



# FortiNAC

FortiNac Control Manager

**Version 8.3**

**7/30/2018**

**FORTINET®**

---

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<http://kb.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING AND CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com/>

FORTIGUARD CENTER

<https://fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>



Monday, July 30, 2018

FortiNAC Control Manager

49-830-503680-20170730

# Contents

---

<b>Chapter 1: Overview</b> .....	<b>1</b>
What's New In This Version .....	1
Key Features .....	3
Getting Additional Help .....	5
Access The FortiNac Control Manager .....	7
License Types And Usage .....	8
Licensed Features .....	8
License Counts .....	8
Licensing Events And Alarms .....	9
Licensing In A FortiNac Control Manager Environment .....	10
Manage Guests In A FortiNac Control Manager Environment .....	11
Manage Hosts In A FortiNac Control Manager Environment .....	13
Icon Key .....	14
<b>Chapter 2: Landing Page</b> .....	<b>19</b>
Menus .....	20
Bookmarks .....	20
Hosts .....	20
Users .....	20
Logs .....	21
Policy .....	21
System .....	21
Help .....	21
Manage Bookmarks .....	22
Admin User Interface Settings .....	24
Legal .....	25
Dashboard .....	25
Add A Panel To The Dashboard .....	34
License Information Panel .....	36
Licenses In Use .....	37

Licenses In Use Detail .....	37
Locate View .....	39
All Search Results .....	40
Locate Devices .....	42
Device Search Results .....	44
Locate Hosts/Users .....	49
Host/User Search Results .....	53
Navigation .....	54
Menu Bar .....	54
Title Bar .....	54
Table Views .....	55
Tabbed Views .....	56
Tree Views .....	57
Field Level Help .....	58
Filters .....	59
<b>Chapter 3: Settings .....</b>	<b>63</b>
Authentication .....	66
Authentication Directories .....	67
Authenticate Using A Domain Name .....	67
Authenticate Using Domain Names And Multiple Directories .....	68
Identification .....	98
Device Types .....	99
Device Type In Use .....	102
Vendor OUIs .....	103
Device Registration After Vendor OUI Database Update .....	110
Network Control Manager .....	111
Server Synchronization .....	111
Security Settings .....	115
Certificate Management .....	116
Obtain a Valid SSL Certificate from a Certificate Authority (CA) .....	117
UI Method: Upload the Certificate Received from the CA .....	121
View the Details and Private Key Information for a Certificate .....	122
System Communication .....	124
Email Settings .....	125

Log Receivers .....	127
Mobile Providers .....	130
SNMP .....	134
Register Hosts And Users With SNMPv3 Traps .....	138
Network Sentry Configuration Requirements .....	138
Trap Sender Configuration Requirements .....	140
Hosts .....	140
Users .....	141
Proxy Settings .....	143
System Management .....	145
Database Archive .....	147
Database Backup/Restore .....	150
High Availability .....	153
License Management .....	156
Modify Time Settings .....	161
Power Management .....	163
Backup To Remote Server .....	165
Configure The Remote Backup Destination .....	166
System Backups .....	170
Updates .....	172
Agent Packages .....	173
Operating System Updates .....	177
System Update .....	180
<b>Chapter 4: Device Profiler .....</b>	<b>189</b>
Device Profiling Process .....	190
Device Profiling Rules .....	192
Manage Device Profiling Rules .....	193
Device Profiling Rules - Best Practices .....	197
Add Or Modify Device Profiling Rule .....	199
Delete A Device Profiling Rule .....	206
Copy A Device Profiling Rule .....	206
Evaluate Rogue Hosts With Device Profiling Rules .....	207
Administrative User Profiles For Device Managers .....	208
Add A Device Manager Admin Profile .....	209

Add An Administrative User For Device Profiler .....	212
Device Profiler Events And Alarms .....	217
<b>Chapter 5: Admin Profiles And Permissions .....</b>	<b>219</b>
Default Admin Profiles .....	222
Permissions List .....	230
Modify Admin Profiles .....	239
Modify Admin Profiles for Administrator Users .....	241
Delete An Admin Profile .....	242
Copy Admin Profiles .....	242
Add An Admin Profile .....	243
Admin Profile Field Definitions .....	245
Admin Profile Mappings .....	252
Admin Profile Mappings Process .....	254
Add/Modify An Admin Profile Mapping .....	258
Delete An Admin Profile Map .....	258
Administrative User Profiles For Guest Manager .....	258
Add A Guest Manager Admin User Profile .....	260
Add A Kiosk Admin Profile .....	263
Add A Guest Self Registration Admin Profile .....	266
Printer Settings For Guest Contractor Badges .....	268
<b>Chapter 6: Admin Users .....</b>	<b>271</b>
Add Administrative Users .....	274
Modify an Admin User .....	277
Delete An Admin User .....	278
Copy An Admin User .....	278
Modify a User's Admin Profile .....	279
User Theme .....	280
Limit Admin Access With Groups .....	282
Add Admin Users To Groups .....	285
Admin User Group Membership .....	287
Configure Secure Mode For Admin Users .....	289
<b>Chapter 7: Import And Export Data .....</b>	<b>291</b>
Import Archived Data .....	293
Import Hosts, Users Or Devices .....	294

---

Create An Import File .....	294
Sample Host, Adapter, User or Device Import Files .....	300
Import Hosts, Users, Devices or IP Phones From A .csv File .....	301
Import Host, User And Adapter Data From A Previous Version .....	303
Import Admin Users .....	304
Create An Import File .....	304
Sample Import File .....	306
Import IP Ranges .....	307
Export Data .....	308
<b>Chapter 8: Hosts, Adapters, and Applications .....</b>	<b>311</b>
Configure Table Columns And Tool-tips .....	313
Search And Filter Options For Hosts, Adapters, Users or Applications .....	317
Wild Cards .....	317
Quick Search .....	317
Custom Filter .....	319
Host View .....	322
Host View Navigation, Menus, Options And Buttons .....	324
Host View And Search Field Definitions .....	327
Host Drill-Down .....	334
Host Properties .....	335
Host Health And Scanning .....	339
Modify a Host .....	344
Delete A Host .....	349
Enable Or Disable Hosts .....	350
Add IP Phones .....	351
Policy Details .....	352
Add Hosts To Groups .....	358
Host Group Membership .....	361
Register A Host As A Device .....	364
Set Host Expiration Date .....	366
Adapter View .....	368
Adapter View Navigation, Menus, Options And Buttons .....	369
Adapter View And Search Field Definitions .....	372
Adapter Properties .....	373

---

Adapter Device Identity .....	375
Enable Or Disable An Adapter .....	377
Modify An Adapter .....	377
Application View .....	378
Show the Host(s) Containing an Application .....	380
Set the Threat Override for an Application .....	380
Aging Out Host Or User Records .....	381
Export Data .....	383
<b>Chapter 9: User View .....</b>	<b>385</b>
User View Navigation, Menus, Options And Buttons .....	388
Configure Table Columns And Tool-tips .....	390
Search And Filter Options For Hosts, Adapters, Users, or Applications .....	394
Wild Cards .....	394
Quick Search .....	394
Custom Filter .....	396
User View And Search Field Definitions .....	400
User Drill-down .....	402
User Properties .....	404
Modify A User .....	408
Delete A User .....	411
Add Users To Groups .....	412
User Group Membership .....	414
Policy Details .....	416
Guest User Account Details .....	422
Set User Expiration Date .....	425
Guest/Contractor Templates .....	429
Guest Account Types Or Visitor Types .....	433
Create Guest/Contractor Templates .....	434
Assign An Endpoint Compliance Policy To A Guest .....	443
Modify Templates .....	445
Copy Templates .....	445
Delete Templates .....	445
<b>Chapter 10: Admin Auditing .....</b>	<b>446</b>
Configuration .....	446

---

Accessing the Admin Auditing Log .....	446
<b>Chapter 11: Event Management .....</b>	<b>451</b>
Enable And Disable Events .....	454
Events For The System .....	454
Events For A Specific Group .....	454
Event Thresholds .....	455
Log Events To An External Log Host .....	458
External Log Host Syslog Format .....	460
External Log Host SNMP Trap Format .....	461
External Log Host CEF (Common Event Format) .....	462
View Events Currently Mapped To Alarms .....	465
Events View .....	466
Event Notes .....	468
Network Sentry Events And Alarms List .....	469
<b>Chapter 12: Alarms View .....</b>	<b>489</b>
Show/Hide Alarm Details .....	491
Map Events To Alarms .....	493
Add or Modify Alarm Mapping .....	497
Bulk Modify Alarm Mappings .....	502
Delete Alarm Mapping .....	503
<b>Chapter 13: Policies .....</b>	<b>505</b>
Policy Assignment .....	507
User/Host Profiles .....	511
Add/Modify A User Or Host Profile .....	514
User/Host Profile Filter Example .....	517
User/Host Profile Example .....	520
User/Host Profiles In Use .....	524
Delete A User/Host Profile .....	524
Endpoint Compliance Policies .....	525
Endpoint Compliance Implementation .....	529
Endpoint Compliance Policy .....	529
Events & Alarms .....	530
Scan Hosts Without Enforcing Remediation - Optional .....	530
Delayed Remediation For Scanned Hosts - Optional .....	530

---

Authentication .....	531
Monitoring .....	531
Testing .....	531
Add/Modify An Endpoint Compliance Policy .....	532
Delete An Endpoint Compliance Policy .....	533
Determining Host Operating System .....	534
Endpoint Compliance Configurations .....	536
Add/Modify An Endpoint Compliance Configuration .....	539
Endpoint Compliance Configurations In Use .....	544
Delete An Endpoint Compliance Configuration .....	544
Scans .....	545
Scan On Connect .....	550
Scan Hosts Without Enforcing Remediation .....	551
Delayed Remediation For Scanned Hosts .....	553
Add/Modify A Scan .....	556
Monitor Custom Scans .....	565
Reset Default Anti-Virus Or Anti-Spyware Values .....	568
Delete A Scan .....	569
Scans In Use .....	569
Schedule A Scan .....	570
Custom Scans Overview .....	578
Create Custom Scans For Windows .....	579
Create Custom Scans For Mac-OS-X .....	594
Create Custom Scans for Linux .....	600
Custom Scans Severity Level .....	606
Custom Scans - Use Case .....	608
<b>Chapter 14: Role Management .....</b>	<b>609</b>
Assigning Roles .....	610
Set Up Role Management .....	614
Roles .....	615
Add A Role .....	618
Modify Or Delete Role From Database .....	619
Role In Use .....	620

---

<b>Chapter 15: Guest Manager</b> .....	<b>623</b>
Guest Manager Implementation .....	624
Guest/Contractor Templates .....	626
Guest Account Types Or Visitor Types .....	631
Create Guest/Contractor Templates .....	632
Assign An Endpoint Compliance Policy To A Guest .....	641
Modify Templates .....	643
Copy Templates .....	643
Delete Templates .....	643
Administrative User Profiles For Guest Manager .....	644
Add A Guest Manager Admin User Profile .....	645
Add A Kiosk Admin Profile .....	648
Add A Guest Self Registration Admin Profile .....	651
Administrative Users For Guest Manager .....	653
Add An Admin User For Guest Manager .....	653
Printer Settings For Guest Contractor Badges .....	656
Guest Manager Events And Alarms .....	657
Use Guest Manager As A Sponsor .....	658
Log Into Guest Manager As A Sponsor .....	658
Guest Or Contractor Accounts .....	660
Create Single Guest Or Contractor Accounts .....	663
Create Bulk Or Multiple Accounts .....	667
Bulk Guest Account Import File .....	668
Provide Account Information To Guest Or Contractor .....	671
Conference Accounts .....	673
Create Conference Accounts .....	673
Guest Account Details .....	676
Guest Or Contractor Login .....	679
Login Procedure .....	679
Manage Guests In A FortiNac Control Manager Environment .....	680
<b>Chapter 16: Groups View</b> .....	<b>681</b>
Add Groups .....	684
Copy A Group .....	692
Delete A Group .....	692

Limit User Access With Groups .....	693
Modify A Group .....	695
Groups - Group Membership .....	696
Show Group Members .....	697
Group In Use .....	698
Aging Hosts In A Group .....	699
System Groups .....	700
Customer Defined Groups .....	703
<b>Chapter 17: Scheduler View .....</b>	<b>705</b>
Add A Task Within The Scheduler .....	707
Copy a Task .....	711
Modify A Task .....	712
Delete A Task .....	712
Run Task Now .....	712
<b>Chapter 17: Send SMS Messages .....</b>	<b>713</b>
Implementation .....	713
<b>Chapter 18: Scan Management .....</b>	<b>717</b>
Manage Scans .....	717
Copy A Scan .....	719
<b>Chapter 19: High Availability Overview .....</b>	<b>721</b>
HA Configuration Using A Shared IP Address (Layer 2) .....	725
Network Infrastructure .....	725
Appliance Configuration .....	725
HA Configuration With Servers On Different Subnets (Layer 3) .....	727
Network Infrastructure .....	727
Appliance Configuration .....	728
Connectivity Configuration .....	729
Network Sentry Primary And Secondary Configuration .....	730
Update Software In A High Availability Environment .....	733
High Availability Concepts .....	734
Startup High Availability .....	734
Monitor High Availability .....	735
Control Sequence .....	737
Recovery .....	739

Stop The Primary Server .....	741
Troubleshooting Tips .....	742
Determine Which Appliance Has The Shared IP .....	742
Determine Appliance Status .....	742
Confirm Database Replication .....	743
Verify License Key Configuration .....	743
<b>Appendix A: Scan Parameters .....</b>	<b>745</b>
Anti-Spyware Parameters .....	746
Anti-Virus Parameters - Windows .....	751
Anti-Virus Parameters - Mac OS X .....	756
Operating System Parameters - Windows .....	758



## Chapter 1: Overview

The FortiNac Control Manager simplifies the task of managing multiple FortiNac Server or FortiNac Control Server appliances, by acting as a central management node in the network. This central server allows you to take advantage of Network Sentry's features across the network.

The FortiNac Control Manager is designed for configurations that consist of two or more FortiNac Server or FortiNac Control Server appliances. The web-based interface provides an interactive management console that provides enterprise-wide communication to multiple FortiNac Server or FortiNac Control Server appliances from a central server. Instead of accessing each FortiNac Server or FortiNac Control Server appliance separately to search for user or data records, you can search and manage from one console.

### What's New In This Version

Following are new features for Version 8.3 of the FortiNac Control Manager. For information on features added between your current version and this, refer to prior versions of the Release Notes.

Feature	Description														
<p><b>User Interface</b></p>	<p>The FortiNac Control Manager views and menus have been updated to align with Network Sentry. Additional views have been added to enable the Administrator to easily manage multiple Network Sentry Servers.</p> <p>The following views have been added to the FortiNac Control Manager:</p> <table border="0" data-bbox="516 457 1307 703"> <tr> <td>Settings</td> <td>Endpoint Compliance Policies</td> </tr> <tr> <td>Admin Profiles</td> <td>Endpoint Compliance Configuration</td> </tr> <tr> <td>Device Profiling Rules</td> <td>Endpoint Compliance Scans</td> </tr> <tr> <td>User/Host Profiles</td> <td>Dashboard - Alarms Panel</td> </tr> </table> <p>The following menu and option have been removed from the FortiNac Control Manager:</p> <p>NS Servers &gt; Server List</p> <div data-bbox="508 919 1421 993" style="border: 1px solid black; background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> The Host Propagation option has been moved to the Settings &gt; Network Control Manager &gt; Server Synchronization View.</p> </div> <p>The following menus have been replaced with the Settings view:</p> <table border="0" data-bbox="516 1119 1339 1375"> <tr> <td>System &gt; High Availability Configuration</td> <td>System &gt; Properties &gt; Control Panel</td> </tr> <tr> <td>System &gt; License Management</td> <td>System &gt; Properties &gt; SNMP Server</td> </tr> <tr> <td>System &gt; Services</td> <td>System &gt; Updates &gt; Download Settings</td> </tr> </table>	Settings	Endpoint Compliance Policies	Admin Profiles	Endpoint Compliance Configuration	Device Profiling Rules	Endpoint Compliance Scans	User/Host Profiles	Dashboard - Alarms Panel	System > High Availability Configuration	System > Properties > Control Panel	System > License Management	System > Properties > SNMP Server	System > Services	System > Updates > Download Settings
Settings	Endpoint Compliance Policies														
Admin Profiles	Endpoint Compliance Configuration														
Device Profiling Rules	Endpoint Compliance Scans														
User/Host Profiles	Dashboard - Alarms Panel														
System > High Availability Configuration	System > Properties > Control Panel														
System > License Management	System > Properties > SNMP Server														
System > Services	System > Updates > Download Settings														

Feature	Description														
	<p>The following menu and option have been removed from the FortiNac Control Manager and replaced with the Users &gt; User View:</p> <p>Users &gt; User License</p> <p>The following menus have been added to the FortiNac Control Manager:</p> <table border="0" data-bbox="444 485 1256 932"> <tr> <td>Users &gt; Admin Profiles</td> <td>Logs &gt; Event Management</td> </tr> <tr> <td>Users &gt; Guest Templates</td> <td>Policy &gt; Policy Configuration</td> </tr> <tr> <td>Hosts &gt; Device Profiling Rules</td> <td>Policy &gt; Roles</td> </tr> <tr> <td>Logs &gt; Admin Auditing</td> <td>System &gt; Groups</td> </tr> <tr> <td>Logs &gt; Alarms</td> <td>System &gt; Scheduler</td> </tr> <tr> <td>Logs &gt; Events</td> <td>System &gt; Settings</td> </tr> <tr> <td>Logs &gt; Event to Alarm Mappings</td> <td></td> </tr> </table>	Users > Admin Profiles	Logs > Event Management	Users > Guest Templates	Policy > Policy Configuration	Hosts > Device Profiling Rules	Policy > Roles	Logs > Admin Auditing	System > Groups	Logs > Alarms	System > Scheduler	Logs > Events	System > Settings	Logs > Event to Alarm Mappings	
Users > Admin Profiles	Logs > Event Management														
Users > Guest Templates	Policy > Policy Configuration														
Hosts > Device Profiling Rules	Policy > Roles														
Logs > Admin Auditing	System > Groups														
Logs > Alarms	System > Scheduler														
Logs > Events	System > Settings														
Logs > Event to Alarm Mappings															
<b>Global Object Synchronization</b>	<p>Global Object Synchronization has been added to enable automatic synchronization of the Network Sentry Server(s) with the FortiNac Control Manager. Views that include global information display the Global column to indicate which information is synchronized with the Network Sentry Server(s). When enabled, automatic synchronization occurs once per minute. See <b>Server Synchronization</b> on page 111.</p>														
<b>Import button</b>	<p>Selected views allow you to import information from the Network Sentry Server(s) to the FortiNac Control Manager. This eliminates the need to manually enter the information on the FortiNac Control Manager. When it is imported to the FortiNac Control Manager, the information is global.</p>														

## Key Features

- **Global User Identity Database**—Data records are maintained on each user accessing the network.
- **Scalability**—Manage an extensive number of FortiNac Servers from a single location.
- **Global Find**—Quickly locate devices and users anywhere in the network. This includes user information such as the MAC address, location, and the port where the user is connected. Perform searches by IP address to resolve the IP address to a specific user or device.
- **Seamless Network-wide Registration**—Users register once and are tracked in the enterprise identity database as they move freely to other managed locations within the network.

- **Global Version Control**—Manage version control on all Network Sentry appliances within the network, from a single management device.
- **Global License Management**—Licenses are shared across FortiNac Servers.
- **Global Scan Management**—Scans can be created and copied across FortiNac Server or FortiNac Control Server appliances. You can configure network scans or sets of rules that are used to scan hosts for compliance. Scans are included in Endpoint Compliance Configurations that are paired with User/Host Profiles, which form Endpoint Compliance Policies.
- **Global Synchronization**—Enables automatic synchronization of the Network Sentry Server(s) with the FortiNac Control Manager. Views that include global information display the Global column to indicate which information is synchronized with the Network Sentry Server(s). When enabled, automatic synchronization occurs once per minute.
- **Import button**—Allows you to import information from the Network Sentry Server(s) to the FortiNac Control Manager. This eliminates the need to manually enter the information on the FortiNac Control Manager. When it is imported to the FortiNac Control Manager, the information is global.

## Getting Additional Help

You can use any of the following resources for additional help.

### **Manuals**

PDF versions of *Network Sentry Administration and Operation*, the *FortiNac Control Manager Guide* and the *Appliance Installation Guide* are located on your Network Sentry appliance in the following directory:

```
/bsc/campusMgr/ui/runTime/docs/pdfs
```

These manuals can also be downloaded to your PC from the Configuration Wizard as follows:

1. Bring up a web browser and point it to the IP Address of the FortiNac Server, FortiNac Control Server or FortiNac Control Manager. Use one of the following URLs:

```
http://<Host IP Address>:8080/configWizard
```

```
http://<Host Name of the appliance>:8080/configWizard
```

2. Enter the **User Name** and **Password**. Click **OK**.
3. Click **OK** on the License Key screen.
4. The Download Documentation wizard is displayed.
5. Download the documentation needed to configure and administer the product. These files are in PDF format and require a PDF viewer to read them. Click the **Download** button to save the files, then click **OK**.
6. You can also download the latest FortiNAC documentation from the Fortinet Documentation Library: <https://docs.fortinet.com/fortinac>.

### **Online Help**

Open the online Help system and look for the information you need.

**Context-sensitive Help**—Click **Help > Current View** on any window in Network Sentry to open the topic for that window.

**Table of Contents**—Click **Help > Current View** on any window. The online Help TOC opens in a Navigation Pane on the left. Navigate through the TOC books and pages to find the information you need. When you click a topic page, it opens.

**Search feature**—Click **Help > Current View** on any window. Click **Search** at the top right side of the Help window. Enter one or more keywords in the field and click the icon. Links to topics containing those keywords are listed in the main help window. When you click a topic link, that topic displays in the workspace. Use quotation marks around multiple words for an exact match search, for example, "Port Properties".

**Glossary**—Click **Help > Current View** on any window. Click **Glossary** at the top of the Navigation Pane on the left side of the Help window. This opens the Help glossary. Click any of the terms in the glossary to see a definition.

**Browse Arrows**—Arrows located on the top right side of the Help window allow you to scroll through topics in order based on either the Table of Contents or the Glossary depending on which tab is displayed.

### **Resource Center**

Log into the Resource Center on our web site. Using the tabs, you can:

- Search the Knowledge Base (by topic or search string)
- Access Product documentation, Release Notes and How-To documents
- Create a case to inform Fortinet about product issues or feature requests
- Download software updates
- Participate in our User Forum
- View open and closed cases

Click on the Resource Center Link at the top of the page on our web-site at <http://www.bradfordnetworks.com>.

### **Customer Support**

To register Fortinet products and for customer and technical support visit the Fortinet Support website.

Email: [support@fortinet.com](mailto:support@fortinet.com)

### **Documentation Feedback**

To report an error or omission in our documentation, e-mail us at:

[techdoc@fortinet.com](mailto:techdoc@fortinet.com)

## Access The FortiNac Control Manager

Access the FortiNac Control Manager through a web browser interface.

1. Enter one of the following URLs in the Address field of the browser window:

`https://<Host Name>:8443/`

or

`http://<Host Name>:8080/`

**Note:** There are no spaces in the entry.

`<Host Name>` is the name of the Network Sentry appliance. You can substitute the IP address for the `<Host Name>`.

2. Login as an Administrative user.
3. The End User License Agreement appears the first time you log in. Click to accept the terms. Click Disagree to return to the Login dialog.
4. You can add FortiNac Control Manager Administrative user accounts as needed. See **Add Administrative Users** on page 274 for instructions.

**Important:** Any Administrator user account that you add to the FortiNac Control Manager must also be created on the FortiNac Server or FortiNac Control Server appliance where the user will have access.

If the Administrator user account does not exist on the FortiNac Server or FortiNac Control Server appliance, the user will not have access to that particular appliance.

## License Types And Usage

The license key installed on your Network Sentry appliance controls both the feature set that is enabled and the number of hosts, users and devices that can be managed by Network Sentry.

### Licensed Features

**High Availability**—Enables the redundant server feature which allows a second Network Sentry server to take over if the primary server has failed.

**Integrated RADIUS**—Enables the integrated RADIUS server which allows you to do authentication in an 802.1x environment without needing an external RADIUS server.

**Device Profiler**—Enables the Device Profiler feature which allows you to manage and categorize rogue devices as they connect to your network by comparing them to pre-established rules or device profiles.

**Guest Manager**—Enables the Guest Manager feature which allows you to create guest/contractor accounts and delegate guest management to administrative users.

**Endpoint Compliance**—Enables the Security Policy feature which allows you to scan end-stations and ensure that they are compliant with your network policies.

**Integration Suite**—Enables third party integration which allows you to receive SNMP traps and Syslog information from third party vendors with devices on the network.

**Wireless Only**—This is provided as a solution for organizations that use only wireless devices on their network. Using the Quick Start feature you can configure HP MSM and Ruckus Controllers and Xirrus Arrays. Other wireless devices and up to five wired devices can be added using the Network Devices View. This license disables the Discovery feature used to scan the network for devices within specified IP address ranges and allows only five wired devices. All devices must be added manually.

### License Counts

**Concurrent Licenses**—These licenses are based on the total number of concurrent connections to your network that are managed by Network Sentry. There may be parts of your network that are not managed by Network Sentry.

This count includes hosts, servers or devices that are online on your network at any given time. When a host, server or device disconnects from the network, the license is released and can be used for another connection. For example, you may have 1000 hosts in your database but if only 100 are connected, then only 100 licenses are used.

License usage information is displayed on the **Dashboard** on page 25 and **License Management** on page 156.

## Licensing Events And Alarms

When the number of licenses used reaches 75% of total licenses an event is generated and an alarm is triggered to warn you. When the number of licenses used reaches 100% of total licenses another event is generated and an alarm is triggered. These percentages are default values. Modify thresholds for these events under Event Management on the Thresholds tab via the Network Sentry server user interface.

Administrators must monitor the Alarm View, the Alarm panel on the dashboard or modify these alarms such that the alarms send a notification to administrators as they occur.

Event	Definition
<b>Maximum Concurrent Connections Warning</b>	Concurrent licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Maximum Concurrent Connections Critical</b>	Concurrent licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
<b>Maximum Concurrent Connections Exceeded</b>	Concurrent licenses in use has reached 100% of total licenses.

Licenses are not released until users, hosts, devices or guests are disconnected from the network.

## Licensing In A FortiNac Control Manager Environment

### **Licensed Features**

In a FortiNac Control Manager environment, each appliance has its own license key that works in combination with the license on the FortiNac Control Manager. Licensed features, such as Device Profiler, Integration Suite, Guest Manager and Endpoint Compliance, can be enabled for all managed appliances by including the feature in the license key for the FortiNac Control Manager. To enable a licensed feature on a single appliance, the feature must be included in the license key for that appliance, but must not be included in the FortiNac Control Manager license key.

### **License Totals**

License counts are shared across all managed Network Sentry appliances, but the maximum number of licenses is controlled by the FortiNac Control Manager. For example, if the total number of Concurrent Connection licenses on the FortiNac Control Manager is 1000, any of the managed appliances can use licenses from that pool, until all 1000 have been consumed. Appliance A may use 200 and appliance B may use 150, leaving 650 available. Dashboards for all appliances including the FortiNac Control Manager would display the following: Total Licenses - 1000, Licenses In Use - 350, Licenses Available 650. Total licenses available and total licenses used are counted by the FortiNac Control Manager and are displayed on the Dashboard of all appliances.

Any number of licenses can be used on any managed appliance as long as total for all combined does not exceed the 1000 licenses configured on the FortiNac Control Manager. This affects Concurrent Connection licenses.

### **License Accounting For Users And Hosts That Move On The Network**

When users and their corresponding hosts move from one part of the network to another the Network Sentry appliance managing their network access may change. For example, if the switches on the first floor are managed by Network Sentry appliance A and the switches on the second floor are managed by Network Sentry appliance B, then network access control changes from Appliance A to Appliance B when a laptop is moved from the first floor to the second floor.

Hosts consume licenses when they are connected to the network. When a host is moved the license is released when the host disconnects. The same host consumes a license the next time it connects to the network regardless of where it connects.

### **License Accounting For Devices That Move On The Network**

When devices are moved from one part of the network to another the Network Sentry appliance managing their network access may change. If moving the device causes it to be managed by a different Network Sentry appliance, one license is released on the original appliance when the device disconnects from the network and then a new license is used when the device reconnects to the network. The device is included in the databases of both appliances but only consumes one license because it only has one connection.

## Manage Guests In A FortiNac Control Manager Environment

When using Guest Manager in an environment where two or more Network Sentry appliances are managed by a central FortiNac Control Manager appliance, guest accounts are not centrally located. Guest accounts can be created on any Network Sentry appliance, but are not replicated to other Network Sentry appliances. When guests arrive, they may connect to the network in a location managed by an appliance other than the one where their accounts were created. When a guest connects to the network and tries to register, the Network Sentry appliance to which the guest is connected checks its own database for the guest's account. If the guest account exists on that Network Sentry appliance, the guest can proceed with the registration process. If the guest account does not exist, the FortiNac Control Manager checks the other Network Sentry appliances it manages until it finds the guest account. The FortiNac Control Manager copies the guest account from the appliance on which it was created to the appliance where the guest is attempting to connect to the network. Then the guest can continue the registration process.

Since guest records are copied and are not centrally located there are some limitations.

- Guest accounts are only copied from one appliance to another as needed and are not synchronized at any time.
- When a guest user account is copied from one appliance to another, FortiNac Control Manager checks the status of the Propagate Hosts setting on the user account. If this setting is enabled, hosts associated with the guest are copied with the guest user account.
- If a guest account is manually deleted on one Network Sentry appliance, it is not deleted from all appliances automatically.
- Because all appliances are not kept in sync, Guest reports on Network Sentry appliance A may not show the same information as a guest report on Network Sentry appliance B. The guest may have been created on appliance A, but registered and authenticated on appliance B. A report on appliance A will not reflect the changes made to appliance B.
- Guest accounts cannot be limited to a particular appliance or set of appliances, which would subsequently limit access to a subset of the network.
- There is no central location where all guest records can be viewed. A best practice would be to use the same Network Sentry appliance to create all guest accounts.
- If the FortiNac Control Manager is not running, guests will not be able to register on any appliance that does not already contain their guest accounts.
- Guest users display under Users > User License. If a Guest User is deleted on the FortiNac Control Manager, the Guest User and corresponding host are also deleted on all the managed Network Sentry appliances. However, the Guest Account is not deleted. This account remains in the database of the managed Network Sentry appliance until it expires or is deleted. This allows a Guest User to

re-register or in the case of conference accounts, allows new guests to be assigned those accounts.

## Manage Hosts In A FortiNac Control Manager Environment

**Important:** Host records are not synchronized across managed Network Sentry Servers. Host state changes are never propagated from one Network Sentry Server to another.

In an environment where multiple Network Sentry Servers are managed by a FortiNac Control Manager, hosts register with the Server that manages the switch to which the hosts connect. The FortiNac Control Manager can query the servers it manages to locate hosts and view host or adapter properties regardless of the server on which the host record resides.

### **Hosts That Move To A Different Network Sentry Server**

When hosts are mobile, such as a laptop or an iPad, the host could connect to a switch that is not managed by the Network Sentry Server where the host originally registered. In this case the process is as follows:

1. Host A connects to the network and registers on Network Sentry Server 1.
2. Later, Host A moves and connects to a switch managed by Network Sentry Server 2.
3. Network Sentry Server 2, does not have a record for that host and queries the FortiNac Control Manager to find out if this is a registered host on a different Network Sentry Server.
4. The FortiNac Control Manager queries all of the Network Sentry Servers it manages and finds a record of Host A on Network Sentry Server 1.
5. The record for Host A is copied from Network Sentry Server 1 to Network Sentry Server 2. If the security policy used to scan Host A, exists on Network Sentry Server 2, then the host state is also copied. If the policy does not exist on Network Sentry Server 2, then the host state is not copied.
6. From this point forward, the two host records are never synchronized. Changes in host state on one Network Sentry Server are never propagated to any other Network Sentry Server.

### **Hosts With Delayed Remediation State**

When a host has been scanned with and failed for a policy set for Delayed Remediation, it is set to Pending - At Risk. This particular host state indicates that the host has failed the policy but is not being prevented from accessing the network until the configured delay for that policy elapses. If in the meantime the host moves somewhere else on the network and connects to a switch managed by a different Network Sentry Server, the host state is not propagated. If the host state is set to Pending - At Risk, the state is never sent to the second Network Sentry Server. However, if the host returns to the first server it must resolve the issues that caused it to fail and rescan before the delay elapses or it will be marked "At Risk" and will not be allowed on the network.

## Icon Key

Icons in Network Sentry represent different devices and users as they connect to and access the network. Host Icons are displayed in the Hosts View. Device Icons are displayed either in Hosts View or Profiled Devices. Host Icons in particular have many states.

To indicate the state of a user, a device or a host, the icons are modified slightly by superimposing an image on top, such as a red box to indicate that the item has been disabled. States can be cumulative. For example, you could see an "X" over a host icon. This indicates that the host has been disabled but is still online. The table below provides a legend for those states.

**Table 1: Icon State**

State	Definition	State	Definition
<b>Hosts, Adapters or Users View</b>			
	<b>Online / Enabled</b> —No image over icon indicates that the item, such as a Host or Adapter is online.		<b>Offline / Enabled</b> —Icon pixelated indicates that the item, such as a Host or Adapter is offline.
	<b>Online / Disabled</b> —Host or User was disabled but is online. This could be due to a misconfiguration of a switch or port or because the host was online at the time it was disabled. Defined as a Violation in some summary windows.		<b>Offline / Disabled</b> —Host or User is disabled and is not online.
	<b>Go To</b> — Allows you to select an icon on the User, Host or Adapter View and navigate to corresponding information on another view. For example, if you have a host selected on the Host view, and you click the Go To on the Adapter icon, the Adapter view is displayed with the appropriate adapter selected.		<b>Offline Device</b> —A device being managed through the Host View is not connected to the network, such as a gaming device or an IP phone.
	<b>Not Authenticated</b> —Located at the upper-left corner of the icon. User has not yet authenticated. There is a delay between when the user's computer is connected to the network and when it is placed in the Authentication VLAN.		<b>Security Risk</b> —Located at the upper-right corner of the icon. Host has been moved to remediation.
	<b>Pending At Risk</b> —Located at the upper-right corner of the icon. Host has failed a scan that is set to delayed remediation for x number of days. Icon indicates that the host has not yet been marked "at risk" but will be after the delay set in the scan has elapsed.		

The icons shown in the table below represent hosts, users and devices that are either online or in a good state, such as hosts that are Safe.

**Table 2: Network Sentry Icons**

Icon	Definition	Icon	Definition
<b>Adapter, Host and User Icons</b>			
	Adapter		Rogue Host
	Registered Host		IP Phone
	Contractor		Guest
	User		Administrator User
<b>System Icons</b>			
	Container		Multi Access Point (multiple hosts connected to one port, and none of the ports are phones)
	New Registered Host/Phone (one registered host and one phone are connected to a port)		New Rogue Host/Phone (one rogue host and one phone are connected to a port)
	New Cloud/Phone Icon Used when one of the following is true: <ul style="list-style-type: none"> <li>• More than one phone and one registered host connected to a port</li> <li>• More than one registered host and one phone connected to a port</li> <li>• More than one registered host and more than one phones connected to a port</li> </ul>		Wired Port
	Link to a neighboring device		Process Plug-In
	Port Aggregate Uplink		SSID — Wireless Connection
	Directory		Process Icon

Icon	Definition	Icon	Definition
<b>Device Icons</b>			
	Alarm System		Android
	Apple Device		Camera
	Card Reader		Cash Register
	Dialup Server		Environmental
	Firewall		Gaming Device
	Generic Monitoring System		Health Care Device
	Hub		Internet TV
	IP Phone		IPS/IDS
	Linux		Mac OS X
	Mobile or Apple iOS or Android		Generic Network Device
	PBX		Pingable Device
	Printer		Router
	Server		Switch
	Unknown Device		Unix

Icon	Definition	Icon	Definition
	UPS		Vending Machine
	VPN Connection	<b>W</b>	Windows
	Wireless Switch		



## Chapter 2: Landing Page

Once you enter the username and password information, the landing page that is specified in the Admin Profile for the logged in user appears. Use the menu bar in this view to perform various functions. If a user logs in as an Administrator, the complete menu bar is displayed. Operator and Help-Desk users have access to the Bookmarks menu, which they can use only for host or user searches.

## Menus

The main Menu bar is located across the top of the window at all times. If you access a view that has a series of options, such as the Roles View, you will see a menu column down the left side of the window. For example, when you access the Roles View, the menu bar on the left contains links for Roles and Groups. Click a menu option to navigate to a view. Click Help to access the online help or to access the About box. Click Logout in the top right corner to logout of the Administrative interface.

## Bookmarks

Use Bookmarks to create a personalized list of frequently visited views. In addition the Bookmarks menu contains default links, such as Locate, that are used by Help Desk and Operator admin users who have limited access to Network Sentry.

Bookmarks Menu	Topic
Manage Bookmarks	Manage Bookmarks on page 22
Dashboard	Dashboard on page 25
Locate	Locate View on page 39

## Hosts

Hosts Menu	Topic
Adapter View	Adapter View on page 368
Host View	Host View on page 322
Device Profiling Rules	Device Profiling Rules on page 192

## Users

Users Menu	Topic
Admin Users	Admin Users on page 271
User View	User View on page 385
Admin Profiles	Admin Profiles And Permissions on page 219
Guest/Contractor Templates	Guest/Contractor Templates on page 626

## Logs

Logs Menu	Topic
<b>Admin Auditing</b>	<b>Admin Auditing</b> on page 446
<b>Alarms</b>	<b>Alarms View</b> on page 489
<b>Events</b>	<b>Events View</b> on page 466
<b>Event to Alarm Mappings</b>	<b>Map Events To Alarms</b> on page 493
<b>Event Management</b>	Event Management on page 451

## Policy

Policy Menu	Topic
<b>Policy Configuration</b>	Policies on page 505
<b>Roles</b>	<b>Roles</b> on page 615
<b>Scan Management</b>	<b>Scan Management</b> on page 717

## System

System Menu	Topic
<b>Groups</b>	<b>Groups View</b> on page 681
<b>Scheduler</b>	<b>Scheduler View</b> on page 705
<b>Settings</b>	<b>Settings</b> on page 63

## Help

Help Menu	Topic
<b>Current View</b>	Displays the help topic associated with the currently displayed screen.
<b>Customer Portal</b>	Takes you to the Fortinet Customer Portal.
<b>Feedback</b>	Opens your default email and populates the subject line with your location in the product allowing you to send feedback to the Documentation department at Fortinet.
<b>Preferences</b>	<b>Admin User Interface Settings</b> on page 24

Help Menu	Topic
Legal	Legal on page 25
About	The About box provides you with information about the specific version of the software that is installed on your Network Sentry appliance. Information includes the Version number for each component and the build date.

### Manage Bookmarks

Use the Bookmarks menu to create links to views you access frequently. Changes to Bookmarks are stored for each user individually based on user name.

Bookmarks can be placed within user specified groups and sub-groups. Create Groups first and then add bookmarks.

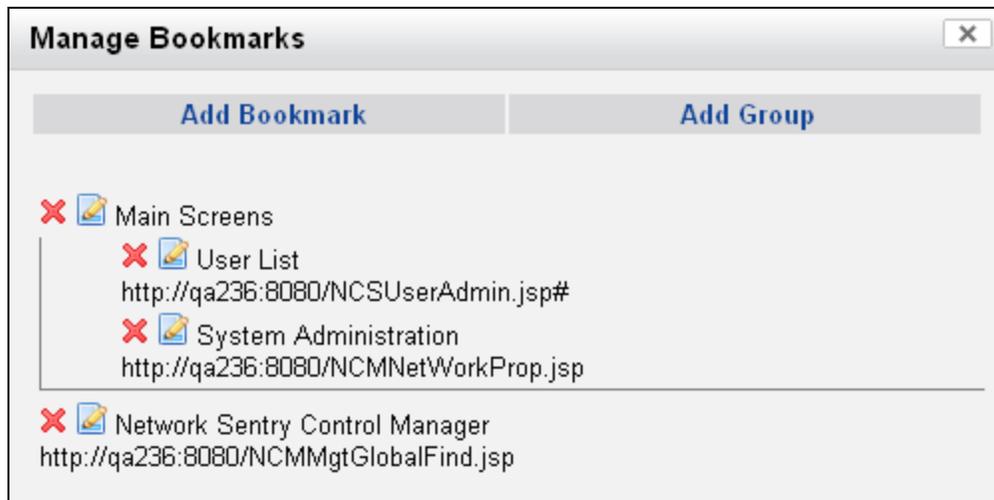


Figure 1: Manage Bookmarks

### Add A Bookmark Group

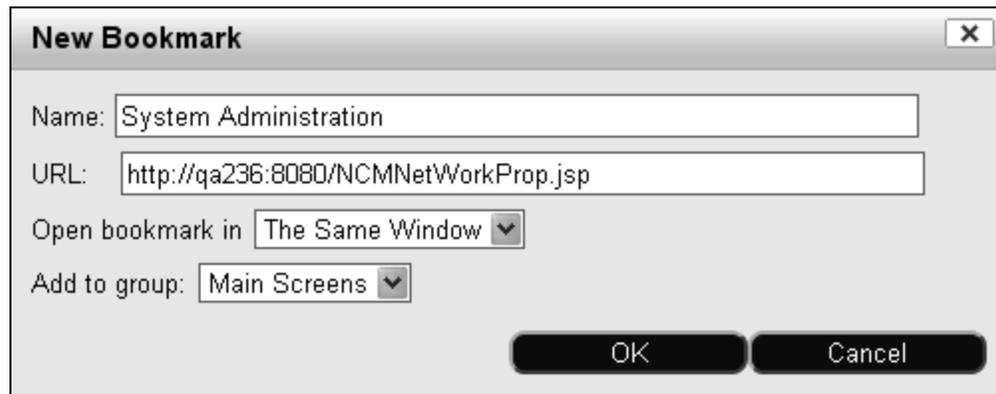


Figure 2: New Group

1. Select **Bookmarks > Manage Bookmarks** and click **Add Group**.
2. The New Group dialog is displayed.

3. In the Name field enter a name for this group.
4. If this group will be a sub-group, click in the **Add to group** drop-down and select the group where this new group should be placed.
5. Click **OK** to save.

### Add A Bookmark



The screenshot shows a dialog box titled "New Bookmark". It has a close button in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "System Administration".
- URL:** A text input field containing "http://qa236:8080/NCMNetWorkProp.jsp".
- Open bookmark in:** A dropdown menu with "The Same Window" selected.
- Add to group:** A dropdown menu with "Main Screens" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

**Figure 3: New Bookmark**

1. Use the menu bar at the top of the window to navigate to the screen you wish to bookmark.
2. Click the **star** in the banner next to the name of the view or select **Bookmarks > Manage Bookmarks** and click **Add Bookmark**.
3. The New Bookmark dialog is displayed.
4. On the Bookmark dialog, the **Name** field is filled in with the name of the view displayed. This is the name that will be displayed on the Bookmarks menu. Edit the name if necessary.
5. The **URL** field is filled in with the name and location of the panel that is currently displayed. If you know the URL of another view you can edit this field, however, it is recommended that you navigate to the view itself to ensure accuracy.
6. In the **Open bookmark in** field select either Same Window or New Window. Same Window will change the current window to the new View. New Window will open another instance of the browser with the new view displayed.
7. If you would like to place this bookmark in a previously created group, click in the **Add to group** drop-down and select the group where this new bookmark should be placed.
8. Click **OK** to save.

### Delete Or Edit A Bookmark

1. Select **Bookmarks > Manage Bookmarks**.
2. The list of bookmarks is displayed.
3. **To delete a bookmark**, click the red **X** to the left of the bookmark name. The bookmark is deleted immediately.
4. **To edit a bookmark**, click the **Edit** icon to the left of the bookmark name.

## Admin User Interface Settings

Allows you to toggle the classic Go menu off and on and to enable or disable Alt key combinations for accessing menus. Settings are stored for the logged in user.

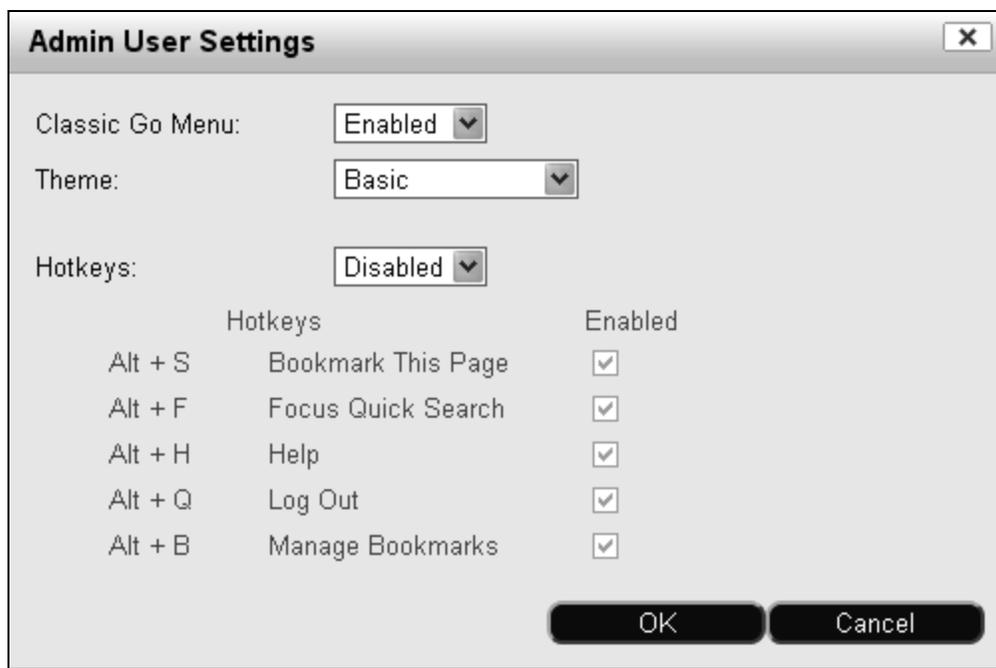


Figure 4: User Settings

1. Select **Help > Settings**.
2. In the **Classic Go Menu** field select enabled or disabled to display or hide the Go Menu. This menu was used in earlier versions of Network Sentry instead of the menu bar across the top of the screen. The Go Menu can be accessed from the top right corner of the screen in the banner.
3. Use the **Theme** field to change the look and feel of the user interface.
4. Use the **Hotkeys** options to enable or disable use of Alt key combinations to access menus or perform specific actions, such as logging out.
5. Click **OK** to save your settings.

## Legal

This view contains links to the Network Sentry End User License Agreement and associated copyright and license information for software used in the development of Network Sentry.

## Dashboard

Use the Dashboard to access Server Maintenance and Management functions for the FortiNac Server or FortiNac Control Server managed by the FortiNac Control Manager.

The FortiNac Control Manager can access one or more FortiNac Server or FortiNac Control Server appliances when it searches for hosts, users or devices. These appliances must have the same version of the Network Sentry software as is currently installed on the FortiNac Control Manager. Contact Customer Support for additional information.

Dashboard panels display to provide you with additional system information at a glance. Much of this data can be accessed from other parts of the system. Each panel can be closed and later restored using the **Add Panel** link. Panels can be refreshed using the refresh button and moved by dragging and dropping the panel to a new location. Set a specific automatic refresh rate for each panel using the Refresh drop-down field in the title bar. If the Refresh drop-down is set to Manual, you must click the **Refresh** button to update the panel.

### Server List

Displays a list of the servers managed by this FortiNac Control Manager. This panel also allows you to add or remove managed servers and view their properties and topology windows. In the list of servers, High Availability appliances are listed beneath the corresponding servers with a status of Running - Not In Control. When a secondary appliance takes control after the primary fails over, the status changes to Running - In Control and the primary is displayed as Running - Not In Control. Servers are listed in alphanumeric order.

Server List:		Refresh: Manual			
Name	Product	IP Address	Status	Views	
playdonpod1	Network Sentry Server	192.168.65.121	Running	P 🏠	
playdonpod2	Network Sentry Server	192.168.65.122	Running	P 🏠	

Add

Figure 5: Server List Panel

Hover over the Synchronize icon to display a tooltip showing the time and date of the last attempted and last successful synchronization. The tooltip will display "Never" for both if synchronization has not occurred.

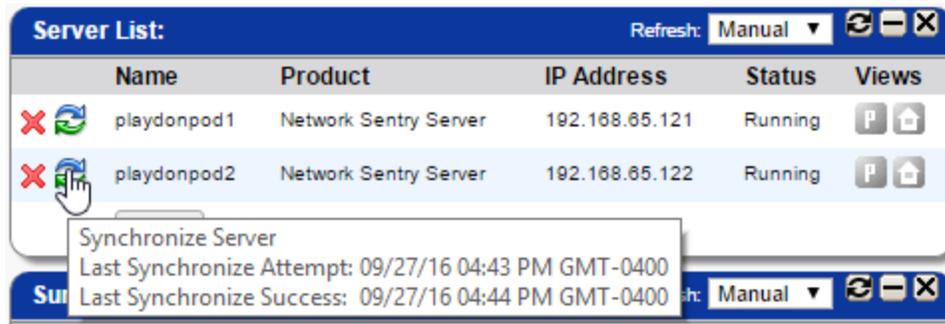


Figure 6: Last Synchronization Attempt and Last Successful Synchronization

Table 3: Server List Field Definitions

Field	Definition
<b>Name</b>	Name of the appliance on which Network Sentry is running.
<b>Product</b>	Software that is installed and running on the appliance.
<b>IP Address</b>	IP Address of the appliance being managed.
<b>Status</b>	Indicates the current status of each appliance displayed. Statuses include: <ul style="list-style-type: none"> <li>• <b>Running</b> — Appliance and software are running.</li> <li>• <b>Not Reachable</b> — Dashboard cannot communicate with the server.</li> <li>• <b>Management Down</b> — Appliance is running but the software is down.</li> <li>• <b>Running - Idle</b> — Appliance and software are up and running but there is currently no activity.</li> <li>• <b>Running - In Control</b> — Appliance and software are up and running. This appliance is in control vs. an appliance that may be the secondary appliance for high availability.</li> <li>• <b>Running - Not In Control</b> — Applies in a High Availability environment, where a secondary server is ready to take over in the event of a failure on the primary server. Indicates that the appliance and software are running, but are not in control.</li> </ul>
<b>Views</b>	<p><b>P Icon</b> — Displays the Properties view of the selected server. Properties view includes Server Name and IP Address.</p> <p><b>Server Icon</b> — Logs into the selected server and displays the first window in the Network Sentry software. This view displayed is based on your user permissions.</p>
<b>Delete Server Button</b>	Allows you to remove managed servers. If you delete a server, the Network Sentry Server will become standalone. All global information becomes local and can be modified.

Field	Definition
<b>Synchronize Server button</b>	Allows you to manually synchronize a single Network Sentry Server.
<b>Add Button</b>	Allows you to add servers to be managed.
<b>Refresh button</b>	Allows you to manually refresh the information in the panel. You can also select the refresh interval from the drop-down list to automatically refresh the information.

### License Information

The License Information panel displays the type and total number of licenses purchased. In addition, this summary indicates the number of licenses being used at any given time. Events can be generated on individual appliances and set to trigger alarms when license usage reaches or exceeds 75% of total licenses and when usage reaches 100% of total licenses. These thresholds are configurable on individual appliances.

Click the drop-down arrow to the left of the license type to expand a breakdown of licenses by server. Blue numbers to the right of the server name are links to a detailed list of how that license type is being used. See **Licenses In Use Detail** on page 37.

License Information:		Refresh: Manual		
Server Name	Total	In Use	Available	% Used
All Servers	600	5	595	0%
playdonpod1		4		0%
playdonpod2		1		0%

**Figure 7: License Information Panel**

### Summary Information

Displays information about your FortiNac Control Manager.

Summary:		Refresh: Manual	
Network Sentry Control Manager			
Host Name	qa236		
Status	Running		
Product	Network Sentry Control Manager		
Version	6.0		
Appliance	NS550		
Firmware	2.3.2.4		

**Figure 8: Summary Panel**

Table 4: Summary Field Definitions

Field	Definition
<b>Host Name</b>	Name of the appliance on which FortiNac Control Manager is running.
<b>Status</b>	Indicates the current status of the appliance displayed. Statuses include: <ul style="list-style-type: none"> <li>• <b>Running</b> — Appliance and software are running.</li> <li>• <b>Not Reachable</b> — Dashboard cannot communicate with the server.</li> <li>• <b>Management Down</b> — Appliance is running but the software is down.</li> <li>• <b>Running - Idle</b> — Appliance and software are up and running but there is currently no activity.</li> <li>• <b>Running - In Control</b> — Appliance and software are up and running. This appliance is in control vs. an appliance that may be the secondary appliance for high availability.</li> <li>• <b>Running - Not In Control</b> — Applies in a High Availability environment, where a secondary server is ready to take over in the event of a failure on the primary server. Indicates that the appliance and software are running, but are not in control.</li> </ul>
<b>Product</b>	Software that is installed and running on the appliance.
<b>Version</b>	Version number of the software listed under Product.
<b>Appliance</b>	Model number of the appliance for which data is displayed.
<b>Firmware</b>	Version number of the internal appliance specific software installed on the displayed appliance.
<b>Refresh button</b>	Allows you to manually refresh the information in the panel. You can also select the refresh interval from the drop-down list to automatically refresh the information.

### Performance Panel

This dashboard panel displays performance information for your software and CPU.

### Hardware Tab

The system uses as much RAM as is available. The underlying operating system is optimized to use RAM as efficiently as possible. Swap space is configurable, but only by Customer Support. The sum total of space available in RAM and available in swap represents the total amount of virtual memory available on the system. The disk space representing each directory on the file system is displayed.

Performance: Refresh: Manual			
Hardware			
	Total	Free	% Used
Memory	2058716	1182200	57%
Swap	0	0	0%
Memory+Swap	2058716	1182200	57%
Disk (/)	45.8 GB	38.0 GB	17%
Disk (/boot)	93.6 MB	81.5 MB	12%

### Software Tab

Memory is allocated to each of the internal loader processes in the FortiNac appliance (e.g., the "slave loader" and the "master loader"). The amount of memory allocated to these processes varies from platform to platform, and is configurable, but only by Customer Support.

Performance: Refresh: Manual				
Software				
System Start Time	Tue Mar 29 15:55:33 EDT 2016			
System Up Time	0 Days 23 Hours 5 Minutes 18 Seconds			
Process	Threads	Total Memory	Free Memory	Used Memory
Principal	52	455.5 MB	402.6 MB	11%

Figure 9: Performance Panel - Software Tab

Field	Definition
<b>System Start Time</b>	Time the software was started.
<b>System Up Time</b>	Amount of time the software has been running.
<b>Process</b>	Processes that are currently running. If a process is not running it is not displayed. Possible processes include: <ul style="list-style-type: none"> <li>• Principal</li> <li>• Registration-Probe</li> <li>• Quarantine-Probe</li> <li>• IP--&gt;MAC</li> <li>• Communication</li> <li>• Nessus</li> </ul>
<b>Threads</b>	Number of threads being used by a particular process.
<b>Total Memory</b>	Total Memory allocated for each process.

Field	Definition
Free Memory	Portion of Total Memory not being used for each process.
Used Memory	Percentage of total memory being used for each process. The amount of memory allocated.
Refresh button	Allows you to manually refresh the information in the panel. You can also select the refresh interval from the drop-down list to automatically refresh the information.

### CPU Usage

The graph contained in this tab displays the percentage of CPU Usage. The data contained within the graph is not stored and is based on data points retrieved at each refresh interval.

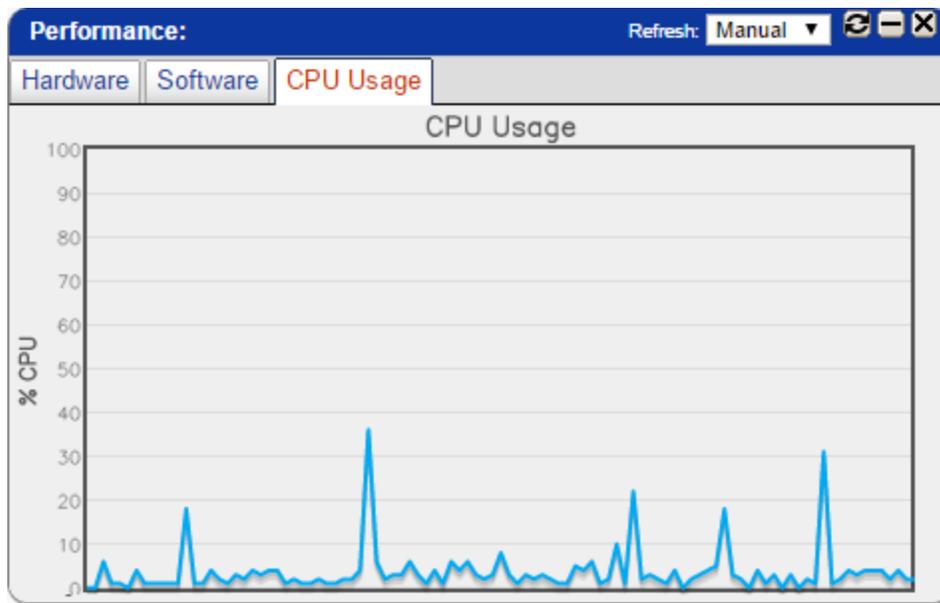


Figure 10: Performance Panel - CPU Tab

### Alarms

The Alarm panel displays a subset of the information available on the Alarms View. It provides an at a glance view of alarms that have been triggered by events. The list is filtered to limit the number and type of alarms displayed. You can Acknowledge or Clear alarms and view alarm details. See **Alarms View** on page 489 and **Add or Modify Alarm Mapping** on page 497 for additional information.

