit Content** button to open the [Edit Action Overrides window](#) where you can change the defaults for this specific notification only.

Result

This section summarizes the notification type, trigger, conditions, and specified actions.

Related Information

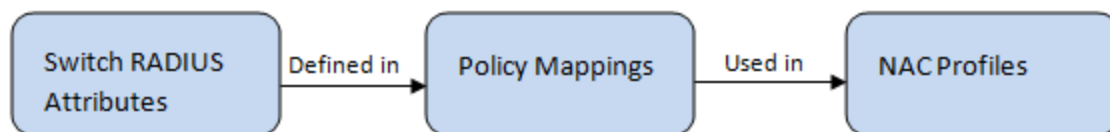
For information on related windows:

- [Manage Notifications Window](#)
- [Edit Action Overrides Window](#)

Edit Policy Mapping Configuration Window

In your NAC profiles, each access policy (Accept, Quarantine, Failsafe, and Assessment) is associated to a *policy mapping* that defines exactly how NAC Manager handles end-system traffic on the network. Each mapping specifies a policy role (created in Policy Manager) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch.

The RADIUS attributes required by a switch are specified in the Gateway RADIUS Attributes to Send field configured in the [Edit Switch window](#). The actual switch RADIUS attribute values (Login-LAT-Port, Custom 1, etc.) are defined within each policy mapping configured in this window. Each policy mapping is associated with the access policy selected in your NAC profiles.



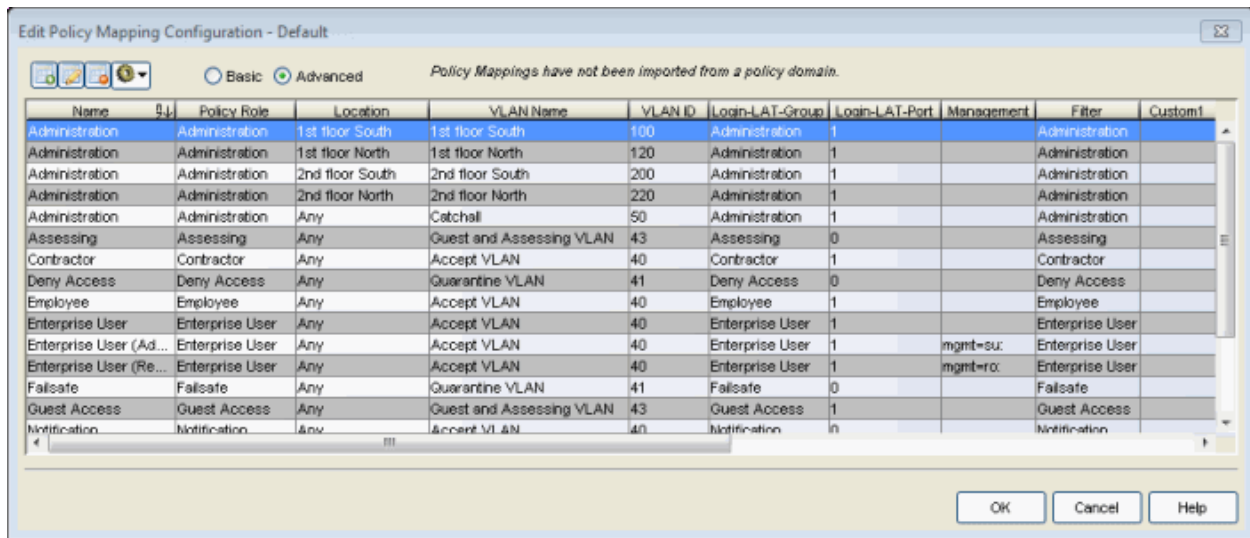
When an end-system authenticates to the network, the NAC profile is applied and the appropriate RADIUS response attributes are extracted from the mapping based on the switch the authentication request originated from. The attributes are returned to the switch in the RADIUS Access-Accept response.


For more information on configuring policy mappings, see [How to Set Up Access Policies and Policy Mappings](#). For a description of each NAC Manager access policy, and some guidelines for creating corresponding policy roles in Policy Manager, see the section on [Access Policies](#) in the Concepts file.


To access this window, click on the **Manage** button in the Policy Mappings section in the [New/Edit NAC Profile window](#). (You can also access your policy mappings in the Advanced Configuration tool by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the NAC Profiles folder and click on the Policy Mappings folder.)

The columns displayed in this window vary depending on whether you are using a Basic or Advanced policy mapping configuration. For a definition of each column, [see below](#).

Advanced Policy Mapping Configuration



NAC Manager provides a list of default policy mappings that you can use, or you can create your own policy mappings, if desired. Use the toolbar buttons  at the top of the window to add, edit, or delete mappings.

Use the configuration menu button  to access options for managing the import and export of mappings.

- Import from File** - Opens a window where you can select a file for importing policy mappings. In the file, policy mappings must be listed one mapping per line using the following format. (Fields in brackets < > are optional; all other fields are required.)

Name, PolicyName, Location, VlanName, VlanId, <LoginLATGRoup>, <LoginLATPort>, <Management>, <Filter>, <Custom1>, <Custom2>, <Custom3>, <Custom4>, <Custom5>

For example: Assessing, Assessing, Any, Default VLAN, 1, Assessing, 0, , Assessing

For an explanation of the different fields, see the [Add Policy Mapping window](#) Help topic.
- Import from Policy Manager Domains** - This operation creates new Policy Mappings in NAC Manager based on policy roles and corresponding VLANs imported from Policy Manager. The import also updates VLAN information for existing policy mappings already in the table. The import removes mappings from NAC Manager if the policy no longer exists in Policy Manager **and** is not being used by NAC Manager (via a NAC profile). If the policy is being used, the policy name is cleared. This results in an error

notification on enforce of the NAC configuration to the Extreme Access Controlengine.

This operation should not be used if policy mapping attributes are being managed outside of Policy Manager. An example would be a scenario in which RFC 3580-capable third-party devices participate in NAC Manager, where default policy mapping names (Enterprise User, Accessing, etc.) have been updated to define VLAN information that is not configured in policy roles of the same name that exist in Policy Manager which is used to configure EOS switches. If this scenario exists, and the duplicate-named policy roles are imported, the imported VLAN information overwrites the existing VLAN information.

- **Export to Policy Manager Domain** - This operation exports the selected policy mappings to a policy domain. It verifies that VLANs in the policy mappings exist in the policy domain. You can select an option to set the VLANs to forward as tagged and existing VLANs are updated. The operation also verifies that policies referenced in NAC Manager exist in the policy domain. Missing policies are added as roles.
- **Clean Up Policies Missing from Policy Manager** - Opens a window that lists any policies not defined in Policy Manager, allowing you to remove mappings or clear policies from NAC Manager if the policy no longer exists in Policy Manager **and** is not being used by NAC Manager in a NAC profile. If the policy is being used in a NAC profile, only the policy name is cleared. Do not select mappings for policies that are being managed outside of Policy Manager, for example, for third-party devices.

Column Definitions

Name

The policy mapping name.

Policy Role

The policy role assigned to this mapping. All policy roles used in your mappings must be part of your Extreme Access Control Controller policy configuration and/or defined in Policy Manager and enforced to the policy-enabled switches in your network.

Location

Policy mapping locations allow authentication requests that match the same NAC rule and corresponding NAC profile to be authorized to different accept attributes (policy/VLAN/Custom Attribute) based on the location the request originated from. For example, in the [Policy Mapping](#)

[Configuration screenshot](#) above, the Administration policy mapping has five entries, with each entry assigning a different VLAN (for RFC 3580-enabled switches) for authentication requests matching the specified location. Requests originating from the 1st floor South location are authorized to VLAN 100, and requests originating from the 2nd floor North location (matching the same NAC rule) are authorized to VLAN 220. Using locations in this manner lets you authorize end-systems to different access criteria using a single NAC rule, whereas the alternative is to create multiple location-based NAC rules each with a NAC Profile that corresponds with the desired access value.

When policy mapping locations are used in this manner, it is important to include a catch-all policy mapping (the fifth Administration mapping in the example above) that has a location of "any" and sets the access behavior for an authorization originating from any other location. The access behavior could be a policy/VLAN/Custom Attribute that grants some form of restricted access, or denies access altogether. If a catch-all mapping is not included, a warning message may appear on enforce indicating that there is no catch-all mapping configured, and authorizations that match the policy but do not originate from a defined location, may result in errors or unpredictable behavior.

VLAN Name

If you have RFC 3580-enabled switches in your network, this column displays the VLAN name assigned to this mapping.

VLAN ID

If you have RFC 3580-enabled switches in your network, this column displays the VLAN ID assigned to this mapping.

Filter

This value is only displayed in Basic mode if ExtremeWireless Controllers have been added to NAC Manager. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Controllers and other switches that support the Filter-Id attribute.

Login-LAT-Group

If your network devices require a Login-LAT-Group, it displays here.

Login-LAT-Port

If you have ExtremeWireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the

authentication is fully authorized. A value of "1" indicates the authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Extreme Access Control engine. This is used in conjunction with the Registration and Assessment features of NAC Manager.

Management

The authorization attribute returned for successful administrative access authentication requests that originate from network equipment configured to use RADIUS as the authentication mechanism for remote management of switches, routers, VPN concentrators, etc. Examples of management values for EOS devices are: "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator is granted when authorized to access the device: superuser, read/write, or read-only.

Custom

Some network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session. These additional attributes can be defined in the five available Custom option fields.

Related Information

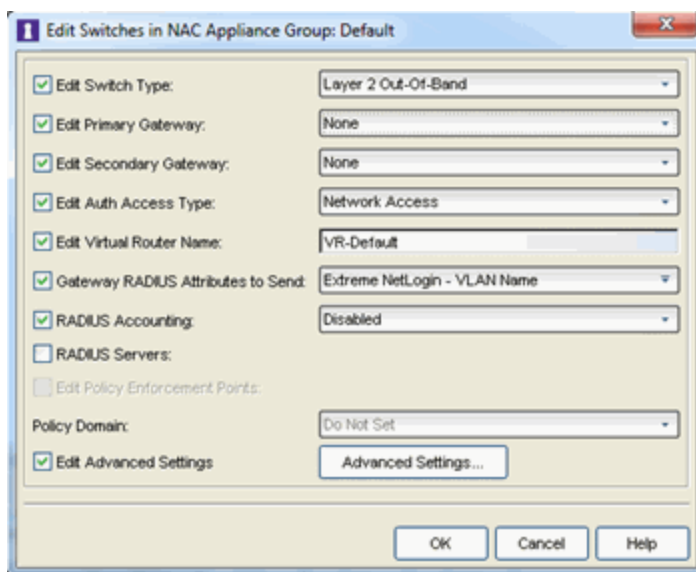
For information on related windows:

- [Add/Edit Policy Mapping Window](#)
- [How to Set Up Access Policies and Policy Mappings](#)

Edit Switches in NAC Appliance Group Window

Use this window to change a switch's primary and secondary Extreme Access Control (Access Control) Gateway, and also edit other switch parameters including the switch's authentication access type and the RADIUS attributes to send, if desired.

You can access this window by selecting an engine or engine group in the left-panel tree. Then, in the right-panel **Switches** tab, select the switches you wish to edit and click the **Edit** button.



Edit Switch Type

Use the drop-down menu to change the type of switch:

- **Layer 2 Out-Of-Band** - A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control gateway.
- **Layer 2 Out-Of-Band Data Center** - A switch within a data center where virtualization and mobility are a factor. If an end-system changes location but does not move to a different Access Control engine, NAC Manager removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in NAC Manager, because only one authenticated session is allowed per end-system within NAC Manager.

- **Layer 2 RADIUS Only** - In this mode, NAC Manager does not require any information from the switch other than the end-system MAC address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the [Advanced Switch Settings window](#). IP resolution and reauthentication may not work in this mode.
- **VPN** - A VPN concentrator being used in a [NAC VPN deployment](#). In this case, you should specify one or more Policy Enforcement Points below. If you do not specify a Policy Enforcement Point, then NAC Manager is unable to apply policies to restrict access after the user is granted access.

Edit Primary Gateway

Use the drop-down menu to select the primary Access Control Gateway for the selected switches. If load balancing has been configured for the switch, this field does not display.

Edit Secondary Gateway

Use the drop-down menu to select the secondary Access Control Gateway for the selected switches. If load balancing has been configured for the switch, this field does not display.

NOTE: To configure additional redundant Access Control Gateways per switch (up to four), use the Display Counts option in the [Display options panel](#) (Tools > Options).

Edit Auth Access Type

Use the drop-down menu to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: For ExtremeXOS devices only. NAC Manager uses CLI access to perform configuration operations on ExtremeXOS devices.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. For management requests handled through NAC Manager, make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator NAC Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database against which NAC Manager authenticates management login attempts.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

-
- **Any Access** - the switch can authenticate users originating from any access type.
 - **Management Access** - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
 - **Network Access** - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The NAC authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
 - **Monitoring - RADIUS Accounting** - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. NAC Manager learns about these session via RADIUS accounting. This allows NAC Manager to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The NAC authentication type precedence from highest to lowest is: Switch

Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.


- **Manual RADIUS Configuration** - NAC Manager does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using Policy Manager or CLI.

Edit Virtual Router Name

Select the checkbox to enter the name of the Virtual Router. The default value for this field is **VR-Default**.

WARNING: For ExtremeXOS devices only. If Extreme Management Center has not detected and populated this field, enter the Virtual Router Name carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

Gateway RADIUS Attributes to Send

Use the drop-down menu to select the RADIUS attributes settings included as part of the RADIUS response from the Access Control engine to the switch. Use the button  to the right to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes. Use the Preview area to preview your attribute settings; click Show Variables to use sample values in the Preview. If you define a new custom attribute, be sure to modify your policy mappings in the [Advanced Edit Policy Mapping view](#).

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time connection status in NAC Manager. It also allows NAC Manager to monitor Auto Tracking, CEP (Convergence End Point), and Quarantine (anti-spoofing) sessions. For more information, see [How to Enable RADIUS Accounting](#).

RADIUS Servers

Select this checkbox to allow editing of Management RADIUS Server and Network RADIUS Server options.

Management RADIUS Server

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in NAC Manager, or select **New** or

Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in NAC Manager, or select **New** or **Manage** RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Edit Policy Enforcement Points

Select this option to configure the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device that you are editing. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then NAC Manager is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

Use this option to assign the switch to a Policy Manager domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

Edit Advanced Settings

Select this option and then click the **Advanced Settings** button to open the [Advanced Switch Settings window](#).

Related Information

For information on related windows:

- [Add Switches to an Appliance Group Window](#)
- [Advanced Switch Settings Window](#)

Edit User Group Window

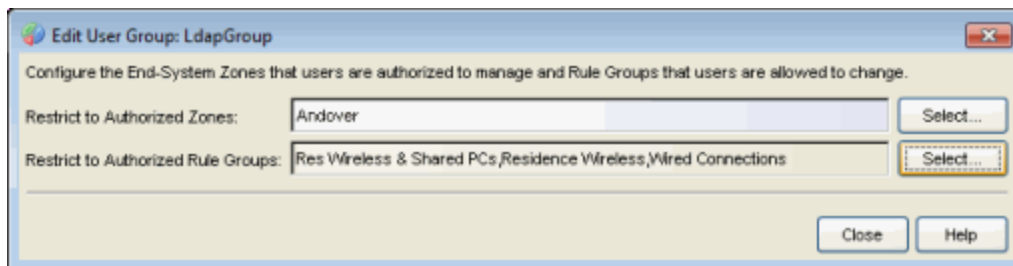
Use this window to configure the end-system zones that users in the selected user group are authorized to manage and the rule groups that they are allowed to modify. Any changes you make in this window do not take effect until the next time a user logs in.

This window provides two ways to limit user access to Extreme Management Center end-system information:

- Limit a user's access to Management Center end-system information and configuration; users are only authorized to view or control a subset of end-systems, delimited by zones.
- Limit a user's access to rule group configuration operations in Management Center; users are only authorized to view or make changes to a subset of rule groups.

For more information on end-system zones and how they are used, see [End-System Zones](#) and [How to Configure End-System Zones](#).

You can access this window from the [Manage End-System Zones Window](#) by selecting a user group and clicking the **Edit** button.



Restrict to Authorized Zones

Enter a list of zones or use the **Select** button to configure the end-system zones that users in the group are authorized to manage.

Restrict to Authorized Rule Groups

Use the **Select** button to configure the rule groups that users in the group are allowed to modify. If you do not select any rule groups, then all rule groups are accessible (unrestricted). If you want to deny access to all rule groups, configure the user group with read-only end-system access using the NAC Manager > OneView End-Systems Read Access authorization capability.

Related Information

For information on concepts:

- [End-System Zones](#)

For information on tasks:

- [How to Configure End-System Zones](#)

For information on related windows:

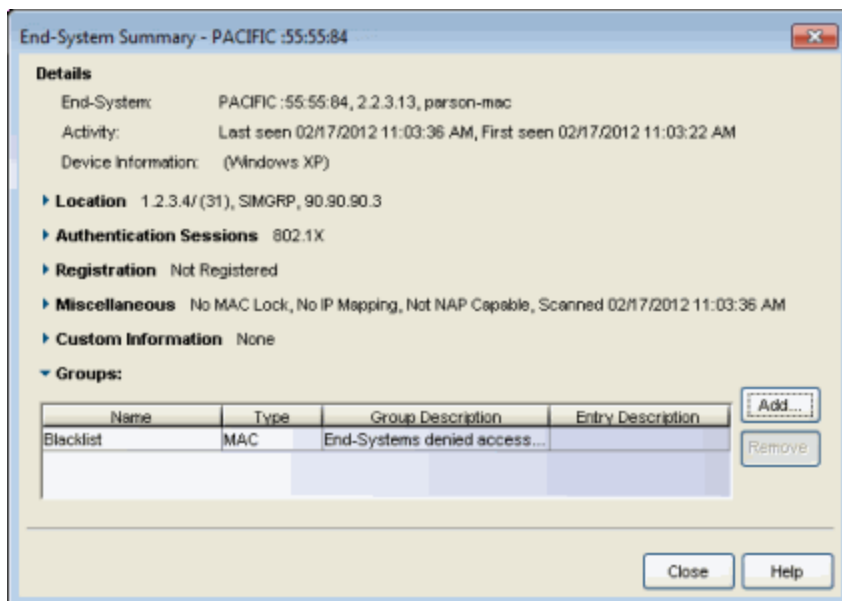
- [Manage End-System Zones Window](#)

End-System Summary Window

This window displays a summary of end-system connection information. You can also use this window to configure the following end-system functionality:

- Groups — add or remove the end-system directly to or from an end-system or user group.
- MAC Lock — lock the end-system's MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch.
- MAC to IP Mappings — map the end-system's MAC address directly to an IP address. The Extreme Access Control engines use this information to resolve the end-system's IP address.

You can access this window by selecting an end-system in the [End-Systems tab](#) and clicking the **Summary** button.



Details

This section displays a summary of the end-system connection information. For an explanation of each field, refer to the [End-Systems table](#) in the **End-Systems** tab.

Location

This section displays location information for the end-system. For an explanation of each field, refer to the [End-Systems table](#) in the **End-Systems** tab.

Authentication Sessions

This section displays information about current authentication sessions for the end-system. Sessions display in order of precedence from highest to lowest: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

Registration

This section displays information about the end-system's registration state and membership in a registration-related end-system group. If a sponsor has assigned the end user to a group that is different from the default access group, then it is listed in the Sponsor Group field.

Miscellaneous

This section displays:

- any MAC lock that is configured for the end-system, and lets you add or edit the MAC lock information using the [Add MAC Lock window](#). A MAC Lock locks the end-system's MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch.
- any MAC to IP Mapping that is configured for this end-system, and lets you add, edit, or remove the mapping. A MAC to IP Mapping lets you map the end-system's MAC address to a statically assigned IP address.
- information on when the end-system was last scanned or quarantined.
- whether the end-system is Microsoft NAP (Network Access Protection) capable.

Custom Information

Displays the custom information for the end-system that is added in the [End-Systems tab](#) or [End-Systems View](#).

Groups

This table displays the end-system, user, and registration groups that the end-system is assigned to. Use the **Add** and **Remove** buttons to change the group membership. Only registered devices can be added to registration groups, and registered devices cannot be removed from registration groups. Changes to group membership do not require an

enforce synchronize with engines immediately. Changes do not affect the end-system until the next authentication or assessment occurs.

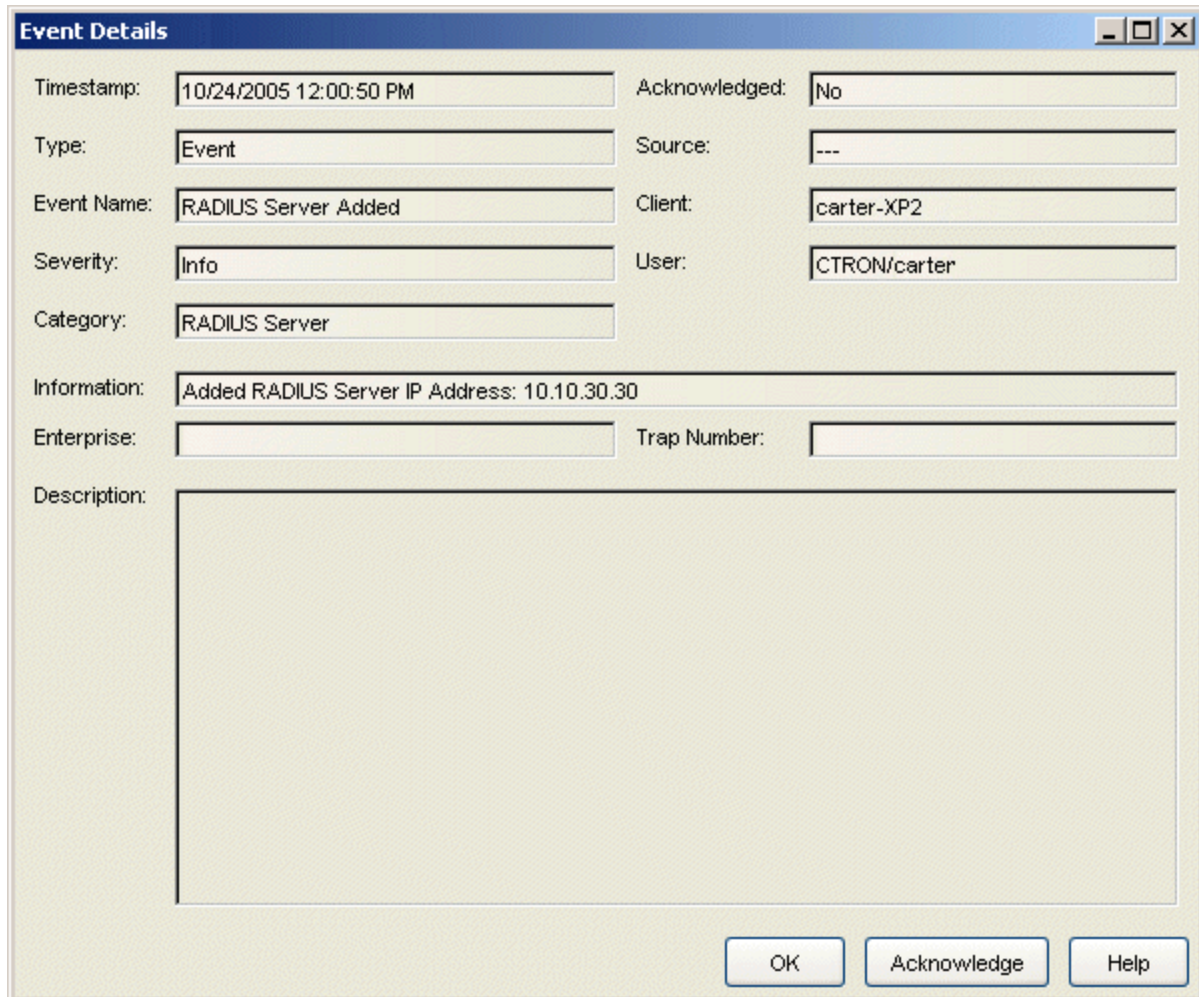
Related Information

For information on related windows:

- [End-Systems Tab](#)

Event Details Window

The Event Details window shows information about a single event selected in the [NAC Manager Events tab](#) of the Event View. To access the window, right-click an event in the NAC Manager **Events** tab and select **Event Details** from the menu.



The screenshot shows a window titled "Event Details" with a blue header bar and standard window controls (minimize, maximize, close). The window contains several input fields and a large text area. The fields are arranged in two columns. The left column contains: Timestamp (10/24/2005 12:00:50 PM), Type (Event), Event Name (RADIUS Server Added), Severity (Info), Category (RADIUS Server), Information (Added RADIUS Server IP Address: 10.10.30.30), Enterprise (empty), and Description (empty). The right column contains: Acknowledged (No), Source (---), Client (carter-XP2), and User (CTRON/carter). At the bottom right, there are three buttons: OK, Acknowledge, and Help.

Timestamp:	10/24/2005 12:00:50 PM	Acknowledged:	No
Type:	Event	Source:	---
Event Name:	RADIUS Server Added	Client:	carter-XP2
Severity:	Info	User:	CTRON/carter
Category:	RADIUS Server		
Information:	Added RADIUS Server IP Address: 10.10.30.30		
Enterprise:		Trap Number:	
Description:			

Timestamp

The date and time when the event occurred.

Acknowledged

Whether or not the selected event has been acknowledged.

Type

The type of information: Event.

Source

The IP address of the host that was the source of the event.

Event Name

The type of event.

Client

The name of the client host machine that triggered the event.

Severity

The event's severity.

Category

The category of event.

User

The name of the user that triggered the event.

Information

Information about the event.

Enterprise

Not applicable to the NAC Manager Event View.

Trap Number

Not applicable to the NAC Manager Event View.

Description

Not applicable to the NAC Manager Event View.

OK Button

Closes the window.

Acknowledge/Unacknowledge Button

Places a check or removes a check in the Acknowledge column in the NAC Manager **Events** tab for the selected event.

Related Information

For information on related windows:

- [Event View](#)

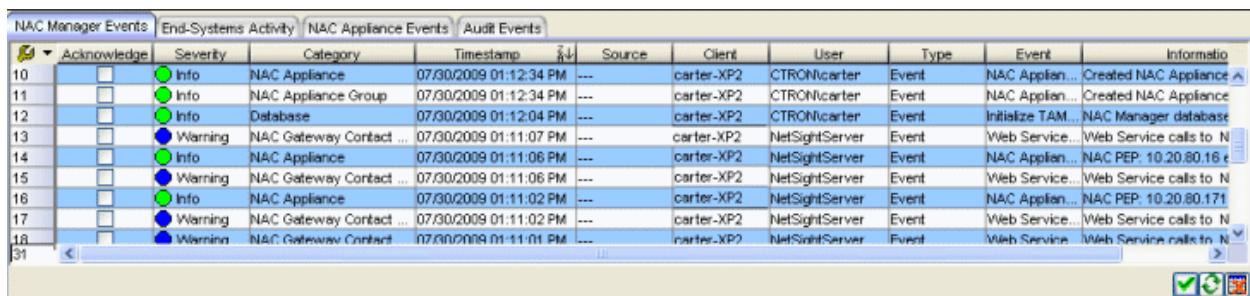
Event View

The Event View at the bottom of the NAC Manager main window displays error and informational messages about NAC Manager operations and provides information on end-systems that have attempted to connect to the network through a Extreme Access Control engine. There are four tabs:

- [NAC Manager Events Tab](#)
 - [Logging of End-System Group Events](#)
- [End-Systems Activity Tab](#)
- [NAC Appliance Events Tab](#)
- [Audit Events Tab](#)


NAC Manager Events Tab

The NAC Manager Events tab at the bottom of the NAC Manager main window displays error and informational messages about NAC Manager system operations. The log displays the most recent 10,000 entries. The current log file is automatically archived when its size reaches 5 megabytes and a new log file is opened. Use the Event Logs view in the Suite-Wide Options window to configure the number of event logs to save and the number of entries to display in the table.



	Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event	Information
10	<input type="checkbox"/>	Info	NAC Appliance	07/30/2009 01:12:34 PM	---	carter-XP2	CTRON\carter	Event	NAC Applian...	Created NAC Appliance
11	<input type="checkbox"/>	Info	NAC Appliance Group	07/30/2009 01:12:34 PM	---	carter-XP2	CTRON\carter	Event	NAC Applian...	Created NAC Appliance
12	<input type="checkbox"/>	Info	Database	07/30/2009 01:12:04 PM	---	carter-XP2	CTRON\carter	Event	Initialize TAM...	NAC Manager database
13	<input type="checkbox"/>	Warning	NAC Gateway Contact ...	07/30/2009 01:11:07 PM	---	carter-XP2	NetSightServer	Event	Web Service...	Web Service calls to N
14	<input type="checkbox"/>	Info	NAC Appliance	07/30/2009 01:11:06 PM	---	carter-XP2	NetSightServer	Event	NAC Applian...	NAC PEP: 10.20.80.16
15	<input type="checkbox"/>	Warning	NAC Gateway Contact ...	07/30/2009 01:11:06 PM	---	carter-XP2	NetSightServer	Event	Web Service...	Web Service calls to N
16	<input type="checkbox"/>	Info	NAC Appliance	07/30/2009 01:11:02 PM	---	carter-XP2	NetSightServer	Event	NAC Applian...	NAC PEP: 10.20.80.171
17	<input type="checkbox"/>	Warning	NAC Gateway Contact ...	07/30/2009 01:11:02 PM	---	carter-XP2	NetSightServer	Event	Web Service...	Web Service calls to N
18	<input type="checkbox"/>	Warning	NAC Gateway Contact ...	07/30/2009 01:11:01 PM	---	carter-XP2	NetSightServer	Event	Web Service...	Web Service calls to N

Acknowledge:

This checkbox lets you acknowledge an event and also hide acknowledged items. Click the checkbox to acknowledge the item and then click the **Show Acknowledged Events** button  to hide or show the checked items.

Severity

The event's severity.

Category

The category of event.

Timestamp

The date and time when the event occurred.

Source

The IP address of the host that was the source of the event.

Client

The name of the client host machine that triggered the event, or the IP address of the machine if the name cannot be resolved.

User

The client username or the name of the NAC component that triggered the event.

Type

The type of information: Event.

Event

The type of event.

Information

Information about the event.

**Show/Hide Acknowledged Events**

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

**Refresh**

Refreshes the log.

**Clear Current View**

Clears entries from the current table.

Logging of End-System Group Events

The following table summarizes data displayed in the **NAC Manager Events** tab when an end-system group change is logged, for example when an end-system is added to a group or deleted from a group. It lists the various actions that can cause an end-system group change, and the resulting Client and User column displayed in the event log.

In the Client column, Client IP refers to the name of the client host machine that triggered the event, or the IP address of the machine if the name cannot be

resolved. The User column lists the client username or the name of the NAC component that triggered the event.

Action	NAC Manager Events Tab	
	Client Column	User Column
End-system group change made from the End-System Summary window.	<Client IP>	<Username>
End-system group change made from the Dashboard.	<Client IP>	<Username>
End-system group change made from the Advanced Configuration window.	<Client IP>	<Username>
End-system group change made from the Registration Administration web page.	<Client IP>	<Username>
End-system added to group in the Add End-Systems to Group window.	<Client IP>	<Username>
End-system deleted from group(s) from the Tools > Remove End-Systems window.	<Client IP>	<Username>
End-system group changes made with the NAC Request Tool.	<Client IP>	<Username> credential used in the script
Tools > Manage Data Persistence > Cleanup Data with the remove from groups option selected.	<Client IP>	Extreme Management CenterServer
Overnight maintenance task with the remove from groups option selected.	<Client IP>	Extreme Management CenterServer
ASM notification adds end-system to Blacklist end-system group.	---	ASM
End-system added to group during Registration (Unauthenticated Registration).	<Extreme Access ControlEngine name>	Guest-<MAC address> ,

End-Systems Activity Tab

This tab provides information on all the end-systems attempting to connect to the network. It displays all end-system activity since the client was launched.

The screenshot shows the 'Event View' window in NAC Manager, specifically the 'End-Systems Activity' tab. The table displays the following data:

Timestamp	MAC Address	IP Address	Switch IP	Switch Location	Switch Port Index	Switch Port	Authentication Type	
08/05/2009 09:20:50 AM	00:60:B8:55:55:87				21		P (L3 NAC Controller On...	Error
08/05/2009 09:20:50 AM	00:0A:CB:55:55:60				59		WEB	Reject
08/05/2009 09:20:50 AM	00:15:AA:55:56:11				1		802.1X (EAP-TLS)	Guarar
08/05/2009 09:20:50 AM	00:08:C1:55:56:46				9		MS NAP (Microsoft NAP)	Guarar
08/05/2009 09:20:50 AM	00:0B:82:55:56:45				46		802.1X (EAP-TTLS)	Scan
08/05/2009 09:20:50 AM	00:0C:D1:55:56:69				29		MS NAP (Microsoft NAP)	Error
08/05/2009 09:20:50 AM	00:10:BC:55:56:44				54		802.1X	Scan
08/05/2009 09:20:49 AM	00:02:BB:55:55:91				44		WEB	Reject

At the bottom right of the window, there is a 'Clear Messages' button.

Timestamp

The date and time the end-system connected.

MAC Address

The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected in the [Options window Display view](#) (Tools > Options).

IP Address

The end-system's IP address.

Switch IP

The IP address of the switch to which the end-system connected. If the end-system is connected to a Extreme Access Control (Access Control) Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

Switch Location

The physical location of the switch to which the end-system connected. If the end-system is connected to a Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

Switch Port Index

The switch port index to which the end-system connected.

Switch Port

The switch port interface name to which the end-system connected.

Authentication Type

Identifies the authentication method used by the end-system to connect to the network. For Layer 3 Access Control Controller engines, this column shows IP.

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine - The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Error - Indicates one of nine problems:
 - the MAC to IP resolution failed, if assessment is enabled
 - the MAC to IP resolution timed out, if assessment is enabled
 - all RADIUS servers are unreachable
 - the RADIUS request was non-compliant
 - all assessment servers are unavailable
 - the assessment server can't reach the end-system
 - no assessment servers are configured
 - the assessment server is not compatible with the current version of NAC Manager
 - the username and password configured in the [Assessment Server panel](#) of the NAC Manager options (Tools > Options > Assessment Server) are incorrect for the assessment server

Extended State

Provides [additional information](#) about the end-system's connection state.

Reason

Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Username

The username used to connect.

Authorization

The attributes returned by the RADIUS server for this end-system. If the end-system is connected to a switch that supports multi-authentication,

then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

State Description

This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

NAC Appliance

The IP address of the Access Control engine with which the end-system is associated.

RADIUS Server

The IP address of the RADIUS server that the end-system is associated with.

Clear Messages button

Clears any messages that are selected in the table.

NAC Appliance Events Tab

This tab provides information on Extreme Access Control engine system events including RADIUS configuration success or failure, completed reauthentications, and management logins (via the console or Telnet). It displays engine activity since the client was launched.

NOTE: Installed certificates using an MD5 RSA signature algorithm now generate an event in Extreme Management Center version 7.

	Acknowledged	Severity	Category	Timestamp	Source	Type	Event	Information
1	<input type="checkbox"/>	Error	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.5	Event	Access Detected	telnet login
2	<input type="checkbox"/>	Critical	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.1	Event	Security Event	Re-Authentication completed
3	<input type="checkbox"/>	Alert	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.2	Event	Access Detected	RADIUS configuration success
4	<input type="checkbox"/>	Info	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.5	Event	Security Event	Re-Authentication completed
5	<input type="checkbox"/>	Critical	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.1	Event	Access Detected	RADIUS configuration failure
6	<input type="checkbox"/>	Notice	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.2	Event	Unexpected Error	RADIUS configuration failure
7	<input type="checkbox"/>	Info	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.2	Event	Access Detected	console login
8	<input type="checkbox"/>	Info	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.1	Event	Access Detected	Re-Authentication completed
9	<input type="checkbox"/>	Alert	NAC Appliance Event	08/05/2009 08:51:51 AM	90.90.90.1	Event	Access Detected	RADIUS configuration success

Acknowledge:

This checkbox lets you acknowledge an event and also hide items that have been acknowledged. Click the checkbox to acknowledge the item and then

click the Show Acknowledged Events button  to hide or show the checked items.

Severity

The event's severity.

Category

The category of event: NAC Appliance Event.

Timestamp

The date and time when the event occurred.

Source

The IP address of the engine that is the source of the event.

Type

The type of information: Event.

Event

The type of event.

Information

Information about the event.

**Show/Hide Acknowledged Events**

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

**Refresh**

Refreshes the log.

**Clear Current View**


Clears entries from the current table.

Audit Events Tab

This tab provides information on NAC Registration events such as when a device or user is added during the registration process, or an end-system is added/removed/updated via the registration administration web page. It displays all registration activity since the client was launched.

NAC Manager Events		End-Systems Activity		NAC Appliance Events		Audit Events							
Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event	Information				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 11:00:45 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered U...	Add Registered User: Guest-00-0A-19-				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 11:00:16 AM	00:0A:19:30...	10.20.32.34	Guest-00-0A...	Event	Registered D...	Added Registered Device for User: Gu				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 11:00:15 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered U...	Add Registered User: Guest-00-0A-19-				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:46 AM	00:0A:19:30...	10.20.32.34	Guest-00-0A...	Event	Registered D...	Added Registered Device for User: Gu				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:46 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered D...	Adding Registered Device to Group: Re				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:45 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered U...	Add Registered User: Guest-00-0A-19-				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:16 AM	00:0A:19:30...	10.20.32.34	Guest-00-0A...	Event	Registered D...	Added Registered Device for User: Gu				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:16 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered D...	Adding Registered Device to Group: Re				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:59:15 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered U...	Add Registered User: Guest-00-0A-19-				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:58:47 AM	00:0A:19:30...	10.20.32.34	Guest-00-0A...	Event	Registered D...	Added Registered Device for User: Gu				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:58:47 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered D...	Adding Registered Device to Group: Re				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:58:46 AM	---	10.20.32.34	Guest-00-0A...	Event	Registered U...	Add Registered User: Guest-00-0A-19-				
<input type="checkbox"/>	Info	Guest Access	08/03/2009 10:58:16 AM	00:0A:19:30...	10.20.32.34	Guest-00-0A...	Event	Registered D...	Added Registered Device for User: Gu				

Acknowledge:

This checkbox lets you acknowledge an event and also hide items that have been acknowledged. Click the checkbox to acknowledge the item and then click the Show Acknowledged Events button  to hide or show the checked items.

Severity

The event's severity.

Category

The category of event.

Timestamp

The date and time when the event occurred.

Source

The MAC address of the end-system that was the source of the event.

Client

The name of the machine that triggered the event, or the IP address of the machine if the name cannot be resolved.

User

The username that initiated the event, or Guest-<MAC address> if the username cannot be determined.

Type

The type of information: Event.

Event

The type of event.

Information

Information about the event.

**Show/Hide Acknowledged Events**

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

**Refresh**

Refreshes the log.

**Clear Current View**

Clears entries from the current table.

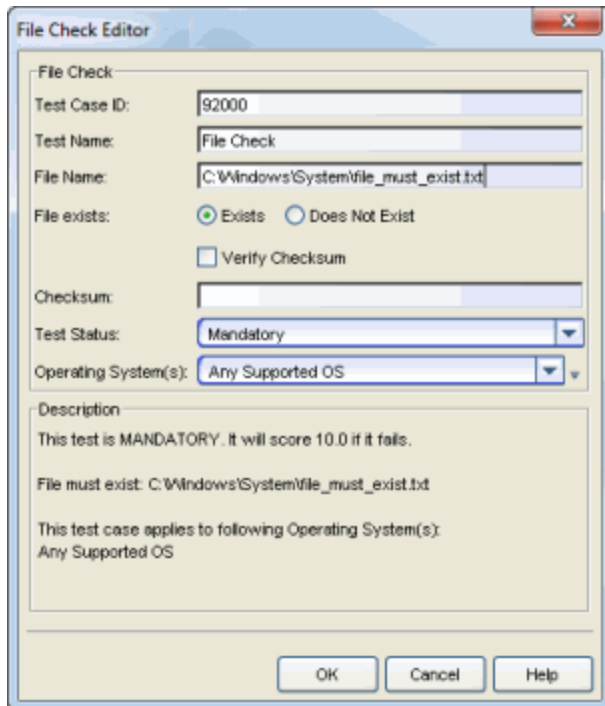
Related Information

For information on related windows:

- [Event Details Window](#)

File Check Editor

This window lets you configure parameters for a File Check test case included in an [agent-based test set](#). This test checks to see if a specific file is on the end-system.



Test Case ID

The test case is automatically assigned a Test Case ID number, although you may change this number, if desired. Refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

File Name

The path and name of the file for which you are checking.

File exists

Specify whether the file must exist or not on the end-system. If you use the Verify Checksum option, File Check also verifies that the checksum you

specify matches the file's checksum to make sure the file is the exact file for which you are checking.

Test Status


Use the Test Status drop-down menu to specify a status for this test. The status determines how the score returned by the assessment test is used.

- Disabled — The test is not run.
- Informational — The test is run and test score results are reported, but are not applied towards a quarantine decision. No end-systems are quarantined.
- Warning — Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) expires.
- Mandatory — Test score results are included as part of the quarantine decision, and end-systems may be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down menu to select the operating systems to which this test case applies. This list is automatically populated with all the operating systems on which this test may be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, adding a Windows operating system with a different service pack requirement. Any changes you make are only reflected in the drop-down menu as long as they are supported by the test.

Description

A description of the test case parameters.

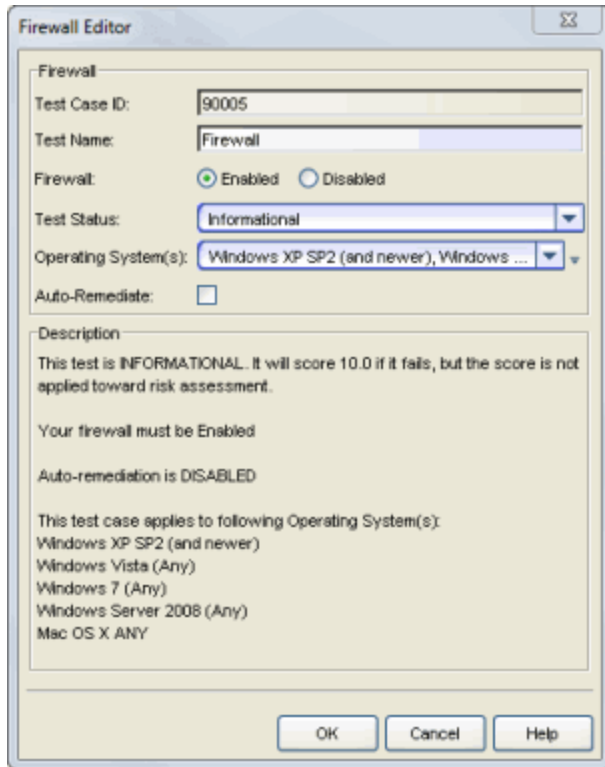
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Firewall Editor

This window lets you configure parameters for the Firewall test case included in an [agent-based test set](#). This test checks to see if the end-system's firewall is enabled or disabled. The test checks for any firewall plugged into the Windows Security Center.



Test Case ID

The Firewall test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Firewall

Use the drop-down menu to select the firewall state for which you want to test: enabled or disabled.

Test Status


Use the Test Status drop-down menu to specify a status for this test. The status determines how the score returned by the assessment test is used.

- Disabled — The test is not run.
- Informational - The test is run and test score results are reported, but are not applied towards a quarantine decision. No end-systems are quarantined. Auto-remediation is performed, if enabled.
- Warning — Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems are quarantined unless a [grace period](#) (if specified) expires. Auto-remediation is performed, if enabled.
- Mandatory — Test score results are included as part of the quarantine decision, and end-systems may be quarantined. Auto-remediation is performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down menu to select the operating systems to which this test case applies. This menu is automatically populated with all the operating systems on which this test may be performed. The Windows Security Center is required to perform this test.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, to add a Windows operating system with a different service pack requirement. Any changes you make are only reflected in the drop-down menu as long as they are supported by the test.

Auto-Remediate

If no firewall is found, and the Auto-Remediate checkbox is selected, the agent attempts to enable the Windows Firewall.

NOTE: If an end-system fails the Firewall test and Auto-Remediate is enabled for the test, the remediation fails if the user on the end-system is not an administrator.

Description

A description of the test case parameters.

Related Information

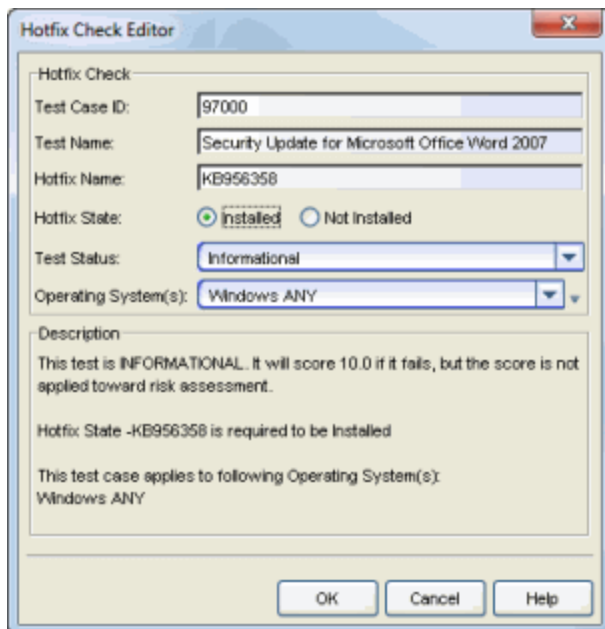
For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Hotfix Check Editor

This window lets you configure parameters for a Hotfix Check test case included in an [agent-based test set](#). This test checks to see if a specific hotfix has been installed on the end-system.

NOTE: If you configure multiple hotfix checks, make sure that the [Self-Monitoring Interval](#) (set in the Advanced Agent Configuration window) is set to at least 5 minutes, so that the assessment agent does not take a lot of CPU cycles trying to monitor these settings.



Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Hotfix Name

The name of the hotfix you are checking for. The hotfix name must be in the format "KB9999999" (without quotation marks).

Hotfix State

Specify whether the hotfix must be installed on the end-system or not installed on the end-system.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Import MAC Entries Window

This window lets you import MAC addresses from a file and assign them to various end-system groups. To access this window, click the **Import MAC Entries** button in the [Manage Rule Groups window](#).

Before you begin the procedure, make sure that the file you are importing uses the correct format. The file entries must specify a MAC address and (optionally) an end-system group name and a description in the following format:

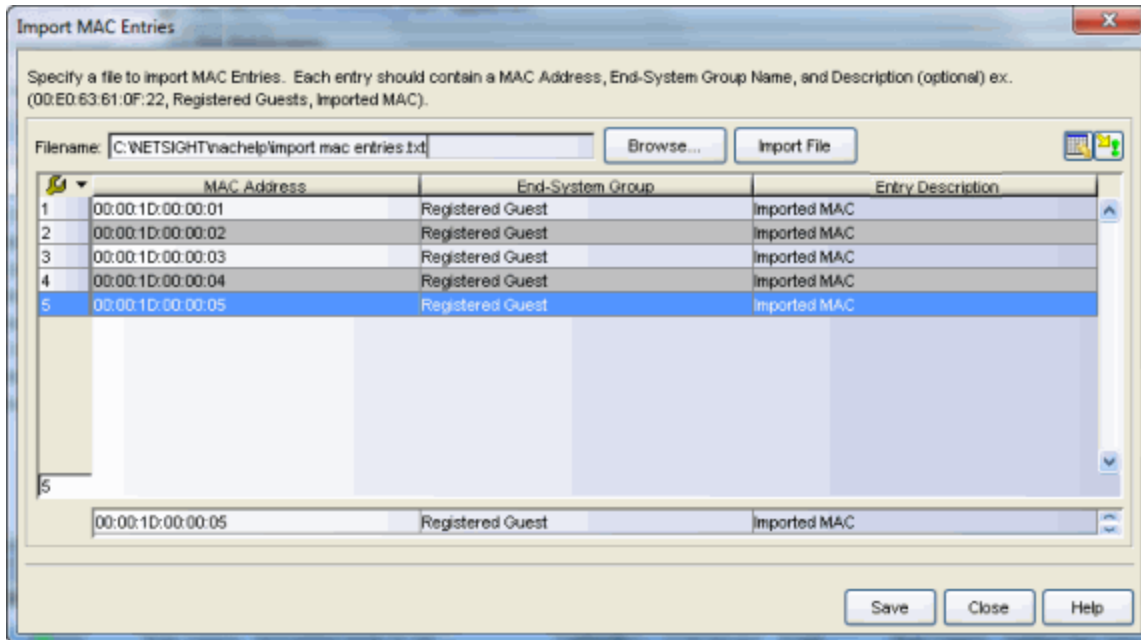
```
MAC address,end-system group name,description
```

For example:

```
00:00:1D:00:00:00,Registered Guest,Imported MAC
```

MAC addresses without separators are allowed, as well as addresses that use spaces, colons, periods, or dashes as separators. The end-system group that you specify must already be defined in NAC Manager or it is not imported.

After you import the file, you can add or edit the information for each MAC address using the Table Editor. You **must** specify an end-system group for each MAC address; only the description field is optional. When you have finished editing the entries, select the MAC addresses in the table that you wish to assign to end-system groups and click **Save**. The end-systems are listed as members of the end-system group.





Filename

Enter the path and filename for the file you want to import and click **Import File**, or click **Browse** to open a file browser where you can navigate and select a file.

MAC Address Table

This table lists all the MAC addresses in your imported file, and their associated end-system group and entry description (if those values were specified in the file). You can change the end-system group and description for each entry using the Table Editor.


Table Editor

The Table Editor allows you to edit the end-system group and description for the MAC addresses selected in the table. Select the row(s) you would like to edit, and toggle the **Show/Hide Table Editor** button  to display the Table Editor row at the bottom of the table. In the Table Editor row, click on the column you wish to edit and use the drop-down menu to select the end-system group or enter the new description. (The drop-down menu only displays end-system groups defined in NAC Manager.) Click **Apply**  to apply the changes to the table.



Show/Hide Table Editor

This button toggles the Table Editor, a row at the bottom of the table that allows you to define an end-system group and description for each MAC address. Click on the column in the editor row and use the drop-down

menu to select the end-system group or enter the new description. Click **Apply**  to apply the changes to the table.



Apply Button

Click this button to apply changes you have made using the Table Editor.

Save Button

Assigns the MAC addresses that are selected in the table to the specified end-system groups.

Related Information

For information on related windows:

- [Manage Rule Groups Window](#)

Installed Program Check Editor

This window lets you configure parameters for an Installed Program Check test case included in an [agent-based test set](#). This test checks to see if a specific program is installed and running on the end-system.

NOTE: The Installed Program Check test case is supported with agent version 1.15.0.0 and later.

The screenshot shows the 'Installed Program Check Editor' dialog box. It features a title bar with a close button. The main area contains several input fields and a description section. The 'Test Case ID' field is set to '96000'. The 'Test Name' field contains 'Installed Program Check'. The 'Application Name' field is empty. The 'Application State' section has two radio buttons: 'Installed' and 'Not Installed', with 'Not Installed' selected. The 'Test Status' field is a dropdown menu currently showing 'Informational'. The 'Operating System(s)' field is a dropdown menu showing 'Any Supported OS'. Below these fields is a 'Description' section with the following text: 'This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.', 'Installed Program Check - is required to be Not Installed', and 'This test case applies to following Operating System(s): Any Supported OS'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Application Name

The name of the application for which you are checking. You can specify the exact program name as listed in the Add/Remove Programs or Programs and Features list on a Windows operating system or in standard install locations the on a Mac operating system.

In addition, on Microsoft Windows systems you can enter .* as a wildcard before the application name, after the application name, or both before and after the application name. Depending on where you enter the wildcard, the agent searches for the application name regardless of the characters preceding, following, or preceding and following the application name. This allows you to search for the application name without needing an exact match. For example, if you do not want VNC or Winzip installed, you

can enter `.*VNC.* | .*winzip.*`. Java Regex expressions are supported for pattern matching.

On Apple OSX systems, the Agent supports a full path match or an application name match looking in the following paths:

- /Applications
- /System/Library/CoreServices
- /Library/Application/Support
- The user's desktop
- The user's documents

On Windows operating systems, the Agent searches until the first file match is found, therefore only one match is returned. The Agent searches for the application in the following order:

1. Searches the full path for an exact match for the application file name.

NOTE: The full path search does not support Java Regex expressions. The following Agent searches (listed in steps 2-6) support Java Regex expressions.

2. Searches the **Description** field of the Registry programs listed in the "Programs and Features". For example: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

3. Searches the system path for the matching EXE file name.

NOTE: Some Windows system folders do not allow search access to the Agent and are skipped when searching for the application.

4. Searches currently running processes to match the process name.

NOTE: Only 32-bit processes that match the application for which you are searching are returned.

5. Searches the Program Files directory, including up to two additional directory levels beyond the Program Files folder.

6. Searches the user's desktop, including up to two additional directory levels beyond the Desktop folder.

NOTE: The Service Agent does not search for a match in the user's desktop. This search is limited to the Dissolving and Persistent Agents.

