ExtremeConnect® User Guide
Version 8.2

2/2019
9036008-01
Subject to Change Without Notice

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/

Contact

If you require assistance, contact Extreme Networks using one of the following methods.

- Global Technical Assistance Center (GTAC) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.

- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

Extreme Connect Overview

The Extreme Management Center Connect tab allows you to integrate third-party software with Extreme Management Center's Extreme Access Control solution.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Extreme Management Center's Extreme Access Control solution allows you to monitor end-systems and configure the appropriate experience for users accessing your network based on a variety of criteria. Network administrators may also have a variety of other tools to help monitor and control the user experience. Extreme Connect bridges the gap between these tools and allows you to control your network configurations from within Extreme Management Center.

NOTE: Extreme Connect requires an Extreme Management Center advanced license (NMS-ADV).

ExtremeXOS devices using Extreme Connect must be running version 21.1.2 or later.

Navigating the Connect Tab

The tab contains three sub-tabs:

- Configuration — Provides information about all of the end-systems and end-system groups analyzed by each of your supported network monitoring tools (called modules) and allows you to configure the end-user experience using each module.
- Domains — Allows you to search for a particular end-system in multiple versions of Extreme Management Center and returns information found using your third-party software. You can also add or remove MAC addresses from end-system groups.
- Services API — Allows you to execute a client/server application, known as a web service.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- Extreme Management Center version 7.0
- Enough switches that support multi-user authentication and policy for the number of end-user sessions on the network.

Related Information

For information on related tabs:

- Configuration
- Domains
- Services API
- Web Service Error Codes
- Dashboard
- Extreme Connect Troubleshooting

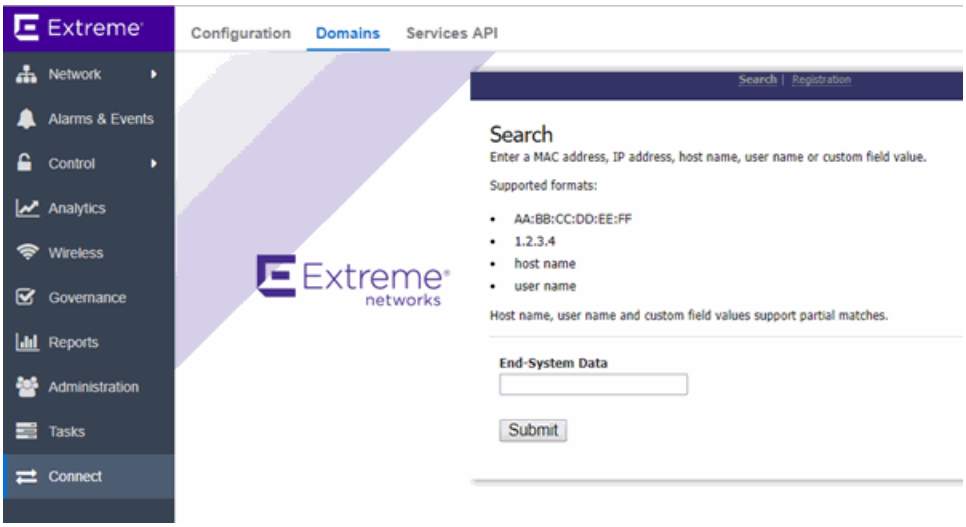
Connect Module Requirements

The Extreme Management Center Connect tab allows you to integrate third-party software with Extreme Management Center's Extreme Access Control solution.

Extreme Management Center's Extreme Access Control solution allows you to monitor end-systems and configure the appropriate experience for users accessing your network based on a variety of criteria. Network administrators may also have a variety of other tools to help monitor and control the user experience. Extreme Management Center Connect bridges the gap between these tools and allows you to control your network configurations from within Extreme Management Center.

To open the Connect tab, select Connect from the tabs at the left in Extreme Management Center.

NOTE: Connect requires an Extreme Management Center advanced license (NMS-ADV).



Navigating the Connect Tab

The tab contains three tabs:

- Configuration — Provides information about all of the end-systems and end-system groups analyzed by each of your supported network monitoring tools (called modules) and allows you to configure the end user experience using each module. For additional information, see Configuration.
- Domains — Search for a particular end-system and return information found using your third-party software as well as add or remove MAC addresses to create end-system groups. For additional information, see Domains.
- Services API — allows you to execute a client/server application, known as a web service.

Additionally, the Menu at the top of the screen provides links to additional information about your version of Extreme Management Center.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- Extreme Management Center version 7.0
- Enough switches that support multi-user authentication and policy for the number of end-user sessions on the network.

For a list of the requirements for each individual module, see Module Requirements.

Related Information

For information on related tabs:

- Administration
- Alarms and Events
- Network
- Reports
- Wireless

ExtremeConnect Configuration

The Configuration tab provides information about the end-systems and end-system groups connecting to your network.

Using third-party software (known as modules) in conjunction with the network monitoring and access control functionality found in the Extreme Management Center Extreme Access Control solution, the Configuration tab provides the most thorough information available about devices accessing your network. Additionally, the Configuration tab allows you to control end-system access to your network using each supported module's functionality.

The Configuration tab contains the following sub-tabs, each providing information about end-systems:

- Dashboard — Provides an overview of the end-systems monitored by each module and the end-systems groups accessing your network.
- End-Systems — Displays the end-systems detected for each module.
- End-System Groups — Displays the end-system groups detected for each module.
- Administration — Allows you to configure how Extreme Management Center communicates with each module and the behavior of the module within Extreme Management Center.

- Statistics — Displays various statistics about the time end-systems spent performing certain operations on the network.
- About — Provides basic information about your version of Extreme Connect, the number of modules being used by your network, and basic information detected by modules in use.

There are many different ways to configure Connect due to the different third-party softwares available.

Module Configuration

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Pending Approval end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Add end-systems to end-system groups	If this is set to “true”, the MAC of the end-system will be added to an end-system group in Extreme Management Center.
Update custom fields for end-systems	If this is set to “true”, the custom field data will be update for each end-system
Update Kerberos username for end-systems	If this is set to “true”, the username will be updated for each end-system and a Kerberos reauthentication is triggered.
Update devicetype for end-systems	If this is set to “true”, the device type data will be update for each end-system.
Reauthorize end-system after update	If this is set to “true”, the end-system will be reauthorized after it has been added to an end-system group
Remove end-system from existing groups	If this is set to “true”, the end-system MAC will be removed from all other end-system groups, if present
Import End-system Groups	If this is set to “true”, all preconfigured MAC End-system Groups will be retrieved from Extreme Management Center. All groups with the values vlan=#NUMBER# approval=#true|false# in their description field will be automatically used by all other modules (i.e. vSphere will create portgroups for vSwitches using these values)

Verification

In order to verify whether Extreme Connect is successfully pushing data from 3rd party data sources to Extreme Management Center:

1. Open Extreme Management Center's Control > **End-Systems** tab.
2. Find an end-system updated by ExtremeConnect and navigate to the custom field – the field displays vmName=MyVirtualMachine;vmGuestFullName=Ubuntu 5…" or something similar, depending on your data sources. The information displayed here differs a bit depending on the module that reports the data to Extreme Management Center.
3. Make sure that the end-system list is actually displaying the custom field that you have chosen during installation.

NOTE: You can rename the Custom field on the Administration > Options > Access Control tab.

Related Information

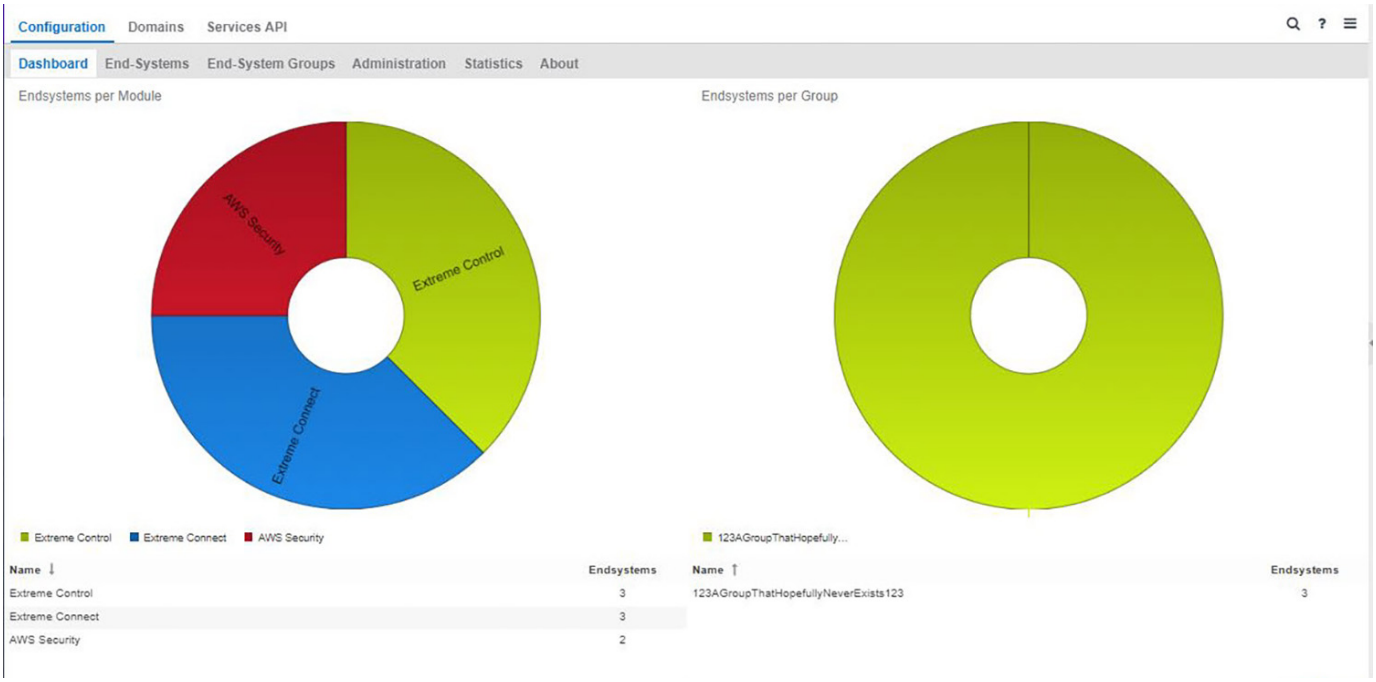
For information on related tabs:

- Data Center/Cloud Integration
- ExtremeConnect Security Configuration
- Connect Mobility Configuration
- ExtremeConnect Management / IT Operations Configuration
- Data Center Manager (DCM) System Configuration
- Connect Convergence Configuration
- Mobile Device Management (MDM) System Configuration
- ExtremeConnect Assessment Configuration
- Connect Configuration Troubleshooting

Dashboard

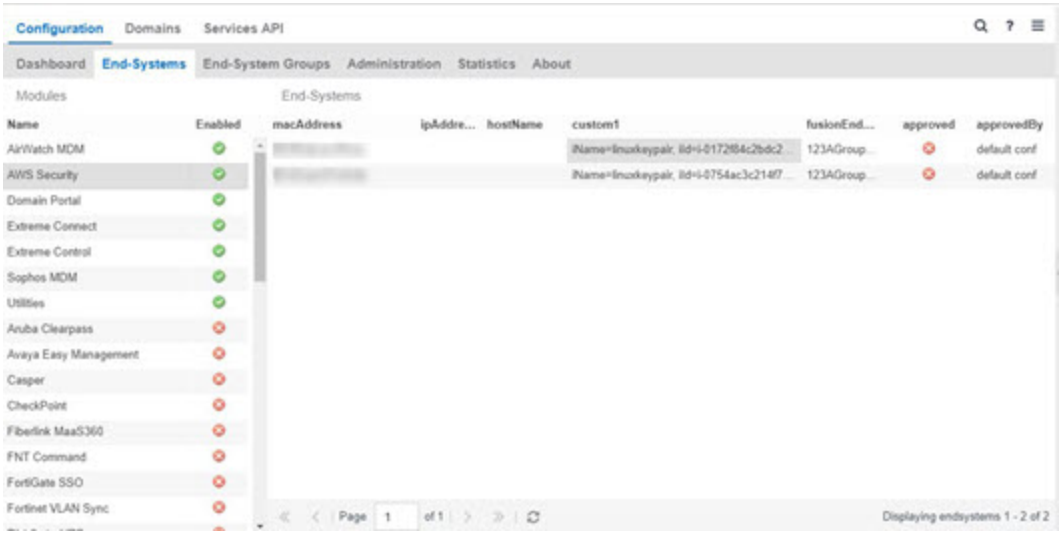
The **Dashboard** tab provides a top-level overview of the end-systems detected on your network. End-systems are grouped by the modules that detected them

and the end-system groups to which they are assigned.



End-Systems

The End-Systems tab provides information about the end-systems connecting to your network.



Left Panel

The left panel of the tab shows all of the modules available in the Connect tab.

The **Enabled** column indicates whether the module is enabled:

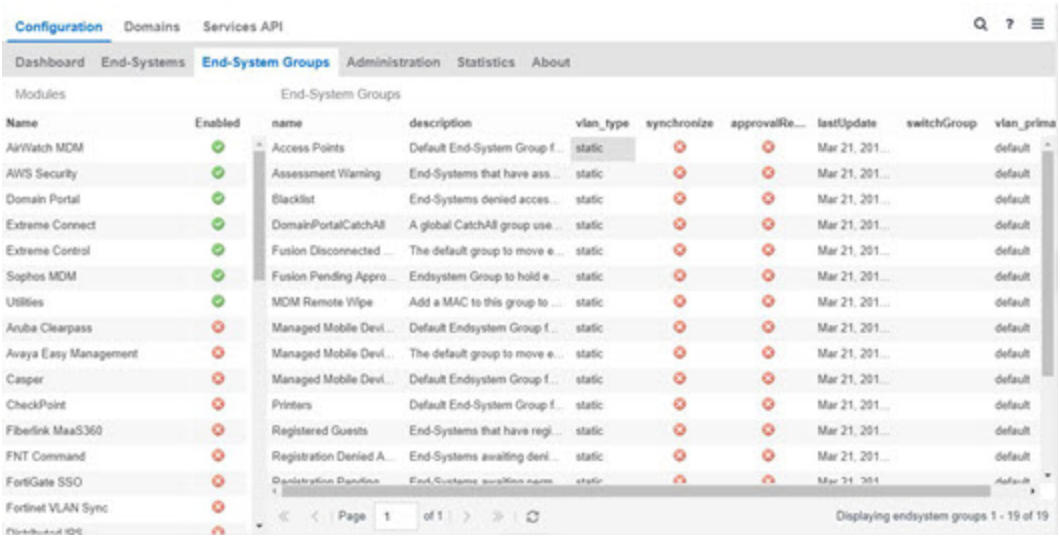
- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end-systems. Add or remove a column by clicking the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

End-System Groups

The **End-System Groups** tab provides information about the end-system groups connecting to your network.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end-system groups. Add or remove a column by clicking the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

Administration

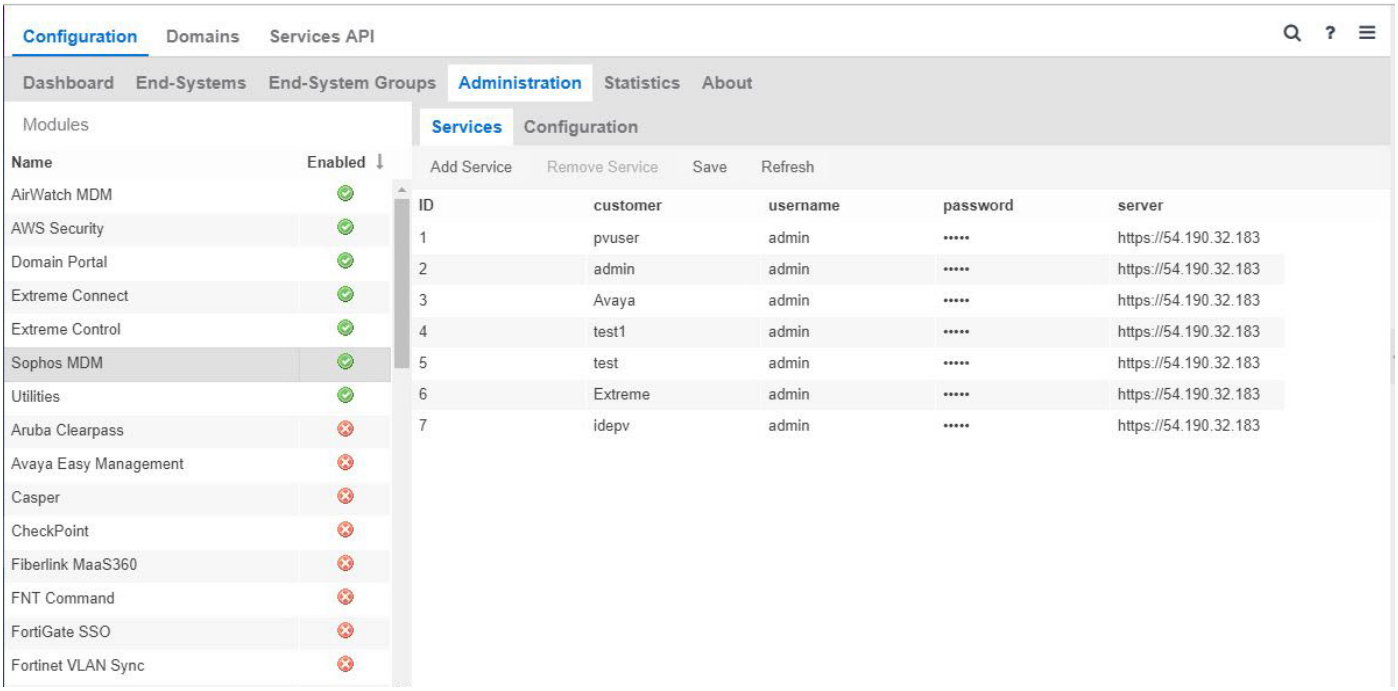
In the Administration tab, enter the information that details how Extreme Management Center connects to the module server and configure the module in Extreme Management Center.

The tab contains two sub-tabs:

- Services — A service outlines to Extreme Management Center how it connects to the server of the module you select. This includes the login credentials, IP, and port information for the module.
- Configuration — Allows you to configure how the module gathers end-system information and controls network access in Extreme Management Center and how that information is presented.

Services

Access the Services tab to specify information detailing how Extreme Management Center contacts the module's server. The Services tab allows you to specify multiple services for modules that have more than one server.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel displays a table containing the services saved for the selected module. The information in this panel varies depending on the module selected in the left panel. The information below is an example using the **Fiberlink MaaS360** module.

ID
: A unique identifier for each service. This field cannot be edited.

Username
: The username used to access the module's server.

Password
: The password used to access the module's server.

apiUrl
The url that provides access to the module's server.

billingIdEncrypt
The billing account ID used for the module.

appId
The application ID used to contact the module's web service.

appVersion
The application version of the module.

platformId
The platform ID of the module.

accessKey
The key used to communicate with the module server.

Add Service
Click this button to add a new row in the Services table from which you can create a new service for the module.

Remove Service
Click this button to remove the selected row from the Services table.

Save
Click the Save button to save any changes made to services in the Services table.

Refresh
Click this button to update the table with any changes.

Configuration

The Configuration tab allows you to determine the information you want the module to gather from end-systems in Extreme Management Center as well as the module's access control behavior on the network.

Left Panel

The left panel of the tab shows all of the modules available in the Connect tab.

The Enabled column indicates whether the module is enabled:

- Check icon () — Module enabled on your network.
- X icon () — Module not enabled on your network.

Right Panel

The right panel displays two tables:

- General Configuration — Allows you to configure certain general Extreme Management Center criteria.
- Specific Configuration — Allows you to configure module-specific functionality.

Each module you select in the left panel displays different configurations, depending on the functionality available when using the module.

Name
The name of the configuration. This column cannot be edited.

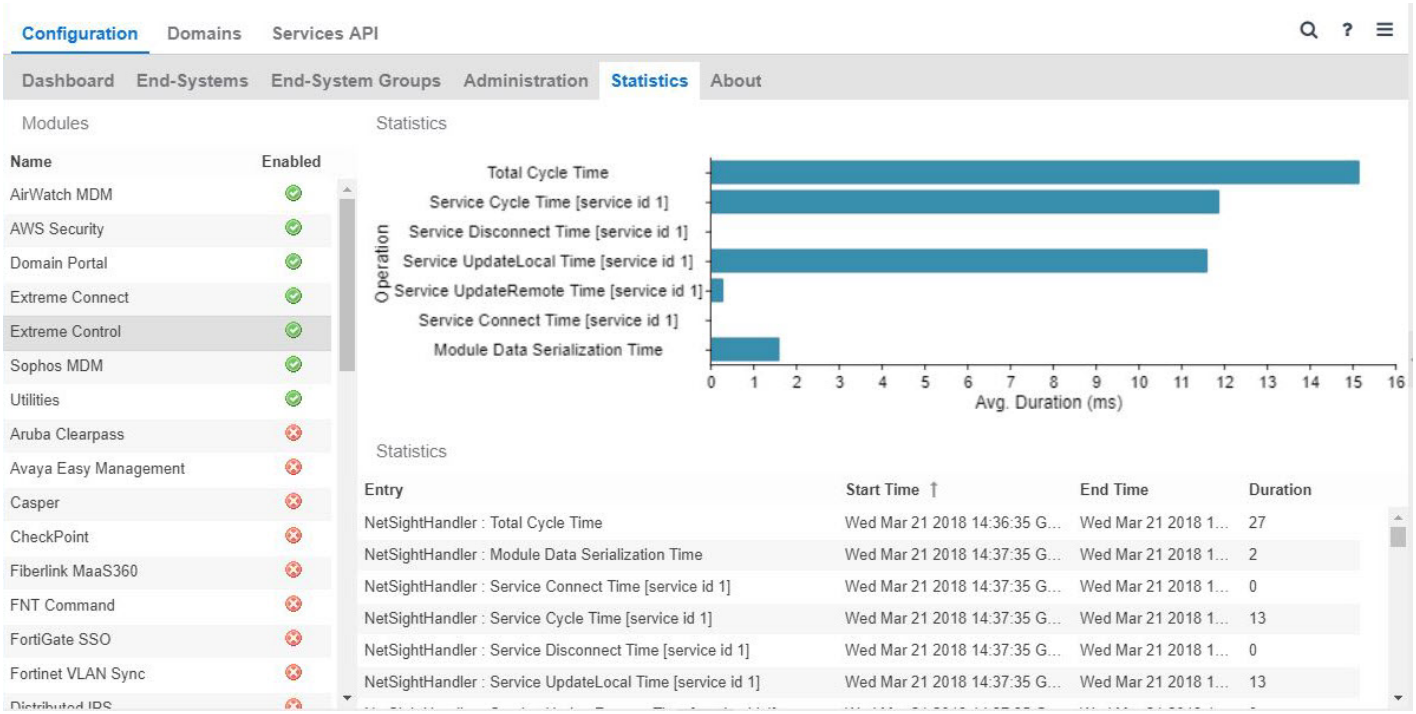
Description
A brief description of the configuration and how it affects Extreme Management Center. This column cannot be edited.

Save
Click the Save button to save your changes to any of the configurations on the tab.

Refresh
Click the Refresh button to update the Configuration tab with any changes you made.

Statistics

Select the Statistics tab to view end-system statistics for each module.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

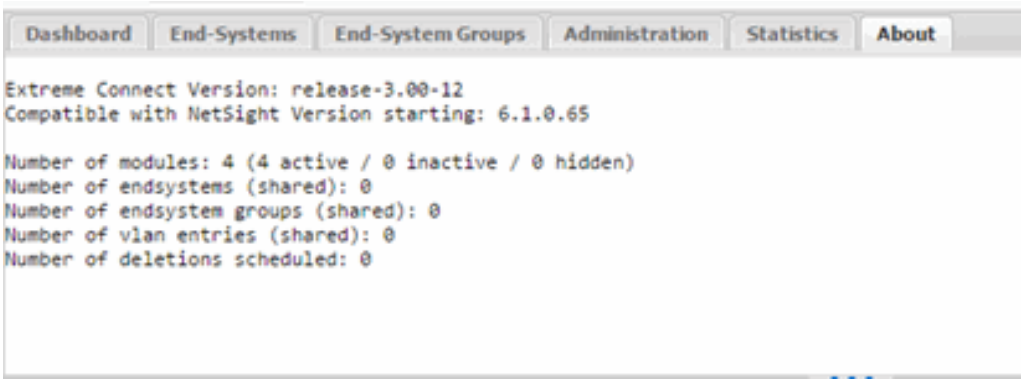
- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel contains a table of the end-system statistics captured by the module and a bar graph displaying an average of the statistical entries contained in the table.

About

The **About** tab contains basic information about your version of Extreme Connect, how it is configured on your network, and information about the end-systems, end-system groups, VLANs, and scheduled deletions Extreme Connect detected on your network.



Related Information

For information on related tabs:

- Extreme Management CenterExtreme Connect Overview
- Domains

Connect Convergence Configuration

Avaya Easy Management

Polycom CMA

Microsoft Lync / Skype For Business

Analytics

Avaya Easy Management

The Avaya Easy Management integration is a one-way integration offering end-system data retrieval from Avaya on phones. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to connect to the Avaya SQL Anywhere 9 DB
Password	Password used to connect to the Avaya SQL Anywhere 9 DB
Avaya DB Server IP	IP Address of the Avaya SQL Anywhere 9 DB Server
Avaya DB Server Port	TCP port of the Avaya SQL Anywhere 9 DB Server

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Avaya DB.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to true, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use for all phones retrieved from Avaya.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for endsystems retrieved from Avaya Easy Management (valid values: 1-4).
Format of the incoming data	Format of the data that gets stored in the custom data field. Syntax: Number: #phoneNumber#; User: #UserDefinedField1#; Hardware: #hardwareVersion#; Software: #swVersion#; Gatekeeper: #currentGatekeeperAddress#; Status: #status# Available Variables: mac, status, ipAddress, currentGatekeeperAddress, phoneNumber, swVersion, hardwareVersion, UserDefinedField1
Use global endsystem groups	This feature allows for the module to use the global endsystem groups of the OneFabric ConnectExtreme Connect.

Verification

To verify proper functioning of the Avaya Easy Management integration, validate that data on Avaya phones has been published within NAC's/OneView's custom field within the end-system list.

Polycom CMA

The Polycom CMA integration is a one-way integration offering end-system data retrieval from Polycom for managed devices. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Required configuration within the Polycom CMA Web Management: navigate to Admin → SNMP Settings and enable SNMPv3:

- Transport: UDP
- Authentication Type: SHA
- Encryption Type: AES 128 Bit

The other values can be customized to your environment. SNMP community and V3 Context Name are not evaluated.

The integration has been tested with Polycom CMA 5.5.0.ER19 but should work with older versions from 5.3.0 upwards. Both CMA 4000/5000 are supported, as well as the complete HDX and VVX 1500 line of end-points. There is no software dependency on the endpoint devices as long as they are monitored by the CMA

Module Configuration

Service Configuration	Description
Server	Polycom CMA Server IP
Password	Password used to connect to the Avaya SQL Anywhere 9 DB
SNMPv3 Security Name	SNMPv3 Security Name
SNMPv3 Auth Passphrase	SNMPv3 Auth Passphrase
SNMPv3 Privacy Passphrase	SNMPv3 Privacy Passphrase

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Polycom CMA.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name to use for all managed devices retrieved from Polycom CMA.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use:	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for endsystems retrieved from Polycom CMA (valid values: 1-4).

Service Specific Configuration	
Format of the incoming data:	Format of the data that gets stored in the custom data field. Syntax: Endpoint ID: #endPointID#, Status: #status#, Type: #type# Available Variables: endPointID, macAddress, status, type

Verification

If you configured a valid NAC end-system group to assign Polycom devices:

1. Verify that the MAC address of your Polycom end-points are now member of that end-system group in NAC.
2. Verify that for each Polycom device the end-point's device type (HDX or VVX) and the end-point's status (offline/online) has been imported.

Microsoft Lync / Skype For Business

The Microsoft Skype for Business (formerly known as Lync) integration offers dynamic call prioritizations and comprehensive reporting capabilities within OneView.

Before installing and configuring the OFConnect integration for MS Skype for Business:

1. Install the Skype for Business SDN API which can be retrieved from Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=44274
2. Make sure to point the Skype for Business SDN management service to your Extreme Management Center server (where Extreme Connect is installed).
3. Read the corresponding solution guide for further details.

Module Configuration

Service Configuration	Description
Skype for Business SDN Management Service IP	IP Address of the Skype for Business SDN management service.

General Module Configuration	
Poll interval in seconds	The time the module will wait during each run. Caution During each run (cycle) the module will perform various steps some of which are putting extra load on the Extreme Management server. It is not recommended to set this value below 600 seconds (=10 minutes). The larger the Extreme Management environment (=number of NAC end-systems, switches, access points, etc.) the higher this value should be. Setting this value too high though (for example: 7200 seconds = 2 hours) will lead to the fact that administrators won't be able to analyze call reports for up to 2 hours before those calls have ended.
Module log-level	Verbosity of the module. Logs are stored in Extreme Management's server.log file.
Module enabled	Whether or not the module is enabled.
Enable Data Persistence	Enabling this option will force the module to store end-system data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	This field is not yet used by this integration so keep set to the default of 1.
NetSight Request Timeout	Timeout in seconds the module waits until it declares a web service call to Extreme Management as timed-out.
Time to wait for a quality update from Skype for Business	When a Skype for Business call finishes Skype for Business sometimes sends a 'QualityUpdate' shortly after the end of the call. We should be able to retrieve call quality information from this message. This timeout value defines the minimum number of seconds the module waits before it declares a call as fully ended (with or without the existence of a QualityUpdate info).
Enable audio call prioritization	Enable this to prioritize audio streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no audio streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the audio flows. Default: true
Enable video call prioritization	Enable this to prioritize video streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no video streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the video flows. Default: true
Enable application sharing call prioritization	Enable this to prioritize application sharing streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no application sharing streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the application sharing flows. Default: true
QoS Profile for audio calls	The name of the QoS profile used on the XOS access switches to prioritize audio calls. This profile must be pre-configured on each access switch manually before using it.
QoS Profile for video calls	The name of the QoS profile used on the XOS access switches to prioritize video calls. This profile must be pre-configured on each access switch manually before using it.

Service Specific Configuration	
QoS Profile for application sharing calls	The name of the QoS profile used on the XOS access switches to prioritize application sharing calls. This profile must be pre-configured on each access switch manually before using it.
DSCP value for audio calls	The DSCP value to apply to audio call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for audio calls. Default: 46
DSCP value for video calls	The DSCP value to apply to video call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for video calls. Default: 36
DSCP value for app sharing calls	The DSCP value to apply to app sharing call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for app sharing calls. Default: 26
Default username for web access to XOS switches	The default username to connect to XOS switches' HTTP(S) interface (xapi). This username is only used if there are no CLI credentials defined for a switch in Extreme Management. Otherwise the Extreme Management CLI username takes priority. This setting is only used if the OpenDaylight option is disabled.
Default password for web access to XOS switches	The default password to connect to XOS switches' HTTP(S) interface (xapi). This password is only used if there are no CLI credentials defined for a switch in Extreme Management. Otherwise the Extreme Management CLI password takes priority. This setting is only used if the OpenDaylight option is disabled.
Hard timeout (in minutes) for Skype for Business calls	The number of minutes after which a Skype for Business call is considered as ended even if no ended notification has been received from Skype for Business in the meantime. If the configured amount of minutes have passed between the start of a call and now this call will be considered ended ⟶ any prioritization will be removed from the infrastructure, the call data will be removed from the in-memory list and reporting data will be created for OneView reporting. This feature handles cases where for some reason the Skype for Business front-end or SDN management servers have been down or communication has been blocked and thus OneFabric Connect didn't receive the 'call ended' notifications for one or more active calls. This setting is only used if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically. Default: 360 (=6 hours).
Use Skype for Business call timestamp instead of local NetSight time	The Skype for Business front-end servers typically report the call start and end timestamps in UTC time - no matter for which timezone each FE server is configured. If this option is set to 'true', these timestamps are used for OneView reporting but also to decide when to end a call (and remove its corresponding prioritizations) using the configured value for "call_hard_ timeout_in_minutes". If you enable this option you need to ensure that your Extreme Management server is also running on UTC timezone otherwise the OneView reports will be off and the hard timeout functionality for call prioritization won't work properly. It is recommended to keep this option set to 'false' -⟶ in this case, the Skype for Business timestamps will be ignored and the local Extreme Management timestamp will be used at the moment the Skype for Business notifications arrive at your Extreme Management server. Default: false.

Service Specific Configuration	
Number of days to store call reporting data	The number of days to store data on Skype for Business calls in the Derby DB. Calls that predate than the configured number of days will automatically be purged from the DB and won't appear in the OneView reports anymore. A higher value will have a negative impact on the overall performance of this module and the OneView reports. Default: 30. Purging is performed every night during the first run of the MSSkype for BusinessSDNHandler module after midnight. So if you set the interval for this module to 600 seconds purging will happen somewhere between midnight and 00:10:00 (0:10 AM).
Enable the cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	Enable this to run an automated cleanup process once per night/week. It will connect to all your XOS switches via Telnet or XAPI (depending on firmware support) and try to identify obsolete Skype for Business-related dynamic ACLs. If found, it will remove those ACLs from all ports and delete the ACLs from the switch afterwards. Set the interval for this process using the next setting cleanUpObsoleteACLsOnXosSwitchesInterval. This setting is only applicable if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically.
Interval for cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	If the feature cleanup_obsolete_acls_from_xos_switches is enabled, use this setting here to define the interval, which will be used for the cleanup routine. Two available options: daily or weekly. The default is weekly.
Enable the clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	Enable this to run an automated clean-up process once per night/week. It will connect to all your EOS switches via Telnet and try to identify obsolete Skype for Business-related policy ACLs. If found, it will delete the ACLs from the switch. Set the interval for this process using the next setting cleanUpObsoleteACLsOnEosSwitchesInterval.
Interval for clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	If the feature cleanup_obsolete_acls_from_eos_switches is enabled, use this setting here to define the interval which will be used for the clean-up routine. Two available options: daily or weekly. The default is weekly.
Gateway Switches	A list of switches that are located at the edge of your network where all external Skype for Business calls pass through. If an external Skype for Business call is detected, a dynamic ACL to prioritize this call's ingressing flow will be created on all switches on this list on their ANY interface. This will enable QoS for external calls as they enter your network at those gateway switches. Ensure that these switches support the required number of dynamic ACLs for the ANY interface. If you don't want to enable this feature simply keep on empty with 127.0.0.1 in the list. If you manually modify this list make sure to keep the "id" values for all entries consistent and unique. Example entry: <gateway_switch_entry desc="Gateway Switch Entry" id="1" type="Entry"> <info>A Gateway Switch Entry</info> <value>127.0.0.1</value> </gateway_switch_entry>
Skype for Business Front-End Server IP addresses	A list of all Skype for Business front-end server IP addresses. If you want to prioritize conference calls but you cannot (or don't want to) enable any end-system tracking mechanism (RADIUS authentication, XOS IDM, OneController plugin) feature on your data center switches where your Skype for Business front-end servers are connected to, provide the list of all your FE server IPs here. When calls from or to your FE servers are seen, they will be prioritized on all gateway switches listed within the feature list "Gateway Switches". Ensure that the list of gateway switches contains all switches where your FE servers are connected. If you don't want to enable this feature simply keep a single entry with IP 127.0.0.1 and ID 1 in the list. If you manually modify this list make sure to keep the "id" values for all entries consistent and unique. This setting is only applicable if the OpenDaylight option is disabled.

Service Specific Configuration	
Use HTTPS for XAPI calls	Enable this to use HTTPS instead of HTTP for any XAPI communication with all XOS switches. If enabled, you will also need to install the SSH mod on all XOS switches and configure "enabled web https". This setting is only applicable if the OpenDaylight option is disabled. Default: false
Use OpenDaylight controller instead of XAPI for call prioritization	Enable this to use an Open Daylight controller to locate Skype for Business call end-points in the network infrastructure and prioritize audio/video calls using OpenFlow. When enabled, you will also need to configure the OpenDaylight server using various settings below. If this is disabled, it will use the Extreme Management API and XAPI on XOS switches to located end-points and prioritize calls. Default: false
IP address of the Open Daylight controller	Management IP of the Open Daylight controller. This configuration only is valid when the option use_opendaylight is set to true.
TCP/HTTP port of the Open Daylight controller	The HTTP port on which the Open Daylight REST API is provided. At the moment, only HTTP is supported. This configuration only is valid when the option use_opendaylight is set to true. Default: 8181.
Username to connect to the Open Daylight controller API	The given user should have admin rights to be able to create new flows and search for host. This configuration only is valid when the option use_ opendaylight is set to true.
Password to connect to the Open Daylight controller API	The password for the given user. This configuration only is valid when the option use_opendaylight is set to true.
Idle timeout for flows created via Open Daylight controller	The idle timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this idle timeout setting. Set this to 0 to disable this feature. Default: 300.
Hard timeout for flows created via Open Daylight controller	The hard timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this hard timeout setting. Set this to 0 to disable this feature. Default: 3600.
Prioritize Wifi Calls	When enabled, it is verified whether the source or destination Lync end-point are connected through an Extreme Identify wireless controller / AP. If that is the case, the corresponding call flow will be prioritized on the switchport where the corresponding Extreme Access Point is connected to. This feature is only available stating with Extreme Management 6.3 and only in Bridged@AP modes. If your wifi topology is Bridged@Controller the call flows will still be prioritized on the corresponding switch access ports but it won't have any effect as the wifi client traffic is transparently tunneled through to the controller and the ACLs/flows/policies configured on the access switch will never match any of those packets. Ensure that LLDP is enabled on both your access switches and all access points. Also ensure that you have enabled device statistics collection for OneView for all access switches where AP's are connected to. Default: true
Prioritize real-time control protocol traffic	Audio and video are typically sent using RTP, which requires two UDP ports, one for the media and one for the control protocol (RTCP). Enable this feature to also prioritize the RTCP traffic/flows. They typcially use the RTP port number reported by the Lync API plus one. So for example, if Lync reports a UDP source port of 5000 for a specific call connection the code will prioritize traffic on both ports 5000 and 5001. Default: false

Verification

In order to verify that the integration is properly assigning dynamic ACLs to prioritize Skype for Business calls in the infrastructure:

1. Start a call between two Skype for Business end-points and keep it running/active
2. Use Telnet or SSH to connect to the switches where these Skype for Business end-points are currently connected (you can use the NAC end-system list to get the switches and ports of your Skype for Business end-points easily)
3. Perform a “show config acl” to list all ACLs currently active on the switch and validate that you see at least one ACL with a name similar to the following syntax: Skype for BusinessSrcA1234567890. The first piece indicates that this ACL has been dynamically created by OFConnect to prioritize a Skype for Business call. The “Src” or “Dst” part indicates whether this ACL is used for the source or destination end-point of a call. The “A” or “V” indicates whether this ACL is used to prioritize the audio or video stream for the Skype for Business call. The rest of the name a part of the call ID retrieved from Skype for Business and thus makes this ACL name unique.
4. If you see two or even four ACL names starting with “Skype for Business…” this would indicate that both Skype for Business end-points are connected to the same switch and/or that this is an audio and video call and both streams get prioritized with unique ACLs.
5. Ensure those ACLs are bound to the correct ingress switch port.
6. In order to verify that the reporting capabilities are working as expected, login to OneView and launch the MS Skype for Business specific report found in the “Reports” tab on the left navigation pain under “VoIP →MS Skype for Business”. If this report is not visible, you might be missing the required xml reporting file.
7. Verify that you do see calls in the first tab of the report and the data seems correct.

Analytics

Reporting

Extreme Connect offers a new set of reports focused around different generalized solution sets like Data Center Management and Mobile Device Management. In addition, end-system data will be propagated in a dedicated custom field across all modules. This field will contain labels to identify

characteristics like “virtual” or “mobile” available to searches across the entire end system table in OneView.

ExtremeConnect Security Configuration

ExtremeXOS Identity Manager

The ExtremeXOS Identity Manager solution provides the network administrator with end-system visibility in Mobile IAM. This visibility will give insight on who, when, and where the user is connected to the network.

Module Configuration

Configuration Parameter	Value
Server	< IP Address(es)of Extreme NAC Appliance(s)> (semi-colon delimited)
Password	< NAC Appliance Shared Secret > (default is ETS_TAG_SHARED_SECRET)
Module Enabled	True

Extreme Management Center NAC Manager Configuration

1. Using a web browser access the Extreme Management Center launch page at the following URL: http://<Extreme Management Center Server IP>:8080
2. Click on “NAC Manager” to launch the NAV Manager application and login using an Extreme Management Center administrator credential.
3. Select the “Switches” tab and click on “Add Switch”.

4. If the ExtremeXOS switch has not previously been added as a device in the Extreme Management Center Console, click on “Add Switch”. Otherwise go to step 8.
5. In the “Add Device” window enter IP address of switch and select a SNMP profile from the drop down list, or create a new profile by selecting “New” if needed. Enter a nickname for the device (optional) then click “OK”.
6. From the device list select the switch and using the drop-down menu, select a primary NAC gateway for the switch, set “Gateway RADIUS Attributes to Send” to “Extreme Netlogin – VLAN ID” and ‘RADIUS Accounting’ to ‘Enabled”. Leave remaining configurations set to their default setting. Click “OK”.
7. Click on the “Enforce All” icon to open the “NAC Appliance Encorce” window.
8. Select the configured NAC Appliance from the list and click “Enforce”.
9. Once enforce is finished click “Close” to close the window
   Note: NAC configurations are used to manage end user connection experience and can control network access based on authentication, time and location. The following section is a basic sample configuration that will authenticate all devices and place them in the same VLAN for devices connected to the switch. Production configuration should be customized based on business needs and security requirements. Refer to Extreme Management Center NAC User’s Guide for additional information on creating custom rules.
10. Select the “Configuration” tab and click on “NAC Configuration: Default”
11. In the “NAC Configuration: Default” window click on the “Add new rule” icon
12. Enter a name for the rule, then using the pull down menu Select “MAC” for Authentication Method.
13. Using the pull down menu Select “New” to create a new location group.
14. In the “Add Location Group” window enter a Name for the location group then click on the “Add Item” icon
15. In the “Add Location Entry” window enter an entry description and select the switch using the selection button . Leave “Interface” to “Any” (all ports), then click OK.
16. Click OK to close the “Add Location Group” window, then click OK to close the “Edit Rule” window.
    Note: The newly created rule will appear in the ordered list of rules. If needed, move the rule up or down the list. Rules will be applied to an end-system based on the first rule it matches.
17. Click OK to close the “NAC Configuration” window.
18. Click on the “Enforce All” icon to open the “NAC Appliance Encorce” window.
19. Select the configured NAC Appliance from the list and click “Enforce”.

ExtremeXOS Configuration

Specific Network Login, IDM related and XML Notification Client configurations are required on the ExtremeXOS switch. Identity Management with ExtremeXOS and Extreme Management Center/NAC use only a subset of ExtremeXOS IDM features. These features including Kerberos and LLDP identity detection. ExtremeXOS FDB, IPARP, IPSecurity DHCP Snooping and Netlogin detection methods are not used.

Note: SSH module must be installed on the ExtremeXOS switch to use the XML notification feature on HTTPS. If the SSH module is not currently installed you must first download and install the separate Extreme Networks SSH software. Once the SSH module is installed, a server certificate should be created that can be used by the HTTPS server.

Refer to Secure Socket Layer section of the ExtremeXOS Concepts Guide for configuration guidelines of the HTTP server and to generate the secure certificate on the ExtremeXOS switch.

RADIUS Netlogin Configuration

1. Set the NAC appliance server as the primary RADIUS server and configure the shared-secret. Shared-secret must match shared-secret configured on the NAC appliance for this device.
    a. configure radius netlogin primary server <NAC IP> client-ip <switch IP address> vr <vr>
    b. configure radius netlogin primary shared-secret <shared secret>
2. Configure Extreme Management Center server as the primary RADIUS server and shared-secret for netlogin. Shared-secret must match shared-secret configured on Extreme Management Center for this device.
    a. configure radius-accounting netlogin primary server <NAC IP> client-ip <switch IP address> vr <vr>
    b. configure radius-accounting netlogin primary shared-secret <shared secret>
3. Enable RADIUS and RADIUS accounting on switch
    a. enable radius netlogin
    b. enable radius-accounting netlogin

Network Login (Netlogin) Configuration

1. Create authentication vlan required for netlogin and configure it the netlogin authentication vlan.
    a. create vlan nvlan
    b. configure netlogin vlan nvlan
2. Enable MAC-based netlogin on the switch and on the edge ports where users and devices will connect.
    a. enable netlogin mac
    b. enable netlogin ports <ports> mac
3. Configure the netlogin port mode for MAC-based vlan. This allows support for devices on the netlogin same port to be assigned to different vlans using MAC-based vlans.
    a. configure netlogin ports <ports> mode mac-based-vlans
4. Configure netlogin to accept and authenticate all client MAC addresses. Only MAC addresses that have a match are sent for authentication and the “default” authenticates all MAC addresses.
    a. configure netlogin add mac-list default

Identity Management Configuration

1. Enable Identity Management on switch and add edge ports where users and end system devices will connect.
    a. enable identity-management
    b. configure identiy-management add ports <ports>
2. Disable the identity-management detection methods that are not used on the edge ports where users and end system devices will connect.
    a. configure identity-management detection off fdb ports <ports>
    b. configure identity-management detection off iparp ports <ports>
    c. configure identity-management detection off ipsecurity ports <ports>
    d. configure identity-management detection off netlogin ports <ports>

LLDP Configuration

Enable LLDP on the edge ports where users and end system devices will connect.

a. enable lldp ports <ports>

XML Notification Configuration

The ExtremeXOS XML Notification feature is used to send IDM events to the Extreme Management Center server.

1. Create and configure a XML notification target.
    a. Create xml-notification target
    b. create xml-notification target Extreme Management Center url https://<Extreme Management Center IP>:8443/fusion_jboss/XosIDM vr <VR>
2. Configure credentials that XML notification will use to access the web services on Extreme Management Center. (After entering the command you will be prompted for password)
    a. configure xml-notification target Extreme Management Center user <Extreme Management Center admin username>
3. Add ExtremeXOS IDM module (idMgr) to the XML notification target in order to receive events from IDM and send them to the configured url (Extreme Management Center server web service)
    a. configure xml-notification target Extreme Management Center add idMgr
4. Enable the XML notification target.

Verification

Verify that the configuration is complete by connecting a domain client or LLDP-enabled device to the switch. The device should be identified by Extreme Management Center MAC manager and displayed End-System view in NAC managers and in Oneview.

Fortinet FortiGate

The Fortinet FortiGate integration provides a single sign-on solution and network access to end-systems by updating the FortiGate local user table and the use of RADIUS accounting.

Module Configuration

Note: FortiGate SSH username and Password must be configured if you want to create users in the FortiGate box.

For the sso-Attribute key, profile is the default value. This field must match with the value set in the FortiGate CLI

FortiGate RADIUS server name: add the value configured for RADIUS server

Configuration Option	Description
Server	FortiGate IP address
Password	FortiGate RADIUS shared secret
SSH Username	FortiGate SSH username
SSH Password	FortiGate SSH password
FortiGate RADIUS Server	FortiGate RADIUS server name, used for username local table
SSO Attribute Key	RADIUS attribute key
Add Class RADIUS Attribute	Option to add SSO attribute key to RADIUS packet
Add User to Local Table	Option to SSH to FortiGate and add username to local table

Extreme Control Configuration

1. Using a web browser access the Extreme Management Center launch page at the following URL:
   http://<Extreme Management Center Server IP>:8080
2. Using the Tools menu, select Management and Configuration → Advanced Configuration→ pull down the NAC Profiles pane.
3. Create a profile you want to match to the firewall to group users.
4. The RADIUS attribute Value references the RADIUS User Group. The group is defined by the NAC Profile.
5. Connect to the FortiGate interface.
6. Select System / Network / interfaces.
7. Select enable Listen for radius accounting messages.
8. In System / config / Features, select Enable End Point Control.
9. Go to User & Device / Authentication / RADIUS Server.
10. Create a new server and add Extreme Control server as RADIUS Server.
11. Enter the IP address and Shared Secret.
12. Check the Include in every user group box.

13. Select Single Sign-on. Add an RSSO_AGENT type RADIUS SSO.
14. Go to Authentication / Single Sign-on and create a new agent.
15. Check on the web interface that the RADIUS Server is configured correctly.
16. Configure RSSO_AGENT through the CLI.
17. For RADIUS attributes expected by the FortiGate box, default values are: (These values should be modified to accord the attribute used by FortiGate Handler)
18. In User & Device / User / User Group, create a User Group.

RADIUS Attribute Value = NAC Profile

To create a policy, go to Policy → Policy → Policy and select your parameters. Create a Policy of subtype User Identity, and add your personal filters.

iBoss Web Security

The iBoss integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership and network location.

Module Configuration

Configuration Options	Description
Server	IP address of the iBoss appliance
Port	iBoss web service port, default is 8015
Password	iBoss authentication key
Delimiter	Delimiter used to specify a location in the Mobile IAM rule name
Max calls	Maximum calls to iBoss appliance per second, default is 5
Max threads	Maximum active processes/calls to the iBoss appliance, default is 8
Strip username	Remove Windows or email domain from the username
Module enabled	True

This section details the steps necessary to install, configure, and test integration between Active Directory, iBoss, and Mobile IAM in a hypothetical K-12 educational environment.