The Latest Alarms tab displays each alarm with date, time, and the elements affected. Elements include items such as, MAC Address or IP Address. Click the **Acknowledge** button to indicate that you are aware of the selected alarm. Click the **Clear** button to remove the selected alarm from the database.

### Set Latest Alarms Filter

1. Click the **Set Filter** button on the Latest Alarms Tab.



**Figure 11: Latest Alarms Filters**

2. In the Filter window, click in the **Display Latest** drop-down list and select the number of alarms to display. The maximum is 100.
3. To filter by Severity, mark the **Severity** check box with a check mark to enable it and select the severity level from the drop-down list. Levels include Critical, Minor, Warning and Informational.
4. To display **Acknowledged Alarms**, mark that check box with a check mark to enable it.
5. Click **OK**. Filter settings are displayed on the Alarms panel to the right of the Set Filter button.

**Note:** Filter settings are stored for each user.

### View Alarm Details

1. Select an alarm from the list displayed in the Latest Alarms tab.
2. Click the **Details** button.
3. Click **Acknowledge** to mark the alarm as acknowledged.
4. Click **Clear** to remove the alarm from the database.
5. Click **Close** to return to the Dashboard.

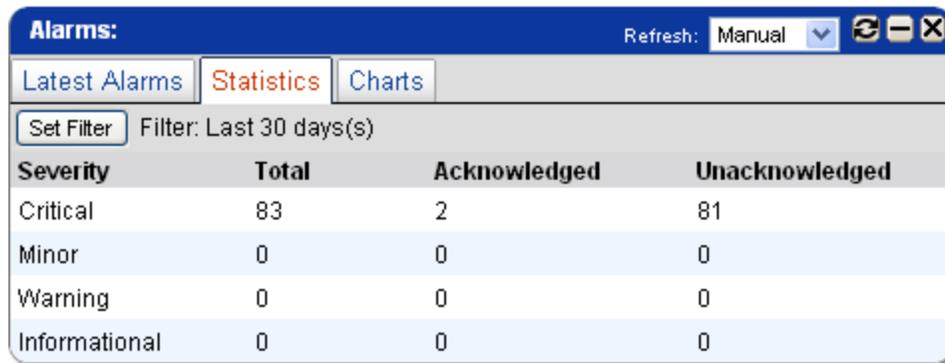
### **Statistics Tab**

The Statistics tab displays alarm totals by severity. In addition, each total is broken down into Acknowledged and Unacknowledged alarms. Alarms can be marked as Acknowledged to indicate that a user is aware of the alarm. You can clear alarms that are no longer needed. Cleared alarms are not included in totals.

The Set Filter button allows you to choose the number of days of data that will be tallied by this Statistics screen. Depending on the age time selected in the Network Sentry Properties window and your archive and purge schedule, you may not be able to view data for the number of days selected on the Statistics tab. For example, the default age time for

events and alarms is seven days. If you select nine days on the Statistics tab, you may not be able to see data for all nine days. See **Database Archive** on page 147 for information on age time.

**Note:** Filter settings are stored for each Admin user.



The screenshot shows a window titled "Alarms:" with a "Refresh: Manual" dropdown and window control buttons. Below the title bar are three tabs: "Latest Alarms", "Statistics" (which is selected and highlighted in red), and "Charts". Under the "Statistics" tab, there is a "Set Filter" button and a text field containing "Filter: Last 30 days(s)". Below this is a table with four columns: "Severity", "Total", "Acknowledged", and "Unacknowledged". The table contains four rows of data.

Severity	Total	Acknowledged	Unacknowledged
Critical	83	2	81
Minor	0	0	0
Warning	0	0	0
Informational	0	0	0

**Figure 12: Alarms Panel - Statistics Tab**

### Set Statistics Filter

1. Click the **Set Filter** button on the Statistics tab.
2. Type the number of days to go back and collect data.
3. Click **OK**.

**Note:** If the number of days is too large, you may see a warning indicating the number of days selected for the age time in the Network Sentry Properties window. If the Age Time for purging alarm data is set to 7 days and you select 30 days for the filter, the panel will display data for as many days as it can access within the range selected.

## Charts Tab

The Charts tab provides a chart of alarms per day for the last 24 days. Depending on the age time settings in the Network Sentry Properties window and the archive and purge schedule, you may not have 24 days of data available. Use the **Show** check boxes across the bottom of the chart to select the alarms to display. The graphical representation of the alarms can be either a line or a stacked bar. Use the **Chart Type** options at the bottom of the window to change the graphic.

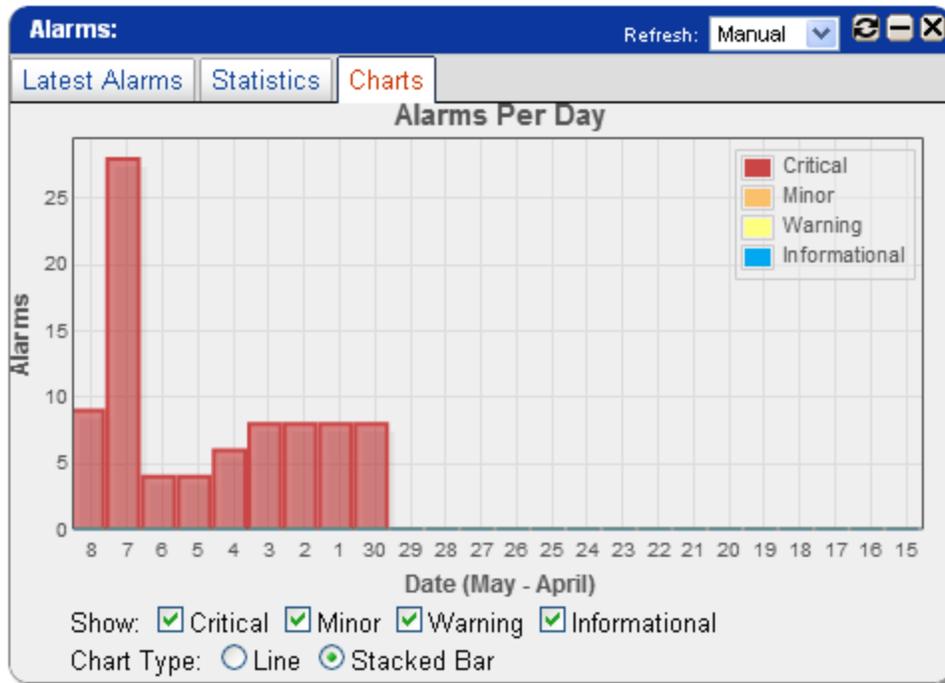


Figure 13: Alarms Panel - Charts Tab

## Add A Panel To The Dashboard

Use this option to add or restore closed panels to the Dashboard.

1. Click the **Add Panel** link at the top of the Dashboard window.
2. Select a panel from the list. To select more than one panel hold down the Ctrl key and click on the panel names.
3. Click **OK** to display the panels on the Dashboard.

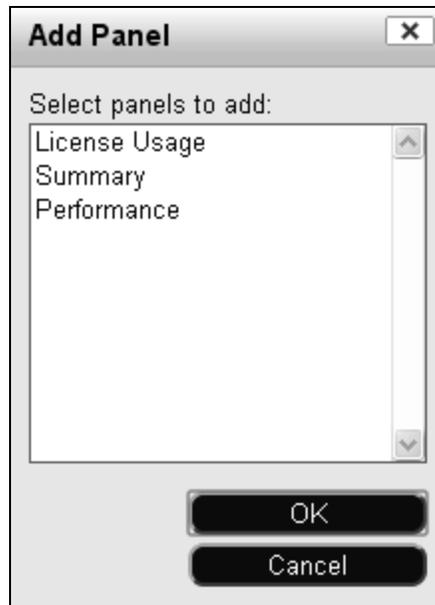


Figure 14: Add Panel Window



## License Information Panel

This dashboard panel displays the total number of licenses purchased. In addition, this summary indicates the number of licenses being used at any given time. Events can be generated and set to trigger alarms when license usage reaches or exceeds 75% of total licenses and when usage reaches 100% of total licenses. These are default thresholds. Thresholds used to calculate % Used information can be modified from the License Information panel by clicking on the colored bar. Thresholds can also be modified from the Events Management window. See **Event Thresholds** on page 455 for instructions.

The color bars in the % Used column change as you exceed certain licensing thresholds. Colors are as follows:

- **Green**—the percentage used is below the threshold.
- **Yellow**—the percentage used is at or above the threshold.
- **Red**—the percentage used is at 100%.

Server Name	Total	In Use	Available	% Used
All Servers	600	5	595	0%
playdonpod1		4		0%
playdonpod2		1		0%

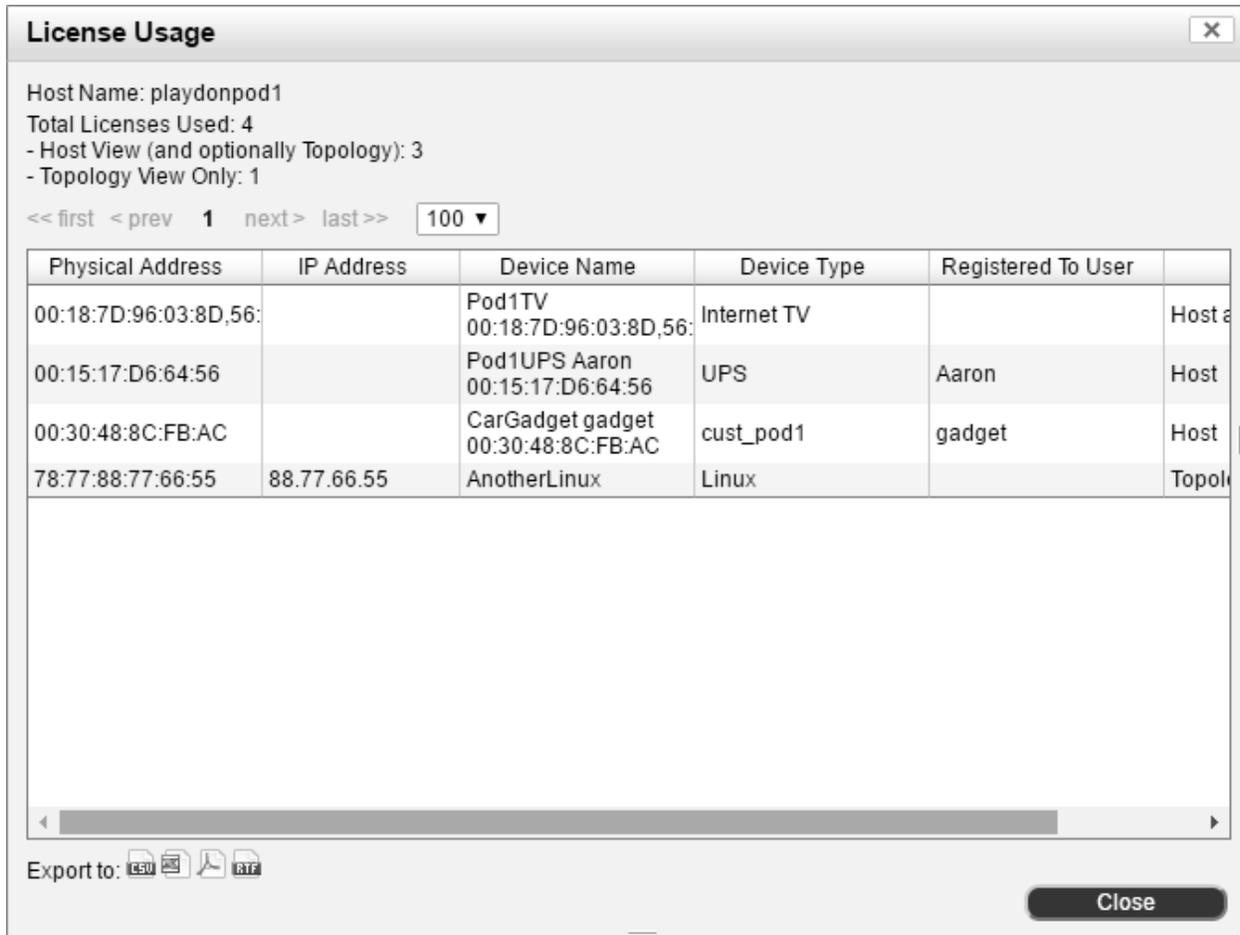
Figure 15: License Information

## Licenses In Use

To determine how licenses are consumed within Network Sentry click the number displayed in the **In Use** column on the License Information panel. A list of the exact element consuming each license is displayed.

Data displayed in the License Usage Panel can be exported in CSV, Excel, PDF or RTF formats. Click the appropriate icon at the bottom of the window to export.

See **License Types And Usage** on page 8 for additional license information.



**License Usage**

Host Name: playdonpod1  
 Total Licenses Used: 4  
 - Host View (and optionally Topology): 3  
 - Topology View Only: 1

<< first < prev **1** next > last >> 100 ▾

Physical Address	IP Address	Device Name	Device Type	Registered To User	
00:18:7D:96:03:8D:56:		Pod1TV 00:18:7D:96:03:8D,56:	Internet TV		Host a
00:15:17:D6:64:56		Pod1UPS Aaron 00:15:17:D6:64:56	UPS	Aaron	Host
00:30:48:8C:FB:AC		CarGadget gadget 00:30:48:8C:FB:AC	cust_pod1	gadget	Host
78:77:88:77:66:55	88.77.66.55	AnotherLinux	Linux		Topol

Export to:    

Close

**Figure 16: Licenses Used**

## Licenses In Use Detail

To determine how licenses are consumed within Network Sentry click drop-down arrow next to the license type in the License Information Panel to display the list of servers. Click the number displayed in the **In Use** column next to the appropriate server name. A list of the exact element consuming a license is displayed.

Data displayed in the License Usage Panels can be exported in CSV, Excel, PDF or RTF formats. Click the appropriate icon at the bottom of the window to export.

See **License Types And Usage** on page 8 for additional license information.

The screenshot shows a window titled "License Usage" with a close button in the top right corner. Below the title bar, the following information is displayed:

- Host Name: playdonpod1
- Total Licenses Used: 4
- Host View (and optionally Topology): 3
- Topology View Only: 1

Navigation controls include: << first < prev 1 next > last >> and a dropdown menu showing "100".

Physical Address	IP Address	Device Name	Device Type	Registered To User	
00:18:7D:96:03:8D:56:		Pod1TV 00:18:7D:96:03:8D:56:	Internet TV		Host a
00:15:17:D6:64:56		Pod1UPS Aaron 00:15:17:D6:64:56	UPS	Aaron	Host
00:30:48:8C:FB:AC		CarGadget gadget 00:30:48:8C:FB:AC	cust_pod1	gadget	Host
78:77:88:77:66:55	88.77.66.55	AnotherLinux	Linux		Topol

At the bottom of the window, there are export options: "Export to:" followed by icons for CSV, Excel, PDF, and RTF. A "Close" button is located in the bottom right corner.

Figure 17: Licenses Used

## Locate View

Use the Locate View to locate devices or hosts on selected appliances by entering information in any or all of the fields. Use an asterisk (\*) as a wild card if you only know a part of the information. For example, entering \*HP\* in the name field locates all hosts and devices with HP anywhere in the name.

**Note:** The Locate View for Operator and Help-Desk users only allows host searches.

To locate devices or hosts:

1. Select one or more appliances from the Server List or click **Select All** to select all managed appliances. See the Server List panel in the **Dashboard** on page 25 for information on how to add managed appliances.
2. To save your list of selected servers, click **Save Server Selections** under the server list.
3. Select the search type.

Search Type	Description
<b>All</b>	This option searches for both devices and hosts. To reduce the number of returned records, use the Devices or Host/User searches.
<b>Devices</b>	Use this option to locate network devices. See Locate Devices on page 42 for additional information.
<b>Host/User</b>	Use this option to locate hosts or users. See Locate Hosts/Users on page 49 for additional information.

4. Enter the search criteria.

**Note:** To reduce the potential for a significant number of records being returned in the Search Results, you must enter a value into one of the search fields.

**Note:** If the Search Type is set to All and you enter data in the Name field, Network Sentry searches for User Last Names and Network Device Names.

5. Click **Search**.

## All Search Results

The Locate All Search results displays the device, host and user information for each of the managed appliances you selected for the search.

36 items found, displaying 21 to 36. [First/Prev] 1, 2 [Next/Last]

Server	Name	IP Address	Physical Address	Type/Location	Status	Views
qa246.bradfordnetworks.com	Cisco-2960-lab-123	192.168.5.69		Cisco Switch	Established	 
qa246.bradfordnetworks.com	192.168.5.75	192.168.5.75		Dell	Established	 
qa246.bradfordnetworks.com	Dell-3324	192.168.5.80		Dell	Established	 
qa246.bradfordnetworks.com	Stk Master	192.168.5.100		Extreme Summit 400-48t	Established	 
<input type="checkbox"/>	qa246.bradfordnetworks.com	Moe	192.168.35.52	00:21:70:D7:CF:E7	HP_SW_25 7	Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	root				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	Jeremy				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	Larry				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	Moe				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	g.washington				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	passivepete				Disconnected  
<input type="checkbox"/>	qa246.bradfordnetworks.com	pete				Disconnected  

Export options: CSV | Excel | XML | PDF | RTF

**Remove Host and Adapters** Remove host and all adapters of the selected entries.

**Remove Adapter** Remove only the adapter selected for each of the selected entries.

**Remove Host Adapters and User** Remove the user, the hosts and all the adapters for the selected entries.

**Remove User** Remove only the user of the selected entries but leave the host and adapters.

Figure 18: All Search Results

## All Search Results Field Definitions

Column	Description
<b>Server</b>	Server managing the host.
<b>Name</b>	User ID of the user (from the user record) or the name of the device.
<b>IP Address</b>	IP address of the host or device.
<b>Physical Address</b>	MAC address of the host or device.
<b>Type/Location</b>	Device the host is connected to, such as a switch or a router, or the Vendor Name and location of a specific device.
<b>Status</b>	<p>The status of the device:</p> <ul style="list-style-type: none"> <li>• <b>Any</b> — Show device regardless of current status.</li> <li>• <b>Management Lost</b> — System is still in contact with the server, but that server is not managing anything.</li> <li>• <b>Lost</b> — Cannot ping a known device.</li> <li>• <b>Unknown</b> — Very brief status that only occurs while pinging a new device. Once the device responds to the ping the status changes.</li> <li>• <b>Established</b> — Device can be pinged and is in contact.</li> <li>• <b>Disconnected</b> — User is no longer connected to the network.</li> </ul>
<b>Views</b>	Icons that provide access to other related information. Click an icon to go to that view from the results window. Options include: Adapter Properties, Host Properties, Group Membership, Ports Properties, SSID Properties, User Properties and Device Properties.
<b>Remove Buttons</b>	<p>Click one or more check boxes in the left column to select items for deletion. Selected items are removed from the server where they were being managed. Note: Only Administrator users can delete.</p> <p>Remove options are as follows:</p> <p><b>Remove Host And Adapters</b> — Deletes the selected host and all corresponding adapters. If a host has a wired and a wireless adapter, both are removed from the database. The host and adapters are only removed from the server shown in the record you selected.</p> <p><b>Remove Adapter</b> — Deletes only the selected adapter but leaves the host record, other adapter records and the user record in the database. The adapter is only removed from the server shown in the record you selected.</p> <p><b>Remove Host Adapters And User</b> — Deletes everything associated with the selected host from the database. The host and adapters are only removed from the server shown in the record you selected. Users are removed from all managed servers that the logged in Admin user can access. A warning is displayed if the Admin user does not have access to all managed servers.</p> <p><b>Remove User</b> — Deletes the user associated with the selected host from the database. Users are removed from all managed servers that the logged in Admin user can access. A warning is displayed if the Admin user does not have access to all managed servers.</p>

Locate Devices

Use this option on the Locate View to locate devices. See **Locate View** on page 39 for additional information.

The screenshot shows a web interface titled "Registered Hosts/Devices". At the top, there is a "Search Type" dropdown menu currently set to "Devices". Below this is a "Server list" area with a scrollable list containing the entry "qa246.bradfordnetworks.com". Underneath the list are two buttons: "Select All" and "Save Server Selection(s)". The interface also features several search filters: "Name" with an asterisk in the input field, "IP Address" with an empty input field, "Status" with a dropdown set to "Any", "Protocol" with a dropdown set to "Both", and "Physical Address" with an empty input field. A large "Search" button is positioned in the bottom right corner of the interface.

Figure 19: Locate Devices

Table 5: Locate Devices Field Definitions

Search Options	Description
<b>Search Type</b>	Select Hosts/Users, Devices or All.
<b>Server List</b>	List of servers being managed. Select one or more servers to be included in the search.  Click <b>Select All</b> to select all servers to be included in the search.  Click <b>Save Server Selections</b> to save the list of servers you have selected for the search.
<b>Name</b>	The name of the device.
<b>IP Address</b>	The IP Address of the device.

Search Options	Description
<b>Status</b>	The status of the device: <ul style="list-style-type: none"><li>• <b>Any</b> — Show device regardless of current status.</li><li>• <b>Management Lost</b> — System is still in contact with the server, but that server is not managing anything.</li><li>• <b>Lost</b> — Cannot ping a known device.</li><li>• <b>Unknown</b> — Very brief status that only occurs while pinging a new device. Once the device responds to the ping the status changes.</li><li>• <b>Established</b> — Device can be pinged and is in contact.</li></ul>
<b>Protocol</b>	The protocol used to communicate with the device: <ul style="list-style-type: none"><li>• Pingable</li><li>• Both</li><li>• SNMP</li></ul>
<b>Physical Address</b>	Physical Address (MAC) of the device. If you enter a value for this option in the All or Device search, all of the device ports with a matching MAC address are shown in the results. If you do not enter a MAC address, only the device model is shown in the results.

## Device Search Results

The Device Search results displays device information for each of the managed appliances you selected for the search.

4 items found, displaying all items. 1

Server	Name	IP Address	Physical Address	Type	Status	Views
qa246.networks.com	SourceFire	192.168.6.241	00:0C:29:F7:99:C7	ips	Established	 
qa246.networks.com	LDAP	192.168.10.170	00:A0:CC:D1:4C:BF	Server	Established	 
qa246.networks.com	3Com4300	192.168.5.33		3Com SuperStack 3 - 4300	Established	  
qa246.networks.com	Concord-3750	192.168.10.1		Cisco Switch	Established	  

Export options: CSV | Excel | XML | PDF | RTF

Figure 20: Device Search Results

### Device Search Field Definitions

Device Results Column	Definition
<b>Server</b>	The name of the FortiNac Server or FortiNac Control Server where the device is located.
<b>Name</b>	The name of the device.
<b>IP Address</b>	The IP address of the device.
<b>Physical Address</b>	MAC Address or Hardware Address of the device.
<b>Type</b>	The device type: vendor name or model.
<b>Status</b>	The contact status of the device.
<b>Views</b>	Icons that provide access to device specific views: <ul style="list-style-type: none"> <li>• Device Properties</li> <li>• Device Group Membership</li> <li>• Ports and Hosts</li> <li>• SSID Properties</li> </ul>

## Device Views

Click the icon in the Device Search window for a view to see additional information about the device.

The screenshot shows the 'Device Properties View' for a device named 'Concord-3750'. The fields are as follows:

- Name:** Concord-3750
- Type:** Cisco Switch
- IP Address:** 192.168.10.1
- Vendor:** 1.3.6.1.4.1.9
- Version:** 3500.IOS.12.2
- VLAN Switching:**  Enable  Disable
- PA Optimization:**  Enable  Disable VLAN Switching Optimization with Persistent Agent
- MAC Filtering:**  Enable  Disable
- Description:** Cisco IOS Software, C3750 Software (C3750-ADVIPSERVICESK9-M), Version 12.2(46)SE, RELEASE SOFTWARE (fc2)  
Copyright (c) 1986-2008 by Cisco Systems, Inc.  
Compiled Thu 21-Aug-08 15:43 by nachen
- Role:** NAC-Default
- SNMP Protocol:** SNMPv1
- Security Strings:** bradford

At the bottom of the form, there is an  Advanced checkbox and three buttons: Groups, Apply, and Reset.

**Figure 21: Device Properties View**

- **Device Properties**—Current device settings are displayed. See the Device Management section of the Network Sentry Administration and Operation document for additional details.
- **Device Group Membership**—All available device groups are displayed. If the device is a member of a group, the check box is selected.

To add the device to a group, check the box next to the group and click **Apply**.

### Group Membership

\* Indicates membership in a subgroup.  
Checked boxes indicate direct membership in the group.

<input type="checkbox"/> Authentication-Executive_Suite-Devices	<input checked="" type="checkbox"/> L2 Wired Devices
<input type="checkbox"/> *L2 Network Devices	<input type="checkbox"/> L2 Wireless Devices
<input type="checkbox"/> Authorized DHCP Servers	<input type="checkbox"/> Physical Address Filtering
<input type="checkbox"/> Dead-End-Executive_Suite-Devices	<input type="checkbox"/> Registration-Executive_Suite-Devices
<input type="checkbox"/> Device Group A	<input type="checkbox"/> Remediation-Executive_Suite-Devices
<input checked="" type="checkbox"/> Device Interface Status	<input type="checkbox"/> Role-Based-Access-Executive_Suite-Devices
<input type="checkbox"/> L3 (IP-->MAC)	<input type="checkbox"/> Switches with Roles

Figure 22: Device Group Membership View

- **Ports and Hosts**—All ports on the device are listed with the current and default VLAN setting for the port. If a host is connected on a port, the host name and IP information is also displayed. Click the port icon to display the Port Properties view for that port. Click the host or adapter icon to display the Properties view.

Index: 0 Total:24				<<prev		next>>	
#	Name	VLAN		Hosts			
		Current	Default	#	Name	IP	
1	Switch 3300 Unit 1 Port 1			0			
2	Switch 3300 Unit 1 Port 2			0			
3	Switch 3300 Unit 1 Port 3			0			
4	Switch 3300 Unit 1 Port 4			1	00:30:48:8F:4C:36	192.168.5.228	
5	Switch 3300 Unit 1 Port 5			1	00:30:48:69:63:CC	192.168.5.226	
6	Switch 3300 Unit 1 Port 6			0			
7	Switch 3300 Unit 1 Port 7			0			
8	Switch 3300 Unit 1 Port 8			0			
9	Switch 3300 Unit 1 Port 9			0			
10	Switch 3300 Unit 1 Port 10			0			
11	Switch 3300 Unit 1 Port 11			0			
12	Switch 3300 Unit 1 Port 12			0			
13	Switch 3300 Unit 1 Port 13			0			
14	Switch 3300 Unit 1 Port 14			0			
15	Switch 3300 Unit 1 Port 15			0			
16	Switch 3300 Unit 1 Port 16			0			
17	Switch 3300 Unit 1 Port 17			0			
18	Switch 3300 Unit 1 Port 18			0			
19	Switch 3300 Unit 1 Port 19			0			
20	Switch 3300 Unit 1 Port 20			0			
21	Switch 3300 Unit 1 Port 21			0			
22	Switch 3300 Unit 1 Port 22			0			
23	Switch 3300 Unit 1 Port 23			0			
24	Switch 3300 Unit 1 Port 24			0			
Index: 0 Total:24				<<prev		next>>	

Figure 23: Device Ports and Hosts View

- **SSIDs**—All SSIDs on the device are listed with the current and default VLAN setting. If a host is connected on a port, the adapter MAC Address and IP information is also displayed.

Index: 0 Total:4	<<prev next>>
Name	
 Ruckus SSID Ruckus-v39	
 Ruckus SSID vlan85	
 Ruckus SSID Ruckus Open	
 Ruckus SSID Ruckus802.1x	
Index: 0 Total:4	<<prev next>>

Figure 24: SSIDs View

## Locate Hosts/Users

Use this option on the Locate Tab to locate hosts or users.

The screenshot shows a web interface titled "Registered Hosts/Devices". It features a "Search Type" dropdown menu set to "Hosts/Users". Below this is a "Server list" area containing a scrollable list of server names: "qa6-100.bradfordnetworks.com" and "qa212.bradfordnetworks.com", with the second one highlighted. There are two buttons: "Select All" and "Save Server Selection(s)". At the bottom, there are two text input fields labeled "Last Name" and "IP Address".

Figure 25: Locate Tab - Registered Hosts/Devices

The screenshot shows a web interface titled "Additional Adapter Info". It contains several configuration options: "MAC type" with a dropdown set to "Both", "Connect State" with a dropdown set to "Both", and "Access" with a dropdown set to "Both". Below these are three text input fields labeled "Physical Address", "Media Type", and "Access Value".

Figure 26: Locate Tab - Additional Adapter Info

Additional Host Info	
Host Name	<input type="text" value="Lab Machine 1"/>
Agent Version	<input type="text"/>
Operating System	<input type="text"/>
Hardware	<input type="text"/>
Host Type	<input type="text" value="All"/>
Authenticated State	<input type="text" value="Both"/>
Security State	<input type="text" value="Both"/>
Persistent Agent	<input type="text" value="Both"/>
Connect State	<input type="text" value="Both"/>
Access	<input type="text" value="Both"/>
Host Role	<input type="text"/>
Security & Access Value	<input type="text"/>

Figure 27: Locate Tab - Additional Host Info

Additional User Info	
First Name	<input type="text" value="John"/>
User ID	<input type="text"/>
Title	<input type="text"/>
User Type	<input type="text" value="All"/>
Sponsor	<input type="text"/>
User Role	<input type="text"/>
Access	<input type="text" value="Both"/>
Security & Access Value	<input type="text"/>

Figure 28: Locate Tab - Additional User Info

## Locate Tab - Host/User Search Fields

Option	Description
<b>Registered Hosts/Devices</b>	
<b>Server List</b>	<p>List of servers being managed. Select one or more servers to be included in the search.</p> <p>Click <b>Select All</b> to select all servers to be included in the search.</p> <p>Click <b>Save Server Selections</b> to save the list of servers you have selected for the search.</p>
<b>Last Name</b>	The last name of a user associated with the registered host or the vendor name of a rogue host.
<b>IP Address</b>	The IP Address of the host machine.
<b>Additional Adapter Info</b>	
<b>MAC Type</b>	The MAC Type for the host. The available options are: Invalid, Valid or Both.
<b>Connect State</b>	The Connect State of the adapter. Options include: Both, Off line or On line.
<b>Access</b>	The Access state of the adapter. Options include, Enabled, Disabled or Both.
<b>Physical Address</b>	The MAC Address of the adapter on the host.
<b>Media Type</b>	Searches the Media Type field in the Adapter Properties. Typically this would be either wired or wireless.
<b>Access Value</b>	Directory Attribute used when determining which security policy the hosts are scanned against. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.
<b>Additional Host Info</b>	
<b>Host Name</b>	Name of the host machine.
<b>Agent Version</b>	Version number of the Persistent or Dissolvable Agent on the host.
<b>Operating System</b>	Operating system on the host.
<b>Hardware</b>	Hardware type of the host machine.
<b>Host Type</b>	Narrow the search by a specific type of host: All, IP Phone, Registered or Rogue.
<b>Authenticated State</b>	Include hosts on which a user has Authenticated, Not-authenticated or Both.
<b>Security State</b>	Include hosts that are Safe, At Risk or Both.

Option	Description
<b>Persistent Agent</b>	The Persistent Agent usage of the host. Options include: <b>No Agent</b> — Hosts with no agent. <b>Agent</b> — Hosts using the Persistent Agent. <b>Both</b> — Hosts using either the Persistent Agent or the Dissolvable Agent.
<b>Connect State</b>	The Connect State of the adapter. Options include: Both, Off line or On line.
<b>Access</b>	The Access state of the host. Options include, Enabled, Disabled or Both.
<b>Host Role</b>	Name of the Role assigned to the host. Roles are used to group hosts and control their access to the network.
<b>Security &amp; Access Value</b>	Directory Attribute used when determining which security policy the hosts are scanned against. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.
<b>Additional User Info</b>	
<b>First Name</b>	First name of the user associated with the host.
<b>User ID</b>	Unique alphanumeric ID. Typically comes from the directory but if you are not using a directory, this field can be created manually.
<b>Title</b>	User's title, this could be a form of address or their title within the organization.
<b>User Type</b>	Searches both Admin Users and network users. Options include: All, Administrative, Administrator, Operator or Helpdesk. To search network users and guests or contractors, select All.
<b>Sponsor</b>	If the administrative user performing the search has Sponsor privileges, his User Name may be filled in this field. Depending on permissions, a Sponsor's search may be limited to the hosts he created.  Sponsors with the ability to view all accounts can use this field to find hosts created by a specific Sponsor by entering that Sponsor's User Name in this field.
<b>User Role</b>	Name of the Role assigned to the user. Roles are used to group users and control their network access.
<b>Access</b>	The Access state of the user. Options include, Enabled, Disabled or Both.
<b>Security &amp; Access Value</b>	Directory Attribute used when determining which security policy the hosts are scanned against. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.

## Host/User Search Results

The Host/User Search results displays the host and user information for each of the managed appliances you selected for the search.

5 items found, displaying all items. 1

Server	Name	ID	IP Address	Physical Address	Location	Views
<input type="checkbox"/>	Network Sentry	Hackert, Alan	hackert	00:19:E3:E8:82:DF	Lab Switch 21	     
<input type="checkbox"/>	Network Sentry	Hackert, Alan	hackert	00:24:A8:88:81:4E	Lab Switch 42	     
<input type="checkbox"/>	Network Sentry	root	root			 
<input type="checkbox"/>	Network Sentry	Riddel, Niles	nvriddel			 
<input type="checkbox"/>	Network Sentry	Hackert, Alan	hackert			 

Export options: CSV | Excel | XML | PDF | RTF

- Remove Host and Adapters** Remove host and all adapters of the selected entries.
- Remove Adapter** Remove only the adapter selected for each of the selected entries.
- Remove Host Adapters and User** Remove the user, the hosts and all the adapters for the selected entries.
- Remove User** Remove only the user of the selected entries but leave the host and adapters.

**Figure 29: Host/User Search Results**

**Table 6: Host/User Results Field Definitions**

Column	Description
<b>Server</b>	Server managing the host.
<b>Name</b>	Last name of the user (from the user record).
<b>ID</b>	ID of the host or user.
<b>IP Address</b>	IP address of the host.
<b>Physical Address</b>	MAC address of the host.
<b>Location</b>	Device the host is connected to, such as a switch or a router.
<b>Views</b>	Icons that provide access to other related information. Click an icon to go to that view from the results window. Options include: Adapter Properties, Host Properties, Group Membership, Ports And Hosts, SSIDs and Device Properties.

Column	Description
Remove Buttons	<p>Click one or more check boxes in the left column to select items for deletion. Selected items are removed from the server where they were being managed. Note: Only Administrator users can delete.</p> <p>Remove options are as follows:</p> <p><b>Remove Host And Adapters</b> — Deletes the selected host and all corresponding adapters. If a host has a wired and a wireless adapter, both are removed from the database.</p> <p><b>Remove Adapter</b> — Deletes only the selected adapter but leaves the host record, other adapter records and the user record in the database.</p> <p><b>Remove Host Adapters And User</b> — Deletes everything associated with the selected host from the database.</p> <p><b>Remove User</b> — Deletes the user associated with the selected host from the database.</p>

## Navigation

The first page displayed when you log into Network Sentry is the Dashboard. The window is divided into several sections that allow you to navigate the program. Individual windows have similar navigation mechanisms throughout the program.

## Menu Bar



Figure 30: Network Sentry Menu Bar

Use the drop-down menus to access program features and functions. The Dashboard can be accessed from the Bookmarks menu. See **Menus** on page 20 for a list of all menu options.

## Title Bar

Views that contain tables provide record totals, navigation and configuration buttons within the title bar.



Figure 31: Title Bar Example 1



Figure 32: Title Bar Example 2

Field	Definition
<b>Refresh</b>	Drop-down list of options to set a refresh rate for the selected view.
	Refresh the data in the view.
	Minimize the view or close a section of the view.
	Close the view.
	Opens the Settings dialog. Configure which columns display in the table view. In the case of the Host, Adapters or User View, tool tips can also be configured.
<b>Displayed</b>	Total number of records displayed. This number is shown on view that have a search or filter capacity to show the number of records displayed versus the total number of records in the database.
<b>Total</b>	Total number of records contained in the database.

## Table Views

Data is presented in tables throughout Network Sentry. Table Views have many common navigation options. Data in some tables, such as Users, is refreshed periodically but is not re-sorted based on the new data until you close and reopen the view or click a column heading.

Enabled	Sponsor	Type	Name	User	Starting
✓	root	Guest	Ann, Green	agreen@hotmail.com	11/18/13 11:23 AM EST
✓	root	Conference	Science in the 21st Century-40	Science in the 21st Century-40	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st Century-39	Science in the 21st Century-39	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st Century-38	Science in the 21st Century-38	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st Century-37	Science in the 21st Century-37	11/18/13 11:22 AM EST

Figure 33: Table View Example

Field	Definition
<b>Paging</b>	<p>Below the title bar there are navigation tools that allow you to quickly move through large numbers of records. These tools include the following:</p> <p><b>&lt;&lt;first</b>—Takes you to the first page of records.</p> <p><b>&lt;prev</b>—Takes you back one page.</p> <p><b>Page Number</b>—Current page number is displayed.</p> <p><b>next&gt;</b>—Takes you forward one page.</p> <p><b>last&gt;&gt;</b>—Takes you to the last page.</p> <p><b>Drop-down Box</b>—Allows you to select the number of records to be displayed on each page.</p>
	Enables the selected record, such as a Device Profiling Rule.
	Disables the selected record, such as a Device Profiling Rule.
	Moves the selected record up or down in the table, changing the records ranking in ranked tables, such as Device Profiling Rules or User/Host Profiles..
	Exports the selected records to CSV, Excel, PDF or RTF formats. See Export Data on page 383.
<b>Import</b>	Imports records from a CSV file.
<b>Options Button</b>	Displays a list of operations that can be done for the selected records. This button mimics the right-click menu options for operating systems that do not display a right-click menu, such as Mac OS X.
<b>Columns</b>	
<b>Sorting</b>	Click a column head to sort by the data contained in that column. Click once to sort ascending. Click again to sort descending. Sort order is not saved once the view is closed.
<b>Order</b>	Change column order by selecting a column and dragging it to its new location. Column order is not saved once the view is closed.
<b>Hide/Show</b>	<p>Right click on a column heading to display a list of all possible columns. Columns with check marks are shown. Click on a column name in the list to hide or show it in the table.</p> <p>or</p> <p>Click the settings button  on the right side of the title bar to display the Settings dialog and select which columns to show in the table.</p>

### Tabbed Views

Some Network Sentry views allow you to perform multiple related functions. These views are presented with tabs along the left side. You are not necessarily required to configure

all of the tabs, they are made available for faster navigation.

- Use the Double Arrow button in the menu bar to open or close the column containing the tabs.
- Click the titles in the tabs to move from one view to another.
- In some cases there are sub-tabs, such as under Portal in the following figure.

Name	Where (Location)	Who/What by Group	Who/What by Attribute
Admin Staff	Any	Admin Staff	No
Administration	Switches with Roles	Any	Yes
Conference Room 257	Device Group A	Any	No
Conference Room 350	Gailz_Ports	Any	No
Endpoint Compliance Policy Profile 2	GA-GROUP	Any	No
Endpoint Compliance Policy Profile 3	Any	Any	Yes
Endpoint Compliance Policy Profile 4	Any	AlansGroup	No
Endpoint Compliance Policy Profile 5	Any	Any	Yes
Endpoint Compliance Policy Profile 6	A_group_gail, Authentication - QA - Devices	Any	Yes
Endpoint Compliance Policy Profile 7	GA-GROUP, Registration - QA - Devices	Any	Yes
Endpoint Compliance Policy Profile 8	Remediation - QA - Devices	Any	Yes
Endpoint Compliance Policy Profile 9	Remediation - QA - Devices, Role-Based-Access - QA - Devices	Any	Yes
Executive Team	Registration-Executive_Suite-Ports	Executive Staff	Yes
Guests	Device Group A	Any	Yes
Matches All Users Hosts	Any	Any	No
Mobile Security Wizard Profile: GuestSSID XAM-Access	XirusXMSecure	Any	Yes
Mobile Security Wizard Profile: XirusXMSecure			
Mobile Security Wizard Profile: OpenUser 44 Ruckus Open	Ruckus Open	Any	Yes
Mobile Security Wizard Profile: OpenUser 110 OpenAccess	OpenAccess	Any	Yes
Mobile Security Wizard Profile: OpenUser 210 OpenAccess2	OpenAccess2	Any	Yes
Mobile Security Wizard Profile:			

**Figure 34: Tabbed View**

## Tree Views

Some complex Network Sentry views use a tree to display configuration options and related tasks. Click + to expand the branches of the tree or - to collapse them. In some cases, there is a Flat View feature that changes the display to list all options in the tree alphabetically.

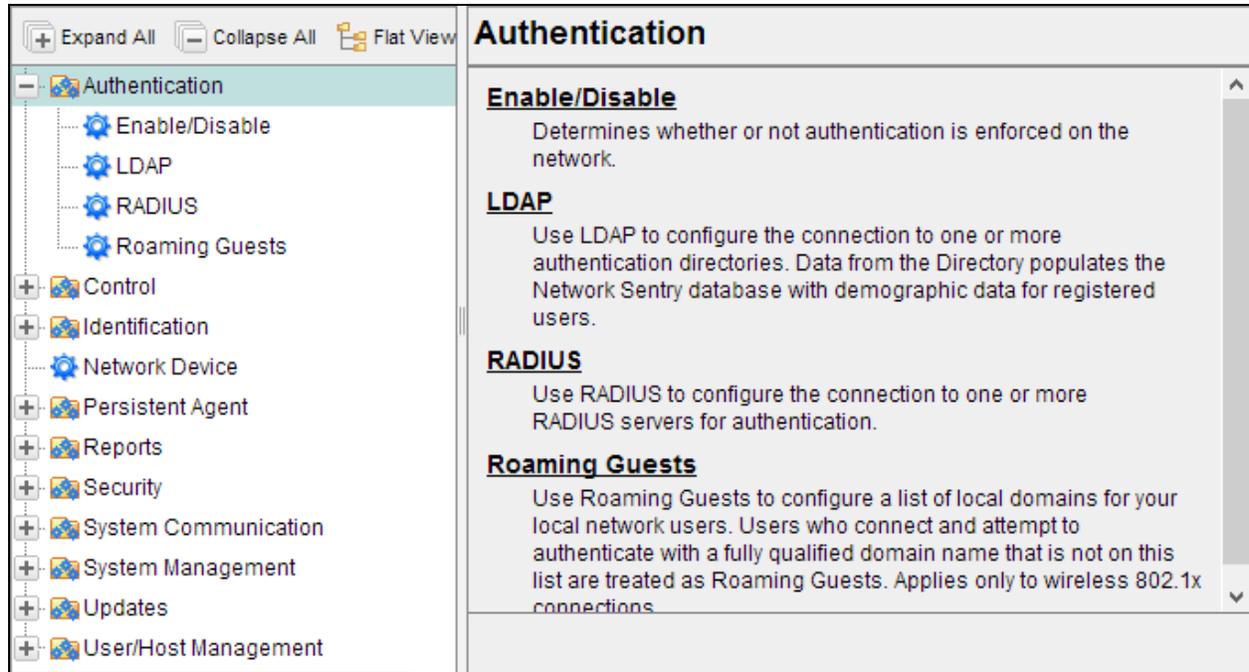


Figure 35: Tree Navigation Example

### Field Level Help

Help is accessed from the menu bar by selecting Help > Current View. In some cases, where a task is complex, field level help has been added. To access help for a field, click the question mark to the right of that field as shown in the next figure.

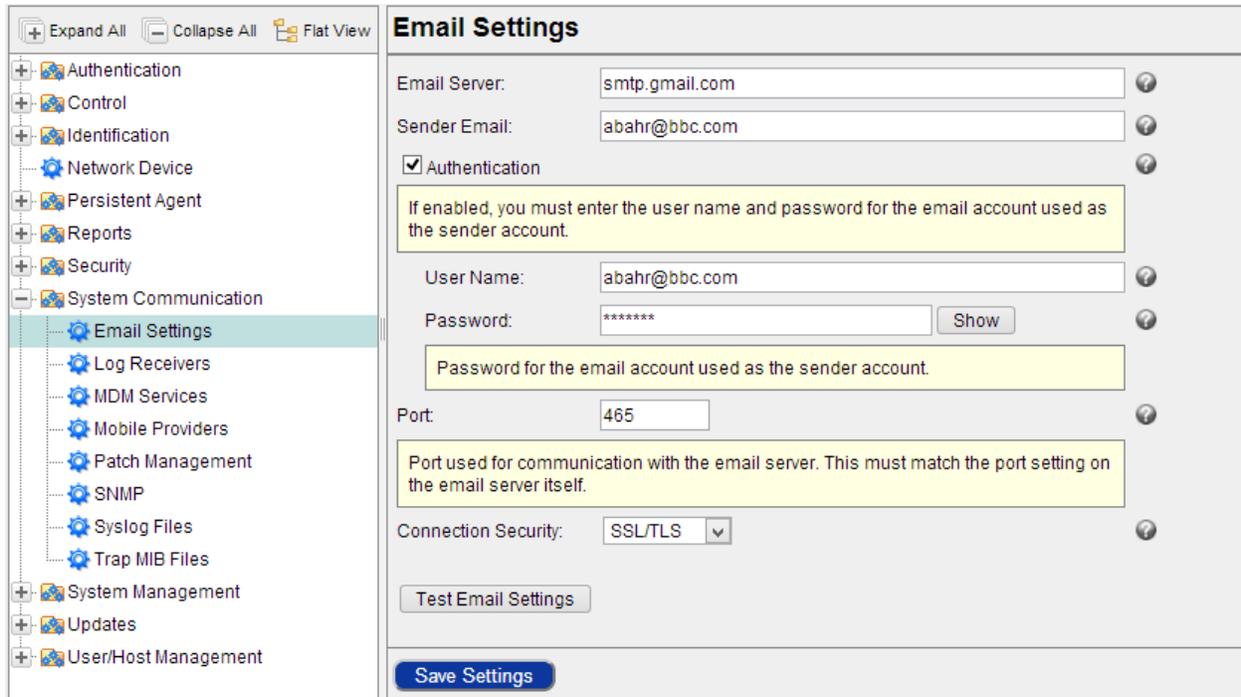


Figure 36: Field Level Help Example

## Filters

Views that allow filtering have additional fields displayed in a panel at the top of the screen. Filter fields are added one at a time from a list of possible pieces of data. Typically this is a list of the column titles that are displayed in the View. Possible fields vary depending on the View being accessed.

The Filter section can be opened or closed using the + and — symbols in the title bar. Wild card characters can be used in text based fields.

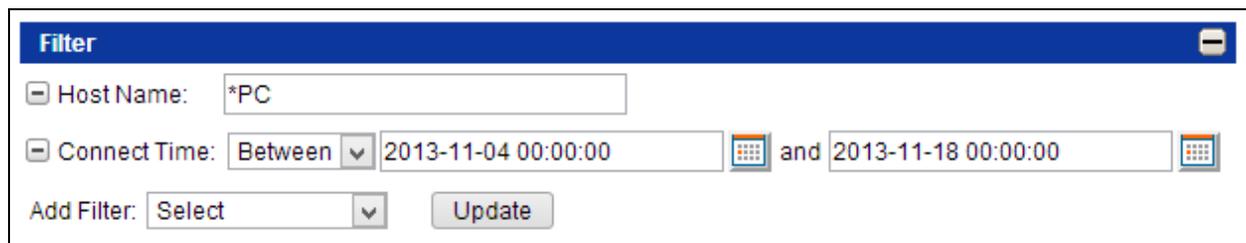


Figure 37: Filter Example

### Filter A View

1. Navigate to a view that has a filter panel at the top.
2. Click in the **Add Filter** field and select a data type to use as a filter, such as Host Name.

3. A field is displayed for the data to be used as a filter. In the example shown above, \*PC is entered as filter for Host Name. Enter the appropriate filter data.
4. Continue adding filter fields and filter data as needed.
5. Click **Update** to display the filtered data in the table.
6. **To remove a filter**, click the - symbol next to the field. Click Update to refresh the data in the table.

### **Filter Types**

Each view that has filters has options that are specific to that particular view. For example, Guest Contractor Accounts allows you to filter by account type. However, there are some filter options that are common to any views. The table below lists filters that are common across many views. Detailed filter information is available in the Help for each individual view.

**Table 7: Filter Types**

<b>Type</b>	<b>Definition</b>
<b>Time</b>	<p>Filters that involve date and time:</p> <p><b>Last</b> — Searches for timestamps within the last X number of minutes, hours or days by counting backwards from the current date and time.</p> <p><b>Between</b> — Searches for timestamps between the Start and End time - entered in YYYY/MM/DD hh:mm AM/PM format.</p> <p><b>Month</b> — Searches for timestamps between the month's start and end dates. For example, if March is selected, the filter searches for timestamps between 03/01/2015 00:00:00 and 03/31/2015 23:59:59.</p> <p><b>After</b> — Searches for timestamps after the Start time entered in YYYY/MM/DD hh:mm AM/PM format.</p> <p><b>Before</b> — Searches for timestamps before the Start time entered in YYYY/MM/DD hh:mm AM/PM format.</p> <p>Use the calendar button at the end of each field to select a date.</p>
<b>Enabled</b>	<p><b>Enabled</b> — Record is enabled, such as a Guest Account.</p> <p><b>Disabled</b> — Record is disabled, such as a guest account.</p>
<b>Host Type</b>	<p><b>Registered</b> — Search includes only registered hosts or devices.</p> <p><b>Rogue</b> — Search includes only rogue or unregistered hosts or devices.</p>

Type	Definition
<b>Authentication Type</b>	<p><b>Local</b> — Validates the user to a database on the local FortiNac appliance.</p> <p><b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</p> <p><b>RADIUS</b> — Validates the user to a RADIUS server. If an integrated RADIUS server has been added under RADIUS Settings and the Authentication Type field is set to RADIUS, a RADIUS User record is automatically added to the RADIUS User's view for this user.</p>
<b>IP Address</b>	IP Address of the connecting host or device.
<b>Physical Address</b>	MAC Address of the connecting host or device.
<b>Location</b>	Name of the device and port where the host or device connected.
<b>Group</b>	Name of the group containing that contains devices, ports, users or hosts.
<b>Container</b>	Name of the Container in which a device is a member.

### Wild Cards

When searching using a text field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP Address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records.  Any search field that starts and ends with square brackets "[]" and has one or more commas "," is treated as a list of values.
!	!192. in the IP Address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
![...]	![Windows] in the Operating System field returns all records that do not contain Windows in the Operating System field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).
<esc>!	<esc>!Windows in the Operating System field returns records that match !Windows. The "<esc>" allows you to search for data that contains an exclamation point (!).



## Chapter 3: Settings

The Settings View provides access to global system configuration options.

The Settings View is navigated using the tree control on the left side. The top level of the hierarchy represents the general configuration area, such as Authentication or System Communication. These areas are used to group similar functions. When a top level option such as System Communication is selected, the panel on the right contains a list of links to options that can be configured. For example, if System Communication is selected, the links provided include: Email Settings, Log Receivers, Mobile Providers, Proxy Settings, and SNMP. These options are also displayed below System Communication in the tree.

Use the **Flat View** button above the tree to list all of the options in alphabetical order instead of grouped in folders. Use the **+ Expand All** and **- Collapse All** buttons at the top of the tree to open and close all of the folders. Click on the **+** symbol next to a folder to open it. Click on the **-** symbol to close the folder. Click on an option to display the corresponding configuration panel on the right.

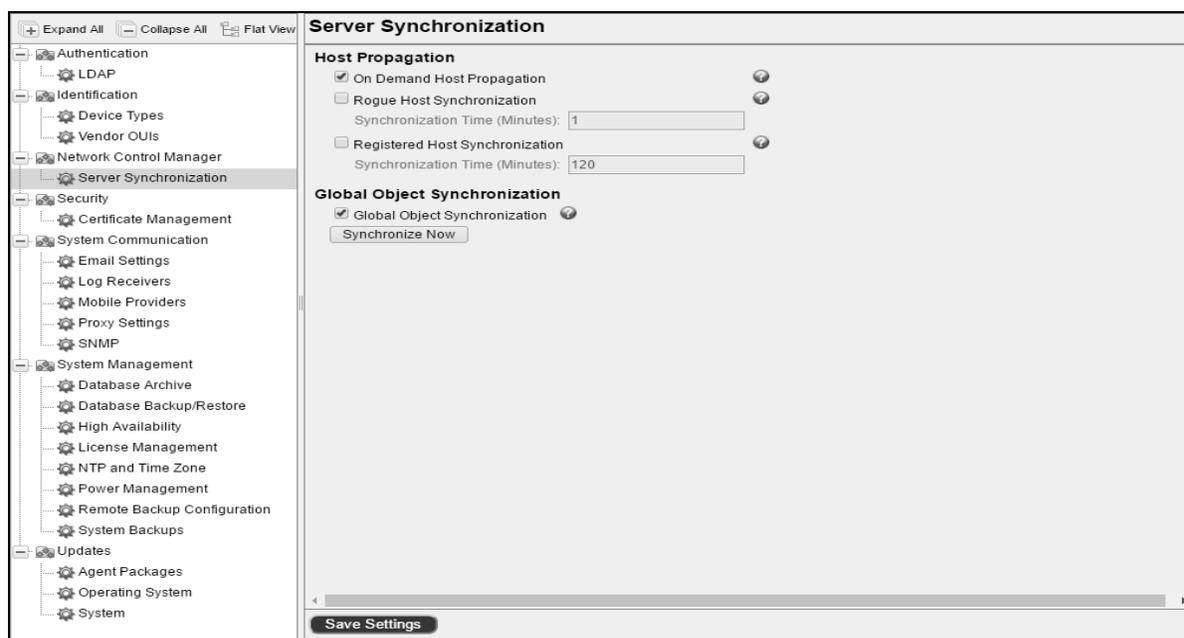


Figure 38: Settings View

Table 8: Settings View Options

Option	Description
Authentication	

<b>Option</b>	<b>Description</b>
<b>LDAP</b>	Configure the connection with one or more LDAP directories for user authentication. See Authentication Directories on page 67 and Directory Configuration on page 71.
<b>Identification</b>	
<b>Device Types</b>	Manage device types that are used in Vendor OUIs, Hosts (registered as devices), Device Profiling Rules, and Pingable Devices. Both system and custom device types are displayed.  See <b>Device Types</b> on page 99.
<b>Vendor OUIs</b>	Allows you to modify the Vendor OUI database, which is used to determine whether or not a MAC address is valid or by Device Profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 103.
<b>Network Control Manager</b>	
<b>Server Synchronization</b>	Create a list of MAC addresses that will be ignored when they connect to the network.  See <b>Server Synchronization</b> on page 111
<b>Security</b>	
<b>Certificate Management</b>	Manage, view, and install certificates with different encoding schemes and file formats.  See <b>Certificate Management</b> on page 116.
<b>System Communication</b>	
<b>Email Settings</b>	Enter settings for your email server. This allows Network Sentry to send email to Administrators and network users. See <b>Email Settings</b> on page 125.
<b>Log Receivers</b>	Configure a list of servers to receive event and alarm messages from Network Sentry. See <b>Log Receivers</b> on page 127.
<b>Mobile Providers</b>	Displays the default set of Mobile Providers included in the database. Network Sentry uses the Mobile Providers list to send SMS messages to guests and administrators. The list can be modified as needed. See <b>Mobile Providers</b> on page 130.
<b>SNMP</b>	Set the SNMP protocol for devices that query Network Sentry for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See <b>SNMP</b> on page 134 and <b>Register Hosts And Users With SNMPv3 Traps</b> on page 138.
<b>System Management</b>	
<b>Database Archive</b>	Set the age time for archived data files and configure the schedule for the Archive and Purge task.  See Database Archive on page 147.

