



# **Extreme Networks Extreme Management Center<sup>®</sup>**

***Inventory Manager User Guide***



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

## Legal Notices

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

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

## Trademarks

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

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

For additional information on Extreme Networks trademarks, please see: [www.extremenetworks.com/company/legal/trademarks/](http://www.extremenetworks.com/company/legal/trademarks/)

## Support

For product support, including documentation, visit: [www.extremenetworks.com/support/](http://www.extremenetworks.com/support/)

## Contact

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

Toll-free: +1 888-257-3000



## Extreme Networks® Software License Agreement

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

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

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

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

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

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED

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

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

7. TITLE AND PROPRIETARY RIGHTS

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

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

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

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

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

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

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



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

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

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

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

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

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

# Table of Contents

---

Legal Notices .....	i
Trademarks .....	i
Support .....	i
Contact .....	i
Extreme Networks® Software License Agreement .....	ii
Table of Contents .....	x
<b>Extreme Management Center® Inventory Manager Help .....</b>	<b>1</b>
Inventory Manager Features .....	1
Document Version .....	2
<b>Inventory Manager Configuration Considerations .....</b>	<b>4</b>
Firmware Considerations .....	4
Firewall Considerations .....	4
Capacity Planning Considerations .....	4
<b>Getting Started with Inventory Manager .....</b>	<b>7</b>
Set Up .....	7
Using Features .....	9
FTP Server Setup .....	10
Configuring FTP Server Properties and Login Information .....	10
Changing Your Firmware Directory .....	12
Setting Your File Transfer Method to FTP .....	12
SCP Server Setup .....	14
Configuring SCP Server Properties and Login Information .....	14
Changing Your Firmware Directory .....	16
Setting Your File Transfer Method to SCP .....	16
TFTP Server Setup .....	18

---

Configuring the NetSight TFTP Service .....	18
Using a Different TFTP Server .....	19
Changing Your Firmware Directory .....	21
Firmware Discovery .....	22
Discovering Your Firmware .....	22
Adding New Firmware Images .....	23
<b>How To Use Inventory Manager .....</b>	<b>24</b>
How to Add and Delete Devices .....	25
Using Console to Discover Devices .....	25
Using Console to Import Devices .....	26
Adding a Single Device .....	26
Deleting Devices from the NetSight Database .....	26
How to Add and Remove Device Groups .....	28
Adding a Device Group .....	29
Adding Devices to a Device Group .....	29
Using the Add Device Window .....	29
Using the Device Group Selection Window .....	29
Dragging and Dropping Devices .....	30
Removing Devices from a Device Group .....	30
Renaming a Device Group .....	31
Deleting a Device Group .....	31
How to Archive .....	32
Using the Archive Wizard .....	33
Saving a New Archive Version .....	35
Editing an Archive .....	35
Renaming an Archive .....	36

---

Deleting an Archive .....	36
How to Assign Firmware .....	37
How to Compare Archives .....	39
How to View and Compare Configuration Files .....	41
Viewing a Configuration File .....	41
Comparing Configuration Files .....	41
How to Create and Download Configuration Templates .....	43
Creating a Configuration Template .....	43
Editing a Configuration Template .....	44
Setting Values for Template Variables .....	45
On a Single Device .....	45
On Multiple Devices .....	45
Assigning Templates to Device Types .....	46
Using the Template Download Wizard .....	46
How to Initialize Inventory Database Components .....	49
How to Push Local Firmware to the Server .....	50
How to Reset a Device .....	51
How to Restore an Archive .....	53
How to Set a File Transfer Method .....	55
Setting the File Transfer Method for a Device .....	55
Setting the Default File Transfer Method for a Device Type Family .....	55
How to Set a Reference Image .....	57
How to Set Inventory Manager Options .....	58
Configuring Alternate Firmware Servers .....	58
Setting the Data Storage Directory Path .....	59
Setting FTP Transfer Settings .....	60

---

Setting TFTP Transfer Settings .....	61
Setting SCP Transfer Settings .....	62
How to Set Up Alternate Firmware Download Servers .....	65
Configuring the Alternate Server .....	65
Creating and Assigning Firmware Records .....	66
Setting the Firmware Server .....	68
How to Set Up Third-Party Device Support .....	70
Device Family Definition Files .....	71
Creating Device Family Definition Files .....	71
Using Script Variables .....	73
System-Defined Variables .....	74
User-Defined Variables .....	75
Sample Script Execution .....	77
File Backup and Restore .....	78
Configuring Devices .....	79
Logging and Error Reporting .....	82
Logging .....	82
Log Output .....	82
Error Troubleshooting .....	83
How to Track a Device .....	85
How to Upgrade Boot PROM .....	86
Preparing to Upgrade .....	86
Performing an Upgrade .....	88
How to Upgrade Firmware .....	91
Preparing to Upgrade .....	91
Performing an Upgrade .....	93

---

Scheduling an Upgrade .....	96
Viewing Scheduled Upgrades .....	98
Canceling a Scheduled Upgrade .....	98
How to Use the BOOTP Service .....	100
Creating a Bootptab File .....	100
Creating a bootptab file automatically .....	100
Creating a bootptab file manually .....	101
<b>Capacity Planning Reports .....</b>	<b>103</b>
Report Templates .....	103
Chassis Capacity Report .....	105
Flow .....	105
Select Report Window .....	105
Select Targets Window .....	107
Specify Time Window .....	109
Chassis Results Window .....	111
Chassis Results - Summary by Chassis (% utilization) .....	111
Table .....	113
Chassis Results - Summary by Chassis (average) .....	114
Table .....	115
Chassis Results - FRU Details .....	115
Table .....	117
Component Change Report .....	120
Flow .....	120
Select Report Window .....	120
Select Targets Window .....	122
Select FRU Types Window .....	123



---

Specify Time Window .....	125
Results Window .....	127
Results - Summary By FRU Type .....	128
Table .....	129
Results - Added FRUs .....	130
Table .....	131
Results - Removed FRUs .....	131
Table .....	133
FRU Results - All FRU Details .....	133
Table .....	134
Field Replaceable Unit (FRU) Report .....	137
Flow .....	137
Select Report Window .....	137
Select Targets Window .....	139
Select FRU Types Window .....	141
Specify Time Window .....	143
FRU Results Window .....	144
FRU Results - Totals By FRU Type .....	145
Table .....	146
FRU Results - FRU Details .....	147
Table .....	149
Submodule Capacity Report .....	151
Flow .....	151
Select Report Window .....	152
Select Targets Window .....	153
Specify Time Window .....	155

---

Submodule Results Window .....	156
Submodule Results - Summary By Chassis .....	157
Table .....	158
Submodule Results - Summary by Device Type .....	159
Table .....	160
Submodule Results - Summary by Submodule Type .....	160
Table .....	161
Submodule Results - All Submodule Details .....	162
Table .....	163
Used/Unused Ports Report .....	165
Flow .....	165
Select Report Window .....	165
Select Targets Window .....	167
Select Port Attributes Window .....	168
Specify Time Window .....	171
Port Results Window .....	173
Port Results - Totals by Group .....	173
Table .....	174
Port Results - Devices Only .....	176
Table .....	177
Port Results - Totals by Port Type .....	178
Table .....	179
Port Results - Port Details .....	181
Table .....	182
Port Results - Used Ports .....	183
Table .....	184

---

Port Results - Unused Ports .....	184
Table .....	185
Used/Unused Slots Report .....	188
Flow .....	188
Select Report Window .....	188
Select Targets Window .....	190
Specify Time Window .....	192
Slot Results Window .....	194
Slot Results - Show Data by Chassis Type .....	194
Table .....	196
Slot Results - Show Data by Chassis .....	197
Table .....	198
<b>Inventory Manager Wizards .....</b>	<b>200</b>
Archive Wizard .....	201
Archive Name Window .....	202
Archive Setup .....	203
Device Selection Window .....	203
Schedule Window .....	205
Devices .....	205
Schedule .....	206
Process .....	206
Restore Wizard .....	208
Archive Version Selection Window .....	208
Archives .....	209
Configurations to Restore .....	209
Restore Configurations Window .....	210

---

Reset Device Wizard .....	213
Device Selection Window .....	213
Select devices to reset .....	214
Selected Devices .....	214
Reset Devices: Timed Reset Supported Window .....	215
Reset Devices: Timed Reset Not Supported Window .....	217
Firmware Upgrade Wizard .....	219
Device Selection Window .....	220
Select devices to upgrade .....	221
Selected Devices .....	221
Firmware Selection Window .....	222
Assignments .....	223
Image List .....	225
Download Progress Window .....	227
Download Schedule Window .....	229
Schedule .....	230
Process .....	230
Reset Devices: Timed Reset Supported Window .....	230
Reset Devices: Timed Reset Not Supported Window .....	233
Boot PROM Upgrade Wizard .....	236
Device Selection Window .....	237
Select devices to upgrade .....	237
Selected Devices .....	238
Boot PROM Selection Window .....	238
Assignments .....	239
Image List .....	240

---

Download Progress Window .....	241
Reset Devices: Timed Reset Supported Window .....	243
Reset Devices: Timed Reset Not Supported Window .....	246
Template Download Wizard .....	249
Template Download Selection Window .....	249
Templates .....	250
General .....	250
Device Selection Window .....	251
Select devices to configure .....	252
Selected Devices .....	252
Download Template Configurations Window .....	253
<b>Inventory Manager Right-Panel Tabs .....</b>	<b>256</b>
Archives Tab (Device) .....	257
Attributes Tab (Configuration) .....	259
Chassis Tab (Chassis Folder) .....	262
Configuration Templates Tab (Device) .....	264
Available Templates .....	265
All Available Template Variables .....	265
Custom Attributes Tab (Configuration) .....	267
Custom Attributes .....	267
Legacy Devices .....	268
SSR Hardware Attributes .....	268
E5 and E6/E7 Power Supply and Fan Attributes .....	269
RoamAbout Radiocard and Base MAC Address Attributes .....	269
Vertical Horizon Attributes .....	269
ELS Serial Number Attribute .....	270

---

Custom Attributes Tab (Device or Device Group) .....	271
Custom Attributes .....	271
Legacy Devices .....	272
SSR Hardware Attributes .....	272
E5 and E6/E7 Power Supply and Fan Attributes .....	273
RoamAbout Radiocard and Base MAC Address Attributes .....	273
Vertical Horizon Attributes .....	273
ELS Serial Number Attribute .....	274
Details View Tabs .....	275
Details View Tab (All Devices Folder) .....	276
Details View Tab (All Firmware Folder) .....	281
Details View Tab (All Templates Folder) .....	284
Details View Tab (Archive) .....	286
Details View Tab (Archive Version) .....	289
Details View Tab (Archives Folder) .....	291
Details View Tab (Device Group) .....	293
Details View Tab (Device Type Folder - Firmware) .....	298
Details View Tab (Firmware Group) .....	301
Details View Tab (Unknown Folder - Firmware) .....	304
Details View Tab (Grouped By Folder) .....	307
Details View Tab (My Network Folder) .....	312
Details View Tab (Device Type Folder - Templates) .....	317
Details View Tab (Template Group) .....	319
Details View Tab (Unknown Folder - Templates) .....	321
General Tabs .....	323
General Tab (Archive) .....	324

---

Schedule .....	325
Process .....	325
Archive Setup .....	326
General Tab (Archive Version) .....	327
General Tab (Configuration) .....	329
General .....	330
Configuration Archive .....	330
Capacity Planning .....	331
General Tab (Device) .....	332
Device Identification .....	332
Profiles .....	335
Description .....	335
General Tab (Device Type) .....	336
General Tab (Firmware Image) .....	339
General Tab (Template) .....	342
Image Information Tab (Device) .....	344
Last Known Images .....	344
Last Known Configuration File .....	345
Features Supported by this Device .....	345
MIB and Script Overrides .....	345
Module Information Tab (Device) .....	347
Template Variables Tab .....	349
<b>Inventory Manager Windows .....</b>	<b>351</b>
Add Device Window .....	352
Add Filters Window .....	355
Add Alternate Firmware Server Window .....	357

---

Server Properties .....	357
TFTP Connection Information .....	358
FTP/SCP Connection Information .....	358
Assign Configuration Template Window .....	360
Assign Firmware Window .....	362
Compare Archives Window .....	364
Comparison Results Table .....	365
Right-Click Menu Options .....	365
Compare Configuration Files Window .....	367
Find Tab .....	367
Filter Tab .....	369
Configuration File Viewer .....	372
Find Tab .....	372
Filter Tab .....	374
Create Firmware Record Window .....	377
Database Properties Window .....	380
Device Group Selection Window .....	381
Device Template Variables Window .....	382
Edit Alternate Firmware Server Window .....	384
Server Properties .....	384
TFTP Connection Information .....	385
FTP/SCP Connection Information .....	385
Edit Configuration Template Window .....	387
E-Mail Configuration Window .....	390
Event Details Window .....	392
File Transfer Method Window .....	394



---

File Transfer Method - Device .....	394
File Transfer Method - Device Type Family .....	395
Inventory Manager Options Window .....	397
Alternate Firmware Servers .....	397
Data Storage Directory Path .....	398
File Transfer Settings .....	399
FTP Transfer Settings .....	399
TFTP Transfer Settings .....	401
SCP Transfer Settings .....	403
Main Window .....	406
Menu Bar .....	407
File Menu .....	408
Edit Menu .....	408
View Menu .....	409
Tools Menu .....	409
Applications Menu .....	415
Help Menu .....	415
Right-Click Menu Options .....	416
Tool Bar .....	417
Left Panel .....	419
Network Elements Tab .....	419
Firmware Mgmt Tab .....	421
Archive Mgmt Tab .....	423
Configuration Templates Tab .....	424
Left-Panel Icons .....	426
Right Panel .....	426

---

Active Status Panel .....	427
Summary View .....	428
Details View .....	429
Right-Click Menu Options .....	431
Event Log .....	431
Right-Click Menu Options .....	432
Status Bar .....	433
Open Configuration Window .....	435
Properties Window .....	437
General Area .....	437
Devices Area .....	438
Push Local Firmware to Server Window .....	440
Scheduled Events Window .....	442
Schedule Report Window .....	444
Schedule .....	445
Notification Settings .....	445
Select Archive Versions to Compare Window .....	447
Select Configurations Window .....	449
Select Devices Window .....	451
Set Firmware Server Window .....	453
Set Template Variables Window .....	455
Template Variables Window .....	457
Track Device Window .....	459
View Devices Window .....	462
<b>Troubleshooting .....</b>	<b>464</b>

# Extreme Management Center® Inventory Manager Help

---

Inventory Manager provides comprehensive network inventory and change management capabilities. Using Inventory Manager's features, you can view a system-level inventory of your network devices and their hardware, configuration, and firmware information. In addition, Inventory Manager tracks and reports changes to your network configuration, and provides a history of device changes that aids in troubleshooting network problems. Inventory Manager's Wizards let you easily perform routine network tasks such as configuration backups and firmware upgrades, and prepare valuable capacity planning reports.

Contact your sales representative for information on obtaining a NetSight software license.

## Inventory Manager Features

### System-level inventory of hardware, configurations, and firmware

- Provides a detailed inventory of products organized by device type.
- Tracks device attributes such as serial number, asset tag, firmware version, CPU type, and memory.
- Organizes firmware by associating it with the supported devices.
- Presents detailed configuration information including date and time of configuration saves, firmware version, and file size.

### Change management and audit functionality

- Records a history of device attributes, and reports any changes made to the device.
- Provides a history of firmware and configuration changes made to a device.
- Compares current device configuration with previously saved configurations and reports any differences.
- Provides a centralized history of Inventory Manager operations via the Active Status Panel and Event Log.

### Capacity Planning reporting capabilities

- Generates valuable, in-depth reports for network inventory planning purposes.
- Provides data on chassis, port, and submodule capacity and utilization.
- Presents detailed information on field replaceable/upgradeable (FRU) components in your network devices.
- Lets you schedule reports to run at specified intervals with report results sent out via a notification e-mail.

### Wizards for ease of use

- Firmware Upgrade Wizard -- download firmware to single or multiple devices simultaneously.
- Boot PROM Upgrade Wizard -- download boot PROM images to single or multiple devices simultaneously.
- Archive Wizard -- archive device configuration data and/or capacity planning data. The Wizard's task scheduler allows you to schedule routine archive saves.
- Restore Wizard -- restore saved device configurations to recover from a problem.
- Reset Wizard -- reset single or multiple devices using timed or manual reset.
- Template Download Wizard -- download text-based (ASCII format) configuration templates to one or more devices.
- Capacity Planning Wizard -- select from a set of report templates to create valuable network inventory planning reports.

## Document Version

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

<b>Date</b>	<b>Revision Number</b>	<b>Description</b>
06-16	7.0 Revision -00	Extreme Management Center (NetSight) 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release
01-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release

<b>Date</b>	<b>Revision Number</b>	<b>Description</b>
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9034982-01

# Inventory Manager Configuration Considerations

---

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

## Firmware Considerations

- Inventory Manager must use SNMPv3 access parameters when performing firmware upgrades, archive restore operations, or reset operations on XSR devices running firmware version 4.0 and higher.
- When restoring a configuration to an X-Pedition, if the configuration file has errors, it will not be restored to the device. You will need to correct any errors in the configuration file prior to restoring it. You can check a configuration file for errors via CLI; lines that contain errors have an "E" after the line number.

## Firewall Considerations

In order for TFTP or FTP services to function correctly, the Internet firewall settings on the Inventory Manager workstation or other workstations providing these services, must be configured to allow TFTP and FTP traffic.

## Capacity Planning Considerations

- The Used/Unused Ports Report correctly reports the total number of switch and router ports, but not repeater ports.
- The GIGAswitch Router 8x00 must be running firmware version E9.x.x.x or higher in order to report the control modules or fabric modules contained in the router.
- SSR devices do not report their HSSI and Serial ports in the Used/Unused Ports Report.
- SSR devices do not report 10 Gigabit ports in the Used/Unused Ports Report or FRU Report.

- SSR 2100 devices report a chassis FRU component in the FRU report, even though they are standalone devices.
- 1H582-25 devices require firmware version 3.0.14 or higher in order to report submodules in the FRU Report.
- 1G694-13 devices do not report any FRU ports in the FRU Report.
- 1G694-13 devices do not report any FRU submodules in the FRU Report or the Submodule Capacity Report.
- XSR devices with NIM cards installed do not report the NIM cards in the FRU Report or Submodule Capacity Report.
- XSR devices with NIM cards installed report the type of card and number of ports, but do not provide port details such as connector type and media type in the Used/Unused Ports Report.
- R2 devices incorrectly report their total number of ports in the Used/Unused Ports Report. It is recommended that you create a "Filter Out" filter for R2 devices when generating this type of report.
- VHSIM-G6, FDDI HSIM-F6, and ATM HSIM-A6DP submodules. Ports in these three submodules are configured to act in a redundant manner and therefore are reported as a single port in the Used/Unused Ports report.
- C1H124-48 devices do not report the connector type or media type correctly for any installed mini-GBIC ports in the Used/Unused Ports Report. These ports are also not identified as FRUs in the FRU Report.
- C1G124-24 devices may not report the existence of mini-GBIC ports in certain situations.
- V-Series stackable devices with older firmware may report an incorrect number of devices in the stack when gathering data for the FRU report.
- 6x2xx and 6x3xx devices always report the fan tray as installed in the FRU Report.
- 6x1xx/6x2xx/6x3xx and stand-alone 2x2xx devices incorrectly report submodule Description information in the FRU Report.
- C2 devices do not report their four SFP GBIC ports in the Used/Unused Ports Report; these combination RJ45/SFP ports are reported simply as RJ45 ports.
- 2E43-27R devices report an incorrect description for HSIM-F6 submodules in the FRU Report.
- If you have devices that are configured with multiple SNMP contexts in your device tree and you run a report on those devices, you may see that

report results display data for the device configured with the default context (switch mode) for each device with context. For example, if you target 10.10.20.20 and 10.10.20.20:context, the report may display results for 10.10.20.20 for both devices. Be aware that this will affect your result totals.



# Getting Started with Inventory Manager

---

Getting Started provides an overview of Inventory Manager features and a summary of the basic steps you must perform to begin using Inventory Manager.

Inventory Manager is a tool that monitors your network devices, including configuration and firmware changes. Inventory Manager provides the following functions:

- save a device's configuration so that it can be restored later
- restore a device's configuration from a previously saved configuration
- compare a device's configuration with a previous configuration and report any differences
- create a configuration template based on a saved configuration file, and download the template to one or more devices
- download firmware or boot PROM images to a device or group of devices
- view a history of firmware and configuration changes made to a device
- generate valuable, in-depth reports for network inventory planning purposes

## Set Up

Because Getting Started is meant to be used side-by-side with Inventory Manager, it will be most useful if you launch Inventory Manager and then use the steps below as an aid in learning how to use Inventory Manager.

Here are the things you'll need to do to begin using Inventory Manager in your network:

- 
- [TFTP Server Setup](#) Inventory Manager provides a NetSight TFTP server to download firmware/boot PROM to network devices, and save and restore device configurations. This help topic provides information on configuring the NetSight TFTP Server or using another TFTP server if desired.
-

---

<ul style="list-style-type: none"><li>• <a href="#">FTP Server Setup</a> <a href="#">SCP Server Setup</a></li></ul>	You can also download firmware/boot PROM images, and save and restore device configurations using an FTP and/or SCP server. These Help topics provides information on configuring FTP/SCP server properties and login information.
<ul style="list-style-type: none"><li>• <a href="#">Firmware Discovery</a></li></ul>	Instructions on storing your firmware and boot PROM images in a firmware directory, and performing a firmware discovery to display them in the Firmware Mgmt tree.
<ul style="list-style-type: none"><li>• <a href="#">Set Options</a></li></ul>	Instructions on setting options for various Inventory Manager functions.
<ul style="list-style-type: none"><li>• <a href="#">Add Devices</a></li></ul>	The NetSight database contains device models that represent the actual devices in your network. There are three ways to add devices to the NetSight database. Initially, you will want to perform a Console Discover to populate the database. You can also use Console to import devices from a .ngf file. After you have initially added your devices, you can use the Inventory Manager (or Console) <a href="#">Add Device window</a> to add a single device to the database. The devices are displayed under the Network Elements tab in the Inventory Manager main window.
<ul style="list-style-type: none"><li>• Define Authorization and Device Access</li></ul>	Use the Authorization/Device Access window (accessed from the Tools menu) to configure your Inventory Manager access privileges. The window has four tabs: <ul style="list-style-type: none"><li>• Users/Groups tab lets you manage user access to specific features and capabilities.</li><li>• Profiles/Credentials tab lets you define SNMP <i>credentials</i> used to access your network devices, and create <i>profiles</i> that use these credentials for various device access levels.</li><li>• Profile/Device Mapping tab lets you specify the <i>profiles</i> that will be used by users when communicating with network devices.</li><li>• Manage SNMP Passwords tab where you can manage the <i>credentials</i> that have been set on your network's devices.</li></ul>
<ul style="list-style-type: none"><li>• <a href="#">Add Device Groups</a></li></ul>	Inventory Manager lets you group your devices into logical groups to facilitate network management. With device groups, you can perform certain operations (like an archive save or restore) on an entire group at once, instead of performing the operation on individual devices.

---

## Using Features

Now that you have set up your devices and firmware, you can start exploring some of Inventory Manager's features:

- **Server Information** The Server Information window (accessed from the Tools menu) lets you view and configure certain NetSight Server functions, including management of client connections, database backup and restore, locks, and licenses. It also provides access to the server log and server statistics.
- [Save Configurations](#) Inventory Manager lets you save device configurations (called archives) using the Archive Wizard. You can schedule these saves to be performed on a regular basis.
- [Restore Configurations](#) Inventory Manager lets you restore your saved device configurations (archives) using the Restore Wizard.
- [Configuration Templates](#) Create a configuration template based on an existing archived configuration file, and then use Template Download Wizard to download the template to one or more devices.
- [Compare Archives](#) Compare archived configuration files and monitor any changes in device attributes.
- [Upgrade Firmware](#) Use the Firmware Upgrade Wizard to easily download firmware images to your network devices.
- [Upgrade Boot PROM](#) Use the Boot PROM Upgrade Wizard to easily download boot PROM images to your network devices.
- [Track a Device](#) Inventory Manager lets you track a device based on its MAC address or serial number. Use this feature as a way to view a history of device attributes, and monitor any configuration or firmware changes made to the device.
- [Capacity Planning](#) Use the Capacity Planning tool to prepare valuable network inventory planning reports on port and slot utilization, submodule and chassis capacity and usage, and field replaceable/upgradeable components (FRUs) in your network.

## FTP Server Setup

---

Before you can perform Inventory Manager archive operations or firmware/boot PROM upgrades using an FTP server, you must configure your FTP server properties and login information. When you install Inventory Manager, FTP server properties are configured according to certain default settings. Use the Options window to verify these settings and make any required changes, and enter your FTP server login information.

Inventory Manager uses the default `tftpboot\firmware\images` directory for storing your firmware. Once you have placed your firmware images in this directory, you must perform a [firmware discovery](#) to display them in the left-panel Firmware Mgmt tab. If you are using a different directory for storing firmware, you must specify the directory in the Options window [FTP Transfer Settings view](#).

In addition, all devices are initially configured with TFTP as their file transfer method, so you must change the devices' file transfer method to FTP.

---

**NOTE:** Refer to [How to Set Up Alternate Firmware Download Servers](#) for information on configuring alternate servers to perform remote firmware downloads.

---

Instructions on:

- [Configuring FTP Server Properties and Login Information](#)
- [Changing Your Firmware Directory](#)
- [Setting Your File Transfer Method to FTP](#)

## Configuring FTP Server Properties and Login Information

Use these instructions to specify the FTP server IP address, set paths to the root and firmware directories, and set login information. The FTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree under the Inventory Manager folder, expand the File Transfer Settings folder and select FTP Transfer Settings. The right-panel [FTP Transfer Settings view](#) is displayed.

3. Select the **Use the NetSight Server's IP** checkbox, or use the **FTP Server IP** field to enter the IP address of the device where the FTP server resides.
4. Enter the port number your FTP server is configured to run on.
5. Specify the **Root Directory Path**. The root directory is the base directory to which the FTP server is allowed access. The FTP server will be allowed to create files to or read files from this directory and any of its sub-directories. The default root directory is the tftpboot directory that Inventory Manager automatically creates when it is installed. If you would like to use a different root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

---

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your FTP server is configured with an FTP root directory, it must match the root directory entered here.
- If your FTP server is **not** configured with an FTP root directory, change the FTP root directory here to the root of the drive (e.g. C:\ or D:\).
- **If you are using an FTP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (UNIX or Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using h:\ (where h:\ is mapped to the tftpboot directory on the remote drive) use  
`\\yourservername\tftpboot\`

- 
6. Specify the **Firmware Directory Path**. The default firmware directory is tftpboot\firmware\images. If you would like to use a different firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an FTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
  7. Specify your FTP Server login information. Select the **Anonymous** checkbox if your FTP server is configured to accept Anonymous logins. (Inventory Manager will automatically fill in the username and password fields.) Otherwise, enter your username and password to access the FTP

server. For increased security, select the **Hide Password** checkbox and your password will be replaced with asterisks when it is typed in.

8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Changing Your Firmware Directory

If you want to change the directory for storing your firmware, you must change the FTP server properties using the [FTP Transfer Settings view](#) in the Options window.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree under the Inventory Manager folder, expand the File Transfer Settings folder and select FTP Transfer Settings. The right-panel FTP File Transfer Settings view is displayed.
3. Enter the path to the new directory in the **Firmware Directory Path** field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. If you are using an FTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
4. Click **OK** to set options and close the window.

## Setting Your File Transfer Method to FTP

You can set a file transfer method for a specific device, or specify a default transfer method for an entire device type using the [File Transfer Method window](#). Once you have specified the file transfer method for a device, all archive save and restore operations and firmware/boot PROM upgrades on that device will be performed using the specified method. All devices are initially configured with TFTP as their file transfer method, until specified otherwise using these windows. For complete instructions, see [How to Set a File Transfer Method](#).

---

### Related Information

For information on related tasks:

- [How to Set Inventory Manager Options](#)
- [Firmware Discovery](#)

- [How to Set a File Transfer Method](#)

For information on related windows:

- [Options Window, Inventory Manager Options](#)
- [File Transfer Method Window](#)

## SCP Server Setup

---

Before you can perform Inventory Manager archive operations or firmware/boot PROM upgrades using an SCP server, you must configure your SCP server properties and login information. When you install Inventory Manager, SCP server properties are configured according to certain default settings. Use the Options window to verify these settings and make any required changes, and enter your SCP server login information.

Inventory Manager uses the default `tftpboot\firmware\images` directory for storing your firmware. Once you have placed your firmware images in this directory, you must perform a [firmware discovery](#) to display them in the left-panel Firmware Mgmt tab. If you are using a different directory for storing firmware, you must specify the directory in the Options window [SCP Transfer Settings view](#).

In addition, all devices are initially configured with TFTP as their file transfer method, so you must change the devices' file transfer method to SCP.

---

**NOTE:** Refer to [How to Set Up Alternate Firmware Download Servers](#) for information on configuring alternate servers to perform remote firmware downloads.

---

Instructions on:

- [Configuring SCP Server Properties and Login Information](#)
- [Changing Your Firmware Directory](#)
- [Setting Your File Transfer Method to SCP](#)

## Configuring SCP Server Properties and Login Information

Use these instructions to specify the SCP server IP address, set paths to the root and firmware directories, and set login information. The SCP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree under the Inventory Manager folder, expand the File Transfer Settings folder and select SCP Transfer Settings. The right-panel [SCP Transfer Settings view](#) is displayed.



3. Select the **Use the NetSight Server's IP** checkbox, or use the **SCP Server IP** field to enter the IP address of the device where the SCP server resides.
4. Enter the port number your SCP server is configured to run on.
5. Specify the **Root Directory Path**. The root directory is the base directory to which the SCP server is allowed access. The SCP server will be allowed to create files to or read files from this directory and any of its sub-directories. The default root directory on Windows is the C:\ directory and on Linux it is the /root/ directory. If you would like to use a different root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

---

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your SCP server is configured with an SCP root directory, it must match the root directory entered here.
- If your SCP server is **not** configured with an SCP root directory, change the SCP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
- **If you are using an SCP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (UNIX or Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using h:\ (where h:\ is mapped to the firmware\images directory on the remote drive) use  
`\\yoursystemname\firmware\images`

- 
6. Specify the **Firmware Directory Path**. The default firmware directory is C:\firmware\images on Windows and /root/firmware/images on Linux. If you would like to use a different firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an SCP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
  7. Specify your SCP Server login information. Select the **Anonymous** checkbox if your SCP server is configured to accept Anonymous logins.

(Inventory Manager will automatically fill in the username and password fields.) Otherwise, enter your username and password to access the SCP server. For increased security, select the **Hide Password** checkbox and your password will be replaced with asterisks when it is typed in.

8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Changing Your Firmware Directory

If you want to change the directory for storing your firmware, you must change the SCP server properties using the [SCP Transfer Settings view](#) in the Options window.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree under the Inventory Manager folder, expand the File Transfer Settings folder and select SCP Transfer Settings. The right-panel SCP File Transfer Settings view is displayed.
3. Enter the path to the new directory in the **Firmware Directory Path** field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. If you are using an SCP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
4. Click **OK** to set options and close the window.

## Setting Your File Transfer Method to SCP

You can set a file transfer method for a specific device, or specify a default transfer method for an entire device type using the [File Transfer Method window](#). Once you have specified the file transfer method for a device, all archive save and restore operations and firmware/boot PROM upgrades on that device will be performed using the specified method. All devices are initially configured with TFTP as their file transfer method, until specified otherwise using these windows. For complete instructions, see [How to Set a File Transfer Method](#).

---

### Related Information

For information on related tasks:

- [How to Set Inventory Manager Options](#)
- [Firmware Discovery](#)
- [How to Set a File Transfer Method](#)

For information on related windows:

- [Options Window, Inventory Manager Options](#)
- [File Transfer Method Window](#)

## TFTP Server Setup

---

The NetSight TFTP service provides the ability to download firmware and boot PROM images to network devices, and save and restore device configurations. You can enable and start this TFTP service during installation, and specify the path to the TFTP root directory, if necessary. After you've installed Inventory Manager, you can use the Suite-Wide Options window Services for NetSight Server view to configure TFTP server properties. If you are using a TFTP server other than the one provided with Inventory Manager, you can use the Options window to configure the correct server properties.

Inventory Manager uses the default `tftpboot\firmware\images` directory for storing your firmware. Once you have placed your firmware images in this directory, you must perform a [firmware discovery](#) to display them in the left-panel Firmware Mgmt tab. If you are using a different directory for storing firmware, you must specify the directory in the Options window [TFTP Transfer Settings view](#).

---

**NOTE:** Refer to [How to Set Up Alternate Firmware Download Servers](#) for information on configuring alternate TFTP servers to perform remote firmware downloads.

---

Instructions on:

- [Configuring the NetSight TFTP Service](#)
- [Using a Different TFTP Server](#)
- [Changing Your Firmware Directory](#)

### Configuring the NetSight TFTP Service

When you install Inventory Manager, TFTP server properties are configured with the default settings for the NetSight TFTP service. Use the following instructions to verify these settings and make any desired changes.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Services for NetSight Server.
3. Specify the **Root Directory Path**. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to

create files to or read files from this directory and any of its sub-directories. The default root directory is the tftpboot directory that Inventory Manager automatically creates when it is installed. If you would like to use a different root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

---

**NOTE:** Changing the TFTP root directory requires restarting the TFTP server.

---

4. If your system is configured with multiple IP addresses, enter the appropriate IP address in the **TFTP Server IP Address** field.
5. Click **Apply** to set the options and leave the window open.
6. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select [TFTP Transfer Settings](#).
7. Specify the **Firmware Directory Path**. The default firmware directory is tftpboot\firmware\images. If you would like to use a different firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).)
8. Click **OK** to set the options and close the window.

## Using a Different TFTP Server

If you are using a TFTP server other than the NetSight TFTP service, use the following instructions to configure your TFTP server properties.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Services for NetSight Server.
3. If necessary, disable the NetSight TFTP service by deselecting the **Automatic Launch** checkbox for the NetSight TFTP service.
4. Configure your TFTP settings.
  - a. Specify the **Root Directory Path**. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to create files to or read files from this directory and any of its sub-directories. The default root directory is the tftpboot directory that Inventory Manager automatically creates when it is

installed. If you would like to use a different root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. Changing the TFTP root directory requires restarting the TFTP server.

---

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

-- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.

-- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive (e.g. C:\ or D:\).

-- **If you are using a TFTP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (UNIX or Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

h:\ (where h:\ is mapped to the tftpboot directory on the remote drive)

use

\\yourservername\tftpboot\

---

- b. If the TFTP server resides on a remote system, or if the local system is configured with multiple IP addresses, enter the IP address for the TFTP service in the **TFTP Server IP Address** field.
5. Click **Apply** to set the options and leave the window open.
6. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select [TFTP Transfer Settings](#).
7. Specify the **Firmware Directory Path**. The default firmware directory is tftpboot\firmware\images. If you would like to use a different firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using a TFTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
8. Click **OK** to set the options and close the window.

## Changing Your Firmware Directory

The default firmware directory is tftpboot\firmware\images. If you want to change the directory for storing your firmware, you must change the TFTP server properties using the [TFTP Transfer Settings view](#) in the Options window. The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).

1. Select **Tools > Options** in the menu bar. The Options window opens.
  2. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select TFTP Transfer Settings.
  3. Enter the path to the new directory in the **Firmware Directory Path** field, or use the **Browse** button to navigate to the directory. The firmware directory must be a sub-directory of the root directory. If you are using a TFTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
  4. Click **OK** to set options and close the window.
- 

### Related Information

For information on related tasks:

- [Firmware Discovery](#)
- [How to Set Inventory Manager Options](#)

For information on related windows:

- [Options Window, Inventory Manager Options](#)

## Firmware Discovery


---

Inventory Manager provides convenient and powerful tools for managing firmware and boot PROM images on your network devices. To take advantage of these tools, you must store your images in a specified firmware directory, and perform a firmware discovery that will automatically display your images in the left-panel Firmware Mgmt tab.

---

**NOTE:** If you are using an alternate firmware download server to perform remote downloads, you will need to manually create the firmware records associated with the alternate server (as opposed to having them automatically discovered during a firmware discovery.) Refer to [How to Set Up Alternate Firmware Download Servers](#) for more information.

---

For information on obtaining Extreme Networks firmware, contact your Extreme Networks sales representative, or access the Extreme Networks firmware download library at: <https://extranet.extremenetworks.com/downloads/> or from the Download icon  in the Firmware Mgmt tab's Details View. (A browser is required to view the website and Linux users must add the browser's path to their PATH environment variable.) If you download a firmware image that is contained in a .zip file, you must unzip the file before placing it into the firmware directory.

Instructions on:

- [Discovering Your Firmware](#)
- [Adding New Firmware Images](#)

## Discovering Your Firmware


Inventory Manager uses the default tftpboot\firmware\images directory for storing your firmware. If you are using an different firmware directory, you must specify that directory in the [TFTP Transfer Settings view](#), the [FTP Transfer Settings view](#), and/or the [SCP Transfer Settings view](#) of the Options window. (For more information, see [TFTP Server Setup](#), [FTP Server Setup](#), or [SCP Server Setup](#).)

---

**NOTE:** The maximum size allowed for a firmware image filename is 128 characters. The maximum size for the path to where the image is stored is 512 characters. Firmware images that exceed these maximums will not be discovered.

---




1. Place your firmware and boot PROM images in your firmware directory.
2. In the left-panel Firmware Mgmt tab, select **View > Refresh** from the menu bar. (You can also use the Refresh icon  in the right-panel Details Views.)

Inventory Manager automatically displays your firmware under pre-defined firmware groups in the left-panel Firmware Mgmt tree. You can assign firmware to multiple firmware groups to facilitate your firmware management according to your network needs. For more information see [How to Assign Firmware](#).

## Adding New Firmware Images

Once you have done an initial firmware discovery, you can add new firmware to the left-panel Firmware Mgmt tab using these instructions.

1. Place your new firmware in your firmware directory.
2. In the left-panel Firmware Mgmt tab, select **View > Refresh** from the menu bar. (You can also use the Refresh icon  in the right-panel Details Views.)

Inventory Manager automatically adds your new firmware to the appropriate firmware groups in the left-panel Firmware Mgmt tree.

---

### Related Information

For information on related tasks:

- [How to Assign Firmware](#)
- [FTP Server Setup](#)
- [TFTP Server Setup](#)
- [SCP Server Setup](#)

For information on related windows:

- [Options Window](#)

# How To Use Inventory Manager

---

The **How To** section contains Help topics that give you instructions for performing tasks in Inventory Manager.

## How to Add and Delete Devices

---

The NetSight database contains device models that represent the actual devices in your network. The models store attributes for your devices and make it possible to manage device access and view device status. Your devices are displayed in the left-panel Network Elements tab in the Inventory Manager main window.

NetSight Console and Inventory Manager (and any other NetSight plugin application) share the NetSight database. The devices displayed in the Console tree are also displayed in the Inventory Manager tree. Any changes you make to the devices are reflected in both trees.

There are three ways to add devices to the NetSight database. Initially, you will want to perform a Console Discover to populate the database. You can also use Console to import devices from a .ngf file. After you have initially added your devices, you can use the Inventory Manager (or Console) [Add Device window](#) to add a single device to the database.

Instructions on:

- [Using Console to Discover Devices](#)
- [Using Console to Import Devices](#)
- [Adding a Single Device](#)
- [Deleting Devices from the NetSight Database](#)

## Using Console to Discover Devices

Console Discover lets you to discover your network devices and add them to the NetSight database. You can perform a discover on a specified range of IP addresses, or perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices. Discover automatically explores a specific network segment and creates a list of discovered devices. You can then save all or a subset of the discovered devices to the NetSight database. Devices that are added to the database are automatically placed in the appropriate groups in the left-panel tree of the Console and Inventory Manager main window.

For step-by-step instructions, see the How to Discover Devices help topic in your Console online help system.

## Using Console to Import Devices

The Console Import Devices feature imports device information and profiles for unique devices (ones that do not exist locally) from a .ngf file. The devices that you import are added to the NetSight database and automatically appended to any existing devices in the left-panel tree of the Console and Inventory Manager main window.

For step-by-step instructions, see the Importing a Device List from a File section of the How to Export and Import a Device List help topic in your Console online help system.

## Adding a Single Device

You can add a single device to the NetSight database using the [Add Device window](#). When you add a single device, a device icon  is created and added to the All Devices folder and the appropriate device groups in the left-panel Network Elements tab. You must specify the device's SNMP profile. This information is used by Inventory Manager to access and manage the device.

1. Select the Network Elements tab.
2. Select any folder in the left-panel tree, right-click and select Add Device from the menu. The [Add Device window](#) opens.
3. Enter the IP address of the device you want to add.
4. Use the drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.
5. Select the checkbox and enter an [SNMP context](#), if desired.
6. Select whether to use the default [nickname](#) or click **Specify** to assign a unique nickname to this device.
7. To add the device and leave the window open, click **Apply**. To add the device and close the window, click **OK**.

## Deleting Devices from the NetSight Database

When devices are deleted from the NetSight database they are removed from all groups where they are a member. To delete devices from the NetSight database:

1. Expand the left-panel tree and select the device being deleted.
  2. Right-click the device and select **Delete** from the menu. A confirmation message advises that you are deleting the device from the NetSight database.
  3. Click **Yes** to delete the device.
- 

### **Related Information**

For information on related windows:

- [Add Device Window](#)

## How to Add and Remove Device Groups

---

You can organize your network devices into device groups and subgroups under the My Network folder in the Network Elements tab. Organizing your devices into groups lets you perform certain operations (like an archive save or restore) on an entire group at once, instead of performing the operation on individual devices. A set of system-created device groups are automatically provided. When a device is created, discovered, or imported, it automatically becomes a member of the appropriate system-created group:

- All Devices - contains all the devices in the NetSight database.
- Grouped By - contains five subgroups:
  - Chassis -- contains subgroups for specific chassis in your network.
  - Contact -- contains subgroups based on the system contact.
  - Device Types -- contains subgroups for the specific product families and device types in your network.
  - IP -- contains subgroups based on the IP subnets in your network.
  - Location -- contains subgroups based on the system location.

Additionally, you can add your own device groups and subgroups under the My Network folder, however you cannot add groups under the system-created groups. A device group cannot have the same name as another device group at the same level. You cannot rename or delete a system-created group. A device can be a member of more than one group.

---

**TIP:** System-created groups are displayed with blue folders in the left-panel tree. Any group you add will display a yellow folder.

---

Instructions on:

- [Adding a Device Group](#)
- [Adding Devices to a Device Group](#)
- [Removing Devices from a Device Group](#)
- [Renaming a Device Group](#)
- [Deleting a Device Group](#)

## Adding a Device Group

1. Click the left-panel Network Elements tab.
2. Right-click on the My Network folder or any user-created group, and select **Add Device Group** from the menu. This opens the Add Device Group window.
3. Enter the device group name and click **OK**. (Device groups cannot have the same name as another device group at the same level.) You can now [add devices](#) to the device group.

## Adding Devices to a Device Group

You can add a device to a group by using the Add Device window, the Device Group Selection window, or by using drag and drop.

### *Using the Add Device Window*

Use the Add Device window to add a single device to the NetSight database and to the group selected in the tree.

1. Right-click the group to which you want to add a device and select **Add Device** from the menu. The [Add Device window](#) opens.
2. Enter an **IP Address**.
3. Use the **Profile** drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.
4. Select the checkbox and enter an [SNMP context](#), if desired.
5. Select whether to use the default [nickname](#) or click **Specify** to assign a unique nickname to this device.
6. Click **OK**. The new device appears in the group and is automatically added to the All Devices group.

### *Using the Device Group Selection Window*

Use the Device Group Selection window to add one or more devices from a right-panel Details View to the My Network group or a user-created group in the left-panel tree.

1. In a right-panel Details View tab, right-click the device(s) that you want to add to a group and select **Add Device(s) to Group** from the menu. The [Device Group Selection window](#) opens.
2. Select the My Network group or the desired user-created group.
3. Click **OK**. The selected device(s) appear in the group.

---

**TIP:** You can also add one or more devices from a right-panel Details View to the My Network group or a user-created group by using the copy and paste toolbar buttons or right-click menu options.

---

### *Dragging and Dropping Devices*

In the left-panel tree, you can add a device to a group by dragging a device from one group and dropping into another. You can also drag and drop an entire device group to create a sub-group in the target group. You can only drag devices to the My Network group or a user-created group.

---

**TIP:** You can also use the copy and paste toolbar buttons or right-click menu options to add a device to a group in the left-panel tree.

---

#### To add a device using drag and drop:

1. In the left panel, expand the hierarchy to show the target group and the device that you want to add.
2. Select the device to be dragged and dropped.
3. Click and hold on the selected device and drag it into the target group.

#### To add a group using drag and drop:

1. In the left panel, expand the hierarchy to show the target group and the group that you want to add.
2. Click and hold on the group and drag it into the target group. The group is added as a sub-group, containing all of the devices that were members of the original group.

## Removing Devices from a Device Group

This function simply removes a device or devices from a device group. It should not be confused with *deleting* a device (right-clicking the device and selecting



**Delete** from the menu), which removes the device from the device group, the All Devices folder, and from the NetSight database.

1. In the left-panel Network Elements tab, expand the device group from which you wish to remove a device.
2. Right-click a single device and select **Remove from Device Group** from the menu.

## Renaming a Device Group

This function allows you to rename a device group. You cannot rename the [system-created device groups](#).

1. In the left-panel Network Elements tab, right-click the device group you wish to rename, and select **Rename Device Group**.
2. Type the device group name in the highlighted box and press **Enter**. (A device group cannot have the same name as another device group at the same level.)

## Deleting a Device Group

This function removes a device group and its devices. Only the group is deleted; the devices remain in the All Devices folder and the NetSight database. You cannot delete the [system-created device groups](#).

1. In the left-panel Network Elements tab, select the device group you wish to delete, and select **Edit > Delete**. You can also right-click the device group and select **Delete** from the menu.
2. A confirmation message appears. Click **Yes**.

---

### Related Information

For information on related tasks:




- [How to Add and Delete Devices](#)

## How to Archive

---

You can archive (save) device configuration data and/or capacity planning data using the Archive Wizard. Archiving device configuration data lets you create archives (backup copies) of your network devices' configurations that can be restored to the devices at a later date, if needed. Archiving capacity planning data lets you store port and FRU information for use by the [Capacity Planning](#) tool to generate reports. You can create an archive that saves both configuration data and capacity planning data, or you can create an archive that targets one type of data or the other.

You can perform archives on a single device, multiple devices, or on an entire device group. Because it is useful to archive data on a regular basis, Inventory Manager lets you schedule archives to be performed at a future time, and/or on a routine basis. Once you have configured an archive's parameters, you can use that archive on a repeated basis to save new versions of the desired data. For example, you may want to create an archive that saves your device configurations on a weekly basis, and also create an archive that saves only capacity planning information on a daily basis to monitor what is changing on the network.

Once an archive operation has been created, it is listed by name in the left-panel [Archive Mgmt tab](#) under the Archives folder. Below the archive name are the archive versions, displayed by the date and time the version was performed. Under the versions are the individual configurations, listed by IP address of the device whose data was saved. Each configuration displays an icon that identifies the type of data being saved:  device configuration data,  capacity planning data,  both device configuration and capacity planning data.

---

**NOTE:** If the device is an X-Pedition router, be aware that when archiving device configuration data, the router's Startup configuration file is saved.

---

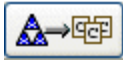
Instructions on:

- [Using the Archive Wizard](#)
- [Saving a New Archive Version](#)
- [Editing an Archive](#)
- [Renaming an Archive](#)
- [Deleting an Archive](#)

## Using the Archive Wizard

Use the Archive Wizard to archive network configuration data and/or capacity planning data. You can perform archives on a single device, multiple devices, or on an entire device group. You must have a TFTP or FTP server running to save a configuration. For more information, see [TFTP Server Setup](#) or [FTP Server Setup](#).

1. Select **Tools > Wizards > Archive Wizard** from the menu bar or click



on the toolbar. The Archive Wizard opens.

2. Enter a name and (optional) description of the archive operation.
3. **Configure the archive setup:**
  - a. Select the appropriate checkbox for the type of data you wish to archive:
    - **Archive Configuration Data** - Create archives (backup copies) of your devices' configurations that can be restored to the devices at a later date, if needed.
    - **Archive Capacity Planning data** - Create archives of port and FRU information to be used by the [Capacity Planning](#) tool to generate reports.
  - b. Specify the maximum number of versions you would like saved for this archive. This allows you to limit the number of versions saved for each archive. Once the maximum number is reached, older versions are automatically deleted.
  - c. Click **Next**.
4. **Select the Archive Members:**
  - a. Expand the folders under Select Devices and select the single device, multiple devices (using the Control or Shift keys) or a single device group. Click **Add**.

---

**NOTE:** If you select multiple tree nodes representing the same device but with varying SNMP contexts, an archive save will be performed for each context. However, the context must provide access to the MIBs required for the archive save operation or the archive for that context will fail. It is recommended that you perform the archive operation on the device with the default context (switch mode.)

---

- b. The devices will be listed under Archive Members. If you want to

remove a member from the list, select the member and click **Remove**.

c. Click **Next**.

---

**TIP:** If you open the Archive Wizard from a selected device or device group in the left-panel **Network Elements** tab, the selected item will be automatically displayed under **Archive Members**.

---

5. **Select devices to be archived.** Use the checkboxes in the **Devices** table to select or deselect devices to be archived. For example, if you selected a device group in the previous window, you can use these checkboxes to deselect individual devices in that group.
6. **Configure scheduling information for the archive:**
  - a. Use the drop-down list to select the frequency with which you want the archive performed: **Never**, **Now**, **Once**, **Daily**, **Weekly**, or **On Server Startup**. The **Never** option lets you create an archive operation without actually performing it. The **Now** option lets you perform an immediate archive.
  - b. Use the drop-down list to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. (This field is grayed out if you have selected the **Never** or **Now** frequency.)
  - c. Set the starting time for the operation and select **AM** or **PM**. (This field is grayed out if you have selected the **Never** or **Now** frequency.)
7. **Configure Process settings for the archive:**
  - a. The archive will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Set the value to **1** to have the operation performed serially, one device after another.
  - b. Select the **Abort on Failure** checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.
8. Click **Finish** to create the archive. The archive will be listed by name in the left-panel [Archive Mgmt tab](#) under the **Archives** folder, and performed according to its scheduled parameters. You can change the archive's parameters; see [Editing an Archive](#) for instructions.

---

**TIP:** You can set up an e-mail notification based on the event log message that is generated when a configuration change is detected. When the current archive differs from the previously saved archive, Inventory Manager generates an event log message. Using the NetSight Console Alarms Manager you can create an alarm that monitors the Inventory Log for the text "Configurations Are Different" and define an e-mail to be executed as the specific alarm action.

---

## Saving a New Archive Version

Once you have created an archive, you can use that archive on a repeated basis to save (stamp) new versions of the desired configurations.

1. With an archive folder selected in the left-panel Archive Mgmt tab, right-click and select **Stamp New Version** from the menu.
2. A new archive version, displayed by the date and time the version was performed, will be listed under the archive folder. Under the version are the individual configurations, listed by IP address of the device whose data was saved.

## Editing an Archive

Once you have created an archive, you can edit the archive parameters, including changing the devices the archive is performed on.

1. With an archive folder selected in the left-panel Archive Mgmt tab, select the right-panel [General tab](#).
2. Edit the archive description and number of versions to save, if desired.
3. Click the **Edit Devices** button and change the devices to be archived. Use the **Add** and **Remove** buttons to select your Archive Members. Expand the folders under Select Devices and select the single device, multiple devices (using the Control or Shift keys) or a single device group. Click **OK**.
4. Use the checkboxes in the Devices table to select or deselect devices to be archived.
5. Edit the schedule information for the archive using the instructions in [step 6](#) above.
6. Edit the Process settings for the archive using the instructions in [step 7](#) above.
7. Click **Save**. The next time the archive is performed, these new parameters will be used.

## Renaming an Archive

You can rename an archive.

1. With an archive folder selected in the left-panel Archive Mgmt tab, right-click and select **Rename** from the menu. The Rename Archive window opens.
2. Enter the new name, and click **OK**.
3. The name of the archive will change in the left-panel tree. All previous versions saved under the old name will be available under the new name. The next time the archive is performed, the new name will be used.

## Deleting an Archive

You can delete an archive, an archive version, or a saved configuration from the Archive Mgmt tree.

1. With an archive, archive version, or configuration selected in the left-panel Archive Mgmt tab, right-click and select **Delete** from the menu.
  2. A Delete confirmation window opens. Click **Yes** to perform the delete.
- 

### Related Information

For information on related tasks:

- [Archive Wizard](#)
- [How to Restore an Archive](#)
- [How to Compare Archives](#)

## How to Assign Firmware

---

The [Assign Firmware window](#) allows you to assign a firmware or boot PROM image to one or more product families or device types. This enables you to download the assigned image to any of your network devices of that family or type, using the Firmware Upgrade Wizard or the Boot PROM Upgrade Wizard.

The Firmware Mgmt tab displays firmware and boot PROM images grouped according to product family and device type. Inventory Manager provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a [firmware discovery](#) or refresh. The Unknown folder contains images that Inventory Manager could not correlate to a device type. Use the Assign Firmware window to assign those images to the correct device type(s).

---

**TIP:** To quickly assign multiple firmware images to a single product family or device type, select the images in a right-panel Details View and drag them into the appropriate left-panel folder.

---

1. Select a firmware or boot PROM image in the left-panel Firmware Mgmt tab (or one or more images in the right-panel Details View tab), then select **Tools > Assign Firmware**. You can also right-click on an image, and select Assign Firmware from the menu. The [Assign Firmware window](#) opens.
  2. In the Device Type list, select the families and/or individual device types where you want to assign the image(s). You can select multiple product families or device types using the **Ctrl** or **Shift** keys.
  3. Click **OK** to assign the image to the selected product families and/or device types and close the window. Click **Apply** to assign the image and leave the window open.
- 

### Related Information

For information on related tasks:

- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)


For information on related windows:

- [Assign Firmware Window](#)



## How to Compare Archives

---

Inventory Manager lets you compare two different archives for the same device and monitor any changes in device attributes. Inventory Manager compares archives using a set group of attributes that were saved when the archive was performed. The values for these attributes are displayed in a table with any differences between the values flagged by a yellow Diff icon . Use the [Select Archive Versions to Compare window](#) to select the configurations you want to compare, and the [Compare Archives window](#) to view the comparison results.


1. Access the Select Archive to Compare window from the Archive Mgmt tab or Network Elements tab:
  - **Archive Mgmt tab** -- select an archive, version, or configuration in the left-panel tab or right-panel Details View and select Tools > Compare Archives from the menu bar (or use the right-click menu option).
  - **Network Elements tab** -- with a device or device group selected in the left-panel tab, select an archive version in the right-panel Archives tab and select Tools > Compare Archives from the menu bar (or use the right-click menu option).

The Select Archive Versions to Compare window opens.


---

**TIP:** If you select **two** archive versions in the right-panel Archives tab or Details View tab and select Tools > Compare Archives, the Compare Archives window opens directly, bypassing the Select Archive Versions to Compare window. In this case, you can skip step 2 and proceed to step 3.

---

2. The Select Archive Versions to Compare window displays two Archive trees (identical to the Archive tree in your Archive Mgmt tab). Expand the folders as necessary to select the two archive versions or configurations you wish to compare. You can compare two individual configurations for the same device, or you can compare two different archive versions (although the versions should share common devices). Click the **Compare** button.
3. The Compare Archives window opens to display the results of the comparison. The smaller Summary table at the top of the window displays each device included in the comparison. Any differences between the two versions will be flagged by a yellow Diff icon . If there are many devices being compared, a progress bar will indicate the progress of the operation.

You can stop the compare operation by pressing the **Abort Compare** button.

4. Once the compare operation is complete, select the device in the Summary table whose comparison results you wish to see. The results are displayed in the Comparison Results table.
5. To select two new archive versions or configuration files to compare, click the **Change** button to return to the Select Archive to Compare window. Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

In addition, the following right-click menu options are available only for archives that include device configuration data:

- **View Configuration File** -- Opens the [Configuration File Viewer](#) and displays the archived config file of the selected device. This option is only available when there are no differences between the two config files being compared.
  - **Compare Configuration Files** -- Opens the [Compare Configuration Files window](#) and displays the two archived config files for the selected device. This option is only available when there are differences between the two config files being compared.
- 

## Related Information

For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)

For information on related windows:

- [Compare Archives Window](#)

# How to View and Compare Configuration Files

---



Inventory Manager lets you view a single archived device configuration file, or compare two configuration files and see any differences between the files.

Instructions on:

- [Viewing a Configuration File](#)
- [Comparing Configuration Files](#)



## Viewing a Configuration File


Use the [Configuration File Viewer](#) to view a single archived device configuration file.

1. In the Archive Mgmt tab tree or right-panel Details View, select a configuration that includes device configuration data (  or  ) and then select **Tools > View Configuration File**. You can also right-click on a configuration and select View Configuration File from the menu. If the configuration file status is "File Not Found/Missing" (see the configuration's General tab), then this menu option is not available.
2. The file is displayed in the viewer in ASCII format. However, if the file is in binary, you still have the option to view it.
3. Use the Find and Filter tabs to target specific lines of interest. For more information on the find and filter functions, see [Find tab](#) or [Filter tab](#).
4. Use the Change button to open the [Open Configuration window](#) where you can select another configuration to view.

## Comparing Configuration Files

Use the [Compare Configuration Files window](#) to view and compare two archived device configuration files.

1. There are several ways to access the window:
  - In the Archive Mgmt tab tree or right-panel Details View, select a configuration that includes device configuration data (  or  ) and then select **Tools > Compare Configuration Files**. You can also right-click on a configuration and select Compare Configuration Files from

- the menu. The [Select Configurations window](#) opens, where you can select the two configurations you want to compare. Click **OK**.
- In the Archive Mgmt tab Details View, select two configurations and then select **Tools > Compare Configuration Files**.
  - In the Compare Archives window, right-click on an entry with a Diff icon , and select Compare Configuration Files from the menu.
2. The configurations are displayed in the Configuration File Compare window in ASCII format. However, if one or both of the configurations are in binary, you have the option to display them. Lines highlighted in green represent lines that have changed. Red highlighting represents lines that have been added.
  3. Use the Find and Filter tabs to target specific lines of interest. For more information on the find and filter functions, see [Find tab](#) or [Filter tab](#).
  4. Use the Change button to open the [Select Configurations window](#) where you can select two new configurations to compare.
- 

### Related Information

For information on related windows:

- [Configuration File Viewer](#)
- [Compare Configuration Files Window](#)
- [Compare Archives Window](#)

# How to Create and Download Configuration Templates

---

Creating a configuration template provides a way to download similar configurations to one or more devices. Use the [Edit Configuration Template window](#) to create a configuration template based on an existing archived device configuration file. The window displays a selected configuration, and allows you to replace portions of it with template variables. Then, you must set device-specific values for your template variables. When you download the template configuration to a device, the variables are replaced with appropriate values for that device.

---



**NOTE:** Configuration templates can be created from text-based (ASCII format) configurations files. Although you can open binary configuration files in the Edit Configuration Template window, you should **not** use binary configuration files to create templates.

---

Instructions on:

- [Creating a Configuration Template](#)
- [Editing a Configuration Template](#)
- [Setting Values for Template Variables](#)
  - [On a Single Device](#)
  - [On Multiple Devices](#)
- [Assigning Templates to Device Types](#)
- [Using the Template Download Wizard](#)

## Creating a Configuration Template

1. In the left-panel Archive Mgmt tab, select a configuration that includes device configuration data (  or  ) and then select **Tools > Create Configuration Template**. (You can also right-click a configuration and select Create Configuration Template from the menu.) The [Edit Configuration Template window](#) opens.
2. When the window opens, all instances of the IP address of the device the configuration was saved from, are automatically replaced with the

%ManagedIP% variable. You can use the Undo Replace button to undo this auto-replacement if desired.

3. In the Find field, enter text you would like to replace with a variable.
4. In the Replace With field, enter the variable that will replace the highlighted (found) text, or use the drop-down list to select a defined variable. To populate the drop-down list, click the **Variables** button to open the [Template Variables window](#) where you can add and delete variables to display in the variable drop-down list.
5. Select the **Replace all occurrences of selected text** checkbox if you would like to replace all instances of the selected text versus replacing one instance at a time.
6. Click **Find** to search for the next instance of the text specified in the Find field. The found text is highlighted in the window.
7. Click **Replace** to replace highlighted (found) text with the specified variable. If the "Replace all occurrences of selected text" checkbox is selected, all instances of the text specified in the Find field will be replaced. Click **Undo Replace** to undo the last replacement, if desired.
8. You can also edit the file by highlighting and replacing or deleting any text directly in the file.
9. When the configuration template has been edited as desired, click the **Save As** button to open the Save Template window where you can name and save the configuration template. Saved templates are listed under the All Templates folder in the left-panel Configuration Templates tab. Once a template has been saved, the name of the template appears in the title bar of this window, and the path to where the saved template is stored is displayed above the configuration template text.

### Editing a Configuration Template

1. In the left-panel Configuration Templates tab, expand the All Templates folder and select the desired configuration template.
2. In the right-panel General tab, click the **Edit Template** button. The [Edit Configuration Template window](#) opens where you can edit the template using the instructions in the section above, starting with [step 3](#).

## Setting Values for Template Variables

Variables are used in configuration templates to substitute for device-specific information. When you download a template configuration to a device, the variables are automatically replaced with assigned values for that device. You can set variable values for a single device or multiple devices.

### *On a Single Device*

You can set variable values for a single device in the [Device Configuration Template tab](#).

1. Select a device in the left-panel Network Elements tab.
2. In the right-panel Configuration Template tab, select the desired variable in the All Available Template Variables list.
3. Click **Set Variable**. The Set Template Variable window opens. Enter a value for the variable and click **OK**. The value will be added to the list.
4. Use these steps to set values for all the variables. When a configuration template is downloaded to the device, these values will be used to replace the variables in the template.

### *On Multiple Devices*

You can set variable values for multiple devices in the [Set Template Variables window](#).

1. Select any device or device group in the left-panel Network Elements and then select **Tools > Set Template Variable Values**. The Set Template Variable window opens.
2. Use the View Template Variables drop-down list to select which variables are displayed in the table. You can select a single variable whose value you want to set, or use the "View All Variables" option to display all variables.
3. The table lists your selected devices and their set values for each of the template variables.
4. Select one or more devices (rows) in the table and click **Edit**. The Table Editor row appears at the bottom of the table. Select or tab to the desired column (variable) and enter your value.
5. Click **Apply** to set the values for all the selected devices. Use the **Undo** button to undo the last edit operation you applied.

6. When you close the window, you will be prompted to save or cancel the variable values you have set.

## Assigning Templates to Device Types

Configuration templates are grouped according to device type in the left-panel Configuration Templates tab. Inventory Manager automatically assigns a template to the appropriate device type when you save the template in the [Edit Configuration Template window](#). The Unknown folder contains templates that Inventory Manager could not correlate to a device type. Use the [Assign Configuration Template window](#) to assign those templates to the correct device type(s).

1. In the left-panel Configuration Templates tab, select a template that needs to be assigned, then select **Tools > Assign Configuration Template**. You can also right-click a template, and select Assign Configuration Template from the menu. The Assign Configuration Template window opens.
2. Expand the Device Type tree and select the device type(s) to which you want to assign the template. You can select multiple device types using the **Ctrl** or **Shift** keys.
3. Click **OK**.

## Using the Template Download Wizard

After you have created your configuration templates, you can use the [Template Download Wizard](#) to download a template to one or more devices.

1. Select **Tools > Wizards > Template Download Wizard** from the menu bar. The Template Download Wizard opens.
2. **Select the template to download:**
  - a. Expand the folders under the Templates tree and select the template you want to download. General information about the selected template will be displayed in the right panel.
  - b. Click **Next**.

---

**TIP:** If you open the Template Download Wizard from a template in the left-panel Configuration Templates tab, that template will be automatically selected in the Templates tree.


---



3. **Select devices for download:**

- a. Expand the folders under the left-panel tree and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys). Only devices that are compatible with this template are displayed; this can be overridden by selecting the **Show All Devices** checkbox. Click **Add**. If you want to remove a device from the list, select the device and click **Remove**.
- b. Click **Next**.


4. **Initiate the Download operation:**

- a. The top of the window displays a table of the devices you have selected for your download operation. An alert icon  will appear for any device that does not have values assigned for all the variables in the template. Click **Set Template Variables** to open the [Set Template Variables window](#) which lists all your devices and their set values for each of your defined template variables. Use this window to set variable values for one or more devices. You can also right-click on a table row and select Edit Device Variables to open the [Device Template Variables window](#), where you can assign variable values for that specific device.
- b. Specify the **Download Type** option. The download will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. By default, the downloads will occur in sequential order (Groups of: 1). This is to protect against possible isolation of other devices that are in the download list.

---

**CAUTION:** Because many devices automatically reset following a download operation, performing a Download Type greater than 1 may isolate other devices in the download list, causing their downloads to fail. It is recommended that you leave the **Groups of** value at 1 (perform the downloads serially), unless you know it is safe to have the selected network devices reset simultaneously.

---

- c. Click **Start** to initiate the download operation. The table at the top of the window will update with status information, as will the status area in the bottom left of the window.
- d. Review results. An alert icon  will appear in the Alert column of the table if a download operation fails for the specific device. You can select to show all devices or show only those that are incomplete or have failed.

5. Click **Finish** to close the wizard.

## Related Information

For information on related windows:

- [Edit Configuration Template Window](#)
- [Assign Configuration Template Window](#)
- [Set Template Variables Window](#)
- [Template Download Wizard](#)

## How to Initialize Inventory Database Components

---

Inventory Manager provides a way for you to initialize the Inventory Manager components in the NetSight Database. The initialize operation removes **all** Inventory Manager data elements from the database including:

- Archive operations, archive versions, and saved configurations.
- Schedules for Inventory Manager operations.
- Capacity Planning saved reports.
- Firmware references.
- Configuration templates.

Using this operation instead of the Restore Initial Database function (accessed in the Server Information window) allows you to initialize your Inventory components while retaining your NetSight Console and Automated Security Manager data elements in the database.

---

**NOTE:** As a precaution, it is recommended that you make a backup of your NetSight Database prior to performing the initialize operation using the Backup Database window accessed from the Server Information window.

---

You must be assigned the appropriate user capability to perform the initialize operation. This operation will cause all current client connections and operations in progress to be terminated. You must restart both the NetSight Server and the Inventory Manager client following an initialize database operation.

1. Make a backup of your database using the Backup Database window accessed from Database tab in the Server Information window (Tools > Server Information.)
2. Select **File > Database > Initialize Inventory Component** to begin the initialize operation. You will see a Warning message asking if you want to remove all Inventory Manager data in the server's database. Click **OK**.
3. When the initialize is complete, restart the NetSight Server and Inventory Manager client.

## How to Push Local Firmware to the Server

---

The [Push Local Firmware to Server window](#) gives a remote client the ability to send a local firmware or boot PROM image to the NetSight Server. This allows a remote client to download a firmware image from the download library website, and then push the firmware to the server where it can be used in Inventory Manager operations such as firmware and boot PROM upgrades.

1. Select **Tools > Push Local Firmware to Server**. The Select Local Firmware File window opens where you can navigate to the file you want to send. Select the file and click **Open**. The Push Local Firmware to Server window opens.
  2. In the window, you can view the path to the local file you have selected to send, and the following information:
    - Server - The name of the server the client is connected to.
    - Server Path - The path to the server's TFTP or FTP firmware directory, depending on what option you have selected. You can extend the path to a different folder in the directory, if desired.
    - File Name - The name of the firmware or boot PROM file being pushed to the server.
  3. Select the **TFTP or FTP Firmware Directory** option depending on whether you want to store the firmware in the FTP or TFTP firmware directory on the server.
  4. Select the **Refresh Firmware** checkbox if you want to perform a firmware discovery following the operation, and update the firmware listed in your Firmware Mgmt tab.
  5. Click **Send** to send the image to the server.
- 

### Related Information

For information on related tasks:

- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

For information on related windows:


- [Push Local Firmware to Server Window](#)

## How to Reset a Device

---

Use the [Reset Device Wizard](#) to reset a single device, multiple devices, or even multiple device groups. The wizard lets you reset devices that support Timed Reset as well as those devices that do not. Timed Reset lets you configure your reset operation with a time delay, so that the actual device resets take place at a later time.

Use these steps to reset a device.

1. Select **Tools > Wizards > Reset Wizard** from the menu bar or click  on the toolbar. The Reset Device Wizard opens.
2. **Select the devices to reset:**
  - a. Expand the folders under the left-panel tree and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys). Click **Add**.

---

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).

---

- b. The devices will be listed in the Selected Devices table. Devices that do not support the reset operation or have never been contacted, are not listed. If you want to remove a device from the list, select the device and click **Remove**.
    - c. Click **Next**.

---

**TIP:** If you open the Reset Device Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed under Selected Devices.

---

3. **Reset devices that support Timed Reset:**

If you are resetting devices that support Timed Reset, you will see a window listing those devices. Timed Reset gives you the flexibility to set up your reset operation with a time delay, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.

- a. In the **Selected column**, select the devices that you want to reset. You can select an option to display devices that do not support timed reset; however, these devices cannot be reset from this window.
  - b. In the **Reset Time** field, click the **Select** button to open the Select Reset Time window where you can schedule a date and time for the reset. Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. Set the starting time for the operation and select AM or PM.
  - c. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
  - d. Click **Start** to initiate the timed resets. Resets occur simultaneously. Once the reset operation has started, you must click **Refresh** to update the device information in the table.
4. **Reset devices that do not support Timed Reset:**  
If you are resetting devices that do not support Timed Reset, you will see a window listing those devices.
- a. In the **Selected column**, select the devices that you want to reset.
  - b. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
  - c. Click **Start** to initiate the resets. Resets occur one at a time, continuing only after a device is fully booted.
  - d. After the reset operation is completed, you can click **Refresh** to update the device information in the table.
5. Click **Finish** to close the wizard.
- 






## Related Information

For information on related tasks:

- [How to Upgrade Firmware](#)
- [How to Upgrade Boot PROM](#)
- [Reset Device Wizard](#)

## How to Restore an Archive

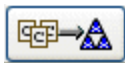
---

You can restore saved (archived) device configuration files to devices using the [Restore Wizard](#). Saved configurations are listed in the left-panel [Archive Mgmt tab](#) under the appropriate archive and version. Each configuration displays an icon that identifies the type of data that was saved:  device configuration data,  capacity planning data,  both device configuration and capacity planning data. Only configurations that include device configuration data (  and  ) are available to be restored.



A configuration can only be restored to a device with the same IP address. In other words, the device you are restoring *to* must have the same IP address as the device the configuration was originally saved *from*. You can restore configurations to a single device or multiple devices. You must have a TFTP or FTP server running to restore a configuration. For more information, see [TFTP Server Setup](#) or [FTP Server Setup](#).

Use these steps to restore a configuration to a device.

1. Select **Tools > Wizards > Restore Wizard** from the menu bar or click



on the toolbar. The Restore Wizard opens.

2. **Select the archive version to restore:**
  - a. Expand the folders under the Archives tree and select the archive version or configuration you want to restore. Only configurations that include device configuration data (  and  ) are available to be restored. Click **Add**.
  - b. The configurations are listed in the Configurations to Restore table. If you have selected an archive version and you want to remove an individual configuration from the list, select the configuration and click **Remove**.
  - c. Click **Next**.

**TIPS:** -- If you open the Restore Wizard from an archive version or configuration in the left-panel Archives Mgmt tab, the selected configuration(s) will be automatically displayed under Configurations to Restore.  
-- Check the FW Match column to see if the current firmware version on the device matches the firmware version that was on the device at the time of the archive.



### 3. Initiate the Restore operation:

- a. Specify the **Restore Type** option. The restore will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. By default, the restores will occur in sequential order (Groups of: 1). This is to protect against possible isolation of other devices that are in the restore list.

---

**CAUTION:** Because some devices automatically reset following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. It is recommended that you leave the **Groups of** value at 1 (perform the restore serially), unless you know it is safe to have the selected network devices reset simultaneously.

---

- b. Click **Start** to initiate the restore operation. The table at the top of the window will update with status information, as will the status area in the bottom left of the screen. Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.
- c. Review results. An alert icon  will appear in the Alert column of the table if a restore operation fails for a specific device. You can select to show all devices or show only those that are incomplete or have failed.

4. Click **Finish** to close the wizard.
- 

## Related Information

For information on related tasks:

- [Restore Wizard](#)
- [How to Archive](#)
- [How to Reset a Device](#)



## How to Set a File Transfer Method

---

You can select a file transfer method for a specific device, or specify a default transfer method for an entire device type or device type family using the [File Transfer Method window](#). Once you have specified the file transfer method for a device, all archive save and restore operations and Firmware/Boot PROM upgrades on that device will be performed using the specified method. All devices are initially configured with TFTP as their file transfer method, until specified otherwise using these windows. Be sure to configure file transfer properties in the [TFTP Transfer Settings](#), [FTP Transfer Settings](#), or [SCP Transfer Settings](#) views in the Options window.

Instructions on setting the:

- [File Transfer Method for a Device](#)
- [Default File Transfer Method for a Device Type](#)

### Setting the File Transfer Method for a Device

You can specify the file transfer method for a single device or multiple devices. Specifying a file transfer method at the device level overrides any default setting made at the [device type](#) level.

1. Select a single device in the left-panel Network Elements tab or multiple devices in a right-panel Details View tab, then select **Tools > File Transfer Method** from the menu bar. You can also right-click a device and select the File Transfer Method option from the menu. The [File Transfer Method window](#) opens.
2. Use the drop-down list to select the file transfer method you would like used for the selected device(s). The default file transfer method set for the device's device type is indicated by the word default in parentheses.
3. Click **OK**.

### Setting the Default File Transfer Method for a Device Type Family

You can specify a default file transfer method for an entire device type or device type family. You can override the device type setting at the [device level](#).

1. Select a device family folder (highest-level device type folder) or a device type folder in the left-panel Firmware Management tab, then select **Tools > Default File Transfer Method** from the menu bar. You can also right-click a device type or family folder and select the Default File Transfer Method option from the menu. The [File Transfer Method window](#) opens.
  2. Use the drop-down list to select the file transfer method you would like used for the selected device type or family.
  3. Select the **Apply method to all devices of this device type** checkbox to change the file transfer method for all current devices in the selected device type or family folder. If this checkbox is **not** selected, only newly discovered devices of this device type or family will have this file transfer method.
  4. Click **OK**.
- 



## Related Information

For information on related windows:

- [File Transfer Method Window](#)
- [General Tab \(Device Type\)](#)
- [FTP Transfer Settings View Options Window](#)
- [TFTP Transfer Settings View Options Window](#)
- [SCP Transfer Settings View Options Window](#)

## How to Set a Reference Image

---

A firmware or boot PROM reference is the image you designate as the preferred image for a specific binary family of devices (devices that share the same firmware image). Firmware images that have been set as a reference image display a  firmware reference icon in the Firmware Mgmt tab. Boot PROM images that have been set as a reference image display a  boot PROM reference icon in the Firmware Mgmt tab. There can only be one reference image per family.

1. Select a firmware or boot PROM image in the left-panel Firmware Mgmt tab or a right-panel Details View.
2. Select **Tools > Set as Reference Image** or right-click on the image and select **Set as Reference Image** from the menu. If the Set as Reference Image option is not available, make sure that the selected image has been assigned to appropriate device types.

The image will be set as a reference for all device types with which it is compatible.

---

### Related Information

For information on related tasks:

- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

## How to Set Inventory Manager Options

---

Use the Options window (**Tools > Options**) to set options for the Inventory Manager application. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Inventory Manager folder in the tree to view all the different options you can set.

Instructions on setting the following Inventory Manager options:

- [Alternate Firmware Servers](#)
- [Data Storage Directory Path](#)
- [FTP Transfer Settings](#)
- [TFTP Transfer Settings](#)
- [SCP Transfer Settings](#)

### Configuring Alternate Firmware Servers

Use the [Alternate Firmware Servers view](#) to configure alternate firmware download servers. Alternate servers allow you to perform remote firmware downloads without having to reconfigure the default NetSight TFTP server settings. By performing firmware downloads via a remote server, you can avoid transferring traffic over a WAN. Alternate servers can be configured to use either the TFTP, FTP, or SCP protocol. These settings apply to all users. You must be assigned the appropriate user capability to add alternate firmware servers.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Inventory Manager folder and select Alternate Firmware Servers. The right-panel Alternate Firmware Servers view displays a list of any configured alternate servers.
3. Click **Add Server** to open the [Add Alternate Firmware Server window](#) where you can configure a new alternate server:
  - a. Enter the IP address of the workstation where the server is running.
  - b. Enter an Identifier -- a description that helps you identify the alternate server.
  - c. Enter the server root path. The root directory is the base directory to which the server is allowed access. The server will be allowed to create files to or read files from this directory and any of its subdirectories.

Keep in mind the following requirements when setting the server root path:

- If your server is configured with a root directory, it must match the root directory entered here.
  - If your server is **not** configured with a root directory, specify the root directory here as the root of the drive (e.g. C:\ or D:\).
- d. Specify the transfer protocol for the alternate server.
  - e. The required connection information changes depending on your selected transfer protocol.
    - For TFTP, specify the port number your TFTP server is configured to run on.
    - For FTP or SCP, specify the port number your server is configured to run on. Select the Anonymous checkbox if your server is configured to accept Anonymous logins; Inventory Manager will automatically fill in the username and password fields. Otherwise, enter your username and password to access the server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.
  4. To edit an alternate server, select a server in the list and click **Edit Server**. The [Edit Alternate Firmware Server window](#) opens where you can edit certain server properties.
  5. To remove a server, select a server and click **Remove Server**.
  6. After you have configured your alternate servers, use the [Create Firmware Record window](#) to create new firmware entries and associate them with the alternate servers. Then, use the [Set Firmware Server window](#) to specify an alternate firmware download server to be used by a device group or by individual devices.

## Setting the Data Storage Directory Path

Use the [Data Storage Directory Path view](#) to specify a different directory where Inventory Manager data will be stored. This data includes capacity planning reports, configuration templates, archived configurations, and property files. If you specify a new data directory, you will need to move the data files stored under the old directory to the new directory so that Inventory Manager can find them.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Inventory Manager folder and select Data Storage Directory Path.
3. Enter the path to the base directory where you want to store Inventory Manager data.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Setting FTP Transfer Settings

Use the [FTP Transfer Settings view](#) to set FTP server properties and login information. Specify the FTP server IP address, set paths to the root and firmware directories, and set login information. The FTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select FTP Transfer Settings. The right-panel FTP Transfer Settings view is displayed.
3. Select the **Use the NetSight Server's IP** checkbox, or use the **FTP Server IP** field to enter the IP address of the device where the FTP server resides.
4. Enter the port number your FTP server is configured to run on.
5. Specify the **Root Directory Path**. The root directory is the base directory to which the FTP server is allowed access. The FTP server will be allowed to create files to or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory that Inventory Manager automatically creates when it is installed. If you would like to use an alternate root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your FTP server is configured with a FTP root directory, it must match the root directory entered here.
- If your FTP server is **not** configured with a FTP root directory, change the FTP root directory here to the root of the drive (e.g. C:\ or D:\).
- **If you are using an FTP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using  
h:\ (where h:\ is mapped to the tftpboot directory on the remote drive)  
use  
\\yourservername\tftpboot\

- 
6. Specify the **Firmware Directory Path**. The default firmware directory is tftpboot\firmware\images. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an FTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
  7. Specify your FTP Server login information. Select the **Anonymous** checkbox if your FTP server is configured to accept Anonymous logins. (Inventory Manager will automatically fill in the username and password fields.) Otherwise, enter your username and password to access the FTP server. For increased security, select the **Hide Password** checkbox and your password will be replaced with asterisks when it is typed in.
  8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Setting TFTP Transfer Settings

Use the [TFTP Transfer Settings view](#) to set TFTP server properties. This view displays the TFTP server IP address and root directory path specified in the

Services for NetSight Server Options view (Suite-Wide options) and lets you set the firmware directory path. These settings apply to all users.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select TFTP Transfer Settings. The right-panel TFTP Transfer Settings view is displayed.
3. Specify the **Firmware Directory Path**. The default firmware directory is `tftpboot\firmware\images`. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).)

---

**NOTE: If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the firmware directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

`h:\` (where `h:\` is mapped to the firmware directory on the remote drive) use

`\\yourservername\tftpboot\firmware\images\`

---

4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Setting SCP Transfer Settings

Use the [SCP Transfer Settings view](#) to set SCP server properties and login information. Specify the SCP server IP address, set paths to the root and firmware directories, and set login information. The SCP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Inventory Manager folder and the File Transfer Settings folder, and select SCP Transfer Settings. The right-panel SCP Transfer Settings view is displayed.



3. Select the **Use the NetSight Server's IP** checkbox, or use the **SCP Server IP** field to enter the IP address of the device where the SCP server resides.
  4. Enter the port number your SCP server is configured to run on.
  5. Specify the **Root Directory Path**. The root directory is the base directory to which the SCP server is allowed access. The SCP server will be allowed to create files to or read files from this directory and any of its subdirectories. The default root directory on Windows is the C:\ directory and on Linux it is the /root/ directory. If you would like to use an alternate root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.
- 

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your SCP server is configured with an SCP root directory, it must match the root directory entered here.
  - If your SCP server is **not** configured with an SCP root directory, change the SCP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
  - **If you are using an SCP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using  
h:\ (where h:\ is mapped to the firmware\images directory on the remote drive)  
use  
`\\yoursystemname\firmware\images`
- 

6. Specify the **Firmware Directory Path**. The default firmware directory is C:\firmware\images on Windows and /root/firmware/images on Linux. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an SCP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.
7. Specify your SCP Server login information. Select the **Anonymous** checkbox if your SCP server is configured to accept Anonymous logins. (Inventory Manager will automatically fill in the username and password

fields.) Otherwise, enter your username and password to access the SCP server. For increased security, select the **Hide Password** checkbox and your password will be replaced with asterisks when it is typed in.

8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.
- 

## Related Information

For information on related tasks:

- [FTP Server Setup](#)
- [TFTP Server Setup](#)
- [SCP Server Setup](#)

For information on related windows:

- [Options Window, Inventory Manager Options](#)

# How to Set Up Alternate Firmware Download Servers

---

Alternate firmware download servers allow you to perform remote firmware downloads without having to reconfigure your default local file transfer servers. By performing firmware downloads via a remote server, you can avoid transferring traffic over a WAN. Alternate servers can be configured to use either the TFTP, FTP, or SCP protocol.

After you have configured your alternate servers, you must create and assign new firmware records, and associate them with the alternate servers. Then, you must specify which alternate firmware download server is to be used by a device group or by individual devices. Once you have finished these set-up procedures, you are ready to perform remote firmware downloads using the [Firmware Upgrade Wizard](#) or the [Boot PROM Upgrade Wizard](#).

Instructions on:

- [Configuring the Alternate Server](#)
- [Creating and Assigning Firmware Records](#)
- [Setting the Firmware Server](#)

## Configuring the Alternate Server

Use the [Alternate Firmware Servers view](#) in the Options window to configure your alternate firmware download servers.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the File Transfer Method folder, and select Alternate Firmware Servers. The right-panel Alternate Firmware Servers view displays a list of any configured alternate servers.
3. Click **Add Server** to open the [Add Alternate Firmware Server window](#) where you can configure a new alternate server:
  - a. Enter the IP address of the workstation where the server is running.
  - b. Enter an Identifier -- a description that helps you identify the alternate server.

- c. Enter the Server Root Path. The root directory is the base directory to which the server is allowed access. The server will be allowed to create files to or read files from this directory and any of its subdirectories. Keep in mind the following requirements when setting the server root path:
  - If your server is configured with a root directory, it must match the root directory entered here.
  - If your server is **not** configured with a root directory, specify the root directory here as the root of the drive (e.g. C:\ or D:\).
- d. Specify the transfer protocol for the alternate server.
- e. The required connection information changes depending on your selected transfer protocol.
  - For TFTP, specify the port number your TFTP server is configured to run on.
  - For FTP or SCP, specify the port number your server is configured to run on. Select the Anonymous checkbox if your server is configured to accept Anonymous logins; Inventory Manager will automatically fill in the username and password fields. Otherwise, enter your username and password to access the server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.
4. To edit an alternate server, select a server in the list and click **Edit Server**. The [Edit Alternate Firmware Server window](#) opens where you can edit certain server properties.
5. To remove a server, select a server and click **Remove Server**.
6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

After you have configured your alternate servers, you must create and assign firmware records, and associate them with the alternate servers. See the instructions below for more information.

## Creating and Assigning Firmware Records

Before you can use an alternate firmware server to perform remote firmware downloads, you need to create the firmware records associated with the alternate server and add them to the Inventory Manager database. Use the

[Create Firmware Record window](#) to create the new firmware entries and associate them with your configured alternate servers.

When you create a firmware record, it is added to the Unknown folder and the All Firmware folder in the Firmware Mgmt tab. You will need to use the [Assign Firmware window](#) to assign the record (firmware image) to one or more product families or device types.

After assigning the firmware, you must configure your remote devices to use the alternate server when performing download operations (see [Setting the Firmware Server](#) below) in order to see these images listed in the Firmware Upgrade Wizard. This enables you to download the image to your remote network devices of that family or type, using the [Firmware Upgrade Wizard](#) or the [Boot PROM Upgrade Wizard](#).

1. Select the All Firmware folder in the left-panel Firmware Mgmt tab and select **Tools > Create Firmware Record**, or right-click the All Firmware folder and select Create Firmware Record from the menu. (You must have a configured alternate firmware server for this menu option to be available.) The Create Firmware Record window opens.
2. Use the radio buttons at the top of the window to specify whether the image is a firmware or boot PROM image.
3. In the **Image file name** field, enter the name of the firmware or boot PROM image as it appears in the image directory.
4. In the **Image directory path** field, enter the path to the location where the image is stored.
5. The table at the bottom of the window lists your configured alternate firmware download servers. Select the appropriate server for the firmware record: the image directory path must exist under the server root path. If you select multiple servers, be sure that the same image type, file name, and directory path are used on all selected servers. Individual firmware records will be created for each selected server.
6. Click **OK** to create the firmware record and close the window. Click **Apply** to create the record and leave the window open, allowing you to create more firmware records. The firmware records are added to the Unknown folder and the All Firmware folder in the Firmware Mgmt tab.
7. Assign the firmware record to the appropriate product families or device types.
  - a. Expand the Unknown folder in the left-panel Firmware Mgmt tab. Select the firmware or boot PROM image, then select **Tools > Assign**

**Firmware.** You can also right-click on the image, and select Assign Firmware from the menu. The [Assign Firmware window](#) opens.

- b. In the Device Type list, select the families and/or individual device types where you want to assign the image. You can select multiple product families or device types using the **Ctrl** or **Shift** keys.
- c. Click **OK** to assign the image to the selected product families and/or device types and close the window.

After you have [configured your alternate servers](#), and created and assigned your firmware records, you must specify which alternate firmware download server is to be used by a device group or by individual devices. See the instructions below for more information.

## Setting the Firmware Server

Before you can use an alternate firmware server to perform remote firmware downloads, you must configure your remote devices to use the alternate server when performing download operations. All devices are initially configured to use the mapped file transfer server (as configured in the Services for NetSight Server view of the Suite-Wide Options window) for firmware downloads. By specifying an alternate firmware download server, you can enable a remote device to use a server in its own local network.

Use the [Set Firmware Server window](#) to specify which firmware download server a device will use when performing firmware downloads. You can set the firmware server for a single device, multiple devices, or a device group.

1. Select a single device or device group in the left-panel Network Elements tab or multiple devices in a right-panel Details View tab, then select **Tools > Alternate Firmware Server** from the menu bar. You can also right-click a device or device group and select the Alternate Firmware Server option from the menu. The Set Firmware Server window opens.
2. Use the drop-down list to select the IP address of the firmware download server you would like used for the selected device(s). The drop-down list displays all the alternate servers that match the file transfer method set for the device(s). All devices are initially configured with TFTP as their file transfer method, until specified otherwise. For more information, see [How to Set a File Transfer Method](#).
3. Click **OK** to set the server and close the window.

After you have [configured your alternate servers](#), [created and assigned your firmware records](#), and set your firmware server using these instructions, you will be ready to perform firmware downloads using your alternate firmware download servers. For information on performing downloads, see the [Firmware Upgrade Wizard](#) or the [Boot PROM Upgrade Wizard](#).

---

### **Related Information**

For information on related windows:

- [Alternate Firmware Servers View, Options Window](#)
- [Create Firmware Record Window](#)
- [Set Firmware Server Window](#)

## How to Set Up Third-Party Device Support

---

Inventory Manager provides device management support for third-party devices by executing scripts on the devices using Telnet or SSH. With this support, Inventory Manager Wizards can perform their operations on third-party devices even though the devices do not support the required SNMP MIBs. The devices are set up to use scripts in place of the MIBs when performing the Inventory Manager functions.