The installer must have technical understanding of the Extreme Networks Mobile IAM solution and the skills required to implement a typical LDAP-integrated deployment of Mobile IAM.

Integration of iBoss and Mobile IAM is accomplished by:

1. Defining needed user groups in Active Directory
2. Defining the various locations requiring differentiated access
3. Configuration of the iBoss appliance
4. Installation and configuration of the Extreme Connect Integration services
5. Configuration of NAC

Defining Groups in Active Directory

When considering an integration project, first determine the various user populations for which you want to define access, and then place those populations into separate AD groups.

Defining Locations

Once you have determined the various end user populations and created/populated the AD groups, next determine what locations require differentiated access for each group.

Listing this location information by user group in a table is most helpful for visualization. Example of listing location by user group in the table below:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

Configuring the iBoss Appliance

There are three areas to configure on the iBoss appliance to integrate with Active Directory and Mobile IAM beyond the standard configuration needed for standard iBoss operation.

Part A – Configure LDAP Settings

1. Open a web browser and go to https://<IP address of appliance> to present the appliance logon screen. Provide the necessary credentials and click the 'Login' button.

2. Select 'LDAP Settings' under Network Settings to configure the Active Directory settings. The LDAP settings page is divided into three sections. The top section contains global settings for the appliance. The default settings should work fine and do not need to be edited.
3. The middle section of this page is where you define the AD domain controller iBoss will use by specifying the LDAP parameters required for communication to that domain controller. Complete this section and then click the 'Add' button to save the server definition.
4. Select 'Done' to save the changes and complete the LDAP configuration.

Part B – Configure AD Plugin

1. Select the 'AD Plugin' screen from the home page.
2. Navigate to the bottom half of the screen where it says 'Registered AD Servers/NAC Agents'. In this screen, add a description of the Extreme Management Center server and its IP address so the iBoss server will listen to updates sent by the NAC servers.
3. The default settings can be used for Filtering Group and subnets unless told differently by support. Once these settings are saved, this section is complete.

Part C – Configure Filters

A filter group is a set of network controls that define what website content categories, programs, QoS settings, and more are allowed or not allowed to pass through the appliance for a given connection. Filter groups are applied to end system traffic on an individual basis.

1. Access the Filter Group definition pageby selecting 'Users' in the navigation menu on the left hand side of the page, then select the 'Groups' submenu link. There are five pages of definitions available for defining filter groups and each page section contains five filter group definitions, for a total of 25 available filter groups.
   Note: Filter group #1 is the default filter group and should remain unchanged.
2. Define a filter group for each AD Group/Location combination by specifying a name for each filter group using the format ADGroupName@Location. The @ symbol acts as a delimiter, so iBoss can separate the AD group name from the location name. The specified group name must be identical to the name of AD group as specified in Active Directory, and the location must be identical to the location name as defined in NAC. Spaces are allowed in both the AD group name and the name of the location.

3. Define the three AD group/location combinations for students. As there are only five filter group definitions on each page, each page of definitions must be saved separately before moving on to the next page.
4. Once you have defined the first five filters, click the 'Save' button at the bottom of the page to save changes. Navigate to the next page of filter group definitions by clicking the arrow to the left of the drop down box at the top of the page.
5. Add the remaining student group/location definition.
6. Once this definition is added be certain to click the 'Save' button at the bottom of the page to save your changes.

Configuration of NAC

The final step in configuring the integration of iBoss and Mobile IAM is to create the location definitions, set up NAC for Active Directory access via LDAP, and configure access rules for each AD group/location combination.

Recall our example table of groups and locations from Defining Locations:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

The first step is to create an LDAP user group in NAC to represent each AD group used for assigning access. Next create locations in NAC to represent the locations listed.

For this exercise we will create three NAC locations: Cafeteria, Gym, and Instructional Areas. We will not need a specific NAC location for everywhere else but instead will create a general rule to assign access for those end systems.

The name of the rule is significant and must be specified using this particular syntax. Name the rule by putting the AD group name this rule refers to on the left side of the "@" symbol, and the location this rule applies to on the right side. Since this rule applies to All Students in the Instructional Areas location, the rule name becomes "All Students@Instructional Areas".

Note: Failure to name your rules in this manner will prevent the integration from working properly.

Next, create the rule for All Students in the Cafeteria and All Students in the Gym using the same syntax.

Note: In all three cases we are assigning the same NAC profile to members of All Students.

Finally, create the two Staff access rules. The rule for All Staff in Instructional Areas follows the same format as the student rules. The final rule is different in how it is named; because there is no specific location information provided, we name the rule using just the name of the AD group itself.

Recall when we configured the filter groups in iBoss that we created a filter group with just the AD group name of All Staff. Because there is no location specified iBoss applies that filter group to any end system registered to AD accounts that are members of All Staff that are not otherwise in a defined location. Naming the rule without the @ symbol or location name tells Extreme Connect to omit the location when making the call to iBoss. Using this naming syntax allows filter groups to be assigned to end systems based solely on AD group membership.

Because this rule is more general than the previous staff access rule, it must be located below the All Staff@Instructional Areas rule in the NAC configuration in order to work correctly.

Verification

1. Using two wireless clients, connect to a test SSID and authenticate using two different accounts.
2. Ensure each account is a member of different active directory groups.
3. Configure two iBoss filtering groups that match the AD groups that each test account are part of.
4. iBoss can display information about the filter groups it assigns to end systems from its web interface. Use both NAC Manager and the iBoss management interface to confirm our integration configuration.
5. Locate both end systems so they connect from the Instructional Areas location. From the Identity and Access tab of OneView we can see that the correct rules have been applied to each end system.
6. To see the corresponding information in iBoss, open the management interface and click on ‘Users’ from the navigation menu on the left hand side of the page, then click the ‘Computers’ submenu item. Our information is listed in the ‘Detected Computers’ section of this page.

Note that both NAC and iBoss list the same end system IP address, filter set name, and AD user name for each end system. This indicates that integration is working and our configuration is correct.

Lightspeed Rocket Web Filter

The Lightspeed integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership.

Module Configuration

Configuration Option	Description
Server	IP address of the Rocket Web Filter appliance
Password	RADIUS Shared Secret
Module Enabled	Enables and Disables Module
RADIUS interim message interval	Send a RADIUS interim message to keep the session active, in minutes
Include Calling-Station-ID	Include the Calling-Station-ID RADIUS attribute, calling station is set to the end system's MAC adding
Include Called-Station-ID	Include the Called-Station-ID RADIUS attribute, called station is set to the switch IP address
Ignore usernames that contain	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
Ignore NAC profiles	Ignore end system's that are assigned a NAC profile, multiple values can be entered with a semi-colon delimiter

Configuring the Rocket Appliance

In addition to the standard configuration of the Rocket Web Filter appliance, steps are required to integrate with Active Directory and Mobile IAM. Only the steps necessary for integration will be covered in this document.

Configure LDAP Settings

1. Log in to the Rocket appliance, https://<IP address of Rocket Appliance>. This presents the appliance login screen. Provide the necessary credentials and click the Login button.
2. Select the Administration menu in the top right corner of the dashboard.
3. Scroll down to the Authentication Sources to configure the Active Directory settings.
4. Select + Add Authentication Source, within this menu to add the required fields.

5. Once the Active Directory server has been saved, verify it is listed in the Authentication Sources section.
6. Select the Test button to verify the Active Directory configuration.
7. Use a known valid domain username and password, click “Test User Login.” A Success message will appear upon a successful query.

Configure RADIUS Accounting

1. The RADIUS Shared Secret is a configurable field within the Rocket appliance.
2. The Shared Secret can be found by accessing the Web Filter menu and scrolling to the bottom of the page.
3. Input the desired Shared Secret to be used between the Lightspeed Systems Rocket Web Filter appliance and the Extreme Connect Lightspeed Systems module. Note the Shared Secret value for later configuration steps.

Configure Policy Management

The next items to configure are the Rule Sets that the Rocket Web Filter appliance assigns to end-systems. Rule Sets are lists of web site categories, keywords, and actions that control how users access the Internet.

1. A pre-defined Rule Set (Block All) is assigned to an Organizational Unit (OU=Solutions Eng,DC=testing,DC=local) that is defined in the previously added Active Directory Server.
2. To access the Policy Management section of the Rocket Appliance, select Web Filter then select Policy Management from the left column.
3. Verify that the Rule Set exists in the Rule Set section of Policy Management.
4. After verifying the Rule Set exists, a new Assignment is created to assign the Rule Set to an object. Navigate to Assignments then select New Assignment.
5. In the New Assignee window, select the Type of object to be used. To browse the Authentication Source, the Search feature can be used to list all OU’s available on the server.
6. Verify the Web Filter Rule in this new assignment at the bottom of the window.

McAfee ePO

The McAfee ePO integration offers end-system assessment via ePO, automatic anti-virus signature file update via ePO and quarantining end-systems via NAC.

NOTE: The McAfee ePO module integration is not supported in Extreme Management Center 8.1.0, but will be supported in version 8.1.1.

Module Configuration

The table below describes the configuration options available for the McAfee ePO OFConnect module
(config file: McAfeeEPOHandler.xml)

Service Configuration	Description
Username	Username used to connect to the ePO API.
Password	Password used to connect to the ePO API.
Server	ePO Server IP
Port	ePO Server Port

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCVMM server.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table. It is recommended to set this option to “true”. You will also need to set this to “true” if you want to populate the username and device type from McAfee in NAC (see additional options below). Default: true.
Default end-system group	The default end-system group name where we assign all McAfee devices to in NAC. If you don't want end-systems from McAfee to be assigned to this default group, configure a group name which doesn't exist in NAC.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use:	The number of the custom data field for each end-system to store the data retrieved from ePO. Available values are: 1, 2, 3 or 4. Default: 1.
Format of the incoming data:	Format of the data that gets stored in the custom data field. You can chose and combine any of the available variables: ipAddress, macAddress, osType, osServicePackVersion, nodeName, userName, datVersion, lastUpdate. But be aware that ePO might update the “lastUpdate” value for each device very regularly and OF Connect is calling Extreme Management Center’s web services to refresh that value in all end-systems custom fields. Depending on your poll interval this might put a lot of stress onto the Extreme Management Center server and it is thus recommended to _NOT_ use this variable here. It should only be used if the poll interval is very low (like once per day) and the number of end-systems isn’t too high (below 1000). Dfault: NodeName=#nodeName#; OS=#osType# (#osServicePackVersion#); User=#userName#; DAT Version=#datVersion#
End-system group for decommissioned devices:	The default end-system group for devices that existed in ePO but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by ePO and that could pose a threat) you can configure the group they should automatically be moved to here and enable the corresponding feature below. Make sure you manually create this end-system group in NAC
Remove device from other groups on decommission:	Enable this to move devices which have been deleted from ePO to the NAC end-system group configured by the corresponding option above. If disabled, devices won't be automatically move to this group but rather stay with their existing group membership(s). Default: false
Delete custom data in Extreme Management Center for decommissioned devices:	If a device is deleted in ePO the end-system's custom data field in Extreme Management Center will be cleared as well. Default: false.
Overwrite the existing username with the one acquired from McAfee ePO:	If set to "true" the username for devices retrieved from ePO will overwrite the username that is already in IAM. If no username could be retrieved from ePO for a given end-system, then no change is performed in IAM. Default: false.
Overwrite the existing device type for devices with the one acquired from McAfee EPO:	If set to "true" the device type (operating system) retrieved from ePO will overwrite the device type that is already in IAM. If no operating system could be retrieved from ePO for a given end-system, then no change is performed in IAM. Default: false.
Max DAT version difference between ePO and client before triggering client update task:	Max DAT version difference between ePO and client before triggering client update task: Setting this value to 0 will disable this feature. Default: 1.
Max DAT version difference between ePO and client before generating a NetSight event	This feature can be used to create NetSight alarms based on these events. These alarms could be configured to alarm the via Email or trigger other mechanisms. Setting this value to 0 will disable this feature. Default: 4.
Max DAT version difference between ePO and client before quarantining client via NAC:	For example: If set to "7" and the difference between the DAT version on ePO's master catalog and the client's DAT version is at least 7 then the value for the corresponding assessment test result will be set to 10 and “HIGH”. You can use your IAM assessment configuration to automatically push those end-systems to a quarantine role if required. Setting this value to 0 will disable this feature. Default: 0.
Name of the ePO client task that OFConnect uses to trigger a DAT version update for individual devices:	Use the exact name as defined in ePO. Ddefine a client task in ePO that will update a client's DAT file (and maybe even more like the agent version, etc.). It will also find any client tasks where the configured name is part of. Default: Update Agent.

Service Specific Configuration	
Time before client update task is aborted by EPO	Number of minutes after which the EPO server should abort the client update task. This value is sent to the EPO server when running the "clienttask.run" web service call as an addtional parameter ("abortAfterMinutes"). Setting this value to 0 disables this feature - the parameter won't be used when making the web service call. Default: 10 minutes.
Max number of client update tasks triggered per client per day	To avoid triggering too many EPO client update tasks you can set this limit to a non-zero value. We will stop triggering EPO client update tasks after the configured maximum number of retries has been reached for the current day. As soon as the next day starts (first run after midnight), the count of retries per MAC address is automatically reset to zero and client update tasks will be triggered again as long as the device is still out of date (see dat_file_max_difference_before_trigger_update_task) or the maximum for that day has been reached again. Setting this value to 0 disables this feature →the code will trigger a client update task on each cycle as long as the device is out of date. Default: 1 update task per client per day
Max number of NetSight events generated per client per day	To avoid generating too many events you can set this limit to a non-zero value. We will stop generating NetSight events after the configured maximum number of retries has been reached for the current day. As soon as the next day starts (first run after midnight), the count of retries per MAC address is automatically reset to zero and events will be generated again as long as the device is still out of date (see dat_file_max_difference_before_generating_netsight_event) or the maximum for that day has been reached again. Setting this value to 0 disables this feature →the code will generate a event on each cycle as long as the device is out of date - no matter how may cycles/triggers per day. Default: 1 event per day
Enable Assessment:	If this is set to “true”, assessment data for all devices managed by ePO will be made available to the assessment adapter. The data will be updated on each cycle. Default: false.
Request an immediate re-assessment of an end-system if its DEVICEOUTOFDATE value changed:	If this is set to “true”, a re-assessment of each end-system where its DEVICEOUTOFDATE value changed (either from "true" to "false" or the other way round) will be requested from IAM. This will ensure that if, for example, an end-system has been pushed to Quarantine since its DAT file version was out-of-date but now it has updated the DAT version, it will immediately be re-assessed and authorized properly. If this feature is disabled, it might take hours/days for the end-system to update its NAC policy/authorization depending on the IAM assessment configuration for this end-system. This feature is only used if the assessment feature is also enabled. Default: true.
Use XAPI to trigger a reauth and thus also a re-assessment of an end-system:	If this is set to true, a re-assessment of an end-system will not be performed via a web service call but rather executed directly on the access switch of the end-system. This will be executed via XAPI so "enable web http(s)" needs to be configured on each XOS switch. This will execute the command 'clear netlogin state mac-address' with the MAC of the end-system to immediately trigger a re-auth. The re-auth then triggers a re-assessment of the end-system which should then immediately change its authorization state from ACCEPT to QUARANTINE or vise versa. This feature is only used if the reassess_endsystem feature is also enabled.
Use HTTPS for XAPI calls:	Enable this to use HTTPS instead of HTTP for any XAPI communication with all XOS switches. If enabled, you will also need to install the SSH mod on all XOS switches and configure "enabled web https". This option is only used if the reauthenticate_endsystem_using_xapi feature is also enabled.
Username to connect to any XOS switch if no CLI credentials are provided within NetSight:	If the feature reauthenticate_endsystem_using_xapi is enabled, the solution will need to authenticate on all XOS switches to perform re-authentication of end-systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management but if there aren't any for a particular switch, then this default value will be used
Password to connect to any XOS switch if no CLI credentials are provided within NetSight:	If the feature reauthenticate_endsystem_using_xapi is enabled, the solution will need to authenticate on all XOS switches to perform re-authentication of end-systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management but if there aren't any for a particular switch, then this default value will be used.
Name of the ePO client task that Connect uses to trigger an agent wake up:	Use the exact name as defined in ePO. Define a client task in ePO that will wake up a client's agent. This is required to Connect to wake up the agent on quarantined end-systems for which a client update task has been triggered. By default, ePO agents only report their DAT version to the ePO server once per hour. Therefore, Connect will only realize that an end-system has updated to the latest DAT Version after quite a long time and thus that end-system might be quarantined for quite a long time. Sending the latest DAT version to the ePO server through an agent wake up task will improve the behavior and get end-systems out of their quarantine state quicker

Service Specific Configuration	
Time before the agent wake up client task is triggered after a quarantine event and update task trigger:	In case an end-system was quarantined by NAC the code is triggering an ePO client update task. This task will try to update the DAT version on the end-system through the ePO agent. This process might take a few minutes. After a successful update, the ePO agent is not immediately reporting the current client DAT version back to the ePO server - it will only report this using its standard poll interval which is typically set to run once per hour. Setting this value to 0 disables this feature. Default: 0.

Verification

Any data (including assessment data) will only be updated during the configured update intervals. Any data retrieved from ePO and any action triggered in direction to Extreme Management Center are handled by the Extreme Control Handler, which has its own update interval and needs to pickup any changes/updates from ePOHandler and push it to Extreme Management Center. Depending on the number of changes/actions during one cycle and the number of end-systems managed, you will need to provide some time before you validate the data in Extreme Management Center.

Data Import to IAM

There are multiple areas to verify when data on all devices managed by ePO is imported to IAM.

The first option is to use OneView's end-system table under the "Identity and Access" tab and display the custom data field which you have configured for the McAfeeEPOHandler. If you enabled the corresponding features you should also see the username retrieved from ePO and a more detailed Device Type also retrieved from ePO.

Another option is to use the general "Search" tab and search for an end-system which is managed by ePO. It should find the end-system and display ePO data as shown below.

Assessment

If it its DAT file is running out-of-date and the corresponding assessment features are enabled, a healthy device did not update to the latest ePO DAT version and is thus running a DAT version which is older than X versions configured in the ePO handler config file. Once Extreme Connect recognizes the outdated DAT file it will populate that fact to the assessment adapter and also try to trigger the corresponding client update script on the EPO server. That update task will only be triggered for end-systems that are in ACCEPT or

QUARANTINE state to avoid trying to update end-systems that are disconnected, rejected or in error state. If IAM triggers an assessment for this end-system before the device could be updated, it will recognize that the device is out-of-date and needs to be quarantined.

At this stage, the device should have a policy (or VLAN) that doesn't allow it to harm other network devices or services but still allows the ePO server to contact and update it.

Once ePO has successfully updated the device and the next OF Connect update cycle has run, the assessment adapter will receive the updated info (from OF Connect) that the device is no longer out-of-date. OF Connect will then immediately trigger a re-assessment within IAM which will lead to re-authorizing the device into its proper policy (VLAN) since the new assessment result showed that the device is compliant and the DAT is not out-of-date anymore.

End-systems which contain the keyword "Server" in their operating system name (as retrieved from EPO) will receive a test score of 6.0 instead of 10.0 for the DEVICEOUTOFDATE test and thus won't be quarantined. This is due to the fact that most customers don't want to quarantine server systems and EPO offers a solution called MOVE which protects virtual servers without applying a DAT file to each server (→DAT version will always be 0 although these systems are protected by EPO).

Handling Deleted ePO Devices

To test this workflow remove/delete a device from ePO and wait for the next OF Connect synchronization. Then verify that:

1. The device's custom field has been emptied (if this feature has been enabled in the config file)
2. The device is now member of the IAM end-system group for decommissioned devices (if this feature has been enabled in the config file)
3. The device does not appear in the end-system list that is displayed at the bottom of the OF Connect management web site (tab: McAfee ePO). This means that the device has been deleted in the internal list as well

Palo Alto Networks

The Palo Alto integration consists of multiple solutions. The user ID solution notifies Palo Alto of IP to username mapping. The distributed IPS solutions

monitor a log file and can take action on an end-system based on the severity of the log message. It is recommended to use the Distributed IPS instead of the Palo Alto Distributed IPS moving forward.

Module Configuration

Configuration Option	Description
Username	Palo Alto username
Password	Palo Alto password
Server	Palo Alto IP address
Version	Palo Alto software version
User-ID (UID) enabled:	Enable user-ID integration
User-ID server:	User-ID agent IP address(es)
User-ID port:	User-ID agent port, default is 5006
User-ID domain:	Default username domain or NAC profile to domain mapping(s)
User-ID concurrent message:	Send concurrent User-ID messages to Palo Alto, this option should be disabled for lower end Palo Altos
User-ID vsys:	Palo Alto vsys to update, default is vsys1
User-ID multi-user message:	Send multiple User-ID mappings in 1 message. It is recommended to enable this option to lessen processing load on the Palo Alto
User-ID multi-user timer:	Time to queue User-ID mappings before sending Palo Alto User-ID message, increasing the timer will increase the number of User-ID mappings
User-ID strip email domain:	Remove email domain from the username
User-ID strip domain name:	Remove Windows domain from the username
User-ID strip domain username delimiter:	Remove all characters after the delimiter in the username
User-ID append to domain username:	Append string to username
User-ID timeout:	Palo Alto User-ID timeout
User-ID ignore usernames that contain:	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
User-ID ignore NAC profiles:	Ignore end system's that are assigned a NAC profile, multiple values can be entered with a semi-colon delimiter
Distributed IPS (DIPS) enabled:	Enable distributed IPS integration
Distributed IPS syslog regular expression:	Regular expression match before action can be taken on an end-system
Distributed IPS syslog file	Syslog file path
Distributed IPS blacklist severity	Severity level needed to blacklist an end-system
Distributed IPS ASM server	ASM server IP address where SNMPv3 informs will be sent to
Distributed IPS ASM username	SNMPv3 username
Distributed IPS ASM password	SNMPv3 password
Distributed IPS SNMP authentication type	SNMPv3 authentication type
Distributed IPS SNMP authentication password	SNMPv3 authentication password
Distributed IPS SNMP privacy type	SNMPv3 privacy type
Distributed IPS SNMP privacy password	SNMPv3 privacy password
Module enabled:	Enable the Palo Alto solution

Distributed IPS

The distributed IPS solution monitors log files for events or opens a port on the Extreme Management server and listens for events. Once an event is received, action can be taken to add the threat to an end system group or notify Automated Security Manager (ASM) to perform a custom action.

Module Configuration

Configuration Option	Description
Name	Event name, this is the default threat name used in the end system group description
Regex	Event regular expression string
File	File, full path, to monitor for events
Port	Port number to open and listen for events on, opening a port may increase vulnerability on the ExtremeManagement server
Protocol	Port number protocol
Sender filter	Process events only from specific IP addresses to prevent spoofing, this field is used in conjunction with the port and protocol
End system group	End system group to add the threat to
End system group type	End system group type, MAC or IP
ASM Server	ASM server IP address where SNMPv3 informs will be sent to
ASM username	SNMPv3 username
ASM password	SNMPv3 password
ASM SNMP authentication type	SNMPv3 authentication type
ASM SNMP authentication password	SNMPv3 authentication password
ASM SNMP privacy type	SNMPv3 privacy type
ASM SNMP privacy password	SNMPv3 privacy password
MAC address regular expression	MAC address regular expression, it is recommended to not change this value
IP address regular expression	IP address regular expression, it is recommended to not change this value
Threat name regular expression	Threat name regular expression, the default regular expression will match a group of words surrounded by double quotes or a group of words without spaces. Example formats that will match the regular expression: “This is a threat 123” This_is_a_threat_123 This-is-a-threat-123 ThisIsAThreat123 This_is_a_Threat(123)

It is recommended to find keywords in the regular expression string and use those keywords as unique identifiers.

The event must contain either the MAC or IP address of the threat. When a MAC address based end system group is used and the threat MAC address is not in

the event, a lookup will be done to resolve the threat's IP address and vice versa for an IP based end system group.

Common wildcards that will be used are:

\w = match a character

\d = match a number

\s = match a space

. = match any character

* = match 0 or more

+ = match 1 or more

Examples of event messages and their regular expression:

Example 1. Checkpoint event message

loc=4220 filename=fw.log fileid=1402093147 time= 6Jun2014 16:01:57 action=block orig=r77 i/f_dir=outbound i/f_name=eth1 has_accounting=0 product=Anti Malware web_client_type=Chrome resource=http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html src=Winsvr2012 s_port=49600 dst=23.203.225.174 service=http proto=tcp session_id=<53924865,00000002,b17361d1,c0000001> Protection name="Check Point - Testing Bot" malware_family=Check Point Confidence Level=5 severity=2 malware_action=Communication with C&C site rule_uid={AE831485-A9C8-4681-BE8F-0E2E66904BDB} Protection Type=URL reputation malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} protection_id=00233CFEE refid=0 log_id=9999 proxy_src_ip=Winsvr2012 scope=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu Suppressed logs=1 sent_bytes=0 received_bytes=0 packet_capture_unique_id=192.168.10.189_maildir_sent_new_time1402095718.mail-4230074710-508316721.localhost packet_capture_time=1402095718 packet_capture_name=src-192.168.10.189.eml UserCheck_incident_uid=80E6C145-7AB6-D2C5-1DC5-A500F1473A70 UserCheck=1 portal_message= Your computer is trying to access a malicious server. It is probably infected by malware. For more information and remediation, please contact your help desk. Click here to report an incorrect classification. Activity: Communication with C&C site URL: http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html Reference: F1473A70 UserCheck_Confirmation_Level=Application frequency=1 days

In the above example, "Check Point - Testing Bot" is the threat name and 192.168.10.189 is the threat IP address.

Regular expression:

Protection name=$threatName malware_family.* packet_capture_name=src-$threatIpAddress

The regular expression contains unique identifiers to avoid ambiguity or incorrect matches. “Protection name=” precedes the threat name and “malware_family” follows the threat name. A wildcard (.*) is used to match against multiple characters after “malware_family.”

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.189, $threatName="Check Point - Testing Bot"}

Example 2. Watchguard event message

Jun 13 13:42:18 10.148.1.254 local1.info Jun 13 13:42:18 QA_LAB_FB 80BE052F336C0 http-proxy[1631]: msg_id="1AFF-0034" Deny 1-Trusted 0-External tcp 192.168.10.180 21.37.51.86 33444 80 msg="ProxyDrop: HTTP APT detected" proxy_act="HTTP-Client.Anti-X" host="fishherder.dyndns.org" path="/tmp/lastline-demo-sample.exe" md5="dd0af53fec2267757cd90d633acd549a" task_ uuid="235ee8f1185e4337986a0a46eb370595" threat_level="high" (HTTP-Proxy-00)

In the above example, “ProxyDrop: HTTP APT detected” is the threat name and 192.168.10.180 is the threat IP address.

Regular expression:

External tcp $threatIpAddress .* msg=$threatName proxy_act

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.180, $threatName="ProxyDrop: HTTP APT detected"}

Example 3. Palo Alto event message

Aug 25 15:51:28 PA-5060-1 -PaloAlto: -threatIpAddress 192.168.10.179 -threatName "Apache Wicket Unspecified XSS Vulnerability(36041)" –severity critical

In the above example, “Apache Wicket Unspecified XSS Vulnerability(36041)” is the threat name and 192.168.10.180 is the threat IP address.

Regular expression:

PaloAlto: -threatIpAddress $threatIpAddress -threatName $threatName

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.179, $threatName="Apache Wicket Unspecified XSS Vulnerability(36041)"}

Check Point User ID

The Check Point user ID integration updates the Check Point gateway with the username IP mapping of end systems that connect to the ExtremeControl appliance(s).

Module Configuration

Module Configuration	Description
Server	Check Point IP address
Password	Check Point shared secret
Ignore usernames that contain	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
Ignore NAC profiles	Ignore end system's that are assigned an ExtremeControl profile, multiple values can be entered with a semi-colon delimiter
Session timeout	API user mapping timeout, in hours

Sample server log output:

```
2017-02-16 12:32:41,937 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Sending -> https://10.224.1.252/_IA_MU_Agent/idasdk/add-identity post
{"shared-secret":"mysharedsecret","requests":[{"ip-address":"192.168.10.181","user":"doe,
john","session-timeout":3600}]}
2017-02-16 12:32:42,278 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Response -> {
"responses" : [
{
"ipv4-address" : "192.168.10.181",
"message" : "Association sent to PDP."
}
]
}
```

Connect Mobility Configuration

AirWatch

Fiberlink MaaS360

JAMF Capser

MobileIron

Sophos Mobile Control

Citrix XenMobile

AirWatch

The AirWatch integration offers provisioning of mobile devices in the network based on device ownership and also provides assessment data within the network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Server Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
AirWatch Server IP	IP or hostname of the MDM server.
AirWatch Webservice URL	Base URL to connect to the API of the service.
AirWatch Tenant Code	API key provided by AirWatch to access a specific customer configuration.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.
Push update to remote service	If this is set to true, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-systemGroup and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	The default end-system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	The default end-system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	The default end-system group for decommissioned mobile devices.
Enable Remote Wipe	If this option is enabled, devices will be wiped if they are moved to the MDM Remote Wipe End-system Group. • off – disabled • enterprise - always perform an enterprise wipe (only deletes corporate data) • adaptive - will perform an enterprise wipe if the device was an employee-owned device and a full wipe if it was a company device • full - always perform a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to “true”, the device will be notified via the selected mode if it is quarantined
Quarantine Notification Text	Message sent in the quarantine notification to the user.
Enable Assessment	If this is set to “true”, assessment data will be made available to the assessment adapter.

Assessment Plugin Map	
Plugin Name	The Plugin ID Name.
Data Field	The AirWatch Data Field being retrieved in this test
Force Reassessment	Force Re-Assessment on content change.

Assessment Plugin Map	
Format of the incoming data	Format of the data that gets stored in the custom data field SYNTAX The end-system is currently #mdmManaged# Available Variables: • id • udid • serialnumber • imei • assetnumber • name • locationgroupid • locationgroupname • username • useremailaddress • ownership • platformid • platform • modelid • model • operatingsystem • lastseen • enrollmentstatus • compromisedstatus • compliancestatus • lastcompliancecheckon • lastcompromisedcheckon • lastenrolledon • macaddress • iscompromised • dataprotectionenabled • blocklevelencryption

Assessment Plugin Map	
	• filelevelencryption • ispasscodepresent • ispasscodecompliant
Update Kerberos username for end-systems	If this is set to "true", the username will be updated for each end-system and a Kerberos re-authentication is triggered.
Update custom fields for end-systems	If this is set to "true", the custom field data will be updated for each end-system.
Update devicetype for end-systems	If this is set to "true", the device type data will be updated for each end-system.

Variables available for custom field string are defined in the AirWatch API documentation.

Note: Look and feel of the MDM interface may change depending on customer's customizations.

Create an API User

Under AirWatch user management, all users and administrator users have access to the web services API. The process below explains how to create a generic user with Full Access:

Note: Any user with role 'API' can access the API; a new user role can be created that only grants access to the API and restricts all other access.

1. From the main Dashboard, select Menu > Accounts > Administrators.
2. From the list of users, click Add > Add User, or edit one of the existing users.
3. Select Basic next to User Type.
4. Provide the user credentials.
5. Add a role, and then click Save.
   The user and password provided in the previous screen must be provided to MDM connect in the corresponding AirWatch plugin configuration file.
6. An additional parameter to obtain for the connectivity with AirWatch´s servers is the Tenant Code. This can be obtained from AirWatch's interface in Configuration > System Settings > System > Advanced > API > REST API:
   The API key is the value that must be provided to the AirWatch module as Tenant Code

Creating a Compliance Profile

The basic variable provided by the Assessment Adaptor is the compliance status. This variable (TestID 100002) contains whether or not the mobile device with that security profile applied is compliant or not with the security requirements specified by the profile.

This variable can be taken as a global indicator of compliance with the security rules of the enterprise. Other variables can be taken into account to provide fine grained access control to the network. From NAC we may decide to use the variable PASSCODEPRESENT (TestID 100028) to verify if a device has defined a password and quarantine devices that don't have a password during the grace period allowed by the security policy.

AirWatch differentiates between Compliance Profiles and Device Profiles. Compliance Profiles define security rules that the device must comply with like:

- Installed applications
- Cellular use
- Encryption
- Version of OS
- Change of SIM

A Device Profile defines a set of configurations that the device must have in order to be considered compliant like:

- Password length
- SSID lists
- Exchange servers
- General restrictions in the device like allowing SIRI, allowing Youtube, Screen Capture, iCloud etc…
- Installed Certificates
- APNs

Some of these can be configured by the MDM itself when the profile is applied; some of them require user intervention and will probably define a grace period until they trigger a security action if the configuration hasn't been performed, e.g. the password change mentioned before.

Device and Compliance Profiles are assigned by device type, location group, ownership, etc.

Example: Define a Compliance Profile for an application.

1. Select Add > Compliance Policy.
   The wizard to create a new policy appears, select application list, the desired operation (contains) and define the name of the application (e.g., verybadapp).
2. Click Next if you have finished, or click + to add more rules to this profile.
3. The next screen will offer several remediation options, like removing or changing the device profile, notifying the user, executing a command, etc. Choose to notify the user cc'ing our systems administrator.
4. Click Next to select the device mapping.
   In the device assignment choose which devices will be checked against this profile. You can choose Platform, Manager, Ownership of the device, etc.
5. Clicking Next will take us to the summary screen.
   Now you have the chance to give a name to the compliance policy and check how many of the currently enrolled devices will pass or fail our test.
6. To enable the policy, click Finish and Activate.

Integrating AirWatch MDM in Mobile IAM's Workflow

Every time a new user is created in AirWatch MDM, the user receives an email or SMS with instructions to register his device

By following the link in the email, the user will be presented with AirWatch's login screen and the possibility to register his or her device in the MDM system.

To integrate this workflow into Extreme Networks Mobile IAM registration workflow, enable registration in Extreme Networks Mobile IAM and link to AirWatch MDM registration page from Mobile IAM captive portal.

Once registration is enabled in Mobile IAM, the administrator can manage the different messages that the user receives during the registration process.

1. Enable web registration in NAC configuration and go to the Portal Options.

2. Select Common Page Settings > change link next to Message Strings.

3. Look for the string 'RegistertoObtainAccess'.

To obtain network access, you must complete the Self Registration form.

We will change that string to contain a string similar to:

```
<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here:
<form action="https://apidev-ds.awmdm.com/DeviceManagement/Enrollment"
method="GET">
<p></p>
GroupID
<select name="AC">
<option value="SE101">SE101</option>
</select>
<p></p>
<input type="submit" name="submit "value="Register your mobile device"></form>
<p></p>
```

This code will create a button that will connect to AirWatch registration page. Make sure that the url (https://apidev-ds.awmdm.com/DeviceManagement/Enrollment) is the same url being used in your deployment.

This code creates a selection for the user to select the location groups he's been assigned in case that there are several to choose.

In the example above, the option is SE101. If there is only one location group in your deployment, you can hide this content with the following code:

```
<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here:
<form action="https://apidev-ds.awmdm.com/DeviceManagement/Enrollment"
method="GET">
<p></p>
<input type=”hidden” name="AC" value="SE101">
<p></p>
<input type="submit" name="submit "value="Register your mobile device"></form>
<p></p>
```

The new look of the mobile registration page is changed to reflect this new code.

In this situation, the user can provide their data in the standard Mobile IAM registration form and register as a guest to the network without control of the MDM. Or they can register the mobile device tapping in the new button and being redirected to AirWatch registration page.

4. When the device has been successfully registered with AirWatch, the Extreme Connect MDM plugin will import its data into Mobile IAM. Devices classified in MDM as Corporate owned will be place in the end-system group 'Mobile Devices Business'

and the devices classified as Personal will be added to the group 'Mobile Devices Personal' (or the group defined to that end during installation or the plugin configuration, see above in installation and post installation tasks).

5. The Mobile IAM ruleset must be adapted to reflect those groups and act accordingly depending on the newly registered devices.

Note: Devices registered by an MDM system may have an important lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the Extreme Connect MDM plugin. Due to the diversity of OSes and connectivity profiles, there is no way to know in advance when a newly registered device will provide all the data needed by the MDM software to complete the registration. It may take up to several minutes from the registration to the final landing in one of the above-mentioned groups and obtaining full access to the network.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with AirWatch servers and via the apple push service with Apple. Android devices require downloading an agent to be registered by AirWatch so Google Play access must be provided as well in this state.

The following policies (or more generic ones) are needed to allow Airwatch registration:

- Allow HTTPS to 12.150.127.0/24 AirWatch network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login

Fiberlink MaaS360

The Fiberlink MaaS360 integration requires Fiberlink authentication credentials and other account settings. This information is used in the Fiberlink MaaS360 module tab.

Module Configuration

Configuration Option	Description
Username	MaaS360 web service username
Password	MaaS360 web service password
API URL	MaaS360 web service URL, use https://services.fiberlink.com unless told otherwise by Fiberlink
Billing/Account ID	MaaS360 billing/account ID

Configuration Option	Description
Application ID	Application ID used to contact MaaS360 web service, use com.networks.extreme unless told otherwise
Application Version	Use 1.0 unless told otherwise
Platform ID	Use 3 unless told otherwise
Access Key	Do not edit this value unless told otherwise
Server	Set value to localhost

Account Billing ID: the account billing ID is used to identify the Fiberlink MaaS360 account. To find the account billing ID, log into the Fiberlink MaaS360 management page.

Service Configuration

Configuration Option	Description
Poll interval	Time period between queries to the MaaS360 web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Verification

1. Enroll new device with MaaS360.
2. Verify device is now being managed by MaaS360.
3. Connect to test SSID, wait for re-synchronization poll to occur, and verify end system in Mobile IAM has device information from MaaS360.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with MaaS360 servers and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by MaaS360 so Google Play and Apple appStore access must be provided as well

in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow MaaS360 registration:

- •Allow HTTPS to MaaS360 network
- •Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- •Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- •Allow HTTPS to 74.125.0.0/16, Google Play Downloads

JAMF Capser

The JAMF Casper integration offers provisioning of mobile devices in the network based on Casper group membership and also provides assessment data within the network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
Server IP	IP or hostname of the MDM server.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
Full Re-Sync Interval	The time after which a full data re-sync will be performed. This will also update data on devices, which are already synchronized.

Service Specific Configuration	
Format of the incoming data for iPhones	Format of the data that gets stored in the custom data field SYNTAX EXAMPLE: OS Version=#osVersion#; Last Inv. Update=#lastInventoryUpdate#; Is Managed=#isManaged#; User=#userName#; Real Name=#realName#; Email=#email# Available Variables: ipAddress, mac, osVersion, lastInventoryUpdate, isManaged, modelDisplay, userName, realName, email, isSecurityDataProtection, isSecurityBlockLevelEncryptionCapable, isSecurityFileLevelEncryptionCapable, isSecurityPasscodePresent, isSecurityPasscodeCompliant, isSecurityPasscodeCompliantWithProfile
Format of the incoming data for computers	Format of the data that gets stored in the custom data field SYNTAX EXAMPLE: OS=#osName# (#osVersion#); User=#userName#; Real Name=#realName#; Email=#email#; Phone=#phone# Available Variables: macAddress, alternateMacAddress, osName, osVersion, ipAddress, userName, realName, email, phone
Default end-system group for all iPhones	The default end-system group name to use if it is not set dynamically for all iPhones.
Default end-system group for all computers	The default end-system group name to use if it is not set dynamically for all computers.
End-system group for decommissioned devices	The default end-system group for decommissioned devices.
Overwrite the existing username for iPhones/iPads with the one acquired from CASPER	If set to "true" the username for iPhones/iPads retrieved from CASPER will overwrite the username that is already in NAC. If no username could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten.
Overwrite the existing username for MACs with the one acquired from CASPER	If set to "true" the username for MACs retrieved from CASPER will overwrite the username that is already in NAC. If no username could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten.
Overwrite the existing device type for iPhones/iPads with the one acquired from CASPER	If set to "true" the device type (iOS) retrieved from CASPER for iPhones/iPads will overwrite the device type which is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.
Overwrite the existing device type for MACs with the one acquired from CASPER	If set to "true" the device type (iOS) retrieved from CASPER for Macs will overwrite the device type that is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.

Service Specific Configuration	
Overwrite the existing device type for Advanced Search computers with the one acquired from CASPER	If set to "true" the device type (operating system) retrieved from CASPER for Advanced Search computers will overwrite the device type which is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.
Import data on iPhones and iPads from CASPER	If set to "true" the module will retrieve data on all iPhones and iPads managed by Casper and push it into NAC. You must set this option to “true” if you want the MDM assessment adapter to work since this data is delivered to the assessment adapter via a file.
Import data on computers (MACs) from CASPER	If set to "true" the module will retrieve data on all MACs managed by Casper and push it into NAC.
Max number of days that the last inventory update for iPhones is allowed to be old	For example: If set to "5" the module will alarm (if assessment is enabled) if an iPhone's last inventory update is older than 5 days.
Write assessment relevant data to an external file or not	If this is set to “true”, assessment data for iPads/iPhones will be made available to the assessment adapter

Assessment Map Entry #	
Plugin Name	The Plugin ID Name
Data Field	The MDM Data Field being retrieved in this test.
Force Reassessment	Force Re-Assessment on content change.

Verification

To verify proper functionality validate the data within the custom field configured to use for the Casper integration in your end-system list (in NAC Manager or OneView). For each iPhone, iPad or MAC you should see information which is retrieved from Casper: If you have enabled the feature to automatically assign Casper devices (iPhones/iPads/MACs) to end-system groups in NAC based on the group name in Casper matching the end-system group name in NAC you can simply verify this functionality by opening one of the groups in OneView and validate whether the correct end-systems (=MAC addresses) are listed there.

As the Casper integration is a one-way integration there is nothing to verify on the Casper server since this integration is neither pushing data to Casper nor modifying any configuration there.

MobileIron

The MobileIron integration offers provisioning of mobile devices in the network based on device ownership and also provides assessment data within the

network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
MobileIron Server IP	IP or hostname of the MDM server.
MobileIron Webservice URL	Base URL to connect to the API of the service.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-systemGroup and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	The default end-system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	The default end-system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	The default end-system group for decommissioned mobile devices.

Service Specific Configuration	
Enable Remote Wipe	If this option is enabled, devices will be wiped if they are moved to the MDM Remote Wipe End-system Group. • off – disabled • enterprise - always perform an enterprise wipe (only deletes corporate data) • adaptive - will perform an enterprise wipe if the device was a employee owned device and a full wipe if it was a company device\ • full - always perform a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to "true", the device will be notified via the selected mode if it is quarantined
Quarantine Notification Text	Message sent in the quarantine notification to the user.
Enable Assessment	If this is set to "true", assessment data will be made available to the assessment adapter.

Assessment Map Entry #	
Plugin Name	The Plugin ID Name.
Data Field	The MDM Data Field being retrieved in this test.
Force Reassessment	Force Re-Assessment on content change.
Format of the incoming data	Format of the data that gets stored in the custom data field SYNTAX The end-system is currently #mdmManaged# Available Variables: Please refer to the MobileIron API Documentation for a full list of all available keywords.
Update Kerberos username for end-systems	If this is set to "true", the username will be updated for each end-system and a Kerberos re-authentication is triggered.
Update custom fields for end-systems	If this is set to "true", the custom field data will be updated for each end-system.
Update devicetype for end-systems	If this is set to true, the device type data will be updated for each end-system.

See MobileIron documentation for keywords available to use in custom field string.

Note: Look and feel of the MDM interface may change depending on customer's customizations.

Creating an API User

MobileIron provides a predefined user role for API access. Assigning the API role to a user automatically enables it to access the MDM API. A user with API access must be created to access MobileIrons API from the Extreme Management Center's interface.

1. From MobileIron's main interface select User Management and Add Local User.

Note: This step is not required if you plan to use an existing user or a user previously synchronized from a LDAP database.

2. Fill in the required fields and note the user ID and password for later use in Extreme Management Center configuration.
3. After creating a user, select it and click Assign Roles.

Once registration is enabled in Mobile IAM, the administrator can manage the different messages that the user receives during the registration process.

1. 1. To perform this configuration, enable web registration in NAC configuration and go to Portal Options.
2. 2. In Portal Options, select Common Page Settings and then click the 'change' link next to Message Strings.
3. 3. Look for the string 'RegistertoObtainAccess'.
   To obtain network access, you must complete registration using the self registration form.
   We will change that string to contain something like:

<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here: <form action="https://<Mobileironserver>/<customername>/ireg" method="GET"><input type="submit" name="submit "value="Register with MobileIron"></form>

This code will create a button that will connect to MobileIron's registration page. Make sure that the url https://<Mobileironserver>/<customername>/ireg is the same being used in your deployment.

4. The new look of the mobile registration page is changed to reflect this new code. In this situation, the user can provide his or her data in the standard Mobile IAM registration form and register as a guest to the network without control of the MDM. Or they can register the mobile device tapping in the new button and being redirected to MobileIron's registration page.
5. After providing the required credentials, the user will be prompted to install a configuration profile granting the MDM software the required permissions to manage the device.
6. After completing the registration, several profiles will be installed under General > Profiles.
   When the device has been successfully registered with MobileIron, the Extreme Connect MDM plugin will import its data into Mobile IAM. Devices classified in MDM as Corporate owned will be place in the end-system group 'Mobile Devices Business'

and the devices classified as Personal will be added to the group 'Mobile Devices Personal' (or the group defined to that end during installation or the plugin configuration, see above in installation o post installation tasks).

7. The Mobile IAM ruleset must be adapted to reflect those groups and act accordingly depending on the newly registered devices.

Note: Devices registered by an MDM system may have an important lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the Extreme Connect MDM plugin. Due to the diversity of OSes and connectivity profiles, there is no way to know in advance when a newly registered device will provide all the data needed by the MDM software to complete the registration. It may take up to several minutes from the registration to the final landing in one of the above-mentioned groups and obtain full access to the network.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with MobileIron servers and via the apple push service with Apple.

Some configurations require downloading an agent to be registered by MobileIron so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow MobileIron registration:

- Allow HTTPS to MobileIron network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Other Integration Options

The integration described in the previous section is one of many possible ways. The different methods will vary depending on specific requirements of the enterprise deploying the MDM-IAM integration.

Sophos Mobile Control

The Sophos Mobile Control integration requires authentication credentials and other account settings. This information is used in the Sophos MDM module tab and supports Mobile Control version 4.0.

Module Configuration

Configuration Option	Description
Customer	Customer name
Username	Web service username
Password	Web service password
Server	Server hostname or IP address. The server value is used to create the web service URL: https:<server>/mdmWebService

Service Configuration

Configuration Option	Description
Poll interval:	Time period between queries to the Sophos web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Verification

1. Enroll new device with Sophos.
2. Connect to test SSID and wait for re-synchronization poll to occur.
3. Verify end system in ExtremeControl has device information from Sophos.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with Sophos server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by Sophos so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow Sophos registration:

- Allow HTTPS to Sophos network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Citrix XenMobile

The XenMobile integration requires authentication credentials and the XenMobile server base URL. This information is used in the XenMobile module tab.

Module Configuration

Configuration Option	Description
Username	Web service username
Password	Web service password
Server	Base URL of XenMobile server. Base URL is used to create the web service URL i.e. <base URL>/xenmobile/api/v1/device/filter

Service Configuration

Configuration Option	Description
Poll interval	Time period between queries to the XenMobile web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Configuration Option	Description
Format of the incoming message	Format of the custom data string. Available fields are: id serialnumber imei username ownership devicename devicemodel devicetype operatingsystem lastseen enrollmentstatus compliancestatus macaddress jailbroken

Verification

1. Enroll new device with XenMobile.
2. Connect to test SSID, wait for re-synchronization poll to occur.
3. Verify end system in ExtremeControl has device information from XenMobile.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with the XenMobile server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by XenMobile so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow XenMobile registration:

- Allow HTTPS to XenMobile network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

ExtremeConnect Management / IT Operations Configuration

FNT Command

The FNT Command integration offers two main functionalities:

1. Mapping of patch panel information from Command to end-systems and switch ports in Extreme Management Center/Control. Data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.
2. Exporting of Extreme Management data to FNT Command: this will export all switches, their modules, ports, GBICs and connected end-systems to Command's ADG database.

Module Configuration

Configuration Option	Description
Username	Username used to connect to the Command Oracle DB
Password	Password used to connect to the Command Oracle DB
ServerIP	IP Address of the Command Oracle DB
Server Port	TCP port of the Command Oracle DB. Default: 6201
Command Service Name	The "SERVICE_NAME" to access the Oracle DB view/table called "MEDMGR.CTFL2D_SWITCH_2_OUTLET". Refer to your Oracle DB administrator to get the service name specific to your FNT Command installation.

General Module Configuration	
Poll interval in seconds	The time (in seconds) the module will wait after each run. Since the data on patch field connections/locations is relatively static it often does not require updating every 60 seconds and it is recommended to increase the value for the poll interval. This will also decrease the processing load on the NetSightExtreme Management Control Center server. Recommendation: 3600 seconds (once per hour) but this depends on the size of your infrastructure and your requirements.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.