Option	Description
<b>Database Backup/Restore</b>	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups on the Network Sentry server, not backups on a remote server.  See <b>Database Backup/Restore</b> on page 150.
<b>License Management</b>	View or modify the license key for this server or an associated Application server.  See <b>License Management</b> on page 156.
<b>High Availability</b>	Configuration for Primary and Secondary appliances for High Availability. Saving changes to these settings restarts both the Primary and Secondary servers.  See <b>High Availability</b> on page 153.
<b>NTP And Time Zone</b>	Reset the time zone and NTP server for your Network Sentry appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up. Requires a server restart to take effect.  See <b>NTP And Time Zone</b> on page 161.
<b>Power Management</b>	Reboot or power off the Network Sentry server. In the case of a Network Sentry Control Server / Application Server pair, reboot or power off each server individually.  See <b>Power Management</b> on page 163.
<b>Remote Backup Configuration</b>	Configure Scheduled Backups to use a remote server via FTP and/or SSH.  See <b>Configure The Remote Backup Destination</b> on page 166.
<b>System Backups</b>	Create a backup of all system files that are used to configure Network Sentry.  See <b>System Backups</b> on page 170.
<b>Updates</b>	
<b>Agent Packages</b>	Displays a list of the Dissolvable, Persistent and Passive Agent versions available on your FortiNac appliance. Download new agents and add them to Network Sentry as they become available from Fortinet using the Download button. Download an Administrative template for GPO configuration to your PC from the FortiNac appliance using the links at the top of the view.  See <b>Agent Packages</b> on page 173.
<b>Operating System</b>	Use Operating System Updates to download and install updates to the operating system on FortiNac Control Manager.  See <b>Operating System Updates</b> on page 177.
<b>System</b>	Use System Updates to configure download settings, download updates from Fortinet, install updates and view the updates log.  See <b>System Update</b> on page 180.

## Authentication

Enabling authentication allows the Administrator to determine whether or not hosts connecting to the network will be forced to authenticate. Hosts can be forced to reauthenticate after a specified period of time.

Once a host is registered the host connecting via a wired connection may or may not have to authenticate depending on what port is being used. Hosts connecting via a wireless connection will be forced to authenticate if an Authentication VLAN has been established.

Switches used in the Forced Authentication process must have a value entered for the Authentication VLAN in the model configuration. The ports on these switches must be added to the Forced Authentication group. See **Groups View** on page 681 for details on adding ports to a group.

Option	Definition
<b>LDAP</b>	Use LDAP to configure the connection to one or more authentication directories. Data from the Directory populates the Network Sentry database with demographic data for registered users.  See Authentication Directories on the facing page

## Authentication Directories

Use the Authentication Directories View to configure the connection with one or more LDAP directories. If you plan to use local authentication via the Network Sentry database or RADIUS authentication then this step is not necessary.

A directory is a database that contains the records of an organization's members. You can organize the members into groups within the directory. If configured in Network Sentry the Directory can be used to authenticate network users.

The Directory configuration validates the user and populates the user record in the Network Sentry databases with user-specific information before they are allowed access to the network. Network Sentry uses the LDAP protocol to communicate to an organization's directory.

A user's record is made up of fields that contain information about the user such as first name, last name, and email address. The name of a field in a directory is defined by a schema. For example, the schema specifies that a user's first name is stored in a field with an attribute name of "givenName". This attribute name is used when retrieving a user's first name from the record. Attribute names can vary from directory to directory, so Network Sentry allows you to define your own fields. Users in an "ou" in the Directory are populated into a group in Network Sentry if the Distinguished Name (DN) attribute is entered in the Directory group attribute mappings view.

**Important:** When an Admin Group is created in Network Sentry with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

## Authenticate Using A Domain Name

If you chose to authenticate using a domain name, you must consider the following:

- When a domain name is specified in the Directory Configuration view and the login includes the matching domain, authentication first uses both the user name and the domain name. If this authentication fails, no further authentications are attempted.
- When a domain name is specified in the Directory Configuration view and the login includes a domain that does not match the Directory Configuration view, the authentication immediately fails.
- When no domain is specified in the Directory Configuration view and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.
- Domain names must be an exact match. For example, if the Directory Configuration view specifies the domain as somedomain.com, a login of

john.smith@it.somedomain.com is not authenticated because the domain specified is not an exact match.

- Valid formats for login are: user, user@domain.com and domain\user.

### Authenticate Using Domain Names And Multiple Directories

If you are using multiple directories to authenticate users, you must consider the following:

- When one directory is configured and no domain is specified in the Directory Configuration view, authentication is attempted using the one directory.
- When multiple directories are configured and no domain is specified in the Directory Configuration view, authentication is attempted to all directories that are in the database. The order in which the directories are processed cannot be controlled, and the first directory that yields a successful authentication is used. Therefore, if settings such as Security & Access Attribute Value, Role, etc., are not identical between all configured directories, a user's network access can vary based on which directory settings are in effect. These settings will depend on the most recent Directory Sync.
- When multiple directories are configured, authentication is attempted against all directories without Domain configurations, or with Domain configurations matching the domain, if one is supplied. If a Domain is configured for the directory, the user must supply a matching value for their domain in order for authentication to be attempted to that directory.

## Directory Set Up Requirements

The following steps provide a basic outline for the procedures required to setup the Directory and its communication with Network Sentry.

1. Enable ping on the Directory Server itself. This allows Network Sentry to ping the Directory server and prevents the server Icon in the Network Device Summary panel on the dashboard from displaying an error as if it had lost contact when, in fact, it is in contact via LDAP.

**Note:** If you plan to use the top level (root) of the Directory tree as a Group search branch, make sure that you use Config Wizard to configure DNS in Network Sentry so that the IP address of the Directory can be resolved to the Directory's hostname. In addition, the IP Address must be resolved by the Primary DNS server.

2. Set up the connection between the Directory application and Network Sentry. This step provides login information allowing Network Sentry to connect and communicate with the Directory. See **Directory Configuration** on page 71 and **Add/Modify Directory - Connection Tab** on page 72.
3. Map directory data fields to Network Sentry data fields. This step allows you to import user and group information into your database. See **Add/Modify Directory - User Attributes Tab** on page 76 and **Add/Modify Directory - Group Attributes Tab** on page 80.
4. Configure User and Group Search Branches. See **Add/Modify Directory - Search Branches Tab** on page 81.
5. Data in your directory can change frequently. Users could be added, removed or modified. Those changes need to be incorporated into your Network Sentry database. Create a schedule to synchronize the directory with the Network Sentry database. See **Schedule Directory Synchronization** on page 83.
6. If you plan to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. See **Create A Keystore For SSL Or TLS Communications To LDAP** on page 85.
7. If you choose to use logon/logoff scripts to register the host machine when a user logs on or off a domain, see **Passive Registration Using The Domain Controller** on page 89.

**Note:** You may need to access your Directory using a separate interface to acquire login, group and user information.

**Note:** If you create new users in the Directory, be sure not to assign a User ID that is the same as an existing user account or guest account in the Network Sentry database. Having duplicate User ID's will prevent one or both of the users from accessing the network.

### **Directory Structure And Synchronization**

When synchronizing Network Sentry with a directory there are specific configuration tasks that must be completed. Network Sentry does not have a view into the structure of your directory, however, you must understand this structure to complete the configuration.

You may have your own application to view the attributes of your directory or there are some available on the Internet, such as, Active Directory Explorer, LDAP Administrator or Apache Directory.

## **Directory Configuration**

The Directory Configuration window allows you to configure the connection to the directory, user attributes that you would like to import, User Search Branches and Group Search Branches. Each configuration section has specific information that must be entered to allow Network Sentry to connect with the Directory and import users and groups.

Use the Schedule button to configure the intervals for synchronizing the database with the selected Directory. Use the Preview button to review data in the selected Directory. Use the Copy button to pre-populate directory configuration fields for a new directory connection. Refer to **Add/Modify Directory - Connection Tab** on page 72 for field definitions.

---

**Note:** Prior versions of Network Sentry did not always require a Physical Address for the Directory server. If you are modifying an existing Directory Configuration and that configuration does not have a Physical Address for the Directory server, you will not be able to save your changes until the Physical Address has been added.

---

Directory Configuration can be accessed from **System > Settings > Authentication > LDAP**.

**Figure 39: Directories View**

### Add/Modify Directory - Connection Tab

The Connection tab contains the parameters required for communication with the Directory. Not all fields are required. Be sure to enter information only in those fields that apply to your directory.

The screenshot shows a 'Modify Directory' dialog box with a 'Connection' tab selected. The dialog contains the following fields and options:

- Name:** Directory
- Primary IP:** 172.16.96.10
- Security Protocol:** None
- MAC Address:** 00:0C:29:6B:39:B2
- LDAP Login:** cm
- LDAP Password:** (masked with asterisks)
- Credential Status:** (empty)
- Validate Credentials** (button)
- Additional Configuration**
- Domain Name:** (empty)
- Secondary Server:** (empty)
- Use only when user names contain domain.** (checkbox, unchecked)
- Version:** 3
- Port:** 389
- Time Limit:** 5 seconds
- Enable Synchronization of Users/Groups at scheduled time**
- Remove Users deleted from the Directory**
- Perform Lookup On Referral**
- Connect by name.**

Buttons for **OK** and **Cancel** are located at the bottom right of the dialog.

Figure 40: Directory - Connections Tab

### Connections Tab Field Definitions

Field	Description
<b>Name</b>	Name of the server where the directory is hosted.
<b>Primary IP</b>	IP Address of the primary directory server. The server will be added as a pingable device.
<b>Security Protocol</b>	<p>The security protocol used when communicating with the server containing your directory. Options are SSL, STARTTLS, and None.</p> <p>See <b>Create A Keystore For SSL Or TLS Communications To LDAP</b> on page 85 for instructions on importing and storing certificates.</p> <p><b>Note:</b> If SSL or STARTTLS are chosen you must have a security certificate from a Certificate Authority. The certificate should be stored in the following directory on your appliance <code>/bsc/campusMgr/</code></p>
<b>MAC Address</b>	Physical Address of the primary directory server. This field is required.
<b>LDAP Login</b>	User login name Network Sentry uses to access the LDAP server.
<b>LDAP Password</b>	Password for the user login.
<b>Validate Credentials</b>	Click to verify that directory credentials are correct.
<b>Credential Status</b>	Displays the results of clicking the Validate Credentials button. Messages such as Credentials Verified or Failed to Validate can be displayed.
<b>Additional Configuration</b>	Displays the fields listed below in this table.
<b>Domain Name</b>	<p>If this field contains a domain name, users must include the domain name in their login to be authenticated against this directory.</p> <p>Example:</p> <p>Valid formats for login are: user, user@domain.com and domain\user.</p> <p>Setting a value here requires all users to supply a domain name during login.</p> <p>When no domain is specified in the Directory Configuration view and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.</p>
<b>Secondary Server</b>	FQDN or IP Address of the secondary directory server. This server would be accessed in the event that the Primary server was unavailable. This server is added as a pingable device.
<b>Version</b>	Directory version. Default = 3

<b>Field</b>	<b>Description</b>
<b>Port</b>	<p>Communication port used by the directory. The default port is based on the security protocol. To use a port other than the default, type the desired port number into this field.</p> <p>Common port values/protocols are:</p> <ul style="list-style-type: none"><li>• None = 389</li><li>• SSL = 636</li><li>• STARTTLS = 389</li></ul>
<b>Time Limit</b>	<p>Time in seconds that Network Sentry waits for a response from the directory. Default = 5.</p> <p>The number of seconds may need to be increased in the Directory or in Network Sentry if the exception "Time Limit Exceeded" begins to be noted more often.</p>
<b>Enable Synchronization of Users/Groups At Scheduled Time</b>	<p>Check this box to synchronize the Network Sentry database with either the Primary or the Secondary Directory servers based on a schedule in the Scheduler View.</p>
<b>Remove Users Deleted From The Directory</b>	<p>When checked, users that have been removed from the directory will be removed from the Network Sentry database when the scheduled resynchronization takes place.</p>
<b>Perform Lookup On Referral</b>	<p>Referrals allow administrators to set up search paths for collecting results from multiple servers. If you have configured your directory for referrals and you want to do authentication on the referred directory servers, enable this option.</p>
<b>Connect by Name</b>	<p>Automatically checked when StartTLS is selected as the Security Protocol.</p> <p>Network Sentry connects to LDAP using the the Name field of the Directory Configuration with a URL such as <code>ldap://dc.example.com</code> to connect to the primary server.</p> <p>When not selected, Network Sentry will connect to LDAP using the Primary IP address field of the Directory Configuration with a URL such as <code>ldap://10.0.0.2</code>.</p>

The Administrator must enter the specific connection information for the Directory server used for user authentication. The Security information required varies depending on the type of directory you are using. Be sure to enter only the data required for your directory type.

The Directories View can be accessed either from **System > Settings > Authentication > LDAP**.

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. To modify a directory, select a directory in the list and click **Modify**.
5. To add a directory, click **Add**.
6. A list of directories found on your network is displayed. Click on the name of the directory to be added. If the directory is not listed, click **Enter Manually**. Directories are found based on SRV records on your corporate DNS.
7. Use the information in the Field Definitions table above to enter connection information.
8. Click the **Connection** tab and enter connection information.
9. Click **Validate Credentials** to verify the connection.
10. If Network Sentry is able to successfully connect to the Directory a **Credentials Verified** message is displayed in the Credential Status field.
11. To ensure that the user data is available to Network Sentry, you must also complete the User Attributes, Group Attributes, Search Branches and Select Groups tabs. See **Add/Modify Directory - User Attributes Tab** on page 76 .
12. Click **Next** to continue.

### Add/Modify Directory - User Attributes Tab

To add users from an LDAP compliant directory, the customer user database schema must be mapped to the Network Sentry user data. Attributes can be mapped for users and groups by selecting the tabs on the left side of the window.

If a user in the directory has multiple attributes with the same attribute ID, Network Sentry uses the first one it finds. For example, if a record looked like the one shown below, Network Sentry would use staff.

eduPersonalAffiliation=staff

eduPersonalAffiliation=employee

eduPersonalAffiliation=alum

eduPersonalAffiliation=student

The Attribute Mappings for the user are entered on the User Attributes Tab. The AD attributes are mapped on this form for User Description, Contact, Hardware, and Security and Access. This allows Network Sentry to retrieve the user information based on the User Search Branches configured on the Search Branches tab. See **Add/Modify Directory - Search Branches Tab** on page 81.

### Enter User Attribute Mappings

When adding a directory Network Sentry attempts to determine the directory type and populates the attribute fields based on the directory type. Do not modify the Directory Type unless it is incorrect. Do not modify the attributes unless they are incorrect.

**Important:** The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by Network Sentry.

1. To access **User Attributes** for an existing Directory select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. If you are **adding a new Directory**, the User Attributes tab is displayed when you click **Next** after completing the Connection tab.
5. The Directory Type drop-down indicates the type of directory being configured. This will scan the directory based on the type selected and pre-populate some of the fields. The directory type should already be listed for you. If the directory type is not listed or you know the field names for your directory, this step is not required.
6. Enter the user attribute mappings. See the **User Tab - Directory Attributes Table** on page 77 for the list of attributes.

**Important:** The Last Name and Identifier (ID) fields are required entries. User records in the directory must have data entered in the selected ID and last name fields.

7. To ensure that the user data is available to Network Sentry, you must also complete the Group Attributes, Search Branches and Select Groups tabs. See **Add/Modify Directory - Group Attributes Tab** on page 80 .
8. Click **Next** to continue.

Figure 41: Directory - User Attribute Mappings Tab

**Note:** If you are using Active Directory, keep in mind that Active Directory only allows access via LDAP to users whose primary group is the Domain Users group.

**User Tab - Directory Attributes Table**

User Attributes	Active Directory	Novell
Object Class	user	person
<b>Description</b>		
First Name	givenName	givenName
Last Name *	sn	sn
Identifier *	sAMAccountName	cn
Title	title	

User Attributes	Active Directory	Novell
E-mail	userPrincipalName	
<b>Contact</b>		
Address	streetAddress	mailstop
City	l	city
State	st	S
Zip/Postal Code	postalCode	
Phone	telephoneNumber	Telephone Number
Mobile Phone	mobile	
Mobile Provider	otherMobile	
<p><b>Important:</b> The provider contained in the Mobile Provider field in the Directory must match a provider in the Network Sentry database or SMS messages cannot be sent to that user's Mobile phone. Depending on the configuration of your directory, otherMobile may not be the location of the Mobile Provider field.</p>		
<b>Security And Access</b>		
Security Attribute	The Directory Attribute that can be used in a filter. Data contained in this field is copied to the Security and Access value field on the User Properties and the Host Properties record for each user and associated host when the directory synchronizes with the database.	
Allowed Hosts	The number of host records each individual user may have in Network Sentry.	
Role	Name of the Directory Attribute used to associate a user with a role.	
<p><b>Important:</b> Matching roles must be created in Network Sentry with the exact same spelling and case as the roles that exist in the directory based on the selected attribute. See Roles on page 615.</p>		
<p><b>Important:</b> When assigning Roles to users, the use of Directory attributes over Directory groups is recommended. Under no circumstances should you use both methods to assign roles.</p> <p>Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the Network Sentry server and could be out-dated.</p>		
Disabled Attribute	<p>Setting this attribute allows the AD Administrator to disable users in Active Directory and have all instances of the user automatically disabled in Network Sentry when the next scheduled resync occurs.</p> <p>Attribute = userAccountControl</p>	

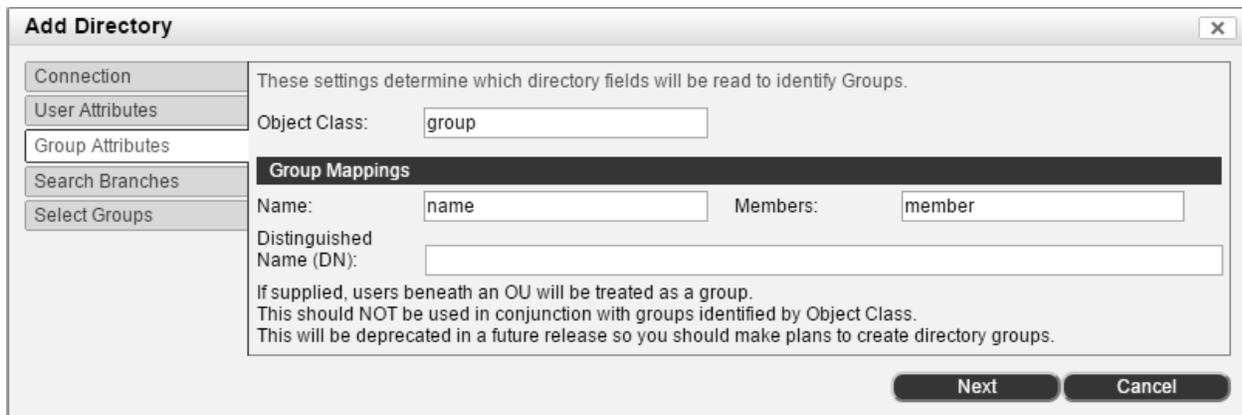
User Attributes	Active Directory	Novell
<p><b>Important:</b> Disabled users are able to access the network until Network Sentry resynchronizes with the Active Directory. To immediately disable all instances of the user in Network Sentry, go the Scheduler View and run the Synchronize Users with Directory task. See <b>Scheduler View</b> on page 705 for more information.</p>		
<b>Disabled Value</b>	<p>When the value for the Disabled Attribute for the user equals the Disabled Value, Network Sentry disables all instances of a user when the next scheduled resync with AD occurs. The user must have previously been disabled in AD.</p> <p>The Disabled Value may vary from directory to directory. Check a user that is currently disabled in the directory to see what the disabled value should be. Enter that value in the Disabled Value field.</p> <p>If "Disabled Value" starts with a "0x", a bitwise comparison is done between the value in the directory and this field.</p> <p>Otherwise, without the "0x" prefix, it will only do an exact match numeric comparison.</p>	
<p><b>Note:</b> If you are using Active Directory, it is possible for the Disabled Value to vary from user to user. The value is affected by other account settings selected within the directory, such as, Password Never Expires or User Must Change Password At Next Login. You may only be able to set the Disabled Value for users that have identical account settings. See <a href="https://support.microsoft.com/en-us/kb/305144">https://support.microsoft.com/en-us/kb/305144</a> for more information on these values.</p>		
<b>Time To Live</b>	<p>The name of the directory attribute that contains the numerical value for the user age time. If the attribute does not have a value the user age time is not set by the directory.</p> <p>Age time can also be set using the Network Sentry Properties window or on the User Properties window for an individual user.</p> <p>All of these options simply modify the Expiration Date in the User Properties window. See <b>User Properties</b> on page 404.</p> <p><b>Note:</b> The value of the attribute in the Time To Live field must be set to the name of the custom attribute that is configured in the directory as the numerical value of hours or days for which the user is valid.</p>	
<b>Time to Live Unit</b>	<p>The time unit set in the User Properties age time if the Time to Live attribute contains a value.</p> <p>Options: Hours or Days</p>	

**Add/Modify Directory - Group Attributes Tab**

The Attribute Mappings for groups are entered on the Group Tab. The AD attributes are mapped on this form for Object Class, Group Name and Members. This allows Network Sentry to retrieve the group information based on the Group Search Branch configured on the Search Branches Tab. See **Add/Modify Directory - Search Branches Tab** on page 81. Groups created in the directory are imported into Network Sentry each time the Directory Synchronization task is run either manually or by the Scheduler.

**Note:** Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields. For additional information see [Microsoft Knowledge Base Article 2009267](#).

**Important:** The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by Network Sentry.



**Figure 42: Directory - Group Attribute Mappings Tab**

1. To access **Group Attributes** for an existing Directory select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. If you are **adding a new Directory**, the Group Attributes tab is displayed when you click **Next** after completing the User Attributes tab.
5. Enter the group attribute mappings.

Group Attributes	Active Directory	Novell
Object Class	group	groupOfMembers

Group Attributes	Active Directory	Novell
Group Name	name	cn
Group Members	member	member
Distinguished Name (DN)		

**Important:** The DN is not to be used in conjunction with groups identified by Object Class.

6. To ensure that the user data is available to Network Sentry, you must also complete the Search Branches and Select Groups tabs. See **Add/Modify Directory - Search Branches Tab** on page 81.
7. Click **Next** to continue.

### Add/Modify Directory - Search Branches Tab

The Search Branches tab is where the Administrator enters the specific User and Group Search Branches information for the Directory server. This tells Network Sentry where the user and group information is located in the Directory.

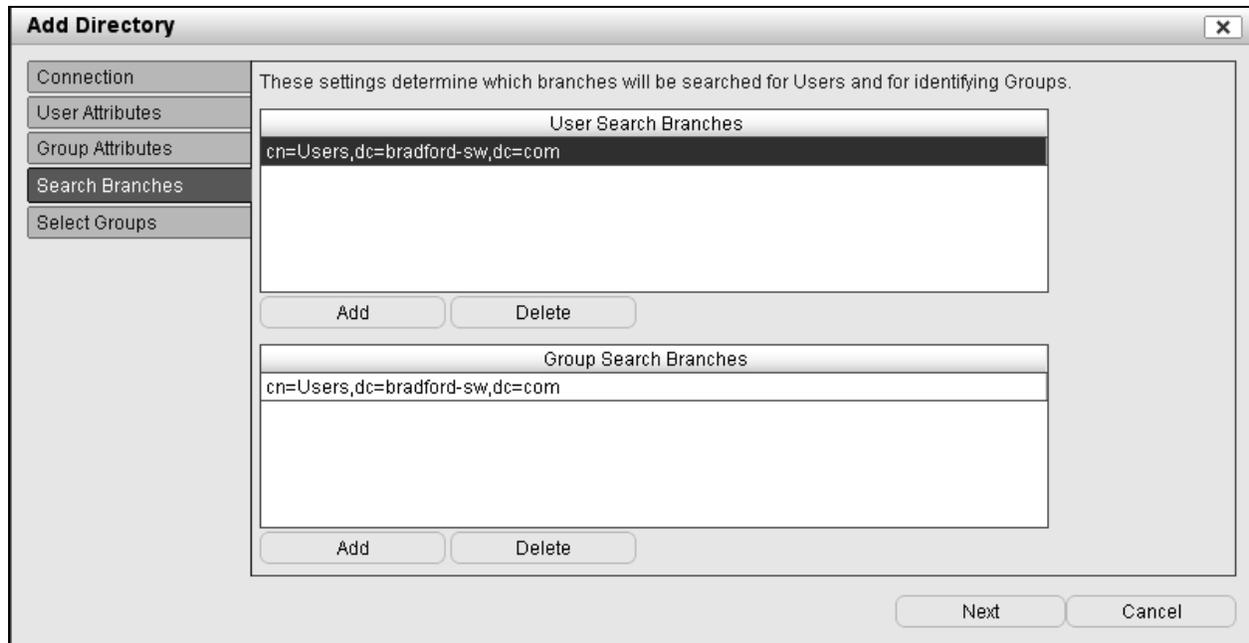
**Note:** Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields. For additional information see [Microsoft Knowledge Base Article 2009267](#).

The example shown in the figure below is for Active Directory. In this example the segments represent the following:

**cn=Users**—The abbreviation cn stands for Common Name. In this case, it is the name of the branch or folder in Active Directory that should be searched for users. The name of that branch could be anything, such as, Employees or Students.

**dc=bradford-sw**—The abbreviation dc stands for Domain Component. In this case it is the second level domain name, such as, yahoo in yahoo.com.

**dc=com**—The abbreviation dc stands for Domain Component. In this case it is the first level domain name, such as, com in google.com or edu in marshalluniversity.edu or org in npr.org.



**Figure 43: Directory - Search Branches Tab**

1. **To access Search Branches** for an existing Directory select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. **To modify an entry** in the Search Branches list, select the **entry** and click **Modify**.
5. **To remove an entry** in the Search Branches list select the **entry** to be removed and click **Delete**.
6. If you are **adding a new Directory**, the Search Branches tab is displayed when you click **Next** after completing the Group Attributes tab.
7. Click **Add** to add new search branch information. Available search branches are listed, however you can enter your own information. If the list of available search branches is too long to display, type the first few letters of the branch needed to narrow the list.
8. In the Add dialog, enter or select the **Search Branch**, and then click **OK**.
9. To ensure that the user data is available to Network Sentry, you must also complete the Select Groups tab. See **Add/Modify Directory - Select Groups Tab** on page 83.
10. Click **Next** to save search branch information.

### Add/Modify Directory - Select Groups Tab

Use the Select Groups tab to choose groups of users to be included when the directory and the Network Sentry database are synchronized. Users that do not already exist in Network Sentry are not imported. However, user data for users already in the database is updated each time the Synchronization task is run. Only the user records for users in the selected groups are updated. Users in the directory that are not in a selected group are ignored during Synchronization.

|

**Figure 44: Directory - Select Groups Tab**

1. **To access Group Selections** for an existing Directory select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
  1. Click **LDAP** to display the Directories window.
  2. If you are **adding a new Directory**, the Select Groups tab is displayed when you click **Next** after completing the Search Branches tab.
  3. Mark the Groups of users that should be included when the Directory and the database are synchronized by checking the box in the **Active** column. If you do not check any boxes, all Groups will be included.
  4. A check mark in the **Is Organizational Unit** column indicates that the group is an OU or a container for other groups. This field cannot be edited.
  5. Click **OK** to save the directory configuration.
  6. An initial Synchronization is done immediately when you save the Directory. It is recommended that you set up a schedule for synchronizing the Directory See **Schedule Directory Synchronization** on page 83.

### Schedule Directory Synchronization

The Schedule button on the Directories View allows the Administrator to select a date/time and poll interval for the directory synchronization task. The scheduled task may also be paused and run manually later. This process adds the **Synchronize Users with Directory** task to the Scheduler View.

When the Directory and Network Sentry are synchronized changes made to users in the Directory are written to corresponding user records in the database. Users from the Directory are only added to the Network Sentry database when they connect to the network and register. Directory groups are added to the Network Sentry database each time a synchronization occurs. Groups created in the directory are displayed in Network Sentry on the Groups View. Specific directory groups can be disabled from Attribute Mappings. See **Add/Modify Directory - Select Groups Tab** on page 83.

If you are using a directory for authentication, user data is updated from the directory based on the User ID during synchronization. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID on the user record matches a User ID in the directory, the Network Sentry database is updated with the directory data.

---

**Important:** When an Admin Group is created in Network Sentry with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

---

**Note:** The Directory Schedule is global and applies to all directories listed. Separate schedules cannot be entered for each directory.

---

|

**Figure 45: Directory Schedule**

### Schedule Field Definitions

Field	Definition
<b>Schedule Interval</b>	Poll interval for the scheduled task. Options are Minutes, Hours, or Days.
<b>Next Scheduled Time</b>	The next date/time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM.
<b>Enabled</b>	When unselected, the scheduled synchronization task is stopped and does not run automatically. To run the task manually click Run Now.
<b>Run Now</b>	Runs the Synchronization task immediately.

### Schedule Directory Resynchronization

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory in the list and click **Schedule**.
5. Set a **Schedule Interval** by entering a number and selecting Minutes, Hours, or Days from the drop-down menu.
6. Click in the **Next Scheduled Time** field and enter the **date/time** to run the synchronization task.
7. To stop the scheduled task, remove the check mark from click in the **Enabled** box.

**Note:** If the scheduled task is disabled, the Administrator can go to the Scheduler view and run the task manually to synchronize the directory with Network Sentry. See **Scheduler View** on page 705 for details.

8. To run the scheduled task immediately, click **Run Now**.
9. Click **OK** to save the schedule.

### Create A Keystore For SSL Or TLS Communications To LDAP

If you choose to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. You must obtain a valid certificate from a Certificate Authority. That certificate must be saved to a specific directory on your FortiNac appliance.

SSL or TLS protocols are selected on the Directory Configuration window when you set up the connection to your LDAP directory. See **Add/Modify Directory - Connection Tab** on page 72 for information on configuring the connection to your LDAP directory. Follow the steps below to import your certificate.

**Note:** You should be logged in as root to follow this procedure.

1. When you have received your certificate from the Certificate Authority, copy the file to the `/bsc/campusMgr/` directory on your FortiNac server.
2. Use the `keytool` command to import the certificate into a keystore file.

For example, if your certificate file is named `MainCertificate.der`, you would type the following:

```
keytool -import -trustcacerts -alias <MyLDAP> -file MainCertificate.der -keystore .keystore
```

**Note:** Depending on the file extension of your certificate file, you may need to modify the command shown above. For additional information on using the `keytool` key and certificate management tool go to the Sun web site [java.sun.com](http://java.sun.com).

3. When the script responds with the **Trust this certificate?** prompt, type **Yes** and press **Enter**.
4. At the prompt for the keystore password, type in the following password and press **Enter**:  
`^8Bradford%23`
5. To view the certificate, navigate to the `/bsc/campusMgr/` directory and type the following:  

```
keytool -list -v -keystore .keystore
```
6. Type the password used to import the certificate and press **Enter**.

**Note:** The keystore is cached on startup. Therefore, it is recommended that you restart Network Sentry after making any changes to the keystore.

## **Preview Directory**

Use **Preview** to view the list of users that are found in the directory. User records in the directory are not listed until a parameter is selected and its associated value is entered in the Filter field.

**Note:** The Directory Configuration must be completed before any records can be previewed. See **Add/Modify Directory - Connection Tab** on page 72 for additional information.

### **Figure 46: Preview Directory - Users**

To view user and group records:

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory in the list and click **Preview**.
5. Enter search criteria in the first text field, such as an ID or Last Name.  
Use asterisks (\*) as wild cards in text fields if you know only a portion of a name. The wild card represents any characters. Searches are not case-sensitive.  
For example, enter F\* in the text field and select the First Name parameter to locate all records where F is the first character in the First Name field.
6. Select a **parameter** from the drop-down list.
7. Click **Search**.

**Note:** An asterisk in the Role column next to an attribute value indicates that the role name has not been configured in Network Sentry. If the role does exist in Network Sentry, the attribute value appears in the Role column without an asterisk.

**WARNING:** Entering just the wild card in the text field returns every record in the directory and may cause time or size limit exceeded errors to occur depending on the total number of records.

**Important:** This is a view only list and is NOT imported into Network Sentry. The user information is only imported into the Network Sentry database as the user registers. The Sync Directory task in the Scheduler View is used to update user information already in the Network Sentry database with any changes made in the Directory database. See **Scheduler View** on page 705 for additional information.

8. Click the **Groups** tab to view the groups in the Directory and select the groups to import.

All the groups in the Directory are listed along with the number of member records contained in each group.

**Note:** Selecting groups is part of the process of adding a Directory configuration, therefore, groups may already be selected.

|

**Figure 47: Preview Directory - Groups**

9. **To import groups** of user records from the Directory to the Network Sentry database when the Directory Synchronization scheduled task runs select the groups to be imported by checking the box(es) next to the group name.
10. A check mark in the **Is Organizational Unit** column indicates that the group is an OU or a container for other groups.
11. Click **OK**

## **Passive Registration Using The Domain Controller**

You can configure Network Sentry to automatically run logon and logoff scripts and register the host machine when a user logs on or off a domain. This process allows users to be tracked as they use various machines on the network. The registration process is not visible to the user. Logon and logoff scripts are provided, but must be customized for your configuration.

To use login or logout scripts, you must be using an LDAP directory for authentication and it must be configured in Network Sentry. See **Directory Set Up Requirements** on page 69 for an overview on configuring your Directory.

Make sure that Authentication is enabled. See **Authentication** on page 66.

## **Host Registration vs Device Registration**

Host registration associates the host with a user. Device registration has no associated user and the host is registered by its host name. Both types of hosts are displayed in the Host View.

## **Customize Login And Logout Scripts**

Network Sentry allows you to register hosts using login and logout scripts. These scripts are provided for you on the appliance. They contain variables that must be modified to match your environment and requirements. Scripts are located in the following directory:

```
/bsc/campusMgr/ui/runTime/config/ldap
```

Scripts that should be modified include `sendLogIn.vbs`, `sendLogOut.vbs`. It is recommended that you review the comments contained within the script. They contain the most up to date information about variables that can be used and additional parameters that can be set.

To use the scripts they must be copied to the directory server, such as your Active Directory Server. After they have been copied, use the information in the **Variables** on page 91 and **Trap Parameters** on page 94 tables below to modify the necessary parameters.

To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from <http://www.net-snmp.org/download.html>. Select the latest binaries. From the list of download files select the file that is in the following format: net-snmp-<version number>.exe.

## **Registration Types**

There are two types of registration that can be done using scripts. A machine can be registered as a host with an associated user or as a device with no identity. When a machine is registered as a device, the host name of the device is used. Machines can also be left as rogues.

If you are registering shared machines, such as computers in a lab, you may want to modify the script to register the computers as devices.

Registration Type	Settings
<b>Host / User</b>	Register the machine as a host by user name.  REG_ROGUE = "0"  REG_BY_USER = "1"
<b>Device</b>	Register the machine as a device by host name.  REG_ROGUE = "0"  REG_BY_USER = "0"

**Registration Examples**

Status	First Name	Last Name	User ID	User Expires	Email	Phone
▼	Moe	Howard	Moe	10/29/10 08:25 AM EDT	mhoward@bnetworks.	603-555-1212
Type	Status	Host Name	Operating System		Role	Actions
Registered		dulcimer	Windows Vista (TM) Business 6.0 Service Pack 2		NAC-Default	

**Figure 48: User View - Registration Type Host/User**

Status	Host Name	Host Role	Registered To	Logged On User	
▼	dulcimer	NAC-Default	Moe		
Status	IP Address	Physical Address	Media Type	Location	Actions
	192.168.10.182	00:19:D1:94:5C:06	Wired	Lab Switch 45	

**Figure 49: Host View - Registration Type Host/User**

In the two examples above, the login script was set to register by user. Both the machine and the user are shown, first from the User View and second from the Host View. The machine shows as Type - Registered, indicating that it is registered to a user. The machine is associated with or Registered To the user.

Status	First Name	Last Name	User ID	Email	Phone	User Role
	Larry	Fine	Larry			NAC-Default
Type	Status	Host Name	Operating System	Role	Actions	
Logged On		LAB_XP	Microsoft Windows XP 5.1 Service Pack 3	NAC-Default		

Figure 50: User View - Registration Type Device

Status	Registered To	Logged On User	Host Name	Host Role	
		Larry	LAB_XP	NAC-Default	
Status	IP Address	Physical Address	Media Type	Location	Actions
	192.168.35.150	00:18:8B:AD:1B:8F	Wired	HF-TestSwitch Fa0/16	
		00:19:D2:48:A4:8E	Wireless		

Figure 51: Host View - Registration Type Device

In the two examples above, the login script was set to register by device. Both the machine and the user are shown, but there is no association between the machine and the user. The User View example shows Type - Logged On, indicating that the user is logged onto this machine but that the machine is not Registered to a user. The Registered To field is blank. The Host View represents the actual computer. The User View represents the temporary user who logged into the machine.

## Variables

Variable	Definition
<b>Required Variables</b>	
<b>ACTION</b>	Indicates whether this script is for logon or logoff.  Type = Integer Logoff = 0 Logon = 1 Logon Started = 2  Example: ACTION = "1"
<b>REG_ROGUE</b>	When Register is enabled, machine is registered either by user name or as a device by host name based on the Register by User setting.  If Do not register is enabled, the machine remains a rogue.  Type = Integer Register = 0 Do not register = 1  Example: REG_ROGUE = "0"

Variable	Definition
<b>WHITELIST</b>	<p>If enabled, adds the machine to the Forced User Authentication Exceptions group. A user logging in on a machine in this group is not forced to authenticate. Default is disabled.</p> <p>Type = Integer Do not add = 0 Add = 1</p> <p>Example: WHITELIST = "0"</p>
<b>REG_BY_USER</b>	<p>Registers the machine by user name as a host or by host name as a device.</p> <p>Type = Integer Register as device = 0 Register by user name = 1</p> <p>Example: REG_BY_USER = "0"</p>
<b>DIRECTORY_SERVER</b>	<p>Your Active Directory server. If you have more than one Active Directory server for failover, it is recommended that you use your domain name instead of the IP address.</p> <p>Example: DIRECTORY_SERVER = "192.168.102.2"</p> <p>Example: DIRECTORY_SERVER = "bradfordnetworks.com"</p>
<b>DIRECTORY_SHARED</b>	<p>Active Directory server's shared directory where the login/logoff scripts, snmp-trap.exe and libsnp.dll files are stored. If you have more than one Active Directory server for failover, it is recommended that you use your domain name instead of the IP address.</p> <p>Example: DIRECTORY_SHARED = "\\192.168.102.2\sysvol\eng.local\scripts\"</p> <p>Example: DIRECTORY_SHARED = "\\bradfordnetworks.com\sysvol\eng.local\scripts\"</p>
<b>Novell Specific Variables</b>	
<b>USE_ENV_USERNAME</b>	<p>Indicates whether or not the user name should come from another variable. To enable, set this to True.</p> <p>If you are <b>not</b> using Novell or if the User Name entered at login is sufficient, set this to False.</p> <p>Example: USE_ENV_USERNAME = False</p>
<b>ENV_USERNAME_VARIABLE</b>	<p>The variable containing the User Name. This information is used only if USE_ENV_USERNAME is set to True.</p> <p>Example: ENV_USERNAME_VARIABLE = "%NWUSERNAME%"</p>
<b>Optional Changes - Sample</b>	

Variable	Definition
<b>Wscript.Sleep 5000</b>	Add before the last "End If" statement. This makes the script wait 5 seconds allowing more time for processes to start or finish.  REM End If Wscript.Sleep 5000 End If Next End Function

You may choose to make other modifications to the script to accommodate requirements outside Network Sentry. For example, you may choose to add a timer that waits a few seconds before ending the script.

### Trap Parameters

The login and logout scripts send a trap to Network Sentry that contains the values of the variables listed above along with registration parameters from the user. To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **lib-snmplib.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from <http://www.net-snmp.org/download.html> . Select the latest binaries. From the list of download files select the file that is in the following format: net-snmp-<version number>.exe.

OID	Description	Definition
1.1	Action	Value of the Action variable.
1.2	User Name	User name of the person logging in or out. Type = String
1.3	Machine Name	Hostname of the machine used to log in or out. Type = String
1.4	Machine IP	IP address of the machine used to log in or out. Type = IP Address
1.5	Machine MAC	MAC address of the machine used to log in or out. Type = String
1.8	Operating System	Operating System of the machine used to log in or out. Type = String
1.10	Register Rogue	Value of the Reg_Rogue variable.
1.11	Whitelist	Value of the Whitelist variable.
1.12	Register by User	Value of the Register by User variable.

## Active Directory Setup For Passive Registration

Passive registration can be set up for one or more groups of users.

1. Copy the following files from the runtime area

```
<Host Name>/ui/runTime/config/ldap
```

to the AD shared directory, generally located at:

```
/WINNT/SYSVOL/<domainname>/sysvol/scripts
```

Files to be copied:

```
sendLogIn.vbs, sendLogOut.vbs
```

**Note:** Permissions should be set such that all users may read and execute on all the files.

2. To receive traps from the scripts, you must have the latest versions of **snmp-trap.exe** and **libsnmp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from <http://www.net-snmp.org/download.html> . Select the latest binaries. From the list of download files select the file that is in the following format: net-snmp-<version number>.exe.
3. If you have not already done so, customize the scripts so that they take into account your network setup. See **Customize Login And Logout Scripts** on page 89 for detailed information.
4. Configure AD to use the following scripts:

```
sendLogIn.vbs and sendLogOut.vbs
```

- a. Start the **Active Directory Users & Computers** application.
- b. Click the **domain name** in the Tree panel to select it.
- c. Right-click and select **Properties**.
- d. In the Properties window, click the **Group Policy** tab.
- e. Double-click the policy (Default Domain Policy) that will enable the scripts.
- f. In the **Group Policy** window click the plus sign (+) next to the **User Configuration** folder, then click the plus sign (+) next to the **Windows Settings** folder, and click **Scripts (Logon/Logoff)**.
- g. In the right panel of the Group Policy view, double-click the logon script to launch the Logon Properties view. Click the **Add** button, then click the **Browse** button and navigate to the `sysvol` folder where files were copied in step 1. Select the following:
 

```
sendLogIn.vbs
```
- h. Once the script file has been added, click **OK**.
- i. In the right panel of the Group Policy view, double-click the logoff script to launch the Logoff Properties view. Click the **Add** button, then click the

**Browse** button and navigate to the `sysvol` folder where the files were copied in step 1. Select the following:

```
sendLogOut.vbs
```

- j. Once the script file has been added, click **OK**.
5. In the Group Policy view, click **New** to add a new policy for each group of users. For **FortiNac users** change the name to **CM\_Policies**.

For **Guest users** change the name to **Guest\_Policies**.

6. Double-click the new policy. The Group Policy window will appear.
7. In the **Group Policy** window click the plus sign (+) next to the **User Configuration** folder, then click the plus sign (+) next to the **Windows Settings** folder, and click **Scripts (Logon/Logoff)**.

- a. In the right panel of the Group Policy view, double-click the logon script to launch the Logon Properties view. Click the **Add** button, then click the **Browse** button and navigate to the `NETLOGON` directory on the domain controller. Select the following:

```
sendLogIn.vbs
```

- b. Once the script file has been added, click **OK**.
- c. In the right panel of the Group Policy view, double-click the logoff script to launch the Logoff Properties view. Click the **Add** button, then click the **Browse** button and navigate to the `NETLOGON` directory on the domain controller. Select the following:

```
sendLogOut.vbs
```

- d. Once the script file has been added, click **OK**.
8. In the **Group Policy** window for the Group Policy created in step 3 Click the plus sign (+) in front of the User Configuration folder.
9. Click the plus sign (+) in front of the Administrative Templates folder, and then click the plus sign (+) in front of the System folder. Click the Logon/Logoff folder.
10. Enable the following policies by double-clicking on them, clicking **Enable**, and then clicking **OK**.

```
Run logon scripts visible
```

```
Run logoff scripts visible
```

```
Run logon scripts synchronously
```

**Note:** Visible mode only needs to be enabled for the testing period. Once the Administrator has determined that the logon/logoff scripts are working, running in visible mode can be disabled.

11. Roll the policy changes to the host. AD has built-in delays so reboot the hosts if the scripts fail to run. The delay can be shortened by setting the "Group Policy

refresh interval for user" to a shorter time period. The policy is located in the User Configuration folder.

This MS link explains the above in detail:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;322241>

### Novell Setup For Passive Registration

This setup can be used for network users. The following steps are only necessary on a PC platform:

1. Copy the files listed below from Network Sentry `/bsc/campusMgr/ui/runTime/config/ldap` to the directory from which the scripts are run.  
`sendLogIn.vbs, sendLogOut.vbs`

Set the permissions on all copied files to read and execute for all.

To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from <http://www.net-snmp.org/download.html> . Select the latest binaries. From the list of download files select the file that is in the following format: net-snmp-<version number>.exe.

2. Configure the "Login Script" attribute in all users and groups within the directory to use the following:

`sendLogIn.vbs`

This is done by setting the "Login Script" attribute to either `sendLogIn.vbs` or `gscLogin.vbs` depending on your users.

See Novell's users guide for detailed instructions.

<http://www.novell.com/documentation/edir873/index.html>

## Identification

Identification options include:

Option	Definition
<b>Device Types</b>	Manage device types that are used in Vendor OUIs, Hosts (registered as devices), Device Profiling Rules, and Pingable Devices. Both system and custom device types are displayed.  See <b>Device Types</b> on page 99.
<b>Vendor OUIs</b>	Allows you to modify the Vendor OUI database, which is used to determine whether or not a MAC address is valid or by Device Profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 103.

## Device Types

The Device Types view allows you to view and manage device types that are used in Vendor OUIs, Hosts (registered as devices), Device Profiling Rules, and Pingable Devices. Both system and custom device types are displayed. You can view all device types in the system, as well as each device type icon state. You can also add, modify, or delete custom device type icons. The In Use button allows you to see whether a device type is currently being used in the system.

**Note:** The supported formats for custom device type icons are .jpg (or .jpeg), .bmp, .wbmp, .png, and .gif.

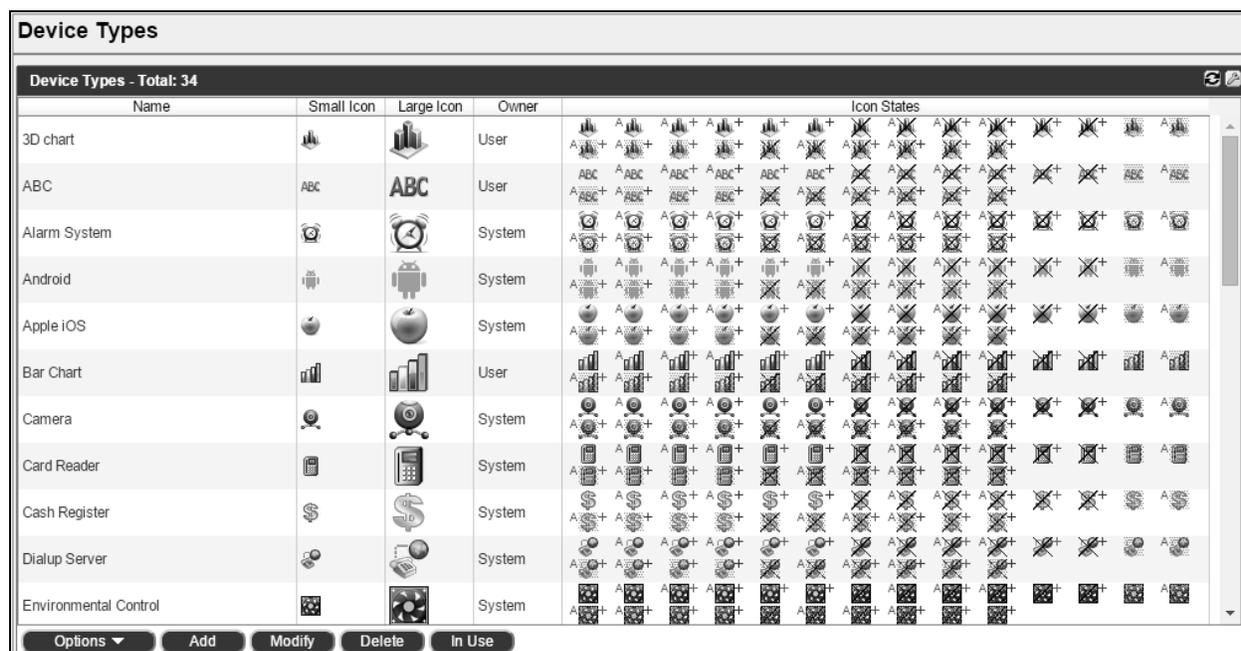


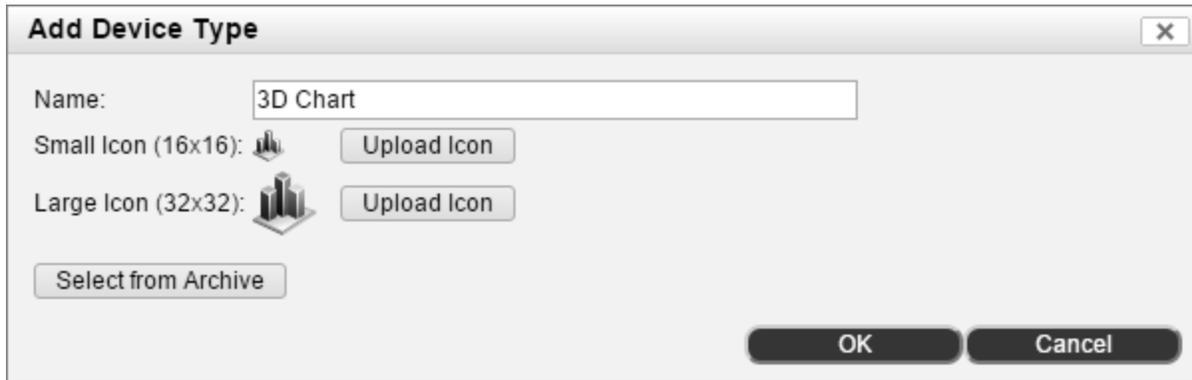
Figure 52: Device Types

### Device Types Field Definitions

Field	Definition
<b>Name</b>	The name of the device type. Custom device type names can be changed. System device type names cannot be changed.
<b>Small Icon</b>	Shows how the small (16 x 16 pixels) device type icon is displayed in the system.
<b>Large Icon</b>	Shows how the large (32 x 32 pixels) device type icon is displayed in the system.
<b>Owner</b>	Indicates whether the device type icon is a pre-defined system icon or a user-defined custom icon.

<b>Field</b>	<b>Definition</b>
<b>Icon States</b>	Displays how the device type icon appears for each icon state. See <b>Icon Key</b> on page 14 for a definition of the icon states.
<b>Buttons</b>	
<b>Add</b>	Allows the user to add custom device types. <b>Note:</b> You must add both a small (16 x 16) and a large (32 x 32) version of the device type icon.
<b>Modify</b>	Allows the user to modify a custom device type icon. <b>Note:</b> You cannot modify system device type icons.
<b>Delete</b>	Allows the user to delete custom device type icons. Only device type icons that are not in use may be deleted.
<b>In Use</b>	Indicates whether or not the selected device type icon is currently being used by any other Network Sentry element. See <b>Device Type In Use</b> on page 102.

## Add/Modify a Device Type



**Add Device Type**

Name:

Small Icon (16x16): 

Large Icon (32x32): 

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Device Types**.
3. Click the **Add** button or select an existing icon and click **Modify**.

**Note:** System icons cannot be modified.

4. Do one of the following:
  - To add a custom icon, click **Upload Icon**. You must upload both a small and large icon.
  - To add select from a list of custom icons, click **Select from Archive**, choose an icon from the list, and then click **OK**.
5. Enter a name for the device type icon, and click **OK**.

### Delete a Device Type

**Note:** System device types cannot be deleted.

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Device Types**.
3. Select the device type you wish to delete. Click **In Use** to confirm whether the device type is in use. Device types that are currently in use cannot be deleted.
4. Click **Delete**.
5. A confirmation message is displayed. Click **Yes** to delete the device type.

#### Device Type In Use

To find the list of Network Sentry features that reference a specific device type, select the device type from the Device Types View and click the **In Use** button. A message is displayed indicating whether or not the device type is associated with any other features. If the device type is referenced elsewhere, a list of each feature that references the device type is displayed.



Figure 53: Device Type In Use

## Vendor OUIs

Use the Vendor OUI database to determine whether a particular MAC is valid. As new IEEE device information becomes available, the database needs to be updated to reflect the new codes. This prevents *invalid physical address* errors when devices with the new MACs are connected to the network. The AutoDef Synchronization scheduled task automatically updates the Vendor OUI database. See **Scheduler View** on page 705 for additional information on scheduling tasks.

You can search the Vendor OUI database, and add, modify, or remove Vendor OUIs. Vendor OUI Added and Vendor OUI Removed events are generated when you add or remove Vendor OUIs.

The Vendor Name appears in the Host view unless you enter a Vendor OUI alias. If you use a Vendor OUI alias to identify the type of device, you can quickly filter all devices with a specific alias. For example, you can manage gaming devices by adding the Vendor OUI to the database with the Vendor OUI alias of *Gaming Device*. Then you can use the Host view filter to find these records by name, change them to registered, and assign them a role without requiring the device to be assigned to a user.

Vendor OUIs are also used with the Device Profiler feature. Device Profiling Rules can use the Vendor OUI to help identify rogue devices connecting the network. Depending on the instructions associated with the rule, the device can be automatically assigned a device type and be placed in the Host View, the Topology View or both. See **Device Profiler** on page 189 for additional information.

To access the Vendor OUI View select **System > Settings > Identification > Vendor OUIs**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

### Vendor OUIs

Filter -

Vendor Name:  (e.g., DELL\*)

Add Filter:  Update

Vendor OUIs - Displayed: 792 Total: 18737 ↻ 🖨

<< first
< prev
1
2
3
4
next >
last >>
200 v

Vendor OUI	Vendor Name	Registration Type	Re
00:00:15	DATAPOINT CORPORATION	Manual	^
00:00:16	DU PONT PIXEL SYSTEMS .	Manual	
00:00:20	DATAINDUSTRIER DIAB AB	Manual	
00:00:4D	DCI CORPORATION	Manual	
00:00:56	DR. B. STRUCK	Manual	
00:00:7A	DANA COMPUTER INC.	Manual	
00:00:8A	DATAHOUSE INFORMATION SYSTEMS	Manual	
00:00:AE	DASSAULT ELECTRONIQUE	Manual	v

<
>

Export to:

Add
Modify
Delete

Figure 54: Vendor OUIs View

## Vendor OUI Field Definitions

Fields used in filters are also defined in this table.

Field	Description
<b>Vendor OUI</b>	First 3 octets of a device's Physical Address. Enter in the hexadecimal format <b>##:##:##</b> (For example, 00:1D:09)
<b>Vendor Name</b>	Name of the Vendor that owns the Vendor OUI.
<b>Vendor Alias</b>	Value entered displays as the Host Name in the Host view. This field is optional when adding a Vendor OUI.
<b>Role</b>	<p>Role for devices associated with this Vendor OUI. Roles assigned by Device Profiler take precedence.</p> <p><b>Note:</b> If a device is registered via the Portal Page, then the role associated with the Vendor OUI is applied.</p> <p>See <b>Device Registration After Vendor OUI Database Update</b> on page 110 and <b>Role Management</b> on page 609.</p>
<b>Registration Type</b>	Type of device registration that is specified through the AutoDef Synchronization update, such as a Camera, a Card Reader or a Gaming Device. In the Add/Modify Vendor Code dialog the current setting for the vendor code Registration Type is displayed. Options include Manual or a specific device type.
<b>Registration Type Override</b>	Used to specify a Registration Type that is different from the default supplied by the AutoDef Synchronization update. Options include Manual or a specific device type.
<b>Description</b>	User specified description of the Vendor OUI.
<b>Last Modified By</b>	User name of the last user to modify the Vendor OUI.
<b>Last Modified Date</b>	Date and time of the last modification to this Vendor OUI.
<b>Right Click Options</b>	
<b>Delete</b>	Deletes the selected Vendor OUI.
<b>Modify</b>	Opens the Modify Vendor OUI dialog.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

### Add A Vendor OUI

The screenshot shows a dialog box titled "Add Vendor OUI". It contains the following fields and values:

- Vendor OUI: 00:1B:08 (e.g., 00:1D:09) ?
- Vendor Name: Dell ?
- Vendor Alias: (empty) ?
- Description: Dell Computers ?
- Role: NAC-Default ?
- Registration Type: Manual ?
- Registration Type Override: Use Default ?

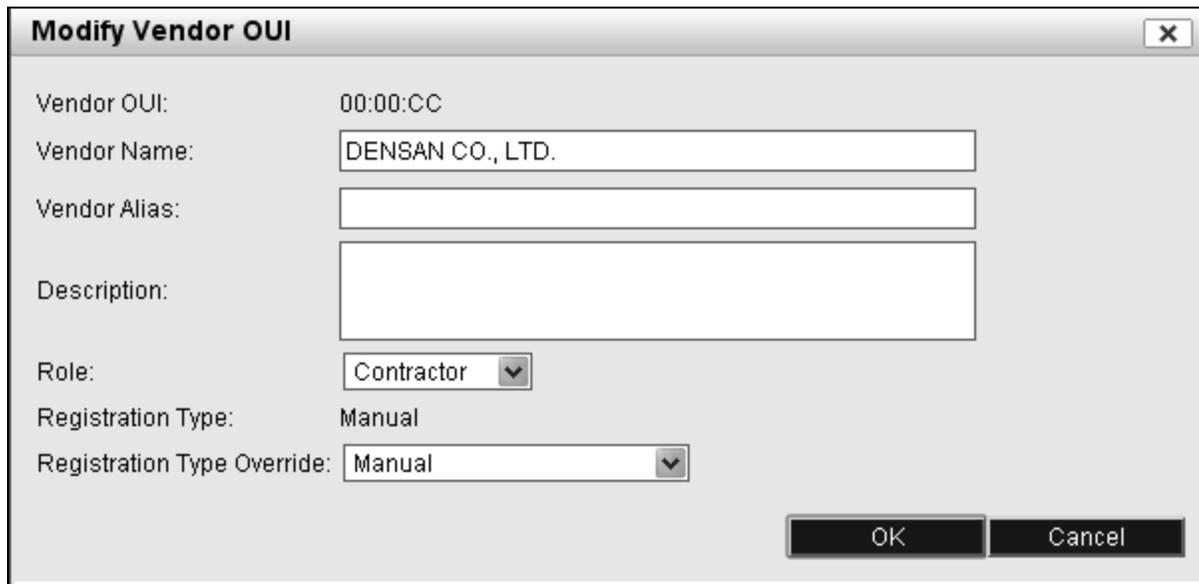
Buttons: OK, Cancel

Figure 55: Vendor OUI - Add

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Click **Add** at the bottom of the window.
4. Enter the Vendor OUI information. See **Vendor OUI Field Definitions** on page 105 for additional details.
5. The **Description** field is optional and allows you to add notes about the OUI. This field is not displayed on the Vendor OUIs view.
6. Select the Registration Type Override for the device.
7. Click **OK**.