The following Inventory Manager functions can be performed on third-party devices through the use of scripts:

- Configuration Upload (Archive Save)
- Configuration Download (Restore Archive)
- Firmware Download (Firmware Upgrade)
- Device Reset
- Device Timed Reset

Scripts are created and stored in Device Family Definition Files. These definition files can include multiple scripts (one for each Inventory Manager function), written for a specific device family. The files can also include regular expressions to determine if the scripts were executed successfully.

The script itself contains the CLI commands used to perform the function on the device, and is executed by the NetSight Command Script Tool. For more information, see the [How to Use the Command Script Tool Help](#) topic located in the Suite-Wide Tools section of the online help or user guide (PDF).

Configuration files and firmware image files for script transfers should be stored in the same directories as files for transfers using MIBs. Files can be transferred through the use of a TFTP, FTP, or SCP server. For information on server setup, see the [TFTP Server Setup](#), [FTP Server Setup](#), and [SCP Server Setup](#) Help topics in the Inventory Manager online help or user guide (PDF).

This Help topic contains information for creating Device Family Definition Files, and the steps for configuring your third-party devices to use the scripts stored in definition files. When you have completed the device configuration, you will be able to perform Inventory Manager Wizard operations on your third-party device.

**Instructions on:**



- [Device Family Definition Files](#)
  - [Creating Device Family Definition Files](#)
  - [Using Script Variables](#)
  - [Sample Script Execution](#)
  - [File Backup and Restore](#)
- [Configuring Devices](#)
- [Logging and Error Reporting](#)
  - [Logging](#)
  - [Log Output](#)
  - [Error Troubleshooting](#)

## Device Family Definition Files

Scripts for each Inventory Manager function for a specific device family are stored together in a Device Family Definition File. These files are available for selection when configuring your devices to use scripts. Inventory Manager provides definition files for several device families: Extreme, Enterasys, Cisco, and Hewlett Packard. These files are stored as resource files and cannot be modified. You can also create your own user-defined Device Family Definition Files to provide additional scripts for your third-party devices.

### *Creating Device Family Definition Files*

You can create your own Device Family Definition Files to contain the scripts to use for your third-party devices. When you create a definition file, you must follow a specific format. There is a file stored in the <data storage directory>\properties\devicefiles called DeviceFamilyDefTemplate.txt that can be used as a template when creating new files. Any new files you create are stored in the devicefiles directory, and these files will be displayed on the list of files available for selection when configuring your devices.

---

**NOTE:** The path to the data storage directory is specified in the [Inventory Manager options](#).

---

Following is an example of a file called "Cisco Systems - TFTP" that contains a script to perform archive saves (configuration uploads) on Cisco devices. The name "Cisco Systems - TFTP" will show up in the selection list when configuring devices to use scripts.

```
--- Use these scripts to manage Cisco devices
name="Cisco Systems - TFTP"
```

```

desc="Cisco Systems SSH/TFTP Scripts"
separator=Windows_File_Separator
timed_reset_delay_format="HH:mm:ss:SS"
-----BEGIN SCRIPT "Configuration Upload"-----
enable
%ENABLEPSWD%
copy running-config tftp:
%TFTP_IP%
%RELATIVE_TARGET_FILE_PATH%
@receive 20
exit
-----END SCRIPT-----
-----BEGIN SUCCESS "Configuration Upload"-----
bytes copied
-----END SUCCESS-----

```

The following table describes the items included in a definition file:

Item	Description
name="Brand X Networks"	This is the name that appears in the Device Family Definition File drop-down list when selecting a script to use. The name is required and must be unique.
desc="scripts for Brand X"	A description of the intended use of the scripts.
separator=Windows_File_Separator	The type of separator to be used when building a directory path. Possible values are UNIX_File_Separator, Windows_File_Separator, or a user-specified string. Where: UNIX_File_Separator= "/" Windows_File_Separator = "\"
timed_reset_delay_format="HH:mm:ss:SS"	The format to be used when specifying the time for the timed reset delay. The default is "HH:mm". Where: H = hours m = minutes s = seconds S = milliseconds
-----BEGIN PRE-SCRIPT "function name"-----	Separator line that denotes the start of a pre-script. If the device won't transfer the file to the path Inventory Manager expects, a pre-script can be used to create an empty file in advance of the file transfer. This would be the case when a device only transfers a file to an absolute path, not a relative one.
-----END PRE-SCRIPT-----	Separator line that denotes the end of the pre-script.

Item	Description
-----BEGIN SCRIPT " <i>function name</i> "-----	Separator line that denotes the start of a script.
-----END SCRIPT-----	Separator line that denotes the end of a script.
-----BEGIN SUCCESS " <i>function name</i> "-----	Separator line that denotes the start of the regular expressions to test for success. If you include multiple expressions, each expression must be successful for the overall script execution to be considered successful. For firmware download and configuration download operations, the script must contain regular expressions to determine the actual success of the script. Note that if the script exits abnormally, then the test for success will not be performed and the Active Status Summary View and Details View in Inventory Manager will show a status of "failure" for the operation. If the script exits normally, then the status will reflect the results of the test ("success" or "failure").
-----END SUCCESS-----	Separator line that denotes the end of the regular expressions to test for success.
-----BEGIN POST-SCRIPT " <i>function name</i> "-----	Separator line that denotes the start of a post-script. If the device transfers the file to a location other than the path Inventory Manager expects, a post-script can be used to copy the transferred file from one location to another. For example, if the device used an absolute path to do the transfer, the file would be created at the <root>/device_ip.cfg path. You can use a post-script to copy the file from the top-level root path to <root>\configs\tmp\device_ip.cfg path so that Inventory Manager can find the file on script completion and copy it to the permanent storage area.
---	Comment. Anything on the line after these characters is ignored. A comment can only exist outside of a script.

The *function name* must be one of the following:

- "Configuration Upload"
- "Configuration Download"
- "Firmware Download"
- "Reset"
- "Timed Reset"

### Using Script Variables

The Command Script tool that executes the script portion of the file supports the use of system-defined and user-defined variables within the scripts. The variable

must appear in the script bracketed by percentage signs, for example, %TFTPIP%. (For more information on creating command scripts, see How to Use the Command Script Tool under Suite-Wide Tools.)

### System-Defined Variables

There are five NetSight system-defined variables that can be used in a script (however, not in a pre-script or a post-script). These variables are resolved by the NetSight Command Script service:

%DEVICEIP% - The IP address of the currently selected device.

%LOGINUSER% - The login username configured in the Profile of the selected device.

%LOGINPSWD% - The login password configured in the Profile of the selected device.

%ENABLEPSWD% - The enable password configured in the Profile of the selected device.

%CONFIGPSWD% - The config password configured in the Profile for the selected device.

The following script variables are defined and resolved by Inventory Manager when a script is executed:

Variables	Description
%TFTP_IP%	The TFTP Server IP address set in the TFTP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to TFTP for the target device.
%TFTP_URL%	The URL used to copy a file using the TFTP server. It is set to: tftp://TFTP_IP/RELATIVE_TARGET_FILE_PATH
%SERVER_IP%	The IP address of the NetSight Server.
%FTP_IP%	The FTP Server IP address set in the FTP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to FTP for the target device.
%FTP_PORT%	The FTP Server Port number set in the FTP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to FTP for the target device.
%FTP_USER%	The Login Username set in the FTP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to FTP for the target device.
%FTP_PSWD%	The Login Password set in the FTP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to FTP for the target device.
%FTP_URL%	The URL used to copy a file using the FTP server. It is set to: fpt://FTP_IP/RELATIVE_TARGET_FILE_PATH
%SCP_IP%	The SCP Server IP address set in the SCP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to SCP for the target device.
%SCP_PORT%	The SCP Server Port number set in the SCP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to SCP for the target device.
%SCP_USER%	The Login Username set in the SCP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to SCP for the target device.

Variables	Description
%SCP_PSWD%	The Login Password set in the SCP Transfer Settings in the Inventory Manager Options. The File Transfer Method must be set to SCP for the target device.
%SCP_URL%	The URL used to copy a file using the SCP server. It is set to: scp://SCP_IP/RELATIVE_TARGET_FILE_PATH
%TIMED_RESET_DELAY_SECONDS%	The amount of time to delay before the reset should occur. The format of the time is HH:mm:ss.SS. Where: H = hours m = minutes s = seconds S = milliseconds
%TARGET_FILE_NAME%	The name of the file that will be uploaded or downloaded, depending on which function is selected. For example, for a configuration file: xx_xx_xx_xx.cfg (where xx_xx_xx_xx is the device IP address).
%RELATIVE_TARGET_FILE_PATH%	The file path to the TARGET_FILE_NAME relative to the root directory of the server (TFTP, FTP, or SCP). This variable is required for configuration upload or download operations (archive save and archive restore) and firmware download operations. For configuration operations, the path is configs/tmp/xx_xx_xx_xx.cfg (where xx_xx_xx_xx is the device IP address). For firmware download operations, the path is firmware/../../Resources/Images/invhelpp/imageFileName (where <i>imageFileName</i> is the name of the firmware file being downloaded).
%RELATIVE_SERVER_DIR_PATH%	The directory path of the TARGET_FILE_NAME relative to the root directory of the server (TFTP, FTP, or SCP). This variable is required for configuration upload or download operations (archive save and archive restore) and firmware download operations. For configuration operations, the path is configs/tmp/. For firmware download operations, the path is firmware/images/.
%ABSOLUTE_TARGET_DIR_PATH%	The absolute file path to the TARGET_FILE_NAME of the server (TFTP, FTP, or SCP). This variable is required for configuration upload or download operations (archive save and archive restore) and firmware download operations. For configuration operations, the path is serverRootDir/configs/tmp/xx_xx_xx_xx.cfg (where xx_xx_xx_xx is the device IP address). For firmware download operations, the path is serverRootDir/firmware/images/imageFileName (where <i>imageFileName</i> is the name of the firmware file being downloaded).
%ABSOLUTE_SERVER_DIR_PATH%	The absolute directory path of the TARGET_FILE_NAME from the root directory of the server (TFTP, FTP, or SCP). This variable is required for configuration upload or download operations (archive save and archive restore) and firmware download operations. For configuration operations, the path is serverRootDir/configs/tmp/. For firmware download operations, the path is serverRootDir/firmware/images/.
%PATH_SEPARATOR%	Value defined by the "separator=" value, if specified.

## User-Defined Variables

User-defined variables let you create custom variables based on device IP address that will be substituted in a script command when it is executed on the specific device.

For example, let's say you want to perform an archive save (configuration upload) on multiple devices using a script command that specifies interface names. You can create a set of variables that define the interface name values for each device, and add the variables to your script.

The variables are defined in their own script section using the following separators. The section can be placed at any location in the script.

```
-----BEGIN USER-DEFINED VARIABLES -----
```

```
-----END USER-DEFINED VARIABLES -----
```

User-defined variables have the following format:

```
userDefinedVariableName.Default=myvalue
```

where:

userDefinedVariableName is replaced with a unique variable name  
Default can be left as Default or replaced with the IP address of a device the script will be used on  
myvalue is the value that the variable will be replaced with

The variable must appear in the script bracketed by percentage signs, for example %InterfaceName%. When a script running on a device encounters a variable, it looks in the user-defined variable section for the variable name and the device IP address. If it finds a match, it substitutes the defined value. If the IP address is not found, the script looks for the default. If it finds a default, it substitutes the defined default value. If no default is found, an empty string value is used.

User-defined variable names are **not** case sensitive and must be unique. They can only contain alphanumeric characters and underscores.

Here are some examples of user-defined variables:

```
-----BEGIN USER-DEFINED VARIABLES -----
INTERFACE_NAME.default = ge.1.0
INTERFACE_NAME.10.20.77.33=ge.1.1
INTERFACE_NAME.10.20.80.138=ge.1.2
--
firmwareVersion.Default=7.07.12
firmwareVersion.10.20.77.33=06.00.01
firmwareVersion.10.20.80.138=06.00.02
--
SOME_PATH.Default=c:\Temp\newFile.txt
SOME_PATH.10.20.77.33=d:\Temp\10_20_77_33.txt
SOME_PATH.10.20.80.138=d:\Temp\10_20_80_138.txt
--
filename.default=slot4/jcn3p.cfg
fileName.10.20.80.138=someotherfile.txt
```

```
--  
finalfile.10.20.77.22=d:/Temp/10207733.cfg  
-----END USER-DEFINED VARIABLES -----
```

### *Sample Script Execution*

This is a description of how Inventory Manager performs an archive (configuration upload) operation using a script file.

1. **Create an empty file before file transfer.** The more secure TFTP/FTP/SCP servers will not allow a file to be written that does not already exist. For this reason, Inventory Manager always creates a zero length file in the Protocol's root\configs\tmp\device\_ip.cfg path. This provides a placeholder for the device to write to during the file transfer operation. (The root directory is configured in the Tools > Options > File Transfer Setting windows.) Note that some devices won't transfer the file to the path that Inventory Manager expects (for example, the device only transfers a file to an absolute path, not a relative one). In this case, an empty file can be created using a pre-script in the Device Family Definition file.
2. **Initiate upload to transfer the configuration file from the device to the file transfer server.** To do this, the script portion of the Device Family Definition file is executed by the NetSight Command Script Tool. A telnet or SSH session is initiated on the device and the script is sent to the device for execution. The file is expected to be transferred to the path relative to the root of the transfer server at configs/tmp/device\_ip.cfg.
3. **Copy the file transferred to a permanent archive location.** Once the device reports back success, Inventory Manager copies the file to the data storage directory. If the file is zero length, it is deleted. Note that some devices will transfer the file to a location other than the path Inventory Manager expects. In this case, the file can be copied to the expected location using a post-script in the Device Family Definition file.

Following is a sample script that uses the pre-script and post-script sections. The pre-script section creates an empty file at the TFTP server's top-level root directory called C:/tftpboot/xx\_xx\_xx\_xx.cfg, where xx\_xx\_xx\_xx is the IP address of the device and the TFTP root directory is C:/tftpboot/. The script section causes the device to transfer the file to the path where the empty file was created. And the post-script section copies the transferred file to the path where Inventory Manager expects to find the file.

```
-- This script shows how the pre-script and post-  
script sections of the DeviceFamilyDefinition file can
```

```

be used.
-- This is only an example and not intended for use
beyond that.
--
name="Enterasys Networks"
desc="Enterasys Networks SSH/TFTP Scripts"
separator=WINDOWS_FILE_SEPARATOR
--
-----BEGIN PRE-SCRIPT "Configuration Upload"-----
create c:%PATH_SEPARATOR%tftpboot%PATH_
SEPARATOR%%TARGET_FILE_NAME%
-----END PRE-SCRIPT-----
-----BEGIN SCRIPT "Configuration Upload"-----
delete slot4/switch.cfg
show config outfile slot4/switch.cfg
@receive 20
copy slot4/switch.cfg tftp://%tftp_IP%/%TARGET_FILE_
NAME%
exit
-----END SCRIPT-----
-----BEGIN POST-SCRIPT "Configuration Upload"-----
copy c:%PATH_SEPARATOR%tftpboot%PATH_
SEPARATOR%%TARGET_FILE_NAME% %ABSOLUTE_TARGET_FILE_
PATH%
-----END POST-SCRIPT-----

```

### *File Backup and Restore*

All user-defined Device Family Definition Files are backed up and restored during a Database Backup and Restore operation. To perform a backup or restore operation, open the Server Information window (Tools > Server Information) and select the Database tab. Use the Backup and Restore buttons in the NetSight Data Set Operations section. The Backup operation places all the files under the <data storage directory>\properties\devicefiles directory in a zip file. The Restore operation unzips them and places them back under the devicefiles directory.

---

**NOTE:** The path to the data storage directory is specified in the [Inventory Manager options](#).

---



## Configuring Devices

This section provides information on setting up your third-party devices to use the scripts stored in Device Family Definition Files. There are several preliminary steps to perform in order to be able to execute a script on a device.

1. The device must have CLI credentials set so that the Command Script Tool can set up a Telnet or SSH session with the device. Use the NetSight Authorization/Device Access tool (accessed from Inventory Manager's Tools menu) to configure the profiles and credentials that provide access to your network devices. Each device is assigned a profile and that profile designates the CLI credentials to use for that device. CLI credentials include the following information:
  - User name
  - Login Password
  - Enable Password
  - Configuration Password
  - Connection Type - SSH or Telnet

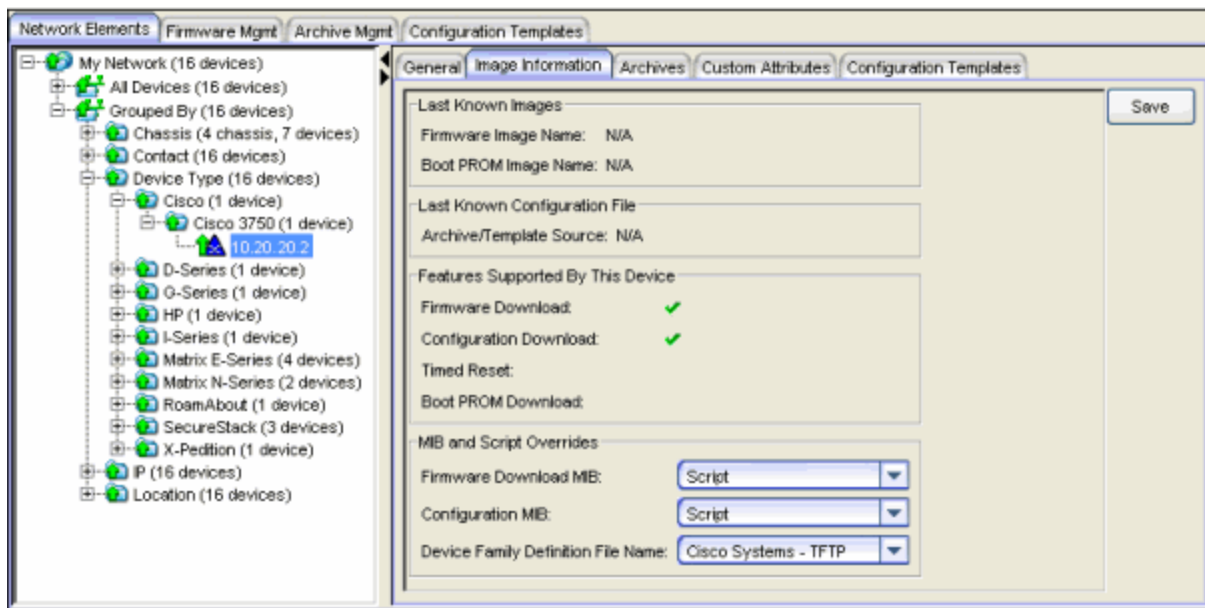
The Command Script tool uses the connection type (SSH or Telnet), user name, and login password specified in the CLI credentials when establishing a connection to the device. If these are not set up correctly, the connection cannot be created.

2. The device must have SNMP read access configured in the Device Access Profile. Use the NetSight Authorization/Device Access tool to configure your profiles.
3. You must have a TFTP, FTP, or SCP server configured and running to perform an upload or download operation.
4. Make sure that the File Transfer Method has been set for the target devices. For information see [File Transfer Method Window](#).
5. The files to be transferred should be stored in the same directories as files for transfers using a MIB.

You must also specify the script that will be used by the third-party devices. You can specify a script for a single third-party device, for multiple devices in a device group, or for multiple devices of a specific device type (Extreme or Enterasys devices only) as outlined in the steps below.

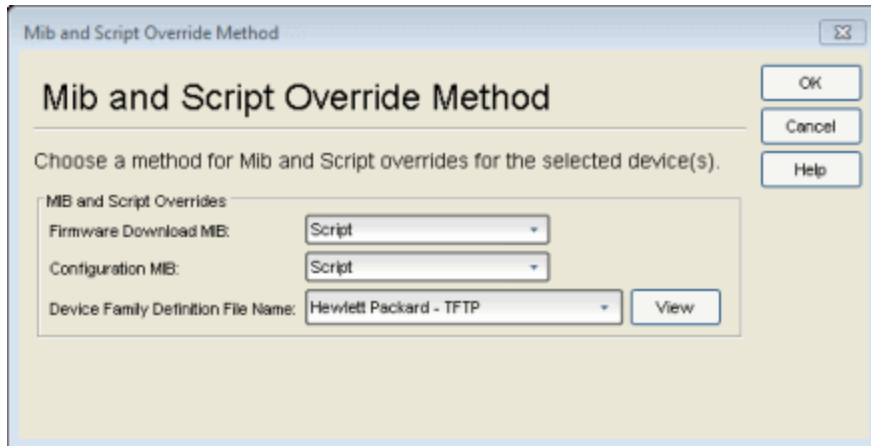
**To select a script to be executed for a single third-party device:**

1. In the left-panel Network Elements tab, select the desired device. Select the Image Information tab in the right panel.
2. In the Firmware Download MIB field, select **Script** from the drop-down list.
3. In the Configuration Download MIB field, select **Script** from the drop-down list.
4. In the Device Family Definition File Name field, select the file that contains the scripts you want to use. Once the file is selected, the "Features Supported By This Device" section is completed with the types of scripts found in the file.



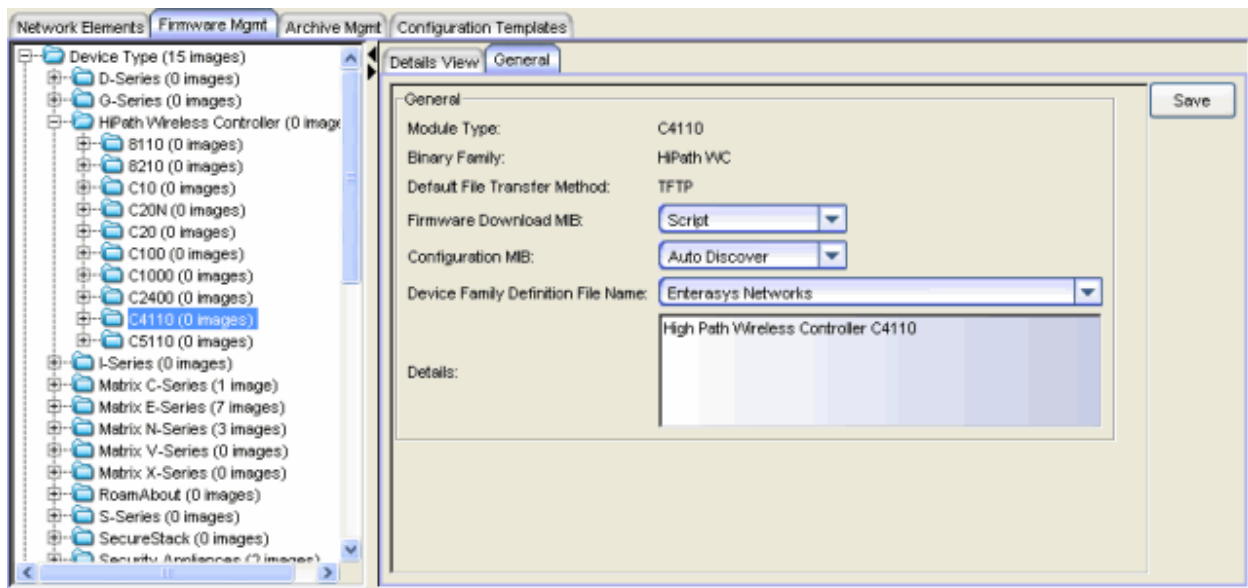
To set a script to be executed for all devices in a device group:

1. In the left-panel Network Elements tab, select the desired device group. Right-click and select **MIB Override Method**. The MIB and Script Override window opens.
2. In the Firmware Download MIB field, select **Script** from the drop-down list.
3. In the Configuration Download MIB field, select **Script** from the drop-down list.
4. In the Device Family Definition File Name field, select the file that contains the scripts you want to use.
5. Click **OK**.



To set a script to be executed for all devices of a specific device type (Extreme or Enterasys devices only):

1. In the left-panel Firmware Management tab, select a device type firmware image folder. Select the General tab in the right panel.
2. In the Firmware Download MIB field, select Script from the drop-down list.
3. In the Configuration Download MIB field, select Script from the drop-down list.
4. In the Device Family Definition File Name field, select the file that contains the scripts you want to use.



When you have finished configuring your devices to use scripts, you will be able to perform Inventory Manager Wizard operations on those devices.

## Logging and Error Reporting

This section provides information about how to enable debug logging and perform troubleshooting using log output and error messages, when using the third-party script functionality.

### *Logging*

You can use the NetSight Server Diagnostics web page to enable debug logging that allows you to see the content of the script before it is sent to the device and the content of the SSH session after the script has been executed.

Access this web page from the NetSight Launch page by clicking the Administration tab. To access the server diagnostics, you will need to log in with your username and password. (If the NetSight Server is a Windows platform system, in the Username field you must enter a domain name and a username using the following format: <domain name>\<username>). Enable the "Inventory Manager" and "Telnet/SSH Command Shell" debug groups by setting the Diagnostic Level to "Verbose." You can view the log output in the Server Information window (Tools > Server Information) on the Server Log tab. You can also access the log output in <install area>\NetSight\appdata\logs\server.log on the NetSight Server.

### *Log Output*

The following debug log error message appears when more than a second has passed without activity over the SSH session. If a script uses the meta command @RECEIVE *n*, there will be *n* number of these messages in the log. It does not necessarily indicate an error.

```
DEBUG [SSHShellConnection] 10.20.80.80:20 socket closed or  
timed out
```

For information on using meta commands, see How to Use the Command Script Tool under Suite-Wide Tools.

This log output displays the Inventory Manager script variable values just before the script is executed. In this example, the File Transfer Method for the device is set to TFTP, so only the TFTPURL is valid. The TIMEDRESET will be set only for a timed reset from the Reset Device Wizard.

```
DEBUG [ScriptMib] TFTP_IP = 10.20.30.40  
DEBUG [ScriptMib] FTP_URL =  
ftp://null:null@10.20.90.30:69/configs/tmp/10_20_80_80.cfg  
DEBUG [ScriptMib] SERVER_IP = 10.20.30.40
```

```
DEBUG [ScriptMib] TARGET_FILE_NAME = 10_20_80_80.cfg
DEBUG [ScriptMib] TIMED_RESET_DELAY_SECONDS = -1
DEBUG [ScriptMib] SCP_URL =
scp://null:null@10.20.90.30:69/configs/tmp/10_20_80_80.cfg
DEBUG [ScriptMib] TFTP_URL =
tftp://10.20.30.40/configs/tmp/10_20_80_80.cfg
DEBUG [ScriptMib] SCP_IP = 10.20.30.40
DEBUG [ScriptMib] FTP_IP = 10.20.30.40
DEBUG [ScriptMib] RELATIVE_TARGET_FILE_PATH = configs/tmp/10_
20_80_80.cfg
```

### *Error Troubleshooting*

Here is a list of some of the possible errors that could be generated from a script and displayed in the Server Log.

#### **authentication failure: The login credentials are invalid.**

Check the CLI credentials of the target device using the Authorization/Device Access window available from the Inventory Manager Tools menu.

#### **connection refused: SSH access is not enabled on the device, and is required for the script to execute.**

Verify that SSH is enabled on the target device.

#### **SSH channel is closed. (The connection is being shutdown): Lost connection to the device.**

This error is produced when the SSH session ends unexpectedly. This can happen during a reset if there are any commands in the script after the "reboot" command. This case is expected and handled in the server.

#### **Config file is empty.**

This error is produced during a Configuration Upload (Archive Save) operation, and can be caused by a number of reasons. Turn on debug logging and check the script output. Here are a few possible reasons:

- The script has an error and did not perform the function properly.
- The TFTP/FTP/SCP server was not running or could not be reached from the target device.
- The session ended before the file was completely transferred.

#### **Error Restoring Config File.**

This error is produced during a Configuration Download (Archive Restore) operation, and can be caused by a number of reasons. Turn on debug logging and check the script output. Here are a few possible reasons:

- The script has an error and did not perform the function properly.

- The TFTP/FTP/SCP server was not running or could not be reached from the target device.
- The session ended before the file was completely transferred.

#### **Error Restoring Firmware.**

This error is produced during a Firmware Download operation, and can be caused by a number of reasons. Turn on debug logging and check the script output. Here are a few possible reasons:

- The script has an error and did not perform the function properly.
- The TFTP/FTP/SCP server was not running or could not be reached from the target device.
- The session ended before the file was completely transferred.

#### **Error Resetting device.**

This error is produced during a Timed Reset operation. Turn on debug logging and check the script output. It is possible that the script has an error and did not perform the function properly.

#### **Device did not reset - System up time did not reset.**

This error is produced during a manual reset. The sysUpTime did not change as expected, so it is determined that the device reset failed. Turn on debug logging and check the script output.

#### **No matches found for Success type regEx from script.**

This error is produced by the output being parsed for the regular expressions given in the Device Family Definition File. Check the file and script output for the cause.

#### **Unknown Ticket Type**

The function selected is not supported.

---

#### **Related Information**


- [TFTP Server Setup](#)
- [FTP Server Setup](#)
- [SCP Server Setup](#)
- [File Transfer Method Window](#)

## How to Track a Device

---

The [Track Device window](#) lets you to track a device based on the device's serial number or MAC address. This allows you to view a history of device attributes, and monitor any changes made to the device. The Track Device information is based on the device's archived configuration files -- there will be one table entry for each saved configuration file.

1. In the left-panel Network Elements tree, select a device and then select **Tools > Track Device** from the menu bar. The Track Device window opens and displays information for the selected device. If you have not performed an archive on that device, the table will be empty and you will see a message that says "No database entries found."
2. After viewing the results, you can enter a new value and perform another track device operation. In the **Track By** field, use the drop-down list to specify whether you want to search for a device by serial number or MAC address.
3. In the **Value** field, enter the serial number or MAC address, depending on what you selected in the **Track By** field.
4. Click **Track** to start the track device operation and display the results. The new results will overwrite the results from the previous tracking operation.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

---

### Related Information

For information on related tabs:

- [General Tab \(Device\)](#)
- [Details View Tab \(Device Group\)](#)

For information on related windows:

- [Track Device Window](#)

# How to Upgrade Boot PROM

---

Use the [Boot PROM Upgrade Wizard](#) to easily upgrade the boot PROM images on your network devices.

Instructions on:

- [Preparing to Upgrade](#)
- [Performing an Upgrade](#)

## Preparing to Upgrade

There are certain steps you must perform before you can upgrade your boot PROM images. The steps vary depending on whether you are using a mapped file transfer server (as configured in the Services for NetSight Server view of the Suite-Wide Options window) or an alternate remote file transfer server (as configured in the [Alternate Firmware Servers view](#) in the Options window) to perform the upgrade.

If you are using a mapped file transfer server:

- You must have a TFTP, FTP, or SCP server configured and running to perform the download operation. See [TFTP Server Setup](#), [FTP Server Setup](#), or [SCP Server Setup](#) for instructions.
- Set the file transfer method for the devices you wish to upgrade. See [How to Set a File Transfer Method](#) for instructions.
- Store the boot PROM images that you want to download in the default tftpboot\firmware\images directory or a specified alternative firmware directory. See [TFTP Server Setup](#), [FTP Server Setup](#), or [SCP Server Setup](#) for instructions on changing your firmware directory.
- Discover your firmware/boot PROM images and display them in the Firmware Mgmt tab. See [Firmware Discovery](#) for instructions.

If you are using an alternate remote file transfer server:

- You must have the alternate server configured and running to perform the download operation. See [Configuring the Alternate Server](#) for instructions.
- Set the file transfer method for the devices you wish to upgrade. See [How to Set a File Transfer Method](#) for instructions.



- Store the boot PROM image that you want to download in a specified alternative firmware directory.
- Create firmware records to associate with the alternate server and add them to the Inventory Manager database. In addition, you must assign the firmware record to the appropriate product families or device types. See [Creating and Assigning Firmware Records](#) for instructions.
- Specify which alternate server a device will use when performing firmware downloads. See [Setting the Firmware Server](#) for instructions.

Once these steps have been performed, you are ready to use the Boot PROM Upgrade Wizard.

**NOTE:** The Boot PROM Upgrade Wizard can also be used to downgrade boot PROM to a previous revision. Downgrading boot PROM is inherently risky due to possible feature differences between revisions. Restoring configurations from different firmware revisions carries the same risk. Should you need to downgrade your boot PROM to an earlier version, it is recommended that you use **one** of the following two procedures:

- Downgrade the boot PROM on a network device using the Boot PROM Upgrade Wizard. Do not proceed to the Reset Devices portion of the wizard, instead select [Finish]. Restore an archived configuration that was previously created with the boot PROM image being downloaded. This will reset the device.
- or**
- Downgrade the boot PROM on a network device using the Boot PROM Upgrade Wizard. Complete the downgrade using the wizard Reset Devices screens. Clear NVRAM on the device and reconfigure the network configuration parameters of the device using the local console.

In addition, when downgrading boot PROM on SNMPv3 devices, it is possible that Inventory Manager will lose contact with the device. SNMPv3 adds a level of difficulty to downgrade operations, because counters and timers related to security features of SNMPv3 may get out of sync. Following the downgrade, you will need to restart Inventory Manager to re-establish contact with the device.

---

**CAUTION:** Prior to upgrading boot PROM on a device, it is recommended that you archive the latest configuration for the device being upgraded. This will aid you in downgrading should you choose to do so.

---


## Performing an Upgrade

Use these steps to upgrade boot PROM. Be sure to perform the steps in [Preparing to Upgrade](#) before beginning the upgrade operation

---

**NOTE:** During the device reset, Inventory Manager learns the current boot PROM version installed on the device. Inventory Manager uses this information to determine whether the boot PROM version installed on the device matches the boot PROM reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

1. Select **Tools > Wizards > Boot PROM Upgrade Wizard** from the menu bar or click  on the toolbar. The Boot PROM Upgrade Wizard opens.
2. **Select the devices to upgrade:**
  - a. Expand the folders under the left-panel tree and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys). Click **Add**.

---

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).

---

- b. The devices are listed in the Selected Devices table. Devices that do not support the boot PROM upgrade operation, or have never been contacted, are not listed. If you want to remove a device from the list, select the device and click **Remove**.
    - c. Click **Next**.

---


**TIP:** If you open the Boot PROM Upgrade Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed under Selected Devices.

---

3. **Assign a boot PROM to each device type or family:**
  - a. If necessary, click the **Refresh Images** button to perform a firmware discovery and update the list of boot PROM images.

- b. Select a family/device type in the left-panel Assignments table.
- c. In the right-panel, select a boot PROM image and use the **Assign to:** arrows to assign the image to the device type or to each entry that is a member of that binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each table entry.
- d. Before proceeding with the upgrade, verify that boot PROM and firmware images that will be on the device after the upgrade operation are compatible. Refer to the boot PROM and firmware release notes for more information.
- e. Click **Next**.

#### 4. Initiate the Boot PROM Upgrade operation:

- a. Specify the **Download Type** option. The downloads will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Enter the value **1** to have the downloads performed serially, one device after another.
- b. Click **Start** to initiate the boot PROM upgrade operation. The table at the top of the window will update with status information as will the status area in the bottom left of the screen.
- c. Review results. An alert icon  will appear in the Alert column of the table if a download fails for the specific device. You can select to show all devices or show only those that are incomplete or have failed.
- d. Click **Next**.

#### 5. Reset devices that support Timed Reset:

If you are resetting devices that support Timed Reset, you will see a window listing those devices. Timed Reset gives you the flexibility to set up your reset operation with a time delay, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.

- a. In the **Selected column**, select the devices that you want to reset. You can select an option to display devices that do not support timed reset and devices that failed the firmware upgrade; however, these devices cannot be reset from this window.
- b. Enter the reset delay. This is the amount of time (in seconds) until the device resets after the reset operation begins. For example, if you start the reset operation at 4:00 pm with a 7 hour reset delay (420

seconds), the device(s) will reset at 11:00 pm. This allows you to schedule your resets for a time when the network is least busy.

- c. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
- d. Click **Start** to initiate the timed resets. Once the devices are back up, click **Refresh** to see if the new boot PROM is running.

6. **Reset devices that do not support Timed Reset:**

If you are resetting devices that do not support Timed Reset, you will see a window listing those devices.

- a. In the **Selected column**, select the devices that you want to manually reset.
- b. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
- c. Click **Start** to initiate the manual resets. Resets occur one at a time, continuing only after a device is fully booted.
- d. After the reset operation is completed, click **Refresh** to see if the devices are running the new boot PROM.

7. Click **Finish** to close the wizard.
- 

## Related Information

For information on related tasks:

- [Boot PROM Upgrade Wizard](#)
- [FTP Server Setup](#)
- [SCP Server Setup](#)
- [TFTP Server Setup](#)
- [Firmware Discovery](#)
- [How to Set Up Alternate Firmware Download Servers](#)
- [How to Set a Reference Image](#)
- [How to Set a File Transfer Method](#)

## How to Upgrade Firmware

---

Use the [Firmware Upgrade Wizard](#) to easily upgrade the firmware images on your network devices. The wizard gives you the flexibility of performing an immediate upgrade or scheduling the upgrade to take place at a later time. If you schedule the upgrade, the wizard will automatically perform the upgrade at the scheduled time, and then alert you that the upgraded devices need to be reset via the Reset Wizard.

Instructions on:

- [Preparing to Upgrade](#)
- [Performing an Upgrade](#)
- [Scheduling an Upgrade](#)
  - [Viewing Scheduled Upgrades](#)
  - [Canceling a Scheduled Upgrade](#)

### Preparing to Upgrade

There are certain steps you must perform before you can upgrade your firmware. The steps vary depending on whether you are using a mapped file transfer server (as configured in the Services for Extreme Management Center Server view of the Suite-Wide Options window) or an alternate remote file transfer server (as configured in the [Alternate Firmware Servers view](#) in the Options window) to perform the upgrade.

If you are using a mapped file transfer server:

- You must have a TFTP, SCP, or FTP server configured and running to perform the download operation. See [TFTP Server Setup](#), [SCP Server Setup](#), or [FTP Server Setup](#) for instructions.
- Set the file transfer method for the devices you wish to upgrade. See [How to Set a File Transfer Method](#) for instructions.
- For TFTP or FTP servers, store the firmware images that you want to download in the default tftpboot\firmware\images directory or a specified alternative firmware directory. For an SCP server, store the firmware images that you want to download in the default root\firmware\images directory or a specified alternative firmware directory. See [TFTP Server Setup](#), [FTP](#)

[Server Setup](#), or [SCP Server Setup](#) for instructions on changing your firmware directory.

- Discover your firmware images and display them in the Firmware Mgmt tab. See [Firmware Discovery](#) for instructions.

If you are using an alternate remote file transfer server:

- You must have the alternate server configured and running to perform the download operation. See [Configuring the Alternate Server](#) for instructions.
- Set the file transfer method for the devices you wish to upgrade. See [How to Set a File Transfer Method](#) for instructions.
- Store the firmware images that you want to download in a specified alternative firmware directory.
- Create firmware records to associate with the alternate server and add them to the Inventory Manager database. In addition, you must assign the firmware record to the appropriate product families or device types. See [Creating and Assigning Firmware Records](#) for instructions.
- Specify which alternate server a device will use when performing firmware downloads. See [Setting the Firmware Server](#) for instructions.

---

**NOTE:** The Firmware Upgrade Wizard can also be used to downgrade firmware on some devices (not Extreme Access Control and Application Analytics appliances) to a previous revision. Downgrading firmware is inherently risky due to possible feature differences between revisions. Restoring configurations from different firmware revisions carries the same risk. Should you need to downgrade your firmware to an earlier version, it is recommended that you use **one** of the following two procedures:

- Downgrade the firmware on a network device using the Firmware Upgrade Wizard. Do not proceed to the Reset Devices portion of the wizard, instead select [Finish]. Restore an archived configuration that was previously created with the firmware image being downloaded. This will reset the device.
- or**
- Downgrade the firmware on a network device using the Firmware Upgrade Wizard. Complete the downgrade using the wizard Reset Devices screens. Clear NVRAM on the device and reconfigure the network configuration parameters of the device using the local console.

In addition, when downgrading firmware on SNMPv3 devices, it is possible that Inventory Manager will lose contact with the device. SNMPv3 adds a level of difficulty to downgrade operations, because counters and timers related to security features of SNMPv3 may get out of sync. Following the downgrade, you will need to restart Inventory Manager to re-establish contact with the device.

---

---

**CAUTION:** Prior to upgrading firmware on a device, it is recommended that you archive the latest configuration for the device being upgraded. This will aid you in downgrading should you choose to do so.

In addition, if you are upgrading devices that support HAU (Highly Available Upgrade) you should perform a [Firmware Discovery](#) or Refresh to ensure you have the latest HAU values before launching the firmware wizard.

---

If you are upgrading a Extreme Access Control or Application Analytics appliance:

When upgrading a Extreme Access Control or Application Analytics appliance, you must also do the following:


- Set up CLI credentials for the device up in the Authorization/Device Access window. For additional information, refer to the [How to Configure Profiles and Credentials](#) Help topic.
- Configure the device family definition file name by performing the following steps:
  1. Select the device in the device list in the Network Elements tab.
  2. Open the Image Information tab.
  3. Select **Script** in the **Firmware Download MIB** drop-down menu.
  4. Select the appropriate option based on the device type for which the upgrade is occurring and the server type from which the firmware is downloading in the **Device Family Definition File Name** drop-down menu.
  5. Click **Save**.

**NOTE:** If you select an option in the Device Family Definition File Name field that does not match the method selected in the Extreme Management Center Inventory Manager Options window, an error message displays. Clicking **Yes** updates the method in the Extreme Management Center Inventory Manager Options window to match the method selected in the **Device Family Definition File Name** field.

## Performing an Upgrade

Use these steps to perform a firmware upgrade. These instructions are for performing an immediate upgrade; to schedule an upgrade for a future time, use the steps in [Scheduling an Upgrade](#). Be sure to perform the steps in [Preparing to Upgrade](#) before beginning the upgrade operation.

**NOTE:** During the device reset part of the wizard, Inventory Manager learns the current firmware version installed on the device. Inventory Manager uses this information to determine whether the firmware version installed on the device matches the firmware reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

1. Select **Tools > Wizards > Firmware Upgrade Wizard** from the menu bar or click  on the toolbar. The Firmware Upgrade Wizard opens.
2. **Select the devices to upgrade:**
  - a. Expand the folders under the left-panel tree and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys). Click **Add**. If there were devices that failed the previous upgrade an **Add Failed** button is displayed. Use the **Add Failed** button to add those devices to the upgrade.

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).
  - b. The devices are listed in the Selected Devices table. Devices that do not support firmware download or have never been contacted, are not listed. If you want to remove a device from the list, select the device and click **Remove**.
  - c. Click **Next**.

---

**TIP:** If you open the Firmware Upgrade Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed under Selected Devices.

---


3. **Assign a firmware image to each device type or family:**
  - a. If necessary, click the **Refresh Images** button to perform a firmware discovery and update the list of firmware images.
  - b. The left panel lists the device types of the devices selected for the firmware upgrade. Select a device type.
  - c. The right panel lists firmware images that are compatible with the selected device type. (Select the **Show All Images** checkbox to display all your firmware images.) Select a firmware image and use the **Assign**



**to:** buttons to assign the image to the device type or to each entry that is a member of that binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each table entry.

- d. If a Device Type and firmware image support HAU (Highly Available Upgrade), you will see HAU compatibility information in both tables. For more information, see [HAU Compatible](#) and [HAU Compatible Key](#) in the [Firmware Upgrade Wizard](#) Help topic.
- e. Before proceeding with the upgrade, verify that boot PROM and firmware images that will be on the device after the upgrade operation are compatible. Refer to the boot PROM and firmware release notes for more information.
- f. Click **Next**.

#### 4. Initiate the Firmware Upgrade operation:

- a. Specify the **Download Type** option. The downloads are performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Enter the value **1** to have the downloads performed serially, one device after another.
- b. Click **Start** to initiate the firmware upgrade operation. The table at the top of the window updates with status information as does the status area in the bottom left of the screen.
- c. Review results. An alert icon  will appear in the Alert column of the table if a download fails for the specific device. You can select to show all devices or show only those that are incomplete or have failed.

**NOTE:** If installing a Extreme Access Control or Application Analytics appliance, the Firmware installation is complete. Click **Finish**.

- d. Click **Next**.

#### 5. Reset devices that support Timed Reset:

If you are resetting devices that support Timed Reset, a window listing those devices appears. Timed Reset gives you the flexibility to schedule a reset operation, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.

- a. In the **Selected column**, select the devices that you want to reset. You can select an option to display devices that do not support timed reset and devices that failed the firmware upgrade; however, these

devices cannot be reset from this window.

- b. In the **Reset Time** field, click the **Select** button to open the Select Reset Time window where you can schedule a date and time for the reset. Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. Set the starting time for the operation and select AM or PM.
  - c. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
  - d. Click **Start** to initiate the timed resets. Resets occur simultaneously. Once the devices are back up, click **Refresh** to see if the new firmware is running.
6. **Reset devices that do not support Timed Reset:**  
If you are resetting devices that do not support Timed Reset, you will see a window listing those devices.
- a. In the **Selected column**, select the devices that you want to reset.
  - b. Select the reset type: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).
  - c. Click **Start** to initiate the resets. Resets occur one at a time, continuing only after a device is fully booted.
  - d. After the reset operation is completed, click **Refresh** to see if the devices are running the new firmware.
7. Click **Finish** to close the wizard.

## Scheduling an Upgrade

Use these steps to schedule a firmware upgrade to take place in the background at a future time. Be sure to perform the steps in [Preparing to Upgrade](#) before beginning the upgrade operation. Although a scheduled upgrade runs automatically and does not require your supervision, you will still need to reset any devices that require reset, once the scheduled upgrades have completed.

1. Select **Tools > Wizards > Firmware Upgrade Wizard** from the menu bar or click the **FW Upgrade** button on the toolbar. The Firmware Upgrade Wizard opens.

## 2. Select the devices to upgrade:

- a. Expand the folders under the left-panel tree and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys). Click **Add**. If there were devices that failed the previous upgrade, use the **Add Failed** button to add those devices.
- b. The devices are listed in the Selected Devices table. Devices that do not support firmware download or have never been contacted, are not listed. If you want to remove a device from the list, select the device and click **Remove**.
- c. Click **Next**.

---

**TIP:** If you open the Firmware Upgrade Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed under Selected Devices.


---

## 3. Assign a firmware image to each device type or family:

- a. If necessary, click the **Refresh Images** button to perform a firmware discovery and update the list of firmware images.
- b. The left panel lists the device types of the devices selected for the firmware upgrade. Select a device type.
- c. The right panel lists firmware images that are compatible with the selected device type. (Select the **Show All Images** checkbox to display all your firmware images.) Select a firmware image and use the **Assign to:** buttons to assign the image to the device type or to each entry that is a member of that binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each table entry.
- d. Before proceeding with the upgrade, verify that boot PROM and firmware images that will be on the device after the upgrade operation are compatible. Refer to the boot PROM and firmware release notes for more information.
- e. Click **Next**.

## 4. Configure Scheduling Information for the upgrade:

- a. In the Download Progress window, click the **Schedule** button. The Download Schedule window opens.

- b. Enter a name for the scheduled upgrade, or use the default name which is based on the date the schedule is created.
  - c. Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field.
  - d. Set the starting time for the operation and select AM or PM.
  - e. The downloads will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Enter the value **1** to have the downloads performed serially, one device after another.
  - f. Select the **Abort on Failure** checkbox to stop the downloads after a failure. This is useful if you are scheduling an upgrade operation on multiple devices and you want the operation to stop after a failure on a single device.
  - g. Click **Finish**. When the scheduled upgrade is performed, you can monitor the progress, if desired, via the Active Status panel, just as you do for scheduled archives.
5. **Reset Devices:**  
After the firmware has been upgraded at the scheduled time, a Reset Device icon  is displayed in the status bar indicating that there are devices that have received new firmware images and need to be reset. Double-click the icon to open the Devices Need Reset window where you can launch the [Reset Device Wizard](#) for those devices.

### *Viewing Scheduled Upgrades*

You can view pending upgrades using the [Scheduled Events window](#) (Tools > Scheduled Events).

### *Canceling a Scheduled Upgrade*

You can cancel a scheduled firmware upgrade using the [Scheduled Events window](#) (Tools > Scheduled Events).

---

## **Related Information**

For information on related tasks:

- [Firmware Upgrade Wizard](#)
- [FTP Server Setup](#)
- [TFTP Server Setup](#)
- [Firmware Discovery](#)
- [How to Set Up Alternate Firmware Download Servers](#)
- [How to Set a Reference Image](#)
- [How to Set a File Transfer Method](#)

## How to Use the BOOTP Service

---

The NetSight BOOTP service (available for Windows only) enables the Inventory Manager workstation to also be a BOOTP server. This allows the workstation to supply devices with firmware images (or other basic identity information) in the event the device's current firmware image becomes corrupt. You may also choose to force a device into a BOOTP state in order to have a new firmware image downloaded from the network.

In order for BOOTP to work, you must have a BOOTP and TFTP service set up on the network, and you need a `bootptab` file, which provides the basic device information (device name, IP address, and appropriate firmware image) to the BOOTP service when required.

BOOTP requests are broadcast messages. Routers must be configured to forward BOOTP requests to the BOOTP service, a process sometimes called IP Helper Addressing. Refer to your X-Pedition Router's User Reference Manual for information on configuring IP Helper.

---

**TIP:** The BOOTP service monitors BOOTP requests on the network. NetSight Console can be configured to display those requests, which will aid in recovering devices in a BOOTP state.

---

## Creating a Bootptab File

A `bootptab` file is a simple ASCII text file that contains basic device information (device name, IP address, and appropriate firmware image) for each device on the network that will use the BOOTP service. You can use Inventory Manager to create a `bootptab` file automatically, or create it yourself manually.

### *Creating a bootptab file automatically*

1. In the menu bar, select **Tools > Create BOOTP Tab**.
2. The Save BOOTP Tab window opens allowing you to save the file in the desired directory.  
**NOTE:** If you are using the NetSight BOOTP service, you must save the bootptab file to the `<install directory>\NetSight\services` directory.
3. The `bootptab` file is automatically created in the selected directory. The file has an entry for every device (organized by subnet), using the following

format:

```
device1:ht=1:ha=00001da0b0c0:ip=192.168.1.2:bf=image1.hex  
device2:ht=1:ha=00001da1b1c1:ip=192.168.1.3:hd=image/path:bf=image2.flr
```

Description of bootptab file parameters:

- **Device host name** -- If desired, you can replace the **devicex** parameter with a unique host name or, if your devices are registered in a DNS, with the registered host name from the DNS map.
- **ht=** -- Specifies the host network type. The value is an unsigned decimal, octal, or hexadecimal integer, or a symbolic name. The value "1" represents 10Mb Ethernet (based on industry standard BOOTP implementation).
- **ha=** -- Specifies the hardware address (MAC address) that Inventory Manager is using.
- **ip=** -- Specifies the device's IP address that Inventory Manager is using.
- **hd=** -- Specifies the home directory path to the image file. This is an optional parameter and is used when the image file is in a different directory than either the TFTP server's default directory or root directory path. The home directory is either the absolute path or the offset from the TFTP server's root path.
- **bf=** -- Specifies the Reference Image for that device (if set), or the last firmware image version downloaded to that device through Inventory Manager.

---

**NOTE:** In a BOOTP situation, you will need to edit the **ha** parameter in the file to match the MAC address in the requesting message, and supply any missing parameters such as the **bf** parameter.

---

### *Creating a bootptab file manually*

Inventory Manager provides a sample bootptab file located in the <install directory>\NetSight\services directory. Use this file as a template or an example when you create your own bootptab file.

1. Open the sample bootptab file in a text editor.
2. Enter a list of devices using the format provided in the examples at the top of the file.

3. Save the bootptab file in the  
`<install directory>\NetSight\services` directory.

---

**NOTE:** However you create or modify the bootptab file, remember that the filename must not have an extension. This is important because most text editors will append their own default extension on a new file. If you edit an existing bootptab file and do a Save instead of a Save As, then the filename should stay the same.

---



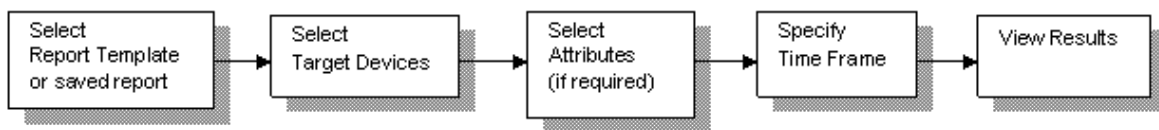
# Capacity Planning Reports

---

Inventory Manager's Capacity Planning tool lets you quickly prepare valuable network inventory planning reports. The tool provides a set of report templates that you can tailor to meet your specific planning needs. Reports are generated based on your selection of a report template and the associated parameters used to define the report. Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification email.

The Capacity Planning tool takes you step-by-step through the process of creating a report. As you move through the steps, the tool's left panel shows you a summary of your settings. You can click on the bold headings in the left panel to navigate backward or forward between steps allowing you to change report parameters. Specific parameters for the current step are defined in the right panel.

The flow chart below shows the sequence of windows that you will encounter when you create a report.



## Report Templates

Following is a summary of the different report templates Inventory Manager provides for your planning purposes. Each template is designed to answer a specific capacity planning question and lets you view report results organized into different categories. Click each template name below for a complete description of how to use the tool to create that report.

Report Template	Description
<a href="#">Used/Unused Ports Report</a>	Generate a report on your network front-panel port utilization. Quickly locate unused ports, and view port details such as port type, speed, media type and connector type.

---

<b>Report Template</b>	<b>Description</b>
<a href="#">Used/Unused Slots Report</a>	Generate a report on your chassis slot utilization to quickly locate unused slots. View results organized by chassis type and by individual chassis.
<a href="#">Field Replaceable Units (FRU) Report</a>	Generate a report on the field replaceable/upgradeable (FRU) components in your network devices. View descriptions and details on a variety of FRU types (such as power supplies, submodule, and ports) to help determine FRU usage.
<a href="#">Component Change Report</a>	Generate a report on the field replaceable/upgradeable (FRU) components in your network devices that have changed over time. Easily monitor changes made to your network and verify network upgrades.
<a href="#">Chassis Capacity Report</a>	Generate a report on the capacity and usage of certain chassis components such as submodules, power supplies, and control modules. View results organized by chassis type or for each individual chassis.
<a href="#">Submodule Capacity Report</a>	Generate a report on your network's submodule capacity and usage. Determine the number of submodule slots available on your network devices and the actual number of submodules that are installed. View a description of each of the installed submodules.

---

## Chassis Capacity Report

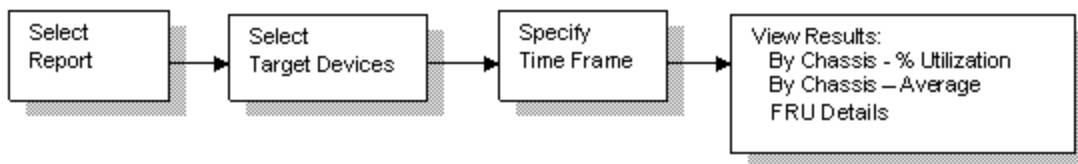
---

Use the Capacity Planning tool to generate a report on your network chassis utilization. The Show Details on Chassis Capacity and Utilization report provides valuable information on the capacity and usage of certain chassis components such as submodules, power supplies, and control modules. You can view report results organized by chassis type or for each individual chassis. In most cases, the report would be based on current data from your devices. However, there is the option to collect historical data if you would like to view a snapshot of your network's chassis usage at an earlier time.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

### Flow

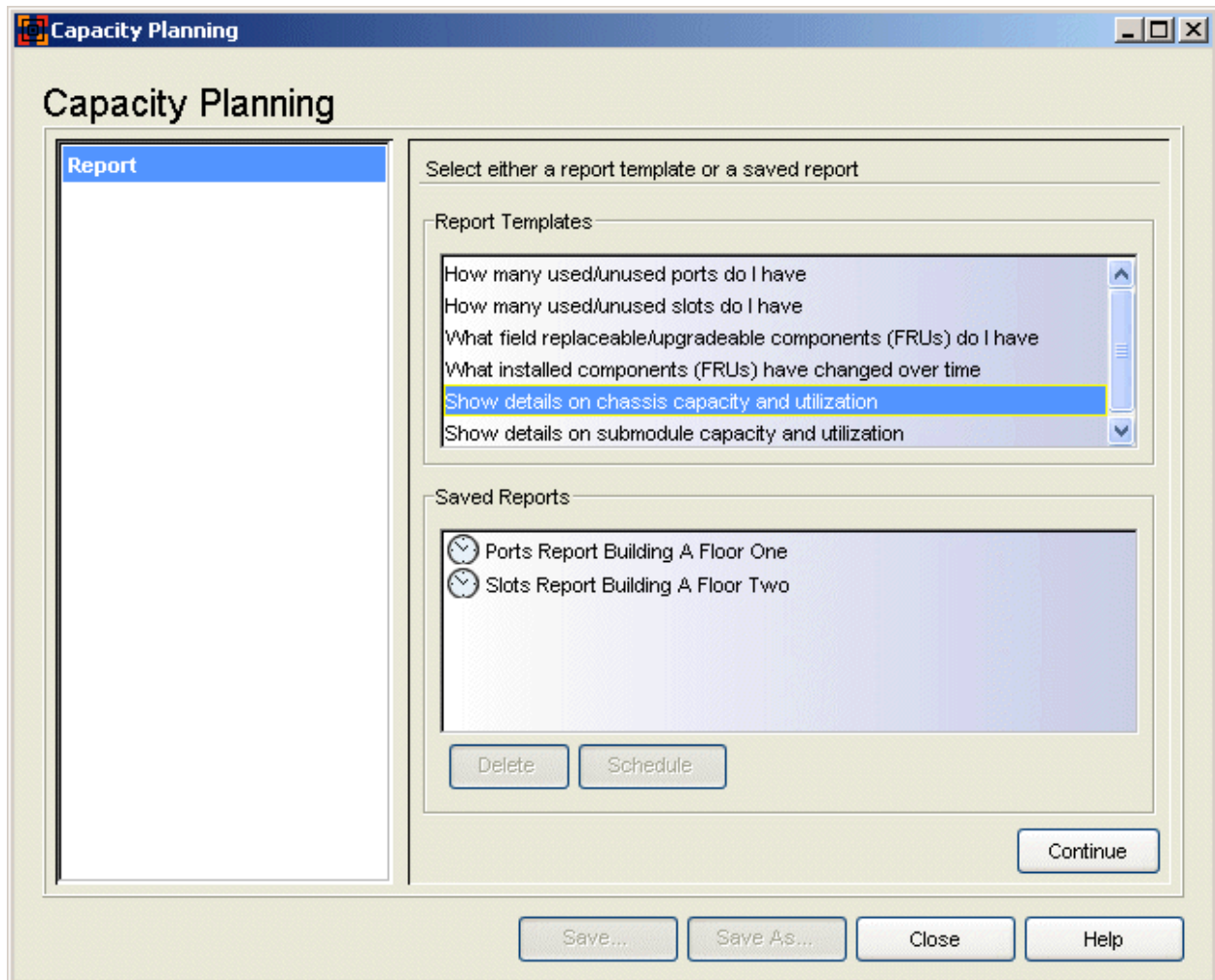
The flow chart below shows the sequence of windows that you will encounter when you create a Chassis Capacity report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



### Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your Chassis


Capacity report, select the "Show details on chassis capacity and utilization" report template.



### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon  indicates that a saved report has been scheduled. You can remove a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

### Delete Button

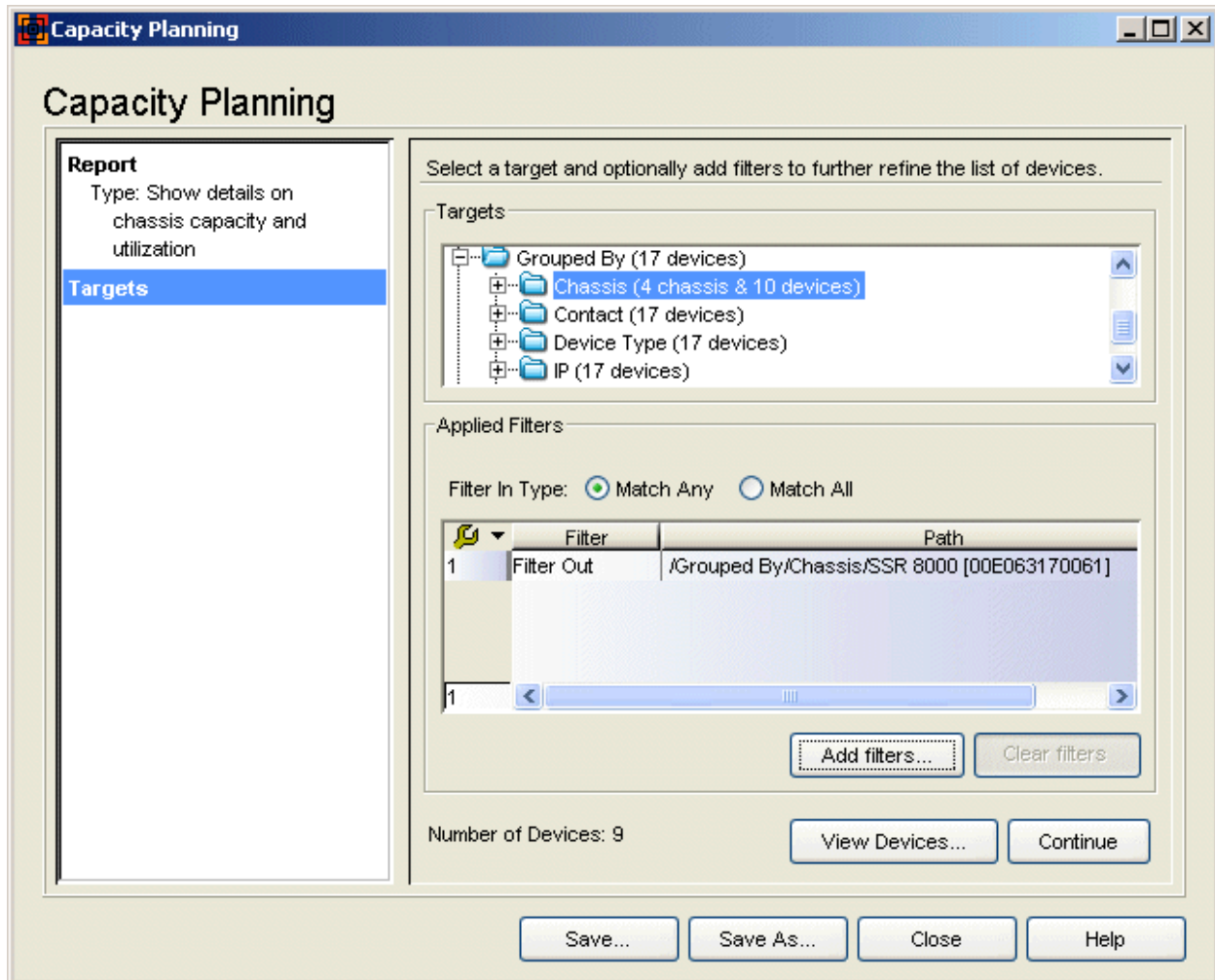
Deletes any report selected in the Saved Reports list.

### Schedule Button

When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.

## Select Targets Window

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Chassis device group, but filter out a single chassis you don't want included in the report. Or, you could target the Chassis device group, and filter in just one specific chassis type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.



## Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report. In most cases, you will want to target a group of chassis for this report. Devices that do not reside in a chassis will not generate any report results.

## Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

## Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Grouped

By device group and you filter in the 6C105 device group and the 6C107 device group, any device that is in the 6C105 **or** 6C107 device group will be included as a target.

- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have targeted the Grouped By device group and you filter in the Floor One device group and the Chassis device group, any device that is on Floor One **and** in the Chassis device group will be included as a target.

### Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

### Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

### Clear Filters Button

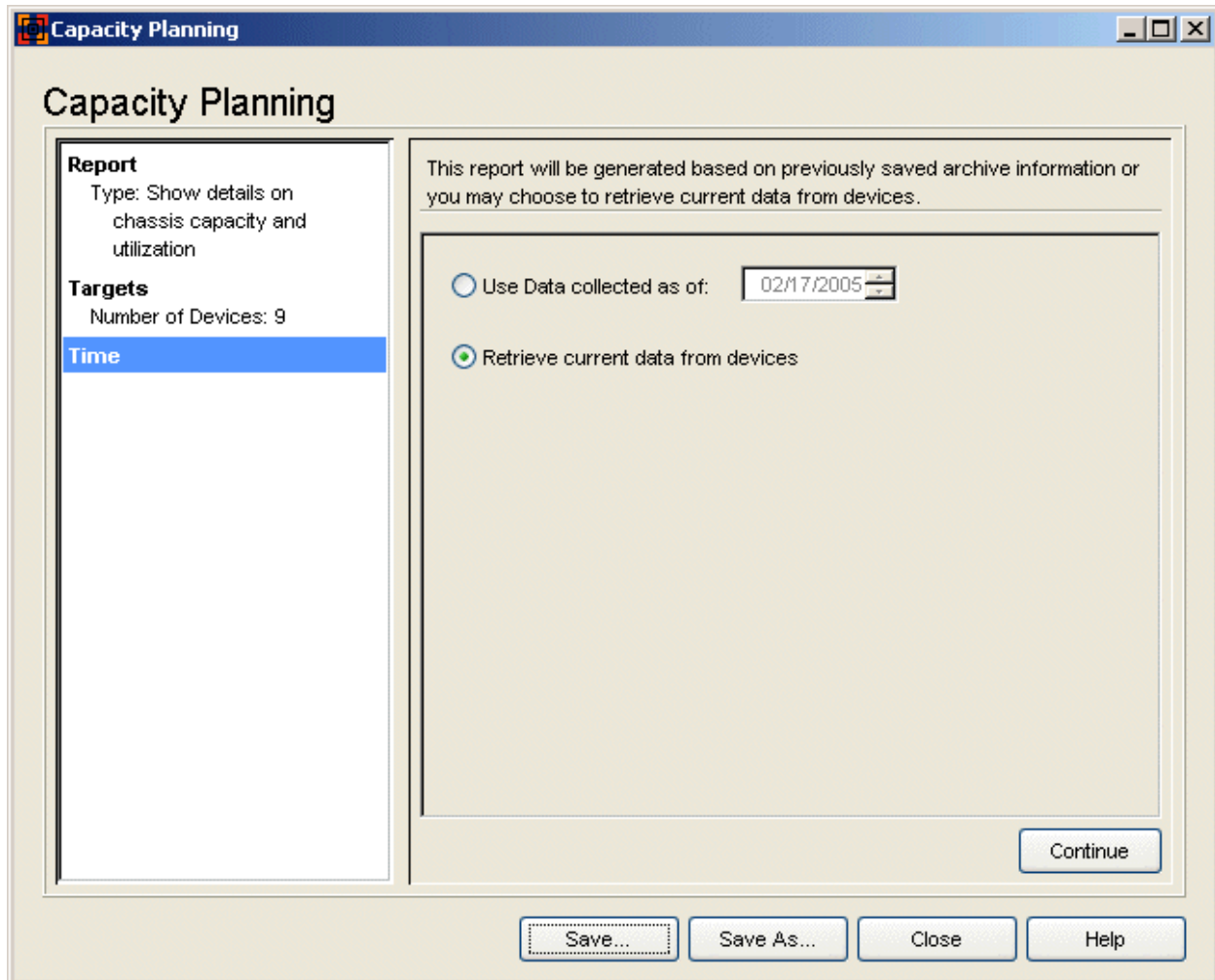
Deletes any filters selected in the Applied Filters list.

### View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Specify Time Window

Use this window to select a date from which report data will be gathered. In most cases, you will want to generate the report using current data. However, you can also generate a report based on historical data. In that case, the report will be generated using device data saved in the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used (see [How to Archive](#) for more information.)



### Use data collected as of

Report data will be collected based on the date selected here. Calculations are based on the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used. If there is no archive for a target device, that device will not be represented in the report results.

### Retrieve current data from devices

The report will use current data from the target devices. Because this requires the report to gather current data from the devices, extra time may be needed when results are calculated.



## Chassis Results Window

Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

- [Summary by Chassis \(% utilization\)](#) -- reports the percentage of chassis components that are installed, summarized by chassis type or by individual chassis.
- [Summary by Chassis \(average\)](#) -- reports the average of the number of chassis components that are installed, summarized by chassis type or by individual chassis.
- [FRU Details](#) -- reports detailed information on the field replaceable/upgradeable (FRU) chassis components, for each individual chassis.

Your selection in the tree determines the results displayed in the table. As you change your selection in the tree, the table is updated with the results for your specific selection. If you have targeted a device that does not reside in a chassis, that device will not be represented in the report results.

### *Chassis Results - Summary by Chassis (% utilization)*

The Summary by Chassis (% utilization) view provides data on the percentage of chassis components that are installed. For example, if a chassis has the capacity for two Control Modules but there is only one Control Module installed, the Control Module column in the results table will display 50%. You can view the report results summarized by chassis type, by individual chassis, or by individual device.

**Capacity Planning**

Report: Show details on chassis capacity and utilization

Display

Summary by Chassis ( % utilization )  Summary by Chassis ( average )  FRU Details

Type	Submodules	Control Mod...	Slots
1 6C105	33%	Unsupported	80%
2 GIGAswitch ...	Unsupported	50%	75%

9 devices selected, 9 with sufficient data

Buttons: Refresh, Export..., Save..., Save As..., Close, Help

## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a chassis group to see results summarized by chassis type, or select an individual chassis to see results for just that chassis. When you change your selection in the tree, the table is updated with the relevant information. If you select an individual device in the target device tree, the information displayed pertains to the chassis the device resides in, except for the Submodules column which reports information for the individual device.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive

used to obtain report results. Target devices that do not reside in chassis will be counted as having insufficient data.

## Table

The Summary by Chassis (% utilization) table displays data by chassis type or for an individual chassis. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device or the device does not reside in a chassis, that device will not be represented in the report results.

---

**NOTE:** Devices that do not support certain components will display "Unsupported" in the results table entry. If a chassis displays "Not Mapped" in its results table entry, it indicates that the device type is not in the Capacity Planning data file. If you encounter the "Not Mapped" entry, please contact Extreme Networks Support for an updated data file for these devices.

---

## Type

The chassis model number or hardware type.

## Submodules

The percentage of submodules installed (based on the installed modules) in the selected chassis type, chassis, or individual device.

## Control Modules

The percentage of control modules installed in the selected chassis type or chassis.

## Slots

The percentage of available slots being used in the selected chassis type or chassis.

## Fans

The percentage of fans installed in the selected chassis type or chassis.

## Power Supplies

The percentage of power supplies installed in the selected chassis type or chassis.

## Fabric Modules

The percentage of fabric modules installed in the selected chassis type or chassis.

## Chassis Results - Summary by Chassis (average)

The Summary by Chassis (average) view provides data on the average number of chassis components that are installed in your network chassis devices. Use this top-level information to quickly determine where to take a closer look using the FRU Details view.

The screenshot shows the 'Capacity Planning' application window. The title bar reads 'Capacity Planning'. The main window has a sidebar on the left with the following sections:

- Report**: Type: Show details on chassis capacity and utilization
- Targets**: Number of Devices: 9
- Time**: Retrieve Current Data
- Chassis Results** (highlighted)

The main area is titled 'Capacity Planning' and contains a report description: 'Report: Show details on chassis capacity and utilization'. Below this is a 'Display' section with three radio buttons: 'Summary by Chassis ( % utilization )', 'Summary by Chassis ( average )' (selected), and 'FRU Details'. The main content area is split into a tree view on the left and a table on the right.

The tree view shows a hierarchy starting with 'Chassis (3 chassis & ...)' which contains two '6C105 [00001D33]' and '6C105 [00001D99]' groups. Each group contains several IP addresses (12.22.120.77 through 12.22.120.81) and a 'GIGAswitch Route' group.

The table on the right has the following columns: 'Type', 'Submodules', 'Control Modules', and 'Slots'. It displays two rows of data:

Type	Submodules	Control Modules	Slots
6C105	1.5	Unsupported	4.0
GIGAswitch ...	Unsupported	1.0	6.0

At the bottom of the window, there is a status bar that says '9 devices selected, 9 with sufficient data'. Below this are buttons for 'Refresh' and 'Export...'. At the very bottom are buttons for 'Save...', 'Save As...', 'Close', and 'Help'.

### Display

Use these radio buttons to select how you would like the results data displayed.

### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table, however, this view is most useful when a chassis group is selected. If you select an individual device in the target device tree, the information displayed pertains to the chassis the device resides in, except for the Submodules column which reports information for the individual device.

**Device Count, Sufficient Data**

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results. Target devices that do not reside in chassis will be counted as having insufficient data.

**Table**

The Summary by Chassis (average) table displays data by chassis type or for an individual chassis, but the view is most useful at the chassis type level. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, or the device does not reside in a chassis, that device will not be represented in the report results.

**Type**

The chassis model number or hardware type.

**Submodules**

The average number of submodules installed in the selected chassis type.

**Control Modules**

The average number of control modules installed in the selected chassis type.

**Slots**

The average number of slots being used in the selected chassis type.

**Fans**

The average number of fans installed in the selected chassis type.

**Power Supplies**

The average number of power supplies installed in the selected chassis type.

**Fabric Modules**

The average number of fabric modules installed in the selected chassis type.

***Chassis Results - FRU Details***

The FRU Details view gives you detailed information on the field replaceable/upgradeable (FRU) chassis components for each individual chassis.

Capacity Planning

Report: Show details on chassis capacity and utilization

Display

Summary by Chassis ( % utilization )  Summary by Chassis ( average )  FRU Details

Chassis	IP Address	Type	Submodule ...
1 6C105 [0000...	10.20.150.117	6C105	4
2 6C105 [0000...	10.20.150.78	6C105	5
3 GIGAswitch ...	10.20.150.1	GIGAswitch ...	Unsupported

9 devices selected, 9 with sufficient data

Refresh Export... Save... Save As... Close Help

## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a chassis group to see results for all the chassis in the group, or select an individual chassis to see results for just that chassis. When you change your selection in the tree, the table is updated with the relevant information. If you select an individual device in the target device tree, the information displayed pertains to the chassis the device resides in, except for the Submodule Capacity and Submodules Installed columns which report information for the individual device.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical

data, a device is counted as having sufficient data if there is one archive used to obtain report results. Target devices that do not reside in chassis will be counted as having insufficient data.

## Table

The FRU Details table displays data for each individual chassis. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, or the device does not reside in a chassis, that device will not be represented in the report results.

---

**NOTE:** Devices that do not support certain components will display "Unsupported" in the results table entry. If a chassis displays "Not Mapped" in its results table entry, it indicates that the device type is not in the Capacity Planning data file. If you encounter the "Not Mapped" entry, please contact Extreme Networks Support for an updated data file for these devices.

---

## Chassis

The chassis type followed by the ID assigned to the chassis. This is usually a serial number or MAC address, depending on the chassis type.

## IP Address

The IP address of the chassis or one of the devices in the chassis.

## Type

The chassis model number or hardware type.

## Submodule Capacity

The submodule capacity (based on the installed modules) for the chassis. If you have an individual device selected in the Target Device Tree, this column reports information for just that specific device.

## Submodules Installed

The number of submodules installed in the chassis. If you have an individual device selected in the Target Device Tree, this column reports information for just that specific device.

## CM Capacity

The control module (CM) capacity for the chassis.

## CMs Installed

The number of control modules (CM) installed in the chassis.

**Slot Capacity**

The slot capacity for the chassis.

**Slots Installed**

The number of modules installed in the chassis.

**Fan Capacity**

The fan capacity for the chassis.

**Fans Installed**

The number of fans installed in the chassis.

**Power Supply Capacity**

The power supply capacity for the chassis.

**Power Supplies Installed**

The number of power supplies installed in the chassis.

**Fabric Module Capacity**

The fabric module capacity for the chassis.

**Fabric Modules Installed**

The number of fabric modules installed in the chassis.

**Abort/Refresh Button**

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time window](#), clicking Refresh allows you to update your report results with the latest data from your devices.

**Export Button**

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

**Save/Save As Button**

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.



## Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)

## Component Change Report

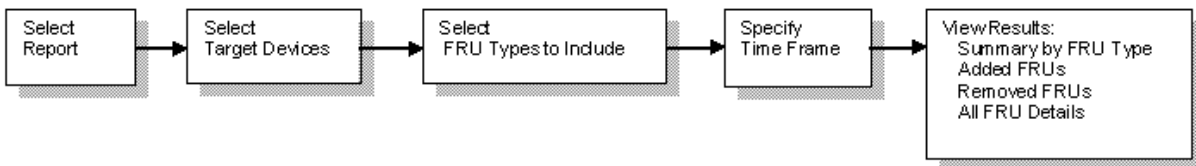
---

Use the Capacity Planning tool to generate a report on field replaceable/upgradeable components (FRUs) in your network devices that have changed over time. Using the Component Change report, you can easily monitor changes made to your network and verify network upgrades.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

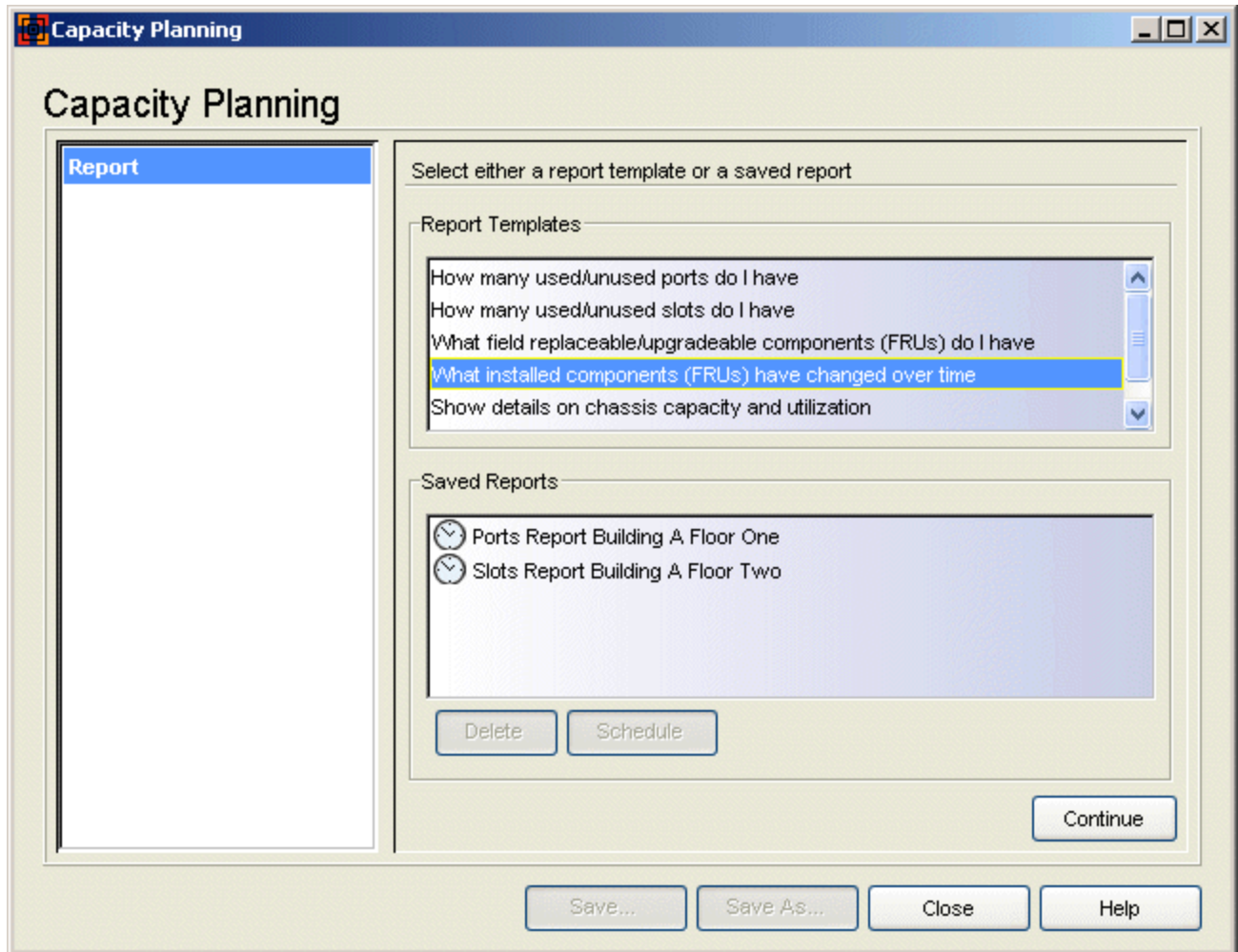
### Flow

The flow chart below shows the sequence of windows that you will encounter when you create a Component Change report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



### Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your Component Change report, select the "What installed components (FRUs) have changed over time" report template.



### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon 🕒 indicates that a saved report has been scheduled. You can remove a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

### Delete Button

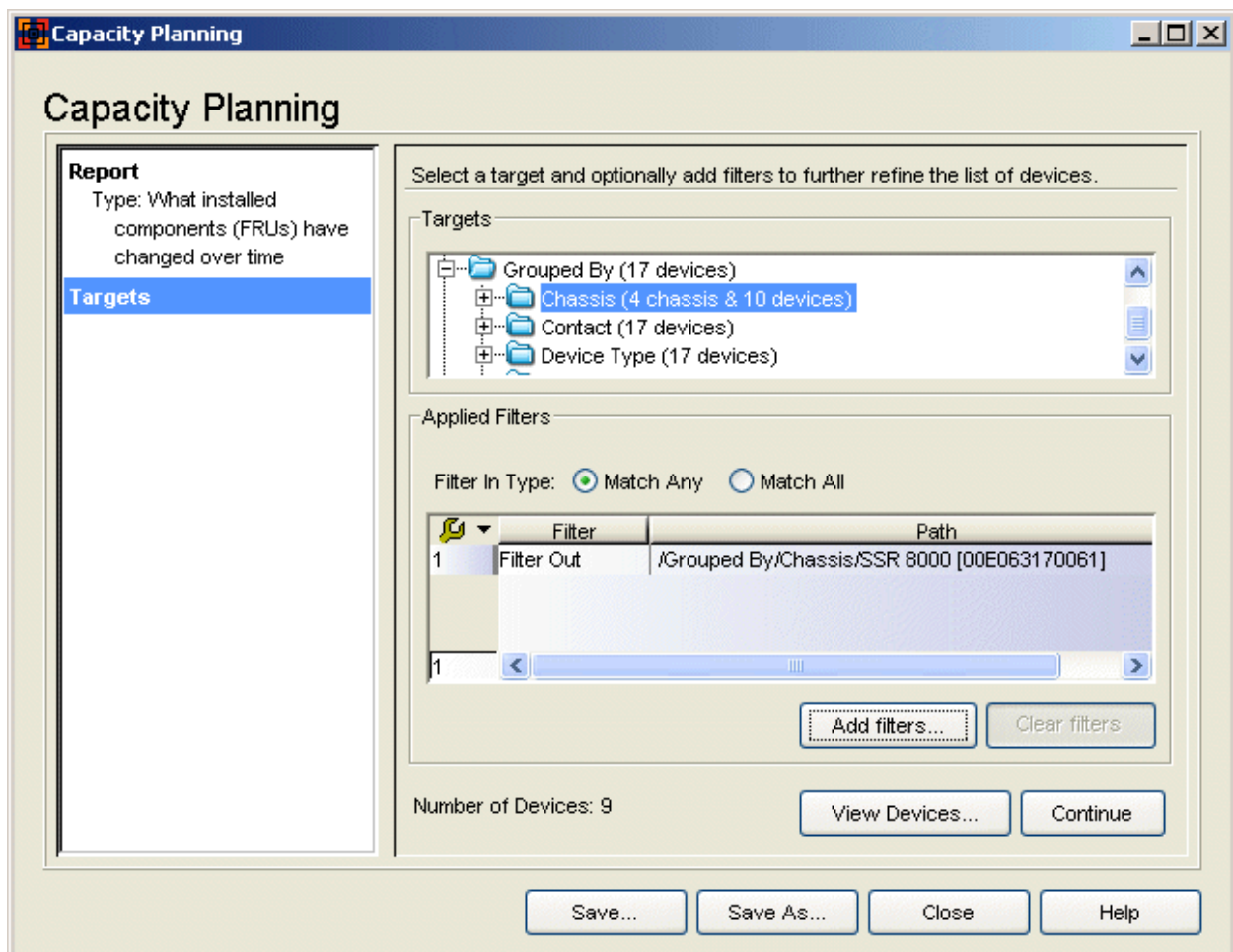
Deletes any report selected in the Saved Reports list.

## Schedule Button

When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.

## Select Targets Window

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Chassis device group, but filter out a single chassis you don't want included in the report. Or, you could target the Chassis device group, and filter in just one specific chassis type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.



## Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report.

## Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

## Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Grouped By device group and you filter in the 6C105 device group and the 6C107 device group, any device that is in the 6C105 **or** 6C107 device group will be included as a target.
- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have targeted the Grouped By device group and you filter in the Floor One device group and the Chassis device group, any device that is on Floor One **and** in the Chassis device group will be included as a target.

## Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

## Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

## Clear Filters Button

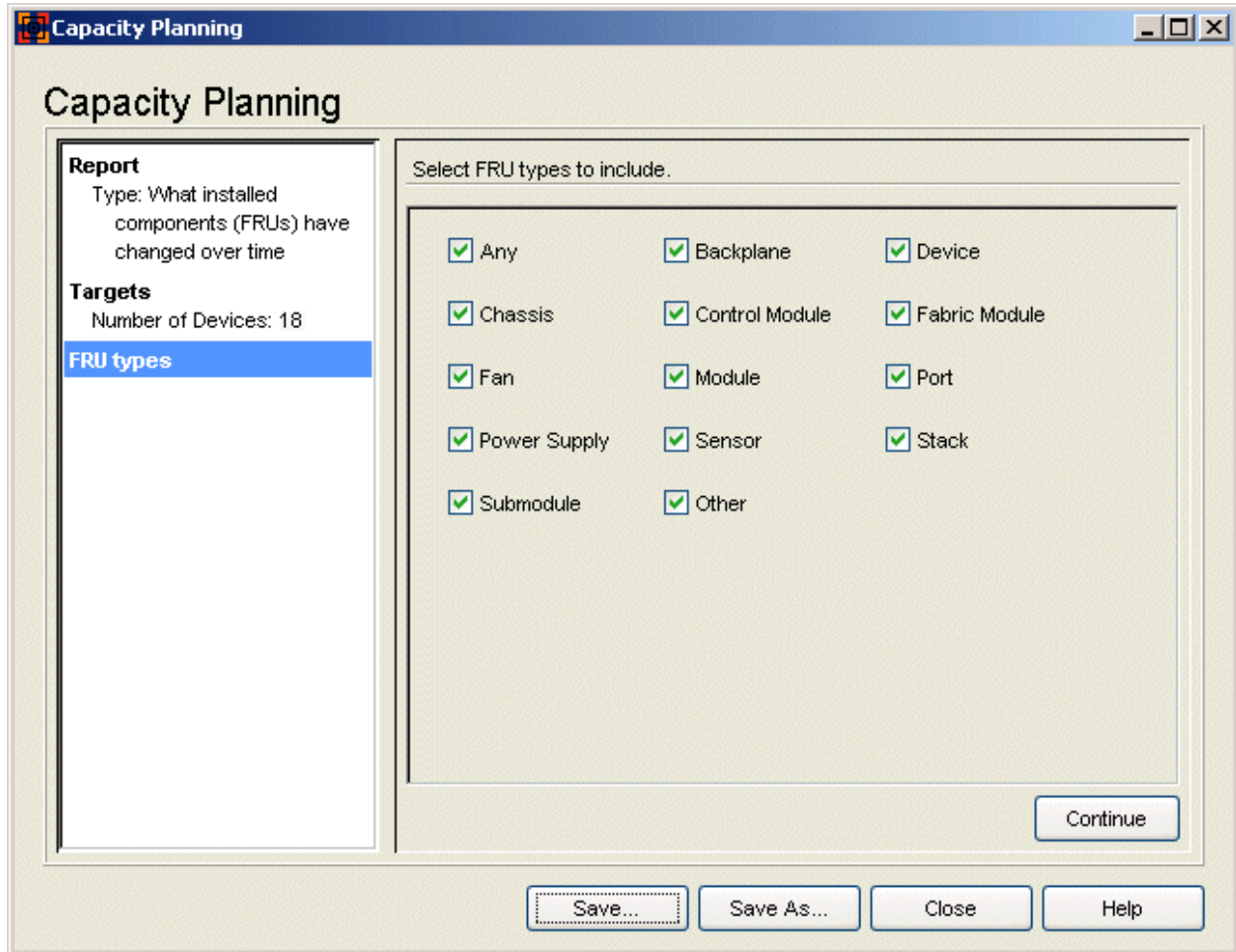
Deletes any filters selected in the Applied Filters list.