General Module Configuration	
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system custom field and group membership data into a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted. It is important to enable this feature, especially in large environments, so that OF Connect doesn’t need a full re-sync of all data everytime you restart your NetSightExtreme Management Control Center server. Default: True.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the data retrieved from Command. Available values are: 1, 2, 3 or 4. Default: 1.
Format of the incoming data	Format of the data that gets stored in the custom data field. You can chose and combine any of the available variables: outletId (ID of the patch field), outletCampus, outletBuilding, outletFloor, outletRoom. Default: #outletId# / #outletCampus# / #outletBuilding# / #outletFloor# / #outletRoom#
Update NAC End-Systems with Command outlet data	If set to True the module will retrieve outlet data (outlet id, room, building, etc.) and map it to the corresponding end-systems/ports in NAC
Command DB table name containing outlet data for NAC import	The name of the Oracle DB table that contains the Command outlet data. This is required if you enable the feature update_nac_endsystems_with_command_ outlet_data so OFC knows which table to query to retrieve data about ports and their outlet data. Default: medmgr.CTFL2D_SWITCH_2_OUTLET
Push NetSight Devices to Command Auto-Discovery Gateway	If set to 'true' the module will push NetSight switch data (IP, firmware, type, descriptor, etc.) to Command's Auto-Discovery Gateway. The module updates the corresponding database tables. The Auto-Discovery Gateway itself manages the import of the data to Command automatically
Push NAC End-Systems to Command Auto-Discovery Gateway	If set to 'true' the module will push all NAC end-systems to Command's Auto-Discovery Gateway. It will then try to "connect" these end-systems to switches and ports exported from NetSight. This option is only available if the option push_ netsight_devices_to_command_adg has also been enabled. The module updates the corresponding database tables. The Auto-Discovery Gateway itself manages the import of the data to Command automatically.
Autodiscovery Gateway DB TCP Port	The TCP port where the Autodiscovery Gateway database is running on. Default: 1521
Autodiscovery Gateway DB Username	The username to connect to the Autodiscovery Gateway database. Default: command
Password	Password used to connect to the Autodiscovery Gateway database. Default: command
The Map to use when exporting NetSight/NAC data to Command's ADG	Specify the map which should be used to export NetSight (switches) and NAC (end-systems) data to ADG. The map needs to be configured correctly in order for ADG to proerply map the incoming device types to existing, well-known device types. Default: 1

Service Specific Configuration	
Automatically process NetSight data pushed to ADG	If set to 'true' the module will automatically call the AutomatedProcessomg.sh script at the end of each synchronization cycle. This will trigger the ADG to immediately import the new data from NetSight. This is currently only supported on ADG Linux installations.
Username to connect to the ADG server via SSH and execute automated processing script	The user name to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. Make sure the user is allowed to remotely login via SSH and has the necessary privileges to execute the script located in your tomcat folder under /webapps/command/axis/WEB-INF. This is only relevant if the option adg_enable_automated_processing has been enabled.
Password to connect to the ADG server via SSH and execute automated processing script	The password to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_ automated_processing has been enabled
Username for the automated processing script (Command user)	The Command user name will be provided as a parameter to the AutomatedProcessing.sh script. Make sure the user has the necessary rights within Command to perform the changes which the script triggers. This is only relevant if the option adg_enable_automated_processing has been enabled.
Password for the automated processing script (Command user)	The Command password will be provided as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_ automated_processing has been enabled.
Tenant (=Mandant) ID for the automated processing script (Command tenant)	The Command tenant (=Mandant) to use for the user provided above. This will be used as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_automated_processing has been enabled.
User group ID for the automated processing script (Command user group name)	The name of the Command user group to use for the user provided above. This will be used as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_automated_processing has been enabled.
Full file path on the ADG server for the script to trigger automated processing	The full file path (path and file name) of the AutomatedProcessing.sh script. This script will be triggered on the ADG server via SSH to automatically start the data import. This is only relevant if the option adg_enable_automated_processing has been enabled. Default: /usr/share/tomcat7/webapps/command/axis/WEB-INF/AutomatedProcessing.sh
Maximum number of end-systems per web service request to NetSightExtreme Control CenterExtreme Management Center	Specify the maximum number (as integer) of end-systems that Fusion will query per request from the NetSightExtreme Control CenterExtreme Management Center server. This setting will allow you to split large end-system queries into smaller badges. Example: There are 10.000 end-systems in NetSightExtreme Control CenterExtreme Management Center/NAC. You set this max_endsystem_ per_request value to 1000. Then Fusion will perform 10 calls to the NetSightExtreme Control CenterExtreme Management Center API and retrieve 1000 end-systems per call. Default: 1000.
Timeout per web service request to NetSightExtreme Control CenterExtreme Management Center	Specify the timeout in seconds (as integer) for each web service call to NetSightExtreme Control CenterExtreme Management Center. Since these calls are handled by the TaskScheduleHandler you need to calculate a value as follows: Take the setting for poll_interval_seconds from your TaskScheduleHandler.xml config file and add a couple of seconds for the expected time it takes for the http transaction to complete. Example: 3 seconds poll interval for the TaskScheduleHandler plus a timeout of 7 seconds for the http request to be performed --> 10 seconds. Default: 10
The ID of the tenant to query Command outlet data for	Specify the Command tenant ID ("Mandant ID") which will be used to filter Command outlet data. This will help reduce the amount of data OFC has to process when importing Command outlet data and matching it to end-systems in NAC. This is only relevant if the option update_nac_endsystems_with_ command_outlet_data has been enabled.

Service Specific Configuration	
Default username for switch CLI access	The default username to connect to any switches' which don't have CLI credentials stored within NetSight. This username is only used if there are no CLI credentials defined for a switch in NetSight. Otherwise the NetSight CLI username takes priority. This is used to gather port optic info from XOS switches using a Telnet connection.
Default password for switch CLI access	The default password to connect to any switches' which don't have CLI credentials stored within NetSight. This password is only used if there are no CLI credentials defined for a switch in NetSight. Otherwise the NetSight CLI password takes priority. This is used to gather port optic info from XOS switches using a Telnet connection.

Verification

1. Login to OneView and verify the incoming data from FNT within the custom data field in the end-system table.
2. Pick a few end-systems and validate that their location data in NAC's custom field is correct according to Command data.

Glue Networks Gluware Control

The Gluware Control integration enables the option to publish Policy Domain configuration to Gluware. The policies are translated into ACL definitions that can be deployed to managed nodes of different manufacturers.

Module Configuration

The table below describes the configuration options available for the Gluware Control module (config file: GlueNetHandler.xml)

Configuration Option	Description
Username	Username used to connect
Password	Password used to connect
Webservice URL	Webservice URL of Gluware Control
Company	Tenant Company Name
Organization	Tenant Organization Name

General Module Configuration	
Poll interval in seconds	The time (in seconds) the module will wait after each run. Since the data on patch field connections/locations is relatively static it often does not require updating every 60 seconds and it is recommended to increase the value for the poll interval here. This will also decrease the processing load on the Extreme Control CenterExtreme Management Center server. Recommendation: 3600 seconds (once per hour) but this depends on the size of your infrastructure and your requirements.

General Module Configuration	
Module loglevel	Verbosity of the module. Logs are stored in Extreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system custom field and group membership data into a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted. It is important to enable this feature, especially in large environments, so that OF Connect doesn't need a full re-sync of all data everytime you restart your Extreme Control CenterExtreme Management Center server. Default: True.

Service Specific Configuration	
Naming Convention	Only policy roles matching the naming convention format will be published (.+ for all)
Provision Switches	Automatically provision switches on enforce
Switches	Name of switch nodes to provision (seperated by ;)

The module will publish every policy domain to Gluware Control that has a matching jboACL object name. (i.e. to publish “Default Policy Domain”, create a new jboACL with the name “Default Policy Domain”).

After the data was published, the description of the ACL will be changed to “Created by Extreme Connect” and contain an Access List for every policy role present in the policy domain.

Note: Support for policy rules depends on the underlying switch hardware. Gluware Control only supports L3-L4 IP policy rules with Accept and Deny actions and only those will be published from the policy domain.

Cisco ACL Support in NAC Manager

In order to use an ACL in conjunction with a RADIUS NAC request, the RADIUS response parameters have to be adjusted for use with Cisco Switches. Certain switch models might require specific licenses to enable per-user ACL and dynamic ACL support. Please refer to the vendor documentation for additional requirements.

When adding a Cisco switch in NAC Manager:

1. Enable the “Gateway RADIUS Attributes to Send” option and select **Edit RADIUS Attribute Settings** from the drop-down menu.

2. Click the Add button to create a new profile and name it “Cisco Wired Dynamic ACL & VLAN ID”. This will send the ACL name and the VLAN ID to the switch upon authorization.
3. Open the Policy Mapping panel in OneView Control > Identity & Access > I&A Configurations > I&AProfiles > Policy Mappings > Default in order to map the policy to the desired VLAN.

Note: The Contain To VLAN action is not supported in IP ACLs and VLAN assignments have to be managed via RADIUS attributes in this case.

4. Continue with the regular NAC configuration steps to assign profiles using rules.

Verification

1. Login to Gluware Control and select Domain Objects > jboAcls.
2. Select the ACL that matches the policy domain in NetSight and verify that the Access Lists match with the policy roles.
3. ACLs are published automatically, but may need to be deployed to switches manually if automatic provisioning is not enabled.

To verify the configuration on a switch:

1. Select Nodes > lanSwitch and connect to the desired switch.
2. In addition to present default ACLs, Gluware will create one ACL matching the Policy Role in name with all rules below it. The rule precedence matches with the default precedence found in Extreme Control.

Microsoft System Center Configuration Manager (SCCM)

The Microsoft SCCM integration is a one-way integration offering end-system data retrieval from SCCM on managed devices. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Note: The SCCM server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the SCCM OFConnect module (config file: SCCMHandler.xml)

Service Configuration	Description
Adapter IP	IP Address of the SCCM adapter
Adapter Port	Port where the SCCM adapter is listening on
Pre-Shared Key	The pre-shared key used to communicate with the SCCM adapter

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCCM server.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name in NAC to assign all MAC addresses found in SCCM. Use a non-existing group name if you don’t want this module to assign all SCCM MAC addresses into any NAC end-system group.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for end-systems retrieved from the adapter running on the SCCM server (valid values: 1-4).
Format of the incoming data	The format of the data which is received from the adapter running on the SCCM server and written to the custom field. Syntax example: Netbios Name=#netbiosName#; User=#lastLogonUserDomain#\#lastLogonUser#; OS=#operatingSystem# (#servicePack#); Manufacturer=#computerManufacturer# Model=#computerModel# Available Variables: path, mac, netbiosName, lastLogonUserDomain, lastLogonUser, operatingSystem, servicePack, computerManufacturer, computerModel
Overwrite the existing username with the one acquired from SCCM	If set to "true" the username retrieved from SCCM will overwrite the username that is already in NAC. If no username could be retrieved from SCCM for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping → this will be overwritten.

Service Specific Configuration	
Overwrite the existing device type with the one acquired from SCCM	If set to "true" the device type (Windows operating system) retrieved from SCCM will overwrite the device type which is already in NAC. If no operating system could be retrieved from SCCM for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping → this will be overwritten. But in most cases this feature should improve your current method (at least for Windows machines managed by SCCM) since the quality of the information retrieved from SCCM is usually very good.

Adapter Installation

Extreme Connect is retrieving data from an SCCM server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter basically consists of a Java executable file (.jar) and a configuration file. There is currently no dedicated installer for the adapter so it's recommended that you follow these steps in order to install the adapter manually:

On the SCCM server:

1. Create a user account which the Extreme Networks adapter should use to access data on the SCCM server.
2. Install the latest Java Runtime Environment.
3. One the SSCM server, create a dedicated folder (example: C:\Program Files\Extreme Networks\SCCM Adapter) and copy the two files: FUSION_SCCM_ADAPTER_ <version>.jar and FUSION_SCCM _ADAPTER.config) into it.
4. Start the adapter by double-clicking the file FUSION_SCCM _ADAPTER.jar or running it within a shell using "java –jar FUSION_SCCM _ADAPTER.jar". AProvide at least the following access rights to this user account:
5. Verify the log file which should have been created in the same folder, where the jar file is located.
6. Make sure that the adapter is automatically started when the Windows Server starts up.

Adapter Configuration

The table below lists the configuration options for the SCCM agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on

Configuration Option	Description
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
SCCM_SERVER	The DNS name of the Configuration Manager server to connect to. So far this has only been tested with this adapter and the SCCM server running on the same server although remote connections might work as well.
SCCM_SITE_CODE	The name of the 'Site' to connect to within Configuration Manager. Example: SCCM_SITE_CODE=mysite
SLEEP_INTERVAL	Set the sleep interval in seconds - the main adapter will update all computer data from SCCM and then sleep for these many seconds before running the next update to retrieve the latest data.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect Hyper-V module
IS_PRE_SHARED_KEY_ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to 'true'. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service

Verification

To verify that the data on Windows-based end-systems could be retrieved from SCCM:

1. Check the custom field within NAC's end-system table and make sure you see info on data like the netbios name, user name, detailed operating system info, etc.
2. If enabled, you will also see a more detailed operating system information within the Device Type column.
3. If enabled, you will also see the last logged on use information within the Username column.

Aruba ClearPass

The Aruba ClearPass integration is a one-way integration offering end-system data retrieval from ClearPass. ClearPass end-systems will be created and updated within Extreme Management Center. That end-system data can then be synced to Extreme Analytics and thus be mapped to flow data (username, device type, policy profile).

Note

Mapping end-system data from ClearPass to flow data within Extreme Analytics requires a correctly configured IP resolution within ClearPass since the mapping is done based on the end-system's IP address.

Module Configuration

The table below describes the configuration options available for the Aruba ClearPass module (config file: ArubaClearpassHandler.xml)

Service Configuration	Description
Server	IP Address of the Aruba ClearPass server
Port	Port of the Aruba ClearPass server API service – usually 443
Access-Token	1. Login to Aruba ClearPass Guest 2. Go to Administration [Symbol] API Services [Symbol] API Clients 3. Click on “Create an API Client” 4. Use these settings: • Enabled: true • Operator Profile: Read-Only Administrator • Grant Type: Client Credentials • Access Token Lifetime: choose a high value (long lifetime) here. Example: 52 weeks 5. Click on “Create API Client” The new client config will be shown in a list – click on that list item and click on “Generate Access Token” [Symbol] copy the HTTP authorization token which is located after the “Bearer” part of the HTTP authorization header. Example: Bearer 01279b5134e633f8df3a36b145657f4f35133f16

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Aruba ClearPass server.
Module loglevel	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name in NAC to assign all MAC addresses found in ClearPass. Use a non-existing group name if you don’t want this module to assign all ClearPass MAC addresses into any NAC end-system group.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from ClearPass (valid values: 1-4).
Format of the incoming data	Format of the data that gets stored in the custom data field: Syntax example: user=#user#, domain=#domain#, online=#online#, updatedAt=#updatedAt#, roles=#roles# Available variables from Aruba Clearpass: ipAddress, user, domain, spt, deviceCategory, deviceFamily,deviceName, online, updatedAt, roles
HTTP socket timeout in seconds (Clearpass API)	HTTP socket timeout in seconds for all HTTP connection sockets to the Clearpass API. Will allow the http client to timeout the established connection if there is no response from the ClearPass server after the configure amount of seconds
Enable device type overwrite	Enable this to use the device family/type retrieved from ClearPass to overwrite the device family/type in Extreme Access Control
End-system group for decommissioned Clearpass end-points	If an end-point gets deleted from Clearpass its corresponding end-system will be pushed to this end-system group
Remove end-systems from other groups on decommission	Enable this to remove a device from all other groups when it is moved to the decommission group
Delete custom data in XMC for decommissioned devices	If an end-point gets deleted from Clearpass the corresponding end-system's custom data field in XMC will be cleared
XMC Server	Hostname or IP of the XMC server. Needed to import Clearpass end-points.
XMC Port	HTTPS port of the XMC service. Default: 8443
XMC Username	Username to connect to the XMC server.
XMC Password	Password to connect to the XMC server.

Configure NAC + Analytics Integration

Ensure to enable the feature that exchanges EAC data with flow data:

Verification

The end-system data from ClearPass will be visible within the XMC end-system list and the Analytics flow data.

Within the end-system table you should see data on all ClearPass end-systems within the configured custom field:

Plus usernames and device types if available through ClearPass.

As soon as the user and device type fields for ClearPass sourced end-systems have been updated within XMC you should start seeing that information within the Analytics “Application Flows” tab as well:

Extreme Management Center Fields Updated

The following end-system table fields in Extreme Management Center are updated by the Aruba Clearpass integration:

- ipAddress
- user
- domain
- spt
- deviceCategory
- deviceFamily
- deviceName
- online
- updatedAt
- roles

Mobile Device Management (MDM) System Configuration

In order to be used by Extreme Networks MDM Connector plugin, the MDM software must be configured to provide the data that is imported by IAM as assessment information or end-system data.

End-System Groups

After initial installation the following groups should be present in IAM:

Group for Managed Business Mobile Devices	Managed Mobile Devices Business
Group for Managed Personal Mobile Devices	Managed Mobile Devices Personal
Group for Decommissioned Mobile Devices	Managed Mobile Devices Decommissioned

We have shown the default names for each group. These names can be changed during installation or in the configuration page.

In addition to these a fourth group will appear for the ‘wipe’ functionality:

End-system group for Managed Devices Wipe	Managed Mobile Devices Wipe

These groups contain the inventory information coming from the MDM provider. End-systems will be classified in each group depending on the ownership information from the MDM provider.

The ‘decomissioned’ group is a placeholder for devices that have been unenrolled in the MDM provider. Typically, its treatment should be the same as unregistered users.

The ‘Wipe’ group is an exception to this rule, the group is only used to trigger a wipe notification to the MDM provider. The wipe signal will reset the configuration of the ensystem to its factory settings. This option is disabled by default.

Related Information

For information on related tabs:

Extreme Management Center Extreme Connect Overview

ExtremeConnect Assessment Configuration

The Extreme Connect Assessment Configuration includes Assessment Map Entries and the Assessment Adapter, which provide you with health tests and results for your Connect modules.

This Help topic provides information on the following:

Assessment MAP Entries

All modules except McAfee EMM currently use the assessment adapter to report health results to Extreme Management Center. The assessment adapter creates 30 new assessment tests or PluginIDs to use by NAC. Each test is reported to NAC by a pluginID created as follows:

- base value = 100.000
- plugin id = base value + ENUM ID (i.e. OWNERSHIP -> 100.000 + 22 = 100.022)

The following is the complete list of tests and IDs:

- EXISTS(1)
- COMPLIANT(2)
- JAILBROKEN(3)
- AUTHORIZED(4)
- WIPED(5)
- UNINSTALLED(6)
- COMPROMISED(7)
- OSOUTOFDATE(8)
- POLICYOUTOFDATE(9)
- DEVICEOUTOFDATE(10)
- BLOCKED(11)
- INFECTED(12)
- LOST(13)
- RETIRED(14)
- UDID(15)
- SERIALNUMBER(16)
- IMEI(17)
- ASSETNUMBER(18)
- NAME(19)
- LOCATION(20)
- USER(21)
- OWNERSHIP(22)
- PLATFORM(23)
- MODEL(24)
- OSVERSION(25)
- PHONENUMBER(26)
- LASTSEEN(27)
- PASSCODEPRESENT(28)
- PASSCODECOMPLIANT(29)
- DATAENCRYPTION(30)

You can map each test to different variables in each MDM connector.

In JAMF Casper module's default configuration, the test EXISTS (pluginID 100001) is mapped to the value of the variable 'managed' in JAMF Casper's database.

NAC Manager can assign risk values and scores to each test using their pluginID. This is needed in order to quarantine devices based on their risk level.

Assessment Adapter

The assessment adapter infrastructure reports health results from Extreme Connect modules to NAC, if available. The assessment adapter is launched with either Linux or Windows:

- Linux:

  <Extreme Management CenterRootdir>/jboss/server/default/deploy/fusion_jboss.war/assessment/launchAS.sh

- Windows:

  <Extreme Management CenterRootdir>\jboss\server\default\deploy\fusion_jboss.war\assessment\launchAS.cmd

McAfee EMM uses a separate assessment plugin to gather data from the server and report it as health results to the Extreme Management Center server. This path points to the location of the MDMAdapter.jar that must be in:

- Linux:

  <Extreme Management CenterRootdir>/jboss/server/default/deploy/fusion_jboss.war/assessment/launchAS.sh

- Windows:

  <Extreme Management CenterRootdir>\jboss\server\default\deploy\fusion_jboss.war\assessment\

Before the assessment adapter can be used in NAC manager, it has to be created as a valid assessment server.

1. From the assessment configuration (1) select assessment servers (2) and click add (3) to add a new assessment server.
2. In the new server dialog, provide the required data.
    - Assessment Server IP: IP address of the Extreme Management Center server.
    - Assessment Server Name: a Name for easily identify our server.
    - Assessment Server Port: if launched with the launchAS commands, the agent runs on server 8448.
    - Assessment Server Type: FusionAssessmentAgent
    - Max Concurrent Scans: leave empty. This can be used afterwards to increase the capacity of the server. By default the server allows 10 concurrent scans.

    In order to use this server for assessment purposes, the server must be in an assessment pool and the assessment pool must be used by an assessment configuration.
3. Create a scoring override for one or more of these test cases to quarantine end-systems in case they match a certain result string within their description field.
4. If you want to quarantine all iPads with an iOS version of 5.x, make sure you have enabled “Use Quarantine Policy” in the corresponding NAC profile and that the corresponding policy on the WLAN controller has a redirect configured within that policy that points to the NAC captive portal.
5. Enable “Assisted Remediation” within the NAC configuration in order for NAC to display the remediation/self-help page.
6. Customize your remediation portal if needed. For example, you can add a remediation link that allows users to register their devices on the MDM portal.
7. Another customization that is recommended is to define the Custom Remediation Actions to improve the user experience with the help texts on the remediation page.

Connect Configuration Troubleshooting

Troubleshooting VMware vSphere Configuration

Troubleshooting Citrix XenServer Configuration with Connect

Troubleshooting Adapters for XenDesktop, Hyper-V, SCVMM and SCCM Configuration

Troubleshooting Citrix XenDesktop Configuration with Connect

Troubleshooting Microsoft Hyper-V and Virtual Machine Manager Configuration with Connect

Extreme Management Center is not responding.

Restart the Extreme Management Center services. Change directory (cd) to /usr/local/Extreme_Networks/Extreme Management Center/scripts.

```
cd /usr/local/Extreme_Networks/Extreme Management Center/scripts
stop Extreme Management Center service by typing:
./stopserver.sh
```

Wait for the prompt and then start Extreme Management Center service by typing:

```
./startserver.sh
```

Is there a log file and where do I find it?

Extreme Connect logs within the JBoss context of the Extreme Management Center server. You may find the server.log file either in the ../appdata/logs/ folder or simply by opening the server log from any Extreme Management Center Client.

What loglevels are available and how do I change them?

Every module of Extreme Connect, including the main application itself have individual loglevel settings in their respective configuration file. The default level should be ERROR and it is strongly suggested to keep it at this level, except for troubleshooting issues. The loglevels are (from least to most talkative):

- ERROR
- WARN
- INFO
- DEBUG

I am getting a lot of errors and would like to turn logging completely off for a certain module.

In addition to the four loglevels used by all modules, Log4J also supports the FATAL loglevel which is currently not used by any module without Extreme

Connect. In order to set a module to use this loglevel, the configuration file has to be edited manually as this option is not provided on the web page to avoid shutting down logging by mistake.

Some modules stop working after some time and report in the log that too many errors happened.

Each module is monitored by the main Extreme Connect process regarding errors that happen during each run cycle (i.e. authentication errors). If a module produces more than 10 failures in a row, the module will be disabled to prevent any further errors. In order to restart a module, try to identify the problem source (i.e. remote server is not responding), remedy it and update the module configuration file. As soon as the timestamp of the configuration file is changed, the configuration will be reloaded and the failure counter is reset to zero until further failures happen. The counter will also be reset, if at least one successful cycle was completed in the meantime.

The logs always note local/remote data storages. What are these?

Extreme Connect logs are always written from the Extreme Connect perspective. Local means the Extreme Connect service and remote relates to another service contacted (i.e. Extreme Control, VMware,...). Each module has its own datastore in order to track changes and update local or remote data. Therefore, if certain information for an end-system is missing from a specific module, it is always a good start to look at the datastore and log for that particular module.

What happens to a module if an error occurs?

The error is logged and the run cycle for the module will go on or end, depending on the severity of the error. If an error should crash a module, a full stack trace will be logged and the module is terminated until the JBoss service has been restarted. All other modules are not affected by this and will continue running, even if they should not receive any further updates from other modules.

After JBoss has started, I don't see any data being updated for some minutes. Is there something wrong?

No, Extreme Connect will first start all modules and wait a bit to verify that everything is running correctly. After that, the modules will enter their run cycle and start retrieving data from various sources. Depending on the delay until the information is retrieved and the interval times of each module, this might take up to a couple of minutes.

Troubleshooting VMware vSphere Configuration with Connect

Do I have to create a dedicated user for Extreme Connect to access the vSphere webservice?

No, but it is recommended to do so as it will allow you to filter events and tasks more easily within the VMware Client.

What are the least permission requirements for the webservice user?

The account should have at least all necessary permissions to:

- register the Extreme Management Center Plugin Extension

- write data to VM annotation fields

- read data from VM configurations (MAC, Network)

Although Extreme Connect seems to be running fine, I only see “n/a” in the annotation fields and no records via the Extreme Connect plugin. Why is that?

Most likely, none of the MAC addresses of the VM is listed in the end-system table of the NAC Manager. Make sure that authentication (at least MAC Auth) is set up properly on the physical switch and that the VM is actually sending some traffic.

How often will Extreme Connect update the information within vSphere (annotations, switches…etc.)?

Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the annotation field and it is generally recommended not to use variables like LastSeenTime in the annotation text, which will change very frequently and have a lot of updates as a result.

Is there any way to get rid of the event/task logs for every update that Extreme Connect performs within vSphere?

No. This functionality is handled by vSphere itself and Extreme Connect has no means to stop it. vSphere offers a filtering mechanism that can be used to limit the information shown and help to find specific data more efficiently.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect retrieves the name of the virtual network/portgroup in its default configuration and uses the part before the first underscore as the end-system group name. This corresponds to the naming convention used if Extreme Connect is automatically creating portgroups from end-system groups. The format used there is always:

endSystemGroup_virtualSwitchName

The reason for this is the requirement within vSphere that two portgroups on the same host may not share the same name. Therefore, the (d)vSwitch name is appended to the end-system group name with an underscore. This also ensures that vMotion is possible for VMs on two hosts which also require that both portgroups on those hosts have the same name.

Is it possible to let Extreme Connect create portgroups automatically, but to let the VM administrator handle VLAN configurations?

Yes, the configuration offers an option to turn off VLAN creation/updates.

What happens if VLAN updates are enabled and a VM administrator changes the settings of a portgroup?

Extreme Connect will update the settings using the local configuration data. It will not delete and recreate the portgroup, but simply update the existing configuration.

What happens if an end-system group is deleted and the portgroup deletion option is enabled?

Extreme Connect will move all VMs attached to that portgroup/network to the “VM Disconnected Systems” group and then delete the original portgroup/network.

If a portgroup has been deleted by Extreme Connect, can another portgroup with the same name be created manually within vSphere afterwards?

Using its local data store, Extreme Connect will put the name of the end-system group onto a special “deletion” stack. During each run cycle, every module will check the stack and remove all portgroups that use the same name until the deletion interval timer runs out. This value is set to 2 minutes per default. After those 2 minutes have passed, a VM administrator can safely create a portgroup of the same name without risking it being deleted.

Although portgroup deletion is enabled, groups are not getting deleted by Extreme Connect. What is the reason for that?

Extreme Connect will delete all groups as long as the group is on the deletion stack and the entry has not timed out. If too much time is required for each run through, try increasing the deletion interval timer so that the module has a better chance of performing the operation.

Troubleshooting Citrix XenServer Configuration with Connect

Do I have to create a dedicated user for Extreme Connect to access the XEN Server webservice?

No, you can use the root account on the XEN Server.

What are the least permission requirements for the webservice user?

The account should have at least all necessary permissions to:

- write data to VM description fields
- read data from VM configurations (MAC, Network)

How often will Extreme Connect update the information within XenCenter (descriptions, networks...etc.)?

Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the description field and it is generally recommended not to use variables like LastSeenTime in the annotation text, which will change very frequently and have a lot of updates as a result.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect creates XEN networks with the exact same name as the corresponding Extreme Management Center end-system group. Extreme Connect then checks all XEN networks it manages and the VMs which are assigned to them. The MAC's of these VMs will then be added to the corresponding end-system group in Extreme Management Center.

Is it possible to let Extreme Connect create networks automatically, but to let the VM administrator handle VLAN configurations?

No, this feature is currently only supported for VMware, not for XEN.

What happens if a XEN administrator changes the settings of a network (VLAN ID, NIC)?

Extreme Connect will update the settings using the local configuration data. For this to take place, all VMs connected to the network will temporarily be disconnected from this network. Then the network will be reconfigured and finally all VMs priory connected to this network will be reconnected.

What happens if an end-system group is deleted and the network deletion option is enabled?

Extreme Connect will move all VMs attached to that network to the "VM Disconnected Systems" network and then delete the original network.

If a network has been deleted by Extreme Connect, can another network with the same name be created manually within XenCenter afterwards?

Using its local data store, Extreme Connect will put the name of the end-system group onto a special "deletion" stack. During each run cycle, every module will check the stack and remove all networks that use the same name until the deletion interval timer runs out. This value is set to 2 minutes per default. After those 2 minutes have passed, a XEN administrator can safely create a network of the same name without risking it being deleted.

I've set an end-system group's description to "sync=true vlan=100" but in XEN only an internal network is being created – not an external one with the corresponding VLAN ID - why?

In order for Extreme Connect to create an external network within XEN two settings are necessary: VLAN ID and physical NIC to connect the external network to.

I've set an end-system group's description to "sync=true nic=eth1" but in XEN only an internal network is being created – not an external one attached to nic eth1 without a VLAN ID - why?

In order for Extreme Connect to create an external network within XEN two settings are necessary: VLAN ID and physical NIC to connect the external network to. It is not possible to create an external XEN network without assigning a VLAN ID (all external XEN networks are tagged).

Troubleshooting Adapters for XenDesktop, Hyper-V, SCVMM and SCCM Configuration with Connect

What is the adapter doing and how?

The adapter is creating a Web Service bound to the IP and port that configure within the configuration file. OneFabric ConnectExtreme Connect is then making web service calls to this adapter to retrieve data on managed end-systems (VMs, Windows devices, etc.) and (depending on which integration is used) also update data on the remote server (for example: update description fields for VMs).

What ports are needed to communicate between the OneFabric ConnectExtreme Connect and the adapter?

Only one port is required and this is the one configured on the adapter side within its configuration file.

Is the communication secure?

All data sent and retrieved from/to the adapter is encrypted using the pre-shared key which the admin defines when setting up the adapter and installing OneFabric ConnectExtreme Connect. The key itself is then automatically encrypted.

No information is synchronized – what else can I check?

Check the adapter's logfile. It will show you when the adapter has been "called" by OneFabric ConnectExtreme Connect, what powershell commands it tries to execute and what the return values of these commands were. You need to set the log level to "DEBUG" and restart the adapter in order for this to print detailed logging information.

How can I check whether the adapter's web service is working and reachable?

Depending on whether your NetSightExtreme Control CenterExtreme Management Center server is installed on a Windows server or on a Linux-based appliance you can use a standard browser or a Linux tool like wget to request one of the following web URLs (depending on the integration (adapter) you are trying to troubleshoot):

- XenDesktop: http://<IPofAdpater>:<PortOfAdapter>/DCM_XENDESKTOP_ADAPTER
- Hyper-V: http://<IPofAdpater>:<PortOfAdapter>/DCM_HYPERV_ADAPTER

- SCVMM: http://<IPofAdpater>:<PortOfAdapter>/DCM_SCVMM_ADAPTER
- SCCM: http://<IPofAdpater>:<PortOfAdapter>/FUSION_SCCM_ADAPTER

If you get a browser error that it cannot connect or the page is not existing you either have an issue with a firewall along the communication path or the adapter's web service did not start properly on the configured IP and port. Also make sure that the configured port for the adapter is not yet used by another service on your Microsoft server.

Troubleshooting Citrix XenDesktop Configuration with Connect

Why do the usernames within Extreme Management Center NAC Manager appear as "Kerberos" usernames?

The XenDesktop adapter uses the same webservice call as the Kerberos snooping process. For the system's functionality this makes no difference: you can create user groups, rules and profiles based on these usernames.

After some time the usernames are deleted or disappear in NAC Manager - why?

1. The corresponding XenDesktop session has ended. In this case, the adapter resets the username on the corresponding end-system VM which will also trigger any existing rule / NAC profile changes.
2. The Kerberos aging timer was triggered. Within NAC Manager you can configure a period after which the Kerberos usernames will automatically age out. If you don't want this timer to interfere with the XenDesktop adapter functionality make sure to set a very high value or disable this feature.

Although some users have disconnected from their XenDesktop session the usernames are still active within NAC Manager - why?

XenDesktop distinguishes between a closed/non-existing session and a disconnected one. A session is first active, then disconnected and then deleted. As long as the session is in the disconnected state, the adapter still doesn't reset the username within Extreme Management Center. In case the user re-activates his/her session, there is no need for the adapter to set the username and the corresponding user-profile is already active within NAC.

Troubleshooting Microsoft Hyper-V and Virtual Machine Manager Configuration with Connect

How often will Extreme Connect update the information within the notes field?

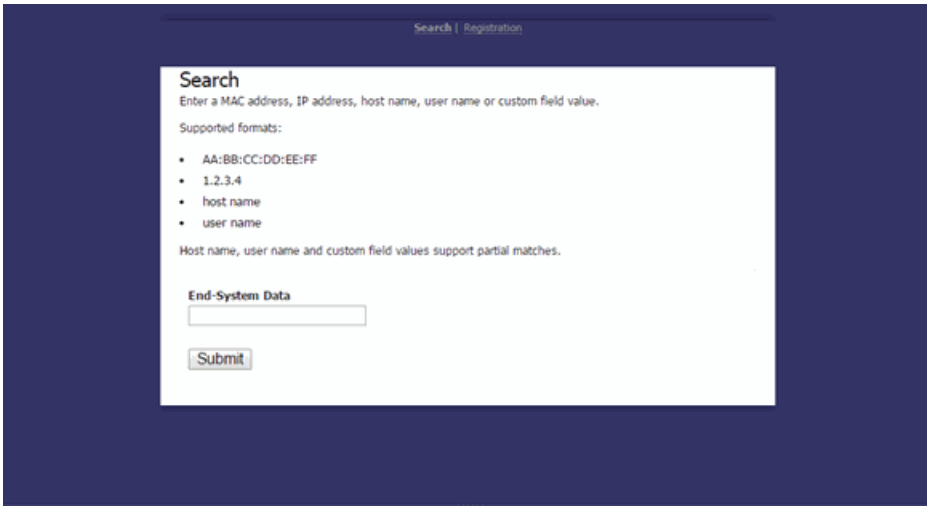
Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the notes field and it is generally recommended not to use variables like LastSeenTime in the notes text, which will change very frequently and have a lot of updates as a result.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect reads the virtual networks (virtual switches) each VM belongs to and puts its MAC address into the corresponding end-system group in Extreme Management Center. For this feature to work, end-system groups with the exact same name as the virtual networks from Hyper-V must exist within Extreme Management Center and the description field must contain “sync=true”.

Connect Domains

The Domains tab allows you to search for a particular end-system in all of the network monitoring modules on your network across multiple instances of Extreme Management Center based on a variety of criteria. In addition, you can configure user membership in end-system groups based on MAC address, allowing you to quickly authorize end-systems in your Extreme Access Control solution to allow network access across all modules.

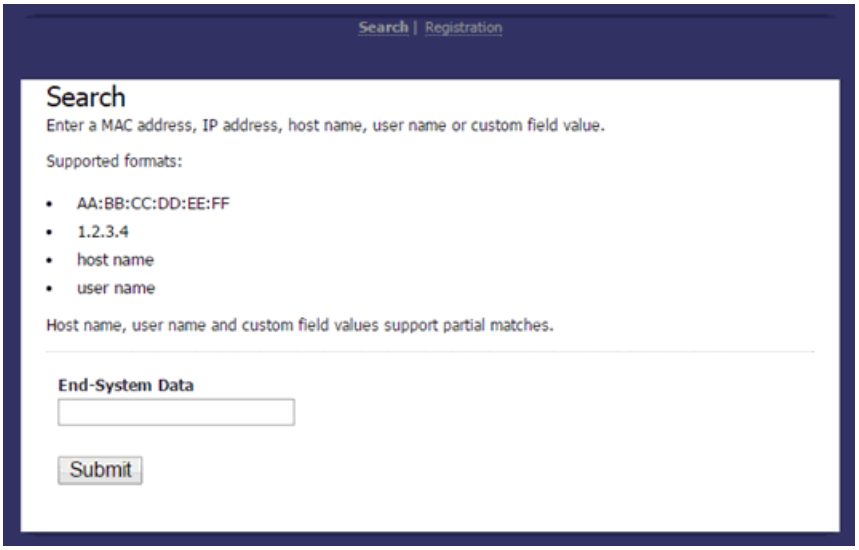


The Domains tab contains two sub-tabs:

- Search — Allows you to search for an end-system across multiple versions of Extreme Management Center in all modules using the following criteria:
  - MAC address
  - IP address
  - Hostname
  - Username
  - Custom Field (user-defined value)
- Registration — Allows you to add a MAC address to an end-system group or remove existing MAC addresses from an end-system group. These end-system groups can then be used to allow or deny access in all modules.

Search

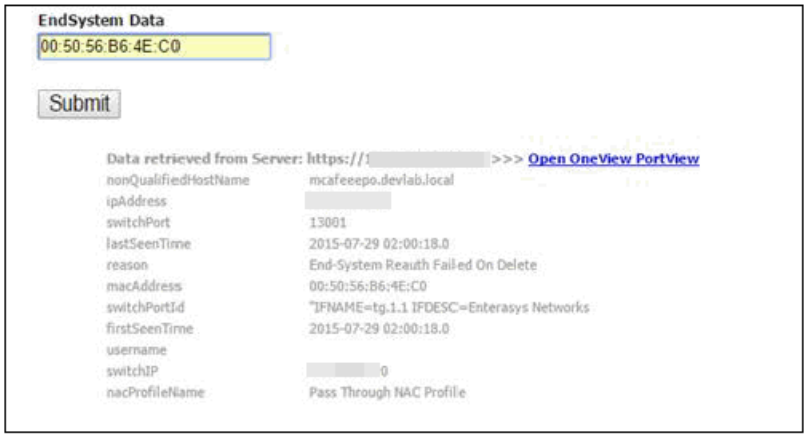
The Search tab allows you to search for a particular end-system in all of your supported network monitoring and network control modules in all versions of Extreme Management Center on your network.



End-System Data

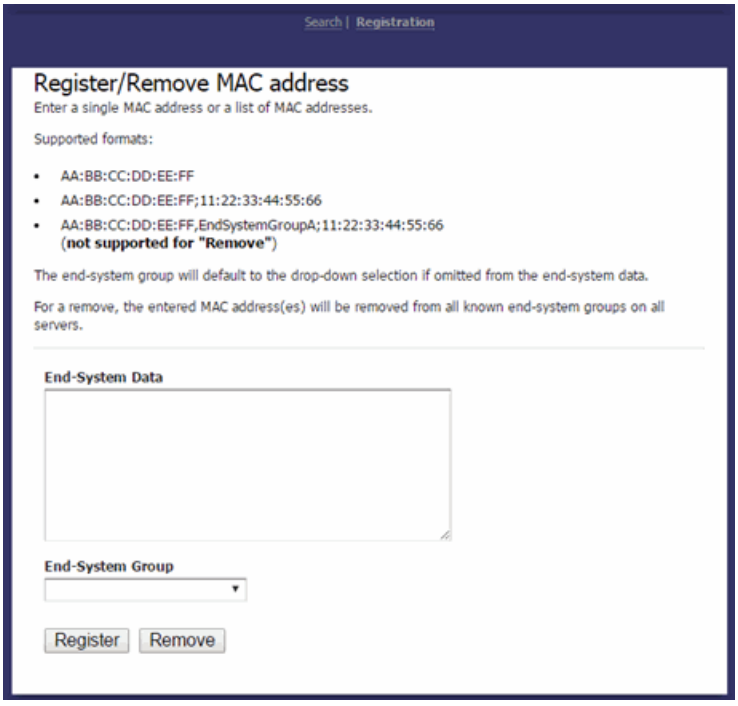
Enter a MAC address, hostname, username, or custom field value (a user-defined field) and click Submit to find an end-system on your network.

Once an end-system is returned, you can open the device to which it is connected in PortView.



Registration

The **Registration** tab allows you to add end-systems to end-system groups by entering lists of MAC addresses or remove end-systems from existing groups. End-system groups allow you to quickly create rules for different groups of end-systems you can use to configure appropriate network access in your Extreme Access Control solution.



End-System Data

Enter a MAC address or multiple MAC addresses separated by a semi-colon to add them to the end-system group selected in the End-System Group drop-down menu.

You can also enter end-systems with the end-system groups to which they are being added separated by a comma (e.g. AA:BB:CC:DD:EE:FF,*<End-SystemGroupName>*). Any end-systems added without their end-system group specifically listed are added to the group selected in the End-System Group drop-down menu.

End-System Group

Select the end-system group into which you are adding the end-systems associated with the MAC addresses listed in the End-System Data field. This field displays all end-system groups from all servers in Extreme Management Center.

Register Button

Click the Register button to add the end-system MAC addresses to the end-system group listed in the End-System Data field or selected in the End-System Group drop-down menu.

Remove Button

Click the Remove button to remove the end-system MAC addresses from the end-system group listed in the End-System Data field or selected in the End-System Group drop-down menu.

Once the end-system group is created, use the Extreme Access Control tab to configure network access rules for the end-systems in the group.

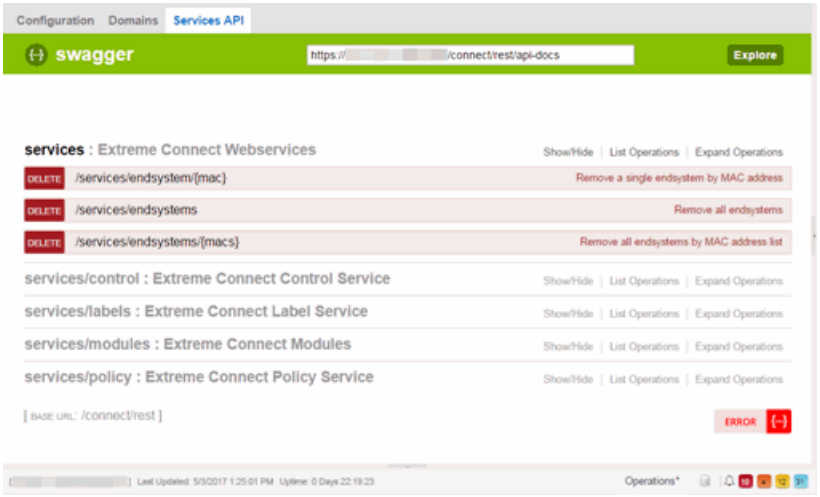
Related Information

For information on related tabs:

- Extreme Management Center Connect Overview
- Configuration

Connect Services API

The Services API tab allows you to execute a client/server application, known as a web service.



The available web services are organized based on the type of function they perform:

- Inventory Web Services — Perform Inventory Manager functions (e.g. backups or retrieving device properties).
- NAC Configuration Web Services — Perform Extreme Access Control configuration functions.
- NAC End-System Web Services — Retrieve and modify Extreme Access Control services, with a focus on accessing end-systems.
- NAC Web Services — Retrieve and modify general Extreme Access Control services.
- NetSight Device Web Services — Retrieve and modify the devices in the Extreme Management Center database.
- Policy Web Services — Perform Policy Manager functions.
- Purview Web Services — Retrieve and modify Application Analytics data and configuration.
- Reporting Web Services — Retrieve and modify the Extreme Management Center reporting engine data configuration.

Related Information

For information on related tabs:

- Extreme Management Center Connect Overview
- Configuration

Inventory Web Service

The Inventory web service provides an external interface to expose Inventory Manager functions such as performing backups or retrieving device properties. The Inventory web service description language is available at:

https://<ManagementCenterServerIP>:<Port>/axis/services/InventoryWebService?wsdl

Method: backupDeviceConfiguration

Backup device configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

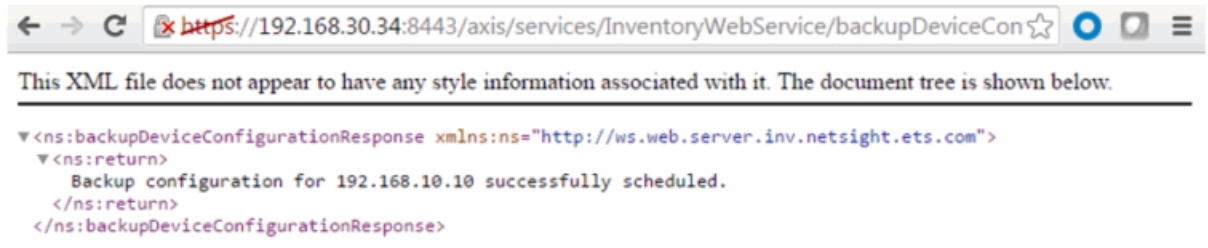
Returns

Returns status message.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/backupDeviceConfiguration?ipAddress=192.168.10.10



Method: backupDeviceConfigurationArchive

Backup device configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device
archiveName	string	Archive name

Returns

Returns status message.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/backupDeviceConfigurationArchive?ipAddress=192.168.10.10&archiveName=Web Service Archive

Method: getDeviceProperties

Returns device information/properties.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceProperty with a structure defined by the following table.

Name	Type	Description
baseMac	string	Base MAC address of the switch
chassisId	string	Chassis ID of the switch
chassisType	string	Chassis type
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
firmware	string	Firmware version installed on the switch
hostName	string	Hostname of the switch
ip	string	IP address of the switch
module	WsModulePropertyResult	Additional switch data
success	boolean	True if operation is successful
sysLocation	string	Switch sysLocation value

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/getDeviceProperties?ipAddress=192.168.10.10

Method: getDevicePropertiesWithRefresh

Force a refresh and return the device information/properties.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceProperty with a structure defined by the following table.

Name	Type	Description
baseMac	string	Base MAC address of the switch
chassisId	string	Chassis ID of the switch
chassisType	string	Chassis type
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
firmware	string	Firmware version installed on the switch
hostName	string	Hostname of the switch
ip	string	IP address of the switch
module	WsModulePropertyResult	Additional switch data
success	boolean	True if operation is successful
sysLocation	string	Switch sysLocation value

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/getDevicePropertiesWithRefresh?ipAddress=192.168.10.10

Method: refreshDevice

Refresh the device.

Parameters

Name	Type	Description
ipAddress	string	IP address of the switch

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

Method: test

Test operation that returns back the current time.

Returns

Returns current time.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/test

NAC Configuration Web Service

The NAC configuration web service provides an external interface to manage Extreme Access Control's configuration data. The NAC configuration web service description language is available at:

https://<ExtremeManagementCenterServer>:<port>/axis/services/NACConfigurationWebService?wsdl

- Method: createDCMVirtualAndPhysicalNetwork
- Method: createSwitch
- Method: createVirtualAndPhysicalNetwork
- Method: deleteSwitch
- NAC Configuration Web Service
- Method: updateSwitch

Method: createDCMVirtualAndPhysicalNetwork

Create a virtual and physical network configuration. This operation creates Extreme Access Control rules, profile, policy mapping, policy role, and VLANs for the Extreme Management Center configuration and domain. Enforce the configuration changes after executing the web service.

Parameters

Name	Type	Description
name	string	Name used for the Extreme Access Control rule, profile, and policy mapping
nacConfig	string	Extreme Access Control configuration name
domain	string	Domain name

Name	Type	Description
isPrivateVlan	boolean	Set to **true** if it is a private VLAN
primaryVlanId	int	Primary VLAN ID
secondaryVlanId	int	Secondary VLAN ID, only required if **isPrivateVlan** is set to **true**. Otherwise it can be set to **-1**
mode	string	VLAN type, available options are: -promiscuous -isolated -community
forwardAsTagged	boolean	Set to **true** for forwarding tagged packets
swGroup	string	Switch group name
nic	string	Network adapter name
isSync	boolean	Set to **true** to synchronize physical and virtual fabric
isApproval	boolean	Set to **true** to approve workflow

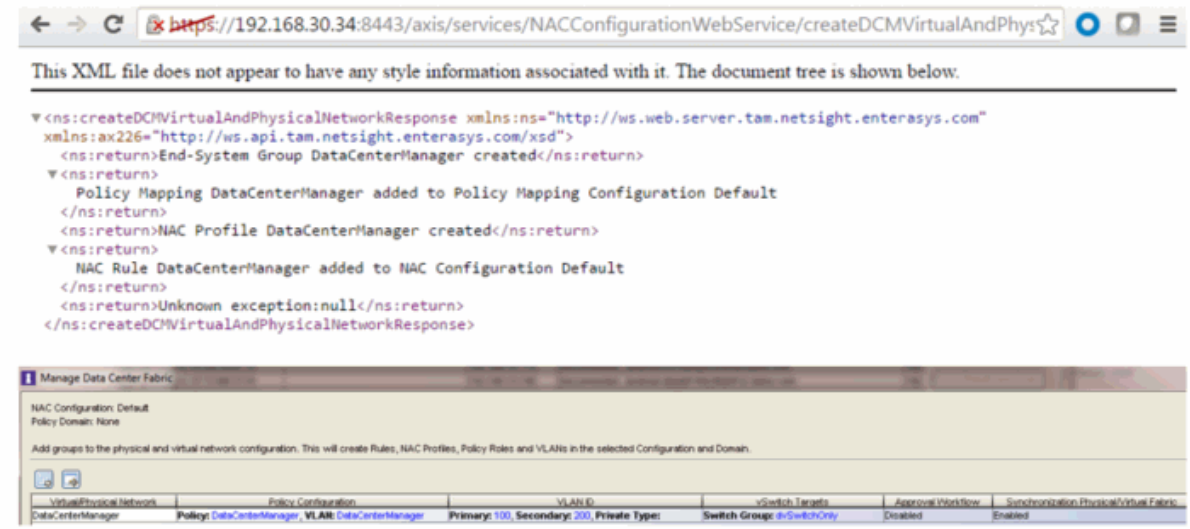
Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/createDCMVirtualAndPhysicalNetwork?name=DataCenterManager&nacConfig=Default&domain=Default&isPrivateVlan=true&primaryVlanId=100&secondaryVlanId=200&mode=promiscuous&forwardAsTagged=true&swGroup=dvSwitchOnly&nic=Default&isSync=true&isApproval=false



Method: createSwitch

Create a switch in the Extreme Access Control configuration.