### Modify A Vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate Vendor OUI and select it. Click **Modify**.
4. Edit the Vendor OUI information. See **Vendor OUI Field Definitions** on page 105 for additional details.
5. The **Description** field is optional.
6. Click **OK**.



The screenshot shows a dialog box titled "Modify Vendor OUI" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Vendor OUI: 00:00:CC
- Vendor Name: DENSAN CO., LTD.
- Vendor Alias: (empty text box)
- Description: (empty text box)
- Role: Contractor (dropdown menu)
- Registration Type: Manual
- Registration Type Override: Manual (dropdown menu)
- Buttons: OK and Cancel

Figure 56: Vendor OUI -Modify

### **Modify Multiple Vendor OUIs**

Multiple Vendor OUIs can be modified at the same time to update fields such as Role or Description.

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate Vendor OUIs. Select all of the affected Vendor OUIs. If they are not part of a continuous list, hold down the CTRL key to select them.
4. Click **Modify**.
5. On the Modify dialog enable the check boxes next to the fields to be updated. Any field that is not enabled will not be affected.
6. Modify the data in the selected fields. See **Vendor OUI Field Definitions** on page 105 for additional details.
7. Click **OK**.

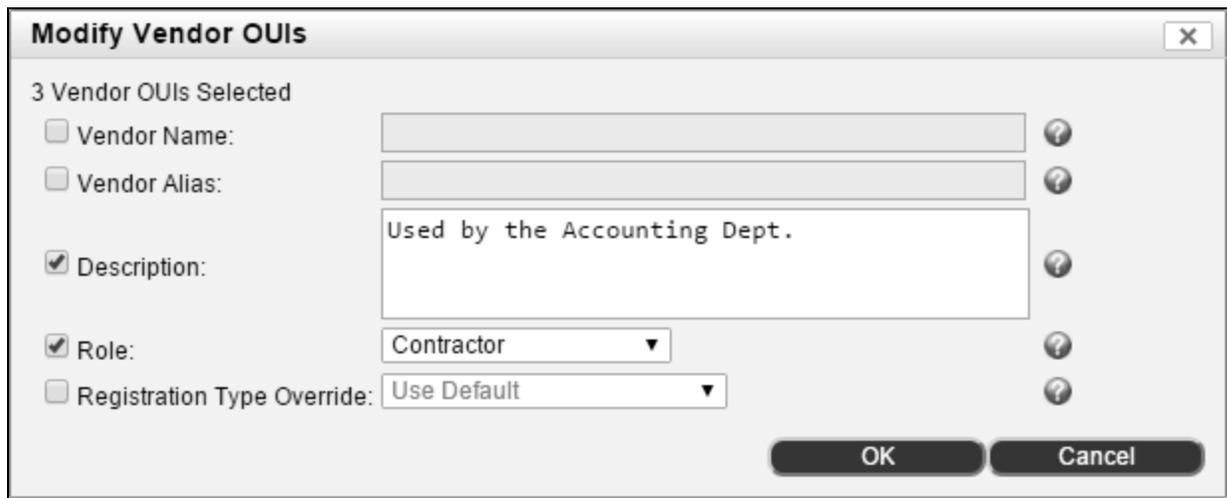


Figure 57: Modify Multiple Vendor OUIs

### **Delete A Vendor OUI**

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the Vendor OUI to be deleted and select it.
4. Click **Delete**.
5. A confirmation message is displayed. Click **Yes** to delete the OUI.

### **Register Devices**

To register devices, such as gaming devices, you must enter the Vendor OUIs in the Vendor OUI database. When the host connects the device to the network a rogue host

record is created.

1. Enter the Vendor OUIs into the database.
2. When entering the Vendor OUI be sure to fill in the **Vendor Alias** field. This alias displays on the Host View when a device with this Vendor OUI connects to the network.
3. If this device requires a role, select a **Role** on the Vendor OUI window.

**Note:** This role is only applied to devices registered manually through the Portal Page.

4. In order to register a device you must make sure that the **Registration Type Override** field in the Vendor OUI window is set to reflect the correct device type. For example, if this Vendor OUI represents a gaming device, you would select Gaming Device from the list in this field.
5. Once the device is connected to the network, click **Hosts > Host View**.
6. Locate the record for the rogue device.
7. Select the record. Then, right-click and select **Register As Device**.
8. See **Add A Vendor OUI** on page 106 for additional information.

**Note:** If you are using the Device Profiler feature, these devices may be processed by a Device Profiling Rule that registers them for you.

### Device Registration After Vendor OUI Database Update

Devices whose Vendor OUIs are not in the database appear in the Host view as rogues when they connect to the network. Once you have entered the Vendor OUI in the database, the information in the Host view displays the Vendor OUI data as part of the rogue record. Use the Vendor Alias to identify the type of device, such as gaming device or security camera, for example. The Vendor Alias is displayed in the Host Name column of the Host view.

1. Add the Vendor OUI information to the database. Include the Vendor Alias to aid in grouping the devices.
2. Go to the Host View and use the filter tabs or column sort features to locate the devices.
3. Select the record(s) and change the device to Registered using the Register As Device option on the right-click menu.

## Network Control Manager

Server Synchronization controls the replication of hosts from one Network Sentry Control Server to another.

Option	Definition
<b>Server Synchronization</b>	Server Synchronization controls the replication of hosts from one Network Sentry Control Server to another and the synchronization of global information. See <b>Server Synchronization</b> on page 111.

## Server Synchronization

Host Propagation controls the replication of hosts from one Network Sentry Control Server to another. In an environment where multiple Control Servers are being managed, it is possible for a host to connect to one Control Server and then move to another building and connect to a different Control Server.

Global Object Synchronization enables automatic synchronization of the Network Sentry Server(s) with the FortiNac Control Manager.

Figure 58: Server Synchronization View

### Host Propagation

Each Control Server then has to determine that host's state. Determining the host's state may include processes such as scanning the host or presenting a registration page, thus delaying the host's access to the network. In addition, hosts could be in conflicting states on different Control Servers.

For example, a host connects to the network via Control Server A and is presented with a registration page. The user cancels out of the page and is listed as a Rogue Host on Control Server A.

Later the same host connects to the network via Control Server B and is presented with a registration page. The user fills out the registration page and becomes a Registered Host on Control Server B. This host is now in two different states on two different Control Servers on the same network. When the host returns to Control Server A, the user will have to register there also.

Enabling the **On Demand Host Propagation** option copies a registered host from one managed server to all other managed servers when the host registers, if the associated user has the Propagate Hosts option enabled. However, if the host is already a rogue on a different managed server, the registered host is not copied. For example, if the host is a rogue on Control Server A, it registers on Control Server B and is unknown on Control Server C, then the registered host exists on Control Server B, it is copied to Control Server C, but the existence of the rogue on Control Server A prevents it from being copied there. The user would need to re-register the host on Control Server A if it connects there.

This setting and the Propagate Hosts option on User records are enabled by default. Disabling this option on the FortiNac Control Manager disables it globally. Disabling Propagate Hosts on an individual user, disables the feature only for that user.

Enabling the **Rogue Host Synchronization** option stops a rogue or unknown host from having to re-register on a second Control Server if they have already registered on any other Control Server. This option copies registered hosts only to Control Servers that have rogue hosts, not to all Control Servers. Choosing this option uses less bandwidth than the Registered Host Synchronization feature. It also allows you to view the servers to which hosts have connected. If you use the Registered Host Synchronization option, all hosts exist on all servers.

Enabling the **Registered Host Synchronization** option alleviates the need to determine whether or not an individual host is registered for each Control Server. When the host registers, that information is passed to all other Control Servers on the network. If you choose this option, you do not need to choose the previous option, since all hosts are copied to all servers.

Once a host is registered on a Control Server, the host's enabled/disabled status will be propagated, but no other attribute or state changes are propagated. The Registered Host Synchronization feature is used to speed up the registration process in an environment with multiple Control Servers.

**Note:** If the synchronization options are enabled as detailed above, registered hosts are copied from one Control Server to another when the host registers. **As the host logs on and off the network and the host state changes, these changes are not copied from one Control Server to another.**

**Note:** If both synchronization options are disabled, the FortiNac Control Manager can query all Control Servers when a host connects to determine the host's previous state. However, choosing one of the copy options reduces the amount of time a host waits to be connected to the network and provides a better user experience.

## **Global Object Synchronization**

When the **Global Object Synchronization** option is enabled, all Network Sentry Servers are automatically synchronized with the FortiNac Control Manager once per minute. Any information on the server that is older than the information on the FortiNac Control Manager is overwritten.

Upon manual synchronization, all information on the Network Sentry Server that is shared globally with the FortiNac Control Manager is overwritten.

Global information on the Network Sentry Server is read-only. The following information is shared globally between the Network Sentry Server and the FortiNac Control Manager:

- Admin Profiles
- Guest Templates
- Device Profiling Rules
- Device Types
- Groups
- Roles
- User/Host Profiles
- Endpoint Compliance Policies
- Endpoint Compliance Configurations
- Endpoint Compliance Scans
- Security Actions that are used by Endpoint Compliance configurations

### **Modify Host Propagation**

1. Select **System > Settings > Network Control Manager**.
2. Select **Server Synchronization**.
3. Under Host Propagation, do the following:
  - Select an option for the synchronization of hosts.
  - Enter a time interval for the enabled host synchronization.

4. Click **Save Settings**.

### Modify Global Object Synchronization

1. Select **System > Settings > Network Control Manager**.
2. Select **Server Synchronization**.
3. Under Global Object Synchronization, do the following:
  - To enable automatic synchronization of global information, select **Global Object Synchronization**, and then click **Save Settings**.
  - To manually synchronize global information, click **Synchronize Now**.

**Note:** Manual synchronization can also be done from **Dashboard > Server List** panel. Click the Synchronize Server icon in front of each listed server

### Server Synchronization Field Definitions

Field	Definitions
<b>Host Propagation</b>	
<b>On Demand Host Propagation</b>	If enabled, copies registered hosts to Control Servers, when the associated user has the Propagate Hosts option enabled. The Propagate Hosts option is enabled by default on every user. This option will not replace an existing rogue with a host that registered on different managed appliance. In that case, the user would have to register again on the appliance where the rogue exists.  Default = Enabled.
<b>Rogue Host Synchronization</b>	If enabled, copies registered hosts to Control Servers that have rogue hosts. Rogues that match registered hosts are replaced by the registered host records.
<b>Synchronization Time (minutes)</b>	Registered hosts are copied to Control Servers with rogue hosts each time this interval elapses.
<b>Registered Host Synchronization</b>	If enabled, copies all registered hosts to all Control Servers.
<b>Synchronization Time (minutes)</b>	Registered hosts are copied to Control Servers each time this interval elapses.
<b>Global Object Synchronization</b>	
<b>Global Object Synchronization</b>	If enabled, automatically synchronizes information between the FortiNac Control Manager and the Network Sentry Servers. The information on the Network Sentry Servers will be read-only. Automatic synchronization occurs once per minute.
<b>Synchronize Now</b>	Lets you manually synchronize information between the FortiNac Control Manager and the Network Sentry Servers.

## Security Settings

Security allows you to manage SSL Certificates.

Option	Definition
<b>Certificate Management</b>	Provides the ability to manage certificates with different encoding schemes and file formats. See Certificate Management on the next page.

## Certificate Management

Certificate Management provides users with the ability to manage certificates with different encoding schemes and file formats. The Certificate Management view shows the certificates that are currently installed on Network Sentry. Users can create and install server certificates for Admin, Portal, Persistent Agent, and RADIUS servers.

**Important:** High Availability is not automatically supported at this time. To add certificates to a secondary appliance, you must fail over and configure certificates through the Admin UI on that appliance.

The screenshot shows the 'Certificate Management' interface. At the top, there is a note: 'NOTE: High Availability is not automatically supported at this time. To add certificates to a secondary appliance, you must fail over and configure certificates through the Admin UI on that appliance.' Below the note, a header indicates 'Certificates - Total: 3'. The main content is a table with the following data:

Certificate Target	Alias	Issued To	Issued By	Expiration
Admin UI	tomcat	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT
Persistent Agent	agent	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT
Portal	portal	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT

At the bottom of the interface, there are export options (CSV, PDF, XLS) and buttons for 'Options', 'Generate CSR', 'Upload Certificate', and 'Details'.

Figure 59: Certificate Management View

### Certificate Management Field Definitions

Field	Definition
<b>Add Filter drop-down list</b>	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See <b>Filters</b> on page 59.
<b>Update button</b>	Displays the filtered data in the table.
<b>Certificate Target</b>	The component where the certificate is applied.
<b>Alias</b>	Indicates how the certificate is stored in the underlying Key-store.

Field	Definition
<b>Issued To</b>	The server that received the certificate. Displays information entered when generating the CSR.
<b>Issued By</b>	The CA that issued the certificate.
<b>Expiration</b>	The date when the certificate expires and a new certificate is required.  Users can map events to alarms when the certificate will expire or has expired. See <b>Map Events To Alarms</b> on page 493.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Buttons</b>	
<b>Generate CSR</b>	Opens the Generate CSR window to enter the CSR details. See <b>Obtain a Valid SSL Certificate from a Certificate Authority (CA)</b> on page 117.
<b>Upload Certificate</b>	Opens the Upload Certificate window to find and select the key and certificate. See <b>UI Method: Upload the Certificate Received from the CA</b> on page 121.
<b>Details</b>	Opens the details and private key information for the selected target. See <b>View the Details and Private Key Information for a Certificate</b> on page 122.

### Obtain a Valid SSL Certificate from a Certificate Authority (CA)

If you do not have a certificate, you must obtain a certificate from a CA.

To obtain a Valid Third Party SSL Certificate from a CA, you must generate a CSR and send it to the CA.

To generate a CSR, and Self-Signed Certificate:

1. Select **System > Settings**
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.

**Generate CSR**

Specify the information to use for your Certificate Signing Request.  
Note: This will generate and store a private key (in a temporary location) for use when uploading the new certificate files. Any certificates currently in place will be unaffected.

Certificate Target: Admin UI

Use Result as Self-Signed Certificate

Common Name (The fully qualified host name)  
qa228.bradfordnetworks.com

Subject Alternative Names  
www.bradfordnetworks.com

Add  
Delete

Organization  
Bradford Networks

Organizational Unit  
Dept A

Locality (City)  
Concord

State / Province  
NH

2 Letter Country Code  
US

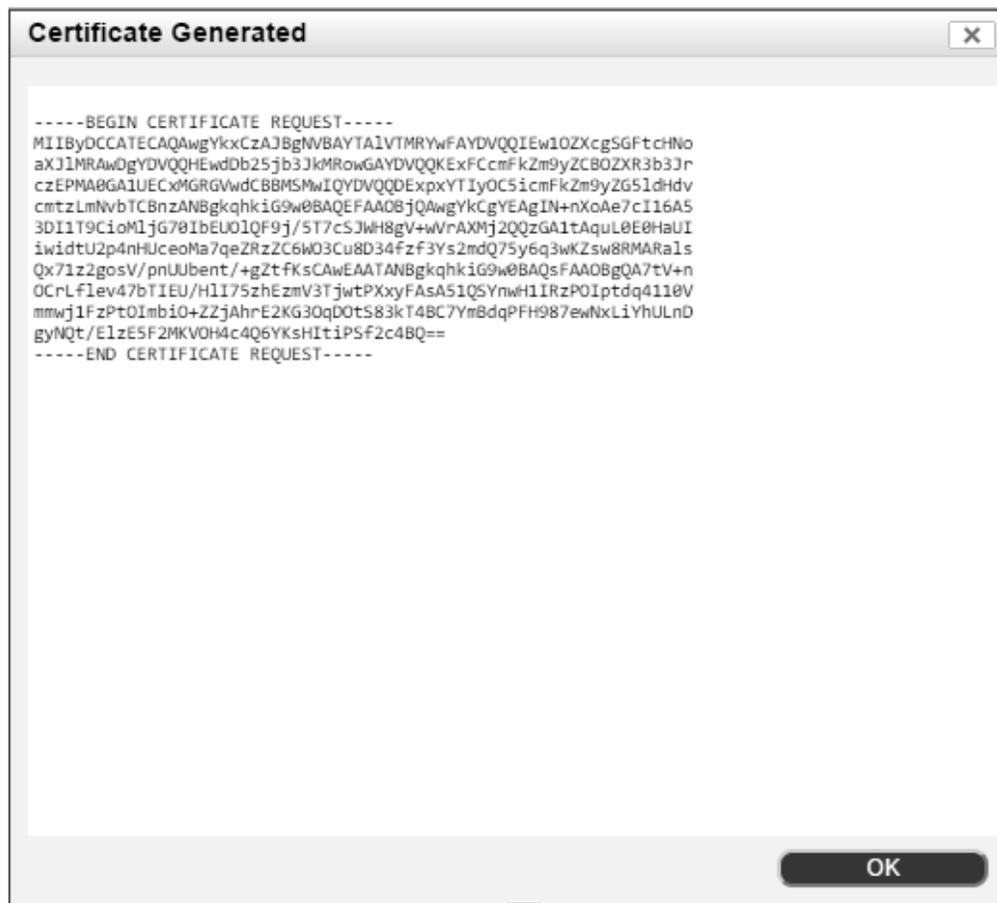
OK Cancel

Figure 60: Generate CSR

5. Select the certificate target (the type of certificate you want to generate).
  - Select **Admin UI** to generate a CSR for the administrative user interface.
  - Select **Persistent Agent** to generate a CSR for the PA communications.
  - Select **Portal** to generate a CSR to secure the captive portal and DA communications.
  - Select **RADIUS Server** to generate a CSR for integrated Network Sentry RADIUS server set to use 802.1x and PEAP.

**Note:** The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

6. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (Example: \*.bradfordnetworks.com).
7. Enter the Subject Alternative Names (leave blank if not requesting a SAN certificate). Click **Add** to enter each additional host name and/or ip address.
8. Enter the remaining information for the certificate in the dialog box.
  - Organization: The name of the server's organization.
  - Organizational Unit: The name of the server's unit (department).
  - Locality (City): The city where the server is located.
  - State/Province: The state/province where the server is located.
  - 2 Letter Country Code: The country code where the server is located.
9. Click **OK** to generate the CSR.



**Figure 61: Generated CSR**

10. Copy the section with the certificate request to include the following:

-----BEGIN CERTIFICATE REQUEST-----

...Certificate Request Data...

-----END CERTIFICATE REQUEST-----

11. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.

**Important:** Make sure there are no spaces, characters or carriage returns added to the Certificate Request.

12. Send the Certificate Request file to the CA to request a Valid SSL Certificate.

**Important Notes:**

- **Do not click OK in the Generate CSR screen after saving the Certificate Request file and sending to the CA.** Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key. Consequently, if a Certificate Request file has been submitted to the CA, and the OK button has been clicked since the original Certificate Request was generated, the returned certificate will not match the current private key, and a new request will have to be issued and sent to the CA.
- Not all Certificate Authorities ask for the same information when requesting a certificate. For example, some CA's ask for a server type (apache, etc) while others do not. Network Sentry requires a non-encrypted certificate in one of the following formats:

PEM

DER

PKCS#7

P7B

This will allow the certificate to be applied to any of the desired components.

If the certificate is in PEM format, opening the certificate in a text editor should look something like the following format:

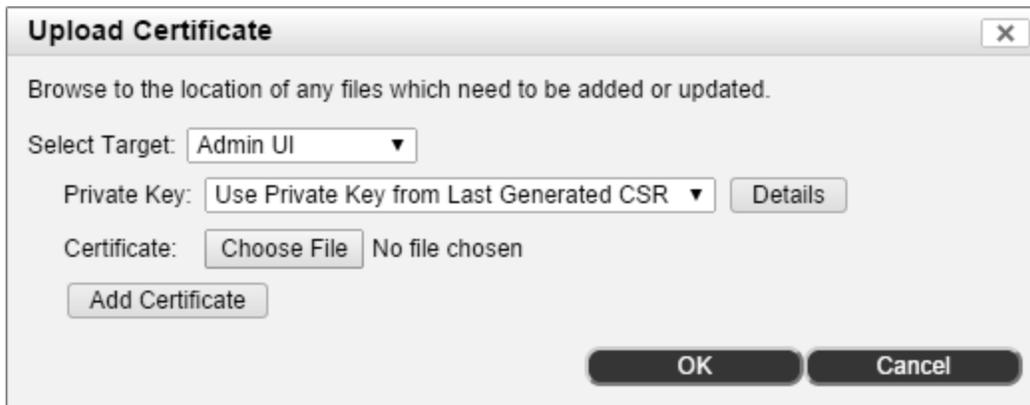
```
-----BEGIN CERTIFICATE1-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFICTATE1-----
-----BEGIN CERTIFICATE2-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFCATE2-----
```

- Certificate requests generated on Network Sentry use the SHA1 RSA encryption signature. However, certificates with SHA2 encryption can be requested using this CSR.
- Agent versions prior to 3.1.5 are not compatible with SHA2. Contact Support to verify appropriate SHA version based on current deployment.
  - Select **Admin UI** to generate a CSR for the administrative user interface.

**Note:** The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

### UI Method: Upload the Certificate Received from the CA

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.



**Figure 62: Upload Certificate**

1. Save the file(s) received from the CA to your PC.
2. Select **System > Settings**.
3. Expand the **Security folder**.
4. Select **Certificate Management** from the tree.
5. Click **Upload Certificate**.
6. Select the target where the certificate will be uploaded.
  - Select **Admin UI** to install the certificate for the administrative user interface.
  - Select **Persistent Agent** to install certificate for the PA communications.
  - Select **Portal** to install the certificate to secure the captive portal.

- Select **RADIUS Server** to install the certificate for integrated Network Sentry RADIUS server set to use 802.1x and PEAP.
7. Do one of the following:
    - Select **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
    - Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
    - Select **Upload Private Key** to upload a key stored outside Network Sentry. Click **Choose** to find and upload the private key.
  8. Click the **Choose File** button to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles.

**Important:** Upload any relevant intermediate certificate files needed for the creation of a complete certificate chain of authority. The Certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.
  9. Click the **Add Certificate** button if multiple certificates were returned. Use this to enter each additional certificate file.
  10. Click **OK**.

### View the Details and Private Key Information for a Certificate

Users can view the certificate details and private key information for the selected target.

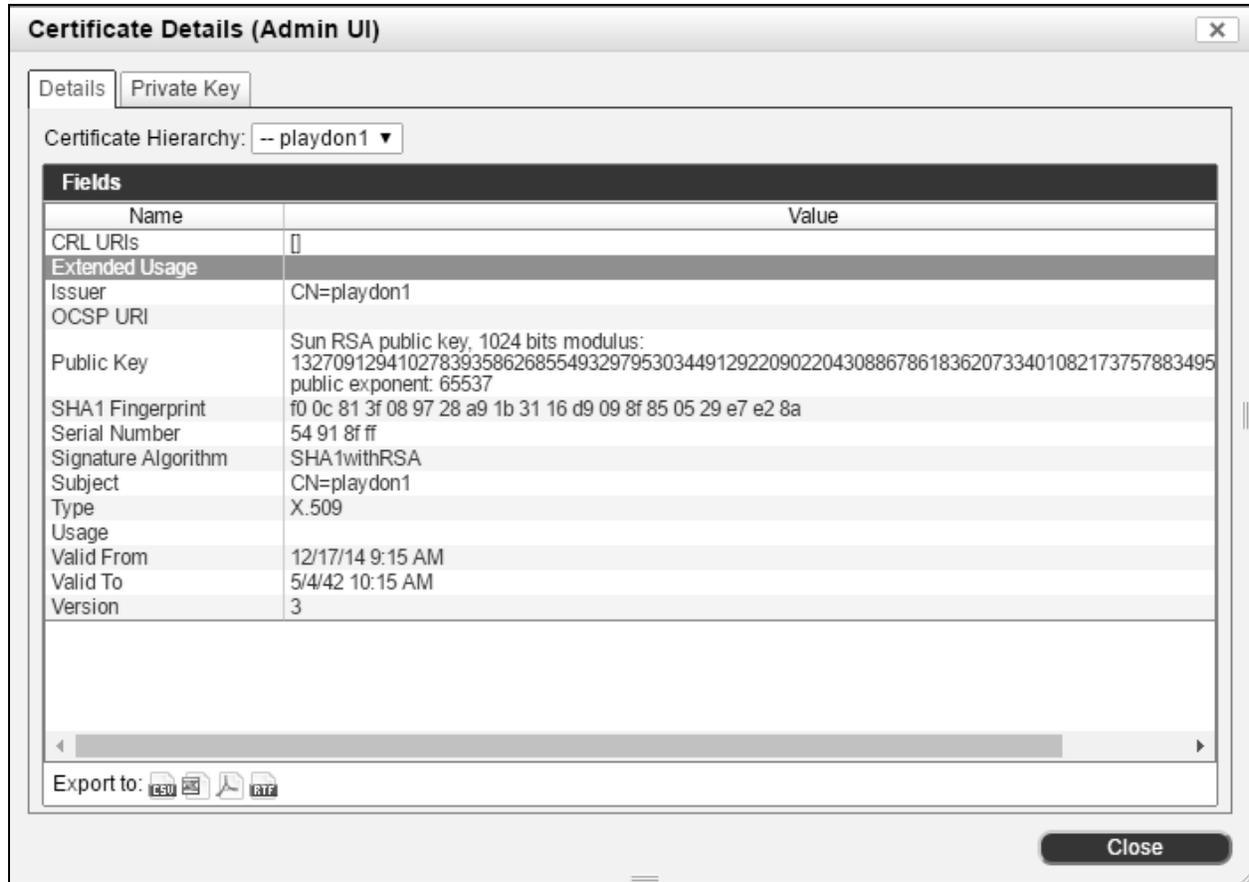


Figure 63: Certificate Details



Figure 64: Private Key

1. Click **System > Settings**.
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Details**.

## System Communication

System Communication groups together features that allow Network Sentry to communicate with other devices or to send email and SMS messages to administrators and network users.

Option	Definition
<b>Email Settings</b>	Enter settings for your email server. This allows Network Sentry to send email to Administrators and network users.  See Email Settings below.
<b>Log Receivers</b>	Configure a list of servers that to receive event and alarm messages from Network Sentry.  See Log Receivers on page 127.
<b>Mobile Providers</b>	Displays the default set of Mobile Providers included in the database. Network Sentry uses the Mobile Providers list to send SMS messages to guests and administrators . The list can be modified as needed.  See Mobile Providers on page 130.
<b>SNMP</b>	Set the SNMP protocol for devices that query Network Sentry for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users.  See SNMP on page 134.
<b>Proxy Settings</b>	Configure Network Sentry to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.

## Email Settings

### Email Settings

Email Server:  ?

Sender Email:  ?

Authentication ?

    User Name:  ?

    Password:  Show ?

Port:  ?

Connection Security:  ?

Advanced ?

---

Figure 65: Email Settings

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Email Settings** from the tree.
4. Use the table of field definitions below to enter the necessary settings.
5. Click **Save Settings**.

**Table 9: Email Settings Field Definitions**

<b>Field</b>	<b>Definition</b>
<b>Email Server</b>	Server used to send email notifications.
<b>Sender Email</b>	Email address that appears as the sender in email sent from FortiNac. You may want to configure an alias for this email address to better inform the recipient that the message is being sent from FortiNac.
<b>Authentication</b>	If enabled, you must enter the user name and password for the email account used as the sender account.
<b>User Name</b>	User Name for the email account used as the sender account.
<b>Password</b>	Password for the email account used as the sender account.
<b>Port</b>	Port used for communication with the email server. This must match the port setting on the email server itself.
<b>Advanced</b>	When enabled, displays the SMTP Timeout and SMTP Connection Timeout fields.
<b>SMTP Timeout</b>	Defines how long Network Sentry will wait if the flow of data has stalled before it fails.
<b>SMTP Connection Timeout</b>	Lets you define the amount of time allowed to connect to the email server before it fails.
<b>Connection Security</b>	Used to encrypt email communication between the FortiNac server and the email server. This setting must match the setting configured on your email server. Options are: None, SSL/TLS or STARTTLS.
<b>Test Email Settings</b>	Click this button to send a test message to the email address entered in the Test Settings dialog.

## Log Receivers

Event and Alarm records may be stored offline on another host. The events and alarms are forwarded by using either a Syslog message or an SNMP Trap. See **Log Events To An External Log Host** on page 458 and **Map Events To Alarms** on page 493 for more information. The host may be either an SNMP Trap receiver or a Syslog server. Use the Log Receivers view to add, modify, and remove external log hosts.

### Log Receivers

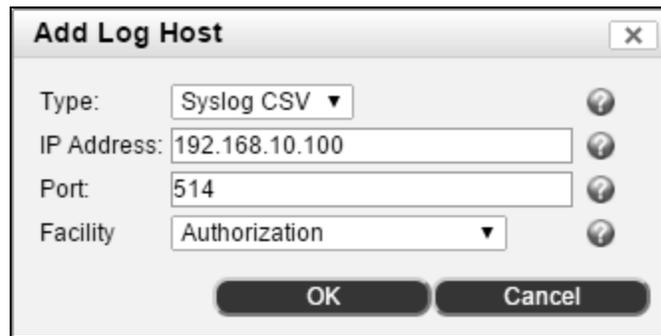
Specify the IP Address and Protocol information for Hosts that need to receive Events and/or Alarms from this server. Use the Event Management and Event-to-Alarm Mapping views to configure the specific events and/or alarms to send.

IP Address	Type	Port	SNMP Security String	Syslog Facility
192.168.102.179	Syslog	514		Authorization
192.168.102.88	CEF	514		
192.168.102.200	SNMP	162	admin	

Add
Modify
Delete

**Figure 66: Log Receivers**

**Add A Log Host Server**



**Figure 67: Add Log Host**

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the IP Address of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Field	Definition
<b>Type</b>	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF).
<b>IP Address</b>	IP Address of the server that will receive Event and Alarm messages.
<b>Port</b>	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default =162

Field	Definition
<b>Facility</b>	<p>Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include:</p> <ul style="list-style-type: none"> <li>0 kernel messages</li> <li>1 user-level messages</li> <li>2 mail system</li> <li>3 system daemons</li> <li>4 security/authorization messages</li> <li>5 messages generated internally by syslogd</li> <li>6 line printer subsystem</li> <li>7 network news subsystem</li> <li>8 UUCP subsystem</li> <li>9 clock daemon</li> <li>10 security/authorization messages</li> <li>11 FTP daemon</li> <li>12 NTP subsystem</li> <li>13 log audit</li> <li>14 log alert</li> <li>15 clock daemon</li> <li>16 local use 0 (local0)</li> <li>17 local use 1 (local1)</li> <li>18 local use 2 (local2)</li> <li>19 local use 3 (local3)</li> <li>20 local use 4 (local4)</li> <li>21 local use 5 (local5)</li> <li>22 local use 6 (local6)</li> <li>23 local use 7 (local7)</li> </ul>
<b>Security String</b>	<p>Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.</p>

### Modify Connection Information For Log Hosts

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Select a Log Receiver from the list and click **Modify**.
4. Edit the log host information.
5. Click **OK**.

### Delete An External Log Host

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Select a Log Receiver from the list and click **Delete**.
4. Click **Yes** on the confirmation message.

## Mobile Providers

The Mobile Providers window displays the default set of providers included in the database. Network Sentry uses the Mobile Providers list to send SMS messages to guests and administrators by sending email to an address that is a combination of the Mobile Phone number and the Mobile Provider's email address.

This list is populated with some known Mobile Providers but is not comprehensive nor is it updated by Fortinet. You can add, delete or modify Mobile Providers as needed. Mobile Providers can be enabled or disabled individually to limit the number of providers displayed in drop-down lists when configuring guests, users and administrators.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

### Mobile Providers

Global Max Message Length:

Mobile Providers - Total: 192

Enable:

Enabled ▾	Provider	SMS Address Format	Country	Max Message Length
<input checked="" type="checkbox"/>	Verizon	xxxxxxxxx@vtext.com	United States	
<input checked="" type="checkbox"/>	Unicel	xxxxxxxxx@utext.com	United States	100 characters
<input checked="" type="checkbox"/>	US Cellular	xxxxxxxxx@email.uscc.net	United States	
<input checked="" type="checkbox"/>	T-Mobile	xxxxxxxxx@tmomail.net	United States	
<input checked="" type="checkbox"/>	Sprint	xxxxxxxxx@sprintpaging.com	United States	
<input checked="" type="checkbox"/>	Qwest	xxxxxxxxx@qwestmp.com	United States	
<input checked="" type="checkbox"/>	Nextel	xxxxxxxxx@messaging.nextel.com	United States	
<input checked="" type="checkbox"/>	Boost Mobile	xxxxxxxxx@myboostmobile.com	United States	
<input checked="" type="checkbox"/>	AllTel	xxxxxxxxx@message.alltel.com	United States	
<input checked="" type="checkbox"/>	AT&T	xxxxxxxxx@txt.att.net	United States	
<input type="checkbox"/>	Wyndtell	xxxxxxxxx@wyndtell.com	United States	
<input type="checkbox"/>	Western Wireless	xxxxxxxxx@cellularonewest.com	United States	

Add
Modify
Delete
In Use

Save Settings

Figure 68: Mobile Providers List

## Mobile Providers Field Definitions

Field	Definition
<b>Global Max Message Length</b>	Enable to set the maximum number of characters that will be included in a single SMS message sent from Network Sentry for all Mobile Providers. If the message is longer than the Max Message Length, it is divided up and sent in multiple messages. If an individual provider has a Max Message Length setting, it overrides the Global setting.
<b>Enable Buttons</b>	Enables or disables the selected provider. If a provider is disabled it is not displayed in the Mobile Provider selection list shown when configuring an Admin user or a guest. You cannot disable a provider that is in use or associated with a user in the database. Click the In Use button to determine which users have the selected provider.
<b>Enabled</b>	A green check mark indicates that the provider is enabled. A red circle indicates that the provider is disabled.
<b>Provider</b>	Name of the company that provides mobile phone services.
<b>SMS Address Format</b>	Format of the address used to send SMS messages via email. For example, for provider AllTel the format is xxxxxxxxx@message.alltel.com, where the x's represent the user's mobile telephone number.
<b>Country</b>	Country to which this SMS Address corresponds. You may have providers that have a different SMS Address for each country in which they operate. You need a separate record for each one.
<b>Right Mouse Click Options</b>	
<b>Delete</b>	Deletes the selected Provider. Providers that are associated with Users cannot be deleted.
<b>In Use</b>	Select a provider and click In Use to determine if any one in the database has this provider listed in their user record.
<b>Modify</b>	Opens the Modify Mobile Provider window for the selected provider.

### In Use

To find the list of users associated with a provider, select the provider and click the In Use button. A message is displayed indicating whether or not the provider is associated with any user or guest records. If users are associated with the provider, a list of User IDs is displayed.

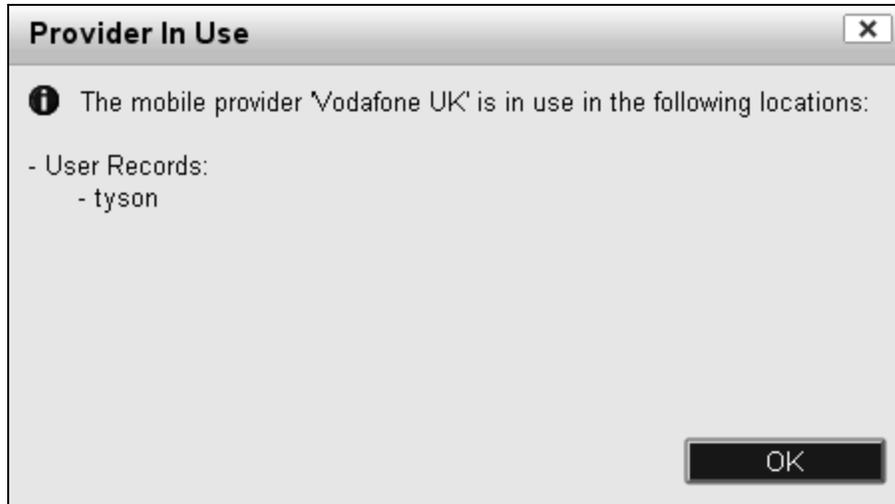


Figure 69: Provider In Use List

**Add/Modify A Mobile Provider**
**Figure 70: Add Mobile Provider**

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Mobile Providers** from the tree.
4. Click the **Add** button or select a provider and click **Modify**.
5. Use the field definitions in the table below to complete the provider information.
6. Click **OK** to save your changes.

**Add/Modify Mobile Provider Field Definitions**

Field	Definition
<b>Enable</b>	Enables/disables the provider. Enable/Disable can also be done from the Mobile Providers list.
<b>Provider</b>	Name of the provider being configured. This name must be unique.
<b>Email Domain</b>	The provider's email domain, such as, nextel.messaging.com.
<b>Country</b>	Country to which this SMS Address corresponds. You may have providers that have a different SMS Address for each country in which they operate. You need a separate record for each one.

Field	Definition
<b>Max Message Length</b>	Controls the number of characters included in a single message when messages are sent to this provider's customers. If the message length exceeds the Max Message Length, it is divided up in to multiple messages.
<b>Prefix</b>	Any numbers that are required before the user's mobile number. For example, you may have users that are in an adjacent country, therefore you may need to enter a number, such as 1, ahead of the mobile number.
<b>Suffix</b>	Any numbers required after the user's mobile number.
<b>SMS Address Format</b>	The format used for the address of the message recipient. Network Sentry sends SMS messages via email. The provider's email server sends the messages to the mobile phone number contained in the SMS Address.  As you enter information in to the Add/Modify Provider dialog, the SMS Address is updated.

### **Delete A Mobile Provider**

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Mobile Providers** from the tree.
4. Select a provider and click **Delete**.
5. If users are associated with the provider, a list of user names is displayed. You cannot delete a Mobile Provider if that provider is listed in a User record. First modify the user record and then delete the provider.
6. If no users are associated with the provider, confirm that you want to delete the provider.

### **SNMP**

Use the SNMP Properties view to select the SNMP protocol for devices that query Network Sentry for information. If SNMP is enabled, Network Sentry responds to SNMP communication from other devices, such as a Network Management system that might include the Network Sentry server in its own database.

Go to **Settings > System Communication > SNMP**.

In addition, this view is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See **Register Hosts And Users With SNMPv3 Traps** on page 138.

Both types of communication pass through port 161. Settings here are global. Therefore, if you choose to use SNMPv3 traps sent from other network devices to register hosts and users, then ALL other devices that query Network Sentry for information must also communicate using SNMPv3. You must modify the configuration of those external devices to use SNMPv3.

The SNMP protocols that are supported are SNMPv1/SNMPv2c and SNMPv3. SNMPv3 uses DES or AES encryption for the Privacy Password.

Privacy protocols supported are:

- DES
- Triple-DES
- AES-128

SNMP MIBs used to communicate with Network Sentry are in:

`/bsc/campusMgr/ui/runTime/docs/mibs/`

### SNMP

Enable SNMP Communication ?

SNMP Protocol:  ?

Security String:  ?

#### Management Hosts

IP

**Save Settings**

Figure 71: SNMP

Table 10: SNMP Field Definitions

Field	Description
<b>Enable</b>	If SNMP is enabled, Network Sentry responds to SNMP requests from other servers.
<b>SNMP Protocol</b>	Select the SNMP protocol Network Sentry will be responding to: SNMPv1/SNMPv2c SNMPv3-AuthPriv (SNMPv3 with Authentication and Privacy) SNMPv3 AuthNoPriv (SNMPv3 with Authentication but no Privacy.)
<b>SNMPv1/SNMPv2c</b>	
<b>Security String</b>	Enter the security string that Network Sentry will respond to when communicating with the server.
<b>SNMPv3</b>	
<b>User Name</b>	User Name for the SNMPv3 credentials.
<b>Authentication Protocol</b>	Specify the SNMPv3 Authentication Protocol. The available Authentication Protocols are <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA1</li> </ul>
<b>Authentication Password</b>	Specify the Authentication Password required by Network Sentry when SNMPv3-AuthPriv or SNMPv3-AuthNoPriv queries are received.
<b>Privacy Protocols</b>	Specify the SNMPv3 Privacy Protocol. The available privacy protocols are: <ul style="list-style-type: none"> <li>• DES</li> <li>• Triple-DES</li> <li>• AES-128</li> </ul>
<b>Privacy Password</b>	Specify the Privacy Password required by Network Sentry when SNMPv3-AuthPriv queries are received.
<b>Management Hosts</b>	
<b>IP Addresses</b>	List of IP addresses of the devices that have communicated with Network Sentry through SNMP.

### Set Up SNMP Communication With Network Sentry

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Enable** and select an **SNMP protocol**.

5. Enter the **parameters** as required for the selected protocol. See the field definitions above for additional information.
6. Click **Save Settings**.

### Disable SNMP Communication With Network Sentry

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Disable**.
5. Click **Save Settings**.

## Register Hosts And Users With SNMPv3 Traps

Network Sentry can use data sent in SNMPv3 traps from external devices to register hosts and users. This speeds up the process of adding hosts and users to your Network Sentry database by taking advantage of information that is readily available from another system. In addition, based on trap parameters hosts and users can be modified or removed from the database.

### Network Sentry Configuration Requirements

- The Trap Sender must be modeled in the Topology View as a pingable device.
- You must enter SNMPv3 settings in **System > Settings > System Communication > SNMP** that match those of the device to which you are sending traps. Note that if you had previously entered SNMPv1/SNMPv2c settings for external devices querying Network Sentry for information, you must modify settings on those devices to use SNMPv3. See **SNMP** on page 134.
- If you are running Network Sentry in a FortiNac Control Manager environment, the Trap Sender must be modeled on each Network Sentry Server or Control Server that should receive this information. Note that if you have enabled any of the **Copy Registered Host** options on the FortiNac Control Manager it may not be necessary to receive traps on more than one managed server.
- When traps are received they can trigger the events listed below in the Event Log. These events can be mapped to Alarms. Make sure the events are enabled. See **Event Management** on page 451. To map events to alarms see **Add or Modify Alarm Mapping** on page 497.

Event	Definition
Add/Modify/Remove Host	Generated whenever a trap is received that adds, modifies or removes a host record in the database.

Event	Definition
<b>Add/Modify/Remove User</b>	Generated when a trap is received that adds, modifies or removes a user record in the database.

### Trap Sender Configuration Requirements

- Use the Management IP address (eth0) of the Network Sentry Server or Control Server as the destination for the trap.
- Send traps to port 161 on the Network Sentry Server or Control Server.
- If you are running Network Sentry in a High Availability environment, send traps to both the primary and the secondary Network Sentry Servers or Control Servers.
- You must have snmptrap.exe and libsnmp.dll on the device sending the traps. Download the latest binaries for the appropriate operating system from [www.net-snmp.org/download.html](http://www.net-snmp.org/download.html).
- Configure the traps on the sending device. See the tables below for information on trap parameters.

### Hosts

- If a trap is received for an existing host, the host's database record is updated with information from the trap.
- When a trap is received for a host that matches a rogue in Network Sentry, the rogue is converted to a registered host if the trap contains user data. It is converted to a registered device if there is no associated user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts either send an additional trap that removes the host or you must go to the Host View and delete them manually. See **Delete A Host** on page 349.
- If the same host is added twice but with different MAC addresses for separate adapters, it is treated as two separate records in the Network Sentry database. The two adapters are not linked to each other in any way and are not considered siblings in Network Sentry.
- Variables with spaces in the names should be in quotation marks, such as, "Windows Vista".
- Separators in MAC Addresses must be colons, such as, 90:21:55:EB:A3:87.

OID	Description	Definition
1.1.1.1	Host Name	Machine name of the host.
1.1.1.2	IP Address	IP address of the host.
1.1.1.3	MAC Address	Physical Address of the host. Required.
1.1.1.4	Host Operating System	Name of the operating system on the host.
1.1.5	Role	Role assigned to the host. Roles are attributes of hosts used as filters in User-/Host Profiles.
1.1.6	Action	Indicates whether this trap is adding or removing a host from the database. Adding an existing host will modify that host's record in the database.  1=Add  2=Remove
1.2.8	Element	Indicates that this trap is registering either a host or a host and its corresponding user.

### Example Traps

To add a host record for the PC with a hostname of **Gateway-notebook**, with an IP address of **160.87.100.117**, a MAC address of **00:26:9E:E2:DD:DB**, an OS of **Windows**, and a role of **Guest**:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 1
```

To remove host record for the PC with a hostname of **Gateway-notebook**, with an IP address of **160.87.100.117**, a MAC address of **00:26:9E:E2:DD:DB**, an OS of **Windows**, and a role of **Guest**. Note that only MAC address is required to remove a host.

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 2
```

### Users

- If an LDAP directory is modeled in the Topology View, Network Sentry checks the directory for information about the user included in the trap. If the user exists in the directory, additional fields are populated for that user in the Network Sentry database. If the user does not exist in the directory, a user record is created in Network Sentry with only the data received in the trap.

- If a trap is received for an existing user, the user's database record is updated with information from the trap.
- If a trap is received for an existing user and the trap contains host information, the host is registered to the user. If the host already has a rogue record, the rogue is converted to a registered host and associated with the user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts you must go to the Host View and delete them manually. See **Delete A Host** on page 349.
- When Network Sentry resynchronizes with the directory, user data may be overwritten by data from the directory depending on the directory attribute mappings. See **Add/Modify Directory - User Attributes Tab** on page 76.
- Variables with spaces in the names should be in quotation marks, such as, "Mary Ann".

### Trap Parameters

OID	Description	Definition
1.1.2.1	User Name	User Name stored in the directory. If the user is not in the directory, this record will still be added, modified or removed.  Required.
1.1.2.2	User First Name	
1.1.2.3	User Last Name	
1.1.2.4	User Title	
1.1.2.5	Email	User's e-mail address.
1.1.5	Role	Role assigned to the User. If this trap is adding both a user and a host, both are set to the same role.
1.1.6	Action	Indicates whether this trap is adding or removing a user from the database. Adding an existing user will modify that user's record in the database.  1=Add  2=Remove
1.2.9	Element	Indicates that this trap is only registering a user.

### Example Traps

To add **testuser** to the database:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''  
1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser .1.3.6.1.4.1.16856.1.1.2.2  
s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe .1.3.6.1.4.1.16856.1.1.2.4 s Mr
```

```
.1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com .1.3.6.1.4.1.16856.1.1.5 s Guest  
.1.3.6.1.4.1.16856.1.1.6 integer 1
```

To delete user record for **testuser** from the database. Note that only User Name is required to remove a user.

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphrase**> 160.87.9.10:161 ''  
1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser .1.3.6.1.4.1.16856.1.1.2.2  
s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe .1.3.6.1.4.1.16856.1.1.2.4 s Mr  
.1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com .1.3.6.1.4.1.16856.1.1.5 s Guest  
.1.3.6.1.4.1.16856.1.1.6 integer 2
```

## Proxy Settings

Proxy Settings allows you to configure Network Sentry to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.

**Important:** Proxy communication is not supported for MDM Services.

**Proxy Settings**

Enable Proxy Configuration

HTTP Proxy

Host: Host A

Port: 80

Authentication

User Name: testuser1

Password: \*\*\*\*\*

Use HTTP Proxy settings for all protocols

HTTPS Proxy

Host:

Port: 443

Authentication

FTP Proxy

Host:

Port: 80

Authentication

Proxy Exclusions

Example: \*.mynetwork.com|192.168.1.0|127.\*[:::1]

**Save Settings**

Figure 72: Proxy Settings

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Proxy Settings** from the tree.
4. Use the table of field definitions below to enter the necessary settings.
5. Click **Save Settings**.

### Proxy Settings Field Definitions

Field	Definition
<b>Enable Proxy Configuration</b>	If enabled, Network Sentry will use the Proxy Configuration to download OS updates and auto-definition updates.
<b>Host</b>	The hostname or address of the proxy server.
<b>Port</b>	Port used for communication with the proxy server. This must match the port setting on the proxy server itself.
<b>Authentication</b>	If enabled, you must enter the user name and password for the proxy server.
<b>User Name</b>	User Name for the email account used as the sender account.
<b>Password</b>	Password for the email account used as the sender account.
<b>Use HTTP Proxy settings for all protocols</b>	If enabled, the HTTP Proxy configuration will be used for both HTTPS and FTP Proxy communication.
<b>Proxy Exclusions</b>	Indicates the hosts that should be accessed without going through the proxy. The list of hosts are separated by the ' ' character. The wildcard character '*' can be used for pattern matching (e.g., Dhttp.nonProxyHosts="*.foo.com localhost" indicates that every host in the foo.com domain and the localhost should be access directly, even if a proxy server is specified).

## System Management

System Management groups together core server features such as data backup and restore, redundant servers, licensing and time zone settings. Options include:

Option	Definition
<b>Database Backup/Restore</b>	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups stored on the Network Sentry server, not backups on a remote server.  See <b>Database Archive</b> on page 147
<b>High Availability</b>	Configuration for Primary and Secondary appliances for High Availability. Saving changes to these settings restarts both the Primary and Secondary servers.  See High Availability on page 153.
<b>License Management</b>	View or modify the license key for this server or an associated Application server.  See License Management on page 156.

<b>Option</b>	<b>Definition</b>
<b>NTP and Time Zone</b>	Reset the time zone and NTP server for your Network Sentry appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up. Requires a server restart to take effect.  See NTP And Time Zone on page 161.
<b>Power Management</b>	Reboot or power off the Network Sentry server. In the case of a Network Sentry Control Server / Application Server pair, reboot or power off each server individually.  See Power Management on page 163.
<b>Remote Backup Configuration</b>	Configure scheduled backups to use a remote server via FTP and/or SSH.  See Configure The Remote Backup Destination on page 166.
<b>System Backups</b>	Create a backup of all system files that are used to configure Network Sentry.  See <b>System Backups</b> on page 170

## Database Archive

Use Database Archive to set age times for selected log files. Log files are archived and then purged from the Network Sentry database when the age time elapses. Archived data can be imported back into the database if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database.

Figure 73: Database Archive Age Time

### Database Archive Field Definitions

Field	Definition
<b>Remove local backups older than</b>	<p>Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the Network Sentry server before they are copied to the remote server. Backups on the remote server are not removed.</p> <p><b>Note:</b> The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.</p>

Field	Definition
<b>Event/Alarms Age Time (days)</b>	Number of days events or alarms are maintained in the Events or Alarms logs and viewable in the Events or Alarms View. Events and Alarms are archived and purged based on the scheduled task settings.  Default setting = 7 days

### Edit Archive Age Time

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Use the information in the field definitions table above to set Age Time.
5. Click **Save Settings**.

### Schedule Event Archive And Purge

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the Name field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
  - a. Click the **box** next to the day(s) to select the day.
  - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
  - c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
  - d. To remove all settings click the **Clear All** button.

11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.

**Note:** A repetition rate of zero causes the task to run only once.

- a. Enter the **Repetition Rate** using whole numbers.
- b. Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
- c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

**Important:** The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

- d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.
12. Click **OK**.

**Table 11: Schedule Field Definitions**

Field	Definition
<b>Remove local backups older than</b>	<p>Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the Network Sentry server before they are copied to the remote server. Backups on the remote server are not removed.</p> <p><b>Note:</b> The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.</p>
<b>Status</b>	Indicates whether the task is Enabled or Disabled.
<b>Schedule Interval</b>	How often the scheduled task runs. Options are Minutes, Hours, or Days.
<b>Next Scheduled Time</b>	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
<b>Modify Schedule</b>	Allows you to modify the scheduled activity.
<b>Run Now</b>	Runs the scheduled task immediately.

## Database Backup/Restore

A database backup creates a backup of the entire database. All database archives can be restored if the database becomes corrupted. To restrict the restoration to only alarms, connections, or events data, go to those specific views and select the Import option. See **Alarms View** on page 489 and **Events View** on page 466 for more information.

**Important:** Restoring a database archive causes the FortiNac Control Manager to restart.

**Database Backup/Restore**

Remove local backups older than  days ?

**Schedule Database Backup**

Status: Enabled  
 Schedule Interval: M\_12:01AM  
 Next Scheduled Time: 08/03/15 12:01 AM EDT

**Database Restore**

NetworkSentry\_DataBase\_BackUp\_2015\_04\_30\_15\_26\_17.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_04\_00\_01\_04.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_06\_09\_12\_51.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_08\_09\_39\_38.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_08\_09\_48\_08.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_11\_00\_01\_52.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_15\_11\_07\_42.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_18\_00\_01\_53.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_18\_10\_32\_49.gz  
 NetworkSentry\_DataBase\_BackUp\_2015\_05\_25\_00\_01\_51.gz

**Figure 74: Database Backup/Restore**

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Backup/Restore** from the tree.

### To Schedule a Database Backup

1. Under Schedule Database Backup, click **Modify Schedule**.
2. Select the **Enabled** check box.

3. Enter a name for the task in the Name field.
4. The **Description** field is optional. Enter a description of the task.
5. Action type and Action are pre-configured based on the task and cannot be modified.
6. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
7. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
  - a. Click the **box** next to the day(s) to select the day.
  - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
  - c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
  - d. To remove all settings click the **Clear All** button.
8. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.

**Note:** A repetition rate of zero causes the task to run only once.

- a. Enter the **Repetition Rate** using whole numbers.
- b. Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
- c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

**Important:** The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

- d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.
9. Click **OK**.

**Table 12: Schedule Field Definitions**

Field	Definition
<b>Remove local backups older than</b>	<p>Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the Network Sentry server before they are copied to the remote server. Backups on the remote server are not removed.</p> <hr/> <p><b>Note:</b> The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.</p>
<b>Status</b>	Indicates whether the task is Enabled or Disabled.
<b>Schedule Interval</b>	How often the scheduled task runs. Options are Minutes, Hours, or Days.
<b>Next Scheduled Time</b>	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
<b>Modify Schedule</b>	Allows you to modify the scheduled activity.
<b>Run Now</b>	Runs the scheduled task immediately.

**To Restore a Database**

1. Click on a backup to select it.
2. Click **Restore Database**.

## High Availability

Use the High Availability view to add to and update High Availability configuration information.

Use the Configuration Wizard to complete the initial configuration for each appliance. See the Appliance Installation Guide that came with the hardware for instructions on using the Configuration Wizard. See the **High Availability Overview** on page 721 for additional information on configuring appliances for a High Availability environment.

### High Availability

Apply these settings to configure Primary and Secondary appliances for High Availability.  
Warning: Saving changes to this configuration restarts both the Primary and Secondary servers.

#### Shared IP Configuration

The Shared IP Address is recommended when the primary and the secondary are in the same subnet. This allows you to use a single IP for administrative use. If they are not in the same subnet and separated by a router, then you will not be able to use a Shared IP Address which means that both IP Address(es) will need to be used for administrative use.

Use Shared IP Address

Network Sentry Server

Shared IP Address:

Shared Subnet Mask(bits):

Shared Host Name:

#### Network Sentry Server Configuration

Primary Appliance	Secondary Appliance
IP Address: <input type="text" value="192.168.5.207"/>	IP Address: <input type="text" value="192.168.5.209"/>
Gateway IP Address: <input type="text" value="192.168.5.1"/>	Host Name: <input type="text" value="nssecondary"/>
CLI/SSH root Password [User:root]: <input type="password" value="*****"/> <input type="button" value="Show"/>	Gateway IP Address: <input type="text" value="192.168.5.1"/>
	CLI/SSH root Password [User:root]: <input type="password" value="*****"/> <input type="button" value="Show"/>

**Figure 75: High Availability**

### [Configure High Availability](#)

Configure the High Availability information for a standalone FortiNac Server:

1. Ensure that all appliances are keyed for High Availability. See **View/Modify License Information** on page 157 and check the High Availability field.
2. Click **System > Settings**.
3. Expand the **System Management** folder.
4. Select **High Availability** from the tree.

5. Use the table of field definitions below to enter the required information.
6. Click **Save Settings** and wait for the success message.

**Note:** When you click Save Settings on the Administration High Availability view, the primary server tries to communicate with the secondary to ensure that the database will be replicated. If the primary server cannot communicate with the secondary, it continues to try until communication is established.

**Note:** If you are configuring High Availability in an environment where you have a Network Sentry Control Server and an Application Server, additional fields are displayed to configure the two Application Servers.