## View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Select FRU Types Window

Use the checkboxes in this window to select the specific components (FRU types) for your report. Select the "Any" checkbox for a report on all the listed types, or select individual types to narrow down the focus of your report.



### FRU Types to Include

Use the checkboxes in this window to select specific FRU types for your report. Select the "Any" checkbox for a report on all listed FRU types, or select individual FRU types of interest. Select the "Other" checkbox if you wish to include data on FRU types other than the ones listed here. For the purposes of this report, the FRU types are defined as follows:

- Backplane -- a device for aggregating and forwarding networking traffic, such as a shared backplane in a modular Ethernet switch. A backplane may be reported as a single physical entity, even if it is actually implemented as multiple discrete physical components within a chassis or stack.
- Device -- a manageable networking device.
- Chassis -- an overall container for networking equipment.

- Control Module -- the module in a chassis that is responsible for maintaining route table and bridge table information, as well SNMP management and system housekeeping functionality.
- Fabric Module -- a switching fabric module that provides direct communication between fabric-enabled line cards in a chassis.
- Fan -- a fan or other heat-reduction component.
- Module -- a self-contained subsystem, such as a plugin card, daughter-card, or DFE module.
- Port -- a media connector added to a module, submodule, or standalone device.
- Power Supply -- a power-supplying component.
- Sensor -- a sensor such as a temperature sensor within a router chassis.
- Stack -- a stack of multiple chassis.
- Submodule -- an expansion module installed on an existing chassis module or standalone device that adds ports to the existing device. This should not be confused with a Port Interface Module (PIM), which adds media connectors to a module, submodule, or standalone device. For example, the 6E129-26 has two PIM slots, which would not be included in the definition of a submodule. These PIMs would be reported as port FRUs.

## Specify Time Window

Use this window to select a time period from which report data will be gathered. The report will be generated using device data saved in archive operations performed during the specified time period. Calculations are based on the first and last archives (data samples) in the time period selected, not on all archive information in the specified time frame. The archive operations must be configured to archive capacity planning data (see [How to Archive](#) for more information.) You can also select to use current data from devices as one of your data samples, in which case the report will use current data from the target devices, instead of the last archive in the time period.

**Capacity Planning**

**Report**  
Type: What installed components (FRUs) have changed over time

**Targets**  
Number of Devices: 18

**FRU types**  
Any

**Time Frame**

Two data samples are required to run this report. If you choose not to retrieve current data from devices, previously saved archives will be used to generate the report. Select a predefined time period or a custom time period.

For the period  Custom time period

Start: 02/01/2005  
End: 02/17/2005

Include all dates  
Current Day  
Current Week  
Current month  
Current year

Retrieve current data from devices

Continue

Save... Save As... Close Help

### For the Period

Select a time period for your report. The report is generated using device data saved in archive operations performed on the targeted devices during the specified time period. Report information is collected from the first and last archives (data samples) in the selected time period, not from every archive in the time period.

- Include all dates -- The report will use the first and last archives that exist for your target devices.
- Current Day -- The report will use the first and last archives from the current day.
- Current Week -- The report will use the first and last archives from the current week.
- Current month -- The report will use the first and last archives from the current month.



- Current year -- The report will use the first and last archives from the current year.
- Last month -- The report will use the first and last archives from the previous month.
- Last 3 months -- The report will use the first and last archives from the previous three months, not including the current month.
- Last 6 months -- The report will use the first and last archives from the previous six months, not including the current month.
- Last 12 months -- The report will use the first and last archives from the previous 12 months, not including the current month.

---

**TIP:** When you make a "For the Period" time selection, the "Custom time period" Start and End dates are automatically filled in with the selected dates. You can then switch to the Custom time period option and refine your time period to the exact dates you would like. For example, you could select the time period "Last 6 months", and then switch to the Custom time period option and change the End date to the current date. This would allow you to generate a report using data from the current month and the last six months.

---

### Retrieve current data from devices

This checkbox is available when you select a time period where the End date is the current date. When the checkbox is selected, the report will use current data from the target devices, instead of the last archive in the time period. Because this requires the report to gather current data from the devices, extra time may be needed while report results are calculated.

### Custom Time Period

Specify a custom time period for your report. Report information will be collected from the first and last archive (data samples) in the selected time period, not from every archive in the time period.

## Results Window

Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

- [Summary by FRU Type](#) -- lists all the FRU components for your target devices, organized by FRU type.
- [Added FRUs](#) -- lists all the FRU components that have been added during the specified time frame.

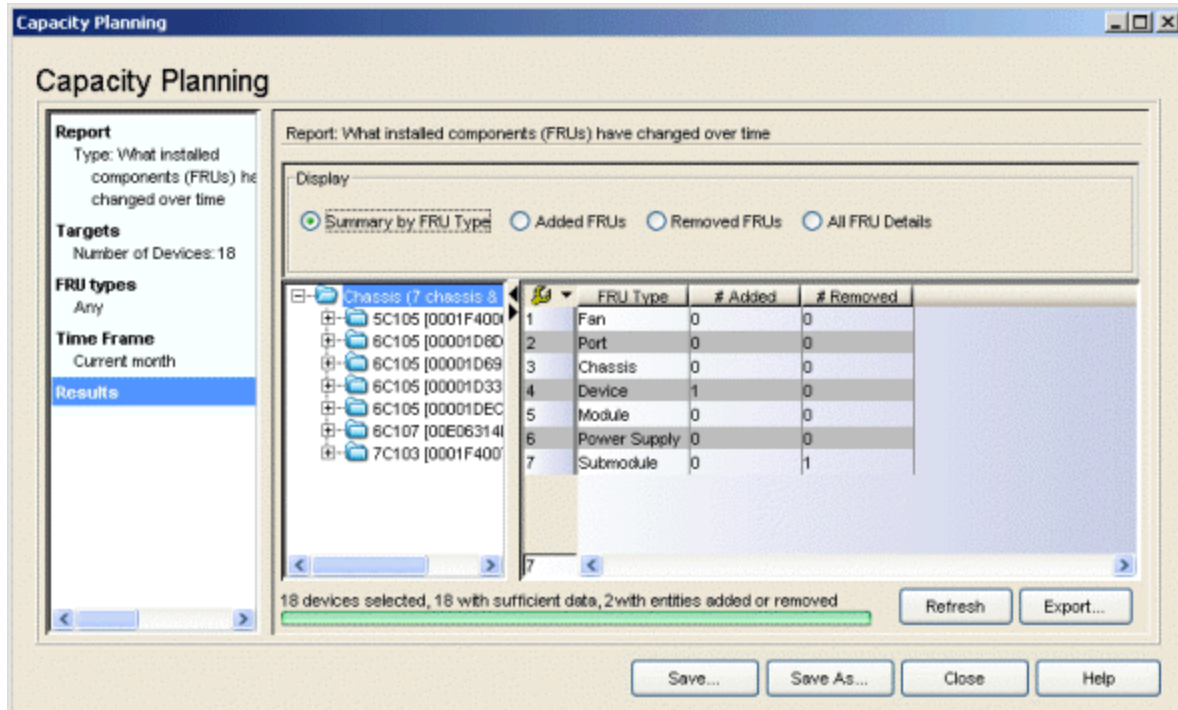
- [Removed FRUs](#) -- lists all the FRU components that have been removed during the specified time frame.
- [All FRU Details](#) -- lists the details for each individual FRU component included in the report.

In addition, your selection in the tree determines the results displayed in the table. For example, you can select a device group and view report data for that group. Then, you can expand the group and view data for a specific device. As you change your selection in the tree, the table is updated with the results for your specific selection.

### *Results - Summary By FRU Type*

The Summary by FRU Type view displays report data organized by FRU type, providing an easy way to view top-level information and quickly determine where to take a closer look. Your selections in the [Select FRU Types window](#) determine what FRU types are reported on.

- 
- NOTES:**
- FRU types are grouped based on individual FRU descriptions. For example, you may see several entries for the FRU type "Module", based on the different module descriptions.
  - Each device is considered a FRU and will have a row in the table.
  - Individual devices that reside in a chassis will report the power supplies and fans for that chassis.
  - Ports that reside on a submodule may be reported as both Ports and Submodule.
-



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see FRU type results summarized for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. This area also reports the number of devices with FRU components that have been added or removed.

## Table

The Summary by FRU Type table displays FRU data for the selected device group or for the individual devices contained in the group. The report is generated based on the first and last data samples in the time period selected.

Devices with no data samples or only one data sample, will not be represented in the report results.

### FRU Type

The type of FRU. Your selections in the [Select FRU Types window](#) determine the FRU types included in the report.

### # Added

The number of FRU components that have been added during the specified time frame.

### # Removed

The number of FRU components that have been removed during the specified time frame.

### Results - Added FRUs

The Added FRUs view provides information on FRU components that have been added during the specified time frame. Your selections in the [Select FRU Types window](#) determine the components included in the report. Depending on your selection in the tree, you can see details for Added FRUs on all the devices in a group or just on an individual device.

The screenshot shows the 'Capacity Planning' application window. The title bar reads 'Capacity Planning'. The main window has a sidebar on the left with the following sections:

- Report**: Type: What installed components (FRUs) have changed over time
- Targets**: Number of Devices: 18
- FRU types**: Any
- Time Frame**: Current month
- Results**: (Selected)

The main content area is titled 'Report: What installed components (FRUs) have changed over time'. It features a 'Display' section with radio buttons for 'Summary by FRU Type', 'Added FRUs' (selected), 'Removed FRUs', and 'All FRU Details'. Below this is a tree view showing a hierarchy of chassis components:

- Chassis (7 chassis & ...)
  - 5C105 [0001F400]
  - 6C105 [00001D8D]
  - 6C105 [00001D69]
  - 6C105 [00001D33]
  - 6C105 [00001DEC]
  - 6C107 [00E06314]
  - 7C103 [0001F400]

The table below the tree view displays the following data:

	IP Address	FRU Name	FRU Type	Description
1	10.20.77.33	Matrix N7 Platinum	Device	Enterasys Networks, ...

At the bottom of the window, a status bar indicates '18 devices selected, 18 with sufficient data, 2 with entities added or removed'. There are buttons for 'Refresh' and 'Export...'. At the very bottom, there are buttons for 'Save...', 'Save As...', 'Close', and 'Help'.

### Display

Use these radio buttons to select how you would like the results data displayed.

### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see Added FRUs for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. This area also reports the number of devices with FRU components that have been added or removed.

### Table

The Added FRUs table displays FRU data for the selected device group or for the individual devices contained in the group. The report is generated based on the first and last data samples in the time period selected. Devices with no data samples or only one data sample, will not be represented in the report results.

### IP Address

The IP address of the device reporting the added FRU component.

### FRU Name

The specific name of the FRU component that was added.

### FRU Type

The type of FRU that was added.

### Description

A description of the FRU component that was added.

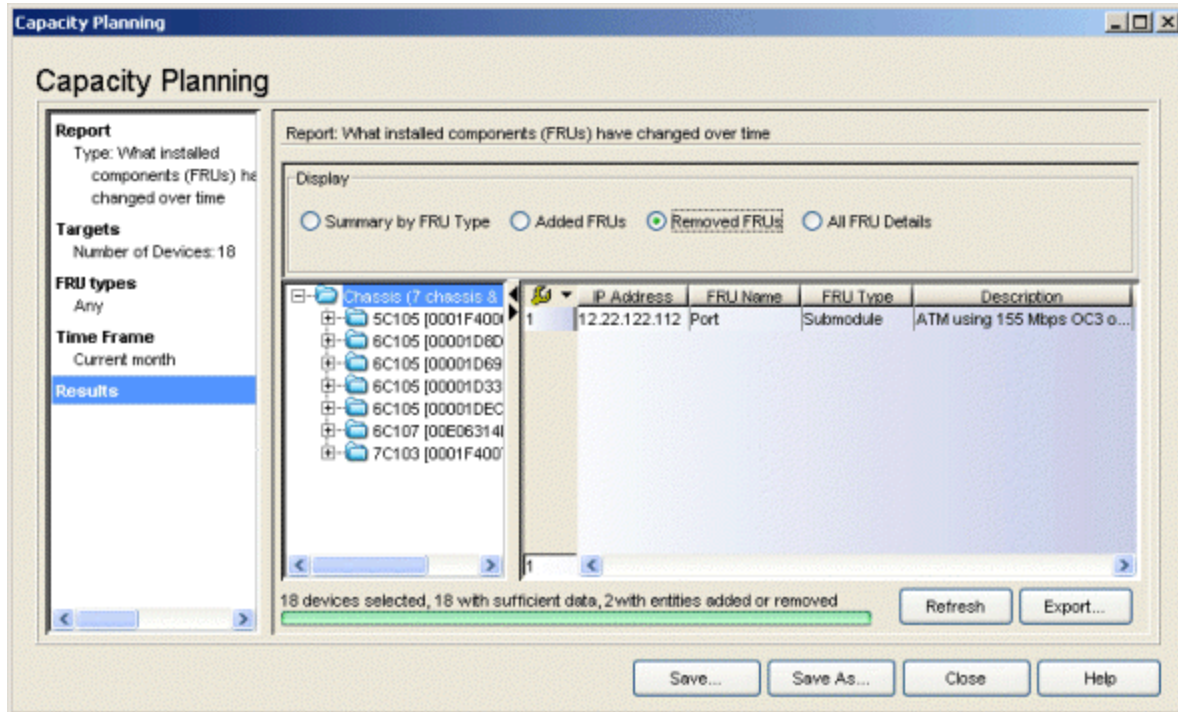
### Serial Number

A unique number assigned to the module or component by the manufacturer.

### *Results - Removed FRUs*

The Removed FRUs view provides information on FRU components that have been removed during the specified time frame. Your selections in the [Select FRU](#)

[Types window](#) determine the components included in the report. Depending on your selection in the tree, you can see details for Removed FRUs on all the devices in a group or just on an individual device.



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see Removed FRUs for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. This area also reports the number of devices with FRU components that have been added or removed.

## Table

The Removed FRUs table displays FRU data for the selected device group or for the individual devices contained in the group. The report is generated based on the first and last data samples in the time period selected. Devices with no data samples or only one data sample, will not be represented in the report results.

### IP Address

The IP address of the device reporting the removed FRU component.

### FRU Name

The specific name of the FRU component that was removed.

### FRU Type

The type of FRU that was removed.

### Description

A description of the FRU component that was removed.

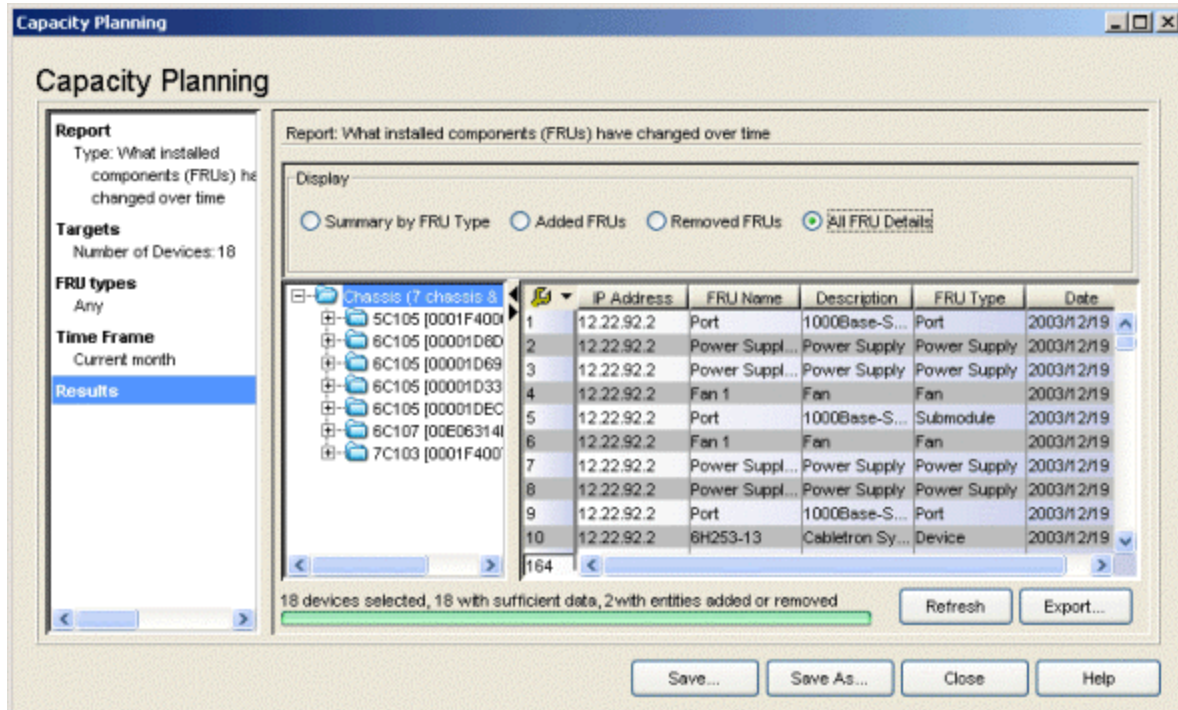
### Serial Number

A unique number assigned to the module or component by the manufacturer.

## *FRU Results - All FRU Details*

The FRU Details view provides information on the individual FRU components installed on your target devices. Your selections in the [Select FRU Types window](#) determine what components are included in the report. The report is generated based on the first and last data samples in the time period selected, resulting in two entries per FRU component (one for each data sample used.) Depending on your selection in the tree, you can see details for FRUs installed on all the devices in a group or just on an individual device.

- 
- NOTES:**
- Each device is considered a FRU and will have an entry in the table for each data sample.
  - Each individual device that resides in a chassis reports the power supplies and fans for that chassis. So, if your report includes a chassis, there will be an entry for power supplies and fans reported by each device in the chassis. For example, if you have four devices in a chassis, each device will report the two power supplies in the chassis, resulting in eight rows of power supplies in the table for that one chassis for each data sample. Use the IP Address column in the report to verify that each device in the chassis is reporting the same information, and that there are actually only two power supplies in the chassis.
-



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see All FRU Details for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. This area also reports the number of devices with FRU components that have been added or removed.

## Table

The All FRU Details table displays information for each FRU component included in the report. The report is generated based on the first and last data samples in the time period selected which means that there will be two entries



per FRU component, one for each data sample used. Devices with no data samples or only one data sample, will not be represented in the report results.

**IP Address**

The IP address of the device reporting the FRU component.

**FRU Name**

The specific name of the FRU component.

**Description**

A description of the FRU component.

**FRU Type**

The type of FRU.

**Serial Number**

A unique number assigned to the module or component by the manufacturer.

**Date**

The date and time the report data was generated using current data, or the date and time of the archive used to generate the report information. There will be two table entries per FRU component, one for each data sample used.

**Abort/Refresh Button**

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time Frame window](#), clicking Refresh allows you to update your report results with the latest data from your devices. In addition, if you have selected a current time frame for your report, and a new archive is saved after your report results are generated, clicking Refresh will regenerate your results using the new archive data.

**Export Button**

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

**Save/Save As Button**

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox

to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.

---

## Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)

## Field Replaceable Unit (FRU) Report

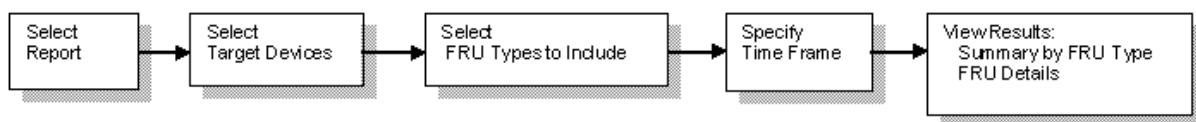
---

Use the Capacity Planning tool to generate a report on field replaceable/upgradeable components (FRUs) in your network devices. The FRU report provides valuable inventory information to help you plan your network needs. For example, you can generate a report on power supplies and control modules, to help determine how well your network devices are taking advantage of redundancy capabilities. In most cases, the report would be based on current data from your devices. However, there is the option to collect historical data if you would like to view a snapshot of your network's FRU components at an earlier time.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

### Flow

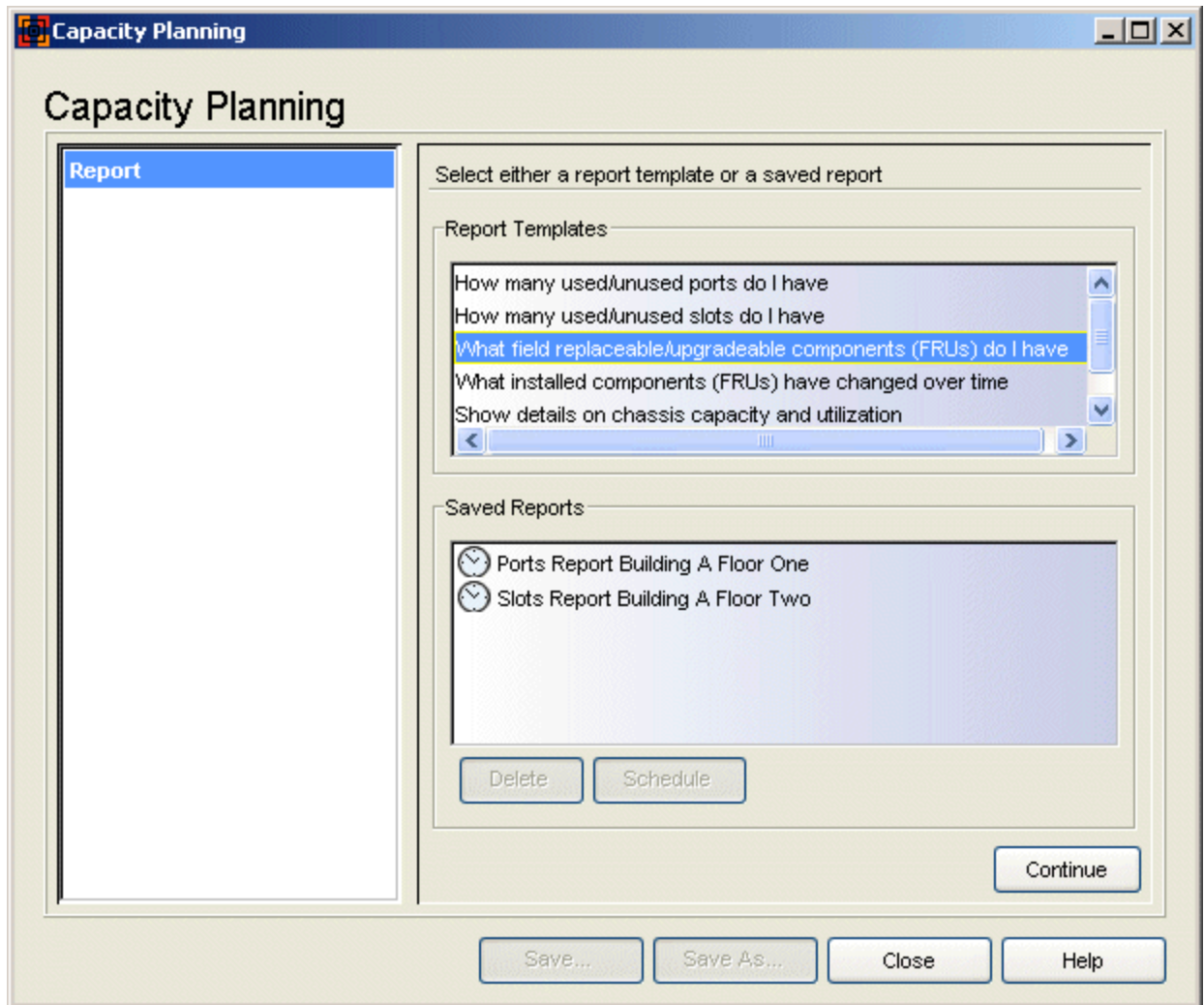
The flow chart below shows the sequence of windows that you will encounter when you create a FRU report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



### Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your FRU

report, select the "What field replaceable/upgradeable components (FRUs) do I have" report template.



### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon 🕒 indicates that a saved report has been scheduled. You can remove

a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

#### **Delete Button**

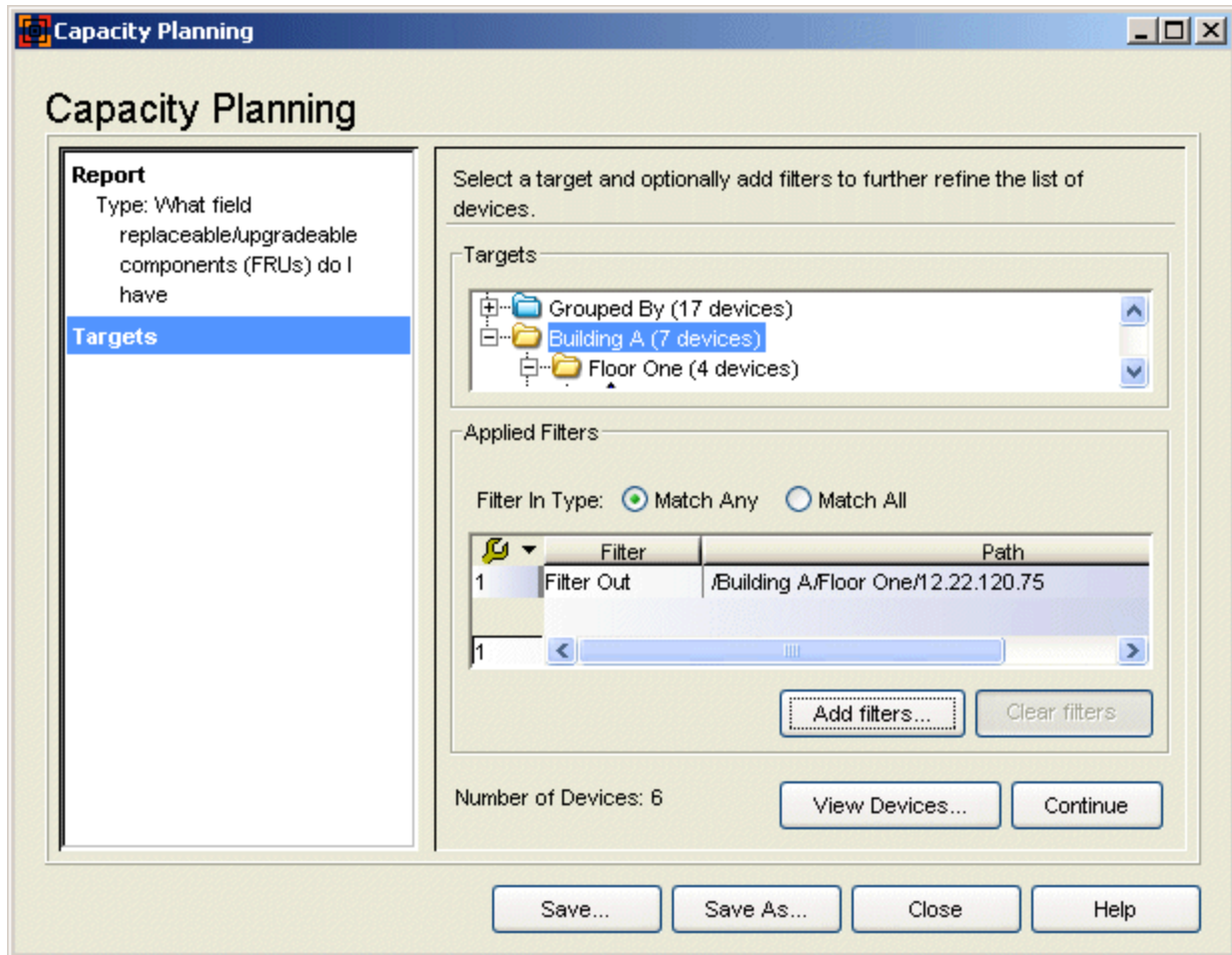
Deletes any report selected in the Saved Reports list.

#### **Schedule Button**

When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.

## **Select Targets Window**

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Floor One device group, but filter out a single device you don't want included in the report. Or, you could target the Building A device group, and filter in just one specific device type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.



## Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report.

## Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

## Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Building A device group and you filter in Floor One devices and E7 devices, any device in Building A that is on Floor One **or** is an E7 device will be included as a target.

- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have selected the Building A device group and you filter in Floor One devices and E7 devices, a Building A device would have to be on Floor One **and** be an E7 device to be included as a target.

#### Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

#### Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

#### Clear Filters Button

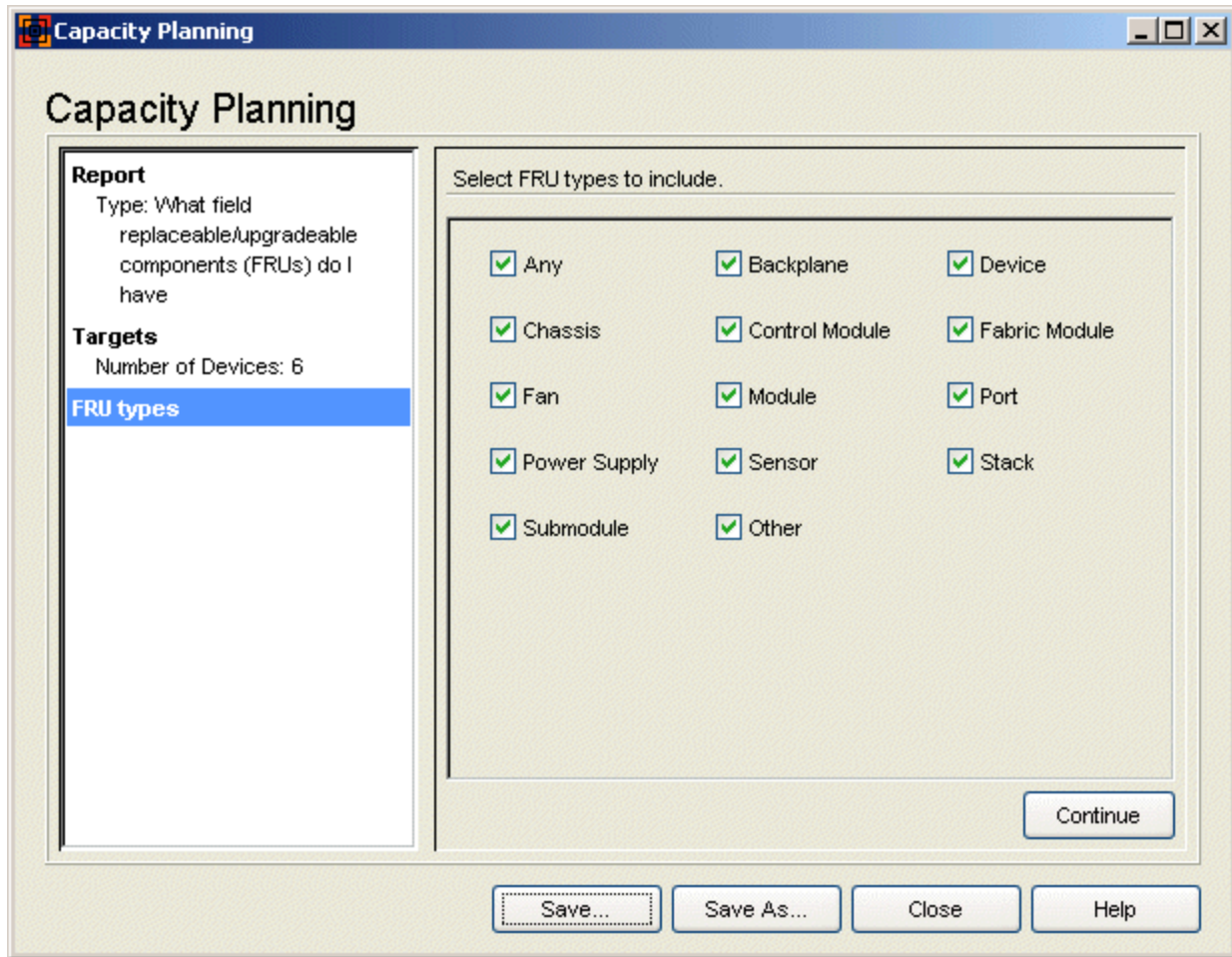
Deletes any filters selected in the Applied Filters list.

#### View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Select FRU Types Window

Use the checkboxes in this window to select specific FRU types for your report. Select the "Any" checkbox for a report on all the listed types, or select individual types to narrow down the focus of your report.



### FRU Types to Include

Use the checkboxes in this window to select specific FRU types for your report. Select the "Any" checkbox for a report on all listed FRU types, or select individual FRU types of interest. Select the "Other" checkbox if you wish to include data on FRU types other than the ones listed here. For the purposes of this report, the FRU types are defined as follows:

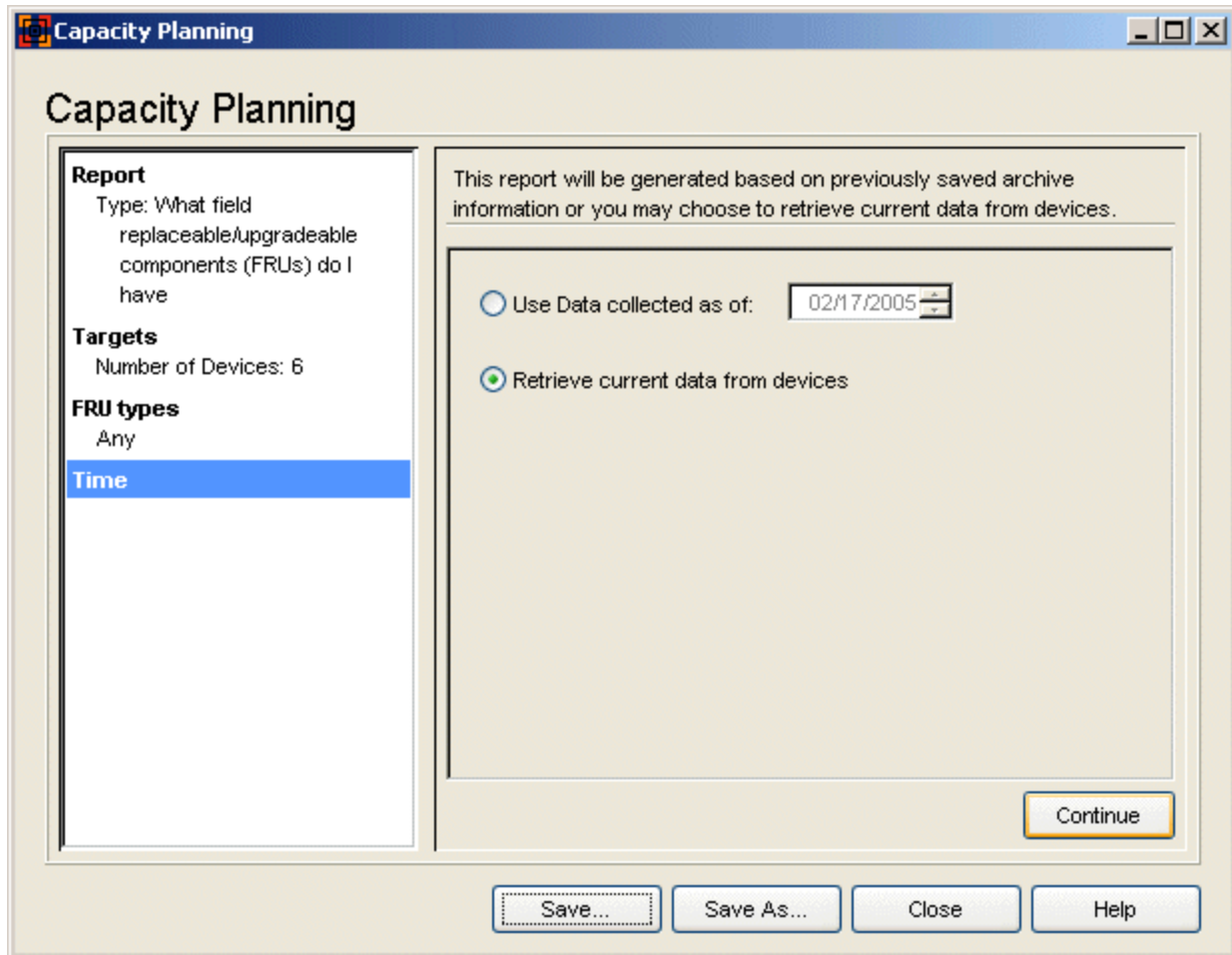
- Backplane -- a device for aggregating and forwarding networking traffic, such as a shared backplane in a modular Ethernet switch. A backplane may be reported as a single physical entity, even if it is actually implemented as multiple discrete physical components within a chassis or stack.
- Device -- a manageable networking device.
- Chassis -- an overall container for networking equipment.



- Control Module -- the module in a chassis that is responsible for maintaining route table and bridge table information, as well SNMP management and system housekeeping functionality.
- Fabric Module -- a switching fabric module that provides direct communication between fabric-enabled line cards in a chassis.
- Fan -- a fan or other heat-reduction component.
- Module -- a self-contained subsystem, such as a plugin card, daughter-card or DFE module.
- Port -- a media connector added to a module, submodule, or standalone device.
- Power Supply -- a power-supplying component.
- Sensor -- a sensor such as a temperature sensor within a router chassis.
- Stack -- a stack of multiple chassis.
- Submodule -- an expansion module installed on an existing chassis module or standalone device that adds ports to the existing device. This should not be confused with a Port Interface Module (PIM), which adds media connectors to a module, submodule, or standalone device. For example, the 6E129-26 has two PIM slots, which would not be included in the definition of a submodule. These PIMs would be reported as port FRUs.

## Specify Time Window

Use this window to select a date from which report data will be gathered. In most cases, you will want to generate the report using current data. However, you can also generate a report based on historical data. In that case, the report will be generated using device data saved in the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used (see [How to Archive](#) for more information.)



### Use data collected as of

Report data will be collected based on the date selected here. Calculations are based on the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used. If there is no archive for a target device, that device will not be represented in the report results.

### Retrieve current data from devices

The report will use current data from the target devices. Because this requires the report to gather current data from the devices, extra time may be needed when results are calculated.

## FRU Results Window

Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

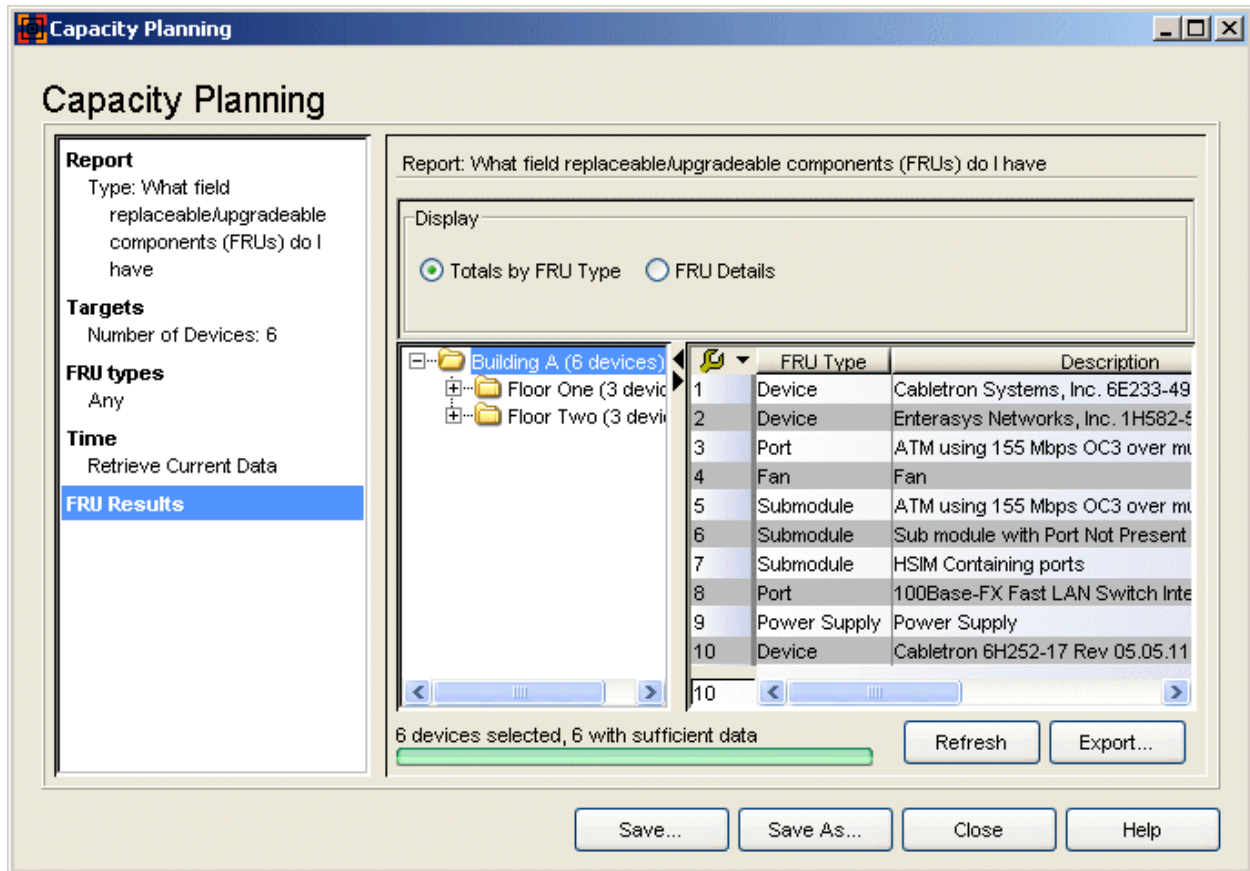
- [Totals by FRU Type](#) -- displays the report results organized by totals based on FRU type.
- [FRU Details](#) -- lists the details for each individual FRU component included in the report.

In addition, your selection in the tree determines the results displayed in the table. For example, you can select a device group and view report data for that group. Then, you can expand the group and view data for a specific device. As you change your selection in the tree, the table is updated with the results for your specific selection.

### *FRU Results - Totals By FRU Type*

The Totals by FRU Type view reports the total number of FRUs for each FRU type. Your selections in the [Select FRU Types window](#) determine what FRU types are reported on. Depending on your selection in the tree, you can see report results summarized for all the devices in a group, or for an individual device.

- 
- NOTES:**
- FRU types are grouped based on individual FRU descriptions. For example, you may see several entries for the FRU type "Module", based on the different module descriptions.
  - Each device is considered a FRU and will have a row in the table.
  - Individual devices that reside in a chassis will report the power supplies and fans for that chassis.
  - Ports that reside on a submodule may be reported as both Ports and Submodule.
-



### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see FRU type results summarized for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

### Table

The Totals by FRU Type table displays FRU data for all the devices in a group, or for an individual device. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the

report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

**FRU Type**

The type of FRU. Your selections in the [Select FRU Types window](#) determine the FRU types included in the report.

**Description**

A description of the FRU component.

**FRU Name**

The specific name of the FRU component.

**Total Installed**

The total number of FRUs of that type/description installed in the selected device group or the individual device.

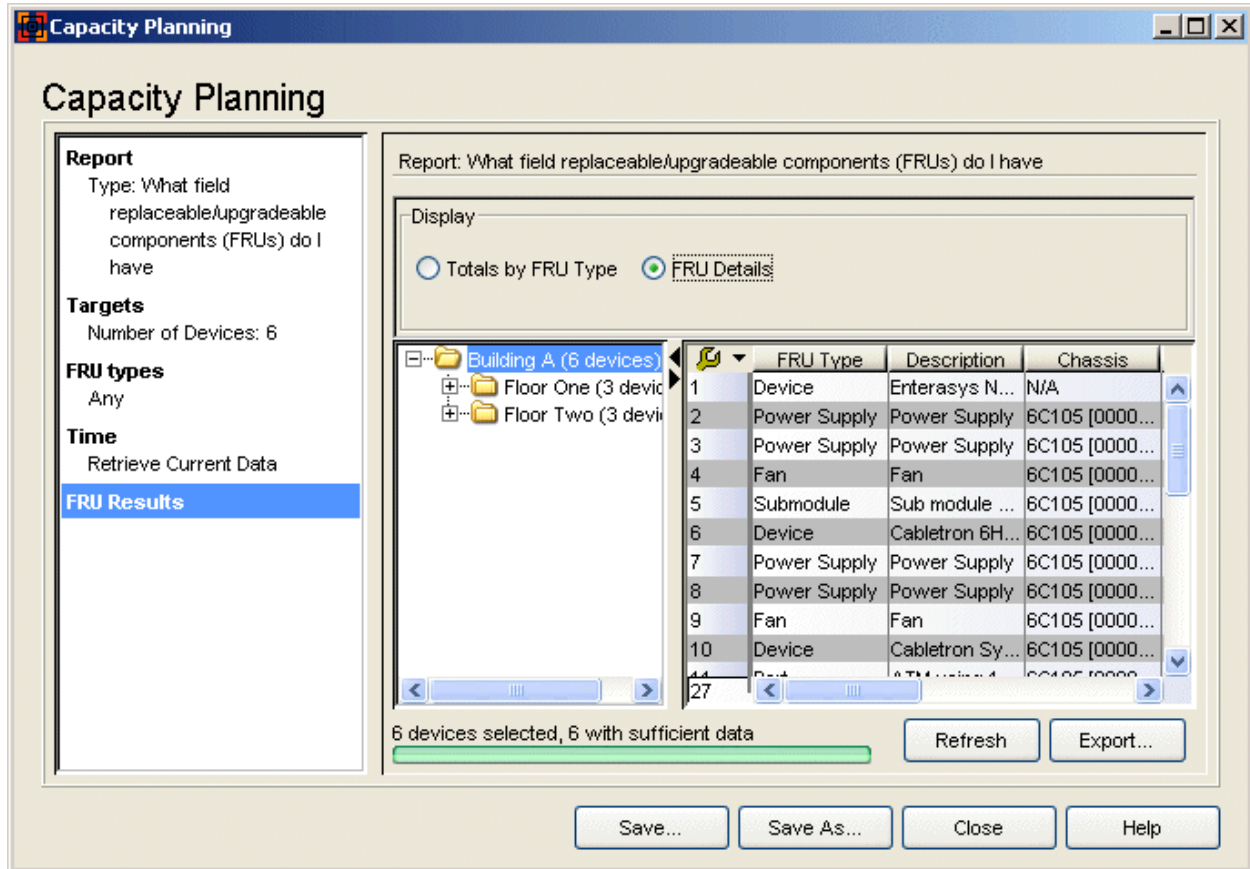
*FRU Results - FRU Details*

The FRU Details view provides details for each individual FRU component included in the report. Depending on your selection in the tree, you can see details for FRUs installed on all the devices in a group or just on an individual device.

---

**NOTES:**

- Each device is considered a FRU and will have a row in the table.
  - Each individual device that resides in a chassis reports the power supplies and fans for that chassis. So, if your report includes a chassis, there will be an entry for power supplies and fans reported by each device in the chassis. For example, if you have four devices in a chassis, each device will report the two power supplies in the chassis, resulting in eight rows of power supplies in the table for that one chassis. Use the IP Address column in the report to verify that each device in the chassis is reporting the same information, and that there are actually only two power supplies in the chassis.
-



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see FRU type details for that group, or select an individual device to see details for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

## Table

The FRU Details table displays information for each FRU component included in the report. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

### FRU Type

The type of FRU. Your selections in the [Select FRU Types window](#) determine the FRU types included in the report.

### Description

A description of the FRU component.

### Chassis

The ID assigned to the chassis where the FRU resides. This is usually a serial number or MAC address, depending on the chassis type.

### Module

The module type where the FRU resides.

### IP Address

The IP address of the module where the FRU resides.

### Date

The date and time the report data was generated. If you generated your report based on historical data, this will be the date and time of the archive version used for the report.

### FRU Name

The specific name of the FRU component.

### Serial Number

A unique number assigned to the module or component by the manufacturer.

### Abort/Refresh Button

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time window](#), clicking Refresh allows you to update your report results with the latest data from your devices.

### Export Button

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

### Save/Save As Button

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.

---

### Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)



## Submodule Capacity Report

---

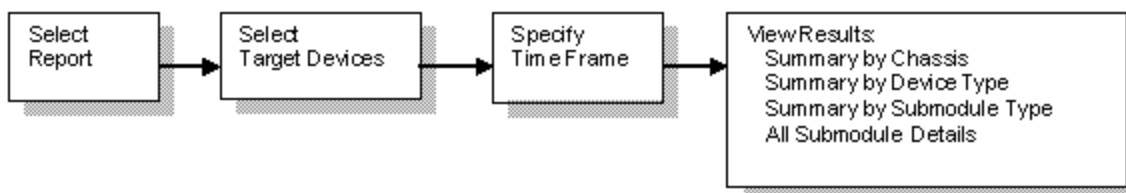
You can use the Capacity Planning Tool to generate a report on your network's submodule capacity and usage. The Show Details on Submodule Capacity and Utilization report provides valuable information on the number of submodule slots available on your network devices, and the actual number of submodules that are installed. In addition, the report provides a description of each of the installed submodules. For this report, a submodule is defined as an expansion module installed on an existing chassis module or standalone device that adds ports to the existing device. This should not be confused with a Port Interface Module (PIM), which adds media connectors to a module, submodule, or standalone device. For example, the 6E129-26 has two PIM slots, which would not be included in the definition of a submodule.

You can view report results organized by chassis, device type, or submodule type. In most cases, the report would be based on current data from your devices. However, there is the option to collect historical data if you would like to view a snapshot of your network's submodule usage at an earlier time.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

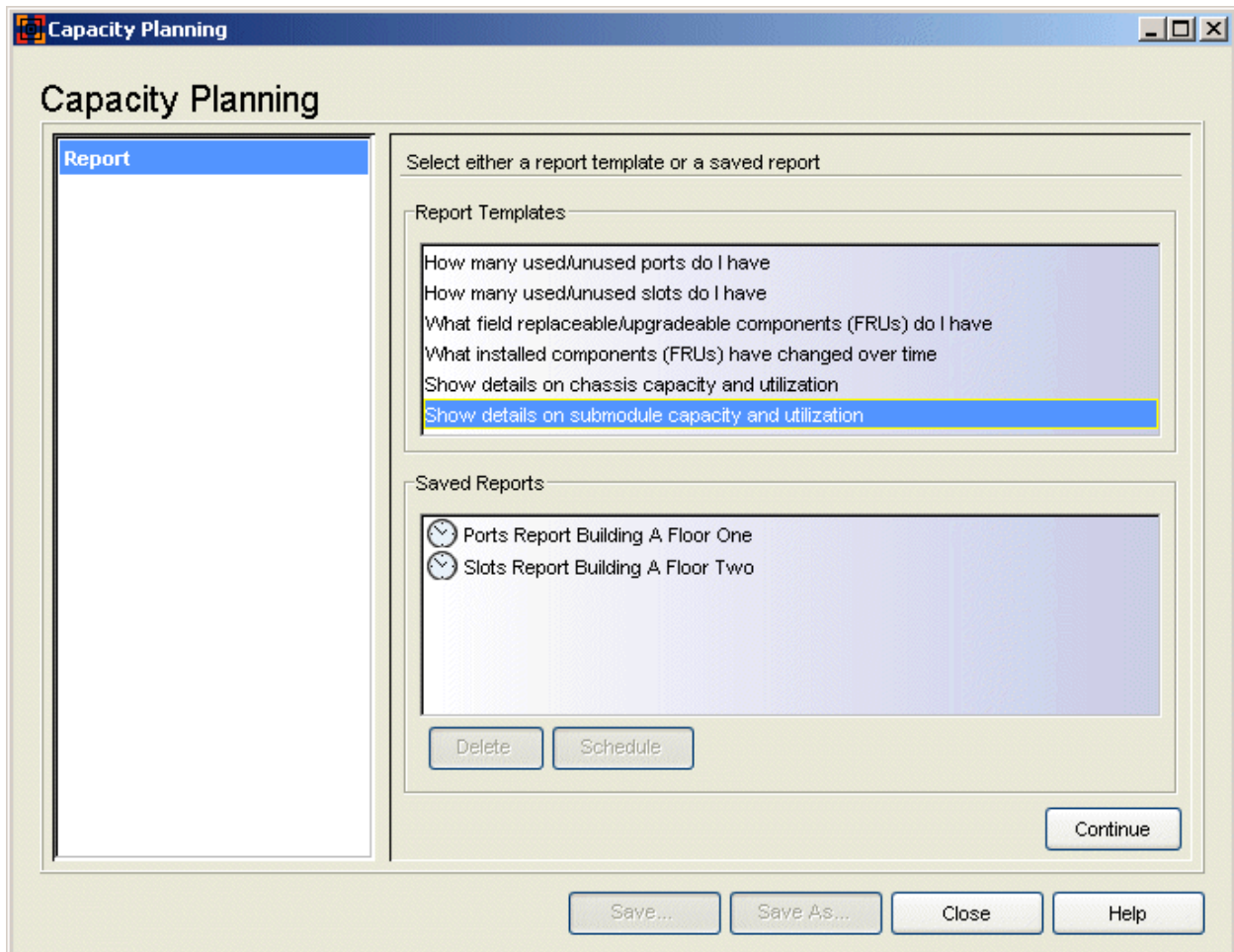
### Flow

The flow chart below shows the sequence of windows that you will encounter when you create a Submodule Capacity report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



## Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your Submodule Capacity report, select the "Show details on submodule capacity and utilization" report template.




### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report

using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon  indicates that a saved report has been scheduled. You can remove a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

#### Delete Button

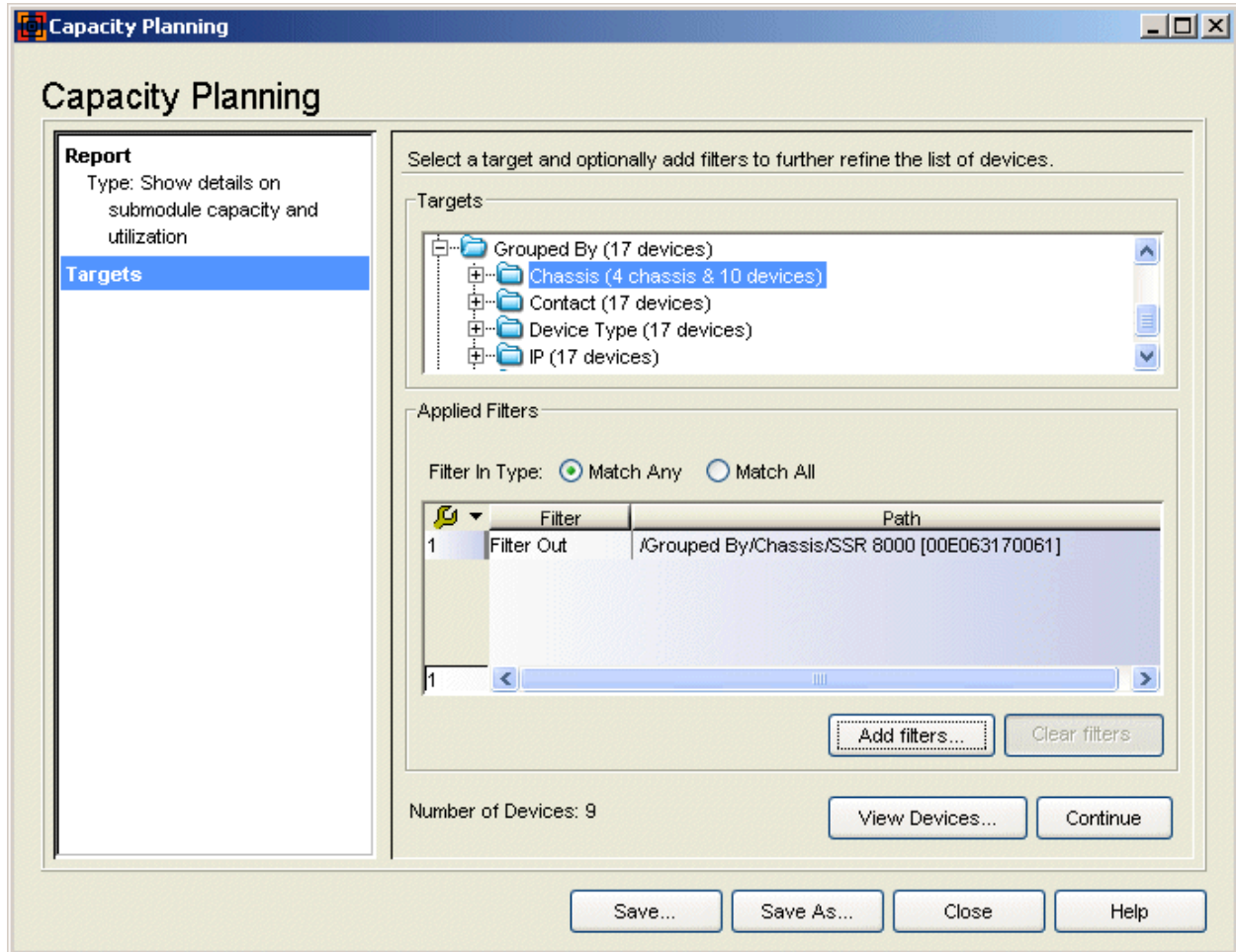
Deletes any report selected in the Saved Reports list.

#### Schedule Button

When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.

## Select Targets Window

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Chassis device group, but filter out a single chassis you don't want included in the report. Or, you could target the Chassis device group, and filter in just one specific chassis type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.



## Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report.

## Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

## Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Grouped By device group and you filter in the 6C105 device group and the 6C107 device group, any device that is in the 6C105 **or** 6C107 device group will be included as a target.

- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have targeted the Grouped By device group and you filter in the Floor One device group and the Chassis device group, any device that is on Floor One **and** in the Chassis device group will be included as a target.

#### Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

#### Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

#### Clear Filters Button

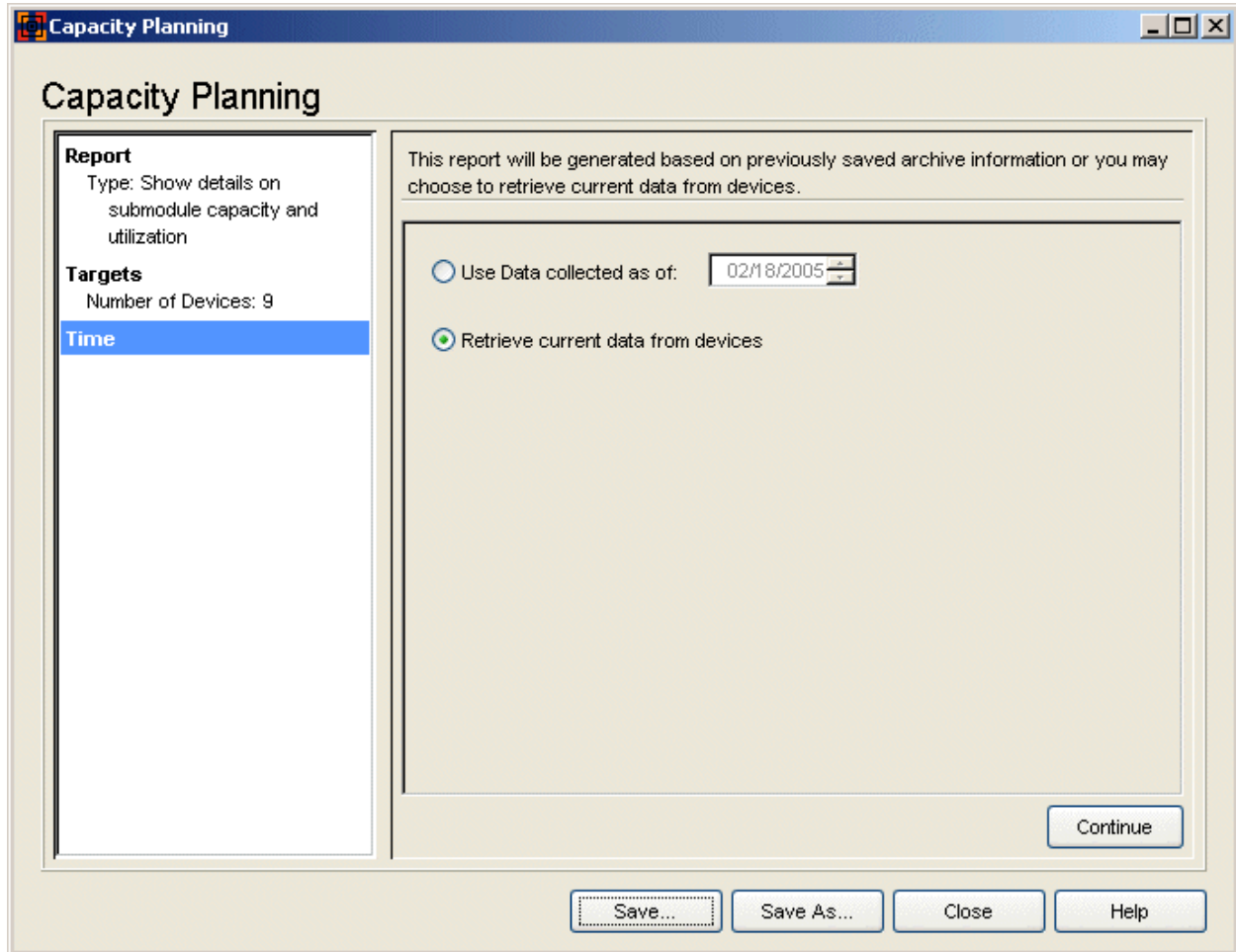
Deletes any filters selected in the Applied Filters list.

#### View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Specify Time Window

Use this window to select a date from which report data will be gathered. In most cases, you will want to generate the report using current data. However, you can also generate a report based on historical data. In that case, the report will be generated using device data saved in the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used (see [How to Archive](#) for more information.)



### Use data collected as of

Report data will be collected based on the date selected here. Calculations are based on the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used. If there is no archive for a target device, that device will not be represented in the report results.

### Retrieve current data from devices

The report will use current data from the target devices. Because this requires the report to gather current data from the devices, extra time may be needed when results are calculated.

### *Submodule Results Window*

Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

- [Summary by Chassis](#) -- reports submodule information summarized by individual chassis.
- [Summary by Device Type](#) -- reports submodule information organized by device type.
- [Summary by Submodule Type](#) -- reports submodule information organized by the type of submodule.
- [All Submodule Details](#) -- provides a description of each submodule and information about the device where it resides.

Your selection in the tree determines the results displayed in the table. For example, you can select a chassis group and view report data for that group. Then, you can expand the group and view data for a specific chassis or device. As you change your selection in the tree, the table is updated with the results for your specific selection.

### *Submodule Results - Summary By Chassis*

The Summary by Chassis view provides data on the number of submodule slots available in each of your chassis, and the actual number of submodules that are installed. You can view submodule information for a chassis group, an individual chassis, or an individual device that resides in a chassis.

The screenshot shows the 'Capacity Planning' application window. On the left, there is a navigation pane with sections for 'Report', 'Targets', and 'Time'. The 'Submodule Results' section is selected. The main area displays a report titled 'Report: Show details on submodule capacity and utilization'. Under the 'Display' section, the 'Summary by Chassis' radio button is selected. Below this, a tree view shows a hierarchy of 'Chassis (3 chassis)'. A table displays the following data:

Chassis ID	Chassis Type	Submodule Capacity	# Submodules Installed
1 00001D331728	6C105	4	0
2 00001D9932AE	6C105	5	3
3 00E063053980	GIGAswitch Router 8	Unsupported	Unsupported

At the bottom of the window, a status bar indicates '9 devices selected, 9 with sufficient data'. There are buttons for 'Refresh', 'Export...', 'Save...', 'Save As...', 'Close', and 'Help'.

### Display

Use these radio buttons to select how you would like the results data displayed.

### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for each chassis in that group, or select an individual chassis to see results for just that chassis. When you change your selection in the tree, the table is updated with the relevant information. Target devices that do not reside in a chassis will not generate any report results.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

### Table

The Summary by Chassis table displays data for each individual chassis. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

---

**NOTE:** Chassis that do not support submodules will display "Unsupported" in the results table entry. If a chassis displays "Not Mapped" in its results table entry, it indicates that the device type is not in the Capacity Planning data file. If you encounter the "Not Mapped" entry, please contact Extreme Networks Support for an updated data file for these devices.

---

### Chassis ID

The ID assigned to the chassis. This is usually a serial number or MAC address, depending on the chassis type.

### Chassis Type

The chassis model number or hardware type.

### Submodule Capacity

The total number of submodule slots on the devices or DFE modules residing in the chassis. For example, if you have five devices installed in a 5-slot chassis, and each device has the capacity to hold two submodules, the



number would be 10. If you have three devices installed in a 5-slot chassis, and each device has the capacity to hold two submodules, the number would be 6.

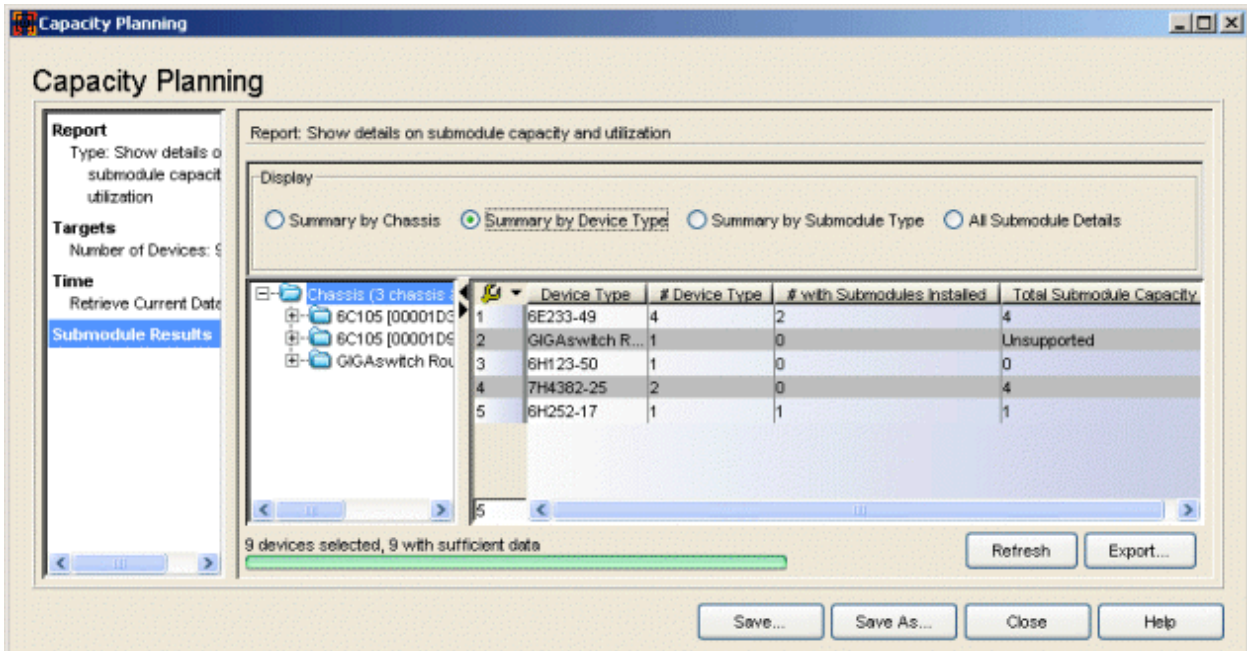
**NOTE:** If the target is not a Chassis folder, then the Submodule Capacity would be the total capacity of the target devices installed in the same chassis. Meaning, if you have a chassis with five devices installed and each has a capacity of one submodule, but only two of the devices are in the target list, then the Submodule Capacity would be 2.

## # Submodules Installed

The total number of submodules installed on the devices or DFE modules in the chassis. For example, if you have five devices installed in a 5-slot chassis, and each device has one submodule, the number would be 5. If you have three devices installed in a 5-slot chassis, and each device has two submodules, the number would be 6.

## Submodule Results - Summary by Device Type

The Summary by Device Type view tells you how many devices of a certain device type have submodules installed.



The screenshot shows the 'Capacity Planning' application window. The 'Report' section is set to 'Summary by Device Type'. The table below shows the results:

Device Type	# Device Type	# with Submodules Installed	Total Submodule Capacity
6E233-49	4	2	4
GIGAswitch R...	1	0	Unsupported
6H123-50	1	0	0
7H4382-25	2	0	4
6H252-17	1	1	1

At the bottom of the window, it indicates '9 devices selected, 9 with sufficient data' and provides buttons for 'Refresh', 'Export...', 'Save...', 'Save As...', 'Close', and 'Help'.

## Display

Use these radio buttons to select how you would like the results data displayed.

### **Target Device Tree**

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see data organized by all the device types in that group, or select a chassis to see data for all the device types in that chassis. When you change your selection in the tree, the table is updated with the relevant information.

### **Device Count, Sufficient Data**

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

### **Table**

The Summary by Device Type table displays submodule information organized by device type. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

### **Device Type**

The model number or hardware type.

### **# Device Type**

The number of devices of that type.

### **# with Submodules Installed**

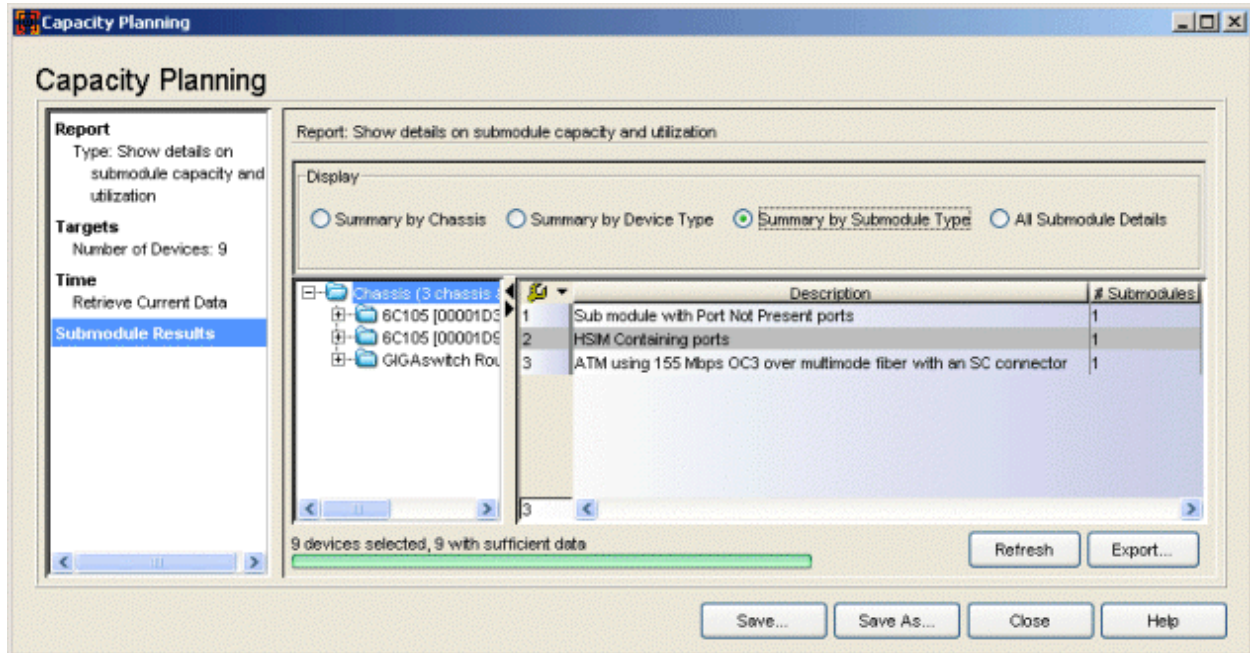
The number of devices of that type with installed submodules.

### **Total Submodule Capacity**

The total submodule capacity for this device type.

### *Submodule Results - Summary by Submodule Type*

The Summary by Submodule Type view provides a description of each submodule type, and the number of that type installed. You can view submodule information for a chassis group, for an individual chassis, or for an individual device.



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see submodule information for all the devices in that group or select a chassis to see submodule information for all the devices in that chassis. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

## Table

The Summary by Submodule Type table displays data organized by submodule type. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

## Description

A description of the submodule.

## # Submodules

The total number of submodules of this type.

## Submodule Results - All Submodule Details

The All Submodule Details view provides a description of each submodule and information about the device where it resides.

Capacity Planning

Report: Show details on submodule capacity and utilization

Display

Summary by Chassis  Summary by Device Type  Summary by Submodule Type  All Submodule Details

	IP Address	Description	Chassis ID	Chassis Type	Device Type
1	12.22.120.77	Sub module with Port Not ...	00001D9932...	6C105	6H252-17
2	12.22.120.79	ATM using 155 Mbps OC3...	00001D9932...	6C105	6E233-49
3	12.22.120.80	HSM Containing ports	00001D9932...	6C105	6E233-49

9 devices selected, 9 with sufficient data

Refresh Export...

Save... Save As... Close Help

## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see submodule details for all the devices in that group, select a chassis to see results for just that chassis, or select an individual device to see submodule information for that device. When you change your selection in the tree, the table is updated with the relevant information.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results.

### Table

The All Submodule Details table displays information for each submodule. If a device has multiple submodules, there will be an entry for each submodule. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, that device will not be represented in the report results.

### IP Address

The IP address of the device reporting the submodule information.

### Description

A description of the submodule.

### Chassis ID

The ID assigned to the chassis where the device resides. This is usually a serial number or MAC address, depending on the chassis type. If the device does not reside in a chassis, this column will display N/A.

### Chassis Type

The chassis model number or hardware type.

### Device Type

The model number or hardware type of the device.

### Abort/Refresh Button

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time window](#), clicking Refresh allows you to update your report results with the latest data from your devices.

### Export Button

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

### Save/Save As Button

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.

---

### Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)

## Used/Unused Ports Report

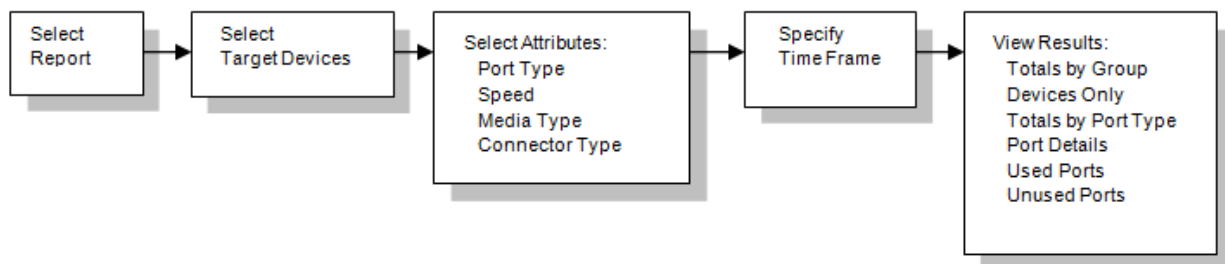
---

Use the Capacity Planning tool to generate a report on your network front-panel port utilization. The Used/Unused Ports report provides valuable information to help you plan your network needs. For example, if you are adding a new department with 15 new employees, you can use this report to locate unused ports of a certain type. You can also use the report to quickly see where ports have been added or removed, or to view specific port details such as port type and speed.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

### Flow

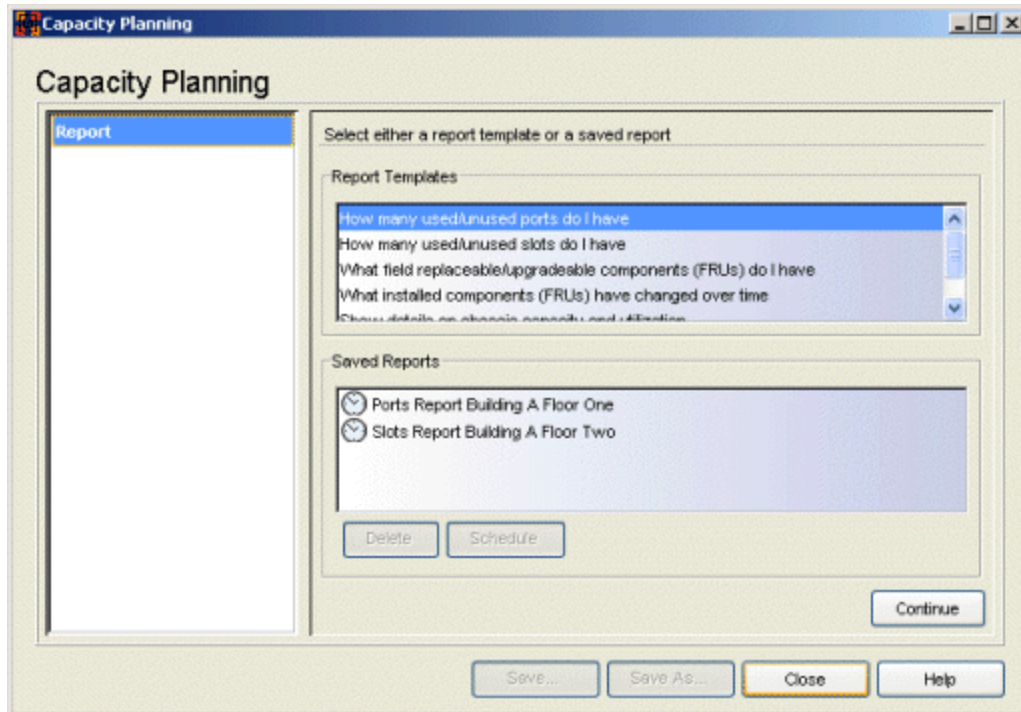
The flow chart below shows the sequence of windows that you will encounter when you create a Used/Unused Ports report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



### Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your

Used/Unused Ports report, select the "How many used/unused ports do I have" report template.



### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon 🕒 indicates that a saved report has been scheduled. You can remove a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

### Delete Button

Deletes any report selected in the Saved Reports list.

### Schedule Button

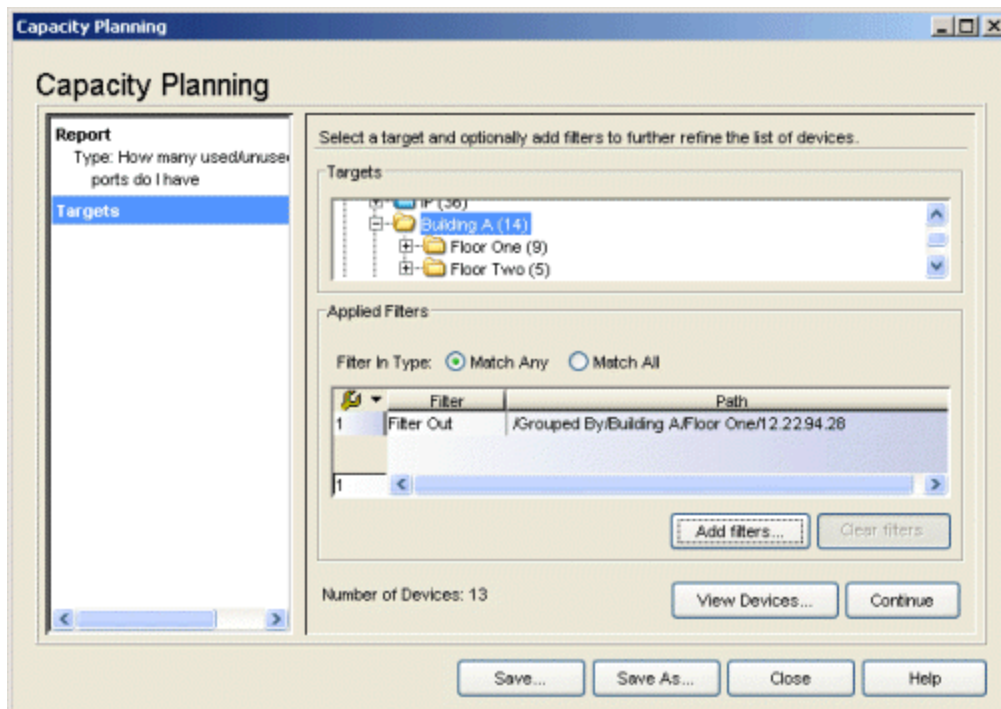
When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.



## Select Targets Window

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Floor One device group, but filter out a single device you don't want included in the report. Or, you could target the Building A device group, and filter in just one specific device type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.

**NOTE: If you will be scheduling this Ports report,** keep in mind when selecting your targets that results from scheduled reports are delivered via e-mail. Depending on the number of target devices you select and the number of ports on those devices, a ports report may generate results that are too large to be delivered via e-mail. In this case, you should consider creating multiple reports based on subnet or device type. This is primarily a concern when selecting the Port Details view for your report results.



### Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report.

### Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

### Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Building A device group and you filter in Floor One devices and E7 devices, any device in Building A that is on Floor One **or** is an E7 device will be included as a target.
- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have selected the Building A device group and you filter in Floor One devices and E7 devices, a Building A device would have to be on Floor One **and** be an E7 device to be included as a target.

### Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

### Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

### Clear Filters Button

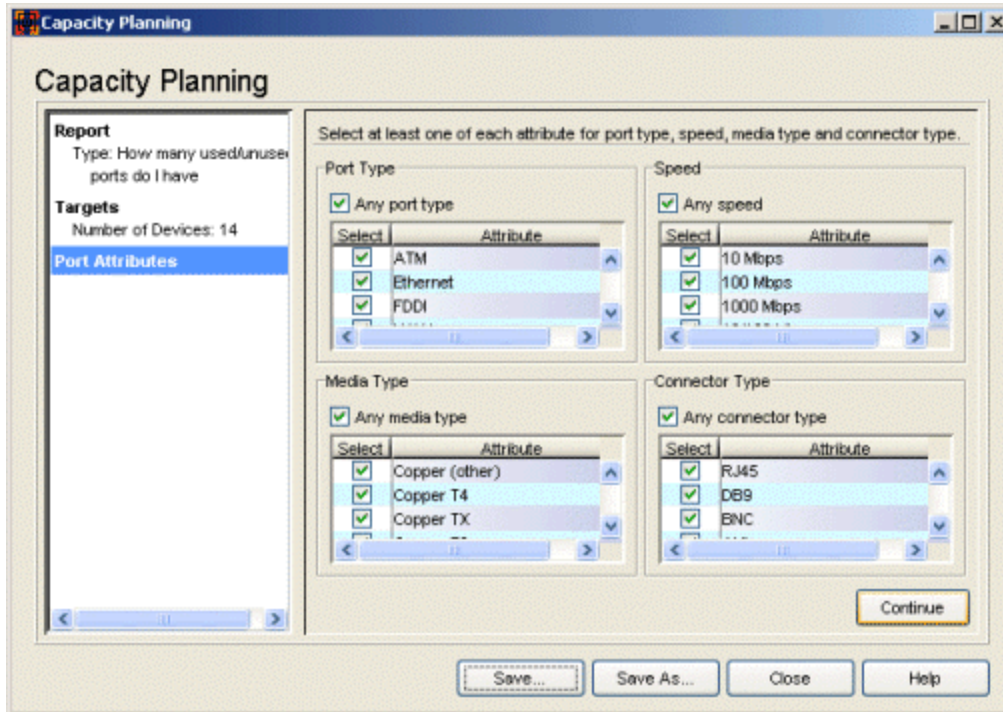
Deletes any filters selected in the Applied Filters list.

### View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Select Port Attributes Window

Use the checkboxes in this window to select specific port attributes for your report. The attributes define the port type, speed, media type, and connector type of the ports to be reported on. You must select at least one of each attribute. Select the "Any" checkbox for a report on all the listed attributes, or select individual attributes to narrow down the focus of your report.



### Port Type

Select the "Any port type" checkbox for a report on all listed port types, or select individual port types of interest. Select the "Other" checkbox if you wish to include data on port types other than the types listed here.

### Speed

Select the "Any speed" checkbox for a report on all listed port speeds, or select individual port speeds of interest. Select the "Other" checkbox if you wish to include data on port speeds other than the speeds listed here. Select the "Unknown Speed" checkbox if you wish to include ports that do not report a speed.

### Media Type

Select the "Any media type" checkbox for a report on all listed port media types, or select individual media types of interest. Select the "Other" checkbox if you wish to include data on media types other than the types listed here. Select the "Unknown Media Type" checkbox if you wish to include ports that do not report a media type. For the purposes of this report, the media types are defined as follows:

- Copper (other) -- Copper media types other than those listed here.
- Copper T4 -- 4 pairs, category 3 UTP (Unshielded Twisted Pair) copper wire.

- Copper TX -- 2 pairs, category 5 UTP (Unshielded Twisted Pair) copper wire.
- Copper T2 -- 2 pairs, category 3 UTP (Unshielded Twisted Pair) copper wire.
- Copper CX -- Copper over 150-Ohm balanced cable.
- Fiber (other) -- Fiber media types other than those listed here.
- Fiber LX -- Fiber over long-wavelength laser.
- Fiber SX -- Fiber over short-wavelength laser.
- Fiber FX -- Fiber Fast Ethernet.
- Empty PIM Slot -- A device port that can accept a Port Interface Module (PIM). PIMs allow you to add ports of various media types to existing devices.
- Other -- Media types other than those listed here.
- Unknown Media Type -- Ports that do not report a media type.

### Connector Type

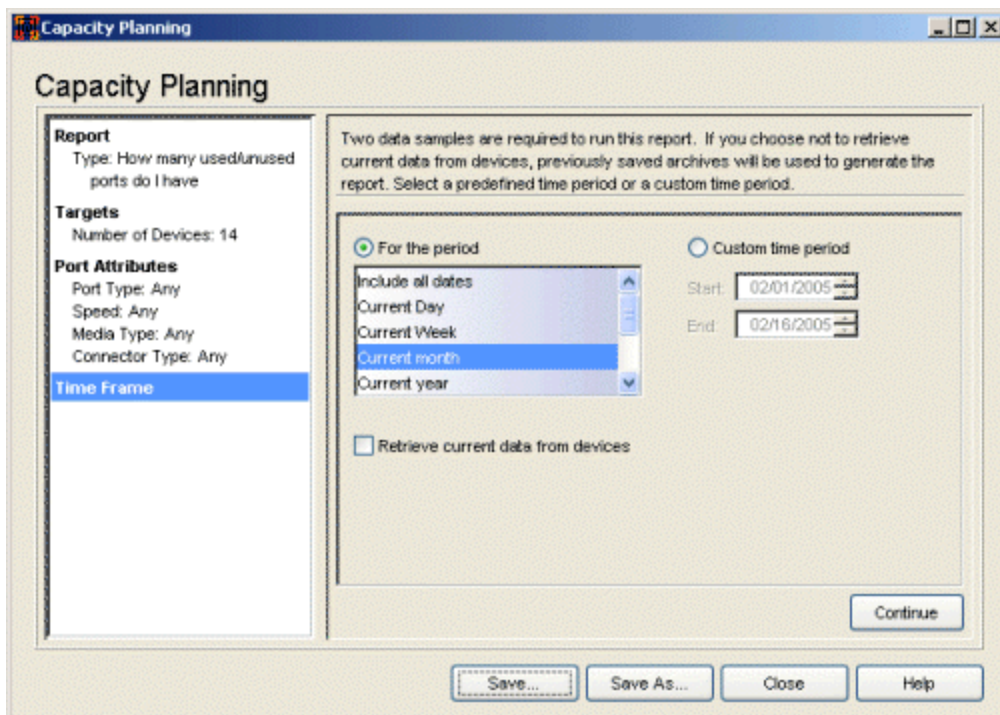
Select the "Any connector type" checkbox for a report on all listed port connector types, or select individual connector types of interest. Select the "Other" checkbox if you wish to include data on connector types other than the types listed here. Select the "Unknown Jack Type" checkbox if you wish to include ports that do not report a connector type. For the purposes of this report, the connector types are defined as follows:

- RJ45 -- An eight-wire modular connector similar to connectors used for a telephone. Used with twisted pair cable.
- DB9 -- A 9-pin connector most commonly used for an RS-232 interface, such as a console port on a network device.
- BNC -- A "bayonet-locking" connector used on 10Base2 thin coaxial cable.
- AUI -- A 15-pin connector interface for connecting transceivers to network devices and to a computer NIC.
- SC -- A fiber-optic "push and pull" cable connector: two fiber cables and two SC connectors provide bidirectional transmission.
- MIC -- A dual-fiber connector most widely used for FDDI and ATM.
- ST -- A fiber-optic "stab and twist" cable connector: two fiber cables and two ST connectors provide bidirectional transmission.

- Telco -- A 50-pin copper connector first used by telephone companies (telco), widely used for 10 and 100 Mbps Ethernet.
- MTRJ -- A fiber-optic connector; two fiber strands.
- SMA -- A fiber-optic connector with a plug that screws into a threaded socket.
- HSSDC -- A High-Speed Serial Data Connector.
- Other -- Connector types other than those listed here.
- Unknown Jack Type -- Ports that do not report a connector type.

## Specify Time Window

Use this window to select a time period from which report data will be gathered. The report will be generated using device data saved in archive operations performed during the specified time period. Calculations are based on the first and last archives (data samples) in the time period selected, not on all archive information in the specified time frame. The archive operations must be configured to archive capacity planning data (see [How to Archive](#) for more information.) You can also select to use current data from devices as one of your data samples, in which case the report will use current data from the target devices, instead of the last archive in the time period.



### For the Period

Select a time period for your report. The report is generated using device data saved in archive operations performed on the targeted devices during the specified time period. Report information is collected from the first and last archives (data samples) in the selected time period, not from every archive in the time period.