Application State

Specify whether the application must be installed or not installed on the end-system.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled — The test will not be run.
- Informational — The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined. Auto-remediation will be performed, if enabled.
- Warning — Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation will be performed, if enabled.
- Mandatory — Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation will be performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems to which this test case applies. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make are only reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Interface Configuration Window

You can use this window to configure the interfaces on a Extreme Access Control engine. Interface configuration allows you to separate management traffic from end-system traffic, providing another layer of protection for sensitive data. It also provides the ability to snoop mirrored traffic on other ports.

This window is accessed from the [NAC Appliance Configuration tab](#), by clicking the **Edit** button in the Interface Summary section. It displays configuration options for each of the interfaces available on the Extreme Access Control engine.

The screenshot shows the 'Interface Configuration' window with two sections:

- Interface eth0 - Management Only**
 - Mode: Management Only
 - Services: Management, Monitoring Services, Network Services, AAA Servers, Device, Portal: Management, Traffic Snooping
 - DHCP/Kerberos Snooping: Enabled
 - Captive Portal HTTP Mirroring
 - Tagged VLANs: (empty)
 - IPv4 Address:
 - IP Address: 10.20.80.22
 - Mask: 255.255.255.0
 - Hostname: nacs2k-8022.nac2003.com
 - Gateway: 10.20.80.1
- Interface eth1 - Registration & Remediation Only**
 - Mode: Registration & Remediation Only
 - Services: End-System, Traffic Snooping
 - DHCP/Kerberos Snooping: Enabled
 - Captive Portal HTTP Mirroring
 - Tagged VLANs: 87
 - IPv4 Address:
 - IP Address: 10.20.89.254
 - Mask: 255.255.255.0
 - Hostname: NACa2k-8022.NetSightNAC.com
 - Gateway: 10.20.89.2

Buttons: OK, Cancel, Help

Interface Modes

There are five different modes that can be configured for an interface: Management, Registration & Remediation, Management Only, Registration & Remediation Only, Listening Only, Advanced Configuration, and Off. The mode determines the type of traffic allowed on the interface and the [services](#) provided by the interface.

You can configure all the interfaces on an engine; however, you cannot change the management interface and you are only allowed to configure one interface to allow management traffic.

Management, Registration & Remediation – This mode is the in-band management mode where both management traffic and registration, assessment, and remediation traffic use the same interface. In this mode, the engine does not limit traffic to each of the services. This behavior is the same as behavior in NAC Manager versions 4.2.x and earlier.

Management Only – In this mode, the engine binds all management services to this interface. This includes:

- traffic to Extreme Management Center and other engines (JMS and HTTP)
- all traffic to switches
- all LDAP and RADIUS traffic
- traffic for the following services: SSH daemon, SNMP daemon, and RADIUS server
- traffic for captive portal administration, sponsorship, pre-registration, and screen preview (on ports 80 and 443)
- traffic for WebView pages and Extreme Management Center web services (on ports 8080 and 8443)

Registration & Remediation Only – In this mode, the engine binds all registration and remediation services to this interface. All traffic to end-systems is initiated through this interface, including:

- assessment traffic
- NetBIOS for IP and hostname resolution
- traffic for registration pages, remediation pages, and self-registration (on ports 80 and 443)
- all agent communication traffic (on ports 8080 and 8443)

Listen Only - In this mode, the engine allows DHCP and Kerberos snooping to be performed on the interface. No IP address or hostname can be assigned to the interface.

Advanced Configuration - This mode allows you to configure the services that are provided by the selected interface, using the link in the [Services](#) field. This is useful for [Extreme Access Control deployments in MSP or MSSP environments](#).

Off - The interface is disabled and not used in any way.

Services

The Services field displays the services that are provided by the Extreme Access Control engine interface, as determined by the selected interface mode. Each mode provides a different set of services on the interface.

If the mode is set to Advanced Configuration, the services list becomes a link that launches an Edit window where you can select or deselect the services provided by the interface. This granularity is useful for [Extreme Access Control deployments in MSP or MSSP environments](#).

The following list describes the various services that are provided by the different modes:

- **Management** - The communication to and from the Extreme Management Center server. Sub-services include JMS, Web Services, and Syslog.
NOTE: The Management service cannot be moved from eth0.
- **Monitoring Services** - The services used to monitor or contact an engine. Sub-services include the SSH daemon and SNMP agent.
- **Network Services** - The communication to external servers that provide networking services. Sub-services include DNS servers and NTP servers.
NOTE: The Network Services service can only be applied to one interface.
- **AAA Servers** - The communication used by external servers for authentication and authorization. Sub-services include RADIUS servers and LDAP servers.
NOTE: The AAA Servers service can only be applied to one interface.
- **Device** - The communication to and from a NAS (switch, router, VPN, or wireless controller). Sub-services include SNMP, RADIUS, RFC3576, SSH/Telnet, and TFTP.
- **Portal: Management** - the captive portal registration management services for an engine.

- **End-System** - The communication to and from end-systems. Sub-services include portal registration and remediation, assessment, NetBIOS, and DNS proxy.
- **Traffic Snooping** - DHCP and Kerberos snooping on the interface. This service is listed if the [DHCP/Kerberos Snooping option](#) is set to Enabled.

DHCP/Kerberos Snooping

Use the DHCP/Kerberos Snooping option to enable or disable DHCP and Kerberos snooping on the interface. DHCP snooping is used for IP resolution and OS detection. Kerberos snooping is used for user name detection and [elevated access](#).

Captive Portal HTTP Mirroring

This is an advanced option that allows the interface to accept mirrored HTTP traffic which is used to display the captive portal to end users. This option is an alternative to using Policy-Based Routing and DNS Proxy.

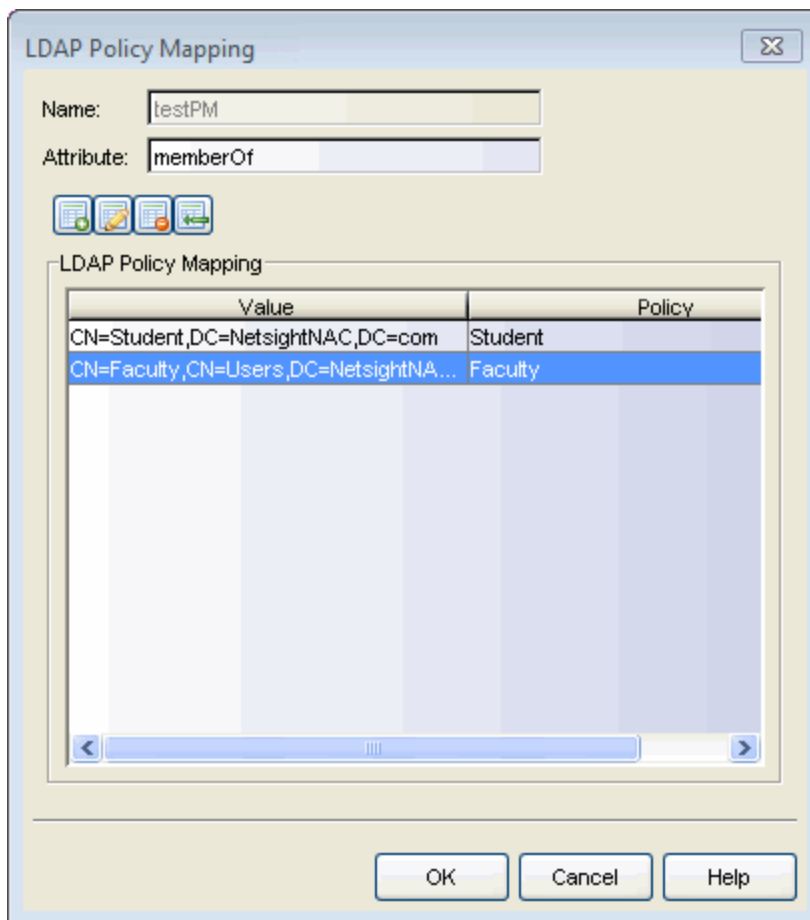
Tagged VLANs

If the mirrored traffic includes an 802.1Q VLAN tag, then the list of VLANs to capture must be explicitly stated in this field by entering a comma-separated list of VLAN IDs from 1 to 4094. If the mirrored traffic is not tagged then this field can be left blank.

LDAP Policy Mapping Window

The LDAP Policy Mapping window lets you map LDAP attribute values to policies you have created in Policy Manager. You can then specify in your [NAC profiles](#) that the Accept policy uses the LDAP Policy Mappings to determine the policy to apply to the end-system.

Access this window from the configuration menu button  displayed to the right of the Accept Policy drop-down menu when you select the "Use User/Host LDAP Policy Mappings" option in the [New/Edit NAC Profile window](#).



Name

The name of the LDAP policy mapping.

Attribute

The LDAP attribute that the value to policy mappings are defined for.



Use these buttons to add, edit, delete, or import value to policy mappings for this LDAP attribute. Use the Add or Edit buttons to specify the mapping's attribute value and corresponding access policy mapping. Use the Delete button to remove the selected mapping(s). Use the Import button to import up to 1000 entries at a time from a file. Imported file entries must be listed in a CSV format as Value, Policy (for example: Jones, Administrator) with one entry per line. Lines starting with "#" or "/" are ignored. Existing mappings with the same value are not overwritten.

Value

The attribute values that have been defined for the mapping.

Policy

The policies to which the attribute values map.

Related Information

For information on related windows:

- [Manage LDAP to Policy Mappings window](#)

Manage Appliance Certificates Window

The Manage Appliance Certificates window provides a central location for managing the security certificates for your Extreme Access Control (Access Control) engines. You can access this window by right-clicking on any engine in the right-panel **Appliances** tab.

NOTE: Extreme Management Center automatically generates alarms as the Access Control Engine Internal Communications Server Certificate, the Captive Server Portal Server Certificate, the RADIUS Server Certificate, the AAA Configuration Truststore, and the Access Control Engine Truststore approach their expiration date. Extreme Management Center generates a Notification alarm 30 days before expiring, a Warning alarm 7 days before expiring, and a Critical alarm when the certificate expires.

The top section of the window lets you modify the engine's security certificates. During installation, server certificates are generated for each Access Control engine. While these certificates provide secure communication, there may be cases where you want to update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which NAC Manager must communicate. Additionally, you may want to use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages. You can use this section to:

- View and update the Captive Portal server certificate
- View and update the Internal Communications server certificate
- View and update the certificate configuration for agent-based assessment
- View and update the RADIUS server certificate

The bottom section of the window provides information about the AAA configuration used by the engine group to which the engine belongs. You can use this section to:

- View the configured AAA authentication behavior to determine whether certificates are used in the authentication process. If your Access Control deployment is using EAP-TLS, PEAP, or EAP-TTLS authentication and the authentication requests are not proxied, certificates are used to provide secure communication between the Access Control RADIUS server and

end-systems that are authenticating. However, if your authentication behavior is configured to proxy all 802.1X authentication requests, then certificates are not used.

- View and update the AAA certificate authorities that are trusted to issue client certificates for 802.1X authentication. You only need to do this if your AAA authentication behavior uses certificates.

Any changes made in this window do not take effect until the engine is enforced.



Appliance

Use this section to view the current configuration for the engine server certificates, and update the certificates, if desired. For complete instructions on replacing and verifying a certificate, see [How to Update Access Control Engine Server Certificates](#).

Captive Portal Server Certificate

The Captive Portal server certificate provides secure communication for the Access Control captive portal web pages. Click **Update Certificate** to open the [Update Captive Portal Server Certificate window](#) where you can replace the certificate.

Internal Communications Server Certificate

The Internal Communications server certificate provides secure communication between components and for Access Control administrative web pages. Click **Update Certificate** to open the [Update Internal Communications Server Certificate window](#) where you can replace the certificate.

Agent-Based Assessment Server Certificate

The server certificate for agent-based assessment provides secure agent communications. Use the button to toggle between the following two selections:

- Use Legacy Certificate - This option causes agent-based assessment to use the legacy (NAC Manager version 4.0.0 and earlier) server certificate in order to provide backward compatibility with older agents.
- Use Internal Certificate - Once agents have been upgraded, this option uses the Internal Communications server certificate for agent communications. Using the Internal Communications server certificate provides increased security and also allows you to update the certificate, if desired.

Any change takes effect when the engine is enforced. When enforced, the agent communications port (8443) is offline for 15 seconds to reload the certificate.

RADIUS Server Certificate

The RADIUS server certificate is the certificate sent to end-systems during certain forms of 802.1X authentication (EAP-TLS, PEAP, and EAP-TTLS). Click **Update Certificate** to open the [Update RADIUS Server Certificate window](#) where you can update to a certificate generated by a Certificate Authority that your connecting end-systems are already configured to trust.

NOTE: The current configuration displays "No certificate information is available" if you have not updated the RADIUS server certificate using this window, even though a certificate is generated during installation.

AAA Configuration

If your Access Control deployment is using EAP-TLS, PEAP, or EAP-TTLS authentication and the authentication requests are not proxied, you need to [update your RADIUS server certificate](#) to a CA certificate your connecting end-systems trust. In addition, you need to configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted.

This information is part of the AAA configuration and shared across all engines in an engine group. This allows end-systems to be trusted on any Access Control engine where they can authenticate.

AAA Configuration

This section displays the current authentication behavior configured for the engine and helps you determine whether certificates may be used during authentication. If the engine RADIUS server proxies all 802.1X authentication requests, then certificates are not used. If the engine RADIUS server can terminate 802.1X authentication requests, then certificates are used if you are using EAP-TLS, PEAP, or EAP-TTLS authentication. Use the **Edit AAA Configuration** button to access your AAA configuration to change this behavior.

AAA Trusted Certificate Authorities

Click **Update Certificates** to open the [Update AAA Trusted Certificate Authorities window](#) where you can create a list of trusted certificate authorities (CAs) to issue client certificates for 802.1X authentication, as well as create a list of CRL distribution points which are used to check for revoked client certificates. Changing this configuration affects all engines that use the AAA configuration.

Related Information

For information on related tasks:

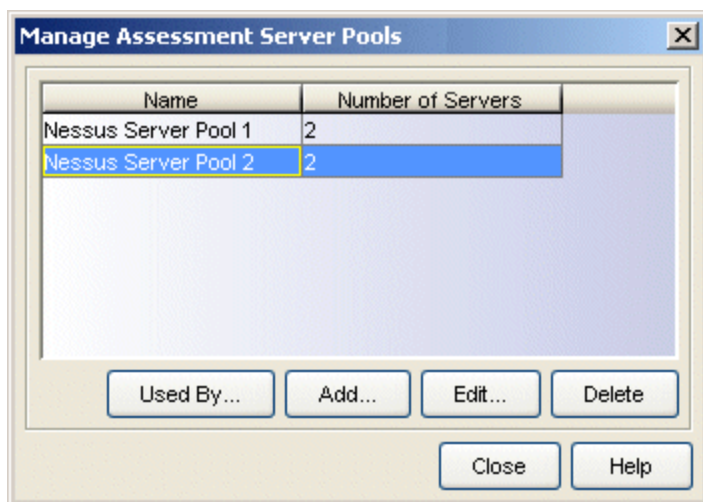
- [How to Update Access Control Engine Server Certificates](#)

Manage Assessment Server Pools Window

This window lets you view and define the assessment server pools used in your assessment configurations. If you have multiple assessment servers on your network, creating assessment server pools allows you to control which assessment server resources are used for each assessment configuration on a very granular level. For example, if you have four Nessus assessment servers, put server A and server B in server pool 1, and server C and server D in server pool 2. Then, in your assessment configuration you can specify which server pool to use.

To access this window, click  (the configuration menu button) in the Test Sets section of the [Edit Assessment Configuration window](#) and select Manage Assessment Server Pools.

NOTE: You can also access the Manage Assessment Server Pools window in the Advanced Configuration tool by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, right-click the Assessment folder and select **Show Assessment Server Pools**. Expand the Assessment Folder and select the Assessment Server Pools icon. The window displays in the right panel.



Name

The name of the assessment server pool.

Number of Servers

The number of assessment servers contained in the pool.

Used By Button

Opens a window that lists all assessment configurations currently using the selected assessment server pool.

Add Button

Opens the [Add Assessment Server Pool window](#) where you can define a new assessment server pool.

Edit Button

Opens the [Edit Assessment Server Pool window](#) where you can edit the selected assessment server pool.

Delete Button

Deletes the selected assessment server pool(s).


Related Information

For information on related tasks:

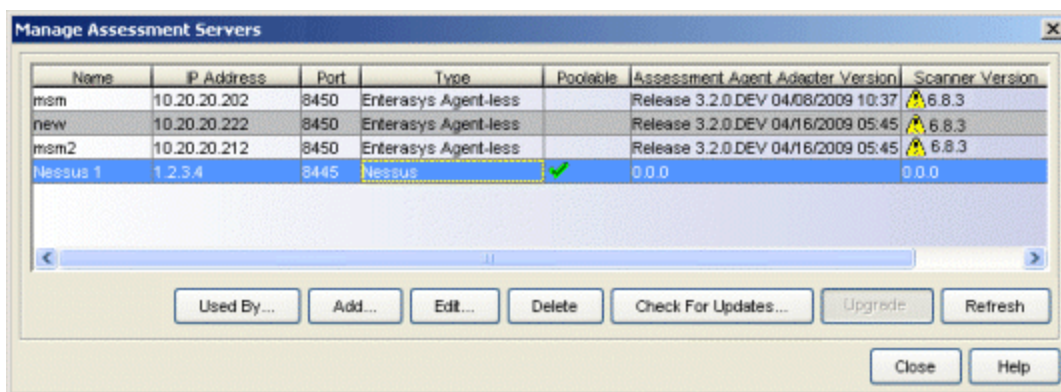
- [Manage Assessment Servers Window](#)
- [Add/Edit Assessment Server Pool Window](#)
- [Edit Assessment Configuration Window](#)

Manage Assessment Servers Window

This window lets you view and configure the assessment servers that perform the end-system assessments in your network. Once you have configured your assessment servers, they can be added to an assessment server pool and participate in assessment server load-balancing, if desired. Agent-less on-board assessment servers are automatically displayed in this window and cannot be edited or deleted. In order to allow your agent-less on-board assessment servers to participate in assessment server load-balancing and server-pools, you must add them manually to this window.

To access this window, click the configuration menu button  in the Test Sets section of the [Edit Assessment Configuration window](#) and select Manage Assessment Servers, or click the **Manage** button in the [Add/Edit Assessment Server Pool window](#).

NOTE: You can also access the Manage Assessment Servers window in the Advanced Configuration tool by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, right-click the Assessment folder and select **Show Assessment Servers**. Expand the Assessment Folder and select the Assessment Servers icon. The window displays in the right panel.



Name

The name of the assessment server. This is the name that is entered when you [add an assessment server](#). For on-board assessment servers, the name is determined by the name of the Extreme Access Control (Access Control) engine. For example, if you create a Access Control engine and name it

MyAccess Controlengine, then the on-board assessment server name is listed as MyAccess Controlengine as well.

IP Address

The IP address of the assessment server. This is the IP address entered when you [add an assessment server](#). For on-board assessment servers, the IP address is determined by the address of the Access Control engine. For example, if you create a Access Control engine with an IP address of 10.20.80.8, then the on-board assessment server IP address is listed as 10.20.80.8 as well.

Port

The port number on the assessment server to which the Access Control engine sends assessment requests.

Type

The assessment server type: Agent-less, Nessus, or a third-party assessment agent (an assessment agent that is not supplied or supported by NAC Manager).


Poolable

A checkmark in this column indicates that the assessment server can be part of an assessment server pool. If you have multiple assessment servers on your network, creating assessment server pools allows you to control which assessment server resources are used for each assessment configuration. External assessment servers are "poolable," however, in order to allow your agent-less on-board assessment servers to participate in server-pools, you must add them manually to this window.

Assessment Agent Adapter Version

The version of assessment agent adapter software that is installed on the assessment server.

Scanner Version

The version of scanner software installed on the assessment server. When an upgrade for the software is available, the upgrade icon  displays. The Upgrade feature is only available for on-board agent-less assessment servers and allows you to upgrade the scanner software installed on the assessment server. When you select the row, the Upgrade button becomes active and you can click the button to initiate the upgrade.

Status

When the assessment server is operational, then the status is Normal. Otherwise, this column provides status information regarding an upgrade

procedure: Downloading, Download failed, Updating..., Update complete, or Update failed.

Used By Button

Opens a window that lists the assessment server pools currently using the selected assessment servers.

Add Button

Opens the [Add Assessment Server window](#) where you can define a new assessment server.

Edit Button

Opens the [Edit Assessment Server window](#) where you can edit the settings for the selected assessment server. You cannot edit on-board assessment server settings.


Delete Button

Deletes the selected assessment server. You cannot delete on-board assessment servers or servers that are currently in use.

Check for Updates Button

This button opens the [Updates Available window](#) which lists any assessment software updates available for download. The download operation downloads any updated software but does not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button here in this window.

Upgrade Button

This feature is only available for on-board agent-less assessment servers and allows you to upgrade the scanner software installed on the assessment server. When an upgrade is available, the upgrade icon  appears in the Scanner Version column. When you select the row, the Upgrade button becomes active and you can click the button to initiate the upgrade.

NOTE: Upgrades are available through the Web Update feature accessed via Help > Check For Assessment Updates or by clicking the **Updates** button. This check downloads any updated software, but does not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button here in this window.

Perform the Check for Assessment Updates and the Upgrade operation at least every two weeks to ensure that the assessment servers are running the latest scanner software that includes the most up-to-date virus definitions. You can schedule the check for assessment updates using the [Assessment Server Web Update option](#).

Because the on-board agent-less assessment license is subscription-based, the Upgrade operation must be performed at least once a month in order to upgrade the license. If the Extreme Management Center (Management Center) server is unable to contact the upgrade server, contact Extreme Networks Support so that a special license can be provided.

If the Management Center Server does not have internet access (and cannot use the Web Update feature), you can perform an upgrade by copying the upgrade file to the Management Center Server install directory and extracting the file in the Management Center directory (it extracts the entire path from there). Clicking the **Upgrade** button in this window to perform the upgrade. The upgrade file is downloaded from: http://www.extremenetworks.com/netsight-renew/netsight-saint/saint_latest.zip.)

Refresh Button

Reloads the latest assessment server information in the table. You can also refresh just the version information by right-clicking on a row in the table and selecting **Refresh Version Info**.

Related Information

For information on related windows:

- [Add/Edit Assessment Server Window](#)
- [Edit Assessment Configuration Window](#)

Manage Assessment Settings Window

The Manage Assessment Settings window is the main window used to manage and configure the assessment servers that performs the end-system assessments in your network. To access this window, select **Tools > Management and Configuration > Assessment Settings** from the menu bar.

The window displays three tabs that provide information on:

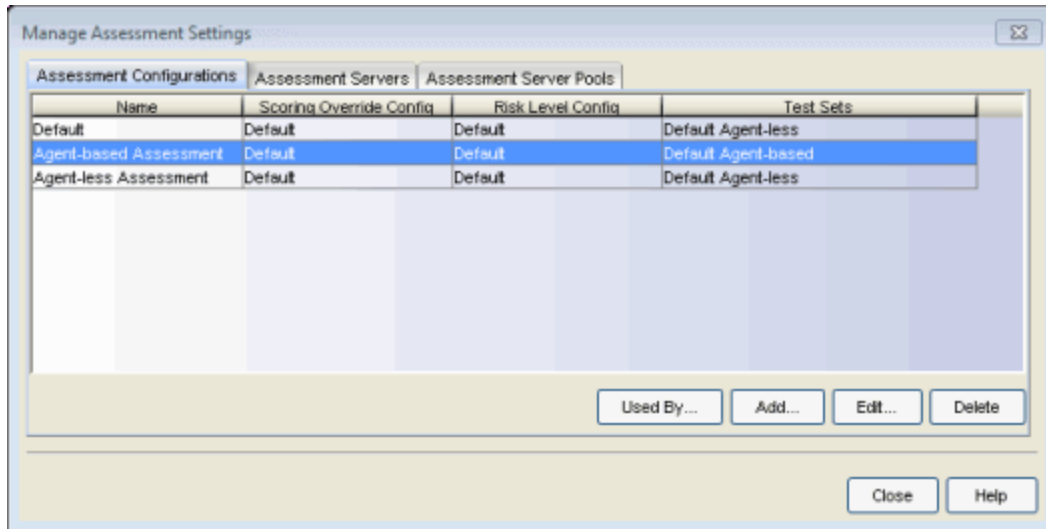
- [Assessment Configurations](#)
- [Assessment Servers](#)
- [Assessment Server Pools](#)

NOTE: You can also access the Manage Assessment information in the Advanced Configuration tool by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the Assessment folder. Select Default to view and configure the default assessment configuration that ships with each Extreme Access Control engine. To create a new assessment configuration, right-click on the Assessment folder and select **Add Assessment Configuration** from the menu. Enter a name for the new configuration and click **OK**. The new configuration name appears in the tree below the Default configuration. When you select the configuration you wish to view or edit, it displays in the right-panel. Right-click on a configuration name in the tree to delete the configuration, change the configuration name, create a copy of the configuration, or see where each configuration is being used by an Extreme Access Control configuration.

You can also display lists of your [assessment servers](#) and your [assessment server pools](#) by right-clicking on the Assessment folder and selecting the appropriate option.

Assessment Configurations

This tab lets you view a listing of your assessment configurations, and add, edit, or delete a configuration. Assessment configurations define the different assessment requirements for end-systems connecting to your network. When you create a NAC profile, select an assessment configuration that defines the assessment requirements for the end-systems using that profile. You can also click the **Used By** button to view a list of all assessment configurations currently being used by Extreme Access Control configurations.



Name

The name of the assessment configuration. This is the name that is entered when you add an assessment configuration in the [Edit Assessment Configuration](#) window.

Scoring Override Config

The scoring override configuration for this assessment configuration. The scoring override configuration lets you override the default scoring assigned by the assessment server to a particular assessment test ID.

Risk Level Config

The risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

Test Sets

The test sets that run for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

Used By Button

Opens a window that lists all assessment configurations currently being used by Extreme Access Control configurations.

Add Button

Opens the [Edit Assessment Configuration](#) window where you can define a new assessment configuration.

Edit Button

Opens the [Edit Assessment Configuration](#) window where you can edit the settings for the selected assessment configuration.

Delete Button

Deletes the selected assessment configuration. You cannot delete assessment configurations currently in use.

Assessment Servers

This tab lets you view and configure the assessment servers that perform the end-system assessments in your network. Once you have configured your assessment servers, they can be added to an assessment server pool and participate in assessment server load-balancing, if desired. Agent-less on-board assessment servers are automatically displayed in this list and cannot be edited or deleted. In order to allow your agent-less on-board assessment servers to participate in assessment server load-balancing and server-pools, you must add them manually to this list.

Name	IP Address	Port	Type	Poolable	Assessment Agent Adapter Version	Scanner Version	Status
nacmsm-vpn-...		8445	Agent-less		Release 5.0.0.DEV 04/08/2013 15:33	7.14.17	Normal
3inline-188-27		8445	Agent-less		Release 4.4.0.101 01/24/2013 08:30	7.14.17	Normal
naca20-200-1...		8445	Agent-less		Release 5.1.0.117 (x86_64) 11/14/...	7.14.14	Normal
Nessus 1		8445	Nessus	✓	0.0.0	0.0.0	Normal
Nessus 2		8445	Nessus	✓	0.0.0	0.0.0	Normal

Name

The name of the assessment server. This is the name that is entered when you [add an assessment server](#). For on-board assessment servers, the name is determined by the name of the Extreme Access Control (Access Control) engine. For example, if you create an Access Control engine and name it MyAccess Controlengine, then the on-board assessment server name is listed as MyAccess Controlengine as well.

IP Address

The IP address of the assessment server. This is the IP address that is entered when you [add an assessment server](#). For on-board assessment servers, the IP address is determined by the address of the Access Control engine. For example, if you create a Access Control engine with an IP address of 10.20.30.40, then the on-board assessment server IP address is listed as 10.20.30.40 as well.

Port

The port number on the assessment server to which the Access Control engine sends assessment requests.

Type

The assessment server type: Agent-less, Nessus, or a third-party assessment agent (an assessment agent that is not supplied or supported by NAC Manager).


Poolable

A checkmark in this column indicates that the assessment server can be part of an assessment server pool. If you have multiple assessment servers on your network, creating assessment server pools allows you to control which assessment server resources is used for each assessment configuration. External assessment servers are "poolable," however, in order to allow your agent-less on-board assessment servers to participate in server-pools, you must add them manually to this list.

Assessment Agent Adapter Version

The version of assessment agent adapter software that is installed on the assessment server.

Scanner Version

The version of scanner software installed on the assessment server. When an upgrade for the software is available, the upgrade icon  is displayed. The Upgrade feature is only available for on-board agent-less assessment servers and allows you to upgrade the scanner software installed on the assessment server. When you select the row, the Upgrade button becomes active and you can click the button to initiate the upgrade.

Status

When the assessment server is operational, then the status is Normal. Otherwise, this column provides status information regarding an upgrade procedure: Downloading, Download failed, Updating..., Update complete, or Update failed.

Max Scans

The maximum number of scans that can be performed concurrently on this assessment server.

Used By Button

Opens a window that lists the assessment server pools currently using the selected assessment servers.

Add Button

Opens the [Add Assessment Server window](#) where you can define a new assessment server.

Edit Button

Opens the [Edit Assessment Server window](#) where you can edit the settings for the selected assessment server. You cannot edit on-board assessment server settings.


Delete Button

Deletes the selected assessment server. You cannot delete on-board assessment servers or servers that are currently in use.

Check for Updates

This button opens the [Updates Available window](#) which lists any assessment software updates available for download. The download operation downloads any updated software but does not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button here in this window.

Upgrade

This feature is only available for on-board agent-less assessment servers and allows you to upgrade the scanner software installed on the assessment server. When an upgrade is available, the upgrade icon  appears in the Scanner Version column. When you select the row, the Upgrade button becomes active and you can click the button to initiate the upgrade.

NOTE: Upgrades are available through the Web Update feature accessed via **Help > Check For Assessment Updates** or by clicking the **Updates** button. This check downloads any updated software but does not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button here in this window.

You should perform the Check for Assessment Updates and the Upgrade operation at least every two weeks to ensure that the assessment servers are running the latest scanner software that includes the most up-to-date virus definitions. You can schedule the check for assessment updates using the [Assessment Server Web Update option](#).

Because the on-board agent-less assessment license is subscription-based, the Upgrade operation must be performed at least once a month in order to upgrade the license. If the Extreme Management Center (Management Center) server is unable to contact the upgrade server, you should contact Extreme Networks Support so that a special license can be provided.

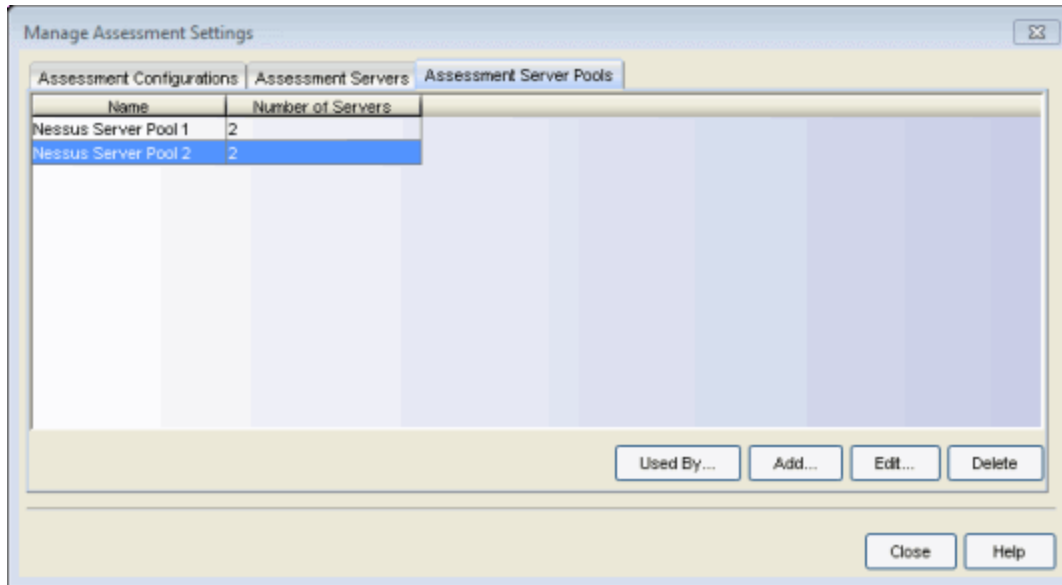
If the Management Center Server does not have internet access (and cannot use the Web Update feature), you can perform an upgrade by copying the upgrade file to the Management Center Server install directory and extracting the file in the Management Center directory (it extracts the entire path from there). You can then perform the upgrade by clicking the **Upgrade** button in this window. The upgrade file is downloaded from: http://www.enterasys.com/netsight-renew/netsight-saint/saint_latest.zip.)

Refresh

Reloads the latest assessment server information in the table. You can also refresh just the version information by right-clicking on a row in the table and selecting **Refresh Version Info**.

Assessment Server Pools

This tab lets you view and define the assessment server pools used in your assessment configurations. If you have multiple assessment servers on your network, creating assessment server pools allows you to control which assessment server resources are used for each assessment configuration on a very granular level. For example, if you have four Nessus assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, in your assessment configuration you can specify which server pool that configuration should use.

**Name**

The name of the assessment server pool.

Number of Servers

The number of assessment servers contained in the pool.

Used By Button

Opens a window that lists all assessment configurations currently using the selected assessment server pool.

Add Button

Opens the [Add Assessment Server Pool window](#) where you can define a new assessment server pool.

Edit Button

Opens the [Edit Assessment Server Pool window](#) where you can edit the selected assessment server pool.

Delete Button

Deletes the selected assessment server pool(s).

Related Information

For information on related windows:

- [Add/Edit Assessment Server Window](#)
- [Add/Edit Assessment Server Pool Window](#)

- [Edit Assessment Configuration Window](#)

Manage Custom Fields Window

This window lets you manage the fields displayed in the web pages presented to the end user when they access the network. It is configured as part of your portal configuration, and is accessed from the Customize Fields **change** link in the [Edit Portal Configuration window](#). You can manage custom fields for both guest and authenticated access types:

- **Guest Access Types** — By default, the guest login/registration web page displays the First Name, Last Name, and Email Address fields. You can use this window to specify other fields you would like to be displayed (visible) and required. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Modifying settings for one access type also changes settings for the other access types.
- **Authenticated Access Types** — By default, the authenticated login/registration web page displays only the Acceptable Use Policy. Use this window to specify other fields to display (by selecting **Visible**) and require (selecting **Required**). These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Modifying settings for one access type also changes settings for the other access types.

Sample Manage Custom Fields Window

Field	Visible	Required	Display String
First Name:	Visible	<input checked="" type="checkbox"/>	
Middle Name:	Visible	<input type="checkbox"/>	
Last Name:	Visible	<input checked="" type="checkbox"/>	
Email Address:	Visible	<input checked="" type="checkbox"/>	
Phone Number:	Not Visible	<input type="checkbox"/>	
1st Custom:	Visible	<input type="checkbox"/>	Student ID Number
2nd Custom:	Not Visible	<input type="checkbox"/>	
3rd Custom:	Not Visible	<input type="checkbox"/>	
4th Custom:	Not Visible	<input type="checkbox"/>	
5th Custom:	Not Visible	<input type="checkbox"/>	
Device Description:	Not Visible	<input type="checkbox"/>	

Acceptable Use Policy: Display [change](#)

Note: Custom Display String fields are common between Unauthenticated and Authenticated Registration types. Modifying a Display String for one Registration type will affect the Display String in the other.

OK Cancel Help

For each field, use the drop-down menu to select whether the field is displayed:

- **Visible** — the field displays in the login/registration web page for the end user. If you want the field information to be required (the end user must enter the information), select the **Required** checkbox.
- **Not Visible** — the field does not display in the login/registration web page for the end user.
- **Admin Only** — the field is visible to network administrators only, in the Add/Edit User web page accessed from the Registration System Administration web page. The end user is not able to see or edit the field.

NOTES: For Guest Registration and Guest Web Access: If you are configuring a Verification Method, the Email Address field and/or the Phone Number field are required (depending on the verification method you select) and must be set to **Visible/Required**. For more information, see [How to Configure Verification for Guest Access Registration](#).

For Secure Guest Access: The Credential Delivery method requires the Email Address field and/or the Phone Number field (depending on the delivery method you select) to be set to **Visible/Required**. For more information, see [Credential Delivery Method](#) in the Edit Portal Configuration window.

For Facebook Registration: Only the First Name, Last Name, and Email Address fields are filled using Facebook data. These fields and the Acceptable Use Policy (AUP) option are the only fields that apply to Facebook registration. If the display AUP option is selected, the captive portal verifies that the AUP is acknowledged before redirecting the user to Facebook.

Use the **Custom fields** to add additional fields to the login/registration web page. Set the field to Visible, and then add the text that you would like displayed by adding a display string. Here are some examples of how to use custom fields:

- In a higher education environment a custom field display string may be set to "Student ID Number" or "Dorm Room Number" to record additional information about students registering to the network.
- In a corporate environment, a custom field display string may be set to "Company Name" to obtain information about organization to which a partner or guest belongs. Or, you might want the end user to enter a device description, such as an asset tag number.
- In a convention deployment, the field may be set to "Booth Number" to record the booth to which a registering end-system is associated.

Select the **Acceptable Use Policy** checkbox if you would like the web page to display your organization's Acceptable Use Policy (AUP) and click the "change" link to open a window where you can add the AUP text.

NOTE: The Pre-Registration web page always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. If selected as required, they display as required on the Pre-Registration web page, otherwise they display as optional. This is because it is important to prompt for a first and last name to be included on the pre-registration voucher that is printed out.

Related Information

- [Edit Portal Configuration Window](#)

Manage Data Center Fabric Window

If your network uses the Extreme Networks Data Center Manager (DCM) product, you can use this window to view a list of virtual/physical network configurations and how they map to the overall network and security configuration.


The window displays data from rules and corresponding end-system groups that contain DCM specific settings for the selected NAC configuration. A list of Policy Manager domains is displayed, based on the switches associated with the NAC Configuration and the Policy Manager domains the switches belong to.

To access this window in NAC Manager, select Tools > Management and Configuration > Data Center Fabric.

For more information, see the NMS Data Center Manager User Guide (version 9034586-02), section 4.1, DCM Configuration in NAC Manager, available on the Network Management Suite (NMS) Documentation web page:

<https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx>.

Virtual/Physical Network	Policy Configuration	VLAN ID	vSwitch Targets	Approval Workflow	Synchroniz
Application Server	Policy: Application Server_Role, VLAN: 1[DEFAULT VLAN]	Primary: 1, Secondary: 2,	Switch Group: includeAll	Enabled	Enabled
Storage	Policy: Storage_Role, VLAN: 3[Edge]	Primary: 3	Switch Group: Storage Closet	Disabled	Enabled
Web Servers	Policy: Web Servers_Role, VLAN: 4[Web Servers_VLAN]	Primary: 4, Secondary: 5,	Switch Group:	Disabled	Disabled
Mail Servers	Policy: Mail Servers_Role, VLAN: 6[Mail Servers_VLAN]	Primary: 6	Switch Group: None	Enabled	Disabled
QA Lab	Policy: QA Lab_Role	Primary: 99	Switch Group: None	Disabled	Disabled
Training Center	Policy: Training Center_Role, VLAN: 199[Training]	Primary: 199	Switch Group: None	Disabled	Disabled
Boston Sales	Policy: Boston Sales_Role	Primary: 184	Switch Group: None	Disabled	Disabled
Automation Lab	Policy: Automation Lab_Role	Primary: 185	Switch Group: None	Disabled	Disabled

Use the  toolbar button to launch the [Create Virtual and Physical Network Configuration window](#) where you can create a new virtual network.

Use the  toolbar button to run the [configuration evaluation tool](#) where you can test the new configuration.

At the bottom of the window, a **Manage** drop-down button contains the following menu items:

- **Manage Policy Domain for Switches** — Manage the policy domain for the switches associated with the selected engine group. Set or change the domain for a selected switch (only Extreme Networks or Enterasys switches), verify the role settings on selected switches, and enforce the domain configuration to the selected switches (from right-click menu option).
- **Verify Domain Policy Settings with Network** — Verify that the roles in the assigned Policy Manager domain are enforced to the associated switches.
- **Enforce Domain Policy Settings to Network** — Enforce the roles in the assigned Policy Manager domain to the associated switches.
- **Edit Policy Mapping Configuration** — opens the [Edit Policy Mapping window](#).

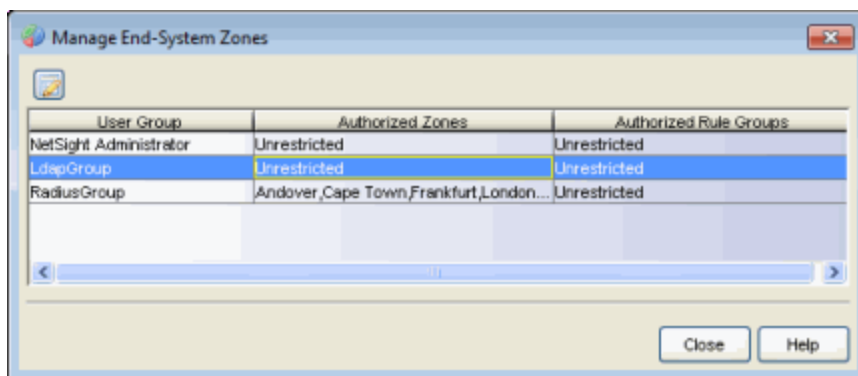
Manage End-System Zones Window

This window lets you view and define the authorized end-system zones and authorized rule groups configured for your Extreme Management Center (Management Center) user groups.

Configuring authorized zones and rule groups for your user groups allows you to limit a Management Center user's ability to access and modify Management Center end-system information.

For more information, refer to [End-System Zones](#) and [How to Configure End-System Zones](#).

To access this window in NAC Manager, select Tools > Management and Configuration > End-System Zones.



User Group

The name of the user group created in the Users/Groups tab in the Authorization/Device Access tool.

Authorized Zones

The end-system zones users in the group are authorized to manage. Selecting **Unrestricted** indicates all zones are accessible.

Authorized Rule Groups

The rule groups users in the group are allowed to modify. Selecting **Unrestricted** indicates all rule groups are accessible.

Edit Button

Select a user group in the table and click **Edit** to open the [Edit User Group window](#), where you can configure the end-system zones that users are authorized to manage and the rule groups that users are allowed to modify.

Related Information

For information on concepts:

- [End-System Zones](#)

For information on tasks:


- [How to Configure End-System Zones](#)

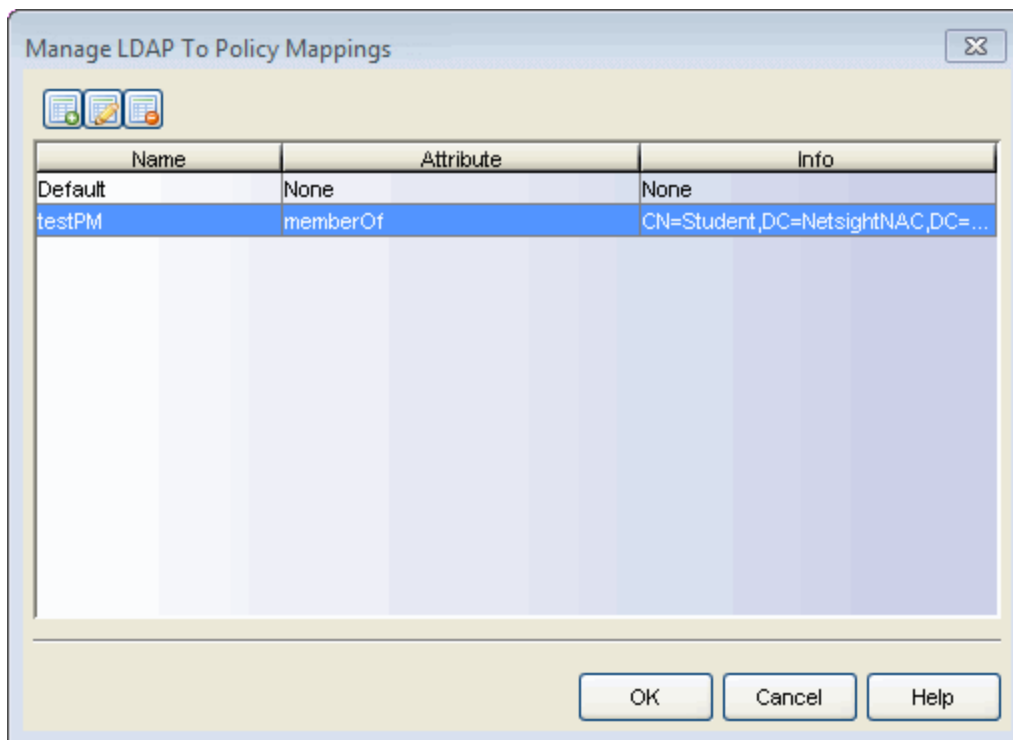
For information on related windows:

- [Edit User Group Window](#)

Manage LDAP to Policy Mappings Window

This window lets you view and define the LDAP to Policy Mappings designated as the [Accept policy in a NAC profile](#).

Access this window from the configuration menu button  displayed to the right of the **Accept Policy** drop-down menu when you select the **Use User/Host LDAP Policy Mappings** options in the [New/Edit NAC Profile window](#) (if you have multiple mappings) or to the right of the LDAP Policy Mapping field in the [Add User to Authentication Mapping window](#).



Use these buttons to add, edit, or delete LDAP to Policy mappings. Click **Add** or **Edit** to open the [LDAP Policy Mapping window](#). Use the **Delete** button to remove the selected mapping(s).

Name

The name of the mapping.

Attribute

The LDAP attribute for which the value to policy mappings are defined.

Info

The attribute values defined for this mapping.

Related Information

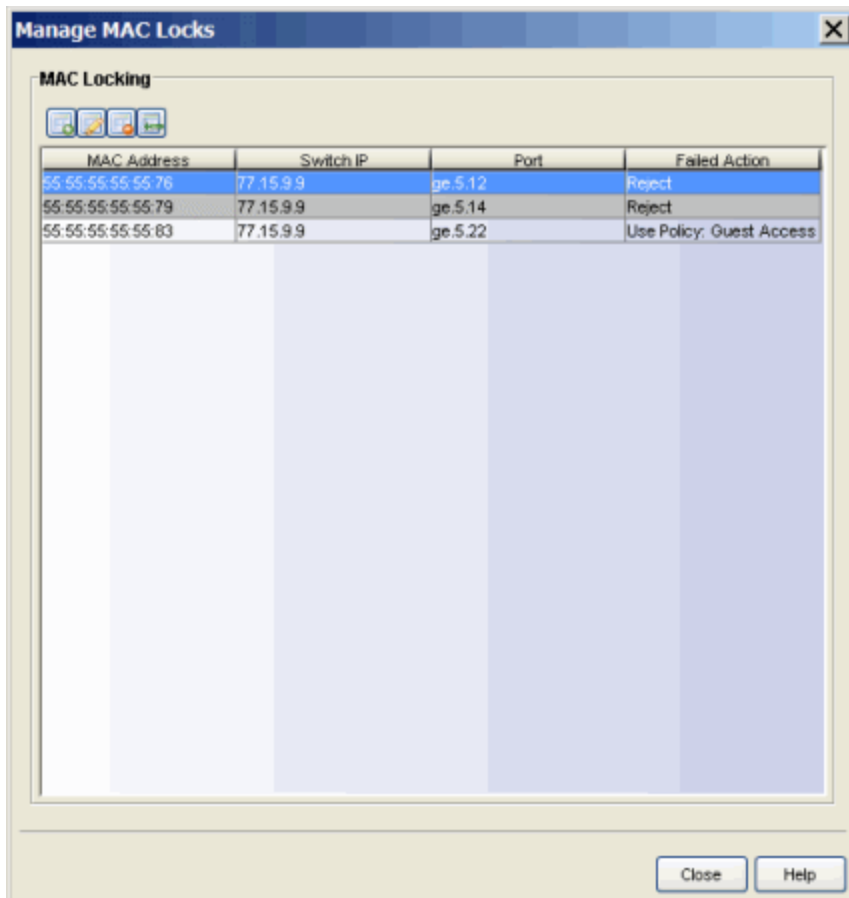
For information on related windows:

- [New/Edit NAC Profile window](#)

Manage MAC Locks Window

MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. The Manage MAC Locks window displays information about all the MAC addresses that are locked. You can also add or delete locked MAC addresses, or import MAC locks from a file. Any changes made in this window are written immediately to the NAC Manager database. To access this window, select **Tools > Management and Configuration > MAC Locks** from the menu bar.

NOTE: You can also access the Manage MAC Locks window in the Advanced Configuration tool by selecting **Tools > Management and Configuration > Advanced Configurations** from the menu bar. In the left-panel tree, expand the Global and Appliance Settings folder and click on MAC Locking. The window will be displayed in the right panel.





Use these buttons to add, edit, delete, or import MAC locking entries.

MAC Address

The MAC address that is locked. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected in the [Options window Display view](#) (Tools > Options).

Switch IP

The IP address of the switch that the MAC address is locked to.

Port

If the MAC address is locked to a specific port, this column displays the port interface name.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name will change and break the MAC Locking settings.

Failed Action

The action that will be taken if this MAC address tries to authenticate on a different port and/or switch:

- Reject - The authentication request will be rejected.
 - Use Policy: - The policy that will be applied to the port the MAC address is attempting to authenticate on.
-

Related Information

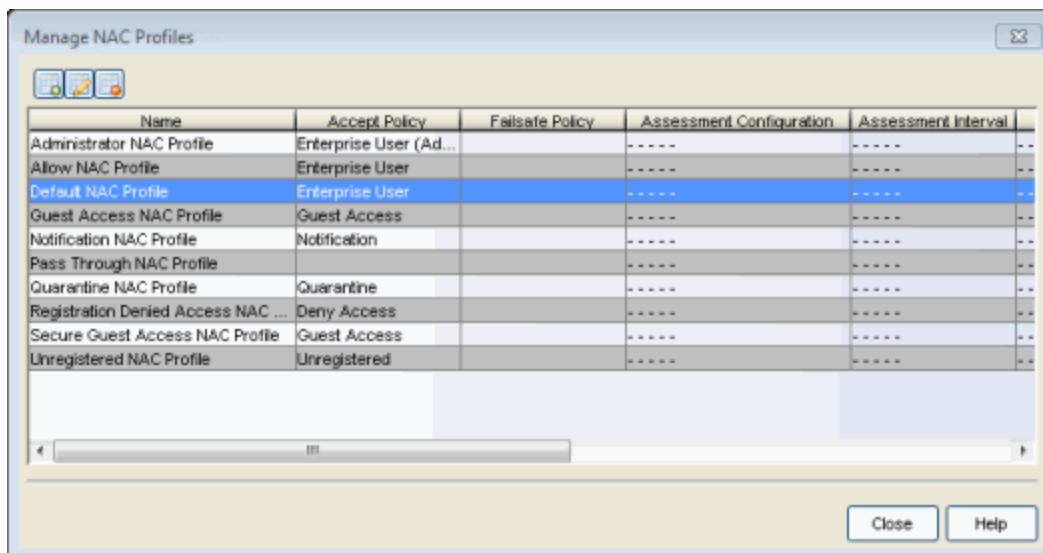
For information on related windows:

- [Add/Edit MAC Lock Window](#)

Manage NAC Profiles Window

NAC Manager comes with ten system-defined NAC profiles that define the authorization and assessment requirements for the end-systems connecting to the network. The system-defined profiles are: Administrator, Allow, Default, Guest Access, Notification, Pass Through, Quarantine, Registration Denied Access, Secure Guest Access, and Unregistered. Use this window to view and edit these profiles, and define new profiles if desired. Any changes made in this window are written immediately to the NAC Manager database.

To access this window, select the **Manage NAC Profiles** button  in the NAC Manager toolbar or select Tools > Management and Configuration > NAC Profiles from the menu bar.



Use these buttons to add, edit, or delete NAC profiles.

Name

The name of the NAC profile.

Accept Policy

The Accept policy defined for this profile. An Accept policy is applied to an end-system when

- an end-system is authorized locally by the Extreme Access Control engine and passed an assessment (if assessment is enabled).

- authentication is configured to replace the attributes returned from the RADIUS server with the Accept policy.

Failsafe Policy

The Failsafe policy defined for this profile. A Failsafe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there is a scanning error and a scan of the end-system did not take place.

Assessment Configuration

The assessment configuration defined for this profile. The configuration define the assessment requirements for end-systems

Assessment Interval

If assessment is required, this defines the interval between required assessments for an end-system.

Quarantine Policy

The Quarantine policy defined for this profile. A Quarantine policy is applied to an end-system if the end-system fails an assessment.

Assessment Policy

The Assessment policy defined for this profile. An Assessment policy is applied to an end-system while it is being assessed.

Hide Assessment/Remediation Details

Denotes whether the option to hide assessment or remediation information on the Remediation Web Page is selected: true (hidden) or false (not hidden).

Reject Authentication Requests

Denotes whether all authentication requests are rejected: true or false.

Related Information

For information on related windows:

- [New/Edit NAC Profile Window](#)

Manage Notifications Window

This window lists all the notifications you create, and lets you enable, add, edit, and test specific notification rules. Notifications allow you to create alert actions performed when specific events or triggers take place in NAC Manager. Notification actions include sending an email, creating a syslog entry, sending an SNMP trap, and launching a custom program or script.