Field	Description
<b>Shared IP Configuration</b>	
<b>Use Shared IP Address</b>	<p>Enables the use of a shared IP address in the High Availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual machine IP address.</p> <p>If your primary and secondary servers are not in the same subnet, do not use a shared IP address.</p>
<b>Shared IP Address</b>	The shared IP address for the High Availability configuration. Added to the <code>/etc/hosts</code> file when the configuration is saved.
<b>Shared Subnet Mask (bits)</b>	The shared subnet mask in bits. For example, 255.255.255.0 = 24 bits.
<b>Shared Host Name</b>	Part of the entry in the <code>/etc/hosts</code> file for the shared IP address. Admin users can access the UI using either the Shared IP address or the shared host name.
<b>Server Configuration</b>	
<b>Primary Appliance</b>	<p><b>IP Address</b>—IP address assigned to eth0 for the primary.</p> <p><b>Gateway IP Address</b>—IP address pinged by the appliances to determine if network connectivity is still available.</p> <p><b>CLI/SSH root Password [User:root]</b>—Root password on the appliance itself. Allows settings to be written to the appliance.</p> <p><b>Retype root CLI/SSH Password [User:root]</b>—Retype the password entered in the CLI/SSH root Password field for confirmation.</p>
<b>Secondary Appliance</b>	<p><b>IP Address</b>—IP address assigned to eth0 for the secondary.</p> <p><b>Host Name</b> — Name assigned to the secondary.</p> <p><b>Gateway IP Address</b>—IP Address that is pinged by the appliances to determine if network connectivity is still available.</p> <p><b>CLI/SSH root Password [User:root]</b>—Root password on the appliance itself. Allows settings to be written to the appliance.</p> <p><b>Retype root CLI/SSH Password [User:root]</b>—Retype the password entered in the CLI/SSH root Password field for confirmation.</p>

### Unconfigure High Availability

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **High Availability** from the tree.
4. Clear the shared and secondary information, and leave the primary information filled in.
5. Click **Save Settings**.

### License Management

Manage license keys on the servers through this view. You can view and modify both the FortiNac Control Server and FortiNac Application Server licenses through this view. Servers that are part of a High Availability configuration appear in the drop-down list.

---

**Note:** License information is displayed on the Dashboard. See **Dashboard** on page 25 for additional information.

---

**Note:** The events related to license use help maintain proper appliance use per environment. Warning and critical events and alarms are generated based on a set of user defined thresholds. See **Event Thresholds** on page 455 to set thresholds. See **Map Events To Alarms** on page 493 to set alarms based on threshold events.

---

## [View/Modify License Information](#)

**Note:** The license options will vary depending on whether pre-2016 (Secure Enterprise Standard, Secure Enterprise Advanced, or Secure Enterprise Mobility) or post-2016 (Secure Enterprise Advanced or Secure Enterprise Premier) license packages are installed on the server.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **License Management** from the tree.

### License Management

Server: 192.168.65.120 -- 08:00:27:5E:B2:D3 -- Network Sentry Control Manager ▾

#### Server Detail

Eth0 IP Address:	192.168.65.120
Eth0 MAC Address:	08:00:27:5E:B2:D3
Server Type:	Network Sentry Control Manager

Note: Please see the Naming Conventions Section in the Appliance Installation Guide for details on how to equate server type to your specific appliance.

#### License Key Detail

License Name:	Secure Enterprise Premier	?
Concurrent Licenses:	600	?
High Availability:	Enabled	?

**Figure 76: License Management - Pre 2016 License Options**

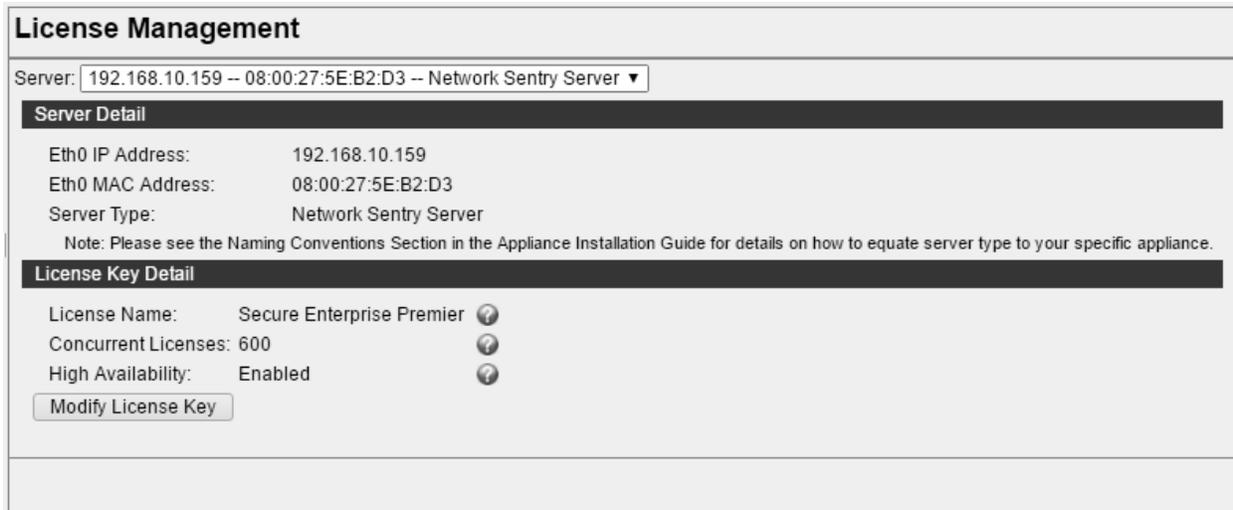


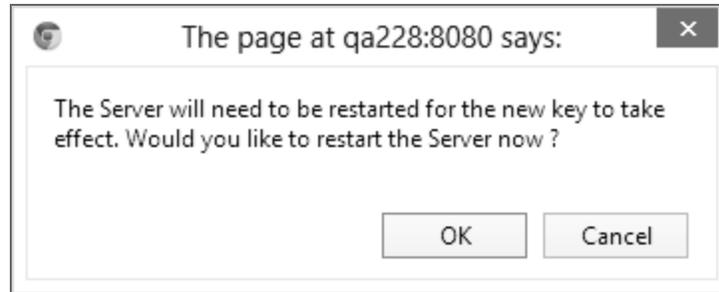
Figure 77: License Management - Post 2016 License Options

4. From the drop-down list select the server containing the license key.
5. Click **Modify**.



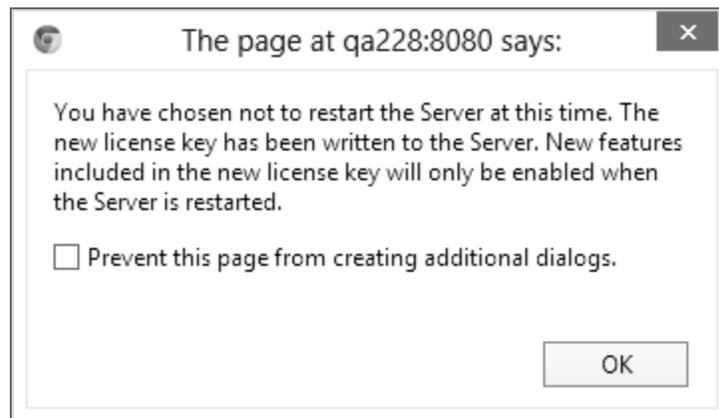
Figure 78: Modify License Key

6. You can modify the license key in two ways.
  - To upload from a text file, click **Upload**, browse to the license key file, and click **Open**. This must be a text file not a zip file.OR
  - From another file, copy and paste the new license key text into the text box.
7. Click **OK** to apply the new license key. The existing key detail is displayed in a pop-up window along with the new key detail.
8. Click **OK** to apply the new license key. Click Undo if you want to revert to the existing license key.
9. **To restart the server immediately**, click **OK** on the dialog box.



**Figure 79: License Management - Restart Server Option**

**To restart the server later**, click **Cancel** on the dialog box. Another dialog box appears stating that the new key will not be applied until the server is restarted. New features or license counts contained in the new license cannot be accessed until the server is restarted. The new license is saved on the server, but is not read until the server is restarted.



**Figure 80: License Management - Restart Server Later**

10. Click **OK** to confirm.

**License Key Detail Field Definitions**

<b>Key</b>	<b>Definition</b>
<b>License Name</b>	Indicates which license installed on the server.
<b>Concurrent Licenses</b>	Number of licenses configured for possible online connections to the network. Connections are counted for hosts and devices that are not switches or routers.
<b>RTR Licenses</b>	Indicates the number of licenses configured for RTR.
<b>Evaluation Time</b>	Indicates the number of days configured for an evaluation license. If you have purchased a full license for the product, this field does not display.
<b>High Availability</b>	Indicates whether or not High Availability has been enabled.
<b>Integrated RADIUS</b>	Indicates whether or not an Integrated RADIUS server has been enabled.
<b>Device Profiler</b>	Indicates whether or not the Device Profiler feature has been enabled.
<b>Guest Manager</b>	Indicates whether or not the Guest Manager feature has been enabled.
<b>Endpoint Compliance</b>	Indicates whether or not the Security Policy features have been enabled.
<b>Integration Suite</b>	Indicates whether or not access to third party information such as SNMP Traps and Syslogs has been enabled.
<b>Wireless Only</b>	<p>Indicates whether or not a limited Wireless Only license has been enabled.</p> <p>Provided as a quick start solution for organizations that use only wireless devices on their network. This feature is not supported for all wireless devices. Currently only HP MSM and Ruckus controllers can be configured. For HP wireless devices, Network Sentry can write configuration changes to the device. For Ruckus controllers, Network Sentry cannot write configuration changes to the device only the device model in the database. Other wireless devices and up to five wired devices can be added using the Network Devices View or the Topology View. In addition, this license disables the Discovery feature. .</p>

## NTP And Time Zone

Use NTP and Time Zone to reset the time zone and NTP server for your Network Sentry appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up.

The NTP server is used to synchronize the clock on the Network Sentry appliance. Network Sentry contacts the NTP server periodically to synchronize its clock with the NTP servers. NTP server keeps time in UTC or Coordinated Universal Time, which corresponds roughly to Greenwich Mean time.

Figure 81: Services - Time Tab

Table 13: Services - Time Tab Field Definitions

Field	Definition
<b>Time</b>	
<b>Network Sentry Servers</b>	Provides a list of servers for which you can change time settings. If you have a Control server and an Application server pair, both servers are displayed in the list. In an HA environment this would include up to four servers, two Control servers and two Application servers. The list may also contain the Integrated RADIUS Server.  Each server's time must be set individually. Settings apply only to the server displayed in this field.
<b>NTP Server</b>	External server used to synchronize or update the clock on the selected Network Sentry server. Defaults to pool.ntp.org.
<b>Time Zone</b>	Time zone where the selected Network Sentry server resides.

### Modify Time Settings

**Note:** Changes to NTP or time zone require a server restart to take effect. Go to the Control Panel to restart the server now. See **Power Management** on page 163.

1. Click **System > Settings**.
2. Expand the **System Management** folder.

3. Select **NTP And Time Zone** from the tree.
4. Click the **Network Sentry Servers** drop-down and choose the server to be modified.
5. Enter your preferred NTP Server in the **NTP Server** field.
6. Click the **Time Zone** drop-down and select the time zone for this server.
7. Click **Save Settings** to save settings for the selected server.
8. To modify another server, select it in the Network Sentry Servers drop-down and repeat steps 4 through 7.

## Power Management

The system can be rebooted or powered down through the Network Sentry interface, by any user whose Admin Profile allows access to the Settings view. In a High Availability environment or in the case where there is a Network Sentry Control Server/Application Server pair, servers must be rebooted or powered off individually.

**Important:** In a HA environment, reboot or power off the secondary servers first.

Events associated with Power Management are as follows:

- **System Power Off**— Indicates that the server has been powered down and provides the user name of the user who initiated the action.
- **System Reboot**—Indicates that the system was rebooted and provides the user name of the user who initiated the action.

The screenshot shows the 'Power Management' interface. At the top, there is a 'Servers' table with the following data:

Host	Status	Product	Version	Appliance	Firmware
playdon1.bradfordnetworks.cor	Running	Network Sentry Control Manager - Primary	8.1.0.437	VM-NS550CM	5.1.0.327

Below the table, there are two buttons: 'Reboot' and 'Power Off'.

### Reboot The Server:

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Power Management** from the tree.
4. Select a server from the list.
5. Click the **Reboot** button. This process may take 2-3 minutes.

### Power Off The Server:

1. Click **System > Settings**.
2. Expand the **System Management** folder.

3. Select **Power Management** from the tree.
4. Select a server from the list.
5. Click the **Power Off** button. This process may take 30 seconds.

## Backup To Remote Server

Backups of the database and other files occur automatically when the Backup Database and Purge Events scheduled tasks run. The backup files are stored on the local appliance.

The Administrator can additionally configure Network Sentry to place a copy of the database and other directories on an ftp and/or other remote server for safekeeping. The backup files are placed in time and date stamped files named `DataBase_BackUp_YYYY-MM_DD_HH_mm_SS.gz`.

### Backup Directory Files

Appliance	Directories Included in Backup File	
<b>FortiNac Server</b>	<ul style="list-style-type: none"> <li>• /etc</li> <li>• /home/cm</li> <li>• /root</li> <li>• /var/spool/cron</li> <li>• /bsc/Registration</li> <li>• /bsc/Remediation</li> <li>• /bsc/Hub</li> <li>• /bsc/Authentication</li> <li>• /bsc/DeadEnd</li> <li>• /bsc/CommonJspFiles</li> </ul>	<ul style="list-style-type: none"> <li>• /bsc/VPN</li> <li>• /bsc/WWW</li> <li>• /bsc/WEB-INF</li> <li>• /home/admin</li> <li>• /bsc/clientValidation</li> <li>• /bsc/siteConfiguration</li> <li>• /bsc/services</li> <li>• /bsc/campusMgr/master_loader/telnetMibs</li> <li>• /bsc/campusMgr/master_loader/customTraps</li> </ul>
<b>FortiNac Control Server</b>	<ul style="list-style-type: none"> <li>• /etc</li> <li>• /root</li> <li>• /home/cm</li> <li>• /home/admin</li> <li>• /var/spool/cron</li> <li>• /bsc/clientValidation</li> </ul>	<ul style="list-style-type: none"> <li>• /bsc/siteConfiguration</li> <li>• /bsc/services</li> <li>• /bsc/campusMgr/master_loader/telnetMibs</li> <li>• /bsc/campusMgr/master_loader/customTraps</li> </ul>
<b>FortiNac Application Server</b>	<ul style="list-style-type: none"> <li>• /etc</li> <li>• /home/cm</li> <li>• /root</li> <li>• /home/admin</li> <li>• /var/spool/cron</li> <li>• /bsc/Registration</li> <li>• /bsc/Remediation</li> <li>• /bsc/Hub</li> </ul>	<ul style="list-style-type: none"> <li>• /bsc/Authentication</li> <li>• /bsc/DeadEnd</li> <li>• /bsc/CommonJspFiles</li> <li>• /bsc/VPN</li> <li>• /bsc/www</li> <li>• /bsc/siteConfiguration</li> <li>• /bsc/services</li> <li>• /bsc/WEB-INF</li> </ul>

**Important:** When configuring the backup for a pair of appliances (FortiNac Control Server and FortiNac Application Server) the remote back up is only configured on the FortiNac Control Server appliance. The backup files from both servers will be placed in the directory specified. The host name of the appliance will be prefixed to the backup filename.

## Configure The Remote Backup Destination

Remote Backup Configuration defines the connection details used to copy files to a third party (remote) server when the Database Backup task is run in Scheduler. Transferring the backup files can be done using FTP and/or SSH protocols.

### **Remote Server Configuration Using FTP**

1. Create an account on the remote FTP server to be used by Network Sentry for backup file transfer.
2. Create a folder to which Network Sentry will copy the files.

For instructions on completing the above tasks, consult documentation specific to the FTP application used.

### **Remote Server Configuration Using SSH**

SSH communication must be established between the FortiNac Control Manager and the remote backup server for the SSH remote backups to be successful. Ensure that the public key for the root user on the machine being backed up has been appended to the `authorized_keys` file in the `<root home dir>/.ssh` directory of the remote server. In the case of High Availability, the SSH keys for both the primary and secondary must be appended to the `authorized_keys` file.

### **Copy the SSH Key to the Remote Server Account (Linux)**

1. Access the CLI on the Network Sentry Control Server as `root`.
2. Navigate to the `.ssh` directory. Type  

```
cd /root/.ssh
```
3. Display and copy the key. Type  

```
cat id_rsa.pub
```
4. Access the remote server where the backups will be stored as `root`.
5. If the `.ssh` directory does not exist, create it. Type  

```
mkdir /home/backup_username/.ssh
```
6. Change the permissions. Type  

```
chmod 700 /home/backup_username/.ssh
```
7. Navigate to the `.ssh` directory, and then paste (append) the key you copied from the Network Sentry to the `authorized_keys` file. Type  

```
cd /home/backup_username/.ssh  
vi authorized_keys
```

**Note:** The format of `authorized_keys` file is one entry per line.

8. Make sure the key you paste is identical to the key on the Network Sentry and does not include extra white space or characters.

---

### Copy the SSH Key to the Remote Server Account (Third Party)

1. Access the CLI on the Network Sentry Control Server as `root`.
2. Navigate to the `.ssh` directory. Type  

```
cd /root/.ssh
```
3. Display and copy the key. Type  

```
cat id_rsa.pub
```
4. Associate the public key to the remote server where the backups will be stored.

**Note:** This process will vary depending on the product. Refer to the SSH server product documentation for instructions.

### Configure The Remote Backup Target in Network Sentry

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Remote Backup Configuration** from the tree.
4. Use the table of field definitions below to complete these steps.
5. In the **Backup Timeout** field enter the number of minutes for the backup to be created and copied to the remote server.
6. Select **Enable FTP Remote Backup** and/or **Enable SSH Remote Backup** to enable the remote backup to that server(s).
7. Enter the connection information for the backup server(s).
8. Click **Test SSH Connection** to validate the SSH Server and SSH Remote Path settings.
9. Click **Save Settings**.

### Remote Backup Configuration

The following settings are used to ftp and/or ssh backup files to a remote server.

Backup Timeout:  minutes ?

Enable FTP Remote Backup ?

Server:  ?

User Name:  ?

Password:   ?

Remote Path:  ?

Enable SSH Remote Backup ?

Server:  ?

Note: For SSH as non-root user, specify user@IP

Remote Path:  ?

Figure 82: Remote Backups

**Remote Backup Destination Field Definitions**

Field	Definition
<b>Backup Timeout</b>	Number of minutes for the backup to be created and copied to the remote server. If this time elapses before the backup is done, the process is interrupted. Be sure to select a time that is long enough for your system to complete its backup. The default is 20 minutes, however, large systems may require more time.
<b>Enable FTP Remote Backup</b>	Remote backups to this server are enabled when this is checked. Default = Unchecked
<b>Display Public SSH Keys</b>	Click to view the public SSH key from the Network Sentry Primary and Secondary Control Servers.
<b>Server</b>	IP Address of the remote server.
<b>User Name</b>	User Name required for write access to the server.
<b>Password</b>	Password required for write access to the server.

Field	Definition
<b>Remote Path</b>	The directory path where the remote backup files will be placed. This directory must exist on the server. In the example shown above, this is a directory in admin's home area.
<b>EnableSSH Remote Backup</b>	Remote backups to this server are enabled when this is checked. The SSH keys must already be established for the SSH remote backups to be successful. Default = Unchecked
<b>Server</b>	The IP Address of the remote server. Format is user@remote-server, such as asmith@192.168.1.1 .
<b>Remote Path</b>	The directory path where the remote backup files will be placed. This directory must exist on the server.
<b>Test SSH Connection</b>	Test the connection to the server using the SSH Server and SSH Remote Path settings to confirm the settings are valid. If the test fails, it means the Remote Backup task will not back up the files to the specified remote server.

### Validate the Connection and Backup Task

#### FTP

1. Navigate to **System > Scheduler**.
2. Add the Database Backup task (if not already present).
3. Highlight the Database Backup task and click **Run Now**.

#### SSH

1. Click the **Test SSH Connection** button to verify SSH communication with the remote server.
2. Once successfully tested, navigate to **System > Scheduler**.
3. Add the Database Backup task (if not already present).
4. Highlight the Database Backup task and click **Run Now**.

## System Backups

A system backup creates a backup of all system files that are used to configure Network Sentry, such as license key and web server configurations.



Figure 83: System Backups

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **System Backups** from the tree.
4. In the **Remove local backups older than field**, enter the number of days for which you would like to keep backups.

**Note:** The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.

5. Click **Modify Schedule**.
6. Select the **Enabled** check box.
7. Enter a name for the task in the Name field.
8. The **Description** field is optional. Enter a description of the task.

9. Action type and Action are pre-configured based on the task and cannot be modified.
10. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
11. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
  - a. Click the **box** next to the day(s) to select the day.
  - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
  - c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
  - d. To remove all settings click the **Clear All** button.
12. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.

**Note:** A repetition rate of zero causes the task to run only once.

  - a. Enter the **Repetition Rate** using whole numbers.
  - b. Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
  - c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

**Important:** The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.
  - d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.
13. Click **OK**.
14. Click **Save Settings**.

Table 14: System Backups Field Definitions

Field	Definition
<b>Remove local backups older than</b>	<p>Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the Network Sentry server before they are copied to the remote server. Backups on the remote server are not removed.</p> <p><b>Note:</b> The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.</p>
<b>Status</b>	Indicates whether the task is Enabled or Disabled.
<b>Schedule Interval</b>	How often the scheduled task runs. Options are Minutes, Hours, or Days.
<b>Next Scheduled Time</b>	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
<b>Modify Schedule</b>	Allows you to modify the scheduled activity.

## Updates

Updates groups together options for updating Network Sentry servers with the latest software release and the latest Agent Packages. Options include:

Option	Definition
<b>Agent Packages</b>	<p>Displays a list of the Dissolvable, Persistent and Passive Agent versions available on your FortiNac appliance. Download new agents and add them to Network Sentry as they become available from Fortinet using the Download button. Download an Administrative template for GPO configuration to your PC from the FortiNac appliance using the links at the top of the view.</p> <p>See Agent Packages on the facing page.</p>
<b>Operating System</b>	<p>Use Operating System Updates to download and install updates to the operating system on Network Sentry servers.</p> <p>See Operating System Updates on page 177.</p>
<b>System</b>	<p>Use System Updates to configure download settings, download updates from Fortinet, install updates and view the updates log.</p> <p>See System Update on page 180.</p>

## Agent Packages

The Agent Packages view displays a list of the Dissolvable, Persistent, Passive and Mobile Agent versions available on your FortiNac appliance. This view allows you to download new agents and add them to Network Sentry as they become available from Fortinet. See **Download New Agent Packages** on page 176.

**Note:** iOS Mobile Agents are not available through Network Sentry. The iOS Agent is distributed through the Apple Apps Store. The Android Agent can be downloaded from the captive portal if the device allows downloads from unknown sources, otherwise it is distributed through Google Play.

Both the Dissolvable and Persistent Agents can be supplied to hosts automatically by Network Sentry through the captive portal when the host reaches the appropriate web page. The agent presented to the host is based on the configuration of the Endpoint Compliance Policy applied to that host. Supplying the Passive agent requires additional configuration.

Hosts who already have a version of the Persistent Agent installed can be automatically updated to a newer version of the agent based on the settings you enter on the Agent Update tab.

You also have the option to download a Persistent Agent from the list to your own computer to be distributed to hosts through your web site, using a login script or some other distribution method. Files are saved on your computer in the default download location. This location varies depending on the browser you are using.

The Windows Persistent Agent is available in two formats: .msi and .exe. The .msi file is recommended for use in a managed install by non-user-interactive means. The .exe file is recommended for user-interactive installation. The Linux Persistent Agent is also available in two formats: .deb or .rpm. The Mac OSX Persistent Agent is available in .dmg format.

If you choose to distribute the agent using Group Policy Objects, you must download and install administrative templates on your Windows server. Use the links at the top of the Agent Distribution view to download the templates.

Use the **Delete** button to remove old versions of the Agent from your server.

**Agent Packages**

The following Agents are available. Use the links to download Persistent Agents in order to distribute through a desktop management system. To download administrative templates for GPO configuration, click the link appropriate for your server OS. (32-bit (x86) or 64-bit (x64))

Package	Agent Version	Name	Operating System	File	Size
agent-4.1.0.32.jar	4.1.0.32	Bradford Dissolvable Agent	Linux (x86_64)	Bradford_Dissolvable_Agent.bin	7,092 KiB
		Bradford Dissolvable Agent	Mac-OS-X	Dissolvable Agent.dmg	7,981 KiB
		Bradford Dissolvable Agent	Windows	Bradford Dissolvable Agent.exe	2,982 KiB
		Bradford Mobile Agent	Android	Bradford Mobile Agent.apk	2,355 KiB
		Bradford Mobile Agent (Store)	iOS iPhone	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS iPad	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS Unknown	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS iPod Touch	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	Android	Bradford Mobile Agent (Store)	2,355 KiB
		Bradford Passive Agent	Windows	Bradford_Passive_Agent.exe	2,386 KiB
		Bradford Persistent Agent (deb)	Linux (x86_64)	bni-persistent-agent_4.1.0.32-1.amd64.deb	11,780 KiB
		Bradford Persistent Agent (dmg)	Mac-OS-X	Bradford Persistent Agent.dmg	10,221 KiB
		Bradford Persistent Agent (exe)	Windows	Bradford Persistent Agent.exe	5,623 KiB
		Bradford Persistent Agent (msi)	Windows	Bradford Persistent Agent.msi	5,490 KiB
agent-4.1.0.30.jar	4.1.0.30	Bradford Persistent Agent (rpm)	Linux (x86_64)	bni-persistent-agent-4.1.0.32-1.x86_64.rpm	11,762 KiB
		Bradford Dissolvable Agent	Windows	Bradford Dissolvable Agent.exe	2,939 KiB
		Bradford Dissolvable Agent	Linux (x86_64)	Bradford_Dissolvable_Agent.bin	7,092 KiB
		Bradford Dissolvable Agent	Mac-OS-X	Dissolvable Agent.dmg	7,981 KiB
		Bradford Mobile Agent	Android	Bradford Mobile Agent.apk	2,355 KiB
		Bradford Mobile Agent (Store)	iOS Unknown	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	Android	Bradford Mobile Agent (Store)	2,355 KiB

Status: **New Agent Packages are Available**

Figure 84: Agent Packages

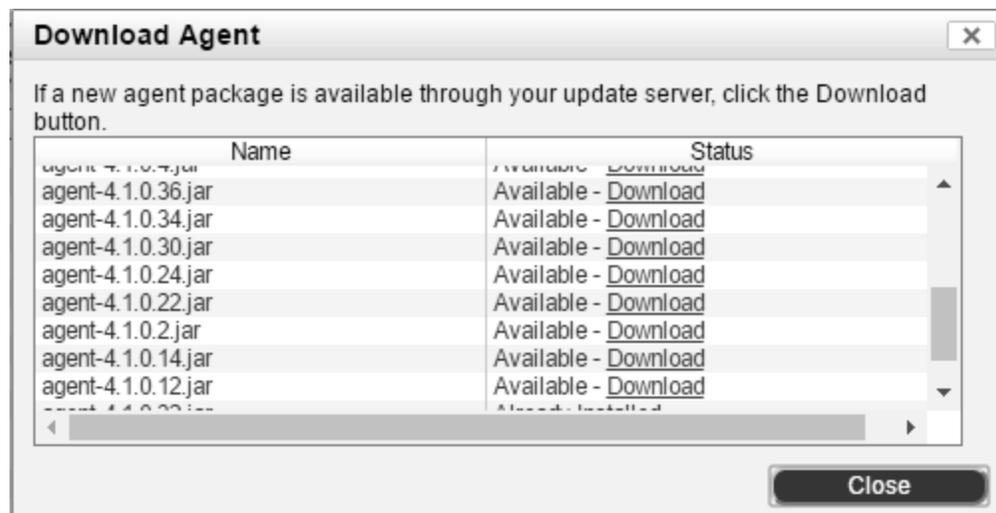
**Agent Packages Field Definitions**

Field	Definition
<b>Package</b>	Name of the .jar file containing the agents and supporting files.
<b>Agent Version</b>	Version number of the agent.
<b>Name</b>	Name of the type of agent. Agents include: <ul style="list-style-type: none"> <li>• Bradford Mobile Agent</li> <li>• Bradford Dissolvable Agent</li> <li>• Bradford Persistent Agent</li> <li>• Bradford Passive Agent</li> </ul>
<b>Operating System</b>	Operating system on which the agent can run.
<b>File</b>	File name and type, such as .exe or .bin.
<b>Size</b>	Download size of the agent file in KiB.
<b>Delete</b>	Allows you to delete old agent packages from the Network Sentry server.
<b>Download Agent Packages</b>	

Field	Definition
<b>Status</b>	Indicates whether there are new agent packages available for download from Fortinet. Status messages include: <ul style="list-style-type: none"><li>• Up to Date</li><li>• New Agent Packages Available</li></ul>
<b>Download</b>	Launches the Agent Download dialog allowing you to select new agent packages to be added to your Network Sentry server. See Download New Agent Packages on the next page.

**Download New Agent Packages**

New Agent packages are placed on the Fortinet update server when they become available. Agent packages contain all of the available Network Sentry agents and agent related files in two jar files: one file for Linux and one file for Windows, Mac OSX, and iOS. The iOS agent must be downloaded from the Apple App Store. The Android Agent can be downloaded from the captive portal if the device allows downloads from unknown sources, otherwise it is distributed through Google Play. However, there are supporting files for Mobile Agents in the Agent package. For any agent update you must download and install the latest agent package.

**Figure 85: Download Agent Packages**

To download a new agent package:

**Note:** Download settings must be configured correctly in order to download agent packages. See the Configure Settings section in **System Update** on page 180.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Agent Packages** from the tree.
4. Scroll to the bottom of the page. When new agents are available, the message **New Agent Packages Available** is displayed next to the Download button. The **Download** button to display a list of available agent packages.
5. Click the **Download** link next to an agent package to initiate the download. A progress page is displayed until the download is complete.
6. Click **Close** to return to the Agent Packages view.

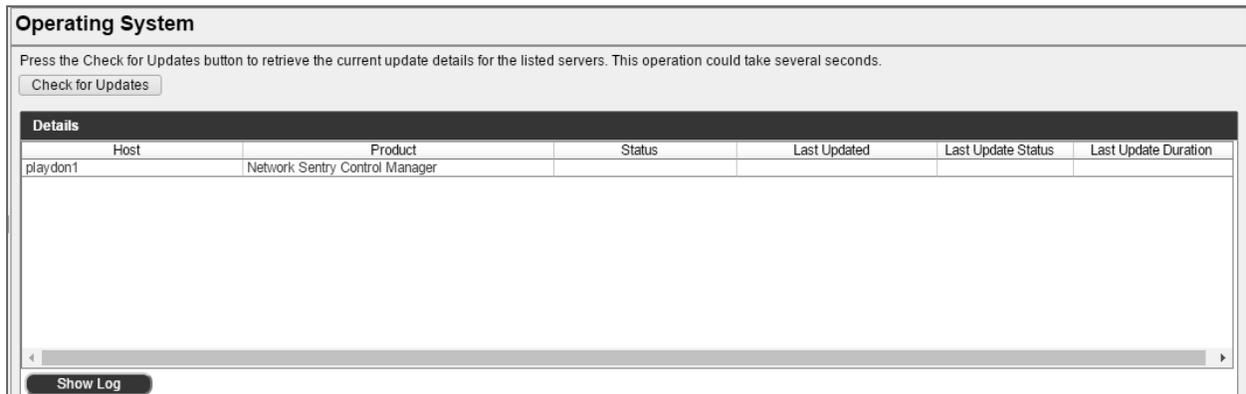
## Operating System Updates

The following information describes the method for updating CentOS on Network Sentry appliances and virtual machines. It is recommended that the operating system be updated regularly to maintain the highest possible level of security on the server. Refer to Bradford Networks CentOS Update Policy for additional details.

In a High Availability (HA) environment with redundant servers or in the case of a Network Sentry Control Server/Application Server pair, all of the servers can be updated from the Operating System Updates panel. If a server cannot be reached an error message displays in the table along with the IP address of the server.

When the Operating System Updates panel is accessed, the table displays the list of hosts. Clicking the Check for Updates button contacts the update repository and determines whether all of the available updates have been installed on each Network Sentry server. The status of each server is displayed in the table. Servers are updated by clicking the Update button. Operating System updates are downloaded from Fortinet via FTP. When an update is initiated the following event is generated: Operating System Update Initiated.

**Note:** The update process can take a long time and requires that the updated servers be rebooted.



**Figure 86: Operating System Updates**

### Requirements:

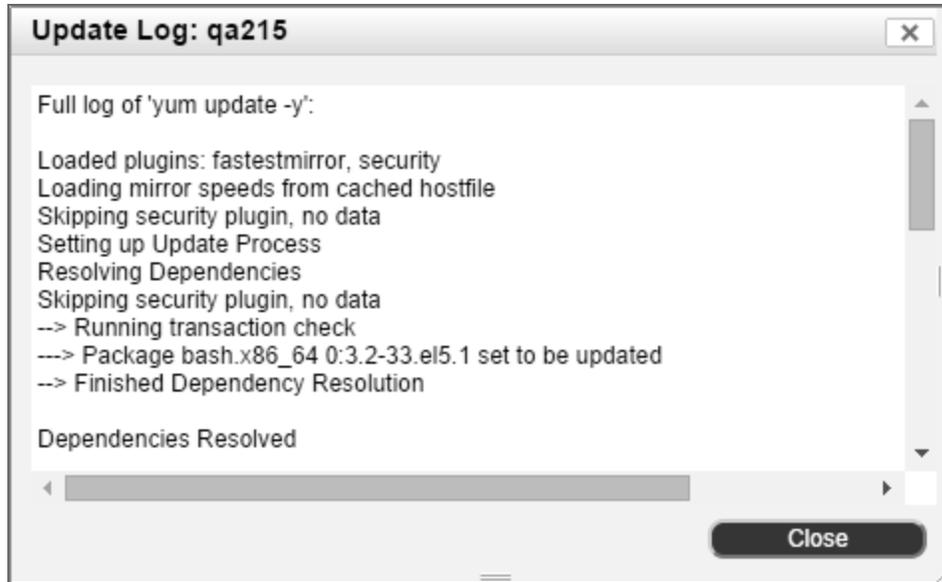
**Note:** Update packages from both CentOS and Fortinet are signed and will not install if keys do not match those on the appliance or virtual machine.

- Network Sentry firmware versions 3.x and higher.
- FTP access to bradfordnetworks.com from each appliance or virtual machine.
- HTTP access to centos.org from each appliance or virtual machine.

- Maintenance window to reboot the appliance or virtual machine after installing the updates.
- If updating appliances, you must have Dell hardware with one of these SKUs:
  - SYS-G-BFN310-XXXX
  - SYS-G-BFN320-XXXX
  - SYS-G-BFN330-XXXX
  - SYS-G-BFN610-XXXX
  - SYS-G-BFN620-XXXX
  - SYS-G-BFN630-XXXX
- Outbound internet access is recommended for all servers that are being updated.
- If you are running Network Sentry in a virtual machine, take a snapshot of the VM before updating the Operating System.

### Update The Operating System:

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Operating System** from the tree.
4. Click the **Check for Updates** button to check the FTP server for updates and assess whether the Network Sentry servers are up to date or not.
5. Click the **Update All** button to begin downloading and installing the Operating System updates.
6. A warning is displayed indicating that this is a long process and that you must reboot the server after the update. Click **Yes** to continue.
7. Use the **Show Log** button at the bottom of the table to view a log of the update process.



**Figure 87: Show Update Log**

8. When the update is complete, select **System Management > Power Management** from the tree.
9. Select each server and click **Reboot** to reboot the Network Sentry Server. If you have a Control Server and an Application Server, they must both be rebooted.

### Operating System Updates Field Definitions

Field	Definition
<b>Check For Updates Button</b>	Queries the Fortinet FTP site to determine if there are updates available and to check the update status of each Network Sentry server.
<b>Update All Button</b>	Displays only when there are updates available. The Status field indicates the status of the server selected in the table. It is the same as the Status column in the table.
<b>Host</b>	Name of the Network Sentry server.
<b>Product</b>	Type of Network Sentry server. Types include: <ul style="list-style-type: none"> <li>• Network Sentry Server</li> <li>• Network Sentry Control Server</li> <li>• Network Sentry Application Server</li> <li>• Network Sentry Integrated RADIUS Server</li> </ul>

Field	Definition
<b>Status</b>	<p>Indicates the overall update status of the Network Sentry Server or Control Server- /Application server pair, including:</p> <p><b>Updates Available</b> —Updates are available for one or more of the Network Sentry servers listed in the table.</p> <p><b>Up To Date</b>—All servers are up to date.</p> <p><b>Error</b> - Unable to establish an FTP session to downloads.bradfordnetworks.com</p> <p><b>Error</b> - Unable to ping host</p> <p><b>Error</b> - Unable to ssh to host</p>
<b>Last Updated</b>	Date and time of the last update attempt.
<b>Last Update Status</b>	<p>Indicates the state of the last update. States include:</p> <p><b>Never Updated</b>—Server has never had an operating system update.</p> <p><b>Success</b>—Server was updated successfully.</p> <p><b>Failed</b>—Update attempt has failed.</p>
<b>Last Update Duration</b>	Amount of time that it took to update the server on the most recent update attempt. If the last update was not successful, this number may be very low.
<b>Show Log</b>	Displays the update log.

### System Update

To update Network Sentry, download the most recent Network Sentry software distribution. Connection settings must be configured for access to the server where the download is hosted.

**Note:** The database is automatically backed up during the update process.

### Update In A High Availability Environment

To update your servers in a High Availability environment note the following:

- The Primary server must be running and in control in order to update the system.
- The Secondary server(s) must be running.
- The Primary server must be able to communicate with the Secondary server(s).
- The Primary server automatically updates the Secondary server(s).
- If the Secondary server(s) is in control, Network Sentry prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.

Update the Primary server following the instructions shown here for a regular update.

If you have a FortiNac Control Manager that manages your Network Sentry servers, you can run the update from the FortiNac Control Manager and select all managed servers to propagate the update throughout your environment.

### Configure Settings

Configure the connection settings for the download location so the Auto-Def Synchronizer, Agent Packages, and the Software Distribution Updates can be completed. You need to change the default settings if another server is used to host the auto-definition or updated distribution files.

**System**

**Actions**

- Download the latest product distribution
- Distribute an update to one or more servers
- Install the downloaded product distribution
- View recent update log

**System Update Settings**

NOTE: These settings take effect for all Updates, e.g. Auto-Definition Synchronization, System Updates, etc.

Host:  ?

Auto-Definition Directory:  ?

Product Distribution Directory:  ?

Agent Distribution Directory:  ?

User:  ?

Password:   ?

Protocol:  ?

Figure 88: System Update Settings

To set the host and protocol settings for the System Update:

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Go to the **System Update Settings** section of the screen.
5. Use the field definitions table below to enter the update settings.

Contact Customer Support for the correct login credentials.

6. Click **Test** to check that the settings allow connection to the Auto-Definition Directory and the Product Distribution Directory.

**Note:** Refer to the System Update Settings section of the Release Notes on our website for information about the distribution directory for the specific version you wish to download and install.

7. Once connection to the server is established, click **Save Settings**.

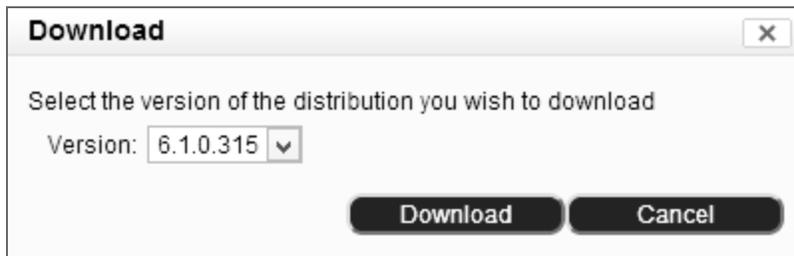
**Table 15: System Update Settings - Field Definitions**

Field	Definition
<b>Host</b>	IP Address, host name, or fully-qualified name of the server that is hosting the updates.
<b>Auto-Definition Directory</b>	<p>The sub-directory where the weekly anti-virus, anti-spyware and operating system updates are located. Default setting for this field is a period (.). If you are downloading these files from a server on your network, specify the directory containing the updates.</p> <p>If you prefer to download and install updates on a delayed schedule, you can choose system updates from one, two, three or four weeks ago by modifying this field with an additional sub-directory. For example, entering /week1 gives you an update that is one week old. Available directories are:</p> <p><b>.week1</b> contains updates that are one week old.  <b>.week2</b> contains updates that are two weeks old.  <b>.week3</b> contains updates that are three weeks old.  <b>.week4</b> contains updates that are four weeks old.</p>
<b>Product Distribution Directory</b>	<p>The sub-directory where the software or agent update files are located. This field will vary depending on the version of the software being updated.</p> <p>A forward slash (/) may be required in the path configuration. Click the Test button to confirm the configuration.</p> <p><b>Note:</b> Refer to the System Update Settings section of the Release Notes on our web site for information about the distribution directory for the specific version or agent package you wish to download and install.</p>
<b>Agent Distribution Directory</b>	Tests the connection between the Network Sentry program and the update server.
<b>User</b>	The user name for the connection.
<b>Password</b>	The password for the connection.

Field	Definition
<b>Protocol</b>	<b>SFTP</b> —Secure FTP. This protocol provides a more secure connection. <b>FTP</b> —File Transfer Protocol. <b>PFTP</b> —Passive FTP. A more secure form of data transfer in which the flow of data is set up and initiated by the FTP client rather than by the FTP server program.
<b>Buttons</b>	
<b>Test</b>	Tests the connection between the Network Sentry program and the update server.
<b>Revert To Defaults</b>	Returns the window to the factory default settings.

### **Download**

To update the software on the appliance, download the distribution files to the appliance.



**Figure 89: Select Distribution for Download**

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Click **Download**. Network Sentry automatically connects to the download server and retrieves a list of the files available for download. Network Sentry displays a warning message if no update files are found.
5. Scroll through the list of files available for download. Select the most recent distribution file and then click **Download**. Available distribution files are listed in order by version number with the most recent number at the top of the list.
6. Click **Download** to start the download process. This process runs in the background and closes automatically.

## **Install**

Once the distribution files have been downloaded to the appliance, you must manually start the installation. Since the update process restarts the appliance, choose a time to install the update when it will have the least impact on services. The update takes several minutes.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Click **Install**.
5. Select the distribution file from the drop-down list and click **Update**.
6. Verify that the update was successful by checking the version number for the currently installed version.

### **From the Admin User Interface:**

- Click the Help Menu and select About.
- Verify that the version number matches the update that was selected and installed.

### **From CLI:**

- Enter the following at the Network Sentry command line prompt:  
`master cat .version`
- Verify that the build date matches the update that was selected and installed.

**Show Log**

A log of the updates is maintained during installation. To view the logs, after installation, click **Show Log** and select the date of the installation.

**Note:** In a High Availability configuration, the Update Log files are located on the Primary appliance, since the Primary appliance must be in control during an update.

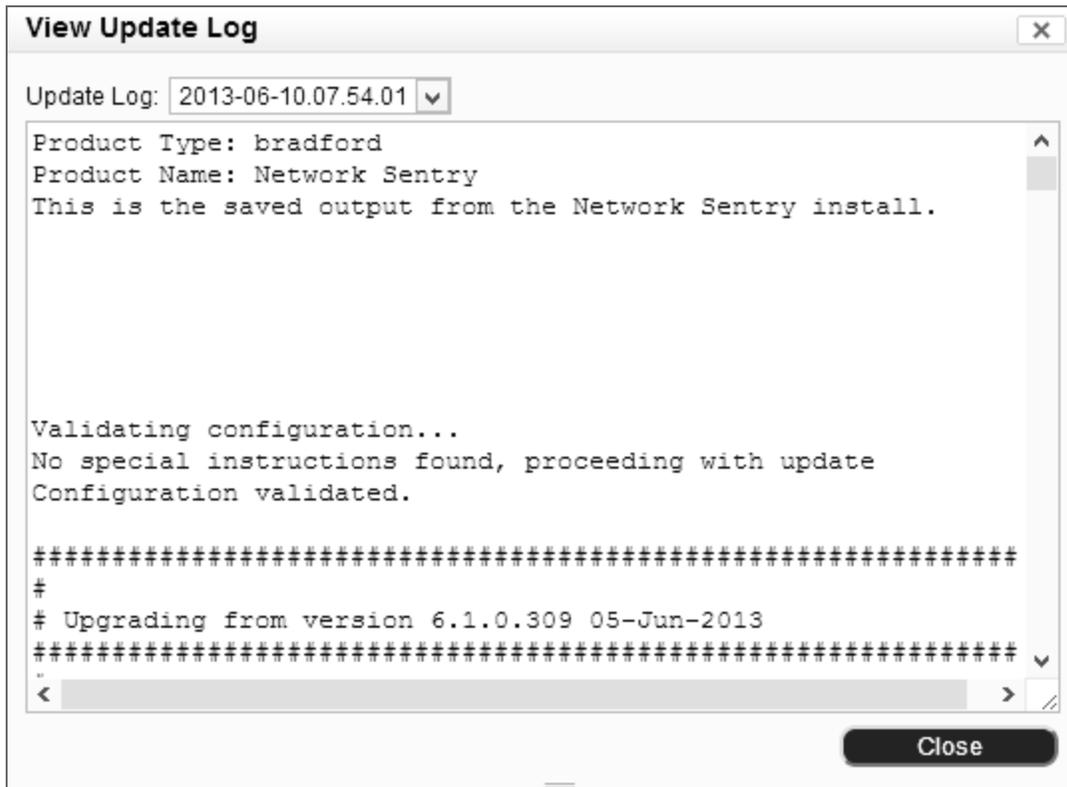


Figure 90: Show Log

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Click **Show Log**.
5. Select the **Date** from the list.
6. The log detail displays in the view.
7. Close the window.





## Chapter 4: Device Profiler

Device Profiler is a mechanism to automatically categorize and control unknown or rogue devices that connect to your network and receive an IP address. This process runs continuously. It scans the host database for rogues with IP addresses and assigns them a device type based on profiles or rules set up in Network Sentry. Device Profile Rules use information such as operating system and Vendor OUI to determine what the connecting device might be. Device Profiler is installed with some default rules which can be refined and new rules can be added. You can evaluate uncategorized rogues manually as new rules are added or existing rules are modified.

During an initial installation of Network Sentry this feature increases the speed with which devices are identified. After installation, Device Profiler provides easy management of new devices as they come online. Devices that are typically identified by Device Profiler include items such as IP Phones, Gaming Devices or Mobile Devices.

After a device has been categorized, the rule used to profile the device is associated with that device. If the device disconnects from the network and later reconnects, Device Profiler confirms that the device still matches the rule. If the device does not match its associated rule, Device Profiler can disable the device or notify the administrator by using events and alarms. Rule confirmation is an optional setting. This setting can be applied globally on the rule itself or individually on a profiled device.

To manage Device Profiler you have the option of creating administrative users known as Device managers with an Admin Profile that limits their permissions within Network Sentry. Creating additional users with limited permissions to manage new devices frees your regular IT staff to perform other tasks.

## Device Profiling Process

As new, unknown devices connect to the network, Device Profiler categorizes them and places the devices within Network Sentry based on its Device Profiling Rules. The process is as follows:

1. A device or host connects to the network.
2. Network Sentry learns that something has connected.
3. The Device Identity feature checks for a MAC address. If the MAC address is available, Device Identity compares it to known MAC addresses.
4. If the MAC address is unknown, the device is placed in the host database as a rogue with any additional information available, such as, IP address or operating system. The time interval that Device Profiler waits to resolve a MAC address to an IP address is 30 minutes, thus allowing time for normal IP to MAC polling to occur.
5. If the device has an IP address, Device Profiler begins to compare the available device information to its Device Profiling Rules. It starts with the rule that is ranked number one and works its way through the list of rules in order by rank until it finds a match to one of the rule's criteria or matching methods. Disabled rules are ignored.
6. A match is determined by a combination of the device type selected on the General Tab for the rule and one or more methods selected on the Methods Tab. For example, if the device type selected is Mobile Device and the Method selected is DHCP Fingerprinting, then a hand held device running Windows CE would match this rule. DHCP Fingerprinting would determine that the device is using Windows CE which is an operating system that corresponds to a Mobile Device.

However, if the device type selected is Gaming Device and the Method selected is DHCP Fingerprinting, then a hand held device running Windows CE would not match this rule because Gaming Devices do not use Windows CE.

Identification methods based on fingerprinting use the Network Sentry fingerprint database which cannot be modified by the user.

The exception to this is the Vendor OUI method. This method ignores the device type selected on the General Tab and uses the information selected within the method, such as the OUI, Vendor name, Vendor Alias or Device Type. Multiple entries are allowed, but the device only has to match one item to match the rule.

7. If Notify Sponsor is enabled, an email is sent by the Network Sentry server or Control server to all Device managers who have permission for devices associated with this rule. Permissions are based on the configuration of the Admin Profile attached to the administrative user. The email indicates that a new device has been processed.

8. The device is assigned the device type contained within the rule. Unless it is the Catch All rule which has no type. The type assigned by Device Profiler takes precedence over any type associated with the device's Vendor in the Network Sentry database. See **Vendor OUIs** on page 103.
9. The device is assigned the role contained within the rule. If no role is selected, the device is assigned the NAC Default role. The role assigned by Device Profiler takes precedence over any role associated with the device's Vendor OUI in the Network Sentry database. See **Vendor OUIs** on page 103.
10. Devices can be registered automatically or manually. If the rule is set to register manually, you must go to the Profiled Devices window to register the device.
11. If **Register As** is enabled in the matching rule, the device can be placed in the Host View or the Topology View or both.
12. If a Host View option was chosen the device can be added to a specific group as it is added to the Host View.
13. If the Access Availability option has been set to Specify Time, network access for devices placed in the Host View is limited to the configured times. To prevent devices from accessing the network outside the configured timeframe, they are marked "At Risk" for the Guest No Access admin scan.
14. When the device has been through the entire process and has been registered either automatically or manually, it will no longer display as a rogue. Depending on the options you chose in the rule it is displayed in the Host View.
15. If the device does not match any rule, it is associated with the default Catch All rule. Depending on the settings configured within this rule, the device can be associated with the rule but still remain a rogue.
16. Devices that are registered and associated with a user are placed in the Host View and removed from the Profiled Devices window. All other devices processed by Device Profiler remain in the Host View.

## Device Profiling Rules

Device Profiling Rules are used by the Device Profiler feature to categorize rogue hosts that connect to the network. As a rogue connects to the network and receives an IP address its information is compared to all methods within each enabled rule in turn until a match is found. The rogue device can be managed in a variety of ways depending on the configuration of the rule.

Any of the following scenarios could result from a match.

- The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and can be seen in the Profiled Devices window. It remains associated with the matching rule and can be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
- The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and is associated with a specific user, thus creating an identity for that device. It is removed from the Profiled Devices window and cannot be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
- The rogue matches a rule, but the rule is not configured to place the device in Topology View or Host View. The device remains a rogue, but is associated with the rule. Future rules can be run against this device as long as it remains unregistered. The device can be seen in the Profiled Devices window. If Notify Sponsor is enabled, the Device manager receives an e-mail that there was a match. The device can be managed by the Device manager. The Device manager can register the device which places it in the Host View or can delete the device. An administrative user can access the device in the Host View and change it to a device if it needs to be in Topology.

**Note:** Device Profiler does not see devices that are no longer rogues and cannot match those devices with new or modified rules.

Devices placed in the Host View display in the Profiled Devices window until the device is associated with a user.

### **Host View**

Device Profiling Rules can be used to place rogue devices in the Host View.

Devices that are kept in the Host View have a connection history and can be associated with a user. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

## Manage Device Profiling Rules

The Device Profiling Rules window displays the default set of rules provided. Use this window to modify the default rules or to create your own set of rules. Default rules vary depending on the version of the software and the firmware installed. Upgrading to a newer version of the software does not add or modify default rules.

Disabled rules are ignored when processing rogues. Device Profiling rules are disabled by default and are set not to register devices. When you are ready to begin profiling, enable the rule or rules you wish to use.

**Note:** Enabling certain rules could result in all unregistered PCs on your network being displayed in the Profiled Devices window. Review each rule carefully before enabling it.

The **Catch All** rule is always at the end of the list and its rank cannot be changed. As new rules are added they are inserted into the list immediately above the Catch All rule. This guarantees that all rogues profiled by Device Profiler are associated with a rule and can be managed by an administrative user with the appropriate Admin Profile, a Device manager. Device managers cannot manage devices that are not associated with a rule. This rule has no identification methods and no device type.

**Note:** Device Profiling Rules created on the Network Sentry server will be ranked above global Device Profiling Rules created on the NCM. The rank of a local Device Profiling Rule can be adjusted above or below another local Device Profiling Rule, but cannot be ranked below a global Device Profiling Rule. The rank of a global Device Profiling Rule cannot be modified from the Network Sentry server.

Device Profiling Rules can be accessed from **Hosts > Device Profiling Rules**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect	Confirm Rule Interval	Confirmation Fa
Yes	<input checked="" type="checkbox"/>	1	Android (DHCP)	Android	Automatic	DHCP	Host View	<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	2	Apple iOS (DHCP)	Apple iOS	Automatic	DHCP	Host View	<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	3	Mobile Device (DHCP)	Mobile Device	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	4	Windows (DHCP)	Windows	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	5	Linux (DHCP)	Linux	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	6	Unix (DHCP)	Unix	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	7	Printer (DHCP)	Printer	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	8	Printer (TCP:80,515,9100)	Printer	Manual	TCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	9	IP Phone (DHCP)	IP Phone	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	10	Gaming (DHCP)	Gaming Device	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	11	Apple iPhone (TCP:62078)	Mobile Device	Manual	TCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	12	Mac OS X (DHCP)	Mac OS X	Manual	DHCP		<input checked="" type="checkbox"/>	None	None
Yes	<input checked="" type="checkbox"/>	13	Catch All		Manual			<input checked="" type="checkbox"/>	None	None

Figure 91: Device Profiling Rules

### Device Profiling Rules Field Definitions

An empty field in a column indicates that the option has not been set.

Field	Definition
<b>Table Configuration</b>	
<b>Rank Buttons</b>	Moves the selected rule up or down in the list. Devices are compared to rules in order by rank.
<b>Set Rank Button</b>	Allows you to type a different rank number for a rule and immediately move the rule to that position. In an environment with a large number of rules this process is faster than using the up and down Rank buttons.
<b>Enable Buttons</b>	Enables or disables the selected rule. If a rule is disabled it is not used when processing a rogue host.
<b>Table Columns</b>	
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Enabled</b>	A green check mark indicates that the rule is enabled. A red circle indicates that the rule is disabled.
<b>Rank</b>	Rule's rank in the list of rules. Rank controls the order in which devices are compared to rules.
<b>Name</b>	User defined name for the rule.
<b>Type</b>	Device type that is assigned when the rule is a match for a rogue host.
<b>Registration</b>	Indicates whether devices matching this rule are registered automatically or manually.
<b>Methods</b>	The method or methods used to identify a device. Methods include: IP Range, DHCP Fingerprinting, Location, TCP, NMAP, Passive Fingerprinting, Vendor OUI and UDP.
<b>Register As Device</b>	When a device is registered it can be placed in the Host View, the Topology View or both. This column indicates where the device is placed when it is registered. If the column is blank, then the registration option has not been set for this rule.
<b>Notify</b>	<p>A green check mark indicates that Notify is enabled. When a new device is detected and it matches this rule, an email is sent to all Device managers that have this rule associated with their Admin Profile.</p> <p>A red circle indicates that the Notify option is disabled.</p>
<b>Role</b>	Role assigned to devices matching this rule.
<b>Access Availability</b>	Times that devices matching this rule are permitted to access the network. Devices matching this rule are marked "At Risk" for the <b>Guest No Access</b> admin scan during the times they are not permitted to access the network.