- Include all dates -- The report will use the first and last archives that exist for your target devices.
- Current Day -- The report will use the first and last archives from the current day.
- Current Week -- The report will use the first and last archives from the current week.
- Current month -- The report will use the first and last archives from the current month.
- Current year -- The report will use the first and last archives from the current year.
- Last month -- The report will use the first and last archives from the previous month.
- Last 3 months -- The report will use the first and last archives from the previous three months, not including the current month.
- Last 6 months -- The report will use the first and last archives from the previous six months, not including the current month.
- Last 12 months -- The report will use the first and last archives from the previous 12 months, not including the current month.

---

**TIP:** When you make a "For the Period" time selection, the "Custom time period" Start and End dates are automatically filled in with the selected dates. You can then switch to the Custom time period option and refine your time period to the exact dates you would like. For example, you could select the time period "Last 6 months", and then switch to the Custom time period option and change the End date to the current date. This would allow you to generate a report using data from the current month and the last six months.

---

### Retrieve current data from devices

This checkbox is available when you select a time period where the End date is the current date. When the checkbox is selected, the report will use current data from the target devices, instead of the last archive in the time period. Because this requires the report to gather current data from the devices, extra time may be needed while report results are calculated.

### Custom Time Period

Specify a custom time period for your report. Report information will be collected from the first and last archive (data samples) in the selected time period, not from every archive in the time period.

## Port Results Window

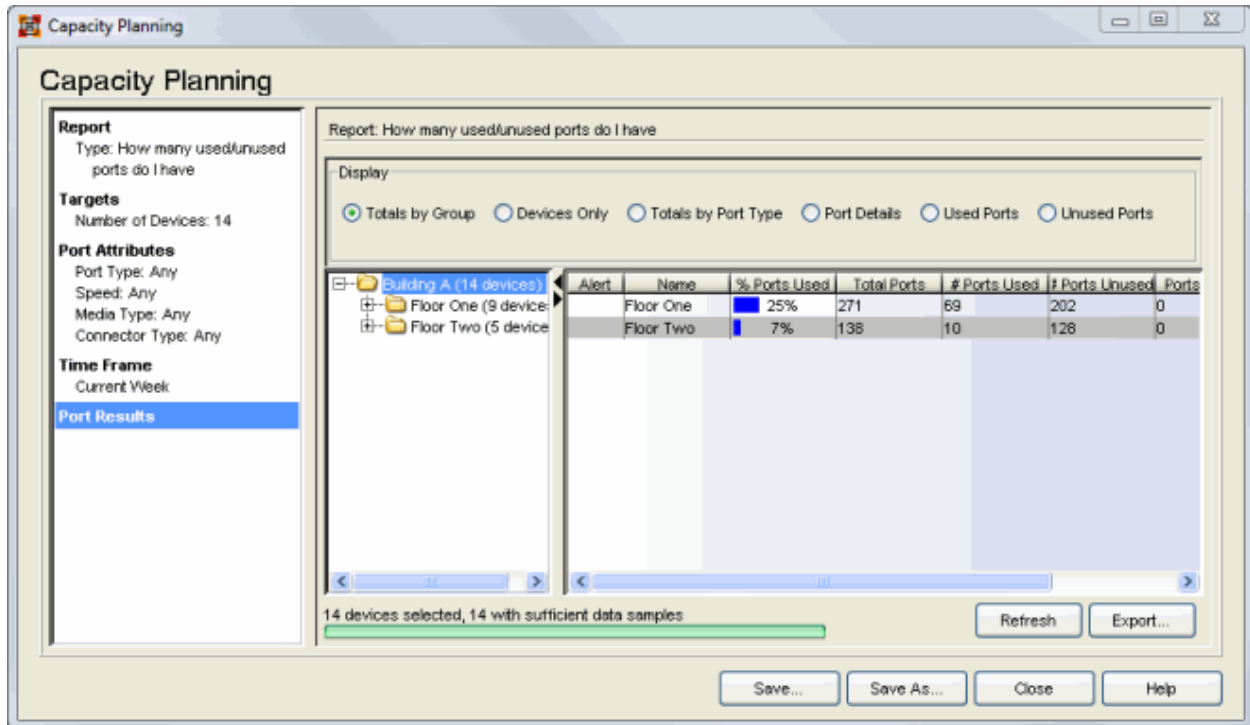
Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

- [Totals by Group](#) -- displays the report results organized by totals based on device group.
- [Devices Only](#) -- lists the report results for each device.
- [Totals by Port Type](#) -- displays the report results organized by totals based on port type.
- [Port Details](#) -- lists the report results for each port.
- [Used Ports](#) -- lists the ports currently in use for the selected device or device group.
- [Unused Ports](#) -- lists the ports currently not in use for the selected device or device group.

In addition, your selection in the tree determines the results displayed in the table. For example, you can select a device group and view report data for that group. Then, you can expand the group and view data for a specific device. As you change your selection in the tree, the table is updated with the results for your specific selection.

### *Port Results - Totals by Group*

The Totals by Group view gives you the flexibility of viewing your port results summarized by group or detailed by device. It provides an easy way to view top-level port information and quickly determine where to take a closer look. Simply by changing your selection in the tree, you can view port data for a group or port data for the individual devices that make up a group.



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. Devices with no data samples or only one data sample will show an alert icon in their table entry, and will display Unknown for some or all of their results.

## Table

The Totals by Group table displays port data for the selected device groups or for the individual devices contained in a group. The report is generated based on



the first and last data samples in the time period selected. Results that are not available are displayed as Unknown.

---

**NOTE:** In the port results, a port is considered **used** when there were two data samples consulted to obtain report data and

- the port's link status for either sample is LINK, or
  - the port's link status for both samples is NO LINK, but the bytes transferred values for both samples are not equal.
- 

### Alert

A yellow alert icon  in this column signifies that the report data for this table entry is questionable. It indicates that:

- there aren't enough data samples in the selected time period to generate report data. At least two data samples (either two archives, or one archive and current data) are required for each device. Devices with no data samples or only one data sample will display Unknown for some or all of their results.
- between the data samples ports were removed, and the port's link status in the first data sample is NO LINK. This causes the validity of the data to be in question because there is no way to determine if bytes had been transferred by a port before it was removed, and therefore the report cannot accurately determine if the port is being used.

Rest your cursor on the alert to display a tooltip that describes the reason for the alert.

### Name

The name of the group or the IP address of an individual device.

### % Ports Used

The percentage of ports being [used](#) in the device group or on the individual device.

### Total Ports

The total number of ports installed in the device group or on the individual device.

### # Ports Used

The number of ports being [used](#) in the device group or on the individual device.

## # Ports Unused

The number of ports not in use in the device group or on the individual device.

## Ports Added

The number of ports added (during the specified time frame) to the device group or to an individual device.

## Ports Removed

The number of ports removed (during the specified time frame) from the device group or from an individual device.

## Port Results - Devices Only

The Devices Only view lets you view port data for each individual target device. Depending on your selection in the tree, you can see report results for all the devices in a group, or for an individual device.

Capacity Planning

Report: How many used/unused ports do I have

Display

Totals by Group  Devices Only  Totals by Port Type  Port Details  Used Ports  Unused Ports

Alert	IP Address	Device Type	% Ports Used	Total Ports	# Ports Used	# Ports Available
	12.22.77.24	PC	100%	1	1	0
	12.22.77.55	6H302-48	0%	48	0	48
	12.22.77.56	6H262-18	17%	17	3	14
	12.22.77.88	1H582-51	2%	48	1	47
	12.22.77.134	3H252-02	3%	26	1	25
	12.22.80.1	Matrix N1 Pla...	50%	54	27	27
	12.22.80.6	Matrix N1 Pla...	45%	24	11	13
	12.22.80.13	C2G124-48	41%	48	20	28
	12.22.80.42	C2400	100%	5	5	0
	12.22.54.10	3H252-02	7%	26	2	24
	12.22.54.31	B3G124-48P	6%	48	3	45
	12.22.54.50	D2G124-12P	8%	12	1	11

14 devices selected, 14 with sufficient data samples

Refresh Export...

Save... Save As... Close Help

## Display

Use these radio buttons to select how you would like the results data displayed.

### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for the devices in that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. Devices with no data samples or only one data sample will show an alert icon in their table entry, and will display Unknown for some or all of their results.

### Table

The Devices Only table displays port data for each individual device. The report is generated based on the first and last data samples in the time period selected. Results that are not available are displayed as Unknown.

**NOTE:** In the port results, a port is considered **used** when there were two data samples consulted to obtain report data and

- the port's link status for either sample is LINK, or
- the port's link status for both samples is NO LINK, but the bytes transferred values for both samples are not equal.

### Alert

A yellow alert icon  in this column signifies that the report data for this table entry is questionable. It indicates that:

- there aren't enough data samples in the selected time period to generate report data. At least two data samples (either two archives, or one archive and current data) are required for each device. Devices with no data samples or only one data sample will display Unknown for some or all of their results.
- between the data samples ports were removed, and the port's link status in the first data sample is NO LINK. This causes the validity of the data to be in question because there is no way to determine if bytes had been transferred by a port before it was removed, and therefore the report cannot accurately determine if the port is being used.

Rest your cursor on the alert to display a tooltip that describes the reason for the alert.

**IP Address**

The IP address of the device.

**Device Type**

The model number of the device.

**% Ports Used**

The percentage of ports being [used](#) on the device.

**Total Ports**

The total number of ports installed on the device.

**# Ports Used**

The number of ports being [used](#) on the device.

**# Ports Unused**

The number of ports [not in use](#) on the device.

**Ports Added**

The number of ports added (during the specified time frame) to the device.

**Ports Removed**

The number of ports removed (during the specified time frame) from the device.

**# Data Samples**

The number of data samples that were consulted to obtain report data. The maximum number would be two.

*Port Results - Totals by Port Type*

The Totals by Port Type view lets you view port data organized by port type: ATM, Ethernet, FDDI, WAN, or Other. Your port type selections in the [Port Attributes window](#) determine what port types are reported on. Depending on your selection in the tree, you can see report results summarized for all the devices in a group, or for an individual device.

Capacity Planning

Report: How many used/unused ports do I have

Display

Totals by Group  Devices Only  Totals by Port Type  Port Details  Used Ports  Unused Ports

Port Type	Description	% Ports Used	Total Ports	# Ports Used	Ports Added
Ethernet	Ethernet CS...	100%	6	6	0
Ethernet	Unspecified ...	0%	4	0	0
Ethernet	1000Base-S...	100%	1	1	0
Ethernet	100Base-TX ...	4%	96	4	0
Ethernet	1000Base-S...	100%	1	1	0
Ethernet	100Base-TX ...	43%	24	11	0
Ethernet	1000Base-S...	0%	1	0	0
Ethernet	1000Base-T ...	17%	160	28	0
Ethernet	Empty PIM Slot	0%	4	0	0
Ethernet	100Base-TX ...	4%	64	3	0
Ethernet	1000Base-T ...	52%	48	25	0

14 devices selected, 14 with sufficient data samples

Refresh Export...

Save... Save As... Close Help

## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see port type results summarized for that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. Devices with no data samples or only one data sample will display Unknown for some or all of their results.

## Table

The Totals by Port Type table displays port data for the selected device groups or for the individual devices contained in a group, organized according to port

type. However, there may be multiple entries for a single port type, due to different media types and connectors being used.

The report is generated based on the first and last data samples in the time period selected. Results that are not available are displayed as Unknown.

---

**NOTE:** In the port results, a port is considered **used** when there were two data samples consulted to obtain report data and

- the port's link status for either sample is LINK, or
  - the port's link status for both samples is NO LINK, but the bytes transferred values for both samples are not equal.
- 

### Port Type

The type of port: ATM, Ethernet, FDDI, WAN, or Other. Your selections in the [Port Attributes window](#) determine the port types included in the report.

### Description

A description of the port.

### % Ports Used

The percentage of ports of that port type being [used](#) in the device group or on the individual device.

### Total Ports

The total number of ports of that port type installed in the device group or on the individual device.

### # Ports Used

The number of ports of that port type being [used](#) in the device group or on the individual device.

### Ports Added

The number of ports of that port type added (during the specified time frame) to the device group or to an individual device.

### Ports Removed

The number of ports of that port type removed (during the specified time frame) from the device group or from an individual device.

### Media

The media being used by that port type.

### Media Type

A detailed description of the media being used by that port type.

**Framing**

The start and stop bit that frame the data transmitted by that port type.

**Speed**

That port type's physical speed.

**Connector**

That port type's connector type.

*Port Results - Port Details*

The Port Details view provides an easy way to look at port information for a specific device. Depending on your selection in the tree, you can see port details for all the devices in a group, or for an individual device.

The screenshot shows the 'Capacity Planning' application window. The main area displays a table of port details for 'Building A (14 devices)'. The table has columns for IP Address, Port Number, Description, Date, Speed, and Bytes Trans. The 'Display' section has radio buttons for 'Totals by Group', 'Devices Only', 'Totals by Port Type', 'Port Details' (selected), 'Used Ports', and 'Unused Ports'. The status bar at the bottom indicates '14 devices selected, 14 with sufficient data samples'.

IP Address	Port Number	Description	Date	Speed	Bytes Trans
12.22.77.24	2	Ethernet CS...	10:50:35 AM...	100 Mbps	398370897
12.22.77.24	48	Ethernet CS...	10:51:52 AM...	100 Mbps	398384196
12.22.77.55	47	100Base-TX ...	10:50:35 AM...	10/100 Mbps	896
12.22.77.55	46	100Base-TX ...	10:50:35 AM...	10/100 Mbps	896
12.22.77.55	45	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	44	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	43	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	42	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	41	100Base-TX ...	10:50:35 AM...	10/100 Mbps	640
12.22.77.55	40	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576
12.22.77.55	39	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576

**Display**

Use these radio buttons to select how you would like the results data displayed.

**Target Device Tree**

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for the devices in that group, or select

an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. Devices with no data samples or only one data sample will display Unknown for some or all of their results.

### Table

The Port Details table displays information for each port on the target devices. The report is generated based on the first and last data samples in the time period selected, resulting in two entries per port (one for each data sample used.) Information that is not available is displayed as Unknown.

---

**TIP:** Right-click on the Port Number column heading to sort the table entries according to port number. This allows you to easily view and compare both data sample entries for each port.

---

### IP Address

The IP address of the device.

### Port Number

The port number on the device.

### Date

The date and time of the data sample used to generate the port information.

### Speed

The port's physical speed.

### Bytes Transferred

The number of bytes transferred since the device was turned on or reset.

### Link Status

The port's link status: LINK or NO LINK.

### Media Type

The port's media type.

### Connector Type

The port's connector type.



**IF Name**

A description of the port.

*Port Results - Used Ports*

The Used Ports view lists all the ports being used for a specific device.

Depending on your selection in the tree, you can see used ports information for all the devices in a group, or for an individual device.

Capacity Planning

Report: How many used/unused ports do I have

Display

Totals by Group  Devices Only  Totals by Port Type  Port Details  Used Ports  Unused Ports

IP Address	Port Number	Description	Date	Speed	Bytes Trans
12.22.77.24	2	Ethernet CS...	10:50:35 AM...	100 Mbps	398370897
12.22.77.24	2	Ethernet CS...	10:51:52 AM...	100 Mbps	398384196
12.22.77.56	3	100Base-TX ...	10:50:35 AM...	10/100 Mbps	529122143
12.22.77.56	2	100Base-TX ...	10:50:35 AM...	10/100 Mbps	619675149
12.22.77.56	1	100Base-TX ...	10:50:35 AM...	10/100 Mbps	488737551
12.22.77.56	1	100Base-TX ...	10:51:52 AM...	10/100 Mbps	488801439
12.22.77.56	2	100Base-TX ...	10:51:52 AM...	10/100 Mbps	619683975
12.22.77.56	3	100Base-TX ...	10:51:52 AM...	10/100 Mbps	529153862
12.22.77.88	2	100Base-TX ...	10:50:35 AM...	10/100 Mbps	134577610
12.22.77.88	2	100Base-TX ...	10:51:52 AM...	10/100 Mbps	134611813
12.22.77.134	1	100Base-TX ...	10:50:35 AM...	10/100 Mbps	19145616
12.22.77.134	1	100Base-TX ...	10:51:52 AM...	10/100 Mbps	19156315

14 devices selected, 14 with sufficient data samples

Refresh Export...

Save... Save As... Close Help

**Display**

Use these radio buttons to select how you would like the results data displayed.

**Target Device Tree**

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for the devices in that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

**Device Count, Sufficient Data**

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and

current data) used to obtain report data. Devices with no data samples or only one data sample will display Unknown for some or all of their results.

## Table

The Used Ports table displays port usage information for the target devices. The report is generated based on the first and last data samples in the time period selected, resulting in two entries per port (one for each data sample used.) Information that is not available is displayed as Unknown.

---

**TIP:** Right-click on the Port Number column heading to sort the table entries according to port number. This allows you to easily view and compare both data sample entries for each port.

---

### IP Address

The IP address of the device.

### Port Number

The port number on the device.

### Date

The date and time of the data sample used to generate the port information.

### Speed

The port's physical speed.

### Bytes Transferred

The number of bytes transferred since the device was turned on or reset.

### Link Status

The port's link status: LINK or NO LINK.

### Media Type

The port's media type.

### Connector Type

The port's connector type.

### IF Name

A description of the port.

## *Port Results - Unused Ports*

The Unused Ports view lists all the ports being not being used for a specific device. Depending on your selection in the tree, you can see used ports

information for all the devices in a group, or for an individual device.

The screenshot shows the 'Capacity Planning' application window. The main report area displays a table of port usage data for 14 devices in Building A. The table columns are IP Address, Port Number, Description, Date, Speed, and Bytes Trans. The data shows 14 ports, all of which are 100Base-TX ports, with varying data transfer rates.

IP Address	Port Number	Description	Date	Speed	Bytes Trans
12.22.77.55	48	100Base-TX ...	10:50:35 AM...	10/100 Mbps	896
12.22.77.55	47	100Base-TX ...	10:50:35 AM...	10/100 Mbps	896
12.22.77.55	46	100Base-TX ...	10:50:35 AM...	10/100 Mbps	896
12.22.77.55	45	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	44	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	43	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	42	100Base-TX ...	10:50:35 AM...	10/100 Mbps	704
12.22.77.55	41	100Base-TX ...	10:50:35 AM...	10/100 Mbps	640
12.22.77.55	40	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576
12.22.77.55	39	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576
12.22.77.55	38	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576
12.22.77.55	37	100Base-TX ...	10:50:35 AM...	10/100 Mbps	576

The interface also includes a left-hand navigation pane with sections for Report, Targets, Port Attributes, Time Frame, and Port Results. The 'Port Results' section is currently selected. At the bottom of the window, there are buttons for Save..., Save As..., Close, and Help, and a status bar indicating '14 devices selected, 14 with sufficient data samples'.

## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a device group to see results for the devices in that group, or select an individual device to see results for just that device. When you change your selection in the tree, the table is updated with the relevant information.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. A device is counted as having sufficient data if there were two data samples (either two archives, or one archive and current data) used to obtain report data. Devices with no data samples or only one data sample will display Unknown for some or all of their results.

## Table

The Unused Ports table displays port usage information for the target devices. The report is generated based on the first and last data samples in the time

period selected, resulting in two entries per port (one for each data sample used.) Information that is not available is displayed as Unknown.

---

**TIP:** Right-click on the Port Number column heading to sort the table entries according to port number. This allows you to easily view and compare both data sample entries for each port.

---

**IP Address**

The IP address of the device.

**Port Number**

The port number on the device.

**Date**

The date and time of the data sample used to generate the port information.

**Speed**

The port's physical speed.

**Bytes Transferred**

The number of bytes transferred since the device was turned on or reset.

**Link Status**

The port's link status: LINK or NO LINK.

**Media Type**

The port's media type.

**Connector Type**

The port's connector type.

**IF Name**

A description of the port.

**Abort/Refresh Button**

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time window](#), clicking Refresh allows you to update your report results with the latest data from your devices. In addition, if you have selected a current time frame for your report, and a new archive is saved after your report results are generated, clicking Refresh will regenerate your results using the new archive data.

### Export Button

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

### Save/Save As Button

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.

---

### Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)

## Used/Unused Slots Report

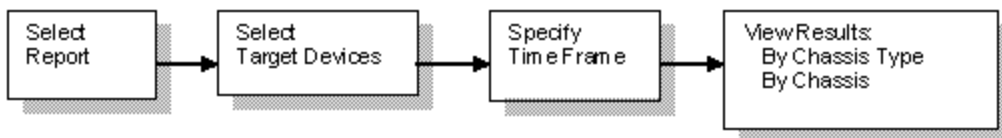
---

Use the Capacity Planning tool to generate a report on your network chassis slot utilization. The Used/Unused Slots report provides valuable information to help you plan your network needs. For example, if you are adding a new department with 30 new employees, you can use this report to locate unused chassis slots where you can add modules to expand your port capacity. You can view slot information for each individual chassis, or organized by chassis type. In most cases, the Used/Unused Slots report would be based on current data from your devices. However, there is the option to collect historical data if you would like to view a snapshot of your network's slot usage at an earlier time.

Report results can be exported as an HTML file or as a delimited text file. In addition, Capacity Planning reports can be saved to use again at a later time, and they can also be scheduled to run at specified intervals with report results sent out via a notification e-mail.

### Flow

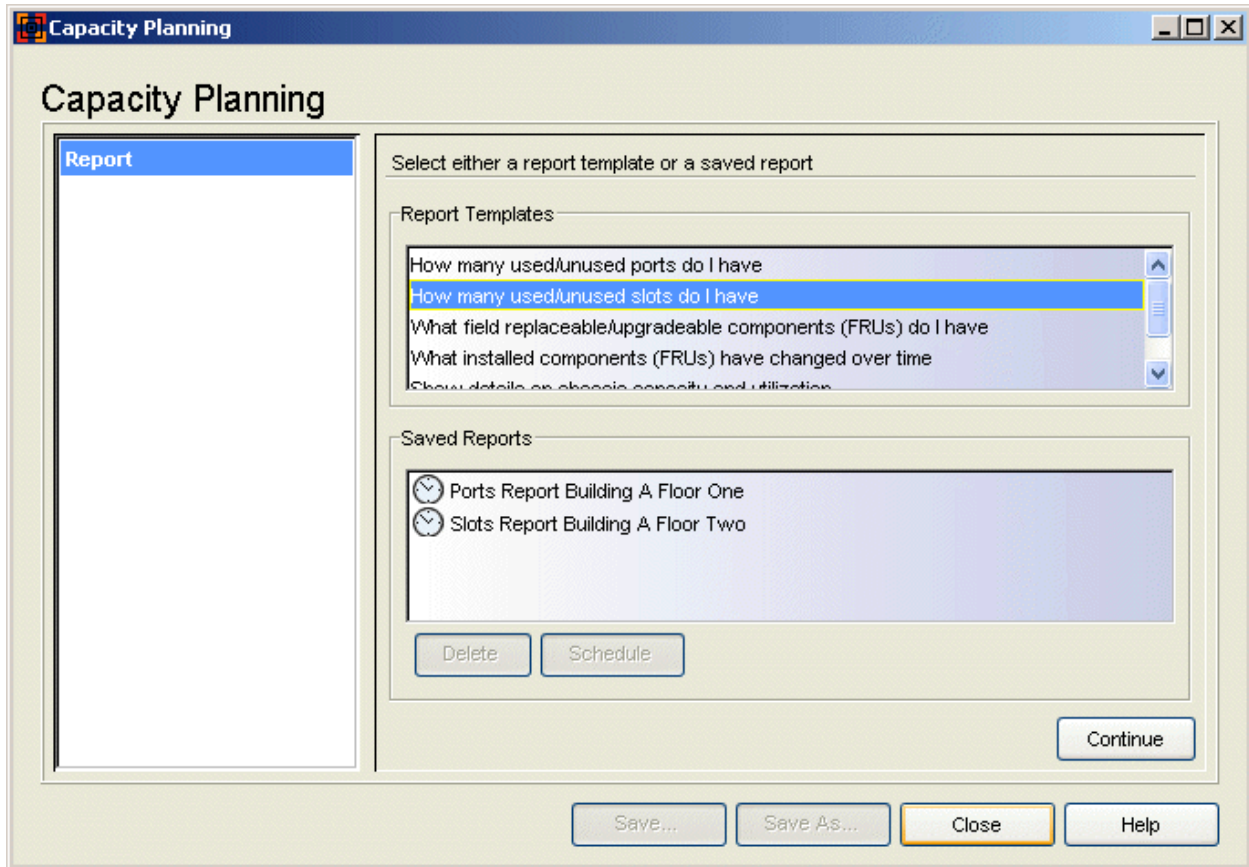
The flow chart below shows the sequence of windows that you will encounter when you create a Used/Unused Slots report using the Capacity Planning tool. As you progress through the steps of creating a report, the tool's left panel shows you a summary of your selections. You can click on the bold headings in this panel to navigate backward or forward between steps allowing you to change your report parameters. The summary information associated with each step appears in plain typeface beneath each step heading.



### Select Report Window

Use this window to select either a report template or a saved report as your report type. Report templates are based on common network capacity planning questions. After you have created a report using one of the templates, you can save it (as a Saved Report) to use again at a later time. To create your

Used/Unused Slots report, select the "How many used/unused slots do I have" report template.



### Report Templates

Lists the available report templates. Each report template is designed to answer a specific capacity planning question.

### Saved Reports

Lists all your saved reports including reports saved by other Inventory Manager clients connected to the server. After you have created a report using a template, you can save it as a Saved Report, by clicking the **Save** button. This allows you to save specific report attributes and parameters, so that you can regenerate the same report at a later time. The schedule icon 🕒 indicates that a saved report has been scheduled. You can remove a schedule from a saved report by right-clicking on the report and selecting Delete > Schedule.

### Delete Button

Deletes any report selected in the Saved Reports list.

### Schedule Button

When you have selected a saved report in the Saved Reports list, this button opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report.

## Select Targets Window

Use this window to select the target devices for your report and add filters to further refine the list of devices, if desired. For example, you could target the Chassis device group, but filter out a single chassis you don't want included in the report. Or, you could target the Chassis device group, and filter in just one specific chassis type. Once you have made your selections, you can view a list of the devices you have targeted for your report to verify that your targets are correct.

---

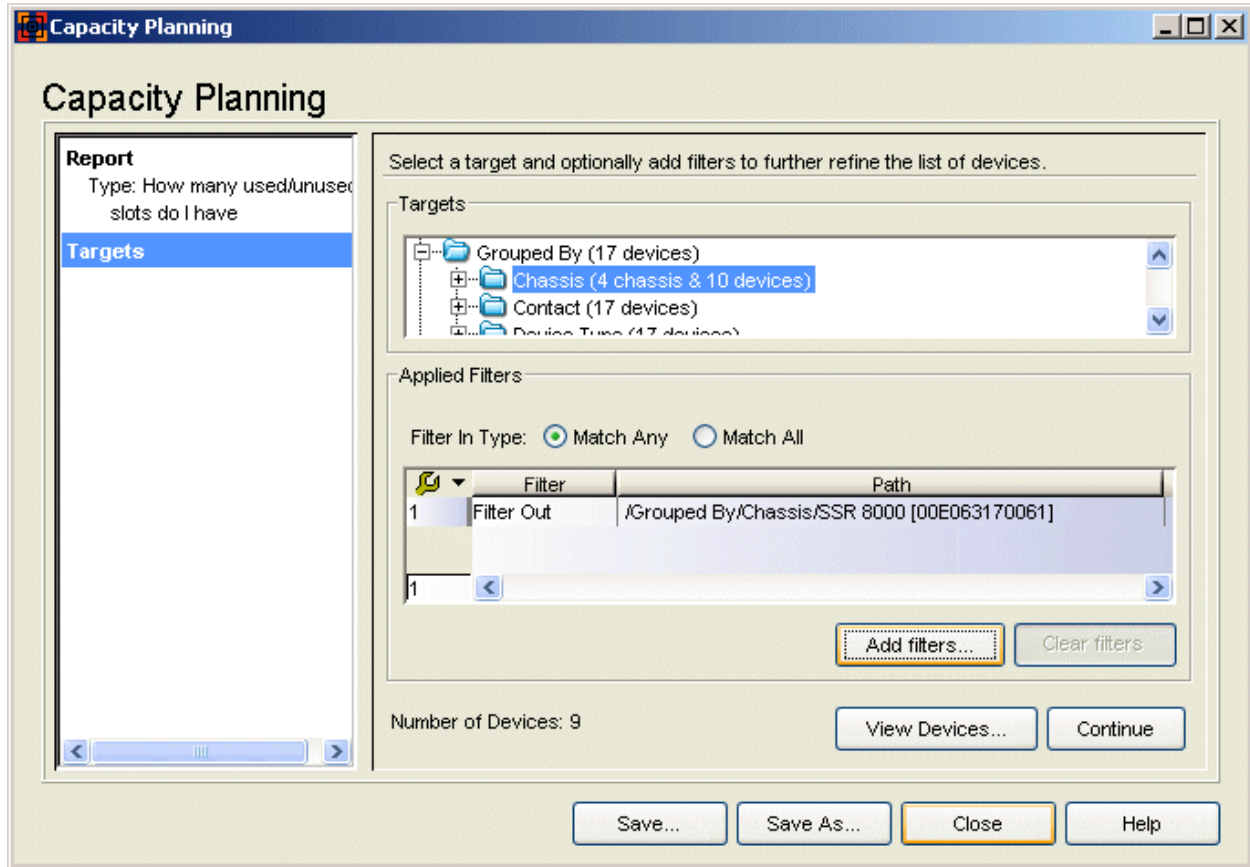
**NOTE:** The slot usage report is generated based on data from individual devices. Basically, the report asks each device, "What chassis and slot are you in?" If the device responds with chassis and slot information, it is included in the report. This can affect the validity of your report results if you are generating a report using historical data (from device archives) as opposed to current data from the device. (See the [Specify Time Window](#) for more information.)

Let's say you want to know what your Chassis One slot usage was as of October 10, 2003. At that time, Chassis One contained devices 1.1.1.1 and 2.2.2.2. But currently, Chassis One contains devices 1.1.1.1 and 3.3.3.3. If you target Chassis One, the report would look at archives of 1.1.1.1 and 3.3.3.3, and no report data would be generated for 2.2.2.2.

To achieve more accurate report results, you could target the All Devices folder. Then, the report would look at archives of all three devices, and would correctly report slot usage for 1.1.1.1 and 2.2.2.2.

---





## Targets

This panel displays your Network Elements tree. Expand the tree to select the target device group or individual device for your report. In most cases, you will want to target a group of chassis for this report. Devices that do not reside in a chassis will not generate any report results. If a device has been configured with SNMP context, you can select each context as a separate target device.

## Applied Filters

Lists any filters applied to your selected targets. Click the **Add Filters** button to open the [Add Filters window](#) and create your filters.

## Filter In Type

If you have defined one or more "Filter In" filters, select how you want the filters to work:

- **Match Any** - A device can match any of the filter-in filters to be included as a target. For example, if you have selected the Grouped By device group and you filter in the 6C105 device group and the 6C107 device group, any device that is in the 6C105 **or** 6C107 device

group will be included as a target.

- **Match All** - A device must match all of the filter-in filters to be included as a target. For example, if you have targeted the Grouped By device group and you filter in the Floor One device group and the Chassis device group, any device that is on Floor One **and** in the Chassis device group will be included as a target.

### Number of Devices

A running total of the number of target devices with filters applied. Click **View Devices** to view a list of the target devices.

### Add Filters Button

Opens the [Add Filters window](#), where you can create filters to further qualify the list of devices for your report.

### Clear Filters Button

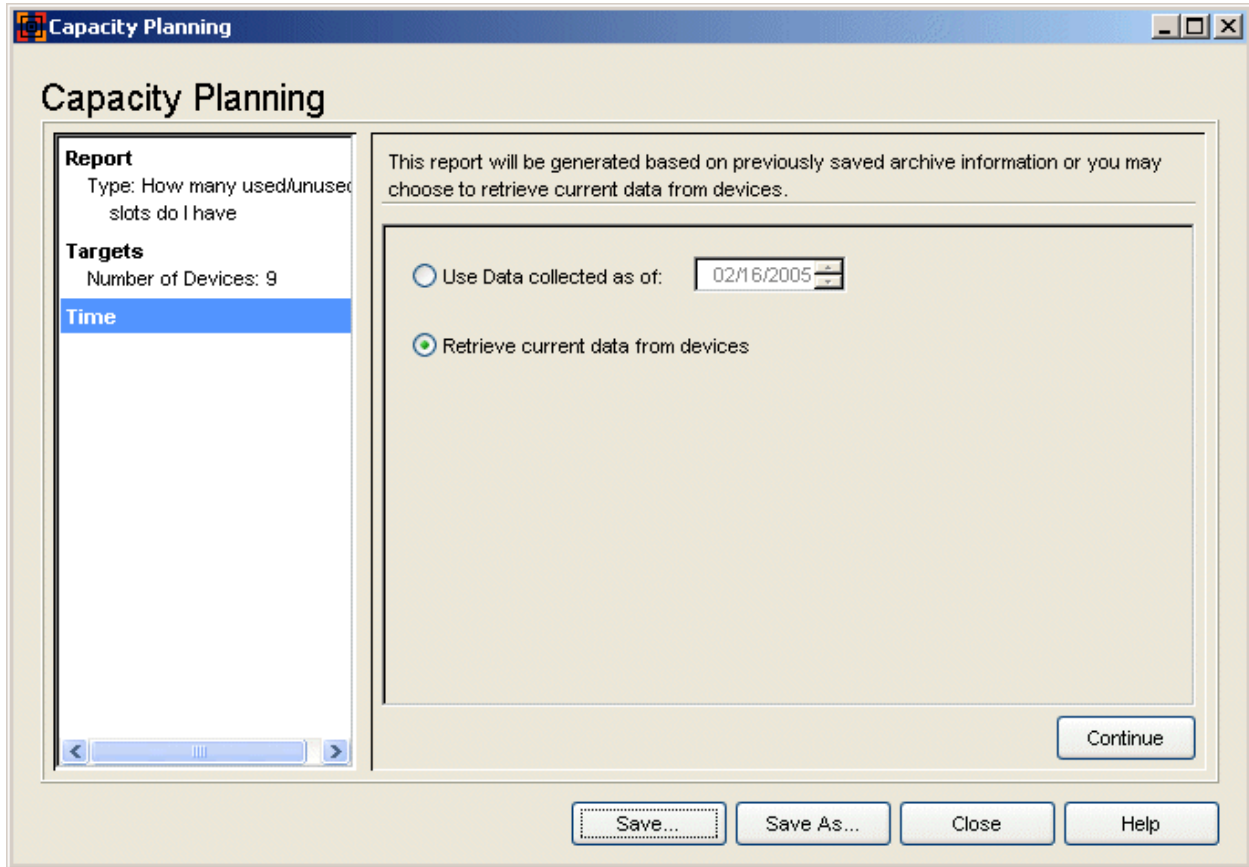
Deletes any filters selected in the Applied Filters list.

### View Devices Button

Opens the [View Devices window](#) where you can see a list of the selected devices that will be included in your report.

## Specify Time Window

Use this window to select a date from which report data will be gathered. In most cases, you will want to generate the report using current data from your devices. However, you can also generate a report based on historical data. In that case, the report will be generated using device data saved in the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used (see [How to Archive](#) for more information.)



### Use data collected as of

Report data will be collected based on the date selected here. Calculations are based on the last archive preceding the specified date. Only archive operations that are configured to archive capacity planning data will be used. If there is no archive for a target device, that device will not be represented in the report results.

If you use this option, be aware that your target selection could affect the validity of your report results. For more information, see the [Note](#) in the Target window section of this Help topic.

### Retrieve current data from devices

The report will use current data from the target devices. Because this requires the report to gather current data from the devices, extra time may be needed when results are calculated.

## Slot Results Window

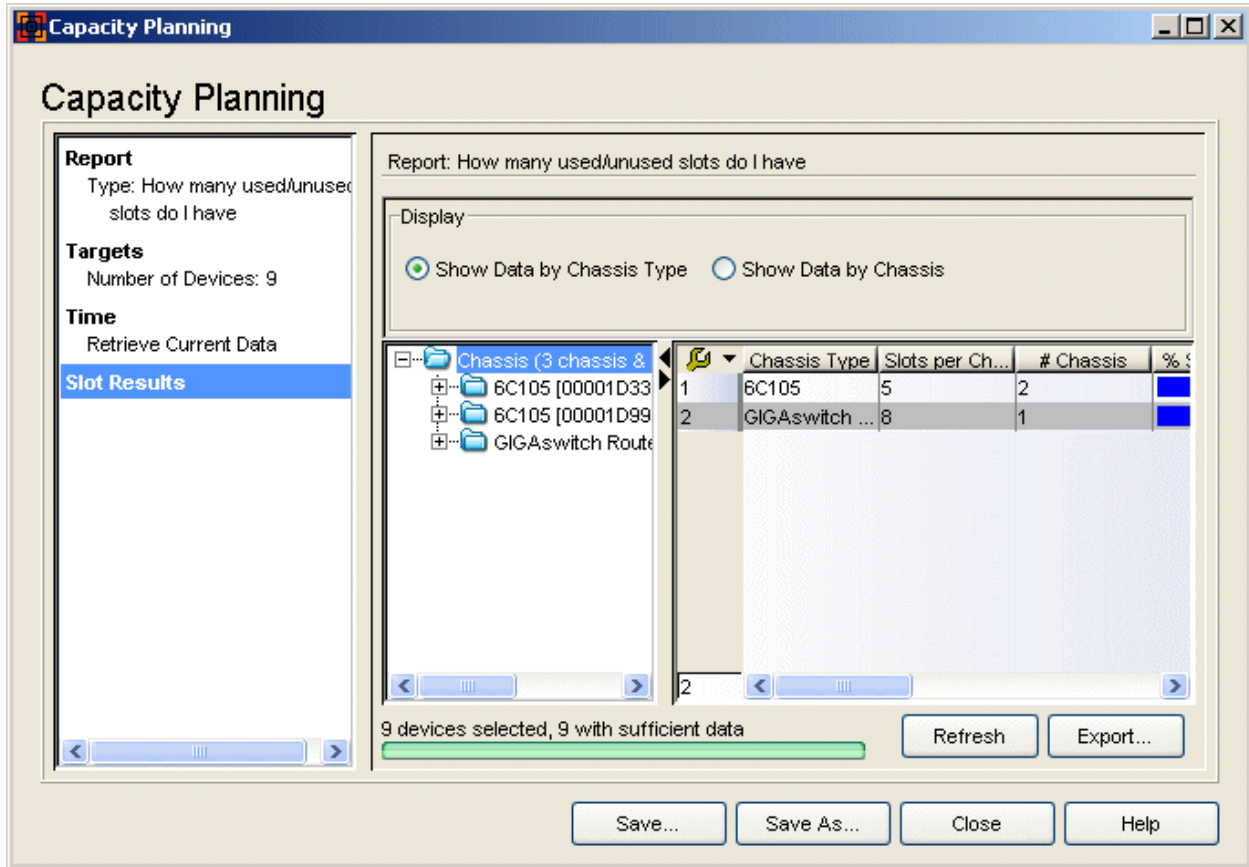
Use this window to view the report data. The radio buttons at the top of the right panel let you select various ways to display the report results:

- [Show Data by Chassis Type](#) -- displays the report results organized by totals based on chassis type.
- [Show Data by Chassis](#) -- lists the report results for each chassis.

In addition, your selection in the tree determines the results displayed in the table. For example, you can select a chassis group and view report data for that group. Then, you can expand the group and view data for a specific chassis. As you change your selection in the tree, the table is updated with the results for your specific selection.

### *Slot Results - Show Data by Chassis Type*

The Show Data by Chassis Type view gives you the flexibility of viewing your slot results summarized by chassis type or detailed by chassis. It provides an easy way to view top-level slot information and quickly determine where to take a closer look. Simply by changing your selection in the tree, you can view slot data for all the chassis of a certain type, or slot data for an individual chassis.



## Display

Use these radio buttons to select how you would like the results data displayed.

## Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a chassis group to see results summarized by chassis type, or select an individual chassis to see results for just that chassis. When you change your selection in the tree, the table is updated with the relevant information. If you select an individual device in the target device tree, the information displayed pertains to the chassis the device resides in.

## Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results. Target devices that do not reside in chassis will be counted as having insufficient data.

## Table

The Show Data by Chassis Type table displays slot data for the selected chassis group or individual chassis, organized according to chassis type. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, or the device does not reside in a chassis, that device will not be represented in the report results.

---

**NOTE:** Devices that do not return information for certain report requests will display "Unsupported" in the results table entry. If a chassis displays "Not Mapped" in its results table entry, it indicates that the device type is not in the Capacity Planning data file. If you encounter the "Not Mapped" entry, please contact Extreme Networks Support for an updated data file for these devices.

---

### Chassis Type

The chassis model number or hardware type.

### Slots per Chassis

The total number of slots in one chassis of that chassis type.

### # Chassis

The total number of chassis of that type.

### % Slot Used

The percentage of slots of that chassis type being used.

### Total Slots

The total number of slots in all the chassis of that type.

### # Slots Used

The total number of slots of that chassis type being used.

### # Slots Unused

The total number of slots of that chassis type that are not in use.

### Average Slots Used

The average number of slots of that chassis type being used.

### Average Slots Unused

The average number of slots of that chassis type that are not in use.

## Slot Results - Show Data by Chassis

The Show Data by Chassis view lets you view slot data for each individual chassis. Depending on your selection in the tree, you can see report results for all the chassis in a group, or for just one individual chassis.

The screenshot shows the 'Capacity Planning' application window. On the left, a sidebar contains sections for 'Report', 'Targets', and 'Time', with 'Slot Results' highlighted. The main area displays a report titled 'Report: How many used/unused slots do I have'. Below the title, there are radio buttons for 'Show Data by Chassis Type' and 'Show Data by Chassis', with the latter selected. A tree view on the left shows a hierarchy of chassis, with 'Chassis (3 chassis & ...)' selected. The main table displays the following data:

	Chassis ID	Chassis Type	% Slots Used	Tr
1	00001D3317...	6C105	60%	5
2	00001D9932...	6C105	100%	5
3	00E063053980	GIGAswitch ...	75%	8

At the bottom of the window, it indicates '9 devices selected, 9 with sufficient data' and provides buttons for 'Refresh', 'Export...', 'Save...', 'Save As...', 'Close', and 'Help'.

### Display

Use these radio buttons to select how you would like the results data displayed.

### Target Device Tree

Displays your target groups and devices. Your selection in the tree determines what results data will be displayed in the table. For example, select a chassis group to see results for all the chassis in that group, or select an individual chassis to see results for just that chassis. When you change your selection in the tree, the table is updated with the relevant information. If you select an individual device in the target device tree, the information displayed pertains to the chassis the device resides in.

### Device Count, Sufficient Data

The total number of target devices, followed by the number of devices with sufficient data to report results. If you generated the report using historical data, a device is counted as having sufficient data if there is one archive used to obtain report results. Target devices that do not reside in chassis will be counted as having insufficient data.

### Table

The Show Data by Chassis table displays slot data for the selected chassis group or individual chassis. In most cases, your report will be generated using current data. However, if you generated your report based on historical data, the report will use device data saved in the last archive preceding the specified date. If there is no archive for a target device, or the device does not reside in a chassis, that device will not be represented in the report results.

---

**NOTE:** Devices that do not return information for certain report requests will display "Unsupported" in the results table entry. If a chassis displays "Not Mapped" in its results table entry, it indicates that the device type is not in the Capacity Planning data file. If you encounter the "Not Mapped" entry, please contact Extreme Networks Support for an updated data file for these devices.

---

### Chassis ID

The ID assigned to the chassis. This is usually a serial number or MAC address, depending on the chassis type.

### Chassis Type

The chassis model number or hardware type.

### % Slots Used

The percentage of slots being used in the chassis.

### Total Slots

The total number of slots in the chassis.

### Slots in Use

The chassis slot numbers being used by devices or DFE modules.

### # Slots Used

The number of slots being used in the chassis.

### # Slots Unused

The number of slots not being used in the chassis.



### Abort/Refresh Button

This button toggles between Abort and Refresh. While a report is being generated, Abort stops the report and clears all data out of the table. Refresh restarts report generation and updates the table with new data. If you have selected the **Retrieve current data from devices** option in the [Specify Time window](#), clicking Refresh allows you to update your report results with the latest data from your devices.

### Export Button

Allows you to export your report results table as an HTML file or as a delimited text file. A Save window opens where you can name your exported file, select the file extension, and navigate to a folder/directory where you want save the file.

### Save/Save As Button

Opens the Save Report window where you can name a report and then save it so that you can run the report again. You can also select a checkbox to schedule the report. This opens the [Schedule Report window](#) where you can configure scheduling information and notification settings for the report. Once you have saved a report, it appears in the Saved Reports list in the [Select Report window](#), where you can select it.

---

## Related Information

For information on related windows:

- [Capacity Planning](#)
- [Add Filters Window](#)
- [View Devices Window](#)
- [Schedule Report Window](#)

# Inventory Manager Wizards

---

Inventory Manager's Wizards let you easily perform routine network tasks such as configuration backups and firmware upgrades. Following is a summary of the different wizards Inventory Manager provides for your ease of use. Click each wizard name below for information on how to use the wizard.

<b>Wizard</b>	<b>Description</b>
<a href="#">Archive Wizard</a>	Create archives (backup copies) of your network devices' configurations that can be restored to the devices at a later date, if needed. The wizard's task scheduler allows you to easily schedule routine backups.
<a href="#">Restore Archive</a>	Restore saved configurations (archives) to one or more devices, allowing you to quickly and easily recover from a problem.
<a href="#">Reset Device Wizard</a>	Reset a single device, multiple devices, or even multiple device groups using timed or manual reset.
<a href="#">Firmware Upgrade Wizard</a>	Upgrade the firmware images on a single device or multiple devices simultaneously. The wizard gives you the flexibility of performing an immediate upgrade or scheduling the upgrade to take place at a later time.
<a href="#">Boot PROM Upgrade Wizard</a>	Upgrade the boot PROM images on a single device or multiple devices simultaneously.
<a href="#">Template Download Wizard</a>	Download text-based (ASCII format) configuration templates to one or more devices. Configuration templates provide an easy way to download similar configurations to multiple devices.

## Archive Wizard

---




Use the Archive Wizard to archive device configuration data and/or capacity planning data. Archiving device configuration data lets you create archives (backup copies) of your network devices' configurations that can be restored to the devices at a later date, if needed. Archiving capacity planning data lets you store port and FRU information for use by the [Capacity Planning](#) tool to generate reports. You can create an archive that saves both configuration data and capacity planning data, or you can create an archive that targets one type of data or the other.

You can perform archives on a single device, multiple devices, or on an entire device group. Because it is useful to archive data on a regular basis, Inventory Manager lets you schedule archives to be performed at a future time, and/or on a routine basis. Once you have configured an archive's parameters, you can use that archive on a repeated basis to save new versions of the desired data. For example, you may want to create an archive that saves your device configurations on a weekly basis, and also create an archive that saves only capacity planning information on a daily basis to monitor what is changing on the network.

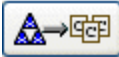
---

**TIP:** You can set up an e-mail notification based on the event log message that is generated when a configuration change is detected. When the current archive differs from the previously saved archive, Inventory Manager generates an event log message. Using the NetSight Console Alarms Manager you can create an alarm that monitors the Inventory Log for the text "Configurations Are Different" and define an e-mail to be executed as the specific alarm action.

---

Once an archive operation has been created, it is listed by name in the left-panel [Archive Mgmt tab](#) under the Archives folder. Below the archive name are the archive versions, displayed by the date and time the version was performed. Under the versions are the individual configurations, listed by IP address of the device whose data was saved. Each configuration displays an icon that identifies the type of data being saved:  device configuration data,  capacity planning data,  both device configuration and capacity planning data.

To access the wizard, select **Tools > Wizards > Archive Wizard** from the menu

bar or click  on the toolbar. You must have a TFTP or FTP server running

to create an archive. For more information, see [TFTP Server Setup](#) or [FTP Server Setup](#).

**NOTE:** If the device is an X-Pedition router, be aware that when archiving device configuration data, the router's Startup configuration file is saved.

## Archive Name Window

Use this window to name and configure the archive.

Archive Wizard

### Archive Name

Input an archive name and an optional description of the archive. You can also set the number of archive versions you wish to store.

Name: Floor Two Archive

Description: Archive Floor Two Building A

Archive Setup

Archive Type

- Archive Configuration Data
- Archive Capacity Planning data

Max Versions

Select the number of archive versions

- Maximum number of versions 30
- No maximum number of versions

Next Cancel Help

### Name

Enter a name for the archive operation.

### Description

Enter a description (optional) of the archive operation.

## Archive Setup

### Archive Type

Select the appropriate checkbox for the type of data you wish to archive:

- **Archive Configuration Data** - Create archives (backup copies) of your devices' configurations that can be restored to the devices at a later date, if needed.
- **Archive Capacity Planning data** - Create archives of port and FRU information to be used by the [Capacity Planning](#) tool to generate reports.

### Max Versions

If desired, specify the maximum number of versions you would like saved for this archive. This allows you to limit the number of versions saved for each archive. Once the maximum number is reached, older versions are automatically deleted. Otherwise, you can select to not have a maximum number of archive versions.

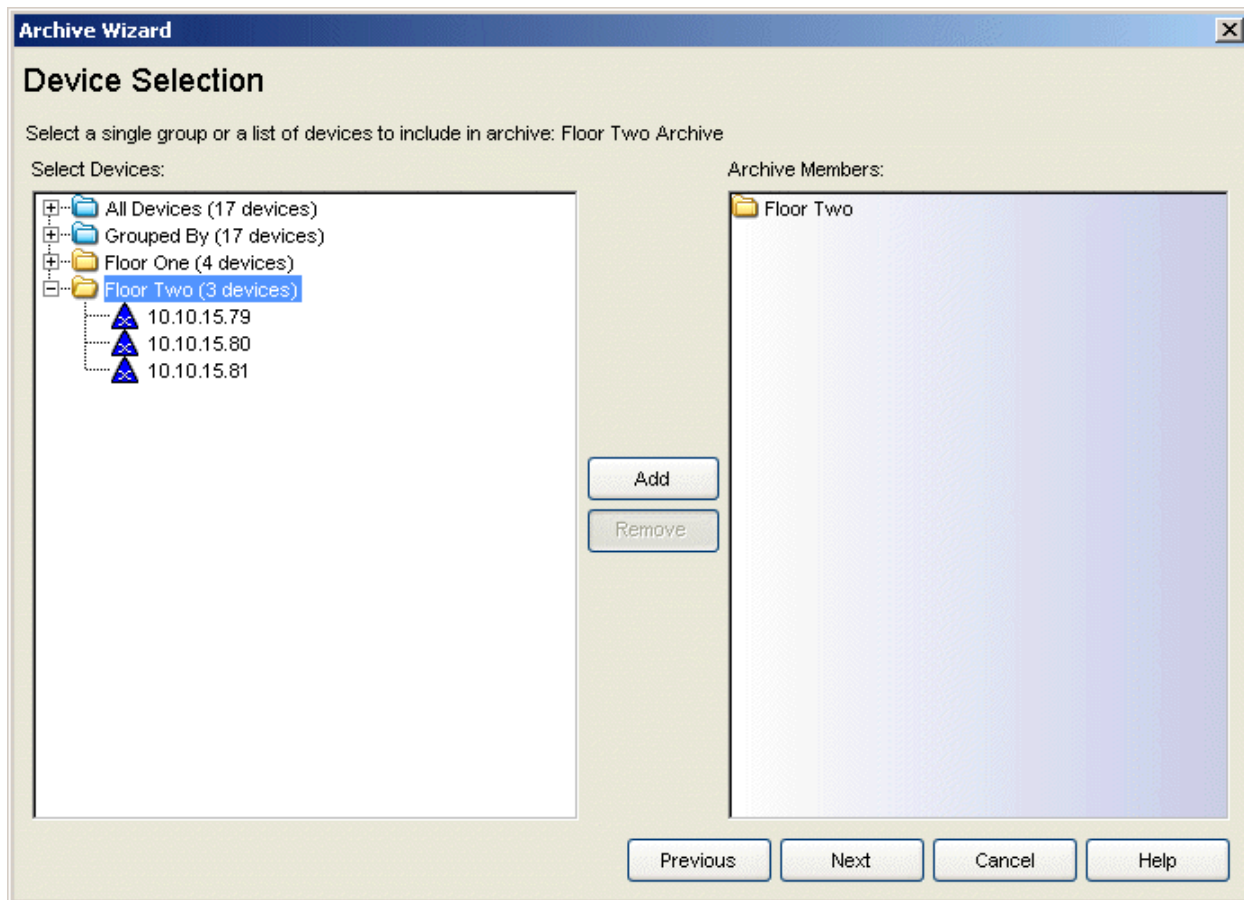
## Device Selection Window

Use this window to select the devices to include in the archive.

---

**NOTE:** If you select multiple tree nodes representing the same device but with varying SNMP contexts, an archive save will be performed for each context. However, the context must provide access to the MIBs required for the archive save operation or the archive for that context will fail. It is recommended that you perform the archive operation on the device with the default context (switch mode.)

---



### Select Devices

This panel displays your current devices as they are listed in the left-panel [Network Elements tab](#). Expand the folders and select the single device, multiple devices (using the Control or Shift keys,) or a single device group that you want to include in the archive. Click the **Add** button to add the devices to the Archive Members list.

### Archive Members

The devices you have selected are listed under Archive Members. If you want to remove a member from the list, select the member and click **Remove**.

---

**TIP:** If you open the Archive Wizard from a device or device group in the left-panel Network Elements tab, the selected device or device group will be automatically displayed under Archive Members.

---

### Add Button

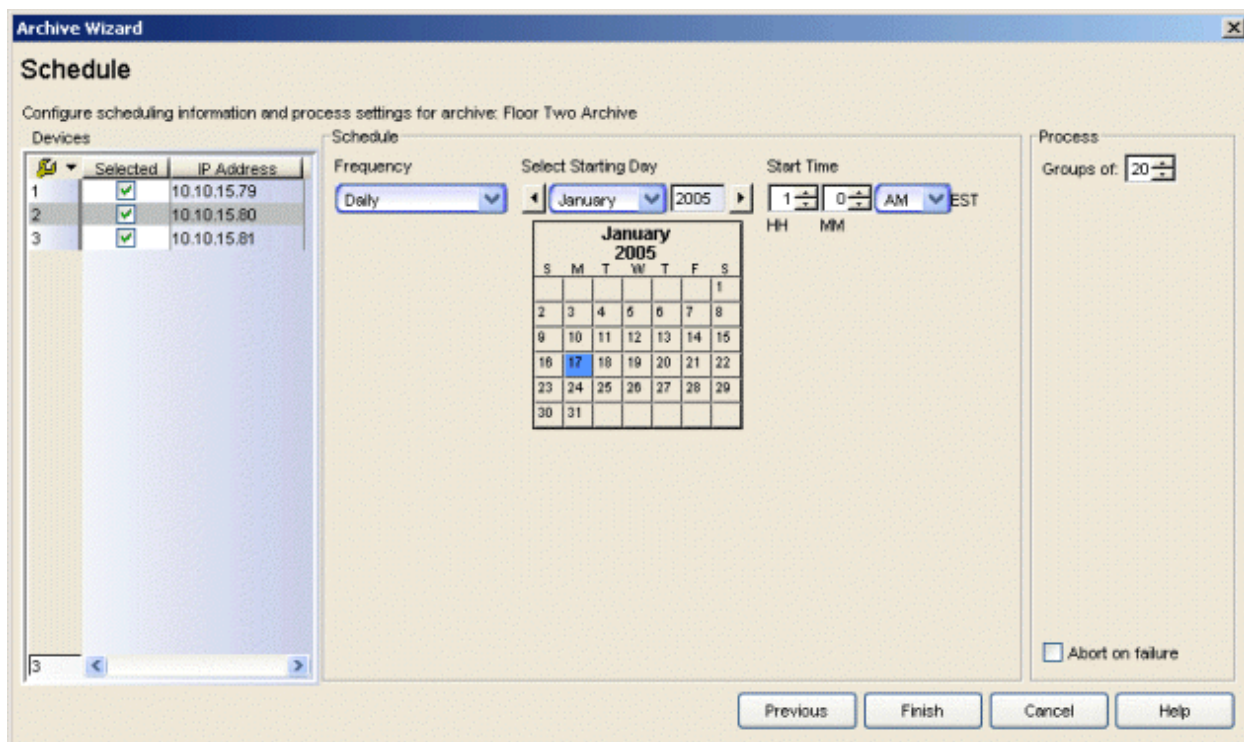
In the Devices tree, select the device(s) or device group you want to archive, and click **Add** to add it to the Archive Members list.

## Remove Button

Select a device or device group in the Archive Members list, and click **Remove** to remove it from the list.

## Schedule Window

Use this window to select devices, and configure scheduling information and process settings for the archive. You can schedule a one-time, daily, or weekly archive, or schedule the archive to be performed on server start-up.



### Devices

#### Selected

Use the checkboxes in this column to select or deselect specific devices to be archived. For example, if you selected a device group in the previous window, you can use these checkboxes to deselect individual devices in that group.

#### IP Address

The IP address of the device to be archived. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a

single management IP even though there may be multiple DFE modules in the chassis.

## *Schedule*

### **Frequency**

Use the drop-down list to select the frequency with which you want the archive performed: **Never**, **Now**, **Once**, **Daily**, **Weekly**, or **On Server Startup**. The Never option lets you create an archive operation without actually performing it. The Now option lets you perform an immediate archive.

### **Select Starting Day**

Use the drop-down list to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. (This field is grayed out if you have selected the Never or Now frequency.)

### **Start Time**

Set the starting time for the operation and select AM or PM. (This field is grayed out if you have selected the Never or Now frequency.)

## *Process*

### **Groups of**

The archive will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Set the value to **1** to have the operation performed serially, one device after another.

### **Abort on failure**

Select the **Abort on failure** checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.

### **Finish Button**

Creates the archive. The archive will be listed by name in the left-panel [Archive Mgmt tab](#) under the Archives folder, and performed according to its scheduled parameters. You can change the archive's parameters; see [Editing an Archive](#) for instructions.








## Related Information

For information on related tasks:

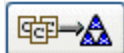
- [How to Archive](#)
- [How to Restore an Archive](#)
- [How to Compare Archives](#)

## Restore Wizard

---

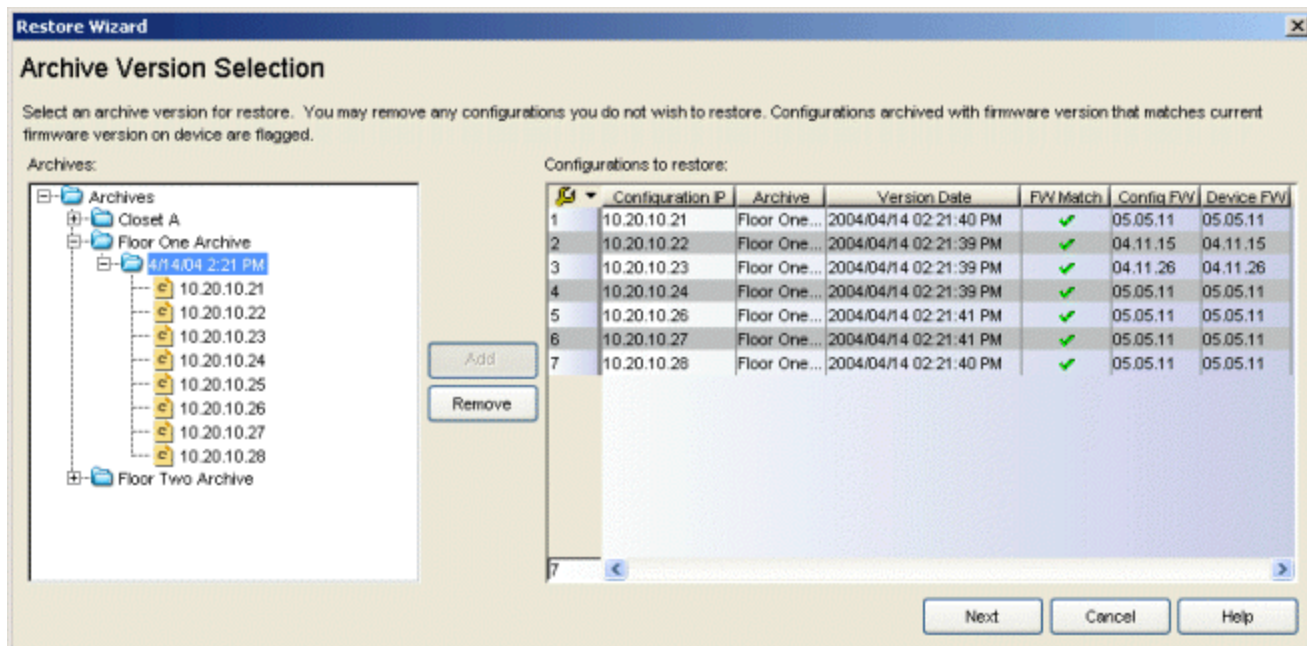
Use the Restore Wizard to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel [Archive Mgmt tab](#) under the appropriate archive and version. Each configuration displays an icon that identifies the type of data that was saved:  device configuration data,  capacity planning data,  both device configuration and capacity planning data. Only configurations that include device configuration data (  and  ) are available to be restored.

A configuration can only be restored to a device with the same IP address. In other words, the device you are restoring *to* must have the same IP address as the device the configuration was originally saved *from*. You can restore configurations to a single device or multiple devices. You must have a TFTP or FTP server running to restore a configuration. For more information, see [TFTP Server Setup](#) or [FTP Server Setup](#).






To access the wizard, select **Tools > Wizards > Restore Wizard** from the menu bar or click  on the toolbar.

## Archive Version Selection Window

Use this window to select an archive version or single configuration to restore. If you select an archive version, you can use the **Remove** button to remove any individual configurations included in the archive version that you do not wish to restore.



## Archives

This panel displays your current archives just as they are listed in the left-panel [Archive Mgmt tab](#). Below each archive name are the archive versions, displayed by the date and time the version was performed. Under the versions are the individual configurations, listed by IP address of the device whose configuration was saved. Each configuration displays an icon that identifies the type of data that was saved:  device configuration data,  capacity planning data,  both device configuration and capacity planning data. Only configurations that include device configuration data (  and  ) are available to be restored.

Expand the folders under the Archives tree and select the archive version or configuration you want to restore. Click the **Add** button to add the configurations to the Configurations to Restore table.

- 
- TIPS:** -- If you open the Restore Wizard from an archive version or configuration in the left-panel Archive Mgmt tab, the selected configuration(s) will be automatically displayed under Configurations to Restore.
- Check the FW Match column to see if the current firmware version on the device matches the firmware version that was on the device at the time of the archive.
- 

## Configurations to Restore

Displays the configurations you have selected to restore. Select a configuration and use the **Remove** button to remove any individual configurations you do not

wish to restore.

### Configuration IP

The IP address of the device whose configuration was saved.


### Archive

The name of the archive operation that saved the configuration.

### Version Date

The date and time that the archive operation was performed.

### FW Match

A  indicates that the current firmware version installed in the device matches the firmware version installed in the device at the time of the configuration save.

### Config FW

The firmware version installed in the device at the time of the configuration save.

### Device FW

The current firmware version installed in the device.

### Add Button

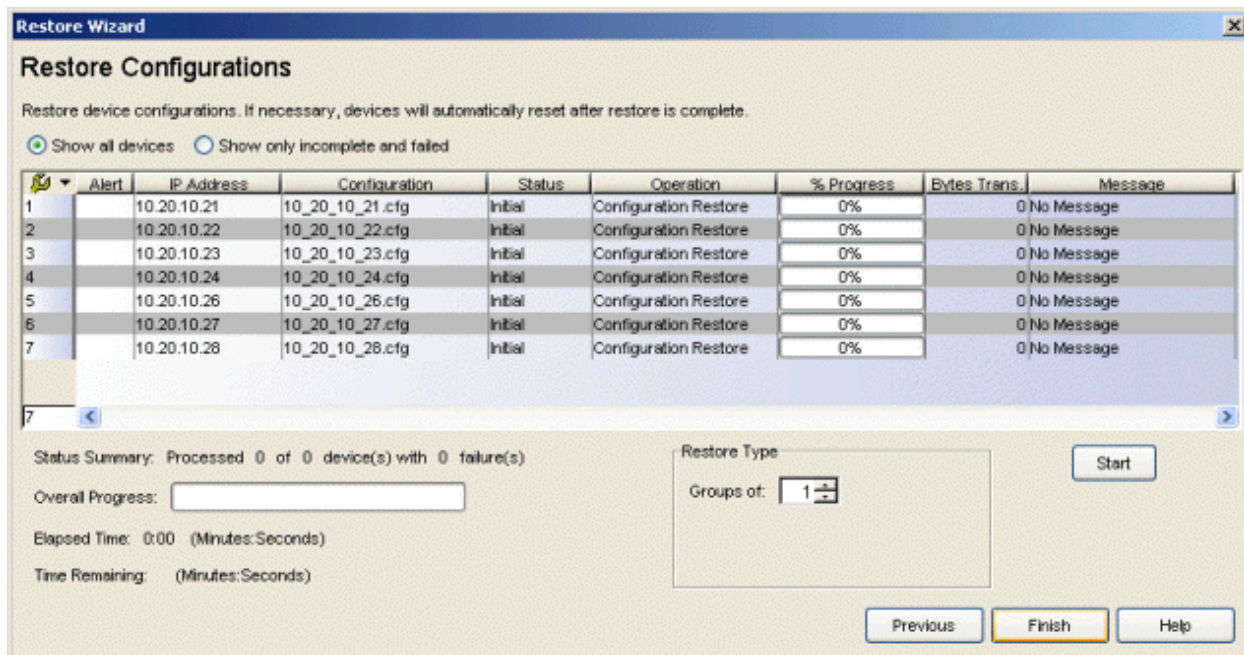
In the Archives tree, select the archive version or configuration you want to restore, and click **Add** to add it to the Configurations to Restore table.

### Remove Button


Select a configuration in the Configurations to Restore table, and click **Remove** to remove it from the table.

## Restore Configurations Window

Use this window to configure restore parameters, initiate the restore operation, and monitor restore progress. Devices that require a reset will be reset automatically after the restore is complete.




### Show all devices/Show only incomplete and failed

Once the restore operation starts, the device list table updates with status information for each device. An alert icon  will appear in the Alert column of the table if a restore operation fails for a specific device. You can use these radio buttons to show all devices or show only those devices whose restore operations are incomplete or have failed.


### Device List Table

A list of the devices you have selected for your restore operation. Once the restore is started, this table updates with status information for the restore operation:

- **Alert** - an alert icon  will appear in the Alert column if a restore operation fails for a specific device.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Configuration** - The name of the configuration file being restored.
- **Status** - The status of the operation for that particular device: Success or Failure.
- **Operation** - The type of operation performed: Configuration Restore.

- **% Progress** - A progress bar showing the percent completed of the operation.
- **Bytes Trans.** - The number of bytes transferred during the operation.
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Status Summary

Once the restore is started, this area updates with status information for the restore operation.

### Restore Type

The restore will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. By default, the restores will occur in sequential order (Groups of: 1). This is to protect against possible isolation of other devices that are on the restore list.

---

**CAUTION:** Because some devices automatically reset following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. It is recommended that you leave the **Groups of** value at 1 (perform the restore serially,) unless you know it is safe to have the selected network devices reset simultaneously.

---

### Start Button

Initiates the restore operation. The table at the top of the window updates with status information, as will the status area in the bottom left of the window.

---

## Related Information

For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)
- [How to Reset a Device](#)

## Reset Device Wizard

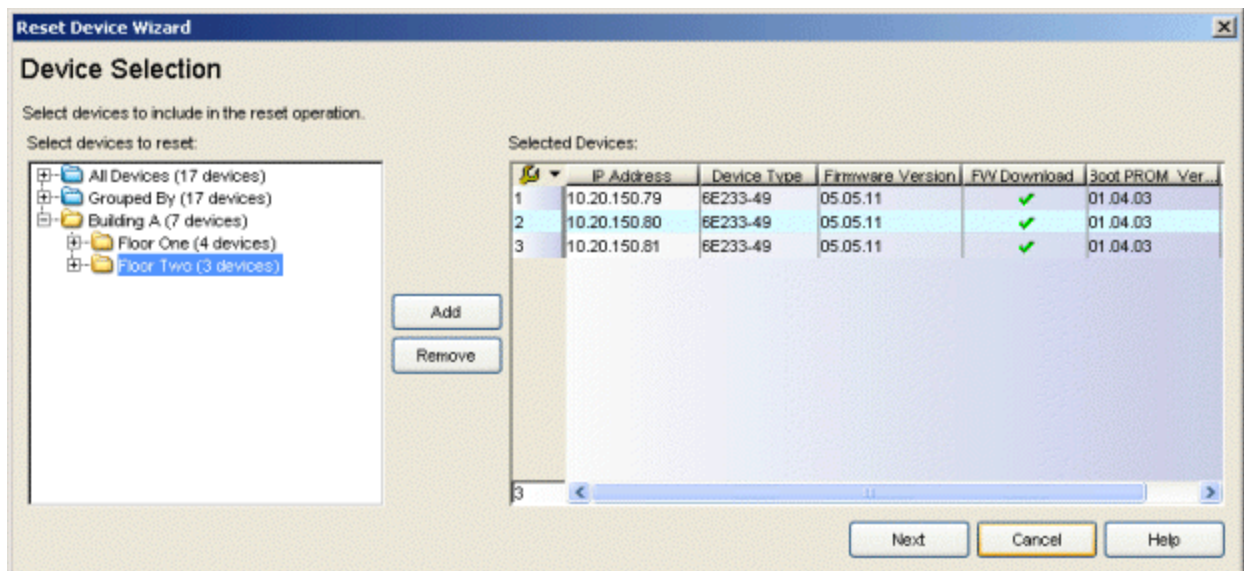
Use the Reset Device Wizard to reset a single device, multiple devices, or even multiple device groups. The Reset Device Wizard allows you to reset devices that support Timed Reset as well as those devices that do not. Timed Reset gives you the flexibility to schedule your reset operation, so that the actual device resets take place at a later time.

To access the wizard, select **Tools > Wizards > Reset Wizard** from the menu bar or click  on the toolbar.

## Device Selection Window

Use this window to select the devices to include in the reset operation.

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).



### *Select devices to reset*

This panel displays your current devices as they are listed in the left-panel [Network Elements tab](#). Expand the folders and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys) that you want to reset. Click the **Add** button to add the devices to the Selected Devices table.

---

**TIP:** If you open the Reset Device Wizard from a device or device group in the left-panel [Network Elements tab](#), the selected device(s) will be automatically displayed in the Selected Devices table.

---

### *Selected Devices*

Lists the devices selected for the reset operation. Devices that do not support the reset operation or have never been contacted, are not listed. If you want to remove a device from the table, select the device and click **Remove**.

#### **IP Address**

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.


#### **Device Type**

The device's model number or hardware type.

#### **Firmware Version**

The current firmware version installed in the device.


#### **Firmware Download**

A  indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

#### **Boot PROM Version**

The current version of Boot PROM installed in the device.

#### **Boot PROM Download**

A  indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

#### **Add Button**

Select a single device or device group, or multiple devices or device groups, and click **Add** to add them to the Selected Devices table.

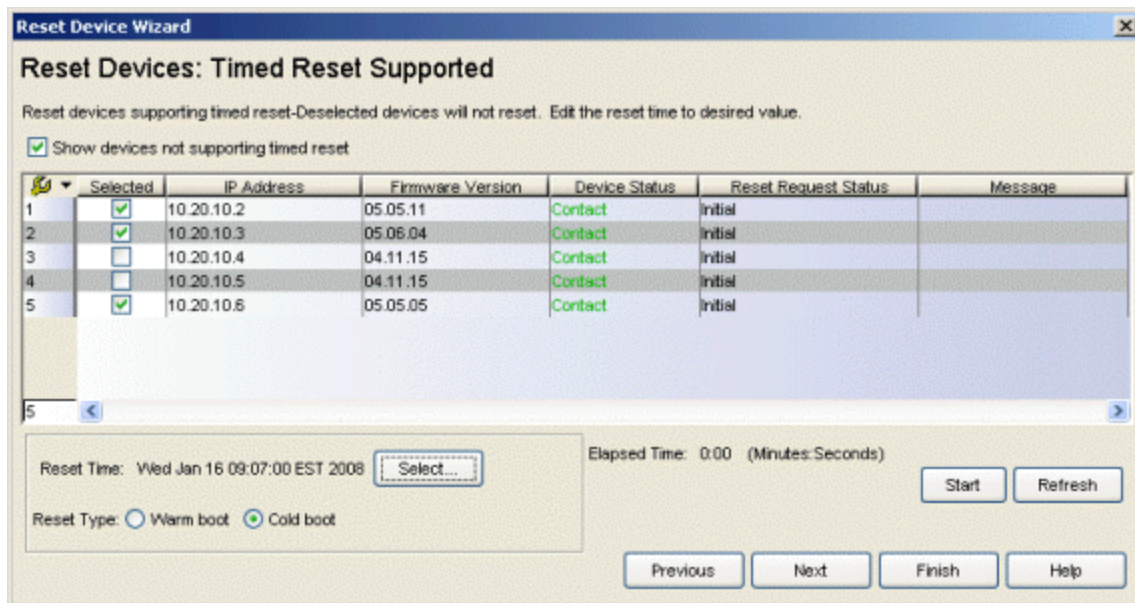


## Remove Button

To remove a device from the Selected Devices table, select the device and click **Remove**.

## Reset Devices: Timed Reset Supported Window

Use this window to reset those devices that support Timed Reset. Timed Reset gives you the flexibility to schedule your reset operation, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.



## Show devices not supporting timed reset

This window lists those devices that support Timed Reset. Select this checkbox to include devices that do **not** support timed reset. Devices that do not support timed reset cannot be reset from this window; proceed to the next window to reset those devices.


## Device List Table

A list of the devices you have selected for your reset operation. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset. Devices that do not support timed reset cannot be selected.

- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Firmware Version** - The current firmware version installed in the device.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.
- **Reset Request Status** - The status of the reset operation: Initial (the operation has not started), Success (the operation succeeded), Failure (the operation failed).
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Reset Time

This field displays the date and time the reset is scheduled to take place. Click the **Select** button to open the Select Reset Time window where you can schedule a date and time for the reset. Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. Set the starting time for the operation and select AM or PM.

### Reset Type

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

### Elapsed Time

The amount of time in minutes:seconds since the reset operation started.

### Start Button

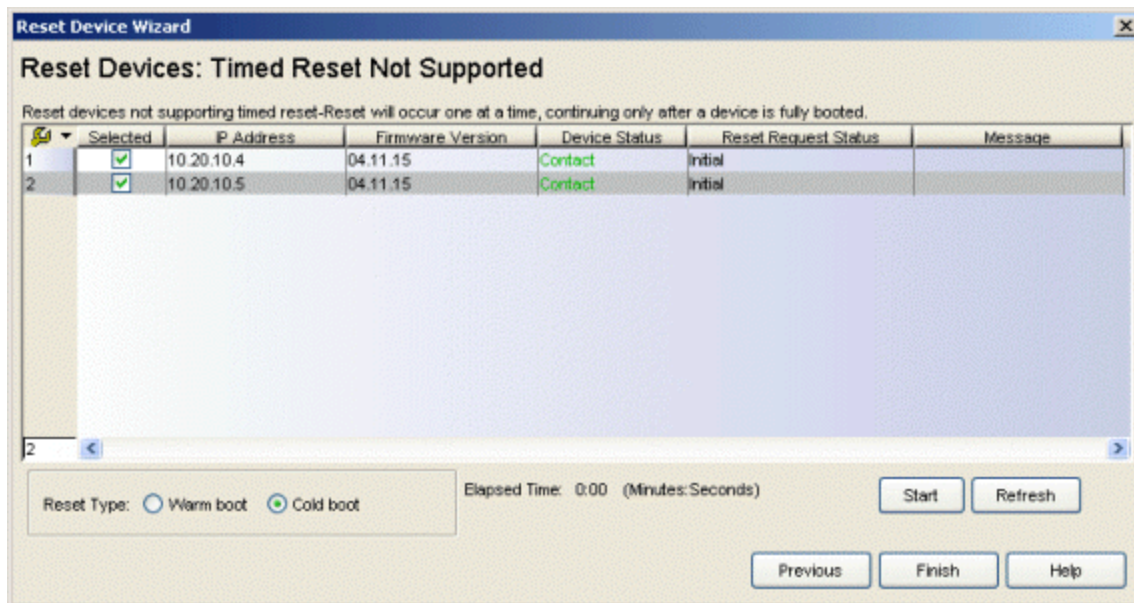
Starts the timed resets. Resets occur simultaneously. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

## Refresh Button

Once the reset operation has started, use the **Refresh** button to update the device information in the table.

## Reset Devices: Timed Reset Not Supported Window

Use this window to reset those devices that do not support Timed Reset. Devices will be reset one at a time, waiting until a device is fully booted before beginning the next device.




## Device List Table

Lists those devices that do not support timed reset. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Firmware Version** - Shows the current firmware version installed in the device.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.

- **Reset Request Status** - The status of the reset operation.
  - **Message** - A message relating to the status of the operation.
- 

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Reset Type

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

### Elapsed Time

The amount of time in minutes:seconds since the reset operation started.

### Start Button

Initiates the reset operation. Resets occur one at a time, continuing only after a device is fully booted. After the reset operation is completed, you can click **Refresh** to update the device information in the table.

### Refresh Button

Once the reset operation has completed, use the **Refresh** button to update the device information in the table.

---

## Related Information

For information on related tasks:

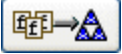
- [How to Reset a Device](#)
- [How to Upgrade Firmware](#)
- [How to Upgrade Boot PROM](#)

## Firmware Upgrade Wizard

---

Use the Firmware Upgrade Wizard to easily upgrade the firmware images on your network devices. The wizard gives you the flexibility of performing an immediate upgrade or scheduling the upgrade to take place at a later time. If you schedule the upgrade, the wizard will automatically perform the upgrade at the scheduled time, and then alert you that the upgraded devices need to be reset via the Reset Wizard.

You can also use the Firmware Upgrade Wizard to upgrade the firmware images on your NAC (64-bit) hardware and virtual appliances, and your Application Analytics hardware and virtual appliances.

To access the wizard, select **Tools > Wizards > Firmware Upgrade Wizard** from the menu bar or click  on the toolbar.

There are certain steps you must perform before you can upgrade your firmware. The steps vary depending on whether you are using a mapped file transfer server (as configured in the Suite-Wide Option Services for NetSight Server view) or an alternate remote file transfer server (as configured in the [Alternate Firmware Servers view](#) in the Options window) to perform the upgrade. For instructions, see [Preparing to Upgrade](#).

**NOTE:** The Firmware Upgrade Wizard can also be used to downgrade firmware to a previous revision. Downgrading firmware is inherently risky due to possible feature differences between revisions. Restoring configurations from different firmware revisions carries the same risk. Should you need to downgrade your firmware to an earlier version, it is recommended that you use **one** of the following two procedures:

- Downgrade the firmware on a network device using the Firmware Upgrade Wizard. Do not proceed to the Reset Devices portion of the wizard, instead select [Finish]. Restore an archived configuration that was previously created with the firmware image being downloaded. This will reset the device.
- or**
- Downgrade the firmware on a network device using the Firmware Upgrade Wizard. Complete the downgrade using the wizard Reset Devices screens. Clear NVRAM on the device and reconfigure the network configuration parameters of the device using the local console.

In addition, when downgrading firmware on SNMPv3 devices, it is possible that Inventory Manager will lose contact with the device. SNMPv3 adds a level of difficulty to downgrade operations, because counters and timers related to security features of SNMPv3 may get out of sync. Following the downgrade, you will need to restart Inventory Manager to re-establish contact with the device.

---

**CAUTION:** Prior to upgrading firmware on a device, it is recommended that you archive the latest configuration for the device being upgraded. This will aid you in downgrading should you choose to do so.

In addition, if you are upgrading devices that support HAU (Highly Available Upgrade) you should perform a [Firmware Discovery](#) or Refresh to ensure you have the latest HAU values before launching the firmware wizard.

---

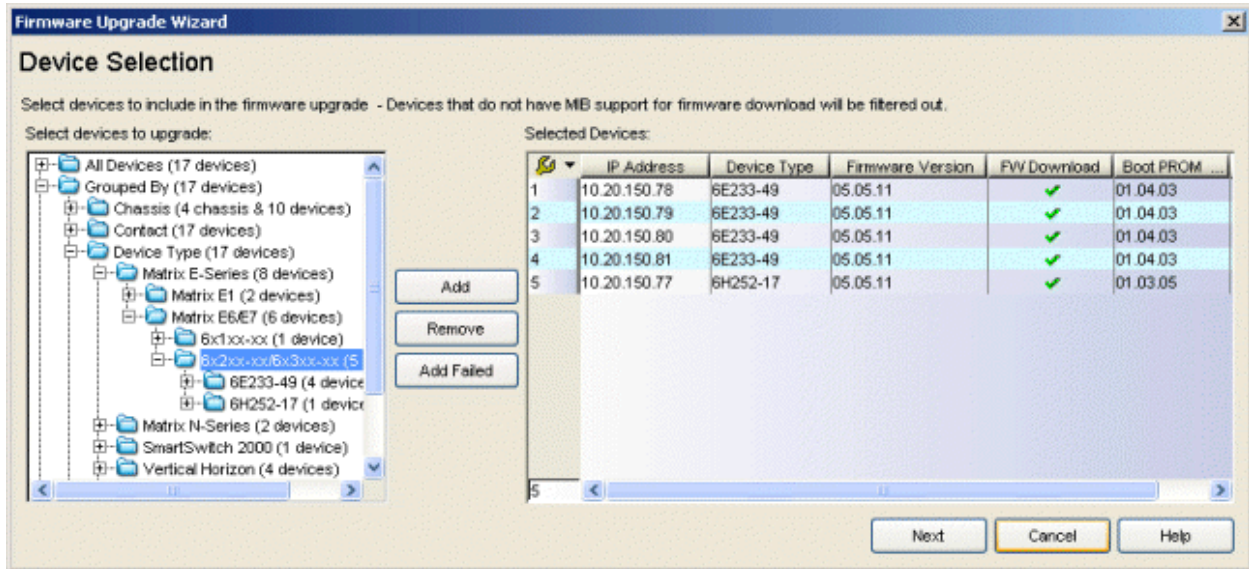
## Device Selection Window

Use this window to select the devices to include in the firmware upgrade operation.

---

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).

---



### Select devices to upgrade

This panel displays your current devices as they are listed in the left-panel [Network Elements tab](#). Expand the folders and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys) that you want to upgrade. Click the **Add** button to add the devices to the Selected Devices table. If there were devices that failed the previous upgrade, use the **Add Failed** button to add those devices to the table.

**TIP:** If you open the Firmware Upgrade Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed in the Selected Devices table.

### Selected Devices

Lists the devices selected for the upgrade operation. Devices that do not support firmware download or have never been contacted, are not listed. If you want to remove a device from the table, select the device and click **Remove**.

#### IP Address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

#### Device Type

The device's model number or hardware type.

**Firmware Version**

The current firmware version installed in the device.


**Firmware Download**

A  indicates the device supports the ability to download firmware images using this wizard.

**Boot PROM Version**

The current version of Boot PROM installed in the device.

**Boot PROM Download**

A  indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

**Add Button**

Select a single device or device group, or multiple devices or device groups, and click **Add** to add them to the Selected Devices table.

**Remove Button**

To remove a device from the Selected Devices table, select the device and click **Remove**.

**Add Failed Button**

If there were devices that failed the previous firmware upgrade, click the **Add Failed** button to add those devices to the Selected Devices table. This button will not be displayed if there are no devices that failed the previous upgrade.

## Firmware Selection Window

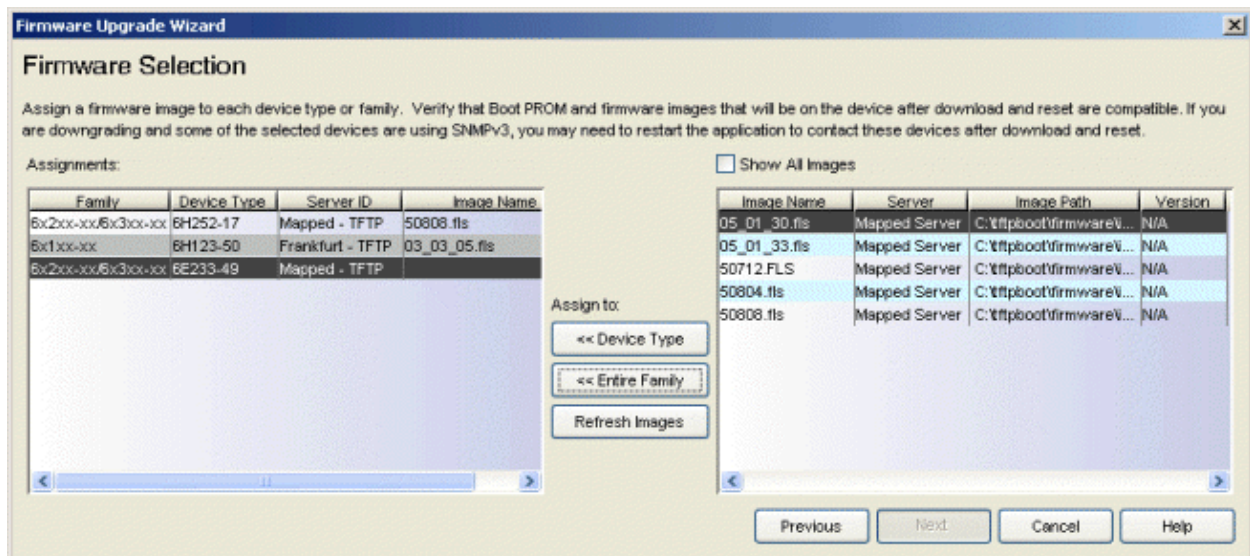
Use this window to select and assign the firmware images to be used in the upgrade. Firmware is assigned according to device type or binary family (device types that share the same firmware image). The left panel lists the device types selected for the firmware upgrade.

The right panel lists firmware images compatible with a selected device type. Use the **Assign to:** buttons to assign an image to a specific device type or to the entire binary family. You must assign an image to each device type. If there are no images listed, it means that there are no images in the firmware images directory on the NetSight server. You must first add your firmware images to the firmware directory and perform a firmware discovery. Inventory Manager uses the default tftpboot\firmware\images directory for storing your firmware. For more information, see the [Preparing to Upgrade](#) section of the How to Upgrade Firmware Help topic and the [Firmware Discovery](#) Help topic.



**NOTES:** If there are no images listed, it means that there are no images in the firmware images directory on the NetSight server. You must first add your firmware images to the firmware directory and perform a firmware discovery. Inventory Manager uses the default `tftpboot\firmware\images` directory for storing your firmware. For more information, see the [Preparing to Upgrade](#) section of the How to Upgrade Firmware Help topic and the [Firmware Discovery](#) Help topic.

Before proceeding with the upgrade, be sure to verify that the boot PROM and firmware images that will be on the device after the upgrade operation are compatible. Refer to the boot PROM and firmware release notes for more information.



## Assignments

This table lists the device types of all the devices selected for the firmware upgrade. Select a device type to display compatible firmware images in the right panel. If necessary, click the **Refresh Images** button to perform a firmware discovery and update the list of firmware images. Then, in the right-panel, select a firmware image and use the **Assign to:** buttons to assign the image to the device type or to each entry that is a member of that binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each device type.

**NOTE:** A device type group may include some devices that use the local mapped file transfer server for firmware downloads, and some that use an alternate remote firmware download server. In that case, the device type would have multiple entries in the Assignments table, one for each server. When you select an entry that uses an alternate server, only firmware records associated with that alternate server will be displayed in the Image list table (unless you select Show All Images.)

---

### Family

The product family to which the device type belongs.

### Device Type

The device's model number or hardware type.

### Server ID



The firmware download server specified for the device type. All devices are initially configured to use the mapped file transfer server (as configured in the Suite-Wide Option Services for NetSight Server view) for firmware downloads. You can specify an alternate firmware download server, which allows a remote device to use a server in its own local network. For more information see [How to Set Up Alternate Firmware Download Servers](#).

### Image Name

The firmware image assigned to the device type.

### HAU Compatible

HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, Inventory Manager will attempt to perform an HAU upgrade if the HAU firmware compatibility key is the same for the currently running firmware and the newly selected firmware. During firmware selection, Inventory Manager will attempt to determine if the keys are compatible. This column displays whether the firmware image and the device are HAU compatible. The icons specify:

-  (Compatible) - The firmware on the device has the same compatibility key as the newly selected firmware and a HAU upgrade will be performed.
-  (Not Compatible) - The firmware on the device does not have the same compatibility key as the newly selected firmware. Downloading images with different compatibility keys can cause the device to be unreachable while the upgrade completes.

- No Icon (Unknown) - Inventory Manager is unable to determine the compatibility key for either image.

---

**NOTE:** The firmware version currently running on the device must have been upgraded to the device using Inventory Manager in order for Inventory Manager to detect compatibility.