To access this window, select the Manage Notifications button  in the NAC Manager toolbar.

NAC Manager comes with four default notifications that you can enable and use as is, or edit if desired. You see the default notifications when you open the Manage Notifications window, as shown below. To enable a default notification, you must perform the following steps:

1. Select the notification in the table and click the **Edit** button to open the [Edit Notification Action window](#).
2. Use the **Edit Email Lists** button and change the default address to an address specific to your network.

Default notifications are configured to send an email to this address.

3. Configure the SMTP E-Mail Server option in the Suite Options (Tools > Options > Suite Options) to identify the SMTP email server used for outgoing messages generated by the Notification feature.
4. Click on the **Enable Notification** checkbox and then click **OK** in the Edit Notification Action window.

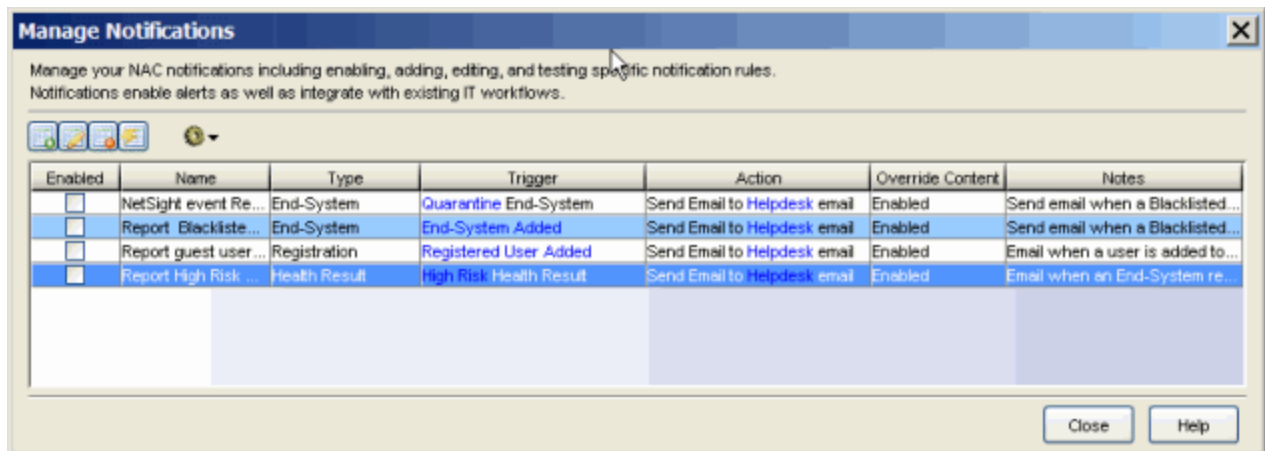
The default notification is now enabled in the Manage Notifications window.

Here are some examples of how notifications can be used to alert you of changes or events in your network:

- Send an email to the Helpdesk when an end-system changes location, for example if it moves from a wired connection in a building to a wireless connection outside.
- Send a trap if an end-system fails registration.

- Send a syslog message if an end-system reports a high risk assessment result.
- Send an email if an end-system that is reported as a stolen laptop authenticates on the network.
- Send an email if someone logs into the network after normal work hours.
- Send an email when an end-system is added or removed from an end-system group, such as the Blacklist end-system group or other defined end-system group.
- Send an email when a user is added or removed from a user group, such as an Administrator or Help Desk user group.

For more information and examples on creating Notifications, see the [Edit Notification Action window](#) Help topic.



Use these buttons to add, edit, delete, or test a notification.

- Add New Notification - opens the [Edit Notification Action window](#) where you can define a new notification rule.
- Edit Notification - select a notification in the table and click this button to open the [Edit Notification Action window](#) where you can edit the notification rule actions.
- Delete Selected Notifications - select one or more notifications in the table and click this button to delete the notifications.
- Test Notification - opens the Edit Test Data window where you can configure the keyword values needed to perform a test of the notification you select in the table. Click the **Send Test** button to perform the test.



Use the configuration menu button to:

- **Create Default SIEM Notifications** - Creates five default notifications that allow the Extreme Access Control notification feature to integrate with Extreme Networks SIEM (Security Information and Event Manager) by sending syslog messages to your SIEM server. The notifications are based on the following conditions and triggers:
 - Any Registration event
 - Any Health Result
 - End-System events:
 - End-System added
 - End-System moved
 - End-System State changed

The generated syslog messages include the following information:

- IP address
 - MAC address
 - Switch IP address
 - Switch port
 - Switch location
 - Hostname
 - Operating system
 - State
 - Extended State
 - Reason
 - Extreme Access Control Engine IP address
- **Change Default SIEM Server** - Use this option to change the default SIEM server IP address used when you generate new default SIEM notifications. The specified default SIEM server only applies to newly generated notifications; manually edit previously generated notifications to change the server.

Enabled

Use the checkbox to enable or disable a notification. When a notification is enabled, the defined action takes place when the [trigger](#) occurs and the [conditions](#) are met.

Name

The name of the notification.

Type

The notification type defines the source of the event triggering the notification: End-System Group, End-System, User Group, Health Result, or Registration.

Trigger

The trigger determines when a notification action occurs, based on filtering for a specific event.

Action

The actions that take place when a notification is triggered.

Override Content

Specifies whether [Override Content](#) is enabled or disabled for the notification. If Override Content is enabled, then the notification action defaults defined in the suite-wide Notification Engine options (Tools > Options > Suite Options) are changed for this specific notification.

Notes

A short description of the notification rule. This description is created when a new notification is added.

Related Information

For information on related windows:

- [Edit Notification Action Window](#)

Manage Operating Systems Window

This window lists the supported operating systems for end-systems connecting to the network through an Extreme Access Control deployment that is implementing agent-based assessment. Use this window to add a new operating system definition to the list. For example, use this window when to add a Windows operating system with a different service pack requirement. To add a new operating system, click the **Add** button at the top of the list and enter the operating system type and family.



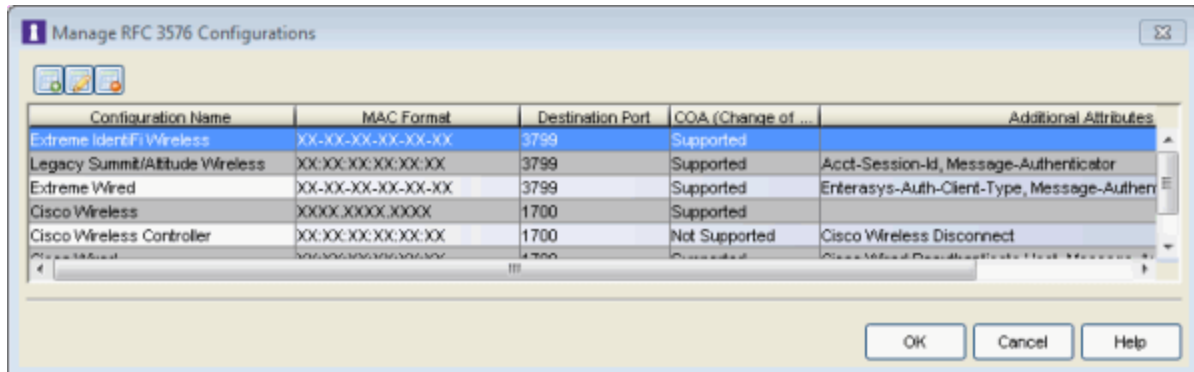
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Manage RFC 3576 Configurations Window

This window displays a table of RFC 3576 configurations and their associated data. Use this window to add a new RFC 3576 configuration or edit an existing one. To access this window, click the Manage RFC 3576 Configurations button in the [New/Edit Switch Reauthentication Configuration window](#).



Use the add or edit button to open the [New/Edit RFC 3576 Reauthentication Configuration window](#) where you can create a new RFC 3576 configuration or edit an existing one.

Configuration Name

The name of the configuration; typically, the name of the switch type.

MAC Format

Specifies how the MAC address of an end-system is formatted when it is sent to the switch during RFC 3576 Disconnect or Change of Authorization (CoA) messages. MAC formats are specified using lower-case 'x' characters as lowercase hexadecimal digits, and upper-case 'X' characters as uppercase hexadecimal digits. All other characters are translated literally.

Destination Port

The switch port to which Disconnect or Change of Authorization (CoA) messages are sent.

Change of Authorization

Displays whether the switch supports Change of Authorization (CoA) messages as defined in RFC 3576.

Additional Attributes


The RADIUS [attributes](#) added to the Disconnect or Change of Authorization (CoA) messages sent to the switch.

Related Information

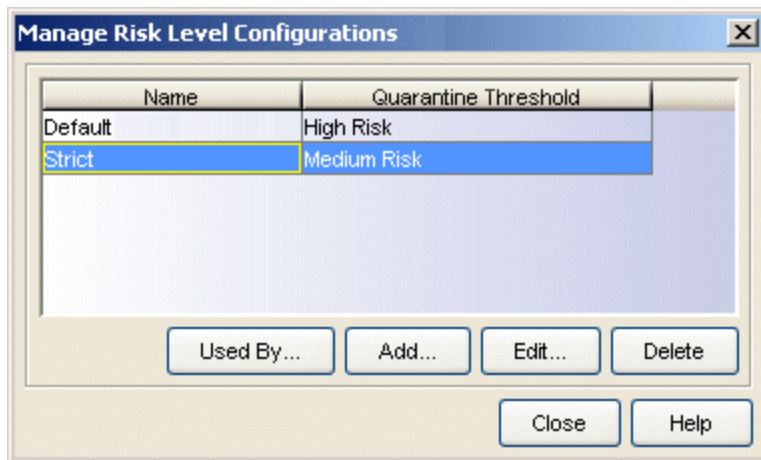
For information on related windows:

- [Add/Edit Appliance Settings Window](#)
- [New/Edit Switch Reauthentication Configuration Window](#)

Manage Risk Level Configurations Window

This window lets you view and define the risk level configurations used in your assessment configurations. To access this window, click  (the configuration menu button next to the Risk Level Configuration field) in the [Edit Assessment Configuration window](#) and select **Manage**.

Risk level configurations determine what risk level to assign to an end-system (high, medium, or low) based on the end-system's health result details score. NAC Manager uses this risk level to determine whether or not to quarantine the end-system. You can create multiple risk level configurations to provide more granularity in determining end-system risk level.



Name

The name of the Risk Level configuration.

Quarantine Threshold

The threshold used to determine whether or not an end-system is quarantined. The criteria for this threshold is defined in the [Add/Edit Risk Level Configuration window](#).

Used By Button

Opens a window that lists all assessment configurations currently using the selected risk level configuration.

Add Button

Opens the [Add Risk Level Configuration window](#) where you can define a new risk level configuration.

Edit Button

Opens the [Edit Risk Level Configuration window](#) where you can edit the selected risk-level configuration.

Delete Button

Deletes the selected risk level configuration(s).

Related Information

For information on related tasks:

- [Edit Assessment Configuration Window](#)
- [Add/Edit Risk Level Configurations Window](#)

Manage Rule Groups Window


This window lists the various rule groups used to define the criteria for the rules used in your NAC configuration. Use this window to view and edit the defined rule groups and to add new rule groups for use in your NAC configuration. Any changes made in this window are written immediately to the NAC Manager database.

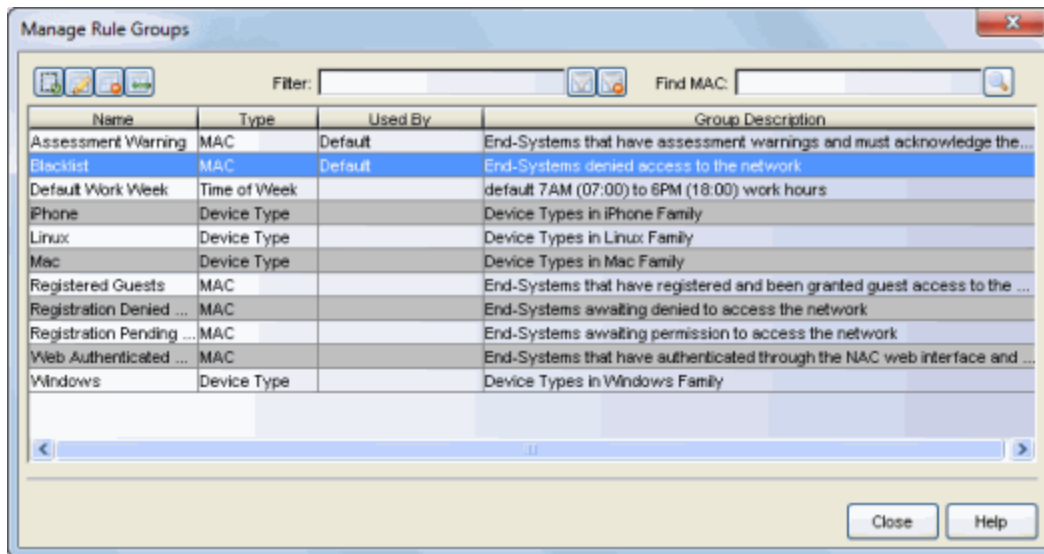
NAC Manager comes with eleven system-defined rule groups. There are six system-defined end-system groups automatically populated by NAC Manager. The first is the Assessment Warning end-system group that includes end-systems with assessment warnings and must acknowledge them before being granted access to the network. The second is the Blacklist end-system group that includes end-systems denied access to the network. The other four system-defined groups are populated as end-systems register through the Registration portal. In addition, there is one system-defined time group called Default Work Week and six system-defined device type groups called Android, Apple iOS, BlackBerry, Linux, Mac, and Windows.

When you create a new rule group, you can select from the following rule group categories:

Category	Group Types	Value Types
User Groups	Username	A list of usernames which can be based on an exact match or a wild card.
	LDAP User Group	A list imported from an LDAP Server, organized by Organization Unit (OU).
	RADIUS User Group	A list of attributes returned by the RADIUS server.
End-System Groups	MAC	A list of MAC addresses, MAC OUI, or MAC Masks.
	IP	A list of IP addresses or subnets.
	Hostname	A list of hostnames: exact match or wild card (for example, *.extremenetworks.com).
	LDAP Host Group	A way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network.
Device Type Groups	Device Type	A list of device types.

Category	Group Types	Value Types
Location Groups	Location	A list of switches, switches and ports, or switches and SSIDs.
Time Groups	Time of Week	A weekly time range.

To access this window, select the **Manage Rule Groups** button  in the NAC Manager toolbar or select Tools > Management and Configuration > Rule Groups from the menu bar.



Use these buttons to add, edit, or delete rule groups, or to import MAC entries from a file for viewing and assigning to various end-system groups.

Filter

Use the Filter field to filter for a specific group based on a numeric value or text. For delimited values such as a MAC or IP address, use the same delimiter used in the group.

Find MAC

Find a MAC address in an end-system group by entering a complete MAC address and clicking the **Search** button.

Name

The name of the rule group.

Type

The type selected for the specific rule group. For example, an end-system group with a type of MAC.

Used By

The name of the NAC configuration using this rule group.

Group Description

A description of the rule group.


Related Information

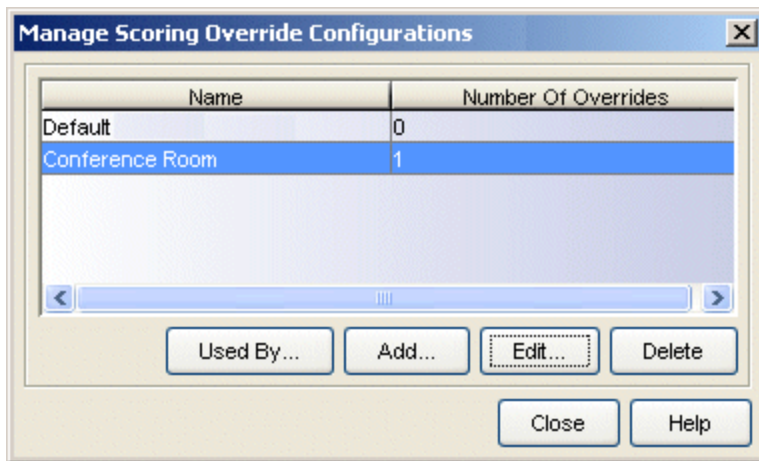
For information on related windows:

- [NAC Configuration Window](#)
- [Create Rule Window](#)

Manage Scoring Override Configurations Window

This window lets you view and define the scoring override configurations used in your assessment configurations. Scoring overrides let you override the test scores automatically assigned to the individual tests performed during end-system assessment.

To access this window, click  (the configuration menu button next to the Scoring Override Configuration field) in the [Edit Assessment Configuration window](#) and select **Manage**.



Name

The name of the scoring override configuration.

Number of Overrides

The number of individual overrides defined for the scoring override configuration.

Used By Button

Opens a window that lists all assessment configurations currently using the selected scoring override configuration.

Add Button

Opens the [Add Scoring Override Configuration window](#), where you can define a new scoring override configuration.

Edit Button

Opens the [Edit Scoring Override Configuration window](#), where you can edit the selected scoring override configuration.

Delete Button

Deletes the selected scoring override configuration(s).

Related Information

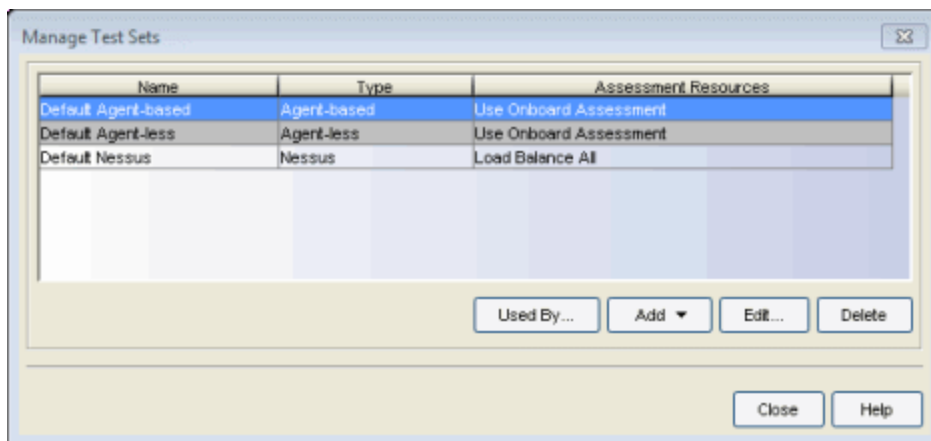
For information on related tasks:

- [Edit Assessment Configuration Window](#)
- [Add/Edit Scoring Override Configuration Window](#)

Manage Test Sets Window

This window lets you view and define the test sets used in your assessment configurations. Test sets let you define what type of assessment to execute, what parameters to pass to the assessment server, and which resources to use. NAC Manager provides four default test sets; one for each type of assessment agent that is either supplied or supported by NAC Manager. You can use these default test sets "as is" or edit them, if desired. When you add a new test set, it becomes available for selection in the [Edit Assessment Configuration window](#).

To access this window, click  (the configuration menu button) in the Test Sets section of the [Edit Assessment Configuration window](#) and select **Manage Test Sets**.



Name

The name of the test set.

Type

The type of assessment server used in the test set.

Assessment Resources

Specifies the network assessment servers that perform the assessments for the test set:

- **Load Balance All** — The assessment load is balanced across all of the servers of the specified type on the network.
- **Use Assessment Server Pool** — The specified assessment server pool is used to perform the assessments.

- **Use Onboard Assessment** — The onboard assessment server is used to perform the assessments.

Used By Button

Opens a window that lists all assessment configurations currently using the selected test sets.

Add Button

Use this button to add a new test set.

Edit Button

Opens a window where you can edit the selected test set.

Delete Button

Deletes the selected test sets.

Related Information


For information on related tasks:

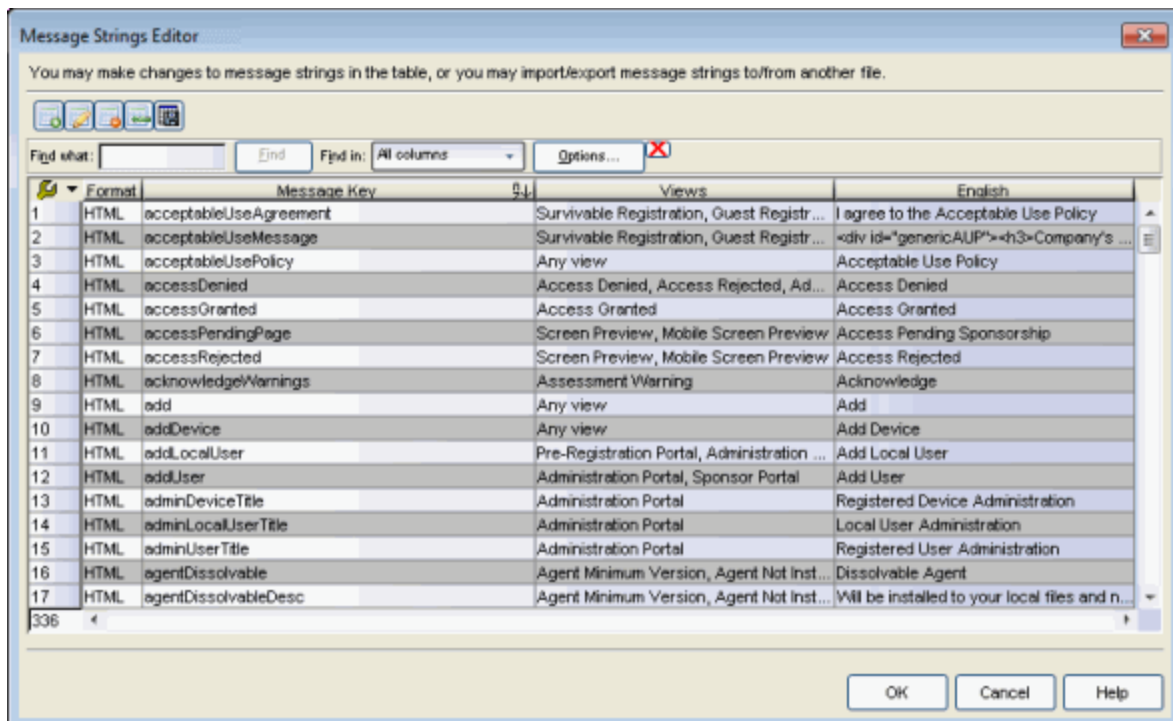
- [Edit Assessment Configuration Window](#)

Message Strings Editor

The Message Strings Editor allows you to edit the text and formatting of the various system-defined messages used on the portal web pages, or add a custom message string, if desired. You can also import a file of message strings or export message strings to a file.

To access the Editor, click the Message Strings **change** link in the Portal Look and Feel view in the NAC Configuration window. Message strings are listed alphabetically according to the Message Key, which is the message identifier. Double-click a message string to open a window where you can edit the message.

Use the table options and tools to find, filter, sort, and print information in the table. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the **Table Tools**  button in the upper left corner of the table (if the row count column is displayed). For more information, see Table Tools.



Use the toolbar buttons to add or change message strings, import a file of message strings or export the message strings to a file.



Add New Message

Opens the Add Localized Entry window where you can add a new message. Enter a Message Key to identify the message and then the text for the message.



Edit Message

Select a message in the table and click this button (or double-click the message) to open the Modify Localized Entry window, which allows you to modify the text for the message. Use the Next/Previous buttons in the window to cycle through all the message strings for easy editing.

NOTE: To change the Message Key for a user-defined message, you must delete and recreate the message using the new key.



Delete Message

Deletes a selected message in the table. You can only delete user-defined messages.



Import Messages

Opens a window where you can select a file of message strings to import for a selected locale. The list of locales includes the [default locale](#) and any [supplemental locales](#) defined in the portal configuration.

Message strings in the file must be in the following format:

messageKey=messageValue

with messageKey being the message identifier and messageValue being the message text.

CAUTION: Importing message strings from a file overwrites the corresponding default message strings for the selected locale. For example, if you import a file with 15 message entries, only the default messages for those 15 entries are overwritten. The other default messages for that locale remain.



Export Messages

Opens a window where you can export messages for a selected locale to a file. In the Export window, select the locale to export. The list of locales includes the [default locale](#) and any [supplemental locales](#) defined in the portal configuration. Specify the encoding to use:

- Native — Use this encoding if you want to read the file in the native language.

- UTF-8 — Use this encoding to export a file in a readable format that you can share. For example, if you export a French locale file and send it to someone in Japan, the characters display correctly (providing the Japanese system can display French characters).
- UTF-8 with Unicode — Use this encoding to export the file in order to use it (import it) on another Extreme Management Center server or client. Note: Non-ASCII characters are not readable and it displays as \u####.

Select the Include System-Defined Messages checkbox to include in the export file all the system-defined messages provide by NAC Manager.

Message Strings Table

This table displays all the message strings used in NAC Manager. It includes the following columns:

- Format — Displays the supported format for the message text: HTML or Text.
 - Message Key — The message identifier.
 - Views — The NAC portal views where this message is used.
 - English — The text of the message.
 - Additional columns for each supplemental locale (language) you configure in the portal configuration.
-

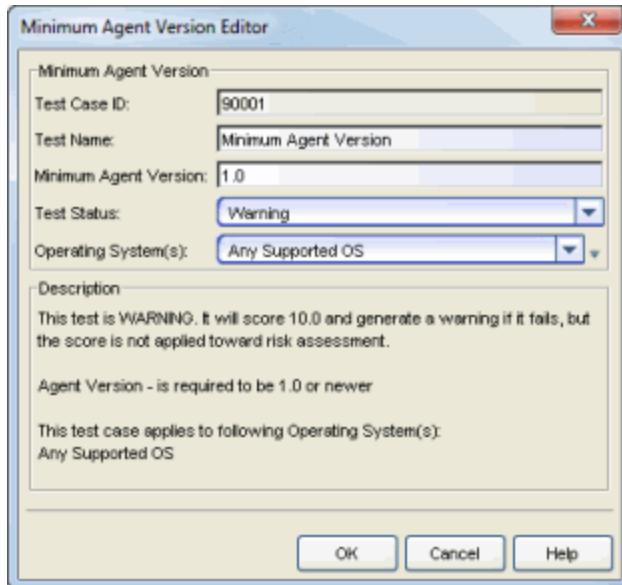
Related Information

For information on related help topics:

- [Portal Configuration](#)

Minimum Agent Version Editor

This window lets you configure parameters for the Minimum Agent Version test case included in an [agent-based test set](#). This test checks to see if the agent version on the end-system is the same as, or newer than, the version level specified here.



The screenshot shows a dialog box titled "Minimum Agent Version Editor". It contains the following fields and options:

- Test Case ID: 90001
- Test Name: Minimum Agent Version
- Minimum Agent Version: 1.0
- Test Status: Warning (dropdown menu)
- Operating System(s): Any Supported OS (dropdown menu)

The Description field contains the following text:

This test is WARNING. It will score 10.0 and generate a warning if it fails, but the score is not applied toward risk assessment.

Agent Version - is required to be 1.0 or newer

This test case applies to following Operating System(s):
Any Supported OS

Buttons: OK, Cancel, Help

Test Case ID

The Minimum Agent Version test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Minimum Agent Version

Enter the agent version that the end-system will be matched against.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

NAC Configuration Window


The NAC Configuration lets you manage the end user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, device type, and location. NAC Manager comes with a default NAC Configuration which is automatically assigned to your Extreme Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

The NAC Configuration window provides access to the various NAC components used to configure different aspects of NAC. This Help topic talks about the Features panel. The other components are discussed in separate Help topics that can be accessed from the links below.

- [Accessing the NAC Configuration](#)
- [Features](#) - Enable the registration, access, and assessment/remediation features you want for your network.
- [Rules](#) - Define the rules that are used by the NAC configuration to assign a NAC Profile to a connecting end-system.
- [AAA Configuration](#) - Define the RADIUS and LDAP configurations that provide the authentication and authorization services for your Extreme Access Control engines.
- [Portal Configuration](#) - Configure the portal website used by the end user during the registration or remediation process.

Accessing the NAC Configuration

Use the following steps to access the NAC Configuration:

1. Click the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
2. In the NAC Configuration window, a left-panel tree that provides access to different NAC components displays. Select the component you wish to edit and make the desired changes.
3. Save any changes made in this window. Enforce the NAC configuration to the engine group.

Features

Use the Features panel to enable or disable the registration, access, and assessment/remediation features you want available to users connecting to the network.

1. Open the NAC Configuration window. Make sure that the Features icon is selected in the left-panel tree.
2. To enable a feature, click the **Enable Feature** button. A menu is displayed with the following features:
 - Guest Registration/Access - Allows unauthenticated access to the network via Guest Registration, Guest Web Access, or Secure Guest Access.
 - Authenticated Registration/Access - Allows authenticated access to the network via Authenticated Registration or Authenticated Web Access.
 - Assessment/Remediation - Allows presentation of vulnerabilities to the end user with links to resources to correct the issues.
 - Advanced Location-Based Access - Allows for the definition of different access features based on location of an end-system. If you select Advanced Location-Based Access, a window opens where you can configure a location. If you are configuring multiple locations, you must use the **Enable Feature** menu each time you want to configure a location.

Select the desired feature. When you enable a feature, it is listed in the Summary section of the Feature panel. Use the menu to select each feature you want to enable.

3. If you selected **Guest Registration/Access**, use the drop-down menu to select the desired access type:
 - Guest Registration - Allows unauthenticated access to the network for the length of the registration. Registration also has provisions for capturing end-user specific information during the registration process.
 - Guest Web Access - Allows presentation of an Acceptable Use Policy to the guest user and allows guest access to the network for the

duration of their session. On each subsequent attempt to access the network, the user is presented with the Guest Web Access login page.

- Secure Guest Access - Allows a guest to gain secure wireless access to your network via 802.1x (PEAP) authentication using credentials that are created when the user registers onto an open SSID. The registration can be configured to expire if desired to allow only temporary access to your network.

After selecting the appropriate type, click on the Guest Registration/Access link to open the portal configuration page where you can configure the corresponding parameters. Refer to the [Portal Configuration](#) Help topic for more information.

4. **If you selected Authenticated Registration/Access**, use the drop-down menu to select the desired type:
 - Authenticated Registration - Allows authenticated access to the network for the length of the registration. Registration also has provisions for capturing end-user specific information during the registration process.
 - Authenticated Web Access - Allows presentation of an Acceptable Use Policy to the user and allows authenticated access to the network for the duration of their session. On each subsequent attempt to access the network, the user is redirected to the Authenticated Web Access login page.

After selecting the appropriate type, click on the Authenticated Registration/Access link to open the portal configuration page where you can configure the corresponding parameters. Refer to the [Portal Configuration](#) Help topic for more information.

5. **If you selected Assessment/Remediation**, click on the Assessment/Remediation link to open the portal configuration page where you can configure the corresponding parameters. Refer to the [Portal Configuration](#) Help topic for more information.
6. **If you selected Advanced Location-Based Access**, use the [Advanced Location-Based Registration and Web Access Behavior window](#) to configure your access.

Related Information

For information on related windows:

- [AAA Configuration](#)
- [NAC Configuration Rules](#)
- [Portal Configuration](#)

NAC Configuration Rules


The NAC Configuration Rules panel displays a list of rules that are used by the NAC Configuration to assign a NAC Profile to a connecting end-system based on rule criteria.

This Help topic provides information for accessing and configuring NAC Configuration Rules:

- [Accessing NAC Configuration Rules](#)
- [Viewing Rules in the Table](#)
- [Creating and Editing Rules](#)

Accessing NAC Configuration Rules

Use the following steps to view and edit your NAC Configuration rules.



1. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the **Edit** button in the [Configuration tab](#).
2. In the left-panel tree, select the Rules icon. The table of your NAC rules is displayed in the right panel. See below for an explanation of the table columns.
3. Use the Rules toolbar buttons to create a new rule or perform actions on the rules. See below for a description of each button.
4. Click **Save** to save your changes.

Viewing Rules in the Table

The Rules table displays the rule name, whether the rule is enabled, and summary information about the rule. It also shows the NAC Profile assigned to any end-system that matches the rule and the portal redirection action, if applicable. Rules are listed in order of precedence. End-systems that do not match any of the listed rules are assigned the Default Catchall rule.

TIP: Right click on a rule in the table to access a menu of options including the ability to edit the NAC profile and any user groups included in the rule.

Enabled

This column displays whether the rule is enabled  or disabled . Right-click on the rule to access a menu where you can enable or disable the rule. You cannot disable any of the system rules provided by NAC Manager.

Rule Name


This column displays the rule name. Double-click on the rule to open the Edit Rule window where you can edit the rule name, if desired. You cannot change the name of the system rules provided by NAC Manager.

Conditions

This column displays the criteria an end-system must meet in order to be assigned the rule, including the authentication method and rule groups that the end-system or user must match. Double-click on the rule to open the Edit Rule window where you can edit the rule criteria, if desired. You cannot change the criteria for the system rules provided by NAC Manager. Click on a rule group name to open a window where you can edit the group's parameters.

Actions

This column displays the actions the rule takes when an end-system matches the rule's criteria. This includes the profile assigned to the end-system and the portal configuration that the end user sees. Click on the profile or portal name to open a window where you can make changes, if desired.

You may see additional columns in the table that were added using the Show Columns option from the Tools and Display Settings menu button . You can see definitions for these columns [below](#).

Creating and Editing Rules

Use the Rules toolbar buttons to create, edit, and modify the rules in the table. Any changes made in this table are written immediately to the NAC Manager database.



Move Rule Up/Down

Move rules up and down in the list to determine rule precedence.



Add New Rule

Opens the [Create Rule window](#) where you can define a new rule to use in the NAC configuration.

TIP: To add a new rule at a specific location in the table, select the rule that you want the new rule to follow, right-click and select Add Rule after Selection. When you create the new rule and click **OK**, it is added after the selected rule. The selected rule must be a custom (user-defined) rule, or it can be the Blacklist or Assessment Warning rule.

 **Edit Rule**

Opens the [Edit Rule window](#) where you can edit the rule criteria for a selected rule.

 **Delete Selected Rules**

Deletes any rules selected in the table.

 **Configure Zone on Selected Rules**

Opens the Configure Rule Zone window where you can select an end-system zone to associate with the selected rules and create a new zone, if needed. See [End-System Zones](#) for more information.

 **Tools and Display Settings**

Provides a menu of the following options:

- **Show All Rules** — Displays all rules including user-created custom rules as well as NAC Manager system rules, such as the blacklist, assessment warning, and catch-all rules. If Registration is enabled, you also see system rules that assign profiles to end users based on registration states.
- **Show User Created Rules Only** — Displays user-created custom rules only. System rules are not displayed.
- **Advanced Rule Ordering** — If you added custom rules and want to change the order of custom and system rules in the list, enable the Advanced Rule Ordering option.
- **Display Verbose** — In Verbose mode, the table displays additional information in the Actions column, including links for editing the rule actions.
- **Display Compact** — In Compact mode, table information is displayed in a compact format. Rest your cursor on the columns to view tooltips that provide additional Actions information and links.
- **Display Tooltips** — Use the checkbox to disable the tooltips in the rules table.
- **Show Columns** - Select additional columns to display in the table:
 - **Authentication Method** — The authentication method the end-system must match in order to be assigned the rule.

- User Group — The user group the end-system must match in order to be assigned the rule.
 - End-System Group — The end-system group the end-system must match in order to be assigned the rule.
 - Location Group — The location group the end-system must match in order to be assigned the rule.
 - Time Group — The time group the end-system must match in order to be assigned the rule.
 - Device Type Group — The authentication method the end-system must match in order to be assigned the rule.
 - Profile — The profile assigned to the end-system when it matches the rule's criteria.
 - Portal Override — The portal configuration the end user sees when it matches the rule's criteria.
 - Zone — The end-system zone that the connection request must match in order to be assigned the rule.
- **Run Configuration Evaluation Tool** — Opens the [Configuration Evaluation Tool window](#) where you can test the rules defined in your NAC Configuration to evaluate what behavior an end-system encounters when it is authenticated on a Extreme Access Control engine.
 - **Launch Rule Configuration Wizard** — Opens the Rule Configuration Wizard which guides you through the process of creating and configuring rules for your NAC configuration.
 - **Manage Policy Mapping Configuration** — Opens the Edit Policy Mapping Configuration window where you can edit the policy mappings used by your NAC profiles.
-

Related Information

For information on related windows:

- [AAA Configuration](#)
- [NAC Configuration](#)
- [Portal Configuration](#)

NAC Manager Options Window

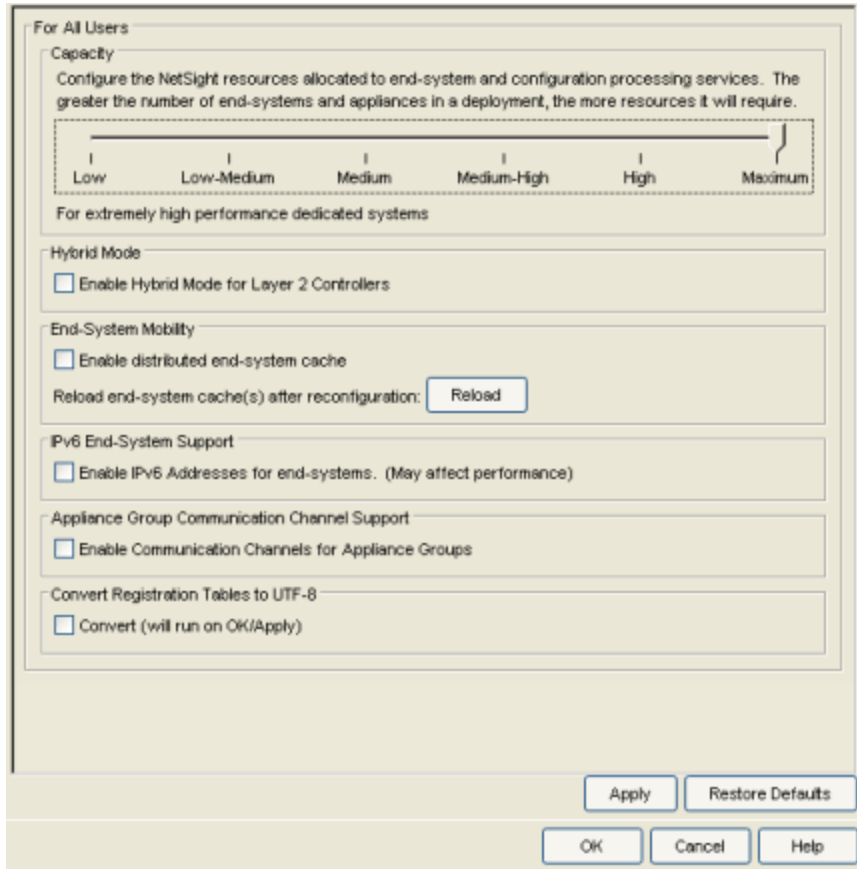
These options apply only to your Extreme Access Control (Access Control) deployment and the settings in the NAC Manager application. In the Options window (**Tools > Options**), the right-panel view changes depending on what you select in the left-panel tree. Expand the NAC Manager folder to view all the different options you can set.

Information on the following NAC Manager options:

- [Advanced Settings](#)
- [Assessment Server](#)
- [Data Persistence](#)
- [Display](#)
- [End-System Event Cache](#)
- [Enforce Warning Settings](#)
- [Features](#)
- [Notification Engine](#)
- [Policy Defaults](#)
- [Port Wizard Defaults](#)
- [Status Polling and Timeout](#)

Advanced Settings

This Options view lets you configure advanced settings for NAC Manager. These settings apply to all users on all clients.



Capacity

The Capacity option lets you configure the Extreme Management Center (Management Center) resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

Hybrid Mode

A Layer 2 Access Control Controller engine can be configured for Hybrid Mode, which allows it to act as a RADIUS proxy for switches, like a Access Control Gateway engine. Select this option to enable Hybrid Mode for your Layer 2 Controllers at a global level. When the option is selected, the Configuration tab for a Layer 2 Controller displays an option to enable Hybrid Mode for that specific controller. For more information, see the [Configuration tab](#) Help topic. Disabling Hybrid Mode at the global level when a controller acts as a reference to switches is similar to deleting a gateway: the controller is removed as a reference from the switches.

End-System Mobility

The **Enable distributed end-system cache** option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling this option improves NAC Manager performance when discovering new end-systems as they connect, or when end-systems move from one place to another in the network.

To use the end-system cache feature, it must be enabled on both the Management Center Server (using this option) and on the Access Control engines using the cache (using the [Access Control Appliance Advanced Configuration window](#)).

When this feature is enabled, the Management Center Server and the Access Control engine exchange additional data each time end-system data is updated. This feature is **not** recommended unless there is sufficient network bandwidth for the additional data, a fast connection between the Management Center Server and the Access Control engine, and end-systems are adding or moving frequently.

When you enable or disable this option, you must click the **Reload** button to reload the cache configuration on the Management Center server.

The **Reload** button is also used if you configure [communication channels](#) for the engine groups on your network. Reload when you first configure your channels and also any time you change your channel configuration. Reload redistributes the end-system information to the new channels.

CAUTION: The Reload operation may take some time and network communication may be temporarily disrupted.

IPv6 End-System Support

The **Enable IPv6 Addresses for end-systems** option allows NAC Manager to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems needs to rediscover their IP addresses in order to reflect the change in the end-system table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system.

Only end-systems with a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems with only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see NAC Manager IPv6 Support in the Management Center Configuration Considerations Help topic.

Appliance Group Communication Channel Support

The **Enable Communication Channels for Appliance Groups** option allows you to create logical groupings of your Access Control engine groups in order to segment data and limit network traffic between geographical or customer sensitive locations. This is an advanced NAC Manager feature and is only appropriate in certain network scenarios. For more information and complete configuration instructions, see [How to Configure Communication Channels](#).

Assessment Server

These options let you schedule updates to NAC Manager assessment server software and provide assessment agent adapter credentials. The options apply to all users on all clients.

The Schedule Updates option pertains only to on-board agent-less assessment servers and allows you to schedule routine checks for assessment server software updates using the web update operation. The web update feature automatically recognizes when an updated version of NAC Manager assessment server software is available and allows you to download the newer version to keep your software current. The update operation uses the Suite Web Update server and proxy settings, which are configured in the Suite Options Web Update view. If your network is behind a firewall, you must specify the HTTP Proxy server being used.

NOTE: The web update feature downloads any updated assessment server software but does not perform the actual upgrade to the assessment server. The actual upgrade must be performed using the **Upgrade** button in the [Manage Assessment Settings](#) window with the Assessment Servers tab selected.

Perform the Check for Assessment Updates and the Upgrade operation at least every two weeks to ensure that the assessment servers are running the latest scanner software that includes the most up-to-date virus definitions.

Because the on-board agent-less assessment license is subscription-based, the Upgrade operation must be performed at least once a month in order to upgrade the license. If the engine is unable to contact the upgrade server, contact Extreme Networks Support so they can provide a special license.

For All Users

Schedule Updates to NAC Assessment Server Software

Uses Suite Web Update Server and Proxy Settings

Last checked for updates: None

Weekly

On: Friday At: 2:52 PM

Assessment Agent Adapter Credentials

Username: admin

Password: *****

Show Passwords Requires Manual Updates to Assessment Agent Adapters

Apply Restore Defaults

OK Cancel Help

Schedule Updates

This section displays the last time a check occurred and lets you define the specific time to check for updates. Use the drop-down menu to set the frequency (**Daily**, **Weekly**, **Disabled**) for checking for updates. If you specified a **Weekly** check, use the drop-down menu to select the day of the week you wish the check to be performed, and set the desired time. If you specified a **Daily** update, set the desired time.

Assessment Agent Adapter Credentials

The password the Access Control engine uses when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server that is not supplied or supported by NAC Manager). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. NAC Manager provides a default password that can be changed, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For instructions, see [How to Change the Assessment Agent Adapter Password](#).

Data Persistence

This Options view lets you customize how NAC Manager ages-out or deletes end-systems, end-system events, and end-system health results (assessment results) from the tables and charts in the [End-Systems tab](#) and the [Statistics tab](#). These settings apply to all users on all clients.

For All Users

Run Data Persistence Checks each day at 02:00 AM

Age End-Systems
 Age End-Systems older than 90 Days
 Remove Associated MAC Locks and Occurrences in Groups
 Remove Associated Registration Data

End-System Event Persistence
 Persist Non-Critical End-System Events
 Delete Events older than 90 Days

End-System Information Events
 Generate NAC Manager Events when End-System Information is modified

Transient End-Systems
 Delete Transient End-Systems older than 1 Days
 Delete Rejected End-Systems

Health Result Persistence
 Save a health result summary for the last 30 health results per end-system
 Save the details for the last 5 health results per end-system
 Only persist health result details for quarantined end-systems (with the exception of agent-based results)
 Persist duplicate health result summary and details

Wireless End-System Events
 Process and include wireless end-system events in End-System event logs.

Apply Restore Defaults

OK Cancel Help

Run Data Persistence Checks

Set the time that the Data Persistence Check are performed each day.

Age End-Systems

Each day, when the Data Persistence check runs, it searches the database for end-systems NAC Manager did not receive an event for in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the [End-Systems tab](#).

If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

The **Remove Associated Registration Data** checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.

End-System Event Persistence

Select the checkbox if you want NAC Manager to store non-critical end-system events, which are events caused by an end-system reauthenticating. End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes all end-system events which are older than the number of days specified (90 days by default).

End-System Information Events

Select the checkbox if you want NAC Manager to generate an event when end-system information is modified.

Transient End-Systems

This option lets you configure the number of days to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are Unregistered end-systems not seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them.

Select the **Delete Rejected End-Systems** checkbox if you want end-systems in the Rejected state to be deleted as part of the cleanup.

You can also delete transient end-systems using the Tools > End-System Operations > Data Persistence option.

Health Result Persistence

This section lets you specify how many health result (assessment results) summaries and details are saved and displayed in the [End-Systems tab](#) for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system along with detailed information for the last five health results per end-system. You can change these values if desired.

There are two additional options:

- You can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).
- You can specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are **not** saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are

not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results are saved.

Wireless End-System Events

Select the checkbox if you want NAC Manager to generate an event when wireless end-system information is modified. This option is disabled by default.

Display

This Options view lets you select how you want to display Extreme Access Control (Access Control) engine names in the left-panel tree, how to display end-system MAC addresses in right-panel tables, and whether to limit table rows in the End-Systems Activity tab and NAC (Access Control) Appliances Activity tab in the Event View. These settings apply only to the current user.

For Current User

Display NAC Appliance Names by:

IP Name Name/IP P/Name

Limit Table Rows

Limit End-Systems Activity Rows to: 5000

Limit NAC Appliances Activity Rows to: 5000

Ignored Dialog Boxes

Re-show all ignored dialog boxes

Re-Show All

Dialog Settings

Reset all secondary dialogs to default size and screen placement

Reset All

Welcome View

Display Welcome View

Custom End-System Information Display Settings

Custom End-System Information Labels

Custom 1: Custom 1

Custom 2: Custom 2

Custom 3: Custom 3

Custom 4: Custom 4

End-System Table Performance:

Display group membership data for the End-System Table

Display Counts:

Displayed NAC Gateways Per Switch: 2

Apply Restore Defaults

OK Cancel Help

Display NAC (Access Control) Appliance Names by

Specify how you want to display Access Control engines in the left-panel tree. You can display the engine's IP address, the name assigned when creating the engine, or a combination of the name and IP address.

Display MAC Addresses by

Specify how you want to display end-system MAC addresses in right-panel tables. You can display them as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix. This allows you to display the associated vendor the MAC address belongs to, if an OUI mapping exists. You can also limit the vendor name to a certain number of characters, if

desired.

When the **Display Unknown MACs as Unknown** checkbox is selected, the MAC address for unknown users is displayed as "Unknown" in the End-Systems view. If the checkbox is not selected, the pseudo MAC address assigned to each device is displayed instead of "Unknown" for end-systems learned on an L3 controller.

Limit Table Rows

These options allow you to limit the number of table rows displayed in the End-Systems Activity tab and NAC (Access Control) Appliances Events tab in the Event View.

Ignored Dialog Boxes

Click the **Re-Show All** button to turn on the display of messages that are turned off in individual message dialog box(es).

Dialog Settings

Click the **Reset All** button to reset all NAC Manager secondary windows to their default size and screen placement.

Welcome Panel

This option lets you hide and show the Welcome Panel that is displayed when you first open NAC Manager and the All NAC (Access Control) Appliances folder is selected in the left-panel tree.

Custom End-System Information Labels

This option lets you specify new text for the Custom column headings in the [End-System table](#) on the End-Systems tab.

End-System Table Performance

Use this option to display group membership data in the End-Systems tab. Deselecting this option removes the Groups column from the End-Systems table and allows the table data to display faster. The option takes effect when the table is loaded (e.g. when you click on the End-Systems tab and the table is displayed).

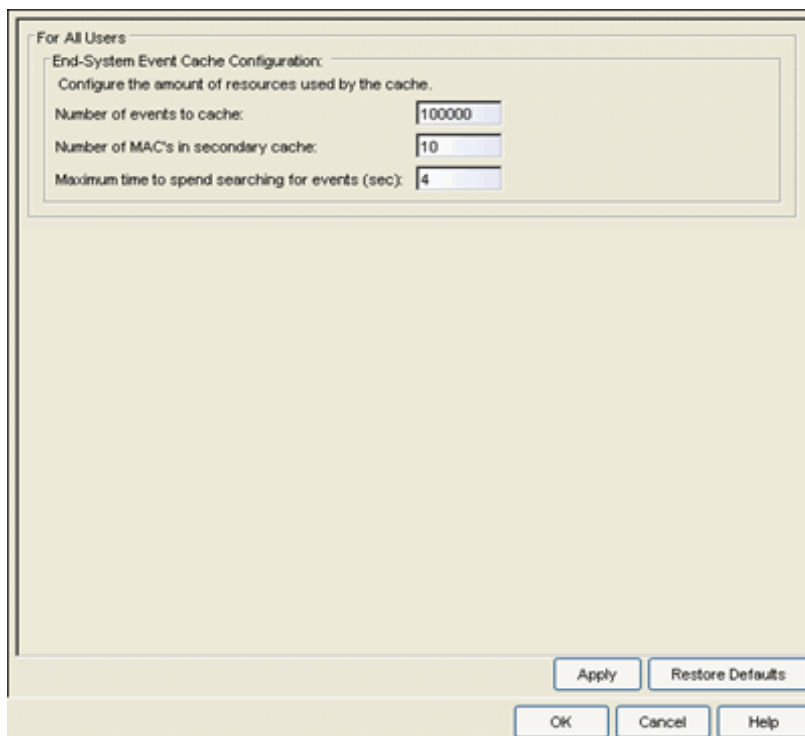
Display Counts

This option allows you to configure up to four redundant Access Control Gateways per switch in the [Add](#) or [Edit Switches in NAC \(Access Control\) Appliance Group](#) windows. By default, these windows allow you to configure two Access Control Gateways per switch for redundancy. You can use this option to increase the number up to three or four gateways per switch.

End-System Event Cache

End-system events are stored in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them in the [End-System Events tab](#). This cache allows NAC Manager to quickly retrieve and display end-system events without having to search through the database.

These options let you configure the amount of resources used by the end-system event cache. These settings apply to all users on all clients.



The screenshot shows a dialog box titled "For All Users" with the subtitle "End-System Event Cache Configuration". Below the subtitle, it says "Configure the amount of resources used by the cache." There are three input fields: "Number of events to cache:" with the value "100000", "Number of MAC's in secondary cache:" with the value "10", and "Maximum time to spend searching for events (sec):" with the value "4". At the bottom of the dialog, there are four buttons: "Apply", "Restore Defaults", "OK", "Cancel", and "Help".

Number of events to cache

Specify the number of events to cache. Keep in mind that the more events you cache, the faster data is returned, but that caching uses more memory.

Number of MACs in secondary cache

The End-System Event Cache also keeps a secondary cache of events by MAC address. This means that a particular end-system's events can be more quickly accessed in subsequent requests. Use this field to specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note that the secondary cache may include events that are not in the main cache, but were retrieved by scanning the database outside the cache boundary.