Parameters

Name	Type	Description
nacApplianceGroup	string	Extreme Access Control engine group for the switch
ipAddress	string	IP address of the switch
switchType	string	Type of switch, a null or empty value will default to Layer 2 Out of Band. Available options are: -Layer 2 Out-Of-Band -Layer 2 Out-Of-Band Data Center -Layer 2 Out-Of-Band with PEPs -Layer 2 Controller PEP -Layer 2 RADIUS Only -Layer 3 Out-Of-Band -Layer 3 Controller PEP -VPN
primaryGateway	string	IP address of primary Extreme Access Control engine

Name	Type	Description
secondaryGateway	string	IP address of secondary Extreme Access Control engine
tertiaryGateway	string	IP address of the third Extreme Access Control engine
quaternaryGateway	string	IP address of the fourth Extreme Access Control engine
authType	string	Authentication type, a null or empty value defaults to Network Access. Available options are: -Any Access -Management Access -Network Access -Monitoring - RADIUS -Accounting -Manual RADIUS Configuration
attrsToSend	string	Gateway RADIUS attributes to send, a null or empty value defaults to Extreme Policy
isRadiusAccountingEnabled	boolean	Set to true to enable RADIUS accounting
managementRadiusServer1	string	Management RADIUS server 1, only available when **authType** is set to **Network Access**
managementRadiusServer2	string	Management RADIUS server 2, only available when **authType** is set to **Network Access**
policyDomain	string	Policy domain
pep1	string	Policy enforcement point 1, only available when **switchType** is set to **VPN**
pep2	string	Policy enforcement point 2, only available when **switchType** is set to **VPN**

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: createVirtualAndPhysicalNetwork

Create a virtual and physical network configuration. This operation creates an Extreme Access Control rule, profile, policy mapping, policy role, and VLANs for the Extreme Access Control configuration and domain. Enforce configuration changes after executing the web service.

Parameters

Name	Type	Description
name	string	Name used for the Extreme Access Control rule, profile, and policy mapping
nacConfig	string	Extreme Access Control configuration name
domain	string	Domain name
isPrivateVlan	boolean	Set to **true** if it is a private VLAN
primaryVlanId	int	Primary VLAN ID
secondaryVlanId	int	Secondary VLAN ID, only required if **isPrivateVlan** is set to **true**. Otherwise it can be set to -1
mode	string	VLAN type, available options are: -promiscuous -isolated -community
forwardAsTagged	boolean	Set to **true** for forwarding tagged packets

Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/createVirtualAndPhysicalNetwork?name=Example&nacConfig=Default&domain=Default&isPrivateVlan=true&primaryVlanId=100&secondaryVlanId=200&mode=promiscuous&forwardAsTagged=true

Method: deleteSwitch

Delete switch from Extreme Access Control configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the switch

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/deleteSwitch?ipAddress=192.168.10.10

Method: updateSwitch

Update switch in the Extreme Access Control configuration.

Parameters

Name	Type	Description
nacApplianceGroup	string	Extreme Access Control engine group for the switch
ipAddress	string	IP address of the switch
switchType	string	Type of switch, a null or empty value defaults to Layer 2 Out of Band. Available options are: -Layer 2 Out-Of-Band -Layer 2 Out-Of-Band Data Center -Layer 2 Out-Of-Band with PEPs -Layer 2 Controller PEP -Layer 2 RADIUS Only -Layer 3 Out-Of-Band -Layer 3 Controller PEP -VPN
primaryGateway	string	IP address of primary Extreme Access Control engine
secondaryGateway	string	IP address of secondary Extreme Access Control engine
tertiaryGateway	string	IP address of a third Extreme Access Control engine
quaternaryGateway	string	IP address of a fouth Extreme Access Control engine

Name	Type	Description
authType	string	Authentication type, a null or empty value defaults to Network Access. Available options are: -Any Access -Management Access -Network Access -Monitoring - RADIUS Accounting -Manual RADIUS Configuration
attrsToSend	string	Gateway RADIUS attributes to send, a null or empty value defaults to Extreme Policy
isRadiusAccountingEnabled	boolean	Set to true to enable RADIUS accounting
managementRadiusServer1	string	Management RADIUS server 1, only available when **authType** is set to **Network Access**
managementRadiusServer2	string	Management RADIUS server 2, only available when **authType** is set to **Network Access**
policyDomain	string	Policy domain
pep1	string	Policy enforcement point 1, only available when **switchType** is set to **VPN**
pep2	string	Policy enforcement point 2, only available when **switchType** is set to **VPN**

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

NAC End System Web Service

The NAC end system web service provides an external interface to retrieve and modify Extreme Management Center services. The end-system web service is very similar to the NAC web service; there are, however, additional operations for accessing end-systems. The NAC end-system web service description language is available at:

https://<Extreme Management Center IP>:<port>/axis/services/NACEndSystemWebService?wsdl

Method: addHostnameToEndSystemGroup

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups.

Parameters

Name	Type	Description

Method: addIPToEndSystemGroup

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end system group name changing
ipAddress	string	The IP address of the end-system

Name	Type	Description
description	string	Optional information stored in the end-system group with the IP address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the IP address from other end-system groups

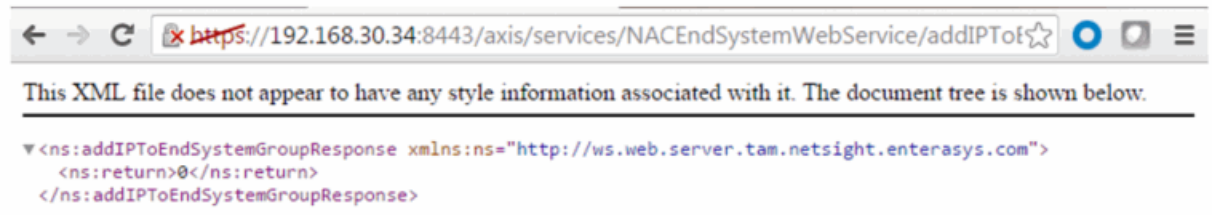
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addIPToEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true



Method: addMACsToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
macs	string	The MAC address(es) of the end-system(s)
description	string	Optional information stored in the end-system group with the MAC address(es)
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

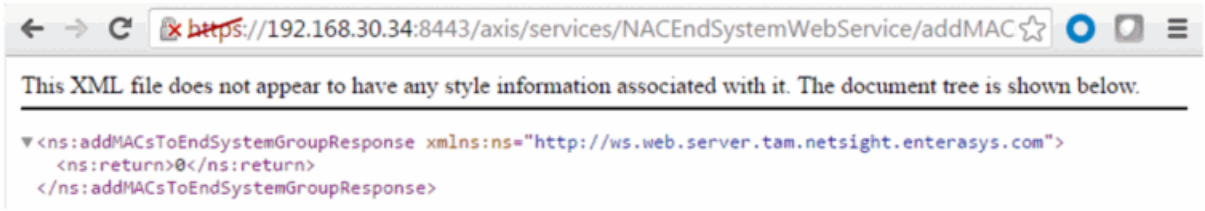
Returns

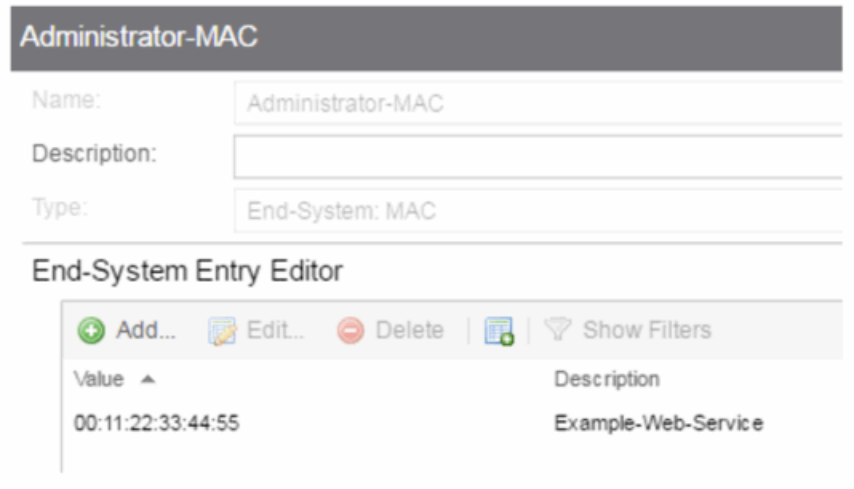
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACsToEndSystemGroup?endSystemGroup=Administrator-MAC&macs=00:11:22:33:44:55&descriptions=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addMACToBlacklist

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

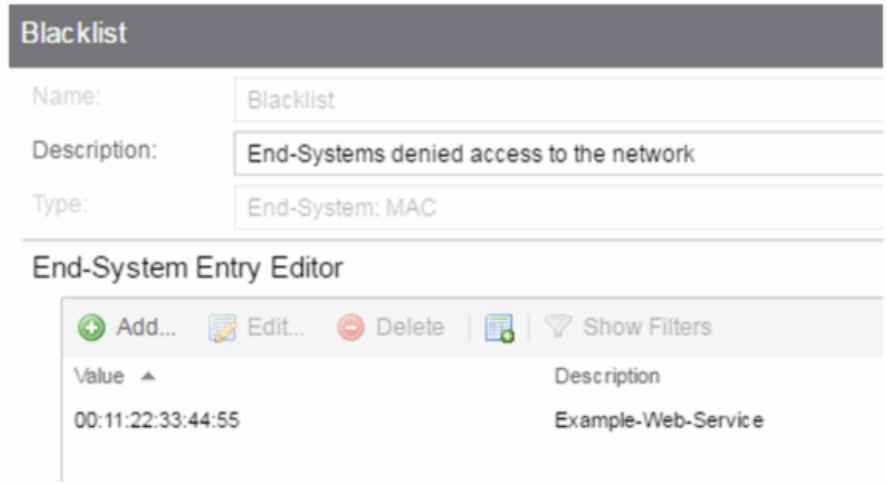
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACToBlacklist?mac=00:11:22:33:44:55&description=Example-Web-Service&reauthorize=true



Method: addMACToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
mac	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

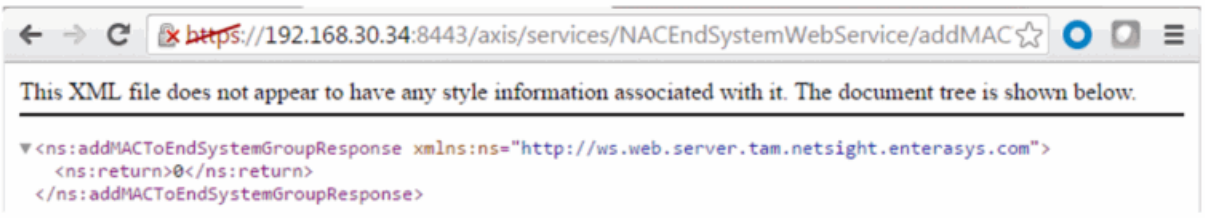
Returns

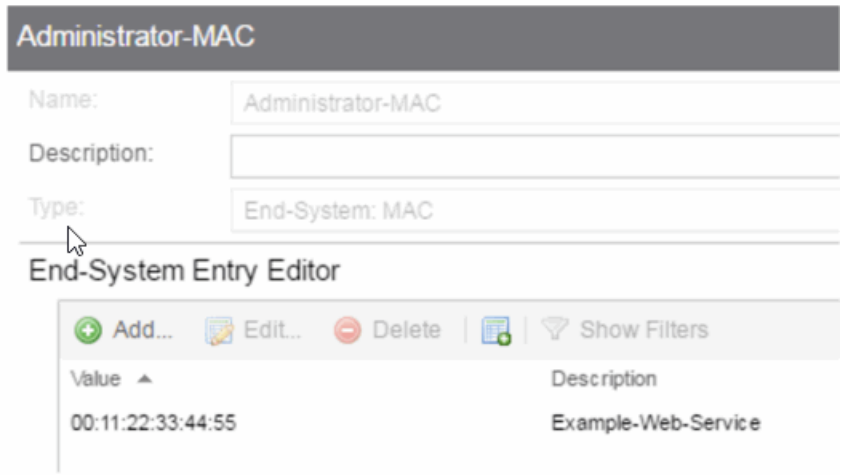
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACToEndSystemGroup?endSystemGroup=Administrator-MAC&mac=00:11:22:33:44:55&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addUsernameToUserGroup

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing

Name	Type	Description
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username
username	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

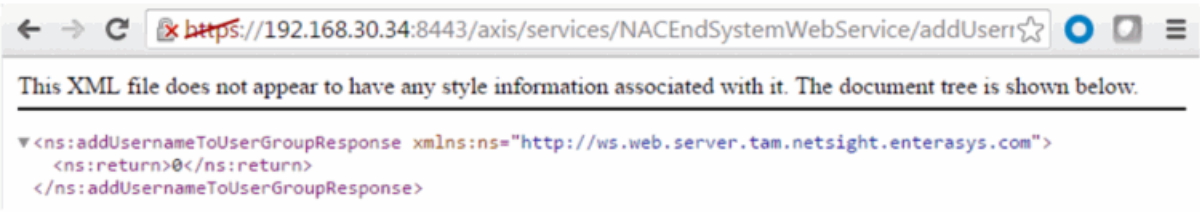
Returns

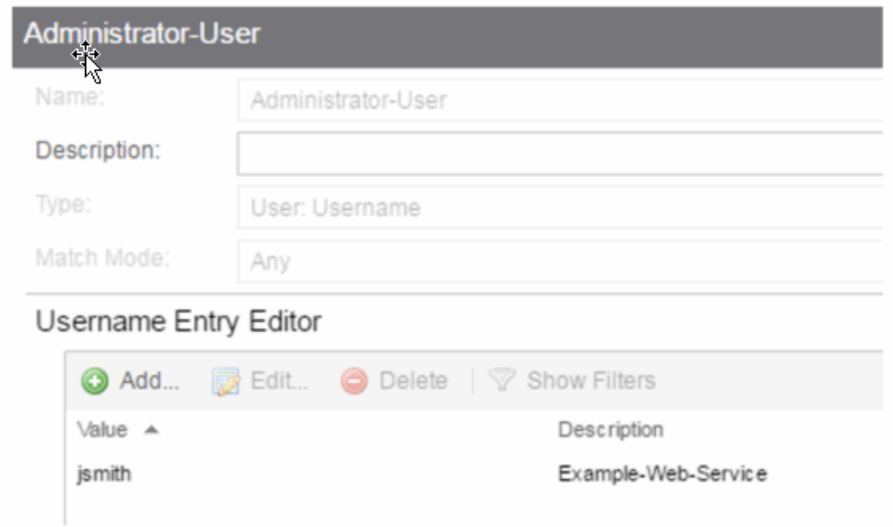
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addUsernameToUserGroup?endSystemGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addValueToNamedList

Add a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addValueToNamedList?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true

Method: addValueToNamedListByWho

Add a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
byWho	string	User requesting the operation
fromWhere	string	Location of the request

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addValueToNamedListByWho?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true&byWho=root&fromWhere=Extreme

Method: clearOldestEndSystemIp

Clear the IP address on all end-systems with the matching parameter.

Parameters

Name	Type	Description
ipAddress	string	IP address to clear

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/clearOldestEndSystemIp?ipAddress=192.168.10.180

Method: collectOsFamilyDataPointStats

Collect the current device types from the Extreme Access Control end-system table and store the results to the reporting database table.

Parameters

Name	Type	Description
overrideTimeStamp	long	Timestamp to store in the reporting database, in milliseconds

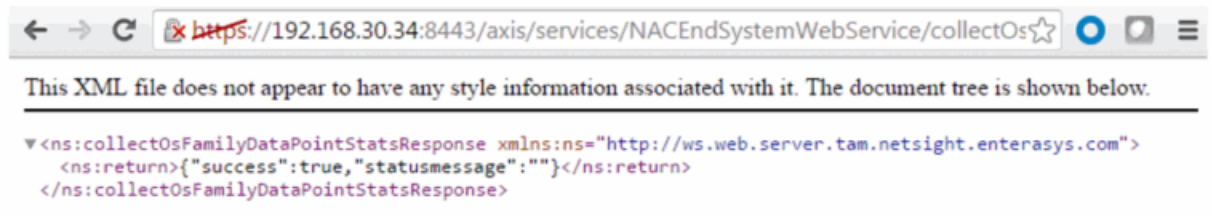
Returns

Returns a string status.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/collectOsFamilyDataPointStats?overrideTimeStamp=1464015739000



Method: collectOsNameDataPointStats

Collect the current device families from the Extreme Access Control end-system table and store the results to the reporting database table.

Parameters

Name	Type	Description
overrideTimeStamp	long	Timestamp to store in the reporting database, in milliseconds

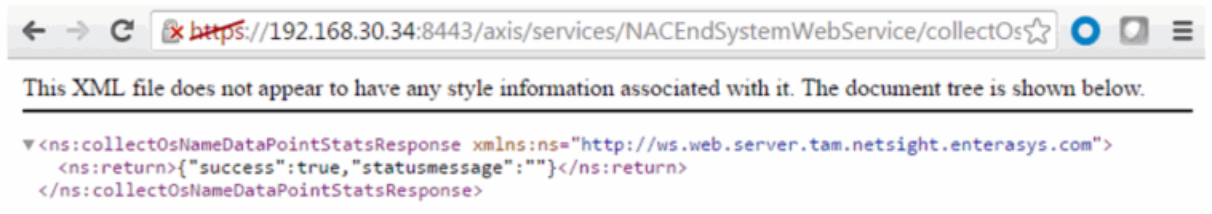
Returns

Returns a string status.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/collectOsNameDataPointStats?overrideTimeStamp=1464015739000



method: createNamedList

Create a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list
listType	string	The named list type, available options are: USERNAME LDAPUSERGROUP RADIUSUSERGROUP MAC IP HOSTNAME LOCATION TIMEOFWEEK
description	string	Description of the named list

Returns

The operation returns an integer error code.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/createNamedList?listName=Example&listType=MAC&description=Web-Service-Example

Method: deleteEndSystemByMac

Delete end-system based on the end-system's MAC address.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system to delete

Name	Type	Description
deleteOptionsMask	int	0x01 – Delete values in named lists 0x02 – Delete MAC locks 0x04 – Delete end-system information 0x08 – Delete registered devices 0x10 – Force delete of end-system

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemByMac?mac=50:7A:55:6F:24:35&deleteOptionsMask=16

Method: deleteEndSystemInfoByHostname

Delete end-system information record based on the end-system's hostname.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system

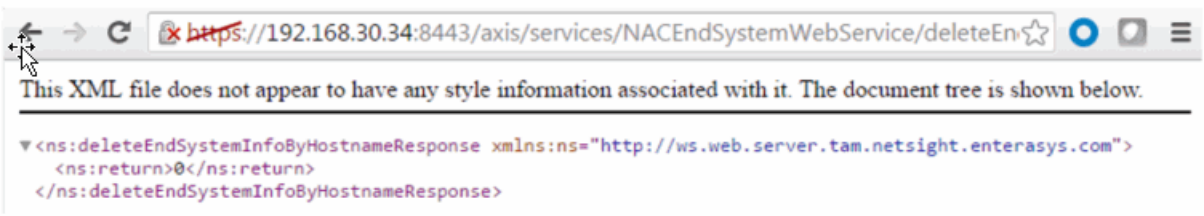
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByHostname?hostname=Captain-Obvious.demo.com



Method: deleteEndSystemInfoByIp

Delete end-system information record based on the end-system's IP address.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system

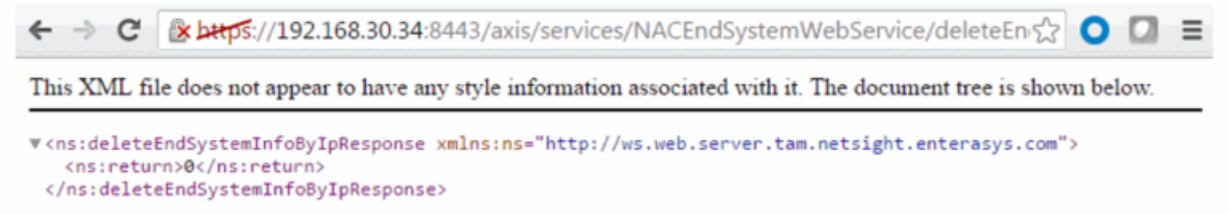
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByIp?ipAddress=192.168.10.180



Method: deleteEndSystemInfoByMac

Delete end-system information record based on the end-system's MAC address.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system

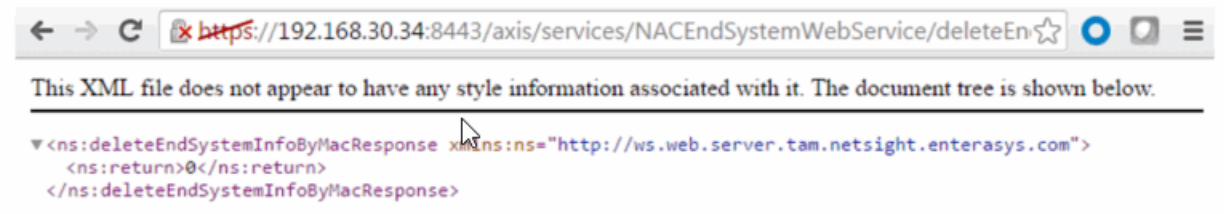
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByMac?mac=14:7D:C5:97:70:CB



Method: deleteEndSystemInfoEx

Delete end-system information record based on the end-system's MAC address. This operation is similar to deleteEndSystemInfoByMac but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

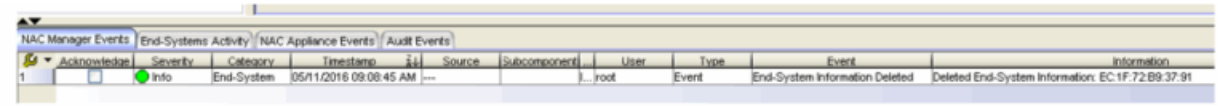
Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system from which information is deleted
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoEx?macAddress=EC:1F:72:B9:37:91



Method: findEndSystem

Find end-systems in the database that match the given search criteria.

Parameters

Name	Type	Description
search	string	Search string, accept values are an IP address, MAC address, or username

Returns

Returns an array of end-systems that match the search criteria.

Example

Execute the following web-service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/findEndSystem?search=18:F6:43:0D:BE:59

Method: getAllEndSystemsAsProperties

Retrieve all end-system information as properties. Use the firstResult and maxResults parameters to paginate the end-systems returned by the web service.

Parameters

Name	Type	Description
firstResult	int	The first index in the query
maxResults	int	The maximum number of end-systems to return

Returns

Returns an array of end-systems.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllEndSystemsAsProperties?firstResult=0&maxResults=100

Method: getAllNacApplianceIpAddresses

Retrieve the IP addresses of all Extreme Access Control engines.

Returns

Returns an array of IP addresses.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllNacApplianceIpAddresses

Method: getAllNamedLists

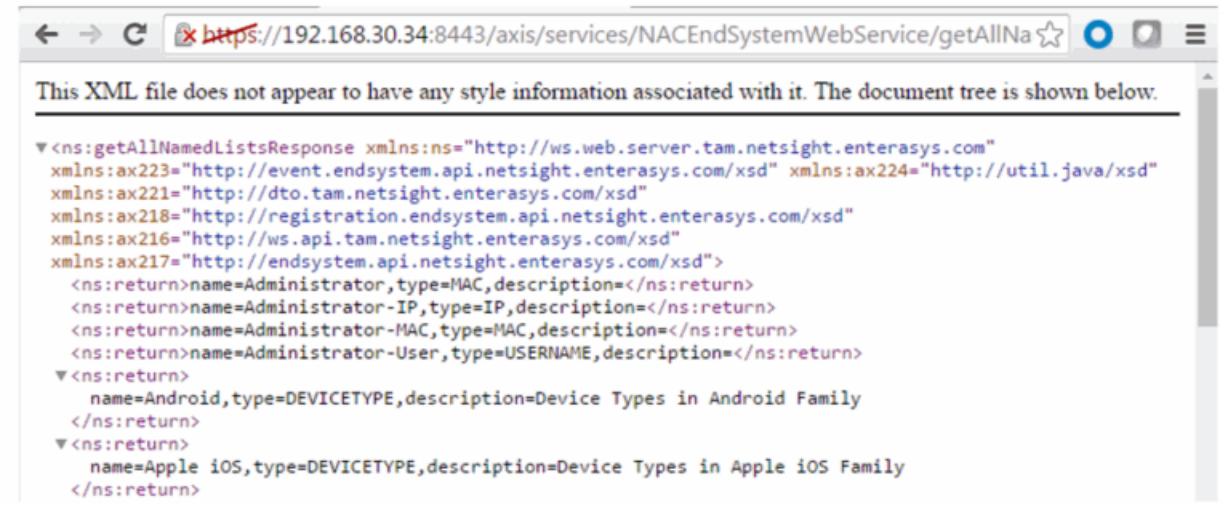
Retrieve all the named lists and their descriptions.

Returns

Returns an array of named lists and their descriptions.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllNamedLists



Method: getDefaultConfigPolicyMappingEntries

Retrieve the policy mappings defined in the default policy mapping configuration.

Returns

Returns a list of policyMappingEntry objects.

Method: getEndSystemAgentServerList

Obtain a list of servers to which an agent connects to provide Extreme Management Center with information about end-systems known by the Extreme

Management Center server.

Parameters

Name	Type	Description
endSystemIp	string	IP address of the end-system
rawMacs	string	MAC addresses of the end-systems

Returns

Returns a list of assessment servers.

Method: getEndSystemAndHrByMac

Returns end system data, based on a MAC address, and it's most recent health result and vulnerabilities.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end system

Returns

Returns end-system data and most recent health result.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemAndHrByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByIP

Return end-system data based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns end-system data.

Example

Execute the following web-service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByIP?ipAddress=192.168.10.190

Method: getEndSystemByIpEx

Return end-system data based on an IP address. The operation is similar to getEndSystemByIP, but returns additional information.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIpEx?ipAddress=192.168.10.190

Method: getEndSystemByMac

Return end system data based on a MAC address.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end system

Returns

Returns end system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByMacEx

Return end-system data based on a MAC address. The operation is similar to getEndSystemByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByMacEx?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoByMacEx

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded in the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Method: getEndSystems

Retrieve 1 or more end-systems based on the MAC address.

Parameters

Name	Type	Description
macs	string	MAC addresses of the end-systems

Returns

Returns end system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystems?macs=00:88:65:66:03:C1&macs=80:D6:05:4A:D6:C4

Method: getEndSystemsByCustomFieldsFuzzy

Retrieve end-systems with custom fields that contain the specified search query.

Parameters

Name	Type	Description
search	string	Custom field string

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByCustomFieldsFuzzy?search=Custom

Method: getEndSystemsByLocationFuzzy

Retrieve end-systems connected to a device with the specified location (sysLocation).

Parameters

Name	Type	Description
search	string	sysLocation string

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByLocationFuzzy?search=AP

Method: getEndSystemsByQuery

Retrieve end-systems with custom fields that contain the specified search query. The search criteria is in the key=value,key=value format.

Parameters

Name	Type	Description
whereClause	string	Query string in key=value format

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByQuery?whereClause=custom4=Custom4

Method: getEndSystemsByUserName

Return end-system data based on a username.

Parameters

Name	Type	Description
userName	string	Username of the end system

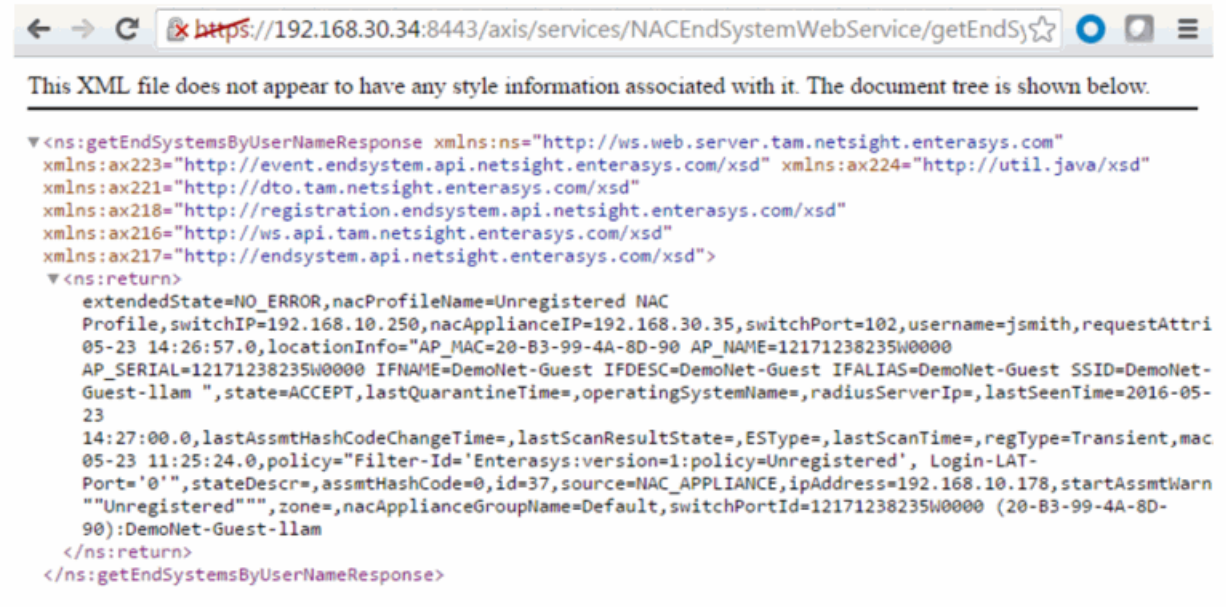
Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserName?userName=jsmith



Method: getEndSystemsByUserNameEx

Return end-system data based on a username. This operation is similar to getEndSystemsByUserName, but returns a verbose message.

Parameters

Name	Type	Description
userName	string	Username of the end-system

Returns

Returns WsEndSystemListResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserName?userName=jsmith

Method: getEndSystemsByUserNameFuzzy

Return end-system data that contains the specified username.

Parameters

Name	Type	Description
userName	string	Username of the end-system

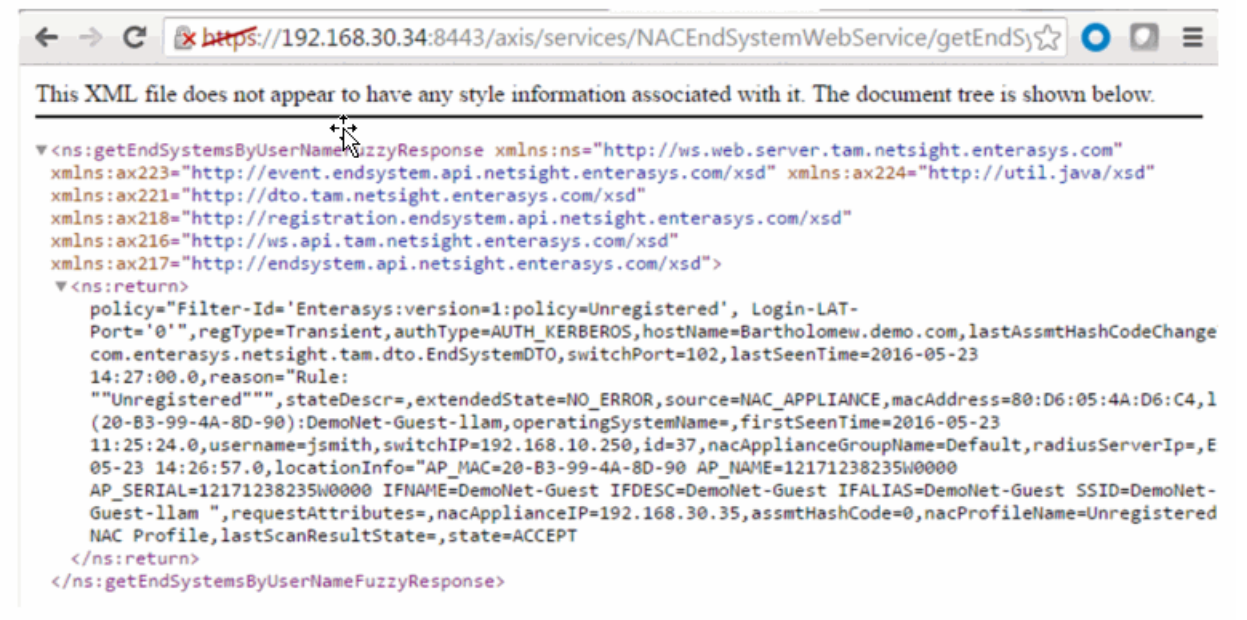
Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserNameFuzzy?userName=smith



Method: getEndSystemTableData

Retrieve end-system table data as a JSON string.

Parameters

Name	Type	Description
start	int	Starting record index
limit	int	Number of end-systems to return
sort	string	Column ID to sort on
dir	string	Sort direction, options are: ASC – ascending DESC – descending
search	string	Search string
userName	string	Username used to determine zone access

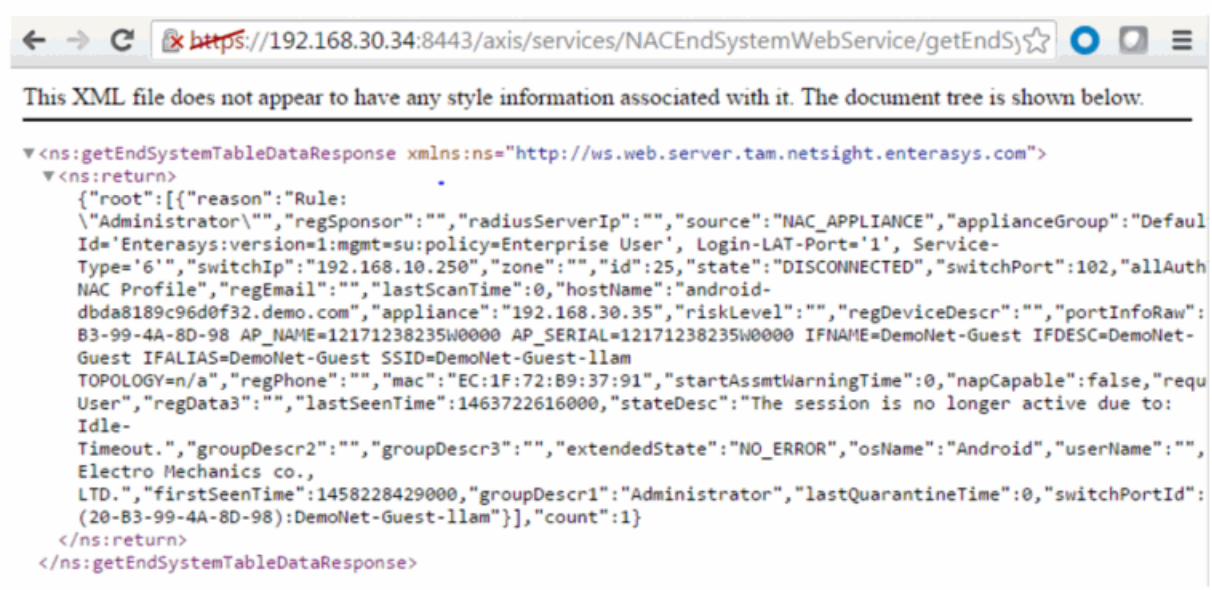
Returns

Returns end-system data in JSON format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemTableData?start=0&limit=100&sort=ipAddress&dir=ASC&search=180&userName=root



Method: getExtendedEndSystemArrByMac

Return an extended set of data (e.g. ELIN, portAlias) for an end-system based on a MAC address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties will be encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

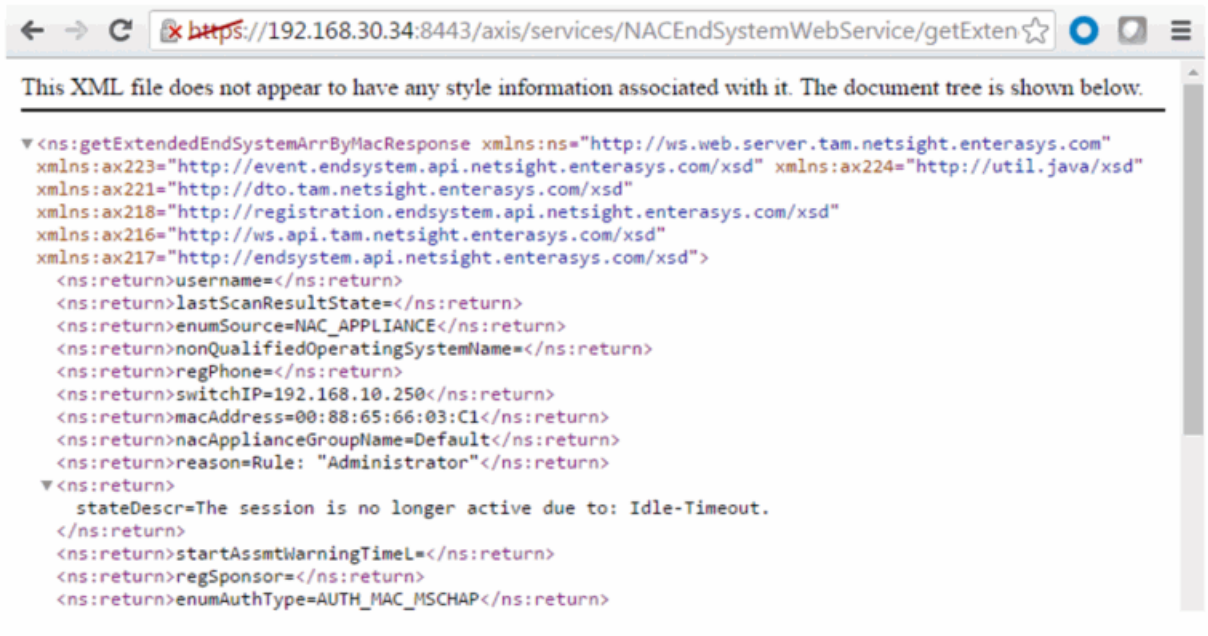
Returns

Returns an array of end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getExtendedEndSystemArrByMac?macAddress=00:88:65:66:03:C1



I Method: getExtendedEndSystemByMac

Return an extended set of data (e.g. ELIN, portAlias) for an end-system based on a MAC address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an extended set of end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getExtendedEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getNACVersion

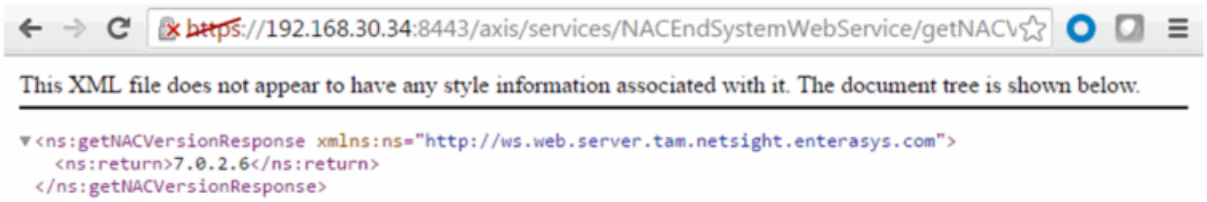
Return the Extreme Access Control version.

Returns

Returns Extreme Access Control version.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getNACVersion



Method: getNamedList

Retrieve a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list

Returns

Returns a named list and its properties.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getNamedList?listName=Administrator

Method: getPollerStatus

Return the last polling status of an Extreme Access Control engine.

Parameters

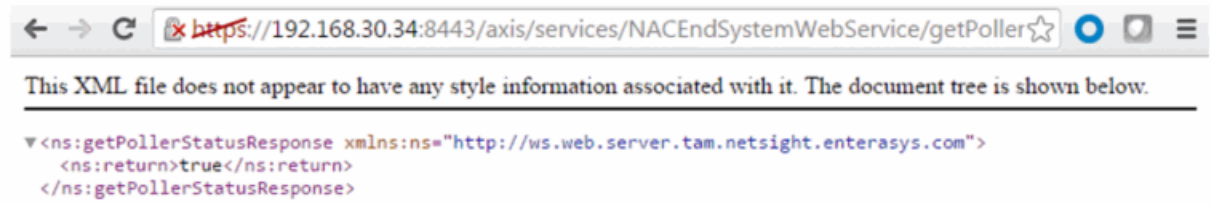
Name	Type	Description
nacIP	string	IP address of an Extreme Access Control engine

Returns

Returns **true**/**false** for the Extreme Access Control engine's last polling status.

Example

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getPollerStatus?nacIP=192.168.30.35



Method: getUnsurfacedNamedList

Return the contents of a named list/end system group without manipulation.

Parameters

Name	Type	Description
listName	string	End-system group name

Returns

Returns a string array that contains the XML representation of values, description, and data.

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getUnsurfacedNamedList?listName=Registered Guests

Method: processFlattenedWsEndSystemEvents

Method to process incoming end-system events from a source. These events are passed as a flattened end-system events.

Parameters

Name	Type	Description
flattenedEvents	string	List of flattened end-system events

Returns

Returns null for a successful operation or an error message.

Method: processNacRequestArrFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End system override (FULL_MAC) – MAC address, end system group, description End system override (FULL_IP) – IP address, end system group, description End system override (HOSTNAME) – hostname, end system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end system override useroverride – user override
isAdd	boolean	**True** for adding the request, **false** for deleting it
type	string	End system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/processNacRequestArrFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC

Method: processNacRequestFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End-system override (FULL_MAC) – MAC address, end system group, description End-system override (FULL_IP) – IP address, end system group, description End-system override (HOSTNAME) – hostname, end system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end system override useroverride – user override
isAdd	boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation was successful

Example

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/processNacRequestFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC

Method: processWsEndSystemEvents

Method to process incoming end-system events from a source. These events are passed in as flattened end-system events.

Parameters

Name	Type	Description
events	WsEndSystemEvent	List of flattened end system events

Returns

Returns null for a successful operation or an error message.

Method: reauthenticate

Force an end system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

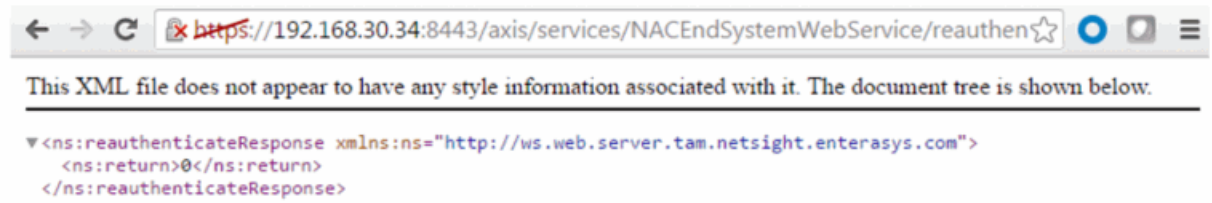
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticate?macAddress=80:D6:05:4A:D6:C4&assess=false



Method: reauthenticateMacs

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

Returns an array of error codes.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacs?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&assess=false

Method: reauthenticateMacsBulk

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddresses	string	MAC address of the end-systems
reason	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

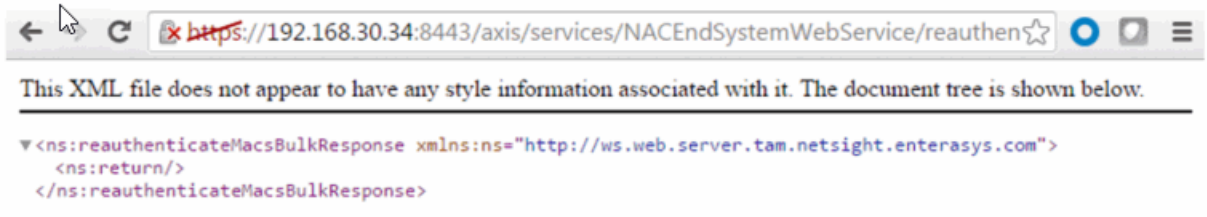
Returns

Returns an empty status.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacsBulk?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&reason=Example-Web-Service&assess=false



Method: reauthenticateMacsWithReason

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddresses	string	MAC address of the end-systems
reauthReasonStr	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

Returns

Returns an array of error codes.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacsWithReason?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&reauthReasonStr=Example-Web-Service&assess=false

Method: reauthenticateWithReason

Force an end-system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
reauthReasonStr	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

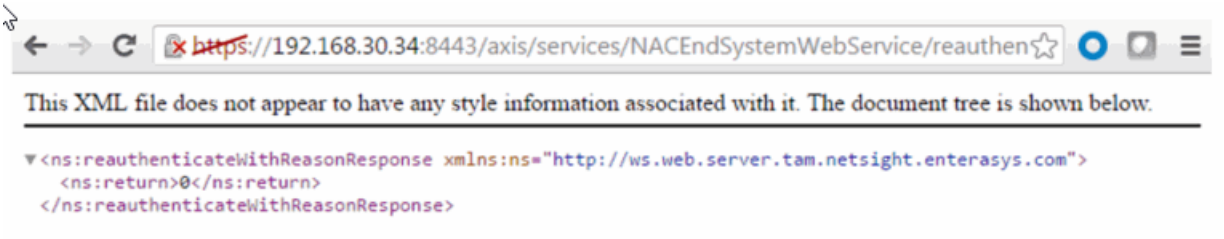
Returns

Returns an array of error codes.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateWithReason?macAddress=80:D6:05:4A:D6:C4&reauthReasonStr=Example-Web-Service&assess=false



Method: registerAgentMacs

Register assessment agent MAC address.

Parameters

Name	Type	Description
macs	string	MAC address of the assessment agents
description	string	Description of the assessment agent(s)

Returns

Returns true for a successful registration.