---

### *Image List*

This table lists all the compatible firmware images for the device type selected in the Assignments table. (If there are no images listed, see the [Note](#) above.) If you select a device type entry that uses an alternate remote firmware download server, only firmware records associated with that alternate server will be displayed. Select a firmware image and use the **Assign to:** buttons to assign the image to the selected device type or to the entire binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each device type. Use the **Refresh Images** button to perform a firmware discovery and update the list of firmware images, if desired.

### **Show All Images**

By default, only firmware images that are compatible with the selected device type are listed. Select the **Show All Images** checkbox to override this filter and display all your firmware images. If by selecting this checkbox you assign a firmware image that's associated with the mapped server, to a device type that specifies an alternate firmware download server, the wizard will use the mapped server to perform the download.

### **Image Name**

The name of the firmware image as it appears in your firmware images directory.

### **Server**

Displays the firmware download server associated with the firmware image. A discovered firmware image that is accessible by the mapped file transfer server (as configured in the Suite-Wide Option Services for NetSight Server view) will display "Mapped Server". A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#). For more information see [How to Set Up Alternate Firmware Download Servers](#).

### **Image Path**

The path to the location where the image is stored.

## Version

The version number of the firmware image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware upgrade using this image, this field will display N/A (not available).

## HAU Compatibility Key

HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, Inventory Manager performs the upgrade based on this status, and the comparison of the HAU firmware compatibility key on the current firmware with the key on the newly selected firmware.

During firmware selection, Inventory Manager will attempt to determine if the keys are compatible. This column displays the HAU Compatibility Key, if one is detected on the firmware image. The [HAU Compatible](#) column (in the Assignments table) displays whether the firmware image and the device are HAU compatible.

The following table explains the upgrade procedure for HAU devices.

<b>HAU Mode on Device</b>	<b>New Image HAU Compatible?</b>	<b>Upgrade Procedure</b>
Never	Yes	Standard Upgrade
Never	No	Standard Upgrade
If Possible	Yes	HAU
If Possible	No	Standard Upgrade
Always	Yes	HAU
Always	No	Upgrade Fails

---

**NOTE:** Firmware images that were discovered with a version of Inventory Manager prior to 4.4 will need to be removed from Inventory Manager and rediscovered in order to populate the compatibility key field.

---

### Assign to Device Type Button

Use the **Assign to: Device Type** button to assign a firmware image to the device type.

### Assign to Entire Family Button

Use the **Assign to: Entire Family** button to assign a firmware image to each entry that is a member of that binary family.

### Refresh Images Button

Performs a firmware discovery and updates the list of firmware images.

## Download Progress Window

Use this window to configure download parameters, start the download, and monitor download progress. Alternately, you can click **Schedule** to open the [Download Schedule window](#) where you can schedule the firmware download to take place in the background at a future time.

**Firmware Upgrade Wizard**

**Download Progress**

Show all devices  Show only incomplete and failed

Alert	IP Address	Image	Status	Operation	% Progress	Bytes Trans	Message
1	10.20.10.1	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
2	10.20.10.24	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
3	10.20.10.2	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
4	10.20.10.3	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
5	10.20.10.27	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
6	10.20.10.28	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
7	10.20.10.6	05_02_00.flr	Initial	Firmware Download	0%	0	Mapped Server, 05_02_00.flr
8	10.20.10.26	20202.flr	Initial	Firmware Download	0%	0	Frankfurt - TFTP, 20202.flr

Status Summary: Processed 0 of 0 devices with 0 failures

Overall Progress:


Elapsed Time: 0:00 (Minutes:Seconds)

Time Remaining: (Minutes:Seconds)

Download Type


Groups of:

### Show all devices/Show only incomplete and failed


Once the upgrade operation starts, the device list table updates with status information for each device. An alert icon  will appear in the Alert column of the table if a download operation fails for a specific device. You can use these radio buttons to show all devices or show only those devices whose download operations are incomplete or have failed.

## Device List Table

A list of the devices you have selected for your download operation. Once the download is started, this table updates with status information for the download operation:

- **Alert** - an alert icon  will appear in the Alert column if a download operation fails for a specific device.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Image** - The name of the image file being downloaded.
- **Status** - The status of the download operation: Initial (the operation has not started), Success (the operation succeeded), Failure (the operation failed).
- **Operation** - The type of operation performed: Firmware Download.
- **% Progress** - A progress bar showing the percent completed of the operation.
- **Bytes Trans.** - The number of bytes transferred during the download.
- **Message** - Initially, this column shows the file transfer server and the firmware image being used for the download operation. Once the download is started, it displays a message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

## Status Summary

Once the download is started, this area updates with status information for the download operation.

## Download Type

The downloads will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Enter the value **1** to have the downloads performed serially, one device after another.


## Start Button

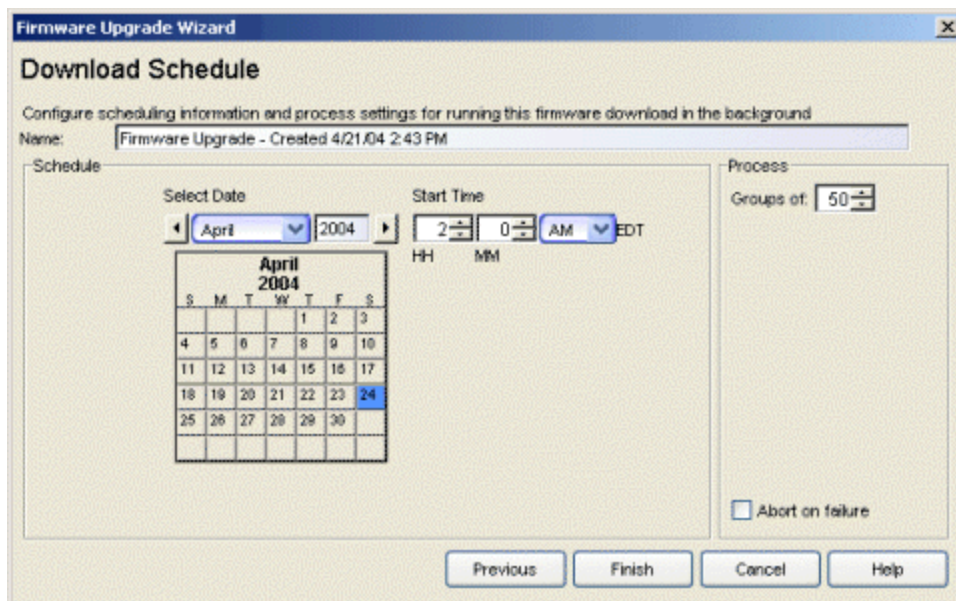
Initiates the download operation. The table at the top of the window updates with status information, as will the status area in the bottom left of the window.

## Schedule Button

Opens the [Download Schedule window](#) where you can schedule the firmware upgrade to take place in the background at a future time.

## Download Schedule Window

If you are scheduling your download for a future time, use this window to configure scheduling information and process settings for the download operation. Although a scheduled download runs automatically and does not require your supervision, you will still need to reset any devices that require reset, once the scheduled downloads have completed. After the firmware has been downloaded at the scheduled time, a Reset Device icon  is displayed in the status bar indicating that there are devices that have received new firmware images and need to be reset. Double-click the icon to open the Devices Need Reset window where you can launch the [Reset Device Wizard](#) for those devices.



## Name

Enter a name for the scheduled download, or use the default name which is based on the date the schedule is created.

## *Schedule*

### **Select Date**

Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field.

### **Start Time**

Set the starting time for the operation and select AM or PM.

## *Process*

### **Groups of**

The download will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Set the value to **1** to have the operation performed serially, one device after another.

### **Abort on failure**

Select the **Abort on Failure** checkbox to stop the download operation after a failure. This is useful if you are performing a download operation on multiple devices and you want the operation to stop after a failure on a single device.

### **Finish Button**

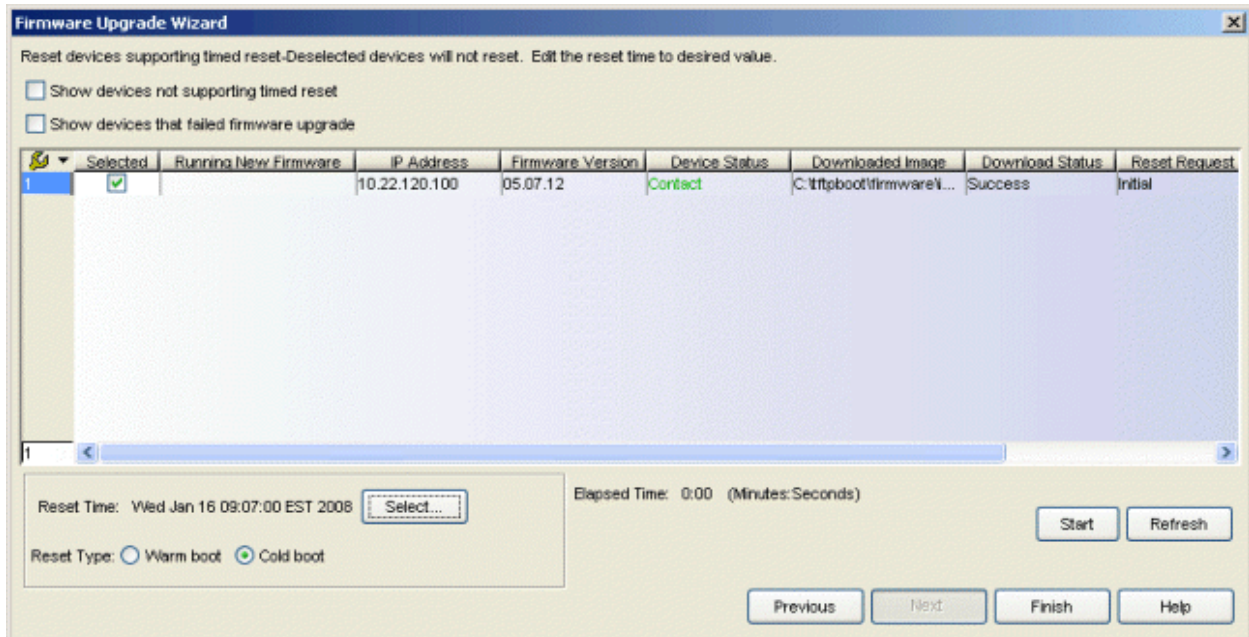
Schedules the download operation. When the scheduled download is performed, you can monitor the progress, if desired, via the Active Status panel, just as you do for scheduled archives. You can view or cancel scheduled downloads using the [Scheduled Events window](#) (Tools > Scheduled Events).

## **Reset Devices: Timed Reset Supported Window**

Once the downloads have completed, use this window to reset those devices that support Timed Reset. Timed Reset gives you the flexibility to schedule your reset operation, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.



**NOTE:** During the device reset, Inventory Manager learns the current firmware version installed on the device. Inventory Manager uses this information to determine whether the firmware version installed on the device matches the firmware reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).



### Show devices not supporting timed reset

This window lists those devices that support Timed Reset. Select this checkbox to include devices that do **not** support timed reset. Devices that do not support timed reset cannot be reset from this window; proceed to the next window to reset those devices.

### Show devices that failed firmware upgrade

Select this checkbox to include devices that failed the firmware upgrade.

### Device List Table


A list of the devices you have selected for your reset operation. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset. Devices that do not support timed reset cannot be selected.
- **Running New Firmware** - Following the reset, a ✓ indicates the device is running the new firmware version. (The checkmark is only displayed

if the firmware version changes.) Remember to click **Refresh** to update the information in the table following the reset.

- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Firmware Version** - Shows the current firmware version installed in the device. Following the reset, the new firmware version will be displayed. Remember to click **Refresh** to update the information in the table following the reset.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.
- **Downloaded Image** - The name of the image file that was downloaded.
- **Download Status** - The status of the download operation: Success (the operation succeeded), Failure (the operation failed).
- **Reset Request Status** - The status of the reset operation: Initial (the operation has not started), Success (the operation succeeded), Failure (the operation failed).
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

## Reset Time

This field displays the date and time the reset is scheduled to take place. Click the **Select** button to open the Select Reset Time window where you can schedule a date and time for the reset. Use the drop-down list to select the month you want the download to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. Set the starting time for the operation and select AM or PM.

### Reset Type

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

### Elapsed Time

The amount of time in minutes:seconds since the reset operation started.

### Start Button

Starts the timed resets. Resets occur simultaneously. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

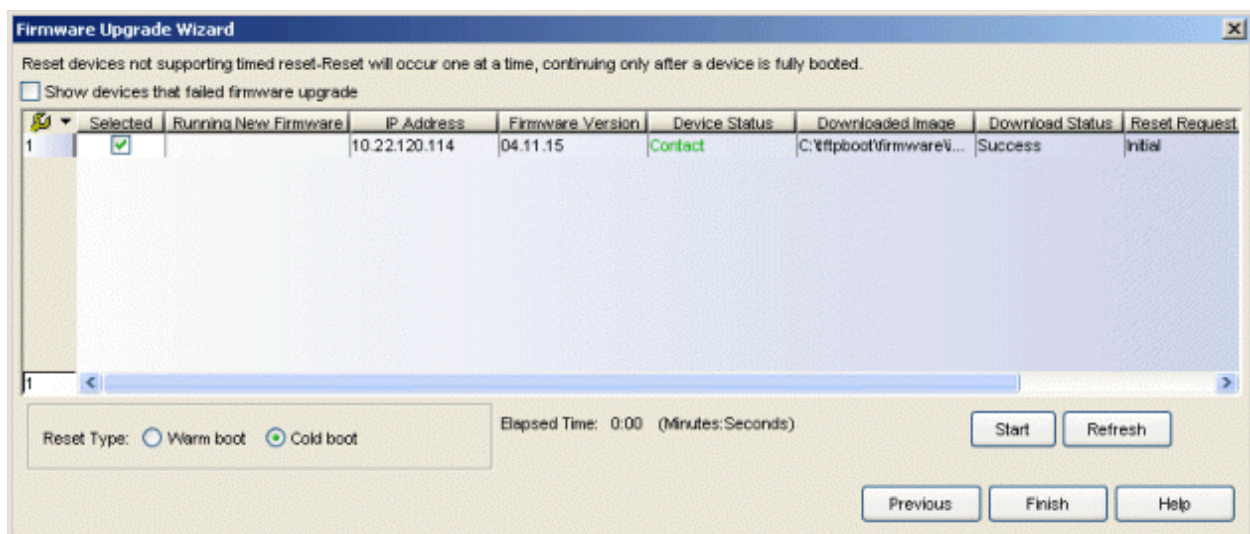
### Refresh Button

Once the reset operation has started, use the **Refresh** button to update the device information in the table.

## Reset Devices: Timed Reset Not Supported Window

Once the downloads have completed, use this window to reset those devices that do not support Timed Reset. Devices will be reset one at a time, waiting until a device is fully booted before beginning the next device.

**NOTE:** During the device reset, Inventory Manager learns the current firmware version installed on the device. Inventory Manager uses this information to determine whether the firmware version installed on the device matches the firmware reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).



## Show devices that failed firmware upgrade


Select this checkbox to include devices that failed the firmware upgrade.

## Device List Table

Lists those devices that do not support timed reset. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset.
- **Running New Firmware** - Following the reset, a ✓ indicates the device is running the new firmware version. (The checkmark is only displayed if the firmware version changes.) Remember to click **Refresh** to update the information in the table following the reset.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Firmware Version** - Shows the current firmware version installed in the device. Following the reset, the new firmware version will be displayed. Remember to click **Refresh** to update the information in the table following the reset.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.
- **Downloaded Image** - The name of the image file that was downloaded.
- **Download Status** - The status of the download operation: Success (the operation succeeded), Failure (the operation failed).
- **Reset Request Status** - The status of the reset request.
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

**Reset Type**

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

**Elapsed Time**

The amount of time in minutes:seconds since the reset operation started.

**Start Button**

Initiates the reset operation. Resets occur one at a time, continuing only after a device is fully booted. After the reset operation is completed, you can click **Refresh** to update the device information in the table.

**Refresh Button**

Once the reset operation has completed, use the **Refresh** button to update the device information in the table.

---

**Related Information**

For information on related tasks:

- [How to Upgrade Firmware](#)
- [How to Upgrade Boot PROM](#)
- [How to Reset a Device](#)

## Boot PROM Upgrade Wizard

---

Use the Boot PROM Upgrade Wizard to easily upgrade the boot PROM images on your network devices.

To access the wizard, select **Tools > Wizards > Boot PROM Upgrade Wizard**

from the menu bar or click  on the toolbar.

There are certain steps you must perform before you can upgrade your boot PROM images. The steps vary depending on whether you are using a mapped file transfer server (as configured in the Suite-Wide Option Services for NetSight Server view) or an alternate remote file transfer server (as configured in the [Alternate Firmware Servers view](#) in the Options window) to perform the upgrade. For instructions, see [Preparing to Upgrade](#).

---

**NOTE:** The Boot PROM Upgrade Wizard can also be used to downgrade boot PROM to a previous revision. Downgrading boot PROM is inherently risky due to possible feature differences between revisions. Restoring configurations from different firmware revisions carries the same risk. Should you need to downgrade your boot PROM to an earlier version, it is recommended that you use **one** of the following two procedures:

- Downgrade the boot PROM on a network device using the Boot PROM Upgrade Wizard. Do not proceed to the Reset Devices portion of the wizard, instead select [Finish]. Restore an archived configuration that was previously created with the boot PROM image being downloaded. This will reset the device.
- or**
- Downgrade the boot PROM on a network device using the Boot PROM Upgrade Wizard. Complete the downgrade using the wizard Reset Devices screens. Clear NVRAM on the device and reconfigure the network configuration parameters of the device using the local console.

In addition, when downgrading boot PROM on SNMPv3 devices, it is possible that Inventory Manager will lose contact with the device. SNMPv3 adds a level of difficulty to downgrade operations, because counters and timers related to security features of SNMPv3 may get out of sync. Following the downgrade, you will need to restart Inventory Manager to re-establish contact with the device.

---

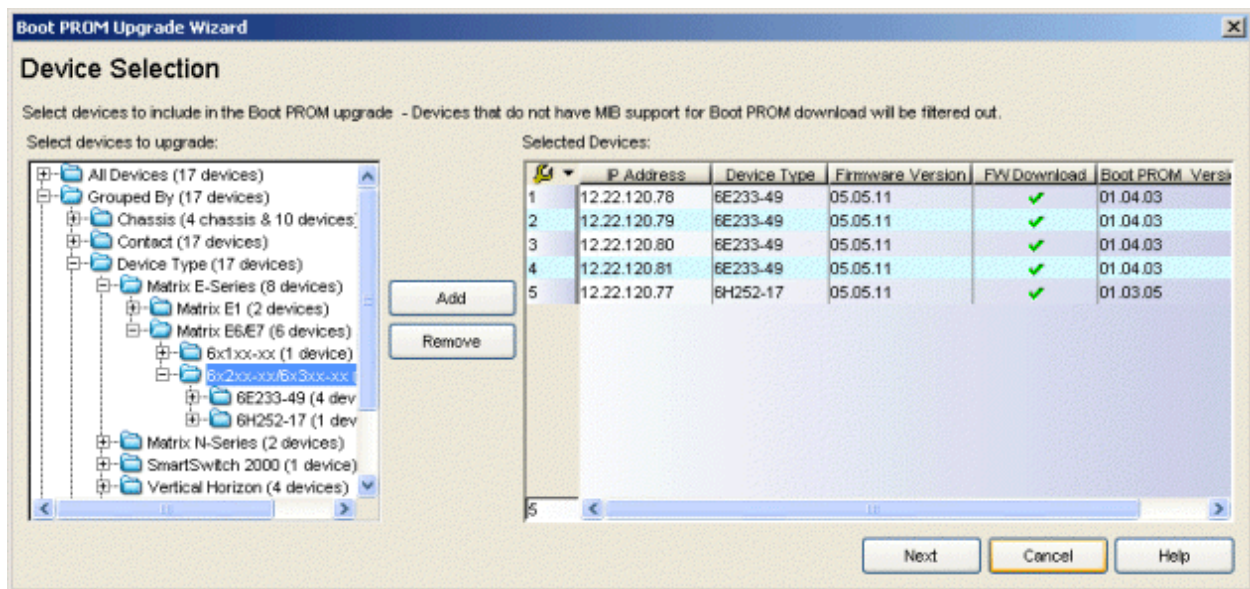
**CAUTION:** Prior to upgrading boot PROM on a device, it is recommended that you archive the latest configuration for the device being upgraded. This will aid you in downgrading should you choose to do so.

---

## Device Selection Window

Use this window to select the devices to include in the boot PROM upgrade operation.

**NOTE:** If you have multiple tree nodes representing the same device but with varying SNMP contexts, keep in mind that not all device contexts will provide access to the MIBs required to perform the operation. When selecting your devices, make sure that any device with SNMP context has access to the required MIBs, or select the device with default context (switch mode).



### Select devices to upgrade

This panel displays your current devices as they are listed in the left-panel [Network Elements tab](#). Expand the folders and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys) that you want to upgrade. Click the **Add** button to add the devices to the Selected Devices table.

**TIP:** If you open the Boot PROM Upgrade Wizard from a device or device group in the left-panel Network Elements tab, the selected device(s) will be automatically displayed in the Selected Devices table.

## *Selected Devices*

Lists the devices selected for the upgrade operation. Devices that do not support boot PROM download or have never been contacted, are not listed. If you want to remove a device from the table, select the device and click **Remove**.

### **IP Address**

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### **Family**

The product family to which the device type belongs.


### **Device Type**

The device's model number or hardware type.

### **Firmware Version**

The current firmware version installed in the device.


### **Firmware Download**

A  indicates the device supports the ability to download firmware images using the [Firmware Upgrade Wizard](#).

### **Boot PROM Version**

The current version of Boot PROM installed in the device.

### **Boot PROM Download**

A  indicates the device supports the ability to download boot PROM images using this wizard.

### **Add Button**

Select a single device or device group, or multiple devices or device groups, and click **Add** to add them to the Selected Devices table.

### **Remove Button**

To remove a device from the Selected Devices table, select the device and click **Remove**.

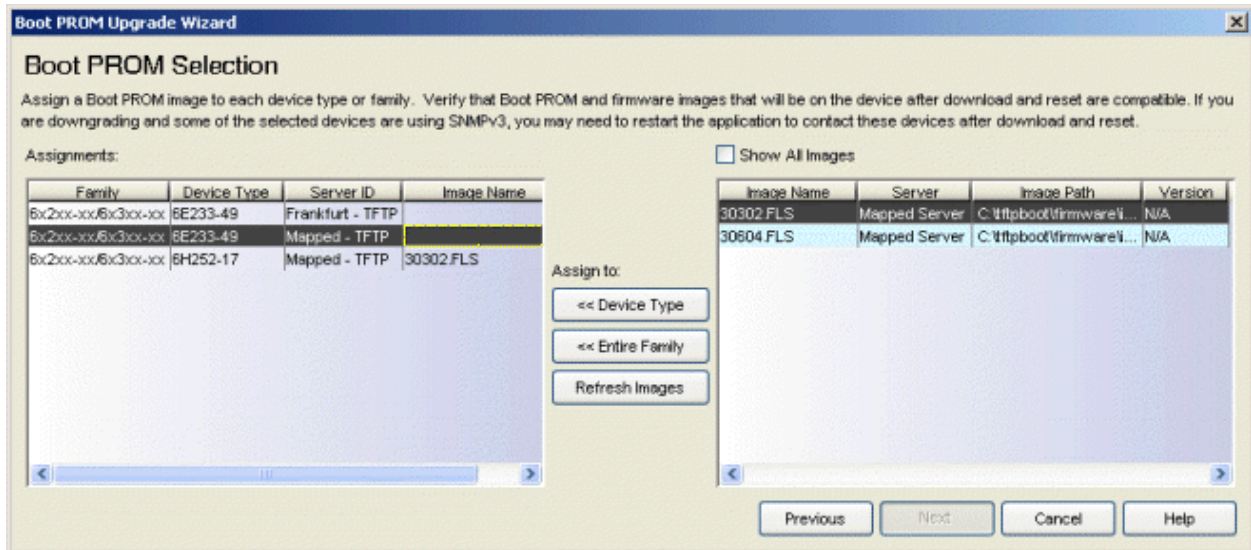
## **Boot PROM Selection Window**

Use this window to select and assign the boot PROM images to be used in the upgrade. Images are assigned according to device type or binary family (device types that share the same firmware image). The left panel lists the device types



selected for the boot PROM upgrade. The right panel lists boot PROM images compatible with a selected device type. Use the **Assign to:** buttons to assign an image to a specific device type or to the entire binary family. You must assign an image to each device type.

**NOTE:** Before proceeding with the upgrade, be sure to verify that the boot PROM and firmware images that will be on the device after the upgrade operation are compatible. Refer to the boot PROM and firmware release notes for more information.



### Assignments

This table lists the device types of all the devices selected for the boot PROM upgrade. Select a device type to display compatible boot PROM images in the right panel. If necessary, click the **Refresh Images** button to perform a firmware discovery and update the list of boot PROM images. Then, in the right-panel, select an image and use the **Assign to:** buttons to assign the image to the device type or to each entry that is a member of that binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each device type.

**NOTE:** A device type group may include some devices that use the local mapped file transfer server for firmware downloads, and some that use an alternate remote firmware download server. In that case, the device type would have multiple entries in the Assignments table, one for each server. When you select an entry that uses an alternate server, only firmware records associated with that alternate server will be displayed in the Image list table (unless you select Show All Images.)

**Family**

The product family to which the device type belongs.

**Device Type**

The device's model number or hardware type.

**Server ID**

The firmware download server specified for the device type. All devices are initially configured to use the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) for firmware downloads. You can specify an alternate firmware download server, which allows a remote device to use a server in its own local network. For more information see [How to Set Up Alternate Firmware Download Servers](#).

**Image Name**

The boot PROM image assigned to the device type.

*Image List*

This table lists all the compatible boot PROM images for the device type selected in the Assignments table. If you select a device type entry that uses an alternate remote firmware download server, only firmware records associated with that alternate server will be displayed. Select a boot PROM image and use the **Assign to:** buttons to assign the image to the selected device type or to the entire binary family. The image will appear in the Image Name column in the Assignments table. You must assign an image to each device type. Use the **Refresh Images** button to perform a firmware discovery and update the list of boot PROM images, if desired.

**Show All Images**

By default, only boot PROM images that are compatible with the selected device type are listed. Select the **Show All Images** checkbox to override this filter and display all your boot PROM images. If by selecting this checkbox you assign a boot PROM image that's associated with the mapped server, to a device type that specifies an alternate firmware download server, the wizard will use the mapped server to perform the download.

**Image Name**

The name of the boot PROM image as it appears in your firmware images directory.

**Server**

Displays the firmware download server associated with the boot PROM image. A discovered boot PROM image that is accessible by the mapped

file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server". A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#). For more information see [How to Set Up Alternate Firmware Download Servers](#).

**Image Path**

The path to the location where the image is stored.

**Version**

The version number of the boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a boot PROM upgrade using this image, this field will display N/A (not available).

**Assign to Device Type Button**

Use the **Assign to: Device Type** button to assign a boot PROM image to the device type.

**Assign to Entire Family Button**

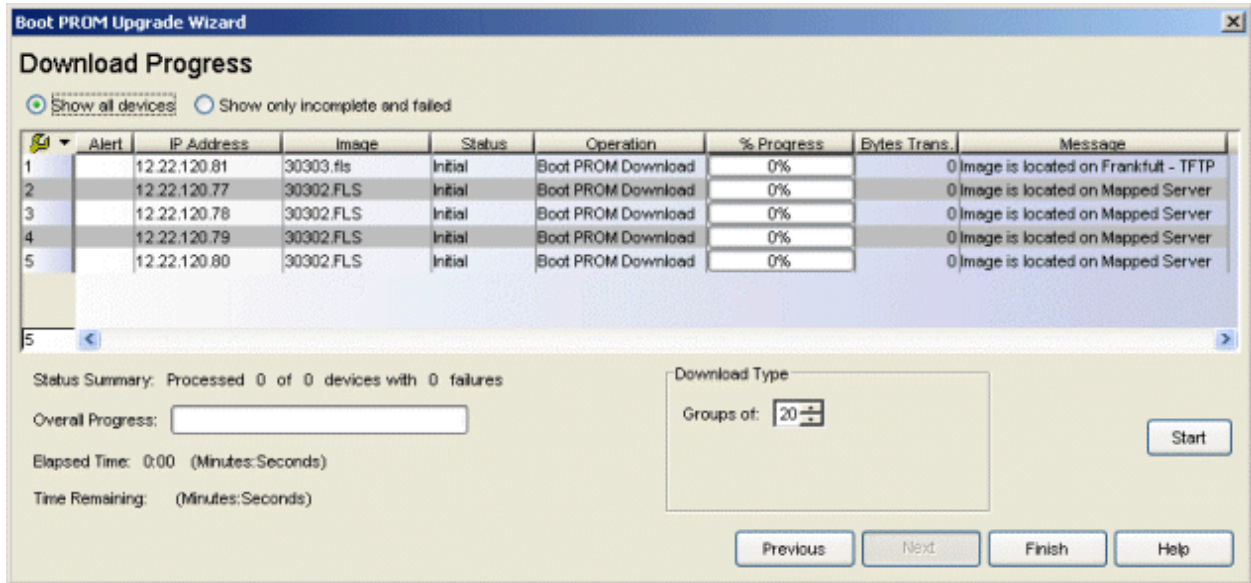
Use the **Assign to: Entire Family** button to assign a boot PROM image to each entry that is a member of that binary family.

**Refresh Images Button**


Performs a firmware discovery and updates the list of boot PROM images.

## Download Progress Window

Use this window to configure download parameters, start the download, and monitor download progress.




### Show all devices/Show only incomplete and failed


Once the upgrade operation starts, the device list table updates with status information for each device. An alert icon  will appear in the Alert column of the table if a download operation fails for a specific device. You can use these radio buttons to show all devices or show only those devices whose download operations are incomplete or have failed.

### Device List Table

A list of the devices you have selected for your download operation. Once the download is started, this table updates with status information for the download operation:

- **Alert** - an alert icon  will appear in the Alert column if a download operation fails for a specific device.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Image** - The name of the image file being downloaded.
- **Status** - The status of the download operation: Initial (the operation has not started), Success (the operation succeeded), Failure (the operation failed).
- **Operation** - The type of operation performed: Boot PROM Download.
- **% Progress** - A progress bar showing the percent completed of the operation.

- **Bytes Trans.** - The number of bytes transferred during the download.
  - **Message** - Initially, this column shows the file transfer server being used for the download operation. Once the download is started, it displays a message relating to the status of the operation.
- 

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Status Summary

Once the download is started, this area updates with status information for the download operation.

### Download Type

The downloads will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. Enter the value **1** to have the downloads performed serially, one device after another.

### Start Button

Initiates the download operation. The table at the top of the window updates with status information, as will the status area in the bottom left of the window.

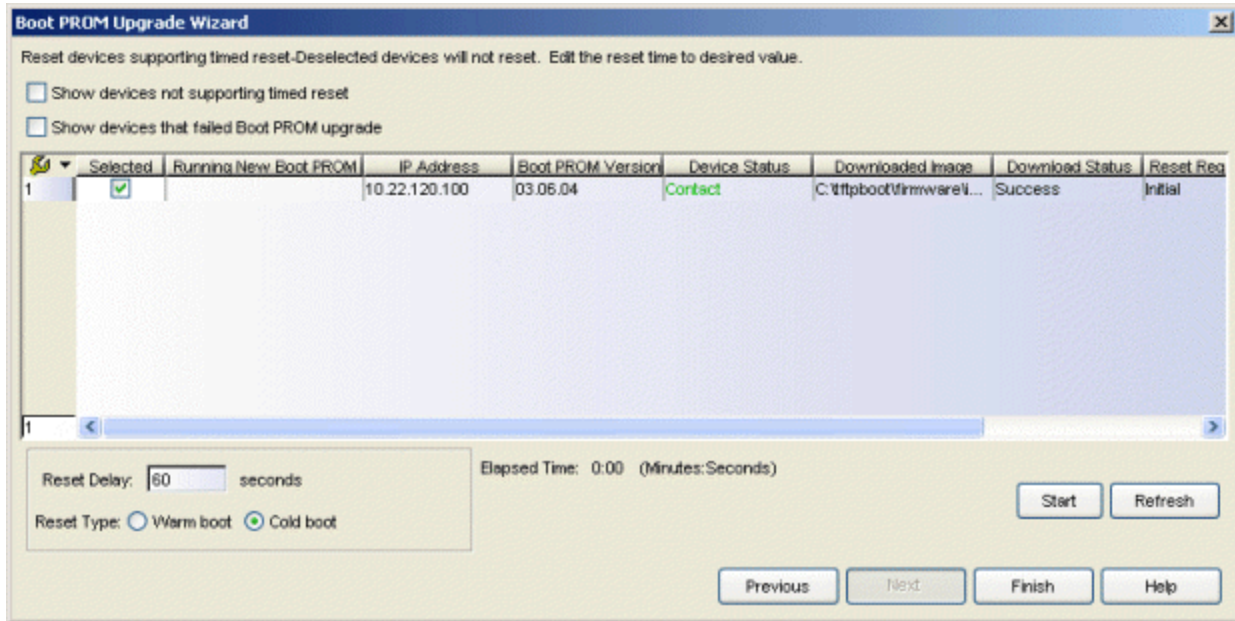
## Reset Devices: Timed Reset Supported Window

Once the downloads have completed, use this window to reset those devices that support Timed Reset. Timed Reset gives you the flexibility to set up your reset operation with a time delay, so that the actual device resets take place at a later time. This can be useful when trying to schedule resets for a time when the network is least busy.

---

**NOTE:** During the device reset, Inventory Manager learns the current boot PROM version installed on the device. Inventory Manager uses this information to determine whether the boot PROM version installed on the device matches the boot PROM reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---



### Show devices not supporting timed reset


This window lists those devices that support Timed Reset. Select this checkbox to include devices that do **not** support timed reset. Devices that do not support timed reset cannot be reset from this window; proceed to the next window to reset those devices.

### Show devices that failed Boot PROM upgrade

Select this checkbox to include devices that failed the boot PROM upgrade.


### Device List Table

A list of the devices you have selected for your reset operation. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset. Devices that do not support timed reset cannot be selected.
- **Running New Boot PROM** - Following the reset, a  indicates the device is running the new boot PROM version. (The checkmark is only displayed if the boot PROM version changes.) Remember to click **Refresh** to update the information in the table following the reset.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

- **Boot PROM Version** - The current boot PROM version installed in the device. Following the reset, the new boot PROM version will be displayed. Remember to click **Refresh** to update the information in the table following the reset.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.
- **Downloaded Image** - The name of the image file that was downloaded.
- **Download Status** - The status of the download operation: Success (the operation succeeded), Failure (the operation failed).
- **Reset Request Status** - The status of the reset operation: Initial (the operation has not started), Success (the operation succeeded), Failure (the operation failed).
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Reset Delay

Enter the amount of time (in seconds) until the device resets after the reset operation begins. For example, if you start the reset operation at 4:00 pm with a 7 hour reset delay (420 seconds), the device(s) will reset at 11:00 pm. This allows you to schedule your resets for a time when the network is least busy.

### Reset Type

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

### Elapsed Time

The amount of time in minutes:seconds since the reset operation started.

### Start Button

Starts the timed resets. Resets occur simultaneously. Once the reset operation has started, you must click **Refresh** to update the device information in the table.

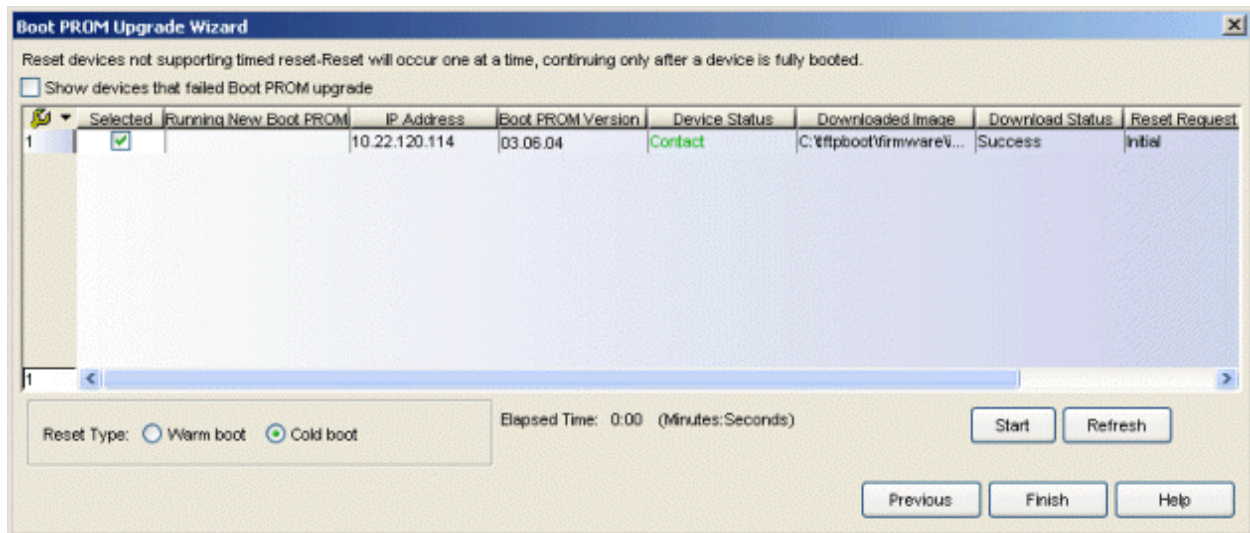
### Refresh Button

Once the reset operation has started, use the **Refresh** button to update the device information in the table.

## Reset Devices: Timed Reset Not Supported Window

Once the downloads have completed, use this window to reset those devices that do not support Timed Reset. Devices will be reset one at a time, waiting until a device is fully booted before beginning the next device.

**NOTE:** During the device reset, Inventory Manager learns the current boot PROM version installed on the device. Inventory Manager uses this information to determine whether the boot PROM version installed on the device matches the boot PROM reference image set for the device's binary family. (This information is displayed in the [All Devices Details View tab](#).) If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).



### Show devices that failed Boot PROM upgrade

Select this checkbox to include devices that failed the boot PROM upgrade.


### Device List Table

Lists those devices that do not support timed reset. Once the reset operation has started, you must click **Refresh** to update the device information in the table.



- **Selected** - Use the checkboxes in this column to select or deselect devices to be reset.
- **Running New Boot PROM** - Following the reset, a ✓ indicates the device is running the new boot PROM version. (The checkmark is only displayed if the boot PROM version changes.) Remember to click **Refresh** to update the information in the table following the reset.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Boot PROM Version** - The current boot PROM version installed in the device. Following the reset, the new boot PROM version will be displayed. Remember to click **Refresh** to update the information in the table following the reset.
- **Device Status** - The device's connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.
- **Downloaded Image** - The name of the image file that was downloaded.
- **Download Status** - The status of the download operation: Success (the operation succeeded), Failure (the operation failed).
- **Reset Request Status** - The status of the reset request.
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Reset Type

Select the type of reset: **Warm boot** (restarts the device) or **Cold boot** (same as turning device power off and on).

### Elapsed Time

The amount of time in minutes:seconds since the reset operation started.

### Start Button

Initiates the reset operation. Resets occur one at a time, continuing only after a device is fully booted. After the reset operation is completed, you

can click **Refresh** to update the device information in the table.

### Refresh Button

Once the reset operation has completed, use the **Refresh** button to update the device information in the table.

---

### Related Information

For information on related tasks:

- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)
- [How to Reset a Device](#)

## Template Download Wizard

---

Use the Template Download Wizard to download a configuration template to one or more devices. To access the wizard, select **Tools > Wizards > Template Download Wizard** from the menu bar.

Configuration templates provide an easy way to download similar configurations to one or more devices. First, use the [Edit Configuration Template window](#) to create a configuration template based on an existing archived device configuration. The window displays a selected configuration, and allows you to replace portions of it with template variables. Then, you must set device-specific values for your template variables. When you download the template configuration to a device, the variables are replaced with appropriate values for that device. Once you have created your configuration template, you are ready to use this wizard to download the template to your devices. For more information, see [How to Create and Download Configuration Templates](#).

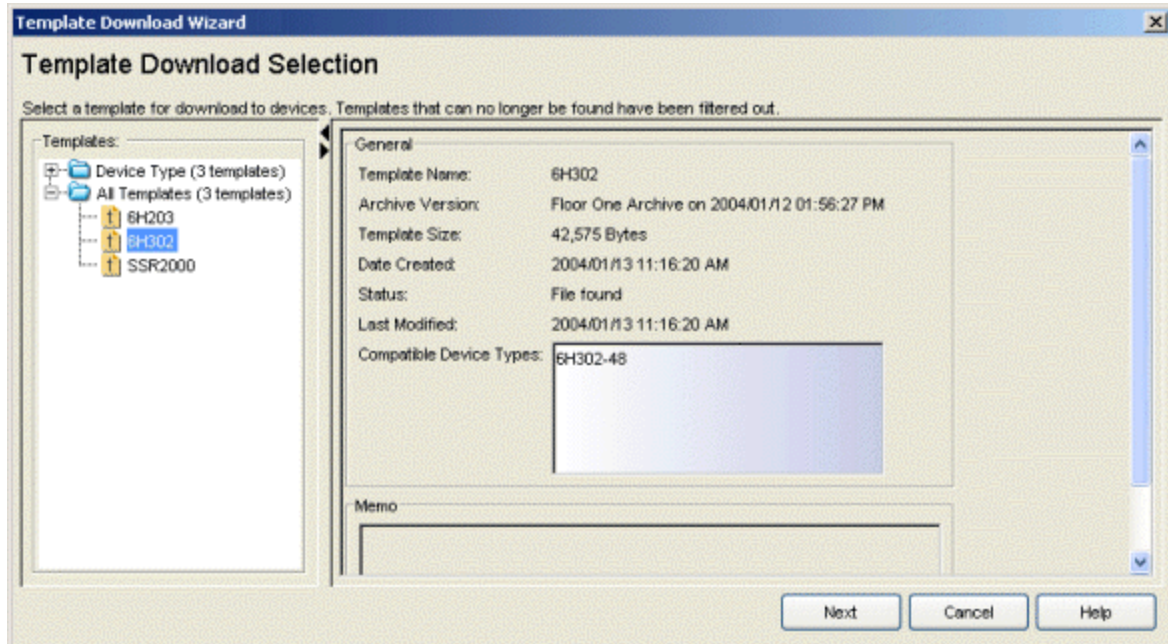
---

**NOTE:** Configuration templates can be created from text-based (ASCII format) configurations files. Although you can open binary configuration files in the Edit Configuration Template window, you should **not** use binary configuration files when you create and download templates.

---

## Template Download Selection Window

Use this window to select a configuration template to download to devices.



## Templates

This panel displays your current configuration templates just as they are listed in the left-panel [Configuration Templates tab](#). Expand the folders and select the template you wish to download. If Inventory Manager can no longer find a template file (it has been deleted or moved,) the template will not be displayed in the tree.

---

**TIP:** If you open the Template Download Wizard from a template in the left-panel Configuration Templates tab, that template will be automatically selected in the Templates tree.

---

## General

This panel displays general information about the template.

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Version

The archive version that contained the configuration file the template was based on.

### Template Size

The size in bytes of the template.

### Date Created

The date and time the template was created.

### Status

The status of the template: File Found. Template files that can no longer be found (they have been deleted or moved,) are not displayed for selection in the Templates tree.

### Last Modified

The date and time the template was last modified.

### Compatible Device Types

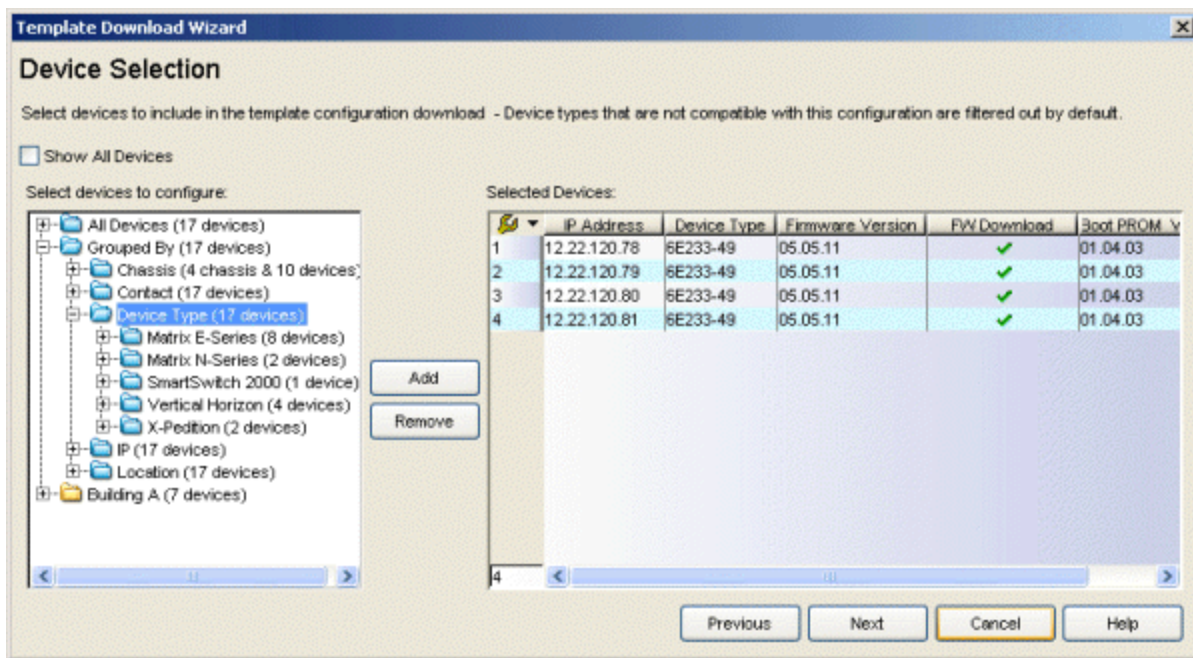
Device types the template is valid for, based on what device types the template has been assigned to.

### Memo

This panel displays Memo information entered in the [General Tab \(Template\)](#).

## Device Selection Window

Use this window to select the devices to include in the template download operation.



### *Select devices to configure*

This tree displays devices that are compatible with the selected template, grouped according to device type. By default, device types that are not compatible with the template are not displayed in the tree. Select the **Show All Devices** checkbox to override this filter. Expand the folders and select the single device or device group, or multiple devices or device groups (using the Control or Shift keys) to include in the download operation. Click **Add** to add the devices to the Selected Devices table.

### *Selected Devices*

Lists the devices selected for the download operation. If you want to remove a device from the table, select the device and click **Remove**.

#### **IP Address**

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.


#### **Device Type**

The device's model number or hardware type.

#### **Firmware Version**

The current firmware version installed in the device.


#### **Firmware Download**

A  indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

#### **Boot PROM Version**

The current version of Boot PROM installed in the device.

#### **Boot PROM Download**

A  indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

#### **Add Button**

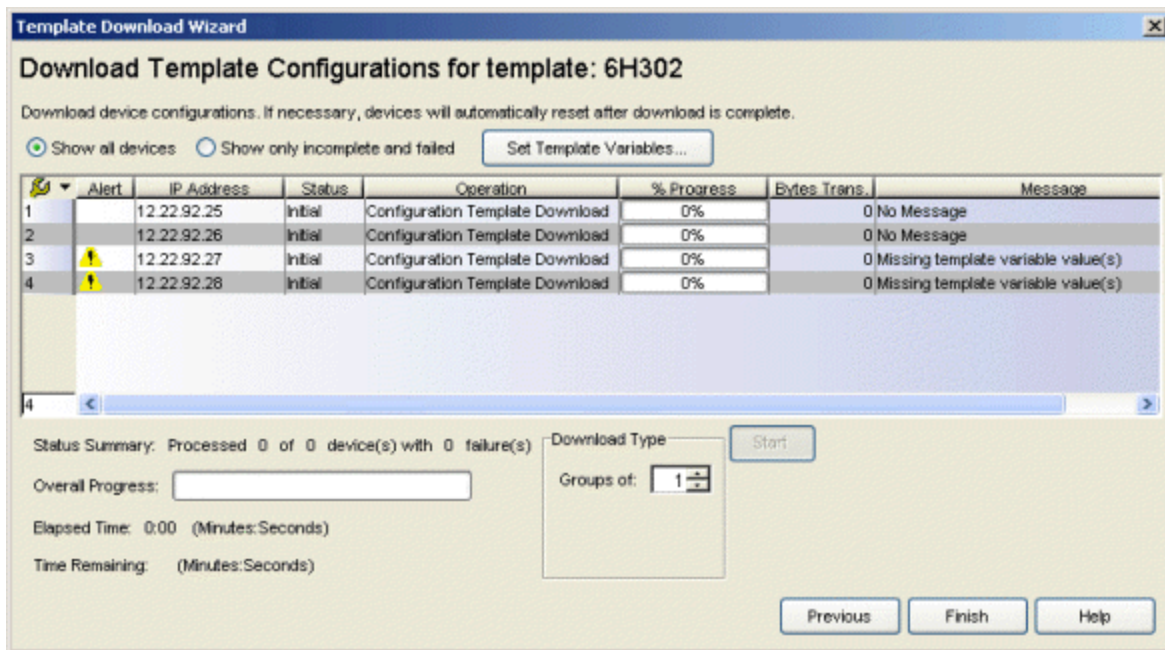
Select a single device or device group, or multiple devices or device groups, and click **Add** to add them to the Selected Devices table.

#### **Remove Button**


To remove a device from the Selected Devices table, select the device and click **Remove**.

## Download Template Configurations Window

Use this window to configure download parameters, set template variable values (if required), initiate the download operation, and monitor download progress. Devices that require a reset will be reset automatically after the download is complete.



### Show all devices/Show only incomplete and failed



Once the download operation starts, the device list table updates with status information for each device. An alert icon  will appear in the Alert column of the table if a download operation fails for a specific device. You can use these radio buttons to show all devices or show only those devices whose download operations are incomplete or have failed.

### Set Template Variables Button


Opens the [Set Template Variables window](#) which lists all your devices and their set values for each of your defined template variables. Use this window to set variable values for one or more devices.

### Device List Table

A list of the devices you have selected for your download operation. Once the download is started, this table updates with status information for the download operation:

- **Alert** - An alert icon  will appear initially for any device that does not have values assigned for all the variables in the template. Click **Set Template Variables** to open the [Set Template Variables window](#) where you can set variable values for one or more devices. You can also right-click on a table row and select Edit Device Variables to open the [Device Template Variables window](#), where you can assign variable values for that specific device. All template variables must have assigned values before the download operation can proceed. Once the download is started, an alert icon  will appear in the Alert column if a download operation fails for a specific device.
- **IP Address** - The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Status** - The status of the operation for that particular device: Success or Failure.
- **Operation** - The type of operation performed: Configuration Template Download.
- **% Progress** - A progress bar showing the percent completed of the operation.
- **Bytes Trans.** - The number of bytes transferred during the operation.
- **Message** - A message relating to the status of the operation.

---

**TIP:** Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

---

### Status Summary

Once the download is started, this area updates with status information for the download operation.

### Download Type

The download will be performed in parallel (simultaneously) on the number of devices specified in the **Groups of** field. By default, the downloads will occur in sequential order (Groups of: 1). This is to protect against possible isolation of other devices that are in the download list.



---

**CAUTION:** Because many devices automatically reset following a download operation, performing a Download Type greater than 1 may isolate other devices in the download list, causing their downloads to fail. It is recommended that you leave the **Groups of** value at 1 (perform the downloads serially), unless you know it is safe to have the selected network devices reset simultaneously.

---

### Start Button

Initiates the download operation. The table at the top of the window updates with status information, as will the status area in the bottom left of the window.

---

### Related Information

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Assign Configuration Template Window](#)
- [Device Template Variables Window](#)
- [Edit Configuration Template Window](#)
- [Set Template Variables Window](#)

# Inventory Manager Right-Panel Tabs


---

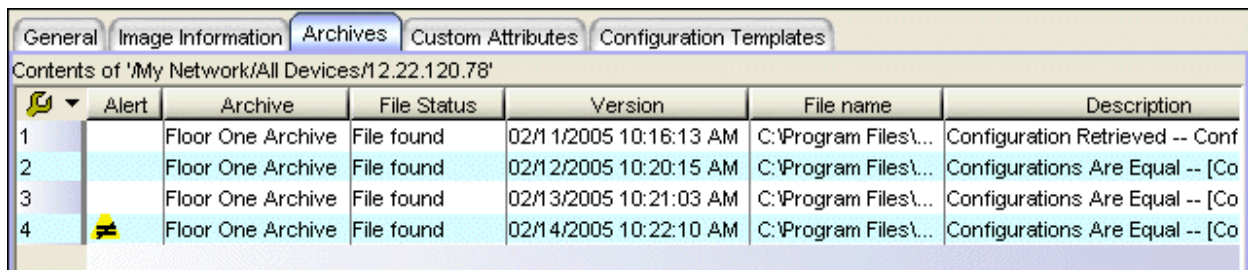
The Inventory Manager main window is divided into three panels: a left panel, a right panel, and a bottom panel.

The right panel displays different tabs and information depending on the item selected in the left-panel tree. Help topics for right-panel tabs are named in a manner to reflect this. For example, the help topic named Details View (Device Group), provides information on the right-panel Details View tab when a device group is selected in the left-panel tree.

## Archives Tab (Device)

The Archives tab appears when you select a device in the left panel's Network Elements tab. It displays a list of archive operations for the selected device. Each time a new archive version is created, the information is added to the bottom of the list. Right-click an item or items for a menu of options.



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with several tabs: General, Image Information, Archives, Custom Attributes, and Configuration Templates. The 'Archives' tab is active, displaying a table titled 'Contents of "/>

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between this saved configuration and the previous configuration saved for this device.
-  -- the last archive save or restore for this device failed.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### Archive

The name of the archive operation.

### Status

The status of the configuration file saved by the archive: File Found or File Not Found/Missing. File Not Found/Missing indicates that Inventory Manager can no longer find the config file (it has been deleted or moved) or the archive operation did not include saving device configuration data.

### Version

The date and time the archive version was performed.

**File name**

The path and filename for the saved configuration. For archive operations that are configured to archive only capacity planning data (and not configuration data), this column will be blank.

**Description**

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. Rest your cursor on the field to display a tooltip of the complete description. For archive operations that are configured to archive only capacity planning data (and not configuration data), this column will display a Warning message stating that the ability to archive configuration data has been disabled for this archive.

---

**Related Information**

For information on related tabs:

- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)

For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)

## Attributes Tab (Configuration)

---

The Attributes tab appears when you select an individual configuration in the left panel's Archive Mgmt tab. It displays the configuration's archive, device, firmware, and configuration attributes.

Captured Attributes	
Archive:	Building A Floor 1
IP Address:	10.22.102.127
Version:	Oct 17, 2002 11:53:56 AM

Device Information	
Device Type:	6E132-25
Serial Number:	193998250133240F
Asset Tag:	13906
Chassis ID:	00001D8DE58A
Chassis Slot:	5
Memory:	16 MB

Firmware/Configuration Information	
Firmware Version:	04.11.14
Firmware Change Count:	N/A
Firmware Change Time:	N/A
Firmware Change Method:	N/A
Configuration Change Count:	N/A
Configuration Change Time:	N/A
Configuration Change Method:	N/A
Configuration File Checksum:	3367089099
Configuration File Size:	20,393 Bytes

### Device Type

The device's model number or hardware type.

### Serial Number

A unique number assigned to the device by the manufacturer.

### Asset Tag

A unique asset number assigned to the device for inventory tracking purposes. The asset tag is defined in the device's [General Tab](#).

### Chassis ID

The ID assigned to the chassis where the device resides (if applicable). This is usually a serial number or MAC address, depending on the chassis type.

### Chassis Slot

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

### Memory

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

### Firmware Version

The firmware version installed in the device at the time of the configuration save.

### Firmware Change Count

The number of successful firmware image downloads. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Firmware Change Time

The date and time of the last successful firmware image download. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Firmware Change Method

The method that was used to cause the last firmware change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Configuration Change Count

The number of successful configuration changes. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Configuration Change Time

The date and time of the last successful configuration change. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Configuration Change Method

The method that was used to make the last configuration change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* will display N/A (Not Available).

### Configuration File Checksum

The checksum is a value calculated on the entire file. You can compare this value to values obtained from different archive versions. Any difference in checksum values would indicate a change in the configuration.

### Configuration File Size

The size of the saved configuration file in bytes. You can compare this size to the size reported in different archive versions. Any difference in size would indicate a change in the configuration file.

---

## Related Information

For information on related tabs:

- [General Tab \(Configuration\)](#)


For information on related tasks:

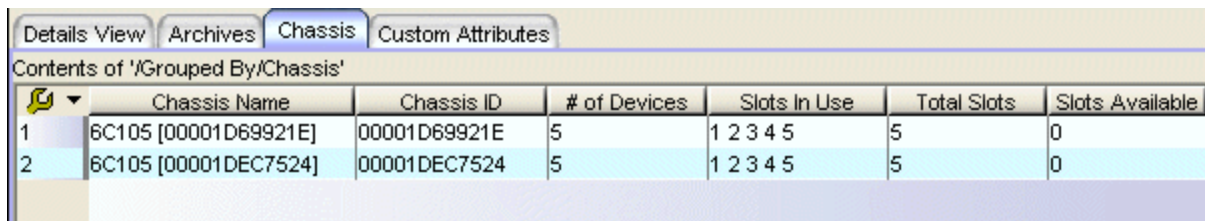
- [How to Archive](#)
- [How to Restore an Archive](#)

## Chassis Tab (Chassis Folder)

The Chassis tab provides detailed information about the chassis in your network, including the number of slots being used and the number of available slots in each chassis. Right-click an item or items for a menu of options. To access this tab, select the Chassis folder in the left panel's Network Elements tab, then click the Chassis tab in the right panel.

Inventory Manager provides the top-level Chassis folder as a pre-defined device group. When you add or import devices that are in a chassis, Inventory Manager automatically adds individual chassis folders using the chassis type and ID, and organizes your chassis devices under the appropriate folder.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



	Chassis Name	Chassis ID	# of Devices	Slots In Use	Total Slots	Slots Available
1	6C105 [00001D69921E]	00001D69921E	5	1 2 3 4 5	5	0
2	6C105 [00001DEC7524]	00001DEC7524	5	1 2 3 4 5	5	0

### Chassis Name

The chassis type followed by the chassis ID in parentheses.

### Chassis ID

The ID assigned to the chassis. This is usually a serial number or MAC address, depending on the chassis type.

### # of Devices

The number of devices residing in the chassis. Chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, are managed by a single IP and will display "1" in this column even though there may be multiple DFE modules in the chassis.

### Slots in Use

The chassis slot numbers being used by devices or DFE modules.



**Total Slots**

The total number of slots in the chassis.

**Slots Available**

The number of available (empty) slots in the chassis.

**Slots Used**


The number of slots being used in the chassis.

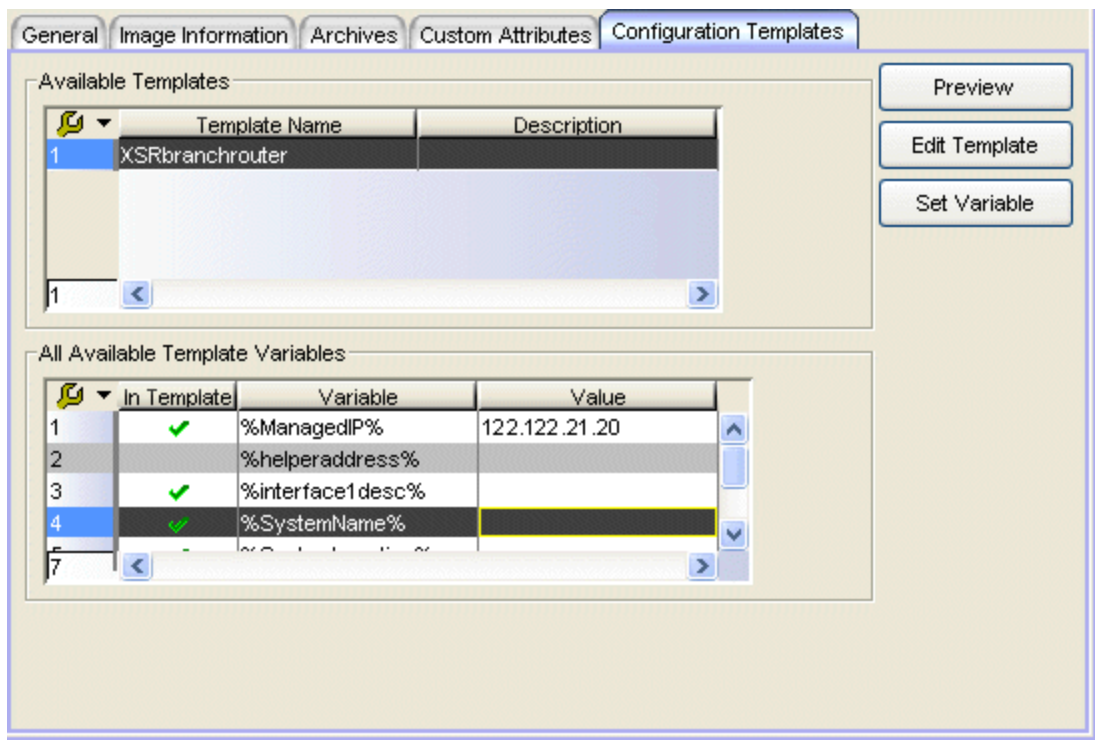
**% Utilized**

The percentage of slots being used in the chassis.

## Configuration Templates Tab (Device)

The Configuration Templates tab appears when you select a device in the left panel's Network Elements tab. It displays information on available configuration templates for the selected device. The information is presented in two tables. The top table lists all the configuration templates that the device can use, based on its device type. The table on the bottom lets you set variable values for the selected device. From the tab, you can also edit a configuration template or preview a template with all the variables filled in.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



Available Templates

Template Name	Description
XSRbranchrouter	

All Available Template Variables

In Template	Variable	Value
1	✓ %ManagedIP%	122.122.21.20
2	%helperaddress%	
3	✓ %interface1desc%	
4	✓ %SystemName%	
5	%...	
6	%...	
7	%...	

Preview  
Edit Template  
Set Variable

## Available Templates

This table lists all the configuration templates that would be available for download to the selected device, based on device type. You can select a template and click **Preview** or **Edit Template** to view or modify the template.

## All Available Template Variables

This table lists all the variables you have defined, and allows you to set a value for each variable for the selected device.

### In Template

If this column is checked, the variable appears in the template selected in Available Templates table.

### Variable

This column lists all the variables you have defined. Select a variable and click **Set Variable** to assign a value to the variable for the selected device.

### Value

This column displays the values you have assigned to the variables for the selected device.

### Preview Button

Opens the [Configuration File Viewer](#) which displays the template with all the variables replaced by the assigned values.

### Edit Template Button

Opens the [Edit Configuration Template window](#) where you can edit the template.

### Set Variable Button

Opens the Set Template window where you can set a value for the selected variable.

---

## Related Information

For information on related tasks:

- [How to Create and Download Configuration Templates](#)


For information on related windows:

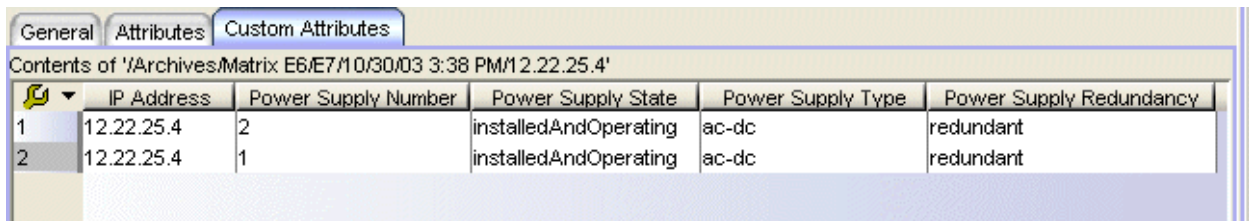
- [Edit Configuration Template Window](#)



## Custom Attributes Tab (Configuration)

The Custom Attributes tab appears in the right panel when you select a configuration in the left panel Archive Mgmt tab. It displays a table of attribute information collected from the device at the time the configuration was saved. The information you see depends on the type of device the configuration was saved from; some device types support one attribute but not another. If the device type returns multiple values for an attribute, each value will be on a separate row. If the device type does not support any of the attributes, the Custom Attributes tab for that configuration will be blank.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



	IP Address	Power Supply Number	Power Supply State	Power Supply Type	Power Supply Redundancy
1	12.22.25.4	2	installedAndOperating	ac-dc	redundant
2	12.22.25.4	1	installedAndOperating	ac-dc	redundant

## Custom Attributes

### Type

A description of the module or component type.

### Name

The name of the module or component.

### Firmware Version

The current firmware version installed in the module.

### Model Name

The model number of the module or component type.

### Description

A description of the module or component.

**Manufacturer**

The manufacturer of the module or component.

**Field Replaceable**

Whether or not the manufacturer considers the component to be field replaceable (true or false).

**Hardware Rev**

The current hardware version of the device.

**Serial Number**

A unique number assigned to the module or component by the manufacturer.

**BootPROM Version**

The current version of Boot PROM installed in the module.

**Asset Tag**

A unique asset number assigned to the module or component for inventory tracking purposes.

## Legacy Devices

### *SSR Hardware Attributes*

**Slot Number**

The slot number in the chassis where the module resides.

**Status**

The current status of the module: online or offline.

**Type**

The physical module type.

**Description**

A description of the module.

**Number of Ports**

The number of physical ports on the module.

**Version**

The module version.

**Memory**

The system memory size available on the module, reported in megabytes (MB).

### *E5 and E6/E7 Power Supply and Fan Attributes*

#### **Power Supply Number**

The number of the power supply.

#### **Power Supply Type**

The power supply type: ac-dc, dc-dc, or highOutput.

#### **Fan State**

The state of the fan: Installed and Operating, Installed and Not Operating, or Not Installed.

#### **Power Supply State**

The state of the power supply: Installed and Operating, Installed and Not Operating, or Not Installed.

#### **Power Supply Redundancy**

Whether the power supply is redundant or not.

### *RoamAbout Radiocard and Base MAC Address Attributes*

#### **Card Type**

The type of PC card inserted in the Access Point.

#### **Versions**

The hardware and firmware versions for the PC card.

#### **Station Name**

The wireless station name sent out as part of the beacon messages. Valid only when a DS card is inserted in the Access Point.

#### **Base MAC Address**

The physical layer address assigned to the interface through which Inventory Manager is communicating.

### *Vertical Horizon Attributes*

#### **Number in Stack**

The total number of switches present on this system.

#### **Number of Ports**

The total number of ports present on this system.

#### **Firmware Version**

The current firmware version installed in the device.

**BootPROM Version**

The current version of Boot PROM installed in the device.

**CPU**

The name of the device's processor (Central Processing Unit).

**Power Status**

Indicates whether the device is using internal power, redundant power, or both.

**Expansion Slot 1**

The type of expansion module in slot 1.

**Expansion Slot 2**

The type of expansion module in slot 2.

**Role in System**

Indicates whether the device is master, backup master, or slave in the system.

*ELS Serial Number Attribute*

**Serial Number**

A unique number assigned to the device by the manufacturer.

---

**Related Information**

For information on related windows:


- [General Tab \(Configuration\)](#)
- [Custom Attributes Tab \(Device or Device Group\)](#)

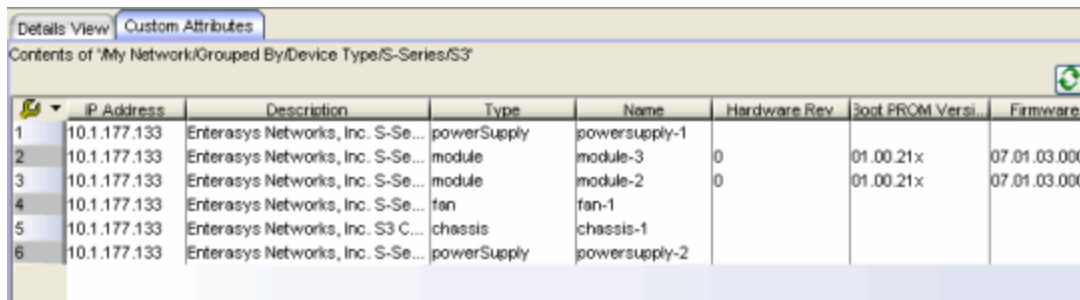


## Custom Attributes Tab (Device or Device Group)

The Custom Attributes tab appears in the right panel when you select a device or device group in the left panel Network Elements tab. It displays a table of attribute information about the selected device(s). The information you see depends on the device type(s) selected; some devices support one attribute but not another. If a device returns multiple values for an attribute, each value will be on a separate row. If a device does not support any of the attributes, the Custom Attributes tab for that single device will be blank.

Custom Attribute tabs for device groups only display devices that support one or more of the attributes. Devices that have been configured with an SNMP context will display separate entries for each context.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with two tabs: 'Details View' and 'Custom Attributes'. The 'Custom Attributes' tab is active, displaying a table titled 'Contents of My Network/Grouped By/Device Type/S-Series/S3'. The table has columns for IP Address, Description, Type, Name, Hardware Rev, Boot PROM Versi., and Firmware. There are six rows of data, each representing a different component of a device.

	IP Address	Description	Type	Name	Hardware Rev	Boot PROM Versi.	Firmware
1	10.1.177.133	Enterasys Networks, Inc. S-Se...	powerSupply	powersupply-1			
2	10.1.177.133	Enterasys Networks, Inc. S-Se...	module	module-3	0	01.00.21x	07.01.03.00C
3	10.1.177.133	Enterasys Networks, Inc. S-Se...	module	module-2	0	01.00.21x	07.01.03.00C
4	10.1.177.133	Enterasys Networks, Inc. S-Se...	fan	fan-1			
5	10.1.177.133	Enterasys Networks, Inc. S3 C...	chassis	chassis-1			
6	10.1.177.133	Enterasys Networks, Inc. S-Se...	powerSupply	powersupply-2			

## Custom Attributes

### Description

A description of the module or component.

### Type

A description of the module or component type.

### Name

The name of the module or component.

**Hardware Rev**

The current hardware version of the device.

**BootPROM Version**

The current version of Boot PROM installed in the module.

**Firmware Version**

The current firmware version installed in the module.

**Serial Number**

A unique number assigned to the module or component by the manufacturer.

**Manufacturer**

The manufacturer of the module or component.

**Model Name**

The model number of the module or component type.

**Asset Tag**

A unique asset number assigned to the module or component for inventory tracking purposes.

**Field Replaceable**

Whether or not the manufacturer considers the component to be field replaceable (true or false).

## Legacy Devices

### *SSR Hardware Attributes*

**Slot Number**

The slot number in the chassis where the module resides.

**Status**

The current status of the module: online or offline.

**Type**

The physical module type.

**Description**

A description of the module.

**Number of Ports**

The number of physical ports on the module.

**Version**

The module version.

**Memory**

The system memory size available on the module, reported in megabytes (MB).

*E5 and E6/E7 Power Supply and Fan Attributes*

**Power Supply Number**

The number of the power supply.

**Power Supply Type**

The power supply type: ac-dc, dc-dc, or highOutput.

**Fan State**

The state of the fan: Installed and Operating, Installed and Not Operating, or Not Installed.

**Power Supply State**

The state of the power supply: Installed and Operating, Installed and Not Operating, or Not Installed.

**Power Supply Redundancy**

Whether the power supply is redundant or not.

*RoamAbout Radiocard and Base MAC Address Attributes*

**Card Type**

The type of PC card inserted in the Access Point.

**Versions**

The hardware and firmware versions for the PC card.

**Station Name**

The wireless station name sent out as part of the beacon messages. Valid only when a DS card is inserted in the Access Point.

**Base MAC Address**

The physical layer address assigned to the interface through which Inventory Manager is communicating.

*Vertical Horizon Attributes*

**Number in Stack**

The total number of switches present on this system.

**Number of Ports**

The total number of ports present on this system.

**Firmware Version**

The current firmware version installed in the device.

**BootPROM Version**

The current version of Boot PROM installed in the device.

**CPU**

The name of the device's processor (Central Processing Unit).

**Power Status**

Indicates whether the device is using internal power, redundant power, or both.

**Expansion Slot 1**

The type of expansion module in slot 1.

**Expansion Slot 2**

The type of expansion module in slot 2.

**Role in System**

Indicates whether the device is master, backup master, or slave in the system.

*ELS Serial Number Attribute*

**Serial Number**

A unique number assigned to the device by the manufacturer.



Performs a device refresh, updating the attribute information in the table.

---

**Related Information**

For information on related windows:

- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)

## Details View Tabs

---

A Details View tab is often displayed in the right panel of the Inventory Manager main window. It provides detailed information for the item currently selected in the left panel.

The Details View tab usually provides the following features:


- *Select multiple items:* Select multiple items by using the **Ctrl** (for non-sequential items) or **Shift** (for sequential items) key.
- *Double-click items:* Double-click an item in the Details View to select the item in the left-panel and display the next level of information for that item in the right panel.
- *Right-click menus:* Right-click an item or items for a menu of options.
- *Sort, Filter, and Find Toolbars:* You can sort and filter the information in an Archives tab, or perform a find operation to locate specific information. Right-click on any column heading or anywhere in the table body, and select the **Sort**, **Filter**, or **Find** menu option. The appropriate toolbar opens.
- *Print and export:* You can print and export the information in an Archives tab. Right-click on any column heading or anywhere in the table body, and select the **Table Tools > Print** or **Table Tools > Export** menu option.
- *Reorder columns:* You can change the order of the columns by clicking on a column heading and dragging it to the desired position.

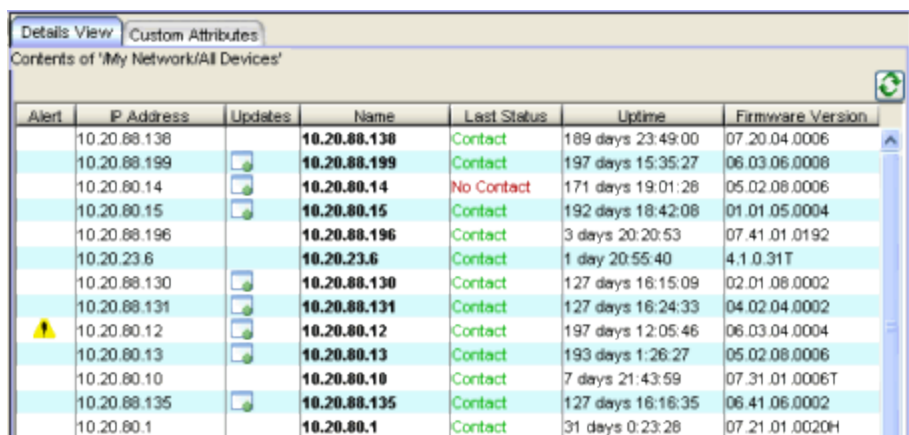
The item you select in the left-panel tree determines what is displayed in the right panel Details View. Help topics for the various Details View tabs are named to reflect this. For example, the help topic for the Details View tab with a device group selected in the left panel is named Details View Tab (Device Group). For more complete information on these tabs, expand the Details View folder and select the desired tab.

## Details View Tab (All Devices Folder)

The Details View tab appears in the right panel when you select the All Devices folder in the left panel's Network Elements tab. The All Devices folder contains all the devices in the NetSight database, and the Details View displays a table of information about those devices. Right-click an item or items for a menu of options.

**TIP:** This information is also displayed in the [General tab](#) and [Image Information tab](#) for each device. The General tab allows you to view the information and also edit certain fields.





Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a window titled 'Details View' with a sub-tab 'Custom Attributes'. The main content is a table titled 'Contents of "/>

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between one or more saved configuration files for this device and a previous file saved for the device.
-  -- the device status is No Contact.
-  -- the last archive save or restore for this device failed.
-  -- the last firmware upgrade for this device failed.

For a description of the alert, see the Alert Description column. To delete

the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### IP address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### Updates

The firmware release status for the device according to the results from the latest Tools > Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

- Firmware Up To Date - The device is running the latest release of firmware.
- New Firmware Available - There is a new release of firmware available for this device. Right-click the icon and select Firmware Releases Available to open the Updates Available window where you can download the new firmware.
- Check Firmware Update - A Check for Firmware Updates needs to be performed to get updates for this device. For more information, see the Suite-Wide Tools How to Check for Updates Help topic.
- No Updates Available - This device does not support the Check for Firmware Updates feature.

### Name

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Tools Data Display Format Options window, followed by the SNMP context, if applicable. Entries in this column are displayed in *italics* to represent that the information may be "stale". Clicking the [Refresh button](#) changes the entries to **bold**, indicating that the information is current for a minute when you first display the view. Changing any other device information (including acknowledging an Alert icon) also changes the entry to **bold**.

### Last Status

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests. The status is updated when you right-click the All Devices folder and select Refresh (Rediscover) from the menu, or click the [Refresh button](#).


### Uptime

The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

### Firmware Version

Shows the current firmware version installed in the device.

### FW Reference

A  indicates that the current firmware version installed in the device matches the firmware reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---


**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current firmware on the device. The version number must be available from the reference image file and the current firmware on the device must have been installed at some point via an Inventory Manager Firmware Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the firmware version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

### Boot PROM Version

Shows the current version of boot PROM installed in the device.

### BP Reference

A  indicates that the current boot PROM version installed in the device matches the boot PROM reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---

**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current boot PROM on the device. The version number must be available from the reference image file and the current boot PROM on the device must have been installed at some point via an Inventory Manager Boot PROM Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the boot PROM version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---



**MAC Address**

The physical layer address assigned to the interface through which Inventory Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

**Device Type**

The device's model number or hardware type.

**System Name**

The assigned name for the device.

**System Contact**

The person responsible for the device.

**System Location**

The physical location of the device.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes.

**System Description**

Description of the piece of equipment, which may include its manufacturer, model number, and firmware revision number.

**Chassis Slot**

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

**Chassis ID**

The ID assigned to the chassis where the device resides.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**CPU**

The name of the device's processor (Central Processing Unit).

**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

**File Transfer Method**

The file transfer method for this device. For more information, see [How to Set a File Transfer Method](#).

**FW Download**

A ✓ indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

**Boot PROM Download**

A ✓ indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

**Config Download**

A ✓ indicates the device supports the ability to save and restore archives (configurations) using the [Archive Wizard](#) and [Restore Wizard](#).

**Timed Reset**

A ✓ indicates the device supports the ability to perform a timed reset using the [Reset Device Wizard](#).

**Alert Description**

Describes the cause of any alert icon appearing in the Alert column.



Performs a device refresh, updating the device information in the table. If the [Name column](#) entry is in *italics* (indicating that the information may be "stale"), clicking this Refresh button changes the Name column entry to **bold**, indicating that you have current device information for a minute when you first display the view.

---


**Related Information**















For information on related windows:

- [Details View Tabs](#)
- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)



## Details View Tab (All Firmware Folder)

The Details View tab appears when you select the All Firmware folder in the left panel's Firmware Mgmt tab. Inventory Manager automatically lists the firmware and boot PROM images stored in your firmware directory under the All Firmware folder when you perform a [firmware discovery or refresh](#). Right-click an item or items for a menu of options.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

Details View						
Contents of 'All Firmware'						
	Referenced	Image Name	Image Filename	Image Path	Date	Ver
1		1_06_02.flx	1_06_02.flx	C:\tftpboot\firmware\i...	12/21/2004 04:11:54 PM	01.06.02
2		2.4.2.1.bix	2.4.2.1.bix	C:\tftpboot\firmware\i...	10/26/2004 02:18:10 PM	N/A
3		05_01_30.flx	05_01_30.flx	C:\tftpboot\firmware\i...	04/23/2002 01:13:53 PM	N/A
4		05_01_33.flx	05_01_33.flx	C:\tftpboot\firmware\i...	04/23/2002 01:13:59 PM	N/A
5		30302.FLS	30302.FLS	C:\tftpboot\firmware\i...	06/16/2000 04:16:16 PM	N/A
6		30604.FLS	30604.FLS	C:\tftpboot\firmware\i...	11/12/2002 09:16:58 AM	N/A
7		50712.FLS	50712.FLS	C:\tftpboot\firmware\i...	05/05/2004 04:18:34 PM	N/A
8		50804.flx	50804.flx	C:\tftpboot\firmware\i...	07/27/2004 12:22:48 PM	N/A
9		50808.flx	50808.flx	C:\tftpboot\firmware\i...	12/03/2004 04:02:24 PM	N/A
10		B050503.bin	B050503.bin	C:\tftpboot\firmware\i...	12/06/2004 10:42:02 AM	N/A
11		C120014.flx	C120014.flx	C:\tftpboot\firmware\i...	12/02/2004 08:06:52 AM	02.00.14
12		DFE-G-50158	DFE-G-50158	C:\tftpboot\firmware\i...	12/30/2004 03:25:08 PM	05.01.58
13		DFE-P-50158	DFE-P-50158	C:\tftpboot\firmware\i...	12/30/2004 03:24:30 PM	05.01.58
14		G050505.Z	G050505.Z	C:\tftpboot\firmware\i...	12/22/2004 01:02:28 PM	N/A

### Referenced

Firmware or boot PROM images that have been set as a reference image display a reference icon ( or ) in this column. A reference image is the image you designate as the preferred image for a specific binary family of devices. To set a reference, select a firmware or boot PROM image in the table or the tree, right-click and select Set as Reference Image from the menu. The image will be set as a reference for all device types with which it is compatible. (If the Set as Reference Image option is not available, make sure that the selected image has been assigned to appropriate device types.)

**Image Name**

The name of the image as it is displayed in the left-panel Firmware Mgmt tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

**Image Filename**

The full name of the image as it appears in your firmware images directory.

**Image Path**

The path to the location where the image is stored.

**Date**

The image file date and time as reported by the file system.

**Version**

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field will display N/A (not available).

**Image Size (Bytes)**

The size in bytes of the image.

**Status**

The status of the image file: "File Found" or "File Not Found." This shows whether the file is still present in the firmware directory. If the image is a user-defined firmware record, this column will display "User-Defined File."

**Server**

Displays the firmware download server associated with the image file. A [discovered firmware image](#) that is accessible by the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server." A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#).



Performs a firmware discovery, updating the information in the table.



Opens the download library website where you can download firmware and release notes. If you download a firmware image that is contained in a .zip file, you must unzip the file before placing it into the firmware directory.

---

**NOTE:** It is possible to customize this button to open a different website. For example, you may want to open a corporate intranet page that lists specific firmware that has been tested and approved for your network. For information on how to do this, contact Extreme Networks Technical Support (Help > Support Center).

---


## Related Information

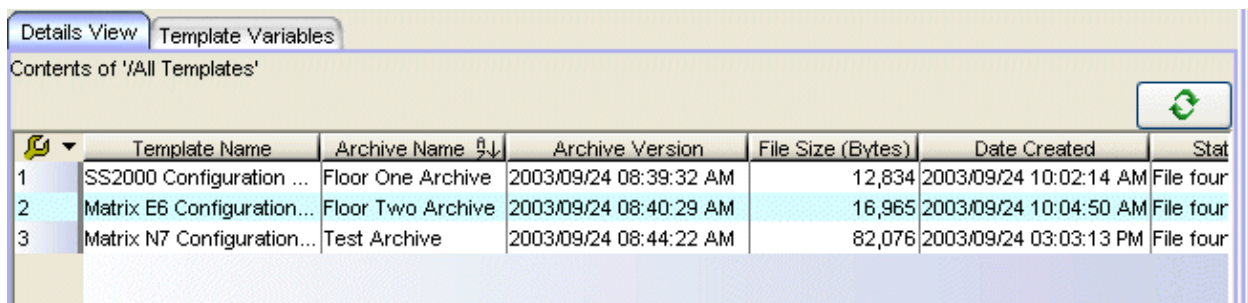
For information on related tasks:

- [How to Assign Firmware](#)
- [How to Upgrade Firmware](#)

## Details View Tab (All Templates Folder)

The Details View tab appears when you select the All Templates folder in the left panel's Configuration Templates tab. Inventory Manager automatically lists each template under the All Templates folder when you save the template in the [Edit Configuration Template window](#). The Details View displays information for each template. Right-click an item or items for a menu of options.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software window with two tabs: 'Details View' (selected) and 'Template Variables'. Below the tabs is a header 'Contents of 'All Templates'' and a refresh button. A table with 7 columns is displayed. The columns are: 'Template Name', 'Archive Name', 'Archive Version', 'File Size (Bytes)', 'Date Created', and 'Stat'. There are three rows of data.

	Template Name	Archive Name	Archive Version	File Size (Bytes)	Date Created	Stat
1	SS2000 Configuration ...	Floor One Archive	2003/09/24 08:39:32 AM	12,834	2003/09/24 10:02:14 AM	File four
2	Matrix E6 Configuration...	Floor Two Archive	2003/09/24 08:40:29 AM	16,965	2003/09/24 10:04:50 AM	File four
3	Matrix N7 Configuration...	Test Archive	2003/09/24 08:44:22 AM	82,076	2003/09/24 03:03:13 PM	File four

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Name

The name of the archive that contained the configuration file the template was based on.

### Archive Version

The archive version that contained the configuration file the template was based on.

### File Size (Bytes)

The size in bytes of the template.

### Date Created

The date and time the template was created.

**Status**

The status of the template: File Found or File Not Found. This shows whether the template is still present in the database.

**Last Modified**

The date and time the template was last modified. You can modify (edit) a template from the template's [General Tab](#).



Updates the information in the table.

---

**Related Information**

For information on related tasks:


- [How to Create and Download Configuration Templates](#)

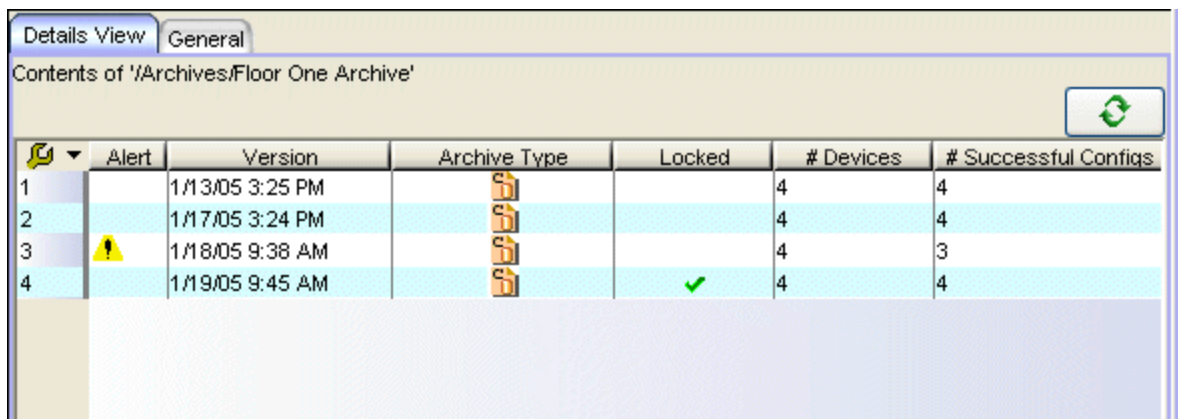
For information on related windows:

- [Assign Configuration Template Window](#)
- [Edit Configuration Template Window](#)







## Details View Tab (Archive)

The Details View tab appears when you select an archive operation in the left panel's Archive Mgmt tab. The Details View displays the archive's versions -- the dates and times that the selected archive has been performed. Right-click an item or items for a menu of options.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.





The screenshot shows a window titled 'Details View' with a 'General' tab. The window displays the contents of '/Archives/Floor One Archive'. A table lists four archive versions with columns for Alert, Version, Archive Type, Locked, # Devices, and # Successful Configs. A yellow alert icon is present in the Alert column for the third version.

	Alert	Version	Archive Type	Locked	# Devices	# Successful Configs
1		1/13/05 3:25 PM			4	4
2		1/17/05 3:24 PM			4	4
3		1/18/05 9:38 AM			4	3
4		1/19/05 9:45 AM			4	4

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between the saved configuration(s) in this version and previous configurations saved for the device(s).
-  -- a configuration save failed for one or more of the devices in this archive version.




### Version

Lists all the dates and times (archive versions) that the selected archive has been performed.


### Archive Type

The icon in this column signifies the type of data the archive is configured to save:



-  -- Device Configuration Data
-  -- Capacity Planning Data
-  -- Both Device Configuration and Capacity Planning Data

### Locked

A  indicates that the archive version is locked. A locked archive version will not be deleted when the maximum number of saved versions for this archive (as specified in the [Archive Wizard](#)) has been reached. To lock and unlock an archive version, select the version in the Archive Mgmt tab, and select **Tools > Lock/Unlock**.

### # Devices

The number of devices that this archive version is responsible for.

### # Successful Configs

The number of successful configuration saves for the archive version.

### # Failed Configs

The number of configuration saves that failed for the archive version.

### # Aborted Configs

The number of configuration saves that were aborted for the archive version.

### # Diff Configs

The number of saved configurations that are different from the previous configurations saved for the device(s).

### Memo

Displays any notes about the version entered into the Memo field in the [Archive Version General tab](#).