Maximum time to spend searching for events (in seconds)

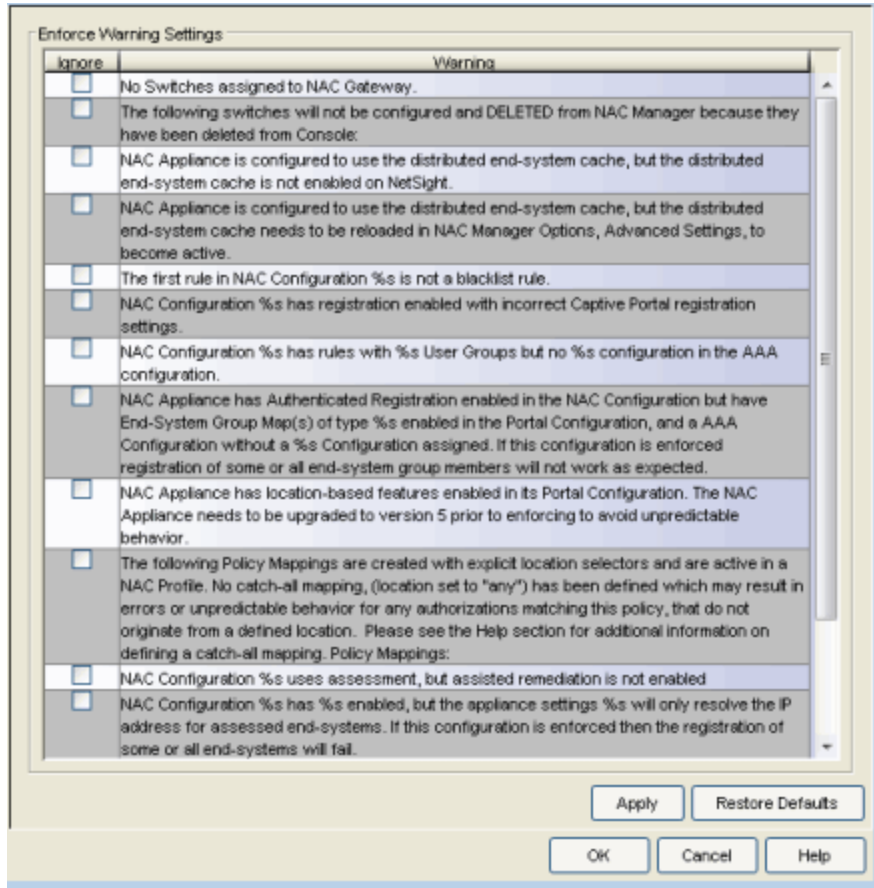
This option specifies the time Extreme Management Center spends when searching for older events outside of the cache. (The search is initiated by using the **Search for Older Events** button in the [End-System Events tab](#).) The search is ended when the number of seconds entered is reached.

Enforce Warning Settings

When an engine configuration audit is performed during an Enforce operation, warning messages may be displayed in the audit results listed in the Enforce window. If a warning occurs for an engine, acknowledge the warning and proceed with the enforce anyway.

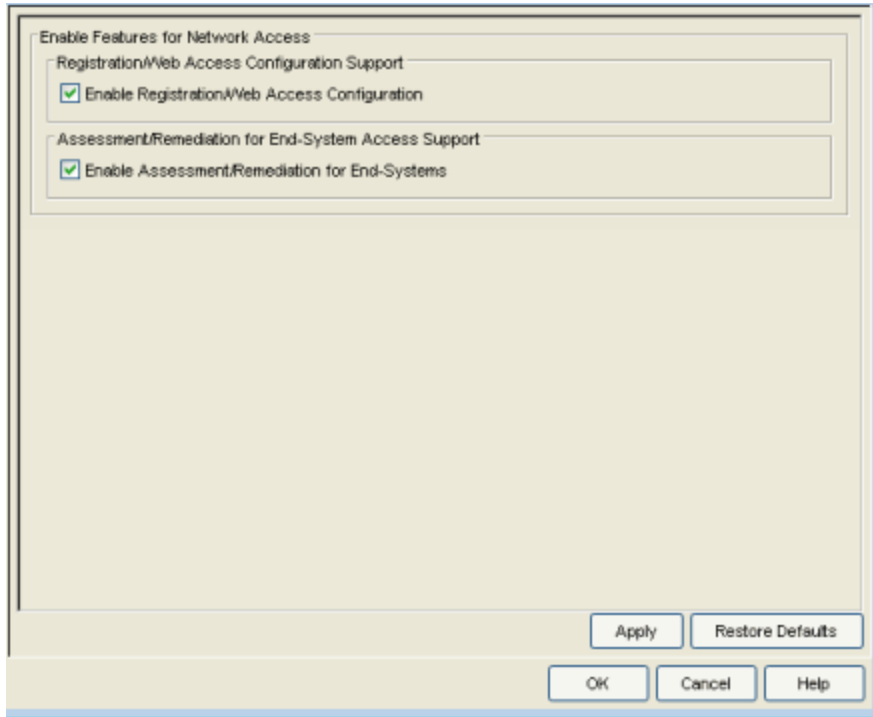
These settings allow you to select specific warning messages you do not want to display in the audit results. This allows you to proceed with the Enforce without having to acknowledge the warning message. For example, a NAC configuration that always results in one of these warning messages. By selecting that warning here, it is ignored in future audit results and you no longer need to acknowledge it before proceeding with the Enforce.

Select the checkbox in the **Ignore** column next to the warning message that you don't want displayed and click **OK**.



Features

This Options view lets you enable registration and web access configuration support, as well as assessment/remediation for end-system access support. If you are not using these features, you can disable them to remove sections that pertain only to those features from certain NAC Manager windows.



Notification Engine

Selecting Notification Engine in the left panel of the Options window provides the following view where you can define the default content contained in NAC Manager notification action messages. For example, with an email notification action, you can define the information contained in the email subject line and body. With a syslog or trap notification action, you can specify certain information that you want contained in the syslog or trap message. These settings apply to all users.

For All Users

Notify Action Defaults

E-Mail Subject: NetSight \$type Trigger \$trigger

E-Mail Body: Conditions: \$conditions
IP: \$ipaddress
MAC: \$macaddress

Syslog Tag: NetSight

Syslog Message: NetSight \$type Trigger \$trigger conditions \$conditions

Trap OID: 1.3.6.1.6.3.1.1.4.1

Trap Message: NetSight \$type Trigger \$trigger conditions \$conditions

Trap Message OID: 1.3.6.1.2.1.1.1.0

Custom Arguments: all

Advanced Settings

Apply Restore Defaults

OK Cancel Help

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For a complete list of available keywords for NAC Manager notifications, see the [Edit Action Overrides window](#) Help topic.

- \$type - the notification type.
- \$trigger - the notification trigger.
- \$conditions - a list of the conditions specified in the notification action.
- \$ipaddress - the IP address of the end-system that is the source of the event.
- \$macaddress - the MAC address of the end-system that is the source of the event.
- \$switchIP - the IP address of the switch where the end-system connected.
- \$switchPort - the port number on the switch where the end-system connected.
- \$username - the username provided by the end user upon connection to the network.

E-Mail Subject

Defines the text and keyword values included in the e-mail subject line.

E-Mail Body

Defines the text and keyword values included in the e-mail body.

Syslog Tag

Defines the string used to identify the message issued by the syslog program.

Syslog Message

Defines the text and keyword values included in the syslog message.

Trap OID

The OID that defines the trap.

Trap Message

The varbind that is sent in the trap.

Trap Message OID

The OID of the varbind being sent that represents the message.

Custom Arguments

If the notification action specifies a custom program or script to be run on the Management Center Server, then you can use this field to enter the "all" option. Using the "all" option returns values for all the NAC Manager Notification keywords applicable to the notification type. The "all" option is the only valid option for this field. For a complete list of available keywords for NAC Manager notifications, see the [Edit Action Overrides window](#) Help topic

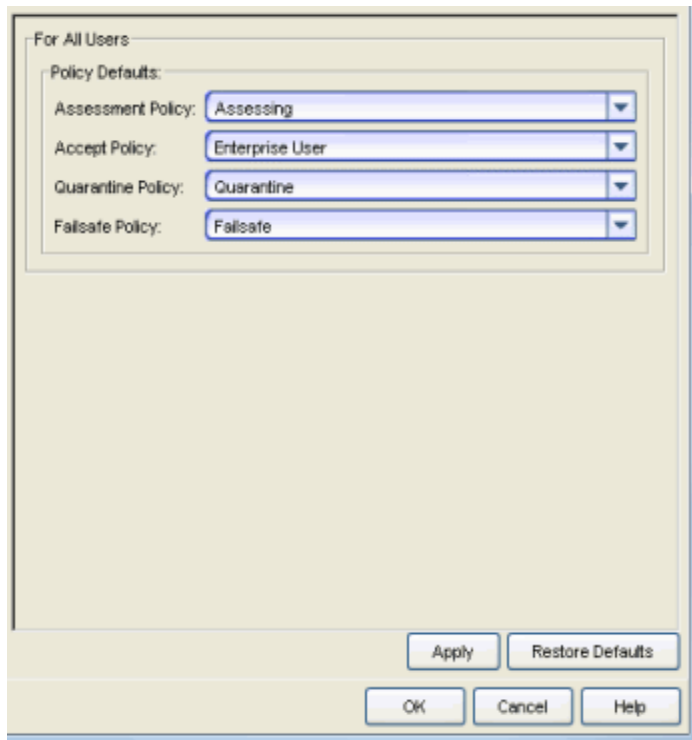
Advanced Settings

Click the Advanced Settings button to open the [Notification Advanced Settings window](#) where you can set parameters for the Action and Event queues processed by the Notification engine.

Policy Defaults

This Options view lets you specify a default policy role for each of the four [access policies](#). These default policy roles display as the first selection in the drop-down menus when you create a NAC profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" automatically displays as the first selection in the Assessment Policy drop-down menu in the [New NAC Profile window](#).

NAC Manager supplies seven policy role names from which to select. You can add more policies in the [Edit Policy Mapping window](#), where you can also define policy to VLAN associations for RFC 3580-enabled switches. Once you add a policy, it becomes available for selection in this view.



Assessment Policy

Select the default Assessment policy. The Assessment policy is applied to an end-system while it is being assessed (scanned).

Accept Policy

Select the default Accept policy. The Accept policy is applied to an end-system when the end-system is authorized locally by the Access Control Gateway and passed an assessment (if an assessment is required), or the "Replace RADIUS Attributes with Accept Policy" option is used when the end-system authenticated.

Quarantine Policy

Select the default Quarantine policy. The Quarantine policy is applied to an end-system if the end-system fails an assessment.

Failsafe Policy

Select the default Failsafe policy. The Failsafe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC

address, or if a scanning error occurs and an assessment of the end-system did not take place.

Port Wizard Defaults

These options let you define the default behavior for the MAC, 802.1X, or MAC + 802.1X authentication port configuration wizards. The wizards can be accessed by right-clicking one or more switches in the Switches tab and selecting Policy Manager Port Configuration Wizard. The options you define here are used as the wizard defaults. These settings apply to all users on the client.

For All Users

Port Mode - Unauthenticated Behavior
Sets the default mode for ports that are not authenticated.

Default Role

Use current Default Role on device

Set Default Role: <None>

Discard

Set Automatic Re-Authentication
Enable/Disable the Automatic Re-Authentication feature, and set an interval (in seconds) for that Re-Authentication.

Re-Authentication Status: Active Inactive

Re-Authentication Frequency: 43200

Set Hold Time
The amount of time (in seconds) authentication will remain timed out after the allowed number of authentication attempts have been exceeded.

600

Apply Restore Defaults

OK Cancel Help

Port Mode - Unauthenticated Behavior

Defines how the traffic of unauthenticated end users are handled on the port.

- **Default Role** - If the end user is unauthenticated, the port implements its default role. You can select to use the current default role on the device or set a default role. If there is no default role specified, there is

no role on the port.

- **Discard** - If the end user is unauthenticated, no traffic is allowed on the port.

Set Automatic Re-authentication

Automatic Re-Authentication lets you set up the periodic automatic re-authentication of logged-in users on the port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information, to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes." Select the **Active** radio button to enable Automatic Re-Authentication. Specify the **Re-Authentication Frequency**, which determines how often (in seconds) the device checks the port to re-authenticate the logged in user.

Set Hold Time

The amount of time (in seconds) authentication remains timed out after exceeding the allowed number of authentication attempts.

Status Polling and Timeout

This Options view lets you specify the enforce timeout and status polling options for Access Control engines. These settings apply to all users on all clients.

For All Users

NAC Appliance Enforce Timeout:
When enforcing to NAC Appliances, specify the number of seconds to wait before determining that contact has failed.
Length of Timeout (in seconds): 10

Status Polling:
The server will poll the NAC Appliances every interval to retrieve their status.
Polling Interval (in seconds): 60
When communicating with NAC Appliances for status polling, specify the number of seconds to wait before determining that contact has failed.
Length of Timeout (in seconds): 30

NAC Inactivity Check:
Enable a check to verify end-system NAC activity is taking place on the network. If no end-system activity is detected, a NAC Inactivity event is sent to the NAC Manager Events view.
 Enable NAC Inactivity Check
Interval between checks (in minutes): 30

Apply Restore Defaults
OK Cancel Help

NAC (Access Control) Appliance Enforce Timeout

When enforcing to Access Control engines, this value specifies the amount of time NAC Manager waits for an enforce response from the engine before determining that the Access Control engine is not responding. During an enforce, a Access Control engine responds every second to report that the enforce operation is either in-progress or complete. Do not increase this timeout value unless you are experiencing network delays that require a longer timeout value.

Status Polling

Polling Interval (in seconds) - Specifies the frequency that NAC Manager polls the Access Control engines to determine engine status.

Length of Timeout (in seconds) - When communicating with Access Control engines for status polling, this value specifies the amount of time NAC Manager waits before determining that contact failed. If NAC Manager does not receive a response from an engine in the defined amount of time, NAC Manager considers the engine to be "down" and the engine icon changes from a green up-arrow to a red down-arrow in the left-panel tree. The engine status refers to Messaging connectivity, not SNMP

connectivity. This means that if the engine is "down," NAC Manager is not able to enforce a new configuration to it.

NAC Inactivity Check

Enable a check to verify end-system NAC activity is taking place on the network. If no end-system activity is detected, a NAC Inactivity event is sent to the NAC Manager Events view. You can use the Console Alarms Manager (in Console, Tools > Alarm/Event > Alarms Manager) to configure custom alarm criteria based on the NAC Inactivity event to create an alarm, if desired.

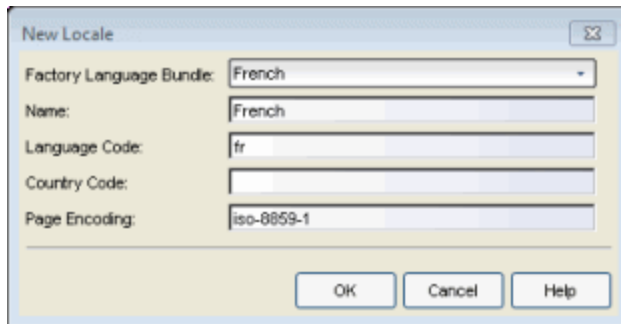
Related Information

For information on related tasks:

- [How to Set NAC Manager Options](#)

New/Edit Locale Window

Use this window to define a new locale (language) or edit an existing locale used as a default or supplemental locale in the captive portal.



Factory Language Bundle

Select the desired language bundle from the drop-down menu. NAC Manager ships with the following locales: Czech, English, French, German, Japanese, Korean, Polish, Romanian, Russian, Simplified Chinese, Spanish, and Traditional Chinese.

Name

Enter the name you want to give to the locale used in captive portal locale configuration.

Language Code

The language must be an ISO 639 two or three-character language identification code, or a registered language subtag of up to eight characters. In case a language uses both a two and three-character language code, use the two-character code. Find a full list of language codes in the IANA Language Subtag Registry.

Country Code

The country code is a two-character code following the ISO 3166 country identification code standard, or a UN M.49 numeric area code. A full list of country and region codes can be found in the IANA Language Subtag Registry.

Page Encoding

If you select a language that is not compatible with UTF-8 page encoding, you must specify the correct page encoding so that client browsers know, which character set is needed to display the messages correctly. For example,

if you are using Korean characters in the messages, you need to use EUC-KR for page encoding.

Related Information

For information on related help topics:

- [Portal Configuration - Look and Feel Panel](#)
- [Message Strings Editor](#)

New/Edit NAC Profile Window

NAC Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies applied to end-systems for network authorization, depending on authentication and assessment results.

NAC Manager comes with ten system-defined NAC profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

If desired, you can edit these profiles or you can define your own profiles to use for your NAC configurations. Use this window to create a new profile, or edit an existing profile. When you create a new profile, it is added to the [Manage NAC Profiles window](#). When you edit a profile, it changes the profile wherever it is used, so you do not need to individually edit each profile.

To create a new profile, click the **Add** button in the Manage NAC Profiles window. **To edit an existing profile**, select a profile in the Manage NAC Profiles window and click the **Edit** button.

Edit NAC Profile

NAC Profile - Employee Profile

Reject Authentication Requests

Authorization

Accept Policy: Enterprise User

Replace RADIUS Attributes with Accept Policy

Use Quarantine Policy: Quarantine

Use Failsafe Policy on Error: Failsafe

Enable Assessment

Assessment Configuration: Agentless Assessment

Assessment Interval: 30 Minutes

Hide assessment details and remediation options from end user

Use Assessment Policy: Employee During All Assessments

Policy Mappings

Manage... Last imported from policy domain Lab Rtr : Jun 5, 2012

OK Cancel Help

Name

Enter a name for a new profile. If you are editing a profile, the name of the profile is displayed and cannot be edited. To change the name of a profile, open the Advanced Configuration window (Tools > Management and Configuration > Advanced Configurations), expand the NAC Configurations folder and the NAC Profiles folder, right-click on the profile name and select **Rename** from the menu.

Reject Authentication Requests

If you check this checkbox, all authentication requests are rejected.

Authorization

Accept Policy

Use the drop-down menu to select the Accept policy you want to use in this NAC profile. An Accept policy is applied to an end-system when:

- the Extreme Access Control (Access Control) engine authorizes the end-system locally (MAC authentication) and the end-system passes an assessment (if assessment is enabled).

- the "Replace RADIUS Attributes with Accept Policy" option is selected .

If you select "No Policy", then the Access Control engine does not include a Filter ID or VLAN Tunnel Attribute in the RADIUS attributes returned to the switch, and the default role configured on the port is assigned to the end-system. This option is necessary when configuring single user plus IP phone authentication supported on C2/C3 and B2/B3 devices.

If you select "Use User/Host LDAP Policy Mappings", then the Access Control engine uses the LDAP policy mappings you configured in NAC Manager. You can access the [LDAP Policy Mappings window](#) from the configuration menu button to the right of the drop-down menu.

NOTE: The **Manage** button at the bottom of this window opens the [Edit Policy Mapping window](#) where you can define the policies available for selection from the drop-down menus in this window. You can also use the window to specify the policy to VLAN associations for RFC 3580-enabled switches.

Replace RADIUS Attributes with Accept Policy

When this option is checked, the attributes returned from the RADIUS server are replaced by the policy designated as the Accept policy. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, the Accept policy is inserted. When this option is unchecked, the attributes returned from the RADIUS server are forwarded back "as is" and the Accept Policy is only used to locally authorize MAC authentication requests. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, no attributes are returned to the switch.

Use Quarantine Policy

Select this checkbox if you want to specify a Quarantine policy. The Quarantine policy is used to restrict network access for end-systems that failed the assessment. You must select the [Enable Assessment checkbox](#) to activate this checkbox.

If a Quarantine policy is not specified and you configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes is applied (unless "Replace RADIUS Attributes with Accept Policy" is selected, in which case the Accept policy is used.) If "Authorize Authentication Requests Locally" is selected in your AAA configuration, then the Accept policy is applied to those locally authorized end-systems. This allows an

end-system onto the network with its usual network access even though the end-system failed the assessment.

Use Failsafe Policy on Error

Select this checkbox if you want to specify a Failsafe policy to be applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there a scanning error occurs and a scan of the end-system could not take place. A Failsafe policy allocates a nonrestrictive set of network resources to the connecting end-system so it can continue its work, even though an error occurred in Access Control operation.

If a Failsafe policy is not specified and you configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes is applied (unless "Replace RADIUS Attributes with Accept Policy" is selected, in which case the Accept policy is used.) If "Authorize Authentication Requests Locally" is selected in your AAA configuration, then the Accept policy is applied to those locally authorized end-systems. This allows end-systems onto the network with their usual network access when an error occurs in Access Control operation.


Assessment

Enable Assessment

Select the Enable Assessment checkbox if you want to require that end-systems are scanned by an assessment server.

NOTE: If you require end-systems to be scanned by an assessment server, you need to configure the assessment servers that performs the scans. The [Manage Assessment Settings](#) window is the main window used to manage and configure assessment servers. To access this window, select **Tools > Management and Configuration > Assessment Settings** from the menu bar.

Assessment Configuration

Use the drop-down menu to select the assessment configuration to use in this NAC Profile. Use the configuration menu button  to add a new assessment configuration or edit a configuration, if needed. Once an assessment configuration is created, it becomes available for selection in the list.

Assessment Interval

Enter an assessment interval that defines the interval between required assessments:

- Minutes - 30 to 120
- Hours - 1 to 48
- Days - 1 to 31
- Weeks - 1 to 52
- None

Hide Assessment Details and Remediation Options from User

If you select this option, the end user does not see assessment or remediation information on the Remediation Web Page. They are informed that they are quarantined and told to contact the Help Desk for assistance.

Use Assessment Policy

Select this checkbox if you want to specify a certain policy to be applied to an end-system while it is being assessed. Use the drop-down menu to select the desired policy.

Select when to apply the policy:

- During Initial Assessment Only — Only initial assessments receive the assessment policy. If the end-system is being re-assessed, it remains in its current policy.
- During All Assessments — All end-systems being assessed receive the specified assessment policy.

If an assessment policy is not specified and you configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes is applied (unless "Replace RADIUS Attributes with Accept Policy" is selected, in which case the Accept policy is used.)

If "Authorize Authentication Requests Locally" is selected in your AAA configuration, then the Accept policy is applied to those locally authorized end-systems. This allows the end-system immediate network access without having to wait for assessment to be complete.

Policy Mappings

Manage

Opens the [Edit Policy Mapping window](#) where you can manually define the policies used for your NAC policy mappings. You can also use the window

to specify the policy to VLAN associations for RFC 3580-enabled switches. The text to the right of the button is a summary of the latest management task performed on the policy mappings.

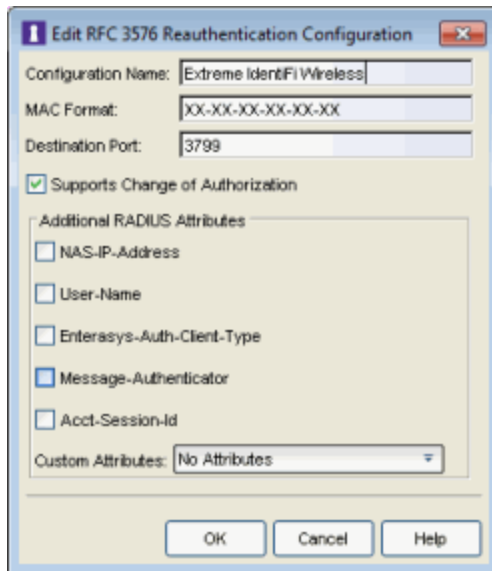
Related Information

For information on related windows:

- [Manage NAC Profiles Window](#)
- [Manage Assessment Settings Window](#)
- [Edit Assessment Configuration Window](#)

New/Edit RFC 3576 Reauthentication Configuration Window

Use this window to add a new RFC 3576 reauthentication configuration or edit an existing one. You can access this window from the **Add** and **Edit** toolbar buttons in the [Manage RFC 3576 Configurations window](#).



Configuration Name

Specify a configuration name used to identify the configuration in the Manage RFC 3576 Configurations window. Typically, this is the name of the switch type.

MAC Format

Specify the MAC format that defines how the MAC address of an end-system is formatted when sent to the switch during RFC 3576 Disconnect or Change of Authorization (CoA) messages. MAC formats are specified using lower-case 'x' characters as lowercase hexadecimal digits, and upper-case 'X' characters as uppercase hexadecimal digits. All other characters are translated literally. For example, the MAC address "01 23 45 67 89 AB" is formatted as shown below:

MAC Format: XX-XX-XX-XX-XX-XX results in "01-23-45-67-89-AB"

MAC Format: xx:xx:xx:xx:xx:xx results in "01:23:45:67:89:ab"

Destination Port

Specify the switch port to which Disconnect or Change of Authorization (CoA) messages are sent.

Supports Change of Authorization

Enable this checkbox if the switch supports Change of Authorization (CoA) messages as defined in RFC 3576. (For more information, see <http://www.ietf.org/rfc/rfc3576.txt>).

Additional Attributes

Select the RADIUS attributes to add to the Disconnect or Change of Authorization (CoA) messages sent to the switch:

- The NAS-IP-Address attribute contains the IP address of the switch.
- The User-Name attribute contains the RADIUS username in the case of an 802.1X session, or the MAC address of the end-system if MAC authentication is used.
- Enterasys-Auth-Client-Type is a vendor specific attribute for Enterasys that is used to tell which session type (MAC, 802.1X, or PWA) you are trying to reauthenticate or change the authorization for.
- The Message-Authenticator attribute should be included in an Access-Request that does not contain a User-Password, CHAP-Password, or EAP-Message attribute. Including this attribute also allows you to detect if the shared secret is incorrect.
- The Acct-Session-Id attribute (defined by RFC 2866), is a unique identifier specified by the device that an end-system is connected to (for example, a wireless controller or wired edge switch). The attribute is used to correlate data about the end-system's session, and is used in all accounting messages about that end-system after it is authenticated. Some devices require this attribute in the RFC3576/5176 message in order to identify the appropriate session to disconnect or change authorization for.
- Custom Attributes - Some third-party devices that support RFC 3576 (such as wireless devices) require vendor-specific attributes. For example, the Cisco Wireless Controller requires the RADIUS Attribute ServiceType=1 attribute. To create a custom attribute, click the configuration menu button and select Edit Custom RADIUS Attributes. The RADIUS Attribute Settings window opens, where you can define custom RADIUS attributes included as part of a RADIUS request.

Related Information

For information on related windows:

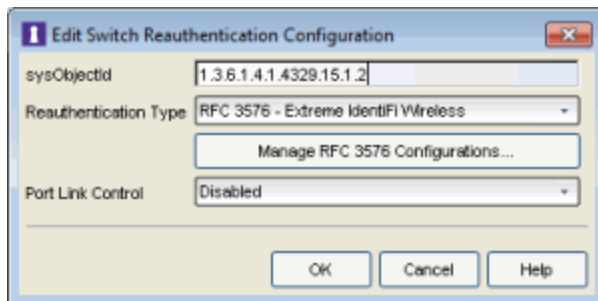
- [Add/Edit Appliance Settings Window](#)
- [New/Edit Switch Reauthentication Configuration Window](#)
- [Manage RFC 3576 Configurations Window](#)

New/Edit Switch Reauthentication Configuration Window

Use this window to add a new switch reauthentication configuration or edit an existing one. For example, you may want to add support for another wireless switch. In this case, you would create a new configuration by entering the sysObjectId of the switch, and setting the Reauthentication Type to either RFC 3576 (if the switch supports it) or Session Timeout.

A Switch Reauthentication Configuration consists of a switch sysObjectId, a reauthentication type, and whether or not port link control is enabled. Only one Switch Reauthentication Configuration can be applied per sysObjectId, so switches of the same type can be easily configured in the same way.

You can access the New/Edit Switch Reauthentication Configuration window from the Reauthentication tab in the [Appliance Settings window](#). Click the Add or Edit toolbar button located at the top of the Switch Reauthentication Configuration table.



SysObjectId

The switch SysObjectId.

Reauthentication Type

Select the reauthentication type for the switch:

- SNMP - uses SNMP to trigger reauthentication using various OIDs in different MIBs. The Extreme Access Control engine checks a series of proprietary Enterasys MIBs, standardized MIBs, and proprietary third-party MIBs to determine availability, and forces reauthentication using any available SNMP method.
- Session Timeout - causes NAC Manager to return a session timeout and terminate action to the end-system via RADIUS response

attributes. The use of this mechanism causes the user to be automatically reauthenticated at a specified interval by the switch they are connected to. This option should only be used for wireless switches that do not have RFC 3576 support or wired switches that do not have SNMP support.

- RFC 3576 - a method of reauthenticating RADIUS sessions through the use of Disconnect-Request messages as defined by RFC 3576. (For more information, see <http://www.ietf.org/rfc/rfc3576.txt>). RFC 3576 configurations must be customized to work with the specific vendor implementation for each device type. To add, edit, or delete an RFC 3576 configuration, click the Manage RFC 3576 Configurations button.

Manage RFC 3576 Configurations

Click this button to open the [Manage RFC 3576 Configurations window](#) where you can add, edit, or delete RFC 3576 configurations. All configurations defined in this window are available for selection from the Reauthentication Type drop-down list, under "RFC 3576 - [Configuration Name]."

Port Link Control

Port link control allows the toggle of the operational mode of a port. Use this option to disable port link control for specific switches. For example, if port link control has been enabled in the [Appliance Settings Miscellaneous tab](#), then it should be disabled for all wireless devices using a wireless switch reauthentication configuration. This is because all end-systems on wireless devices are authenticated through the same radio port; toggling the operational mode of this port would reauthenticate all end-systems authenticated through the port.

Related Information

For information on related windows:

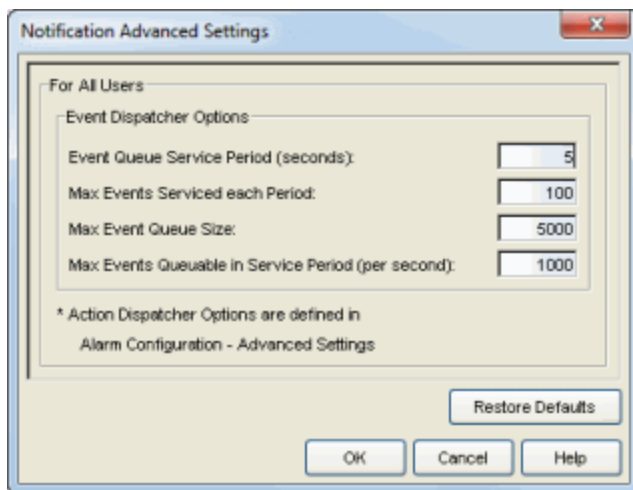
- [Add/Edit Appliance Settings Window](#)
- [Manage RFC 3576 Configurations Window](#)

Notification Advanced Settings Window

Use this window to limit resources used by Extreme Management Center Event handling.

When events are triggered, they are moved into the Event queue for processing by the event dispatcher. A specified number of events are taken from the queue and processed once each service period, according to the option values specified here.

You can access the window from the [Notification Engine view](#) in the NAC Manager options (Tools > Options).



Event Queue Service Period (seconds)

This controls how often the queue is checked for events to process. The dispatcher runs once every service period. So by default, the dispatcher processes events every 5 seconds.

Max Events Serviced each Period

The maximum number of events pulled from the queue for processing each service period. By default, the dispatcher processes 100 events every service period.

Max Events Queue Size

The maximum number of events that can be queued. By default, the dispatcher drops events after 5000 events are queued.

Max Events Queuable in Service Period (per second)

This limits the rate that events can be added to the queue (not processed from the queue) and protects the event engine against a large amount of events arriving too quickly. If events arrive at a rate that exceeds this amount, they are discarded.

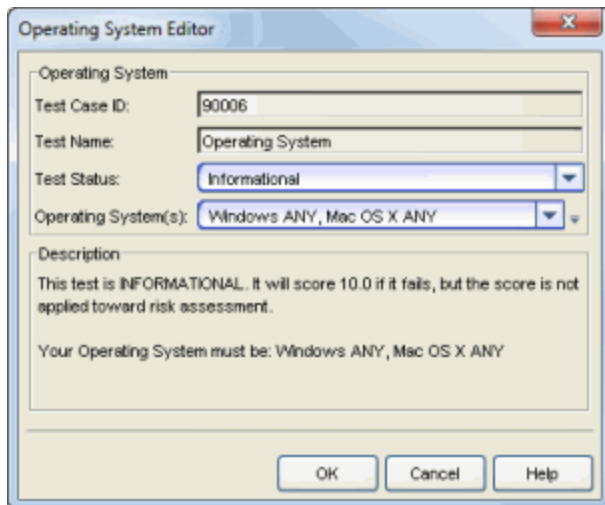
Related Information

For information on related windows:

- [Notification Engine View](#)

Operating System Editor

This window lets you configure parameters for the Operating System test case included in an [agent-based test set](#). This test checks to see if the operating system on the end-system matches the operating system(s) specified here. The Operating System test case is system-defined and cannot be deleted from the test set.



Test Case ID

The Operating System test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

The Operating System test case name cannot be changed.

Test Status

Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.


- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.

- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that the end-system will be matched against. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

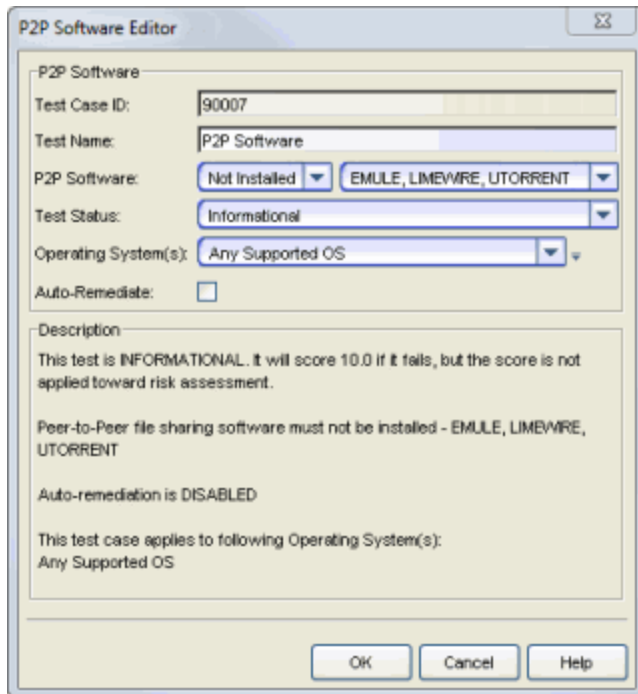
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

P2P Software Editor

This window lets you configure parameters for the P2P Software test case included in an [agent-based test set](#). This test checks to see if the selected file transfer software is installed or running on the end-system.



The screenshot shows the 'P2P Software Editor' dialog box. It contains the following fields and options:

- Test Case ID:** 90007
- Test Name:** P2P Software
- P2P Software:** Not Installed (dropdown), EMULE, LIMEWRE, UTORRENT (dropdown)
- Test Status:** Informational (dropdown)
- Operating System(s):** Any Supported OS (dropdown)
- Auto-Remediate:**

Description:

This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.

Peer-to-Peer file sharing software must not be installed - EMULE, LIMEWRE, UTORRENT

Auto-remediation is DISABLED

This test case applies to following Operating System(s):
Any Supported OS

Buttons: OK, Cancel, Help

Test Case ID

The test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

P2P Software

Use the drop-down list to select the software you want to test for.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined. Auto-remediation will be performed, if enabled.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation will be performed, if enabled.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation will be performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Auto-Remediate

If the Auto-Remediate checkbox is selected and P2P software is installed, the agent will attempt to uninstall it.

NOTE: If the user on the end-system is not an administrator, Auto-Remediate will be able to stop the process but not uninstall the software.

Description

A description of the test case parameters.

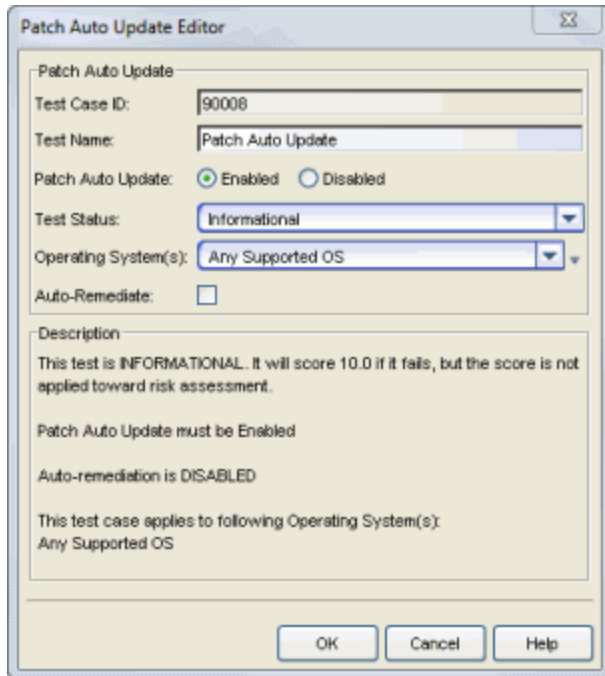
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Patch Auto Update Editor

This window lets you configure parameters for the Patch Auto Update test case included in an [agent-based test set](#). This test checks to see if Patch Auto Update is enabled or disabled on the end-system. This test relies on the Windows Update software program.



The screenshot shows the 'Patch Auto Update Editor' dialog box. It contains the following fields and options:

- Test Case ID:** 90008
- Test Name:** Patch Auto Update
- Patch Auto Update:** Enabled (selected), Disabled
- Test Status:** Informational (selected)
- Operating System(s):** Any Supported OS (selected)
- Auto-Remediate:**

Description:

This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.

Patch Auto Update must be Enabled

Auto-remediation is DISABLED

This test case applies to following Operating System(s):
Any Supported OS

Buttons: OK, Cancel, Help

Test Case ID

The test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Patch Auto Update

Use the drop-down list to select the patch auto update state you want to test for: enabled or disabled.

Test Status

Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be


used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined. Auto-remediation will be performed, if enabled.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation will be performed, if enabled.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation will be performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Auto-Remediate

If the Auto-Remediate checkbox is selected, the agent will attempt to enable or disable the auto update feature, depending on the selected value.

NOTE: If an end-system fails the Patch Auto Update test and Auto-Remediate is enabled for the test, the remediation will fail if the user on the end-system is not an administrator.

Description

A description of the test case parameters.

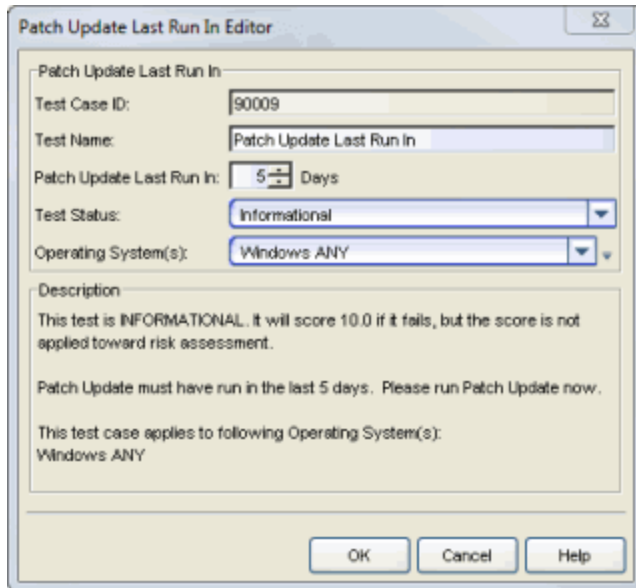
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Patch Update Last Run In Editor

This window lets you configure parameters for the Patch Update Last Run In test case included in an [agent-based test set](#). This test checks to see if the last time a Windows patch update was run on the end-system falls within the specified time frame. This test relies on the Windows Update software program.



The screenshot shows the 'Patch Update Last Run In Editor' dialog box. It contains the following fields and options:

- Test Case ID:** 90009
- Test Name:** Patch Update Last Run In
- Patch Update Last Run In:** 5 Days
- Test Status:** Informational
- Operating System(s):** Windows ANY

Description:
This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.
Patch Update must have run in the last 5 days. Please run Patch Update now.
This test case applies to following Operating System(s):
Windows ANY

Buttons: OK, Cancel, Help

Test Case ID

The test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Patch Update Last Run In

Specify the desired number of days.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Portal Configuration


If your network is implementing [registration](#) or [assessment/remediation](#), you define the branding and behavior of the portal website used by the end user during the registration or assessment/remediation process using a Portal Configuration. Extreme Access Control engines ship with a default Portal Configuration. Use this default configuration as is, or make changes to the default configuration using this window.

This Help topic provides the following information for accessing and configuring the Portal Configuration:

- [Accessing the Portal Configuration](#)
- [Network Settings](#)
- [Administration](#)
- [Look and Feel](#)
- [Common Settings](#)
- [Guest Registration](#)
- [Guest Web Access](#)
- [Secure Guest Access](#)
- [Authenticated Registration](#)
- [Authenticated Web Access](#)
- [Assessment/Remediation](#)
- [Portal Web Page URLs](#)

Accessing the Portal Configuration

Use the following steps to access the Portal Configuration:

1. Use the NAC Manager  toolbar button to open the NAC Configuration window or use the Edit button in the [Configuration tab](#).
2. In the left-panel tree, select the Portal icon. If needed, use the Portal Configuration drop-down menu in the right panel to select the configuration to specify for your NAC Configuration, or to create a new one.

3. Expand the Portal icon and select the portal configuration settings you want to edit. Refer to the sections below for information on the different settings.

At the bottom of the window there is an **Appliance Portal Pages** button that displays a menu to let you quickly launch the following portal web pages:

- **Preview Web Page** — allows you to preview web pages that may be accessed by the end user during the assessment/remediation and registration process.
- **Registration Administration Page** — used by Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network. For more information, see [Registration Administration](#).
- **Registration Sponsor Page** — used by sponsors to view, delete, and add registered end-systems that they sponsor. For more information, see [Sponsored Registration](#).
- **Pre-Registration Page** — lets selected personnel register guest users in advance of an event, and print out a registration voucher that provides registration credentials. For more information, see [Pre-Registration Portal](#).
- **Self-Registration Page** — allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems). For more information, see [Enable Self-Registration Portal](#).

You can also launch these web pages using a URL. For a list of URLs for accessing commonly used portal web pages, see [Portal Web Page URLs](#).

Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment/Remediation and the Registration portal web pages.

The screenshot shows a configuration window titled "Network Web Page Settings". It contains the following fields and options:

- Allowed Web Sites: [change](#)
- Use Fully Qualified Domain Name:
- Use Mobile Captive Portal:
- Display Welcome Page:
- Redirect User Immediately: Test Image URL:
- Redirection: To URL:
- Portal HTTP Port:
- Portal HTTPS Port:
- Force Captive Portal HTTPS:

Allowed Web Sites

Click on the "change" link to open the [Allowed Web Sites window](#), where you can configure the web sites to which end users are allowed access during the assessment/remediation and registration process.

Use Fully Qualified Domain Name

Select this checkbox if you would like the URLs in the portal web pages to display the engine's hostname instead of IP address. When this is enabled, the user's browser performs a DNS lookup to find the IP address for the fully qualified hostname of the Extreme Access Control engine. Only enable this option if all Access Control engine hostnames are defined in DNS.

Use Mobile Captive Portal

Select this checkbox to allow end users using mobile devices to access the network via captive portal registration and remediation. In addition, it allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network using a mobile device. This feature is supported on the following mobile devices: iPod Touch, iPad, iPhone, Android Phone/Tablet/NetBook, and Windows phones.

Display Welcome Page

Select this checkbox to display the welcome page. If the checkbox is not selected, users bypass the welcome page and access the portal directly.

Redirect User Immediately

This option redirects end users to the specified test image URL as soon as they have network access. The redirect occurs regardless of where the end user is in the connection process. If the end-system's browser can reach the test image URL, then it assumes that the end user has network access and redirects the end user out of the captive portal. The test image URL should be an internal image on your own website that end users don't have access to until they're accepted. It is recommended that the test image URL is a link to an SSL site. The reason for this is that if the NAC Manager captive portal is configured for Force Captive Portal HTTPS, the browser does not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies, (typically the Unregistered, Assessing, and Quarantine policies), are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. In the event access to the test image is available, the user may experience the captive portal reverting to the "click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on the network.

Redirection

There are three Redirection options that specify where the end user is redirected following successful registration or remediation, when the end user is allowed on the network:

- **To URL** — This option lets you specify the URL for the web page to which the end user is redirected. This is also the connection URL that is displayed on the Guest User Voucher when using [Pre-Registration](#). This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."
- **Disabled** — This option disables redirection. The end user stays on the same web page, where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.

You can override this setting and specify different Redirection URLs for your remediation and registration configurations settings.

Portal HTTP Port

Specify which port the Extreme Management Center server and Access Control engine uses for HTTP web server traffic. Any change do not take effect on the Access Control engine until an Enforce is performed in NAC Manager.

Portal HTTPS Port

Specify which port the NetSight server and Access Control engine uses for HTTPS web server traffic. Any change do not take effect on the Access Control engine until an Enforce is performed in NAC Manager.

Force Captive Portal HTTPS

Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. It is recommended that this checkbox is enabled if [Authenticated Registration](#) is configured for the registration process. The default setting is unchecked, specifying to serve the captive portal web pages over HTTP.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network. The web page also provides access to the Pre-Registration Portal (if pre-registration is enabled) and the Screen Preview web page. For more information, see [Registration Administration](#).

The screenshot shows two main sections of a configuration window:

- Administration Web Page Settings:**
 - Welcome Message: [change](#)
 - Force Administration HTTPS:
 - Session Timeout (Minutes):
 - Login Failure Image:
 - Limit Sponsor's View To Own Users:
 - LDAP Email Address Attribute Name:
 - RADIUS Email Address Attribute Name:
- Administrative Login Configuration:**

Controls portal access for administrators and sponsors.

Authentication	User Name, LDAP, or RADIUS User Gro.	Role Summary
Local Password Repository	Admin	Role Name: Admin Role - Capabili...
Local Password Repository	Sponsor	Role Name: Sponsor Role - Capabili...

Buttons on the right: Move Up..., Move Down..., Add..., Delete, Edit..., Roles...

Administration Web Page Settings

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed to users when they log into the administration or sponsor portal. The default welcome message is "Registration System Administration."

Force Administration HTTPS

Select this checkbox to force the administration web page to be served securely over HTTPS (instead of HTTP) to administrators and sponsors on the network. It is recommended that this is enabled for security reasons.

Session Timeout (Minutes)

Use this field to specify how long an administrator can be inactive on the administration web page before getting automatically logged out. The default value is 10 minutes.

Login Failure Image

Select the image you would like displayed when the end user fails to correctly log in to the web page. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, click the configuration menu button to the right of the drop-down list and select Manage Images to open the Images window.

Limit Sponsor's View to Own Users

Select this checkbox if you want to limit a sponsor's view to only the users they have sponsored. This option is valid only if you configure LDAP or RADIUS authentication of your sponsors. If you select this checkbox, you must enter the LDAP or RADIUS email address attribute name so that a sponsor's login name can be matched to their email address, and only the registered users for that sponsor are displayed.

Administrative Login Configuration

Use this section to configure administrative user access to the Registration Administration web page, the Sponsor Administration web page, and the Pre-Registration Portal. (To see the URLs for these web pages, refer to [Portal Web Page URLs](#).)

Users authenticate to a local database or through an LDAP or RADIUS server and receive a role assignment based on their login. The assigned role determines their level of access to the portal web pages.

There are two default roles already configured:

- Admin Role — provides access to the administration page, sponsor page, and pre-registration portal. Allows the ability to add registered users and change user expiration, assign end users to all end-system and user groups, and view users from all engine groups.
- Sponsor Role — provides access to the sponsor page and pre-registration portal. Allows the ability to add registered users and change user expiration, assign end users to all end-system and user groups, and view users from all engine groups.

Use the default roles or create a new role. For example, create a role that defines access capabilities for administrative personnel that only accesses the Pre-Registration Portal, such as receptionists pre-registering guests to the network.

The table in this section lists the available login configurations, and lets you add, delete, and edit configurations. You can also add and modify the roles used to define access.

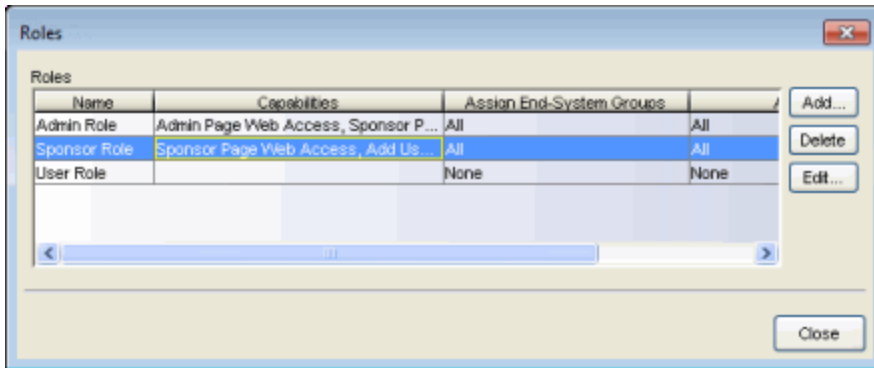
Use the following steps to add a new login configuration:

1. Click the **Add** button to open the Add Login Configuration window.

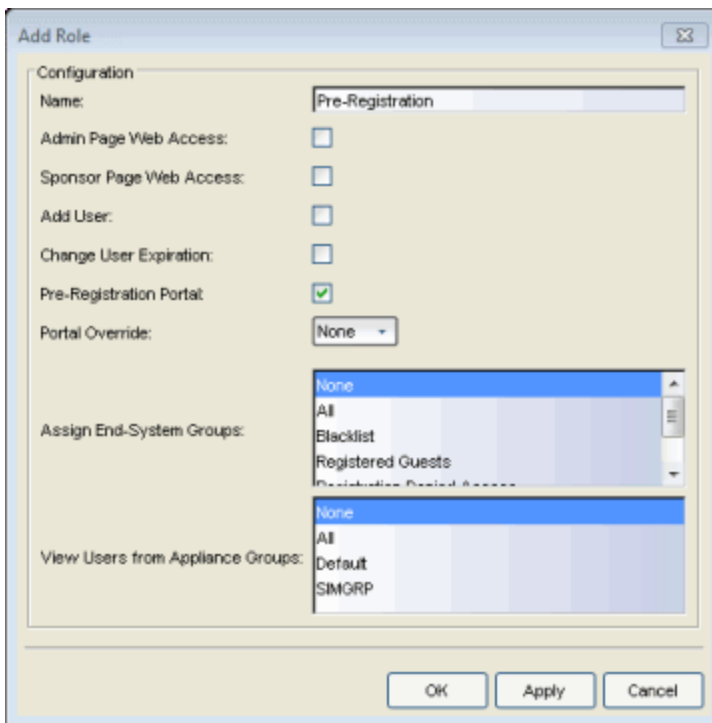
2. Define the configuration's authentication based on a local password repository user or user group, or an LDAP or RADIUS user group. Local repository users are configured through [AAA Configuration](#). You can add or edit user groups using the drop-down menu. User groups can also be defined in the [Manage Rule Groups window](#).
3. Select a role to assign to authenticated users.
4. Click **OK** to create the new login configuration in the Administrative Login Configuration table.
5. Use the **Move Up/Move Down** buttons to change the order of the configurations in the table list. This determines the precedence of the configurations, which is useful when you are using user groups and an end user falls into more than one group. For example, if a user is a member of both the Admin LDAP user group and the Sponsors LDAP user group in the LDAP server, list the Admin group first, otherwise the user never matches the Admin group and is never able to access the administration web page.
6. Use the **Edit** or **Delete** buttons to modify or remove a login configuration.

Use the following steps to modify or create a new Role.

1. Click the **Roles** button to open the Roles window that lists available roles and their capabilities, and allows you to add, edit, and delete roles.



- Click **Add** to open the Add Role window and enter a name for the new role. Click **Edit** to modify an existing role.



- Specify the role's access capabilities:
 - Select whether the role provides access to the Admin Page, Sponsor Page, or Pre-Registration Portal.
 - Select whether the role provides the ability to add registered users and change user expiration.
 - The Portal Override is used in environments where advanced location-based access is defined and allows you to specify the appropriate portal for the administrator logging in. For example, using two roles

with two different portal overrides, you can make sure that when an administrator from company ABC logs in, they see company ABC's portal, while an administrator from company XYZ sees company XYZ's portal.

- Select whether users are able to assign end users to all end-system and user groups (All), select groups, or no groups (None).
 - Select whether users are able to view users from all engine groups (All), select groups, or no groups (None).
4. Click **OK** to create or modify the role. You can now use the role in your login configurations.

Look and Feel

Use this panel to configure common web page settings that are shared by both the Assessment/Remediation and the Registration portal web pages.



The screenshot shows a configuration window titled "Common Web Page Settings". It contains the following settings:

Header:	change
Footer:	change
Helpdesk Information:	change
Images:	change
Colors:	change
Style Sheet:	change
Mobile Style Sheet:	change
Message Strings:	change
Default Locale:	English ▾
Supplemental Locales:	add
Display Locale Selector:	<input type="checkbox"/>
Display Powered By Logo:	<input checked="" type="checkbox"/>
Header Background Image:	Default ▾
Header Image:	None ▾
Favorites Icon:	Default ▾
Access Granted Image:	Default ▾
Error Image:	Default ▾
Busy Image:	Default ▾

Header

Click on the "change" link to open a window where you can configure the link for the header image displayed at the top of all portal web pages. By default, the header image is configured as the Extreme Networks logo

acting as a link to the Extreme Networks website. Text entered in this window can be formatted in HTML.

Footer

Click on the "change" link to open a window where you can configure the footer displayed at the bottom of all portal web pages. By default, the footer is configured with generalized information concerning an organization. Change the "example" text in this section to customize the footer to your own organization. Text entered in this window can be formatted in HTML.

Helpdesk Information

Click on the "change" link to open a window where you can configure the Helpdesk contact information that is provided to end users in various scenarios during the assessment/remediation and registration process (e.g. an end-system has exceeded the maximum number of remediation attempts). By default, this section is configured with generalized Helpdesk information, such as contact URL, email address, and phone number. Change the "example" text to customize the Helpdesk information for your own organization. Text entered in this window can be formatted in HTML. In addition, the entire contents of the Helpdesk Information section are stored in the variable "HELPDESK_INFO". By entering "HELPDESK_INFO" (without the quotation marks) in any section that accepts HTML in the Common Page Settings (or any other settings), all information configured in this section is displayed in place of "HELPDESK_INFO".