Method: removeHostnameFromEndSystemGroup

Remove an end-system hostname from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name changing
hostname	string	The hostname of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

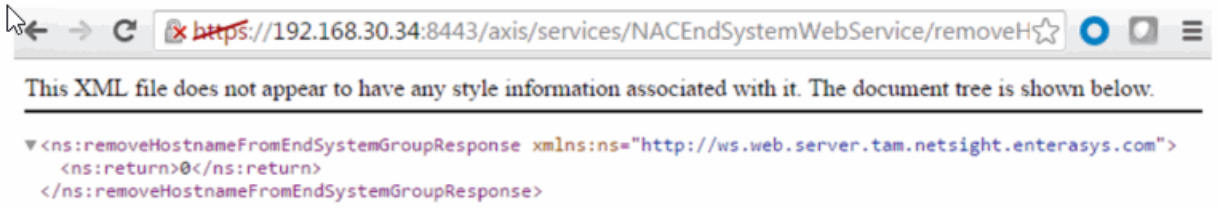
Returns

The operation returns an integer error code.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeHostnameFromEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&reauthorize=true



Method: removeIPFromEndSystemGroup

Remove an end-system IP address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
ip	string	IP address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

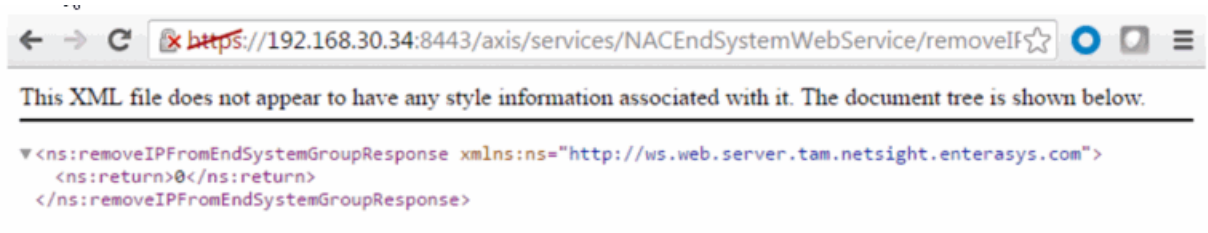
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeIPFromEndSystemGroup?endSystemGroup=Administrator-IP&ip=192.168.10.180&reauthorize=true



Method: removeMACFromBlacklist

Remove an end-system MAC address from the blacklist end-system group.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

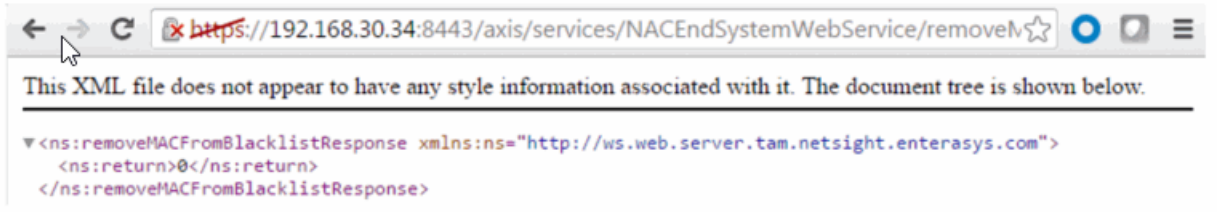
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACFromBlacklist?mac=00:11:22:33:44:55&reauthorize=true



Method: removeMACFromEndSystemGroup

Remove an end-system MAC address from an Extreme Access Control end-system group

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
mac	string	MAC address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

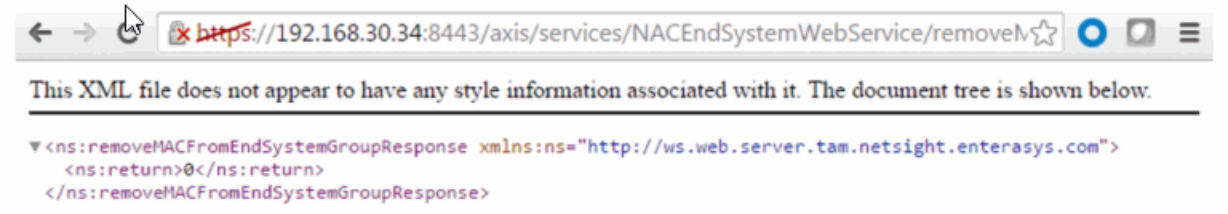
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACFromEndSystemGroup?endSystemGroup=iOS&mac=00:11:22:33:44:55&reauthorize=true



Method: removeMACsFromEndSystemGroup

Remove multiple end system MAC addresses from an Extreme Access Control end-system group

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
macs	string	MAC address of the end-systems
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

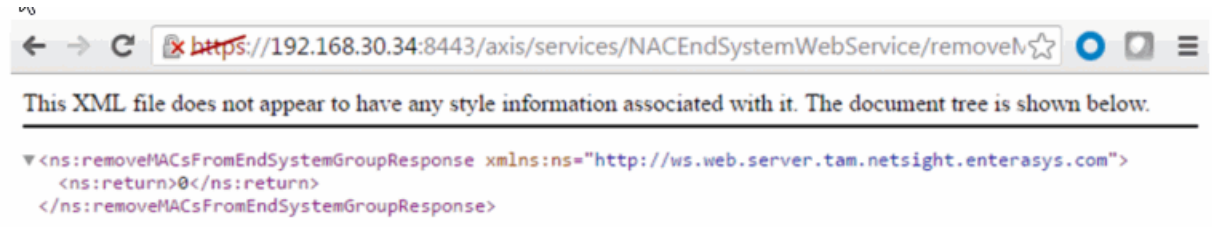
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACsFromEndSystemGroup?endSystemGroup=iOS&macs=00:11:22:33:44:55&macs=00:11:22:33:44:66&reauthorize=true



Method: removeNamedList

Remove a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list

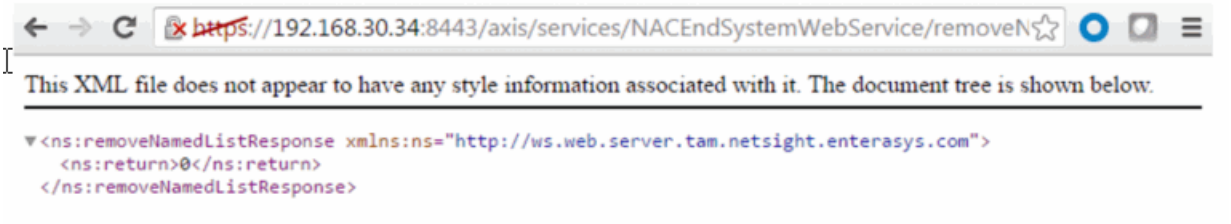
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeNamedList?listName=iPhone



Method: removeUsernameFromUserGroup

Remove a username from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The name of the end-system group you are changing
username	string	Username of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeUsernameFromUserGroup?endSystemGroup=Administrator-User&username=jsmith&reauthorize=true

Method: removeValueFromNamedList

Remove a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeValueFromNamedList?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true

Method: removeValueFromNamedListByWho

Remove a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
byWho	string	User requesting the operation
fromWhere	string	Location of the request

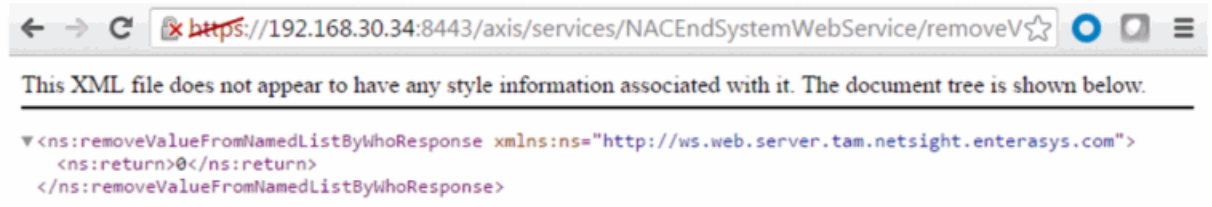
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeValueFromNamedListByWho?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true&byWho=root&fromWhere=Extreme



Method: saveEndSystemInfo

Update end system information. The end-system is identified by using the macAddress, ipAddress, or hostname property.

Parameters

Name	Type	Description
propString	string	Custom field data in custom1=value1,custom2=value2,custom3=value3,custom4=value4 format

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfo?propString=macAddress=EC:1F:72:B9:37:91,custom1=Custom1,custom2=Custom2,custom3=Custom3,custom4=Custom4

Method: saveEndSystemInfoByHostname

Update end system information.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

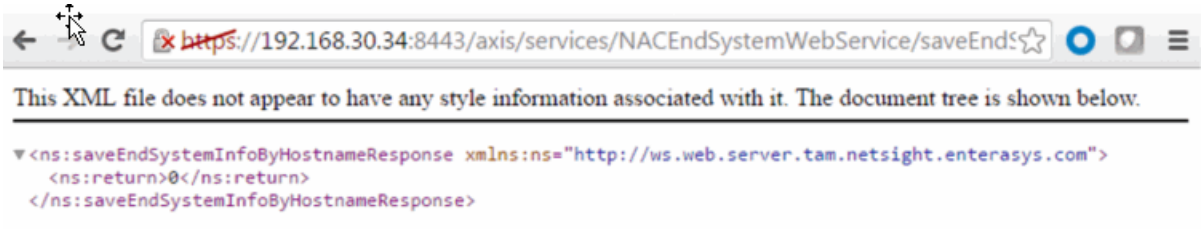
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByHostname?hostname=MacBookPro.demo.com&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByIp

Update end system information.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

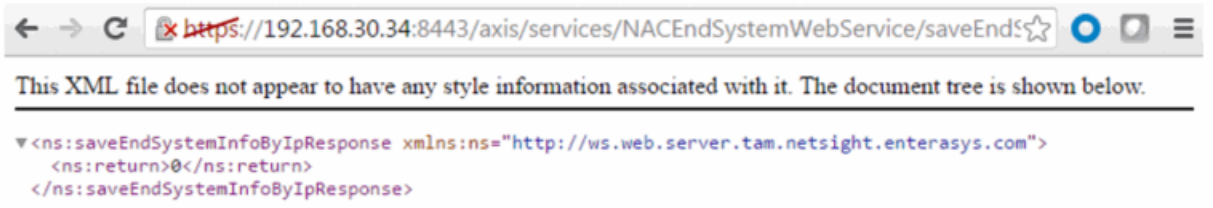
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByIp?ipAddress=192.168.10.178&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByMac

Update end system information.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

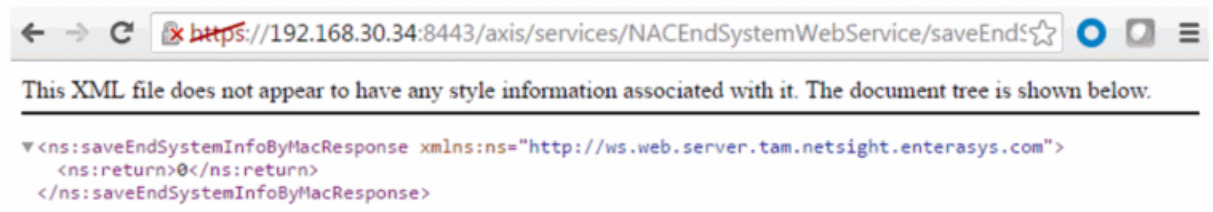
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByMac?mac=80:A5:89:33:67:37&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoEx

Update end system information

Parameters

Name	Type	Description
info	EndSystemInfo	End-system information to save

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system that had information saved
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation was successful

Method: sendKerberosMessageByIp

Send Kerberos messages to all Extreme Access Control engine.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system
userName	string	Username of the end-system
hostName	string	Hostname of the end-system
lastSeenTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to 0 to use Extreme Management Center's current time
lastAuthTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to 0 to use Extreme Management Center's current time
sourceIp	string	Source IP address of the Keberos message

Name	Type	Description
clearUserName	boolean	Setting to **true** clears the end-system's username

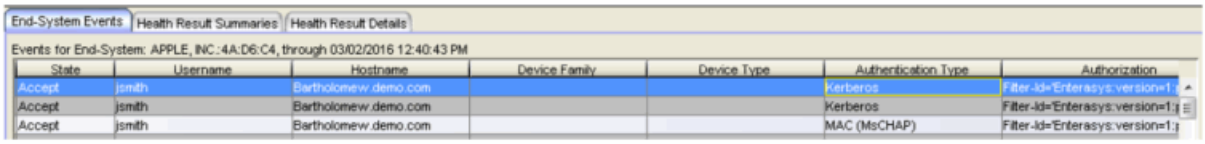
Returns

The operation does not return a value.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/sendKerberosMessageByIp?ipAddress=192.168.10.178&userName=jsmith&hostName=jsmith-test-system&lastSeenTime=0&lastAuthTime=0&sourceIp=192.168.30.34&clearUserName=false



Method: sendKerberosMessageByMAC

Send Kerberos message to all Extreme Access Control engines.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
userName	string	Username of the end-system
hostName	string	Hostname of the end-system
lastSeenTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to **0** to use Extreme Management Center's current time
lastAuthTime	long	The timestamp, in milliseconds, the Keberos message was snooped at. Set to **0** to use Extreme Management Center's current time
sourceIp	string	Source IP address of the Keberos message
clearUserName	boolean	Set to **true** to clear the end-system's username

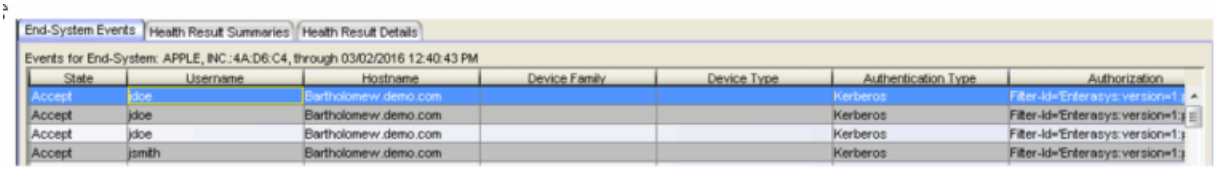
Returns

The operation does not return a value.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/sendKerberosMessageByMAC?macAddress=80:D6:05:4A:D6:C4&userName=jdoe&hostName=jdoe-test-system&lastSeenTime=0&lastAuthTime=0&sourceIp=192.168.30.34&clearUserName=false



Method: setDeviceTypeByIp

Update the end-system's device type.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system
deviceType	string	New device type value
isAccurate	boolean	Set to **true** if you know the new device type is accurate
reason	string	A brief description as to the reason for the Extreme Access Control event

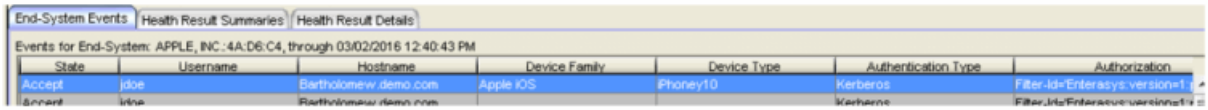
Returns

Returns a string status indicating whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/setDeviceTypeByIp?ipAddress=192.168.10.178&deviceType=iPhoney10&isAccurate=true&reason=Web-Service-Example



Method: setDeviceTypeByMAC

Update the end-system's device type.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
deviceType	string	New device type value
isAccurate	boolean	Set to **true** if you know the new device type is accurate
reason	string	A brief description as to the reason for the Extreme Access Control event

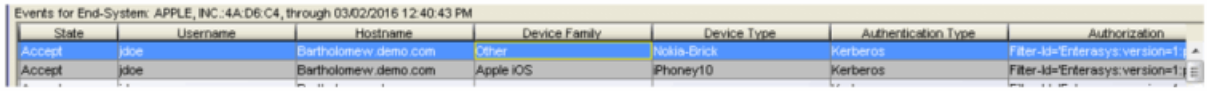
Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/setDeviceTypeByMAC?macAddress=80:D6:05:4A:D6:C4&deviceType=Nokia-Brick&isAccurate=true&reason=Web-Service-Example



Method: updateNamedListDescription

Update the named list description with the new provided description.

Parameters

Name	Type	Description
listName	string	Named list to update
descr	string	Named list description

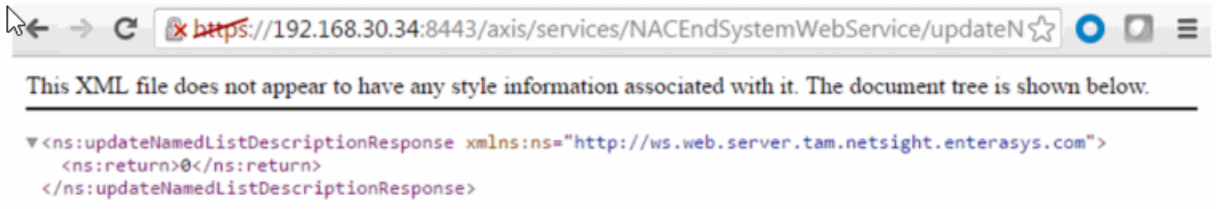
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/updateNamedListDescription?listName=iOS&descr=Example-Web-Service



Method: updateNamedListDescriptionEx

Update the named list description with the new provided description. This operation is similar to updateNamedListDescription, but returns a verbose message.

Parameters

Name	Type	Description
listName	string	Named list to update
descr	string	Named list description

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorCode	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/updateNamedListDescriptionEx?listName=iOS&descr=Example-Web-Service

NAC Web Service

The NAC web service provides an external interface to retrieve and modify the Extreme Access Control services. The NAC web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/NACWebService?wsdl

Method: addHostnameToEndSystemGroup

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

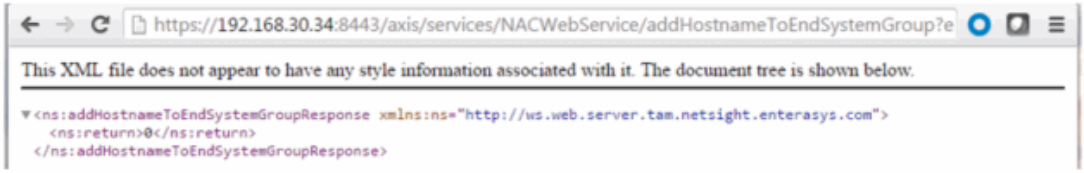
Returns

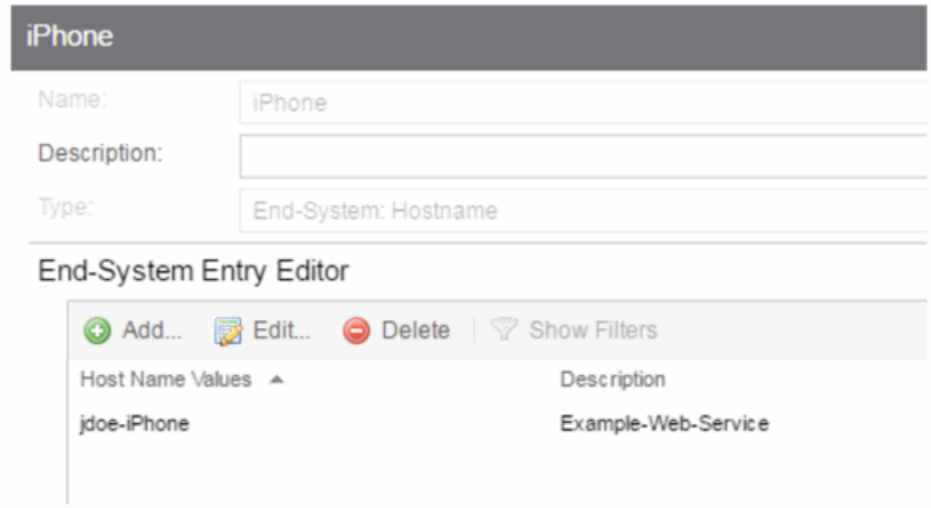
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true





Method: addHostnameToEndSystemGroupEx

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups. This operation is similar to addHostnameToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

Returns

Returns a WsResult with a structure defined by the following table.

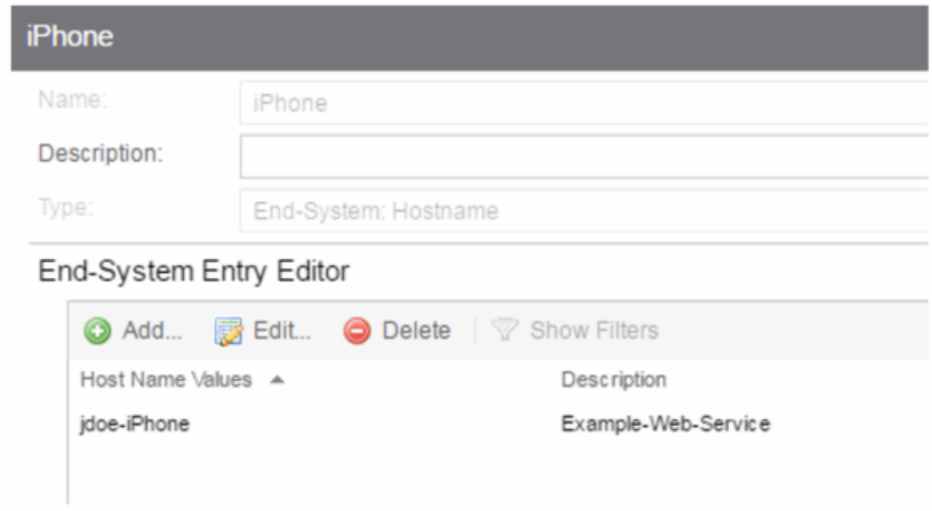
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes

Name	Type	Description
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroupEx?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=



Method: addHostnameToEndSystemGroupWithCustomDataEx

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups
custom	string	The end-system's new custom fields

Returns

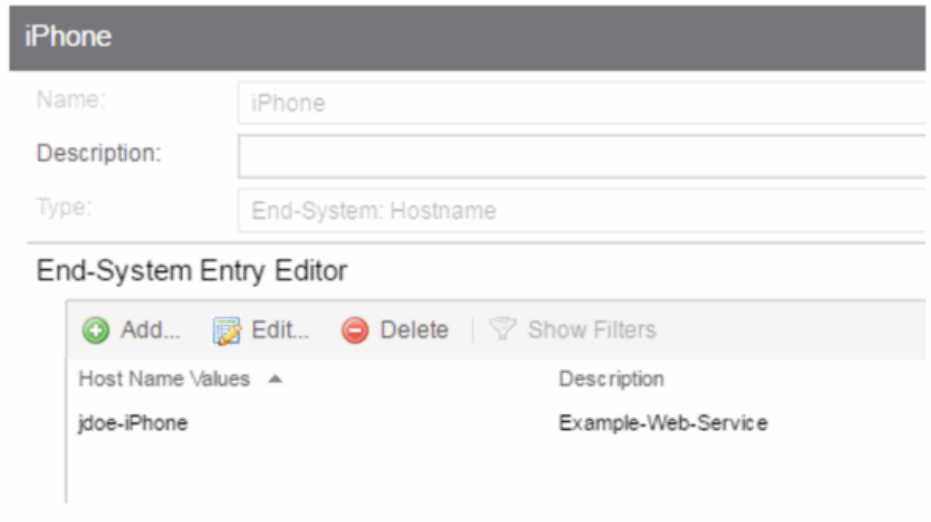
Returns a WsResult with a structure defined by the following table.

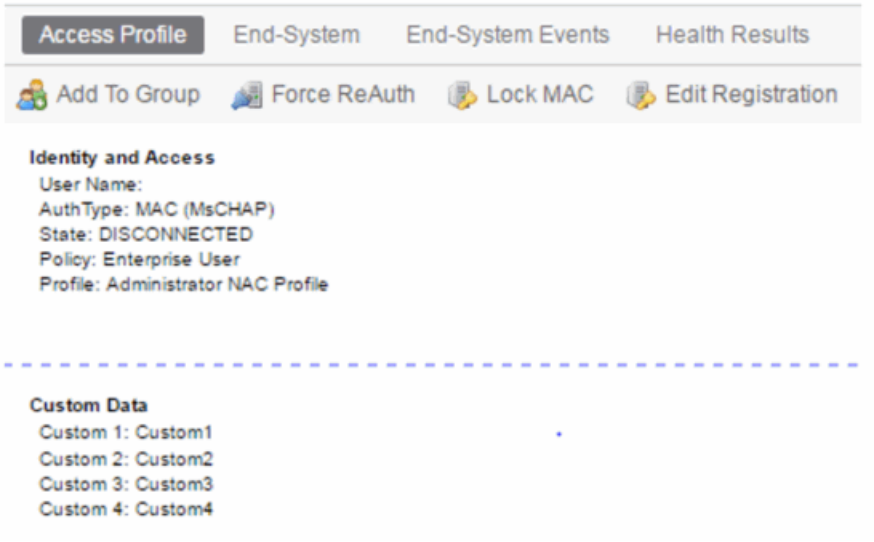
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser. Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroupWithCustomDataEx?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4





Method: addIPToEndSystemGroup

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddress	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

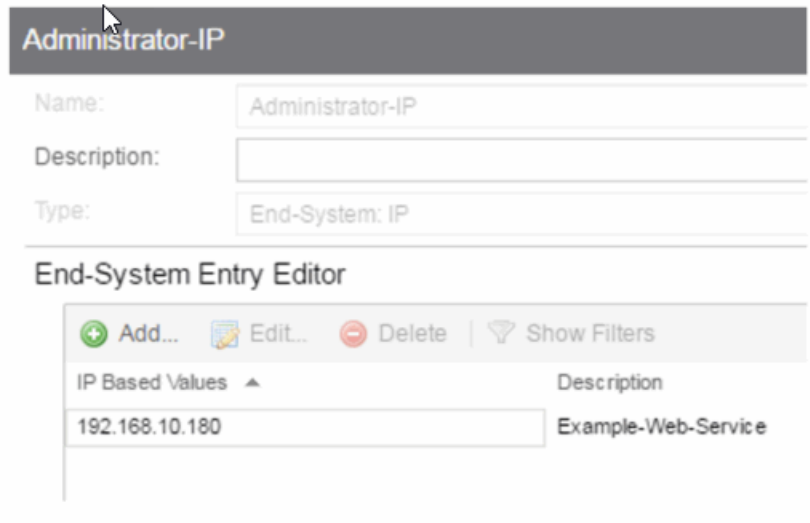
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addIPToEndSystemGroupEx

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups. This operation is similar to addIPToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddess	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end system groups

Returns

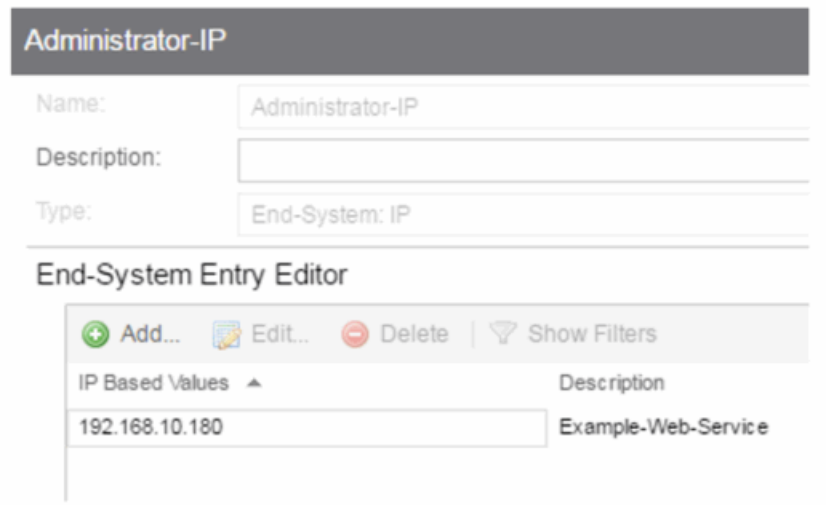
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroupEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addIPToEndSystemGroupWithCustomDataEx

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups and configure the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddress	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

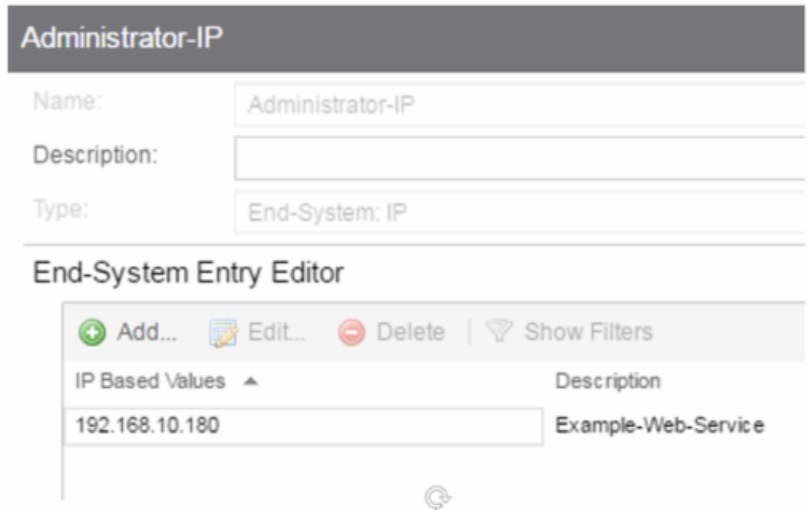
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes

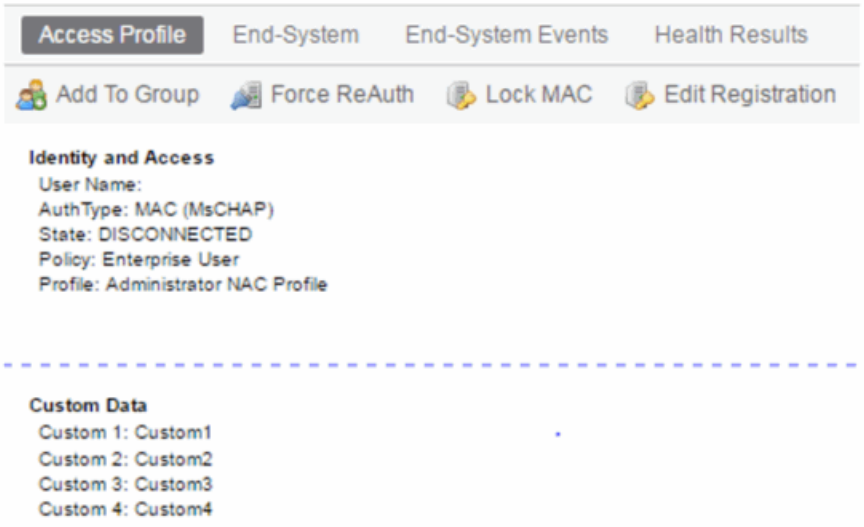
Name	Type	Description
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser. Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroupWithCustomDataEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4





Method: addMACToBlacklist

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

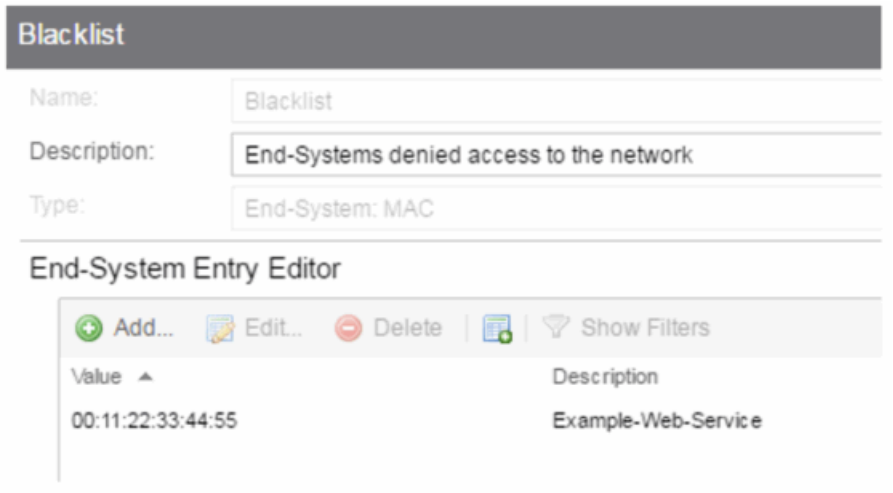
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklist?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true



Method: addMACToBlacklistEx

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. This operation is similar to the addMACToBlackList, but returns a verbose message. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

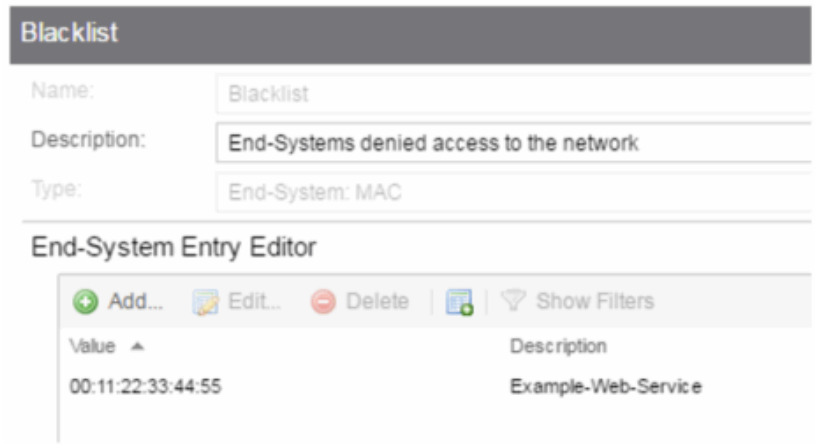
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklistEx?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true



Method: addMACToBlacklistWithCustomDataEx

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. You can configure the custom fields. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to true to force reauthentication on the affected end-system
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

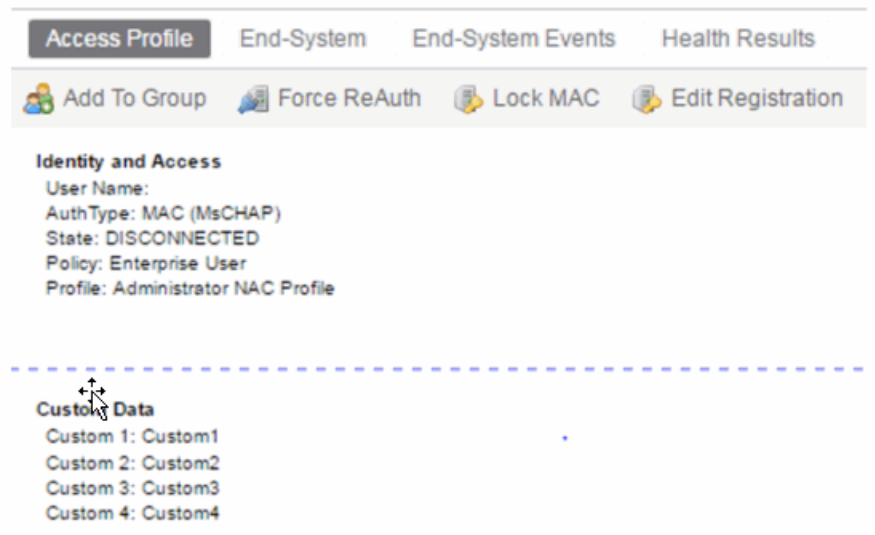
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser.

Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklistWithCustomDataEx?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4



Method: addMACToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and configure custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

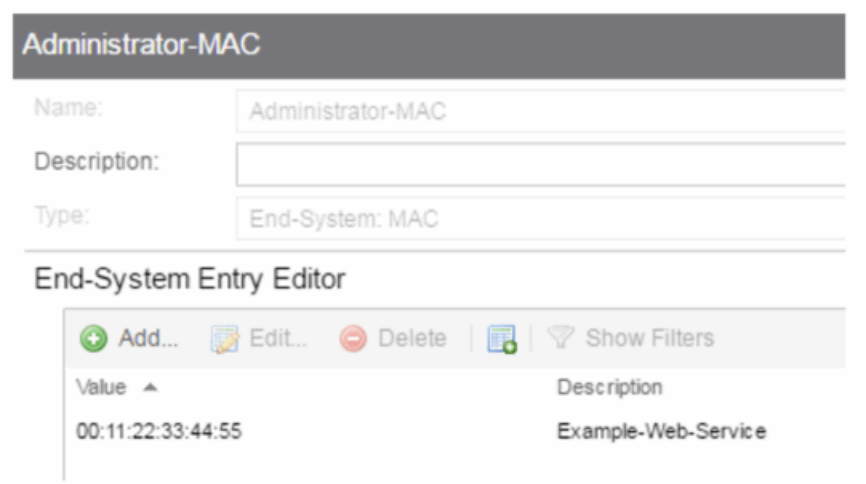
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroup?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addMACToEndSystemGroupEx

Add an end system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups. This operation is similar to addMACToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

Returns

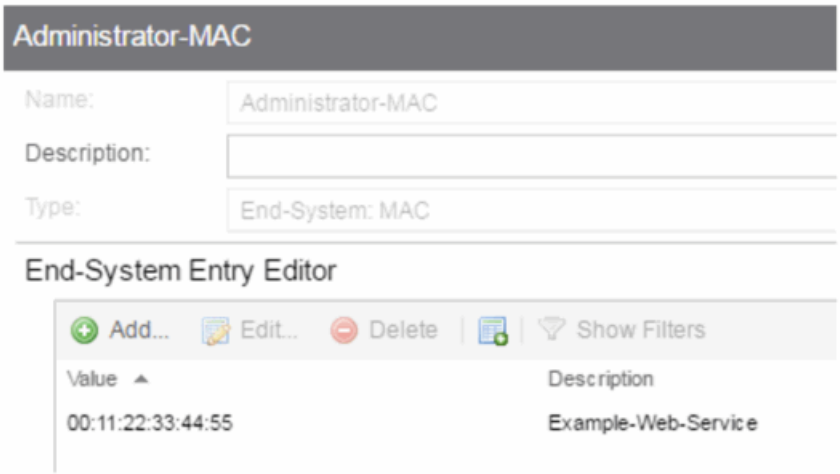
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroupEx?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addMACToEndSystemGroupWithCustomDataEx

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and configure the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Name	Type	Description
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

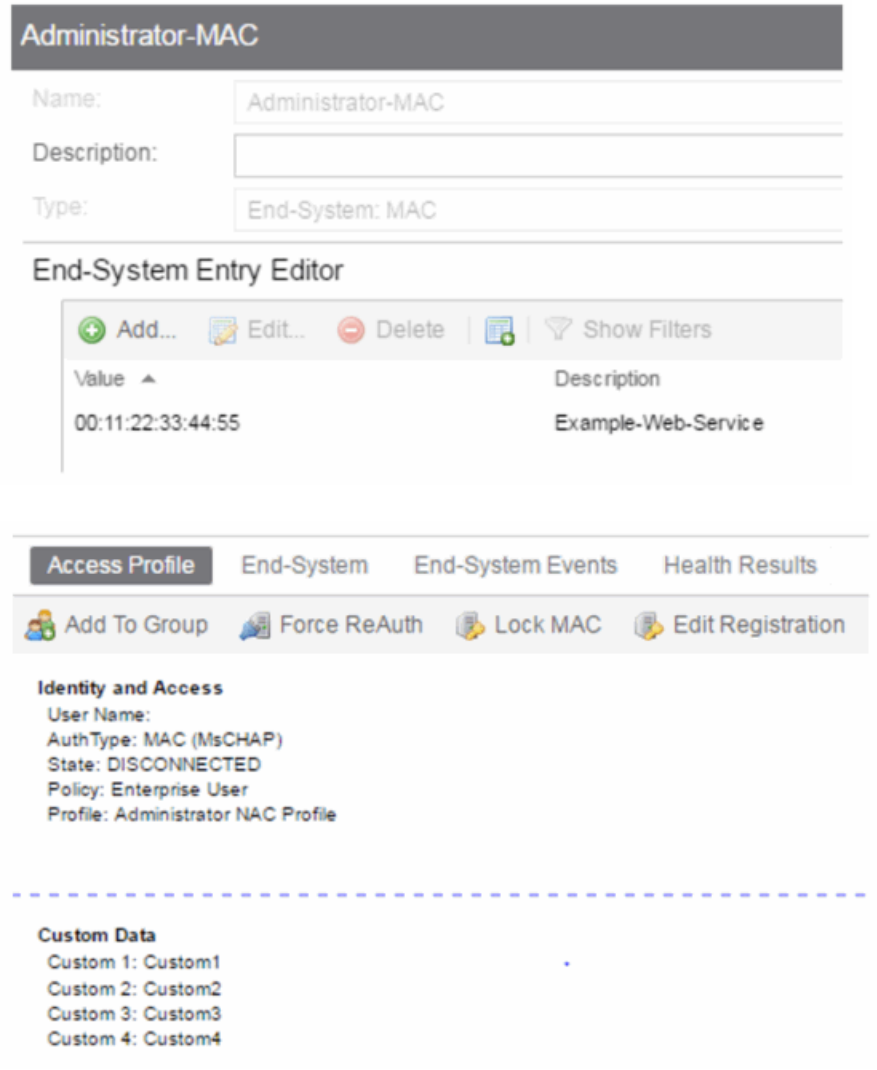
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser.

Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroupWithCustomDataEx?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4



Method: addUsernameToUserGroup

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end-system groups.

Parameters

Name	Type	Description
userGroup	string	The end-system group name you are changing
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

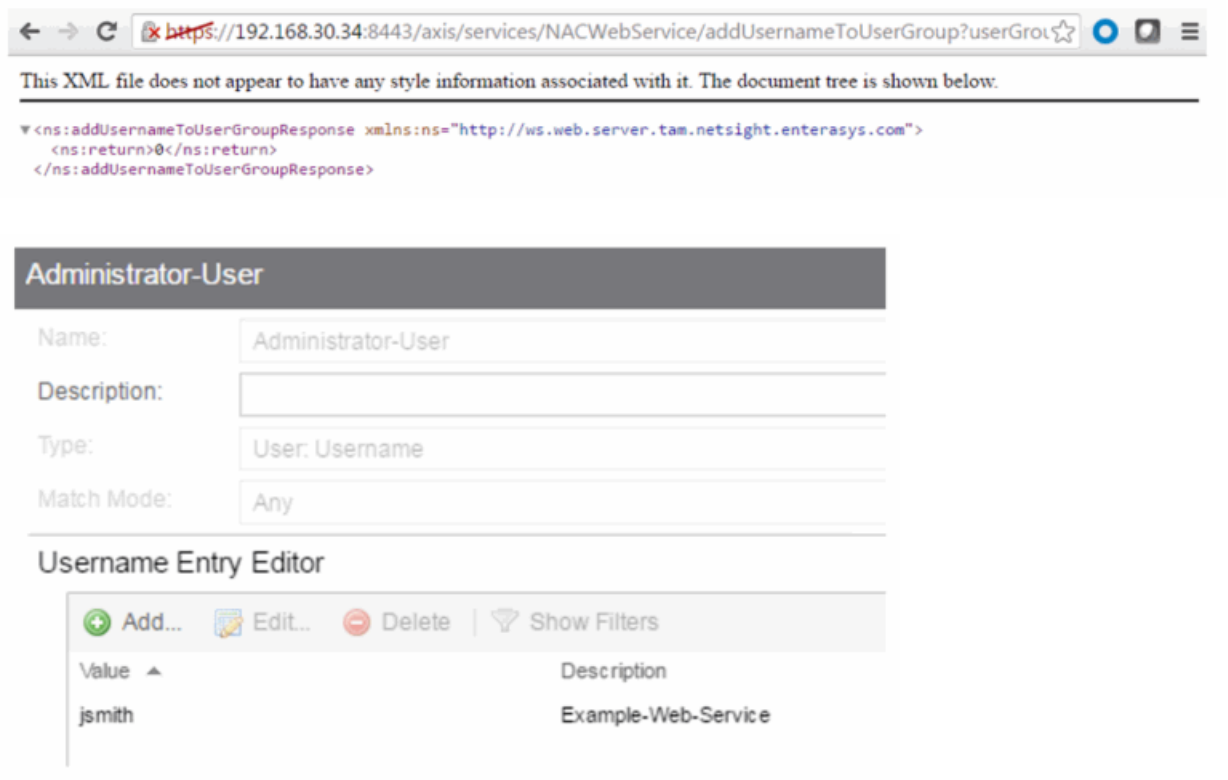
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addUsernameToUserGroup?userGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addUsernameToUserGroupEx

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end-system groups. This operation is similar to addUsernameToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
userGroup	string	The end-system group name you are changing
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

Returns

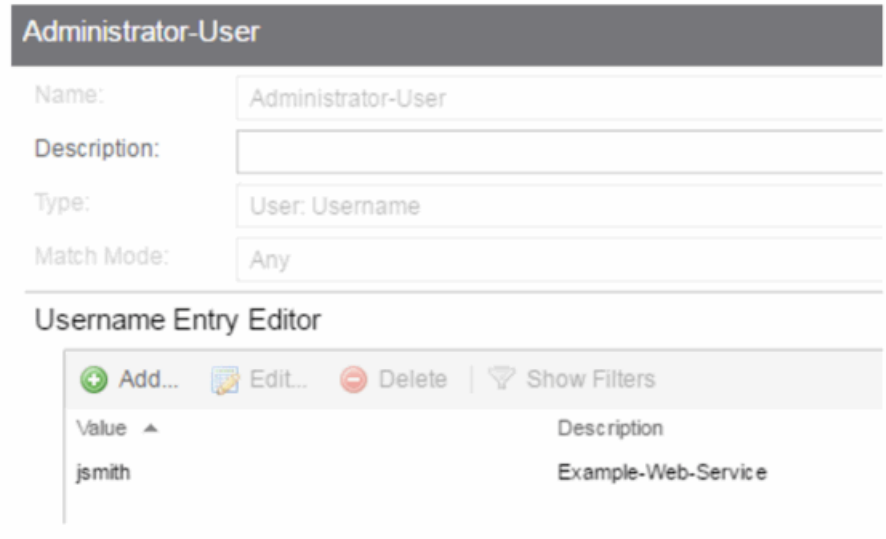
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addUsernameToUserGroupEx?userGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addValueToNamedList

Add a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end system group you are changing
list	string	The value to add

Name	Type	Description
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

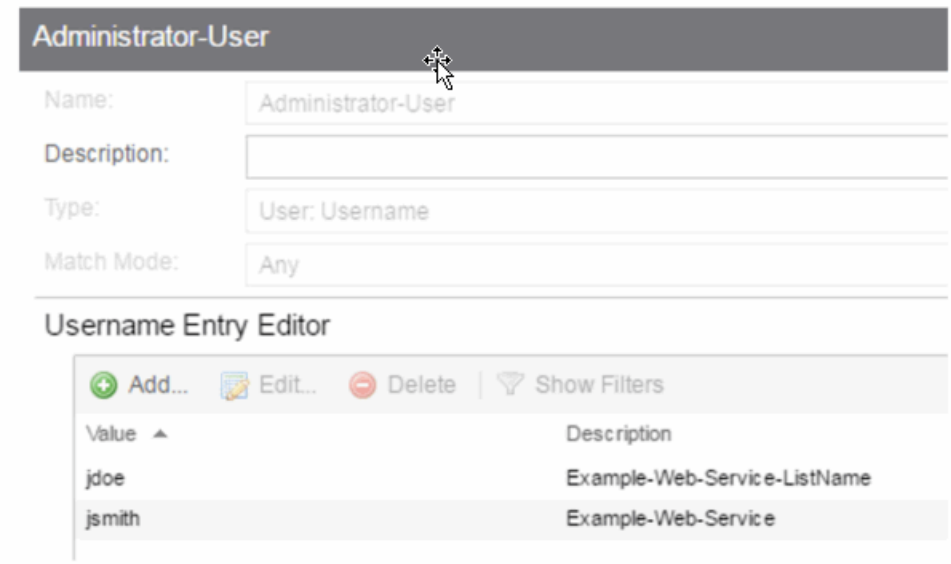
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addValueToNamedList?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true



Method: addValueToNamedListEx

Add a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group. This operation is similar to addValueToNamedList, but returns a verbose message. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
Value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

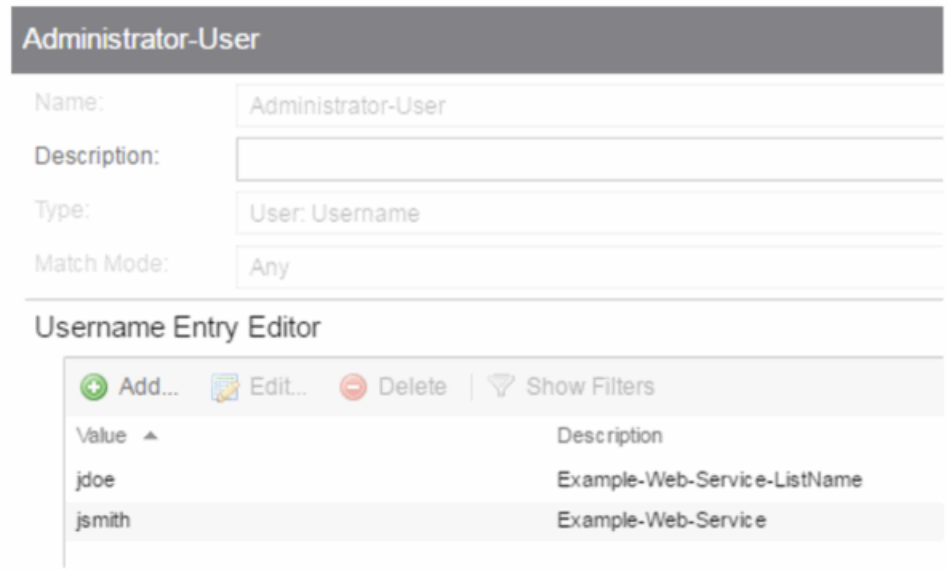
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addValueToNamedListEx?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true



Method: auditEnforceNacAppliances

Enforce changes to a list of Extreme Access Control engines.

Parameters

Name	Type	Description
nacAppliances	string	List of Extreme Access Control engines.