Performs a configuration discovery, updating the archive information in the table.

---

## Related Information

For information on related tabs:


- [General Tab \(Archive\)](#)

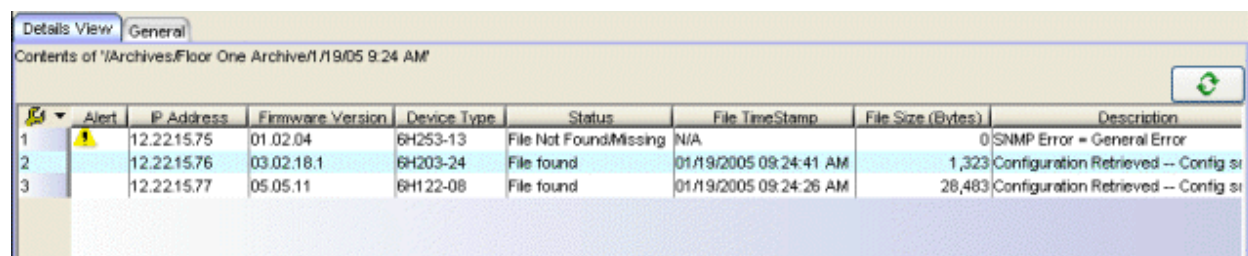
For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)

## Details View Tab (Archive Version)

The Details View tab appears when you select an archive version in the left panel's Archive Mgmt tab. The archive version is the date and time that an archive operation was performed. The Details View displays the individual configurations that were saved for this archive version, listed by device IP address. Right-click an item or items for a menu of options.



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a window titled 'Details View' with a 'General' tab. The window content is 'Contents of "/>

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between this saved configuration and the previous configuration saved for the same device.
-  -- the configuration save failed.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### IP Address

Lists the individual devices (by device IP address) whose configuration files were saved by this version of the archive operation.

### Firmware Version

Shows the firmware version for this device at the time of the save operation.

### Device Type

The device's model number or hardware type.

**Status**

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that Inventory Manager can no longer find the config file (it has been deleted or moved) or the archive operation did not include saving device configuration data. Check the [Description field](#) for more information.

**File TimeStamp**

The date and time the configuration was created.

**File Size**

The size of the saved configuration in bytes.

**Description**

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. It also displays information pertaining to any alert icon displayed in the Alert column. If the archive did not include a device configuration save, this field will display "Device archived without configuration file." Rest your cursor on the field to display a tooltip of the complete description.



Performs a configuration discovery, updating the archive information in the table.

---

**Related Information**

For information on related tabs:


- [Details View Tab \(Archive\)](#)

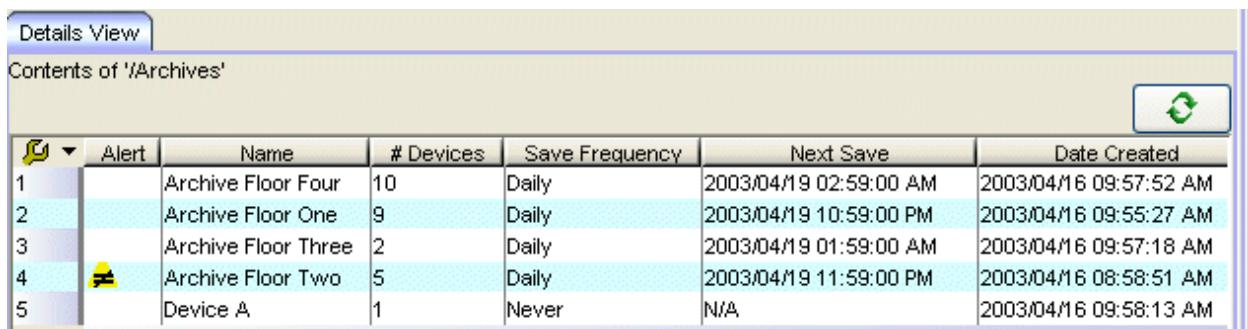
For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)


## Details View Tab (Archives Folder)

The Details View tab appears when you select the top-level Archives folder in the left panel's Archive Mgmt tab. The Details View displays information about your archive operations. Right-click an item or items for a menu of options.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.





The screenshot shows a window titled 'Details View' with a sub-header 'Contents of 'Archives''. The table has the following data:

	Alert	Name	# Devices	Save Frequency	Next Save	Date Created
1		Archive Floor Four	10	Daily	2003/04/19 02:59:00 AM	2003/04/16 09:57:52 AM
2		Archive Floor One	9	Daily	2003/04/19 10:59:00 PM	2003/04/16 09:55:27 AM
3		Archive Floor Three	2	Daily	2003/04/19 01:59:00 AM	2003/04/16 09:57:18 AM
4		Archive Floor Two	5	Daily	2003/04/19 11:59:00 PM	2003/04/16 08:58:51 AM
5		Device A	1	Never	N/A	2003/04/16 09:58:13 AM

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between saved configuration(s) for the versions of this archive.
-  -- a configuration save failed for one or more of the devices that this archive is responsible for.

### Name

The name of the archive operation.

### # Devices

The number of devices that this archive is responsible for.

### Save Frequency

The frequency with which the archive operation is performed. A frequency of Never signifies that the archive is not currently scheduled to be performed again.

**Next Save**

The next scheduled save operation this archive will perform.

**Date Created**

The date and time the archive operation was created.

**Description**

A description of the archive operation. You can edit this description in the [archive General tab](#).



Performs a configuration discovery, updating the archive information in the table.

---

**Related Information**


For information on related tasks:

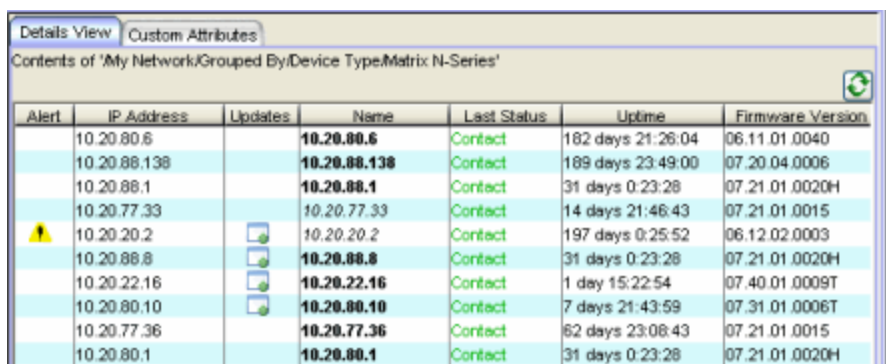
- [How to Archive](#)
- [How to Restore an Archive](#)

## Details View Tab (Device Group)






The Details View tab appears in the right panel when you select a device group in the left panel's Network Elements tab. It displays a table of information about all the devices in the selected group and any subgroups. Right-click an item or items for a menu of options. For information on the system-created device groups and how to create your own device groups, see [How to Add and Remove Device Groups](#).

**TIP:** The right-panel data is also displayed in the [General tab](#) and [Image Information tab](#) for each device. The General tab allows you to view the information and also edit certain fields.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.







The screenshot shows a table titled 'Contents of 'My Network/Grouped By/Device Type:Matrix N-Series''. The table has columns for Alert, IP Address, Updates, Name, Last Status, Uptime, and Firmware Version. The data is as follows:

Alert	IP Address	Updates	Name	Last Status	Uptime	Firmware Version
	10.20.80.6		<b>10.20.80.6</b>	Contact	182 days 21:26:04	06.11.01.0040
	10.20.88.138		<b>10.20.88.138</b>	Contact	189 days 23:49:00	07.20.04.0006
	10.20.88.1		<b>10.20.88.1</b>	Contact	31 days 0:23:28	07.21.01.0020H
	10.20.77.33		10.20.77.33	Contact	14 days 21:46:43	07.21.01.0015
	10.20.20.2		10.20.20.2	Contact	197 days 0:25:52	06.12.02.0003
	10.20.88.8		<b>10.20.88.8</b>	Contact	31 days 0:23:28	07.21.01.0020H
	10.20.22.16		<b>10.20.22.16</b>	Contact	1 day 15:22:54	07.40.01.0009T
	10.20.80.10		<b>10.20.80.10</b>	Contact	7 days 21:43:59	07.31.01.0006T
	10.20.77.36		<b>10.20.77.36</b>	Contact	62 days 23:08:43	07.21.01.0015
	10.20.80.1		<b>10.20.80.1</b>	Contact	31 days 0:23:28	07.21.01.0020H

### Alert Icon

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between one or more saved configuration files for this device and a previous file saved for the device.
-  -- the device status is No Contact.
-  -- the last archive save or restore for this device failed.
-  -- the last firmware upgrade for this device failed.

For a description of the alert, see the Alert Description column. To delete

the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### IP address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### Updates

The firmware release status for the device according to the results from the latest Tools > Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

- Firmware Up To Date - The device is running the latest release of firmware.
- New Firmware Available - There is a new release of firmware available for this device. Right-click the icon and select Firmware Releases Available to open the Updates Available window where you can download the new firmware.
- Check Firmware Update - A Check for Firmware Updates needs to be performed to get updates for this device. For more information, see the Suite-Wide Tools Help topic How to Check for Updates.
- No Updates Available - This device does not support the Check for Firmware Updates feature.

### Name

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Tools Device Display Format Options window, followed by the SNMP context, if applicable. Entries in this column are displayed in *italics* to represent that the information may be "stale". Clicking the [Refresh button](#) changes the entries to **bold**, indicating that the information is current for a minute when you first display the view. Changing any other device information (including acknowledging an Alert icon) also changes the entry to **bold**.

### Last Status

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests. The status is updated when you right-click the device group folder and select Refresh (Rediscover) from the menu, or click the [Refresh button](#).




### Uptime

The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

### Firmware Version

Shows the current firmware version installed in the device.

### FW Reference


A  indicates that the current firmware version installed in the device matches the firmware reference image set for this device's binary family. (See [How to Set a Reference Image](#).) This column allows you to easily identify devices that need to be upgraded to the reference image.

**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current firmware on the device. The version number must be available from the reference image file and the current firmware on the device must have been installed at some point via an Inventory Manager Firmware Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the firmware version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

### Boot PROM Version

Shows the current version of Boot PROM installed in the device.

### BP Reference

A  indicates that the current Boot PROM version installed in the device matches the Boot PROM reference image set for this device's binary family. (See [How to Set a Reference Image](#).) This column allows you to easily identify devices that need to be upgraded to the reference image.

**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current boot PROM on the device. The version number must be available from the reference image file and the current boot PROM on the device must have been installed at some point via an Inventory Manager Boot PROM Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the boot PROM version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

### MAC Address

The physical layer address assigned to the interface through which Inventory Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

**Device Type**

The device's model number or hardware type.

**System Name**

The assigned name for the device.

**System Contact**

The person responsible for the device.

**System Location**

The physical location of the device.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes.

**System Description**

Description of the piece of equipment, which may include its manufacturer, model number, and firmware revision number.

**Chassis Slot**

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

**Chassis ID**

The ID assigned to the chassis where the device resides.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**CPU**

The name of the device's processor (Central Processing Unit).


**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

**File Transfer Method**

The file transfer method for this device. For more information, see [How to Set a File Transfer Method](#).

**FW Download**

A  indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

### Boot PROM Download

A ✓ indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

### Config Download

A ✓ indicates the device supports the ability to save and restore archives (configurations) using the [Archive Wizard](#) and [Restore Wizard](#).

### Timed Reset

A ✓ indicates the device supports the ability to perform a timed reset using the [Reset Device Wizard](#).

### Alert Description

Describes the cause of any alert icon appearing in the Alert column.



Performs a device refresh, updating the device information in the table. If the [Name column](#) entry is in *italics* (indicating that the information may be "stale"), clicking this Refresh button changes the Name column entry to **bold**, indicating that you have current device information for a minute when you first display the view.

---

### Related Information

For information on related tabs:

- [Details View Tabs](#)
- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)


For information on related tasks:

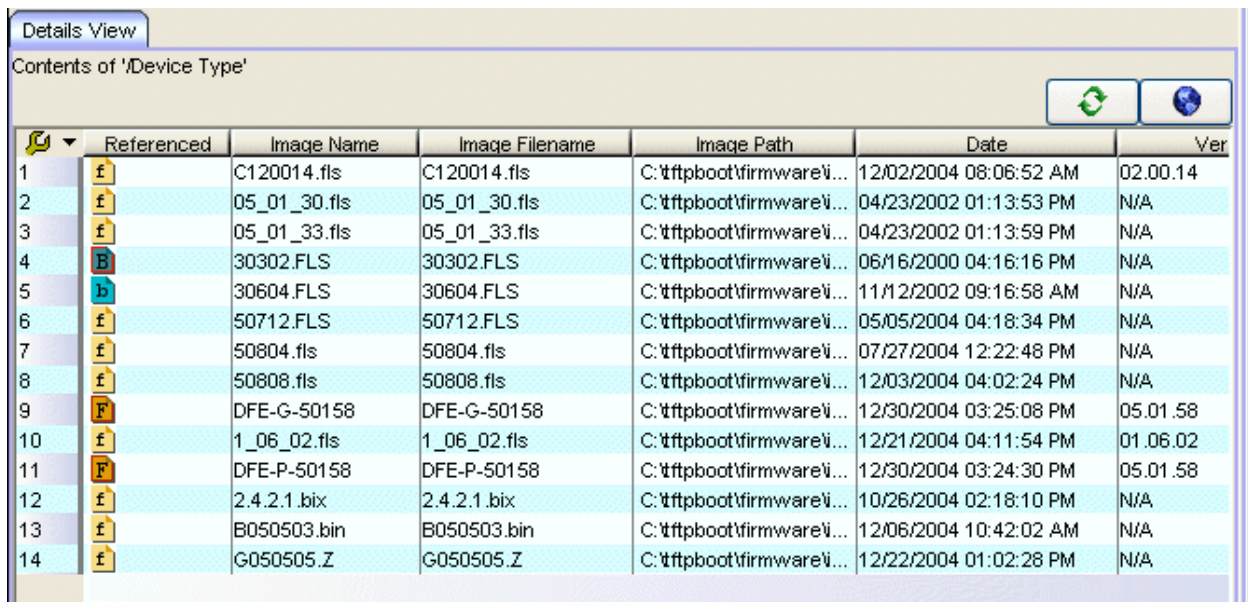
- [How to Add and Remove Device Groups](#)

## Details View Tab (Device Type Folder - Firmware)

The Details View tab appears in the right panel when you select the Device Type folder in the left panel's Firmware Mgmt tab. The Details View displays a list of information about all the firmware and boot PROM images listed in the left panel under the firmware groups and subgroups. Right-click an item or items for a menu of options.

Inventory Manager provides pre-defined firmware groups based on product family and device type, and automatically organizes the firmware and boot PROM images stored in your firmware directory under the appropriate group when you perform a [firmware discovery or refresh](#). All of these groups are organized under the top-level Device Type folder in the Firmware Mgmt tab.



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of \'Device Type\'' and a table of firmware and boot PROM images. The table has columns for 'Referenced', 'Image Name', 'Image Filename', 'Image Path', 'Date', and 'Ver'. The 'Referenced' column contains icons: a folder icon (f), a blue folder icon (B), and a red folder icon (P). The 'Image Name' and 'Image Filename' columns contain the same text. The 'Image Path' column contains paths starting with 'C:\tftpboot\firmware\'. The 'Date' column contains dates and times. The 'Ver' column contains version numbers or 'N/A'.

	Referenced	Image Name	Image Filename	Image Path	Date	Ver
1	f	C120014.flx	C120014.flx	C:\tftpboot\firmware\i...	12/02/2004 08:06:52 AM	02.00.14
2	f	05_01_30.flx	05_01_30.flx	C:\tftpboot\firmware\i...	04/23/2002 01:13:53 PM	N/A
3	f	05_01_33.flx	05_01_33.flx	C:\tftpboot\firmware\i...	04/23/2002 01:13:59 PM	N/A
4	B	30302.FLS	30302.FLS	C:\tftpboot\firmware\i...	06/16/2000 04:16:16 PM	N/A
5	B	30604.FLS	30604.FLS	C:\tftpboot\firmware\i...	11/12/2002 09:16:58 AM	N/A
6	f	50712.FLS	50712.FLS	C:\tftpboot\firmware\i...	05/05/2004 04:18:34 PM	N/A
7	f	50804.flx	50804.flx	C:\tftpboot\firmware\i...	07/27/2004 12:22:48 PM	N/A
8	f	50808.flx	50808.flx	C:\tftpboot\firmware\i...	12/03/2004 04:02:24 PM	N/A
9	P	DFE-G-50158	DFE-G-50158	C:\tftpboot\firmware\i...	12/30/2004 03:25:08 PM	05.01.58
10	f	1_06_02.flx	1_06_02.flx	C:\tftpboot\firmware\i...	12/21/2004 04:11:54 PM	01.06.02
11	P	DFE-P-50158	DFE-P-50158	C:\tftpboot\firmware\i...	12/30/2004 03:24:30 PM	05.01.58
12	f	2.4.2.1.bix	2.4.2.1.bix	C:\tftpboot\firmware\i...	10/26/2004 02:18:10 PM	N/A
13	f	B050503.bin	B050503.bin	C:\tftpboot\firmware\i...	12/06/2004 10:42:02 AM	N/A
14	f	G050505.Z	G050505.Z	C:\tftpboot\firmware\i...	12/22/2004 01:02:28 PM	N/A

### Referenced

Firmware or boot PROM images that have been set as a reference image display a reference icon (  or  ) in this column. A reference image is the image you designate as the preferred image for a specific binary family of

devices. To set a reference, select a firmware or boot PROM image in the table or the tree, right-click and select Set as Reference Image from the menu. The image will be set as a reference for all device types with which it is compatible. (If the Set as Reference Image option is not available, make sure that the selected image has been assigned to appropriate device types.)

**Image Name**

The name of the image as it is displayed in the left-panel Firmware Mgmt tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

**Image Filename**

The full name of the image as it appears in your firmware images directory.

**Image Path**

The path to the location where the image is stored.

**Date**

The image file date and time as reported by the file system.

**Version**

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field will display N/A (not available).

**Image Size (Bytes)**

The size in bytes of the image.

**Status**

The status of the image file: "File Found" or "File Not Found". This shows whether the file is still present in the firmware directory. If the image is a user-defined firmware record, this column will display "User-Defined File."

**Server**

Displays the firmware download server associated with the image file. A [discovered firmware image](#) that is accessible by the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server." A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#).



Performs a firmware discovery, updating the information in the table.



Opens the download library website where you can download firmware and release notes. If you download a firmware image that is contained in a .zip file, you must unzip the file before placing it into the firmware directory.

---

**NOTE:** It is possible to customize this button to open a different website. For example, you may want to open a corporate intranet page that lists specific firmware that has been tested and approved for your network. For information on how to do this, contact Extreme Networks Technical Support (Help > Support Center).

---

## Related Information

For information on related tasks:


- [How to Assign Firmware](#)
- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

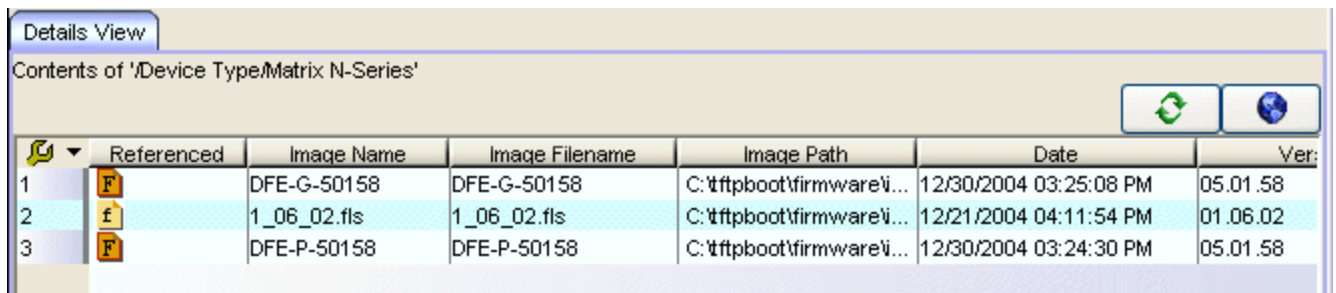
## Details View Tab (Firmware Group)

The Details View tab appears in the right panel when you select a firmware group in the left panel's Firmware Mgmt tab. It displays a list of information about all the firmware and boot PROM images for the selected group and any subgroups. Right-click an item or items for a menu of options.

Inventory Manager provides pre-defined firmware groups and automatically organizes the firmware and boot PROM images stored in your firmware directory under the appropriate group when you perform a [firmware discovery or refresh](#). Images are grouped according to:

- **Product Family** -- Devices that belong to the same product families.
- **Binary Family** -- Devices that share the same firmware image.
- **Device Type** -- Specific module types.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of '/Device Type/Matrix N-Series''. The table below lists three firmware images. The first and third rows have a reference icon (F) in the 'Referenced' column, while the second row has a file icon (f). The table columns are: Referenced, Image Name, Image Filename, Image Path, Date, and Ver:.

	Referenced	Image Name	Image Filename	Image Path	Date	Ver:
1	F	DFE-G-50158	DFE-G-50158	C:\tftpboot\firmware\i...	12/30/2004 03:25:08 PM	05.01.58
2	f	1_06_02.flx	1_06_02.flx	C:\tftpboot\firmware\i...	12/21/2004 04:11:54 PM	01.06.02
3	F	DFE-P-50158	DFE-P-50158	C:\tftpboot\firmware\i...	12/30/2004 03:24:30 PM	05.01.58

### Referenced

Firmware or boot PROM images that have been set as a reference image display a reference icon (F or B) in this column. A reference image is the image you designate as the preferred image for a specific binary family of devices. To set a reference, select a firmware or boot PROM image in the table or the tree, right-click and select Set as Reference Image from the menu. The image will be set as a reference for all device types with which it is compatible. (If the Set as Reference Image option is not available, make

sure that the selected image has been assigned to appropriate device types.)

**Image Name**

The name of the image as it is displayed in the left-panel Firmware Mgmt tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

**Image Filename**

The full name of the image as it appears in your firmware images directory.

**Image Path**

The path to the location where the image is stored.

**Date**

The image file date and time as reported by the file system.

**Version**

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field will display N/A (not available).

**Image Size (Bytes)**

The size in bytes of the image.

**Status**

The status of the image file: "File Found" or "File Not Found." This shows whether the file is still present in the firmware directory. If the image is a user-defined firmware record, this column will display "User-Defined File."

**Server**

Displays the firmware download server associated with the image file. A [discovered firmware image](#) that is accessible by the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server." A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#).

**HAU Compatibility Key**

This field displays the HAU Compatibility Key if one is detected on the firmware image. HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a



---

FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, Inventory Manager will attempt to perform an HAU upgrade if the HAU firmware compatibility key is the same for the currently running firmware and the newly selected firmware.

---

**NOTE:** Firmware images that were discovered with a version of Inventory Manager prior to 4.4 will need to be removed from Inventory Manager and rediscovered to populate the compatibility key field.

---



Performs a firmware discovery, updating the information in the table.



Opens the download library website where you can download firmware and release notes. If you download a firmware image that is contained in a .zip file, you must unzip the file before placing it into the firmware directory.

---

**NOTE:** It is possible to customize this button to open a different website. For example, you may want to open a corporate intranet page that lists specific firmware that has been tested and approved for your network. For information on how to do this, contact Extreme Networks Technical Support (Help > Support Center).

---

## Related Information


For information on related tasks:

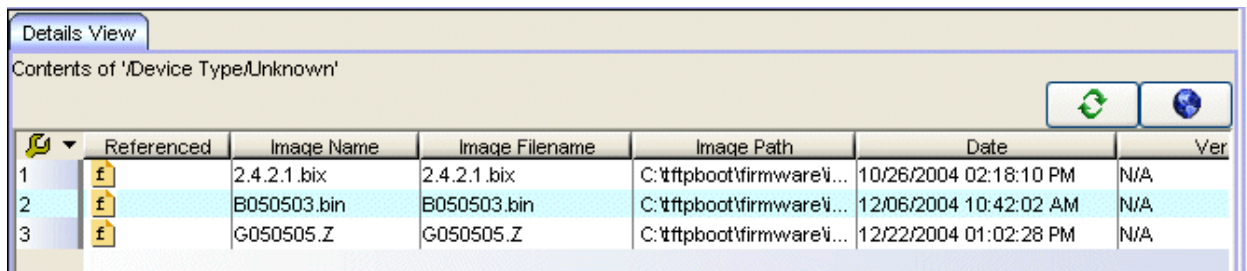
- [How to Assign Firmware](#)
- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

## Details View Tab (Unknown Folder - Firmware)




The Details View tab appears when you select the Unknown folder in the left panel's Firmware Mgmt tab. The Firmware Mgmt tab displays firmware and boot PROM images grouped according to product family and device type. Inventory Manager provides pre-defined firmware groups and automatically organizes the firmware and boot PROM images stored in your firmware directory under the appropriate group when you perform a [firmware discovery or refresh](#). The Unknown folder contains images that Inventory Manager could not correlate to a device type. Right-click an item or items for a menu of options.

**TIP:** To quickly assign an image to a device type, drag the image from the right-panel Details View into the appropriate left-panel Device Type folder.



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a window titled 'Details View' with the subtitle 'Contents of 'Device Type/Unknown''. The window contains a table with the following columns: 'Referenced', 'Image Name', 'Image Filename', 'Image Path', 'Date', and 'Ver'. There are three rows of data, each with a reference icon (a small 'f' in a square) in the 'Referenced' column. The table also includes a 'Table Tools' icon in the upper left corner and a 'Refresh' icon in the upper right corner.

	Referenced	Image Name	Image Filename	Image Path	Date	Ver
1		2.4.2.1 .bix	2.4.2.1 .bix	C:\tftpboot\firmware\i...	10/26/2004 02:18:10 PM	N/A
2		B050503 .bin	B050503 .bin	C:\tftpboot\firmware\i...	12/06/2004 10:42:02 AM	N/A
3		G050505 .Z	G050505 .Z	C:\tftpboot\firmware\i...	12/22/2004 01:02:28 PM	N/A

### Referenced

Firmware or boot PROM images that have been set as a reference image display a reference icon ( or ). However, a reference icon will never be displayed in this column for the Unknown folder because only images that have been assigned to a device type can be set as a reference image. For more information, see [How to Set a Reference Image](#).

### Image Name

The name of the image as it is displayed in the left-panel Firmware Mgmt tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

### Image Filename

The full name of the image as it appears in your firmware images directory.

### Image Path

The path to the location where the image is stored.

### Date

The image file date and time as reported by the file system.

### Version

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field will display N/A (not available).

### Image Size (Bytes)

The size in bytes of the image.

### Status

The status of the image file: "File Found" or "File Not Found." This shows whether the file is still present in the firmware directory. If the image is a user-defined firmware record, this column will display "User-Defined File."

### Server

Displays the firmware download server associated with the image file. A [discovered firmware image](#) that is accessible by the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server." A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#).



Performs a firmware discovery, updating the information in the table.



Opens the download library website where you can download firmware and release notes. If you download a firmware image that is contained in a .zip file, you must unzip the file before placing it into the firmware directory.

---

**NOTE:** It is possible to customize this button to open a different website. For example, you may want to open a corporate intranet page that lists specific firmware that has been tested and approved for your network. For information on how to do this, contact Extreme Networks Technical Support (Help > Support Center).

---

## Related Information


For information on related tasks:

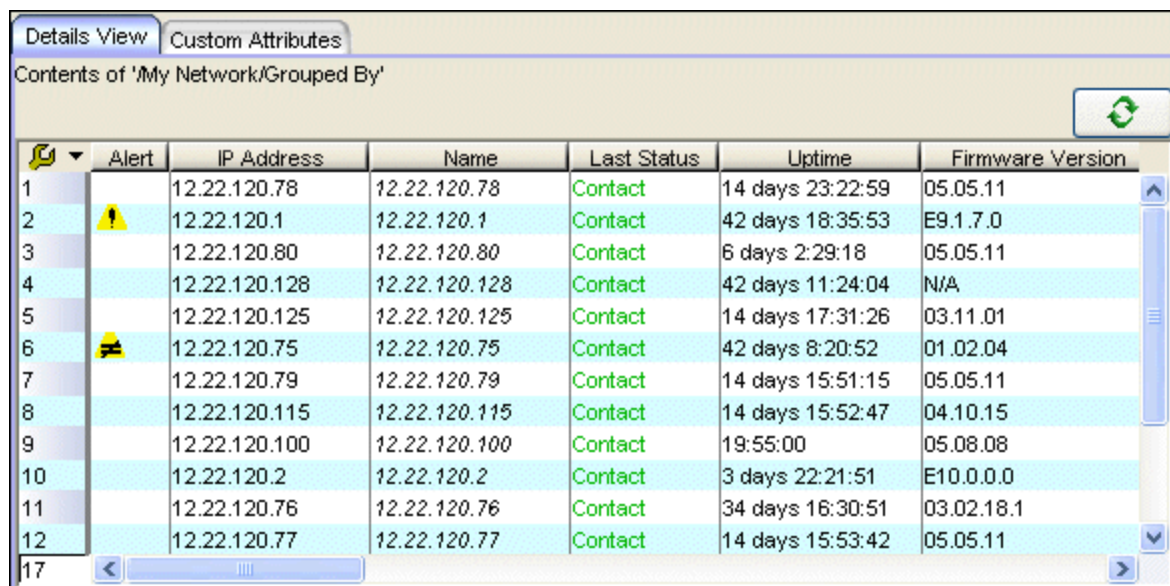
- [How to Assign Firmware](#)
- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)



## Details View Tab (Grouped By Folder)

The Details View tab appears in the right panel when you select the Grouped By folder in the left panel's Network Elements tab. It displays a table of information about all the devices grouped below this folder into the various device groups and any subgroups. Right-click an item or items for a menu of options.

**TIP:** This information is also displayed in the [General tab](#) and [Image Information tab](#) for each device. The General tab allows you to view the information and also edit certain fields.



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.





	Alert	IP Address	Name	Last Status	Uptime	Firmware Version
1		12.22.120.78	12.22.120.78	Contact	14 days 23:22:59	05.05.11
2		12.22.120.1	12.22.120.1	Contact	42 days 18:35:53	E9.1.7.0
3		12.22.120.80	12.22.120.80	Contact	6 days 2:29:18	05.05.11
4		12.22.120.128	12.22.120.128	Contact	42 days 11:24:04	N/A
5		12.22.120.125	12.22.120.125	Contact	14 days 17:31:26	03.11.01
6		12.22.120.75	12.22.120.75	Contact	42 days 8:20:52	01.02.04
7		12.22.120.79	12.22.120.79	Contact	14 days 15:51:15	05.05.11
8		12.22.120.115	12.22.120.115	Contact	14 days 15:52:47	04.10.15
9		12.22.120.100	12.22.120.100	Contact	19:55:00	05.08.08
10		12.22.120.2	12.22.120.2	Contact	3 days 22:21:51	E10.0.0.0
11		12.22.120.76	12.22.120.76	Contact	34 days 16:30:51	03.02.18.1
12		12.22.120.77	12.22.120.77	Contact	14 days 15:53:42	05.05.11

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between one or more saved configuration files for this device and a previous file saved for the device.
-  -- the device status is No Contact.

-  -- the last archive save or restore for this device failed.
-  -- the last firmware upgrade for this device failed.

For a description of the alert, see the Alert Description column. To delete the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### IP address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### Name

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Data Display Format Options window, followed by the SNMP context, if applicable. Entries in this column are displayed in *italics* to represent that the information may be "stale". Clicking the [Refresh button](#) changes the entries to **bold**, indicating that the information is current for a minute when you first display the view. Changing any other device information (including acknowledging an Alert icon) also changes the entry to **bold**.

### Last Status

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests. The status is updated when you right-click the Grouped By folder and select Refresh (Rediscover) from the menu, or click the [Refresh button](#).


### Uptime

The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

### Firmware Version

Shows the current firmware version installed in the device.

### FW Reference

A  indicates that the current firmware version installed in the device matches the firmware reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---


**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current firmware on the device. The version number must be available from the reference image file and the current firmware on the device must have been installed at some point via an Inventory Manager Firmware Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the firmware version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

### BootPROM Version

Shows the current version of Boot PROM installed in the device.

### BP Reference

A  indicates that the current Boot PROM version installed in the device matches the Boot PROM reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---

**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current boot PROM on the device. The version number must be available from the reference image file and the current boot PROM on the device must have been installed at some point via an Inventory Manager Boot PROM Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the boot PROM version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

### MAC Address

The physical layer address assigned to the interface through which Inventory Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

### Device Type

The device's model number or hardware type.

### System Name

The assigned name for the device.

### System Contact

The person responsible for the device.

**System Location**

The physical location of the device.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes.

**System Description**

Description of the piece of equipment, which may include its manufacturer, model number, and firmware revision number.

**Chassis Slot**

The slot number in the chassis where the device resides.

**Chassis ID**

The ID assigned to the chassis where the device resides.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**CPU**

The name of the device's processor (Central Processing Unit).


**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).


**File Transfer Method**

The file transfer method for this device. For more information, see [How to Set a File Transfer Method](#).


**FW Download**

A  indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

**Boot PROM Download**

A  indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

**Config Download**

A  indicates the device supports the ability to save and restore archives (configurations) using the [Archive Wizard](#) and [Restore Wizard](#).

**Timed Reset**

A  indicates the device supports the ability to perform a timed reset using the [Reset Device Wizard](#).



### Alert Description

Describes the cause of any alert icon appearing in the Alert column.



Performs a device refresh, updating the device information in the table. If the [Name column](#) entry is in *italics* (indicating that the information may be "stale"), clicking this Refresh button changes the Name column entry to **bold**, indicating that you have current device information for a minute when you first display the view.

---

### Related Information

For information on related tabs:

- [Details View Tabs](#)
- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)


For information on related tasks:

- [How to Add and Remove Device Groups](#)



## Details View Tab (My Network Folder)

The Details View tab appears in the right panel when you select the My Network folder in the left panel's Network Elements tab. The My Network folder contains all the devices in the NetSight database, and the Details View displays a table of information about those devices. Right-click an item or items for a menu of options.

**TIP:** This information is also displayed in the [General tab](#) and [Image Information tab](#) for each device. The General tab allows you to view the information and also edit certain fields.





Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



Alert	IP Address	Updates	Name	Last Status	Uptime	Firmware Version
	10.20.88.138		10.20.88.138	Contact	189 days 23:49:00	07.20.04.0006
	10.20.88.199		10.20.88.199	Contact	197 days 15:35:27	06.03.06.0008
	10.20.80.14		10.20.80.14	No Contact	171 days 19:01:28	05.02.08.0006
	10.20.80.15		10.20.80.15	Contact	192 days 18:42:08	01.01.05.0004
	10.20.88.196		10.20.88.196	Contact	3 days 20:20:53	07.41.01.0192
	10.20.23.6		10.20.23.6	Contact	1 day 20:55:40	4.1.0.31T
	10.20.88.130		10.20.88.130	Contact	127 days 16:15:09	02.01.08.0002
	10.20.88.131		10.20.88.131	Contact	127 days 16:24:33	04.02.04.0002
	10.20.80.12		10.20.80.12	Contact	197 days 12:05:46	06.03.04.0004
	10.20.80.13		10.20.80.13	Contact	193 days 1:26:27	05.02.08.0006
	10.20.80.10		10.20.80.10	Contact	7 days 21:43:59	07.31.01.0006T
	10.20.88.135		10.20.88.135	Contact	127 days 16:16:35	06.41.06.0002
	10.20.80.1		10.20.80.1	Contact	31 days 0:23:28	07.21.01.0020H

### Alert

A yellow alert icon in this column signifies one or more of the following:

-  -- there is a difference between one or more saved configuration files for this device and a previous file saved for the device.
-  -- the device status is No Contact.
-  -- the last archive save or restore for this device failed.
-  -- the last firmware upgrade for this device failed.

For a description of the alert, see the Alert Description column. To delete

the alert icon, right-click the icon and select Acknowledge Alert from the menu.

### IP address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### Updates

The firmware release status for the device according to the results from the latest Tools > Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

- Firmware Up To Date - The device is running the latest release of firmware.
- New Firmware Available - There is a new release of firmware available for this device. Right-click the icon and select Firmware Releases Available to open the Updates Available window where you can download the new firmware.
- Check Firmware Update - A Check for Firmware Updates needs to be performed to get updates for this device. For more information, see Suite-Wide Tools Help topic How to Check for Updates.
- No Updates Available - This device does not support the Check for Firmware Updates feature.

### Name

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Tools Data Display Format Options window, followed by the SNMP context, if applicable. Entries in this column are displayed in *italics* to represent that the information may be "stale". Clicking the [Refresh button](#) changes the entries to **bold**, indicating that the information is current for a minute when you first display the view. Changing any other device information (including acknowledging an Alert icon) also changes the entry to **bold**.

### Last Status

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests. The status is updated when you right-click the All Devices folder and select Refresh (Rediscover) from the menu, or click the [Refresh button](#).


### Uptime

The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

### Firmware Version

Shows the current firmware version installed in the device.

### FW Reference

A  indicates that the current firmware version installed in the device matches the firmware reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---


**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current firmware on the device. The version number must be available from the reference image file and the current firmware on the device must have been installed at some point via an Inventory Manager Firmware Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the firmware version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

### Boot PROM Version

Shows the current version of boot PROM installed in the device.

### BP Reference

A  indicates that the current boot PROM version installed in the device matches the boot PROM reference image set for this device's binary family. For more information, see [How to Set a Reference Image](#). This column allows you to easily identify devices that need to be upgraded to the reference image.

---

**NOTE:** In order to provide this information, Inventory Manager compares the name and version number of the reference image file to the current boot PROM on the device. The version number must be available from the reference image file and the current boot PROM on the device must have been installed at some point via an Inventory Manager Boot PROM Upgrade Wizard operation that included a device reset. Otherwise, this column may be blank even though the boot PROM version installed on the device may actually match the reference image. If the version number is not available from an image file, you can manually set the version number in the [Firmware Image General Tab](#).

---

**MAC Address**

The physical layer address assigned to the interface through which Inventory Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

**Device Type**

The device's model number or hardware type.

**System Name**

The assigned name for the device.

**System Contact**

The person responsible for the device.

**System Location**

The physical location of the device.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes.

**System Description**

Description of the piece of equipment, which may include its manufacturer, model number, and firmware revision number.

**Chassis Slot**

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

**Chassis ID**

The ID assigned to the chassis where the device resides.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**CPU**

The name of the device's processor (Central Processing Unit).

**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

**File Transfer Method**

The file transfer method for this device. For more information, see [How to Set a File Transfer Method](#).

**FW Download**

A ✓ indicates the device supports the ability to download firmware using the [Firmware Upgrade Wizard](#).

**Boot PROM Download**

A ✓ indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

**Config Download**

A ✓ indicates the device supports the ability to save and restore archives (configurations) using the [Archive Wizard](#) and [Restore Wizard](#).

**Timed Reset**

A ✓ indicates the device supports the ability to perform a timed reset using the [Reset Device Wizard](#).

**Alert Description**

Describes the cause of any alert icon appearing in the Alert column.



Performs a device refresh, updating the device information in the table. If the [Name column](#) entry is in *italics* (indicating that the information may be "stale"), clicking this Refresh button changes the Name column entry to **bold**, indicating that you have current device information for a minute when you first display the view.

---

**Related Information**


For information on related windows:

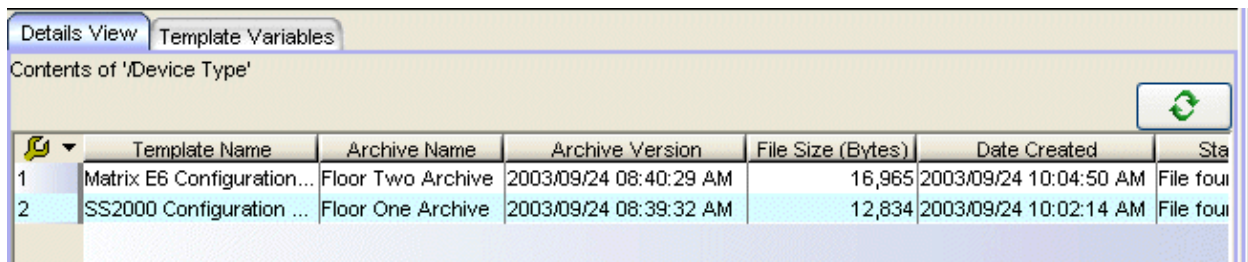
- [Details View Tabs](#)
- [General Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)

## Details View Tab (Device Type Folder - Templates)

The Details View tab appears in the right panel when you select the Device Type folder in the left panel's Configuration Templates tab. The Details View displays information about all the configuration templates listed in the left panel under the template groups and subgroups. Right-click an item or items for a menu of options.

Inventory Manager provides pre-defined template groups based on product family and device type, and automatically organizes each template under the appropriate group when you save the template in the [Edit Configuration Template window](#). All of these template groups are organized under the top-level Device Type folder in the Configuration Templates tab.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with two tabs: 'Details View' (selected) and 'Template Variables'. Below the tabs is a header 'Contents of 'Device Type'' and a refresh button. A table with 7 columns is displayed. The columns are: a row count column (1, 2), 'Template Name', 'Archive Name', 'Archive Version', 'File Size (Bytes)', 'Date Created', and 'Sta'. The first row shows 'Matrix E6 Configuration...' with a file size of 16,965 bytes and a date of 2003/09/24 10:04:50 AM. The second row shows 'SS2000 Configuration ...' with a file size of 12,834 bytes and a date of 2003/09/24 10:02:14 AM.

	Template Name	Archive Name	Archive Version	File Size (Bytes)	Date Created	Sta
1	Matrix E6 Configuration...	Floor Two Archive	2003/09/24 08:40:29 AM	16,965	2003/09/24 10:04:50 AM	File fou
2	SS2000 Configuration ...	Floor One Archive	2003/09/24 08:39:32 AM	12,834	2003/09/24 10:02:14 AM	File fou

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Name

The name of the archive that contained the configuration file the template was based on.

### Archive Version

The archive version that contained the configuration file the template was based on.

### File Size (Bytes)

The size in bytes of the template.

**Date Created**

The date and time the template was created.

**Status**

The status of the template: File Found or File Not Found. This shows whether the template is still present in the database.

**Last Modified**

The date and time the template was last modified. You can modify (edit) a template from the template's [General Tab](#).



Updates the information in the table.

---

**Related Information**

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:


- [Assign Configuration Template Window](#)
- [Edit Configuration Template Window](#)

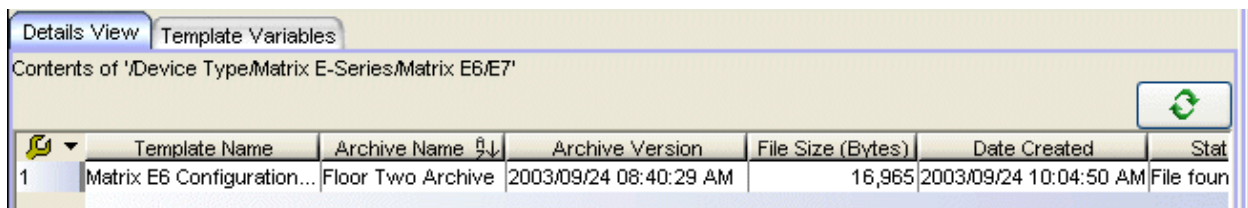


## Details View Tab (Template Group)

The Details View tab appears in the right panel when you select a template group in the left panel's Configuration Templates tab. The Details View displays a list of information about all the templates for the selected group and any subgroups. Right-click an item or items for a menu of options.

Inventory Manager provides pre-defined groups based on product family and device type, and automatically organizes each template under the appropriate device type when you save the template in the [Edit Configuration Template window](#). You can also assign a template to any template group using the [Assign Configuration Template window](#).

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with two tabs: 'Details View' (selected) and 'Template Variables'. Below the tabs, the text reads 'Contents of '/Device Type/Matrix E-Series/Matrix E6/E7''. A table is displayed with the following columns: Template Name, Archive Name, Archive Version, File Size (Bytes), Date Created, and Stat. A single row is visible with the following data: 1, Matrix E6 Configuration..., Floor Two Archive, 2003/09/24 08:40:29 AM, 16,965, 2003/09/24 10:04:50 AM, File four. A right-click menu icon is visible in the top left of the table area, and a refresh icon is in the top right.

	Template Name	Archive Name	Archive Version	File Size (Bytes)	Date Created	Stat
1	Matrix E6 Configuration...	Floor Two Archive	2003/09/24 08:40:29 AM	16,965	2003/09/24 10:04:50 AM	File four

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Name

The name of the archive that contained the configuration file the template was based on.

### Archive Version

The archive version that contained the configuration file the template was based on.

### File Size (Bytes)

The size in bytes of the template.

### Date Created

The date and time the template was created.

**Status**

The status of the template: File Found or File Not Found. This shows whether the template is still present in the database.

**Last Modified**

The date and time the template was last modified. You can modify (edit) a template from the template's [General Tab](#).



Updates the information in the table.

---

**Related Information**

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:


- [Assign Configuration Template Window](#)
- [Edit Configuration Template Window](#)

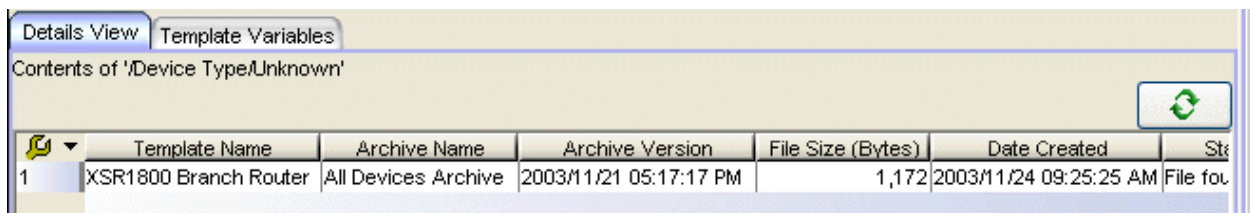
## Details View Tab (Unknown Folder - Templates)

The Details View tab appears in the right panel when you select the Unknown folder in the left panel's Configuration Templates tab. It displays information about all the templates listed under the Unknown folder. Right-click an item or items for a menu of options.

Inventory Manager provides pre-defined groups based on product family and device type, and automatically organizes each template under the appropriate device type when you save the template in the [Edit Configuration Template window](#). The Unknown folder contains any templates that Inventory Manager could not correlate to a device type.

**TIP:** To quickly assign a template to a device type, drag the template from the right-panel Details View into the appropriate left-panel Device Type folder. You can also assign a template to any template group using the [Assign Configuration Template window](#).

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with two tabs: 'Details View' (selected) and 'Template Variables'. Below the tabs is a header 'Contents of 'Device Type/Unknown'' and a refresh button. A table with 7 columns is displayed:

	Template Name	Archive Name	Archive Version	File Size (Bytes)	Date Created	St
1	XSR1800 Branch Router	All Devices Archive	2003/11/21 05:17:17 PM	1,172	2003/11/24 09:25:25 AM	File fou

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Name

The name of the archive that contained the configuration file the template was based on.

### Archive Version

The archive version that contained the configuration file the template was based on.

---

**File Size (Bytes)**

The size in bytes of the template.

**Date Created**

The date and time the template was created.

**Status**

The status of the template: File Found or File Not Found. This shows whether the template is still present in the database.

**Last Modified**

The date and time the template was last modified. You can modify (edit) a template from the template's [General Tab](#).



Updates the information in the table.

---

**Related Information**

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Assign Configuration Template Window](#)
- [Edit Configuration Template Window](#)

## General Tabs

---

A General tab is available in the right panel of the Inventory Manager main window when an archive, device, firmware image, configuration, template, or device type folder is selected in the left-panel tab. It provides general properties information about the selected item.

Help topics for the right-panel General tabs are named to reflect the item selected in the left-panel tree. For example, the help topic for the General tab with a device selected in the left panel is named General Tab (Device). For more complete information on these tabs, expand the General folder and select the desired tab.

## General Tab (Archive)

The General tab appears when you select an archive operation in the left panel's Archive Mgmt tab. It allows you to edit an archive's attributes including devices, schedule, process, and setup.

**Name:** Floor One Archive

**Description:** Archive Floor One  
Building A

**Devices in: Floor One**

Enabled	IP Address	Start Time
<input checked="" type="checkbox"/>	10.10.15.75	01/20/2005 01:10:00 AM
<input checked="" type="checkbox"/>	10.10.15.76	01/20/2005 01:10:00 AM
<input checked="" type="checkbox"/>	10.10.15.77	01/20/2005 01:10:00 AM
<input checked="" type="checkbox"/>	10.10.15.78	01/20/2005 01:10:00 AM

**Schedule**

Frequency: Weekly

Select Starting Day: January 20, 2005

**January 2005**

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Start Time: 1:10 AM EST

HH MM

**Process**

Groups of: 20

Abort on failure

**Archive setup**

**Max Versions**

Select the number of Archive versions

Maximum number of versions: 30

No maximum number of versions

**Archive Type**

Archive Configuration Data

Archive Capacity Planning data

Buttons: Save, Edit Devices...

**Name**

The name of the archive operation. You cannot change the archive name here. To rename an archive, select the archive in the left-panel Archive Mgmt tab, and then select **Edit > Rename**.

**Description**

A brief description to help you identify the archive operation.

**Devices**

Lists the devices selected for the operation. Using the checkboxes, select or deselect the devices you want to archive. To edit this device list, click [Edit Devices](#).

*Schedule***Frequency**

Use the drop-down list to select the frequency with which you want the archive performed: Never, Now, Once, Daily, Weekly, or On Server Startup. The Never option lets you create an archive operation without actually performing it. The Now option lets you perform an immediate archive.

**Select Starting Day**

Use the drop-down list to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field.

**Start Time**

Set the starting time for the operation and select AM or PM. (This field is grayed out if you have selected the Never or Now frequency.)

*Process***Groups of**

The archive will be performed simultaneously on the number of devices specified in the **Groups of** field. Enter the value **1** to have the operation performed serially, one device after another.

**Abort on failure**

Select this checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.

## Archive Setup

### Max Versions

Specify the maximum number of versions you would like saved for this archive. This allows you to limit the number of versions saved for each archive. Once the maximum number is reached, older versions are automatically deleted. If you specify a number that is less than the current number of saved versions, older versions over the maximum number will be automatically deleted the next time the archive is performed.

### Archive Type

Select the appropriate checkbox for the type of data you wish to archive:

- **Archive Configuration Data** - Create archives (backup copies) of your devices' configurations that can be restored to the devices at a later date, if needed.
- **Archive Capacity Planning data** - Create archives of port and FRU information to be used by the [Capacity Planning](#) tool to generate reports.

### Save Button

Saves any changes you have made to the archive attributes. If you have selected a Frequency of **Now**, the archive will be performed.

### Edit Devices button

Opens the [Select Devices window](#) where you can select a single group or a list of devices to include in this archive. This allows you to change the devices the archive will be performed on.

---

## Related Information

For information on related tabs:

- [Details View Tab \(Archive\)](#)

For information on related tasks:

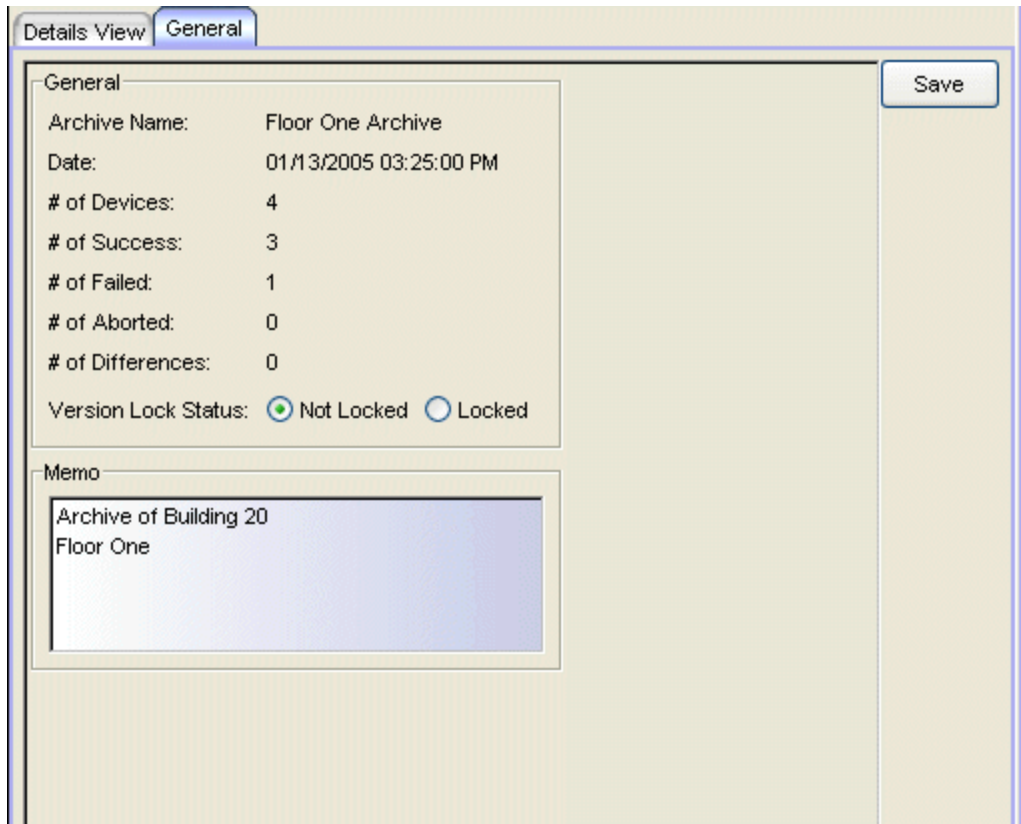
- [How to Archive](#)
- [How to Restore an Archive](#)



## General Tab (Archive Version)

---

The General tab appears when you select an archive version in the left panel's Archive Mgmt tab. The archive version is the date and time that an archive operation was performed. The General tab displays information about the version, including the number of successful and failed saves for that version.



The screenshot shows a software interface with two tabs: 'Details View' and 'General'. The 'General' tab is active. It contains a 'General' section with the following fields:

Archive Name:	Floor One Archive
Date:	01/13/2005 03:25:00 PM
# of Devices:	4
# of Success:	3
# of Failed:	1
# of Aborted:	0
# of Differences:	0
Version Lock Status:	<input checked="" type="radio"/> Not Locked <input type="radio"/> Locked

Below the 'General' section is a 'Memo' section with a text area containing the text: 'Archive of Building 20' and 'Floor One'. A 'Save' button is located in the top right corner of the 'General' section.

### Archive Name

The name of the archive operation.

### Date

The date and time the version was created.

### # of Devices

The number of devices that this archive version is responsible for.

### # of Success

The number of successful saves for the archive version.

### # of Failed

The number of saves that failed for the archive version.

**# of Aborted**

The number of saves that were aborted for the archive version.

**# of Differences**

The number of saved configurations that are different from the previous configurations saved for the device(s).

**Version Lock Status**

Whether the version is locked or not locked. A locked archive version will not be deleted when the maximum number of saved versions for this archive (as specified in the [Archive Wizard](#)) has been reached. To lock and unlock an archive version, select the version in the Archive Mgmt tab, and select **Tools > Lock/Unlock**.

**Memo**

Use this field to add additional notes about the version and save them using the **Save** button.

**Save Button**

Saves any notes you made in the Memo field.

---

**Related Information**




For information on related tabs:

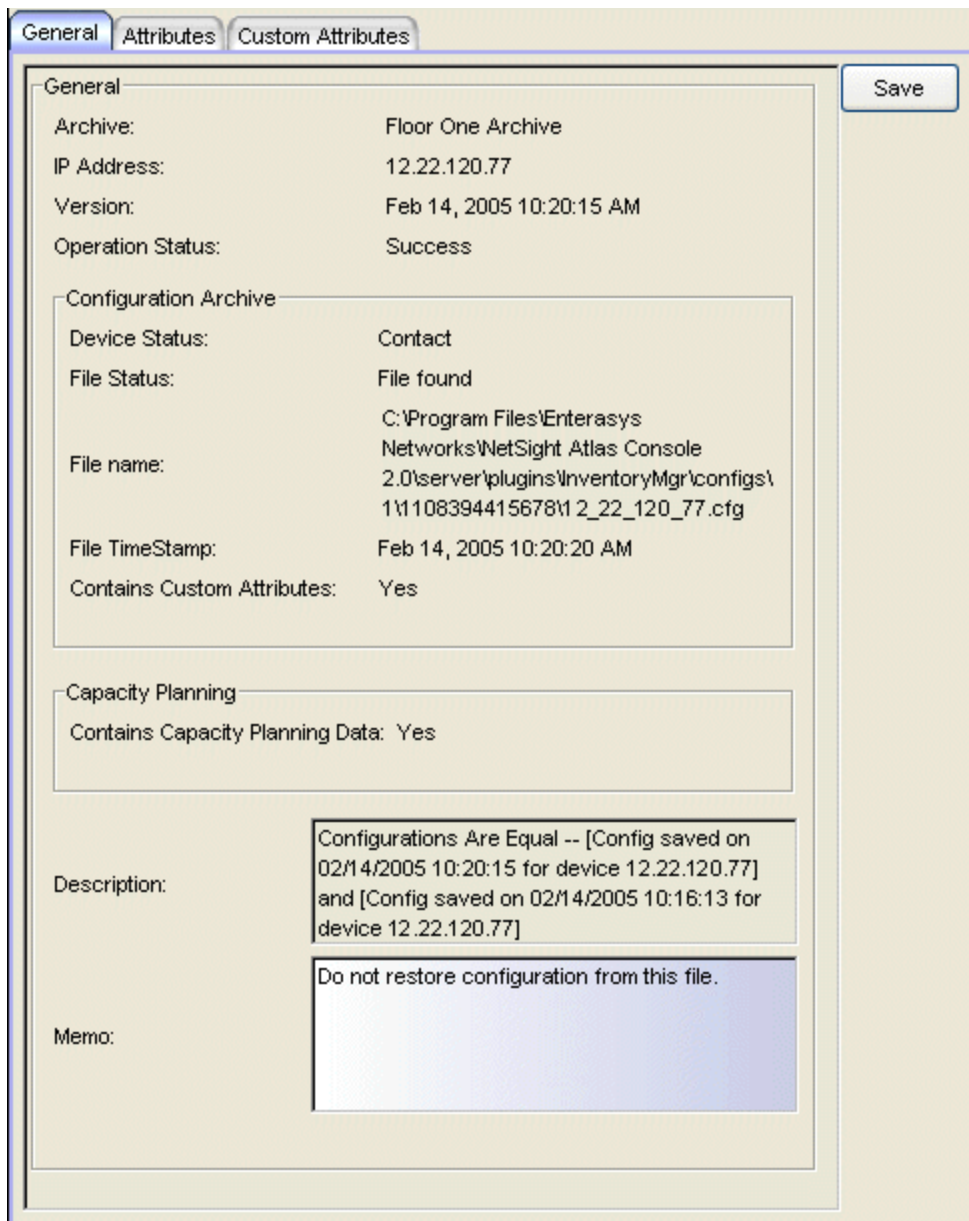
- [Details View Tab \(Archive\)](#)

For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)

## General Tab (Configuration)

The General tab appears when you select an individual configuration in the left panel's Archive Mgmt tab. Each configuration displays an icon that identifies the type of data that it contains:  device configuration data (an individual .cfg config file),  capacity planning data,  both device configuration and capacity planning data. The General tab displays information about the data that was saved.



The screenshot shows a software window with three tabs: "General", "Attributes", and "Custom Attributes". The "General" tab is active. It contains several sections of information:

- General:**
  - Archive: Floor One Archive
  - IP Address: 12.22.120.77
  - Version: Feb 14, 2005 10:20:15 AM
  - Operation Status: Success
- Configuration Archive:**
  - Device Status: Contact
  - File Status: File found
  - File name: C:\Program Files\Enterasys Networks\NetSight Atlas Console 2.0\server\plugins\InventoryMgr\configs\111108394415678\1\_2\_22\_120\_77.cfg
  - File TimeStamp: Feb 14, 2005 10:20:20 AM
  - Contains Custom Attributes: Yes
- Capacity Planning:**
  - Contains Capacity Planning Data: Yes
- Description:** Configurations Are Equal -- [Config saved on 02/14/2005 10:20:15 for device 12.22.120.77] and [Config saved on 02/14/2005 10:16:13 for device 12.22.120.77]
- Memo:** Do not restore configuration from this file.

A "Save" button is located in the top right corner of the window.

---

## *General*

### **Archive**

The name of the archive operation.

### **IP Address**

The IP address of the device whose data was saved, followed by the SNMP context, if applicable.

### **Version**

The date and time that the archive operation was performed.

### **Operation Status**

The status of the operation: Success or Failure.

### **Description**

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. For archive operations that are configured to archive only capacity planning data (and not configuration data), this column will display a Warning message stating that the ability to archive configuration data has been disabled for this archive.

### **Memo**

Use this field to add additional notes about the configuration and save them using the **Save** button.

## *Configuration Archive*

This section indicates whether device configuration data was saved when the archive was performed. Device configuration data is saved as a .cfg config file, and information about that file is displayed here. You can select whether or not to save device configuration data when you create an archive using the [Archive Wizard](#), or when you edit an archive using the [Archive General Tab](#).

### **Device Status**

The status of the device at the time the archive operation was performed: Contact or No Contact.

### **File Status**

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that Inventory Manager can no longer find the config file (it has been deleted or moved) or the archive operation did not include saving device configuration data. Check the [Description field](#) for more information.

**File Name**

The path and filename for the saved configuration. For archive operations that are configured to archive only capacity planning data (and not configuration data), this column will be blank.

**File Time Stamp**

The date and time the configuration file was created. For archive operations that are configured to archive only capacity planning data (and not configuration data), this column will be blank.

**Contains Custom Attributes**

Indicates whether the device's custom attributes were saved when the archive was performed. These attributes are displayed in a configuration's [Custom Attributes tab](#). If the device type does not support custom attributes or if the archive was not successful, this field will display "No."

*Capacity Planning*

This section indicates whether the device's port and FRU information was saved when the archive was performed. This information is used by the [Capacity Planning](#) tool to generate reports. You can select whether or not to save port and FRU information when you create an archive using the [Archive Wizard](#), or when you edit an archive using the [Archive General Tab](#).

**Contains Capacity Planning Data**

Indicates whether the device's port and FRU information was saved when the archive was performed.

**Save Button**

Saves any notes you made in the Memo field.

---

**Related Information**

For information on related tabs:

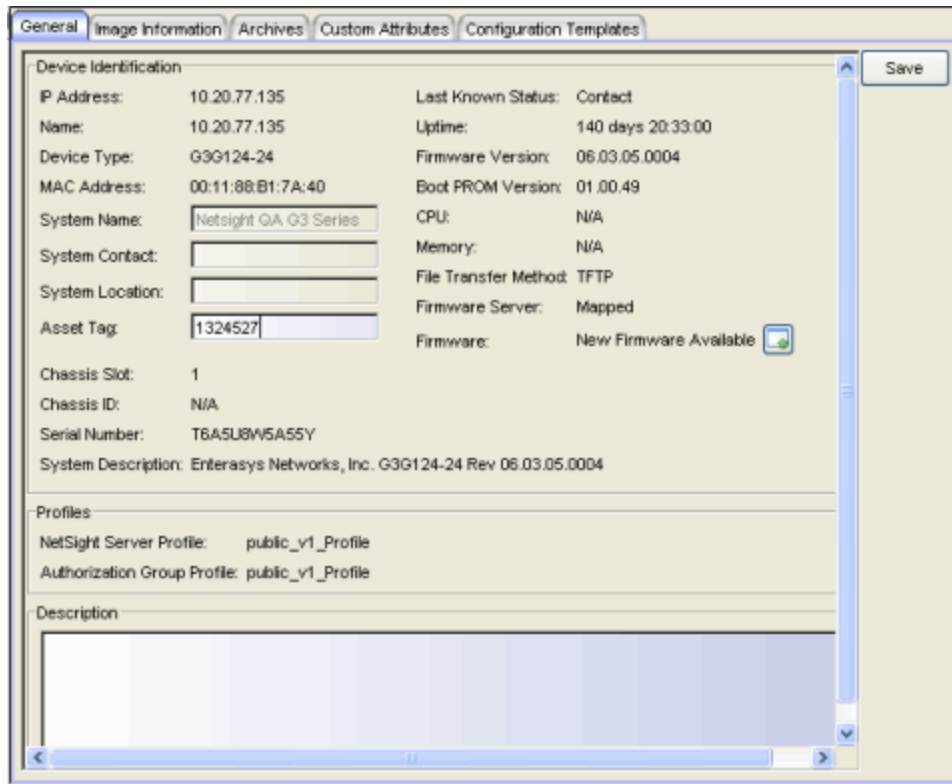
- [Attributes Tab \(Configuration\)](#)

For information on related tasks:

- [How to Archive](#)
- [How to Restore an Archive](#)

## General Tab (Device)

The General tab displays general identification and configuration information for the device selected in the left panel's Network Elements tab. It also provides a place for you to enter or change an asset tag, and save a description of the device.



The screenshot shows a web-based interface for device configuration. The 'General' tab is active, displaying the following information:

Device Identification	
IP Address:	10.20.77.135
Name:	10.20.77.135
Device Type:	G3G124-24
MAC Address:	00:11:88:B1:7A:40
System Name:	Netsight QA G3 Series
System Contact:	
System Location:	
Asset Tag:	1324527
Chassis Slot:	1
Chassis ID:	N/A
Serial Number:	T6A5U8W5A55Y
System Description:	Enterasys Networks, Inc. G3G124-24 Rev 06.03.05.0004

Profiles	
NetSight Server Profile:	public_v1_Profile
Authorization Group Profile:	public_v1_Profile

Description	
[Empty text area]	

Additional information displayed on the right side of the form:

Last Known Status:	Contact
Uptime:	140 days 20:33:00
Firmware Version:	06.03.05.0004
Boot PROM Version:	01.00.49
CPU:	N/A
Memory:	N/A
File Transfer Method:	TFTP
Firmware Server:	Mapped
Firmware:	New Firmware Available

A 'Save' button is located in the top right corner of the form.

### *Device Identification*

#### **IP Address**

The device's IP address.

#### **Name**

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Data Display Format Options window, followed by the SNMP context, if applicable.

#### **Device Type**

The device's model number or hardware type.

**MAC Address**

The physical layer address assigned to the interface through which Inventory Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

**System Name**

The assigned name of the device as stored in the device's *sysName* MIB object.

**System Contact**

The name of the person responsible for the device as stored in the device's *sysContact* MIB object.

**System Location**

The physical location of the device as stored in the device's *sysLocation* MIB object.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes. Enter a number and click **Save**. The asset tag will be stored in the Inventory Manager database and on the device. If Inventory Manager could not store the asset tag on the device, an asterisk (\*) will show up in the asset tag field indicating that the asset tag was saved only to the Inventory Manager database.

**Chassis Slot**

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

**Chassis ID**

The ID assigned to the chassis where the device resides. This is usually a serial number or MAC address, depending on the chassis type.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**System Description**

Description of the piece of equipment, including its manufacturer, model number, and firmware revision number.

**Last Known Status**

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests. The status is updated each time you select the device in the left-panel Network Elements tab.

**Uptime**

The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

**Firmware Version**

Shows the current firmware version installed in the device.

**Boot PROM Version**

Shows the current version of Boot PROM installed in the device.

**CPU**

The name of the device's processor (Central Processing Unit).

**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

**File Transfer Method**

The file transfer method for this device. For more information, see [How to Set a File Transfer Method](#).

**Firmware Server**

The firmware download server specified for the device via the [Set Firmware Server window](#). All devices are initially configured to use the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view of the Options window) for firmware downloads. By specifying an alternate firmware download server, you can enable a remote device to use a server in its own local network, and avoid performing downloads over a WAN. Use the [Alternate Firmware Servers view](#) in the Options window to configure alternate firmware download servers.

**Firmware**

The firmware release status for the device according to the results from the latest Tools > Check for Firmware Updates operation.

- Firmware Up To Date - The device is running the latest release of firmware.
- New Firmware Available - There is a new release of firmware available for this device. Click the icon to open the Updates Available window where you can download the new firmware.
- Run 'Check Firmware Updates' - A Check for Firmware Updates needs to be performed to get updates for this device. For more information, see the Suite-Wide Tools Help topic How to Check for Updates.



- Update Not Supported - This device does not support the Check for Firmware Updates feature.

### *Profiles*

This section displays the profiles assigned to the device via the Profile/Device Mapping tab in the Authorization/Device Access window.

#### **NetSight Server Profile**

The profile assigned to the device for the NetSight Administrator group. The Read Credential of this profile is used to determine contact status for this device.

#### **Authorization Group Profile**

The profile assigned to the user's Authorization Group. The credentials of this profile define the user's access privileges for SNMP communication with the device.

### *Description*

#### **Description**

Use this area to enter a description of the device and any other pertinent information. Click **Save** to save the information.

#### **Save Button**

Saves any information entered into the General tab.

---

### **Related Information**

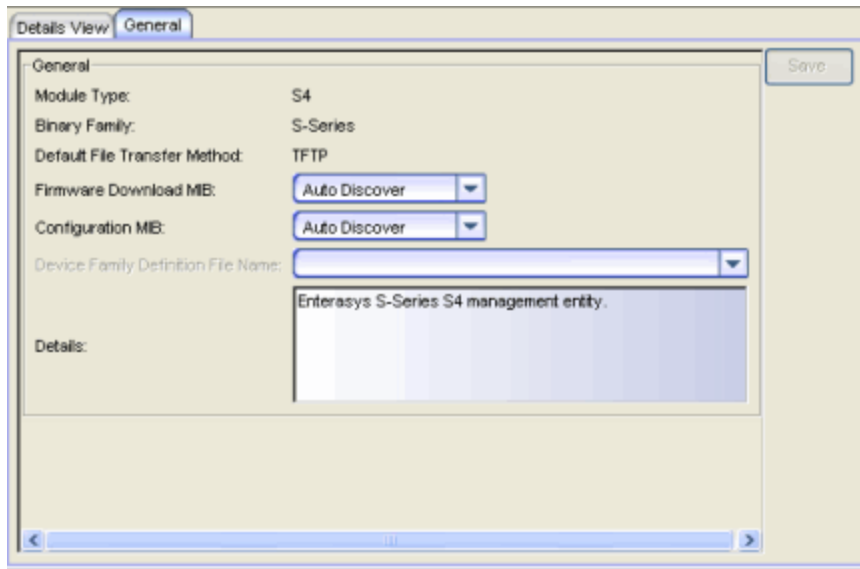
For information on related tabs:

- [Archives Tab \(Device\)](#)
- [Image Information Tab \(Device\)](#)

## General Tab (Device Type)

---

The General tab appears when you select a device type folder (lowest level folder only) in the left panel's Firmware Mgmt tab. It displays information about the device type. You can view and/or edit the information, and save your changes.



### Module Type

The device's model number or hardware type.

### Binary Family

The binary family to which the device type belongs. Device types in the same binary family share the same firmware image.

### Default File Transfer Method

The default file transfer method for this device type. To set the default file transfer method for a device type, right-click on a device type folder (lowest level folder) and select Default File Transfer Method. You can override this default at the device level. For more information, see [How to Set a File Transfer Method](#).

### Firmware Download MIB

The Firmware Download MIB supported by this device type. If the device type supports more than one Firmware Download MIB, you can use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Auto Discover** - Inventory Manager reads the Firmware Download MIB on the first device of this device type that you add or import, and display it here. Inventory Manager then uses that MIB to perform firmware and boot PROM downloads on all devices of this device type.
- **Disabled** - Firmware download functionality will not be allowed for this device type.
- **Script** - Allows the firmware download function to be executed through the use of a script. This option is used when upgrading NAC and Purview appliances as well as for third-party devices that do not support the required SNMP MIBs. For information on using scripts to upgrade Extreme Access Control and Application Analytics appliances, refer to [How to Upgrade Firmware](#). For more information on using scripts to support Inventory Manager functions, refer to [How to Set Up Third-Party Device Support](#).

Click **Save** to save any changes. You can override the MIB specified here on a per-device basis using the MIB and Script Overrides section on the [Image Information Tab \(Device\)](#).

### Configuration MIB

The Configuration MIB supported by this device type. If the device type supports more than one Configuration MIB, you can use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Auto Discover** - Inventory Manager will read the Configuration MIB on the first device of this device type that you add or import, and display it here. Inventory Manager will then use that MIB to perform archive operations on all devices of this device type.
- **Disabled** - Archive functionality will not be allowed for this device type.
- **Script** - Allows the archive functionality to be executed through the use of a script. This option is used for third-party devices that do not support the required SNMP MIBs. For more information on using scripts to support Inventory Manager functions, refer to [How to Set Up Third-Party Device Support](#).

Click **Save** to save any changes. You can override the MIB specified here on a per-device basis using the MIB and Script Overrides section on the [Image Information Tab \(Device\)](#).

### Device Family Definition File Name

If you have selected the **Script** option to allow the Firmware Download and/or Configuration functionality to be executed through a script, you must select the file containing the scripts to be used. Device Family Definition Files include all the scripts and data for each supported Inventory Manager function for specific third-party devices. Inventory Manager provides sample Definition Files for Extreme, Enterasys, Cisco Systems, and Hewlett Packard devices. For information on creating additional files, refer to [How to Set Up Third-Party Device Support](#).

### Details

Displays a description of the device type. Use this field to add information regarding the device and click **Save** to save any changes.

---

### Related Information

For information on related tabs:

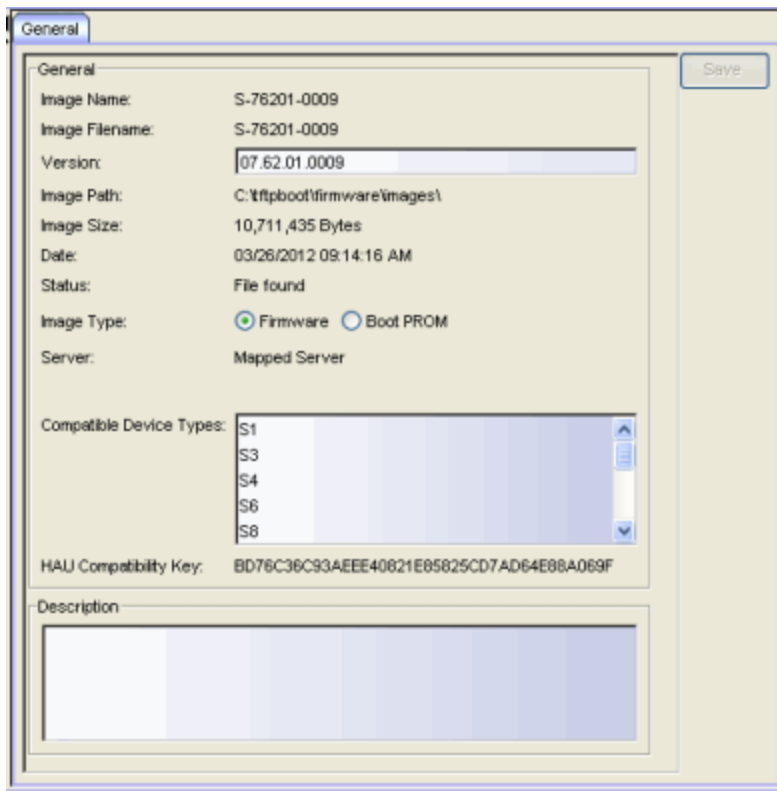
- [Details View Tab \(Device Group\)](#)
- [Details View Tab \(Firmware Group\)](#)

For information on related tasks:

- [How to Set a File Transfer Method](#)
- [How to Set Up Third-Party Device Support](#)

## General Tab (Firmware Image)

The General tab appears when you select an individual firmware or boot PROM image in the left panel's Firmware Mgmt tab. It displays information about the image.



The screenshot shows a 'General' tab window with the following fields and values:

- Image Name: S-76201-0009
- Image Filename: S-76201-0009
- Version: 07.62.01.0009
- Image Path: C:\ftpboot\firmware\images\
- Image Size: 10,711,435 Bytes
- Date: 03/26/2012 09:14:16 AM
- Status: File found
- Image Type:  Firmware  Boot PROM
- Server: Mapped Server
- Compatible Device Types: S1, S3, S4, S6, S8
- HAJ Compatibility Key: BD76C36C93AEEE40621E85825CD7AD64E88A069F

There is a 'Save' button in the top right corner and a 'Description' field at the bottom which is currently empty.

### Image Name

The name of the image as it is displayed in the left-panel Firmware Mgmt tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

### Image Filename

The full name of the image as it appears in your firmware images directory.

### Version

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field

will display N/A (not available). Enter a version number and click **Save** to manually set a version number for the image.

**Image Path**

The path to the location where the image is stored.

**Image Size**

The size in bytes of the image.

**Date**

The image file date and time as reported by the file system.

**Status**

The status of the image file: File Found or File Not Found. This shows whether the image file is still present in the firmware directory. If the image is a user-defined firmware record, this column will display "User-Defined File."

**Image Type**

Displays whether the image is a firmware or boot PROM image. Use the radio buttons to change the designation if necessary.

**Server**

Displays the firmware download server associated with the firmware image. A [discovered firmware image](#) that is accessible by the mapped file transfer server (as configured in the Suite-Wide Options Services for NetSight Server view) will display "Mapped Server". A user-defined firmware record will display its associated alternate firmware download server, as configured in the [Create Firmware Record window](#).

**Root Directory**

Displays the root directory for the firmware download server if the server is an [alternate firmware download server](#) and the image is a [user-defined firmware record](#). Otherwise, this field will not be displayed.

**Compatible Device Types**

Device types the image is valid for.

**HAU Compatibility Key**

This field displays the HAU Compatibility Key if one is detected on the firmware image. HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, Inventory Manager will

attempt to perform an HAU upgrade if the HAU firmware compatibility key is the same for the currently running firmware and the newly selected firmware.

---

**NOTE:** Firmware images that were discovered with a version of Inventory Manager prior to 4.4 will need to be removed from Inventory Manager and rediscovered to populate the compatibility key field.

---

### Description

Use this field to add a brief description of the image and any information regarding its use. Click **Save** to save any changes.

### Save

Saves any changes you have made to the version or description field.

---

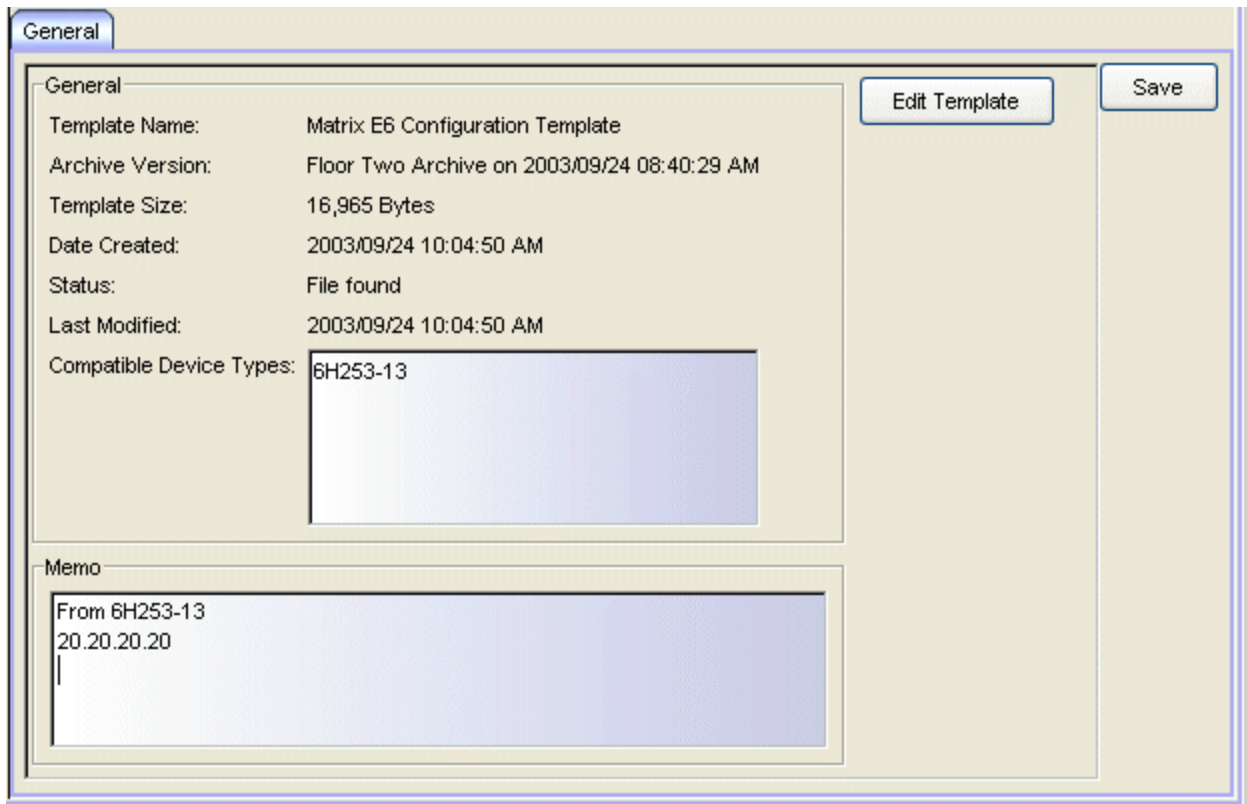
### Related Information

For information on related tasks:

- [How to Assign Firmware](#)
- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

## General Tab (Template)

The General tab appears when you select an individual configuration template in the left panel's Configuration Templates tab. It displays information about the template and allows you to edit the template, if desired.



The screenshot shows a software interface with a 'General' tab selected. The tab contains a 'General' section with the following fields:

Template Name:	Matrix E6 Configuration Template
Archive Version:	Floor Two Archive on 2003/09/24 08:40:29 AM
Template Size:	16,965 Bytes
Date Created:	2003/09/24 10:04:50 AM
Status:	File found
Last Modified:	2003/09/24 10:04:50 AM
Compatible Device Types:	6H253-13

Below the 'General' section is a 'Memo' section with a text area containing:

```
From 6H253-13  
20.20.20.20  
|
```

On the right side of the 'General' section, there are two buttons: 'Edit Template' and 'Save'.

### Template Name

The name of the configuration template, as assigned when you saved the template in the [Edit Configuration Template window](#).

### Archive Version

The archive version that contained the configuration file the template was based on.

### Template Size

The size in bytes of the template.

### Date Created

The date and time the template was created.



**Status**

The status of the template: File Found or File Not Found. File Not Found indicates that Inventory Manager can no longer find the template file; it has been deleted or moved.

**Last Modified**

The date and time the template was last modified.

**Compatible Device Types**

Device types the template is valid for, based on what device types the template has been assigned to.

**Memo**

Use this field to add any notes about the template. Click **Save** to save any changes.

**Edit Template Button**

Opens the [Edit Configuration Template window](#) where you can modify the template.

**Save Button**

Saves any changes you have made to the Memo field.

---

**Related Information**

For information on related tasks:

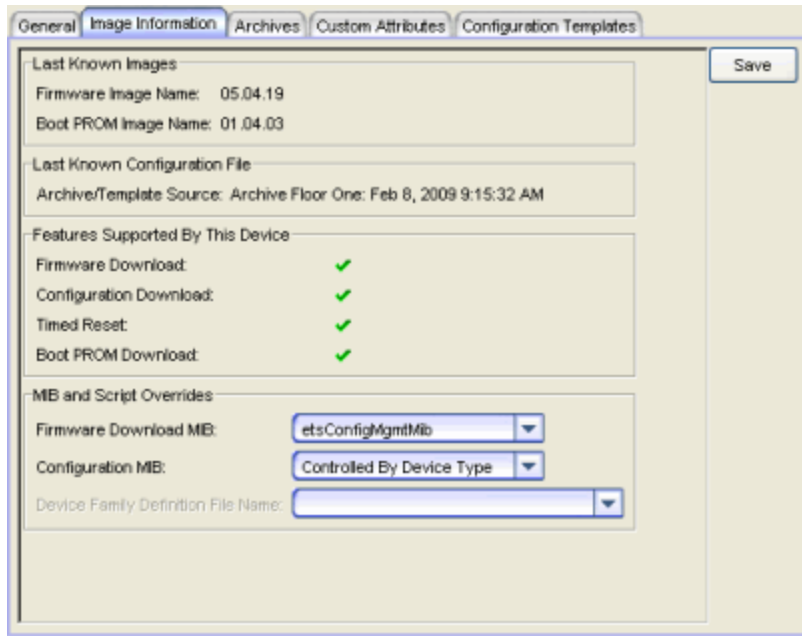
- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Assign Configuration Template Window](#)
- [Edit Configuration Template Window](#)

## Image Information Tab (Device)

The Image Information tab appears when you select a device in the left panel's Network Elements tab. It displays last known firmware and archive information for the selected device, and provides information on Inventory Manager features supported by the device.



The screenshot shows a web-based configuration interface with several tabs: General, Image Information (selected), Archives, Custom Attributes, and Configuration Templates. The Image Information tab contains the following sections:

- Last Known Images:** Firmware Image Name: 05.04.19; Boot PROM Image Name: 01.04.03.
- Last Known Configuration File:** Archive/Template Source: Archive Floor One: Feb 8, 2009 9:15:32 AM.
- Features Supported By This Device:** Firmware Download: ✓; Configuration Download: ✓; Timed Reset: ✓; Boot PROM Download: ✓.
- MB and Script Overrides:** Firmware Download MB: etsConfigMgmtMib; Configuration MB: Controlled By Device Type; Device Family Definition File Name: (empty dropdown).

A Save button is located in the top right corner of the form.

### Last Known Images

#### Firmware Image Name

Shows the last firmware image that was downloaded to the device through Inventory Manager. If no firmware image has been downloaded to the device through Inventory Manager, the field will display N/A.

#### Boot PROM Image Name

Shows the last boot PROM image that was downloaded to the device through Inventory Manager. If no boot PROM image has been downloaded to the device through Inventory Manager, the field will display N/A.


## Last Known Configuration File

### Archive/Template Source

Shows the name and version of the last archive operation performed on the device, or the name of the last configuration template downloaded to the device, through Inventory Manager. If neither operation has been performed on the device, this field will display N/A.

## Features Supported by this Device

### Firmware Download

A  indicates the device supports the ability to download firmware images using the [Firmware Upgrade Wizard](#).


### Configuration Download

A  indicates the device supports the ability to save and restore archives using the [Archive Wizard](#) and [Restore Wizard](#).

### Timed Reset

A  indicates the device supports the ability to perform a timed reset using the [Reset Wizard](#).

### Boot PROM Download

A  indicates the device supports the ability to download boot PROM images using the [Boot PROM Upgrade Wizard](#).

## MIB and Script Overrides

### Firmware Download MIB

The Firmware Download MIB supported by this device. Initially, **Controlled by Device Type** is displayed here, meaning that Inventory Manager will use the MIB specified in the Firmware Download MIB field on the [General Tab \(Device Type\)](#). If you would like to override the Device Type MIB, use the drop-down list here to select the desired MIB. Other menu options include:

- **Disabled** - Firmware download functionality will not be allowed for this device.
- **Script** - Allows the firmware download function to be executed through the use of a script. This option is used for third-party devices that do not support the required SNMP MIBs. For information on using scripts to support Inventory Manager functions, refer to [How to Set Up Third-Party Device Support](#).

Click **Save** to save any changes.

### Configuration MIB

The Configuration MIB supported by this device. Initially, **Controlled by Device Type** is displayed here, meaning that Inventory Manager will use the MIB specified in the Configuration MIB field on the [General Tab \(Device Type\)](#). If you would like to override the Device Type MIB, use the drop-down list here to select the desired MIB. Other menu options include:

- **Disabled** - Firmware download functionality will not be allowed for this device.
- **Script** - Allows the firmware download function to be executed through the use of a script. This option is used for third-party devices that do not support the required SNMP MIBs. For information on using scripts to support Inventory Manager functions, refer to [How to Set Up Third-Party Device Support](#).

Click **Save** to save any changes.

### Device Family Definition File Name

If you have selected the **Script** option to allow the Firmware Download and/or Configuration functionality to be executed through a script, you must select the file containing the scripts to be used. Device Family Definition Files include all the scripts and data for each supported Inventory Manager function for specific third-party devices. Inventory Manager provides sample Definition Files for Extreme, Enterasys, Cisco Systems, and Hewlett Packard devices. For information on creating additional files, refer to [How to Set Up Third-Party Device Support](#).

### Save Button

Saves any changes you have made in the MIB and Script Overrides section.