Images

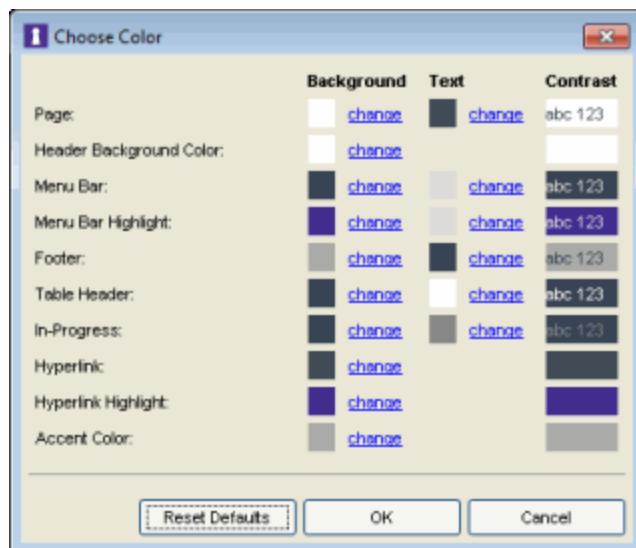
Click on the "change" link to open the Images window where you can specify the image files used in the portal web pages. All image files used for Assessment/Remediation and Registration portal web pages must be defined in this list. Once an image file is defined here, it is available for selection from the configuration drop-down menus (for example, when you configure the [Access Granted Image](#)), and may be referenced in the sections supporting HTML. The image files defined here are sent to the Access Control engine along with the web page configuration.

Use the **Add** button to select an image file to add to the list. You can select an image in the list and use the **Display Image** button to preview the image.

Colors

Click on the "change" link to open the Choose Color window, where you can define the colors used in the portal web pages:

- Page — Define the background color and the color of all primary text on the web pages.
- Header Background Color — Define the background color displayed behind the header image.
- Menu Bar — Define the background color and text color for the menu bar.
- Menu Bar Highlight — Define the background color and text color used for the menu bar highlights in the Administration pages.
- Footer — Define the background color and text color for the footer.
- Table Header — Define the background color and text color for the table column headers in the Administrative web pages.
- In-Progress — Define the background color and text color for task in-progress images.
- Hyperlink — Define the color used for hyperlinks on the web pages.
- Hyperlink Highlight — Define the color of a hyperlink when it is highlighted.
- Accent Color — Define the color used for accents on various parts of the web pages.



Style Sheet

Click on the "change" link to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the portal web pages.

Mobile Style Sheet

Click on the "change" link to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the mobile version of the portal web pages.


Message Strings

Click on the "change" link to open the [Message Strings Editor window](#) where you can edit the text and formatting of the various messages used on the portal web pages or replace them with message strings from another file. You can also use the Message Strings Editor to create a new message, if your portal configuration requires it. For example, you might want to add a welcome message to the Portal landing page. If you have defined supplemental locales (languages), you can edit those message strings here as well.

Default Locale

Select the locale (language) displayed to any captive portal user unless the client locale detected from their browser matches one of the defined supplemental locales. The list from which you select includes the current default locale and any supplemental locales defined.

Supplemental Locales

This field lists the locales (languages) presented as options to the user in the captive portal, in addition to the default locale. If no supplemental locales are defined, click the "add" link to open the Portal Locale Entries window, where you can define the locales to use. (In the Portal Local Entries window, click the  button and use the [New Locale window](#) to add a new locale.) If supplemental locales are defined, they are listed here as a link, which you can click to open the locale editor.

Display Locale Selector

Select this checkbox if you want a locale (language) selector to be displayed as a drop-down menu in the menu bar on the captive portal welcome and login pages. Use this option for a shared machine where the users of the machine may speak different languages. (On the mobile captive portal, the selector is displayed as a list of links at the bottom of the welcome screen.)

Display Powered by Logo

Select this checkbox to display the Extreme Networks logo at the bottom of all of your portal web pages.

Header Background Image

Select the background image you would like displayed behind the header image at the top of all portal web pages. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Header Image

Select the image displayed at the top of all portal web pages. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Favorites Icon

Select the image displayed as the Favorites icon in the web browser tabs. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Access Granted Image

Select the image displayed when the end user is granted access to the network either based on compliance with the network security policy or upon successful registration to the network. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Error Image

Select the image displayed when there is a communication error with the NetSight Server. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Busy Image

Select the progress bar image displayed to the end user when the web page is busy processing a request. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Common Settings

Use this tab to configure the common settings used by the different registration web pages.

The screenshot shows a configuration window titled "Registration Web Page Settings". It contains four settings:

- Title:** A text field with a blue "change" link next to it.
- Welcome Message:** A text field with a blue "change" link next to it.
- User Registration Success:** A text field with a blue "change" link next to it.
- Access Denied Image:** A drop-down menu currently showing "Default".

Below these settings is a section for "Survivable Registration" with a checkbox that is currently unchecked. The text below the checkbox reads: "This option will allow for a temporary Registration when communication to NAC Manager fails. During this time, any registrations will receive the Failsafe policy of the Unregistered NAC Profile. When communication is restored, the user will be put through the normal Registration process."

Title

Click on the "change" link to open a window where you can modify the text that appears in the title bar of the registration and web access page browser tabs. The default page title is "Enterprise Registration."

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed to users on the menu bar of any registration or web access page. The default welcome message is "Welcome to the Enterprise Network's Registration Center."

User Registration Success

Click the "change" link to open a window where you can edit the message displayed to the end user after successfully registering their end-system to the network.

Access Denied Image

Select the image you would like displayed when the end user has been denied access to the network. The drop-down menu displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Enable Survivable Registration

This feature provides temporary Registration for unregistered end-systems when the NetSight server is unreachable. If you select this checkbox, unregistered users that try to register while the NetSight server is

unreachable are redirected to the Registration web page. After entering the required information, users are assigned the Failsafe policy and allowed on the network. Once the connection to the NetSight server is reestablished, the users are reassigned the Unregistered policy and forced to re-register. If you enable Survivable Registration, make sure that the Failsafe policy provides the appropriate network services for unregistered users.

Guest Registration

Guest registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network. Guests are initially redirected to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

The end user's level of network access is determined by the settings specified here, and whether they are required to have a sponsor. With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

NOTE: If you configure both Guest Registration and [Authenticated Registration](#) for an area on your network, the end user is presented with a choice on the registration web page whether to authenticate or not.

The screenshot displays a configuration interface with several sections:

- Web Page Customizations (Shared)**: Includes links for "Introduction Message" and "Customize Fields".
- Redirection (Shared)**: Features a "Redirection" dropdown menu set to "Use Network Settings Redirection" and a text input field containing "http://www.enterasys.com".
- Registration Settings**: Includes a "Verification Method" dropdown set to "Disabled" and a "Default Expiration" field set to "30 Days (0=never)".
- Facebook Registration**: A checkbox is unchecked. Below it are input fields for "Facebook App ID" and "Facebook App Secret", and a "Show Secret" checkbox.
- Sponsorship**: Contains explanatory text about user assignment and access, and a "Sponsorship Mode" dropdown menu set to "None".

Introduction Message (Shared)

Click the "change" link to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the [Allowed Web Sites window](#) accessed from the [Network Settings](#). By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed

on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#). This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page to which the end user is redirected. Typically, this is the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User Verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see [How to Configure Verification for Guest Registration](#).

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user

must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by a sponsor.

Facebook Registration

Select the Facebook Registration checkbox if you are implementing guest registration using Facebook as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Facebook in order to complete the registration process. For more information, see [How to Implement Facebook Registration](#) for information regarding how to create a Facebook application. When you create an application, you are given a Facebook App ID and Facebook App Secret you enter here.

Sponsorship

Use this section to configure sponsorship for Guest Registration. Select the required Sponsorship Mode. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see [How to Configure Sponsorship for Guest Registration](#).

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Guest Web Access

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

End users are initially redirected to the captive portal when they first connect to the network. After the user enters the required information on the Guest Web Access login page (typically, their name and email address), they are allowed access on the network according to the assessment and authorization defined in the Guest Access profile.

Guest web access provides a single session, and no permanent end user records are stored. This provides increased network security, and also allows you to minimize the number of registration records stored in the NetSight database.

Implementing guest web access requires web redirection or DNS proxy.

Web Page Customizations (Shared)

Introduction Message: [change](#)

Customize Fields: [change](#)

Redirection (Shared)

Redirection: Use Network Settings Redirection

Web Access Settings

Verification Method: SMS Gateway or Email

SMS Gateway Email:

Message Strings: [change](#)

Verify Pin Characters: Alpha Numeric with No Vowels

Verify Pin Length:

Introduction Message (Shared)

Click the "change" link to open a window where you can edit the introductory message displayed to end users when gaining web access as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the [Allowed Web Sites window](#) accessed from the [Network Settings](#). By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Guest Web Access login page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#). This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Verification Method

User verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see [How to Configure Verification for Guest Registration](#).

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Guest Web Access login page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).

- **SMS Gateway** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).
- **SMS Text Message** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the **"SMS Text Message"** or the **"SMS Text or Email"** **Verification method:** click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to send an email to. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the **"SMS Gateway"** or **"SMS Gateway or Email"** **method:** enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Here are three scenarios where Secure Guest Access provides increased network security:

- An enterprise provides secure guest access for visitors. Guests self-register through the captive portal and receive connection credentials and instructions for the secure SSID via a text message on their mobile phone.
- A hospitality company provides guests with secure Internet access using pre-registration. A receptionist generates a voucher using the NAC Manager pre-registration portal. The voucher is handed to the guest, providing them with instructions and credentials for connecting directly to the secure SSID.
- An enterprise provides secure guest access with the option of elevated access through employee sponsors. Guests self-register through the captive portal and receive connection credentials and instructions via a text message. Sponsors approve guests for secure guest access. Later, sponsors can elevate guest access using the sponsorship portal.

Web Page Customizations (Shared)	
Customize Fields:	change
Secure Access Settings	
Credential Delivery Method:	<input type="text" value="SMS Text Message"/>
Service Providers:	change
Message Strings:	change
Default Expiration:	<input type="text" value="30"/> <input type="text" value="Days"/> (0=never)
Default Maximum Registered Devices:	<input type="text" value="2"/>
Enable Pre-Registration Portal:	<input type="checkbox"/> <input type="text" value="Multi and Single User"/>
Generate Password Characters:	<input type="text" value="Alpha Numeric with No Vowels"/>
Generate Password Length:	<input type="text" value="8"/>
Sponsorship	
End users will be assigned to Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.	
Sponsorship Mode:	<input type="text" value="None"/>

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Secure Access Settings

Credential Delivery Method

Select the method used to send guests their credentials and access instructions for the secure SSID. For more information and complete instructions, see [How to Configure Credential Delivery for Secure Guest Access](#).

- **Captive Portal** — The credential information displayed on the Registration web page.
- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).
- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the [Manage Custom Fields window](#).
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the [Manage Custom Fields window](#).

If you have selected the "SMS Text Message" or the "SMS Text or Email" **Verification method**: click the Service Providers "change" link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows NAC Manager to correctly format the email address to which to send an email. This email is then received by the service provider and converted

to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings "change" link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", modify the "secureGuestAccessEmailSentFromAddress" message string to be the appropriate email address for your company.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by the sponsor.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Enable Pre-Registration Portal

Use this checkbox to enable Pre-Registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users attending a company presentation, sales seminar, or a training session need network access. From the drop-down menu, select whether to pre-register a single user (to pre-register one user at time) or multiple users (when a larger group of users is pre-registering) or both. For more information, see [How to Configure Pre-Registration](#).

Generate Password Characters (Shared)

NAC Manager uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

NAC Manager uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Sponsorship

Use this section to configure sponsorship for Secure Guest Access registration. Select the Sponsorship Mode required. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see [How to Configure Sponsorship for Guest Registration](#).

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Authenticated Registration

Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

It is recommended that the [Force Captive Portal HTTPS](#) option is enabled if authenticated registration is required for security reasons.

NOTE: If you configure both [guest registration](#) and authenticated registration for an area on your network, the end user is presented with a choice on the registration web page whether to authenticate or not.

Authentication (Shared)	
AAA Configuration:	Default
Authentication To End-System Group:	Local change
Local Password Repository:	Default
Max Failed Logins:	<input type="checkbox"/>
Web Page Customizations (Shared)	
Login or Register Message:	change
Introduction Message:	change
Failed Authentication Message:	change
Customize Fields:	change
Redirection (Shared)	
Redirection:	Use Network Settings Redirection <input type="text" value="http://www.enterasys.com"/>
Registration Settings	
Default Maximum Registered Devices:	<input type="text" value="2"/>
Default Expiration:	<input type="text" value="30"/> <input type="text" value="Days"/> (0=never)
Delete Expired Users:	<input type="checkbox"/>
Delete Local Password Repository Users:	<input type="checkbox"/>
Enable Self Registration Portal:	<input type="checkbox"/>
Enable Pre-Registration Portal:	<input type="checkbox"/> <input type="text" value="Multi and Single User"/>
Generate Password Characters:	<input type="text" value="Alpha Numeric with No Vowels"/>
Generate Password Length:	<input type="text" value="8"/>


Authentication (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the NAC configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple NAC Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Click on the "change" link to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key  indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click on the Local Password Repository link to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this option if you want to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Web Page Customizations (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Login or Register Message

Click the "change" link to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the "change" link to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the "change" link to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Customize Fields (Shared)

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed in the Registration web page.

Redirection (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#).

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings (Shared)

The Generate Password Character and Generate Password Length settings are shared by Authenticated Registration and Secure Guest Access.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the registration list. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network. Individual registration expiration time can also be set by the administrator/sponsor through the Registration Administration web page.

Delete Expired Users

Specifies whether users should be deleted from the Registered users list in the Registration Administration web page when their registration expires. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network.

Delete Local Password Repository Users

If you have selected the Delete Expired Users option, then selecting this checkbox also deletes the expired user from the local password repository.

Enable Self Registration Portal

This checkbox allows an authenticated and registered user to be directed to a URL (provided by an administrator) to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. Once the additional devices have been registered, the student can access the network using those devices. The URL for the Self Registration web page is `https://<Access ControlEngineIP>/self_registration`. You can change the instructions displayed on this web page using the [Message Strings Editor](#) on the [Look and Feel Settings](#); select the selfRegIntro message string.

Enable Pre-Registration Portal

Use this checkbox to enable pre-registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session. From the drop-down menu, select whether you want to pre-register a single user (when you want to pre-register one user at a time) or multiple users (when you have a larger group of users to pre-register) or both. For more information, see [How to Configure Pre-Registration](#).

Generate Password Characters (Shared)

This option is available if you have enabled the Pre-Registration Portal. During the pre-registration process, NAC Manager can automatically generate the password that the guest user uses when connecting to the network. The password is generated according to the specification selected here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

This option is available if you have enabled the Pre-Registration Portal. During the pre-registration process, NAC Manager can automatically generate the password that the guest user uses when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Authenticated Web Access

Authenticated web access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy.

End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Implementing authenticated web access requires web redirection or DNS proxy.

The screenshot displays a web configuration interface with the following sections:

- Authentication (Shared)**
 - AAA Configuration: [basic](#)
 - Authentication To End-System Group: Local [change](#)
 - Local Password Repository: [Default](#)
 - Max Failed Logins:
- Web Page Customizations (Shared)**
 - Login or Register Message: [change](#)
 - Introduction Message: [change](#)
 - Failed Authentication Message: [change](#)
 - Customize Fields: [change](#)
- Redirection (Shared)**
 - Redirection: Use Network Settings Redirection ▾
- Web Access Settings**
 - Enable Agent-Based Login:


Authentication (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the NAC configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple NAC Configurations that are using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Click on the "change" link to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group is mapped to a user group, the icon for the end-system group changes to display a key  indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated web access.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click on the Local Password Repository link to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this option if you want to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Web Page Customizations (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Login or Register Message

Click the "change" link to open a window where you can edit the message displayed to the end user when they are logging in as an authenticated user. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the "change" link to open a window where you can edit the introductory message displayed to the end user when they are logging in as an authenticated user. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the "change" link to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Customize Fields

Click the "change" link to open the [Manage Custom Fields window](#) where you can manage the fields displayed on the Authenticated Web Access login page.

Redirection (Shared)

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the [Network Settings](#).

- **Use Network Settings Redirection** — Use the Redirection option specified on the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page where the end user is redirected. Typically this is the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Web Access Settings

Enable Agent-Based Login

If this option is enabled, when the end user connects to the network with an agent installed, the login dialog is displayed in an agent window instead

forcing the user to go to the captive portal via a web browser. This allows you to provide authenticated web access without having to set up the captive portal. Agent-based login is useful for shared access end-systems running an agent because it prompts for a login dialog and also provides a logout option. Login credentials are limited to username/password and an Acceptable Use Policy is not displayed.

You can customize the messages in the Agent Login window using the [Message Strings Editor](#) available in the [Look and Feel Settings](#). Use the agentLoginMessage string to change the message. Any changes you make in the Message Strings Editor override the internationalized messages used in the Agent Login window.

Assessment/Remediation

Use this panel to configure settings for the Assessment/Remediation portal web page.

The screenshot shows a configuration window with the following sections:

- Web Page Settings:**
 - Title: [change](#)
 - Welcome Message: [change](#)
 - Display Violations:
 - Do Not Allow Rescan:
 - Allow Blacklist Remediation:
 - Permanently Removed Message: [change](#)
 - Custom Agent Install Message: [change](#)
 - Redirection:
 - Access Denied Image:
 - Image During Reattempt:
 - Agent Scan In Progress Image:
- Remediation Attempt Limits:**
 - Limit Remediation Attempts:
 - Limit Time for Remediation (min):
- Remediation Links and Custom Remediation Actions:**
 - Remediation Links (selected):

Name	Link
MAC OS Update	http://www.apple.com/support/downloads
Microsoft Update	http://update.microsoft.com
 - Custom Remediation Actions: (empty)

Web Page Settings

Title

Click on the "change" link to open a window where you can modify the message displayed in the title bar of the Assessment/Remediation web pages. The default page title is "Enterprise Remediation."

Welcome Message

Click on the "change" link to open a window where you can modify the message displayed in the banner at the top of the Assessment/Remediation web page. The default welcome message is "Welcome to the Enterprise Remediation Center."

Display Violations

Use this drop-down list to select an option for displaying assessment violation information to the end user:

- **None** — No violations are displayed to the web page. This option might be used for a Access Control engine that is serving web pages to guest users, when you do not want the guest users to attempt to remediate their end-system.
- **Description and Solution** — Both the description and solution are displayed for violations. This provides the end user with information concerning what violation was found and how to fix it. Providing complete information concerning the violation gives the end user the best chance of self-remediation, however, the technical details of the violation may result in end user confusion. Therefore, this configuration may be appropriate for scenarios where the user population of the network possesses more technical IT knowledge.
- **Description** — Only the description is displayed for violations. This provides the end user with information concerning what violation was found, but no information concerning how it can be fixed. This configuration may be appropriate for scenarios where the user population of the network does not possess technical IT knowledge and is not expected to self-remediate. It provides the Helpdesk personnel with technical information about the violation when the end user places a call to the Helpdesk.
- **Solution** — Only the solution is displayed for violations, allowing the end user to perform self-service remediation without knowing what the violation is. This configuration may be appropriate for scenarios where the user population on the network does not possess technical IT knowledge but is expected to self-remediate.

Do Not Allow Rescan

Select this checkbox if you do not want the end user to have the ability to initiate a rescan of their end-system when quarantined. When selected, the "Reattempt Network Access" button is removed from the Assessment/Remediation web page, and the user is not provided with any way to initiate a rescan on-demand for network access. The end user is forced to contact the Help Desk for assistance. You can edit the "Permanently Removed Message" which, by default, advises the end user to contact the Helpdesk to obtain access to the network. Note that the default configuration of the "Permanently Removed Message" references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Allow Blacklist Remediation

Select this checkbox if you want black-listed end users to have the ability to remediate their problem and attempt to reconnect to the network. When selected, a "Reattempt Network Access" button is added to the Blacklist web page, allowing end users to remove themselves from the blacklist and reauthenticate to the network.

Permanently Removed Message

Click on the "change" link to open a window where you can modify the message displayed when users can no longer self-remediate and must contact the Help Desk for assistance. Note that the default message references the "HELPDESK_INFO" variable which represents the [Helpdesk Information](#) that is defined in the [Look and Feel Settings](#).

Custom Agent Install Message

Click on the "change" link to open a window where you can create a message containing additional agent install information to add to the default text on the Install Agent portal web page.

Redirection

There are four Redirection options that specify where the end user is redirected following successful remediation, when the end user is allowed on the network. The option selected here overrides the Redirection option specified in the [Network Settings](#) for Remediation only.

- **Use Network Settings Redirection** — Use the Redirection option specified in the [Network Settings](#).
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.

- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Access Denied Image

Select the image you would like displayed when the end user has been quarantined and denied access to the network. The drop-down menu displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Image During Reattempt

Select the image you would like displayed while the end-user is reattempting network access after they have repaired their system. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Agent Scan in Progress Image

Select the progress bar image you would like displayed while the end-user is being scanned. The drop-down selection list displays all the images defined in the [Images window](#) for your selection. To add a new image, select Manage Images to open the Images window.

Remediation Attempt Limits

Limit Remediation Attempts

Select this checkbox if you would like to limit the maximum number of times an end-user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the number of attempts allowed.

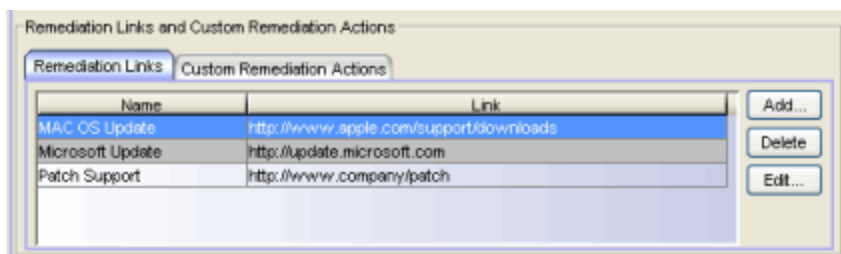
Limit Time for Remediation

Select this checkbox if you would like to limit the total interval of time an end user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the amount of time in minutes.

Remediation Links Subtab

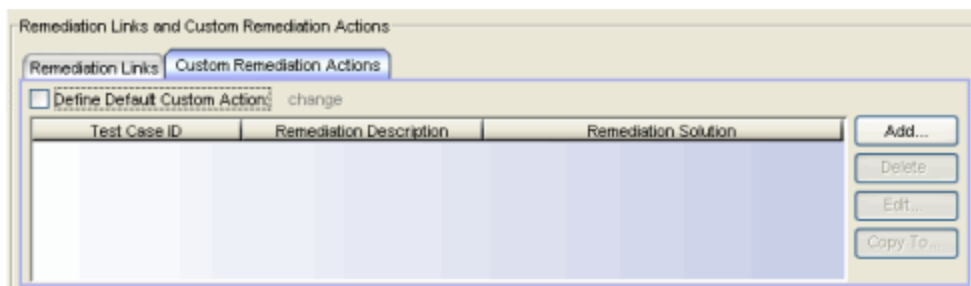
This tab lists the links displayed on the Assessment/Remediation web page for the end users to use to remediate their end-system violations. There are two default remediation links: Microsoft Support and MAC OS Support. Use this tab to add additional links such as an internal website for patches. Links must contain a valid protocol prefix (http://, https://, ftp://).

Click **Add** to open a window where you can define a new link's name and URL. Select a link and click **Edit** to edit the link's information.



Custom Remediation Actions Subtab

Use this tab to create your own custom remediation action for a particular violation to use in place of the remediation action provided by the assessment server.



Use the following steps to add a custom remediation action:

1. Click the **Add** button to open the Add Custom Remediation Action window.
2. Enter the Test Case ID for the particular violation being remediated by the custom action. You can identify the Test Case ID by looking in the Health Results Details subtab in the End-Systems tab.
3. Add a custom description of the violation (required) and an optional custom solution.

4. If you have multiple portal configurations and you would like to use this custom remediation action in all of your configurations, select the **Add to all Portal Configurations** option. This option overwrites any existing custom actions defined for the test case ID.
5. Click **OK**. Whenever the test case ID is listed as a violation on the web page, the custom violation description and solution you define is displayed instead of the remediation actions provided by the assessment server.

Back in the subtab, select the **Define Default Custom Action** checkbox if you would like to advise end users to contact the Helpdesk regarding additional security violations not explicitly listed with custom remediation actions. If this checkbox is selected, only the violations and associated custom remediation actions listed on this tab would be presented to the user, along with a message advising them to contact the Helpdesk for any other security violations not explicitly configured with a custom remediation action. Click the "change" link to edit this message.

To copy a custom action to another portal configuration, select the action in the table and click the **Copy To** button. A window opens where you can select the portal configurations where you want to copy the action, and whether you want it to overwrite any existing custom remediation actions already defined for that test case ID.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Appliance Portal Pages** button at the bottom of the NAC Configuration window.

Web Page	URL
Preview Web Page Allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process.	https://<Access ControlEngineIP>/screen_ preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://<Access ControlEngineIP>/administration

Web Page	URL
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://<Access ControlEngineIP>/sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://<Access ControlEngineIP>/pre_ registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://<Access ControlEngineIP>/self_ registration

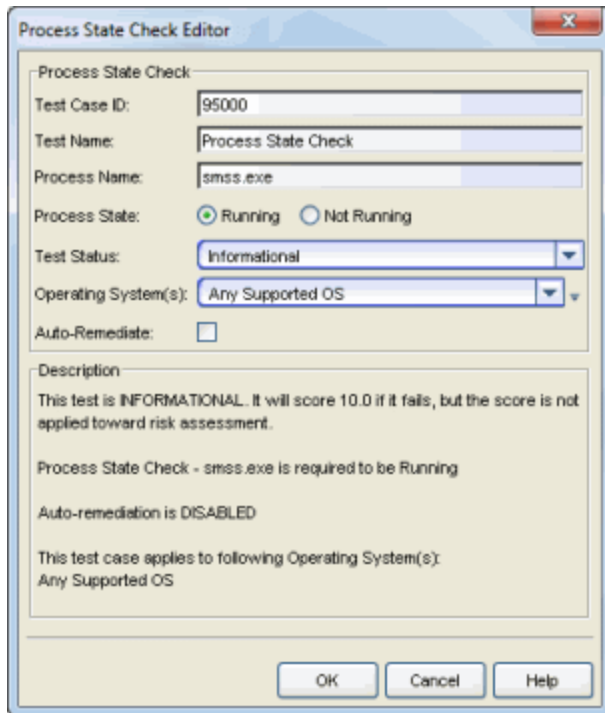
Related Information

For information on related help topics:

- [How to Set Up Assisted Remediation](#)
- [How to Set Up Registration](#)
- [How to Configure Verification for Guest Registration](#)

Process State Check Editor

This window lets you configure parameters for a Process State Check test case included in an [agent-based test set](#). This test checks to see if a specific process is running on the end-system.



The screenshot shows the 'Process State Check Editor' dialog box. It contains the following fields and options:

- Process State Check** (Section Header)
- Test Case ID:** 95000
- Test Name:** Process State Check
- Process Name:** smss.exe
- Process State:** Running Not Running
- Test Status:** Informational (dropdown menu)
- Operating System(s):** Any Supported OS (dropdown menu)
- Auto-Remediate:**
- Description:**
 - This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.
 - Process State Check - smss.exe is required to be Running
 - Auto-remediation is DISABLED
 - This test case applies to following Operating System(s): Any Supported OS

Buttons at the bottom: OK, Cancel, Help.

Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Process Name

The name of the process you are checking for.

Process State

Specify whether the process must be running or not running on the end-system.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined. Auto-remediation will be performed, if enabled.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation will be performed, if enabled.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation will be performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Auto-Remediate

If Auto-Remediate is selected, the agent will attempt to start or stop the process, depending on the selected Process State. For remediation to start the process, the .exe must be on the system path. When remediation stops the process, it will attempt to kill all instances of the process.

Description

A description of the test case parameters.

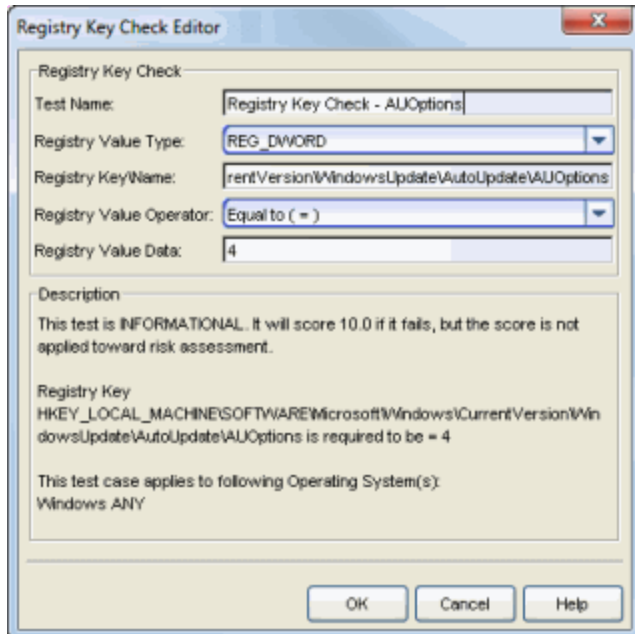
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Registry Key Check Editor

This window lets you create a registry key test to be used in an [Advanced Registry Key Check](#) test case. The advanced test case allows you to group individual registry key checks together into a single test case. Each individual test checks to see if the end-system has a one specific Windows registry key.



Test Name

You can use this field to change or edit the test case name, if desired.

Registry Value Type

Select the registry value type from the following options:

- REG_SZ (STRING)
- REG_DWORD
- REG_BINARY
- KEY EXISTS - checks to see if the registry key is installed
- KEY NOT EXIST - checks to see if the registry key is not installed

Registry Key Name

Enter the Registry Key\Name using the format shown in the following example:

HKEY_LOCAL_

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\AutoUpdate\AUOptions

If you are verifying that a folder exists in the registry (a default registry entry) the Registry Key Name must end with either (Default) or \\\, as shown below:

HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap\(\Default)
HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap\\

NOTE: The Registry Key check does not currently support checking for the Multi-String, Expandable String, and QWORD registry key values.

Registry Value Operator

Select the Registry Value Operator (not used for KEY EXISTS and KEY NOT EXIST options).

Registry Value Data

Enter the Registry Value Data (not used for KEY EXISTS and KEY NOT EXIST options).

Description

A description of the test case parameters.

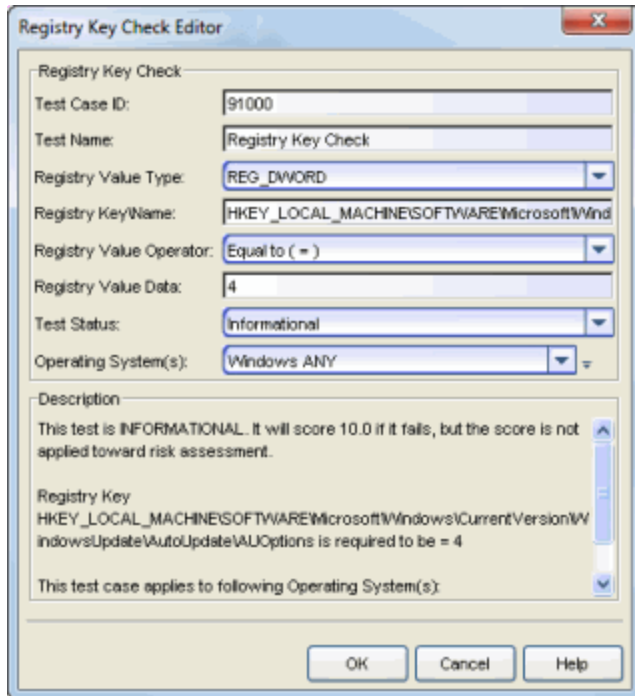
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)
- [Registry Key Check Advanced Editor](#)

Registry Key Check Editor

This window lets you configure parameters for a Registry Key Check test case included in an [agent-based test set](#). This test checks to see if the end-system has one specific Windows registry key. If you would like to create a test that checks for multiple registry keys, use the [Registry Key Check Advanced Editor](#).



Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Registry Value Type

Select the registry value type from the following options:

- REG_SZ (STRING)
- REG_DWORD
- REG_BINARY

- KEY EXISTS - checks to see if the registry key is installed
- KEY NOT EXIST - checks to see if the registry key is not installed

Registry Key Name

Enter the Registry Key\Name using the format shown in the following example:

HKEY_LOCAL_

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\AutoUpdate\AUOptions

If you are verifying that a folder exists in the registry (a default registry entry) the Registry Key Name must end with either (Default) or \\\, as shown below:

HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap\(\Default)

HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap\\

NOTE: The Registry Key check does not currently support checking for the Multi-String, Expandable String, and QWORD registry key values.

Registry Value Operator

Select the Registry Value Operator (not used for KEY EXISTS and KEY NOT EXIST options).

Registry Value Data

Enter the Registry Value Data (not used for KEY EXISTS and KEY NOT EXIST options).

Test Status

Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.


- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.

- **Mandatory** - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. If the status is Mandatory, the end-system will fail the test if the registry key is not found or if the registry key is found, but the value does not match. For the KEY EXIST and KEY NOT EXIST options, if the status is Mandatory, the end-system will fail the test if the registry is found or not found respectively.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.

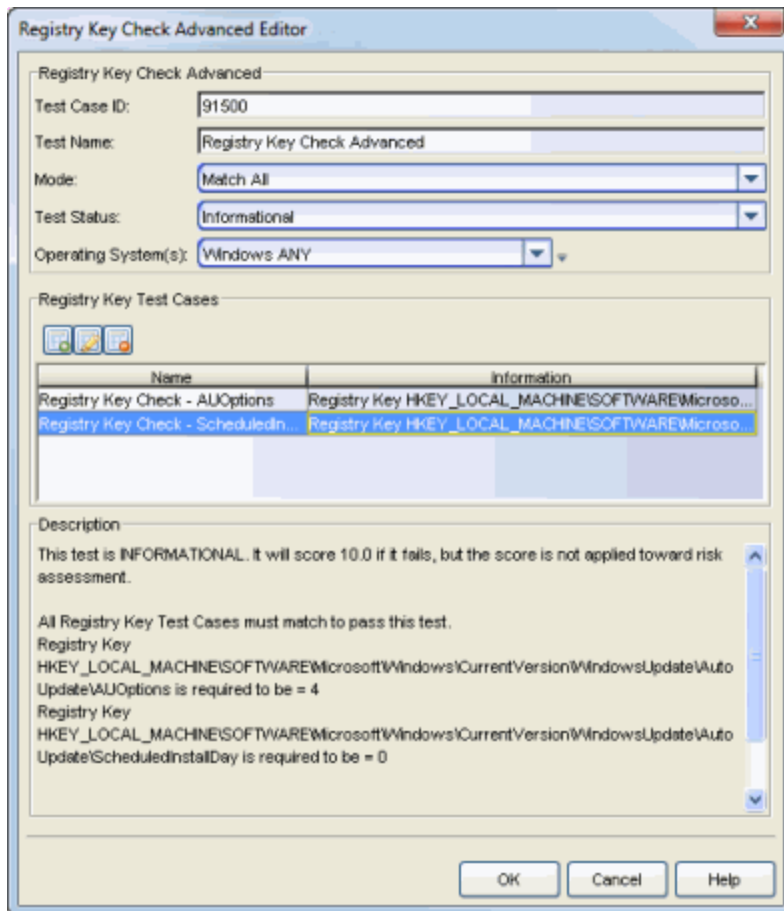
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Registry Key Check Advanced Editor

This window lets you configure parameters for a Registry Key Check Advanced test case included in an [agent-based test set](#). This test allows you to group individual registry key checks together into a single advanced test case. Use this window to configure your advanced test case parameters and the individual registry checks that will be included.



Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Mode

Use the drop-down list to select the test mode:

- Match Any - A match with any of the Registry Key Test Cases will pass the test.
- Match All - A match with all of the Registry Key Test Cases is required to pass the test.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. If the status is Mandatory, the end-system will fail the test if the registry key is not found or if the registry key is found, but the value does not match. For the KEY EXIST and KEY NOT EXIST options, if the status is Mandatory, the end-system will fail the test if the registry is found or not found respectively.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Registry Key Test Cases

Use the Test Cases table to view and define the individual registry key checks that will be included in the advanced test case.



Use these buttons to add, edit, or delete registry key checks listed in the table. Use the Add button to open the [Registry Key Check Editor window](#) where you can create a key check to add to the list.

Name

The name of the test case.

Information

Information about the test case requirements that have been configured.

Description

A description of the test case parameters.

Related Information

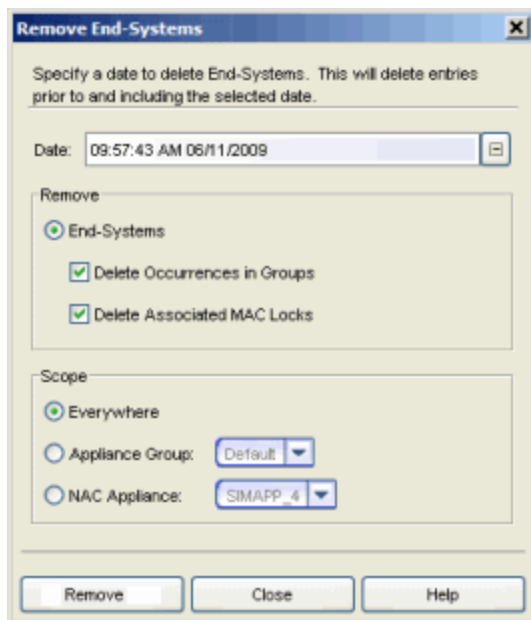
For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)
- [Registry Key Check Editor Window \(for Advanced Test Case\)](#)

Remove End-Systems Window

Use this window to remove end-systems from the tables and charts in the [End-Systems tab](#) and the [Statistics tab](#). End-systems are removed based on the date you specify in this window and the options you select. You can also select a scope for the Remove operation which lets you specify whether to remove the end-systems from everywhere, from a selected engine group, or from a selected Extreme Access Control engine.

You can access this window by selecting **Tools > End-System Operations > Remove End-Systems** from the menu bar.



Date

Select a date to use when removing end-systems. End-systems with a [Last Seen](#) date prior to and including the selected date are removed.

Remove End-Systems

Select this option to remove end-systems based on the specified date. The database is searched for end-systems with a [Last Seen](#) date prior to and including that date. Those end-systems are removed from the tables in the [End-Systems tab](#).

If you select the **Delete Occurrences in Groups** and the **Delete Associated**

MAC Locks checkboxes, any group assignments or MAC locks associated with the end-systems are also removed.

NOTE: Selecting **Delete Occurrences in Groups** does not remove an end-system from the Blacklist group. Blacklist is a special group that requires end-systems to be manually removed using the [Edit End-System Group window](#).

Scope

These options let you select where to remove the end-systems.

- Everywhere - Remove from all Extreme Access Control engines and engine groups.
 - Appliance Group - Remove from the selected engine group.
 - NAC Appliance - Remove from the selected engine .
-

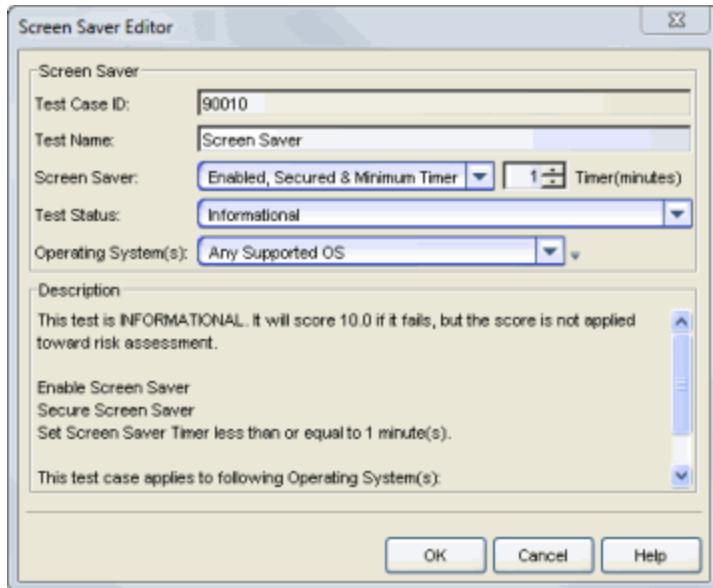
Related Information

For information on related tabs and windows:

- [End-Systems Tab](#)
- [Statistics Tab](#)
- [Data Persistence](#)

Screen Saver Editor

This window lets you configure parameters for the Screen Saver test case included in an [agent-based test set](#). This test checks to see if a screen saver is enabled, if the screen saver is secured (password protected), and the time before the screen saver starts.



The screenshot shows the 'Screen Saver Editor' dialog box. It contains the following fields and controls:

- Test Case ID:** A text box containing '90010'.
- Test Name:** A text box containing 'Screen Saver'.
- Screen Saver:** A dropdown menu set to 'Enabled, Secured & Minimum Timer' and a spinner box set to '1' with the label 'Timer(minutes)'.
- Test Status:** A dropdown menu set to 'Informational'.
- Operating System(s):** A dropdown menu set to 'Any Supported OS'.
- Description:** A scrollable text area containing the text: 'This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.' Below this are three sub-items: 'Enable Screen Saver', 'Secure Screen Saver', and 'Set Screen Saver Timer less than or equal to 1 minute(s)'. At the bottom of the description area, it says 'This test case applies to following Operating System(s):'.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Test Case ID

The test case is automatically assigned a Test Case ID number, which you cannot change. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Screensaver

Specify whether the screen saver must be enabled, whether the screen saver must be secured (password protected), and the time before the screen saver starts.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Description

A description of the test case parameters.


Related Information

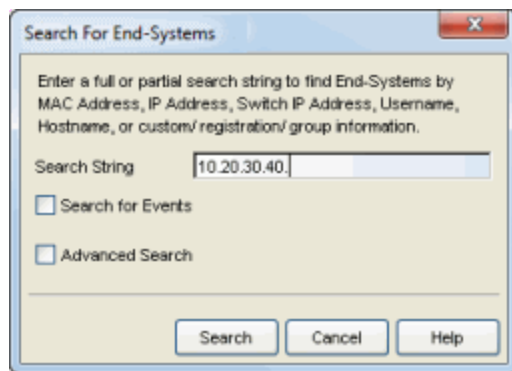
For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Search for End-Systems Window

This window lets you search your NAC Manager database for end-systems and end-system events that match the search criteria you specify. You can search for full or partial matches on MAC address, IP address, switch IP address, user name, hostname, or custom, registration, or group information. Enter the full or partial value you are searching for and click the **Search** button. Search results are displayed in the [End-Systems tab](#) (presented as a separate window).

You can access the Search for End-Systems window by selecting **Tools > End-System Operations > Search for End-Systems** from the menu bar or clicking the **Search for End-Systems** toolbar button .



Use the **Search for Events** checkbox to search end-system events for the specified information. When searching for events, NAC Manager matches the criteria you specify against historical end-system connection information. The search scans through the end-system event cache and stops after finding 1,000 matches or reaching the end of the cache. Results are displayed in an End-System Events Search Results table. Click on the **Search for Older Events** button at the bottom of the results table to extend the search to older events stored in the database outside of the cache. The maximum search parameters for this extended search are configured in the [End-System Event Cache options](#) in the NAC Manager Options view (Tools > Options). The extended search is ended when any one of the search parameters is reached:

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

For advanced end-system search features, select the **Advanced Search** checkbox. In the Advanced Search, you can specify more detailed search criteria as explained below. The search criteria you specify is matched against the last known connection state for each end-system attempting to connect. For example, if you search for end-systems with a state of **Accept**, the search return all end-systems currently in that state, and not end-systems that were in that state at one time or another. With the **Enable Auto Complete** checkbox selected, as you type search criteria into the fields in this window, NAC Manager lists possible matches based on information in the NAC Manager database.

Search window with Advanced Search feature selected.

The screenshot shows the 'Search For End-Systems' window with the 'Advanced Search' checkbox checked. The window contains a 'Search Criteria' section with various search options and fields. The 'Enable Auto Complete' checkbox is also checked. The 'NAC Appliance' dropdown is set to 'SMAPP_1'. The 'Switch IP' field is filled with '77.12.4.4'. The 'State' dropdown is set to 'Quarantine'. The 'Last Seen', 'First Seen', and 'Last Scanned' fields are set to 'Before' with a date of '12:00:00 AM 04/05/2011'. The 'Search' button is highlighted.

Search Criteria	Operator	Value	Search Criteria	Operator	Value
<input checked="" type="checkbox"/> Enable Auto Complete			<input checked="" type="checkbox"/> NAC Appliance		SMAPP_1
<input type="checkbox"/> MAC Address	Equals		<input type="checkbox"/> End-System IP		
<input checked="" type="checkbox"/> Switch IP		77.12.4.4	<input type="checkbox"/> Hostname	Equals	
<input type="checkbox"/> Device Type	Equals		<input type="checkbox"/> Device Family	Equals	
<input type="checkbox"/> Username	Equals		<input type="checkbox"/> NAC Profile	Equals	
<input type="checkbox"/> Authentication Type		MAC	<input checked="" type="checkbox"/> State		Quarantine
<input type="checkbox"/> Extended State		Scan Requested	<input type="checkbox"/> State Description	Equals	
<input type="checkbox"/> Authorization	Equals				
<input type="checkbox"/> Last Seen	Before	12:00:00 AM 04/05/2011	and		12:00:00 AM 04/05/2011
<input type="checkbox"/> First Seen	Before	12:00:00 AM 04/05/2011	and		12:00:00 AM 04/05/2011
<input type="checkbox"/> Last Scanned	Before	12:00:00 AM 04/05/2011	and		12:00:00 AM 04/05/2011
<input type="checkbox"/> Custom 1	Equals		<input type="checkbox"/> Custom 2	Equals	
<input type="checkbox"/> Custom 3	Equals		<input type="checkbox"/> Custom 4	Equals	
<input type="checkbox"/> Registered User	Equals		<input type="checkbox"/> Registered Email	Equals	
<input type="checkbox"/> Sponsor	Equals		<input type="checkbox"/> Registration 1	Equals	
<input type="checkbox"/> Registration 2	Equals		<input type="checkbox"/> Registration 3	Equals	
<input type="checkbox"/> Registration 4	Equals		<input type="checkbox"/> Registration 5	Equals	
<input type="checkbox"/> Registration Descr	Equals		<input type="checkbox"/> Groups	Equals	
<input type="checkbox"/> Group 1	Equals		<input type="checkbox"/> Group 2	Equals	
<input type="checkbox"/> Group 3	Equals				

Advanced Search

Search Cancel Help

Enable Auto Complete

Select **Enable Auto Complete** to list possible matches based on information in the NAC Manager database as you type search criteria into the fields in this window.

With the Advanced Search checkbox selected, choose from the following advanced search criteria:

NAC Appliance

If you specify a NAC (Extreme Access Control) engine, NAC Manager only searches for end-systems last seen connecting to that engine. If you don't specify a Extreme Access Control (Access Control) engine, NAC Manager searches for all end-systems matching the selected criteria across all engines.

MAC Address

Search for an end-system's MAC address.

End-System IP

Search for an end-system's IP address.

Switch IP

Search by the IP address of the switch to which the end-system connected.

Hostname

Search by the hostname of the end-system.

Device Type

Search by the detected device type for the end-system. Device type can be the hardware type or the operating system.

Device Type Family

Search by the detected device type family for the end-system. Device type family can be the hardware family or the operating system family.

Username

Search by the username the end-system used to connect.

NAC Profile

Search by the name of the NAC profile that was assigned to the end-system when it connected to the network.

Authentication Type

Search by the end-system's authentication type. The following authentication types are supported in NAC Manager:

- MAC - includes the following MAC authentication types
 - MAC (PAP)
 - MAC (EAP-MD5)
 - MAC (CHAP)
- IP (L3 Access Control Controller only)
- PAP
- CHAP
- 802.1X - includes the following 802.1X authentication types
 - 802.1X (EAP-TLS)
 - 802.1X (EAP-TTLS)
 - 802.1X (EAP-MD5)
 - 802.1X (EAP-PEAP)
 - 802.1X (EAP-FAST)
 - 802.1X (EAP-LEAP)
 - 802.1X (EAP-RSA)
 - 802.1X (EAP-SIM)
- MS NAP (Microsoft NAP)
- Registration Administration
- Kerberos

State

Search by the end-system's connection state:

- Accept - The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Reject - The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Scan - The end-system is currently being scanned.
- Quarantine - The end-system is quarantined because the scanning test failed.
- Disconnected - All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches with

RADIUS accounting enabled, or if the Session Deactivate Timeout option is enabled on the [Reauthentication tab](#) in Appliance Settings.

- Error - Indicates one of nine problems:
 - the MAC to IP resolution failed, if assessment is enabled
 - the MAC to IP resolution timed out, if assessment is enabled
 - all RADIUS servers are unreachable
 - the RADIUS request was non-compliant
 - all assessment servers are unavailable
 - the assessment server can't reach the end-system
 - no assessment servers are configured
 - the assessment server is not compatible with the current version of NAC Manager
 - the username and password configured in the [Assessment Server panel](#) of the NAC Manager options (Tools > Options > Assessment Server) are incorrect for the assessment server

Extended State

Search by the end-system's extended state:

- Scan Requested - A scan is requested for the end-system.
- Scan in Progress - The end-system re-authenticated while a scan was already in progress.
- MAC to IP Resolution Failed - The scan cannot be performed because the end-system's MAC address cannot be resolved to an IP address.
- Assessment Server(s) Unavailable - There are no Assessment servers available to perform a scan on the end-system.
- Assessment Server Can't Reach Host - The Assessment server cannot reach the end-system to perform a scan.
- No Assessment Servers Configured - A scan is required for the end-system, but no Assessment servers are configured in NAC Manager.
- MAC to IP Resolution Timed Out - The scan cannot be performed because the end-system's MAC address was not resolved to an IP address in the allowed time.
- Resolving IP Address - MAC to IP Address Resolution is being performed for the end-system.
- Scan Complete - A scan is completed for the end-system.

- RADIUS Request Missing Required Attributes - The attributes returned from the RADIUS server were not sufficient for processing.
- Invalid Assessment Server Login Credentials - The login credentials supplied to communicate with the third-party assessment software (Nessus) are invalid.
- Invalid Assessment Server Type for Configuration - The assessment server being used doesn't match the assessment server type specified in the assessment configuration.
- There is an error with the test set configuration
- Assessment Discarded - Only one scan can be running against an end-system at a time. If a scan is in progress and a Force Reauth and Scan operation is performed, the existing scan is discarded and a new scan starts. This may also occur if a scan is in progress and the agent reconnects/disconnects. In both of these cases, when the first scan is aborted, the following message displays: "assessment discarded, because of new assessment request".
- License not found - The third-party assessment software (Saint) no license file.
- License expired - The third-party assessment software license (Saint) is expired.
- License error - Generic error concerning third-party assessment software licensing, but NAC Manager can't determine the exact cause.
- Agent not connected to server - The assessment agent is not connected to the assessment server.
- Assessment Incompatibility - The assessment server is not compatible with the current version of NAC Manager.
- Communication Error - A communication error between Extreme Management Center Server and NAC Manager occurred during registration. The end-system was registered via Survivable Registration (if enabled) and assigned the Failsafe policy.
- Unrecognized Condition
- Assessment Bypass enabled - The NAC Manager assessment process is disabled using the [NAC Bypass feature](#).
- Assessment Warning - During the last scan, the end-system was put into the Assessment Warning end-system group.

State Description

Search by the end-system's state description.

Authorization

Search by the attributes returned by the RADIUS server for the end-system. For Layer 3 Access Control Controller engines, you can search by the policy assigned to the end-system for its authorization.

Last Seen

Search by the last date and time the end-system was seen by the Access Control engine.

First Seen

Search by the first date and time the end-system was seen by the Access Control engine.

Last Scanned

Search by the last date and time an assessment (scan) was performed on the end-system.

Custom 1-4

Search by matching the text in any of the four custom end-system information columns.

Registered User

Search by the registered username supplied by the end user during the registration process.

Registered Email

Search by the email address supplied by the end user during the registration process.

Sponsor

Search by the registered device's sponsor.

Registration 1-5

Search by the information that was entered in custom registration fields by the end user during the registration process.

Registration Descr

Search by the device description supplied by the end user during the registration process.

Groups

Search by the end-system and/or user groups to which the end-system belongs.

Group 1-3

Search by the entry description that was entered when the end-system was added to a MAC-based end-system group.

Advanced Search

Use this checkbox to display or hide the Advanced Search features.