Field	Definition
<b>Add To Group</b>	Devices matching this rule are added to the group displayed. Add to Group is only available for devices that are added to the Host View.
<b>Container</b>	Devices matching this rule are added to the Container displayed. Devices can only be placed in a Container if they are being added to the Topology View.
<b>Confirm Rule On Connect</b>	If enabled, Device Profiler confirms that previously profiled devices associated with this rule still match this rule the next time they connect to the network. A green check mark indicates that the option is enabled. A red circle indicates that the option is disabled.
<b>Confirm Rule Interval</b>	If enabled, Device Profiler confirms at set intervals that previously profiled devices associated with this rule still match this rule.
<b>Confirmation Failure Action</b>	If enabled, Device Profiler disables previously profiled devices that no longer match their associated rule.
<b>Last Modified By</b>	User name of the last user to modify the rule.
<b>Last Modified Date</b>	Date and time of the last modification to this rule.
<b>Right Mouse Click Menu Options</b>	
<b>Copy</b>	Copy the selected Rule to create a new record.
<b>Delete</b>	Deletes the selected Rule(s). Removes the association between that rule and the devices it matched. Devices associated with deleted rules will no longer display on the Profiled Devices window.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Modify</b>	Opens the Modify Device Profiling Rule window for the selected rule.
<b>Buttons</b>	

Field	Definition
<p><b>Import</b></p>	<p>Enables you to import information from the Network Sentry Server(s) to the FortiNac Control Managers so that during the next Global Synchronization (if enabled), the information will be written to other Network Sentry Servers in your network. This eliminates the need to manually enter the information on the FortiNac Control Manager. When it is imported to the FortiNac Control Manager, the information is treated as global information.</p> <p>The following describes some caveats to consider when importing items:</p> <p>If the name of an item that is being imported already exists on the FortiNac Control Manager, the item will not be imported.</p> <p>If an item being imported from a Network Sentry Server has a dependent item with the same name as a dependent item that already exists on the FortiNac Control Manager, the dependent item is not imported to the FortiNac Control Manager. The item will be imported and use the dependent item that already existed on the Network Sentry Control Manager.</p> <p>For example, if a User/Host Profile called "Student" exists on the FortiNac Control Manager and an Endpoint Compliance Policy is imported from a Network Sentry Server that also uses a User/Host Profile called "Student", the "Student" Profile (dependent item) that exists on the FortiNac Control Manager will not be imported. The Endpoint Compliance Policy will be imported and use the dependent item (User/Host Profile) that was already there. This results in the settings for the Network Sentry Control Manager's Endpoint Compliance Policy's User/Host Profile possibly differing from the Endpoint Compliance Policy's User/Host Profile on the FortiNac Control Manager.</p>
<p><b>Export</b></p>	<p>Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.</p>
<p><b>Run Button</b></p>	<p>Used to re-run the Device Profiler process when rules have been modified or added. Devices that have already been categorized are not affected. Only rogues that remain in the Host View are processed. If rules are set to notify Device managers via e-mail when rogues connect, processing existing rogues triggers those e-mails again.</p> <p>Rogues that are no longer connected are ignored.</p>

## Device Profiling Rules - Best Practices

The configuration of Device Profiling rules should be considered carefully to optimize performance. The list below outlines concepts that should be taken into account when configuring rules.

1. When a device or host connects to the network, the Device Profiling Rules are checked in order starting with the rule ranked number 1. The order of the rules is important. For the best performance, it is recommended that you rank rules based on the Methods used to categorize devices and hosts as follows: OUI rules first, DHCP rules next and Active, TCP/UDP port, IP Range, Location rules last.

**Note:** In an environment where static IP addresses are used, DHCP rules should be at the end of the list. Devices with static IP addresses do not send out DHCP broadcast packets. Therefore, Network Sentry will never receive a DHCP fingerprint for those devices and the profiling process will not continue past the DHCP rules.

**Note:** It is recommended that you set up IP Helper addresses for DHCP on your routers when using DHCP fingerprinting. Use the IP address of eth0 on the Network Sentry Server or the Application Server. Do not use the IP address of the Network Sentry Control Server.

2. The device information necessary to compare against a rule, must be available for Device Profiler to successfully move from one rule to the next. If the information required for a rule to be matched is unavailable, the evaluation of that device ends. For example, if the IP address of the device cannot be determined, Device Profiler cannot move past any rule that uses IP address as match criteria. The reason that the Device Profiler does not skip the rule and continue with the next one is that combinations of rules would not work. In the example below, if the Device Profiler skips the first rule because the TCP port cannot be found, the Apple iPhone will be miscategorized. If the Device Profiler does not skip the rule, Apple iPhone remains uncategorized and the user can either manually determine what the device is or can adjust the rules to catch it.

**Example:** This example outlines how two rules can be used together to provide greater accuracy when profiling devices. Apple iPhone and MAC OS fingerprints tend to be almost identical, but the iPhone can be distinguished by a TCP port which can be used in a rule to identify that device. In this case, you can create two rules: the first to identify iPhones by scanning for the iPhone TCP port and the second to scan for MAC OS in general. The iPhone rule is more granular and will catch the phone before it is categorized by the MAC OS rule.

3. OUI only rules are the quickest to process because no outside data is necessary.
4. Rules that require an IP address take longer to process because the Network Sentry server may need to read the DHCP leases file or layer 3 tables from the routers.
5. Device Profiler uses the latest IP address from the IP-to-MAC cache, if the IP address exists. It does not rely on the IP address seen in the Adapter View

because it may be stale. If the IP address does not exist in the cache, Network Sentry starts an IP –to-MAC lookup on all L3 devices. Network Sentry stops the lookup as soon as the address is found, therefore, in most cases every L3 device will not be polled. If the Network Sentry server is not properly configured to read layer 3 from the routers, it may cause Device Profiling rules that require an IP address to fail.

### Add Or Modify Device Profiling Rule

1. Click **Hosts > Device Profiling Rules**.
2. Click the **Add** button or select a rule and click **Modify**.
3. Refer to the tables below for information on each option on this window.
4. On the **Methods** tab you can select one or more methods for identification.

**Note:** The device must meet criteria established for all of the methods selected.

Select a single method of identification. If you find that too many devices match the rule, add a second method to refine the profiling process and reduce the number of false matches.

5. Click **OK** to save.

**Device Profiling Rule - General Tab**

**Add Device Profiling Rule**

General | Methods

Enabled

Name:

Description:

Note:

Notify Sponsor

Registration Settings

Registration:  Automatic  Manual

Type:

Role:

Register To Logged In User ( If Present )

Register as:

Container:

Add to Group:

Access Availability:

Rule Confirmation Settings

Confirm Device Rule on Connect

Confirm Device Rule on Interval:

Disable Device If Rule No Longer Matches Device

**Figure 92: Add Device Profiling Rule - General**

## Device Profiling Rule - General Tab Field Definitions

Field	Definition
<b>Enabled</b>	Mark with a check mark to enable this rule. Disabled rules are skipped when comparing devices to rules.
<b>Name</b>	User specified name for this rule. Required.
<b>Description</b>	Description of the rule.
<b>Note</b>	User specified note that can be viewed by administrators and users with the appropriate Admin profile who manage devices that match this rule.
<b>Notify Sponsor</b>	<p>If enabled, users whose Admin Profile gives them permission to manage devices associated with this rule are notified whenever a device has been matched to this rule. This includes rogues that have been processed again by clicking the Run button on the Device Profiling Rules window.</p> <p>An e-mail is sent by the Network Sentry server or Control server indicating that a device matched this rule. The message would read as follows:</p> <p>A new rogue (00:12:3F:19:1A:F4), matching rule Windows, was found.</p> <p>Requires that the Device Profile Rule Match event be enabled. It is enabled by default and should not be disabled.</p>
<b>Registration Settings</b>	
<b>Registration</b>	<p>Indicates whether device registration is automatic or manual.</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> The device is registered immediately if the Register As option is enabled.</li> <li>• <b>Manual:</b> The device is registered manually from the Profiled Devices window. The <b>Register As</b> option on this window must be enabled in order to manually register the device.</li> </ul>
<b>Type</b>	Device category in which a device matching this rule should be placed. This controls the icon associated with the device in the Host or Topology Views.
<b>Role</b>	<p>Roles are attributes of users and hosts and are used as filters in User/Host Profiles. Those profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant Easy Connect Policy to apply.</p> <p>If you are using Role-based access for hosts/devices managed in Topology View, select the role that controls access to the network for this device. If you are not using Role-based access, select NAC-Default.</p>
<b>Register To Logged In User (If Present)</b>	<p>If a user logs into the device being profiled, the user becomes the owner of that device in the Network Sentry database.</p> <p><b>Note:</b> This applies only to users that log in with an 802.1x supplicant configured to send the User ID.</p> <p>If the device is registered to the logged in user, then any options selected under <b>Register As</b> are ignored even if <b>Register As</b> is enabled.</p>

Field	Definition
<b>Register As</b>	<p>If <b>Register To Logged In User</b> is enabled, and a user is logged in, this option is ignored even if it is enabled.</p> <p>If <b>Register To Logged In User</b> is disabled, this option is used to determine where to place the connecting device.</p> <p>Click the check box to enable this option. Indicates where the registered device will be placed. Options include:</p> <ul style="list-style-type: none"> <li>• Device in Host View</li> <li>• Device in Topology View</li> <li>• Device in Host And Topology View</li> </ul> <p>If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.</p>
<b>Container</b>	<p>Select or create a container for this type of device. Click the <b>New</b> button to create a new Container. Containers are a mechanism used to group items in Topology.</p> <p>This field remains disabled unless one of the Topology View options is selected in the Register As field.</p>
<b>Add to Group</b>	<p>Place devices in an existing group or create a new group for them. Grouping devices to manage them as a group instead of individually. See <b>Groups View</b> on page 681.</p> <p>This field remains disabled unless one of the Host View options is selected in the Register As field.</p>
<b>Access Availability</b>	<p>Allows you to control when devices that match this rule can access the network. Options include: Always or Specify Time. This option is only enabled for devices that are managed in the Host View or both the Host View and the Topology View.</p> <p>If you set times for Access Availability, devices that match this rule are marked "At Risk" for the <b>Guest No Access</b> admin scan during the time that they are not permitted to access the network.</p>
<b>Rule Confirmation Settings</b>	
<b>Confirm Device Rule On Connect</b>	<p>If enabled, Device Profiler confirms that previously profiled devices associated with this rule still match this rule the next time they connect to the network.</p>
<b>Confirm Device Rule On Interval</b>	<p>If enabled, Device Profiler confirms at set intervals that previously profiled devices associated with this rule still match this rule. Interval options include Minutes, Hours, or Days.</p>
<b>Disable Device If Rule No Longer Matches Device</b>	<p>If enabled, Device Profiler disables previously profiled devices that no longer match their associated rule.</p>

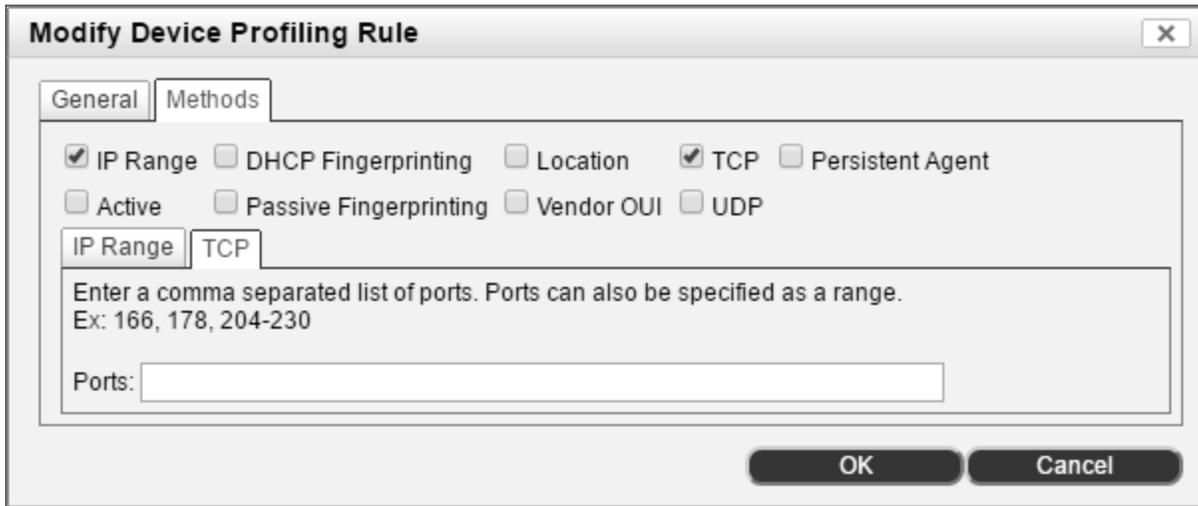
### **Specify Access Availability Time For Device Profiling Rule**

This option allows you to limit network access for a device based on the time of day and the day of the week. Any device associated with a rule, can only access the network as specified in the Access Availability field for the rule. This option is only enabled for devices that are managed in the Host View or both the Host View and the Topology View.

If you set times for Access Availability, Network Sentry periodically checks the access time for each device associated with the rule. When the device is not allowed to access the network it is marked "At Risk" for the **Guest No Access** admin scan. When the time is reached that the device is allowed to access the network, the "At Risk" state is removed. These changes in state occur on the device record whether the device is connected to the network or not. If the device has a browser and connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your Network Access has been disabled. You are outside of your allowed time window. To regain network access call the help desk."

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Modify**.
3. In the **Access Availability** field select **Specify Time**.
4. In the **Time Range** section enter the From and To times for the time of day that devices should be able to access the network.
5. In the **Days of the Week** section select the days during which these devices should be allowed to access the network.
6. Click **OK**.

**Device Profiling Rule - Methods Tab**



**Figure 93: Add Device Profiling Rule - Methods Tab**

**Device Profiling Rule - Methods Tab Field Definitions**

Method	Definition
IP Range	Matches if the IP address of a device falls within one of the ranges specified. You must specify at least one IP range.
DHCP Fingerprinting	<p>Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled. The DHCP fingerprint is used to determine the Operating System of the device.</p> <p>For example, if the Operating System is Windows CE and the device type on the General Tab is Mobile Device, then the device matches this rule. If the Operating System is Windows CE and the device type on the General Tab is Gaming Device, then the device does not match this rule.</p> <p>DHCP fingerprinting is more accurate than Passive fingerprinting.</p> <p>Based on Network Sentry's fingerprint database.</p> <p><b>Note:</b> It is recommended that you set up IP Helper addresses for DHCP on your routers when using DHCP fingerprinting.</p>
Location	Matches if the device connects to the selected location on your network. Options are: anything within a Container in the Topology View, anything in a Port Group or anything in a Device Group.

Method	Definition
<b>TCP</b>	Matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports can be entered separated by commas, such as, 162, 175, 188. A range of ports can be entered using a hyphen, such as 204-215.
<b>Active</b>	Matches if the device type selected on the General tab is the same as that determined by NMAP for the connecting device.
<b>Persistent Agent</b>	Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled, and if the device has an Agent installed on the host, such as, the Persistent Agent or one of the Mobile Agents. The Agent is used to determine the Operating System of the device. To register hosts running the Persistent Agent using this method, you must disable registration under Persistent Agent Properties. If you do not, the Persistent Agent may register the host before the Device Profiler has the opportunity to register it.
<b>Passive Fingerprinting</b>	Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled. The DHCP Fingerprint is used to determine the Operating System of the device. Based on Network Sentry's fingerprint database.
<b>Vendor OUI</b>	<p>Matches if the Vendor OUI for the device corresponds to the OUI information selected for this method. You must specify at least one Vendor option. If there are multiple entries, the device only has to match one to match this rule. Options include:</p> <p><b>Vendor Code</b> — A specific Vendor OUI selected from the list in the Network Sentry database. To select the OUI begin typing the first few characters. A list of matching OUIs is displayed in a drop-down list.</p> <p><b>Vendor Name</b> — A single Vendor Name selected from the list in the Network Sentry database. To select the name, begin typing the first few characters. A list of matching Vendors is displayed in a drop-down list.</p> <p><b>Note:</b> The asterisk (*) wildcard can be used at the beginning and end to capture all variations of the Vendor Name (e.g., Avaya*).</p> <p><b>Vendor Alias</b> — Enter a Vendor alias that exists in the Network Sentry vendor database. Must be an exact match.</p> <p><b>Note:</b> The asterisk (*) wildcard can be used at the beginning and end to capture all variations of the Vendor Alias.</p> <p><b>Device Type</b> — Select a device type from the drop-down list provided. Includes items such as Alarm System or Card Reader. If this option is selected the device type associated with the Vendor OUI of the connecting device must match the device type for the Vendor in the Network Sentry vendor database.</p>
<b>UDP</b>	Matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports can be entered separated by commas, such as, 162, 175, 188. A range of ports can be entered using a hyphen, such as 204-215.

### Delete A Device Profiling Rule

When a Device Profiling Rule is deleted the association between that rule and the devices it matched is removed. Devices associated with that rule will no longer display on the Profiled Devices window. They will continue to display in the Host View.

The **Catch All** rule is a default system rule that cannot be removed. Other default rules can be removed.

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

### Copy A Device Profiling Rule

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Copy**.
3. The Add Device Profiling Rule window displays with the information from the selected rule.
4. You must, at minimum, modify the name of the rule. Modify other fields as needed and click **OK** to save.
5. For field definitions see **Add Or Modify Device Profiling Rule** on page 199.

## Evaluate Rogue Hosts With Device Profiling Rules

Over time you may have hosts that remain rogues because they do not match any of the rules enabled in the Device Profiling Rules window. You may also have hosts that have been categorized incorrectly. At any time you can modify the rules or create additional rules and then re-evaluate hosts. Only those hosts that remain unregistered can be re-evaluated.

If a host has been categorized incorrectly and has been registered, you have two options. Either manually modify the host or delete the host and when it connects to the network again, it will be evaluated by the rules.

**Note:** Rogues that are no longer connected or are offline are ignored.

To re-evaluate rogue hosts:

1. Click **Hosts > Device Profiling Rules**.
2. Click **Run**.
3. A message displays asking if you would like to evaluate rogues. Click **Yes** to continue.
4. A new message displays indicating that x number of rogues are being evaluated.
5. Device Profiler compares any rogue hosts to the list of enabled Device Profiling Rules and processes them accordingly. See **Device Profiling Process** on page 190 for additional information.
6. When the process is complete, click **OK** to close the message box.

### Administrative User Profiles For Device Managers

In Network Sentry, you can create an administrative user and give that user an Admin Profile that contains permissions for the Device Profiler feature set. These privileges are designed to restrict this user to certain parts of the program.

For Device Profiler, the Admin Profile, referred to as a Device manager in documentation, requires permission for Profiled Devices. This allows the user to manage new devices and categorize them.

Additional permissions can be given to Device Managers based on the parameters of their responsibilities. Create one or more Admin Profiles for these types of users. See **Admin Profiles And Permissions** on page 219.

## Add A Device Manager Admin Profile

This procedure describes how to create an Admin Profile for an administrative user with permissions for Device Profiler. This user can access the Profiled Devices tab and use that window to register, delete, enable or disable hosts and enter notes about a host. The Profiled Devices window displays devices that are treated as hosts and are also displayed in the Host View.

You can have an Admin Profile that allows an administrative user to perform additional tasks by adding more permission sets. These step-by-step instructions assume that the Admin Profile will provide permissions only for Device Profiler. Details on other settings and permissions sets see **Add An Admin Profile** on page 243.

To create a Device manager Admin Profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Device Manager.
4. Under **Manage Hosts and Ports** select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
7. The minimum that this Device Manager must have is the **Profiled Devices** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Profiled Devices permission set, the Landing Page field defaults to Profiled Devices.
9. The Profile Devices tab is enabled when Custom is selected for the Profiled Devices permission set. Click on the **Profiled Devices** tab.
10. Use the field definitions below to configure the Profile Devices specific fields.
11. Click **OK** to save.

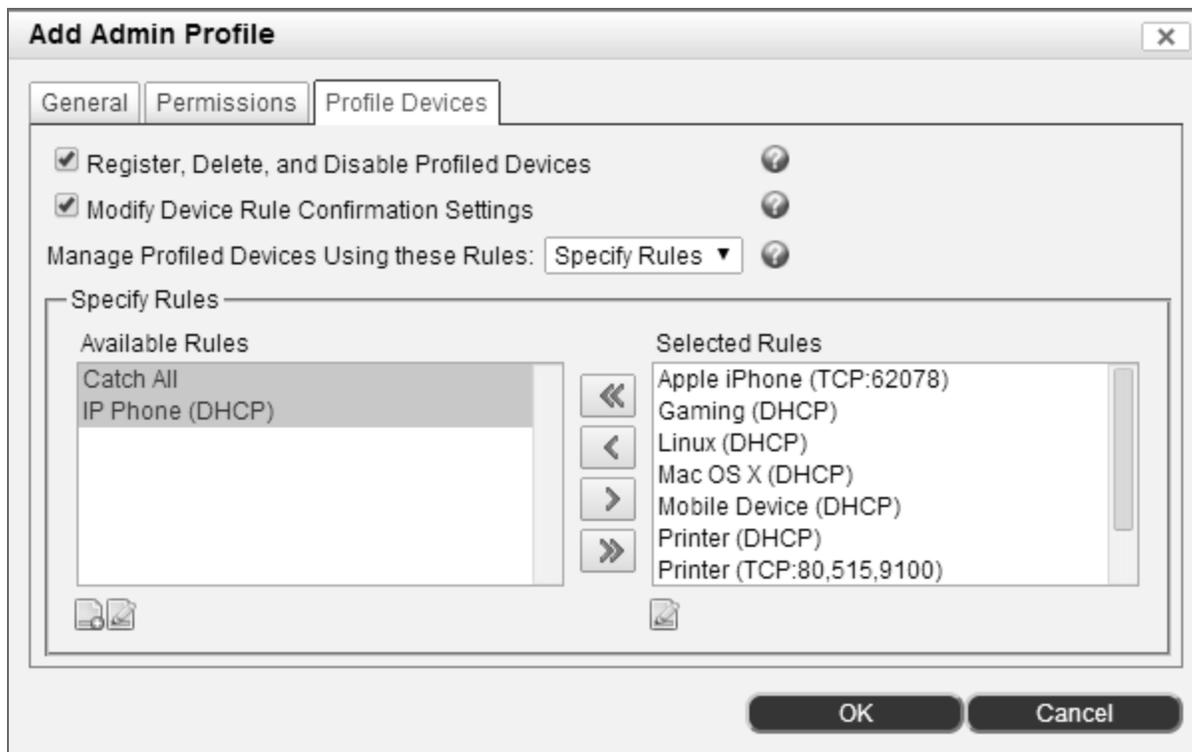


Figure 94: Add Device Manager Admin Profile

### Admin Profile Fields For Device Managers

Field	Definition
<b>Register, Delete, and Disable Profiled Devices</b>	If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler.
<b>Modify Device Rule Confirmation Settings</b>	If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.
<b>Manage Profiled Devices Using These Rules</b>	<b>All Rules</b> —includes current rules and any rules created in the future. <b>Specify Rules</b> —you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
<b>Available Rules</b>	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
<b>Selected Rules</b>	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
<b>Add Icon</b>	Click this button to create a new Device Profiling Rule. For information on rules, see Add Or Modify Device Profiling Rule on page 199.
<b>Modify Icon</b>	Click this button to modify the selected Device Profiling Rule. For information on rules, see Add Or Modify Device Profiling Rule on page 199.

### Add An Administrative User For Device Profiler

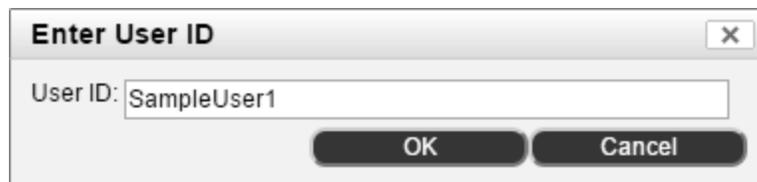
If you are creating Admin Users to manage guests or devices, you must create an Administrative User who has the appropriate Admin User Profile associated. See **Admin Profiles And Permissions** on page 219.

To add an Administrative user account:

1. Create the Administrator, Operator, or Help Desk user on the FortiNac Server or FortiNac Control Server that the user has access to for searches.

**Note:** For Local Authentication make the password for the user the same on the FortiNac Server, FortiNac Control Server, or FortiNac Control Manager.

2. Log in to the FortiNac Control Manager.
3. Select **Users > Admin Users**.
4. Click **Add**.
5. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.



**Figure 95: Enter the User ID**

This allows you to give a network user administrator privileges to help with some administrative tasks.

**Add User** X

Asterisk (\*) indicates required fields.

**User Information**

\*Authenticate Type: Local ▼

\*Admin Profile: Device Manager ▼  

\*User ID: SampleUser1 \*Password: \*\*\*\*

First Name: Sample \*Last Name: User

Address: 55 Main St.

City: Concord State: NH

Zip/Postal Code: 03301 Phone: 603-555-1234

Email: sampleuser@email.com Title:

Mobile Number: 603-555-1111

Mobile Provider: AT&T (xxxxxxxxxx@txt.att.net) ▼

Notes:

User Never Expires

**OK** **Cancel**

### Admin User Field Definitions

Field	Definition
<b>Authentication Type</b>	<p>Authentication method used for this Admin user. Types include:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server. If an integrated RADIUS server has been added under RADIUS Settings and the Authentication Type field is set to RADIUS, a RADIUS User record is automatically added to the RADIUS User's view for this user.</li> </ul> <p><b>Note:</b> Authentication of Admin Users via RADIUS is not currently available, however, Admin Users can still be created with the RADIUS authentication type for use on NetworkSentry pods.</p>

Field	Definition
<b>Admin Profile</b>	<p>Profiles control permissions for administrative users. See Admin Profiles And Permissions on page 219.</p> <p><b>Add</b> — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window.</p> <p><b>Modify</b> — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.</p>
<b>User ID</b>	Unique alphanumeric ID for this user.
<b>Password</b>	<p>Password used for local authentication.</p> <p><b>Note:</b> If you authenticate users through LDAP, the password field is disabled and the user must log in with their LDAP password.</p>
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>Address</b>	Optional demographic information.
<b>City</b>	
<b>State</b>	
<b>Zip/Postal Code</b>	
<b>Phone</b>	
<b>E-mail</b>	
<b>Title</b>	User's title, such as Mr. or Ms.
<b>Mobile Number</b>	Mobile Phone number used for sending SMS messages to administrators.
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
<b>Notes</b>	Free form notes field for additional information.
<b>User Never Expires</b>	<p>If enabled, Admin users are never aged out of the database. The default is enabled.</p> <p><b>Note:</b> Admin Users assigned the Administrator Profile cannot be aged out.</p>

## Admin User Field Definitions

Field	Definition
<b>Authentication Type</b>	<p>Authentication method used for this Admin user. Types include:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server. If an integrated RADIUS server has been added under RADIUS Settings and the Authentication Type field is set to RADIUS, a RADIUS User record is automatically added to the RADIUS User's view for this user.</li> </ul> <p><b>Note:</b> Authentication of Admin Users via RADIUS is not currently available, however, Admin Users can still be created with the RADIUS authentication type for use on NetworkSentry pods.</p>
<b>Admin Profile</b>	<p>Profiles control permissions for administrative users. See Admin Profiles And Permissions on page 219.</p> <p><b>Add</b> — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window.</p> <p><b>Modify</b> — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.</p>
<b>User ID</b>	Unique alphanumeric ID for this user.
<b>Password</b>	<p>Password used for local authentication.</p> <p><b>Note:</b> If you authenticate users through LDAP, the password field is disabled and the user must log in with their LDAP password.</p>
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>Address</b>	Optional demographic information.
<b>City</b>	
<b>State</b>	
<b>Zip/Postal Code</b>	
<b>Phone</b>	
<b>E-mail</b>	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>Title</b>	User's title, such as Mr. or Ms.

Field	Definition
<b>Mobile Number</b>	Mobile Phone number used for sending SMS messages to administrators.
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
<b>Notes</b>	Free form notes field for additional information.
<b>User Never Expires</b>	If enabled, Admin users are never aged out of the database. The default is enabled.  <b>Note:</b> Admin Users assigned the Administrator Profile cannot be aged out.

## Device Profiler Events And Alarms

Certain actions within Device Profiler generate events that appear in the Event Log. Examples of Device Profiler events are listed in the following table.

Event	Definition
<b>Device Profile</b>	Generated whenever device profiling updates a rogue.
<b>Device Profile Rule Match</b>	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
<b>Device Profiling Automatic Registration</b>	A rogue host has been registered by device profiling based on a device profiling rule.
<b>Device Profiling Rule Missing Data</b>	Indicates that Device Profiler cannot compare a rogue against a rule because Network Sentry does not have enough information about the rogue, such as a DHCP fingerprint. If Device Profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
<b>Device Rule Confirmation Success</b> <b>Device Rule Confirmation Failure</b>	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.

Events can be mapped to alarms. Alarms can be set to notify an administrator when they are triggered. Alarms can also be viewed on the Alarms Panel on the Dashboard. For more information on events and alarms, e-mail notifications, and how to map events to alarms see **Map Events To Alarms** on page 493.



## Chapter 5: Admin Profiles And Permissions

Admin Profiles are templates assigned to Administrative Users to define what a user can do in Network Sentry. Every Administrative User is required to have an Admin Profile. An Admin Profile can be assigned to more than one Administrative User.

Each Admin Profile contains a list of permissions that are inherited by the associated Administrative Users. Permissions configured in Admin Profiles control the views in Network Sentry that can be accessed. If permission for access is given, in most cases, the Administrative User can Add/Modify and Delete data.

**Note:** If an Admin Profile that is in use is changed, the changes do not take effect until the associated Administrative Users log out of Network Sentry and log in again.

### **Custom Setting**

For special functions such as Guest Manager or Device Profiler there are Advanced permissions. Advanced permissions control items such as the Guest Account templates that can be used by someone with permission for Guest/Contractor Accounts.

### **Landing Page**

Admin Profiles also designate the first screen or landing page displayed when the Administrative User logs into Network Sentry, days and times that users can log in and the number of minutes of inactivity that trigger an automatic logout. Due to the complexity of the permissions structure, it is recommended that you define the job functions of your Administrative Users to ensure that you have considered the permissions required for each Admin Profile.

### **Profile Mapping**

Admin Profiles can be mapped to Groups to automatically assign a profile to Administrative Users as they are added to selected groups. Note that if Admin Profile Mapping is configured, moving an Administrative User to a group that is mapped changes their profile to the profile for the group. See **Admin Profile Mappings Process** on page 254 for additional information.

### **Administrator Profile**

The Administrator profile is a default system profile that cannot be copied, deleted or renamed. This is the only profile that has access to every view in Network Sentry including: Admin Users, Admin Profiles and the Quick Start wizard. See **Default Admin Profiles** on page 222.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Inactivity Time	Login Availability	Landing Page	NCM Landing Page	Note	Last Modified By	Last Modified Date
Yes	Administrator	60 minutes	Always	Dashboard	Roles	Default Admin Profile Added By SYSTEM.	root	07/14/16 01:14 PM EDT
Yes	BadProfile	60 minutes	Always	Guest/Contractor Accounts			root	07/21/16 10:24 AM EDT
Yes	GuestTemplateOnly	60 minutes	Always	Guest/Contractor Templates			root	07/13/16 04:34 PM EDT
Yes	Help Desk	60 minutes	Always	Locate		Default Admin Profile Added By SYSTEM.	SYSTEM	05/09/16 08:17 AM EDT
Yes	Logs	60 minutes	Always	Admin Auditing			root	06/20/16 01:59 PM EDT
Yes	Operator	60 minutes	Always	Manage Hosts & Ports		Default Admin Profile Added By SYSTEM.	SYSTEM	05/09/16 08:17 AM EDT
Yes	Security Analyst	60 minutes	Always	Dashboard		Default Admin Profile Added By SYSTEM.	SYSTEM	05/09/16 08:17 AM EDT
Yes	Test	60 minutes	Always	Security Actions	Scheduler		root	07/14/16 10:56 AM EDT

Figure 96: Admin Profiles

Admin Profiles Field Definitions

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Name</b>	User specified name for the profile. This name is displayed in the Admin User window when you are attaching the profile to an Administrative User.
<b>Inactivity Time</b>	User is logged out after this amount of time has elapsed without any activity.
<b>Login Availability</b>	Indicates when users with this profile can log in to Network Sentry. Options include: Always or Specify Time. If you choose Specify Time, the user is limited to certain times of day and days of the week.
<b>Landing Page</b>	Indicates the first view displayed when an Admin User with this profile logs into Network Sentry.
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry
<b>Last Modified By</b>	User name of the last user to modify the profile.
<b>Last Modified Date</b>	Date and time of the last modification to this profile.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

Field	Definition
<b>Copy</b>	Copy the selected Profile to create a new record. The Administrator Profile cannot be copied.
<b>Delete</b>	Deletes the selected Profile. Profiles cannot be deleted if they are in use. The Administrator Profile can never be deleted.
<b>Modify</b>	Opens the Modify Admin Profile window for the selected profile. On the Administrator Profile only the Inactivity Time can be modified.
<b>In Use</b>	Opens a list of Administrative Users that have the selected profile attached.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Audting Log, see <b>Admin Auditing</b> on page 446</p>
	<p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>

**Default Admin Profiles**

Network Sentry has some default profiles that can be used to control system access. These profiles are always included in the database. With the exception of the Administrator Profile, they can be modified, deleted or copied.

**Default Profiles - New Database**

The table below describes the profiles that are in any new Network Sentry database and the default settings for each profile.

<b>View</b>	<b>Access</b>	<b>Permissions Enabled</b>
<b>Administrator</b>		
<b>All</b>	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The Administrator profile has access to every part of Network Sentry.	All
<b>Help Desk</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Locate Hosts &amp; Users</b>	User can search for Hosts and Users but cannot modify data.  This is the default landing page when a user with this profile logs into Network Sentry.	Access
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Operator</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.  Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access

View	Access	Permissions Enabled
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, but cannot send a message.</li> <li>• User Properties - View Only.</li> <li>• Device Identity - View and export data.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Profile_Sample</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Guest/Contractor Accounts</b>	<p>User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.</p> <p>User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.</p>	Access, Add/Modify Custom Settings
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Security Analyst</b>		
<b>Dashboard</b>	User can access and view the Dashboard	Access
<b>Network Devices</b>	<p>User can view, add, modify, or delete network devices in the following views:</p> <ul style="list-style-type: none"> <li>• CLI Configuration</li> <li>• Device Profiling Rules</li> <li>• L2 Polling</li> <li>• L3 Polling</li> <li>• Locate</li> <li>• Port Changes</li> <li>• Topology</li> </ul>	Access Add/Modify Delete

View	Access	Permissions Enabled
<b>Users/Hosts/ Adapters</b>	User can access, add, modify, or delete users, hosts, and adapters in the following views: <ul style="list-style-type: none"> <li>• Adapters View</li> <li>• Connections</li> <li>• Device Identity</li> <li>• Hosts View</li> <li>• Scan Results</li> <li>• Users View</li> </ul>	Access Add/Modify Delete

**Possible Profiles - Upgraded Database**

Prior versions of Network Sentry contained several user types with varying permissions. From Version 7.0 forward there is only one type of user, Administrative, and access is controlled based on the settings of the Admin Profile associated with each user. During the upgrade process any existing Admin User types and their corresponding permissions are converted to Admin Profiles and assigned to Admin Users. There may be many as two Help Desk profiles and eight Operator profiles created during the upgrade. The table below contains the full list of Admin Profiles that could be created.

View	Access	Permissions Enabled
<b>Administrator</b>		
<b>All</b>	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The Administrator profile has access to every part of Network Sentry.	All
<b>Help Desk</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Locate Hosts &amp; Users</b>	User can search for Hosts and Users but cannot modify data.  This is the default landing page when a user with this profile logs into Network Sentry.	Access
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify

View	Access	Permissions Enabled
<b>Help Desk With Messaging</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Locate Hosts &amp; Users</b>	User can search for Hosts and Users but cannot modify data.  This is the default landing page when a user with this profile logs into Network Sentry.	Access
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent or Bradford Mobile Agent for Android installed.	Access
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Operator</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.  Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, but cannot send a message.</li> <li>• User Properties - View Only.</li> <li>• Device Identity - View and export data.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete

<b>View</b>	<b>Access</b>	<b>Permissions Enabled</b>
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Operator With Messaging</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, and can send a message.</li> <li>• User Properties-View Only.</li> <li>• Device Identity - View and export data.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent installed.	Access
<b>Operator With Add Hosts</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access

View	Access	Permissions Enabled
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, but cannot send a message.</li> <li>• User Properties-View only.</li> <li>• Device Identity - View and export data.</li> <li>• User can add hosts.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access Add/Modify
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Operator With Delete Hosts</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, but cannot send a message.</li> <li>• User Properties-View only.</li> <li>• Device Identity - View and export data.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access Delete
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Operator With Add Hosts And Messaging</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify

<b>View</b>	<b>Access</b>	<b>Permissions Enabled</b>
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, and can send a message.</li> <li>• User Properties-View only.</li> <li>• Device Identity - View and export data.</li> <li>• User can add hosts.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access Add/Modify
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent installed.	Access
<b>Operator With Delete Hosts And Messaging</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, and can send a message.</li> <li>• User Properties-View only.</li> <li>• Device Identity - View and export data.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access Delete
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete

View	Access	Permissions Enabled
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent installed.	Access
<b>Operator With Delete Hosts, Add Hosts And Messaging</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Locate Hosts &amp; Users</b>	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
<b>Manage Hosts &amp; Ports</b>	<ul style="list-style-type: none"> <li>• Adapter List - Disable adapters.</li> <li>• Adapter Properties- View only.</li> <li>• Host Properties-View and modify access, and can send a message.</li> <li>• User Properties-View only.</li> <li>• Device Identity - View and export data.</li> <li>• User can add hosts.</li> </ul> <p>This is the default landing page when a user with this profile logs into Network Sentry.</p>	Access Add/Modify Delete
<b>Guest/Contractor Accounts</b>	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent installed.	Access
<b>Profile_Sample</b>		
<b>Group Membership</b>	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
<b>Guest/Contractor Accounts</b>	<p>User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.</p> <p>User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.</p>	Access, Add/Modify Custom Settings

<b>View</b>	<b>Access</b>	<b>Permissions Enabled</b>
<b>Self-Registration Requests</b>	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
<b>Security Analyst</b>		
<b>Dashboard</b>	User can access and view the Dashboard	Access
<b>Network Devices</b>	User can view, add, modify, or delete network devices in the following views: <ul style="list-style-type: none"><li>• CLI Configuration</li><li>• Device Profiling Rules</li><li>• L2 Polling</li><li>• L3 Polling</li><li>• Locate</li><li>• Port Changes</li><li>• Topology</li></ul>	Access Add/Modify Delete

## Permissions List

Admin Profiles contain permissions settings. An Administrative User inherits permissions from the Admin Profile applied to his user account. The table below contains a list of the permissions that can be set in an Admin Profile and any special information about each setting.

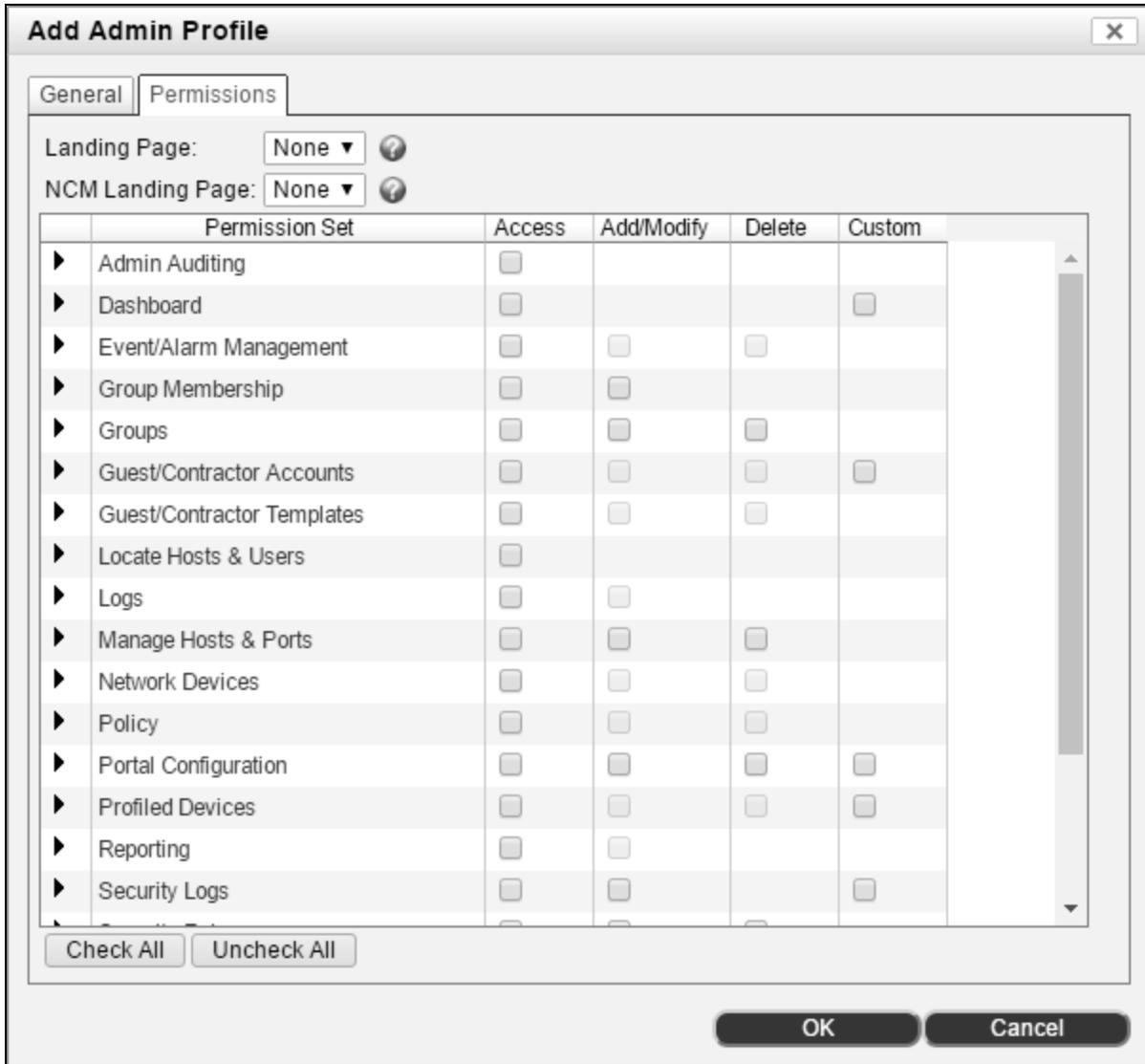


Figure 97: Admin Profile - Permissions

**Table 16: Access Levels**

<b>Level</b>	<b>Definition</b>
<b>Access</b>	<p>If enabled, the user will be able to see data in the views shown in the Permission Set, but not add, modify or delete. There are some exceptions to this that are noted in the table of permissions.</p> <p>In some cases, by enabling Access, other permissions are automatically enabled. For example, if you enable Access for Guest/Contractor Accounts, Add/Modify and Delete are automatically enabled and cannot be disabled.</p>
<b>Add/Modify</b>	<p>If enabled, the user can add or modify data in the views shown in the Permission Set.</p>
<b>Delete</b>	<p>If enabled, the user can delete data in the views shown in the Permission Set.</p>
<b>Custom</b>	<p>If enabled, an additional tab is shown that contains advanced settings for the Permission Set. For example, if Access to Guest/Contractor Accounts is enabled and Custom is enabled, advanced options can be set on the Manage Guests tab.</p>

Table 17: Permissions List

**Note:** Where applicable, this table assumes that Access, Add/Modify, Delete and Custom options are enabled.

Views	Permissions	Notes
<b>Admin Auditing</b>		
<b>Admin Auditing</b>	Provides access to the Admin Auditing Log.	
<b>Dashboard</b>		
<b>Dashboard</b>	<p>Provides access to the Dashboard Tiles. Tiles require additional permissions as follows:</p> <ul style="list-style-type: none"> <li>• <b>Alarms Panel</b>—Requires access to Event/Alarm, links and buttons are enabled if Add/Modify is enabled.</li> <li>• <b>Summary Panel</b>—Requires access to System Settings.</li> <li>• <b>Network Device Summary Panel</b>—Requires access to Devices, links are enabled if Add/Modify or Delete are enabled for Devices.</li> <li>• <b>Host Summary Panel</b>—Requires access to Users/Hosts/Adapters.</li> <li>• <b>Scans Panel Panel</b>—Requires access to Policy.</li> <li>• <b>User Summary Panel</b>—Requires access to Users/Hosts/Adapters.</li> <li>• <b>License Information Panel</b>—Requires access to System Settings.</li> <li>• <b>Persistent Agent Summary Panel</b>—Requires access to Policy.</li> <li>• <b>Performance Summary Panel</b>—Requires access to Event/Alarm.</li> </ul>	Requires that other permissions be selected to display associated tiles.
<b>Event/Alarm</b>		
<b>Event to Alarm Mappings</b> <b>Event Management</b>	If enabled, the views shown in the left column can be accessed.	Reports can be accessed but not all options can be used without access to User/Host/Adapter being enabled.
<b>Group Membership</b>		

Views	Permissions	Notes
<b>Group Membership</b>	<p>Allows access to Host, User, Device or Port group membership. Requires that one of the following additional permissions be enabled:</p> <ul style="list-style-type: none"> <li>• Devices</li> <li>• Locate Hosts &amp; Users</li> <li>• Manage Hosts &amp; Ports</li> <li>• Users/Hosts/Adapters</li> </ul>	
<b>Groups</b>		
<b>Groups</b>	If enabled, allows access to the Groups View where you can view, add, modify or delete a group.	
<b>Guest/Contractor Accounts</b>		
<b>Guest/Contractor Accounts</b>	If enabled, allows access to the Guest Contractor Accounts View where you can view, add, modify or delete a guest account.	Has a Custom option that enables the Manage Guests Tab.
<b>Custom/Manage Guests</b>	<p>This tab displays when the Custom permission is enabled. Custom Options include:</p> <ul style="list-style-type: none"> <li>• <b>Guest Account Access</b>—Indicates whether user can access All, Own or No guest accounts after they have been created.</li> <li>• <b>Account Types</b>—Allows user to create Individual, Bulk and or Contractor accounts</li> <li>• <b>Create Accounts Days in Advance (Maximum)</b>—Number of days before guest registers that the account can be created.</li> <li>• <b>Create Accounts Active For Days (Maximum)</b>—Maximum number of days that accounts created by this user are allowed to be active.</li> <li>• <b>Allowed Templates</b>—Templates that can be used to create Guest Accounts</li> </ul> <p>Refer to Add A Guest Manager Admin User Profile on page 645 for detailed information.</p>	
<b>Integrated RADIUS</b>		
<b>NAS Clients RADIUS Logs RADIUS Users.</b>	<p>If enabled, the views shown in the left column can be accessed.</p> <p>To add an integrated RADIUS server to Network Sentry you must have System Settings permission.</p>	
<b>Locate Hosts &amp; Users</b>		

Views	Permissions	Notes
<b>Locate Hosts &amp; Users</b>	<p>If enabled, the views shown in the column on the left can be accessed.</p> <ul style="list-style-type: none"> <li>• User can view Adapter, Host, User and Device Identity.</li> <li>• User can view Group Membership for Hosts and Users.</li> <li>• User can modify Host information including registering a host.</li> <li>• User can modify User properties for network users and Admin users.</li> <li>• User can delete Host and Adapter records.</li> </ul>	
<b>Logs</b>		
<b>Alarms</b>  <b>Connections</b>  <b>Events</b>  <b>Scan Results</b>	<p>If enabled, the views shown in the column on the left can be accessed.</p> <p>Users can view information about events within the system and on the network.</p>	
<b>Manage Hosts &amp; Ports</b>		
<b>Manage Hosts &amp; Ports</b>	<p>If enabled, the views shown in the column on the left can be accessed. Access is limited to users, hosts and adapters in groups for which user has permission. See Limit User Access With Groups on page 693.</p> <ul style="list-style-type: none"> <li>• User can view Adapter, Host, User and Device Identity.</li> <li>• User can modify Host information including registering a host.</li> <li>• User can modify User properties for network user.</li> <li>• User can enable or disable an adapter.</li> <li>• User can view Port properties for the ports where an adapter is connected.</li> </ul>	
<b>Network Devices</b>		

Views	Permissions	Notes
<b>Network Device Summary Dashboard Tile</b>  <b>CLI Configuration</b> <b>Device Profiling Rules</b> <b>L2 Polling</b> <b>L3 Poling</b> <b>Locate</b> <b>Port Changes</b> <b>Topology</b>	<p>If enabled, the views shown in the left column can be accessed.</p>	<p>To see Profiled Devices that option must be enabled separately.</p>
<b>Policy</b>		
<b>Control Access</b>  <b>Network Device Roles</b>  <b>Passive Agent Configuration</b>  <b>Persistent Agent Properties</b>  <b>Policy Configuration</b>  <b>Remediation Configuration</b>  <b>Roles</b>	<p>If enabled, the views shown in the left column can be accessed.</p> <p>The Passive Agent Registration View requires access to Groups to add or modify Passive Agent Configurations.</p>	
<b>Portal Configuration</b>		
<b>Portal Configuration</b>	<p>If enabled, allows the user to view and edit settings for portals. Users with the Policies permission set enabled will also have this permission set enabled.</p> <p>Custom options include:</p> <ul style="list-style-type: none"> <li>• <b>Access</b> — Allows the user to view the portal settings.</li> <li>• <b>Add/Modify</b> — Allows the user to view the settings, add new portal settings, and delete existing portal configurations. Requires that Access permissions be enabled. Permissions can be further modified to prevent the user from adding new portal configurations or modifying the Default Portal Configuration.</li> <li>• <b>Delete</b> — Allows the user to view portal settings, add new ones, and modify and delete existing portal configurations. Requires that Add/Modify permissions be enabled.</li> </ul>	
<b>Profiled Devices</b>		

Views	Permissions	Notes
<p><b>Profiled Devices</b></p>	<p>If enabled, allows the user to view the list of profiled devices. User can also Export devices, register a device, enable or disable a device, delete the device from the list and view details and notes for a selected device.</p> <p>The Views column on the Profiled Devices View contains icons that provide access to details about the selected device. these icons only display if additional permissions are enabled for the Administrative User. Possible views include: Adapter Properties, Group Membership, Port Properties and Device Properties.</p> <p><b>Adapter Properties</b>—Requires permission for Users, Hosts and Adapters.</p> <p><b>Group Membership</b>—Requires permission for Group Membership.</p> <p><b>Port Properties</b>—Requires permission for Devices.</p> <p><b>Device Properties</b>—Requires permission for Users, Hosts and Adapters or Devices.</p>	<p>Has a Custom option that enables the Profile Devices Tab.</p>

Views	Permissions	Notes
<b>Custom/Profile Devices</b>	<p>This tab displays when the Custom permission is enabled. Custom Options include:</p> <ul style="list-style-type: none"> <li>• <b>Register, Delete, and Disable Profiled Devices</b>—If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler.</li> <li>• <b>Modify Device Rule Confirmation Settings</b>—If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.</li> <li>• <b>Manage Profiled Devices Using These Rules</b>— <ul style="list-style-type: none"> <li><b>All Rules</b>—includes current rules and any rules created in the future.</li> <li><b>Specify Rules</b>—you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.</li> </ul> </li> <li>• <b>Available Rules</b>—Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.</li> <li>• <b>Selected Rules</b>—Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.</li> </ul> <p>Refer to Add A Device Manager Admin Profile on page 209 for detailed information.</p>	
<b>Reporting</b>		
<b>Analytics</b>	If enabled, the views shown in the left column can be accessed.	
<b>Reports</b>		
<b>Security Logs</b>		
<b>Security Alarms</b>	If enabled, the views shown in the left column can be accessed.  User has access to view security alarms created when a security rule is matched. Users can take action on a security alarm if it was not done automatically. The user's Admin Profile settings determine the actions they are allowed to complete.	This permission set is only available when RTR is enabled within your current license package.  Has a Custom option that enables the Security Events tab.
<b>Security Events</b>		
<b>Security Rules</b>		

Views	Permissions	Notes
<b>Security Actions</b>  <b>Security Rules</b>  <b>Security Triggers</b>	If enabled, the views shown in the left column can be accessed.  User can create security devices, threat analysis engines, and security event rules. Users will establish and maintain all rules and the default actions associated with each rule.	This permission set is only available when RTR is enabled within your current license package.
<b>Self Registration Requests</b>		
<b>Self Registration Requests</b>	If enabled, user can manage requests for network access submitted by Guests from the captive portal.	
<b>Send Message</b>		
<b>Send Message</b>	User can send messages to hosts with the Persistent Agent or Bradford Mobile Agent for Android installed.	
<b>System Settings</b>		
<b>Scheduler</b>  <b>Settings</b>	If enabled, the views shown in the left column can be accessed.	All settings can be accessed when this permission is enabled. Refer to Settings on page 63 for a complete list.
<b>Users/Hosts/Adapters</b>		
<b>Adapters View</b>  <b>Device Identity</b>  <b>Hosts View</b>  <b>Users View</b>	If enabled, the views shown in the left column can be accessed.	

### Modify Admin Profiles

To modify an existing Admin Profile, do the following:

1. Log into your Administrator account.
2. Click **Users > Admin Profiles**.
3. A list of existing profiles is displayed..
4. Select a profile and click **Modify**. Refer to **Add An Admin Profile** on page 243 for field definitions.
5. Change the information and click **OK** to save.

**Note:** If you modify an Admin Profile, the changes apply to all administrative accounts it is attached to, including those created before you modified the profile. Changes do not take effect until the associated Administrative Users log out of Network Sentry and log in again

**Note:** The Modify Admin Profile window can also be accessed from the Admin Users View by clicking on the profile link associated with each Admin user.

## Modify Admin Profiles for Administrator Users



The screenshot shows a dialog box titled "Modify Admin Profile" with a close button in the top right corner. The dialog contains the following fields and controls:

- Name:** Administrator
- Logout After:** 60 minutes of inactivity
- Landing Page:** Dashboard (dropdown menu)
- Buttons:** OK and Cancel

To modify an Admin Profile for an Administrator user, do the following.

1. Log into your Administrator account.
2. Click **Users > Admin Profiles**.
3. Select the Administrator profile and click **Modify**.
4. Enter the amount of time needed to elapse without any activity in the user interface before the user is logged out.
5. Select the Landing Page for the Administrator user from the drop-down list.
6. Click **OK** to save.

**Note:** If you modify an Admin Profile, the changes apply to all administrative accounts it is attached to, including those created before you modified the profile. Changes do not take effect until the associated Administrative Users log out of Network Sentry and log in again

### Delete An Admin Profile

To delete an existing Admin Profile from the system, do the following.

**Note:** You can not delete an Admin Profile if it is in use.

1. Log into your Administrator account.
2. Click **Users > Admin Profiles**.
3. Select an Admin Profile and click **Delete**.
4. A message displays asking if you are sure. Click **Yes** to continue.

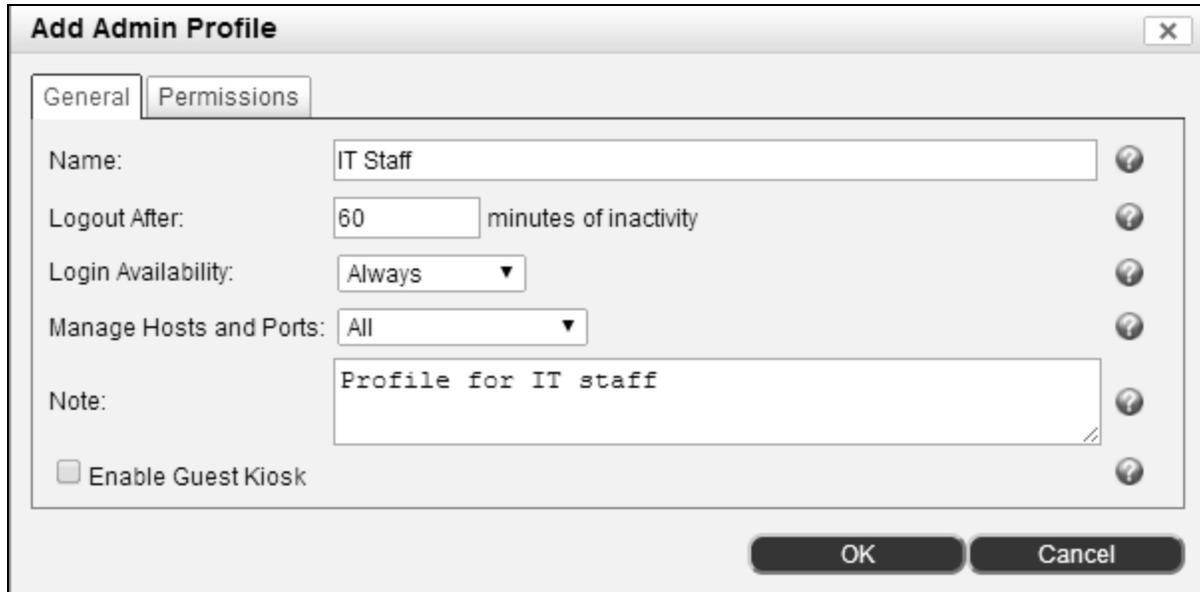
### Copy Admin Profiles

You can create a copy of an existing Admin Profile and save it with a different name. This saves time when you create Admin Profiles if you are only changing a few fields.

1. Log into your Administrator account.
2. Click **Users > Admin Profiles**.
3. The Admin Profiles option opens a window containing existing profiles.
4. To copy an Admin Profile, select the profile and click **Copy**.
5. Modify information as needed. For detailed field information refer to one of the following:
  - Admin Profile Field Definitions** on page 245
  - Add A Guest Manager Admin User Profile** on page 645
  - Admin Profile Fields For Device Managers** on page 211
6. Click **OK**.

## Add An Admin Profile

Admin Profiles control permissions for Administrative Users.