---

### Related Information


For information on related tabs:

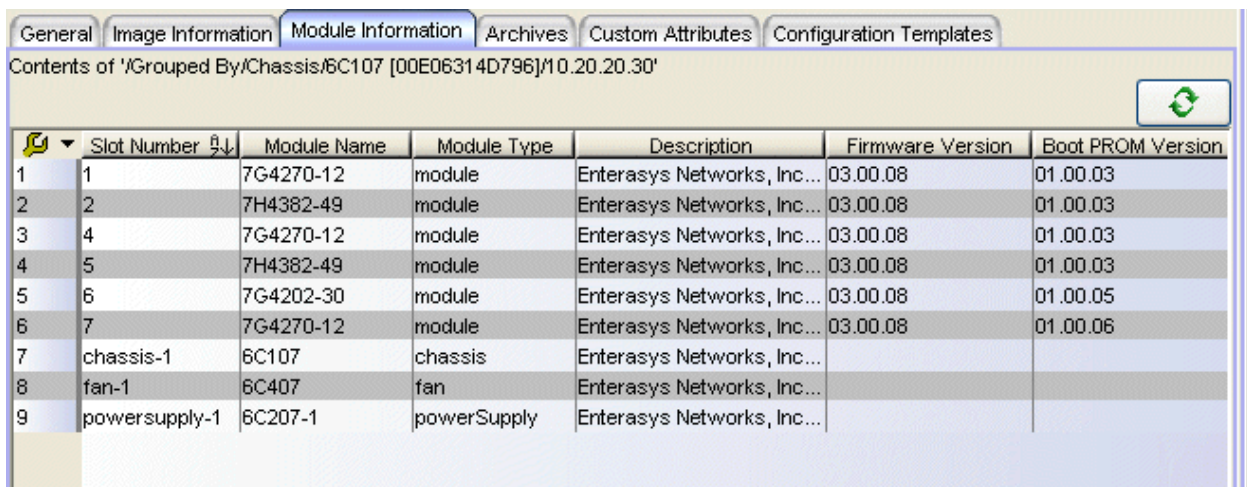
- [Archives Tab \(Device\)](#)
- [General Tab \(Device\)](#)

## Module Information Tab (Device)

The Module Information tab provides detailed information for certain devices/chassis that contain multiple modules and components, while being managed by a single IP address. This group of devices includes the N-Series devices, and certain X-Pedition devices including the SSR-8000 and SSR-8600, the ER-16, and the GIGAswitch Router 8.

To access this tab, select the device in the left panel's Network Elements tab, then click the Module Information tab in the right panel. The information displayed varies slightly depending on the device type. If a column displays N/A (not available), it means that the module or component did not return a value for that parameter. If a column is blank, it means that the module or component returned an empty value.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a web interface with several tabs: General, Image Information, Module Information (selected), Archives, Custom Attributes, and Configuration Templates. Below the tabs is a title bar: 'Contents of '/Grouped By/Chassis/6C107 [00E06314D796]/10.20.20.30''. A table is displayed with the following columns: Slot Number, Module Name, Module Type, Description, Firmware Version, and Boot PROM Version. The table contains 9 rows of data.

Slot Number	Module Name	Module Type	Description	Firmware Version	Boot PROM Version
1	7G4270-12	module	Enterasys Networks, Inc...	03.00.08	01.00.03
2	7H4382-49	module	Enterasys Networks, Inc...	03.00.08	01.00.03
3	7G4270-12	module	Enterasys Networks, Inc...	03.00.08	01.00.03
4	7H4382-49	module	Enterasys Networks, Inc...	03.00.08	01.00.03
5	7G4202-30	module	Enterasys Networks, Inc...	03.00.08	01.00.05
6	7G4270-12	module	Enterasys Networks, Inc...	03.00.08	01.00.06
7	chassis-1	chassis	Enterasys Networks, Inc...		
8	fan-1	fan	Enterasys Networks, Inc...		
9	powersupply-1	powerSupply	Enterasys Networks, Inc...		

### Slot Number

The slot number in the chassis where the module or component resides.

### Module Name

The information in this column varies depending on the selected device. For N-Series devices it displays the model number of the module or

component. For other devices, it displays a description of the module.

**Module Type**

The information in this column varies depending on the selected device. For N-Series devices it displays a description of the module or component type. For other devices, it displays the physical module type.

**Description**

A description of the module or component.

**Firmware Version**

The current firmware version installed in the module.

**BootPROM Version**

The current version of Boot PROM installed in the module.

**Serial Number**

A unique number assigned to the module or component by the manufacturer.

**Asset Tag**

A unique asset number assigned to the module or component for inventory tracking purposes.

**Memory**

The system memory size available on the module, reported in megabytes (MB).



Updates the information in the table.

---

**Related Information**


For information on related tabs:

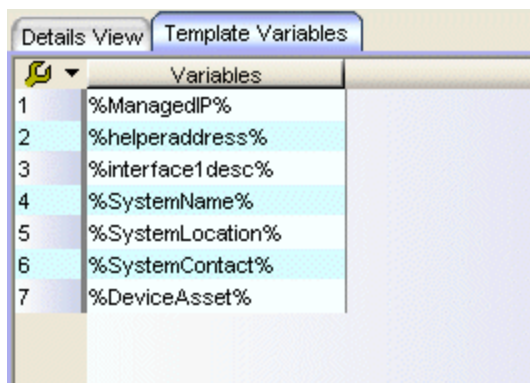
- [Custom Attributes Tab](#)

## Template Variables Tab

---

The Template Variables tab can be selected in the right panel when you select any folder in the left panel's Configuration Templates tab. It lists all the variables that have been defined for use in creating a configuration template. To add a variable, right-click in the table and select Create Template Variable. (You can also define template variables in the [Template Variables window](#) accessed from the [Edit Configuration Template window](#).) To delete a variable, right-click the variable and select Delete. For more information on creating templates and assigning values to template variables, see [How to Create and Download Configuration Templates](#).

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.



The screenshot shows a software interface with two tabs: 'Details View' and 'Template Variables'. The 'Template Variables' tab is active and displays a table with the following content:

Variables	
1	%ManagedIP%
2	%helperaddress%
3	%interface1desc%
4	%SystemName%
5	%SystemLocation%
6	%SystemContact%
7	%DeviceAsset%

### Variables

Lists all the template variables that have been defined. To add a variable, right-click in the table and select Create Template Variable. To delete a variable, right-click the variable and select Delete.

---

### Related Information

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Edit Configuration Template Window](#)
- [Template Variables Window](#)



# Inventory Manager Windows

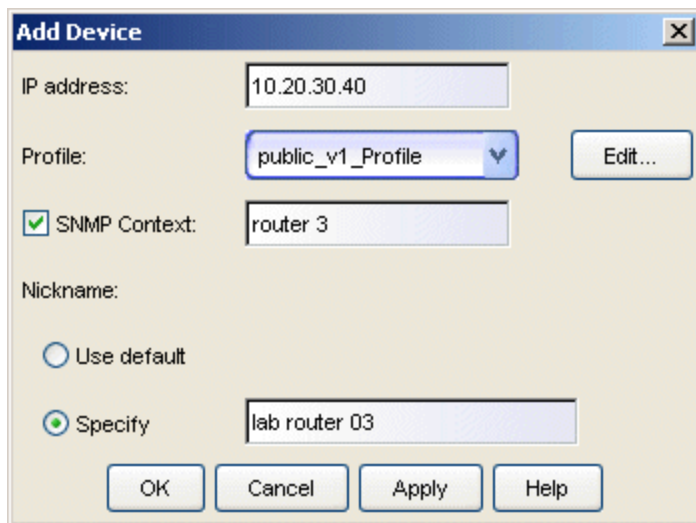
---

The **Windows** Help section contains Help topics describing Inventory Manager windows and their field definitions.

## Add Device Window

---

This window lets you add a single device to your NetSight database, as opposed to [discovering](#) devices or [importing](#) devices from a device list. When you add a device, it is added to the All Devices folder and also automatically organized under the appropriate groups in the left-panel tree. You can access this window by right-clicking a group in the left panel and choosing **Add Device** from the right-click menu.



### IP Address

Enter the IP address of the device you want to add.

### Profile

Use the drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.

### SNMP Context

Select the checkbox and enter an SNMP context that has been configured on the device. An SNMP context is a collection of MIB objects, often associated with an entity. By specifying the SNMP context here, you can access the subset of MIB objects related to that context on the device.

The use of context differs depending on the protocol version being used with a user's credentials:

- When used with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.
- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, an SNMPv1 or SNMPv2 community name can be mapped through Local Management, to a particular SNMP context on the device. Then, when SNMPv1/v2 credentials are used, access is granted to the subset of MIB objects associated with that credential (community name).

Inventory Manager treats each context for a given device (IP address) as a distinct device. The devices are displayed in the tree with the same IP address followed by the different SNMP contexts. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to a device *Configuration Guide* for more information about setting and showing SNMP contexts.

### Nickname

You can use the default nickname or click **Specify** to assign a unique nickname to this device. The default nickname for SNMP devices is the `sysName` MIB object, or if no `sysName` has been assigned, the device's IP address. The default nickname for pingable devices is the IP address.

### Edit Buttons

Opens the Profiles/Credentials tab in the Authorization/Device Access window where you can add or modify an existing profile to be associated with this device.

### OK Buttons

Adds the device and closes the window.

### Apply Buttons

Adds the device and leaves the window open so that you can add another device.

### Cancel Buttons

Closes the window, but does not remove any devices that have already been added.

## Related Information

For information on related tasks:

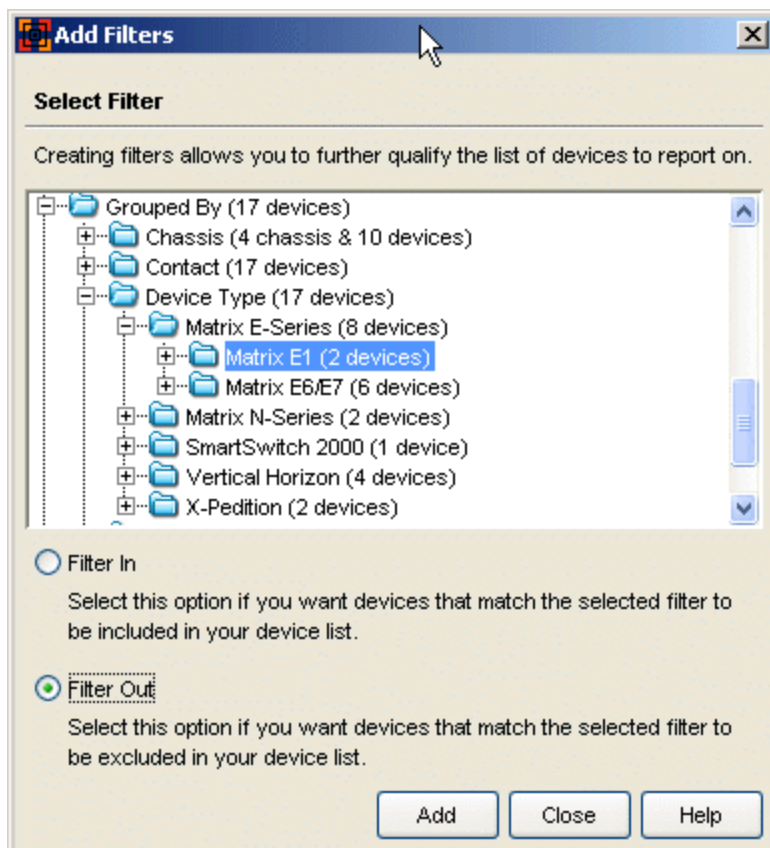
- [How to Add and Delete Devices](#)

## Add Filters Window

Use the Add Filters window to create filters that will refine your list of targeted devices for your [Capacity Planning report](#). Select a device group or single device for your filter, and then specify whether your selection should be filtered in or filtered out of your targeted devices. Click **Add** to create the filter and add it to the Applied Filters list in the Select Targets window.

**TIP:** After you have defined your filters, you can view a list of the devices you have selected for your report by clicking the **View Devices** button in the Select Targets window.

Access this window from the Select Targets window in the Capacity Planning tool by clicking the **Add Filters** button.



### Tree

Displays all your network devices, and allows you to select a device group or single device to filter in or filter out of your devices list.

**Filter In**

Select this option if you want devices that match the selected filter to be included in your device list.

**Filter Out**

Select this option if you want devices that match the selected filter to be excluded from your device list.

**Add Button**

Creates the filter. You can then create another filter or click **Close** to return to the Select Targets window.

**Close Button**

Closes the window and returns you to the Targets window. The filters you created will be added to the Applied Filters list in the Select Targets window.

---

**Related Information**

For information on related windows:

- [Capacity Planning](#)
- [View Devices Window](#)

## Add Alternate Firmware Server Window

---

Use the Add Alternate Firmware Server window to configure properties for alternate firmware download servers and specify connection information based on the selected transfer protocol. Access this window by clicking **Add Server** in the [Alternate Firmware Servers view](#) of the Options window.

The screenshot shows the 'Add Alternate Firmware Server' dialog box. It is divided into two main sections: 'Server Properties' and 'Connection Information'. The 'Server Properties' section contains four input fields: 'Server IP' with the value '1.2.3.4', 'Identifier' with 'Frankfurt', 'Server Root Path' with 'c:\tftpboot\'', and 'Transfer Protocol' with a dropdown menu set to 'TFTP'. The 'Connection Information' section contains a 'Port' field with '69'. Below this is a sub-dialog box for connection details, which includes a 'Port' field with '21', a checked 'Anonymous' checkbox, a 'Username' field with 'anonymous', a 'Password' field with '\*\*\*\*', and a checked 'Hide password' checkbox. On the right side of the main dialog, there are four buttons: 'OK', 'Apply', 'Cancel', and 'Help'.

### Server Properties

Use this area to specify the alternate server's IP address, identifier, and transfer protocol, and set the path to the root directory.

#### Server IP

Enter the IP address of the workstation where the TFTP, FTP, or SCP server is running.

#### Identifier

Enter a description that helps you identify the alternate server.

### Server Root Path

Specify the server root path. The root directory is the base directory to which the server is allowed access. The server will be allowed to create files to or read files from this directory and any of its subdirectories.

---

**NOTE:** Keep in mind the following requirements when setting the server root path:

- If your server is configured with a root directory, it must match the root directory entered here.
  - If your server is **not** configured with a root directory, specify the root directory here as the root of the drive (e.g. C:\ or D:\).
- 

### Transfer Protocol

Specify the transfer protocol for the alternate server and then enter the connection information in the section below.

## TFTP Connection Information

Use this area to specify connection information for an alternate server that has been configured with TFTP protocol.

### Port

Specify the port number your TFTP server is configured to run on.

## FTP/SCP Connection Information

Use this area to specify connection information for an alternate server that has been configured with FTP or SCP protocol.

### Port

Specify the port number your FTP/SCP server is configured to run on.

### Anonymous

Select this checkbox if your FTP/SCP server is configured to accept Anonymous logins. Inventory Manager will automatically fill in the username and password fields.

### Username/Password

Enter your username and password to access the FTP/SCP server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.



## **Related Information**

For information on related windows:

- [Alternate Firmware Servers View, Options Window](#)

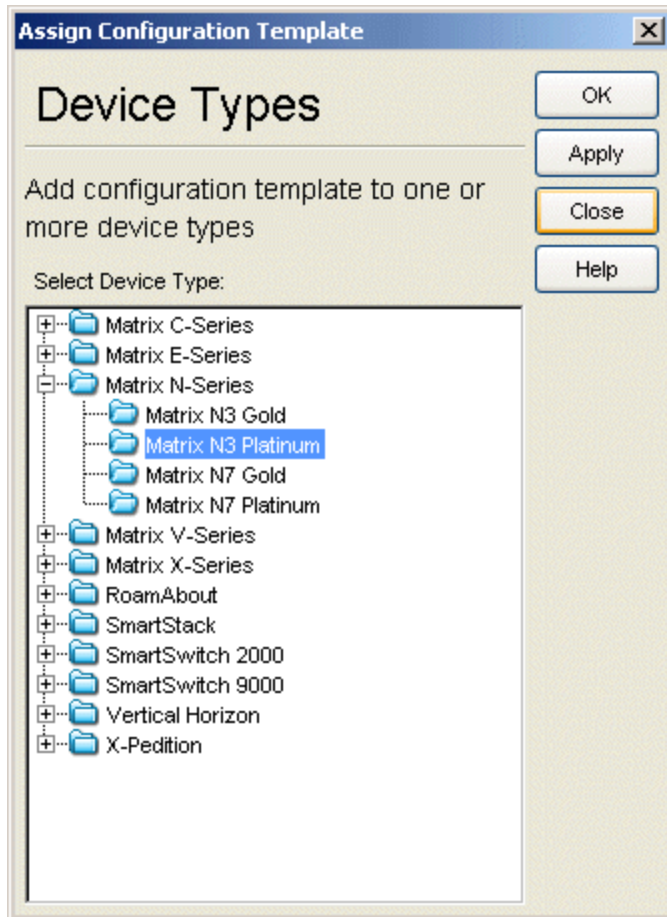
## Assign Configuration Template Window

---

The Assign Configuration Template window allows you to assign a template to one or more device types. This enables you to download the assigned template to any of your network devices of that type, using the [Template Download Wizard](#).

The left-panel Configuration Templates tab displays configuration templates grouped according to device type. Inventory Manager provides pre-defined groups and automatically organizes the templates under the appropriate device type when you save the template in the [Edit Configuration Template window](#). The Unknown folder contains templates that Inventory Manager could not correlate to a device type. Use the Assign Configuration Template window to assign those templates to the correct device type(s).

To access this window, select a template in the Configuration Templates tab (or one or more templates in the right-panel Details View tab), then select **Tools > Assign Configuration Template**. You can also right-click on a template, and select Assign Configuration Template from the menu.



## Device Types

Lists the device types to which you can assign the template. You can select multiple device types using the **Ctrl** or **Shift** keys.

## Related Information

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Edit Configuration Template Window](#)

## Assign Firmware Window

---

The Assign Firmware window allows you to assign a firmware or boot PROM image to one or more product families or device types. This enables you to download the assigned image to any of your network devices of that family or type, using the Firmware Upgrade Wizard or the Boot PROM Upgrade Wizard.

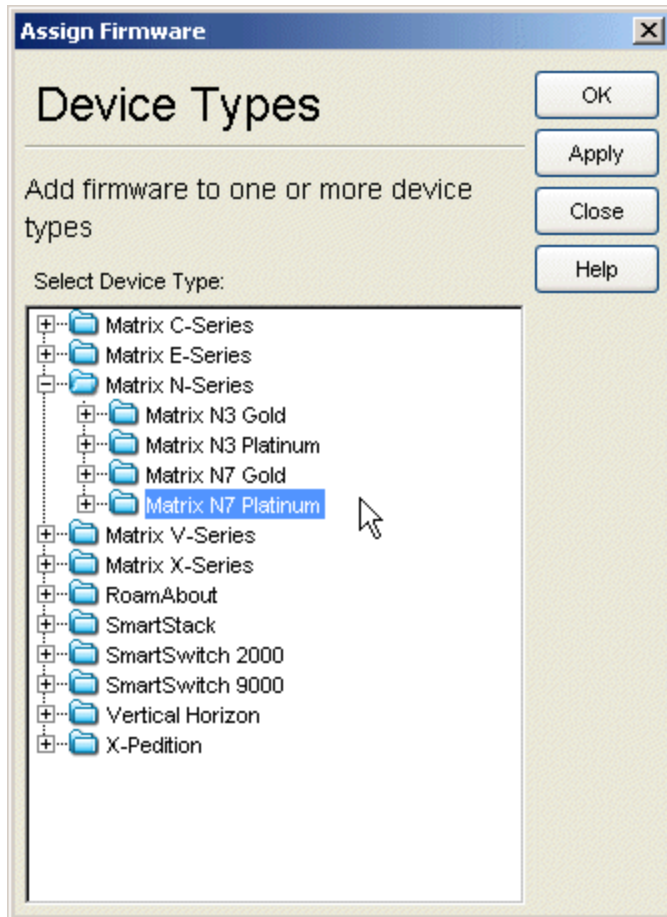
The Firmware Mgmt tab displays firmware and boot PROM images grouped according to product family and device type. Inventory Manager provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a [firmware discovery](#) or refresh. The Unknown folder contains images that Inventory Manager could not correlate to a device type. Use the Assign Firmware window to assign those images to the correct device type(s).

To access this window, select a firmware or boot PROM image in the left-panel Firmware Mgmt tab (or one or more images in the right-panel [Details View tab](#)), then select **Tools > Assign Firmware**. You can also right-click on an image, and select Assign Firmware from the menu.

---

**TIP:** To quickly assign multiple images to a single product family or device type, select the images in a right-panel Details View and drag them into the appropriate left-panel folder.

---



## Device Types


Lists the product families and device types to which you can assign the firmware or boot PROM image. You can select multiple product families or device types using the **Ctrl** or **Shift** keys.

## Related Information

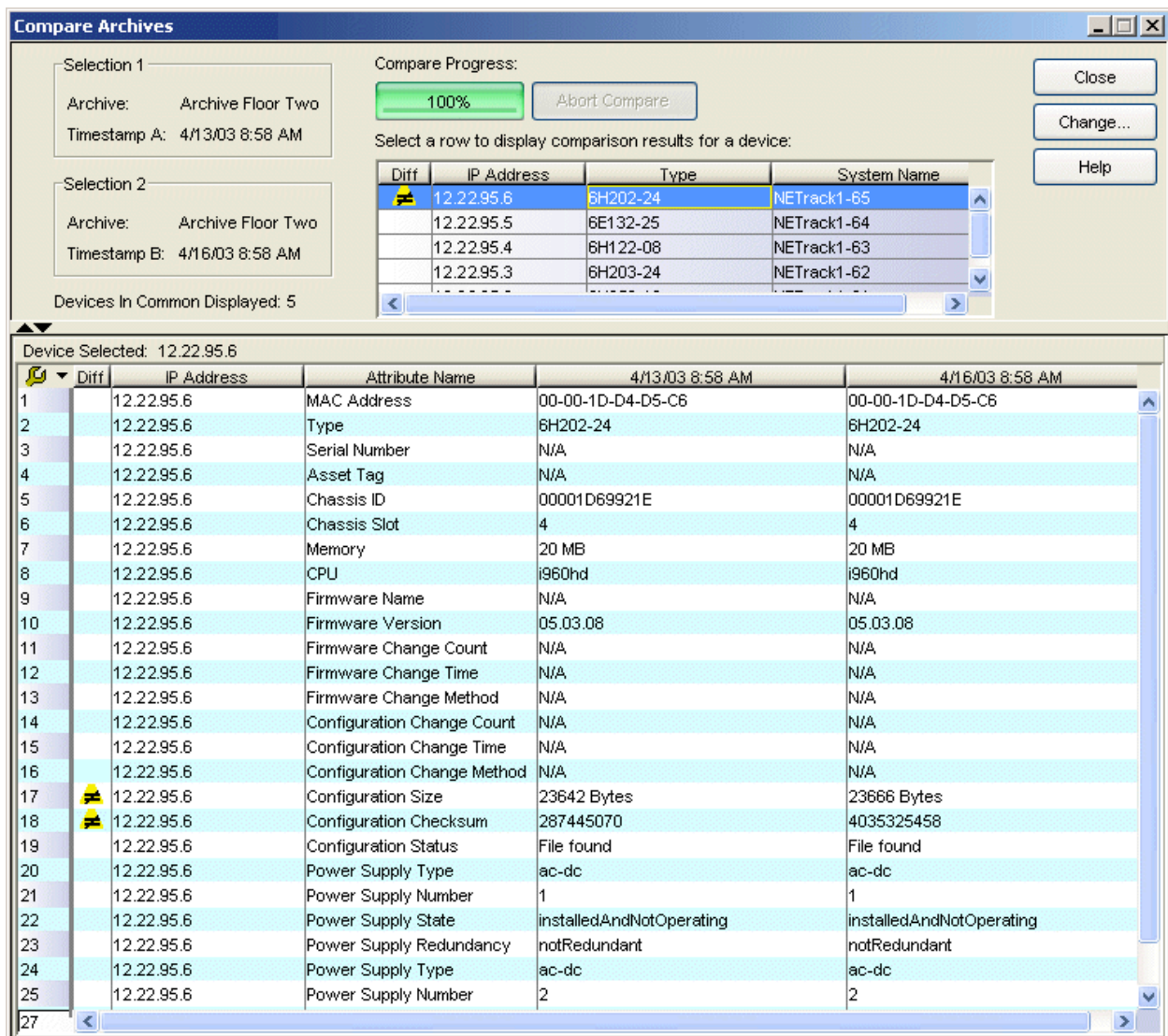
For information on related tasks:

- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)


## Compare Archives Window

The Compare Archives window lets you compare two different archives for the same device and monitor any changes in device attributes. Inventory Manager compares archives using a set group of attributes that were saved when the archive was performed. The values for these attributes are displayed in a table with any differences between the values flagged by a yellow Diff icon .



For information on how to perform a compare archive operation, see [How to Compare Archives](#).



The screenshot shows the 'Compare Archives' window with two selections: 'Archive Floor Two' at timestamp '4/13/03 8:58 AM' and 'Archive Floor Two' at timestamp '4/16/03 8:58 AM'. The comparison progress is 100%. A table displays comparison results for device 12.22.95.6, with a yellow Diff icon in the first column. The table below shows the detailed comparison for this device.

Diff	IP Address	Type	System Name
	12.22.95.6	6H202-24	NETrack1-65
	12.22.95.5	6E132-25	NETrack1-64
	12.22.95.4	6H122-08	NETrack1-63
	12.22.95.3	6H203-24	NETrack1-62

Device Selected: 12.22.95.6				
Diff	IP Address	Attribute Name	4/13/03 8:58 AM	4/16/03 8:58 AM
	12.22.95.6	MAC Address	00-00-1D-D4-D5-C6	00-00-1D-D4-D5-C6
	12.22.95.6	Type	6H202-24	6H202-24
	12.22.95.6	Serial Number	N/A	N/A
	12.22.95.6	Asset Tag	N/A	N/A
	12.22.95.6	Chassis ID	00001D69921E	00001D69921E
	12.22.95.6	Chassis Slot	4	4
	12.22.95.6	Memory	20 MB	20 MB
	12.22.95.6	CPU	i960hd	i960hd
	12.22.95.6	Firmware Name	N/A	N/A
	12.22.95.6	Firmware Version	05.03.08	05.03.08
	12.22.95.6	Firmware Change Count	N/A	N/A
	12.22.95.6	Firmware Change Time	N/A	N/A
	12.22.95.6	Firmware Change Method	N/A	N/A
	12.22.95.6	Configuration Change Count	N/A	N/A
	12.22.95.6	Configuration Change Time	N/A	N/A
	12.22.95.6	Configuration Change Method	N/A	N/A
	12.22.95.6	Configuration Size	23642 Bytes	23666 Bytes
	12.22.95.6	Configuration Checksum	287445070	4035325458
	12.22.95.6	Configuration Status	File found	File found
	12.22.95.6	Power Supply Type	ac-dc	ac-dc
	12.22.95.6	Power Supply Number	1	1
	12.22.95.6	Power Supply State	installedAndNotOperating	installedAndNotOperating
	12.22.95.6	Power Supply Redundancy	notRedundant	notRedundant
	12.22.95.6	Power Supply Type	ac-dc	ac-dc
	12.22.95.6	Power Supply Number	2	2


### Selection 1/Selection 2

Displays the two archive versions you have selected to compare and gives the total number of devices in common between the two versions that were compared. For more information, see [How to Compare Archives](#).


### Compare Progress

The bar shows the progress of large compare operations. The **Abort Compare** button allows you to stop a compare operation; any comparisons that were completed will be available for viewing.

### Summary Table

Displays a list of the devices included in the comparison. If differences were found, the yellow Diff icon  will be displayed. Select the device whose comparison results you wish to see. The results are displayed in the Comparison Results table.

## Comparison Results Table

This section displays the results of the comparison for the device selected in the Summary table, with any differences between the two versions flagged by a yellow Diff icon . For a definition of each attribute, see [Attributes Tab \(Configuration\)](#).

### Diff

A yellow Diff icon  in this column signifies a difference between the two attributes.

### IP Address

Lists the IP address of the device whose attributes are being compared.

### Attribute Name


Lists the name of the attribute being compared. For a definition of each attribute, see [Attributes Tab \(Configuration\)](#).

### Attribute Values

These two columns list the attribute values for the versions being compared.

## Right-Click Menu Options

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by

clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

In addition, the following right-click menu options are available only for archives that include device configuration data:

#### **View Configuration File**

Opens the [Configuration File Viewer](#) and displays the archived config file of the selected device. This option is only available when there are no differences between the two config files being compared.

#### **Compare Configuration Files**

Opens the [Compare Configuration Files window](#) and displays the two archived config files for the selected device. This option is only available when there are differences between the two config files being compared.

#### **Change Button**

Opens the [Select Archive Versions to Compare window](#) where you can select two new archives to compare.

---

### **Related Information**

For information on related tasks:




- [How to Archive](#)
- [How to Compare Archives](#)
- [How to Restore an Archive](#)



## Compare Configuration Files Window

---

The Compare Configuration Files window lets you compare two archived configuration files. There are several ways to access the window:

- Select a configuration that includes device configuration data (  or  ) in the Archives Mgmt tab tree or Details View, and select **Tools > Compare Configuration Files**. You can also right-click on a configuration and select Compare Configuration Files from the menu. The [Select Configurations window](#) opens, where you can select the two configurations you want to compare. Click **OK** and the Compare Configuration Files window opens.
- Select two configurations in the Archive Mgmt tab Details View, and select **Tools > Compare Configuration Files**.
- In the Compare Archives window, right-click on an entry with a Diff icon , and select Compare Configuration Files from the menu.

The files are displayed in ASCII format. However, if one or both of the files are in binary, you have the option to display them. Lines highlighted in green represent lines that have changed. Red highlighting represents lines that have been added.

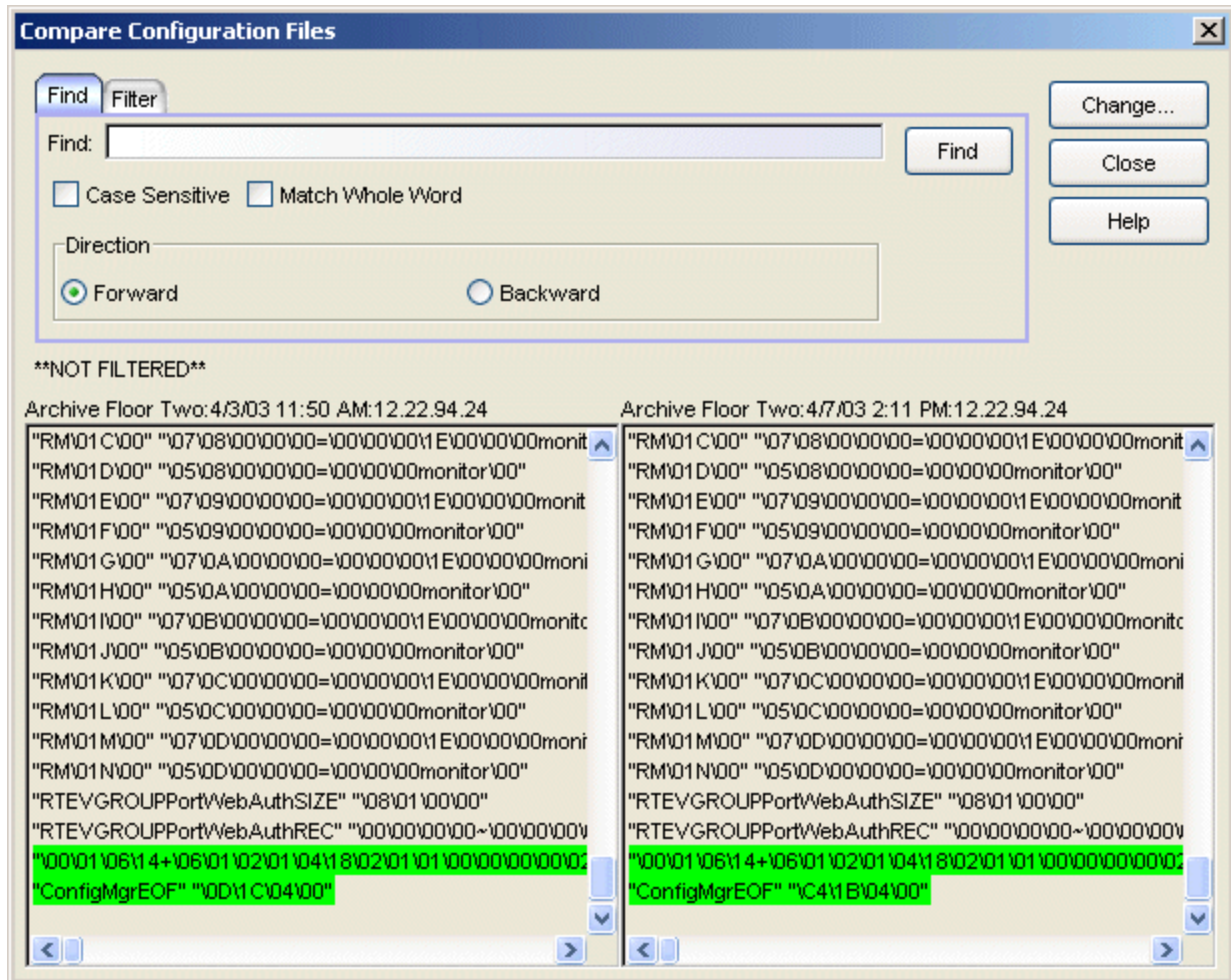
You can perform Find and Filter operations on the configuration files to target specific lines of interest. The last Filter and Find settings you enter remain in the viewer until you refresh the display.

Information on the following tabs:

- [Find Tab](#)
- [Filter Tab](#)

### Find Tab

The Find tab lets you search the configuration files (filtered or unfiltered) for a specific set of characters, like a word, phrase, or number. Enter your search criteria in the Find field, and when you click the **Find** button, any search terms found will be highlighted in the files. You can search forward or backward from your current position, and restrict your search to match the exact upper or lowercase, and/or whole word.

**Find:**

Enter the text or numeric value you want to find.

**Case Sensitive**

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Find** field.

**Match Whole Word**

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Find** field.

**Forward**

Select **Forward** to search from your current position to the end of the configuration file.

**Backward**

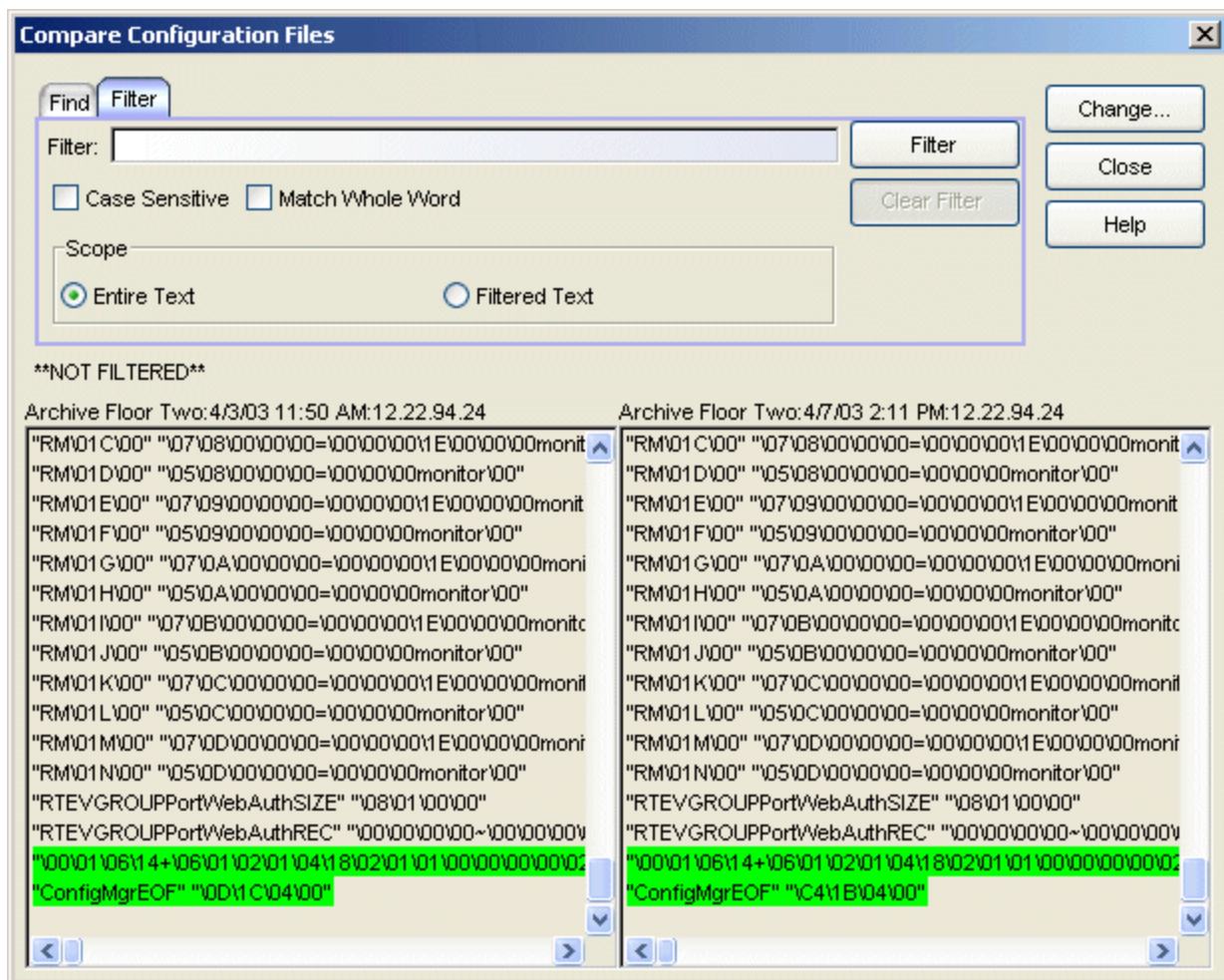
Select **Backward** to search from your current position to the beginning of the configuration file.

## Configuration Files

Displays the selected configuration files. Directly above the display you can see the status of whether the files are filtered or not filtered. Any search terms found are highlighted.

## Filter Tab

The Filter tab lets you specify which lines to display in the configuration files. Enter the information you want to see, and only matching lines will be displayed. You can use any combination of filter options, and you can perform consecutive filters on the filtered events.



### Filter:

Enter the text or numeric value you want to use as a filter.

### Case Sensitive

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Filter** field.

### Match Whole Word

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Filter** field.

### Entire Text

Select the **Entire Text** option to filter the entire text by the value in the **Filter** field. If you have already performed a filter, this will enable you to perform a new filter on the entire files instead of just the filtered text.

### Filtered Text

Select the **Filtered Text** option to perform a new filter on the results of the previous filter.

### Configuration Files

Displays the selected configuration files. After running the filter, this area displays the matching lines in the configuration files. Click **Clear Filter** to remove the filter currently in effect. Directly above the display you can see the status of whether the files are filtered or not filtered.

### Find Button

Performs the Find operation on the configuration files currently displayed in the window.

### Filter Button

Performs the filter and displays the results.

### Clear Filter Button

Removes the filter currently in effect.

### Change Button

Opens the [Select Configurations window](#) where you can select two new configuration files to compare.

---

## Related Information

For information on related windows:



- [Configuration File Viewer](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

## Configuration File Viewer

---

The Configuration File Viewer lets you view an archived device configuration file. To access the viewer, select a configuration that includes device configuration data (  or  ) in the Archives Mgmt tab tree or right-panel Details View, and select **Tools > View Configuration File**. You can also right-click on a configuration and select View Configuration File from the menu. If the configuration file status is "File Not Found/Missing" (see the configuration General tab), then this menu option is not available. The file is displayed in ASCII format. However, if the file is in binary, you still have the option to view it.

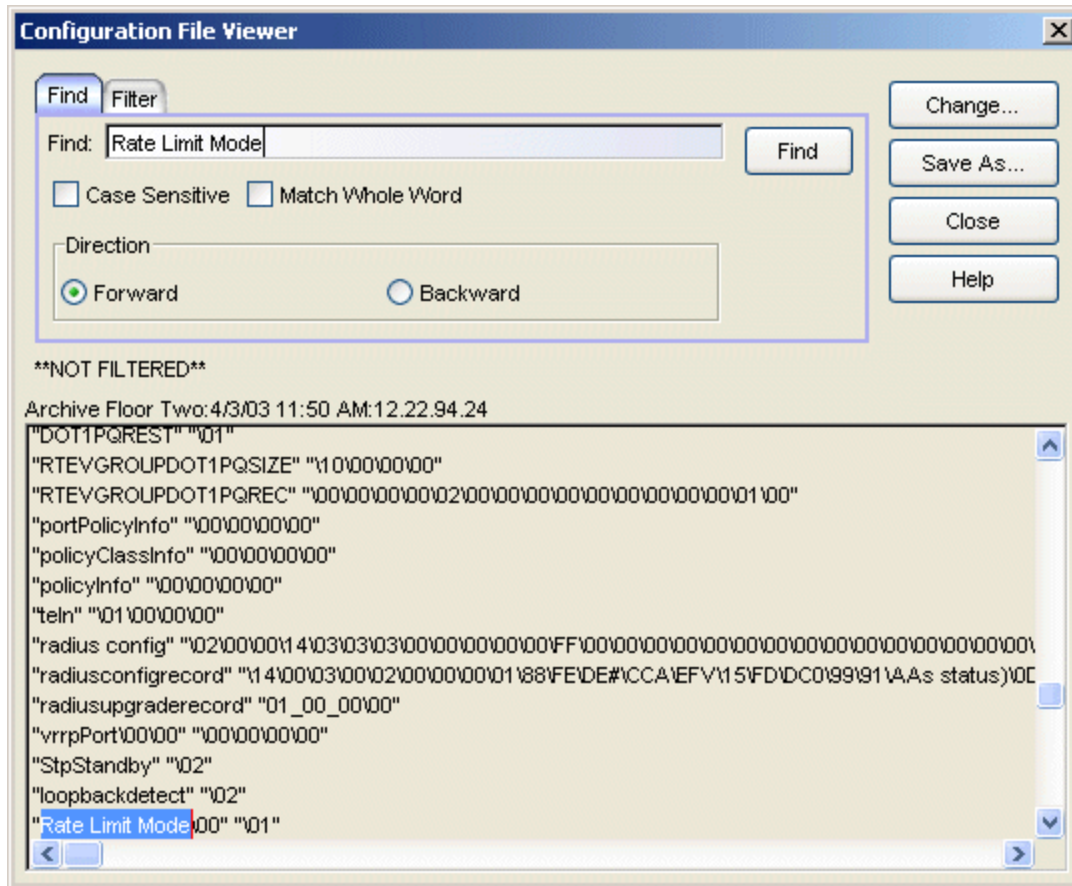
You can perform Find and Filter operations on the configuration file to target specific lines of interest. The last Filter and Find settings you enter remain in the viewer until you refresh the display.

Information on the following tabs:

- [Find Tab](#)
- [Filter Tab](#)

### Find Tab

The Find tab lets you search the configuration file (filtered or unfiltered) for a specific set of characters, like a word, phrase, or number. Enter your search criteria in the Find field, and when you click the **Find** button, any search terms found will be highlighted in the viewer. You can search forward or backward from your current position, and restrict your search to match the exact upper or lowercase, and/or whole word.

**Find:**

Enter the text or numeric value you want to find.

**Case Sensitive**

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Find** field.

**Match Whole Word**

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Find** field.

**Forward**

Select **Forward** to search from your current position to the end of the configuration file.

**Backward**

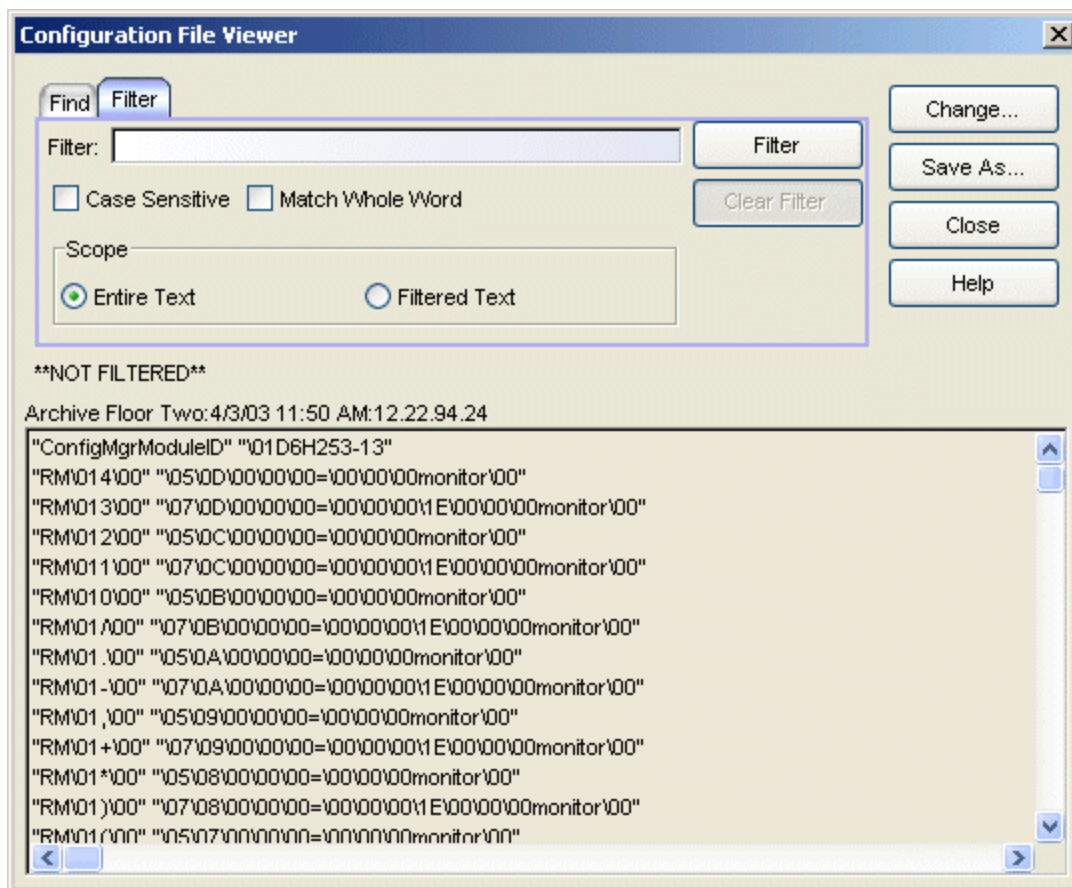
Select **Backward** to search from your current position to the beginning of the configuration file.

## Configuration File

Displays the selected configuration file and highlights any search items that were found. Directly above the display you can see the status of whether the file is filtered or not filtered.

## Filter Tab

The Filter tab lets you specify which lines to display in the configuration file. Enter the information you want to see, and only matching lines will be displayed. You can use any combination of filter options, and you can perform consecutive filters on the filtered events.



### Filter:

Enter the text or numeric value you want to use as a filter.

### Case Sensitive

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Filter** field.



### Match Whole Word

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Filter** field.

### Entire Text

Select the **Entire Text** option to filter the entire file by the value in the **Filter** field. If you have already performed a filter, this will enable you to perform a new filter on the entire file instead of just the filtered text.

### Filtered Text

Select the **Filtered Text** option to perform a new filter on the results of the previous filter.

### Configuration File

After running the filter, this area displays the matching lines in the configuration file. Click **Clear Filter** to remove the filter currently in effect. Directly above the display you can see the status of whether the file is filtered or not filtered.

### Find Button

Performs the Find operation on the information currently displayed in the viewer.

### Filter Button

Performs the filter and displays the results.

### Clear Filter Button

Removes the filter currently in effect.

### Change Button

Opens the [Open Configuration window](#) where you can select another configuration file to view.

### Save As Button

Lets you save the configuration file as a text file.

---

## Related Information

For information on related windows:

- [Compare Configuration Files Window](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

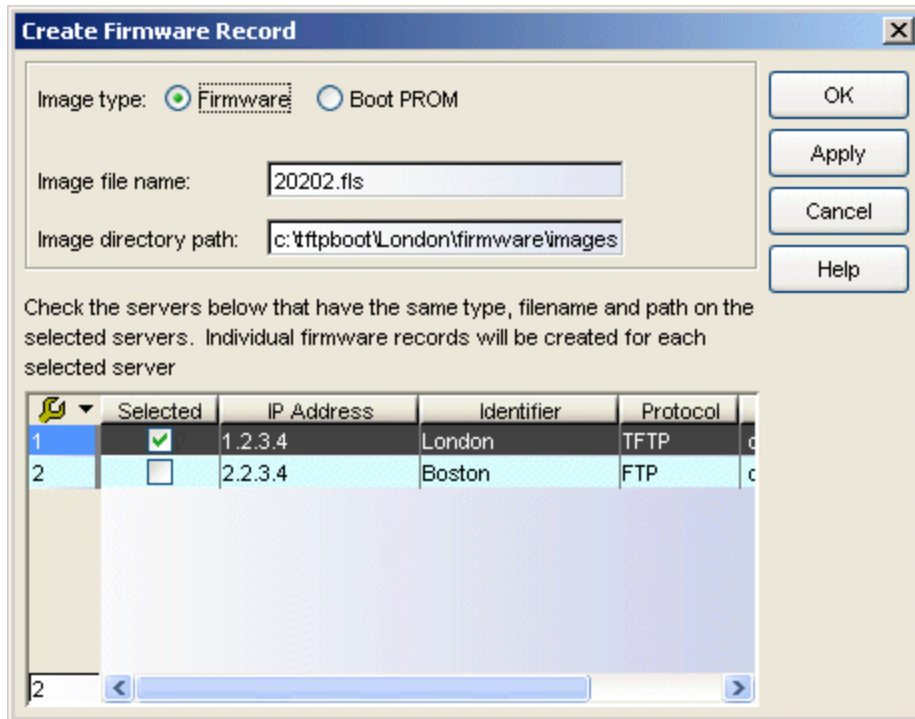
## Create Firmware Record Window

---

This window lets you add a firmware or boot PROM image to your Firmware Mgmt tab manually, as opposed to having Inventory Manager automatically discover the image during a [firmware discovery](#). When you are using an [alternate firmware server](#) to perform remote firmware downloads, you must use this window to manually create the firmware records associated with the alternate server, and add them to the Inventory Manager database.

When you create a firmware record, it is added to the All Firmware folder and the Unknown folder in the Firmware Mgmt tab. You will need to use the [Assign Firmware window](#) to assign the firmware or boot PROM image to the appropriate product families or device types. You must also assign the alternate firmware server to the appropriate devices using the [Set Firmware Server window](#) in order to see this image listed in the Firmware Upgrade Wizard. This enables you to download the image to your remote network devices of that family or type, using the [Firmware Upgrade Wizard](#) or the [Boot PROM Upgrade Wizard](#).

To access this window, select the All Firmware folder in the left-panel Firmware Mgmt tab and select **Tools > Create Firmware Record**, or right-click the All Firmware folder and select Create Firmware Record from the menu. (You must have a configured alternate firmware server for this menu option to be available.)



### Image Type

Specify whether the image is a firmware or boot PROM image.

### Image File Name

Enter the name of the firmware or boot PROM image as it appears in the image directory.

### Image Directory Path

Enter the path to the location where the image is stored.

### Selected Servers Table

This table lists any alternate firmware download servers you have defined in the [Alternate Firmware Servers view](#) in the Options window. Select the appropriate server for the firmware record: the image directory path must exist under the server root path. If you select multiple servers, be sure that the same image type, file name, and directory path are used on all selected servers. Individual firmware records will be created for each selected server.

### Apply

Creates the firmware record and leaves the window open.

---

## Related Information

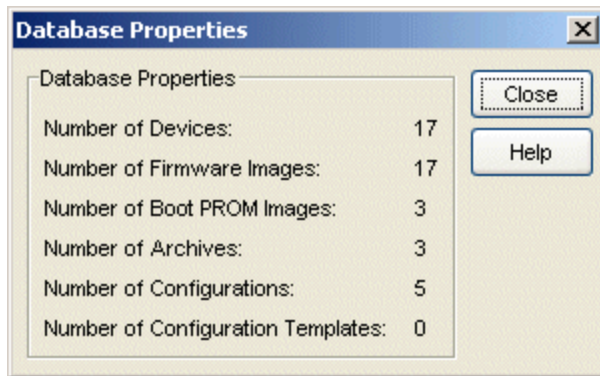
For information on related windows:

- [Alternate Firmware Servers View, Options Window](#)
- [Set Firmware Server Window](#)

## Database Properties Window

---

This window displays information about certain Inventory Manager components stored in the NetSight database. To access this window, select **File > Database > Properties**.



### Number of Devices

The number of devices in the database.

### Number of Firmware Images

The number of firmware images in the database. This number includes user-defined firmware records but does not include images with a status of File Not Found.

### Number of Boot PROM Images

The number of boot PROM images in the database. This number includes user-defined firmware records but does not include images with a status of File Not Found.

### Number of Archives

The number of archives stored in the database.

### Number of Configurations

The total number of configurations saved in the database.

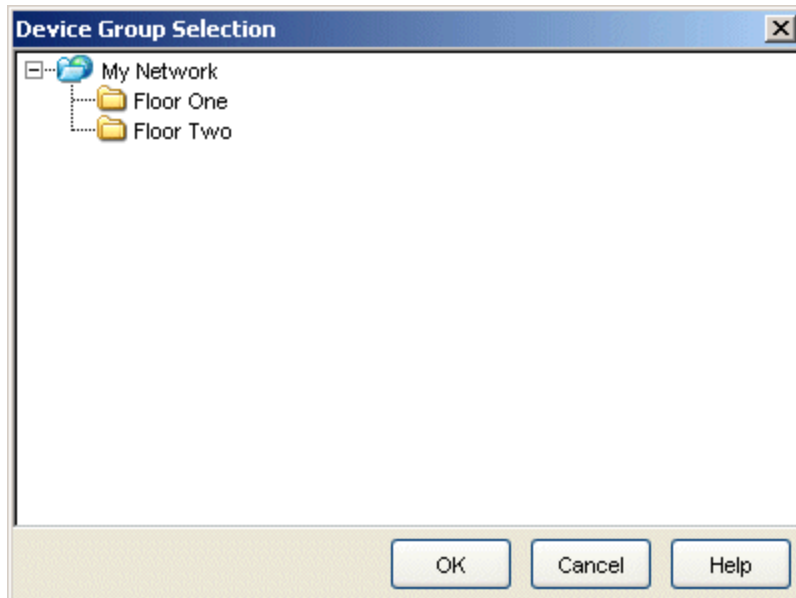
### Number of Configuration Templates

The total number of configuration templates saved in the database.

## Device Group Selection Window

---

The Device Group Selection window lets you add one or more devices from a right-panel Details View to the My Network Group or a user-created group in the left-panel Network Element tab. See [Adding Devices to a Device Group](#) for more information.



### Group Selection Panel

Use this panel to select the group to which you want to add the selected devices.

---


### Related Information

For information on related tasks:

- [How to Add and Remove Device Groups](#)

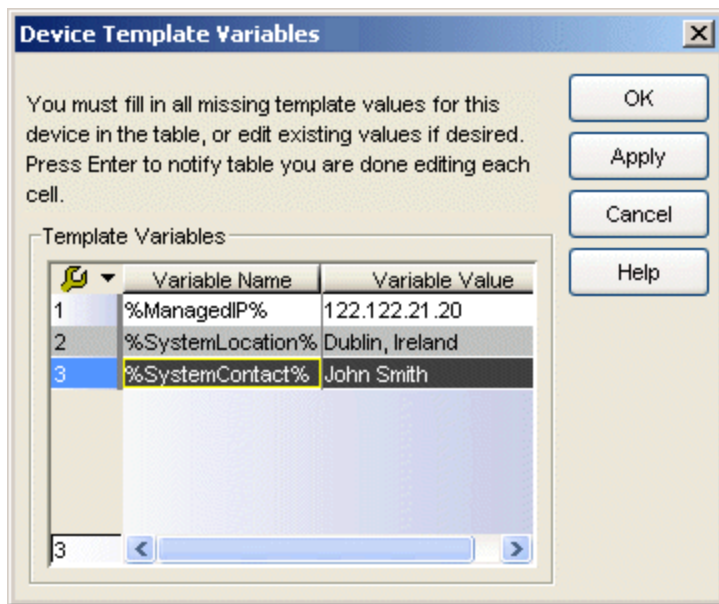
## Device Template Variables Window

---

This window allows you to set template variable values for a single device. It is accessed from the last window of the [Template Download Wizard](#), which displays a table of the devices you have selected for your download operation. An alert icon  appears for any device that does not have values assigned for all the variables in the template. Right-click that device and select Edit Device Variables to open the Device Template Variables window, where you can assign variables values for that specific device.

**TIP:** You can also set variable values for an individual device on the device's [Configuration Templates tab](#).

---



### Template Variables

This table lists all the template variables and their set values for your selected device. You must fill in all missing values, or modify existing values, if desired. Press **Enter** when you have finished entering the value in each cell. When you have filled in all the template values, click **OK** to return to the Template Download Wizard.

---

### Related Information

For information on related tabs:



- [Configuration Templates Tab \(Device\)](#)

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Edit Configuration Template Window](#)
- [Set Template Variable Window](#)

## Edit Alternate Firmware Server Window

Use the Edit Alternate Firmware Server window to change certain properties and/or connection information for alternate firmware download servers. Access this window by selecting a server and clicking **Edit Server** in the [Alternate Firmware Servers view](#) of the Options window.

The screenshot shows the 'Edit Alternate Firmware Server' dialog box. The 'Server Properties' section includes fields for Server IP (1.2.3.6), Identifier (Canada), Server Root Path (c:\tftpboot), and Transfer Protocol (TFTP). The 'Connection Information' section shows a Port field (69). A foreground window displays a Port field (21), an unchecked 'Anonymous' checkbox, a Username field (anonymous), a Password field (\*\*\*\*), and a checked 'Hide password' checkbox.

### Server Properties

Use this area to edit two of the alternate server's properties: the identifier and the server root path.

#### Server IP

The IP address of the workstation where the TFTP, FTP, or SCP server is running. You cannot edit this property. To change the server IP, you must remove this alternate server from the list, and add a new one using the [Add Alternate Firmware Server window](#).

### Identifier

Edit the description that helps you identify the alternate firmware server.

### Server Root Path

Edit the server root path. The root directory is the base directory to which the server is allowed access. The server will be allowed to create files to or read files from this directory and any of its subdirectories.

---

**NOTES:** Changing the root directory requires restarting the server. Also, keep in mind the following requirements when setting the server root path:

- If your server is configured with a root directory, it must match the root directory entered here.
  - If your server is **not** configured with a root directory, specify the root directory here as the root of the drive (e.g. C:\ or D:\).
- 

### Transfer Protocol

The transfer protocol for the alternate firmware server. You cannot edit this property. To change the transfer protocol, you must remove this alternate server from the list, and add a new one using the [Add Alternate Firmware Server window](#).

## TFTP Connection Information

This area displays connection information for an alternate server that has been configured with TFTP protocol.

### Port

The port number your TFTP server is configured to run on. You cannot edit this property. To change the port number, you must remove this alternate server from the list, and add a new one using the [Add Alternate Firmware Server window](#).

## FTP/SCP Connection Information

This area displays connection information for an alternate server that has been configured with FTP or SCP protocol.

### Port

The port number your FTP/SCP server is configured to run on. You cannot edit this property. To change the port number, you must remove this

alternate server from the list, and add a new one using the [Add Alternate Firmware Server window](#).

#### **Anonymous**

Select or deselect this checkbox depending on whether your FTP/SCP server is configured to accept Anonymous logins.

#### **Username/Password**

Edit the username and password used to access the FTP/SCP server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.

---

#### **Related Information**



For information on related windows:

- [Alternate Firmware Servers View, Options Window](#)

## Edit Configuration Template Window

---

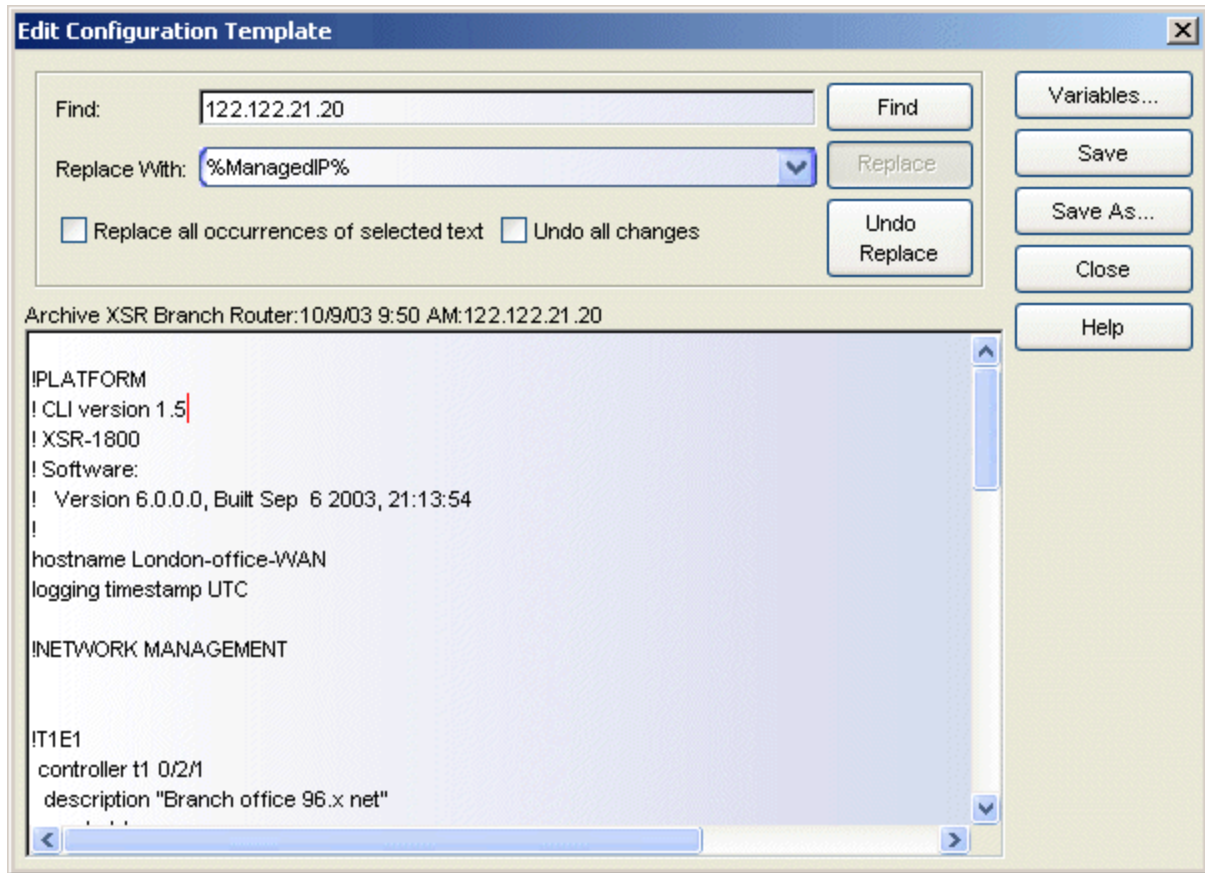
Use the Edit Configuration Template window to create a configuration template based on an archived device configuration file. Creating a configuration template lets you easily download similar configurations to one or more devices. The window displays a selected configuration file, and allows you to replace portions of it with template variables. Then, when you download the template configuration to a device (using the [Template Download Wizard](#)), the variables are automatically replaced with assigned values for that device. For more information, see [How to Create and Download Configuration Templates](#).

To access the window, select a configuration that includes device configuration data (  or  ) in the left-panel Archive Mgmt tab and select **Tools > Create Configuration Template**. You can also right-click a configuration and select Create Configuration Template from the menu. When the window opens, the configuration file is displayed. You can edit the displayed text directly, or use the Find and Replace buttons to edit the file with the desired variables. All instances of the IP address of the device the configuration was saved from, will be automatically replaced with the %ManagedIP% variable. You can use the Undo Replace button to undo this auto replacement if desired.

---

**NOTE:** Configuration templates can be created from text-based (ASCII format) configurations files. Although you can open binary configuration files in the Edit Configuration Template window, you should **not** use binary configuration files to create templates.

---



### Find

Enter the text you would like to edit. When you click **Find**, the first occurrence of the text will be highlighted, and you can select to replace that single occurrence or replace all occurrences of the selected text. Click **Find** again to highlight the next occurrence.

### Replace With

Enter the variable you want to use to replace the highlighted (found) text, or use the drop-down list to select a defined variable. Variables are defined in the [Template Variables window](#), accessed from the **Variables** button.

### Replace all occurrences of selected text

Select this checkbox when you would like to replace all occurrences of the selected text versus replacing one occurrence at a time.

### Undo all changes

Select this checkbox when you would like to undo all replacements since the last template Save or Save As.

### Find Button

Searches for the next occurrence of the text specified in the Find field. The found text is highlighted in the window.

### Replace Button

Replaces highlighted (found) text with the specified variable. If the "Replace all occurrences of selected text" checkbox is selected, all instances of the text specified in the Find field will be replaced.

### Undo Replace Button

Reverses the last replacement. Use the "Undo all Changes" checkbox to reverse all replacements since the last template Save or Save As.

### Variables Button

Opens the [Template Variables window](#) where you can add and delete variables to display in the variable drop-down list.

### Save Button

Updates the template with your changes.

### Save As Button

Opens the Save Template window, allowing you to name and save the configuration template. Saved templates are listed under the All Templates folder in the left-panel Configuration Templates tab. Once a template has been saved, the name of the template appears in the title bar of this window, and the path to where the saved template is stored is displayed above the configuration template text.

---

## Related Information

For information on related tasks:

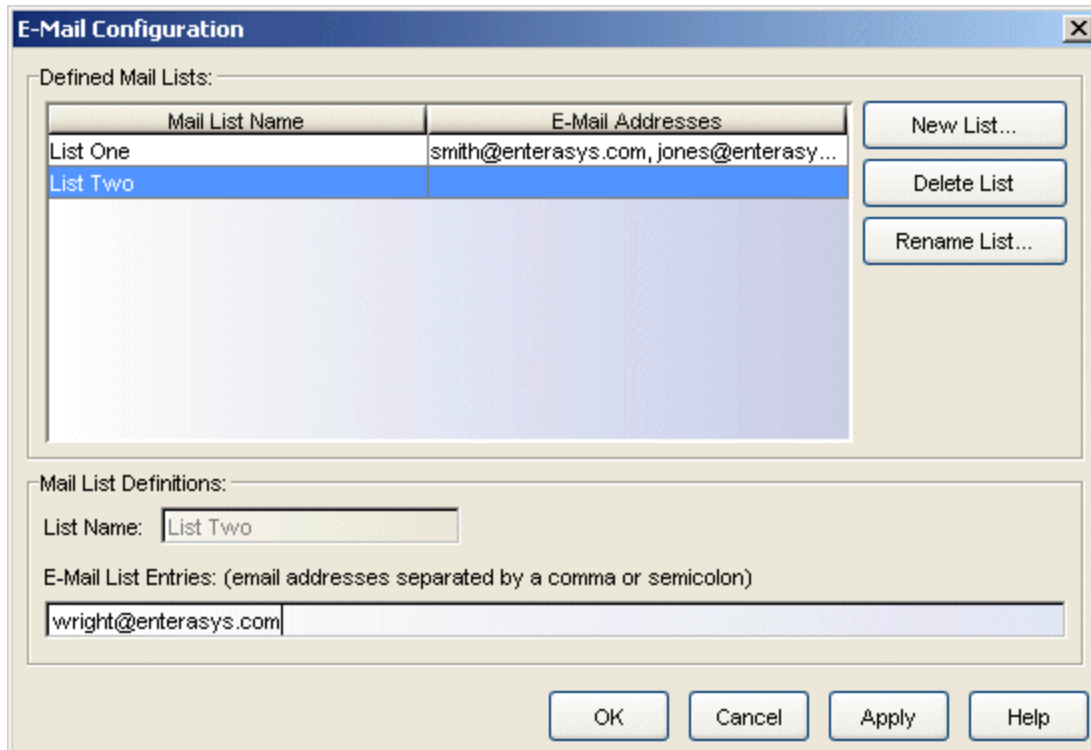
- [How to Create and Download Configuration Templates](#)

For information on related windows:

- [Template Variables Window](#)
- [Assign Configuration Template Window](#)
- [Set Template Variables Window](#)

## E-Mail Configuration Window

The E-Mail Configuration window lets you create an e-mail recipient list to use when configuring e-mail notification settings for a scheduled Capacity Planning report. The window is accessed from the Edit Mail List button in the [Schedule Report window](#).



### Defined Mail Lists

Displays the currently defined mail lists. Use the **New List** button to add a mail list name to the list.

### Mail List Definitions

Use the E-Mail List Entries field to configure the "send to" e-mail addresses for the selected list. Addresses in the list can be separated with a comma or a semicolon. The list is not verified for valid addresses.

### New List Button

Lets you create a new mail list name.

### Delete List Button

Deletes the selected list.



### Rename List Button

Lets you rename the selected list.

---

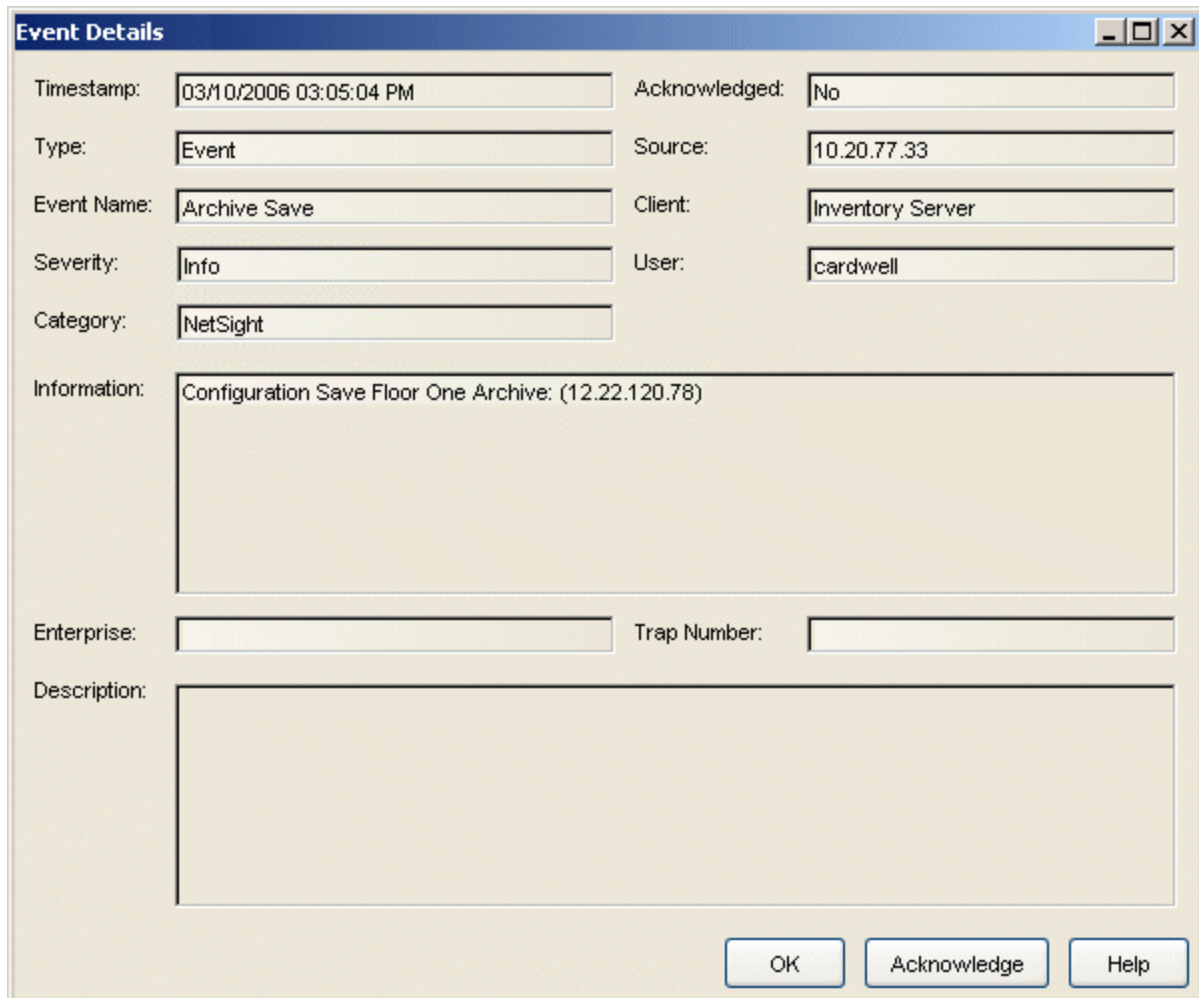
### Related Information

For information on related windows:

- [Capacity Planning](#)
- [Schedule Report Window](#)

## Event Details Window

The Event Details window shows information about a single event selected in the Event Log. To access the window, right-click an event in the Event Log and select **Event Details** from the menu.



The screenshot shows a window titled "Event Details" with a blue header bar and standard window controls (minimize, maximize, close). The window contains several text input fields and a large text area. The fields are arranged in two columns. The left column contains: Timestamp (03/10/2006 03:05:04 PM), Type (Event), Event Name (Archive Save), Severity (Info), Category (NetSight), Enterprise (empty), and Description (empty). The right column contains: Acknowledged (No), Source (10.20.77.33), Client (Inventory Server), and User (cardwell). Below the Enterprise and Description fields are three buttons: OK, Acknowledge, and Help.

Timestamp:	03/10/2006 03:05:04 PM	Acknowledged:	No
Type:	Event	Source:	10.20.77.33
Event Name:	Archive Save	Client:	Inventory Server
Severity:	Info	User:	cardwell
Category:	NetSight		
Information:	Configuration Save Floor One Archive: (12.22.120.78)		
Enterprise:		Trap Number:	
Description:			

Buttons: OK, Acknowledge, Help

### Timestamp

The date and time when the event occurred.

### Acknowledged

Whether or not the selected event has been acknowledged.

### Type

The type of information: Event.

**Source**

The IP address of the host that was the source of the event.

**Event Name**

The type of event.

**Client**

The name of the client host machine that triggered the event.

**Severity**

The event's severity.

**Category**

The category of event.

**User**

The name of the user that triggered the event.

**Information**

Information about the event.

**Enterprise**

Not applicable to the Inventory Manager Event Log.

**Trap Number**

Not applicable to the Inventory Manager Event Log.

**Description**

Not applicable to the Inventory Manager Event Log.

**Acknowledge/Unacknowledge Button**

Places a check or removes a check in the Acknowledge column in the Event Log for the selected event.

---

**Related Information**

For information on related windows:

- [Active Status Panel](#)
- [Event Log](#)

## File Transfer Method Window

---

Use this window to select a file transfer method for a specific device, or specify a default transfer method for an entire device type family. Once you have specified the file transfer method for a device, all archive save and restore operations and Firmware/Boot PROM upgrades on that device will be performed using the specified method. All devices are initially configured with TFTP as their file transfer method, until specified otherwise using these windows. Be sure to configure file transfer properties in the [TFTP Transfer Settings](#) or [FTP Transfer Settings](#) views in the Options window.

There are two File Transfer Method windows, depending on whether you are setting the method at the device level, or for an entire device type family.

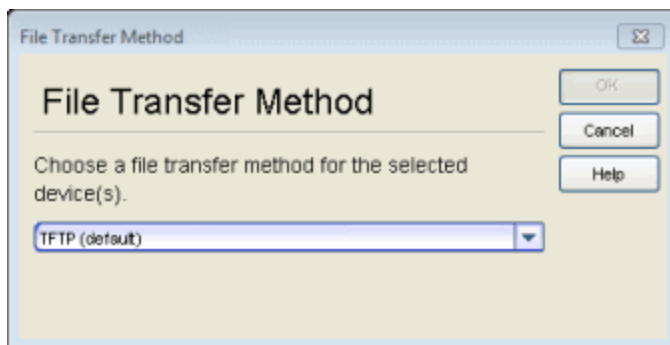
Information on:

- [File Transfer Method - Device](#)
- [File Transfer Method - Device Type Family](#)

### File Transfer Method - Device

Use this window to specify the file transfer method for a single or multiple devices. Specifying a file transfer method at the device level will override any default setting made at the [device family](#) level.

To access this window, select a single device in the left-panel Network Elements tab or multiple devices in a right-panel Details View tab, then select **Tools > File Transfer Method** from the menu bar. You can also right-click a device and select the File Transfer Method option from the menu.

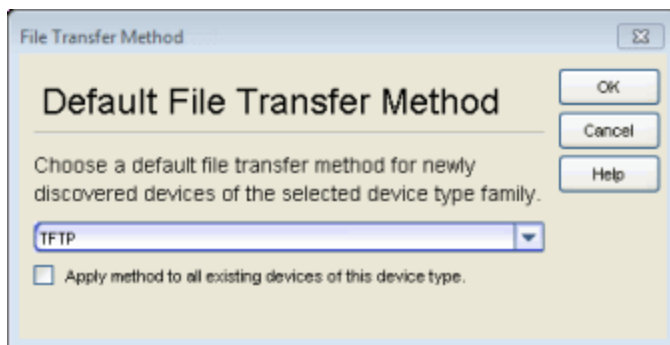


Use the drop-down list to select the file transfer method you would like used for the selected device(s). The default file transfer method set for the device's device type is indicated by the word default in parentheses, as shown in the graphic above.

## File Transfer Method - Device Type Family

Use this window to specify a default file transfer method for newly discovered devices of an entire device type or device type family. You can override this device family setting at the [device level](#).

To access this window, select a device family folder (highest-level device type folder) or a device type folder in the left-panel Firmware Management tab, then select **Tools > Default File Transfer Method** from the menu bar. You can also right-click a device type or family and select the Default File Transfer Method option from the menu.



Use the drop-down list to select the file transfer method you would like used for the selected device type or family.

Select the checkbox to change the file transfer method for all current devices in the selected device type or family folder. If this checkbox is **not** selected, only newly discovered devices of this device type or family will have this file transfer method.

---

### Related Information

For information on related tasks:

- [How to Set a File Transfer Method](#)

For information on related windows:

- [General Tab \(Device Type\)](#)
- [FTP Transfer Settings View, Options Window](#)
- [TFTP Transfer Settings View, Options Window](#)

## Inventory Manager Options Window

---

These options apply only to the NetSight Inventory Manager application. In the Options window (**Tools > Options**), the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Inventory Manager folder to view all the different options you can set.

Information on the following Inventory Manager options:

- [Alternate Firmware Servers](#)
- [Data Storage Directory Path](#)
- [File Transfer Settings](#)
  - [FTP Transfer Settings](#)
  - [TFTP Transfer Settings](#)
  - [SCP Transfer Settings](#)

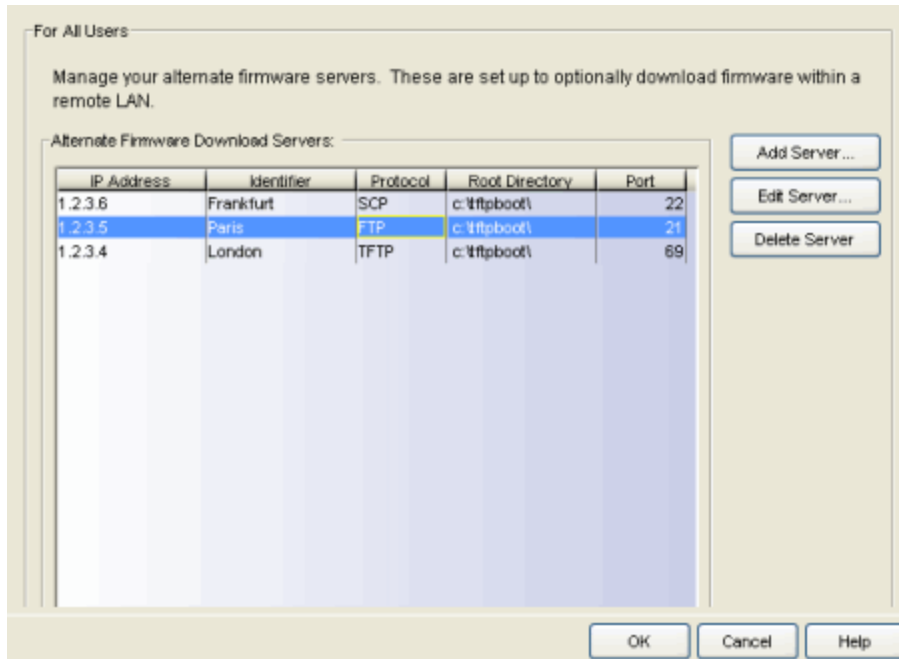
### Alternate Firmware Servers

Selecting Alternate Firmware Servers in the left panel of the Options window provides the following view where you can configure alternate firmware download servers. Alternate servers allow you to perform remote firmware downloads without having to reconfigure the default NetSight TFTP server settings. By performing firmware downloads via a remote server, you can avoid transferring traffic over a WAN. Alternate servers can be configured to use either the TFTP, FTP, or SCP transfer protocols. These settings apply to all users.

---

**NOTE:** After you have configured your alternate servers, use the [Create Firmware Record window](#) to create new firmware entries and associate them with the alternate servers. Then, use the [Set Firmware Server window](#) to specify an alternate firmware download server to be used by a device group or by individual devices.

---



### Alternate Firmware Download Servers

Lists the configured alternate servers. Use the **Add Server** button to add a server to the list.

### Add Server

Opens the [Add Alternate Firmware Server window](#) where you can configure an alternate firmware download server.

### Edit Server

Opens the [Edit Alternate Firmware Server window](#) where you can edit certain alternate server properties.

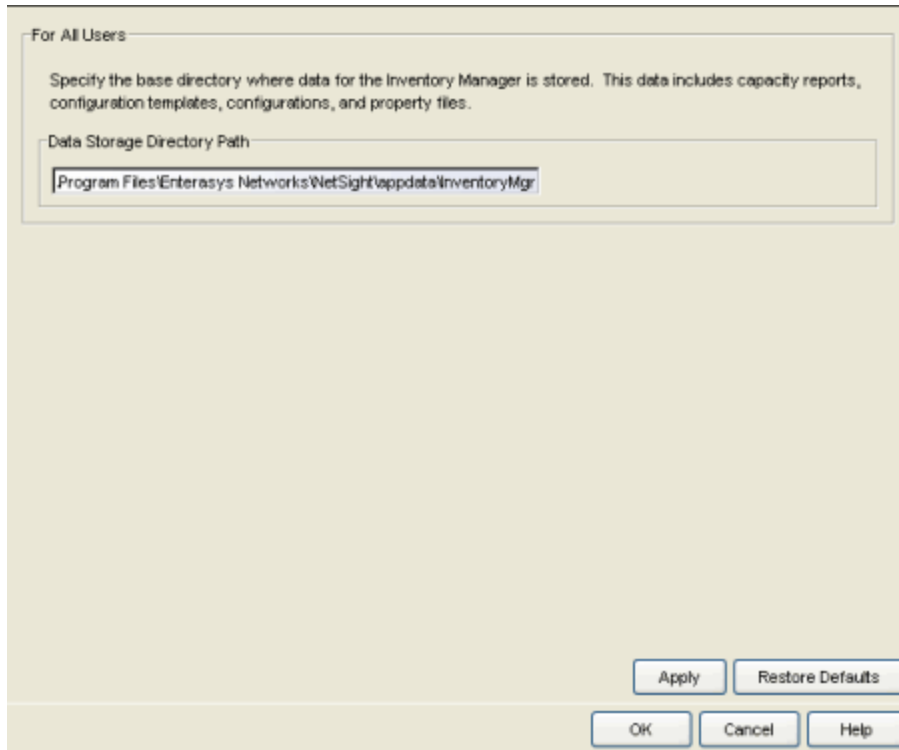
### Delete Server

Deletes the selected alternate server from the list.

## Data Storage Directory Path

This option allows you to specify a different base directory where Inventory Manager data will be stored. This data includes capacity planning reports, configuration templates, archived configurations, and property files. If you specify a new data directory, you will need to move the data files stored under the old directory to the new directory so that Inventory Manager can find them.





## File Transfer Settings

These options specify the FTP, TFTP, or SCP file transfer settings to be used when using the Upgrade and Archive Wizards.

Information on the following File Transfer Settings options:

- [FTP Transfer Settings](#)
- [TFTP Transfer Settings](#)
- [SCP Transfer Settings](#)

### *FTP Transfer Settings*

Selecting FTP Transfer Settings in the left panel of the Options window provides the following view where you can set FTP server properties and login information. Use this view to specify the FTP server IP address, set paths to the root and firmware directories, and set login information. The FTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.

The screenshot shows a dialog box titled "For All Users" with two main sections: "FTP Server Properties" and "Login Information".

**FTP Server Properties:**

- Use the NetSight Server's IP
- FTP Server IP:
- Port:
- Root Directory Path:
- Firmware Directory Path (must contain root path):

**Login Information:**

- Anonymous
- Username:
- Password:
- Hide password

Buttons at the bottom: Apply, Restore Defaults, OK, Cancel, Help.

## FTP Server Properties

### Use the NetSight Server's IP

Select this checkbox if your FTP server is on the same machine as the NetSight Server.

### FTP Server IP

First deselect the "Use the NetSight Server's IP" checkbox, then enter the IP address of the device where the FTP server resides.

### Port

Specify the port number your FTP server is configured to run on.

### Root Directory Path

The root directory is the base directory to which the FTP server is allowed access. The FTP server will be allowed to create files to or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory that Inventory Manager automatically creates when it is installed. If you would like to use an alternate root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your FTP server is configured with an FTP root directory, it must match the root directory entered here.
- If your FTP server is **not** configured with an FTP root directory, change the FTP root directory here to the root of the drive (e.g. C:\ or D:\).
- **If you are using an FTP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

h:\ (where h:\ is mapped to the tftpboot directory on the remote drive)

use

\\yourservername\tftpboot\

---

### Firmware Directory Path

The default firmware directory is tftpboot\firmware\images. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an FTP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.

### Login Information

#### Anonymous

Select this checkbox if your FTP server is configured to accept Anonymous logins. Inventory Manager will automatically fill in the username and password fields.

#### Username/Password

Enter your username and password to access the FTP server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.

### *TFTP Transfer Settings*

Selecting TFTP Transfer Settings in the left panel of the Options window provides the following view where you can set TFTP server properties. This view

displays the TFTP server IP address and root directory path specified in the Services for NetSight Server Suite-Wide Options view and lets you set the firmware directory path. These settings apply to all users.

The screenshot shows a dialog box titled "For All Users" with the following content:

- Settings specified from the "Services for NetSight Server" options:
  - TFTP Server IP: 134.141.90.168
  - Root Directory Path: C:\tftpboot
- TFTP Server Properties:
  - Firmware Directory Path (must contain root path): C:\tftpboot\firmware\images\

Buttons at the bottom: Apply, Restore Defaults, OK, Cancel, Help.

### Settings specified...

These are the TFTP settings specified in the Services for NetSight Server Suite-Wide Options view.

### Firmware Directory Path

The default firmware directory is tftpboot\firmware\images. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).)

---

**NOTE: If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the firmware directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

h:\ (where h:\ is mapped to the firmware directory on the remote drive)  
use

\\yourservername\tftpboot\firmware\images\  

---

## SCP Transfer Settings

Selecting SCP Transfer Settings in the left panel of the Options window provides the following view where you can set SCP server properties and login information. Use this view to specify the SCP server IP address, set paths to the root and firmware directories, and set login information. The SCP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.

The screenshot shows a dialog box titled "For All Users" with the following sections:

- SCP Server Properties:**
  - Use the NetSight Server's IP    SCP Server IP:     Port:
  - Root Directory Path:
  - Firmware Directory Path (must contain root path):
- Login Information:**
  - Anonymous
  - Username:
  - Password:      Hide password

Buttons at the bottom: Apply, Restore Defaults, OK, Cancel, Help.

### SCP Server Properties

#### Use the NetSight Server's IP

Select this checkbox if your SCP server is on the same machine as the NetSight Server.

#### SCP Server IP

First deselect the "Use the NetSight Server's IP" checkbox, then enter the IP address of the device where the SCP server resides.

#### Port

Specify the port number your SCP server is configured to run on.

## Root Directory Path

The root directory is the base directory to which the SCP server is allowed access. The SCP server will be allowed to create files to or read files from this directory and any of its subdirectories. The default root directory on Windows is the C:\ directory and on Linux it is the /root/ directory. If you would like to use an alternate root directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory.

---

**NOTE:** Keep in mind the following requirements when setting the path to your root directory:

- If your SCP server is configured with an SCP root directory, it must match the root directory entered here.
- If your SCP server is **not** configured with an SCP root directory, change the SCP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
- **If you are using an SCP server on a remote system**, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using  
h:\ (where h:\ is mapped to the firmware\images directory on the remote drive)  
use

\\yoursystemname\firmware\images

---

## Firmware Directory Path

The default firmware directory is C:\firmware\images on Windows and /root/firmware/images on Linux. If you would like to use an alternate firmware directory, enter a path to that directory in this field, or use the **Browse** button to navigate to the directory. The firmware directory must be a subdirectory of the root directory. (The firmware images stored in the firmware directory are added to the left-panel Firmware Mgmt tree when you perform a [firmware discovery](#).) If you are using an SCP server on a remote system, be sure to use the UNC standard described in the [Note](#) above when specifying the path.