Related Information

For information on related windows:

- [End-Systems Tab](#)
- [Statistics Tab](#)

Search for End-Systems by Assessment Results Window

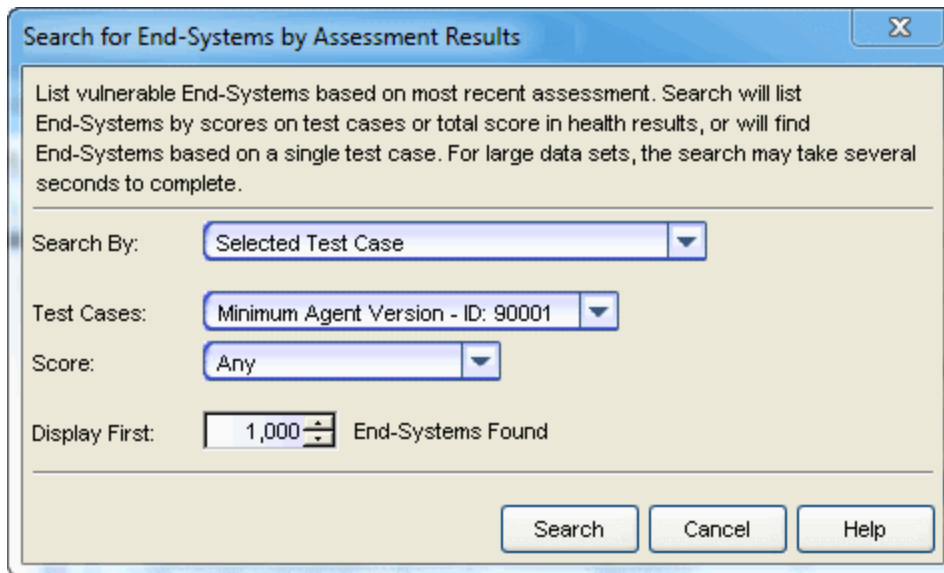
This window lets you search for vulnerable end-systems based on their assessment results. In order to display the most current data, searches are limited to information from the latest assessment results for each end-system. Search results display in the [End-Systems tab](#), presented as a separate window.

You can perform a search using the following criteria:

- Highest Test Case Scores to Lowest — Sorts the end-systems according to their highest individual test case score (from the **Health Result Details** tab), listing the most vulnerable end-system with the highest score first.
- Highest Total Health Result Scores to Lowest — Sorts the end-systems according to their total health result score (from the **Health Result Summaries** tab), listing the most vulnerable end-system with the highest total score first. The total score is the total sum of the scores for all the health details that were included as part of the quarantine decision.
- Highest Total Health Result Actual Scores to Lowest — Sorts the end-systems according to their actual health result score (from the Health Result Summaries tab), listing the most vulnerable end-system with the highest actual score first. The actual score is the total score with all health details included as part of the quarantine decision, including those marked Informational and Warning.
- Selected Test Case — Searches for end-systems where a specific test case and score are part of their latest assessment results.
- Test Case ID — Searches for end-systems where a specific test case ID and score are part of their latest assessment results.
- Outstanding Warnings — Searches for end-systems that acknowledged warnings sent by NAC Manager, but did not clear them.
- Unacknowledged Warnings — Searches for end-systems that received warnings, but did not acknowledge them.

Access the Search window by selecting **Tools > End-System Operations > Search for End-Systems by Assessment Results** from the menu bar.

Search window with Test Case Search selected.



Search By

Use the drop-down menu to select the search [criteria](#).

Test Case/Test Case ID and Score

Select the test case name or enter the test case ID if searching for a specific test case or test case ID . Specify a score to match, if desired.

Display First

Specify the number of end-systems listed in the search results.

Related Information

For information on related windows:

- [End-Systems Tab](#)

Send Message to End System Agents Window

Use this window to send a message to one or more end-systems running an assessment agent. End-systems do not have to be authenticated to the same Extreme Access Control engine, however all Extreme Access Control engines must be running version 6.3 or higher. This window is accessed via the [End-Systems tab](#).

Icon: Informational

Title: New Version Available

Message: A new version of the NAC Assessment Agent is available. Click on the link to upgrade.

Link: Upgrade Now...

Url: https://%NAC_IP%/agent_download




Display Time: 0

(seconds) 0 = display until clicked

OK Cancel

Icon

Select the icon displayed to indicate the priority of the message, **Informational**, **Warning**, or **Error**. The icons appear within messages as follows:

- Informational —  **New Version Available**
A new version of the NAC Assessment Agent is available. Click on the link to upgrade.
[Upgrade Now...](#)
- Warning —  **New Version Available**
A new version of the NAC Assessment Agent is available. Click on the link to upgrade.
[Upgrade Now...](#)
- Error —  **New Version Available**
A new version of the NAC Assessment Agent is available. Click on the link to upgrade.
[Upgrade Now...](#)

Title

Enter a title for the message.

NOTE: Entering **%NAC_IP%** in the **Title**, **Message**, **Link**, or **URL** fields enters the IP address for the Extreme Access Control engine when the message is sent to the agent.

Message

Enter the text displayed when the message is sent.

Link

Enter the text that appears as a hperlink to the location defined in the **URL** field. This field is optional.

URL

Enter the URL that corresponds to the **Link**. This field is optional.

Display Time

Enter the amount of time (in seconds) the message displays on the end-system. Entering **0** displays the message until it is manually closed by the user.

Related Information

For information on related windows:

- [End-Systems Tab](#)

Service State Check Editor

This window lets you configure parameters for a Service State Check test case included in an [agent-based test set](#). This test checks to see if a specific service is installed and running on the end-system.



Test Case ID

The test case is automatically assigned a Test Case ID number, although you can change this number, if desired. You can refer to this Test Case ID number when creating [scoring overrides](#) or looking at the [Health Result Details Tab](#) in the End-Systems tab.

Test Name

You can use this field to change or edit the test case name, if desired.

Service Name

The name of the service you are checking for. You must specify the actual service name. To see the names of running services you can run `tasklist /SVC` from a command prompt. This command will show the registered names of the services and not the alias names that may be shown in the Windows Administrative Services UI.

Service State

Specify whether the service must be installed or installed and running on the end-system.

Test Status


Use the Test Status drop-down list to specify a status for this test. The status determines how the score returned by the assessment test will be used.

- Disabled - The test will not be run.
- Informational - The test will be run and test score results will be reported, but are not applied towards a quarantine decision. No end-systems will be quarantined. Auto-remediation will be performed, if enabled.
- Warning - Test score results are only used to provide end user assessment warnings via the Notification portal web page. No end-systems will be quarantined unless a [grace period](#) (if specified) has expired. Auto-remediation will be performed, if enabled.
- Mandatory - Test score results will be included as part of the quarantine decision, and end-systems can be quarantined. Auto-remediation will be performed, if enabled.

The default scoring for agent-based tests is 0 for pass and 10 for fail. You can use [scoring overrides](#) if you wish to customize the default scoring.

Operating System(s)

Use the checkboxes in the drop-down list to select the operating systems that this test case will apply to. This list is automatically populated with all the operating systems on which this test can be performed.

 Use the configuration menu button to open the Manage Operating Systems window where you can add a new operating system for selection. For example, you may want to add a Windows operating system with a different service pack requirement. However, keep in mind that any changes you make will only be reflected in the drop-down selection list as long as they are supported by the test.

Auto-Remediate

If the service state is "Installed and not Running" or "Installed and Running", and Auto-Remediate is selected, the agent will attempt to start or stop the service. When remediation starts the service, its startMode will be set to Automatic. When remediation stops a service, its startMode will be set to Manual. For remediation to start a service, it must exist.

Description

A description of the test case parameters.

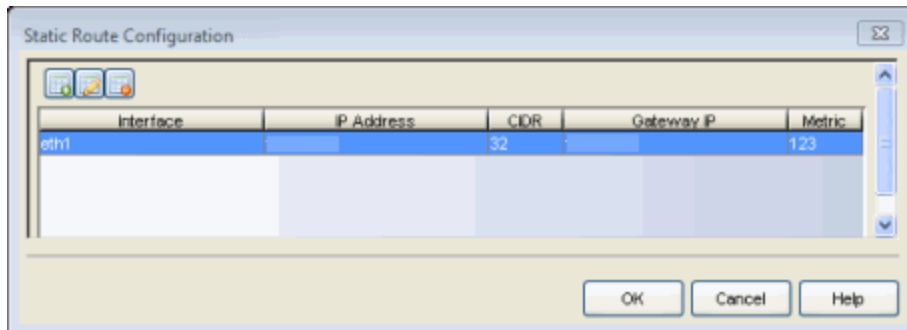
Related Information

For information on related topics:

- [Add/Edit Agent-Based Test Set Window](#)
- [How to Deploy Agent-Based Assessment](#)

Static Route Configuration Window

This window displays the static routes used for advanced routing configuration. Use the toolbar buttons to add, edit, or delete a route. This window is accessed from the Static Routes button on the [Appliance Configuration tab](#).



Interface

The Extreme Access Control engine interface used for the static route.

IP Address

The IP address used to define the subnet or individual device whose traffic is assigned to the route.

CIDR

The CIDR notation for the subnet or device.

Gateway IP

The IP address of the device where traffic matching the Network value is sent.

Metric

A number used to configure route precedence. The lower the number, the higher the precedence.

Synchronize Appliances with Console Window

This window allows you to synchronize the NAC Manager device database with the Console's database. It lets you import Extreme Access Control engines currently defined in Console but not in NAC Manager, and lets you export engines that are defined in NAC Manager, but not in Console. You can access this window by selecting **Tools > Synchronize With Console** from the menu bar.

Synchronize Appliances With Console

Import NAC Appliances From Console

These are the NAC Appliances that are currently defined in Console, but are not defined in NAC Manager. In the table below, select the Appliances you wish to create and choose the associated RADIUS Servers to use for those Gateways.

Select	IP Address	Primary RADIUS Server	Secondary RADIUS Server
<input type="checkbox"/>	10.20.93.147	89.98.89.98	89.98.89.98
<input type="checkbox"/>	10.20.93.179	89.98.89.98	89.98.89.98
<input checked="" type="checkbox"/>	10.20.93.150	89.98.89.98	89.98.89.98

Export NAC Appliances To Console

These are the NAC Appliances that are currently defined in NAC Manager, but are either not defined in Console, or are not recognized as Appliance devices in Console. In the table below, select the Appliances you wish to create in Console and choose the associated profile to use for those Appliances.

Select	IP Address	Profile
<input checked="" type="checkbox"/>	90.90.90.5	public_v1_Profile
<input checked="" type="checkbox"/>	90.90.90.3	public_v1_Profile
<input checked="" type="checkbox"/>	90.90.90.2	public_v1_Profile
<input checked="" type="checkbox"/>	90.90.90.1	public_v1_Profile

Import NAC (Extreme Access Control) Appliances From Console

This table lists the Extreme Access Control (NAC) Engines currently defined in Console but not in NAC Manager. Select the engines you want to import. If you are using the engine as a proxy RADIUS server, use the drop-down menus to select the primary and secondary RADIUS servers for the engine. If there are no RADIUS servers configured, click the **Manage RADIUS Servers** button to open the Manage RADIUS Servers window where you can add your RADIUS servers. Once a RADIUS Server is added, it becomes available for selection as a primary or secondary server. Click **Import Appliances** to import the selected engines.

Export NAC Appliances To Console

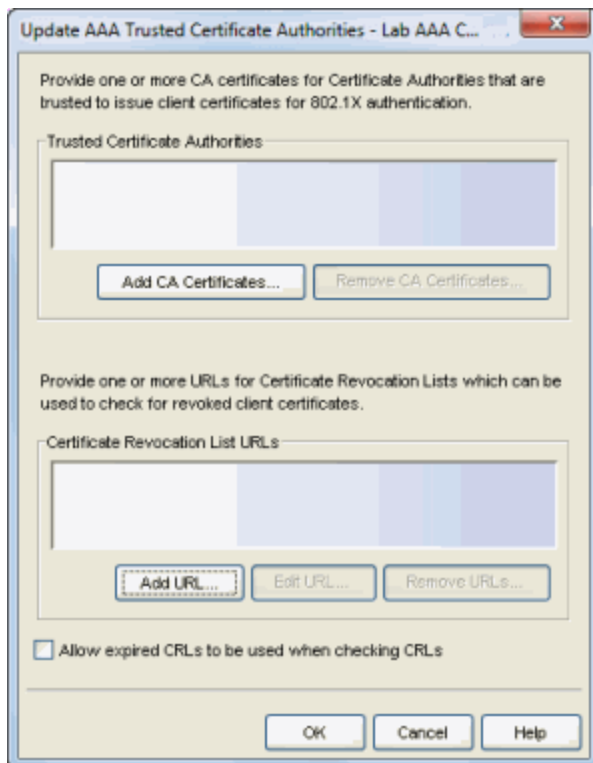
This table lists the Extreme Access Control (NAC) engines currently defined in NAC Manager, but not in Console. Select an engine and use the drop-down menu to select one of the SNMP profiles defined for device access. (SNMP profiles are defined in the Profiles/Credentials tab of the Authorization/Device Access window.) Click **Export to Console** to export the selected engines.

Update AAA Trusted Certificate Authorities Window

If your NAC deployment is configured for EAP-TLS, PEAP, or EAP-TTLS authentication and the authentication requests are not proxied, you will need to [update your RADIUS server certificate](#) to a CA certificate that your connecting end-systems trust. In addition, you will need to use this window to configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted.

This information is part of the AAA configuration and shared across all appliances in an appliance group. This allows end-systems to be trusted on any NAC appliance where they can authenticate. You can access this window from the [Manage Appliance Certificates window](#) or your [AAA Configuration](#).

The information entered in this window is saved in the appliance configuration in the NetSight database and written to the appliance when it is enforced. When enforced, the RADIUS server on the appliance will be restarted automatically to load the changes. Changing this configuration affects all appliances that use the AAA configuration.



Trusted Certificate Authorities

Use **Add CA Certificate** and **Remove CA Certificates** to create a list of certificate authorities (CAs) that are trusted to issue client certificates for 802.1X authentication. When you add a CA, you must provide a file that contains the CA's certificate. The CA's name appears in the list.

Certificate Revocation List URLs

Use **Add URL**, **Edit URL**, and **Remove URLs** to create a list of CRL distribution points which will be used to check for revoked client certificates. When an end-user's access to the network has been revoked, the end-user's client certificate is revoked. This will cause the CA to add the revoked certificate's serial number to its CRL. The NAC appliance will download a new copy of any configured CRL every hour from the CRL distribution point identified by the URL. If the CRL has been updated, the RADIUS server will be restarted to load the new data. The RADIUS server will then reject any client certificate found in the CRL.

When CRLs are used, there must be a CRL configured for every trusted certificate authority. Only CRLs that are distributed through an http:, https:, or file: URL are supported, and only CRLs that correspond to a listed trusted certificate authority can be used. Delta CRLs are not allowed.

Expired CRLs

Generally, CRLs are updated at about the same time the current CRL expires. By default, if a CRL has expired, all certificates from the corresponding certificate authority are rejected. If this option is selected, it allows the expired CRL to continue to be used until a new, updated version is downloaded.

Related Information

For information on related tasks:

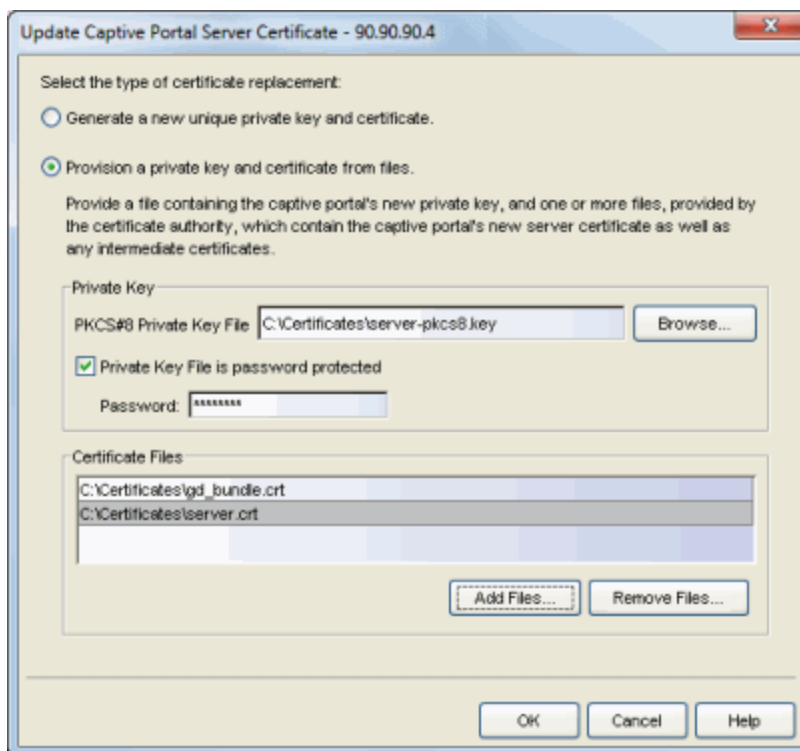
- [How to Update NAC Appliance Server Certificates](#)
- [Manage Appliance Certificates Window](#)
- [Update RADIUS Server Certificate Window](#)

Update Captive Portal Server Certificate Window

The NAC appliance server uses a private key and server certificate to provide secure communication for the NAC Manager captive portal web pages. The Update Captive Portal Server Certificate window lets you replace the server certificate. You can access this window from the [Manage Appliance Certificates window](#).

During installation, NetSight generates a unique private server key and server certificate for the captive portal server. While these provide secure communication, you may want to update to a "browser-friendly" certificate in order to eliminate the browser warnings that might appear when end users access the NAC Manager captive portal web pages for registration or remediation, and when administrators and sponsors access the NAC registration administration and sponsor administration web pages. For complete instructions on replacing and verifying the certificate, see [How to Update NAC Appliance Server Certificates](#).

After you have updated the certificate, you must enforce the appliance to deploy the new private key and server certificate. When enforced, the server's secure port 443 will be offline for 15 seconds to reload the certificate.



Select the type of certificate replacement

You can select from two types of certificate replacement:

- **Generate a new unique private key and server certificate.** This option allows you to automatically generate a new private key and certificate using the same method that is used when NAC is installed.
- **Provision a private key and certificate from files.** This option lets you update the server certificate to a custom certificate provided from an external certificate authority. For complete instructions on replacing and verifying the certificate using this option, see [How to Update NAC Appliance Server Certificates](#).

Private Key

Provide a file containing the RSA or DSA private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field. If you do not have the private key, refer to the [instructions for generating](#) them.

Certificate Files

Use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

NOTE: If the Captive Portal server certificate identifies the appliance by a fully qualified host name, be sure the captive portal is configured with the Use Fully Qualified Domain Name option enabled in the Edit Captive Portal window, [Common settings](#). Verify that end users are routed to the captive portal with the appliance's fully qualified host name (the same name used on the certificate) instead of IP address in the portal URL and that there are no unexpected browser warnings. If the option is not enabled, then end users may get certificate warning messages in their browsers about the wrong server name. This would happen because the IP address in the URL will not match the domain name in the server certificate.

Related Information

For information on related windows:

- [How to Update NAC Appliance Server Certificates](#)
- [Manage Appliance Certificates Window](#)

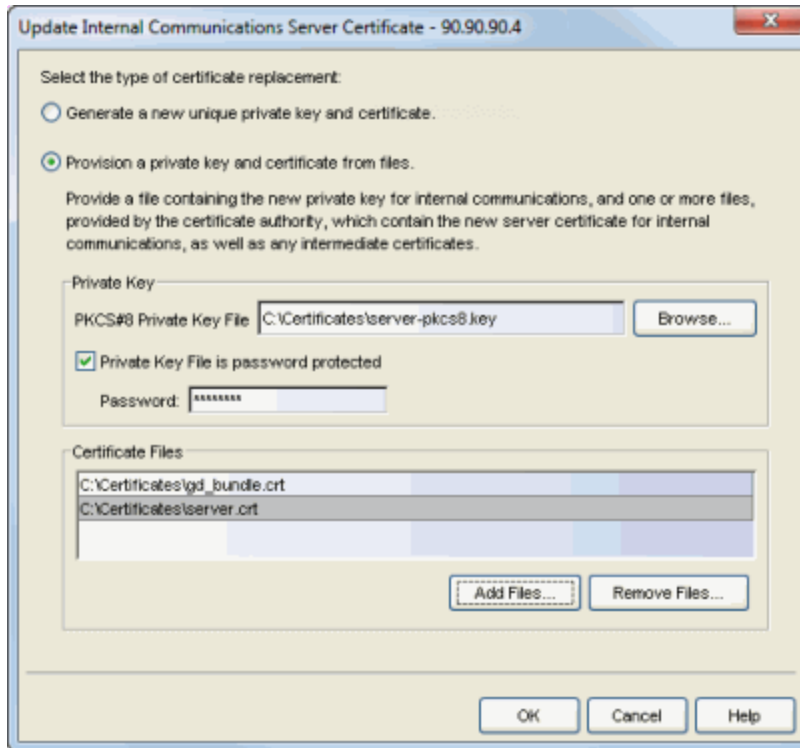
Update Internal Communications Server Certificate Window

The NAC appliance Internal Communications server uses a private key and server certificate to provide secure communication between the appliance and the NetSight server, other NAC appliances, and NAC assessment servers. It also provides secure communication for the NAC administrative web pages and with the assessment agent. The Internal Communications Server Certificate window lets you replace the server private key and server certificate. You can access this window from the [Manage Appliance Certificates window](#).

During installation, NetSight generates a unique private server key and server certificate for the Internal Communications server. While these provide secure communication, there may be cases where you want to update the Internal Communications server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which NAC must communicate. Additionally, you may want to use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access administrative web pages. For complete instructions on replacing and verifying the certificate, see [How to Update NAC Appliance Server Certificates](#).

After you have updated the certificate, you must enforce the appliance to deploy the new private key and server certificate. When enforced, the server's secure port 8444 will be offline for 15 seconds to reload the certificate. Additionally, if the Agent-Based Assessment Server Certificate is configured to use the Internal Certificate (in the [Manage Appliance Certificates window](#)), port 8443 will be offline for 15 seconds.

NOTE: Whenever the Internal Communications server certificate is changed, other NetSight components may be affected by the change and stop trusting the server. You can specify how other servers will handle updated certificates by configuring the server trust mode settings. Before updating the Internal Communications server certificate, be sure that the server trust modes are configured to trust the new certificate. For more information, see the Suite-Wide Tools Server Information Help topic Update Server Certificate Trust Mode Window.



Select the type of certificate replacement

You can select from two types of certificate replacement:

- **Generate a new unique private key and certificate.** This option allows you to automatically generate a new private key and certificate using the same method that is used when NAC is installed.
- **Provision a new private key and certificate from files.** This option lets you update the server certificate to a custom certificate provided from an external certificate authority. For complete instructions on replacing and verifying the certificate using this option, see [How to Update NAC Appliance Server Certificates](#).

Private Key

Provide a file containing the RSA or DSA private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field. If you do not have the private key, refer to the [instructions for generating](#) them.

Certificate Files

Use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

Related Information

For information on related windows:

- [How to Update NAC Appliance Server Certificates](#)
- [Manage Appliance Certificates Window](#)

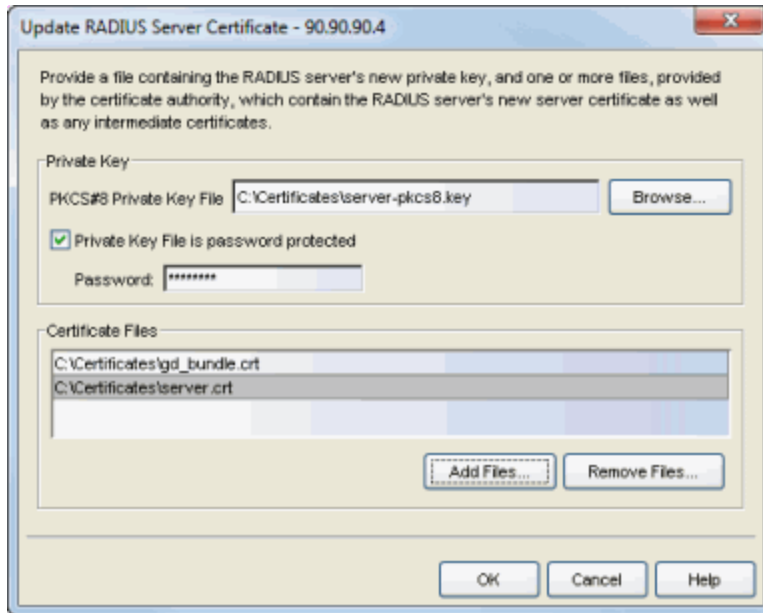
Update RADIUS Server Certificate Window

The RADIUS server certificate is the certificate sent to end-systems during certain forms of 802.1X authentication. If the appliance RADIUS server will proxy all 802.1X authentication requests, then certificates are not used. If the appliance RADIUS server can terminate 802.1X authentication requests, then certificates will be used if you are using EAP-TLS, PEAP, or EAP-TTLS authentication. The Update RADIUS Server Certificate window lets you replace the server certificate. You can access this window from the [Manage Appliance Certificates window](#).

During installation, NetSight generates a unique private key and server certificate for the NAC RADIUS server. This certificate provides basic functionality while you are configuring and testing your NAC deployment, but you will want to update to a certificate generated by a Certificate Authority that your connecting end-systems are already configured to trust. This allows you to integrate with the certificate structure you already have on your network. For complete instructions on replacing and verifying the certificate, see [How to Update NAC Appliance Server Certificates](#).

After you have updated the certificate, you must enforce the appliance to deploy the new private key and server certificate. When enforced, the RADIUS server on the appliance will be restarted automatically to load the new certificate.

In addition to updating the RADIUS server certificate, you will need to configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted. You can do this using the [Update AAA Trusted Certificate Authorities window](#) accessed from your [Advanced AAA Configuration](#) or the [Manage Appliance Certificates window](#).



Private Key

Provide a file containing the RSA or DSA private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field. If you do not have the private key, refer to the [instructions for generating](#) them.

Certificate Files

Use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

Related Information

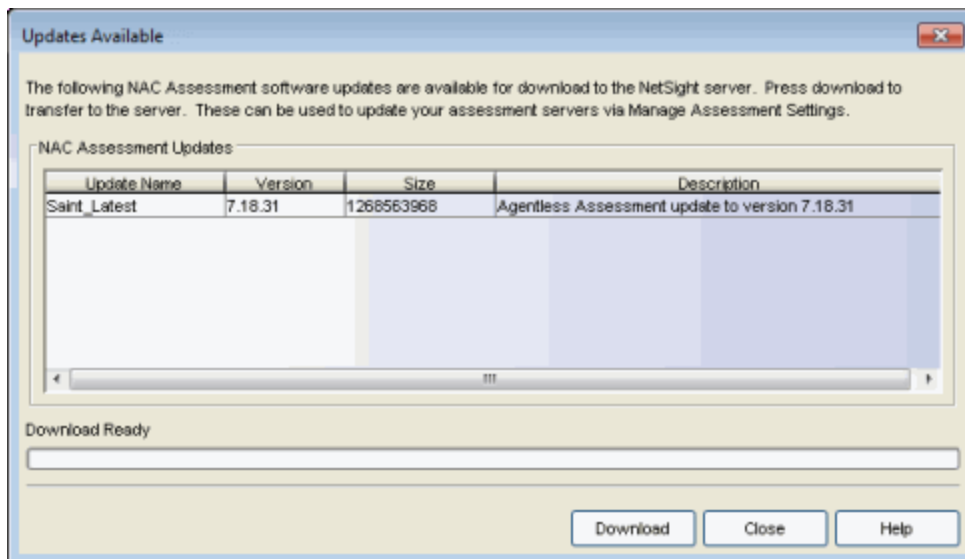
For information on related tasks:

- [How to Update NAC Appliance Server Certificates](#)
- [Manage Appliance Certificates Window](#)
- [Update AAA Trusted Certificate Authorities window](#)

Updates Available Window

This window lists any assessment software updates that are available for updating your on-board agent-less assessment servers in your NAC appliances. The download operation will download the software updates to the NetSight server, but will not perform the actual upgrade to the assessment server on the NAC appliance. The actual upgrade must be performed using the **Upgrade** button in the [Manage Assessment Settings window](#).

The window can be accessed from the **Help > Check for Assessment Updates** menu option or from the **Check for Updates** button in the [Manage Assessment Settings window](#) with the Assessment Servers tab selected.



Update Name

The name of the software update.

Version

The version number of the available update.

Size

The size of the update in bytes.

Description

A description of the software update.

Download Progress

A progress bar showing the percent completed of the download operation.

Download Button

Initiates the download operation. The download operation will download the software updates to the NetSight server, but will not perform the actual upgrade to the assessment server on the NAC appliance. The actual upgrade must be performed using the **Upgrade** button in the [Manage Assessment Settings window](#) with the Assessment Servers tab selected.

Related Information

- [Manage Assessment Settings Window](#)

Extreme Access Control (NAC) Deployment Guide

The Extreme Access Control Deployment Guide provides technical and administrative information for deploying, managing, and troubleshooting your Access Control deployment. The following topics are discussed:

- [Phased Rollout Strategy](#)
 - [Authentication Only](#)
 - [Assessment without Quarantine](#)
 - [Location-Based Assessment and/or Registration](#)
- [Important Links in Extreme Access Control and Extreme Management Center](#)
 - [Extreme Access Control Pages on the Extreme Management Center Server](#)
 - [Assessment/Remediation and Registration Pages on Extreme Access Control Appliances](#)
 - [Extreme Access Control Appliance Administration Web Pages](#)
- [MAC and IP Resolution](#)
 - [MAC to IP Resolution](#)
 - [IP to MAC Resolution](#)
- [Agent-Based Assessment](#)
 - [Configure OS-Based Test Cases](#)
 - [Exclude End-Systems from Assessment Using MAC OUIs](#)
- [Third-Party Device Considerations](#)
- [Extreme Management Center Server Data Retention Tools](#)
 - [Extreme Access Control Capacity Option](#)
 - [Data Persistence Options](#)
- [Troubleshooting](#)
 - [Extreme Access Control Appliance](#)
 - [Extreme Management Center Server](#)
 - [Extreme Management Center Server and Extreme Access Control Appliance Connectivity](#)

Phased Rollout Strategy

The Extreme Networks Access Control solution supports the five key network access control functions of detection, authentication, assessment, authorization, and remediation. These five Access Control functions do not need to be implemented concurrently in a Access Control deployment. Access Control can be rolled out in a phased deployment approach with each phase building on the knowledge gained along the way. A phased approach helps you to avoid wide-scale problems that can be associated with deploying all Access Control functionality at once throughout the network. It allows you to fix any underlying network, end-system, or user perception issues as they appear in each phase, making for a smooth deployment process.

A phased deployment:

- Allows full control over infrastructure changes during deployment.
- Minimizes impact to business processes.
- Initially deploys each function without enforcement and verifies results before enabling enforcement.

Following is a suggested rollout strategy that includes three phased Access Control deployments: Authentication Only, Assessment without Quarantine, and Location-Based Assessment and/or Registration.

Authentication Only

The first phase of the rollout strategy is called Authentication Only. In this phase, Access Control operates in a passive mode, providing you with information about who and what is connecting to the network, and when and where those connections are taking place. At this stage of the deployment, any end-system connecting to the network is authenticated and gets the basic access policy. Access Control is only detecting and tracking what is authenticating to your network; no access control decisions (apart from assigning the basic policy) are made. Then, as you come to understand what end-systems are connecting to the network, you can create Access Control Configuration rules that allow you to provide different access to specific end-systems.

This phase also allows you to work out the basic RADIUS configuration (if RADIUS authentication is being used), and gives you time to spread the end-system load across the Access Control appliances by moving switches from one appliance to another, as needed.

Assessment without Quarantine

The second phase of the rollout strategy is called Assessment without Quarantine. In this phase, Access Control is again operating in a passive mode, allowing you to understand the health of devices on the network without impacting end user connectivity. This is done by enabling assessment with all policies (including the Quarantine policy) set to full access -- no end users will be denied access based on assessment results. Then in NAC Manager, you can use the End-Systems tab to view each end-system's state to determine how many end-systems would lose network access with the configured assessment security level. In this way, you can roll out Access Control assessment, while avoiding problems that can result from a large number of end users suddenly being quarantined and unable to access the network because their patches or antivirus software aren't up-to-date. Once these issues are fixed, then assessment with quarantine can be enabled.

Location-Based Assessment and/or Registration

When deploying agent-based or agent-less assessment, a location-based rollout allows you to fix any problems as they appear for each location, making for a smoother deployment. It is also important to verify that end-systems can communicate with all Access Control appliances on the network, so that the assessment state can be maintained. In addition, Access Control appliances must also be able to communicate with each other. This is because when an end-system moves from one appliance to another (for example, the end user logs off in the dorm, then logs on in a classroom), Access Control has to be able to reconcile the connection and move the end-system from one appliance to another. You can test this by moving an end-system across the network and verifying that the agent stays connected.

For authenticated registration, a location-based rollout allows you to work out the LDAP configuration details prior to pushing out the configuration to the entire network. If an advanced LDAP configuration is used, it is important to test registration for users from different groups to verify that the LDAP rules are mapping the users to the correct group. Have an LDAP browser installed to aid in initial LDAP setup and rule creation.

Important Links in Extreme Access Control and Extreme Management Center

The following tables provide lists of URLs for accessing commonly used Extreme Access Control and Extreme Management Center web pages.

Access Control Pages on the Management Center Server

<p>Extreme Management Center Launch Page Opens the Management Center Launch Page where you can launch Management Center applications. From the Launch Page you can also access the Administration web page that provides specific server administration functions such as client and server diagnostics, server utilities, and Access Control Server diagnostics.</p>	<p><a href="http://<ManagementCenterServerIP>:8080">http://<ManagementCenterServerIP>:8080</p>
<p>Extreme Access Control Diagnostics on Extreme Management Center Launches the Access Control Server Administration web page that provides advanced diagnostic tools for Access Control. The page can also be accessed from the Management Center Launch page by clicking on the Administration tab and then the Access Control Server tab.</p>	<p><a href="http://<ManagementCenterServerIP>:8080/Clients/admin.jsp?tab=NAC">http://<ManagementCenterServerIP>:8080/Clients/admin.jsp?tab=NAC</p>
<p>Extreme Management Center Launches Management Center, providing access to web-based reporting, network analysis, troubleshooting, and helpdesk tools. Management Center includes wired/wireless dashboards, reports, Access Control Management information and control, interactive topology maps, web-based FlexViews, device views and event logs. Search functionality enables end-systems to be searched by MAC address, IP address, end-system name, or user name.</p>	<p><a href="https://<ManagementCenterServerIP>:8443/Monitor/jsp/reporting/reporting.jsp">https://<ManagementCenterServerIP>:8443/Monitor/jsp/reporting/reporting.jsp</p>
<p>Control T Launches the Control tab that displays a selection of reports providing an overview of end-system connection and assessment information. This page can also be launched from the Extreme Access Control Dashboard button on the NAC Manager toolbar.</p>	<p><a href="https://<ManagementCenterServerIP>:8443/Monitor/jsp/nac/IdentityAndAccess.jsp">https://<ManagementCenterServerIP>:8443/Monitor/jsp/nac/IdentityAndAccess.jsp</p>
<p>Extreme Management Center Online Help Launches searchable online help for all Management Center applications. The online help can also be launched from the Management Center Launch page Home tab and from the Help > Help Topics menu option in any Management Center application.</p>	<p><a href="http://<ManagementCenterServerIP>:8080/Clients/help">http://<ManagementCenterServerIP>:8080/Clients/help</p>

Assessment/Remediation and Registration Pages on Extreme Access Control Appliances

<p>Extreme Access Control Screen Preview The screen preview web page allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process. You can also access this web page using the Appliance Portal Pages > Preview Web Page button at the bottom of the Edit Portal Configuration window.</p>	<p><a href="https://<AccessControlApplianceIP>/screen_preview">https://<AccessControlApplianceIP>/screen_preview</p>
--	--

Important Links in Extreme Access Control and Extreme Management Center

Extreme Access Control Mobile Screen Preview The mobile screen preview web page allows you to preview the mobile version of the web pages that may be accessed by the end user during the assessment/remediation and registration process. You can also access this web page using the Appliance Portal Pages > Preview Web Page button at the bottom of the Edit Portal Configuration window.	<a href="https://<AccessControlApplianceIP>/mobile_screen_preview">https://<AccessControlApplianceIP>/mobile_screen_preview
Extreme Access Control Self-Registration Web Page The self-registration web page allows an authenticated and registered end user to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. Once the additional devices have been registered, the student can access the network using those devices.	<a href="https://<AccessControlApplianceIP>/self_registration">https://<AccessControlApplianceIP>/self_registration
Extreme Access Control Administration Page The administration web page lets administrators view registered devices and users, and manually add, delete, and modify users.	<a href="https://<AccessControlApplianceIP>/administration">https://<AccessControlApplianceIP>/administration
Extreme Access Control Sponsor Page The sponsor web page lets sponsors view registered devices and users, and manually add, delete, and modify users.	<a href="https://<AccessControlApplianceIP>/sponsor">https://<AccessControlApplianceIP>/sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	<a href="https://<AccessControlApplianceIP>/pre_registration">https://<AccessControlApplianceIP>/pre_registration
Agent Download Page The agent download page lets an end user download an agent regardless of the connection state of their end-system.	<a href="https://<AccessControlApplianceIP>/agent_download">https://<AccessControlApplianceIP>/agent_download (Displays only the agents applicable to the end user's operating system.) <a href="https://<AccessControlApplianceIP>/all_agent_download">https://<AccessControlApplianceIP>/all_agent_download (Displays all agents available for download.)

Extreme Access Control Appliance Administration Web Pages

Extreme Access Control Appliance Administration Web Page Displays appliance performance information including debugging information (such as CPU usage) that can help you determine if the appliance is being overloaded with requests.	<a href="https://<AccessControlApplianceIP>:8444/Admin/">https://<AccessControlApplianceIP>:8444/Admin/
Connected Agents Page Displays information about the agent-based clients connected to Access Control.	<a href="https://<AccessControlApplianceIP>:8444/Admin/status.jsp?tab=AGENTBASED-INFO">https://<AccessControlApplianceIP>:8444/Admin/status.jsp?tab=AGENTBASED-INFO
Downloads Page Displays links for downloading agents and the assessment agent adapter for agent-based assessment.	<a href="https://<AccessControlApplianceIP>:8444/Admin/downloads.jsp">https://<AccessControlApplianceIP>:8444/Admin/downloads.jsp
Connection Diagnostics Page Used to troubleshoot connection problems between the Access Control appliance and the Management Center Server.	<a href="https://<AccessControlApplianceIP>:8444/Admin/diagnostics.jsp?tab=COMMUNICATION-DIAGNOSTICS">https://<AccessControlApplianceIP>:8444/Admin/diagnostics.jsp?tab=COMMUNICATION-DIAGNOSTICS

MAC and IP Resolution

MAC to IP resolution is the process used by the Access Control L2 Controller and Access Control Gateway appliance to determine the IP address of an end-system from its MAC address. IP to MAC resolution is the process used by the Access Control L3 Controller to determine the MAC address of an end-system from its IP address. The following sections describe the MAC and IP resolution processes used by Extreme Access Control, and provide information for enabling diagnostic tools.

MAC to IP Resolution

Access Control L2 Controllers and Access Control Gateway appliances use MAC to IP resolution to determine an end-system's IP address from the MAC address that is learned from the RADIUS request used to authenticate the end-system. There are several reasons why MAC to IP resolution is critical to the Access Control process:

- The IP address is required for the end-system to be scanned with agent-less or agent-based assessment.
- The IP address is required for the Access Control Registration and Assessment/Remediation features. When the end user navigates to the Registration or Assessment/Remediation portal web page they are identified by the IP address found via the resolution process.
- The IP address also provides a way to identify an end-system in addition to its MAC address. This is useful when locating an end-system for blacklisting based on an Automated Security Manager (ASM) notification, which uses an IP address to specify what end-system to blacklist.

By default, Access Control is configured to always resolve the IP address for every end-system Access Control sees. If you have not deployed assessment, registration, and/or remediation on your network, you can disable MAC to IP Resolution by using the Advanced Configuration window (available from the Tools menu > Manage Advanced Configurations) and selecting Appliance Settings > IP Resolution Tab > Resolve IP Address Only for Assessment.

The MAC to IP Resolution Process

The MAC to IP Resolution process begins when an end-system authenticates to the network via a RADIUS request. From the RADIUS request, Access Control determines the end-system's MAC address by reading the Calling-Station-ID attribute. After determining what policy to assign to the end-system (Accept, Reject, or Scan), the MAC address to IP address resolution begins.

First, Access Control checks to see if there is a static MAC to IP address mapping defined in NAC Manager for the end-system's MAC address. If there is, then that IP address is used. If there is not, then the IP resolution process starts trying to resolve the IP address using IP discovery on the network access switch (NAS).

NOTES: NAC Manager provides a delay that allows the DHCP process to be completed prior to beginning the IP resolution process. You can configure the length of the delay via **Appliance Settings > IP Resolution Tab > DHCP Resolution Delay Time** option. The default delay time is 10 seconds.

In order for NAC to resolve IP addresses from the ipNetToMedia table on ExtremeXOS devices, each VLAN that an authenticated end-system could belong to needs to have an IP address assigned in order for IP's from that VLAN to populate in that table.

IP Discovery on Network Access Switch

Access Control makes SNMP requests for the IP information to the network access switch (NAS) that sent the RADIUS authentication request for the end-system. There are five supported MIBs that Access Control can read for the IP address information, depending on what MIBs the switch supports:

- ctAliasMacAddressTable - This MIB table contains IP address information for end-systems, indexed by MAC address.
- ctAliasTable - This MIB table is used only if the ctAliasMacAddressTable is not supported by the switch.
- CiscoDHCP Snooping - This MIB table is used for Cisco devices that are running the appropriate firmware.
- ipNetToMedia - This MIB table is used for third-party switches and for ExtremeWireless Controllers.
- ipNetToPhysical - This MIB table supports IPv6 addresses and is the IPv6 replacement for the ipNetToMedia table.

Following the SNMP requests, Access Control evaluates the IP addresses that it discovered. First, Access Control filters out any IP addresses that are invalid, such as 0.0.0.0. If there is only one IP address remaining, then this address is used and the process stops here. If there are no IP addresses remaining, Access Control proceeds to the [router IP discovery process](#). If there are multiple IP addresses, then Access Control goes to the next step in the filtering process, VLAN IP Subnet Filtering.

If VLANs are being used for access control, Access Control looks up the IP subnet for the VLAN that the end-system is in. IP subnets can be defined for each VLAN to provide an IP range filter, which can be used to filter the list of IPs discovered on the switch. IP subnets are defined in NAC Manager under the Appliance Settings > IP Resolution Tab. If no IP subnet is found, Access Control proceeds to the router IP discovery process. If a subnet is found and filters down to one IP address, then that address is used and the process stops here. If the filter results contain no IP addresses, then Access Control proceeds to the router IP discovery process. If there are multiple IP addresses, then Access Control goes to the next step in the filtering process, NetBIOS IP Filtering.

Access Control makes NetBIOS requests to the list of IP addresses to determine the correct IP address. If the NetBIOS requests filter the list down to one IP address, then that IP address is used and the process stops here. If there are no IP addresses remaining, then Access Control proceeds to the router IP discovery process. If there are multiple IP addresses, then Access Control goes to the next step in the filtering process, Clear Duplicate IPs.

NOTE: If a firewall is enabled on the end-systems, disable the NetBIOS IP Filtering feature in NAC Manager via the Appliance Settings > IP Resolution Tab and the NetBIOS Hostname Resolution feature should be disabled via the Appliance Settings > Hostname/Username Resolution tab. The NetBIOS timing options can be controlled from Appliance Settings > Miscellaneous Tab > NetBIOS.

Access Control clears the duplicate IPs from the network access switch to which the end-system authenticated, and then tries to re-read the IP address from the switch to find the most recent entry. The only filtering done at this point is removing invalid IP addresses and VLAN IP Subnet Filtering. If only one IP address is read this time, then that IP address is used and the process stops here. If no IP addresses are read, then Access Control proceeds to the router IP discovery process. If there are multiple IP addresses, then Access Control looks to see if one IP address is the last one heard with DHCP, and if the DHCP information can be used. If so, then that IP address is used and the process stops here.

NOTES: The Clear Duplicate IPs process can be disabled in NAC Manager via the Appliance Settings > IP Resolution Tab > Clear Duplicate IPs on Switches.

You can disable the use of DHCP Request IPs from Appliance Settings > IP Resolution Tab > Use DHCP Request IPs. By default this option only allows IPs learned from DHCP requests to be used in non-VLAN environments. This is because as an end-system transitions through VLANs, it will request the IP address of the previous VLAN making it inaccurate for Access Control to use.

IP Discovery on Router

If the Access Control appliance was unable to resolve the end-system's IP address by querying the network access switch, Access Control makes SNMP requests to an end-system's gateway router ARP table to try to resolve the IP address. Access Control determines the router IP address by one of two mechanisms. If VLANs are being used for access control, Access Control looks up the IP subnet for the VLAN that the end-system is in. IP subnets are defined in NAC Manager in the Appliance Settings > IP Resolution Tab. If no IP subnet is found, Access Control will look for the last relay router heard for that end-system from any DHCP data. The router IP discovery process can be disabled via the Appliance Settings > IP Resolution Tab > Router IP Discovery option.

There are four supported MIBs that Access Control can read for the IP address information, depending on what MIBs the router supports:

- ipAddrTable - This MIB table is used to find the ifIndex for the IP address of the router in order to reduce the number of reads that need to be made against the ipNetToMedia or ipNetToPhysical MIB tables.
- ipAddressTable - This MIB table supports IPv6 addresses and is the IPv6 replacement for the ipAddrTable table.
- ipNetToMedia - This MIB table is used to locate the IP to MAC bindings.
- ipNetToPhysical - This MIB table supports IPv6 addresses and is the IPv6 replacement for the ipNetToMedia table.

Following the SNMP request, Access Control evaluates the IP addresses it discovered. First, Access Control filters out any invalid IP addresses, such as 0.0.0.0. If there is only one IP address remaining, then this address is used and the process stops here. If there are no IP addresses remaining, Access Control proceeds to the [DHCP IP address process](#). If there are multiple IP addresses, then Access Control goes to the next step in the filter process, router IP subnet filtering.

If an IP subnet is defined with the relay router's IP as one of the gateways, then that subnet can be used to provide a filter. IP subnets are defined in NAC Manager in the Appliance Settings > IP Resolution Tab. If no IP subnet is found, Access Control proceeds to the DHCP IP address process. If a subnet is found and filters down to one IP address, then that address is used and the process stops here. If results after the filter contain no IP addresses, then Access Control proceeds to the DHCP IP address process. If there are multiple IP addresses, then Access Control goes to the next step in the filtering process, the NetBIOS filter.

Access Control makes NetBIOS requests to the list of IP addresses to determine the correct IP address. If the NetBIOS filters down to one IP address, then that IP address is used and the process stops here. If the filter results contain no IP addresses, then Access Control proceeds to the DHCP IP address process. If there are multiple IP addresses, then Access Control goes to the next step in the filtering process, Clear Duplicate IPs.

NOTE: If a firewall is enabled on the end-systems, enable the NetBIOS IP Filtering feature in NAC Manager via the Appliance Settings > IP Resolution Tab and the NetBIOS Hostname Resolution feature should be disabled via the Appliance Settings > Hostname/Username Resolution tab. The NetBIOS timing options can be controlled from Appliance Settings > Miscellaneous > NetBIOS.

Access Control clears the duplicate IPs in the ARP tables of an end-system's gateway router and then try to re-read the IP address from the router to find the most recent entry. The only filtering done at this point is removing invalid IP addresses and VLAN IP Subnet Filtering. If only one IP address is read this time, then that IP address is used and the process stops here. If no IP addresses are read, then Access Control proceeds to the DHCP IP address process. If the results contain multiple IP addresses, then Access Control looks to see if one IP address is the last one heard with DHCP, and if the DHCP information can be used. If so, then that IP address is used and the process stops here.

NOTES: The Clear Duplicate IPs process can be disabled in NAC Manager via the Appliance Settings > IP Resolution Tab > Clear Duplicate IPs on Routers.

You can disable the use of DHCP Request IPs from Appliance Settings > IP Resolution Tab > Use DHCP Request IPs. By default this option only allows IPs learned from DHCP requests to be used in non-VLAN environments. This is because as an end-system transitions through VLANs, it will request the IP address of the previous VLAN making it inaccurate for Access Control to use.

Agent IP Discovery

If the Access Control appliance was unable to resolve the end-system's IP address by querying the end-system's gateway router ARP table, then Access Control can use an IP address reported by a connected agent. This process looks for the end-system's MAC address in the list of MAC addresses from known connected agents. If an agent is connected and heartbeats during the IP Resolution process, then Access Control uses the IP address of that agent.

DHCP IP Address

If the IP address resolution process has still not obtained an IP address, then Access Control uses a DHCP address, if one was heard and was deemed usable. Access Control uses it even though it could not be verified. You can disable the use of DHCP Request IPs in Appliance Settings > IP Resolution Tab > Use DHCP Request IPs. By default, this option only allows IPs learned from DHCP requests to be used in non-VLAN environments. This is because the IP addresses from request packets in a VLAN environment is always incorrect, because as an end-system transitions through VLANs, it always requests the IP from the previous VLAN.

If IP Resolution Fails

If Access Control is unable to resolve an IP address and assessment is enabled, the end-system is assigned the Error connection state, and its extended state is set to "MAC To IP Resolution Failed." If the IP resolution process takes more time than allowed by the IP Address Resolution Timeout setting, the end-system's extended state is set to "MAC to IP Resolution Timed Out." (The default timeout setting is 60 seconds and can be changed in Appliance Settings > IP Resolution Tab > IP Address Resolution Timeout.) When IP address resolution fails:

- Access Control is unable to apply rules that use IP-based end-system groups to this end-system.
- Access Control is unable to resolve the hostname, and is therefore be unable to apply rules using hostname-based end-system groups to this end-system.
- The Failsafe policy is applied to the end-system, if assessment is enabled.
- Assessment of the end-system (agent-less or agent-based) does not take place.
- The end-system is not be able to see the Registration web page.
- The end-system is not be able to see the Assessment/Remediation web page.

Deployment Considerations

The following Node/Alias configuration changes may increase the accuracy of IP resolution:

- Turn off learning on uplink ports.
- Increase the maximum number of entries per port for all downstream ports to the maximum, so that entries are timed out on a oldest per-switch basis instead of oldest per-port.

Diagnostics for IP Resolution

You can enable diagnostics for IP Resolution by going to the Access Control appliance administration web page and enabling diagnostic groups that provides troubleshooting information. Launch the Access Control appliance administration web page by right-clicking on the Access Control appliance in the NAC Manager left-panel tree and selecting WebView or by using the following URL: <https://<Access ControlApplianceIP>:8444/Admin>. The default user name and password for access to this web page is "admin/Extreme@pp." Expand the Diagnostics folder in the left-panel tree and click on the Appliance/Server Diagnostics page.

Debug Group	Definition
IP Address Resolution	<p>This group enables debugging for the core IP address resolution logic. There are three useful diagnostic levels that can be used:</p> <p>Informational - Enables high-level diagnostics to determine what methods of detection are being used, including device information.</p> <p>Verbose - Provides the same information as Informational, as well as enabling detailed logging that also specifies information such as what OIDs were read and the results of those reads. Note that this verbose mode is likely to incur a performance hit.</p> <p>Warning - Can be used to determine why failures occurred. For every IP Address Resolution Failed event, a verbose message will be printed out describing the entire process used and why the resolution ultimately failed. Note that running in this mode will incur the same performance hit that Verbose mode takes, but it will make the logs easier to read. This mode cannot be used for timeouts or errors where Access Control determines the incorrect IP.</p>
DHCP	This group enables DHCP snooping diagnostics that describe what data is coming in from snooped DHCP packets.

Debug Group	Definition
NetBIOS	This group enables diagnostics for the core NetBIOS interaction with end-systems. This does not control the diagnostics on the timeout mechanism.
NetBIOS Timeout	This group enables diagnostics for the NetBIOS timeout logic. Note that this logging can be very verbose and is likely to incur a performance hit.

The log output is saved in /var/log/tag.log on the Access Control appliance.

Debug diagnostic log data indicating a failure in the IP Resolution process is shown below.

```

2012-07-19 16:58:10,011 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C Requesting resolve of IP: 00-18-8B-D6-E6-0C
2012-07-19 16:58:10,011 INFO [ResolveIpAddress] ESDMAC:D6-E6-0C Starting IP Resolution for EndSystem: 00-18-8B-D6-E6-0C
2012-07-19 16:58:10,011 INFO [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Starting CtAliasMacAddressTable IP resolution for: 00-18-8B-D6-E6-0C on switch:
10.20.80.126 and ifIndex: 17
2012-07-19 16:58:10,012 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Starting to read from: 1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12
2012-07-19 16:58:10,020 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Testing OID:
1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12.1.4.10.20.87.200.3304, interface: 18 == 17
2012-07-19 16:58:10,020 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Testing OID:
1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12.1.4.10.20.87.200.3305, interface: 18 == 17
2012-07-19 16:58:10,020 INFO [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Discovered IP List (0): null
2012-07-19 16:58:10,020 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C Switch SNMP request returned 'no' IPs.
2012-07-19 16:58:10,020 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C Not using Agent Based IP under any circumstances, skipping...
2012-07-19 16:58:10,020 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C Agent Discovery is disabled for IP resolution, skipping.
2012-07-19 16:58:10,020 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C The DHCP entry IP: null is invalid, skipping...