Returns

Returns a WsEnforceApplianceResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/auditEnforceNacAppliances?nacAppliances=192.168.30.35

Method: createMacLock

Create a MAC lock to limit a device to a single switch port.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system
switchIp	string	IP address of the switch to which the end-system is limited
switchPort	string	Switch port to which the end-system is limited

Name	Type	Description
reject	boolean	Set to **true** to reject the authentication request if the end system tries to authentication on a different switch or port
policy	string	Policy that applies if the end-system tries to authenticate to a different switch or port

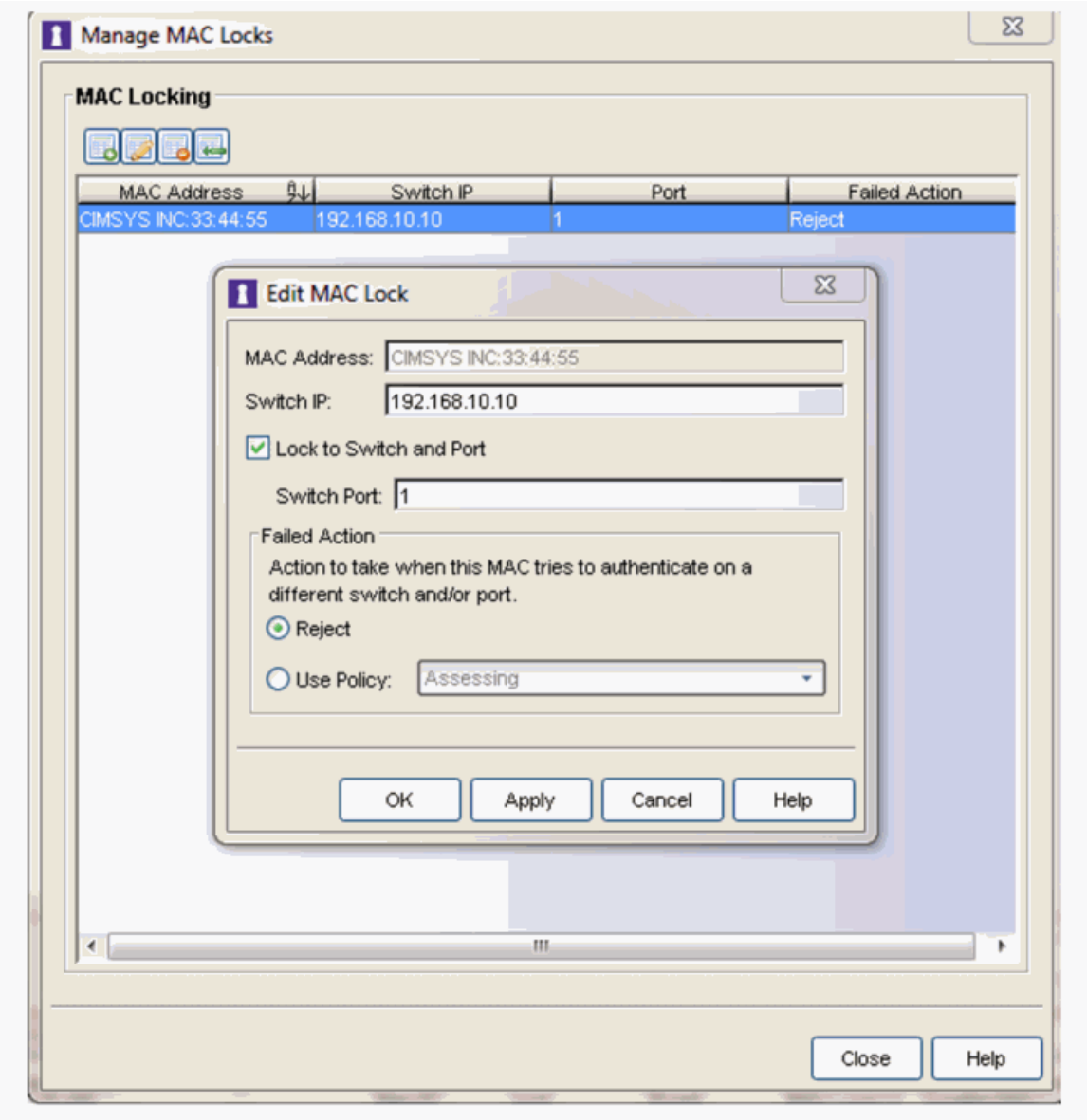
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/createMacLock?mac=00:11:22:33:44:55&switchIp=192.168.10.10&switchPort=1&reject=true



Method: deleteEndSystemByMac

Delete end system based on the end system's MAC address.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system to delete

Name	Type	Description
deleteOptionsMask	int	0x01 – Delete values in named lists 0x02 – Delete MAC locks 0x04 – Delete end-system information 0x08 – Delete registered devices 0x10 – Force delete of end-system

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemByMac?mac=78:E4:00:44:7E:E6&deleteOptionsMask=16

Method: deleteEndSystemInfoByHostname

Delete end-system information record based on the end-system's hostname.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByHostname?hostname=Captain-Obvious.demo.com

Method: deleteEndSystemInfoByIp

Delete end system information record based on the end system's IP address.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByIp?ipAddress=192.168.10.181

Method: deleteEndSystemInfoByMac

Delete end-system information record based on the end-system's MAC address.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByMac?macAddress=14:7D:C5:97:70:CB

method: deleteEndSystemInfoEx

Delete end-system information record based on the end system's MAC address. This operation is similar to deleteEndSystemInfoByMac, but returns a verbose

message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

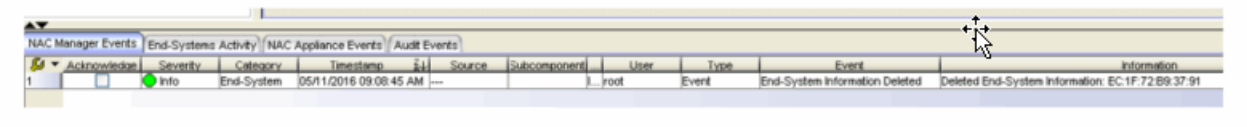
Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system from which you are deleting information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoEx?macAddress=EC:1F:72:B9:37:91



Method: deleteLocalUsers

Delete users from the local user database, specifying the users by a list of local user IDs.

Parameters

Name	Type	Description
localUserIdsCSV	string	The list of local user IDs separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

The operation returns an integer error code.

Example

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsers?localUserIdsCSV=3,4&requestingUser=root

Method: deleteLocalUsersbyLoginIdEx

Delete users from the local user database, specifying the repository and list of usernames.

Parameters

Name	Type	Description
repository	string	The name of the password repository from which you are deleting the user
localUserLoginIdsCSV	string	The list of local usernames separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsersbyLoginIdEx?repository=Default&localUserLoginIdsCSV=jdoe&requestingUser=root

Method: deleteLocalUsersEx

Delete users from the local user database, specifying the users by a list of local user IDs. This operation is similar to deleteLocalUsers, but returns a verbose message.

Parameters

Name	Type	Description
localUserIdsCSV	string	The list of local user IDs separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsersEx?localUserIdsCSV=7&requestingUser=root

Method: deleteMacLock

Delete MAC lock.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteMacLock?mac=00:11:22:33:44:55

Method: deleteRegisteredDevice

Remove a registered device with the matching properties from the database.

Parameters

Name	Type	Description
propString	string	The properties string used to delete the device, string is in the following format: userName=value1,macAdress=value2,applianceGroup=value3
requestingUser	string	The user requesting the deletion

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteRegisteredDevice?propString=userName=jane.smith,macAddress=80:D6:05:4A:D6:C4,applianceGroup=Default&requestingUser=root

Method: deleteRegisteredDevices

Remove registered devices with the matching properties from the database.

Parameters

Name	Type	Description
propStrings	string	The properties string used to delete the device, string is in the following format: userName=value1,macAdress=value2,applianceGroup=value3
requestingUser	string	The user requesting the deletion

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteRegisteredDevices?propStrings=userName=jane.smith,macAddress=80:D6:05:4A:D6:C4,applianceGroup=Default&propStrings=userName=jane.smith,macAddress=50:7A:55:6F:24:35,applianceGroup=Default&requestingUser=root

Method: deleteRegisteredUserAndDevices

Remove a registered user and their associated devices from the database.

Parameters

Name	Type	Description
propString	string	The properties string used to delete the user, string is in the following format: userName=value1,userType=value2,applianceGroup=value3
requestingUser	string	The user requesting this user to be deleted

Returns

The operation returns an integer error code.

Method: deleteRegisteredUsers

Delete a set of registered users in the database.

Parameters

Name	Type	Description
propStrings	string	A list of property strings of users to be deleted from the database, string is in the following format: userName=value1,userType=value2,applianceGroup=value3
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: enforceNacAppliances

Enforce changes to a list of Extreme Access Control engines.

Parameters

Name	Type	Description
nacAppliances	string	List of Extreme Access Control engines
forceMask	long	Mask to disable enforce optimizations, forcing a reset behavior. Options are: 0x0000 – default behavior 0x0001 - force reconfiguration for all switches 0x0002 – force reconfiguration for captive portal
ignoreWarnings	boolean	**True** to ignore configuration warnings

Returns

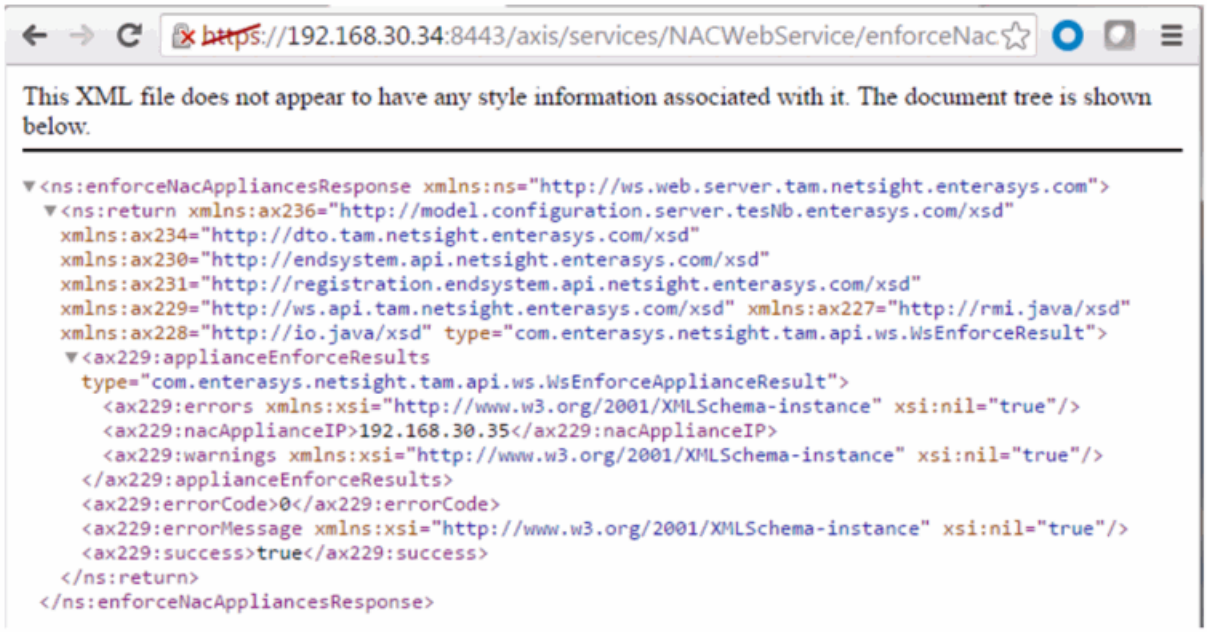
Returns a WsEnforceResult with the structure defined by the following table.

Name	Type	Description
applianceEnforceResults	WsEnforceApplianceResult	Extreme Access Control engine errors or warnings encountered during an enforcement
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/enforceNacAppliances?nacAppliances=192.168.30.35&forceMask=0&ignoreWarnings=true



Method: getAllEndSystemMacs

Return a list of end-system MAC addresses known to Extreme Management Center and Extreme Access Control.

Returns

Returns a list of MAC addresses.

Name	Type	Description
Return	string	List of MAC addresses

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getAllEndSystemMacs

Method: getAllEndSystems

Returns data for all end-systems known to Extreme Management Center and Extreme Access Control. This operation can be data intensive on both the Extreme Management Center server and client requesting the operation. The response is stored in memory, so the client (PHP) may need to increase memory.

Returns

Returns a list of end-system data.

Name	Type	Description
Return	string	List of end-system data

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getAllEndSystems

Method: getEndSystemAndHrByMac

Returns end-system data, based on a MAC address, and it's most recent health result and vulnerabilities.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns end-system data and most recent health result.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemAndHrByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByIp

Return end-system data based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIp?ipAddress=192.168.10.190

Method: getEndSystemByIpEx

Return end-system data based on an IP address. The operation is similar to getEndSystemByIp, but returns additional information.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIpEx?ipAddress=192.168.10.190

Method: getEndSystemByMac

Return end-system data based on a MAC address.

Parameters

Name	Type	Description
ipAddress	string	MAC address of the end-system

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByMacEx

Return end-system data based on a MAC address. The operation is similar to getEndSystemByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data

Name	Type	Description
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByMacEx?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoArrByMac

Return end-system data based on a MAC Address. The data is returned, in an array, as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

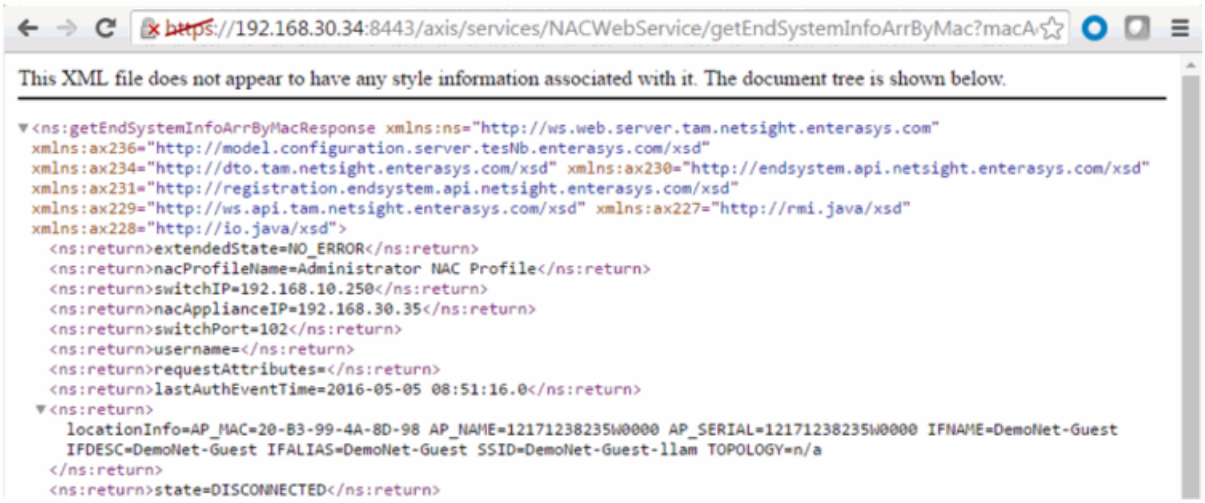
Returns

Returns an array of end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemInfoArrByMac?macAddress=00:88:65:66:03:C1



Method: getEndSystemInfoByMac

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemInfoByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoByMacEx

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result. The operation is similar to getEndSystemInfoByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data

Name	Type	Description
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Method: getEndSystemsByMacEx

Return end-system data based on a MAC address(es).

Parameters

Name	Type	Description
macAddresses	string	MAC addresses of the end-systems

Returns

Returns a WsEndSystemList with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemsByMacEx?macAddresses=00:88:65:66:03:C1&macAddresses=EC:1F:72:B9:37:91

Method: getExtendedEndSystemArrByMac

Return an extended set of data for an end-system based on a MAC address. The data includes additional information such as ELIN, portAlias, etc. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an array of end system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getExtendedEndSystemArrByMac?macAddress=00:88:65:66:03:C1

Method: getExtendedEndSystemByMac

Return an extended set of data for an end-system based on a MAC address. The data includes additional information such as ELIN, portAlias, etc. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an extended set of end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getExtendedEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getLocalUser

Return a local user from the user database.

Parameters

Name	Type	Description
passwordRepository	string	Password repository in which the user is saved
loginId	string	The username of the user

Returns

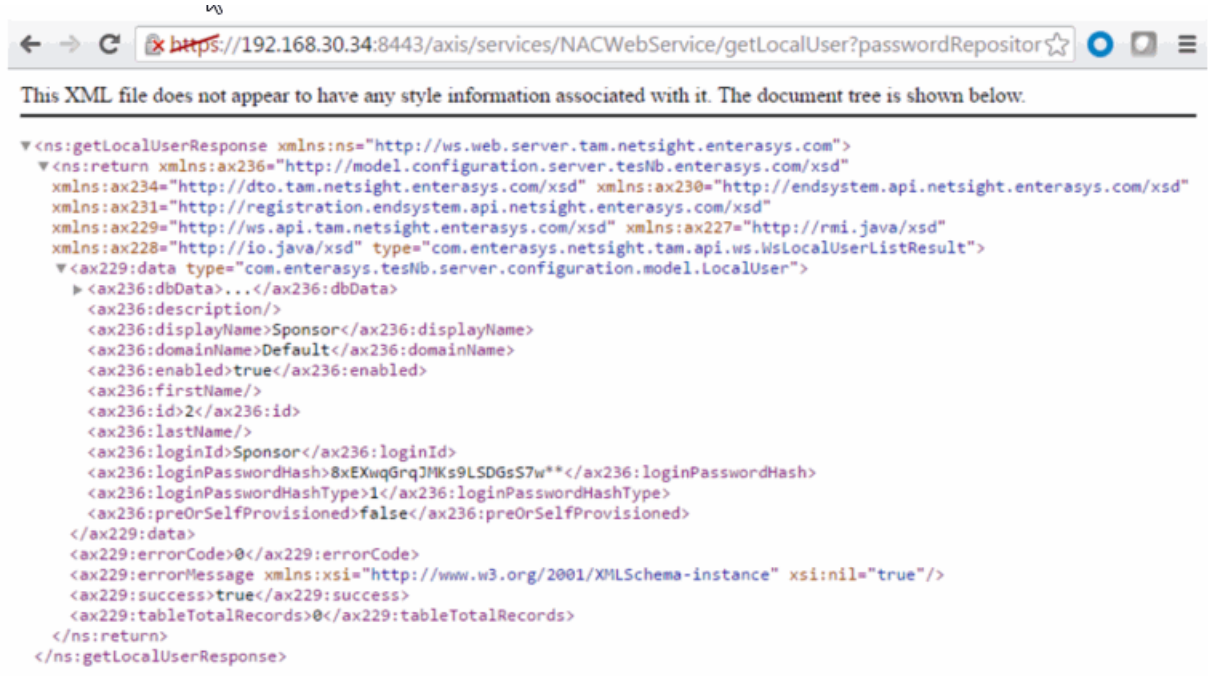
Returns a WsLocalUserListResult with a structure defined by the following table.

Name	Type	Description
data	LocalUser	User information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getLocalUser?passwordRepository=Default&loginId=Sponsor



Method: getNACVersion

Return the Extreme Access Control version.

Returns

Returns Extreme Access Control version.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getNACVersion

Method: getPollerStatus

Return the last polling status of an Extreme Access Control engine.

Parameter

Name	Type	Description
nacIP	string	IP address of an Extreme Access Control engine

Returns

Returns true/false for the Extreme Access Control engine's last polling status.

Example

https://192.168.30.34:8443/axis/services/NACWebService/getPollerStatus?nacIP=192.168.30.35

Method: getRegisteredDevicesByMacAddress

Retrieve an array of registered devices as KEY=VALUE comma separated string based on a MAC address.

Parameters

Name	Type	Description
macAddress	string	MAC address of the registered device

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegisteredDevicesByMacAddress?macAddress=50:7A:55:6F:24:35

Method: getRegisteredUsersByUsername

Retrieve an array of registered users as KEY=VALUE comma separated string.

Parameters

Name	Type	Description
username	string	Username of the registered user

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegisteredUsersByUsername?username=jane.smith

Method: getRegistredDevicesByUsername

Retrieve an array of registered devices as KEY=VALUE comma-separated string based on a username.

Parameters

Name	Type	Description
username	string	Username of the registered user

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegistredDevicesByUsername?username=jane.smith

Method: getRegistredUsersByMacAddress

Retrieve an array of registered users as KEY=VALUE comma separated string based on a MAC address.

Parrameters

Name	Type	Description
macAddress	string	MAC address of the registered device

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegistredUsersByMacAddress?macAddress=50:7A:55:6F:24:35

Method: getUnsurfacedNamedList

Return the contents of a named list/end-system group without manipulation.

Parameters

Name	Type	Description
listName	string	End-system group name

Returns

Returns a string array that contains the XML representation of values, description, and data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getUnsurfacedNamedList?listName=Registered Guests

Method: hashLocalUserPassword

Generate a hashed password for a local user.

Parameters

Name	Type	Description
password	string	Password in clear text

Returns

Returns a hashed password.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/hashLocalUserPassword?password=MySuperDuperSecurePassword

Method: hashLocalUserPasswordEx

Generate a hashed password for a local user.

Parameters

Name	Type	Description
Password in clear text	Password in clear text	Password in clear text
hashAlgorithm	int	Hashing algorithm, available options are: 0 - SHA1 non reversible hash 1 - PKCS5 reversible hash

Returns

Returns a hashed password.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/hashLocalUserPasswordEx?password=MySuperDuperSecurePassword&hashAlgorithm=1

Method: importEndSystemInfoEx

Save a batch of end system information.

Parameters

Name	Type	Description
infoList	EndSystemInfo	An array of end-system information
isSave	Boolean	**True** to save end-system information, **false** to delete it

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: importEndSystemInfoFromCsv

Save a batch of end-system information provided by a CSV file.

Parameters

Name	Type	Description
csvData	string	A string version of CSV file with new line delimiters
isSave	boolean	**True** to save end-system information, **false** to delete it

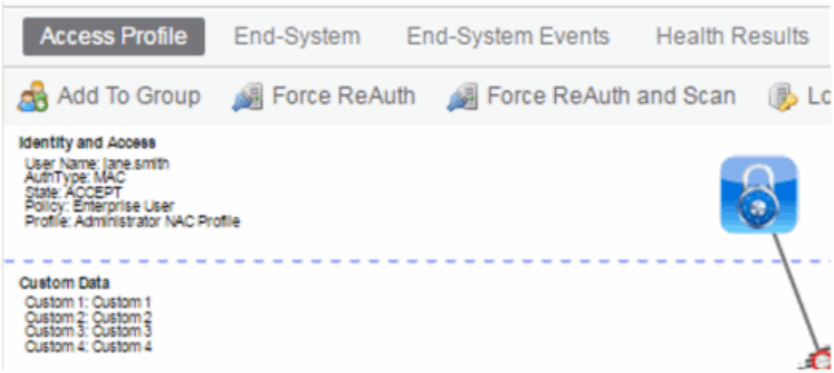
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/importEndSystemInfoFromCsv?csvData=50:7A:55:6F:24:35,Custom 1,Custom 2,Custom 3,Custom 4&isSave=true



Method: processNacRequestArrFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End-system override (FULL_MAC) – MAC address, end-system group, description End-system override (FULL_IP) – IP address, end-system group, description End-system override (HOSTNAME) – hostname, end-system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end-system override useroverride – user override
isAdd	Boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

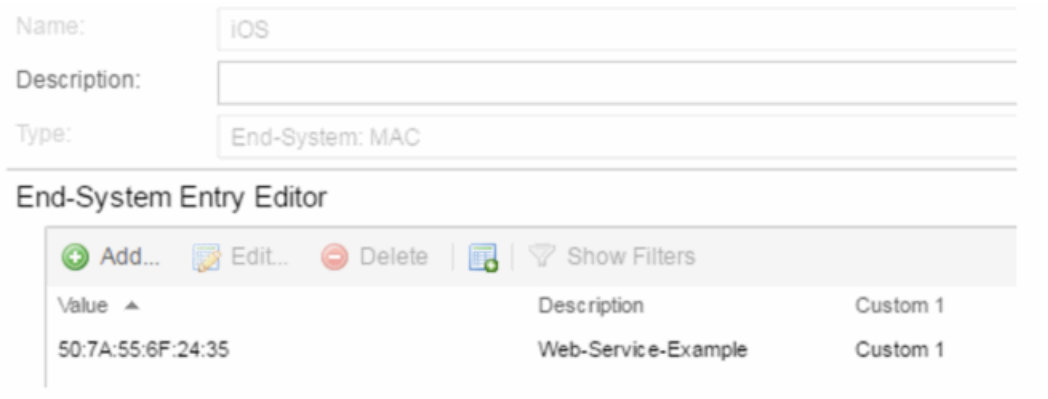
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/processNacRequestArrFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC



Method: processNacRequestFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End system override (FULL_MAC) – MAC address, end-system group, description End system override (FULL_IP) – IP address, end-system group, description End system override (HOSTNAME) – hostname, end-system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end-system override useroverride – user override
isAdd	Boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

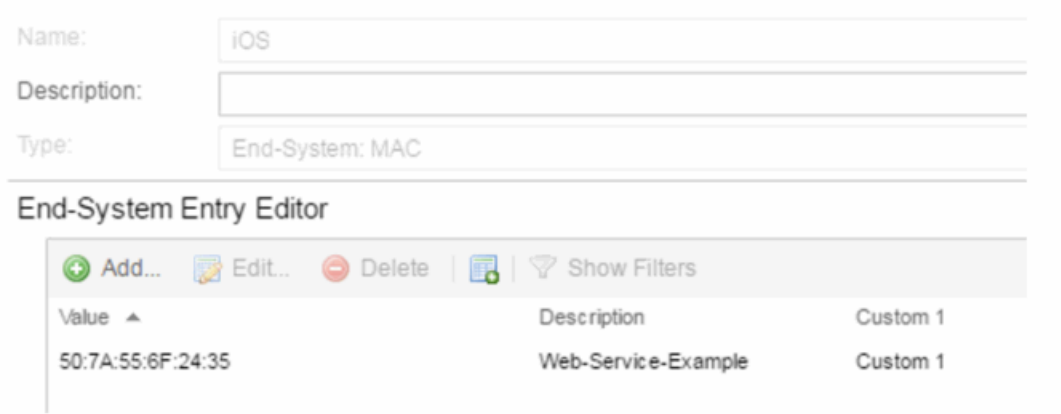
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/processNacRequestFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC



Method: reauthenticate

Force an end-system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/reauthenticate?macAddress=50:7A:55:6F:24:35&assess=false

Method: reauthenticateEx

Force an end-system to reauthenticate. This operation is similar to reauthenticate, but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

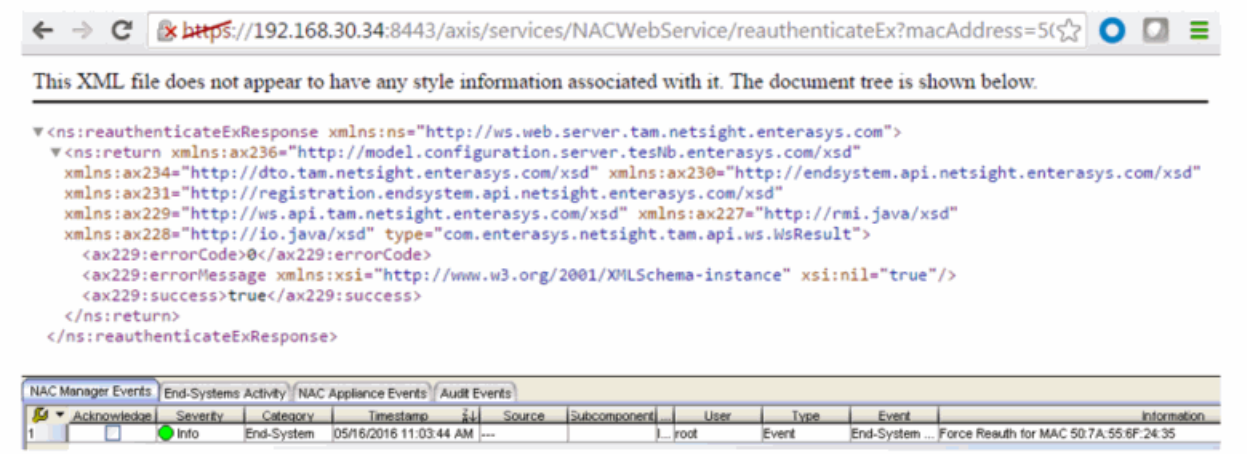
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/reauthenticateEx?macAddress=50:7A:55:6F:24:35&assess=false



Method: removeHostnameFromEndSystemGroup

Remove an end-system hostname from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
hostname	string	The hostname of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

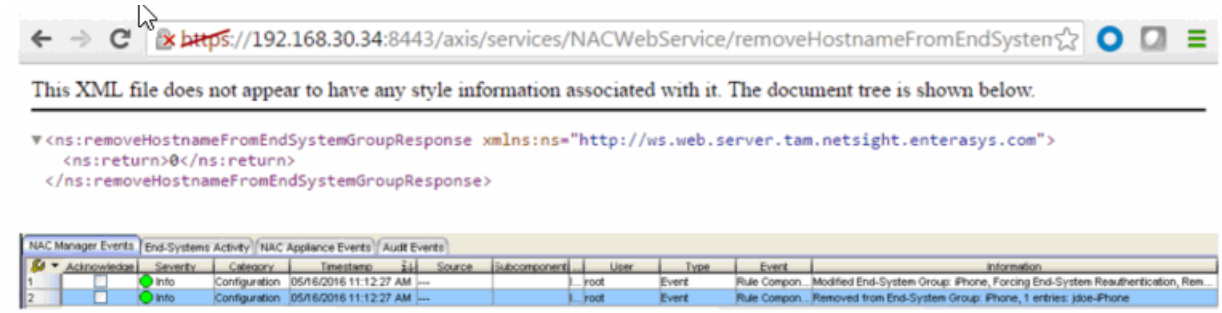
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeHostnameFromEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&reauthenticate=true



Method: removeHostnameFromEndSystemGroupEx

Remove an end-system hostname from an Extreme Access Control end-system group. This operation is similar to removeHostnameFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
hostname	string	The hostname of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

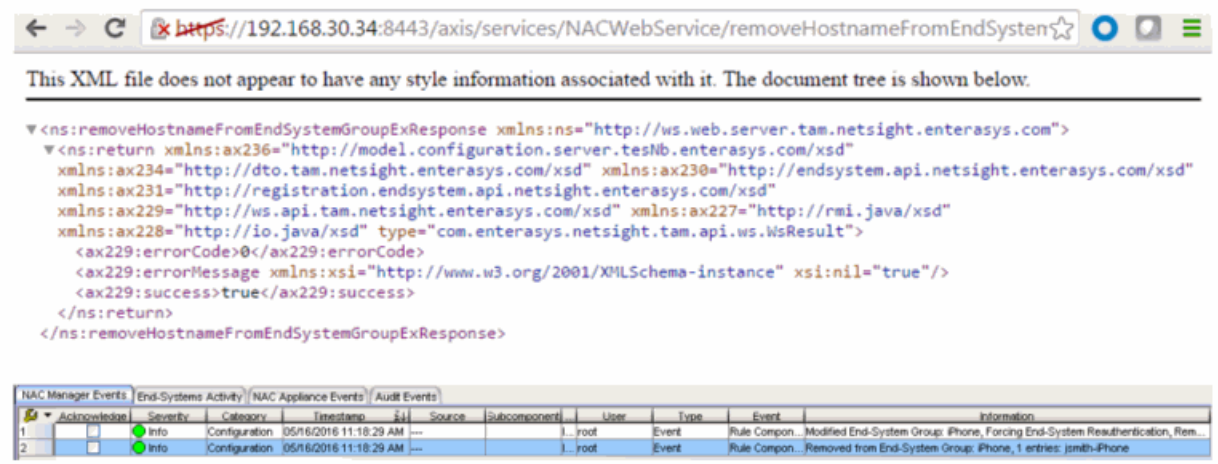
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeHostnameFromEndSystemGroupEx?endSystemGroup=iPhone&hostname=jsmith-iPhone&reauthenticate=true



Method: removeIPFromEndSystemGroup

Remove an end system IP address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
ipAddress	string	IP address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

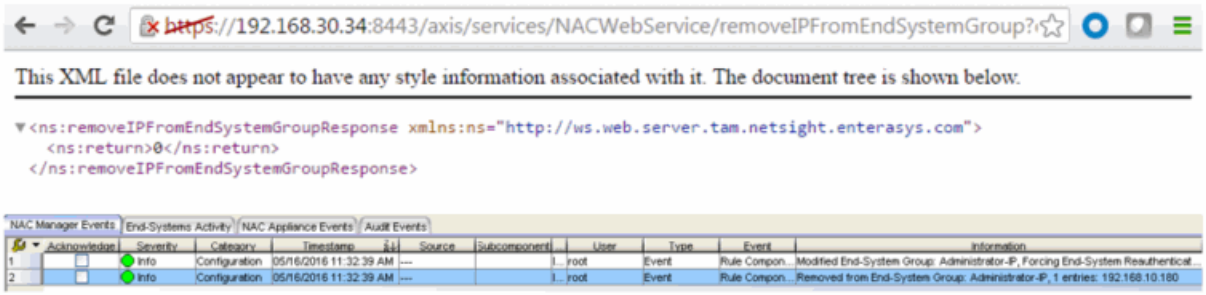
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeIPFromEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&reauthenticate=true



Method: removeIPFromEndSystemGroupEx

Remove an end-system IP address from an Extreme Access Control end-system group. This operation is similar to removeIPFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
ipAddress	string	IP address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

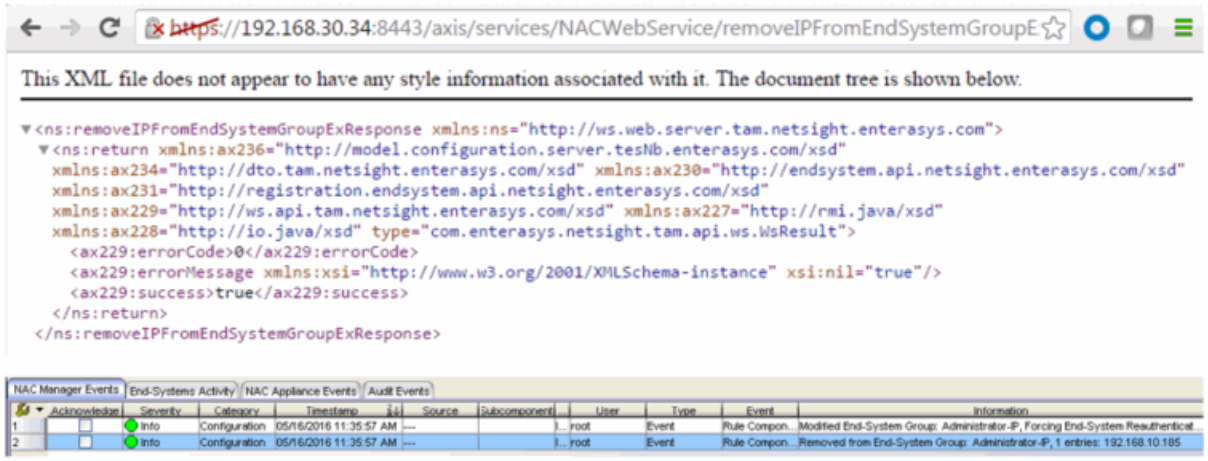
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeIPFromEndSystemGroupEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.185&reauthenticate=true



Method: removeMACFromBlacklist

Remove an end-system MAC address from the blacklist end-system group.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

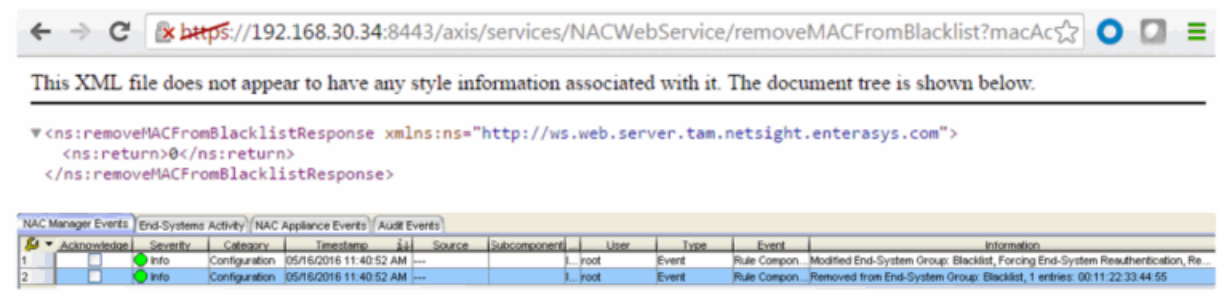
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromBlacklist?macAddress=00:11:22:33:44:55&reauthenticate=true



Method: removeMACFromBlacklistEx

Remove an end-system MAC address from the blacklist end-system group. This operation is similar to removeMACFromBlacklist, but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

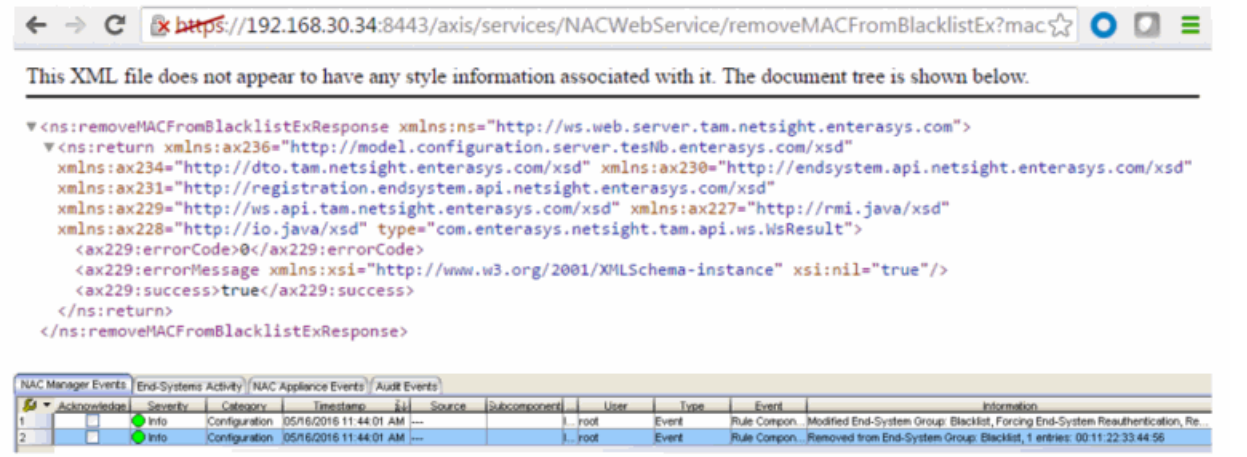
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromBlacklistEx?macAddress=00:11:22:33:44:56&reauthenticate=true



Method: removeMACFromEndSystemGroup

Remove an end-system MAC address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

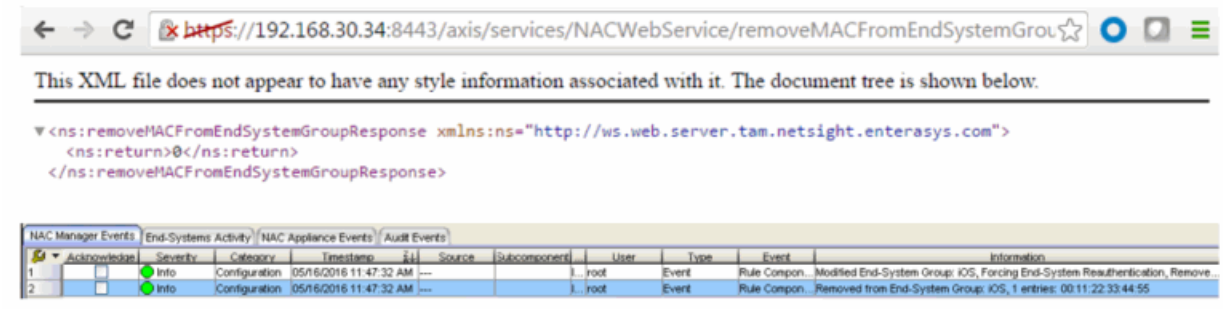
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromEndSystemGroup?endSystemGroup=iOS&macAddress=00:11:22:33:44:55&reauthenticate=true



Method: removeMACFromEndSystemGroupEx

Remove an end-system MAC address from an Extreme Access Control end-system group. This operation is similar to removeMACFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

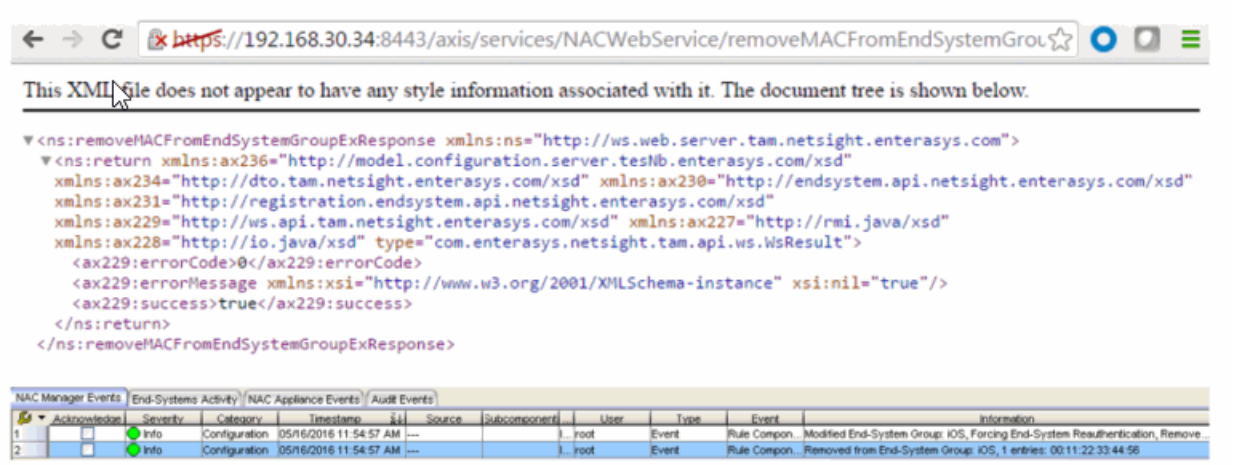
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromEndSystemGroupEx?endSystemGroup=iOS&macAddress=00:11:22:33:44:56&reauthenticate=true



Method: removeUsernameFromUserGroup

Remove a username from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
usergroup	string	The username group name you are changing
username	string	Username of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

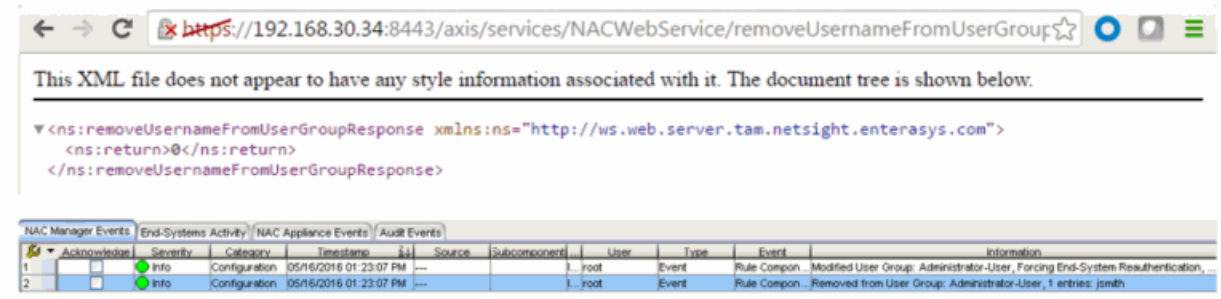
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeUsernameFromUserGroup?userGroup=Administrator-User&username=jsmith&reauthenticate=true



Method: removeUsernameFromUserGroupEx

Remove a username from an Extreme Access Control end-system group. This operation is similar to removeUsernameFromUserGroup, but returns a verbose message.

Parameters

Name	Type	Description
userGroup	string	The username group name you are changing
username	string	Username of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

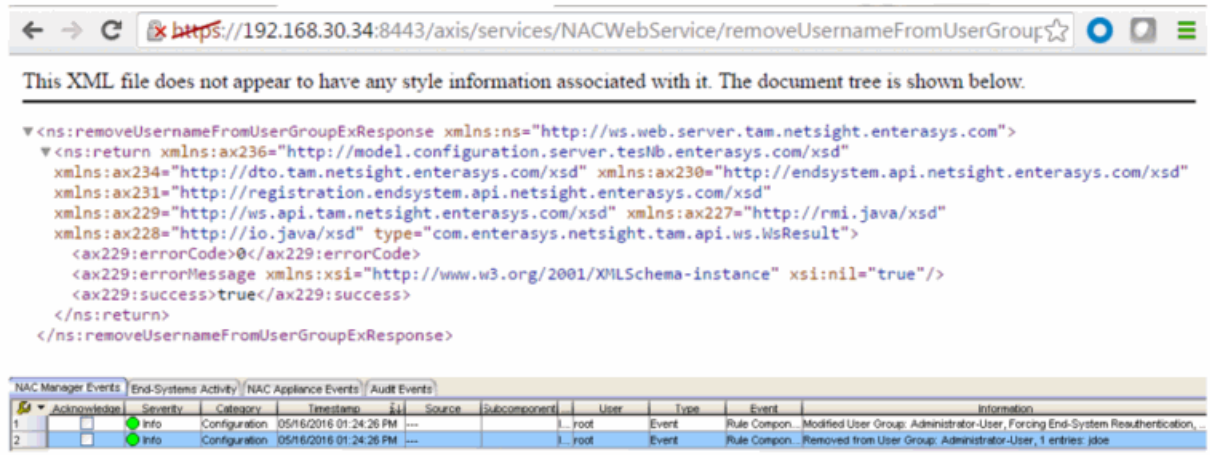
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeUsernameFromUserGroupEx?userGroup=Administrator-User&username=jdoe&reauthenticate=true



Method: removeValueFromNamedList

Remove a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

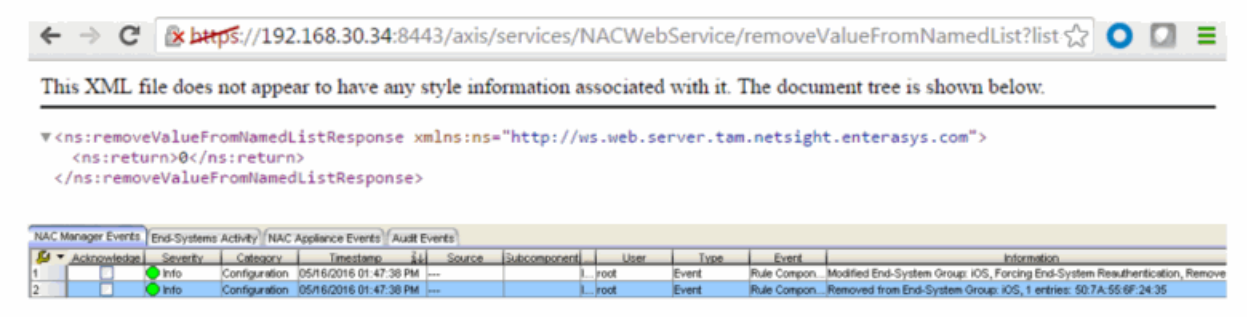
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeValueFromNamedList?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true



Method: removeValueFromNamedListEx

Remove a value to an Extreme Access Control end-system group. This operation is similar to removeValueFromNamedList, but returns a verbose message.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

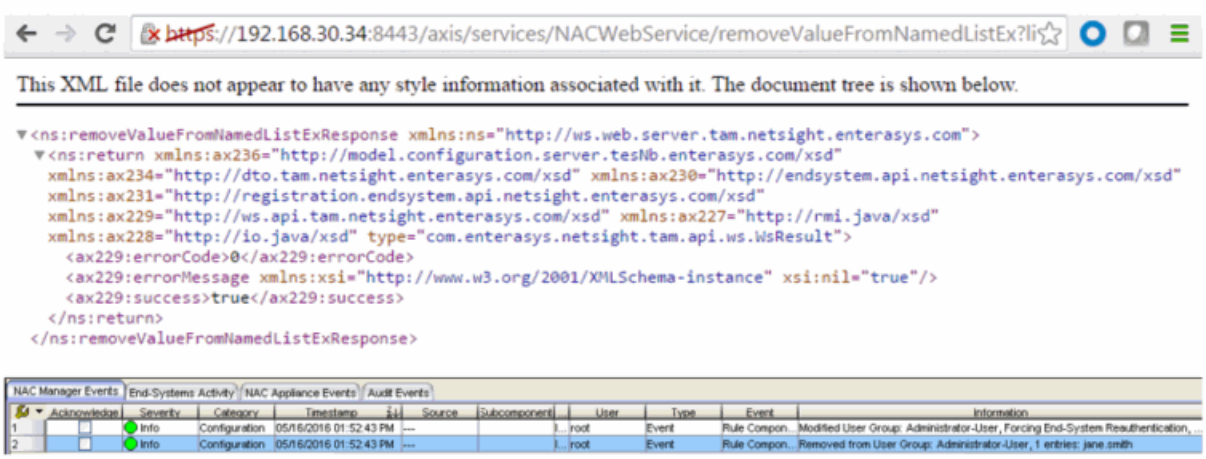
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeValueFromNamedListEx?list=Administrator-User&value=jane.smith&reauthenticate=true



Method: saveEndSystemInfo

Update end-system information. The end-system is identified by using the macAddress, ipAddress, or hostname property.

Parameters

Name	Type	Description
properties	string	Custom field data in custom1=value1,custom2=value2,custom3=value3,custom4=value4 format

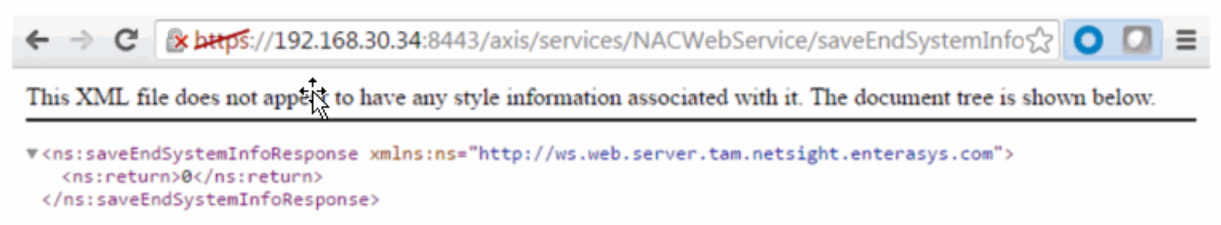
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfo?properties=macAddress=EC:1F:72:B9:37:91,custom1=Custom1,custom2=Custom2,custom3=Custom3,custom4=Custom4



Method: saveEndSystemInfoByHostname

Update end-system information.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

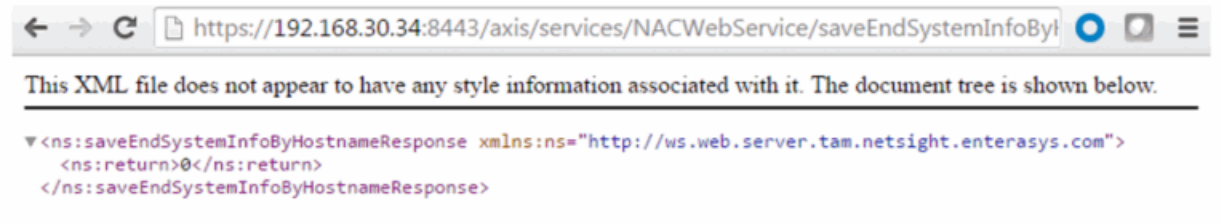
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByHostname?hostname=MacBookPro.demo.com&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByIp

Update end-system information.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

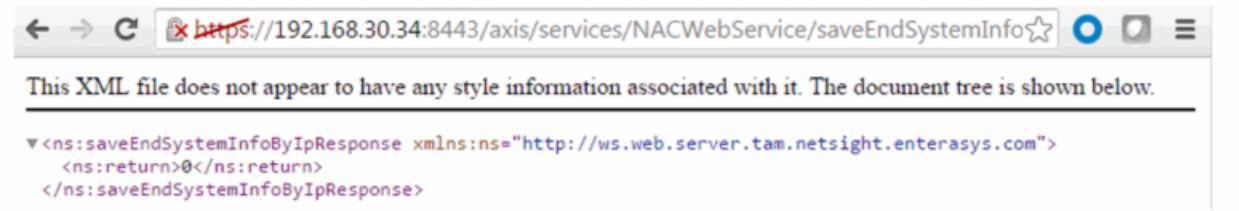
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByIp?ipAddress=192.168.10.178&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByMac

Update end-system information.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Name	Type	Description
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

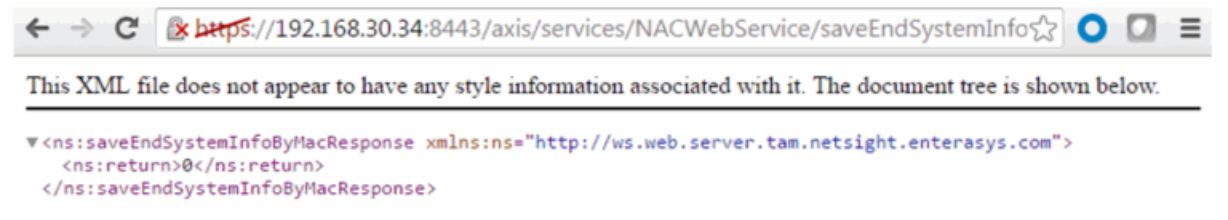
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByMac?macAddress=80:A5:89:33:67:37&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoEx

Update end-system information.