The screenshot shows a dialog box titled "Add Admin Profile" with a close button (X) in the top right corner. It has two tabs: "General" (selected) and "Permissions". The "General" tab contains the following fields:

- Name:** A text input field containing "IT Staff".
- Logout After:** A text input field containing "60" followed by the text "minutes of inactivity".
- Login Availability:** A dropdown menu set to "Always".
- Manage Hosts and Ports:** A dropdown menu set to "All".
- Note:** A text area containing "Profile for IT staff".
- Enable Guest Kiosk**

Each field has a help icon (question mark) to its right. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Figure 98: Add Admin Profile - General Tab

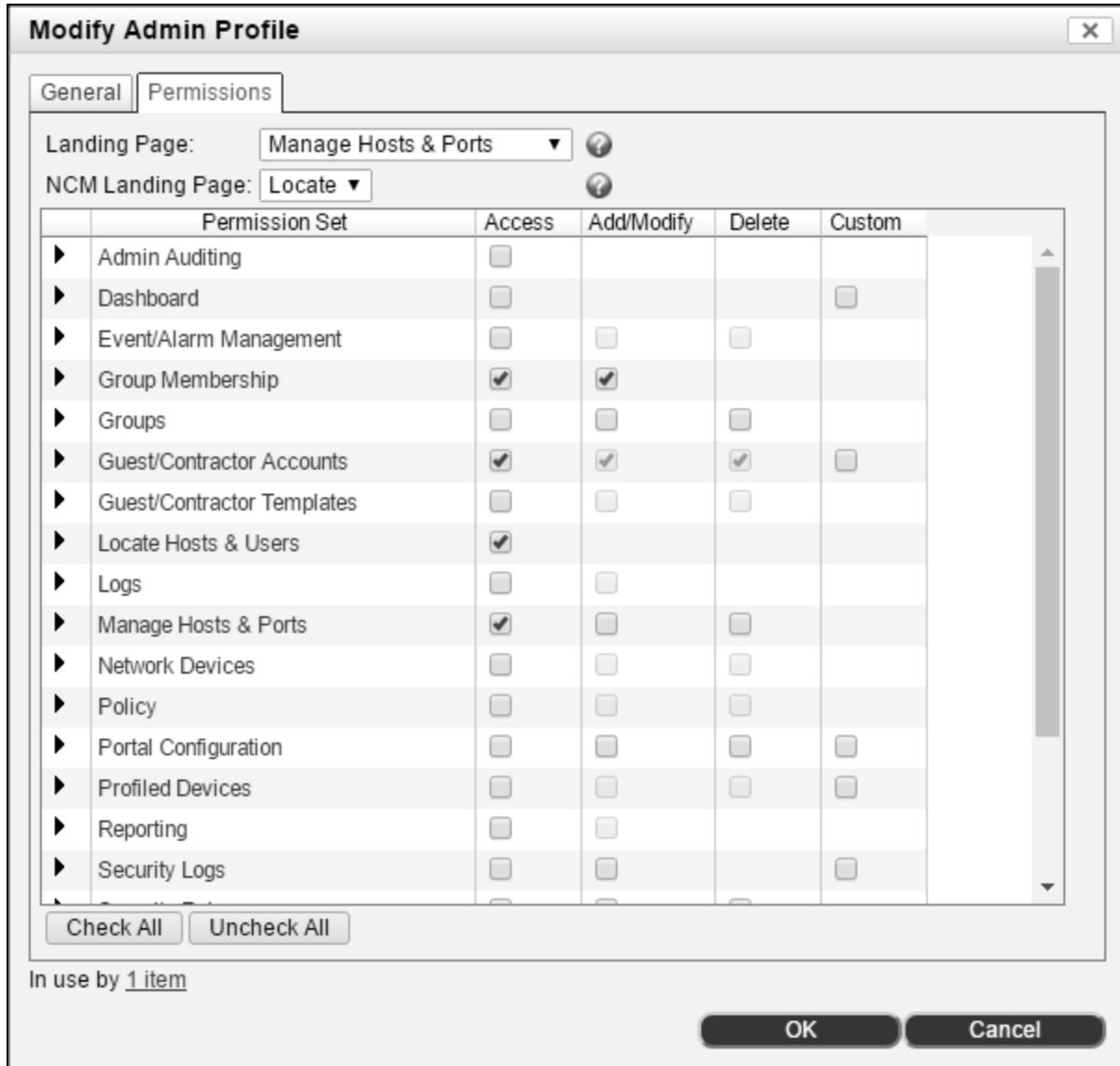


Figure 99: Add Admin Profile - Permissions Tab

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. Enter a name for the profile.
4. Use the field definitions below to configure the new Admin Profile.
5. On the **Permissions** tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
6. Click **OK** to save.

## Admin Profile Field Definitions

**General Tab Fields**

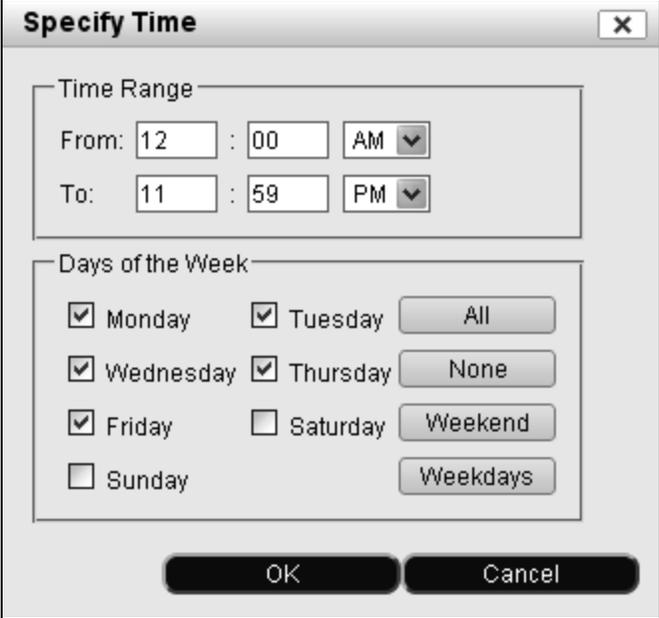
Field	Definition
<b>General Tab</b>	
<b>Name</b>	Enter a name that describes the profile, such as Librarian or IT Staff.
<b>Logout After ... Minutes of Inactivity</b>	User is logged out after this amount of time has elapsed without any activity in the user interface.
<b>Login Availability</b>	<p>Indicates when users with this profile can log in to Network Sentry. Options include: <b>Always</b> or <b>Specify Time</b>. If you choose Specify Time, user access to Network Sentry is limited to certain times of day and days of the week.</p> <p>See Specify Login Availability Time For Admin Profile on the next page.</p>
<b>Manage Hosts And Ports</b>	<p>Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users.</p> <p>Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in Network Sentry. Typically, this type of user would ONLY have the Manage Hosts &amp; Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All.</p> <p><b>All</b>—All groups containing hosts and ports can be accessed.</p> <p><b>Restrict By Groups</b>—Enables the restriction of Administrative Users to specific hosts and ports.</p> <p>For an overview and additional setup information see Limit Admin Access With Groups on page 282.</p>
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry for an existing Admin Profile record.
<b>Enable Guest Kiosk</b>	<p>If you enable this mode, the ONLY thing that the Administrative User can access is the self-service Kiosk. Everything else in Network Sentry is disabled.</p> <p>The Administrative User can log into Network Sentry to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser.</p>
<b>Kiosk Template</b>	Field displays only if Enable Guest Kiosk is selected. Select a Kiosk template for this Admin Profile. All visitors who use the self-service Kiosk when this Administrative User is logged in are assigned this guest template.
<b>Kiosk Welcome Message</b>	Field displays only if Enable Guest Kiosk is selected. Enter the message that will appear when the kiosk user creates a guest account.

**Permissions Tab Fields**

Field	Definition
<b>Permissions Tab</b>	
<b>Landing Page</b>	Indicates the first view displayed when an Admin User with this profile logs into Network Sentry. There are no options displayed in this field until permissions are selected.
<b>NCM Landing Page</b>	Indicates the first view displayed when an Admin User with this profile logs into FortiNac Control Manager. There are no options displayed in this field until permissions are selected.
<b>Permission Set</b>	Click the arrow next to a permission set to see the Views that can be accessed when this permission set is enabled.
<b>Access</b>	Indicates that the user will have view access to the permission set in the left column. Depending on the permission set, enabling Access automatically enables Add/Modify and/or Delete.
<b>Add/Modify</b>	Indicates that the user will be able to add or modify records in the permission set in the left column.
<b>Delete</b>	Indicates that the user will be able to delete records in the permission set in the left column.
<b>Custom</b>	When Custom is enabled for a permission set an addition tab is displayed. For example, if Custom is enabled for Guest Contractor Accounts a Manage Guests tab is displayed allowing you to configure additional controls for guest account creation.  See Add A Guest Manager Admin User Profile on page 645 for information on the Manage Guest tab.  See Add A Device Manager Admin Profile on page 209 for information on the Profile Devices tab.
<b>Check All Uncheck All Buttons</b>	Checks or unchecks all permissions.

**Specify Login Availability Time For Admin Profile**

This option allows you to limit access to Network Sentry for an Administrative User based on the time of day and the day of the week. Any Administrative User associated with this profile can only access Network Sentry as specified in the Login Availability field for the Admin Profile.



The image shows a dialog box titled "Specify Time" with a close button (X) in the top right corner. It is divided into two main sections: "Time Range" and "Days of the Week".

**Time Range:** This section contains two rows of input fields. The first row is labeled "From:" and has three input boxes: "12", "00", and a dropdown menu set to "AM". The second row is labeled "To:" and has three input boxes: "11", "59", and a dropdown menu set to "PM".

**Days of the Week:** This section contains a grid of checkboxes for each day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Monday, Tuesday, Wednesday, and Thursday are checked. To the right of these checkboxes are four buttons: "All", "None", "Weekend", and "Weekdays".

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Figure 100: Specify Time

1. Click **Users > Admin Profiles**.
2. Click select a rule and click **Modify**.
3. In the **Login Availability** field select **Specify Time**.
4. In the **Time Range** section of the Specify Time dialog enter the From and To times for the time of day that Administrative Users should be able to access the network.
5. In the **Days of the Week** section select the days during which these users should be allowed to access the network.
6. Click **OK**.

Custom Manage Guests Tab Fields

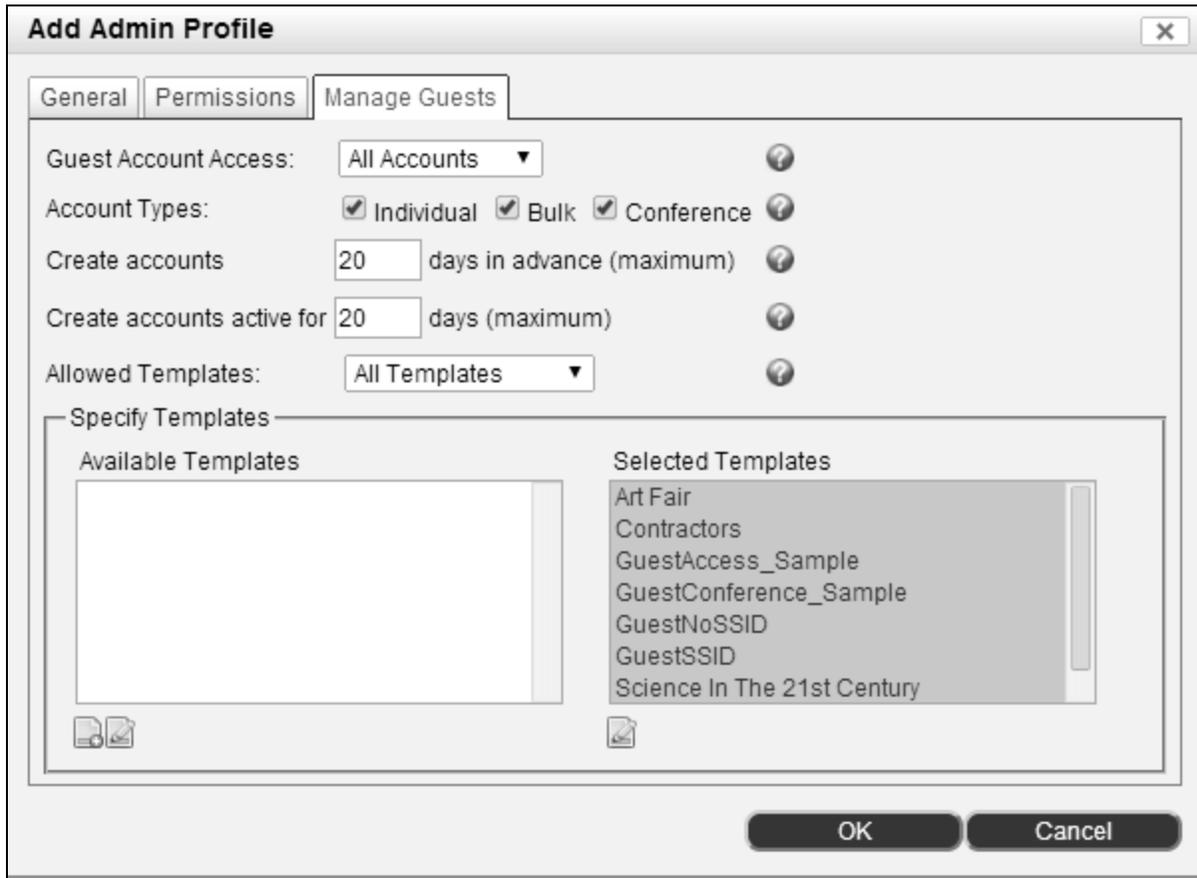


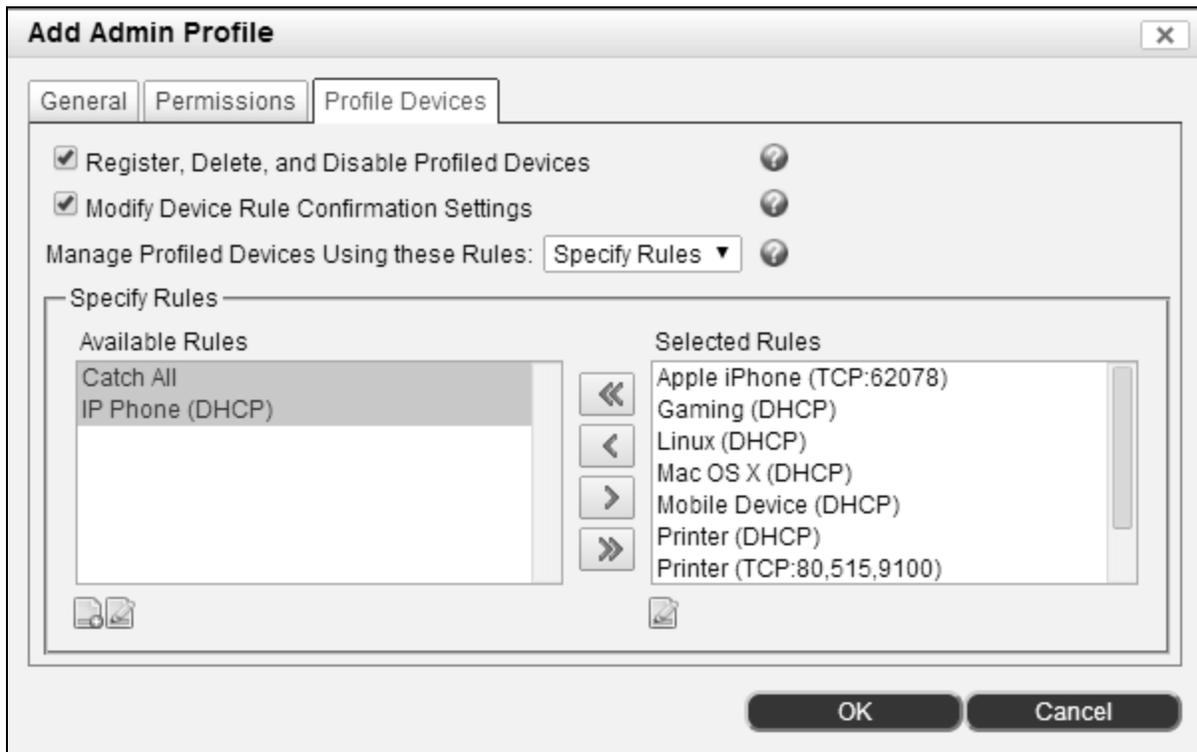
Figure 101: Add Admin Profile - Manage Guests Tab

Field	Definition
<b>Guest Account Access</b>	<p>You can give Administrative Users with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts.</p> <p>The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports.</p> <p><b>No</b>—Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts.</p> <p><b>Own Accounts</b>—Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts.</p> <p><b>All Accounts</b>—User can see all Guest accounts in the database, send credentials to guests and modify or delete any guest accounts.</p>

Field	Definition
<b>Account Types</b>	<p><b>Individual</b>—Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it.</p> <p><b>Bulk</b>—Sponsors may create multiple accounts with unique passwords by importing a bulk account file.</p> <p><b>Conference</b>—Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.</p>
<b>Create Accounts Days in Advance (Maximum)</b>	The maximum number of days in advance this sponsor is allowed to create accounts.
<b>Create Accounts Active For Days (Maximum)</b>	<p>Determines the length of time the guest account remains active in the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>
<b>Allowed Templates</b>	<p>Indicates whether the Administrative User can use all guest templates or only those in the Specify Templates &gt; Selected Templates field. Default = All. Options include:</p> <p><b>All Templates</b>—Profile gives the Administrative User access to all templates in the database when creating guest accounts.</p> <p><b>Specify Templates</b>—Profile gives the Administrative User access to the templates listed in Selected Templates.</p>
<b>Specify Templates</b>	<p>Allows you to select guest/contractor templates available for Administrative Users with this Admin User Profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column.</p> <p>If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.</p>
<b>Available Templates</b>	Shows the templates that have not been selected to be included in this Admin User Profile.
<b>Selected Templates</b>	Shows the templates selected to be included in this Admin User Profile.

Field	Definition
<b>Add Icon</b>	Click this button to create a new Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.
<b>Modify Icon</b>	Click this button to modify the selected Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.

**Custom Profile Devices Tab Fields**



**Figure 102: Add Admin Profile - Profile Devices Tab**

Field	Definition
<b>Register, Delete, and Disable Profiled Devices</b>	If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler.

Field	Definition
<b>Modify Device Rule Confirmation Settings</b>	If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.
<b>Manage Profiled Devices Using These Rules</b>	<b>All Rules</b> —includes current rules and any rules created in the future. <b>Specify Rules</b> —you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
<b>Available Rules</b>	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
<b>Selected Rules</b>	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
<b>Add Icon</b>	Click this button to create a new Device Profiling Rule. For information on rules, see Add Or Modify Device Profiling Rule on page 199.
<b>Modify Icon</b>	Click this button to modify the selected Device Profiling Rule. For information on rules, see Add Or Modify Device Profiling Rule on page 199.

### Custom Security Events Tab Fields

**Note:** The Security Events tab is only available when RTR is enabled within your current license package.

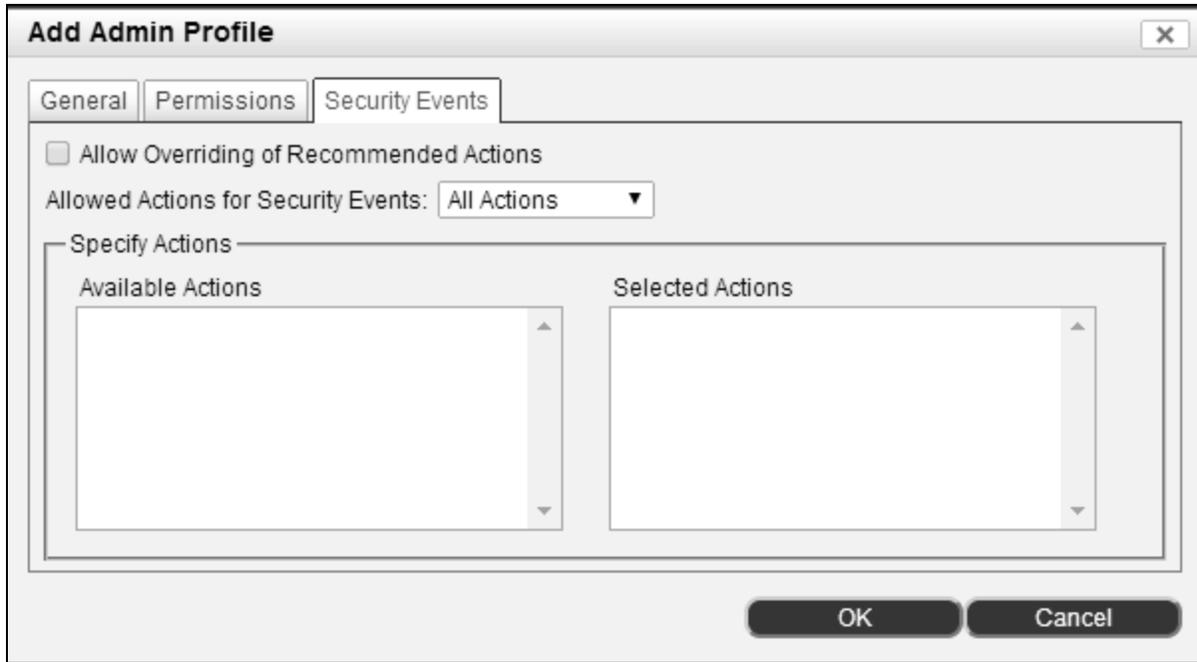


Figure 103: Add Admin Profile - Security EventsTab

Field	Definition
<b>Allow Overriding of Recommended Actions</b>	If enabled, the user can override the associated action when taking action on the alarm.
<b>Allowed Actions for Security Events</b>	<b>All Actions</b> —includes current actions and any actions created in the future. <b>Specify Actions</b> —you must choose the rules from the Available Actions field and manually move them to the Selected field.
<b>Available Actions</b>	Shows the existing actions you can select for this profile. Select the action and click the right arrow to move it to the Selected Actions pane.
<b>Selected Actions</b>	Shows the actions you selected from the Available Actions section. The user can only complete the actions in this list.

## Admin Profile Mappings

Admin Profile Mappings allow you to apply an Admin Profile to an Administrative User when the user is added to an Administrator Group. An Admin Profile Mapping consists of a Administrative Profile that is linked to an Administrator Group.

Admin Profiles can be assigned to Administrative Users based on the users' group membership. Admin Profile Mappings Policies are ranked in priority starting with number 1. When an Administrative User is added to an Administrator Group the group name is compared to the group in each Admin Profile Mapping starting with the first mapping (Rank

1) in the list. If the group does not match in the first mapping, the next one is checked until a match is found.

**Note:** When groups are nested within a parent group, admin profiles must be mapped to the groups that contain the users, and not the parent group only.

**Note:** There may be more than one Administrator Group that is match for this Administrative User, however, the first match found is the one that is used.

**Note:** Admin Profile assignments are not permanent. The Administrative User is reevaluated each time that user is added to or deleted from an Administrator Group.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Admin Profile Mappings - Total: 2				
Rank	Admin Profile	Group	Last Modified By	Last Modified Date
1	Guest Sponsor	Admins Northwest Region	root	02/06/14 02:44 PM EST
2	Device Manager	Admins Southern Region	root	02/06/14 02:45 PM EST

Export to:

Options

Figure 104: Admin Profile Mappings

**Admin Profile Mappings Field Definitions**

Field	Definition
<b>Rank Buttons</b>	Moves the selected mapping up or down in the list. Administrative Users are compared to Admin Profile Mappings in order by rank.
<b>Table Columns</b>	
<b>Rank</b>	Mapping's rank in the list of mappings. Rank controls the order in which Administrative Users are compared to mappings.
<b>Admin Profile</b>	Name of the profile that is assigned when an Administrative User becomes a member of the associated group. See Admin Profiles And Permissions on page 219.
<b>Group</b>	Contains the required group for an Administrative User.
<b>Last Modified By</b>	User name of the last user to modify the mapping.
<b>Last Modified Date</b>	Date and time of the last modification to this mapping.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Copy</b>	Copies the selected mapping.
<b>Delete</b>	Deletes the selected mapping.
<b>Modify</b>	Opens the Modify Mapping window for the selected mapping.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446
	<b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243

**Admin Profile Mappings Process**

Admin Profile Mappings establishes a profile for Administrative Users who are members of a particular Administrator Group. Admin Profile Mappings are ranked so that if an Administrative User is a member of more than one group, Network Sentry can determine which Admin Profile should be applied to the user.

**Example:**

1. Administrative User John is in Group A and Group B.
2. Group A is mapped to a Guest Sponsor Profile and Ranked #5.
3. Group B is mapped to a Device Manager Profile and Ranked #2.
4. Network Sentry associates John with the Device Manager Profile because that mapping is higher in Rank and is the first match for John.

---

**Note:** Adding an Administrative User to a Group that has an Admin Profile mapped can change the Admin Profile applied to that user.

---

Admin Profiles are ONLY applied to members of an Administrator Group when the Administrative User is added to the group or deleted from a higher ranking group. The Administrative User could be added to the group manually or on directory resynchronization. Review the scenarios below for information on the behavior of Admin Profile Mappings.

#### **Administrative User Added To A Group Manually**

- An existing Administrative User is added to Administrator Group A that is mapped to Admin Profile C. The user is not in any other Administrator groups. The Administrative User's profile is updated to Profile C because it is mapped to Group A.
- An existing Administrative User is added manually to Administrator Group A that is mapped to Admin Profile C. The user is also in Administrator Groups B and C, but the new group A is ranked higher in the Admin Profile Mappings list and the new Admin Profile C is assigned.

#### **Administrative User Added To A Group Based On Directory Group Membership**

- Admin Users are created automatically in Network Sentry when users authenticate to the Directory and then access Network Sentry through the Admin UI or by registering a host. The users are then assigned group membership according to their Directory groups.

Possible scenarios that create Admin Users automatically are:

- If a user exists in the directory, for example jdoe, but the user is not a user of any kind in Network Sentry, when jdoe logs into the Network Sentry User Interface using a directory user id and password, a user "jdoe" is created in Network Sentry as an Administrator user.
- If a user exists in the directory, for example asmith, but the user is not a user of any kind in Network Sentry, when asmith registers a host via Network Sentry, a user for asmith, of type "user" is created. Then, when the Directory Synchronization task runs, asmith becomes an administrator user in Network Sentry.
- If a user exists in the directory, for example tjones, but the user is not a user of any kind in Network Sentry, when tjones registers a host via Network Sentry, a user for tjones, of type "user" is created. If, before the Directory Synchronization task runs, the user logs into the Network Sentry Admin UI, the tjones user will transition to be an Administrator user at that time (i.e., not waiting for the Directory Sync.)
- When the Directory Synchronization is run, users are added to Network Sentry Administrator Groups that match the groups in the Directory. Adding Admin Users to a group triggers an evaluation of Admin Profile Mappings. If the Admin

User is in multiple Directory groups, the user will be assigned to multiple groups in Network Sentry, and the Admin Profile will be assigned according to the Admin Profile ranking.

**Important:** When an Admin Group is created in Network Sentry with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

### **Modify Ranks Of Admin Profile Mappings**

- The order of the Admin Profile Mapping records is changed modifying the ranking. A scheduled directory synchronization runs. Administrative Users' groups are updated each time the synchronization is run causing the Admin Profile Mappings to be analyzed again. Since the ranking has changed, some Administrative Users that are members of more than one group are assigned different Admin Profiles based on the new ranking.
- The order of the Admin Profile Mapping records is changed modifying the ranking. No directory is being used. Administrative Users continue to have the same Admin User Profiles because there is no mechanism to trigger a re-evaluation of group membership.

### **Administrative User Deleted From A Group Manually**

- An existing Administrative User is deleted from Administrator Group A that is mapped to Admin Profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the Admin Profile Mapping with the highest rank.

Administrator Group B is mapped to Admin Profile D. Administrator Group C is mapped to Admin Profile F. The mapping for Group B has the highest rank, therefore the Administrative User's profile is updated to Admin Profile D.

- An existing Administrative User is deleted from Group A that is mapped to an Admin Profile C. The user is not a member of any other group mapped to a profile. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under Users > Users View. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

### **Administrative User Deleted From A Group In The Directory**

- An existing Administrative User is deleted from Administrator Group A in the Directory. The directory resynchronizes with Network Sentry which deletes the Administrative user from Group A that is mapped to Admin Profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the Admin Profile Mapping with the highest rank.

Administrator Group B is mapped to Admin Profile D. Administrator Group C is mapped to Admin Profile F. The mapping for Group B has the highest rank, therefore the Administrative User's profile is updated to Admin Profile D.

- An existing Administrative User is deleted from Administrator Group A in the Directory. The directory resynchronizes with Network Sentry which deletes the Administrative user from Group A that is mapped to Admin Profile C. The user is not a member of any other group mapped to a profile. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under Users > Users View. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

#### **Administrator Group Is Deleted From Network Sentry**

- An existing Administrative User is in Group A that is mapped to Admin Profile C. The user is not a member of any other group mapped to a profile. Group A is deleted from the Groups View. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under Users > Users View. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

#### **Admin Profile Mapping Is Deleted From Network Sentry**

- Administrative Users are not affected when an Admin Profile Mapping is deleted from the data base until a user is added to or deleted from a Group. If the group is no longer mapped their profile is not updated. If the group continues to be mapped, their profile is updated as described in the previous scenarios.

---

**Note:** When groups are nested within a parent group, admin profiles must be mapped to the groups that contain the users, and not the parent group only.

---

---

**Note:** Changing the Ranking on existing Admin Profile Mapping records does not change profiles on Administrative Users unless those users are in the directory and the directory is resynchronized.

---

---

**Note:** Adding a new Admin Profile Mapping does not affect existing Administrative Users until the directory is resynchronized or a user's membership in a mapped group changes.

---

---

**Note:** If you are not using a directory there is no mechanism for Administrative Users to be re-evaluated.

---

### Add/Modify An Admin Profile Mapping

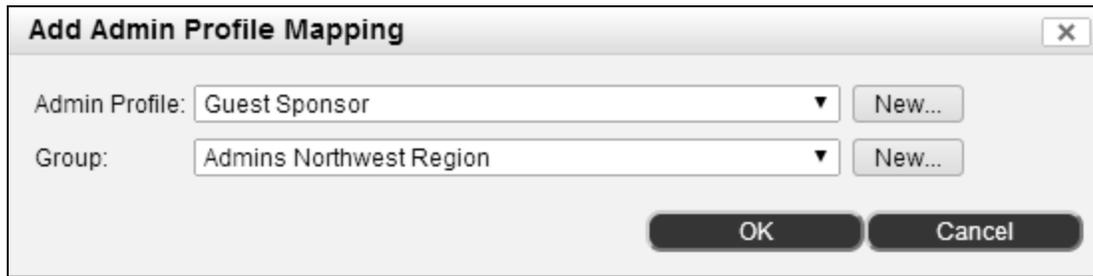


Figure 105: Add Admin Profile Mapping

1. Click **Users > Admin Profiles**.
2. Select Admin Profile Mappings from the menu on the left.
3. Select an existing mapping and click **Modify** or click **Add**.
4. In the **Admin Profile** drop-down select a profile. If the profile you need is not in the list, use the New button to create it. See **Add An Admin Profile** on page 243 for instructions.
5. In the Group drop-down select an Administrator Group. If the Group you need is not in the list, use the New button to create it. See **Add Groups** on page 684 for instructions.
6. Click **OK** to save.

### Delete An Admin Profile Map

Deleting an Admin Profile Map does not affect profiles assigned to Administrative Users. They continue to have the same Admin Profile until something triggers a re-evaluation such as a directory synchronization.

1. Click **Users > Admin Profiles**.
2. Select **Admin Profile Mappings** from the menu on the left.
3. Select an existing mapping and click **Delete**.
4. Confirm that you want to delete the mapping.

### Administrative User Profiles For Guest Manager

In Network Sentry, you can create an administrative user and give that user an Admin Profile that contains special permissions for the Guest/Contractor feature set. These privileges are designed to restrict this user to certain parts of the program. See **Admin Profiles And Permissions** on page 219.

For Guest Manager, this type of user is referred to as a Sponsor in documentation because that person sponsors incoming guests and contractors. Creating a Sponsor Admin Profile allows the user to manage guest, contractor, conference or Self-Registered Guest accounts. For more information on the types of accounts, see **Guest Account Types Or Visitor Types** on page 631.

Guest Manager supports multiple UPN formats (for example, @gcs.xyztech.com) so sponsors do not have to type their full user login name. As administrative users create guest or contractor accounts, their administrative login name within Guest Manager is added as a part of the guest or contractor record for reporting purposes.

Additional permissions can be given to Sponsors based on the parameters of their responsibilities. Create one or more Admin Profiles for these types of users. Sponsor Admin User Profiles determine whether the sponsor can manage Guest accounts, Kiosk Accounts or Self-Registered Guest accounts. See the following for additional information:

**Add A Guest Manager Admin User Profile** on page 645

**Add A Kiosk Admin Profile** on page 648

**Add A Guest Self Registration Admin Profile** on page 651

## Add A Guest Manager Admin User Profile

This procedure describes how to create a specific Admin User Profile for an administrative user with permissions for Guest Manager. As a sponsor, the administrative user can create guest or contractor accounts. For details on all of the options that can be include in an Admin User Profile see **Add An Admin Profile** on page 243.

If an Admin User Profile has Kiosk Mode enabled, the corresponding user can only log into the Kiosk computer to make it available to arriving guests. That user cannot create accounts. You may need to create a sponsor who can manage accounts and a second sponsor to use for the self-service Kiosk. See **Add A Kiosk Admin Profile** on page 648



**Figure 106: Add Admin Profile - Manage Guests Tab**

To create an Admin User Profile you must first be logged into your Administrator account. Follow the steps below to add an Admin User Profile for an Administrative User that is considered a Sponsor for incoming guests:

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Guest Sponsor.

4. Under **Manage Hosts and Ports** select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
7. The minimum that this sponsor must have is the **Guest/Contractor Accounts** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Guest/Contractor permission set, the Landing Page field defaults to Guest Contractor Accounts.
9. In addition you may want include Self Registration Requests, which allow a Sponsor to Allow or Deny guest access to a user who has registered through the captive portal. This is not required.
10. The Manage Guests tab is enabled when Custom is selected for the Guest/Contractor Accounts permission set. Click on the **Manage Guests** tab.
11. Use the field definitions below to configure the Guest Manager specific fields.
12. Click **OK** to save.

**Custom Manage Guests Tab Fields**

Field	Definition
<p><b>Guest Account Access</b></p>	<p>You can give Administrative Users with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts.</p> <p>The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports.</p> <p><b>No</b>—Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts.</p> <p><b>Own Accounts</b>—Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts.</p> <p><b>All Accounts</b>—User can see all Guest accounts in the database, send credentials to guests and modify or delete any guest accounts.</p>
<p><b>Account Types</b></p>	<p><b>Individual</b>—Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it.</p> <p><b>Bulk</b>—Sponsors may create multiple accounts with unique passwords by importing a bulk account file.</p> <p><b>Conference</b>—Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.</p>
<p><b>Create Accounts Days in Advance (Maximum)</b></p>	<p>The maximum number of days in advance this sponsor is allowed to create accounts.</p>
<p><b>Create Accounts Active For Days (Maximum)</b></p>	<p>Determines the length of time the guest account remains active in the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

Field	Definition
<b>Allowed Templates</b>	Indicates whether the Administrative User can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include:  <b>All Templates</b> —Profile gives the Administrative User access to all templates in the database when creating guest accounts.  <b>Specify Templates</b> —Profile gives the Administrative User access to the templates listed in Selected Templates.
<b>Specify Templates</b>	Allows you to select guest/contractor templates available for Administrative Users with this Admin User Profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column.  If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
<b>Available Templates</b>	Shows the templates that have not been selected to be included in this Admin User Profile.
<b>Selected Templates</b>	Shows the templates selected to be included in this Admin User Profile.
<b>Add Icon</b>	Click this button to create a new Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.
<b>Modify Icon</b>	Click this button to modify the selected Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.

### Add A Kiosk Admin Profile

A kiosk allows visitors to your facility to create their own account. Guests have a maximum of 24 hours of access to your network, which may be only during certain hours of the day, or a pre-defined number of hours from when they log on. Guests may simply be queried for pre-defined contact data. In any case, at 11:59 PM each day, or after the allowed number of hours has elapsed, kiosk guest accounts expire.

**Note:** All other profile options are disabled if Kiosk Mode is enabled, because guests creating their own accounts would not need access to other options.

For added security, sponsors should use a kiosk browser. Kiosk browsers block users from accessing other programs on the machine or other web sites.

This procedure describes how to create a profile that gives a sponsor permission to manage a kiosk. A sponsor with Kiosk Mode enabled cannot access any of the regular Network Sentry windows. That user can log in to display the Guest Login web page and make it available on the Kiosk PC.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Kiosk Sponsor.
4. Use the table of field definitions below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Click on **Enable Guest Kiosk** to mark it with a check mark.
7. In the **Kiosk Template** field select a Guest/Contractor Account template. All guest accounts created through the Kiosk will use this template.
8. In the **Kiosk Welcome Text** field type the message that a guest will see when they create a guest account through the Kiosk.
9. Click **OK** to save.

The screenshot shows a dialog box titled "Add Admin Profile" with a close button (X) in the top right corner. The "General" tab is selected. The form contains the following fields and controls:

- Name:** Text input field containing "Kiosk Sponsor".
- Logout After:** Text input field containing "60" followed by "minutes of inactivity".
- Login Availability:** Dropdown menu set to "Always".
- Manage Hosts and Ports:** Dropdown menu set to "All".
- Note:** Large empty text area.
- Enable Guest Kiosk**
- Kiosk Template:** Dropdown menu set to "Art Fair".
- Kiosk Welcome Text:** Text area containing "Welcome to the Art Fair! Click Start to create your guest account.".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 107: Add Kiosk Profile

### Admin Profile Fields For Kiosk Sponsors

Field	Definition
<b>Name</b>	Enter a name that describes the profile, such as Kiosk Sponsor.
<b>Logout After</b>	User is logged out after this amount of time has elapsed without any activity in the user interface.
<b>Login Availability</b>	Specify when this sponsor can log into the network: <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify time</li> </ul> <p>The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.</p>
<b>Manage Hosts And Ports</b>	Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users. <p>Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in Network Sentry. Typically, this type of user would ONLY have the Manage Hosts &amp; Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All.</p> <p><b>All</b>—All groups containing hosts and ports can be accessed.</p> <p><b>Restrict By Groups</b>—Enables the restriction of Administrative Users to specific hosts and ports.</p> <p>For an overview and additional setup information see Limit Admin Access With Groups on page 282.</p>
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry for an existing Admin Profile record.
<b>Enable Guest Kiosk</b>	If you enable this mode, sponsors can log into Network Sentry to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. <p>Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.</p>
<b>Kiosk Template</b>	Select a Kiosk template for this sponsor. All visitors who use the self-service Kiosk when this sponsor is logged in will be assigned this template.
<b>Kiosk Welcome Message</b>	Enter the message that will appear when the kiosk user creates a guest account.

### Add A Guest Self Registration Admin Profile

Guest Self-Registration allows visitors to request a temporary or guest account from their own device. A sponsor receives an email indicating that a request has been received from a guest. The sponsor responds to the request by approving or denying it. Sponsors with the Guest Self Registration Admin Profile or with a Guest Manager Admin Profile and Administrators can respond to a Self-Registration request from a guest.

Anyone in your organization can be a sponsor for Guest Self-Registration. They must be entered into Network Sentry as an Administrative User and that user account must have a Guest Self-Registration Admin Profile applied. You can quickly create Sponsors by using Directory Groups.

Guests can access your network for the length of time specified by the Account Duration. Availability can be 24 hours a day or limited to specific hours during the day.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Self-Registered Guest Sponsor.
4. Use the table of field definitions below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Leave the defaults for the remaining fields and click on the **Permissions** tab.
7. On the Permissions tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
8. The minimum that this sponsor must have is the **Self Registration Requests** permission set. Select all of the check boxes for this set.
9. When you select the Self Registration Requests permission set, the **Landing Page** field defaults to Self Registration Requests.
10. Click **OK**.

#### Admin Profile Fields For Self Registered Guest Sponsors

Field	Definition
<b>Name</b>	Enter a name that describes the profile, such as Kiosk Sponsor.
<b>Logout After</b>	User is logged out after this amount of time has elapsed without any activity in the user interface.

Field	Definition
<p><b>Login Availability</b></p>	<p>Specify when this sponsor can log into the network:</p> <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify time</li> </ul> <p>The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.</p>
<p><b>Manage Hosts And Ports</b></p>	<p>Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users.</p> <p>Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in Network Sentry. Typically, this type of user would ONLY have the Manage Hosts &amp; Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All.</p> <p><b>All</b>—All groups containing hosts and ports can be accessed.</p> <p><b>Restrict By Groups</b>—Enables the restriction of Administrative Users to specific hosts and ports.</p> <p>For an overview and additional setup information see Limit Admin Access With Groups on page 282.</p>
<p><b>Note</b></p>	<p>User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry for an existing Admin Profile record.</p>
<p><b>Enable Guest Kiosk</b></p>	<p>Do not enable this field for the Self Registered Guest Admin User Profile.</p> <p>If you enable this mode, sponsors can log into Network Sentry to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser.</p> <p>Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.</p>

## Printer Settings For Guest Contractor Badges

In Guest Manager, administrative users you designate as sponsors can access guests' account credentials that show the user name, password, and access start time and end time. Sponsors may print the account details, e-mail them or send them via an SMS message directly to guests after account creation.

If sponsors managing guest kiosks or conferences need to print badges, contact your IT Manager to assure that printer settings are optimized for badge creation:

- Make sure the label printer is the default printer for kiosks.
- In the Printer Properties, Paper Options settings, set the paper label size to a minimum of 2" x 2-3/4" (5.1 cm x 7 cm).
- In the Page Handling Settings, make sure that Auto-Rotate is enabled to automatically adjust the orientation to fit the label's orientation on the sheet.
- Test to make sure that text is centered and fits on each label.





## Chapter 6: Admin Users

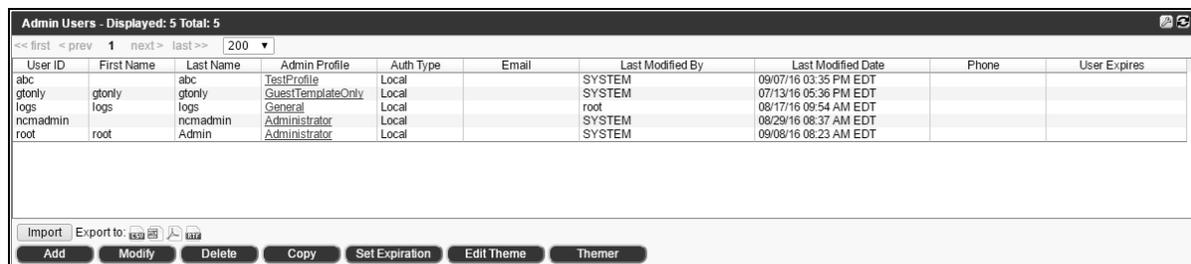
The Admin Users View displays a list of existing system users. Use this window to add, modify or delete Network Sentry users. Admin users are also network users, therefore, Network Sentry also displays them in the Users View. If you are logged in as an Admin user, you cannot delete the Admin user account that you are using.

**Note:** Administrator Users cannot select a different Admin Profile for their own account. Use a second Administrator account to access the Administrator User and select a different Admin Profile.

If there are more than 1000 Admin Users in the database, the users are not automatically displayed. Instead, a confirmation dialog is shown asking if you would like to continue. Note that large numbers of records may load very slowly if not filtered. Choose Yes to display all Admin Users or No to reduce the number displayed by using the filters.

Admin Users can be accessed from **Users > Admin Users**.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.



The screenshot shows a web interface titled "Admin Users - Displayed: 5 Total: 5". It features a table with the following columns: User ID, First Name, Last Name, Admin Profile, Auth Type, Email, Last Modified By, Last Modified Date, Phone, and User Expires. The table contains five rows of user data. Below the table, there are buttons for "Import", "Export to:" (with icons for CSV, PDF, and XLS), and a row of action buttons: "Add", "Modify", "Delete", "Copy", "Set Expiration", "Edit Theme", and "Themer".

User ID	First Name	Last Name	Admin Profile	Auth Type	Email	Last Modified By	Last Modified Date	Phone	User Expires
abc	abc	abc	TestProfile	Local		SYSTEM	09/07/16 03:35 PM EDT		
gtonly	gtonly	gtonly	GuestTemplateOnly	Local		SYSTEM	07/13/16 05:36 PM EDT		
logs	logs	logs	General	Local		root	08/17/16 09:54 AM EDT		
ncmadmin	ncmadmin	ncmadmin	Administrator	Local		SYSTEM	08/29/16 08:37 AM EDT		
root	root	Admin	Administrator	Local		SYSTEM	09/08/16 08:23 AM EDT		

Figure 108: Admin Users View

### Admin Users View Field Definitions

Fields used in filters are also defined in this table.

Field	Definition
<b>Add Filter drop-down list</b>	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See <b>Filters</b> on page 59.
<b>Update button</b>	Displays the filtered data in the table.

Field	Definition
<b>Admin Users</b>	
<b>User ID</b>	Unique alphanumeric ID for this user. Required.
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name. Required.
<b>Type</b>	Indicates the type of Admin user being created. Types include Administrator and Administrative.
<b>Admin Profile</b>	Admin Users must have an associated Admin Profile that provides them with permissions for features in Network Sentry. Click the link in the Admin Users table for the selected user to go to the profile displayed. See <b>Administrative User Profiles For Guest Manager</b> on page 644.
<b>Auth Type</b>	Authentication method used for this Admin user. Types include: <ul style="list-style-type: none"> <li>• <b>Local</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server.</li> </ul>
<b>E-mail</b>	E-mail address used to send system notifications associated with features such as alarms or profiled devices.
<b>Phone</b>	Optional demographic information.
<b>Address</b>	
<b>City</b>	
<b>State</b>	
<b>Postal Code</b>	
<b>Title</b>	
<b>Mobile Number</b>	
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
<b>User Expires</b>	<p>The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. The default setting for Administrator users is blank or Never Expire. Administrative Users may or may not have an expiration date depending on how the account was created. See <b>Aging Out Host Or User Records</b> on page 381. To configure aging see, Set User Expiration Date on page 425.</p> <p><b>Note:</b> Admin Users assigned the Administrator Profile cannot be aged out.</p>

Field	Definition
<b>User Inactivity Date</b>	Controls the number of days a User is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See <b>Aging Out Host Or User Records</b> on page 381.
<b>User Inactivity Limit</b>	Number of days the user must remain continuously inactive on the network to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Last Login/Logout</b>	Date of the last time the user logged into or out of the network or the Network Sentry Admin UI. This date is used to count the number of days of inactivity.
<b>Last Modified By</b>	User name of the last user to modify the admin user.
<b>Last Modified Date</b>	Date and time of the last modification to this admin user.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Copy</b>	Copy the selected User to create a new record.
<b>Delete</b>	Deletes the selected User.
<b>Group Membership</b>	Displays groups in which the selected user is a member.  Note:Admin Users are also regular Users, therefore, separate options are displayed for Admin User Groups and User Groups. Options are labeled Group Membership (User) and Group Membership (Administrator).
<b>Groups</b>	Displays groups in which the selected user is a member. See <b>Admin User Group Membership</b> on page 287.
<b>Modify</b>	Opens the Modify User window for the selected profile.
<b>Set Admin Profile</b>	Allows you to modify the Admin Profile for one or more users. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user. See <b>Modify a User's Admin Profile</b> on page 279
<b>Set Expiration</b>	Launches a tool to set the date and time for the user to age out of the database. See <b>Set User Expiration Date</b> on page 425.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item.  For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446  <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Edit Theme</b>	Opens the User Theme dialog and allows you to modify the look and feel of the user interface for each Admin User..
<b>Import/Export</b>	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats.

## Add Administrative Users

Administrator users other than the root user can be created on the FortiNac Control Manager. **It is recommended that at least one Administrator user be added and used in lieu of using the root user account.** Make sure these accounts also exist on the FortiNac Server or FortiNac Control Server appliances so the Administrator users can have access to the data.

FortiNac Control Manager Administrators can be authenticated via LDAP, by selecting LDAP in the authentication field when the user account is configured. When an Administrator user logs in, the FortiNac Control Manager checks the Directory configured for each managed server in turn until it locates the user record. If the authentication is successful, the FortiNac Control Manager updates the user fields, such as address and telephone number, and allows the user to access the Admin user interface.

User ID	First Name	Last Name	Admin Profile	Auth Type	Email	Phone	User Expires	User Inactivity Date	User Inactivity Limit
Laura	Sample	User6	Administrator	Local	sampleuser@bradford		Never		None
gail.sponsor	Sample	User1	Sponsor_Profile	Local			Never		None
laura.sponsor	Sample	User2	Administrator	Local			08/23/14 11:55 AM EDT		1 Days
root	root	Admin	Administrator	Local			Never		None
test.user1	Joe	Smith	Administrator	Local			Never		None
test.user2	Sample	User4	Help Desk	Local			Never		None
test.user3	Sample	User5	Administrator	Local			Never		None

**Figure 109: User List**

To add an Administrative user account:

1. Create the Administrator, Operator, or Help Desk user on the FortiNac Server or FortiNac Control Server that the user has access to for searches.

**Note:** For Local Authentication make the password for the user the same on the FortiNac Server, FortiNac Control Server, or FortiNac Control Manager.

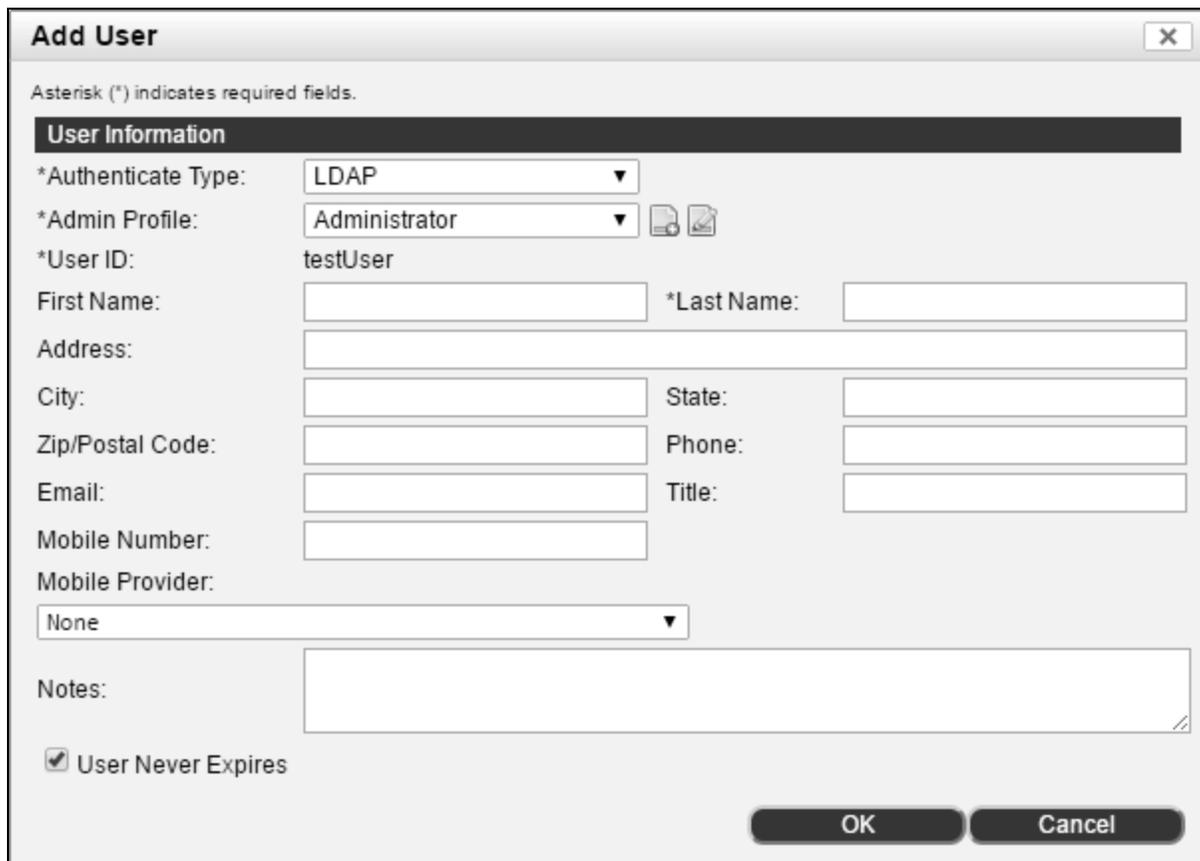
2. Log in to the FortiNac Control Manager.
3. Select **Users > Admin Users**.
4. Click **Add**.
5. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.



The dialog box titled "Enter User ID" has a close button (X) in the top right corner. It contains a text input field labeled "User ID:" with the text "SampleUser1" entered. Below the input field are two buttons: "OK" and "Cancel".

**Figure 110: Enter the User ID**

This allows you to give a network user administrator privileges to help with some administrative tasks.



The dialog box titled "Add User" has a close button (X) in the top right corner. Below the title bar, it says "Asterisk (\*) indicates required fields." The dialog is divided into sections. The "User Information" section is highlighted with a dark header. It contains the following fields:

- \*Authenticate Type: LDAP (dropdown menu)
- \*Admin Profile: Administrator (dropdown menu) with document and image icons to the right
- \*User ID: testUser
- First Name: [text input]
- \*Last Name: [text input]
- Address: [text input]
- City: [text input]
- State: [text input]
- Zip/Postal Code: [text input]
- Phone: [text input]
- Email: [text input]
- Title: [text input]
- Mobile Number: [text input]
- Mobile Provider: None (dropdown menu)
- Notes: [text area]
- User Never Expires

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

**Figure 111: Add User**

6. Use the table of field definitions below to complete the information in the Add User dialog.
7. Click **OK** to save the new user.

**Admin User Field Definitions**

Field	Definition
<b>Authentication Type</b>	<p>Authentication method used for this Admin user. Types include:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization’s directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server. If an integrated RADIUS server has been added under RADIUS Settings and the Authentication Type field is set to RADIUS, a RADIUS User record is automatically added to the RADIUS User's view for this user.</li> </ul> <p><b>Note:</b> Authentication of Admin Users via RADIUS is not currently available, however, Admin Users can still be created with the RADIUS authentication type for use on NetworkSentry pods.</p>
<b>Admin Profile</b>	<p>Profiles control permissions for administrative users. See Admin Profiles And Permissions on page 219.</p> <p><b>Add</b> — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window.</p> <p><b>Modify</b> — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.</p>
<b>User ID</b>	Unique alphanumeric ID for this user.
<b>Password</b>	<p>Password used for local authentication.</p> <p><b>Note:</b> If you authenticate users through LDAP, the password field is disabled and the user must log in with their LDAP password.</p>
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>Address</b>	Optional demographic information.
<b>City</b>	
<b>State</b>	
<b>Zip/Postal Code</b>	
<b>Phone</b>	
<b>E-mail</b>	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>Title</b>	User's title, such as Mr. or Ms.

Field	Definition
<b>Mobile Number</b>	Mobile Phone number used for sending SMS messages to administrators.
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
<b>Notes</b>	Free form notes field for additional information.
<b>User Never Expires</b>	<p>If enabled, Admin users are never aged out of the database. The default is enabled.</p> <p><b>Note:</b> Admin Users assigned the Administrator Profile cannot be aged out.</p>

### Modify an Admin User

**Note:** Administrator Users cannot select a different Admin Profile for their own account. Use a second Administrator account to access the Administrator User and select a different Admin Profile.

1. Select **Users > Admin Users**.
2. Select a user from the list.
3. Click the **Modify** button.
4. On the Modify User window, edit your data as needed.
5. Click the **Change Password** button to modify this user's password. This button is only available if the user is set for Local authentication. Users who authenticate through the directory or a RADIUS server must change their passwords in the directory or RADIUS server directly.
6. Click **OK** to save your changes.

For information on individual fields, see **Admin User Field Definitions** on page 276.

### Delete An Admin User

1. Select **Users > Admin Users**.
2. Select a user from the list.
3. Click the **Delete** button.
4. A message is displayed asking if you are sure. Click **OK** to continue.

You are asked if you would like to delete registered hosts. If the Admin User is also the owner of any registered hosts, it is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

### Copy An Admin User

You may copy a user, save it under another name, and use it as the basis for a new user.

1. Log into your Administrator account.
2. Click **Users > Admin Users**.
3. The **Admin Users** window opens with a list of current users.
4. Select the user and click, **Copy**.
5. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

This allows you to give administrator privileges to a network user to help with some administrative tasks.

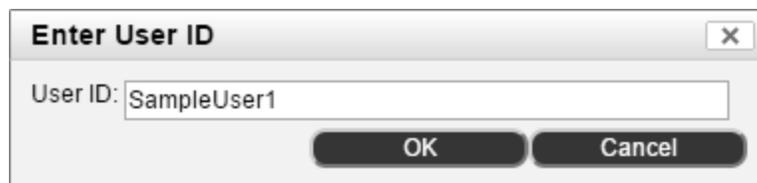
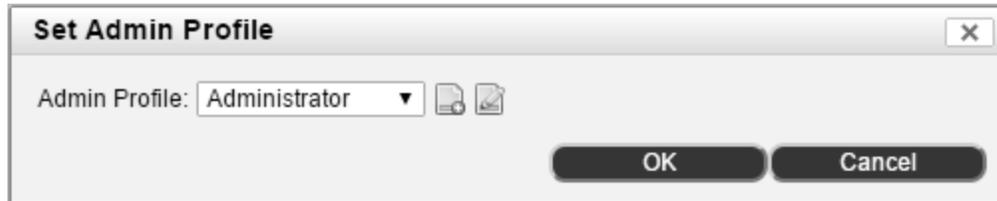


Figure 112: Enter User ID

6. Change the name of the user, or other information and parameters.
7. Click **OK**.

## Modify a User's Admin Profile

You can modify the Admin Profile for one or multiple users at a time. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user.