```

Debug diagnostic log data indicating a successful IP Resolution is shown below.

```

2012-07-19 17:05:36,049 DEBUG [ResolveIpAddress] ESDMAC:D6-E6-0C Requesting resolve of IP: 00-18-8B-D6-E6-0C
2012-07-19 17:05:36,049 INFO [ResolveIpAddress] ESDMAC:D6-E6-0C Starting IP Resolution for EndSystem: 00-18-8B-D6-E6-0C
2012-07-19 17:05:36,049 INFO [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Starting CtAliasMacAddressTable IP resolution for: 00-18-8B-D6-E6-0C on switch: 10.20.80.126 and
ifIndex: 17
2012-07-19 17:05:36,049 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Starting to read from: 1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12
2012-07-19 17:05:36,056 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Testing OID: 1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12.1.4.10.20.87.200.3304, interface: 18
== 17
2012-07-19 17:05:36,056 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Testing OID: 1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12.1.4.10.20.87.200.3305, interface: 18
== 17
2012-07-19 17:05:36,056 DEBUG [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Testing OID: 1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1.0.24.139.214.230.12.1.4.10.20.87.200.3600, interface: 17
== 17
2012-07-19 17:05:36,056 INFO [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C,ESDIP:10.20.87.200 Discovered IP Address: 10.20.87.200
2012-07-19 17:05:36,056 INFO [CtAliasMacAddressIpResolutionSnmpWorker] ESDMAC:D6-E6-0C Discovered IP List (1): IpAddressCollection [ipv4Addresses=[10.20.87.200], ipv6Addresses=null]

```

IP to MAC Resolution

Access Control L3 Controllers use IP to MAC resolution to determine an end-system's MAC address after traffic from a new source IP address is detected on the controller. NAC Manager must know the end-system's MAC address in order to track the end-system through the Access Control process.

The IP to MAC Resolution Process

The IP to MAC Resolution process begins when an end-system authenticates to the network via a packet containing the end-system's IP address that crosses the Access Control L3 Controller.

First, Access Control checks to see if there is a static MAC to IP address mapping defined in NAC Manager for the end-system's IP address. If there is, then that MAC address is used. If there is not, then the MAC resolution process will make NetBIOS requests to the end-system's IP address.

NOTE: Static MAC resolution can be disabled in NAC Manager via the Appliance Settings > MAC Resolution Tab > Static MAC Resolution.

The NetBIOS request is made asynchronously, and until a MAC address is determined, all traffic from this end-system is dropped by the controller. If a valid response comes back, the MAC address is used if it is not one of the unusable MAC addresses defined under the Appliance Settings > MAC Resolution Tab > Unusable MAC Addresses section. If the MAC address is not valid, then Access Control proceeds to the DHCP MAC Resolution process.

NOTE: The NetBIOS request can be disabled in NAC Manager via the Appliance Settings > MAC Resolution Tab > NetBIOS MAC Resolution option. The NetBIOS timing options can be controlled from Appliance Settings > Miscellaneous Tab > NetBIOS.

If Access Control is able to snoop a DHCP packet for the end-system's IP address, it uses the data from that packet to obtain the MAC address. If no DHCP information is available for that IP address, then Access Control proceeds to NetBIOS Hostname Pseudo MAC Generation.

NOTE: The DHCP MAC Resolution process can be disabled in NAC Manager via the Appliance Settings > MAC Resolution Tab > DHCP MAC Resolution option.

If a NetBIOS response was heard, but the MAC address was deemed to be unusable, Access Control looks for the hostname within the NetBIOS response. If there is one, a pseudo MAC address is generated starting with the prefix of AB:CD. The last four octets are generated by the hostname and are guaranteed to be unique on each Access Control Controller. However, there is the possibility that two end-systems with different names on different controllers could end up with the same pseudo MAC address. Because of this possibility, this option is disabled by default, but can be enabled in NAC Manager via Appliance Settings

> MAC Resolution Tab > NetBIOS MAC Resolution > Allow Use of NetBIOS Hostname for Pseudo MAC Generation option.

If Access Control is unable to determine the MAC address through any of the processes described above, Access Control generates a pseudo MAC address from the IP address of the end-system. This method always generates the same MAC address, and it is more likely to generate an address that uniquely identifies the end-system if IP addresses are statically mapped to end-systems. Because a MAC address is required by Access Control to identify and track an end-system, there is no way to disable this final method.

Diagnostics for MAC Resolution

You can enable diagnostics for MAC Resolution by going to the Access Control appliance administration web page and enabling diagnostic groups that help with troubleshooting. Launch the Access Control Appliance administration web page by right-clicking on the Access Control appliance in the NAC Manager left-panel tree and selecting WebView or by using the following URL: <https://<Access ControlApplianceIP>:8444/Admin>. The default user name and password for access to this web page is "admin/Extreme@pp." Expand the Diagnostics folder in the left-panel tree and click on the Appliance/Server Diagnostics page.

Debug Group	Definition
MAC Address Resolution	<p>This group enables debugging for the core MAC address resolution logic. There are three useful diagnostic levels that can be used:</p> <p>Informational - Enables high-level diagnostics to determine what methods of detection are being used, including device information.</p> <p>Verbose - Provides the same information as Informational, as well as enabling detailed logging. Note that this verbose mode is likely to incur a performance hit.</p> <p>Warning - Can be used to determine why failures occurred. Whenever MAC resolution fails and Extreme Access Control generates a pseudo MAC address, a verbose message will be printed out describing the entire process used and why the resolution failed. Note that running in this mode will incur the same performance hit that Verbose mode takes, but it will make the logs easier to read.</p>
DHCP	<p>This group enables DHCP snooping diagnostics that describe what data is coming in from snooped DHCP packets.</p>

Debug Group	Definition
NetBIOS	This group enables diagnostics for the core NetBIOS interaction with end-systems. This does not control the diagnostics on the timeout mechanism.
NetBIOS Timeout	This group enables diagnostics for the NetBIOS timeout logic. Note that this logging can be very verbose and is likely to incur a performance hit.

Agent-Based Assessment

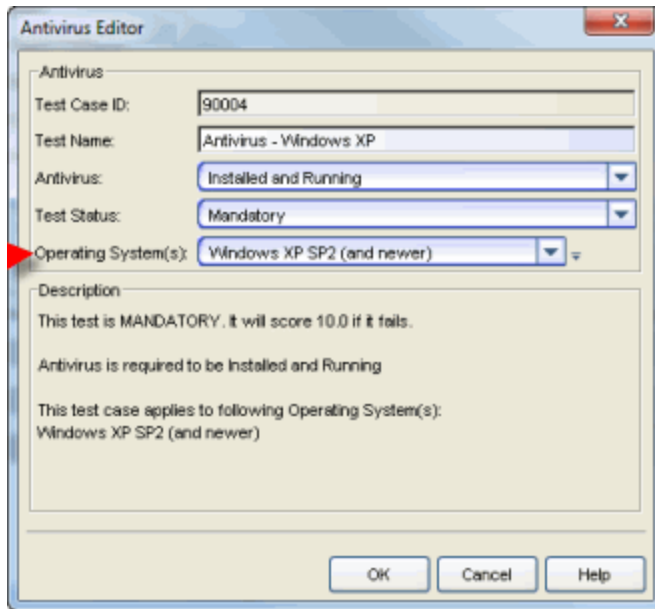
This section provides strategies on how to set up your Extreme Access Control assessment to take advantage of certain Extreme Access Control features. It includes information on how to configure assessment test cases based on the end-system's operating system, and how to use MAC OUIs to exclude end-systems such as printers and phones from assessment.

NOTE: Before configuring assessment, you must enable the Assessment/Remediation for End-Systems option in the NAC Manager Features options accessed from Tools > Options in the NAC Manager menu bar.

Configure OS-Based Test Cases

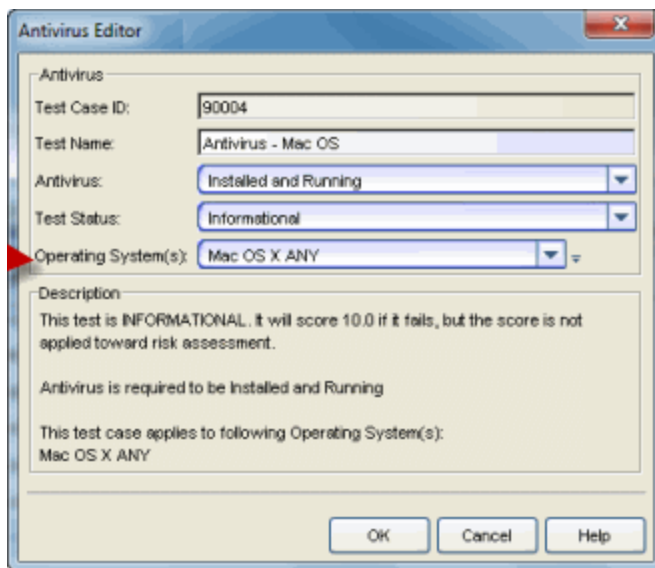
Agent-based test sets can be configured to include individual test cases that apply only to end-systems running certain operating systems. Here are three examples of how this functionality could be used:

- **Create different versions of the same test case based on the different operating systems.** For example, create a Mandatory test that requires antivirus software to be installed and running on Windows XP end-systems (as shown below). The end-system must pass the test, or it will be scored against them.



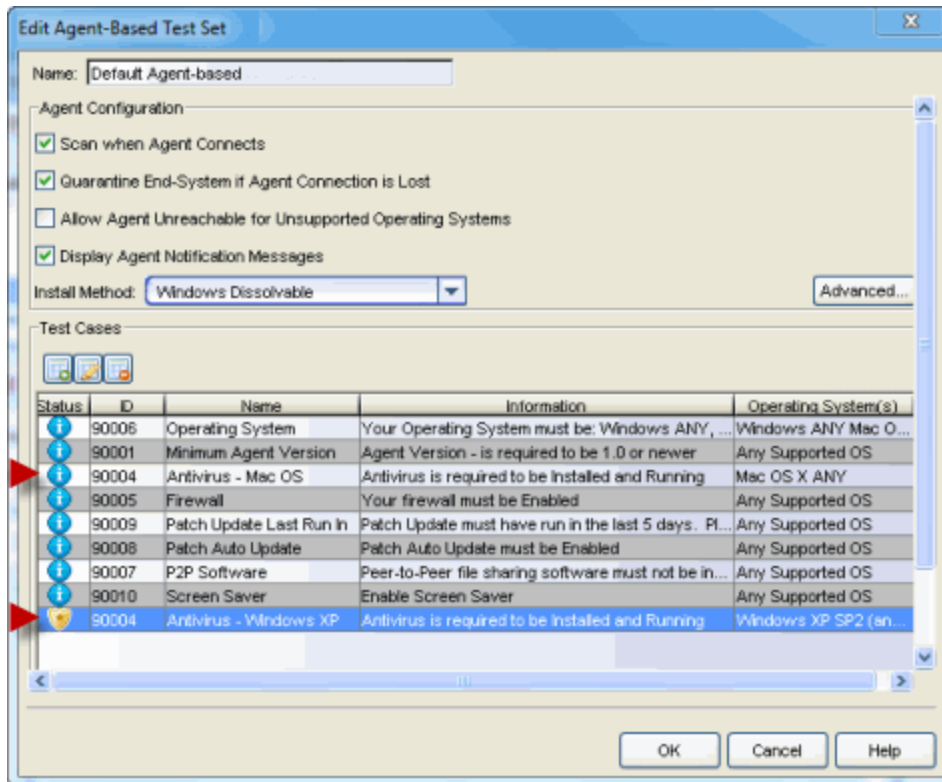
The screenshot shows the 'Antivirus Editor' dialog box. The 'Antivirus' section contains the following fields: 'Test Case ID' with the value '90004', 'Test Name' with 'Antivirus - Windows XP', 'Antivirus' set to 'Installed and Running', and 'Test Status' set to 'Mandatory'. The 'Operating System(s)' dropdown is set to 'Windows XP SP2 (and newer)'. The 'Description' text area contains: 'This test is MANDATORY. It will score 10.0 if it fails.', 'Antivirus is required to be Installed and Running', and 'This test case applies to following Operating System(s): Windows XP SP2 (and newer)'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Then, create a Warning or Informational test for Mac end-systems that checks for antivirus software and reports the results without any score being applied towards risk assessment (as shown below).

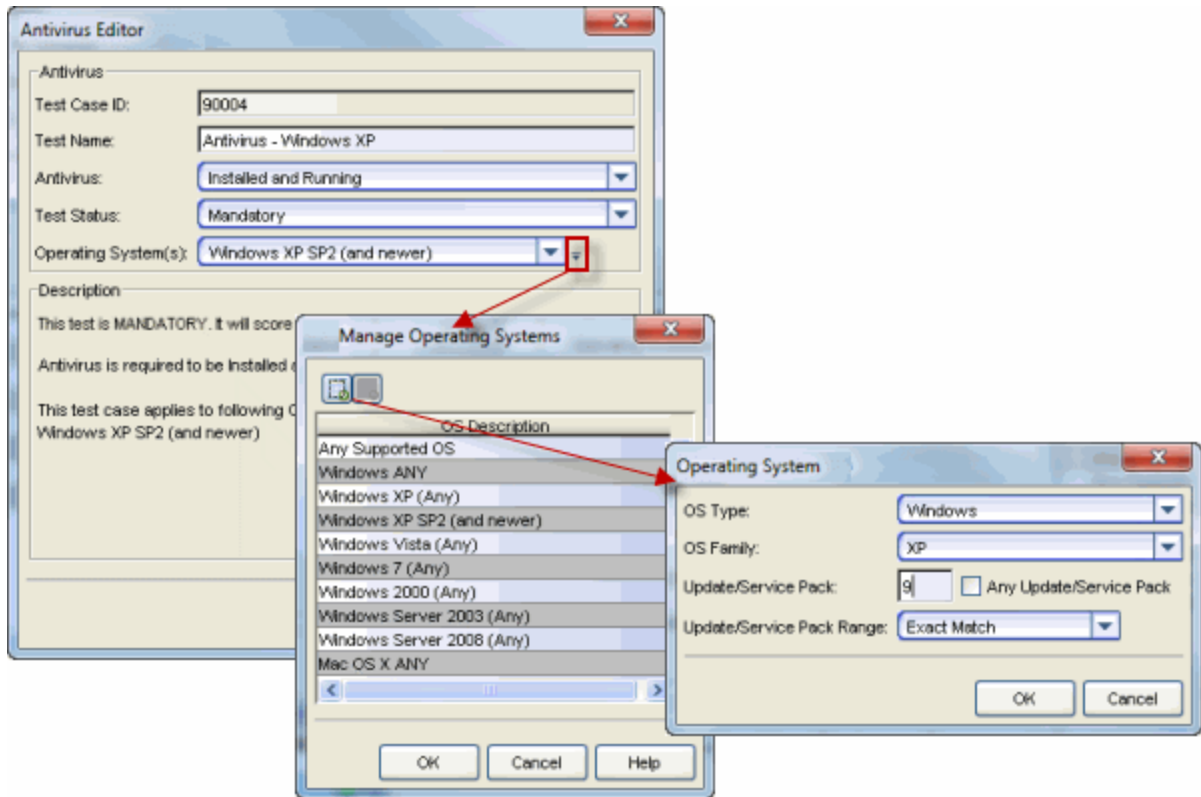


The screenshot shows the 'Antivirus Editor' dialog box for a Mac OS test case. The 'Antivirus' section contains: 'Test Case ID' with '90004', 'Test Name' with 'Antivirus - Mac OS', 'Antivirus' set to 'Installed and Running', and 'Test Status' set to 'Informational'. The 'Operating System(s)' dropdown is set to 'Mac OS X ANY'. The 'Description' text area contains: 'This test is INFORMATIONAL. It will score 10.0 if it fails, but the score is not applied toward risk assessment.', 'Antivirus is required to be Installed and Running', and 'This test case applies to following Operating System(s): Mac OS X ANY'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

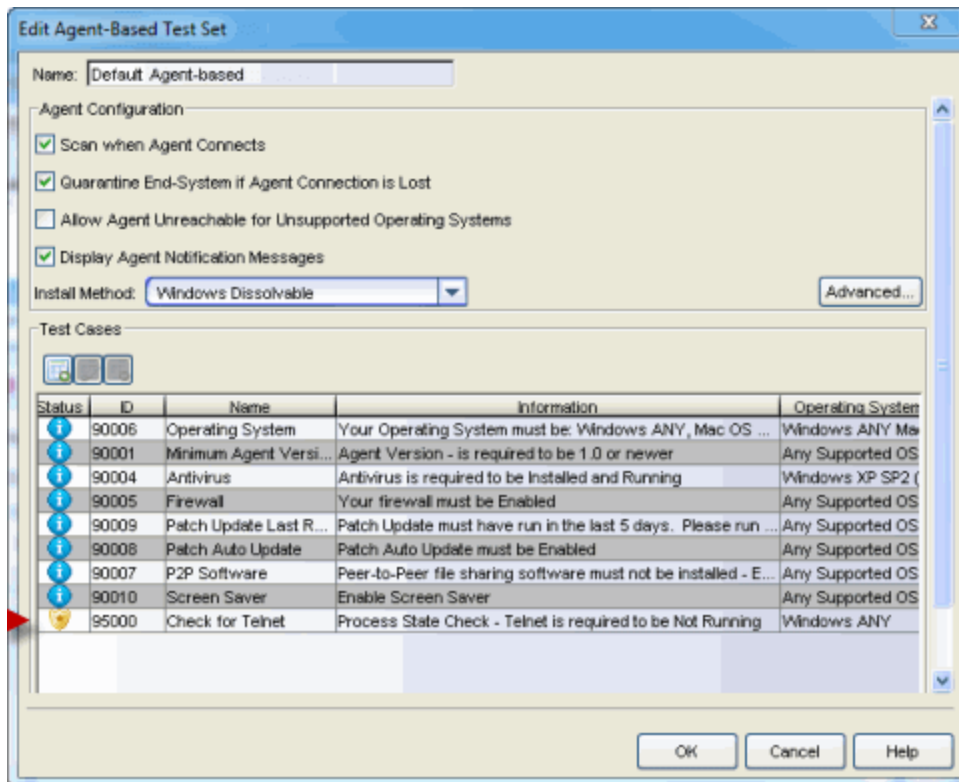
The Agent-Based Test Set shown below lists the two test cases: Antivirus - Windows XP and Antivirus - Mac OS.



- **Create tests that take into account operating system versions.** This allows you to create a test case where end-systems running an older version of the operating system must be tested while end-systems with newer versions are not tested. For example, if Microsoft released a new service pack that was incompatible with a certain agent-based test, the test could be disabled for that new service pack. To do this, you can define a new operating system definition for the new service pack using the Manage Operating Systems window accessed from the Operating System(s) configuration menu button in the test Editor window (as shown below).



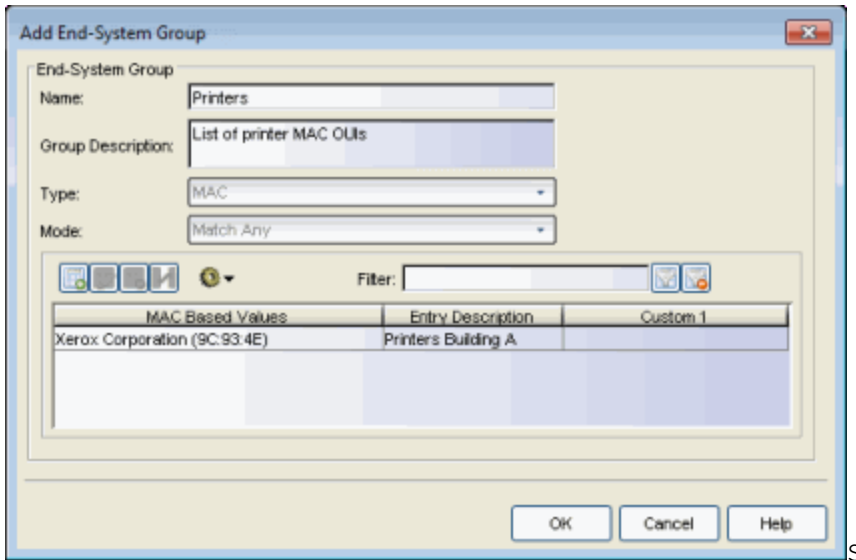
- Create a test case that checks for a specific process on a specific operating system. For example, you could create a test that checks for Telnet installed on any Windows end-system, while Mac end-systems would not be checked. The Agent-Based Test Set shown below shows an example of a Check for Telnet test case.



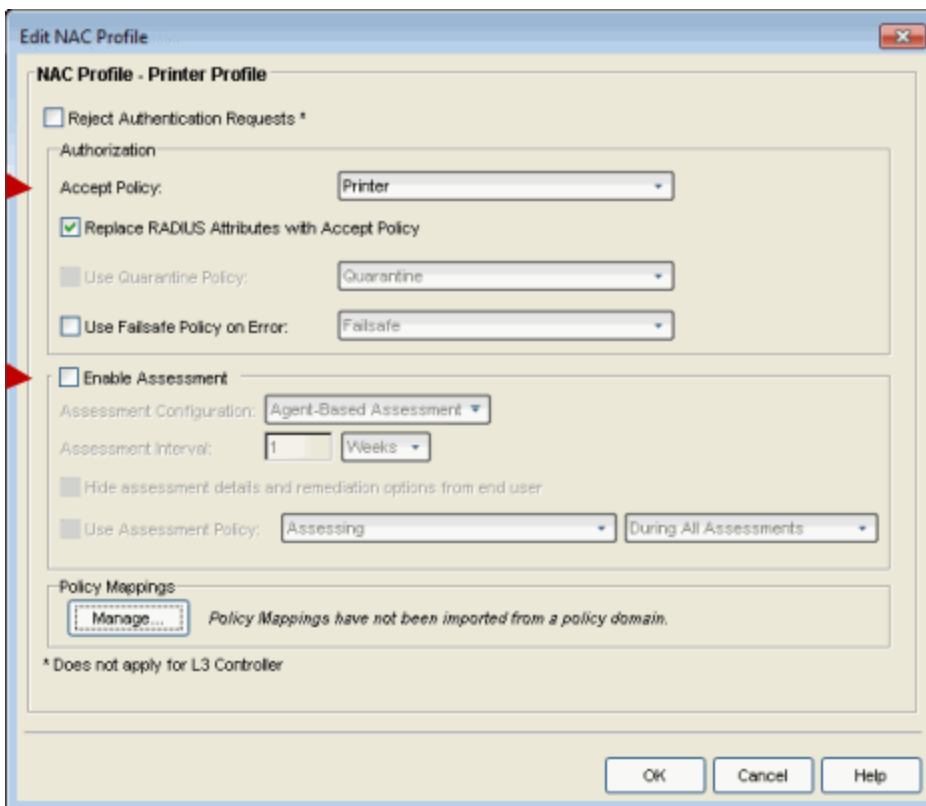
Exclude End-Systems from Assessment Using MAC OUIs

If you have assessment enabled on your network, you can use Extreme Access Control Configuration rules and MAC OUI end-system groups to exclude specific end-systems such as printers and phones from being assessed. Here are the steps you would use to create a printer end-system group and rule for your Extreme Access Control Configuration:

1. Create an end-system group for your printers selecting a MAC OUI as your end-system type.



2. Create a printer profile that specifies a Printer Accept Policy and does not enable assessment. (Use the Manage Policies button at the bottom of the Edit Extreme Access Control (NAC) Profile window to open the Edit Policy Mapping window if you need to define a Printer Accept Policy.)



3. Add a new rule to your Extreme Access Control (NAC) Configuration that uses the Printers end-system group and Printer Profile.

The screenshot shows a 'Create Rule' dialog box with the following configuration:

- Name: Printer
- Authentication Method: Any (Invert checkbox is unchecked)
- User Group: Any (Invert checkbox is unchecked)
- End-System Group: Printers (Invert checkbox is unchecked)
- Device Type Group: Any (Invert checkbox is unchecked)
- Location Group: Any (Invert checkbox is unchecked)
- Time Group: Any (Invert checkbox is unchecked)
- Zone: None
- Profile: Printer Profile
- Portal: Default
- Rule Enabled

Buttons: OK, Cancel, Help

4. Your Extreme Access Control Configuration now includes a Printer rule based on a MAC OUI. Any end-system connecting to the network that matches the MAC OUI will be assigned to the Printers end-system group and receive the Printer Profile. That end-system is not assessed.

An ordered list of Rules used to select a NAC Profile for an end-system based on its criteria.

Enabled	Rule Name	Conditions	Actions
✓	Lab BlackList	End-System is in Blacklist	Profile: Quarantine NAC Profile Accept Policy: Quarantine Portal: NetSight-NAC Lab Portal Configuration User will be redirected to the Blacklist notification web p...
✓	Assessment Warning	End-System is in Assessment Warning	Profile: Notification NAC Profile Accept Policy: Notification Portal: NetSight-NAC Lab Portal Configuration User will be redirected to the remediation assessment ...
✓	Switch Administrators	Authentication is Management Login and User is in NetSight-NAC Switch Admin Users	Profile: Switch Administrator Profile Accept Policy: Enterprise User (Administrator)
✓	Phone	End-System is in Phones	Profile: Phone Profile Accept Policy: Phone
✓	Printer	End-System is in Printers	Profile: Printer Profile Accept Policy: Printer
✓	802.1x NAC2003 Employees	Authentication is 802.1X and User is in NAC2003 Users	Profile: Employee Profile Accept Policy: Employee Assessment Policy: Employee Quarantine Policy: Quarantine Portal: NetSight-NAC Lab Portal Configuration User will be redirected to the remediation violations web...
✓	802.1x DEVLAB Employees	Authentication is 802.1X and User is in DEVLAB Users	Profile: Employee Profile Accept Policy: Employee Assessment Policy: Employee Quarantine Policy: Quarantine Portal: NetSight-NAC Lab Portal Configuration User will be redirected to the remediation violations web...
✓	802.1x End-System Authenti...	Authentication is 802.1X and User is in End-System Authentications	Profile: Logged Off Secure End-System Profile Accept Policy: Secure EndSystem
✓	Contractors	End-System is in Contractor End-Systems	Profile: Contractor Profile Accept Policy: Contractor Assessment Policy: Employee Quarantine Policy: Quarantine

Third-Party Device Considerations

This section provides information on deploying Extreme Access Control with third-party devices.

RADIUS Configuration

RADIUS configuration on third-party devices must be performed manually, outside of NAC Manager.

RADIUS Attributes

For third-party devices that support RFC 3580, NAC Manager access policies are by default associated to VLAN ID assignment based on RFC 3580 tunnel attributes. NAC Manager also allows you to define custom RADIUS attributes (such as vendor-specific ACL-based attributes) which are included as part of the RADIUS response.

Reauthentication

For third-party wireless devices (such as Cisco Wireless devices), reauthentication is accomplished using RFC 3576. For third-party wired switches, reauthentication is accomplished via dot1x MIB (standards), HP User Auth MIB, or by linking down the port.

IP Resolution

Third-party devices must have the ipNetToMedia MIB for Extreme Access Control to be able to perform IP resolution. Extreme Access Control also uses the Cisco DHCP Snooping MIB for Cisco devices.

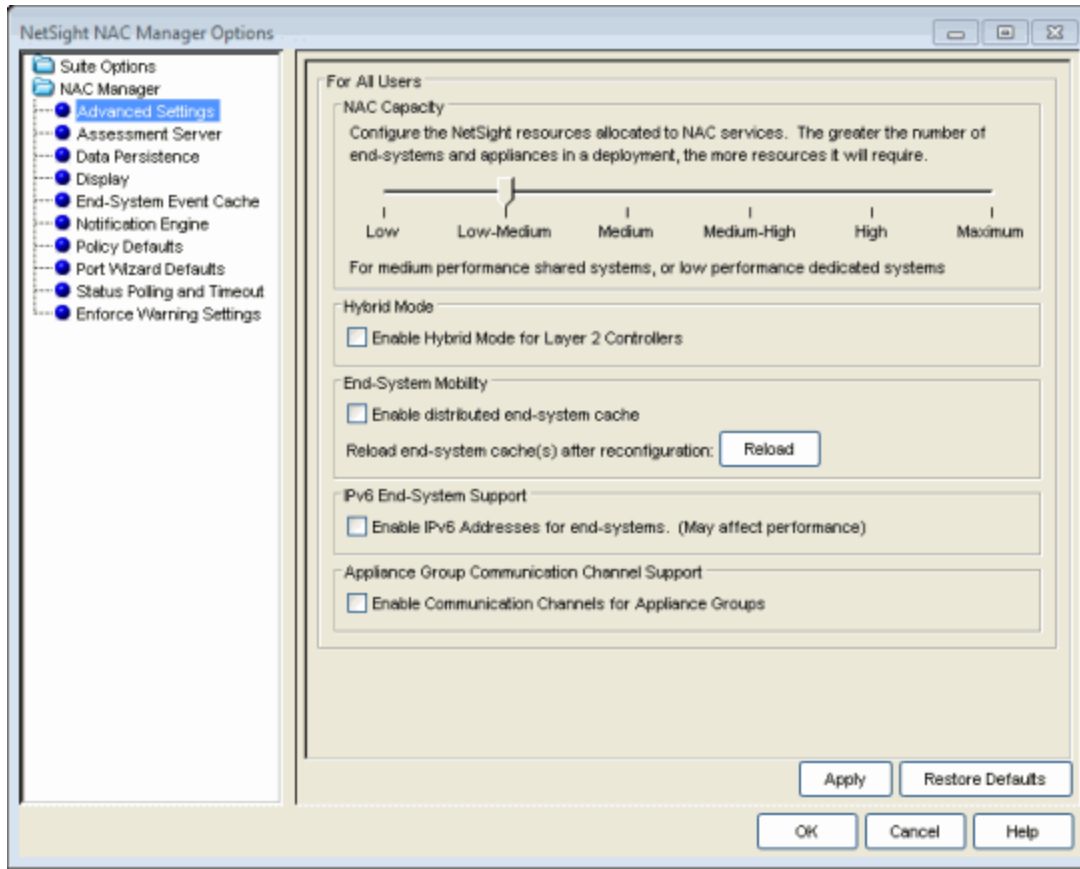
Extreme Management Center Server Data Retention Tools

There are several NAC Manager options that allow you to configure the amount of data retained in the Extreme Management Center Server database. To access these options, select Tools > Options from the NAC Manager menu bar. In the NAC Manager Options window, expand the NAC Manager folder in the left-panel tree to see the options.

Extreme Access Control Capacity Option

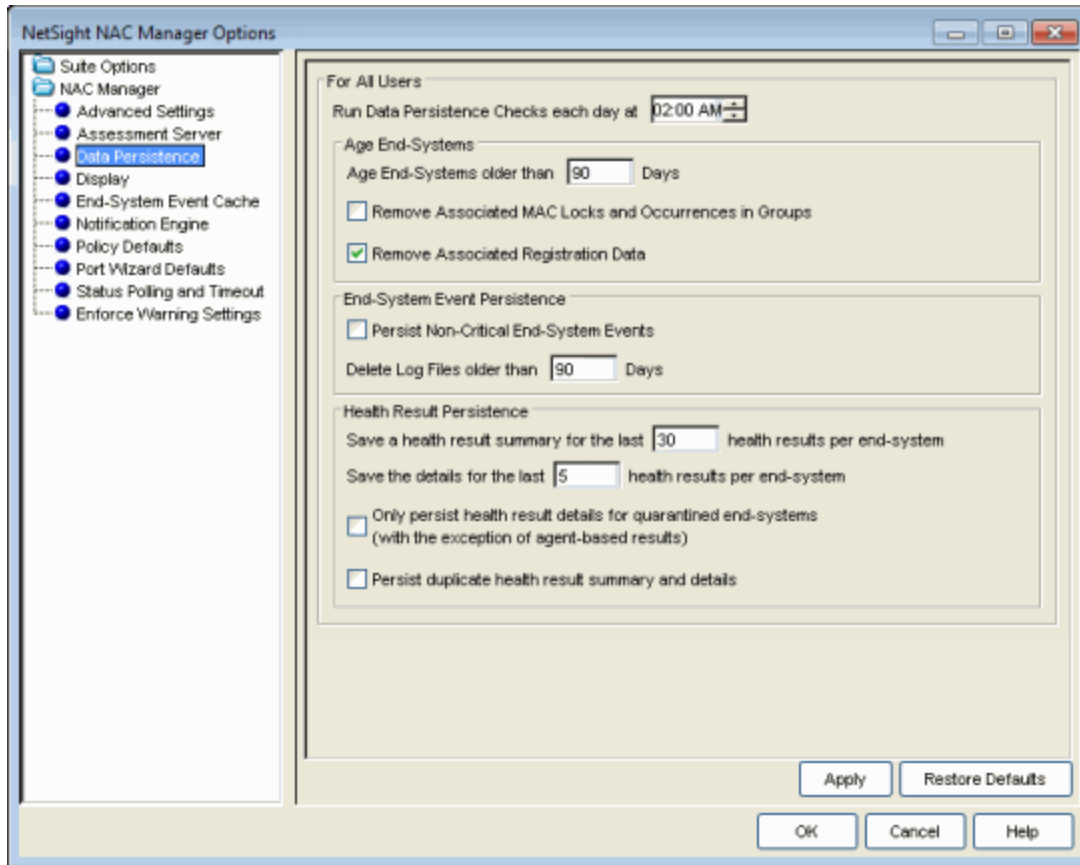
In the Advanced Settings Options panel, the Extreme Access Control (NAC) Capacity option (shown below) lets you configure the amount of Extreme Management Center resources allocated to Extreme Access Control services. The greater the number of end-systems and appliances in your Extreme Access Control deployment, the more resources Extreme Access Control services require. Use the slide bar to select the appropriate setting for your server.

- Low - For low performance shared systems.
- Medium - For medium performance shared systems, or low performance dedicated systems.
- High - For high performance shared systems, or medium performance dedicated systems.
- Maximum - For high performance dedicated systems.



Data Persistence Options

The Data Persistence options (shown below) let you customize how NAC Manager ages-out or deletes end-systems, end-system events, and end-system health results (assessment results) from the tables and charts in the [End-Systems tab](#) and the [Statistics tab](#). By default, a data persistence check is performed each day at 2:00 a.m. (You can change the time that the check is performed, if desired.) Use the following options to configure what the data persistence check ages-out or deletes.



Age End-Systems

Each day, when the Data Persistence check runs, it searches the database for end-systems that NAC Manager has not received an event for in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the [End-Systems tab](#).

If the **Remove Associated MAC Locks and Occurrences in Groups** checkbox is selected, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

End-System Event Persistence

If this checkbox is selected, NAC Manager stores non-critical end-system events, which are events caused by an end-system reauthenticating. End-system events are stored daily in the database. Each day, when the Data Persistence check runs, it removes all events which are older than the number of days specified (90 days by default).

Health Result Persistence

This section lets you specify how many health result (assessment results) summaries and details are saved and displayed in the [End-Systems tab](#) for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system along with detailed information for the last five health result details per end-system.

In addition, you can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).

You can also specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are not saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results are saved.

Troubleshooting

This section provides information on tools supplied by Extreme Networks Extreme Access Control that provide diagnostic and troubleshooting information for the Extreme Access Control appliance and Extreme Management Center Server.

Extreme Access Control Appliance

The following tools can be used to collect and view diagnostic and troubleshooting information for the Extreme Access Control appliance.

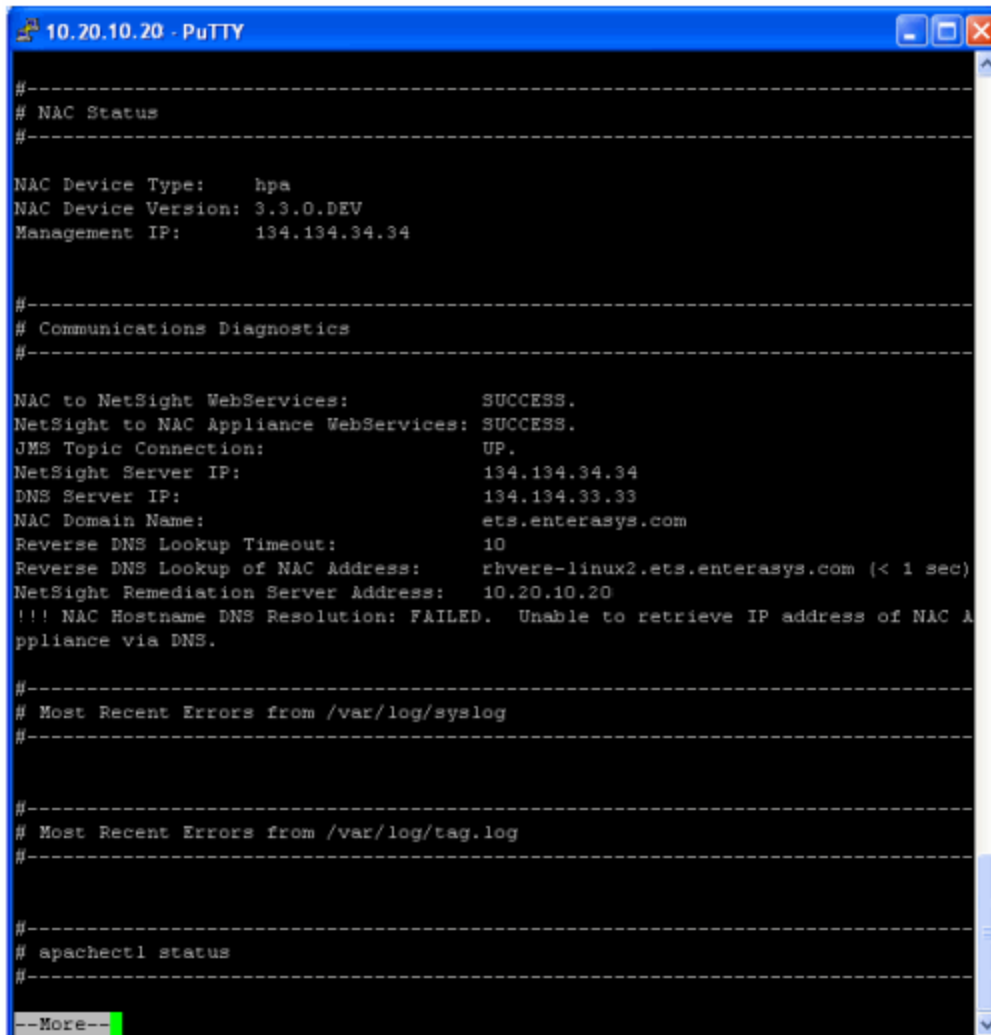
Appliance Command Line Diagnostics

Use the following two commands to display Extreme Access Control (NAC) appliance data:

nacstatus

From the appliance command line, enter the command **nacstatus** to display appliance status information including communications diagnostics, recent errors, DNS configuration, and Navis configuration.

TIP: To collect this information from your Extreme Access Control appliances and save it to a file on the Extreme Management Center Server, use the [Generate Show Support](#) feature in Extreme Management Center.



```
10.20.10.20 - PuTTY
#-----
# NAC Status
#-----
NAC Device Type:    hpa
NAC Device Version: 3.3.0.DEV
Management IP:     134.134.34.34
#-----
# Communications Diagnostics
#-----
NAC to NetSight WebServices:    SUCCESS.
NetSight to NAC Appliance WebServices: SUCCESS.
JMS Topic Connection:          UP.
NetSight Server IP:            134.134.34.34
DNS Server IP:                  134.134.33.33
NAC Domain Name:                ets.enterasys.com
Reverse DNS Lookup Timeout:     10
Reverse DNS Lookup of NAC Address: rhvere-linux2.ets.enterasys.com (< 1 sec)
NetSight Remediation Server Address: 10.20.10.20
!!! NAC Hostname DNS Resolution: FAILED.  Unable to retrieve IP address of NAC A
ppliance via DNS.
#-----
# Most Recent Errors from /var/log/syslog
#-----
#-----
# Most Recent Errors from /var/log/tag.log
#-----
#-----
# apachectl status
#-----
--More--
```

nachelp

From the appliance command line, enter the command **nachelp** to display appliance status information including the location of specific log files and a list of administrative commands for the Extreme Access Control appliance.

```

10.20.10.20 - PuTTY
root@nachpa:~$ nachelp
Enterasys Networks NetSight NAC Device Help
/var/log/tag.log           - NAC Log File
/var/log/syslog           - System Log File
/var/log/message         - System Info
/var/log/navisradius<date>.log - Radius Log
/var/log/httpd/*         - Apache Logs
/var/log/squid/*         - Squid Logs
/etc/resolv.conf         - DNS Configuration

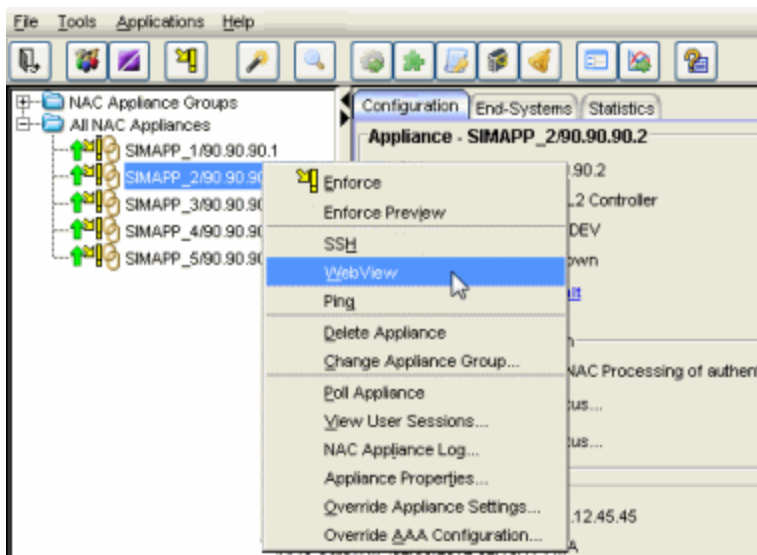
nacdb                    NAC Database Script
naccapture               Protocol-specific packet capture
nacstatus               General NAC Appliance Status
nacreinitializedb       Deletes NAC database, restarts appliance
nacradiuslogging enable|disable Enable/disable NAC RADIUS logging
tagctl start|stop|restart Start/stop/restart NAC process
apachectl start|stop|restart Start/stop/restart webserver
aglsctl start|stop|restart Start/stop/restart agentless assessment
/opt/tag/configMgmtIP <ip> Set management server IP address

CTRL+ALT+<F1-F4> provides access to multiple login shells.
root@nachpa:~$

```

Extreme Access Control Appliance Administration Web Page

To access status and diagnostic information for a Extreme Access Control appliance, launch the Extreme Access Control appliance administration web page by right-clicking on a Extreme Access Control appliance in the left-panel tree and selecting WebView, as shown below. (You can also access the administration web page using the following URL: <https://<Extreme Access ControlApplianceIP>:8444/Admin.>)



The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in NAC Manager using the Advanced Configuration window (available from the Tools menu > Management and Configuration > Advanced Configurations) and selecting the Appliance Settings > Miscellaneous Tab > Web Service Credentials field.

The left-panel tree in the administration web page displays a Home folder plus several other folders: Status, Diagnostics, Log Files, Downloads, and Utilities. Following is an overview of each folder and the web pages it contains.

Home

The Home web page provides appliance performance information including debugging information (such as CPU usage) that helps you determine if the appliance is being overloaded with requests.

NOTES: Memory usage is normally close to 100% to allow for better performance.

A Extreme Access Control virtual appliance has an additional License Status field that displays whether the appliance has a license allocated to it. For more information on virtual appliance licensing, see the Suite-Wide Tools Server Information Window Help topic section on Extreme Access Control VM license.

Home Web Page

The screenshot shows the web interface of a Network Access Control Appliance. The top navigation bar includes the logo, 'Network Access Control Appliance', and 'NAC Manager'. A secondary bar contains 'Logout | Support | About'. A left sidebar lists navigation options: Home, Status, Diagnostics, Log Files, Downloads, and Utilities. The main content area is divided into three sections:

Configuration Details

NAC Engine Information	NAC Gateway - IA-A-300 v.6.0.0.59
NAC Engine IP	10.20.20.15
NetSight Server IP Address	120.141.20.208
NAC Server Status	up, ready since Thu Feb 20 15:53:47 EST 2014
NAC Up Time (HH:MM:SS.mmmm)	24:28:09.889

Resource Details

CPU Usage	User=0.03% System=0.02% Niced=0.00% Idle=99.95% Total=0.05%
Memory Usage	Used=33.27% Free=66.73% Total=11.63 GB
Swap Space	Used=0.00% Free=100.00% Total=11.63 GB
NAC Process	Heap=54.06% Non-Heap=45.94% Total=130.21 MB

Status Details

Statistic	Current	Maximum	Total	Max Reached
Authentication Requests	0/min	11/min	103	Fri Feb 21 10:41:02
Authentication Successes	0/min	1/min	1	Fri Feb 21 10:41:02
Authentication Failures	0/min	1/min	52	Fri Feb 21 12:52:02
Radius Challenges	0/min	10/min	10	Fri Feb 21 10:41:02
Invalid Authentication Requests	0/min	0/min	0	Not /
Duplicate Authentication Requests	0/min	2/min	24	Fri Feb 21 11:57:02
Malformed Authentication Requests	0/min	0/min	0	Not /
Bad Authentication Requests	0/min	0/min	0	Not /

The footer of the interface displays the current date and time: 'Fri Feb 21 2014 16:24:10 GMT-0500 (Eastern Standard Time)' and the copyright notice: 'Copyright © 2014 Extreme Networks, Inc. All rights reserved.'

Status

The Status folder provides the following diagnostic information:

- Agent-Based - Displays information about the agent-based clients connected to Extreme Access Control. Click the **Show All** button to display all connected agents.
- Assessment - Provides performance information related to Extreme Access Control assessment.
- Captive Portal - Provides debug information for the captive portal including statistics on the number of requests served and the interaction with Extreme Management Center.

- Details - Provides additional Extreme Access Control performance information showing where performance bottlenecks may be occurring. The Throttled Tasks column can be used to help diagnose whether there is a problem in a specific part of the Extreme Access Control process.
- End-System Authentication - Provides information on currently managed end-systems and all end-systems managed in the last 24 hours.
- Messaging - Provides information on sent and received JMS Statistics.
- NamedLists - Provides information about named lists (rule groups).
- Network Configuration - Provides a history of network configuration commands.
- Threads - Provides debug information by showing the tasks that Extreme Access Control is currently performing.
- Switches & Routers - Displays basic configuration information about the switches that are configured to use this Extreme Access Control appliance.

Examples of the Details and Agent-Based web pages are shown below.

Status - Details Web Page

Network Access Control Appliance

NAC Manager

[Logout](#) | [Support](#) | [About](#)

- Home
- Status
 - Agent Based
 - Alerts
 - Assessment
 - Captive Portal
 - Database
 - Details**
 - End-System Authentication
 - Messaging
 - Named Lists
 - Network Configuration
 - Other NAC Appliances
 - Threads
 - Switches & Routers
- Diagnostics
- Log Files
- Downloads
- Utilities

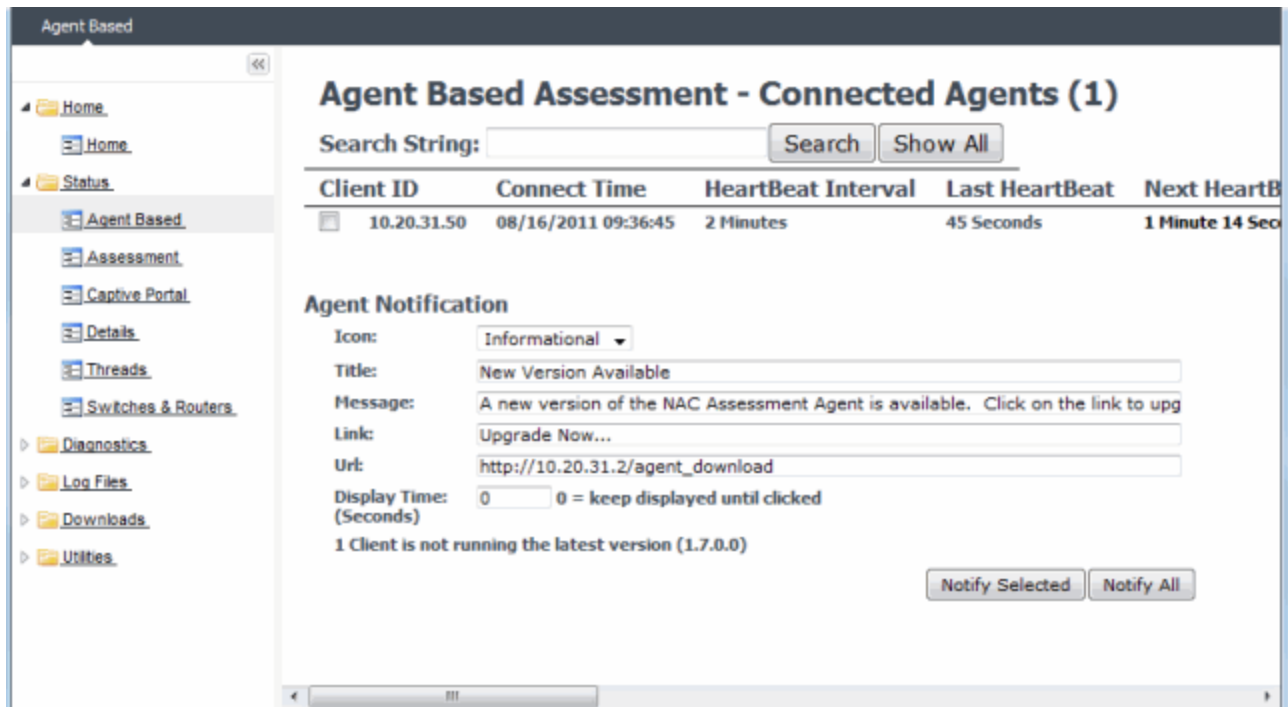
NAC Thread Pool Details

Thread Name	Active Count	Pool Size
Assessment Controller Thread Pool	0	10
BridgeService Thread Pool	0	1
EndSystemEventNotification Thread Pool	0	1
Initialize Switch Thread Thread Pool	0	20
IP Resolution Collapsed HIB Walker Scheduled Thread Pool	0	5
NAC 2 NAC Message Handler Thread Pool	0	1
NAC Manager Config Message Handler Thread Pool	0	1
NAC Manager Status Message Handler Thread Pool	0	1
NAC Status Request Executor Thread Pool	0	1
NacCaptivePortalAdminRegAction - Task Thread Pool	0	10
NacCaptivePortalMainAction - Task Thread Pool	0	10
NacCaptivePortalOsUtils - OS Update Thread Pool	0	10
NacCaptivePortalPreRegAction - Task Thread Pool	0	10
NacCaptivePortalScreenPreviewAction - Task Thread Pool	0	10
NacCaptivePortalSponsorRegAction - Task Thread Pool	0	10
Named List Update Handler Thread Pool	0	1
NetBIOS Request Manager Thread Pool	0	5
RADIUS Session Deactivate Queue Thread Pool	0	1
Reauthentication Service Thread Pool	0	10
ResolveIpAddressService Thread Pool	0	10
SNMP Manager Refresh Child Thread Pool	0	1
SNMP Manager Refresh Parent Thread Pool	0	1
Switch Configuration Thread Pool	0	1
Switch Configuration Scheduled Thread Pool	0	1
Switch Configuration Task Thread Pool	0	10
UpdateService Thread Pool	0	30
UpdateService Scheduled Thread Pool	0	30

No System Events Currently Available.

Fri Feb 21 2014 16:27:45 GMT-0500 (Eastern Standard Time)
Copyright © 2014 Extreme Networks, Inc. All rights reserved.