Parameters

Name	Type	Description
info	EndSystemInfo	End-system information you are saving

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system for which information is saved

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: saveLocalUser

Create or update a user in the local user database.

Parameters

Name	Type	Description
propString	string	The properties string used to create/update the user, string is in the following format: loginId=value1,domainName=value2,description =value3,enabled=true,password=value4
propString	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveLocalUser?propString=loginId=jdoe,domainName=Default,description=Sample-User,enabled=true,password=mysuperduperpassword

Method: saveLocalUserEx

Create or update a user in the local user database.

Parameters

Name	Type	Description
user	LocalUser	Local user to save in the database
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: saveRegisteredDevice

Create a new registered device.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state= Approved,description =value4,applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: saveRegisteredDeviceEx

Create a new registered device.

Parameters

Name	Type	Description
device	RegisteredDevice	Device to register
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: saveRegisteredDevices

Create a new registered device.

Parameters

Name	Type	Description
propStrings	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state= Approved,description=value4, applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredDevi

ces?propStrings=userName=jane.smith,macAddress=80:D6:05:4A:D6:C5,state=Approved,applianceGroup=Default&requestingUser=root

Method: saveRegisteredDeviceWithSponsorship

Create a new registered device with sponsorship.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state=Approved, description=value4,applianceGroup=value5
requestingUser	string	The user requesting the operation
defaultSponsorEmail	string	Sponsor email address
nacApplianceIp	string	Extreme Access Control engine IP address

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredDeviceWithSponsorship?propString=userName=jane.smith,macAddress=80:D6:05:4A:D6:C5,state=Approved,applianceGroup=Default&requestingUser=root&defaultSponsorEmail=jdoe@jdoe.com&nacApplianceIp=192.168.30.35

Method: saveRegisteredDeviceWithSponsorshipEx

Create a new registered device with sponsorship.

Parameters

Name	Type	Description
device	RegisteredDevice	Device to register
requestingUser	string	The user requesting the operation
defaultSponsorEmail	string	Sponsor email address
nacApplianceIp	string	Extreme Access Control engine IP address

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: saveRegisteredUser

Create a new registered user.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2

Name	Type	Description
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredUser?propString=userName=john.doe,applianceGroup=Default&requestingUser=root

Method: saveRegisteredUserEx

Create a new registered user.

Parameters

Name	Type	Description
user	RegisteredUser	User to register
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: saveRegisteredUsers

Create a new registered user.

Parameters

Name	Type	Description
propStrings	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2
requestingUser	string	The user requesting the operation

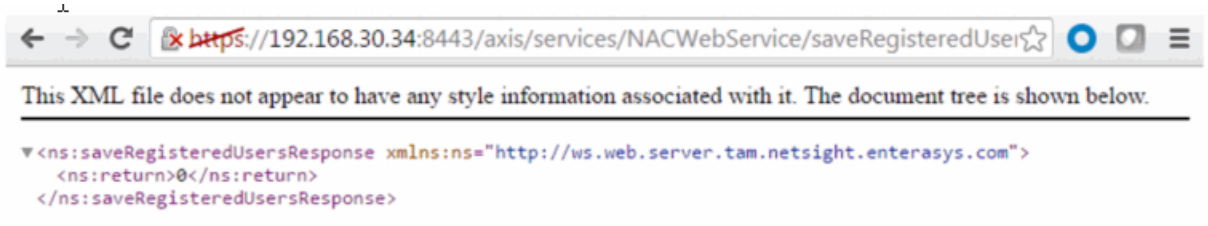
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredUsers?propStrings=userName=john.smith,applianceGroup=Default&requestingUser=root



Method: updateRegisteredDevice

Update an existing registered device.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress=value2, ipAddress=value3,state=Approved, description=value4,applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: updateRegisteredUser

Update an existing registered user.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2
requestingUser	string	The user requesting the operation

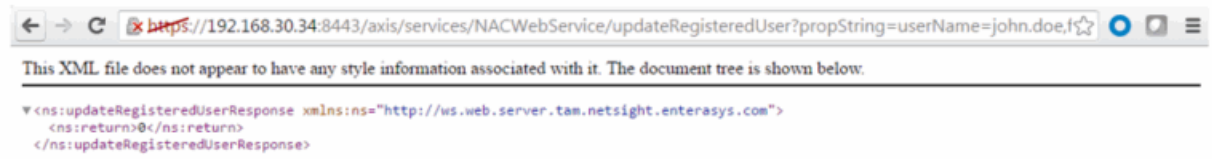
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/updateRegisteredUser?propString=userName=john.doe,firstName=John,lastName=Doe,applianceGroup=Default&requestingUser=root



Netsight Device Web Service

The NetSight device web service provides an external interface to retrieve and modify the managed devices in the database.

https://<Extreme Management Center Server IP>:<port>/axis/services/NetSightDeviceWebService?wsdl

Method: addAuthCredential

Add a command line interface credential to the database.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

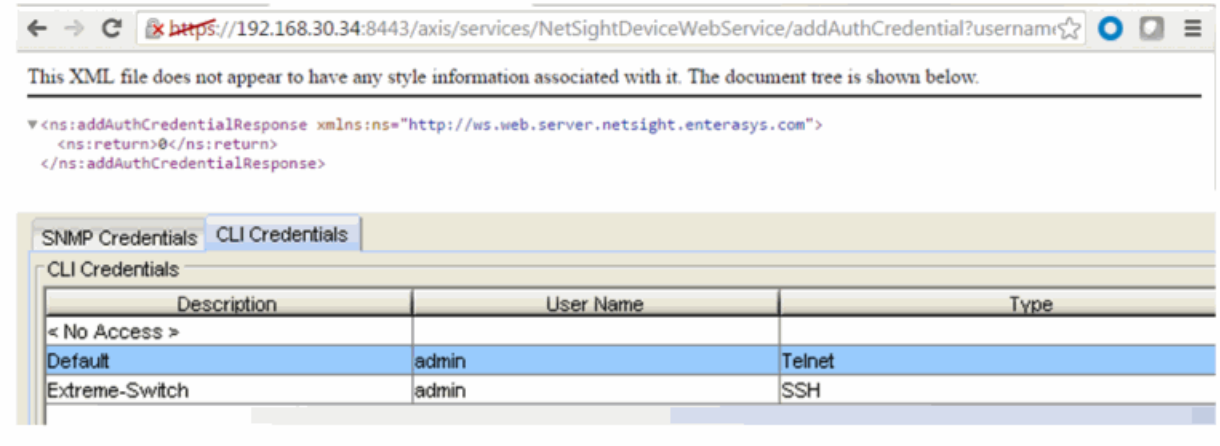
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addAuthCredential?username=admin&description=Extreme-

Switch&loginPassword=password&enablePassword=&configurationPassword=&type=SSH



Method: addAuthCredentialEx

Add a command line interface credential to the database. This operation is similar to addAuthCredential, but returns a verbose message.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

Returns a NsWsResult with a structure defined by the following table.

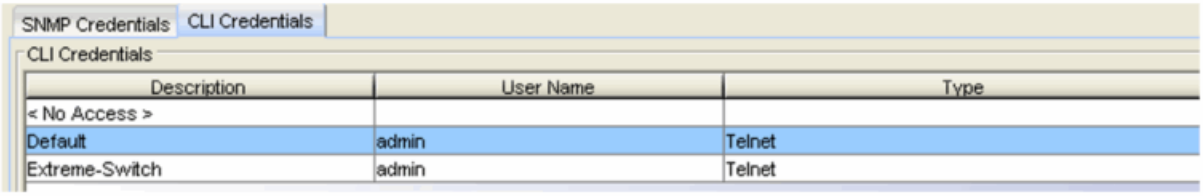
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes

Name	Type	Description
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addAuthCredentialEx?username=admin&description=Extreme-Switch&loginPassword=password&enablePassword=&configurationPassword=&type=Telnet



Method: addCredentialEx

Add a SNMP credential to the database.

Parameters

Name	Type	Description
name	string	Name of the credential
snmpVersion	int	SNMP version
communityName	string	SNMP community name
userName	string	SNMPv3 username

Name	Type	Description
authPassword	string	SNMPv3 authentication password
authType	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privPassword	string	SNMPv3 privacy password
privType	string	SNMPv3 privacy type, available options are: -AED -DES

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addCredentialEx?name=SNMPv2-Readonly&snmpVersion=2&communityName=readonly&userName=&authPassword=&authType=&privPasswod=&privType=

Method: addDeviceEx

Add a device to the database.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device
profileName	string	Profile name associated to the device
snmpContext	string	SNMP context associated to the device
nickName	string	Device nickname

Returns

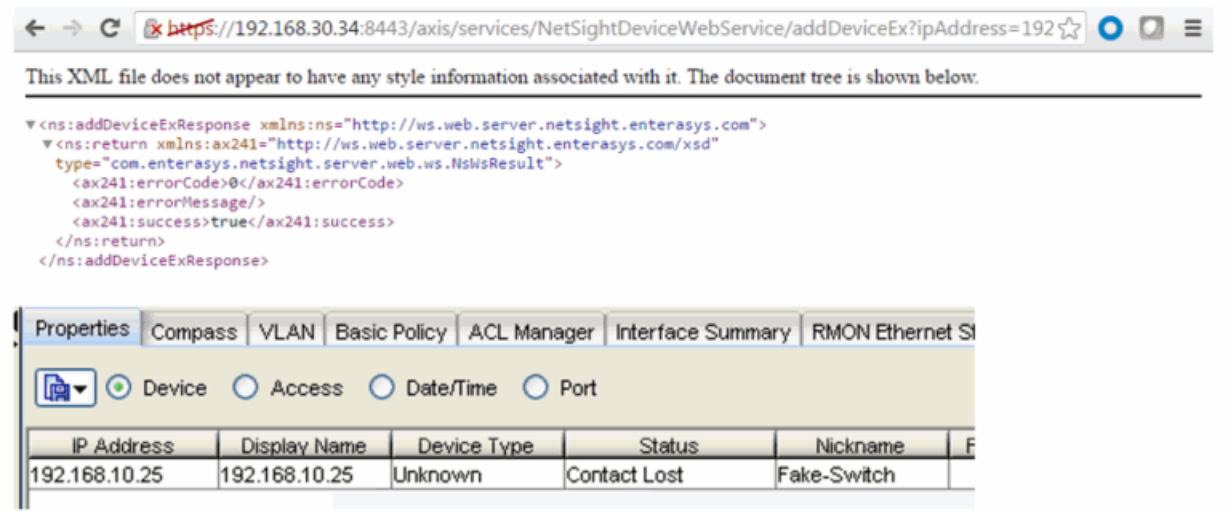
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addDeviceEx?ipAddress=192.168.10.25&profileName=public_v1_Profile&snmpContext=&nickName=Fake-Switch



Method: addProfileEx

Add credential profile to the database.

Parameters

Name	Type	Description
name	string	Name of the profile
snmpVersion	int	SNMP version
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
auth	string	CLI credential

Returns

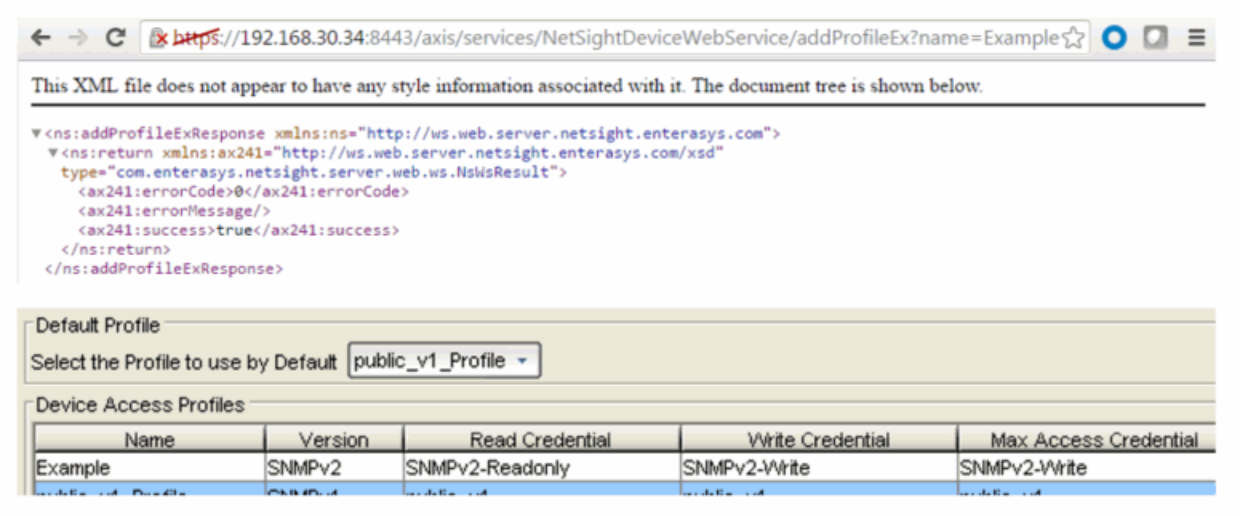
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addProfileEx?name=Example&snmpVersion=2&read=SNMPv2-Readonly&write=SNMPv2-Write&maxAccess=SNMPv2-Write&auth=Extreme-Switch



Method: deleteDeviceByIpEx

Delete a device from the database.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/deleteDeviceByIpEx?ipAddress=192.168.10.25

Method: exportDevicesAsNgf

Export all devices in a NetSight grouping format.

Returns

Returns a string representation of all devices from the database.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/exportDevicesAsNgf

Method: getAllDevices

Retrieve all the devices from the database.

Returns

Returns a WsDeviceListResult with a structure defined by the following table.

Name	Type	Description
data	WsDevice	Device Information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getAllDevices

Method: getDeviceByIpAddressEx

Retrieve the device based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceListResult with a structure defined by the following table.

Name	Type	Description
data	WsDevice	Device Information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getDeviceByIpAddressEx?ipAddress=192.168.10.10

Method: getSnmpCredentialAsNgf

Retrieve SNMP credentials, in NetSight Grouping Format, for a device.

Parameters

Name	Type	Description
ipAddress	string	

Returns

Returns a string representation of device settings from the database.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getSnmpCredentialAsNgf?ipAddress=192.168.10.10

Method: importDevicesAsNgfEx

Import a list of devices, in NetSight grouping format, to the database.

Parameters

Name	Type	Description
ngfDevices	string	Devices in NetSight grouping format

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/importDevicesAsNgfEx?ngfDevices=cliUsername=admin cliType=Telnet snmp=v1 dev=192.168.10.25 mt=2 pg=1 ro=public rw=public su=public cliDesc=Default cliUsername=admin cliType=Telnet snmp=v1

Method: isIpV6Enabled

Queries the Extreme Management Center server to determine if IPv6 support is enabled.

Returns

Returns **true** if IPv6 is supported.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/isIpV6Enabled

Method: isNetSnmpEnabled

Queries the Extreme Management Center server to determine if the Net SNMP stack is enabled.

Returns

Returns true if IPv6 is supported.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/isNetSnmpEnabled

Method: updateAuthCredential

Update command line interface credentials.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateAuthCredential?username=admin&description=Extreme-Switch&loginPassword=login&enablePassword=enable&configurationPassword=config&type=SSH

Method: updateAuthCredentialEx

Update command line interface credentials. This operation is similar to updateAuthCredential, but returns a verbose message.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateAuthCredentialEx?username=admin&description=Extreme-Switch&loginPassword=login&enablePassword=enable&configurationPassword=config&type=Telnet

Method: updateCredential

Update SNMP credential.

Parameters

Name	Type	Description
name	string	Name of the credential
communityName	string	SNMP version
userName	string	SNMP community name
authPassword	string	SNMPv3 username
authType	string	SNMPv3 authentication password
privPassword	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privType	string	SNMPv3 privacy password
		SNMPv3 privacy type, available options are: -AED -DES

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateCredential?name=SNMPv2-Readonly&snmpVersion=2&communityName=public&userName=&authPassword=&authType=&privPasswod=&privType=

Method: updateCredentialEx

Update SNMP credential. This operation is similar to updateCredential, but returns a verbose message.

Parameters

Name	Type	Description
name	string	Name of the credential
communityName	string	SNMP version
userName	string	SNMP community name
authPassword	string	SNMPv3 username
authType	string	SNMPv3 authentication password
privPassword	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privType	string	SNMPv3 privacy password
		SNMPv3 privacy type, available options are: -AED -DES

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateCredentialEx?name=SNMPv2-Readonly&snmpVersion=2&communityName=Read_Only&userName=&authPassword=&authType=&privPasswod=&privType=

Method: updateDevicesEx

Update a set of devices in the database.

Parameters

Name	Type	Description
devices	string	Updated devices to be saved in the database

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: updateProfile

Update credential profile in the database.

Parameters

Name	Type	Description
name	string	Name of the profile
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
authCred	string	CLI credential

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateProfile?name=Example&read=public_v2&write=SNMPv2-Write&maxAccess=SNMPv2-Write&authCred=Default

Method: updateProfileEx

Update credential profile in the database. This operation is similar to updateProfile, but returns a verbose message.

Parameters

Name	Type	Description
name	string	Name of the profile
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
authCredName	string	CLI credential

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateProfileEx?name=Example&read=public_v2&write=public_v2&maxAccess=SNMPv2-Write&authCredName=Extreme-Switch

Policy Web Service

The Policy web service provides an external interface to Policy Manager.

https://<Extreme Management Center Server IP>:<port>/axis/services/PolicyService?wsdl

Method: addRoleMapping

Add an IP or MAC role mapping to the specified switches.

Parameters

Name	Type	Description
station	string	IP/MAC address to add
role	string	Role name to map station to
devices	string	IP address of the switches

Returns

The operation returns an integer error code.

Error Code	Description
0	Operation successful
1	General error
2	Truststore missing
3	Bad parameters
4	Timeout
5	Connection refused
6	Connection reset
7	No server
8	Unauthorized transport
9	Server communication failed
10	Policy domain lock failure
11	Policy domain save failure
12	Nonvolatile mapping exists

Error Code	Description
13	Mapping role not found
14	Mapping unknown device

Method: addRule

Add a rule to a service in a specified policy domain. The policy domain and service you are creating if they do not exist.

Parameters

Name	Type	Description
domainName	string	Policy domain to which to add the rule
serviceName	string	Service to which to add the rule
ruleName	string	Rule name, a null or AUTO value generates the name based on the traffic description data

Name	Type	Description
trafficDescrType	string	Rule type, available options are: 1 – Ethernet type 2 – LLC DSAP SSAP 3 – IP type of service 4 – IP protocol 5 – IPX class of service 6 – IPX packet type 7 – Source IP address 8 – Destination IP address 9 – Bilateral IP address 10 – Source IPX network 11 – Destination IPX network 12 – Bilateral IPX network 13 – UDP source port 14 – UDP destination port 15 – UDP bilateral port 16 – TCP source port 17 – TCP destination port 18 – TCP bilateral port 19 – IPX source socket 20 – IPX destination socket 21 – IPX bilateral socket 22 – Source MAC address 23 – Destination MAC address 24 – Bilateral MAC address 25 – IP fragment 26 – IP UDP source port range 27 – IP UDP destination port range 28 – IP UDP bilateral port range 29 – IP TCP source port range 30 – IP TCP destination port range 31 – IP TCP bilateral port range 32 – ICMP Type 33 – VLAN ID 34 – TCI 43 – IPv6 source address 44 – IPv6 destination address 45 – IPv6 bilateral address

Name	Type	Description
		46 – IPv6 source socket 47 – IPv6 destination socket 48 – IPv6 bilateral socket 49 – IPv6 type 50 – IPv6 flow label
trafficDescrValue	string	Value associated with the rule
trafficDescrMask	string	Mask associated with value, use 0 for no mask
expandedTrafficDescrValue	string	Additional value for rules that require multiple values i.e. TCP port + IP address
expandedTrafficDescrMask	string	Mask associated to the additional value, only applicable to multiple value rules
vlanAction	string	VLAN action, available options are: -1 – None 0 – Discard 4095 – Permit

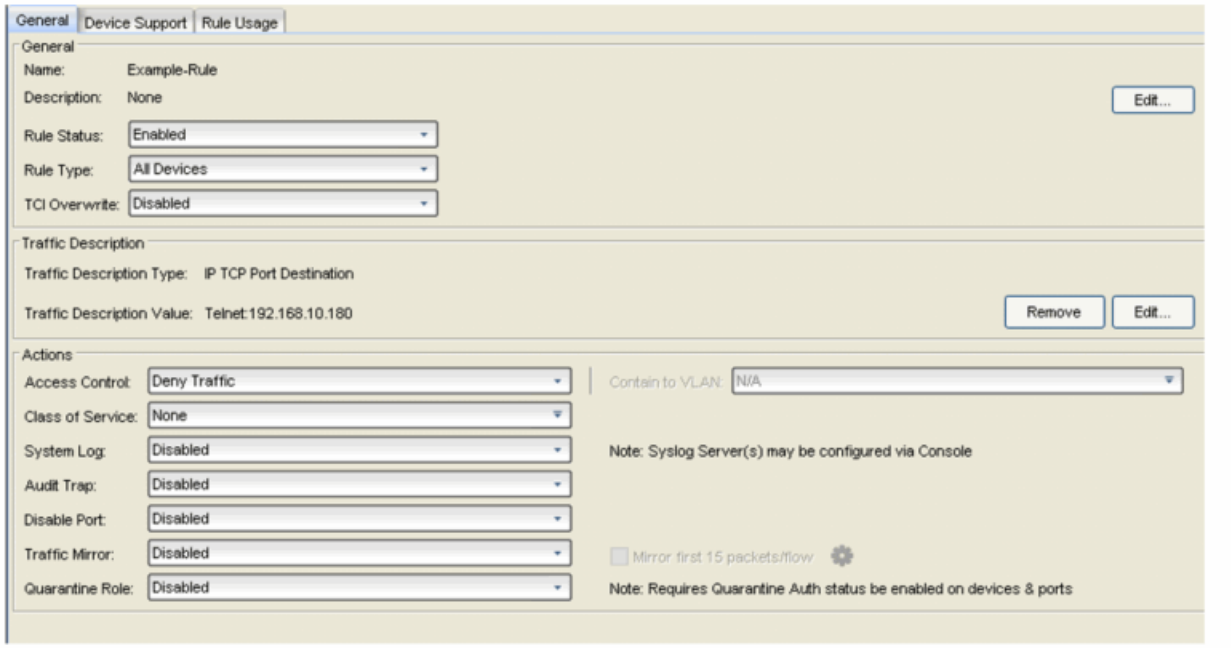
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser. The web service creates a policy rule that drops all telnet (port 23) from 192.168.10.180.

https://192.168.30.34:8443/axis/services/PolicyService/addRule?domainName=Default Policy Domain&serviceName=Example-Service&ruleName=Example-Rule&trafficDescrType=17&trafficDescrValue=23&trafficDescrMask=0&expandedTrafficDescrValue=192.168.10.180&expandedTrafficDescrMask=0&vlanAction=0



Method: addSwitchesToDomain

Add switches to the policy domain.

Parameters

Name	Type	Description
domainName	string	Policy domain to add switches to
switches	string	IP address of the switches

Returns

The operation returns an integer error code.

Method: getRoleMapping

Retrieve an IP or MAC role mapping for the specified switch.

Parameters

Name	Type	Description
station	string	Mapping you are retrieving
device	string	IP address of the switch

Returns

Returns a string array role mapping.

Method: removeRoleMapping

Remove an IP or MAC role mapping for the specified switches.

Parameters

Name	Type	Description
station	string	Mapping you are removing
devices	string	IP address of the switches

Returns

The operation returns an integer error code.

Purview Web Service

The Purview web service provides an external interface to retrieve and modify the Application Analytics data and configuration. The Purview web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/PurviewWebService?wsdl

Method: addLocation

Create a new location with the specified name.

Parameters

Name	Type	Description
locationGroup	string	Location group name
name	string	Name of new location
description	string	Location description
masks	string	IP subnets and masks of location

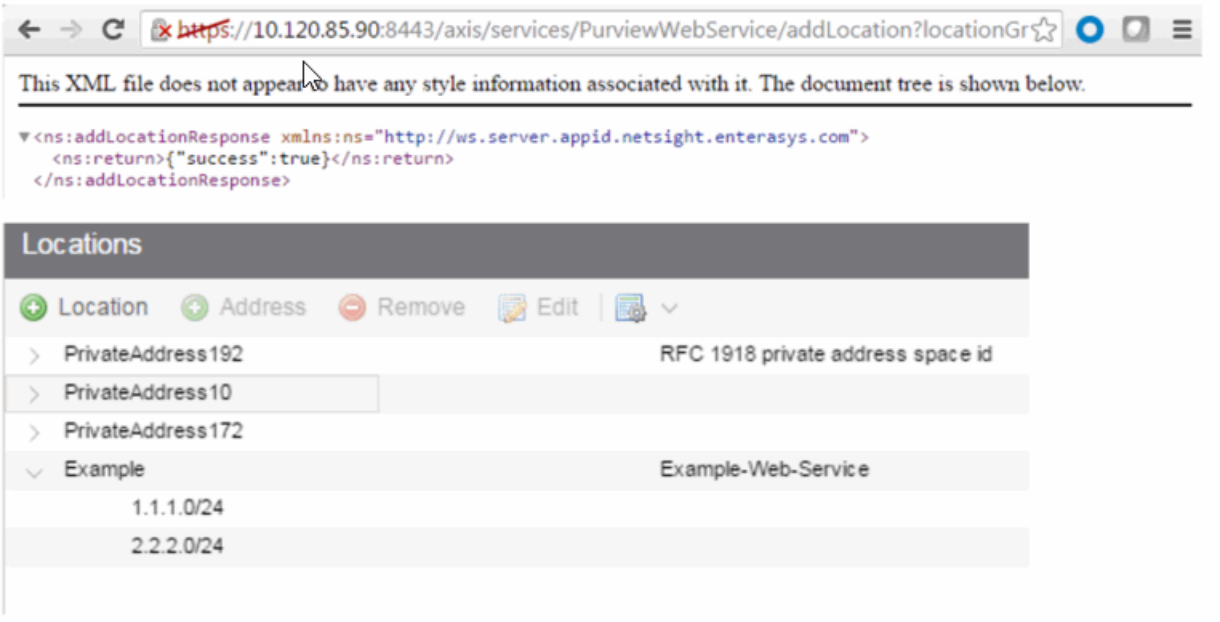
Returns

Returns a string status.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/addLocation?locationGroup=Default&name=Example&description=Example-Web-Service&masks=1.1.1.0/24&masks=2.2.2.0/24



Method: addLocationGroup

Create a new location group.

Parameters

Name	Type	Description
name	string	Name of new location group
description	string	Description of location group

Returns

Returns a string status.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/addLocationGroup?name=Example Location Group&Description=Example-Web-Service

Method: getAppliances

Retrieve the list of Extreme Management Center engines.

Returns

Returns a list of Extreme Management Center engines in JSON format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getAppliances

Method: getApplicationBrowserTableData

Retrieve data from the application browser.

Parameters

Name	Type	Description
tableId	int	The table to retrieve the data from, available options are: 0 – appid_attribute (client & server data) 1 – appid_datapoint (application data) 2 – topn_tables 3 – application_usage_default (hourly application data) 4 – application_usage_hr_default (high rate application data)
target	string	The target to retrieve data from, available options are: application application_group location profile target_address client target source target_type datafamily user_data TopN specific targets: appsByClient server

Name	Type	Description
statistics	string	The statistic to retrieve, available options are: byte_count – total byte count flow_count – total flow count target_address – client/server IP address app_rsp_time – application response time tcp_rsp_time – network response time total – total clients, used with TopN tx_byte_count – transmit byte count rx_byte_count – receive byte count tx_flow_count – transmit flow count rx_flow_count – receive flow count client_count – client count server_count – server count application_count – application count user_data – user data contains different fields based on the tableId all_stats – all the above stats
searchCriteria	string	Key value (key=value) pair used in the database query. The available targets, with the exception of TopN, and statistics can be used as a key.
start	long	Starting timestamp for the query in milliseconds
end	long	Ending timestamp for the query in milliseconds
limit	int	Number of results to return
queryType	string	Query type, available options are: grid chartovertime
aggType	string	Aggregation type, available options are: SUM – sum AVG - average

Returns

Returns a TableData with a structure defined by the following table.

Name	Type	Description
extraData	anyType	Additional data from the operation

Name	Type	Description
lastChange	long	Timestamp of last valid data
noChange	boolean	**True** if the data is being stored
success	boolean	**True** if operation is successful
tableData	string	JSON data

Example

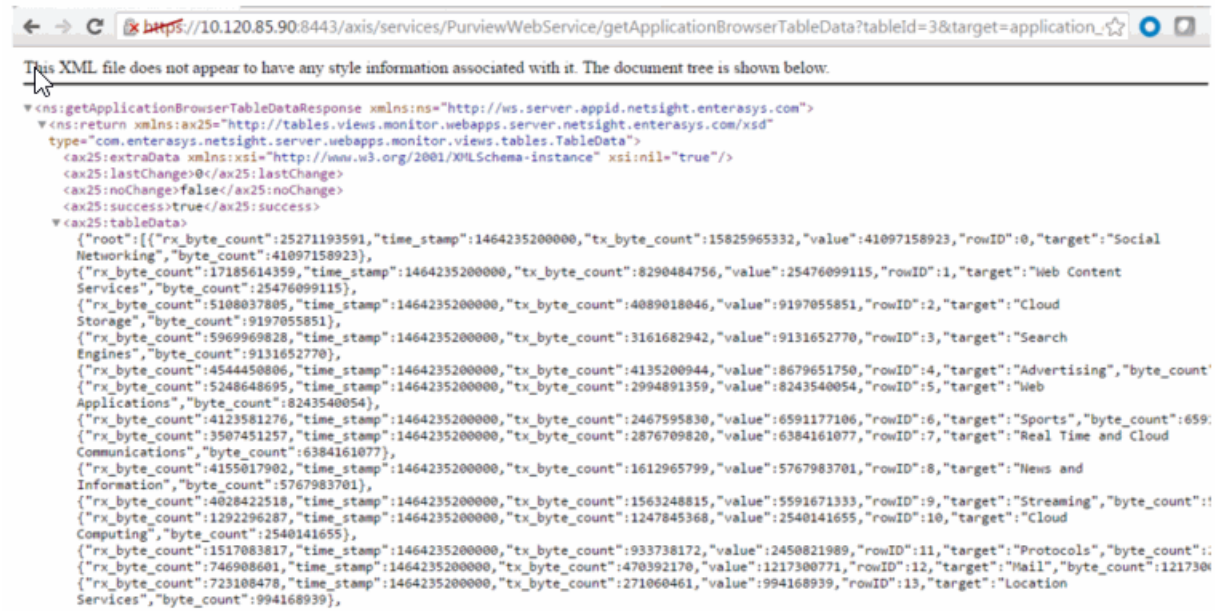
Execute the following web service with a browser:

Retrieve all the statistics for Facebook from the hourly table.

https://10.120.85.90:8443/axis/services/PurviewWebService/getApplicationBrowserTableData?tableId=3&target=application&statistics=all_stats&searchCriteria=application=Facebook&start=1464235200000&end=1464321600000&limit=100&queryType=grid&aggType=AVG

Retrieve the total bytes for the top application groups from the hourly table.

https://10.120.85.90:8443/axis/services/PurviewWebService/getApplicationBrowserTableData?tableId=3&target=application_group&statistics=byte_count&searchCriteria=&start=1464235200000&end=1464321600000&limit=100&queryType=grid&aggType=SUM



Method: getBidirectionalFlowsData

Retrieve the latest filtered bidirectional flow data from an Application Analytics engine.

Parameters

Name	Type	Description
maxRows	int	Maximum number of flows to return
searchString	string	Search string used to query the data
source	string	Application Analytics engine IP address

Returns

Returns flow data in JSON format.

Example

Execute the following web service with a browser:

Retrieve the latest 100 flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getBidirectionalFlowsData?maxRows=100&searchString=&source=10.120.85.91

Retrieve the latest Facebook flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getBidirectionalFlowsData?maxRows=100&searchString=Facebook&source=10.120.85.91

Method: getLocations

Retrieve the list of location groups and locations.

Returns

Returns a list of location groups and locations in JSON format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getLocations

Method: getUnidirectionalFlowsData

Retrieve latest flow data from an Application Analytics engine.

Parameters

Name	Type	Description
maxRows	int	Maximum number of flows to return
searchString	string	Search string used to query the data
source	string	Extreme Analytics appliance IP address

Returns

Returns flow data in JSON format.

Example

Execute the following web service with a browser:

Retrieve the latest 100 flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getUnidirectionalFlowsData?maxRows=100&searchString=&source=10.120.85.91

Retrieve the latest Instagram flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getUnidirectionalFlowsData?maxRows=100&searchString=Instagram&source=10.120.85.91

Method: getVersion

Retrieve Application Analytics version.

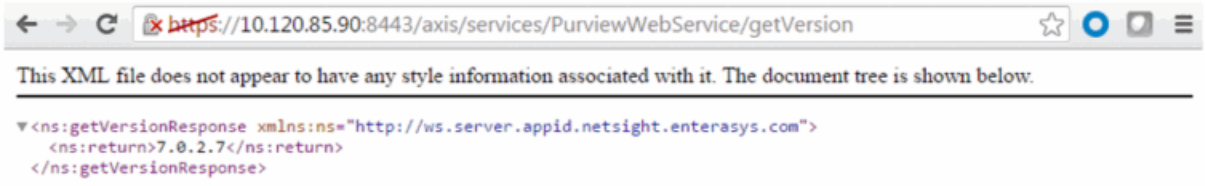
Returns

Returns version in string format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getVersion



Method: importLocationCSV

Create locations with a provided CSV string.

Parameters

Name	Type	Description
locationGroup	string	Location group name
csv	string	CSV data, data must be in a format where line 1 contains “name,ipmask” without quotes. Subsequent lines contain the “<location name>,<IP subnet/mask>” without quotes.
overwrite	boolean	**True** to replace locations with the same name
purge	boolean	**True** to remove locations not imported
protect	boolean	**True** to prevent a location from being overwritten

Returns

Returns a string status.

Reporting Web Service

The Reporting web service provides an external interface to retrieve and modify the Extreme Management Center reporting engine data and configuration. The Reporting web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/Reporting?wsdl

The Reporting web services use complex data types. It is recommended to use a WSDL converter to generate the source code to execute the web service operations. In these examples, the Java source code is generated via the Axis2 1.6.2 wsdl2java utility.

Method: addDataPointObj

Add a data point to the reporting table.

Parameters

Name	Type	Description
dp	DataPoint	The raw statistic which contains the target ID, statistic ID, value, and timestamp

Returns

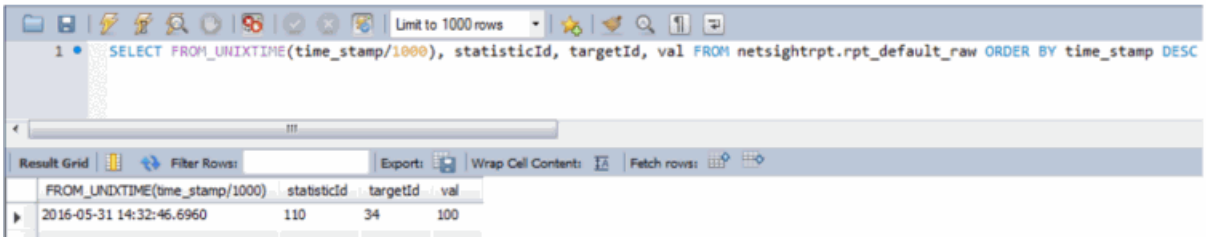
Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the SsidAssociatedClients, with statisticID 100, on Fake SSID, with targetID 34, to 100.


```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataPointObjDocument document = AddDataPointObjDocument.Factory.newInstance();
AddDataPointObj dpObj = document.addNewAddDataPointObj();
DataPoint dp = dpObj.addNewDp();
Domain domain = Domain.Factory.newInstance();
domain.setName("Default");
dp.setDomain(domain);
dp.setStatisticID(110);
dp.setTargetID(34);
dp.setValue(100);
dp.setTimeStamp(System.currentTimeMillis());
stub.addDataPointObj(document);
```



Method: addDataPointObjs

Add multiple data samples to the reporting table.

Parameters

Name	Type	Description
dp	DataPoint	The raw statistic which contains the target ID, statistic ID, value, and timestamp

Returns

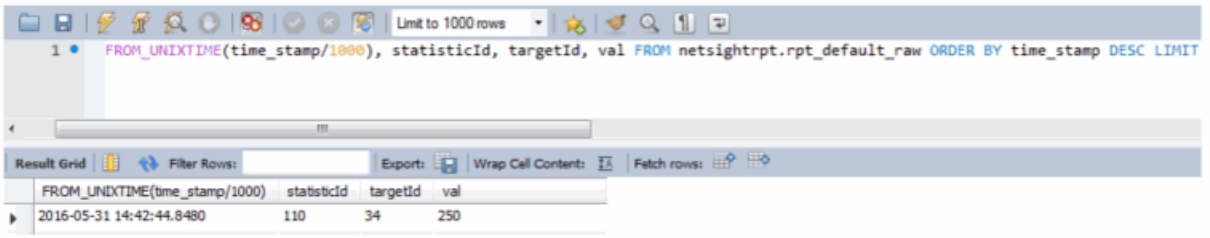
Returns a MultiObjRptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** if the operation does not complete
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the SsidAssociatedClients, with statisticID 100, on Fake SSID, with targetID 34, to 250.

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataPointObjsDocument document = AddDataPointObjsDocument.Factory.newInstance();
AddDataPointObjs dpObj = document.addNewAddDataPointObjs();
DataPoint dp = dpObj.addNewDp();
Domain domain = Domain.Factory.newInstance();
domain.setName("Default");
dp.setDomain(domain);
dp.setStatisticID(110);
dp.setTargetID(34);
dp.setValue(250);
dp.setTimeStamp(System.currentTimeMillis());
stub.addDataPointObjs(document);
```



Method: addDataSample

Add a data sample to the reporting table.

Parameters

Name	Type	Description
newSample	DataSample	The raw statistic which contains the target name, statistic name, value, and timestamp

Returns

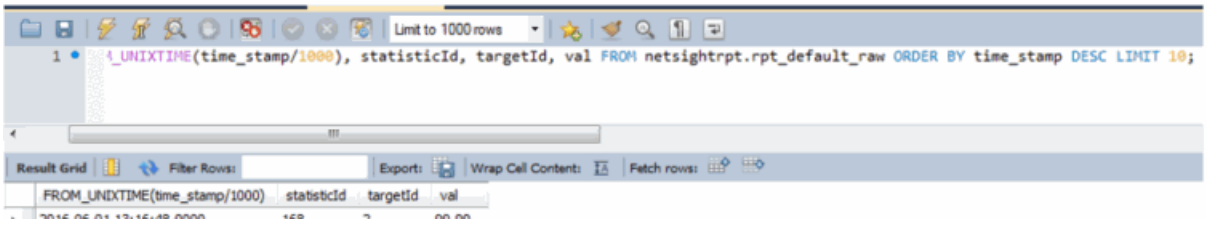
Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the NsServerDiskUsedPercent statistic on the NetsightServer to 99.99.


```
eportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
ttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataSampleDocument document = AddDataSampleDocument.Factory.newInstance();
AddDataSample data = document.addNewAddDataSample();
DataSample ds = data.addNewNewSample();
ds.setDomainName("Default");
ds.setSingleValue(BigDecimal.valueOf(99.99));
ds.setStatName("NsServerDiskUsedPercent");
ds.setTargetName("NetsightServer");
ds.setTargetSubName("Server");
ds.setTimeStamp(System.currentTimeMillis());
stub.addDataSample(document);
```



Method: addDataSamples

Add multiple data samples to the reporting table.

Parameters

Name	Type	Description
ds	DataSample	The raw statistic which contains the target name, statistic name, value, and timestamp

Returns

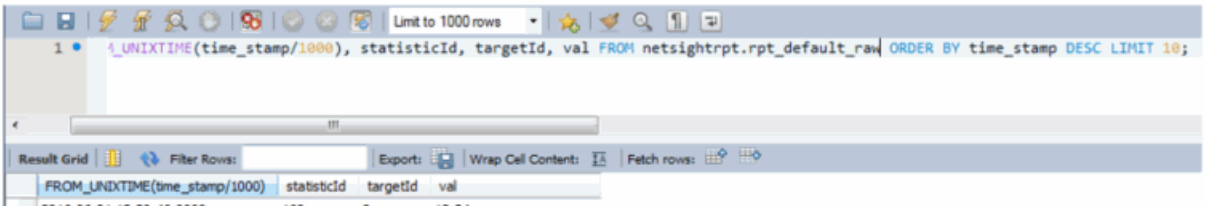
Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** if the operation did not complete
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the NsServerDiskUsedPercent statistic on the NetsightServer to 12.34.


```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataSamplesDocument document = AddDataSamplesDocument.Factory.newInstance();
AddDataSamples data = document.addNewAddDataSamples();
DataSample ds = data.addNewDs();
ds.setDomainName("Default");
ds.setSingleValue(BigDecimal.valueOf(12.34));
ds.setStatName("NsServerDiskUsedPercent");
ds.setTargetName("NetsightServer");
ds.setTargetSubName("Server");
ds.setTimeStamp(System.currentTimeMillis());
stub.addDataSamples(document);
```



Method: addOrModifyCollectorConfigObjs

Add or update a collector configuration.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configuration

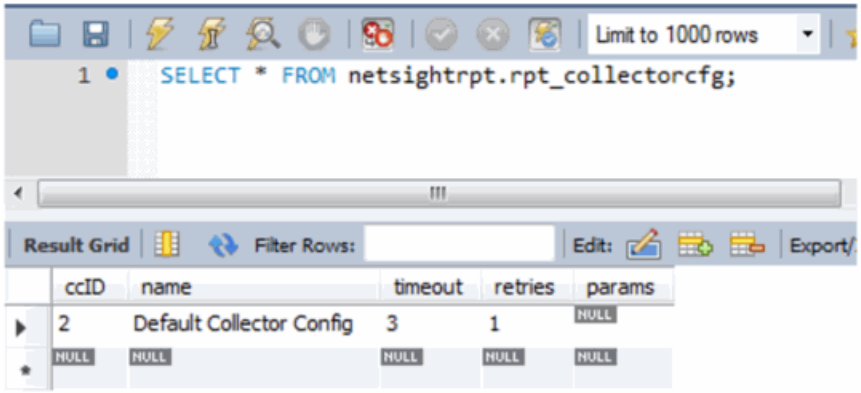
Returns

Returns a RptResultCollectorCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Collector configuration
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyCollectorConfigObjsDocument document = AddOrModifyCollectorConfigObjsDocument.Factory.newInstance();
AddOrModifyCollectorConfigObjs objs = document.addNewAddOrModifyCollectorConfigObjs();
CollectorConfig cfg = objs.addNewCcs();
cfg.setName("Default Collector Config");
cfg.setRetries(1);
cfg.setTimeout(3);
stub.addOrModifyCollectorConfigObjs(document);
```



Method: addOrModifyCollectorConfigs

Add or update a collector configuration.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configuration

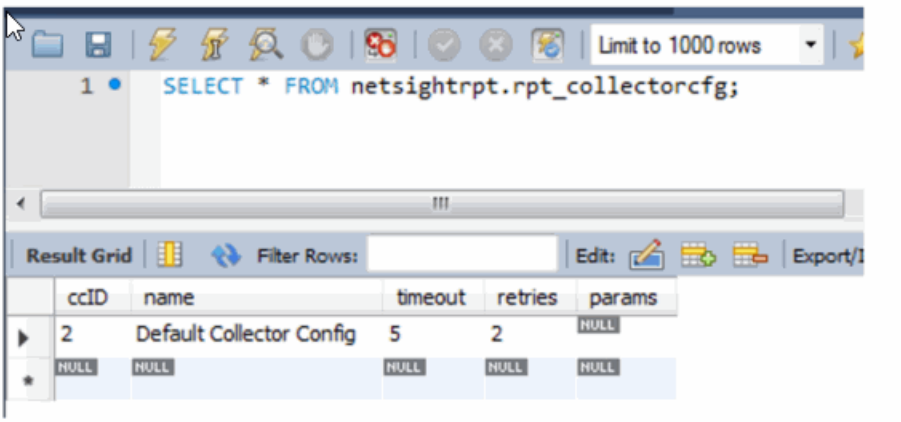
Returns

Returns a MultiObjRptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** indicates the operation did not complete
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyCollectorConfigsDocument document = AddOrModifyCollectorConfigsDocument.Factory.newInstance();
AddOrModifyCollectorConfigs objs = document.addNewAddOrModifyCollectorConfigs();
CollectorConfig cfg = objs.addNewCcs();
cfg.setName("Default Collector Config");
cfg.setRetries(2);
cfg.setTimeout(5);
stub.addOrModifyCollectorConfigs(document);
```



Method: addOrModifyStatistic

Add or update a statistic.

Parameters

Name	Type	Description
name	string	Statistic name
dt	DataType	Statistic data type

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
stat	Statistic	Updated Statistic
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticDocument document = AddOrModifyStatisticDocument.Factory.newInstance();
AddOrModifyStatistic statistic = document.addNewAddOrModifyStatistic();
statistic.setName("ExtremeControlAuthenticatedUserCount");
DataType data = statistic.addNewDt();
data.setVal("Counter");
stub.addOrModifyStatistic(document);
```

Method: addOrModifyStatisticObj

Add or update a statistic.

Parameters

Name	Type	Description
stat	Statistic	Statistic to update

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
stat	Statistic	Updated Statistic

Name	Type	Description
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticObjDocument document = AddOrModifyStatisticObjDocument.Factory.newInstance();
AddOrModifyStatisticObj obj = document.addNewAddOrModifyStatisticObj();
Statistic statistic = obj.addNewStat();
statistic.setDataTypeString("Counter");
statistic.setDescription("Example Statistic");
statistic.setDisplayName("This is an example");
statistic.setName("ExtremeControlAuthenticatedUserCount");
statistic.setObjectType("NAC");
statistic.setStatisticID(205);
stub.addOrModifyStatisticObj(document);
```

Method: addOrModifyStatisticObjs

Add or update multiple statistics.

Parameters

Name	Type	Description
stats	Statistic	Statistics to update

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
stat	Statistic	Updated Statistic
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticObjsDocument document = AddOrModifyStatisticObjsDocument.Factory.newInstance();
AddOrModifyStatisticObjs objs = document.addNewAddOrModifyStatisticObjs();
Statistic statistic = objs.addNewStats();
statistic.setDataTypeString("Counter");
statistic.setDescription("Updated example statistic");
statistic.setDisplayName("This is another example");
statistic.setName("ExtremeControlAuthenticatedUserCount");
statistic.setObjectType("NAC");
statistic.setStatisticID(205);
stub.addOrModifyStatisticObjs(document);
```

Method: addOrModifyTarget

Add or update a target.

Parameters

Name	Type	Description
objectID	string	Target object ID

Name	Type	Description
objectSubID	string	Target object sub ID
description	string	Description of target
tags	string	Optional field for collector specific values

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetDocument document = AddOrModifyTargetDocument.Factory.newInstance();
AddOrModifyTarget data = document.addNewAddOrModifyTarget();
data.setDescription("Example Target");
data.setObjectID("SSID");
data.setObjectSubID("SSID");
stub.addOrModifyTarget(document);
```

Method: addOrModifyTargetObj

Add or update a target.

Parameters

Name	Type	Description
targ	Target	Target to update

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetObjDocument document = AddOrModifyTargetObjDocument.Factory.newInstance();
AddOrModifyTargetObj data = document.addNewAddOrModifyTargetObj();
Target target = data.addNewTarg();
target.setDescription("Updated example description");
target.setDisplayName("SSID Example");
target.setObjectID("SSID");
target.setObjectSubID("SSID");
target.setTargetID(34);
stub.addOrModifyTargetObj(document);
```

Method: addOrModifyTargetObjs

Add or update multiple targets.