## Login Information

### Anonymous

Select this checkbox if your SCP server is configured to accept Anonymous logins. Inventory Manager will automatically fill in the username and password fields.

### Username/Password

Enter your username and password to access the SCP server. If you select the **Hide Password** checkbox, your password will be replaced with asterisks when it is typed in.

---

### Related Information

For information on related tasks:

- [Firmware Discovery](#)
- [FTP Server Setup](#)
- [TFTP Server Setup](#)
- [SCP Server Setup](#)
- [How to Set Inventory Manager Options](#)

## Main Window

---

The Inventory Manager main window is the central point for all Inventory Manager tasks. It is divided into a left panel, right panel, and bottom panel. The title bar displays the client's authorization group, user name, and client host. The four tabs in the left panel display the devices and device groups, firmware, archive, or configuration template information for your network depending on what tab you have selected. The right-panel tabs display detailed information about the item selected in the left panel. The Active Status/Event Log panel at the bottom of the window provides a chronological summary of operations that Inventory Manager has performed as well as error and informational messages about Inventory Manager system operations.

The Menu Bar and the Tool Bar at the top of the window let you perform inventory-related tasks. The Status Bar at the bottom of the window displays error and status information.

**Information on the Main window features:**

- [Menu Bar](#)
- [Tool Bar](#)
- [Left Panel](#)
- [Right Panel](#)
- [Active Status Panel](#)
- [Event Log](#)
- [Status Bar](#)



NetSight Inventory Manager [NetSight Administrator/carter : Connected to carter-xp2]

File Edit View Tools Applications Help

Network Elements Firmware Mgmt Archive Mgmt Configuration Templates

My Network (17 devices)

All Devices (17 devices)

12.22.120.1  
12.22.120.2  
12.22.120.75  
12.22.120.76  
12.22.120.77  
12.22.120.78  
12.22.120.79  
12.22.120.80  
12.22.120.81  
12.22.120.100  
12.22.120.115  
12.22.120.117  
12.22.120.125  
12.22.120.127  
12.22.120.128  
12.22.120.130  
12.22.120.131

Grouped By (17 devices)

Building A (7 devices)

Floor One (4 devices)

Floor Two (3 devices)

Details View Custom Attributes

Contents of 'My Network/All Devices'

Alert	IP Address	Name	Last Status	Uptime	Firmware
1	12.22.120.1	12.22.120.1	Contact		E9.1.7.0
2	12.22.120.2	12.22.120.2	Contact		E10.0.0.0
3	12.22.120.75	12.22.120.75	Contact	57 days 8:57...	01.02.04
4	12.22.120.76	12.22.120.76	Contact	49 days 20:4...	03.02.18.1
5	12.22.120.77	12.22.120.77	Contact	29 days 20:0...	05.05.11
6	12.22.120.78	12.22.120.78	Contact	29 days 20:0...	05.05.11
7	12.22.120.79	12.22.120.79	Contact	29 days 20:0...	05.05.11
8	12.22.120.80	12.22.120.80	Contact	20 days 23:2...	05.05.11
9	12.22.120.81	12.22.120.81	Contact	30 days 3:20...	05.05.11
10	12.22.120.100	12.22.120.100	Contact		05.08.09
11	12.22.120.115	12.22.120.115	Contact	29 days 20:1...	04.10.15
12	12.22.120.117	12.22.120.117	Contact		04.00.20m
13	12.22.120.125	12.22.120.125	Contact		03.11.01
14	12.22.120.127	12.22.120.127	Contact	55 days 23:1...	N/A
15	12.22.120.128	12.22.120.128	Contact	57 days 10:1...	N/A
16	12.22.120.130	12.22.120.130	Contact		02.04.07.06
17	12.22.120.131	12.22.120.131	Contact	403 days 2:2...	02.05.18

Active Status: Summary Active Status: Details Event Log

Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type
20	Info	NetSight	02/23/2005 11:18:05 AM	---	carter-XP2	NetSightServ...	Event
21	Info	NetSight	02/23/2005 11:18:05 AM	---	carter-XP2	NetSightServ...	Event
22	Notice	Client	02/23/2005 11:11:56 AM	---	---	carter	Event
23	Notice	Authentication	02/23/2005 11:11:56 AM	---	---	carter	Event

Ready

## Menu Bar

The Menu Bar on the Main Window provides access to Inventory Manager functions. Some menu options are standard, and some depend on what left-panel item and right-panel tab you have selected. Many of the menu options available from the menu bar are also available from right-click menus. For information on menu options available only from right-click menus, see [Right-](#)

---

[click Menu Options](#). For information on right-click menu options available in the Active Status panel, see [Active Status Right-click Menu Options](#).

### *File Menu*

#### **File > Database > Properties**

Opens the Database Properties window which displays information about certain Inventory Manager components stored in the NetSight database

#### **File > Database > Initialize Inventory Components**

Opens a window where you can choose to initialize all Inventory Manager components in the NetSight database. This removes all Inventory Manager data elements from the database. You must have the appropriate user capability to perform this operation. For more information, see [How to Initialize Inventory Database Components](#).

#### **File > Close**

Exits the Inventory Manager application. This menu option serves the same function as the **Close** button on the toolbar.

### *Edit Menu*

The Edit Menu options and the action taken depends on what is currently selected in the left panel or right panel.

#### **Edit > Copy**

Copies an item selected in the left panel or right panel. The option may or may not be available, depending on where you are in the application. This menu option serves the same function as the **Copy** button on the toolbar.

#### **Edit > Paste**

Pastes what has been copied into the specified location. The option may or may not be available, depending on where you are in the application. This menu option serves the same function as the **Paste** button on the toolbar.

#### **Edit > Rename**

Lets you change the name of the currently selected archive.

#### **Edit > Rename Device Group**

Lets you change the name of the currently selected device group.

#### **Edit > Delete**

Lets you delete the item currently selected in the left panel.

## *View Menu*

Lets you make changes to the appearance of the Inventory Manager main window and the information contained in the right panel. The View Menu options depend on what is currently selected in the left panel.

### **View > Tool Bar**

Hide or display the Tool Bar by selecting or deselecting the checkbox.

### **View > Status Bar**

Hide or display the Status Bar by selecting or deselecting the checkbox.

### **View > Expand All**

Expands (opens) all the folders under the folder selected in the left panel.

### **View > Collapse All**

Collapses (closes) all the folders under the folder selected in the left panel.

### **View > Refresh (Rediscover)**

With a device or device group selected in the Network Elements tab, Refresh (Rediscover) attempts to contact the selected device(s) to update the properties information. The Profile for the Read Access Level of the NetSight Administrator Authorization Group is used to refresh information..

### **View > Refresh**

Updates different information depending on what left-panel tab is selected. With the Archive Mgmt tab selected, Refresh performs a configuration discovery and updates the archive information. With the Firmware Mgmt tab selected, Refresh performs a firmware discovery and checks for new firmware images. With the Configuration Templates tab selected, Refresh performs a configuration template discovery and updates the template information.

## *Tools Menu*

Lets you perform administrative tasks. The Tools Menu options vary depending on what is currently selected in the left panel or right panel.

### **Tools > Authorization/Device Access**

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in NetSight applications.

**Tools > Server Information**

Opens the Server Information window where you can view and configure certain NetSight Server functions, including management of client connections, locks, and licenses.

**Tools > Capacity Planning**

Opens the Capacity Planning tool that helps you quickly prepare valuable network inventory planning reports. Each report is designed to answer a specific capacity planning question and lets you view results organized into different categories. For more information, see [Capacity Planning](#).

**Tools > Create BOOTP Tab**

Automatically creates a `bootptab` file and allows you to save the file in the desired directory. For instructions, see [Creating a Bootptab File](#).

**Tools > Scheduled Events**

Opens the [Scheduled Events window](#) where you can view any scheduled operations, and disable them if desired.

**Tools > Push Local Firmware to Server**

Opens the Select Local Firmware File window where you can select a firmware file and access the [Push Firmware to Server window](#) which gives a remote client the ability to send a local firmware or boot PROM image to the NetSight Server.

**Tools > Export Serial Numbers**

Opens the Export Serial Numbers window that displays a list of FRU serial numbers. The data in this view can be used to create a comma separated value (.csv) file of serial numbers or you can register the serial numbers with Extreme Networks. Registering serial numbers requires an Extreme Networks account, which can be created through Support at [www.extremenetworks.com/support/](http://www.extremenetworks.com/support/). Unless you have entered your account credentials in the ExtremeNetworks.com Update options panel (Tools > Options > Suite Options), you will be prompted for them when you register.

**Tools > Check for Firmware Updates**

Checks for the latest firmware releases for each device type in the NetSight database. The results are displayed in the Updates Available window with links to a firmware download web page. For more information, see Suite-Wide Tools Help topic How to Check for Updates.

**Tools > Wizards > Firmware Upgrade Wizard**

Opens the Firmware Upgrade Wizard where you can download a firmware image to a single device or a group of devices. For instructions, see Suite-Wide Tools Help topic [How to Upgrade Firmware](#).

**Tools > Wizards > Boot PROM Upgrade Wizard**

Opens the Boot PROM Upgrade Wizard where you can download a boot PROM image to a single device or a group of devices. For instructions, see [How to Upgrade Boot PROM](#).

**Tools > Wizards > Archive Wizard**

Opens the Archive Wizard where you can create a backup copy of your network devices' current configurations. For instructions, see [How to Archive](#).

**Tools > Wizards > Template Download Wizard**

Opens the Template Download Wizard where you can download a configuration template to one or more devices. For instructions, see [Template Download Wizard](#).

**Tools > Wizards > Restore Wizard**

Opens the Restore Wizard where you can restore saved configurations (archive versions) to devices. For instructions, see [How to Restore an Archive](#).

**Tools > Wizards > Reset Wizard**

Opens the Reset Device Wizard where you can reset a single device, multiple devices, or even multiple device groups. For instructions, see [How to Reset a Device](#).

**Tools > Options**

Opens the Options window where you can set Suite-Wide options and [Inventory Manager options](#).

**Tools > Remove from Device Group**

Removes the currently selected device from the device group. You must have a device in a device group selected in the left-panel Network Elements tab to see this menu option.

**Tools > Add Device(s) to Group**

Lets you add a device to a user-defined device group. You must have a device selected in the left-panel Network Elements tab to see this menu option.

**Tools > Telnet**

Launches a Telnet session to the selected device's Local Management.

**Tools > SSH**

Launches the Secure Shell (SSH) server and, after entering an appropriate username, opens a shell window, which provides the means to communicate with the selected device using a secure command-line based mechanism.

**Tools > Track Device**

Opens the [Track Device window](#) where you can track a device by serial number or MAC address. This allows you to view a history of device attributes, and monitor any changes made to the device. For instructions, see [How to Track a Device](#).

**Tools > File Transfer Method**

Opens the [File Transfer Method window](#) where you can specify the file transfer method for a single or multiple devices. Once you have specified the file transfer method for a device, all archive save and restore operations and firmware/boot PROM upgrades on the device will be performed using the specified method. For instructions, see [How to Set a File Transfer Method](#). You must have a single device selected in the Network Elements tab, or multiple devices selected in a right-panel Details View tab, to see this menu option.

**Tools > Alternate Firmware Server**

Opens the [Set Firmware Server window](#) where you can specify which firmware download server a device will use when performing firmware downloads. You must have a device or device group selected in the Network Elements tab to see this menu option.

**Tools > Acknowledge Alert**

Adds a check to an alert icon indicating that the alert has been reviewed and acknowledged or, for alerts in a right-panel Details View for a device or device group, it removes the alert icon from the column. You must select an entry with an active alert icon in a right-panel tab to see this menu option.

**Tools > Set Template Variable Values**

Opens the [Set Template Variables window](#) where you can set variable values for multiple devices at one time. Variables are used in configuration templates to substitute for device-specific information. You must have a device or device group selected in the Network Elements tab to see this menu option.

**Tools > Execute Command Script**

Opens the NetSight Command Script tool that lets you execute a sequence of CLI commands (a script) on a set of devices. You must have a device or device group selected in the Network Elements tab to see this menu option.

**Tools > Execute Show Support Script**

Runs the Show Support command for the selected devices using the Execute Command Script window. You must have a device or device group selected in the Network Elements tab to see this menu option.

**Tools > Default File Transfer Method**

Opens the [File Transfer Method window](#) where you can specify a default file transfer method for an entire device type. Once you have specified the file transfer method for a device type, all archive save and restore operations and firmware/boot PROM upgrades on devices of that type will be performed using the specified method. For instructions, see [How to Set a File Transfer Method](#). You must have a device type (lowest-level device type folder) selected in the Firmware Management tab, to see this menu option.

**Tools > Create Firmware Record**

Opens the [Create Firmware Record window](#) where you can add a firmware or boot PROM image to your Firmware Mgmt tab manually, as opposed to having the image automatically discovered during a [firmware discovery](#). When you are using an [alternate firmware server](#), you must use this window to manually create the firmware records associated with the alternate server. (You must have a configured alternate firmware server for this menu option to be available.)

**Tools > Assign Firmware**

Opens the [Assign Firmware window](#) where you can assign a firmware image to one or more product families or device types. You must have a firmware image selected in the left-panel Firmware tab to see this menu option. For instructions, see [How to Assign Firmware](#).

**Tools > Remove Firmware From Group**

Removes the currently selected firmware image from the firmware group. You must have an image in a firmware group selected in the left-panel Firmware Mgmt tab to see this menu option.

**Tools > Set as Reference Image**

Designates the selected firmware or boot PROM image as the preferred image for a specific binary family of devices. The image will be set as a

reference for all device types with which it is compatible. (If the Set as Reference Image option is not available, make sure that the selected image has been assigned to appropriate device types.)

#### **Tools > Stamp New Version**

Creates a new version of the selected archive. You must have an archive selected in the left-panel Archive Mgmt tab to see this menu option. For more information, see [Saving a New Archive Version](#).

#### **Tools > Compare Archives**

Opens the [Select Archive Versions to Compare window](#) to select archived configurations you want to compare, and the [Compare Archives window](#) to view the comparison results. You must have an archive, version, or configuration file selected in the left-panel Archive Mgmt tab to see this menu option. For instructions, see [How to Compare Archives](#).

#### **Tools > Lock/Unlock**

Allows you to lock and unlock an archive version. A locked archive version will not be deleted when the maximum number of saved versions for this archive (as specified in the [Archive Wizard](#)) has been reached. You must have an archive version selected in the left-panel Archive Mgmt tab to see this menu option.

#### **Tools > View Configuration File**

Opens the [Configuration File Viewer](#) and displays the archived configuration file selected in the left-panel Archive Mgmt tab.

#### **Tools > Create Configuration Template**

Opens the [Edit Configuration Template window](#) where you can create a configuration template based on an archived configuration file. Creating a configuration template lets you easily download the same configuration file to multiple devices. You must have a configuration file selected in the left-panel Archive Mgmt tab to see this menu option. For more information, see [How to Create and Download Configuration Templates](#).

#### **Tools > Compare Configuration Files**

Opens the [Select Configurations window](#) to select two archived configuration files to compare, and the [Compare Configuration Files window](#) to view the comparison results. You must have a configuration file selected in the left-panel Archive Mgmt tab to see this menu option.

#### **Tools > Copy File to Client**

Allows you to copy a configuration file from the NetSight Server to your local client system. Opens a Save window where you can navigate to the



directory where you want the file to be saved. You must have a configuration file selected in the left-panel Archive Mgmt tab to see this menu option.

#### **Tools > Assign Configuration Template**

Opens the [Assign Configuration Template window](#) where you can assign a template to one or more device types. You must have a template selected in the left-panel Configuration Template tab to see this menu option. For instructions, see [Assigning Templates to Device Types](#).

#### **Tools > Edit Configuration Template**

Opens the [Edit Configuration Template window](#) where you can modify the template. You must have a template selected in the left-panel Configuration Template tab to see this menu option. For more information, see [How to Create and Download Configuration Templates](#).

#### **Tools > Remove Configuration Template From Group**

Removes the currently selected template from the template group. You must have a template selected in the left-panel Configuration Template tab to see this menu option.

#### **Tools > Rename Template**

Lets you change the name of the currently selected configuration template. You must have a template selected in the left-panel Configuration Template tab to see this menu option.

### *Applications Menu*

Lets you launch other NetSight applications from Inventory Manager. You can also customize the Applications menu to launch your own applications. For more information, see the Console Help topic [How to Add Third-Party Application Support](#).

### *Help Menu*

Lets you access the components of the Inventory Manager online information system.

#### **Help > Help Topics**

Opens the Inventory Manager Help system.

#### **Help > Release Notes**

Displays the NetSight Release Notes.

**Help > About This Window**

Displays detailed information about the currently selected right panel tab. This menu option serves the same function as the **Help** button on the toolbar.

**Help > Support Center**

Opens the Extreme Networks Support website.

**Help > Check for Updates**

Allows you to update Inventory Manager with newly supported device types and obtain the latest version of release notes. For more information, see the Suite-Wide Tools Help topic Setting Web Update Options.

**Help > Getting Started**

Displays the Getting Started help topic that provides an overview of Inventory Manager features and a summary of the basic steps you must perform to begin using Inventory Manager.

**Help > About NetSight Inventory Manager**

Displays product information for the NetSight Suite.

*Right-Click Menu Options*

The following menu options are only available from right-click menus. They are listed in alphabetical order.


**Firmware Releases Available**

This menu option is available by right-clicking on a firmware update icon in the Updates column of a device group Details View tab. It opens the Updates Available window where you can download the new firmware that is available for the device.

**Reload Device Tree From Database**

Reloads the device tree with the device data from the NetSight database. You must have the My Network folder selected in the Network Elements tab to see this menu option. If the application is showing incorrect device details (System Name, Contact, Location) or if device group membership is incorrect (particularly the system-created device groups), use this menu option to synchronize the device tree to the data in the database.

**Table Options**

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper

left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

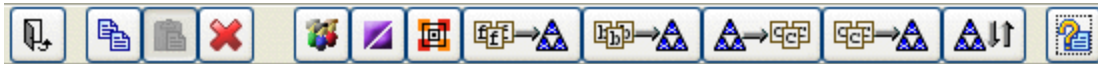
## Related Information

For information on related windows:

- [Main Window](#)

## Tool Bar

The Tool Bar on the Main Window provides easy access to some of the more commonly used Inventory Manager functions. Some Tool Bar buttons may not be available, depending on your current location within the Inventory Manager application.



### Close

Exits the Inventory Manager application. This button serves the same function as the **File > Close** menu option.

### Copy

Copies an item selected in the left panel or right panel. This button serves the same function as the **Edit > Copy** menu option.

### Paste

Pastes what has been copied into the specified location. This button serves the same function as the **Edit > Paste** menu option.

### Delete

Deletes the current selection in the left panel. This button serves the same function as the **Edit > Delete** menu option.

### Authorization/Device Access

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in NetSight applications. This button serves the same function as the **Tools > Authorization/Device Access** menu option.

**Server Information**

Opens the Server Information window where you can view and configure certain NetSight Server functions, including management of client connections, locks, and licenses. This button serves the same function as the **Tools > Server Information** menu option.

**Capacity Planning**

Opens the [Capacity Planning](#) tool that helps you quickly prepare valuable network inventory planning reports. This button serves the same function as the **Tools > Capacity Planning** menu option.

**FW Upgrade**

Opens the [Firmware Upgrade Wizard](#) that helps you easily upgrade firmware images on your network devices. This button serves the same function as the **Tools > Firmware Upgrade Wizard** menu option.

**BP Upgrade**

Opens the [Boot PROM Upgrade Wizard](#) that helps you easily upgrade boot PROM images on your network devices. This button serves the same function as the **Tools > Boot PROM Upgrade Wizard** menu option.

**Archive**

Opens the [Archive Wizard](#) that lets you create archives and save backup copies of your devices' configurations. This button serves the same function as the **Tools > Archive Wizard** menu option.

**Restore**

Opens the [Restore Wizard](#) that lets you restore saved configurations (archives) to devices. This button serves the same function as the **Tools > Restore Wizard** menu option.

**Reset**

Opens the [Reset Device Wizard](#) that lets you reset a single device, multiple devices, or even multiple device groups. This button serves the same function as the **Tools > Reset Wizard** menu option.

**Help**

Displays detailed information about the currently selected right-panel tab. This button serves the same function as the **Help > About This Window** menu option.

---

**Related Information**

For information on related windows:

- [Main Window](#)
- [Menu Bar](#)

## Left Panel

---

The left panel of the Inventory Manager main window contains four tabs: Network Elements, Firmware Mgmt, Archive Mgmt, and Configuration Templates. These tabs display various management information in an hierarchical tree format. To switch tabs, click on the desired tab.

Features of the left panel include:

- *Expanding and collapsing items in the hierarchy:* Double-click the item or its icon, or single-click the turner to the left of the icon.
- *Right-click menus:* Right-click a folder or other item in the left panel, and a menu of the options you can perform on your selection appears.
- *Drag and drop:* In the Network Elements and Firmware Mgmt tabs, you can populate groups by dragging and dropping a device or firmware image into the desired group.

The item you select in the left-panel tree determines what is displayed in the right panel of the Inventory Manager main window. For many of the items you select in the left panel, the default display in the right panel is a [Details View tab](#). For information on Details Views and the other tabs that appear in the right panel, click on the name of the tab in the Right-Panel Tabs section of the Inventory Manager Help Contents.

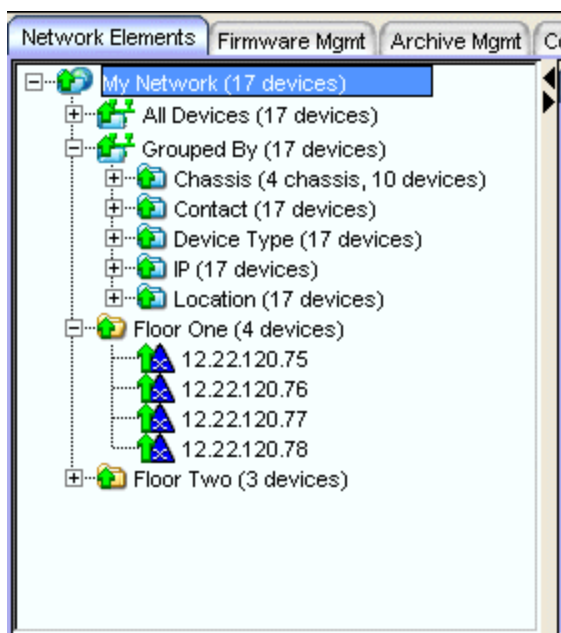
Information on the left-panel tabs and icons:

- [Network Elements Tab](#)
- [Firmware Mgmt Tab](#)
- [Archive Mgmt Tab](#)
- [Configuration Templates Tab](#)
- [Left-Panel Icons](#)

### *Network Elements Tab*

The Network Elements tab is displayed in the left panel when you open Inventory Manager. This tab displays your network devices and device groups.

Each device group name is followed by the total number of devices in that group and any subgroups, in parentheses.



### My Network

My Network displays all your devices, plus the system-created device groups and any user-created device groups. For information on creating device groups, see [How to Add and Remove Device Groups](#).

### All Devices Folder

This folder contains all the devices in the NetSight database. For information on adding devices to the database, see [How to Add and Delete Devices](#).

### Grouped By Folder

The top-level Grouped By folder contains five system-created groups: Chassis, Contact, Device Type, IP, and Location. When a device is added, discovered, or imported, it automatically becomes a member of the appropriate group.

### Chassis Folder

Contains subgroups for specific chassis in your network.

### Contact Folder

Contains subgroups of your devices based on the system contact. Subgroups in this folder are automatically created based on the Contact value in the Console Properties (Device) tab. For example, a contact defined as *NOC/Rochester/Jones* will automatically create a hierarchy of three sub-

groups under the **Grouped By > Contact** folder. The Contact sub-groups are removed when the last device with a particular contact is deleted from the database.

### Device Type Folder

Contains subgroups for the specific product families and device types in your network. The Unknown folder contains devices that could not be correlated to a device type.

### IP Folder

Contains subgroups based on the IP subnets in your network.

### Location Folder

Contains subgroups of your devices based on the system location. Subgroups in this folder are automatically created based on the Location value in the Console Properties (Device) tab. For example, a location defined as *New Hampshire/Rochester/Building 3* will automatically create a hierarchy of three sub-groups under the **Grouped By > Location** folder. The Location sub-groups are removed when the last device for a particular location is deleted from the database.

### User-created Device Groups

You can add your own device groups and subgroups (displayed with yellow folders) according to your network needs. See [How to Add and Remove Device Groups](#) for more information.

### Switch Icon

This icon represents an individual switch that has been discovered, imported, or added to the NetSight database. It appears below the All Devices folder and also below any device group of which it is a member. See [Left-Panel Icons](#) for a table of all possible icons.

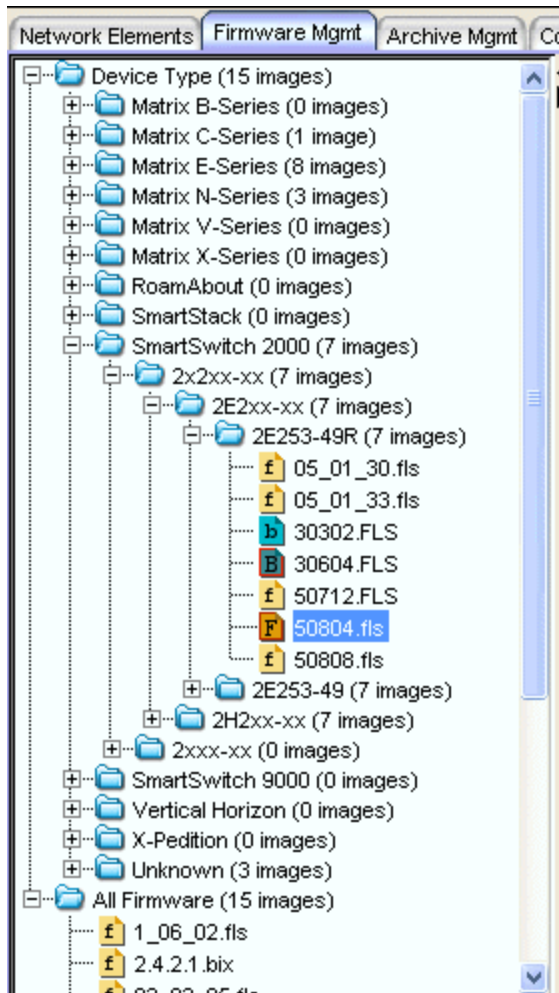
### Router Icon

This icon represents an individual router that has been discovered, imported, or added to the NetSight database. It appears below the All Devices folder and also below any device group of which it is a member. See [Left-Panel Icons](#) for a table of all possible icons.

## *Firmware Mgmt Tab*

The left-panel Firmware Mgmt Tab displays firmware images grouped according to product family, binary family, and device type. Inventory Manager provides pre-defined firmware groups and automatically organizes the firmware images stored in your firmware directory under the appropriate group when you

perform a firmware discovery or refresh. For instructions, see [Firmware Discovery](#). Each firmware group name is followed by the total number of images in that group and any subgroups, in parentheses.



### Device Type Folder

This folder contains pre-defined product family, binary family, and device type folders.

### Firmware Groups

Inventory Manager provides pre-defined firmware groups and automatically organizes your firmware images under the appropriate group when you perform a [firmware discovery or refresh](#).

### Unknown Folder

The Unknown folder contains firmware images that Inventory Manager could not correlate to a device type. You can assign this firmware to firmware groups using drag and drop or the [Assign Firmware window](#).




## All Firmware Folder

This folder contains all the firmware images discovered during a firmware discovery or refresh, or created using the Create Firmware Record window.

## Firmware Image Icon

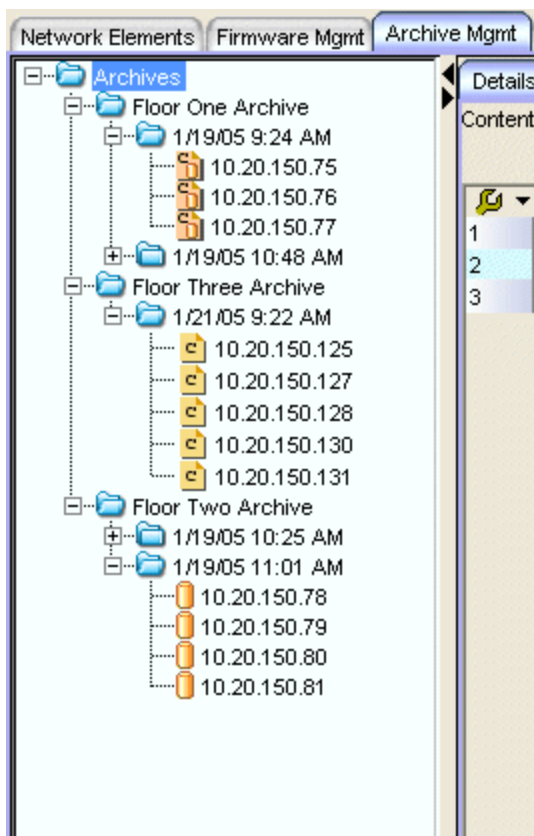
This icon represents an actual firmware image. Images that have been designated as a reference image display a reference icon .

## Boot PROM Icon

This icon represents a boot PROM image that is being stored in your firmware directory. Images that have been designated as a reference image display a reference icon .

## Archive Mgmt Tab

The left-panel Archive Mgmt tab displays information about your archive operations. The information is organized in a hierarchical tree format, with each archive operation listed by name. Under each archive are the archive versions, listed by the date and time that the version was performed. Individual configurations that were saved for each version are listed by the IP address of the device whose data was saved. For more information, see [How to Archive](#).



### Archives Folder

This folder contains all your archive operations.

### Archive Name Folder

This is the name that you gave the archive operation when you created it. This folder contains a list of all the archive versions that have been performed.

### Archive Version Folder

This is the date and time when the archive operation was performed. Each version contains a list of all the individual files that were saved during the archive operation.

### Configuration File Icon

This icon represents an archived device configuration file. Individual files are listed by the IP address of the device whose configuration was saved, followed by the SNMP context, if applicable.

### Capacity Planning File Icon

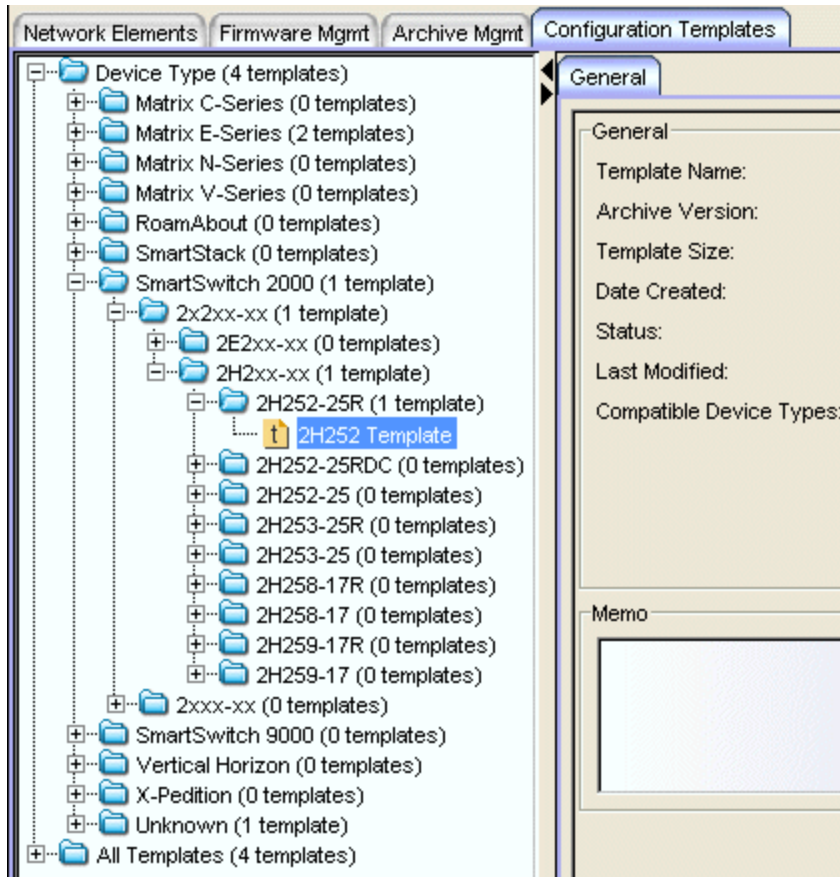
This icon represents an archived capacity planning file. Individual files are listed by the IP address of the device whose capacity planning data was saved, followed by the SNMP context, if applicable.

### Both Configuration and Capacity Planning File Icon

This icon represents an archived file that includes both device configuration and capacity planning data. Individual files are listed by the IP address of the device whose configuration and capacity planning data was saved, followed by the SNMP context, if applicable.

## *Configuration Templates Tab*

The left-panel Configuration Templates tab displays your configuration templates grouped according to product family and device type. Inventory Manager provides pre-defined template groups, and automatically assigns a template to the appropriate group when you create the template. For more information, see [How to Create and Download Configuration Templates](#). Each template group name is followed by the total number of configuration templates in that group and any subgroups, in parentheses.



### Device Type Folder

This folder contains pre-defined product family and device type folders.

### Template Groups

Inventory Manager provides pre-defined template groups and automatically organizes your templates under the appropriate group when you [create a configuration template](#).

### Unknown Folder

The Unknown folder contains configuration templates that Inventory Manager could not correlate to a device type. You can assign unknown templates to template groups using the [Assign Configuration Template window](#).

### All Templates Folder

















This folder contains all the configuration templates you have created.

### Configuration Template Icon

This icon represents an actual configuration template.

## Left-Panel Icons

The following table defines icons that can appear in the left-panel tree. A red down arrow on a device indicates lost contact with that device. A red down arrow on a Device Group icon indicates lost contact status for at least one device within the group. A green up arrow on a device icon indicates that contact is established with that device. A green up arrow on a Device Group icon indicates contact is established for all devices within a group. Group icons that appear without either arrow have no members.

Icon	Definition	Icon	Definition
	System-Created Groups		User-Created Groups
	Switch		Router
	Wireless		VPN
	SNMP (Workstations)		Unknown
	Firmware Image		Firmware Reference Image
	Boot PROM Image		Boot PROM Reference Image
	Configuration Archive		Configuration Template
	Capacity Planning Archive		Configuration and Capacity Planning Archive

## Related Information


For information on related windows:

- [Main Window](#)

## Right Panel

The right panel of the Inventory Manager main window displays a tab or tabs containing information about the item selected in the left panel.

For many of the items you select in the Inventory Manager left panel, the default display in the right panel is a [Details View tab](#). Details View tabs provide detailed information in tabular format for the current selection in the left panel. Often, if you right-click an item in the list, a menu of available options appears.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Suite-Wide Tools Table Tools Help topic.

For information on Details Views and the other tabs that appear in the right panel, click on the name of the tab in the Right-Panel Tabs section of the Inventory Manager Help Contents.

---

## Related Information

For information on related windows:

- [Main Window](#)

## Active Status Panel

---

The Active Status panel at the bottom of the Inventory Manager main window presents a chronological summary of operations that Inventory Manager has performed, including archive saves and restores, firmware/boot PROM upgrades, and reset device operations. As operations take place, the Active Status is updated with specific information about each event, and the status (results) of the operation. The Active Status panel lists operations performed by all Inventory Manager clients connected to the server.

The panel presents the status in two different views: Summary and Details. Use the buttons at the top of the panel to select the desired view. The Summary view lists the operations that have been performed, while the Details view lists the individual devices the operations have been performed on. If you select an operation in the Summary view then switch to the Details view, the corresponding device entries are highlighted. For even more detailed information about each entry, select the entry, then right-click and select **View** from the menu to open a [Properties window](#).

Entries remain in the Active Status panel until you restart the application. If the Active Status panel reaches a total of 1000 entries, the 500 oldest entries will be automatically purged. You can delete entries by right-clicking and selecting **Purge** from the menu. Deleting an entry causes that entry and all older entries to be purged. You cannot delete entries from the middle of the table because that would disrupt the sequence of events.


To stop an operation, select the operation entry, then right-click and select **Abort** from the menu. Any part of the operation that is currently in progress will complete before the operation is terminated.


Information on the following Active Status views:

- [Summary](#)
- [Details](#)
- [Right-Click Menu Options](#)

### Summary View


The Summary view presents a chronological summary of operations that Inventory Manager has performed, including archive saves and restores, firmware upgrades, and reset device operations. Select the Summary option at the top of the panel to display this view.


Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

Active Status: Summary    Active Status: Details    Event Log								
Alert	Schedule Name	Operation	Target	Status	% Progress	Date	Message	
	Write To Device	Device Data Updated	12.22.120.79	Success	100%	02/24/2005 10:30:17 AM	Operation Complete.	
	Floor Two Archive	Archive Save	Floor Two	Success	100%	02/24/2005 10:27:03 AM	Operation Complete.	
	Floor One Archive	Archive Save	Floor One	Failure	100%	02/24/2005 10:26:43 AM	Operation Complete.	
	Device Discovery	Device Discovery	Several Devices	Success	100%	02/24/2005 10:21:52 AM	Operation Complete.	

### Alert

A yellow alert icon in this column signifies:

-  -- the operation failed for one or more of the devices that the operation is responsible for.

-  -- for a successful configuration save operation, the alert signifies that there is a difference between one of the saved configuration files and the previous file saved for that device.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select **Acknowledge Alert** from the menu.

### Schedule Name

The name of the operation. For certain operations such as archive saves, this is the name you assigned the operation when you created it.

### Operation

The type of operation performed, such as Archive Save or Device Discovery.

### Target

What the operation is acting on.

### Status

The status of the operation: Success or Failure. If the operation was performed on multiple devices, the status will be listed as Success only if it was successful on all devices. If it fails on any device, the status will be listed as Failure. Select the entry, then right-click and select **View** to open the Properties window and see which device(s) failed.

### % Progress

A progress bar showing the percent completed of the operation.

### Date


The date and time the operation was performed.

### Message

A message relating to the status of the operation.

## *Details View*

The Details view presents a chronological listing of each device on which an operation was performed and the status (results) of the operation for that device. Select the Details option at the top of the panel to display this view.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

Alert	Schedule Name	Device IP	Operation	Status	% Progress	Bytes Trans.	File name
	Floor One Archive	12.22.120.78	Archive Save	Success	100%	50,286	C:\Program Files\Enterasys ...
	Floor One Archive	12.22.120.77	Archive Save	Success	100%	28,482	C:\Program Files\Enterasys ...
	Floor One Archive	12.22.120.76	Archive Save	Success	100%	1,323	C:\Program Files\Enterasys ...
!	Floor One Archive	12.22.120.75	Archive Save	Failure	100%	0	C:\Program Files\Enterasys ...
	Device Discovery	12.22.120.81	Device Discovery	Success	100%	0	N/A
	Device Discovery	12.22.120.79	Device Discovery	Success	100%	0	N/A

## Alert

A yellow alert icon in this column signifies:

- ! -- the operation failed for this device.
- ! -- for a successful configuration save operation, the alert signifies that there is a difference between this saved configuration file and the previous file saved for this device.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select **Acknowledge Alert** from the menu.

## Schedule Name

The name of the operation. For certain operations such as archive saves, this is the name you assigned the operation when you created it.

## Device IP

The IP address of the device.

## Operation

The type of operation performed, such as Archive Save or Device Discovery.

## Status

The status of the operation for that particular device: Success or Failure. Select the entry, then right-click and select **View** to open the Properties window for more information.

## % Progress

A progress bar showing the percent completed of the operation.

## Bytes Trans.

The number of bytes transferred during the operation.

## File name

For operations involving a file (such as a configuration file or firmware image file), the path and filename of the file.

## Date

The date and time the operation was performed on that device.



## Message

A message relating to the status of the operation.

### *Right-Click Menu Options*

Select an entry in either the Summary or Details view and then right-click to see a menu of standard table options plus some active status options. The table tools help you find, filter, sort, print, and export information in the table, and customize table settings. For more information, see the Table Tools Help topic. The active status options include:

- **View** - Opens the [Properties window](#) which displays additional details on the entry.
  - **Purge** - Deletes the selected entry and all older entries. You cannot delete entries from the middle of the table because that would disrupt the sequence of events.
  - **Acknowledge Alert** - Places a checkmark on the alert icon signifying that the alert has been acknowledged.
  - **Abort** - Stops an operation. Any part of the operation that is currently in progress will complete before the operation is terminated. This option is only available in the Summary view.
- 

## Related Information

For information on related windows:

- [Properties Window](#)
- [Event Log](#)


## Event Log

---

The Event Log at the bottom of the Inventory Manager main window displays error and informational messages about Inventory Manager system operations. The log displays the most recent 10,000 entries. The current log file is automatically archived when its size reaches 5 megabytes and a new log file is opened. Use the Event Logs view in the Suite-Wide Options window to configure the number of event logs to save and the number of entries to display in the table. You must be assigned the appropriate user capability to view the Event Log.

Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event	Information
<input type="checkbox"/>	Info	NetSight	02/14/2005 10:16:18 AM	---	carter-XP2	NetSightServer	Event	---	Configuration Save Fix
<input type="checkbox"/>	Info	NetSight	02/14/2005 10:16:14 AM	---	carter-XP2	NetSightServer	Event	---	Scheduled Create Arc
<input type="checkbox"/>	Notice	Client	02/14/2005 08:55:58 AM	---	carter	carter	Event	Client Startup	Start NetSight Inventor...
<input type="checkbox"/>	Notice	Authentication	02/14/2005 08:55:58 AM	---	---	carter	Event	Authentication S...	Authentication Succes...
<input type="checkbox"/>	Notice	Client	02/11/2005 04:57:48 PM	---	carter-XP2	carter	Event	Client Shutdown	End NetSight Inventor...

### Acknowledge:

This checkbox lets you acknowledge an event and also hide items that have been acknowledged. Click the checkbox to acknowledge the item and then click the Show Acknowledged Events button  to hide or show the checked items.

### Severity

The event's severity.

### Category

The category of event.

### Timestamp

The date and time when the event occurred.

### Source

The IP address of the host that was the source of the event.

### Client

The name of the client host machine that triggered the event.

### User

The name of the user that triggered the event.

### Type

The type of information: Event.

### Event


The type of event.

### Information

Information about the event.

### Right-Click Menu Options

The event log right-click menu lets you *Acknowledge* and *Unacknowledge* events. It also provides options and a standard set of table tools to help you find, filter, sort, print, and export information in a table and customize table settings.

You can access the menu options through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

#### Show/Hide Acknowledged Events Button

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

#### Refresh Button

Refreshes the log.

#### Clear Current View Button

Clears entries from the current table.

---

## Related Information

For information on related windows:

- [Active Status Panel](#)

## Status Bar

---

The status bar at the bottom of the window displays status information on the left side. A progress bar on the right side shows the percentage of completion for certain lengthy operations. In addition, status bar icons serve as reminders of tasks that need to be performed.

#### Event Log Icon

An Event Log icon is displayed when a new Warning or Error message has been logged to the Event Log. Double-clicking the icon will display the [Event Log](#) in the bottom panel, provided you have the appropriate user capability to view the Event Log.

#### Reset Device Icon

A Reset Device icon is displayed when there are devices that have received new firmware images and need to be reset. Double-click the icon to open the Devices Need Reset window. From this window you can launch the [Reset Device Wizard](#) for those devices or simply clear the reset flags without resetting the devices.

## Related Information

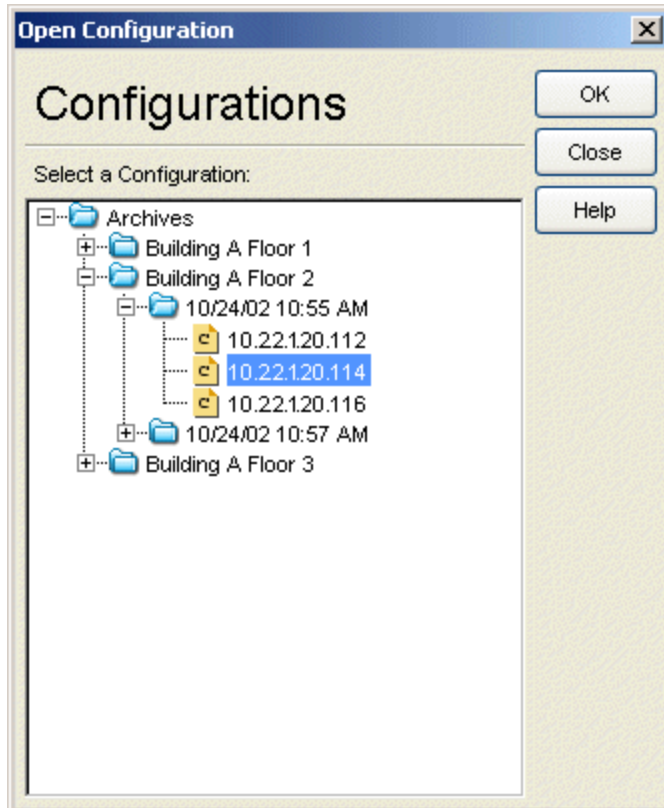
For information on related windows:

- [Main Window](#)

## Open Configuration Window

---

This window is accessed from the **Change** button in the [Configuration File Viewer](#), and lets you select a new configuration file to view.



### Select a Configuration

Expand the folders as necessary and select the configuration file you wish to view.

### OK Button

Opens the [Configuration File Viewer](#) with the selected file displayed.

---

## Related Information

For information on related windows:

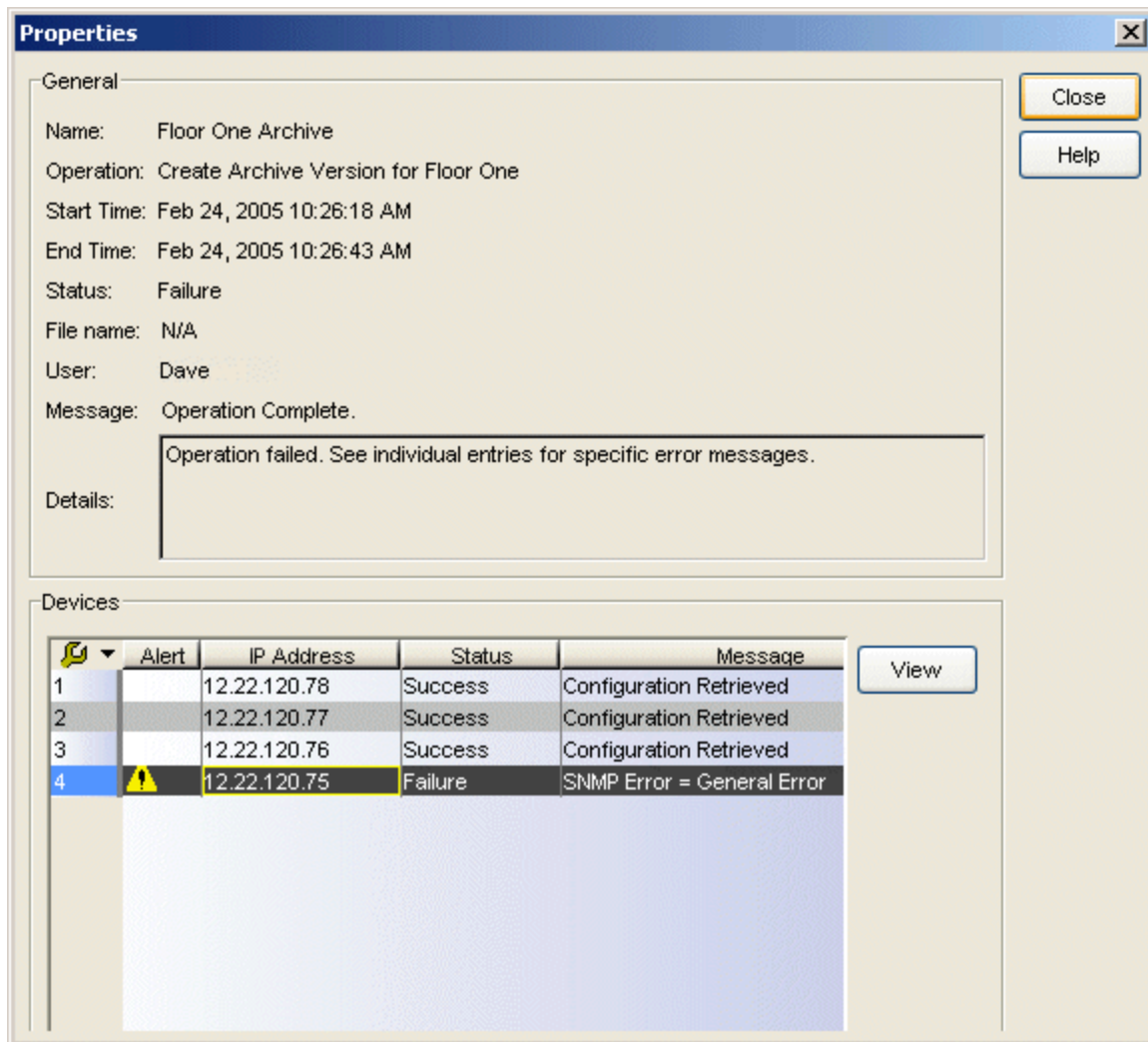
- [Compare Configuration Files Window](#)
- [Configuration File Viewer](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

## Properties Window

The Properties window provides detailed information about a specific entry in the [Active Status panel](#) at the bottom of the Inventory Manager window. Access the Properties window from the Active Status panel (either the [Summary View](#) or the [Details View](#)), by double-clicking an entry, or by selecting an entry, then right-clicking and selecting **View** from the menu.



### General Area

#### Name

The name of the operation.

### Operation

The type of operation performed, plus the name of the device group or the IP address of the single device on which the operation was performed.

### Start time

The date and time the operation was started.

### End Time

The date and time the operation was completed.

### Status

The status of the operation.

### File name

The name and path to the file used or created in the operation (if applicable). For example, in an Archive Save operation, this field will display the name and path to the configuration file created as a result of the operation. If the operation was performed on a device group, this field will display N/A.

---

**NOTE:** When launched from the Summary View, this field will not show a file name, since it will normally be a summary for a group of devices.

---

### User

The user ID of the person who was running Inventory Manager when the operation was performed.

### Message


Messages regarding the status of the operation.

### Details

Additional details about the outcome of the operation that was performed.

## Devices Area

This table displays a list of the devices included in the operation, and a status and message pertaining to each individual device. You can select a device and click **View** to open an additional Properties window specifically for that device. This area is only displayed when the Properties window is launched from the [Active Status Summary View](#).



Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you



have the row count column displayed). For more information, see the Table Tools Help topic.

### Alert

A yellow alert icon in this column signifies:

-  -- the operation failed for this device.
-  -- for a successful configuration save operation, the alert signifies that there is a difference between this saved configuration file and the previous file saved for this device.

### IP Address

The device's IP address. Note that chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

### Status

The status of the operation, Success or Failure, for that particular device.

### Message

Messages regarding the outcome of the operation for that particular device.

### View Button

Select a device and click **View** to open a secondary Properties window that displays general information for a particular device. This button is only available in a Properties window that includes the Devices Area (which is only displayed when the Properties window is launched from the [Active Status Summary View](#).)

---

## Related Information

For information on related windows:

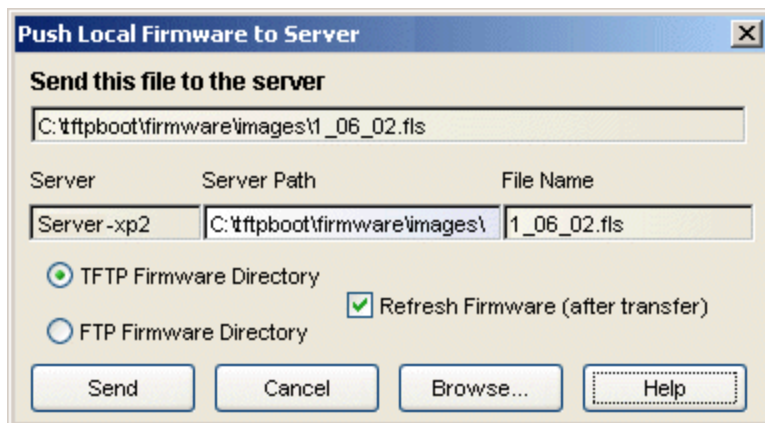
- [Active Status Panel](#)

## Push Local Firmware to Server Window

---

The Push Local Firmware to Server window gives a remote client the ability to send a local firmware or boot PROM image to the NetSight Server. This allows a remote client to download a firmware image from the download library website, and then push the firmware to the server where it can be used in Inventory Manager operations such as firmware and boot PROM upgrades.

To access this window, select **Tools > Push Local Firmware to Server**. The Select Local Firmware File window opens, where you can navigate to the file you want to send. Select the file and click **Open**. The Push Local Firmware to Server window opens.



### Send this file to the Server

The path to the local file you have selected to send. Use the **Browse** button to select another file, if desired.

### Server

The name of the server the client is connected to.

### Server Path

The path to the server's TFTP or FTP firmware directory, depending on what option you have selected below. You can extend the path to a different folder in the directory, if desired.

### File Name

The name of the firmware or boot PROM file being pushed to the server.

### TFTP/FTP Firmware Directory

Select whether you want to store the file in the FTP or TFTP firmware directory on the server.

### Refresh Firmware

Select this checkbox if you want to perform a firmware discovery following the operation, and update the firmware listed in your Firmware Mgmt tab.

### Send Button

Sends the image to the server and closes the window.

### Browse Button

Opens the Select Local Firmware File window where you can select another file to send.

---


## Related Information

For information on related tasks:

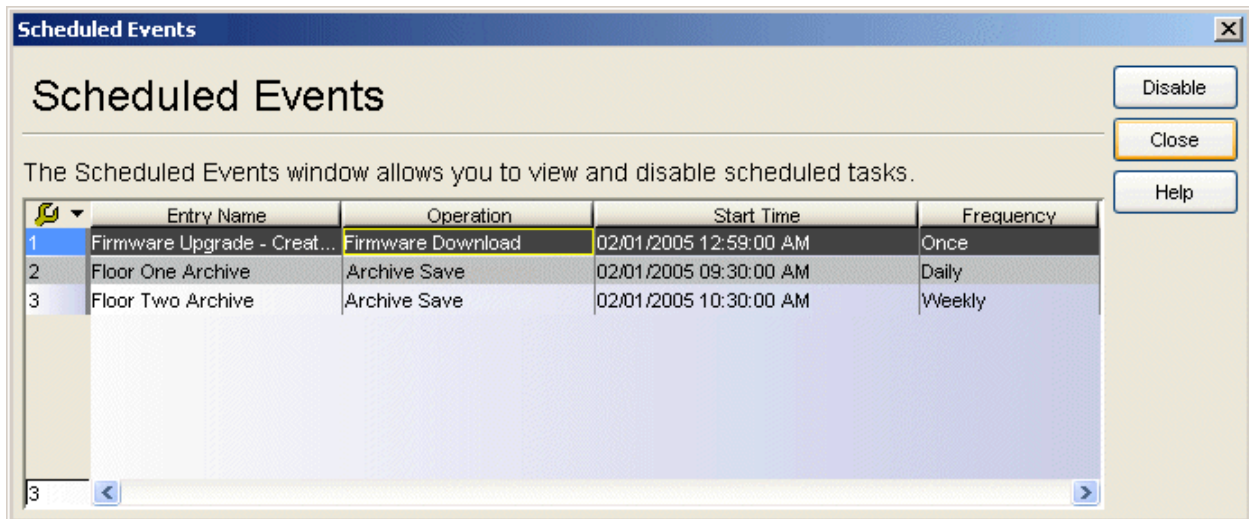
- [How to Upgrade Boot PROM](#)
- [How to Upgrade Firmware](#)

## Scheduled Events Window

Inventory Manager lets you schedule firmware upgrades, configuration archive operations, and capacity planning reports. You can use the Scheduled Events window to view any scheduled operations for all Inventory Manager clients connected to the server, and disable them if desired. Scheduled events are listed in a table, starting with the next scheduled event. You must be assigned the appropriate user capability to view this window and perform the disable function.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

To access this window, select **Tools > Scheduled Events**.



### Entry Name

The name of the scheduled event.

### Operation

A description of the scheduled event.

### Start Time

The next scheduled time the operation will be performed.

### Frequency

The frequency the scheduled event is performed.

### Disable Button

Disables the selected scheduled event so that it will not be performed. The disable action behaves differently depending on the type of scheduled event you are disabling:

- Firmware Upgrade - the scheduled upgrade is cancelled.
- Archive (Configuration Save) - The scheduled archive's frequency is set to "Never". You can reschedule the archive in the [Archive General tab](#).
- Capacity Planning Report - The scheduled report's frequency is set to "Never". You can reschedule the report using the [Capacity Planning tool](#).

You can also disable an event by selecting it and using the right-click menu.

---

### Related Information

For information on related tasks:

- [Scheduling a Firmware Upgrade](#)
- [Using the Archive Wizard](#)
- [Capacity Planning](#)

## Schedule Report Window

Use the Schedule Report window to configure scheduling information and e-mail notification settings for a Capacity Planning report. You can access the window from the Capacity Planning tool while you are creating a report. Select the schedule report checkbox when you save the report, or use the Schedule button in the Select Report window to schedule a report that has already been saved.

**NOTE: Scheduling Ports Reports.** Depending on the size of your network and the number of ports on the devices in your network, a ports report may generate results that are too large to be delivered via e-mail. In this case, you should consider creating multiple reports based on subnet or device type. This is primarily a concern when selecting the Port Details view for your report results.

The screenshot shows the 'Schedule Report' window with the following configuration:

- Name:** Ports Report Building A Floor One
- Schedule:**
  - Frequency: Weekly
  - Select Starting Day: February 2005
  - Calendar: February 2005 (with the 23rd selected)
  - Start Time: 1:00 PM EST
- Notification Settings:**
  - E-Mail Recipient List: List One (with an Edit Mail List button)
  - Report Format: Comma Separated Values - \*.csv
  - Delimited Field Options:
    - Field delimiter: Comma
    - Text delineation: "
  - Report Options:
    - Totals by Group
    - Devices Only
    - Totals by Port Type
    - Port Details

Buttons at the bottom: Save, Close, Help.

Name

The name of the report being scheduled.

## Schedule

### Frequency

Use the drop-down list to select the frequency with which you want the report to be run: Never, Now, Once, Daily, Weekly, or On Server Startup. The Never option lets you create a schedule for a report without actually running the report. The Now option will immediately run the report.

### Select Starting Day

Use the drop-down list to select the month you want the schedule to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field.

### Start Time

Set the starting time for the schedule and select AM or PM. (This field is grayed out if you have selected the Never or Now frequency.)

## Notification Settings

---

**NOTE:** For the e-mail notification feature to work correctly, you must set your SMTP Email Server options (in the Suite-Wide Options window) in addition to these e-mail notification settings here.

---

### E-Mail Recipient List

Use the drop-down list to select the e-mail recipient list for the report. Use the **Edit Mail List** button to open the [E-Mail Configuration window](#) and create your e-mail lists.


### Report Format

Use the drop-down list to select the format for the report results: Comma Separated Values file (.csv), HTML file, or Delimited Text file (.txt). If you select Delimited Text, use the Delimited Field Options section to select your field delimiter and text delineation specifications.

### Report Options

Use this section to select the report results you want included in the e-mail notification.

### Save Button

Saves the scheduling information. The saved report will be listed in the Select Report window of the Capacity Planning tool with a schedule icon  to indicate that it has been scheduled. You can remove a schedule from

a saved report by right-clicking on the report and selecting Delete > Schedule.

**Close Button**

Closes the window without saving scheduling information.

---

**Related Information**

For information on related windows:

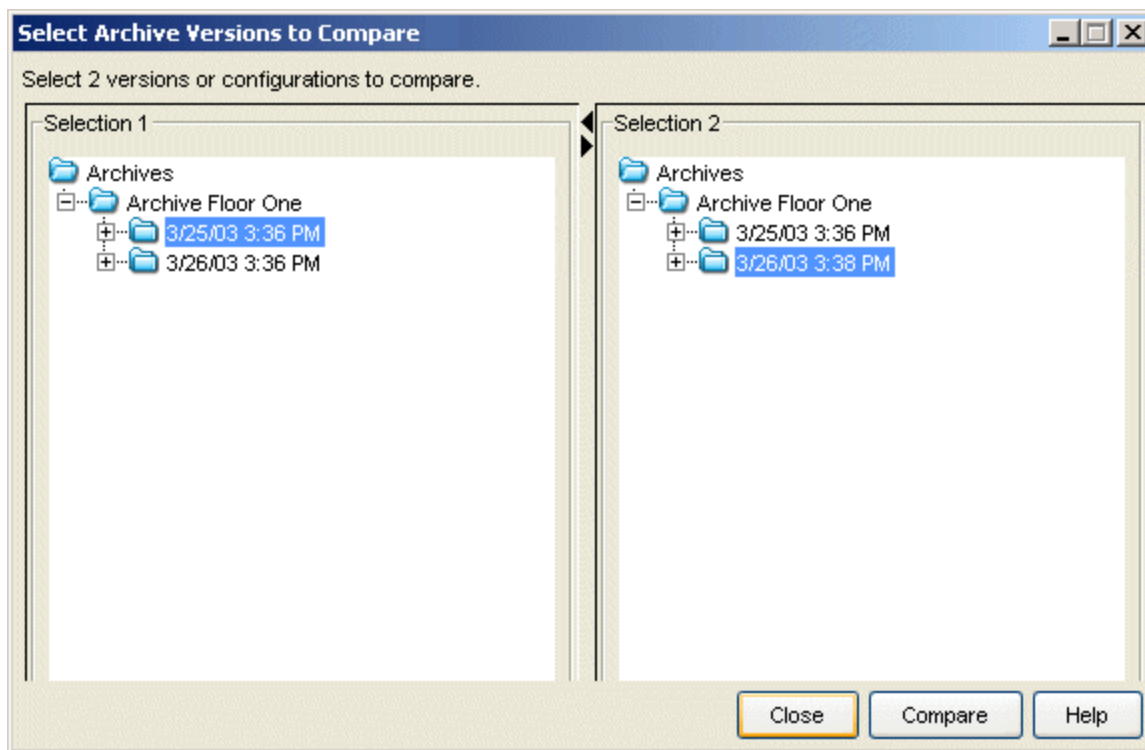
- [Capacity Planning](#)
- [E-Mail Configuration Window](#)



## Select Archive Versions to Compare Window

This window lets you select two archive versions or configurations to compare in the [Compare Archives window](#). It displays two Archive trees (identical to the Archive tree in your Archive Mgmt tab). Use these trees to select the two archive versions or configuration files you wish to compare. You can compare two individual configurations for the same device, or you can compare two different archive versions (although the versions should share common devices).

For information on how to access the window, see [How to Compare Archives](#).



### Selection 1

Expand the folders as necessary to select the first version or configuration you wish to compare.

### Selection 2

Expand the folders as necessary to select the second version or configuration you wish to compare.

### Close Button

Closes the window.

### Compare Button

Performs the comparison and opens the [Compare Archives window](#) where you can view the comparison results.

---

### Related Information



For information on related windows:

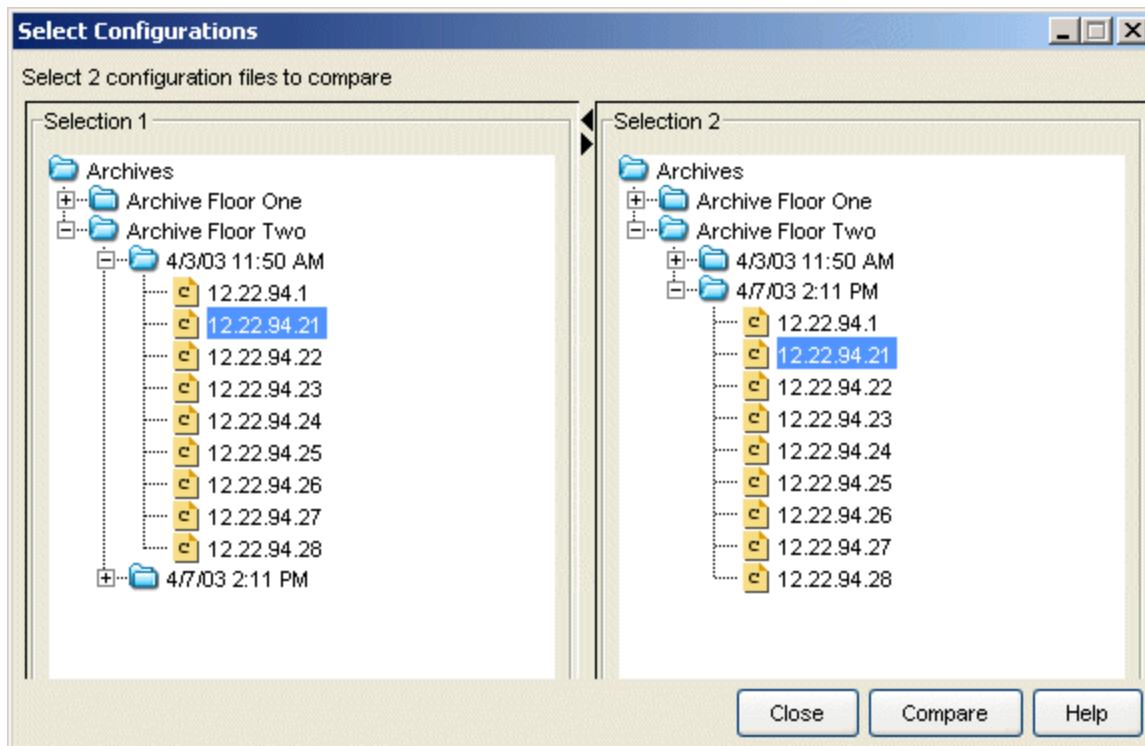
- [Compare Configuration Files Window](#)
- [Configuration File Viewer](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

## Select Configurations Window

This window lets you select two configuration files to compare in the [Compare Configuration Files Window](#). To access the window, select a configuration that includes device configuration data (  or  ) in the Archives Mgmt tab tree or Details View, and select **Tools > Compare Configuration Files**. You can also right-click on a file and select Compare Configuration Files from the menu.



### Selection 1

Expand the folders as necessary to select the configuration file you wish to compare. This file will be displayed in the left panel of the Compare Configuration Files window.

### Selection 2

Expand the folders as necessary to select the second configuration file you wish to compare. This file will be displayed in the right panel of the Compare Configuration Files window.

### Compare Button

Performs the configuration comparison and opens the [Compare Configuration Files window](#) where you can view the comparison results.

---

### Related Information

For information on related windows:

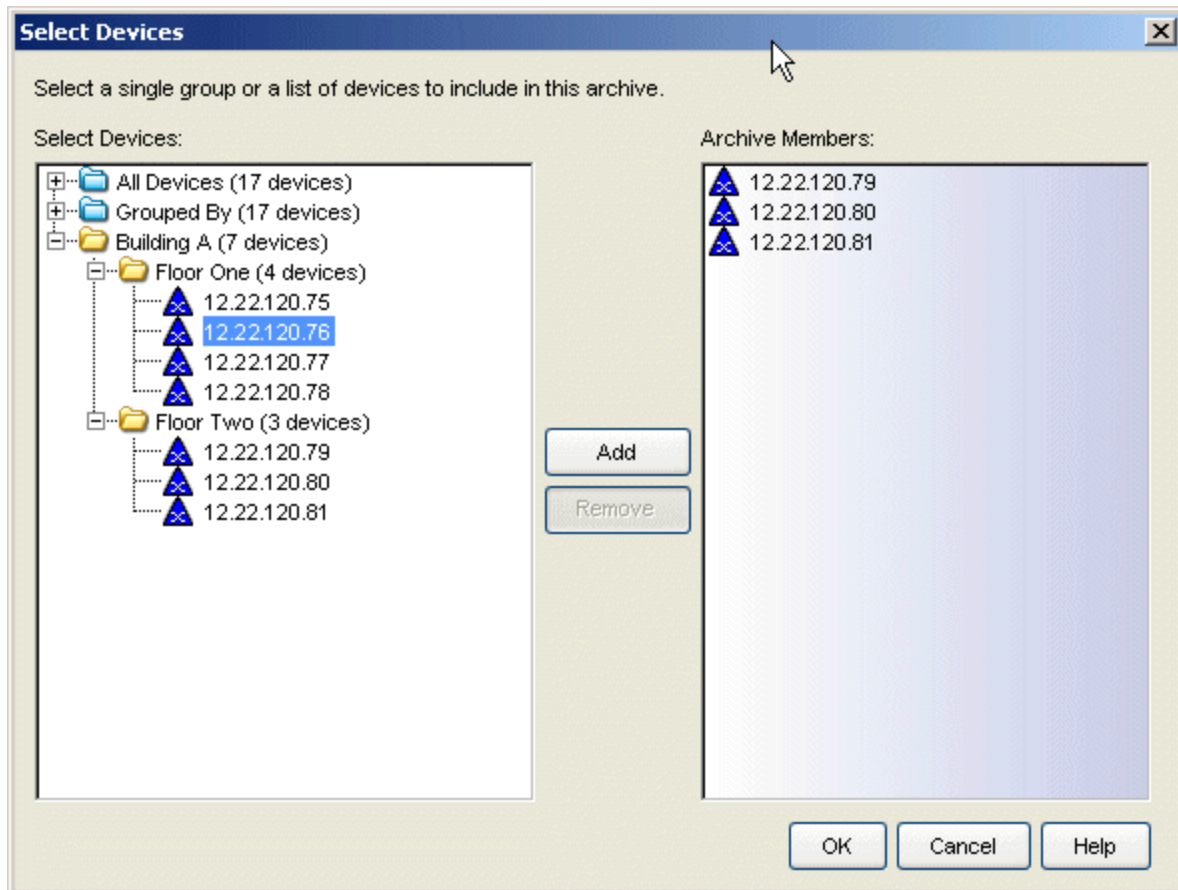
- [Compare Configuration Files Window](#)
- [Configuration File Viewer](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

## Select Devices Window

This window lets you edit the device(s) an archive will be performed on. The current archive members are listed when you open the window. Access the window from the **Edit Devices** button in the archive's [General tab](#).



### Select Devices

Expand the folders and select a single device, multiple devices (using the Control or Shift keys) or a single device group. Click **Add**. The devices will be listed under Archive Members.

### Archive Members

Lists the device(s) or device group the archive will be performed on. To remove a member from the list, select the member and click **Remove**.

### Add Button

Adds the selected device(s) or device group to the Archive Members list.

**Remove Button**

Removes the selected device(s) or device group from the Archive Members list.

**OK Button**

Changes the archive members according to your selections and displays the device(s) in the Archive General tab.

---

**Related Information**

For information on related tabs:

- [General Tab \(Archive\)](#)

For information on related tasks:

- [How to Archive](#)
- [How to Compare Archives](#)

## Set Firmware Server Window

---

Use this window to specify which firmware download server a device will use when performing firmware downloads. You can set the firmware server for a single device, multiple devices, or a device group.

All devices are initially configured to use the mapped file transfer server (as configured in the Services for NetSight Server view of the Suite-Wide Options window) for firmware downloads. By specifying an alternate firmware download server, you can enable a remote device to use a server in its own local network. Performing firmware downloads via a remote server lets you avoid transferring traffic over a WAN. The actual transfer takes place in the local network where the device and the designated server live.

Alternate firmware download servers are configured using the [Alternate Firmware Servers view](#) in the Options window. You must configure your alternate servers prior to using the Set Firmware Server window. For more information, see the section on [Alternate Firmware Servers](#) in How to Set Options.

To access the Set Firmware Server window, select a single device or device group in the left-panel Network Elements tab or multiple devices in a right-panel Details View tab, then select **Tools > Alternate Firmware Server** from the menu bar. You can also right-click a device or device group and select the Alternate Firmware Server option from the menu.



### Server drop-down list

Select the IP address of the firmware download server you would like used for the selected device(s). The drop-down list displays the alternate servers (configured via the [Add Alternate Firmware Server window](#)) that match the file transfer method set for the device(s). All devices are initially configured

to use the mapped file transfer server (as configured in the Services for NetSight Server view of the Suite-Wide Options window) for firmware downloads.

---

### **Related Information**

For information on related windows:

- [Add Alternate Firmware Server Window](#)
- [Alternate Firmware Servers View, Options Window](#)

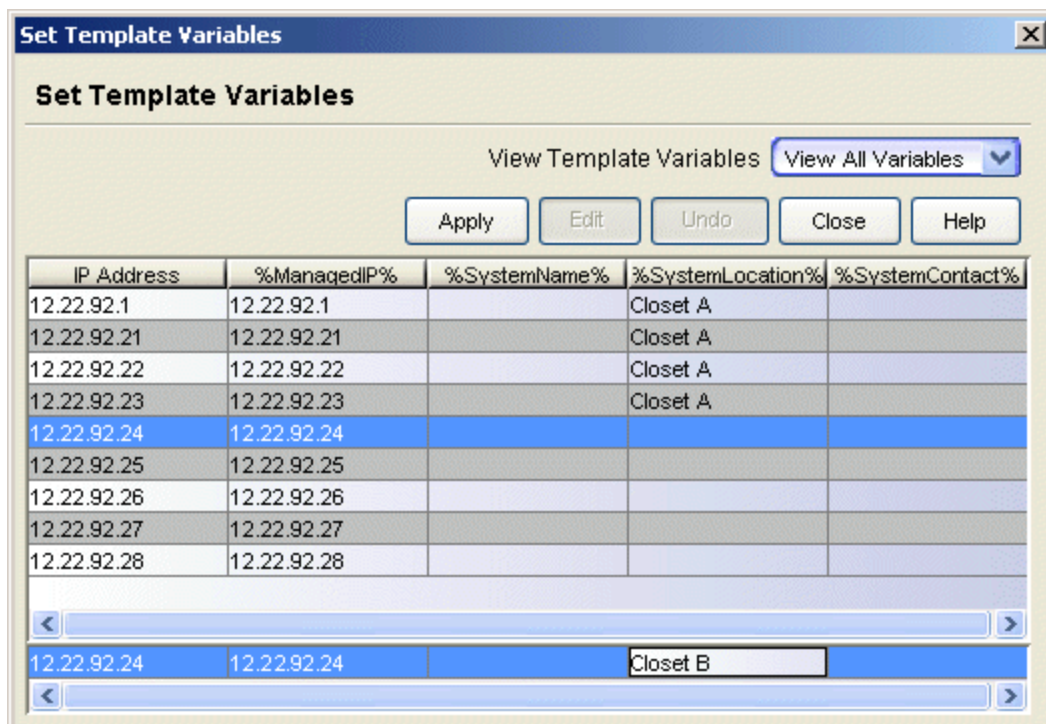


## Set Template Variables Window

The Set Template Variables window allows you to set variable values for multiple devices at one time. Variables are used in configuration templates to substitute for device-specific information. When you download a template configuration to a device, the variables are automatically replaced with the assigned values for that device. For more information, see [How to Create and Download Configuration Templates](#).

**TIP:** You can also set variable values for an individual device on the device's [Configuration Templates tab](#).

To access this window, select any device or device group in the left-panel Network Elements tab and then select **Tools > Set Template Variable Values**, or right-click and select Set Template Variable Values from the menu. You can also access this window by clicking the **Set Template Variables** button in the last window of the [Template Download Wizard](#).



### View Template Variables

Use this drop-down list to control which variables are displayed in the table. You can select a single variable whose value you want to set, or use

the "View All Variables" option to display all variables.

### Table

This table lists your selected devices and their set values for each of your defined template variables. Use the Table Editor to add or modify variable values.

### Table Editor

Use the Table Editor row to add or modify variable values. Select one or more rows in the table and click **Edit**. The Table Editor row appears at the bottom of the table. Select or tab to the desired column (variable) and enter your value. Click **Apply** to set the values.

### Apply Button

After you have edited the variable values, click **Apply** to set the values.

### Edit Button

Select one or more rows in the table and click **Edit** to open the Table Editor. After you have entered the desired variable values, click **Apply** to set the values.

### Undo Button

Use this button to undo the last edit operation you performed.

---

## Related Information

For information on related tabs:

- [Configuration Templates Tab \(Device\)](#)

For information on related tasks:

- [How to Create and Download Configuration Templates](#)

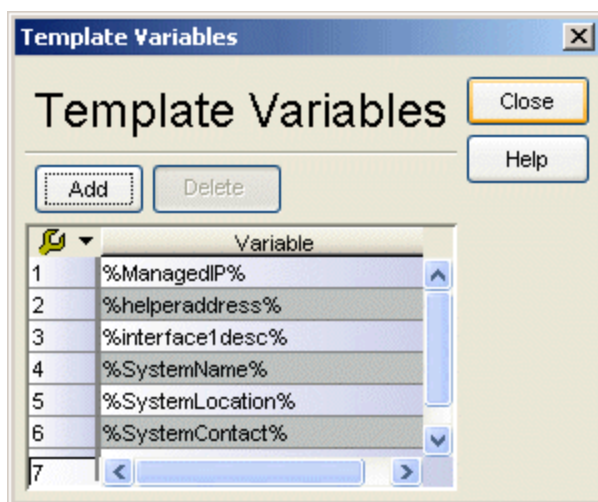
For information on related windows:

- [Edit Configuration Template Window](#)

## Template Variables Window

Use the Template Variables window to define variables for use in configuration templates. Once a variable is defined, you will be able to access it from the drop-down list in the [Edit Configuration Template window](#). You can also view your template variables in the [Template Variables tab](#). For more information, see [How to Create and Download Configuration Templates](#).

Access this window by clicking the **Variables** button in the Edit Configuration Template window.




### Add button

Opens the Add Template Variable window where you can enter a variable name.

### Delete Button

Deletes the selected variable(s).

### Variable

Lists the existing template variables. The %ManagedIP% variable is created automatically by Inventory Manager and cannot be deleted. You can sort the list by clicking the column heading, or use the table tools to find, filter, sort, print, or export the list. Access the Table Tools through a right-mouse click on the column heading or by using the Table Tools  button in the upper left corner of the table.

## Related Information

For information on related tasks:


- [How to Create and Download Configuration Templates](#)

For information on related windows:

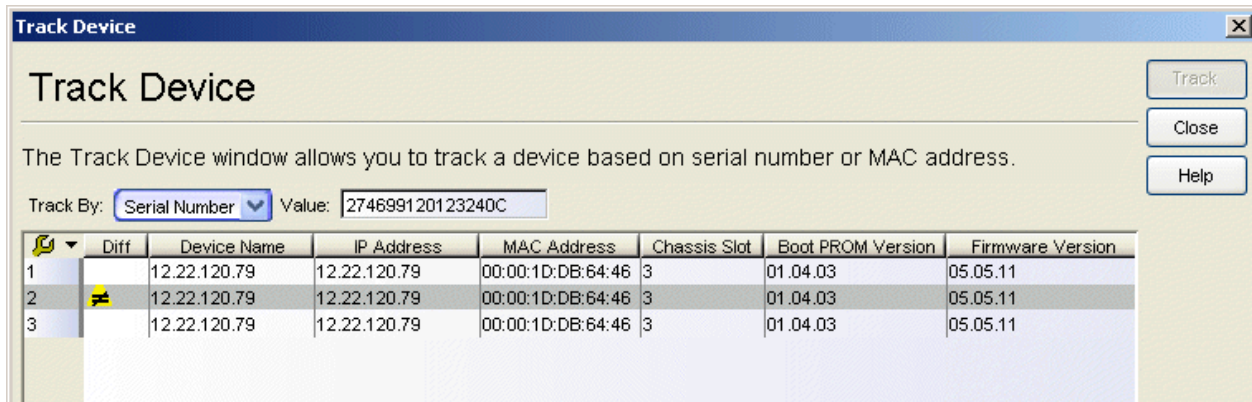
- [Edit Configuration Template Window](#)
- [Set Template Variables Window](#)

## Track Device Window


The Track Device window allows you to track a device based on the device's serial number or MAC address. This allows you to view a history of device attributes, and monitor any changes made to the device. The table entries are based on the device's archived configuration files -- there will be one entry for each saved configuration file.

Use the table options and tools to find, filter, sort, print, and export information in a table and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed). For more information, see the Table Tools Help topic.

To access this window, select a single device in the left-panel Network Elements tree, and select **Tools > Track Device**. When the window opens, the information for that device will be displayed. If you have not performed an archive on that device, the table will be empty and you will see a message that says "No database entries found."



The screenshot shows the 'Track Device' window with a title bar and a close button. Below the title bar, there is a 'Track Device' heading and a 'Track' button. A descriptive text states: 'The Track Device window allows you to track a device based on serial number or MAC address.' Below this, there is a 'Track By:' dropdown menu set to 'Serial Number' and a 'Value:' text box containing '274699120123240C'. To the right of the text box are 'Close' and 'Help' buttons. At the bottom, there is a table with the following data:

	Diff	Device Name	IP Address	MAC Address	Chassis Slot	Boot PROM Version	Firmware Version
1		12.22.120.79	12.22.120.79	00:00:1D:DB:64:46	3	01.04.03	05.05.11
2		12.22.120.79	12.22.120.79	00:00:1D:DB:64:46	3	01.04.03	05.05.11
3		12.22.120.79	12.22.120.79	00:00:1D:DB:64:46	3	01.04.03	05.05.11


### Track By:

Use the drop-down list to select whether you want to search for a device based on serial number or MAC address.

### Value:

Enter the serial number or MAC address, depending on what you selected in the **Track By** field.

**Diff**

A yellow Diff icon  in this column signifies a change has been detected in the device attributes for this configuration and the previous configuration.

**Device Name**

Displays the device display name (IP address, System Name, or Nickname) as configured in the Suite-Wide Data Display Format Options window.

**IP Address**

Displays the device IP address.

**MAC Address**

Media Access Connection (hardware) address of the device.

**Chassis Slot**

The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

**BootPROM Version**

Shows the current version of Boot PROM installed in the device.

**Firmware Version**

Shows the current firmware version installed in the device.

**Serial Number**

A unique number assigned to the device by the manufacturer.

**Device Type**

The device's model number or hardware type.

**Asset Tag**

A unique asset number assigned to the device for inventory tracking purposes.

**CPU**

The name of the device's processor (Central Processing Unit).

**Memory**

The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

**Last Status**

The device's last known connection status (Contact or No Contact) and, therefore, its ability to respond to SNMP requests.

### System Description

Description of the piece of equipment, usually including the model number and firmware revision number. The firmware revision typically displays a revision number, then a date.

### Chassis ID

The ID assigned to the chassis where the device resides.

### Alert Description

Explains the significance of the [Diff icon](#).

### Date

Displays the date and time the configuration was saved.

### Track Button

Searches for device information based on the serial number or MAC address specified in the Track By field.

---

## Related Information

For information on related tabs:

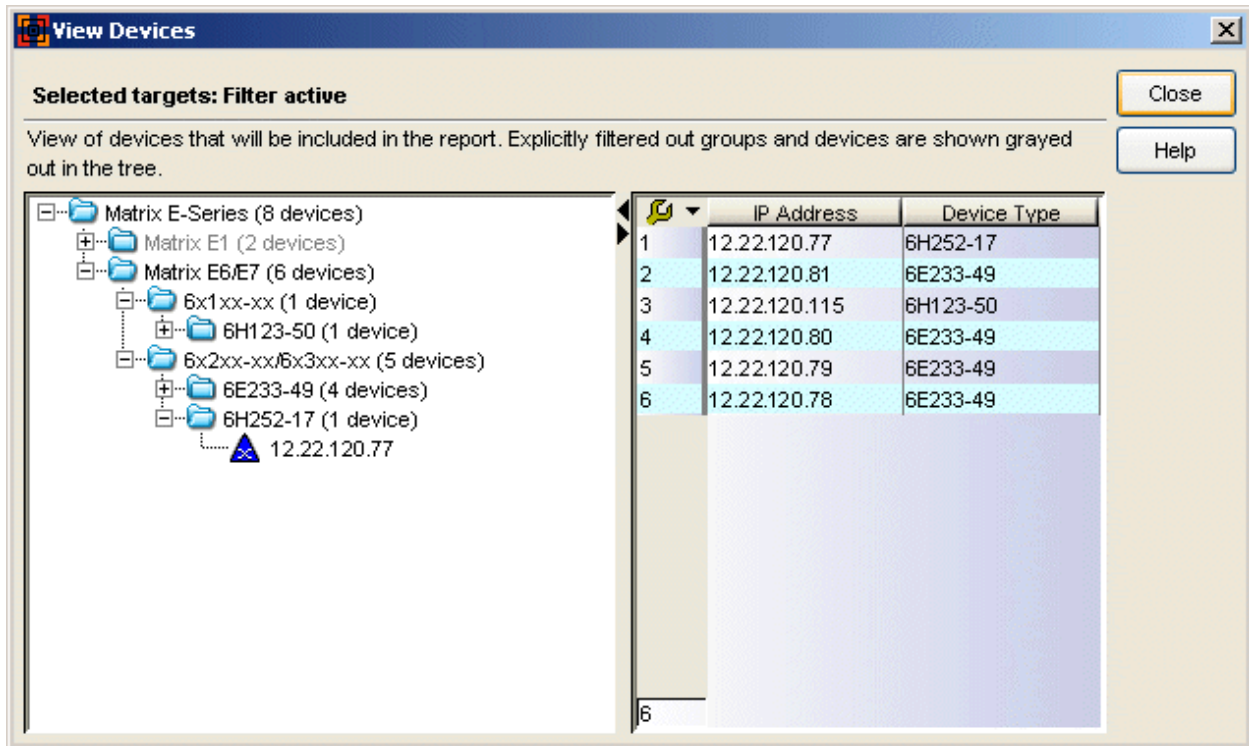
- [General Tab \(Device\)](#)
- [Details View Tab \(Device Group\)](#)

For information on related tasks:

- [How to Track a Device](#)

## View Devices Window

The View Devices window lets you view the groups and devices you have selected for your [Capacity Planning](#) report. The devices are displayed in tree format and are also listed individually in a table. Access this window from the Select Targets window in the Capacity Planning tool by clicking the **View Devices** button.



The screenshot shows the 'View Devices' window with the title bar 'View Devices' and a close button. Below the title bar, it says 'Selected targets: Filter active'. A descriptive text reads: 'View of devices that will be included in the report. Explicitly filtered out groups and devices are shown grayed out in the tree.' There are 'Close' and 'Help' buttons on the right. The main area is split into two panes. The left pane shows a tree view of device groups: 'Matrix E-Series (8 devices)' (expanded), 'Matrix E1 (2 devices)', 'Matrix E6/E7 (6 devices)' (expanded), '6x1xx-xx (1 device)' (grayed out), '6H123-50 (1 device)', '6x2xx-xx/6x3xx-xx (5 devices)' (expanded), '6E233-49 (4 devices)', and '6H252-17 (1 device)' (expanded) with IP address '12.22.120.77'. The right pane is a table with columns 'IP Address' and 'Device Type'. The table contains 6 rows of data:

	IP Address	Device Type
1	12.22.120.77	6H252-17
2	12.22.120.81	6E233-49
3	12.22.120.115	6H123-50
4	12.22.120.80	6E233-49
5	12.22.120.79	6E233-49
6	12.22.120.78	6E233-49

### Tree

Displays your selected devices in hierarchical tree format starting with the top-level device group you have selected. Groups and devices that have been explicitly filtered out (using the [Add Filters](#) window) are shown grayed out in the tree.

### Table

Lists each selected device by its IP address and device type. You can use the Table Tools to find, filter, sort, print, and export information in the table.

## Related Information

For information on related windows:



- [Add Filters Window](#)
- [Capacity Planning](#)

# Troubleshooting

---

This troubleshooting guide provides a list of items to check when certain Inventory Manager functionality is failing to perform correctly. Locate a problem in the left column and then review the troubleshooting steps in the right column.

<b>Problem</b>	<b>Troubleshooting Steps</b>
<b>Configuration Save Fails</b>	<p>Verify that the appropriate configuration MIB is being used to perform the configuration save:</p> <ol style="list-style-type: none"><li>1. Select the device in the left-panel Networks Element tab.</li><li>2. Select the right-panel <a href="#">Image Information tab</a>.</li><li>3. In the MIB Overrides section, verify that the Configuration MIB listed as supported by this device is the desired MIB. Initially, Controlled by Device Type is displayed in this field, meaning that Inventory Manager will use the MIB specified in the Configuration MIB field on the <a href="#">General Tab (Device Type)</a>. If you would like to override the Device Type MIB, use the drop-down list here to select the desired MIB and click Save to save the change.</li></ol>
<b>Firmware Download Fails</b>	<p>Verify that the appropriate firmware download MIB is being used to perform the download:</p> <ol style="list-style-type: none"><li>1. Select the device in the left-panel Networks Element tab.</li><li>2. Select the right-panel <a href="#">Image Information tab</a>.</li><li>3. In the MIB Overrides section, verify that the Firmware Download MIB listed as supported by this device is the desired MIB. Initially, Controlled by Device Type is displayed in this field, meaning that Inventory Manager will use the MIB specified in the Firmware Download MIB field on the <a href="#">General Tab (Device Type)</a>. If you would like to override the Device Type MIB, use the drop-down list here to select the desired MIB and click Save to save the change.</li></ol>