Status - Agent-Based Web Page



Diagnostics

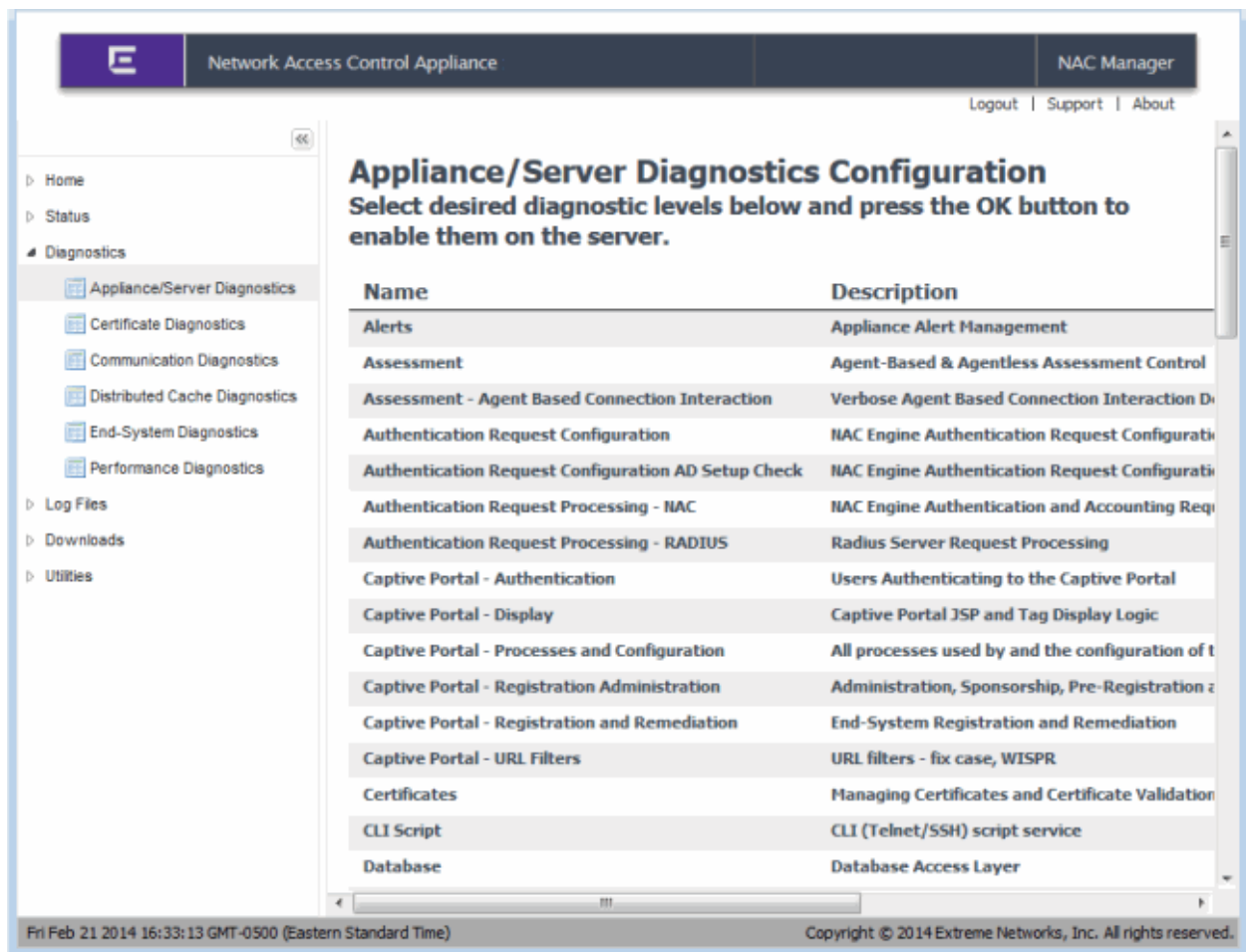
The Diagnostics folder provides the following diagnostic information:

- Appliance/Server Diagnostics - Lets you enable diagnostic groups and diagnostic level that helps with troubleshooting.
- Certificate Diagnostics - Provides information on your Extreme Access Control appliance security certificates including the Internal Communications server certificate chain, the captive portal server certificate chain, the RADIUS server certificate chain, the Extreme Access Control Appliance Trusted Certificate Store, the AAA Trusted Certificate Store, and AAA Certificate Revocation Lists.
- Communication Diagnostics - Displays diagnostic information and provides active tests to help troubleshoot communication issues between the Extreme Access Control appliance and the Extreme Management Center Server. Note that when using the RADIUS request test, RADIUS servers must be enforced to a Extreme Access Control appliance before they are available for selection from the drop-down menu.
- Distributed Cache Diagnostics - Provides information and tools used to diagnose issues with data shared between the Extreme Management Center Server and Extreme Access Control appliances.

- End-System Cache Diagnostics - Provides information and tools to diagnose issues with Extreme Access Control's end-system cache.
- End-System Diagnostics - If the debug information provided in the Server Diagnostics tab is too extensive, this tab allows you to enable debug information for a single end-system, making it easier to search through the database for specific information.
- Server Diagnostics - Allows you to enable different levels of logging on specific Extreme Access Control appliance functionality and view the debug information in /var/log/tag.log on the Extreme Access Control appliance and in the [Server Log](#) web page. By default, error and informational data is logged to the tag.log file, with a new file created each day. You can set the diagnostic level to "Verbose" to collect additional data that is presented in an easy-to-read format.

An example of the Server Diagnostics web page is shown below.

Diagnostics - Server Diagnostics Web Page



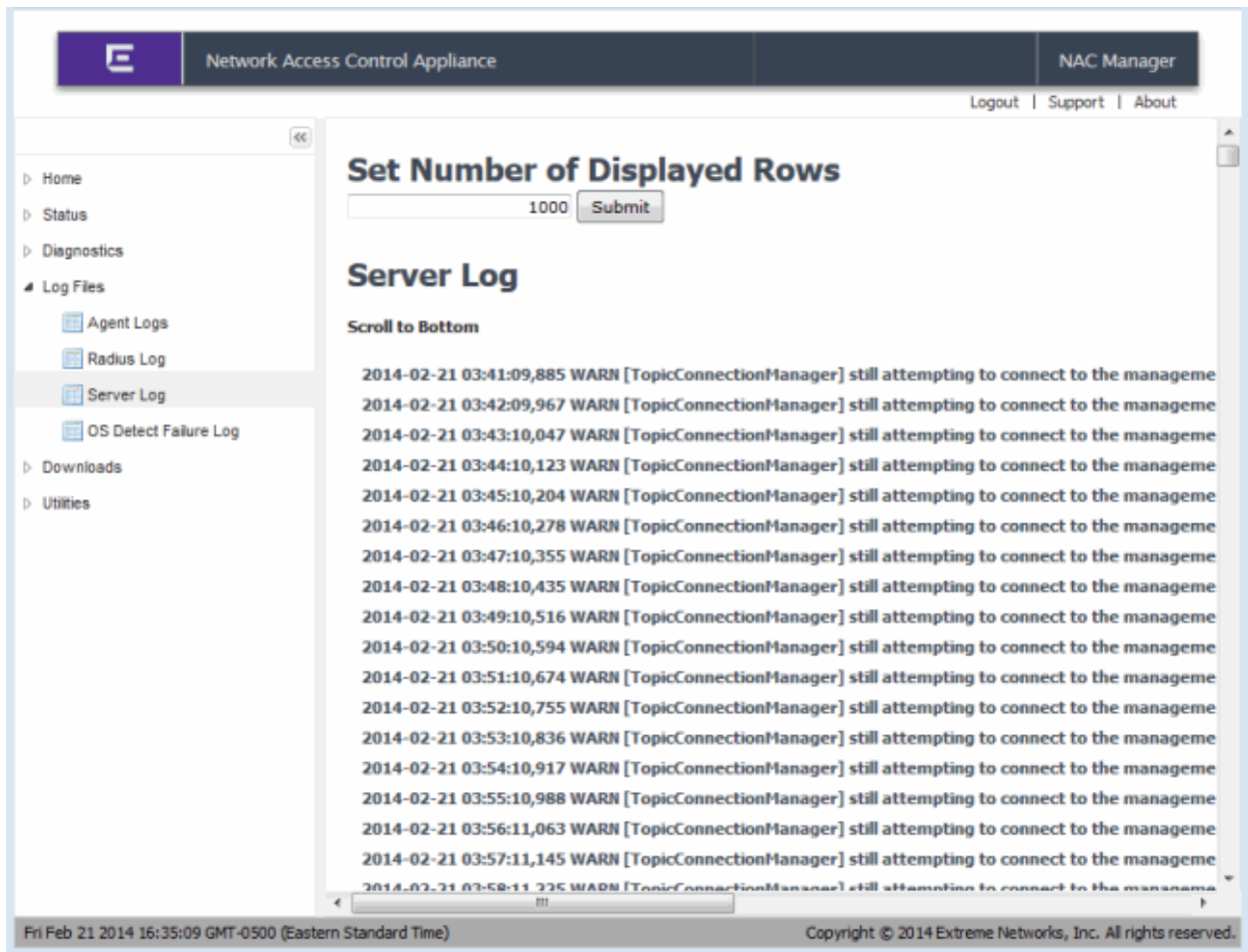
Log Files

The Log Files folder provides the following logs:

- Agent Logs - Displays the agent log files that have been retrieved from remote end-systems via the Client Diagnostics section on the Status > Agent-Based web page.
- RADIUS Log - Displays the last 1000 lines printed in the Extreme Access Control appliance RADIUS log (/var/log/radius/radius.log on the Extreme Access Control appliance).
- Server Log - Displays the last 1000 lines printed in the Extreme Access Control appliance server log (/var/log/tag.log on the Extreme Access Control appliance).
- OS Detect Failure Log - Displays the last 1000 OS detection failures (/var/log/osdetectfailure.log on the Extreme Access Control appliance).

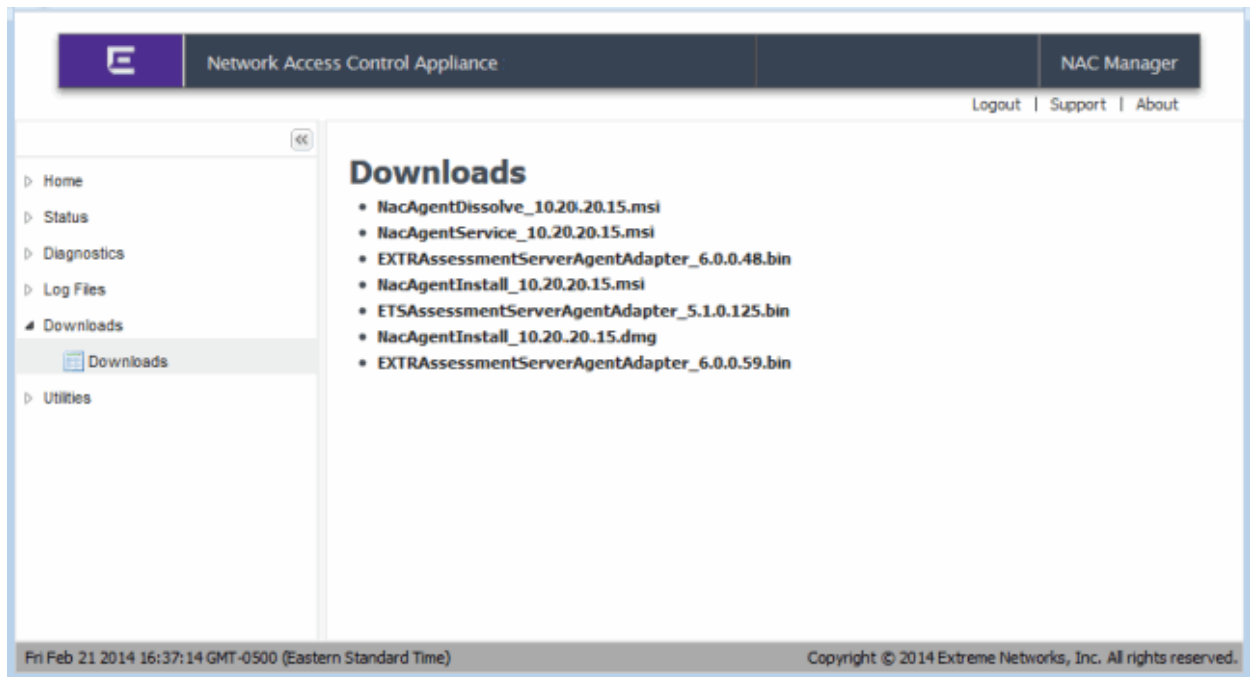
You can change the number of displayed rows using the input box at the top of the page. An example of the Server Log web page is shown below.

Log Files - Server Log Web Page



Downloads

The Downloads web page screen provides links to the assessment agent adapter install file and the installers for agent-based assessment. The assessment agent adapter is required for communication between the Extreme Access Control appliance and the Nessus assessment server.

Downloads Web Page

Utilities

The TCP Dump web page provides the ability to run the TCP Dump packet analyzer and stores the packet capture files, which you can then download to view. Packet capture files (.pcap files) are stored on the Extreme Access Control appliance in `/opt/nac/pcap`.

You create a TCP Dump process by using the Add Process form or by typing in a CLI command in the Custom Command form. Two pcap files are created for each capture. When the first file reaches the maximum file size, the second file is started. When you download them, the server automatically zips these files together. If the server shuts down while a TCP Dump process (initialized through this interface) is running, the process automatically stops.

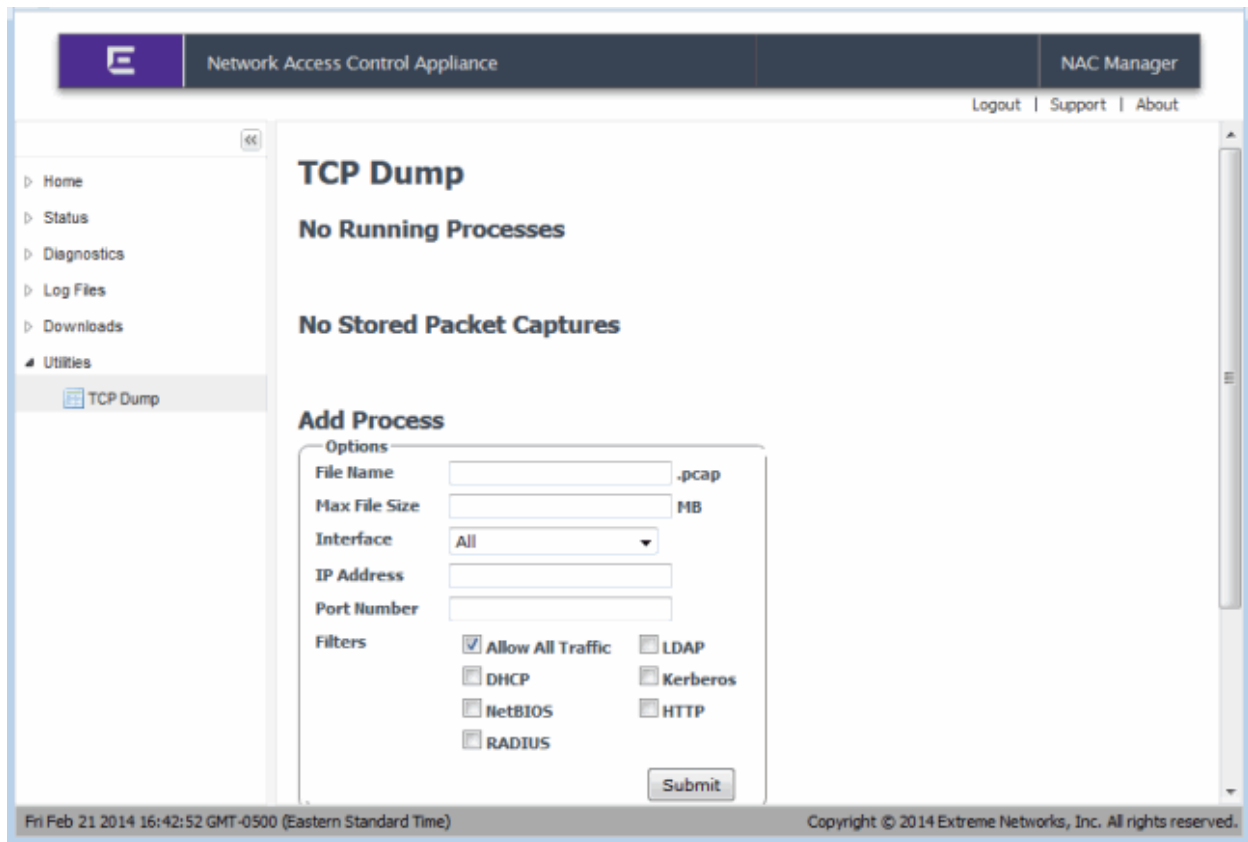
The options for the Add Process form are:

- **File Name:** Enter a name for the .pcap files. The .pcap extension is automatically added to the filename.
- **Max File Size:** Enter a maximum size for a single capture file. The default is 100 MB. A check is done to make sure there is enough disk room before running the process.
- **Interface:** Select a network interface on the server or use All (the default). Loopback is automatically ignored.

- IP Address: If you enter an IP address, only traffic going to or from this host is captured.
- Port Number: If you enter a port number, only traffic on this port is captured.
- Filters: Select the protocols on which to capture traffic or use Allow All Traffic (the default). If you have entered a port number, these checkboxes are ignored. Following are the ports associated with each protocol:
 - DHCP - port 67 and 68
 - RADIUS - port 1645, 1646, 1812, 1813
 - LDAP - port 389 and 636
 - Kerberos - port 88
 - HTTP - port 80, 443, 8080, 8443, and 8444

CAUTION: If you enable an HTTP capture, you should not download any pcap files while the download is running because the capture will grow by the size of the pcap file. You should refrain from downloading pcap files while an HTTP capture is running.

For information on the proper syntax for using the Custom Command form, see: http://www.tcpdump.org/tcpdump_man.html.

Utilities - TCP Dump Web Page


Network Access Control Appliance | NAC Manager

Logout | Support | About

Home
Status
Diagnostics
Log Files
Downloads
Utilities
TCP Dump

TCP Dump

No Running Processes

No Stored Packet Captures

Add Process

Options

File Name: .pcap

Max File Size: MB

Interface:

IP Address:

Port Number:

Filters

Allow All Traffic LDAP

DHCP Kerberos

NetBIOS HTTP

RADIUS

Fri Feb 21 2014 16:42:52 GMT-0500 (Eastern Standard Time) Copyright © 2014 Extreme Networks, Inc. All rights reserved.

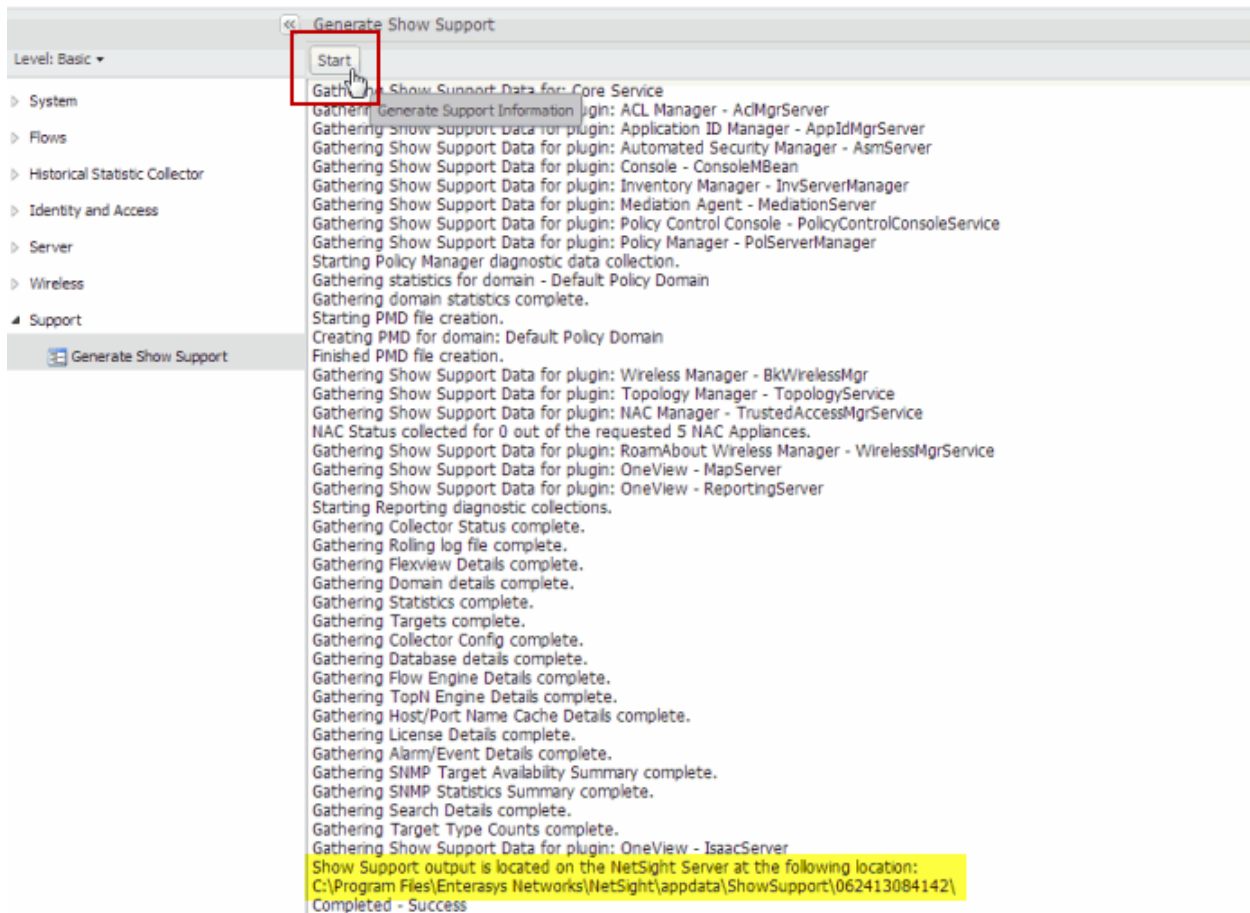
Extreme Management Center Server

The following Extreme Access Control diagnostic features can be used to collect and view diagnostic and troubleshooting information for the Extreme Management Center Server.

Generate Show Support

You can use Extreme Management Center to collect and save Extreme Access Control status information for your Extreme Access Control appliances and the Extreme Management Center Server to a file, allowing you to easily view the data and also send it to Extreme Networks Support for troubleshooting purposes. Extreme Access Control Status information includes communications diagnostics, recent errors, DNS configuration, and Navis configuration.

In Management Center, select the **Administration** tab. Under Support (in the left-panel tree), select the Generate Show Support report and click the **Start** button, as shown below.



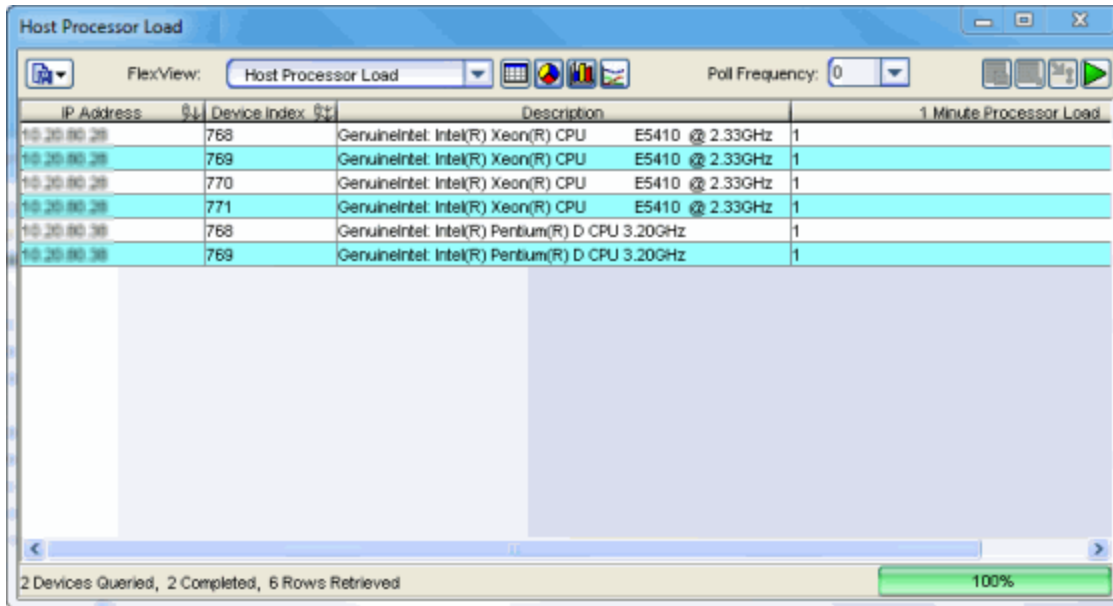
The Extreme Access Control status information is collected and saved in a dated subdirectory under the <install directory>\NetSight\appdata\ShowSupport directory on the Extreme Management Center Server. After you unzip the file, you see separate directories for the different Extreme Access Control appliance and Extreme Management Center server information saved.

Monitoring

Use the following NAC Manager menu options to monitor Extreme Access Control appliance and switch performance information.

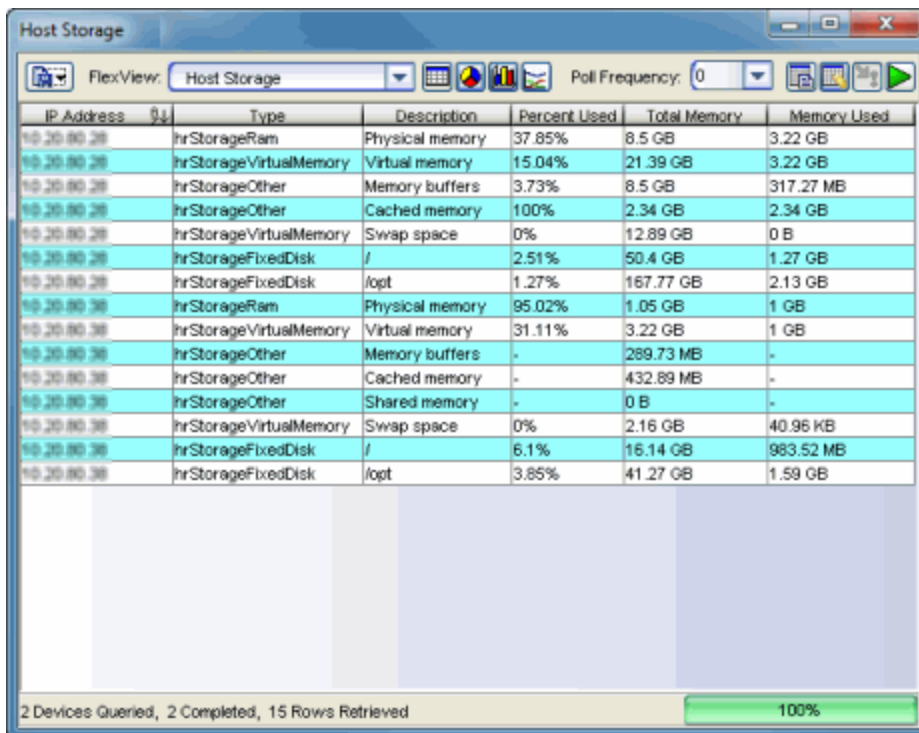
Launch CPU Utilization View

From NAC Manager, right-click on one or more appliances in the right-panel Extreme Access Control (formerly NetSight) **Appliances** tab and select Launch CPU Utilization View to open the Host Processor Load FlexView (shown below).



Launch Memory and Diskspace Utilization View

From NAC Manager, right-click on one or more appliances in the right-panel Extreme Access Control (NAC) Appliances tab and select Launch Memory and Diskspace Utilization View to open the Host Storage FlexView (shown below).



Launch RADIUS Client Information View

From NAC Manager, right-click on one or more switches in the right-panel Switches tab and select Launch RADIUS Client Information View to open the RADIUS Client Information FlexView (shown below).

IP Address	Server	Server Address	Server Port	Round Trip Time	Access Requests	Access Retrs
10.20.80.129	1	10.20.80.28	1812	0 Days 0:00:00.0	7	21

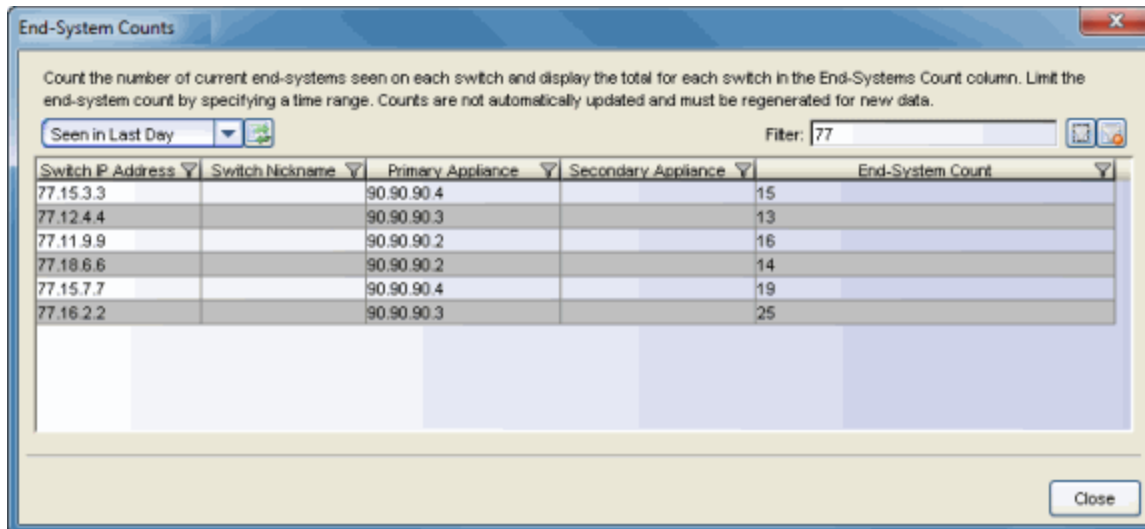
Launch Node Alias and Multi Auth View

From NAC Manager, right-click on one or more switches in the right-panel Switches tab and select Launch Node Alias and Multi Auth View to open the Node Alias and Multi Auth FlexView (shown below).

IP Address	Alias Active	Alias Total	MultiAuth Current Users	MultiAuth Max Users	MultiAuth
10.20.80.129	36	4096	0	48	ieee8021x;pwa,macAuth

View End-System Counts

From NAC Manager, select Tools > View End-System Counts to open a window where you can view the total number of current end-systems seen on each switch. Counts can be limited by specifying a time range, if desired.



Switch IP Address	Switch Nickname	Primary Appliance	Secondary Appliance	End-System Count
77.15.3.3		90.90.90.4		15
77.12.4.4		90.90.90.3		13
77.11.9.9		90.90.90.2		16
77.18.6.6		90.90.90.2		14
77.15.7.7		90.90.90.4		19
77.16.2.2		90.90.90.3		25

Extreme Management Center Server and Extreme Access Control Appliance Connectivity

There are four communications channels between the Extreme Management Center Server and the Extreme Access Control appliance: SNMP, Web Services from the Extreme Access Control appliance to the Extreme Management Center Server, Web Services from the Extreme Management Center Server to the Extreme Access Control appliance, and JMS (Java Message Service). Extreme Management Center Console, Policy Manager, and Inventory Manager use SNMP to communicate with the Extreme Access Control appliance and determine its state. NAC Manager uses Web Services and JMS communication instead of SNMP to determine appliance status, providing more robust connectivity information. NAC Manager status should always be used as the primary determination of appliance connectivity. For example, Extreme Access Control appliance status could be "up" in Console while "down" in NAC Manager.

The following sections explain how to determine the status of each communication channel, and provide troubleshooting information for connectivity problems.

SNMP

SNMP is the most basic communication method used to talk to the Extreme Access Control appliance. Extreme Management Center Console use SNMP to poll the Extreme Access Control appliance (both Extreme Access Control Gateways and Extreme Access Control Controllers) and determine its status. Policy Manager and Inventory Manager can be used to verify SNMP status for Extreme Access Control Controllers only. SNMP status is determined by looking at the device status icons in the left-panel tree. If the arrow on the Extreme Access Control appliance icon is green, SNMP connectivity is established. If the arrow is orange or red, there is an issue with SNMP connectivity. An orange arrow indicates that an SNMP error was returned (check the event log for an error description). A red arrow indicates an SNMP timeout. Check ping access between the server and the appliance, and verify SNMP credentials. Alternatively, MIB Tools can be used to verify SNMP connectivity between the server and the Extreme Access Control appliance.

Web Services

Java Web Services is an XML-based communications protocol that provides symmetric communication channels from the Extreme Access Control appliance to the Extreme Management Center Server and from the Extreme Management Center Server to the Extreme Access Control appliance.

When troubleshooting Web Services, start by verifying the following basic configuration requirements:

- Web Services occur over SSL with a destination of port 8444. Verify that port 8444 is not blocked between the server and appliance, in both directions.
- Verify that the Extreme Access Control appliance has DNS servers configured, and that the Extreme Management Center Server can resolve all appliance hostnames and the Extreme Access Control appliances can resolve the Extreme Management Center Server hostname.
- Verify that the Extreme Management Center server is bound to the proper interface (if there are multiple interfaces). For information see Systems with Multiple NICs in the Extreme Management Center Installation Guide.
- Ensure that the Extreme Access Control appliance has the correct IP address configured as the Management Server IP address by running the command `cat /opt/nac/mgmtServerIP`. Run the command `/opt/nac/configMgmtIP` at the appliance CLI to configure the IP address

if necessary, and use the Extreme Management Center Server's IP address (the bound IP in the Extreme Management Center Server's server.log) as the Management Server IP address. To start using the new Extreme Management Center Server, you must restart the appliance by entering the command `nacctl restart`.

- Verify Web Service credentials in NAC Manager (Tools > Manager Advanced Configurations > Global and Appliance Settings > Appliance Settings > Default > Credentials Tab).
- Reset the web service credentials on the Extreme Access Control appliances to ensure a match. From the `/opt/nac/` directory, enter the command `./configWebCredentials`.

The next step is to determine the current Web Service status for the appliance. The current status of the Web Service for a Extreme Access Control appliance is found on the Communications Diagnostics page of the Extreme Access Control Appliance Administration web page, as shown below.

Launch the Extreme Access Control Appliance administration web page by right-clicking on the Extreme Access Control appliance in the NAC Manager left-panel tree and selecting WebView or by using the following URL: `https://<Extreme Access ControlApplianceIP>:8444/Admin`. The default user name and password for access to this web page is "admin/Extreme@pp." Click on the Diagnostics page and then the Communication Diagnostics page.

Communication Diagnostics Web Page

The screenshot displays the 'Communication Diagnostics' web page on a Network Access Control Appliance. The page title is 'Communication Diagnostics' with the subtitle 'Tools used to diagnose issues communicating with NetSight'. The left sidebar contains navigation options: Home, Status, Diagnostics (with sub-items: Appliance/Server Diagnostics, Certificate Diagnostics, Communication Diagnostics, Distributed Cache Diagnostics, End-System Diagnostics, Performance Diagnostics), Log Files, Downloads, and Utilities. The main content area is divided into two sections: 'Communication Status Information' and 'Active Tests'.

Communication Status Information:

JMS Topic:	Topic Connection is Up
Web Service Authorization:	Web Service is Authorized
Last Web Service Request:	Request Succeeded
NetSight Server Address:	134.145.90.208
Local Port used by NetSight:	8444
Name Server Address:	10.54.188.120
Name Lookup Timeout:	10
NAC Host Name:	nac300-20015.nac2003.com
NAC Domain Name:	nac2003.com

Active Tests:

Test Name Lookup for NetSight Server: (could take 2 mins)

Test Web Service Request to NetSight Server:

At the bottom of the page, the status bar shows: 'Fri Feb 21 2014 16:46:57 GMT-0500 (Eastern Standard Time)' and 'Copyright © 2014 Extreme Networks, Inc. All rights reserved.'

On the Communications Diagnostics page, you will find the Web Service Authorization and Last Web Service Request status. These two fields provide information on whether or not the Extreme Access Control appliance can contact the Extreme Management Center Server with Web Service calls. If Web Service Authorization says "Extreme Access Control (NAC) Appliance is not Authorized," there is a communication issue between the Extreme Access Control appliance and the Extreme Management Center Server. In this case, check the following points:

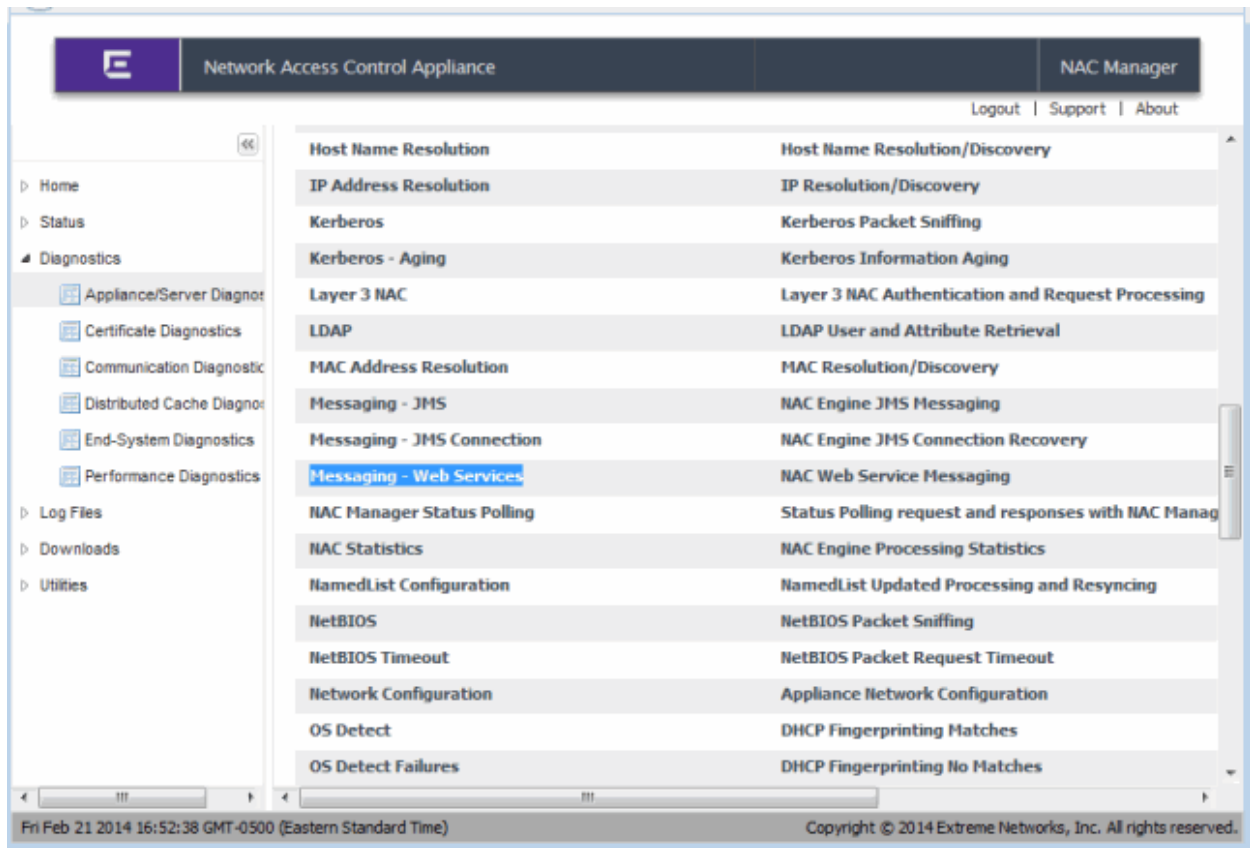
- If the JMS Topic status does not say "Topic Connection is Up," refer to the section on troubleshooting [JMS Connections](#) to resolve this issue.
- Verify that DNS is configured with hostnames of the Extreme Access Control appliance and Extreme Management Center Server. Test DNS resolution with the **Test Name Lookup** button.
- Verify that SSL Certificates have been configured for Web Service connections. To do this, open the Extreme Access Control Appliance Administration Web Page and view the certificate via the browser window.

For Internet Explorer 8, use View > Security Report > View Certificates. For Internet Explorer 7, use File > Properties > Certificates. For Firefox 3.5, use Tools > Page Info > Security > View Certificate.

- Verify that the Web Service Credentials are configured correctly. Web credentials are used to negotiate Web Services between the Extreme Management Center Server and Extreme Access Control appliance. They can be configured on the Extreme Management Center Server through NAC Manager, by going to Tools > Management and Configuration > Advanced Configuration > Global and Appliance Settings > Appliance Settings. Select the Appliance Settings to edit, click on the Credentials tab, and configure the credentials in the Web Service Credentials section. Changes to the credentials is propagated to the Extreme Access Control appliances on Enforce. (If for some reason the credentials are out of sync on the Extreme Access Control appliance, use the `/opt/nac/configWebCredentials` command to configure the Web Service Credentials on the appliance. Restart the appliance by entering the command `nacctl restart`.)

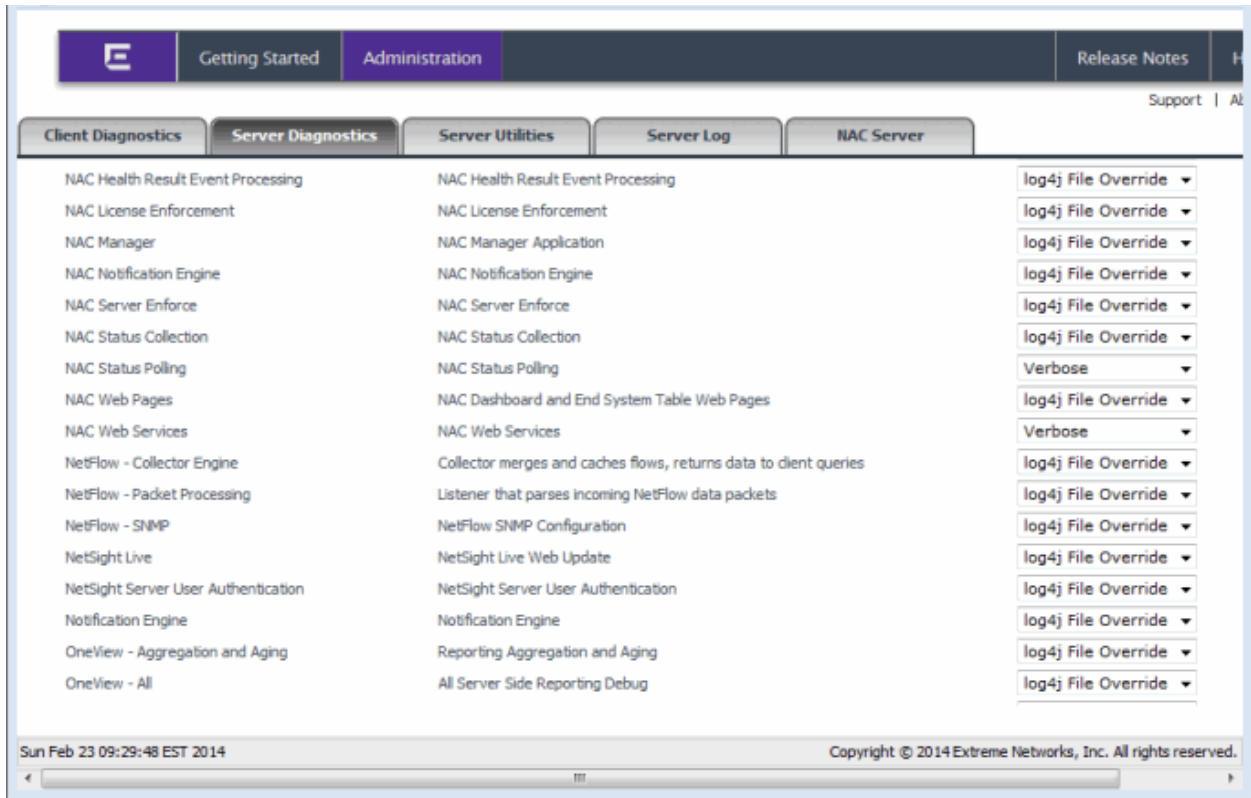
Use the appliance's Server Diagnostics page to obtain additional information on Web Service connectivity. Access this web page from the [Extreme Access Control Appliance administration web page](#) by clicking on the Diagnostics page and then the Appliance/Server Diagnostics page. Enable the "Messaging - Web Services" debug group to log detailed debug information on Web Service connectivity. Set the Diagnostic Level to "Verbose" and access the debug information in `/var/log/tag.log` on the Extreme Access Control appliance or in the Server Log web page.

Server Diagnostics Web Page for Extreme Access Control Appliance



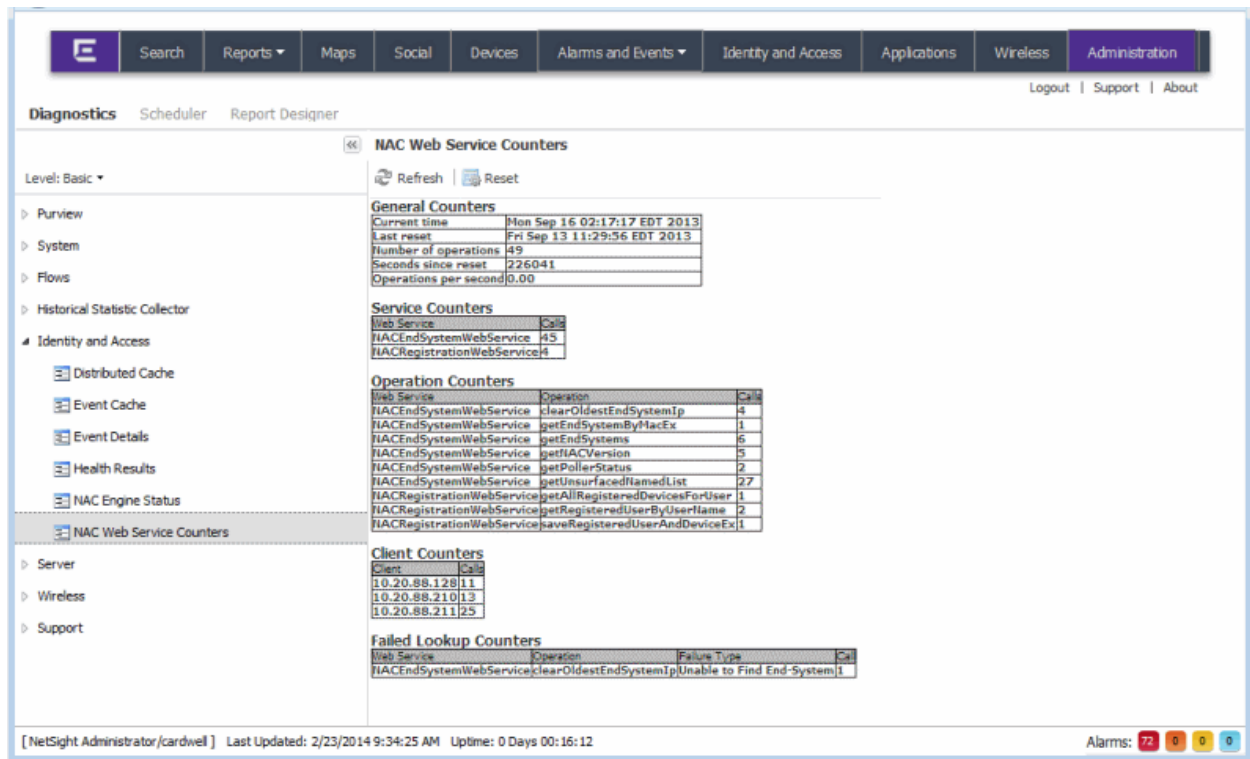
On the Extreme Management Center Server, use the Server Diagnostics page to obtain detailed debug information on Web Service connectivity. Access this page from the Extreme Management Center Launch page by clicking the Administration tab. To access the server diagnostics, you need to log in with your username and password. (If the Extreme Management Center Server is a Windows platform system, in the Username field you must enter a domain name and a username using the following format: <domain name>\<username>). Enable the "Extreme Access Control Web Services" and "Extreme Access Control Status Polling" debug groups by setting the Diagnostic Level to "Verbose." Access the debug information in <install directory>\NetSight\appdata\logs\server.log on the Extreme Access Control Server.

Server Diagnostics Web Page for Extreme Management Center Server



Use the **Administration** tab to view Extreme Access Control web service counters. Launch Management Center and select the **Administration** tab. Click on the **Diagnostics** sub-tab, expand the Extreme Access Control folder, and click on Extreme Access Control Web Service Counters.

Administration Tab



JMS Connections

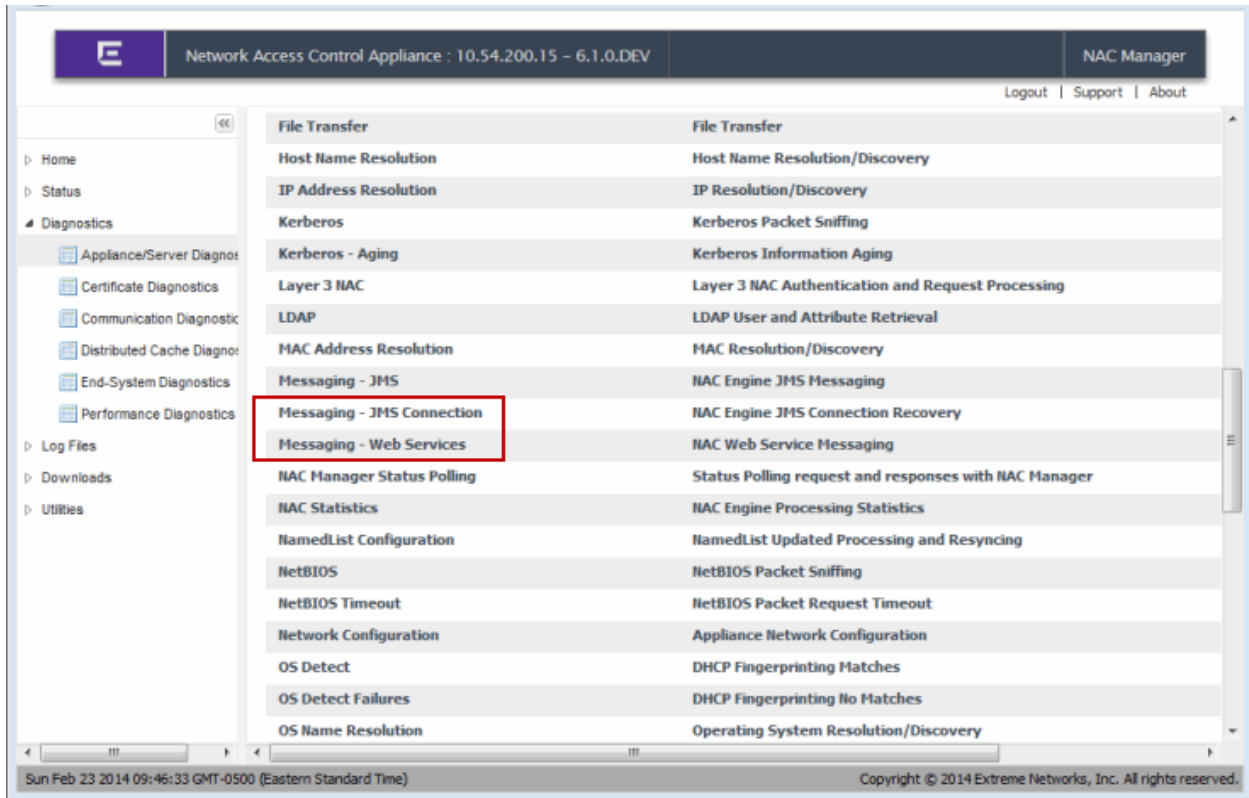
The Extreme Management Center Server and Extreme Access Control appliance also use JMS (Java Message Service) as a communications channel for sending messages back and forth. JMS is proprietary socket-based and the Extreme Management Center Server and Extreme Access Control appliance listen on message "topics" for new messages to and from each other.

The state of JMS connections can be determined by looking at the JMS Topic field on the Communication Diagnostics page on the Extreme Access Control Appliance. Access this web page from the [Extreme Access Control Appliance Administration web page](#) by clicking on the Diagnostics page and then the Communications Diagnostics page. You can also determine the state of JMS connections from the /var/log/tag.log file on the Extreme Access Control appliance, which contains error messages from TopicConnectionManager that helps troubleshoot JMS connectivity issues.

Additional debug information can be retrieved on the Extreme Access Control appliance by enabling the "Messaging - JMS" and "Messaging - JMS Connection" debug groups on the Server Diagnostics page. Access this web page from the [Extreme Access Control Appliance Administration web page](#) by

clicking on the Diagnostics page and then the Server Diagnostics page. Set the Diagnostic Level for these two groups to "Verbose" and access the debug information in /var/log/tag.log on the Extreme Access Control appliance or in the Server Log web page.

Server Diagnostics Web Page for Extreme Access Control Appliance



NAC Manager Reference Information

The **Reference Information** section contains reference information and procedures for NAC Manager.

Microsoft® NAP Processing

Microsoft NAP (Network Access Protection) detection is enabled by default on NAC appliances. When a connection request is received from a NAP-enabled end-system, the end-system is assigned the authentication type of MS NAP (Microsoft NAP) and proceeds through the typical NAC process. If NAP has quarantined the end-system, then NAC Manager will also quarantine the end-system.

If the end-system is not quarantined, and it is assigned a profile that does not have assessment enabled and does not have the "Replace RADIUS Attributes with Accept Policy" option enabled, then NAC Manager will forward the RADIUS response attributes from the NPS Server without scanning. If the end-system is assigned a profile that has assessment enabled, then the end-system will be assessed. If the "Replace RADIUS Attributes with Accept Policy" option is enabled, then the RADIUS response attributes from the NPS Server will be overridden by the Accept policy configured in the profile.

If you do not want NAC Manager to override the RADIUS response attributes from the NPS Server, you can create the following rule for your NAC configuration:

1. In your NAC Configuration, create a rule named NAP Enabled End-Systems.
2. Set the Authentication Type to MS NAP (Microsoft NAP).
3. Set the NAC profile to the Pass Through NAC Profile.

With this rule, if the end-system is NAP enabled, NAC Manager allows NAP to control authentication and assessment for the end-system. NAC Manager will proxy the RADIUS requests and create a health result from the RADIUS Accept packet. NAP will return values indicating the quarantine state of the end-system, which will be displayed in the health result. The health result will not display a score since NAP is determining how quarantine decisions are made. If NAC Manager gets a RADIUS Reject packet, then the end-system is rejected as normal.

There is an option available in the Advanced Configuration View where you can disable NAP processing, if desired.

1. Select Tools > Management and Configuration > Advanced Configurations to open the Advanced Configuration View.
2. In the left-panel tree, expand the Global and Appliance Settings folder and then the Appliance Settings folder.
3. Select the Default Appliance Settings configuration listed under the folder.
4. In the right panel, select the Miscellaneous tab. You will see a Microsoft NAP option titled "Reset Authentication Type for NAP Enabled End-Systems." Deselect this option to disable NAP processing.