Parameters

Name	Type	Description
targ	Target	Target to update

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetObjsDocument document = AddOrModifyTargetObjsDocument.Factory.newInstance();
AddOrModifyTargetObjs data = document.addNewAddOrModifyTargetObjs();
Target target = data.addNewTarg();
target.setDescription("Updated Example Description");
target.setDisplayName("Updated SSID Example");
target.setObjectID("SSID");
target.setObjectSubID("SSID");
target.setTargetID(34);
stub.addOrModifyTargetObjs(document);
```

Method: deleteCollectorConfig

Delete a collector configuration.

Parameters

Name	Type	Description
cc	CollectorConfig	Collector configuration to delete

Returns

Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteCollectorConfigDocument document = DeleteCollectorConfigDocument.Factory.newInstance();
DeleteCollectorConfig config = document.addNewDeleteCollectorConfig();
CollectorConfig cc = config.addNewCc();
cc.setName("Default Collector Config");
stub.deleteCollectorConfig(document);
```

Method: deleteCollectorConfigs

Delete multiple collector configurations.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configurations to delete

Returns

Returns a RptResultCollecotrCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Deleted collector configurations
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteCollectorConfigsDocument document = DeleteCollectorConfigsDocument.Factory.newInstance();
DeleteCollectorConfigs config = document.addNewDeleteCollectorConfigs();
CollectorConfig cc = config.addNewCcs();
cc.setName("Default Collector Config");
stub.deleteCollectorConfigs(document);
```

Method: deleteDomain

Delete a domain.

Parameters

Name	Type	Description
domain	string	Domain to delete

Returns

Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Method: deleteStatistic

Delete a statistic.

Parameters

Name	Type	Description
name	string	Statistic name

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
stat	Statistic	Updated statistic
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteStatisticDocument document = DeleteStatisticDocument.Factory.newInstance();
DeleteStatistic statistic = document.addNewDeleteStatistic();
statistic.setName("ExtremeControlAuthenticatedUserCount");
stub.deleteStatistic(document);
```

Method: deleteTarget

Delete a target.

Parameters

Name	Type	Description
objectID	string	Target object ID

Name	Type	Description
objectSubID	string	Target object sub ID

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteTargetDocument document = DeleteTargetDocument.Factory.newInstance();
DeleteTarget target = document.addNewDeleteTarget();
target.setObjectID("SSID");
target.setObjectSubID("SSID");
stub.deleteTarget(document);
```

Method: deleteTargetObjs

Delete multiple targets.

Parameters

Name	Type	Description
targs	Target	Targets to delete

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteTargetObjsDocument document = DeleteTargetObjsDocument.Factory.newInstance();
DeleteTargetObjs objs = document.addNewDeleteTargetObjs();
Target target = objs.addNewTargs();
target.setObjectID("SSID");
target.setObjectSubID("Example");
stub.deleteTargetObjs(document);
```

Method: getAllCollectorConfigs

Retrieve collector configurations.

Returns

Returns a list of collector configurations.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllCollectorConfigs

Method: getAllStatistics

Retrieve all statistics.

Returns

Returns a list of statistics.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllStatistics

Method: getAllTargets

Retrieve all targets.

Returns

Returns a list of all the targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargets

Method: getAllTargetsForObjectID

Retrieve all targets with a matching object ID.

Parameters

Name	Type	Description
objectID	string	Object ID name

Returns

Returns a list of matching targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargetsForObjectID?objectID=NAC

Method: getAllTargetsForObjectType

Retrieve all targets with a matching object type.

Parameters

Name	Type	Description
objectType	string	Object type name

Returns

Returns a list of matching targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargetsForObjectType?objectType=ESPROFILE

Method: getCollectorConfigForName

Retrieve collector configuration.

Parameters

Name	Type	Description
name	string	Collector configuration name

Returns

Returns a RptResultCollecotrCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Collector configuration data
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getCollectorConfigForName?name=Default Collector Config

Method: getGoogleChartApiUrl

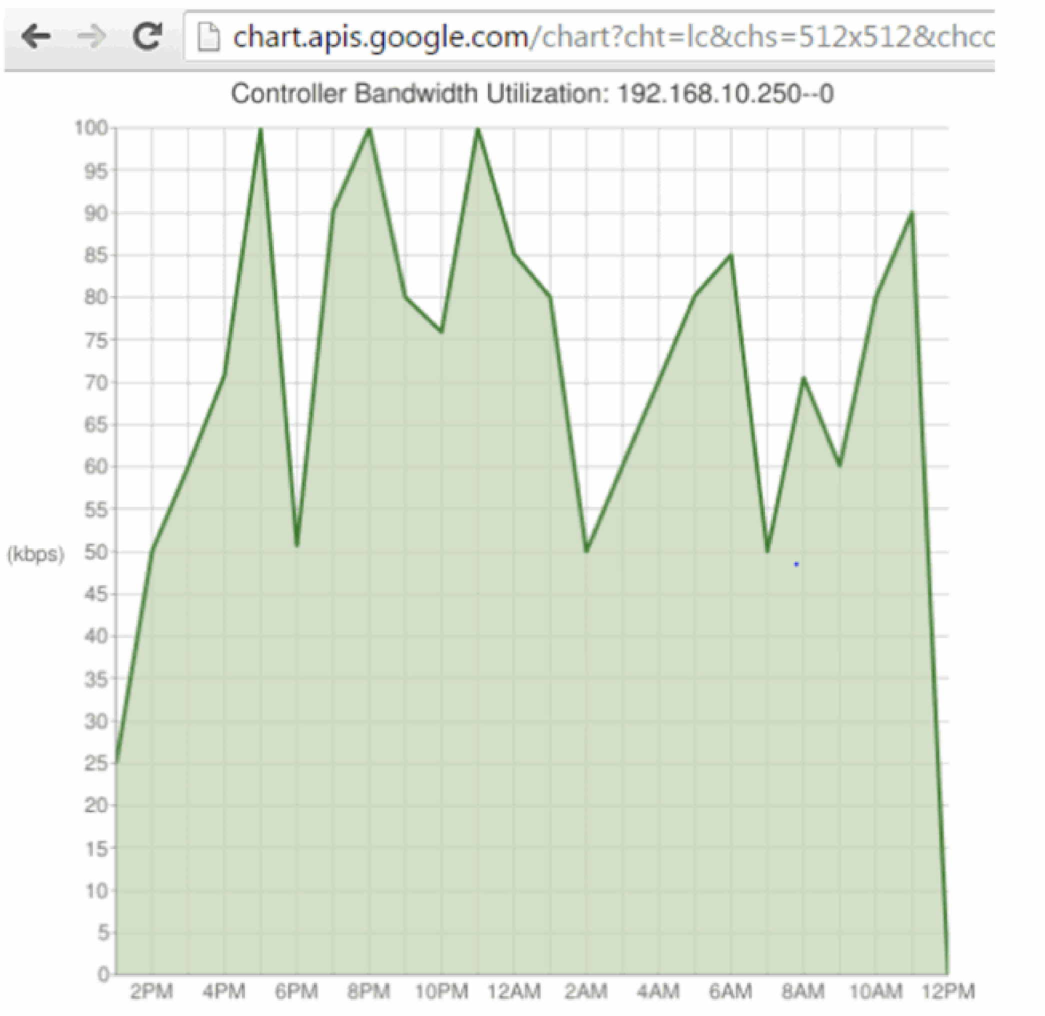
Generate an online chart using Google's chart API. Collections must be enabled for the AP and/or wireless controller for this operation to work correctly.

Parameters

Name	Type	Description
type	string	Type of statistic, available options are: APBwUtil – AP bandwidth ControllerBwUtil – wireless controller bandwidth
params	string	Chart parameters in key=value format, available parameters are: target – AP serial number for APBwUtil or wireless controller IP address for ControllerBwUtil width – chart width height – chart height

Returns

The values from the URL were modified in the example below.



Method: getPerformanceSummary

Retrieve the Extreme Management Center reporting engine performance summary.

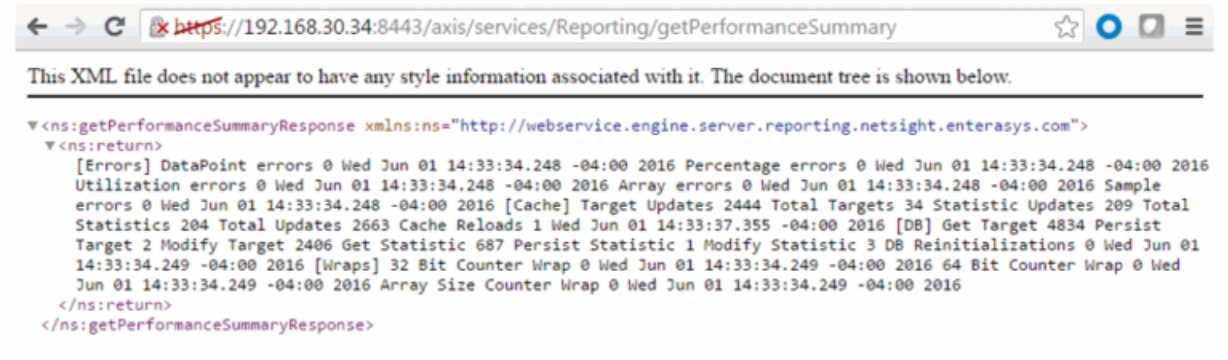
Returns

Returns a summary of the Extreme Management Center reporting engine.

Example

Execute the following web service with a browser: >

https://192.168.30.34:8443/axis/services/Reporting/getPerformanceSummary



Method: getProperties

Retrieve a list of properties from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve properties from

Returns

Returns a list of properties.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertiesDocument document1 = GetPropertiesDocument.Factory.newInstance();
GetProperties properties = document1.addNewGetProperties();
properties.setTarget(target);
System.out.println(stub.getProperties(document1));
```

```
<ns:getPropertiesResponse xmlns:ax21="http://model.common.reporting.netsight.ente
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>apIsStandalone</ax23:name>
    <ax23:value>true</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.controllerIp</ax23:name>
    <ax23:value>192.168.10.250</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.apState</ax23:name>
    <ax23:value>1</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.apStatus</ax23:name>
    <ax23:value>1</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.RADIOIDX</ax23:name>
    <ax23:value/>
  </ns:return>
```

Method: getProperty

Retrieve a property from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve property from
key	string	Property key to retrieve

Returns

Returns property key and value.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertyDocument document1 = GetPropertyDocument.Factory.newInstance();
GetProperty property = document1.addNewGetProperty();
property.setTarget(target);
property.setKey("C1.controllerIp");
System.out.println(stub.getProperty(document1));
```

```
<ns:getPropertyResponse xmlns:ns="http://web
  <ns:return type="com.enterasys.netsight.re
    <ax23:name>C1.controllerIp</ax23:name>
    <ax23:value>192.168.10.250</ax23:value>
  </ns:return>
</ns:getPropertyResponse>
```

Method: getPropertyAsLong

Retrieve a property from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve property from
key	string	Property key to retrieve
defaultVal	long	Default value

Returns

Returns property key and value.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertyAsLongDocument document1 = GetPropertyAsLongDocument.Factory.newInstance();
GetPropertyAsLong property = document1.addNewGetPropertyAsLong();
property.setTarget(target);
property.setKey("updateTime");
property.setDefaultVal(0);
System.out.println(stub.getPropertyAsLong(document1));
```

```
<ns:getPropertyAsLongResponse xmlns:ns="http://webs
  <ns:return>1464892909437</ns:return>
</ns:getPropertyAsLongResponse>
```

Method: getServerStatus

Retrieve the Extreme Management Center server status.

Returns

Returns a status.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getServerStatus

Method: getTargetByNameAndType

Return target based on the object ID name and type.

Parameters

Name	Type	Description
objectIDName	string	Object ID name
objectType	string	Object type

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getTargetByNameAndType?objectIDName=192.168.10.250&objectType=HWC

Method: modifyTarget

Update existing target with new object ID and object sub ID.

Parameters

Name	Type	Description
targetID	long	Target ID to modify
newObjectID	string	New object ID
newObjectSubID	string	New object sub ID

Returns

Returns a RptResultTarget with a structure defined by the following table.

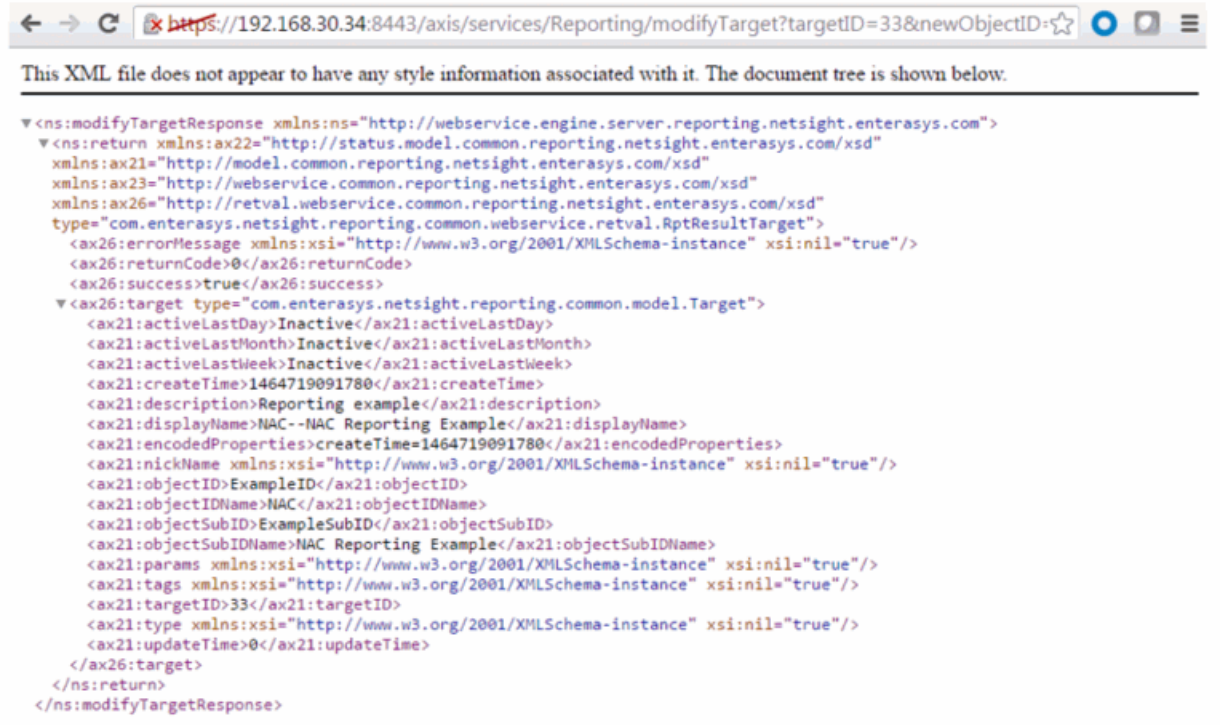
Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful

Name	Type	Description
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/modifyTarget?targetID=33&newObjectID=ExampleID&newObjectSubID=ExampleSubID



Method: setProperty

Set target property.

Parameters

Name	Type	Description
target	Target	Target to update
prop	Property	Property to update

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
SetPropertyDocument document = SetPropertyDocument.Factory.newInstance();
SetProperty property = document.addNewSetProperty();
Target t = property.addNewTarget();
t.setObjectID("ExampleID");
t.setObjectSubID("ExampleSubID");
t.setTargetID(33);
Property p = property.addNewProp();
p.setName("MyKey");
p.setValue("MyValue");
System.out.println(stub.setProperty(document));
```

```
<ns:setPropertyResponse xmlns:ns="http://webservice.engine.server.reporting.netsight.enterasys.com" xmlns:soapenv="http:
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.retval.RptResultTarget" xmlns:ax22="http://status.
    <ax26:errorMessage xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
    <ax26:returnCode>0</ax26:returnCode>
    <ax26:success>true</ax26:success>
    <ax26:target type="com.enterasys.netsight.reporting.common.model.Target">
      <ax21:activeLastDay>Active</ax21:activeLastDay>
      <ax21:activeLastMonth>Active</ax21:activeLastMonth>
      <ax21:activeLastWeek>Active</ax21:activeLastWeek>
      <ax21:createTime>1464896964676</ax21:createTime>
      <ax21:description xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:displayName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:encodedProperties>MyKey=MyValue,updateTime=1464896964676,createTime=1464896964676</ax21:encodedProperties>
      <ax21:nickName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:objectID>ExampleID</ax21:objectID>
      <ax21:objectIDName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:objectSubID>ExampleSubID</ax21:objectSubID>
      <ax21:objectSubIDName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:params xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:tags xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:targetID>33</ax21:targetID>
      <ax21:type xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:updateTime>1464896964676</ax21:updateTime>
    </ax26:target>
  </ns:return>
</ns:setPropertyResponse>
```

Method: statExists

Check if statistic exists.

Parameters

Name	Type	Description
name	string	Statistic Name

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
stat	Statistic	Statistic information
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/statExists?name=ifInOctets

Method: targetExists

Check if target exists.

Parameters

Name	Type	Description
objectID	string	Target object ID
objectSubID	string	Target object sub ID

Returns

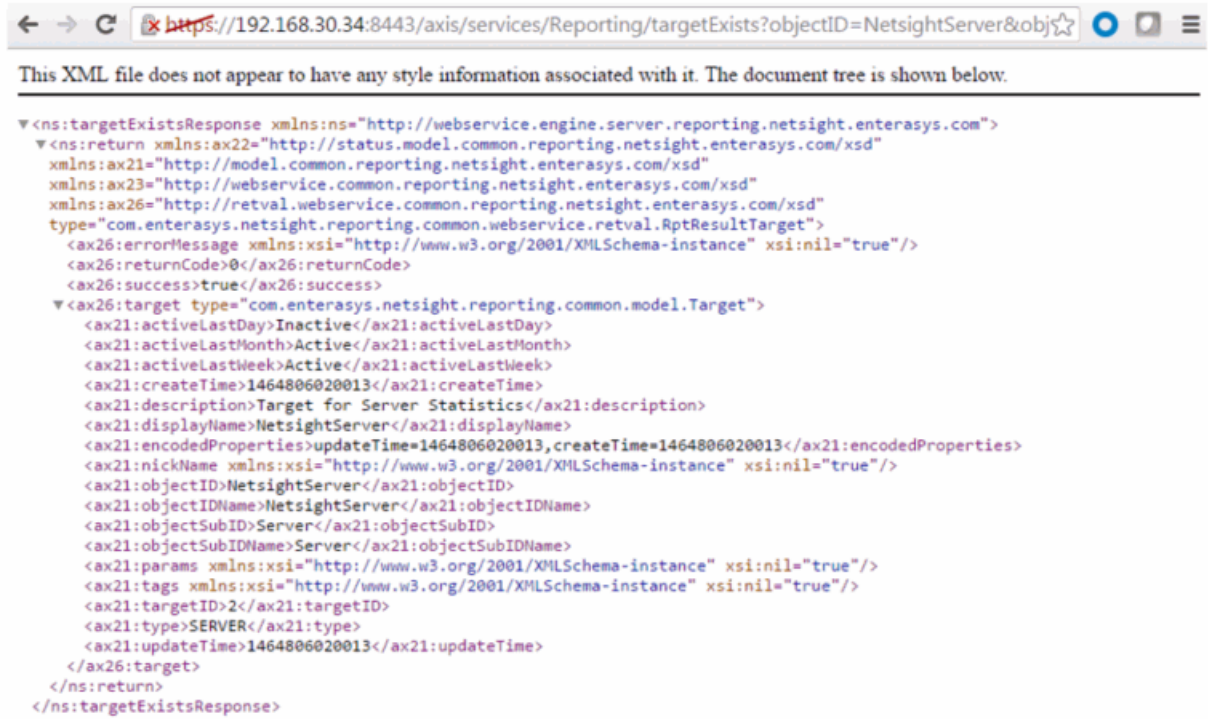
Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/targetExists?objectID=NetsightServer&objectSubID=Server



Data Center/Cloud Integration

The various integrations for Data Center/Cloud focus on the automation of provisioning highly mobile end-systems like virtual machines or providing user information for virtual desktops. Depending on the capabilities of the 3rd party product, the automation can include the creation of virtual networks and VLAN configuration within the respective product.

- Citrix XenServer
- Citrix XenDesktop
- Microsoft Intune
- Google G Suite
- Microsoft System Center Virtual Machine Manager (SCVMM)

- Microsoft Hyper-V
- VMware vSphere
- VMware View

Citrix XenServer

The XenServer integration offers provisioning of virtual machines in the network as well as automating the creation of virtual networks based on end-system access groups. In addition, data within Extreme Management Center is enriched for each end-system and conversely made available within XenCenter (=management tool for XenServer environments).

Module Configuration

Service Configuration	Description
Username	Username used to connect to the XenServer's web service. Read/Write/Execute permissions required.
Password	Password used to connect to the XenServer's web service.
XenCenter Webservice URL	Web service url of the XenSever
XenCenter Server IP	IP address of the XenServer.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the XenServer.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group:	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Control to update the information for end-systems retrieved from XEN (valid values: 1-4).
Outgoing data format	The format of the Extreme Control data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within XEN. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from XEN and written to the custom field.

Service Specific Configuration	
Use global end-system groups	This feature allows for the module to use the global end-system groups of the Extreme Connect. This will enable the XEN module to use the end-system groups retrieved from the Extreme Control module and assign XEN VMs to these end-system groups.
Network deletion	If this option is enabled, networks created by end-system groups will be deleted if the end-system group does not exist anymore or sync is disabled. Any connected VM will be rerouted to the Deletion Group below.
Deletion Group	If the “Network Deletion” feature is enabled, this setting will define the catchall network for VMs that have been connected to a XEN network after it has been deleted in Extreme Management Center. For example: If you have a XEN network “VM Test” that is managed by Extreme Connect and you delete the corresponding end-system group in Extreme Management Center, this feature will make sure that all VMs that are connected to “VM Test” will be disconnected from it and automatically reconnected to the XEN network defined with this setting. This feature is meant to provide a fallback network for all VMs that have been connected to Extreme Connect managed XEN networks.
Destroy NIC Bonds	If enabled, Extreme Connect will automatically destroy (remove) a bonding of 2 or more NICs on the Citrix XenServer in case the last network that used this bond has been removed using the Extreme Management Center group configuration. Example: Let’s assume you have created a new end-system group using multiple NICs with “nic=eth0:eth1”, Extreme Connect will create - A bond over eth0 + eth1 with a default naming schema and - A new external network connected to that bond named as your end-system group. Now you create a second end-system group also using the same NIC definition “nic=eth0:eth1”. This will only create a new external network connected to the already existing bond and called according to your end-system group. If you now delete (or set “sync=false”) one of these end-system groups, only the external Xen network will be removed, not the bond since it is in use by the other network. If you then also delete the other end-system group, the corresponding external network will be deleted and the bond between eth0 and eth1 will be destroyed.

Verification

1. Click on a virtual machine.
2. Click the “General” tab on the right side of the screen.
3. At the top of the "General" tab there is a description field that will contain the corresponding data from Extreme Management Center. If this data is correct, then the integration is verified.

Citrix XenDesktop

The integration with XenDesktop is a one-way integration: information on virtual desktops is retrieved from XenDesktop and used within NAC but no data nor configuration is written from NAC towards XenDesktop.

Module Configuration

The table below describes the configuration options available for the XendDesktop OFConnect module (config file: XenDesktopHandler.xml)

Service Configuration	Description
Adapter IP	The IP address on which the Extreme XenDesktop adapter is running (this is configurable within the adapter's config file). It should be running on the same IP as your XenDesktop server.
Adapter Port	The TCP port on which the Extreme XenDesktop adapter is running (this is configurable within the adapter's config file).
Pre-Shared Key	The key used to encrypt traffic from and to the adapter running on the XenDesktop server. This must match the configured pre-shared key from the adapter's config file.

General Module Configuration	
Poll interval in seconds	The wait time between two polls. The module will contact the XenDesktop adapter and request the latest data on the VDI infrastructure, then wait for this interval to pass and then poll the adapter again.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from the adapter running on the XenDesktop server (valid values: 1-4).
Format of the incoming data	The format of the data that is received from the adapter running on the XenDesktop server and written to the custom field.

Adapter Installation

OFConnect retrieves data from the XenDesktop server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within OFConnect. The adapter consists of a Java executable file (.jar) and a configuration file. To install the adapter:

1. Install Windows .NET Framework 3.5 SP1 or above, Windows Powershell 2.0 and the latest Java Runtime Environment on the XenDesktop server.
2. Locate the file "Datacenter Manager XenDesktop Adapter.zip" on the Extreme Control server in the directory../jboss/server/default/deploy/fusion_ jboss.war/XenPlugin/ (it can also be downloaded via browser at https://Extreme Control-IP:8443/fusion_jboss/XenPlugin/ Datacenter%20Manager%20XenDesktop%20Adapter.zip).
3. Copy the executable jar file (DCM_XENDESKTOP_ADAPTER_<version>.jar) and the configuration file (DCM_XENDESKTOP_ADAPTER.config) into a separate directory, created under "Program Files/Extreme Networks/XenDesktop Adapter" directly on the XenDesktop server.
4. Edit the configuration file according to your environment. The configuration file contains an explanation of all settings. You can also find them listed below.
5. Save and close the configuration file.
6. Start the adapter manually by opening a cmd shell or Powershell,
7. Navigate into the installation directory and use the following command: java –jar DCM_XENDESKTOP_ADAPTER_<version>.jar.
8. Check the log file to validate proper functionality.
9. Check the end-system list within OneView or NAC Manager to see data for the XenDesktop virtual machines coming into the custom column you've configured within the XenDesktopHandler.xml config file.
10. After successfully verifying the integration, you will need to ensure that the DCM_ XENDESKTOP_ADAPTER_1.00.jar file is getting started on Windows server startup automatically. Stop the adapter currently running within the cmd/Powershell window.
11. Configure the auto-start for the .jar file (this depends on your Windows Server version) and restart your XenDesktop server, when appropriate, in order to test the auto-start of the .jar file (you should see a java process running in the process tree).

Adapter Configuration

The table below lists the configuration options for the XenDesktop agent.

Configuration Option	Description
NETSIGHT_IP	The IP address of the Extreme Management Center server.
NETSIGHT_ USERNAME	The username to authenticate against the Extreme Management Center server.
NETSIGHT_ PASSWORD	The password to authenticate against the Extreme Management Center server.
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on.
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
XENDESKTOP_ SERVER	The host/DNS name of the XenDekstop Deliver Controller to connect to. So far this has only been tested with this adapter and the XD Deliver Controller running on the same server although remote connections might work as well. Example: XenDesktop5 or with FQDN: XenDesktop5.test.local.
PRE_SHARED_ KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect XenDesktop module.
IS_PRE_ SHARED_KEY_ ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to “true”. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service.
ENABLE_ PUSH_USER_ TO_NETSIGHT	If set to "true" the adapter will use web service calls to Extreme Management Center to push the user name for each virtual desktop session to the corresponding end-system in Extreme Management Center/NAC. If configured properly in NAC, this will cause a re-authentication of the user on this virtual desktop and assign a user-based policy.
ENABLE_ PUSH_DATA_ TO_NETSIGHT	If set to "true" the adapter will push end-system data back to the corresponding module within OFConnect/Extreme Management Center. This will enable you to retrieve data on the virtual desktop within Extreme Management Center/OFConnect and display it within the end-system table inside of NAC manager

Verification

To verify proper functionality, validate the data within the custom field configured to use for the XenDesktop integration in your end-system list (in NAC Manager or OneView).

You will only see the username being set accordingly if you enable the following option within the adapter’s config file: ENABLE_PUSH_USER_TO_ NETSIGHT=true

You will only see the additional information (within the custom column that you’ve specified in your OFConnect XenDesktopHandler config file) if you’ve enabled the following option within the adapter’s config file:

ENABLE_PUSH_DATA_TO_NETSIGHT=true

Be aware that the username from XenDesktop can also be used to automatically assign a policy to each user as you could do with any 802.1X or Kerberos username. So make sure you've configured your rule set in NAC correctly before enabling this feature.

Microsoft Intune

The Intune integration requires registering a Microsoft Azure application. The Azure application will act as a proxy to execute REST API calls on behalf of Connect. This information is used in the Intune module tab.

Module Configuration

The table below lists the configuration options for the MS Intune agent.

Configuration Option	Description
Client ID:	Application client ID
Password:	Application client secret
Tenant:	Tenant ID to retrieve specific customer devices

Service Configuration

The table below lists the configuration options for the MS Intune server.

Configuration Option	Description
Poll interval:	Time period between queries to the Intune NAC web service
End system group for managed business mobile devices:	Mobile IAM end-system group that corporate-owned devices will be part of
End system group for managed personal mobile devices:	Mobile IAM end system group that personal devices will be part of
Default end system group for managed mobile devices:	Mobile IAM end-system group that unknown devices will be part of
Update Kerberos username:	Enable/disable option to update end-system username
Update device type:	Enable/disable option to update end-system device type
Notify user when quarantined:	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment:	Enable/disable option to use Mobile IAM assessment agent

Register Azure Application

An Azure application is required to access Microsoft's Intune NAC API. The application will need permission from an administrator to access device

information from Intune.

1. Login the Azure portal https://portal.azure.com.
2. Select “More services >” at the bottom of the page and select “App registrations."
3. Create a new application.
4. Enter the application name, type, and sign-on URL. In this example, the application name is Connect. The application type must be set to “Web app / API.” The sign-on URL is used as a redirection page once the permissions have been accepted. In this example, the web page will be redirected to the ExtremeManagement server.
5. Once the information is entered, the client ID will be made available. The client ID in the example below is 344763b9-8615-439b-b9dd-0f4c5eeafb9c. This is the ID used in the service configuration.
6. The Azure application will use the Microsoft Intune API and permissions must be enabled to access mobile device information.
7. Select the Azure application permissions, in this example all available permissions are enabled.
8. Select the Keys menu to generate the client secret.

   In this example, the description is set to Secret and the duration is set to expire in 2299. It is recommended to set the duration to a lower value. The generated secret is XZeGGzca8e1saCVgNtdbMIFvlpzSuYG17Esqo8tW5+c=. This is the secret used in the service configuration.

Verification

1. Enroll new device with Microsoft Intune.
2. Connect to test SSID, wait for re-synchronization poll to occur, and verify end system in ExtremeControl has device information from Intune.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with the Intune server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by Intune so Google Play and Apple appStore access must be provided as well in this

state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow Intune registration:

1. Allow HTTPS to Microsoft Intune network.
2. Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service.
3. Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login.
4. Allow HTTPS to 74.125.0.0/16, Google Play Downloads.

Google G Suite

Combining Extreme Networks Access Control (EAC) solution with Google's G Suite allows network and security administrators to ensure that only registered Chrome OS devices are able to use the network and its resources. The solution also pulls extensive device data from G Suite and updates the end-systems in EAC to provide network administrators with a unique view of Chrome OS data within a single management interface.

The solution currently only support Chrome OS devices.

Module Configuration

The table below lists the configuration options for the Google GSuite agent.

Configuration Option	Description
Service Account ID:	Email address of the service account to use for authentication. You can find your service account ID within your Google API Manager project (https://console.developers.google.com/projectselector/apis/credentials?pli=1) where you configured/created your service account when you go into the account details. Example: gsuiteserviceaccount2@extreme-gsuite-test.iam.gserviceaccount.com
Service Account User:	Email address of a user account from your G Suite account / domain. This is used for Connect to know to which domain to connect to. Example: kurt@extremetest.net

Service Configuration

The table below lists the configuration options for the Google GSuite server.

Configuration Option	Description
Poll interval:	The time (in seconds) the module will wait after each run. For example, if you want to run the synchronization once per hour you can configure '3600' here.

Configuration Option	Description
Default end-system group for all devices from G Suite:	The default end-system group name where we assign all G Suite devices to in NAC. If you don't want end-systems from G Suite to be assigned to this default group, configure a group name which doesn't exist in NAC or disable the group assignment feature on the “Extreme Control” module. Default: Chrome Devices
Format of the incoming data for devices from G Suite:	Format of the data that gets stored in the custom data field. You can choose and combine any of the available variables: nwAdapterType, mac, annotatedAssetId, annotatedLocation, annotatedUser, recentUsers, currentUser, deviceId, etag, firmwareVersion, kind, lastEnrollmentTime, lastSync, model, notes, orderNumber, orgUnitPath, osVersion, platformVersion, serialNumber, status, supportEndDate, willAutoRenew. But be aware that G Suite might update the “lastSync” and “lastEnrollmentTime” values for each device very regularly and Connect is calling XMC's API to refresh that value in all end-systems custom fields. Depeding on your poll interval this might put a lot of stress onto the XMC server and it is thus recommended to _NOT_ use these variables in large environments. It should only be used if the poll interval is very low (like a few times per day) and the number of end-systems isn't too high (below 1000). Default: user=#currentUser#, recentUsers=#recentUsers#, annotatedUser=#annotatedUser#, adapterType=#nwAdapterType#; OS=#osVersion#, firmware=#firmwareVersion#
End-system group for decommissioned devices:	The default end-system group for devices which existed in G Suite but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by G Suite anymore and that could pose a threat) you can configure the group they should automatically be moved to here and enable the corresponding feature below. Make sure you manually create this end-system group in NAC.
Remove device from other groups on decommission:	Enable this to move devices which have been deleted from G Suite to the NAC end-system group configured by the corresponding option above. If disabled, devices won't be automatically move to this group but rather stay with their existing group membership(s). Default: false
Delete custom data in XMC for decommissioned devices:	If a device is deleted in G Suite the end-system's custom data field in XMC will be cleared as well. On the one hand this will keep your data clean in NAC but on the other hand it might often be helpful to still see the (old) G Suite data for those end-systems which have once been managed by G Suite. Default: false
Overwrite the existing username with the one acquired from G Suite:	If set to "true" the username for devices retrieved from G Suite will overwrite the username which is already in NAC. If no username could be retrieved from G Suite for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten! Default: false

Google APIs

You will need to create a “service account” within the Google APIs management site: https://console.developers.google.com

That service account provides Connect with a credentials that enables it to authenticate and authorize against the Google Admin SDK that is used to pull data from your G Suite domain.

1. Access the API Console Credentials page: https://console.developers.google.com/project/_/apis/credentials
2. Select your project (or create a new one) from the drop-down menu.
3. On the Credentials page, select the Create credentials drop-down, then select Service account key.

4. From the Service account drop-down, select an existing service account or create a new one.
5. For Key type, select the P12 key option, then select Create. The file automatically downloads to your computer.
6. Rename the downloaded credentials file to “gSuiteCredentials.p12“ and copy it to your XMC server (using WinSCP for example) to this location /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect/gSuiteCredentials.p12
7. Go into the details on your newly created Credentials and note down the “Client-ID” (number) [Symbol] this will be needed later on to authorize these credentials on your G Suite domain

Google Admin

If not already done, create a Google G Suite account and connect it with your domain. For test accounts, use: https://gsuite.google.com/signup/basic/welcome.

You will need to authorize the Extreme Connect application to provide it with access to your domain and two scopes. The basic process is described at https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#delegatingauthority

To delegate domain-wide authority to a service account, first enable domain-wide delegation for an existing service account in the Service accounts page (https://console.developers.google.com/permissions /serviceaccounts) or create a new service account (https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#creatinganaccount) with domain-wide delegation enabled.

Then, an administrator of the G Suite domain must complete the following steps:

1. Access the G Suite domain’s Admin console.
2. Select Security from the list of controls. If you don't see Security listed, select More controls from the gray bar at the bottom of the page, then select Security from the list of controls. If you can't see the controls, make sure you're signed in as an administrator for the domain.
3. Select Show more and then Advanced settings from the list of options.
4. Select Manage API client access in the Authentication section.

5. In the Client Name field, enter the service account's Client ID. You can find your service account's client ID in the Service accounts page.
6. In the One or More API Scopes field, enter the list of scopes that your application should be granted access.
7. Enter these two scopes for the API client that you authorize for Connect: https://www.googleapis.com/auth/admin.directory.device.chromeos, https://www.googleapis.com/auth/admin.directory.user.readonly

   The first one allows Connect to view and manage your Chrome OS devices' metadata, and the second one allows Connect to view users on your domain.
8. Click Authorize.
9. Remember to enable “domain-wide authority delegation” as described in the link above.

User Privileges

Ensure that the configured user is configured to have at least the prvileges to manage Chrome OS devices as shown below. This privilege is needed to retrieve data on Chrome OS devices.

Verification

You should verify that data from all devices managed by G Suite is imported to NAC. Navigate to the end-system table under the “Connect” tab and display the custom data field which you have configured for the G Suite module. You might need to make the corresponding column visible first. If you enabled the corresponding features you should also see the username retrieved from G Suite.

You can also verify whether all devices managed by G Suite have been assigned to configured end-system group in NAC (if you created such a group and configured it within the “G Suite” module).

Deleting G Suite Devices

To test this workflow, simply “deprovision” a device from G Suite and wait for the next Connect synchronization. Then verify that

1. This device’s custom field has been emptied (if this feature has been enabled in the config file).

2. This device is now member of the NAC end-system group for decommissioned devices (if this feature has been enabled).
3. This device does not appear in the end-system list that is displayed at the bottom of the Connect management web site (tab: G Suite). This means that the device has been deleted in the internal list as well.

Microsoft System Center Virtual Machine Manager (SCVMM)

The SCVMM integration offers provisioning of virtual machines into NAC end-system groups based on the virtual interfaces to which each VM is connected. Data within Extreme Management Center is enriched for each end-system and conversely made available within SCVMM. The VMM is a central Microsoft server that enables management of multiple Hyper-V servers from one console.

Note: The SCVMM server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the SCVMM OFConnect module (config file: SCVMMHandler.xml)

Service Configuration	Description
ADapter IP	IP Address of the Virtual Machine Manager adapter.
Adapter Port	Port where the Virtual Machine Manager adapter is listening on.
Pre-Shared Key	The pre-shared key used to communicate with the SCVMM adapter.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCVMM server.
Module loglevel	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.

General Module Configuration	
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from the adapter running on the SCVMM server (valid values: 1-4).
Outgoing data format	The format of the Extreme Management Center data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within the SCVMM management console. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from the adapter running on the SCVMM server and written to the custom field.
Use network name as end-system group	If this is set to true, the name of the portgroup /network will be used as the name for the end-system group (Note: Only data before the first _ will be used).

Adapter Installation

OFConnect is retrieving and setting datato/from a Virtual Machine Manager (VMM) server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within OFConnect. The adapter consists of a Java executable file (.jar) and a configuration file. To install the adapter:

1. Install the latest Java Runtime Environment, .NET framework and Windows Powershell 2.0 on the SCVMM server.
2. Acquire the file “Datacenter Manager SCVMM Adapter.zip” from GTAC or by contacting your local Extreme representative.
3. Copy the executable jar file (DCM_SCVMM_ADAPTER_<version>.jar) and the configuration file (DCM_SCVMM_ADAPTER.config) into a separate directory created under “Program Files/Extreme Networks/SCVMM Adapter” directly on the SCVMM server.
4. Edit the configuration file according to your environment. The configuration file contains an explanation of all settings and you can also find them listed below.
5. Save and close the configuration file.

6. Start the adapter manually first by opening a cmd shell or Powershell, navigate into the installation directory and use the following command: java –jar DCM_SCVMM_ ADAPTER_<version>.jar.
7. Check the log file to validate proper functionality.
8. Check the end-system list within OneView or NAC Manager to see data for the SCVMM virtual machines coming into the custom column you've configured within the SCVMMHandler.xml config file.
9. After you have successfully verified the integration, ensure that the DCM_ SCVMM _ ADAPTER_<version>.jar file is getting started on Windows server startup automatically. Stop the adapter currently running within the cmd/Powershell window, configure the auto-start for the .jar file (this depends on your Windows Server version) and restart your SCVMM server when appropriate in order to test the auto-start of the .jar file (you should see a java process running in the process tree).

Adapter Configuration

The table below lists the configuration options for the SCVMM agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
SCVMM_DLL	Location (path + file name) of Microsoft.SystemCenter.VirtualMachineManager.dll Example: C:\Program Files\Microsoft System Center Virtual Machine Manager 2008 R2\bin\Microsoft.SystemCenter.VirtualMachineManager.dll
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect SCVMM module.
IS_PRE_SHARED_KEY_ENCRYPTED	If set to "false" the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to "true". To change this key at a later stage, change the key above, set this value back to "false" and restart the adapter service
SCVMM_SERVER	The DNS name of the Virtual Machine Manager server to connect to. So far this has only been tested with this adapter and the VMM server running on the same server although remote connections might work as well.

Verification

Within the SCVMM management console, add the description field/column to the overview list of all VMs. You should see network related information retrieved from Extreme Management Center/NAC within this column as well as additional data from SCVMM within the end-system list in OneView or NAC Manager.

Microsoft Hyper-V

The Hyper-V integration offers provisioning of virtual machines into NAC end-system groups based on the virtual interfaces to which each VM is connected. Data within Access Control engine is enriched for each end-system and conversely made available within Hyper-V. When integrating with multiple Hyper-V servers you can either add each of those servers as a new entry within this module's config (list of services/agents to connect to) or use the integration with System Center Virtual Machine Manager.

Note: The Hyper-V server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the Hyper-V OFConnect module (config file: HyperVHandler.xml)

Service Configuration	Description
Adapter IP	IP Address of the Hyper-V adapter.
Adapter Port	Port where the Hyper-V adapter is listening on.
Pre-Shared Key	The pre-shared key used to communicate with the Hyper-V adapter.

General Module Configuration	
Poll Interval in seconds	Number of seconds between connections to the adapter running on the Hyper-V server.
Module loglevel	Verbosity of the module. Logs are stored in Access Control engine's server.log file.
Module Enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Access Control engine to update the information for end-systems retrieved from the adapter running on the Hyper-V server (valid values: 1-4).
Outgoing data format	The format of the Access Control engine data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within the Hyper-V management console. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from the adapter running on the Hyper-V server and written to the custom field.
Use network name as end-system group	If this is set to "true", the name of the portgroup /network will be used as the name for the end-system group (Note: Only data before the first _ will be used).

Adapter Installation

Extreme Management CenterConnect retrieves and sets data from and to a Hyper-V server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within Extreme Management Center. The adapter consists of a Java executable file (.jar) and a configuration file and uses a Powershell module as a prerequisite. To install the adapter manually:

1. The adapter utilizes a Powershell module that needs to be downloaded and installed prior to installing the adapter. Download the module here: http://pshyperv.codeplex.com/releases/view/62842#DownloadId=219013
2. Right click on zip file and UNBLOCK.
3. Copy the zip file to the following location: C:\Windows\System32\WindowsPowerShell\v1.0\Modules
4. Unzip and install the HyperV module using the "install.cmd" file.
5. Bring up Powershell and enter "Set-ExecutionPolicy Unrestricted"
6. Run the command "Import-Module HyperV" and make sure that no errors occur. If this doesn't load the module you can insert the folder "<folderwhereyouunzippedthedownloadedfile>\Hyper-V" into your PATH environment variable so Windows knows from where to load the module.
7. As a final test run "get-command -module HyperV" and check if this prints out the available Hyper-V commands.
8. Install the latest Java Runtime Environment.

9. Create a dedicated folder (example: “C:\Program Files\Extreme Networks\HyperV Adapter”) and copy the two files (DCM_HYPERV_ADAPTER_<version>.jar and DCM_HYPERV_ADAPTER.config) into it
10. Edit the configuration file DCM_HYPERV_ADAPTER.config according to your environment.
11. You are now ready to start the adapter by double-clicking the file DCM_HYPERV_ADAPTER.jar or running it within a shell using “java –jar DCM_HYPERV_ADAPTER.jar”. Verify the log file that should have been created in the same folder where the jar file is located. The adapter is automatically started when the Windows Server starts up.
12. Repeat these steps on all Hyper-V servers that you want to integrate with Extreme Management Center.

Adapter Configuration

The table below lists the configuration options for the Hyper-V agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on.
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect Hyper-V module.
IS_PRE_SHARED_KEY_ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to 'true'. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service.

Verification

Within the Hyper-V management console, click on a virtual machine. You should see the corresponding data from Extreme Management Center in the “Notes” field on the bottom of the page.

VMware vSphere

The Vmware vSphere integration offers provisioning of virtual machines in the network as well as automating the creation of virtual networks based on end-

system access groups. In addition, data within Extreme Management Center is enriched for each end-system and conversely made available within vSphere.

Module Configuration

Configuration Option	Description
Username	Username used to connect to the vSphere web service. Read/Write/Execute permissions required.
Password	Password used to connect to the vSphere web service.
VMware Webservice URL	Web service URL of the VMware vSphere server.
Module enabled	Enables and Disables Module.

- Outgoing data format: The format of the Extreme Control data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within VMware or XEN. You can customize the appearance and what information you want to include/exclude from there. Hint: For the VMware vSphere client the annotation field is limited in size. The default outgoing format is very close to the maximum string length allowed for this field. If you want to add additional information to this field consider replacing it with some of the existing default value.
- Format of the incoming data: The format of the data that is coming from VMware or XEN and that is written to the custom field.
- Create Private VLAN Entries: If set to false, the Datacenter manager will not automatically create any pVLAN entries on dvSwitches even if you configured any. This feature is disabled per default and needs to be enabled manually if needed.
- Create Portgroups from End-system Groups: If set to true, the Datacenter manager will automatically create new portgroups within VMware based on the Extreme Access Control engine end-system groups and your other configuration.
- Update Portgroup VLAN IDs: Only useful if the setting above is set to true. If you change the “vlan=XXXX” value within an end-system group this setting will automatically also change your portgroup VLAN IDs accordingly.
- Use Global End-system Groups: Only if this is set to true, the VMware module will have access to the global end-system groups that are provided by the Extreme Control module within the main module. This is necessary if you want to automatically create portgroups based on Extreme Control NAC end-system groups.
- Enable NAC Plugin: Using this option, the automatic Extreme Access Control engine Plugin Extension registration may be disabled.
- NAC Plugin URL: The URL of the configuration file for the Extreme Datacenter manager plugin for VMware. This is used by vCenter server to tell any connecting vCenter clients from where to download the Extreme plugin.

- Enable Custom Attributes: En-/Disables the creation and updates of Custom Attributes for vCenter Servers.
- Custom Attributes Data Format: This text field allows the configuration of Custom Attributes for vCenter Servers. Connect will create and update these attributes for each VM and allow for searching and sorting for this data within vCenter. Each attribute has to be configured on a single line and follow the format: NAME=VALUE where NAME is the name of the Custom Attribute and VALUE is a free text that may utilize all variables that are available in the "Outgoing data format" option. If a VM should use more than one network interface, the data for each variable is presented as "NIC1DATA/NIC2DATA/...".
- Deletion Group: Name of the portgroup that a VM will be redirected to if it's current endsystem group is deleted.
- Port Group Import: Enables the automatic creation of endsystemgroups in Extreme Control based on port groups. The port group name will be used for the endsystem group. Be aware that the delimiter also applies here. In the default configuration, the text after the last delimiter will be truncated from the name.
  i.e. MyPortGroup_VLAN1_dvSwitch0 will be imported as MyPortGroup_VLAN1 in Extreme Control. VLAN IDs will be updated if they change.
- Automatic Enforce after import: Enables the automatic enforcement of all appliances and the policy domain (only for extended import) if a portgroup was imported.
- Extended PortGroup Import: Also creates NAC Configuration and policy profiles during PortGroup Import. Requires the options for NAC Configuration, Policy Domain and Forward as Tagged also to be defined. Be aware that the truncated port group name will also be used as the VLAN name and must adhere to naming limitations.
- Enable PortGroup Import Removal: Delete the NAC Configuration and/or End-System Group if the portgroup is deleted.

Stop then start the Extreme Management Center services (refer to Extreme Connect Installation section for instructions).

Verification

Within the vSphere Client, click on a virtual machine and then on the "Summary" tab on the right side. At the bottom of this tab there should be an annotations field that should contain the corresponding data from Extreme Management Center (for example, information on the switch port and switch IP to which this VM is physically connected).

VMware View

The integration of VMware View does not require any special tool or software to integrate. The virtual desktops need to be configured to use 802.1x and users have to use the View Client to access those desktops via PCoIP in order to allow user-based authentication. Any Extreme switch with a reasonable amount of multi-user authentication capacity is suitable to authenticate each virtual desktop individually and apply a policy based on the username.

In addition to that, standard Extreme Connect operation may be used to provision a NAC rule for the connected portgroup of each VM, if user authentication via 802.1x is not available.

Please see the VMware View VDI documentation for further information regarding the setup procedure.

Related Information

For information on related tabs:

Extreme Management CenterExtreme Connect Overview

Web Service Error Codes

- Inventory Web Service
- NAC Configuration Web Service
- NAC End System Web Service
- NAC Web Service
- Netsight Device Web Service
- Policy Web Service
- Purview Web Service
- Reporting Web Service

Error Code	Description
0	Operation was successful

Error Code	Description
1	The requested object does not exist
2	Object already exists
3	Parameter value is incorrect
4	Error parsing an input
5	Result would be an Invalid configuration
6	Remote connection error
7	Unexpected error condition
8	End system group does not exist
9	CSV operation error