**Figure 113: Set Admin Profile**

1. Select **Users > Admin Users**.
2. Select one or more users from the list.
3. Right-click and select **Set Admin Profile**.
4. Select the Admin Profile from the drop-down list.

**Note:** Click the Add button to add a new profile, or the Edit button to modify the selected profile.

5. Click **OK**.

### User Theme

Themes control the look and feel of the Network Sentry user interface for each individual user.

#### **Set User Theme**

1. Select **Users > Admin Users**.
2. The **Admin Users** window opens with a list of users.
3. Select the user to be modified.
4. Select **Edit Theme**.
5. Use the field definitions table below to enter settings.
6. Select the **Switch User(s) to Custom Theme Automatically** check box to automatically apply the custom theme to the selected user(s).

**Note:** Selecting the **Switch User(s) to Custom Theme Automatically** check box allows an Administrator to apply the custom theme to the selected user(s) without the need for the user to log in and change the theme manually.

7. Click **Apply To** to enable this theme for more users.
8. Click **OK** to set the theme.

|

**Figure 114: User Theme**

#### **Enable User Theme**

After a theme is set for a specific user, that user must log into Network Sentry and enable the new theme as follows:

1. Navigate to **Help > Preferences** to display the Admin User Preferences dialog.
2. From the **Theme** drop-down select **Custom**.
3. Click **OK**.

## Edit User Theme - Field Definitions

Field	Definition
<b>Header</b>	
<b>Header</b>	Controls the colors and text in the banner at the top of the window.
<b>Product Title</b>	Removes the logo displayed in the banner and adds the text included in the Product Title field.
<b>Text Color</b>	Controls the color of any text displayed in the banner at the top of the window.
<b>Primary Color</b>	Controls the background color of the banner. Depending on the Blend Direction setting this is the first color starting from the top down or from left to right.
<b>Secondary Color</b>	Controls the background color of the banner. Depending on the Blend Direction setting this is the second color starting from the top down or from left to right.
<b>Blend Direction</b>	Controls how the Primary and Secondary colors are blended in the banner. Vertical blends from top to bottom with the Primary at the top. Horizontal blends from left to right with the Primary on the left.
<b>Navigation</b>	
<b>Navigation</b>	Controls the text and background colors of the menu bar.
<b>Navigation Style</b>	Controls the navigation method of the menu bar. Navigation bar is a plain menu bar in which the menu options are links and the menu with focus is underlined. Gradient with Tabs is a menu bar where the selected background color becomes lighter from top to bottom, and the menu with focus looks like a tab with a different background color. In this case, the color of the tab is controlled by the Detail Color option.
<b>Text Color</b>	Controls the color of the text on the menu bar.
<b>Background Color</b>	Controls the background color of the menu bar.
<b>Detail Color</b>	Controls the background color of a selected menu item when Navigation Style is set to Gradient With Tabs.
<b>Selection Color</b>	Color of the underline that indicates that a menu has focus when Navigation Style is set to Navigation Bar.
<b>Panels</b>	
<b>Panels</b>	Controls the colors and text in the title bars of panels such as tables of data.
<b>Text Color</b>	Controls the color of the text in the title bars of panels and dialog boxes.
<b>Header Background</b>	Controls the background color of the title bars of panels and dialog boxes.
<b>Buttons</b>	
<b>Buttons</b>	Controls the text and background colors of buttons.
<b>Primary Color</b>	Controls the background color of primary buttons throughout the system.
<b>Primary Text Color</b>	Controls the color of the text in primary buttons throughout the system.

Field	Definition
<b>Secondary Color</b>	Controls the background color of secondary buttons throughout the system.
<b>Secondary Text Color</b>	Controls the color of the text in secondary buttons throughout the system.
<b>Side Bar</b>	
<b>Side Bar</b>	Controls the colors and text in side menus displayed on the left.
<b>Text Color</b>	Controls the color of the text in the side menus displayed on the left.
<b>Background Color</b>	Controls the background color of the side menus displayed on the left.
<b>Hover Text Color</b>	Controls the color of the text when the mouse hovers over a menu item in the side menus displayed on the left.
<b>Hover Background Color</b>	Controls the background color of a menu option when the mouse hovers over it in the side menus displayed on the left.
<b>Dialog Buttons</b>	
<b>Preview</b>	Displays selected theme settings in the User Interface.
<b>Remove Customizations</b>	Returns the settings to the factory defaults for the selected user.
<b>Switch User(s) to Custom Theme Automatically</b>	Applies the theme to selected user(s) automatically without the need for the user(s) to manually change it.
<b>Apply To</b>	Allows you to select a list of users to whom this theme should apply.

### Limit Admin Access With Groups

To control which hosts and ports Admin users can access you can place those Admin users in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

**Example:**

Assume you have two Administrative Users that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two Administrative Users in a special Administrator Group.
- Assign these two Administrative User to a profile with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the General Tab of the profile is set to **Restrict by Groups**.

- Set the Administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two Administrative Users from the All Management Group or they will have access to all hosts and ports.

When those Administrative Users log into the Admin user interface, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.

---

**Note:** Make sure to remove affected Administrative Users from the All Management group or they will continue to have access to all hosts and ports.

---

---

**Note:** Administrative Users can still view all hosts and users from the Locate View if their Admin Profile gives them permission for that view, but they can only modify those that are in the group they are managing.

---

1. Create the group of hosts or ports. See **Add Groups** on page 684 for instructions.
2. Create an Admin Profile for with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the General Tab of the profile is set to **Restrict by Groups**. See **Add Administrative Users** on page 274
3. Create an Administrator group that contains the Administrative Users responsible for the devices or ports.
4. Remove the Administrative Users from the All Management group. See **Modify A Group** on page 695 for instructions.
5. Right-click on the Administrator group of Administrative Users and select **Manages**.
6. On the Manages window select the group(s) to be managed by marking them with a check mark.
7. Click **OK**.

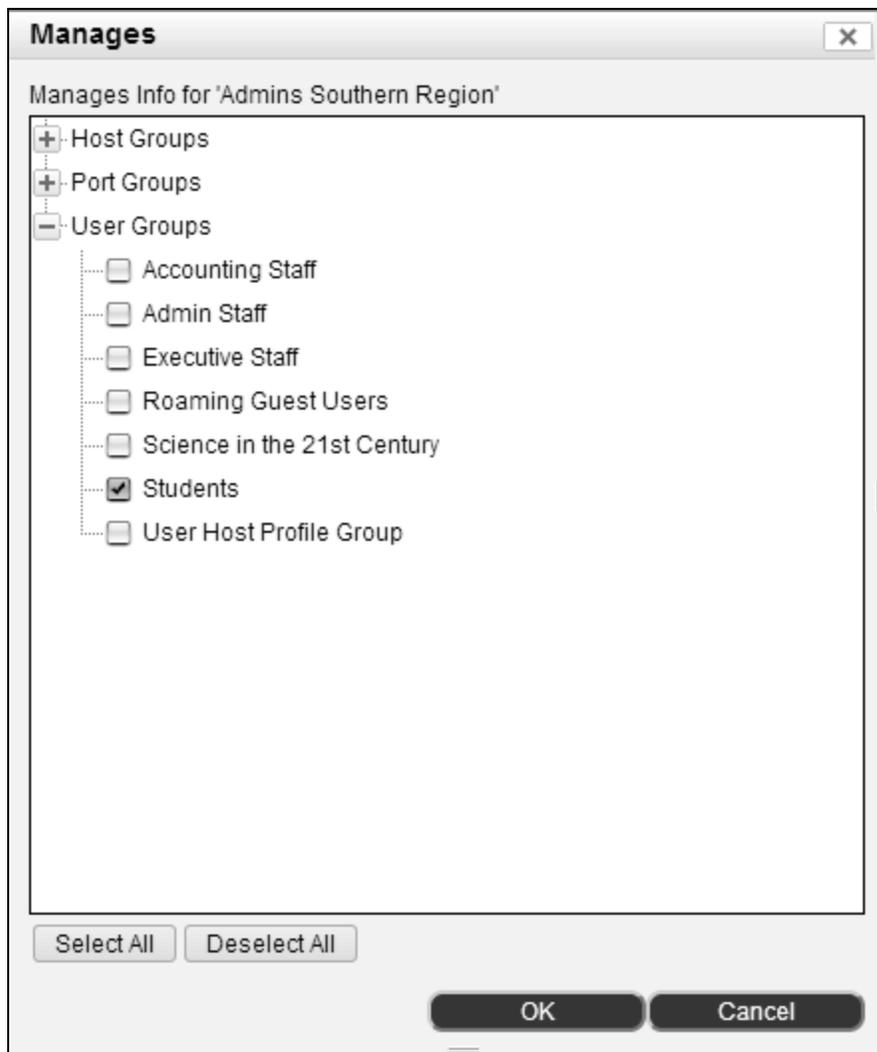
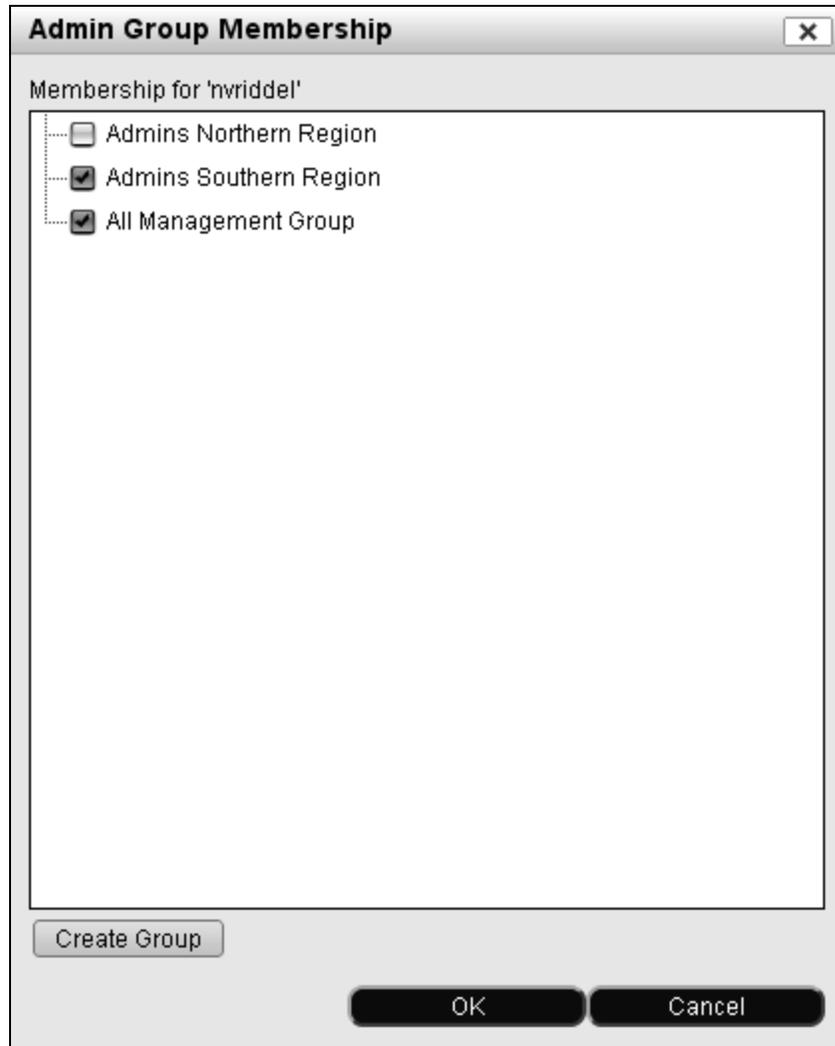


Figure 115: Group Management Dialog

## Add Admin Users To Groups

You can add selected Admin Users to groups you have created. See **Groups View** on page 681 for detailed information on Groups and how they are used in Network Sentry.



**Figure 116: Add Users To Group**

1. Select **Users > Admin User View**.
2. Use the Filters to locate the appropriate Admin User(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the Options button and select **Add Admin Users To Groups**.
5. The Group Membership view lists the available Admin User groups and sub-groups. Sub-groups are displayed under their parent group or groups.

6. **To add the users to a group**, click the box next to the group name and then click **OK**.
7. **To create a missing group**, click the **Create Group** button.

Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.

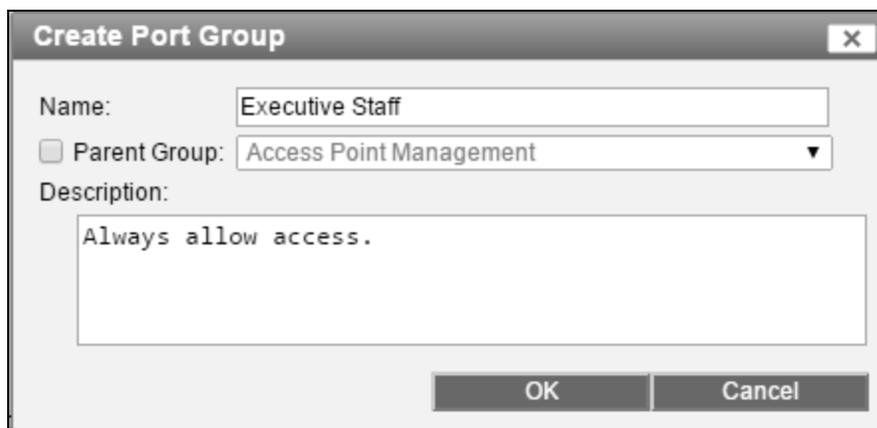


Figure 117: Create Port Group

8. Click **OK**.

## Admin User Group Membership

From the Admin Users View you can view or modify the group membership of an individual User.

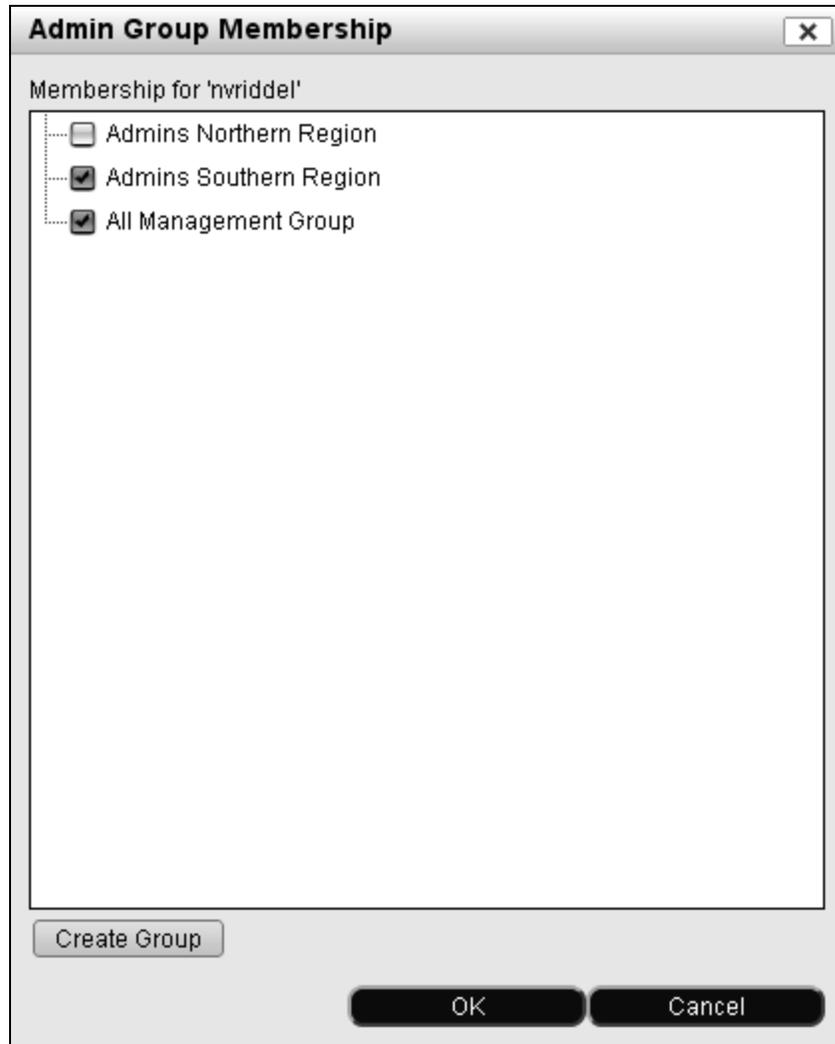


Figure 118: Admin User Group Membership

1. Select **Users > Admin Users**.
2. Select the User and click the **Groups** button.
3. The Group Membership view lists the available Administrator groups. A check next to a group name indicates that this user is contained in that group.
4. **To add the user to a group**, click the box next to the group name and then click **OK**.
5. **To remove the user from a group**, click to uncheck the box next to the group name and then click **OK**.

6. To create a missing group, click the **Create Group** button.

Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.

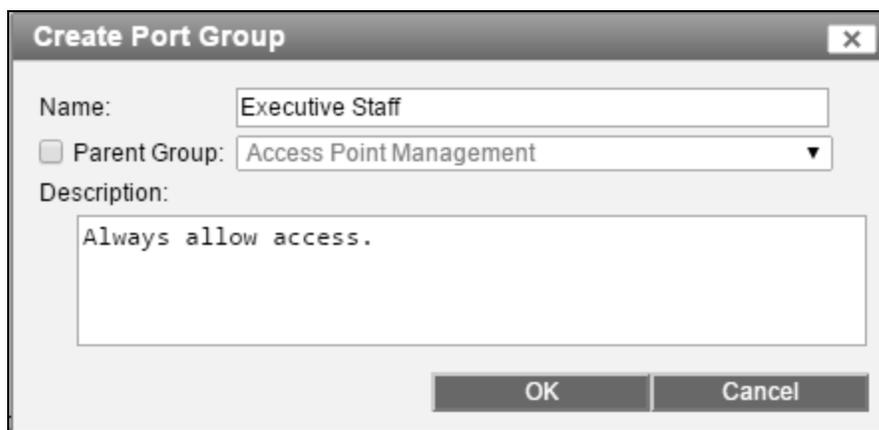


Figure 119: Create Port Group

## Configure Secure Mode For Admin Users

Secure SSL Mode can be used for Administrative User access. Unique security certificates for the appliances are required to use secure mode. Secure certificates in a High Availability configuration may be used on both the primary and secondary appliances if the certificate provider licensing allows them to be transferred to their counterpart in the configuration.

Network Sentry appliances are pre-configured with a self-signed security certificate. The administrative user logs in at the following URL, which provides secure access:

```
https://<host name_or_IP>:8443
```



## Chapter 7: Import And Export Data

Importing and exporting data allows you to leverage information across products, manipulate data outside your software or restore archived data. Import and export methods vary greatly depending on the type and location of the data. Review the tables below for information on import and export types and links to corresponding instructions.

**Table 18: Import Types**

Import Type	Definition
<b>Import Archived Data</b> on page 293	Network Sentry periodically archives and purges data from the database. Use this import to retrieve archived data for review.
<b>Import Hosts, Users Or Devices</b> on page 294	Allows you to import hosts, users with associated hardware, devices and IP Phones.
<b>Import Admin Users</b> on page 304	Allows you to import data for Admin users.
Import IP Ranges on page 307	Allows you to import ranges of IP Addresses into the Access Point Management configuration view.

**Table 19: Export Types**

Export Types	Definitions
<b>Export Data</b> on page 383	Allows you to export data from table views in Network Sentry.
<b>Conference Accounts</b> on page 673	Guest/Contractor Account views that allow you to export the data displayed.
<b>Create Single Guest Or Contractor Accounts</b> on page 663	
License Information Panel on page 36	Allows you to export data from the License Usage dialog. Click on the number in the In Use column on the License Information panel to open License Usage dialog. Export options are displayed at the bottom of the window.

## Import Archived Data

When the Purge Events task runs, Network Sentry creates an archive of several different types of records. You can reimport this data if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database. Records that are archived and can be re-imported include the following:

- **Alarms View** on page 489
- **Events View** on page 466

1. Navigate to one of the views listed above.
2. Click the **Import** button at the bottom of the view to display the Import window.
3. Select the **archive** from the drop-down list. The archives are listed by date with the name of the view at the beginning. For example, for the Connections View the archive would have the following format:

```
DYNAMICLOG_Archive_YY_MM_DD.bua.gz
```

4. Click **OK**.

Some archive files can be quite large and make take several minutes to import. A progress dialog is displayed as the import is taking place. A message is displayed when the import is complete.

## Import Hosts, Users Or Devices

Hosts, users or devices can be imported into the database from a .csv (comma separated value) file. Devices imported through the Host View are displayed in the Host View.

### Create An Import File

To add Hosts, users, devices or IP Phones create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records. You can mix the types of records you are importing. For example, you can import hosts, users and IP Phones in the same file as long as you have all of the appropriate fields in the header row.

To add Hosts or Devices create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import hosts and their corresponding adapters the header row could have the following fields:

```
adap.mac, adap.ip, host.owner, host.host, siblings
```

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have User IDs SMITH123 and Smith123, the database treats these as two separate user records.

If you import something that already exists in the database, the existing record is updated with the new data from the import. For example, assume the database contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.10.102 and host name Taylor1 and you import a record that has MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1. The MAC address remains the same since that is the key, but the other fields are updated. The database now contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1.

Imported data is displayed on multiple views. Adapter data is displayed on the Adapter View and in Adapter Properties. Host data is displayed in the Host View, in Host Properties and Topology View if Container is used in the import file. User data is displayed in the User View and User Properties.

The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

Table 20: Import File Data Fields

Header Field	Required For	Properties Field — Definition
<b>Adapter Fields</b>		
<b>adap.ip</b>		<b>IP Address</b> — IP address of the adapter. Use a valid IP format, such as, 127.0.0.1.
<b>adap.mac</b>	host	<b>Physical Address</b> — MAC address of the adapter. Use a valid MAC format, such as 00:19:D1:94:5C:06.
<b>adap.loc</b>		<b>Location</b> — The switch and port where the adapter is connected to the network.
<b>adap.media</b>		<b>Media Type</b> — Network interface type (wired or wireless).
<b>adap.accessVal</b>		<b>Access Value</b> — VLAN to which the adapter is assigned.
<b>adap.descr</b>		<b>Description</b> — Description of the adapter, such as, Intel(R) 82566DM Gigabit Network Connection.
<b>adap.venName</b>		<b>Vendor Name</b> — Name of the vendor for the adapter based on the first three octets of the MAC address, such as, Intel Corporation. Vendor OUIs are stored in the database and can be viewed through the Vendor OUI screen. See <b>Vendor OUIs</b> on page 103.
<b>Host Fields</b>		
<b>host.host</b>		<b>Host Name</b> — Machine name of the host.
<b>host.role</b>		<b>Role</b> — Roles are attributes on hosts that can be used as filters by Network Sentry when selecting a Network Access Policy, an Endpoint Compliance Policy or a Supplicant EasyConnect Policy. The role must be defined in Network Sentry and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
<b>host.owner</b>		<b>Registered User</b> — User ID of the host's owner. On import Network Sentry checks for the user in its own database and in the LDAP directory. If the user does not exist a new user record is created. If the user does exist the user is connected to the host.

Header Field	Required For	Properties Field — Definition
host.expireDate		<p><b>Expiration Date</b> — Date that the host is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST. If not included in the import, the global setting in Network Sentry Properties is used.</p> <p>The value "<b>Never</b>" can be used to prevent a host from ever being removed from the database by the aging process.</p> <p><b>Note:</b> Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.</p>
host.inact		<p><b>Days Inactive</b> — the host can be inactive before being aged out. This number is used to calculate the date to age the host out of the database. If not included in the import, the global setting in Network Sentry Properties is used.</p> <p>To avoid using the default settings you must enter a number in this field. You can use a very large number to ensure that the host is not deleted, such as 1825 Days (equals five years). Make sure that there is a space between the number and the word Days. The format for the value must be as follows:</p> <p>xxx Days</p> <p>1825 Days</p>
host.sn		<b>Serial Number</b> — Serial number of the host.
host.hwType		Hardware Type
host.os		<p><b>Operating System</b> — Host's operating system such as Windows XP or Mac OS X.</p> <p><b>Note:</b> Only hosts that have an operating system listed in Host Properties are rescanned at the scheduled rescan time. Valid operating systems include: Windows or Mac.</p>
host.agentVer		<b>Agent Version</b> — Version number of the Persistent Agent installed on the host.
host.hasAgent		<b>Persistent Agent</b> — Indicates whether or not the host has an agent installed. Use true or false. If the field is left blank, the default is false.
host.notes		<b>Notes</b> — Data is imported into the Notes field in Host Properties.

Header Field	Required For	Properties Field — Definition
<b>host.topo</b>	host - if importing into Topology	<b>Topology</b> — Container in Topology where this host should be placed on import. This field is required if importing into Topology. Host is managed by the Host View but displays in both the Host View and the Topology View.
<b>host.dirPoVal</b>		<b>Security And Access Value</b> — Security and Access Value is an attribute used as a filter for User/Host Profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory or if this host does not have an owner, the Security and Access Value can be entered manually.
<b>host.devType</b>		<p><b>Device Type</b> — Must be one of the following device types or blank:</p> <ul style="list-style-type: none"> <li>• Alarm System</li> <li>• Android</li> <li>• Apple iOS</li> <li>• Camera</li> <li>• Card Reader</li> <li>• Cash Register</li> <li>• Dialup Server</li> <li>• Environmental Control</li> <li>• Gaming Device</li> <li>• Generic Monitoring System</li> <li>• Health Care Device</li> <li>• Hub</li> <li>• IP Phone</li> <li>• Linux</li> <li>• Mac OS X</li> <li>• Mobile Device</li> <li>• Network</li> <li>• PBX</li> <li>• Pingable</li> <li>• Printer</li> <li>• Registered Host</li> <li>• Server</li> <li>• StealthWatch</li> <li>• Top Layer IPS</li> <li>• Unix</li> <li>• UPS</li> <li>• Vending Machine</li> <li>• Windows</li> <li>• Wireless Access Point</li> <li>• VPN</li> <li>• IPS / IDS</li> </ul>
<b>siblings</b>		<p><b>Siblings</b> — Adapters that are on the same host are siblings. For example, if a PC has a wireless adapter and a wired adapter, those adapters are siblings.</p> <p>Enter the MAC addresses of all of the adapters for this host separated by semi-colons (;). See the example below:</p> <p>00:15:70:CA:7D:01;00:15:70:CA:7D:00</p> <p>Each adapter must have a separate record in the .csv file, with a siblings field listing all of the adapters on the host.</p> <p>Some device types may have only one adapter, such as IP Phones. To import those devices, include the MAC Address of the single adapter in the siblings field with no semi-colon.</p>

Header Field	Required For	Properties Field — Definition
<b>User Fields</b>		
<b>user.fn</b>		User's first name.
<b>user.ln</b>		User's last name.
<b>user.uid</b>	user	<b>ID</b> — Unique alpha numeric User ID.  If a directory is used for authentication,when the Network Sentry database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.
<b>user.email</b>		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>user.addr</b>		User's mailing address.
<b>user.city</b>		User's city.
<b>user.st</b>		User's state.
<b>user.zip</b>		User's postal code.
<b>user.ph</b>		User's telephone number.
<b>user.title</b>		User's title.
<b>user.role</b>		<b>Role</b> — Roles are attributes on users that can be used as filters by Network Sentry when selecting a Network Access Policy, an Endpoint Compliance Policy or a Supplicant EasyConnect Policy. The role must be defined in Network Sentry and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
<b>user.notes</b>		<b>Notes</b> — Data is imported into the Notes field in User Properties.
<b>user.pw</b>		<b>Password</b> — Password for this user.
<b>user.dirPoIVal</b>		<b>Security And Access Value</b> — Security and Access Value is an attribute of a user that can be used as a filter for User/Host Profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory the Security and Access Value can be entered manually.
<b>user.expireDate</b>		<b>Expiration Date</b> — Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.

Header Field	Required For	Properties Field — Definition
<b>user.maxHosts</b>		<b>Allowed Hosts</b> — Maximum number of hosts that can be associated with or registered to this user and connect to the network.
<b>user.delHosts</b>		<p><b>Delete Associated Hosts</b> — Indicates whether or not hosts registered to this user should be deleted when the user is aged out of the database. Enter either Yes or No. This data displays on the User Properties window in the Time section and is set when the expiration date is set.</p> <hr/> <p><b>Note:</b> Importing this field requires that you also include <b>user.expireDate</b> in your import file. If you do not include <b>user.expireDate</b>, the <b>user.delHosts</b> field data is not imported.</p>
<b>user.smsNum</b>		<b>Mobile Number</b> — User's mobile phone number. This can be used to send SMS Messages based on events and alarms.
<b>user.smsPro</b>		<b>Mobile Provider</b> — The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database.

## Sample Host, Adapter, User or Device Import Files

Hosts, Adapters, Users or Devices can be imported through the Hosts View using a .csv file. All of these items can be included in the same import file as long as the header row contains the appropriate database field names. See **Create An Import File** on page 294. Below are sample import files for each type as well as an import file containing records of all types.

### **Host Import**

The `adap.mac` field is required for this import.

**`adap.mac,siblings,adap.ip,host.owner,host.devType`**

```
00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Smith2010,Windows
00:15:70:D9:46:B0,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux
00:15:70:D9:46:B1,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux
```

### **Pingable Device Import**

The `adap.mac` field is required for this import. The `host.devType` field is recommended to ensure that the correct icon displays. Use the `host.topo` field to display this device both in the Host View and the Topology View. Entering the name of the Topology Container in the `host.topo` field triggers Network Sentry to display the device in the Topology View. The device is automatically displayed in the Host View.

**`adap.mac,siblings,adap.ip,host.topo,host.devType`**

```
00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Blding_B,PBX
00:15:70:D9:46:B0,00:15:70:D9:46:B0,192.168.20.10,Blding_A,Camera
00:15:70:D9:46:B2,00:15:70:D9:46:B2,192.168.20.12,Blding_A,Printer
```

### **IP Phone Import**

The `adap.mac` field is required for this import. The `host.devType` field is not required, however, since IP Phones are treated differently to prevent dropped calls, it is recommended that you include this field.

**`adap.mac,host.devType`**

```
00:12:C2:6C:56:74,IP Phone
00:12:C2:D9:46:B0,IP Phone
```

### **User Import**

The `user.uid` field is required for this import.

**`user.uid,user.fn,user.ln`**

```
Hebert2010, Frank, Hebert
Miller2009, Tammy, Miller
```

### Mixed Record Types Import

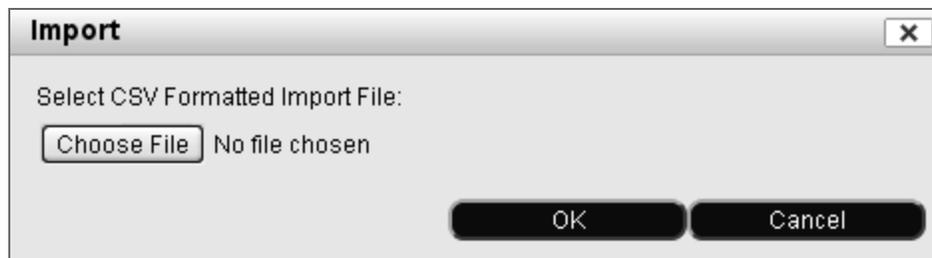
When combining different record types into a single import file, all of the fields for each record type must exist in the header row. For fields that do not apply to a particular record type, you must still include commas. Required fields for each type must be included.

```
adap.mac,siblings,host.owner,host.devType,user.uid,user.fn,user.ln
,,,,Hebert2010, Frank, Hebert
00:12:C2:6C:56:74,,,,IP Phone,,,
00:13:CE:6C:56:75,00:13:CE:6C:56:75,Smith2010,Windows,,,,
```

### Import Hosts, Users, Devices or IP Phones From A .csv File

To import from a .csv file created in V4.1.1 or higher, see **Import Host, User And Adapter Data From A Previous Version** on page 303 for file format information.

1. Click **Hosts > Hosts View**.
2. At the bottom of the Host View, click **Import**.
3. Browse to the .csv file containing the items to be imported.
4. Select the file and click **Open**.
5. Click **OK** on the Import window.



**Figure 120: Import Window**

6. Network Sentry processes the import file and displays a list of records in the Import Results window. Verify that the data is displaying in the correct columns.
7. Click **OK** to continue the import.



The screenshot shows a window titled "Import Results" with a close button (X) in the top right corner. Below the title bar, there are navigation controls: "<< first < prev 1 next > last >>" and a dropdown menu showing "200". The main content is a table with the following data:

#	Adapter - Physical Address	Host - Container (T	Host - Device Type	Host - Registered To
1	00:30:48:DF:25:4D		Registered Host	hackert
2	28:37:37:B0:91:C5		Alarm System	
3	00:1E:C2:AF:8C:27		Registered Host	
4	00:1F:5B:E8:E4:51		Registered Host	
5	00:30:48:69:63:CC	Executive_Suite	Alarm System	
6	00:1C:BF:B4:9D:30		Registered Host	Curly
7	00:1C:23:41:14:72		Registered Host	Curly

At the bottom of the window, there are two buttons: "OK" and "Cancel".

**Figure 121: Import Results Window**

8. If the required columns are missing or data is not in the correct format, an error message is displayed and the import will not proceed.
9. If there are no issues with the data, a message is displayed indicating that the import is complete.

### Import Host, User And Adapter Data From A Previous Version

If you have a .csv file created for or exported from version 4.1.1 or higher, you can import that data into the current version of Network Sentry. You must modify the .csv file so that it conforms to the new import format.

The first row in the .csv file must be a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter, but the order in the header row must match the order of the data contained in the file.

For the names and definitions of the fields that should be used in the header row see **Import File Data Fields** on page 295.

Once your .csv file is formatted correctly, see **Import Hosts, Users, Devices or IP Phones From A .csv File** on page 301 for import instructions.

## Import Admin Users

Admin users can be imported into the database from a .csv (comma separated value) file through the Admin Users View.

### Create An Import File

To import Admin users create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import admin users the header row could have the following fields:

```
profileName,uid,authType,fn,ln
```

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have User IDs SMITH123 and Smith123, the database treats these as two separate user records. If you import something that already exists in the database, the existing record is updated with the new data from the import.

**Note:** If you import an existing Admin user, all fields will be replaced by those in the import file.

**Note:** When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

Imported data is displayed on both the Admin User view and the User View. The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

**Table 21: Import File Data Fields**

Header Field	Required	Properties Field — Definition
profileName	Yes	<b>Admin Profile</b> — Administrative Users must have an associated Admin Profile that provides them with permissions for features in Network Sentry. Enter the name of the Admin Profile that matches an existing Profile in the database.

Header Field	Required	Properties Field — Definition
<b>uid</b>	Yes	<p><b>User ID</b> — Unique alpha numeric User ID.</p> <p>If a directory is used for authentication, when the Network Sentry database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.</p>
<b>authType</b>		<p>Authentication method used for this Admin user. Types include:</p> <ul style="list-style-type: none"> <li>• <b>CM</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server.</li> </ul>
<b>fn</b>		User's first name.
<b>ln</b>		User's last name.
<b>email</b>		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>addr</b>		User's mailing address.
<b>city</b>		User's city.
<b>st</b>		User's state.
<b>zip</b>		User's postal code.
<b>ph</b>		User's telephone number.
<b>title</b>		User's title.
<b>notes</b>		Notes about this user.
<b>expireDate</b>		<b>Expiration Date</b> — Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
<b>createDate</b>		<b>Creation Date</b> — Date that the user record was created. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
<b>smsNum</b>		<b>Mobile Number</b> — User's mobile phone number. This can be used to send SMS Messages based on events and alarms.

Header Field	Required	Properties Field — Definition
smsPro		<b>Mobile Provider</b> — The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database. See Mobile Providers on page 130.

### Sample Import File

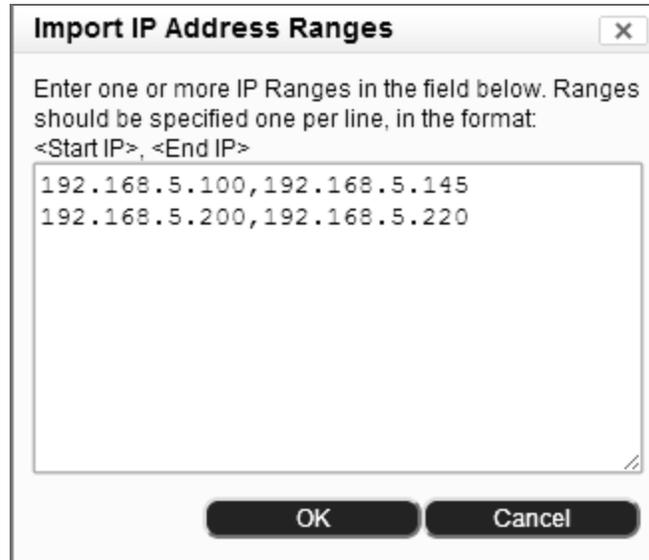
Below is a sample .csv file for importing Admin users. the `profileName` and `uid` fields are required.

`profileName,uid,authType,fn,ln`

```
Administrator,ajones111,LDAP,,Jones
Administrator,admin111,CM,Admin,User111
Conference Accounts,dpcuser,CM,Elaine,White
Conference Accounts,ajames,CM,james,james
```

## Import IP Ranges

Some views in Network Sentry require lists of IP Address ranges. An import mechanism is provided to speed up the process of entering this data.



**Figure 122: Import IP Address Ranges**

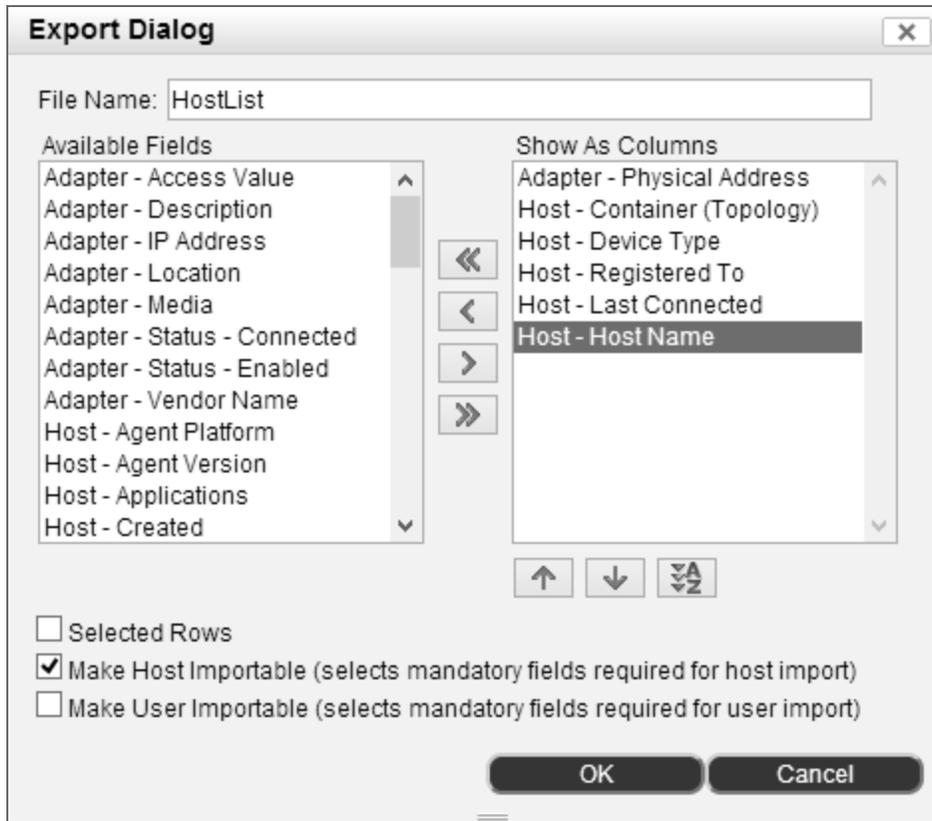
1. Click **System > Settings**.
2. Navigate to the view where you would like to import IP Address Ranges.
3. Click **Import** at the bottom of the screen.
4. In the Import window type the first and last IP address of each range separated by a comma.

Press Enter to start a new line. You should not have overlapping ranges or ranges that cross subnets such as 192.168.5.100-192.168.6.150.

5. Click **OK** to import the IP address range.
6. Click **Save Settings** to save your changes.

## Export Data

Export data to a CSV file, an Excel spreadsheet, a PDF document or an RTF document. Select from a list of possible fields and control the order of the data in the export. If you plan to re-import the same file after editing it, you must use a CSV file. See **Import Hosts, Users Or Devices** on page 294 for a list of fields that can be exported or imported and their definitions.



**Figure 123: Sample Export Dialog**

1. Navigate to a View with export options at the bottom, such as the Host View.
2. Use the Search or Filters to display a list of records.
3. Use Ctrl-click or Shift-click to select the records you wish to export. If you do not select specific records, all displayed records are exported. When the Export dialog is displayed, check the Selected Rows check box to export only selected records.
4. At the bottom of the window, click the icon for the type of export file needed, such as PDF.
5. In the File Name field, enter a name for the export file. Do not add an extension. It is added when you click OK based on the file type you selected in the previous step.

6. The fields contained in the Export Dialog vary based on the View from which you are exporting.
7. Select the field(s) you want to export and click the right-arrow to move the field to the Show As Columns list. Ctrl-click to select more than one field at a time.
8. Click the double-arrows to move all of the fields from one column to the other.
9. To remove fields from the export, select them in the Show As Columns list and click the left-arrow.
10. To reorder the fields in the **Show As Columns** list, click the field and then click the Up or Down arrows. The order displayed from top to bottom corresponds to the columns in the export from left to right. For example, if the first field at the top of the list is Last Name, that is the left most column in the export.
11. To sort fields alphabetically, click the **Sort** button labeled AZ.
12. Check the **Selected Rows** check box to export only the records selected in the View. If you leave this box unchecked, all the records in the View are exported.
13. A Header line consisting of the field names is inserted in the .csv file if you check either or both of the **Make Importable** check boxes. In addition, the fields required for import are automatically added to your export.

---

**Note:** When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

---

**Note:** Only the Export Dialog accessed from Users, Hosts or Adapters views includes two Make Importable check boxes because of the relationship between Users and their corresponding Hosts. The Export Dialog accessed from other views may have one Make Importable check box, such as, Admin Users, or no Make Importable check boxes, such as Connections.

---

14. Click **OK**.
15. Depending on your browser, the file is either generated and saved to a Downloads location or you may need to navigate to the **location** where the file is to be placed.



## Chapter 8: Hosts, Adapters, and Applications

Hosts are devices that require network services and can be associated with a user, such as a PC or a gaming device. Adapters are the network interfaces on these devices. There are other types of hosts not associated with users, such as IP phones or printers. The Hosts, Adapters, and Users views provide an individual menu option for each, but uses a shared search capability to simplify management of hosts, adapters and their associated users on your network. Regardless of the menu item selected and displayed, the navigation and search or filter options are the same.

Applications that are contained on a host are scanned when the host is connected to the network, and appear in the Applications View. The list of applications is continuously updated as hosts are scanned.

The Quick Search field at the top of the Host View and Adapter View windows allows you to search based on an IP address, MAC Address, User ID, User First and Last Name or Host Name. Wild card searches, such as 192.168.10.1\* can be used. The drop-down arrow at the end of the Search field allows you to set up a filter and use it once or save it for future use. See **Search And Filter Options For Hosts, Adapters, Users or Applications** on page 317 for additional information.

The mouse-over feature displays a pop-up window or tool tip when you place the mouse over any icon in the Status column. This tool tip contains detailed data about the user, host or adapter.

Add or remove columns from the table by clicking the Configuration button and selecting your options from the Settings window. The Settings window also controls the data included on in tool tips displayed when you hover over any icon on the left side of the view. See **Configure Table Columns And Tool-tips** on page 313 for additional information. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Hosts - Displayed: 532 Total: 532

Servers: All Search

<< first < prev 1 2 next > last >> 500

Server	Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent	Host Created	Host Expires	Host Ina
qa217.bradfordnetworks.com		rmacintosh			Contractor			06/13/16 04:36 PM GMT-0400		
qa217.bradfordnetworks.com		rmacdonald			Contractor			06/13/16 04:27 PM GMT-0400		
qa217.bradfordnetworks.com		AP00EB-D510-37E0						09/06/16 02:41 PM GMT-0400	10/06/16 02:41 PM GMT-0400	10/20/16 0400
qa217.bradfordnetworks.com								09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	
qa217.bradfordnetworks.com								09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	
qa217.bradfordnetworks.com								09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	10/20/16 0400
qa217.bradfordnetworks.com								09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	
qa217.bradfordnetworks.com		SeahagIII				Windows Vista7		09/07/16 07:55 AM GMT-0400	10/07/16 07:55 AM GMT-0400	
qa217.bradfordnetworks.com		BNLAPTOP-QA	a.lincoln		NAC-Default	Windows 7 Professional 6.1 Service Pack 1		09/09/16 01:34 PM GMT-0400		
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com								09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	

Export to:

Options Modify Delete Enable Disable

Figure 124: Host View

## Configure Table Columns And Tool-tips

Use the configuration button on the User View, Adapter View, Host View, and Applications View to open the Settings window. The Settings window controls the columns displayed in each view and the details displayed in tool-tips when you hover over an icon.

### Configure Columns

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Columns** tab.
3. Mark the columns to be displayed in the table on the User, Adapter or Host View with a check mark and click **OK**.
4. These settings are saved for the logged in user.

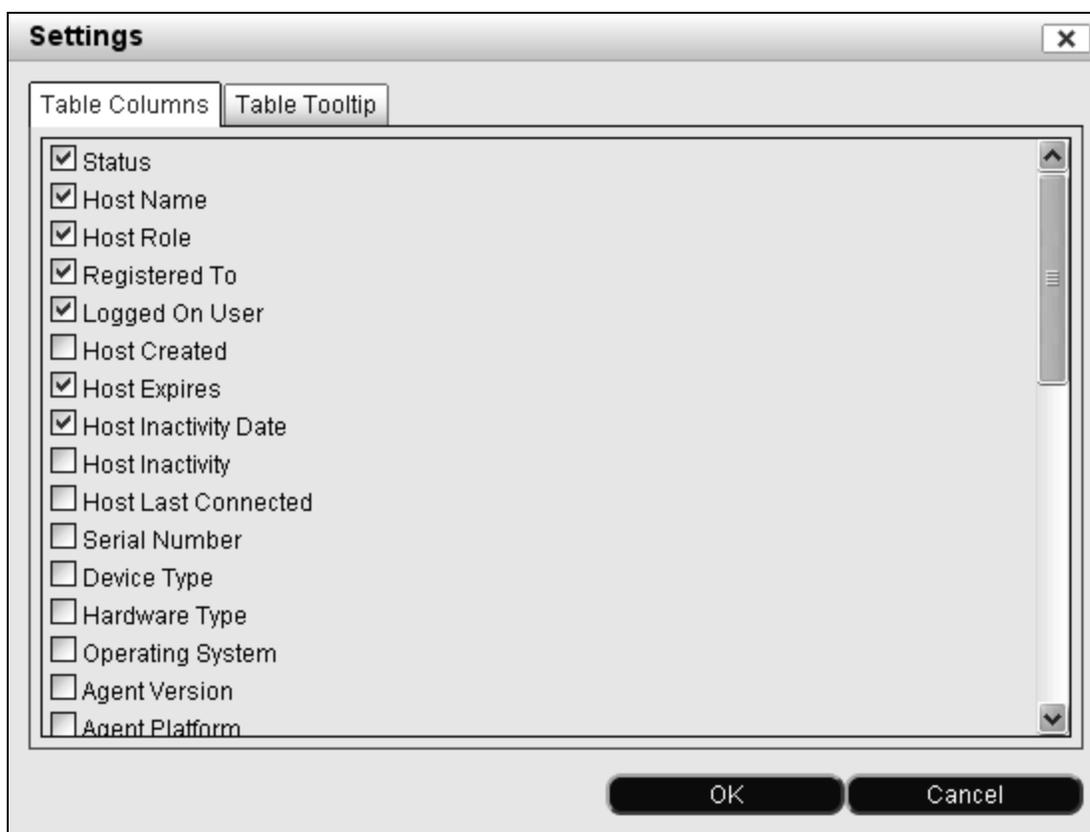


Figure 125: Configure Settings - Table Columns

### Configure Tool-Tips

Select the fields to be displayed in the tool-tip when you hover the mouse over the status icon of either a User, an Adapter or a Host. Available fields vary depending on which item you are configuring.

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Tooltip** tab.
3. The **Available Fields** column displays fields that can be displayed, but have not yet been selected. The Selected Fields column displays fields that will display in the tool-tip.
4. Use the arrows in the center of the window to move fields from one column to the other until the appropriate set of fields is displayed in the **Selected Fields** column.
5. Select a field in the Selected Fields column and use the up and down arrow buttons to change the order of display. Use the AZ button to sort fields alphabetically.
6. The **Hide Blank Fields** option is enabled by default. It reduces the size of the tool-tip when selected fields are blank for a particular item. For example, if you have selected Host Expires and the selected Host does not have an expiration date, then when the tool-tip for that host is displayed, the Host Expires field is hidden.
7. Click **OK** to save your changes. These settings are saved for the logged in user.

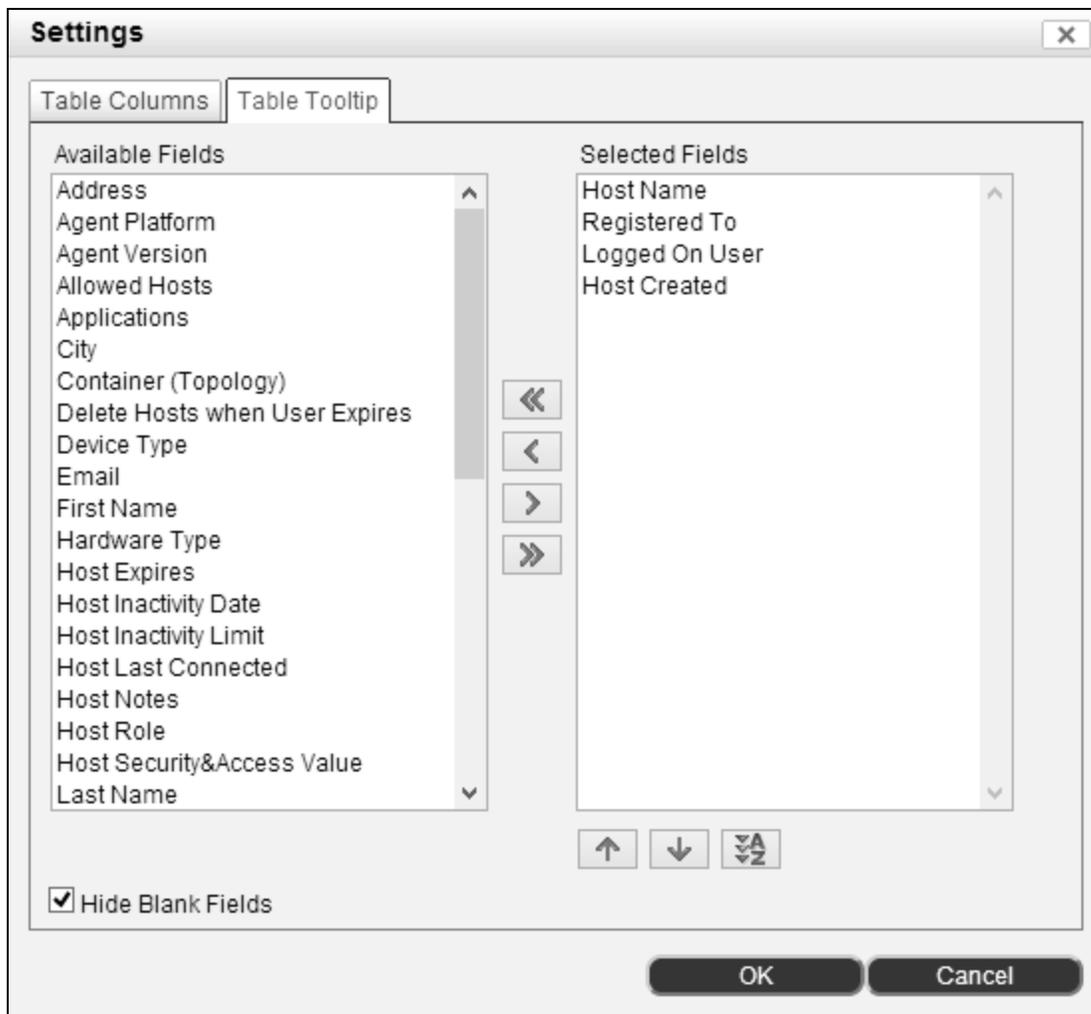
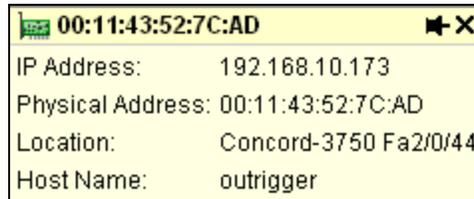


Figure 126: Configure Settings - Table Tool-tips

### Using Tool-Tips

Tool-tips are displayed when you hover the mouse over a status icon in the User, Adapter or Host views. Tool-tips details are configured using the Settings window shown in the previous section.



**Figure 127: Sample Tool-tip**

- When a tool-tip is displayed, click the Push Pin icon to anchor it to the screen. Now you can move the tool-tip around your desktop without it closing.
- High-light text in a tool-tip and press Ctrl-C to copy it. Press Ctrl-V to paste the text in a field.
- Open and anchor multiple tool-tips to quickly compare data.
- Hover over the status icon in the top left corner for text based status information.

## Search And Filter Options For Hosts, Adapters, Users or Applications

There are several search and filter mechanisms used to locate Hosts, Adapters, Users or Applications. These four tabs share a single view and search mechanism. Options include: Quick Search and Custom Filters, which can be used once or saved for reuse.

When a search or filter is run, the search data or the name of the filter remains in the search field at the top of the window. If you then click on a different tab, that search is rerun in the context of the new tab.

### Wild Cards

When searching using a text field in a Custom Filter or the Quick Search field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP Address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records.  Any search field that starts and ends with square brackets "[" and has one or more commas "," is treated as a list of values.
!	!192. in the IP Address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).

### Quick Search

The Quick Search field at the top of the window allows you to search based on a single piece of data, such as IP Address, and display all matching records. The following fields are included in the Quick Search: IP Address, MAC Address, Host Name, User First Name, User Last Name, Registered User, Logged On User, and User ID. To search by MAC Address you must use one of the following formats:

```
xx:xx:xx:xx:xx:xx
xxxxxxxxxxxxxx
xx.xx.xx.xx.xx.xx
```

xx-xx-xx-xx-xx-xx

xxxx.xxxx.xxxx

Wild card searches can also be done. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5\*. Without the separators the search option cannot distinguish that it is a MAC address.

If you are searching by IP Address you enter 192.168.5.1\* and you get all records for IP addresses from 192.168.5.1 to 192.168.5.199. See **Wild Cards** on page 317.

The information displayed varies depending on the tab that is selected. As you click from tab to tab the search in the Quick Search field is applied automatically.

**Users Tab** — Displays all users associated with a device that matches the IP range.

**Hosts Tab** — Displays all hosts with an adapter that matches the IP range.

**Adapters Tab** — Displays all adapters that match the IP range

To broaden the search, enter less information, such as \*11\*. This returns any User Name, User ID, IP, MAC, or Host Name containing 11 depending on the tab you have selected.

To use the Quick Search option:

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts or Users Tab.
3. Enter a single piece data in the search field and press **Enter**. Wild card searches can be done.

## Custom Filter

The Custom Filter is the equivalent to an advanced search feature. It provides many fields that can be used in combination to narrow the list of Users, Adapters or Hosts displayed. A Custom Filter can be created and used just once or can be saved under a filter name. The new filter then displays in the drop-down menu accessed by clicking the arrow on the Quick Search field at the top of the window. Custom Filters can be modified, copied or deleted as needed. You can also export Custom Filters to a .txt file which allows Custom Filters to be imported and used by other Admin users.

Use your mouse to hover over a saved filter in the drop-down menu and display a tool-tip with details about that filter. There is currently only one default Custom Filter, Online Hosts, that displays a list of hosts that are connected to the network.

For filter field definitions refer to the following:

### Create and Save a New Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. From the drop-down menu select **New Filter**.
5. Enter the name of the new filter and click **OK**.
6. Continue with the topic below, Configure A Filter.



Figure 128: Add New Filter

### Configure a Filter

This window is used in two ways. First if you have selected New Filter from the menu off of the Quick Search drop-down, you can configure the filter and Network Sentry saves it for future use. Second, if you have selected Custom Filter from the menu off of the Quick Search, you can configure this filter and use it just one time.

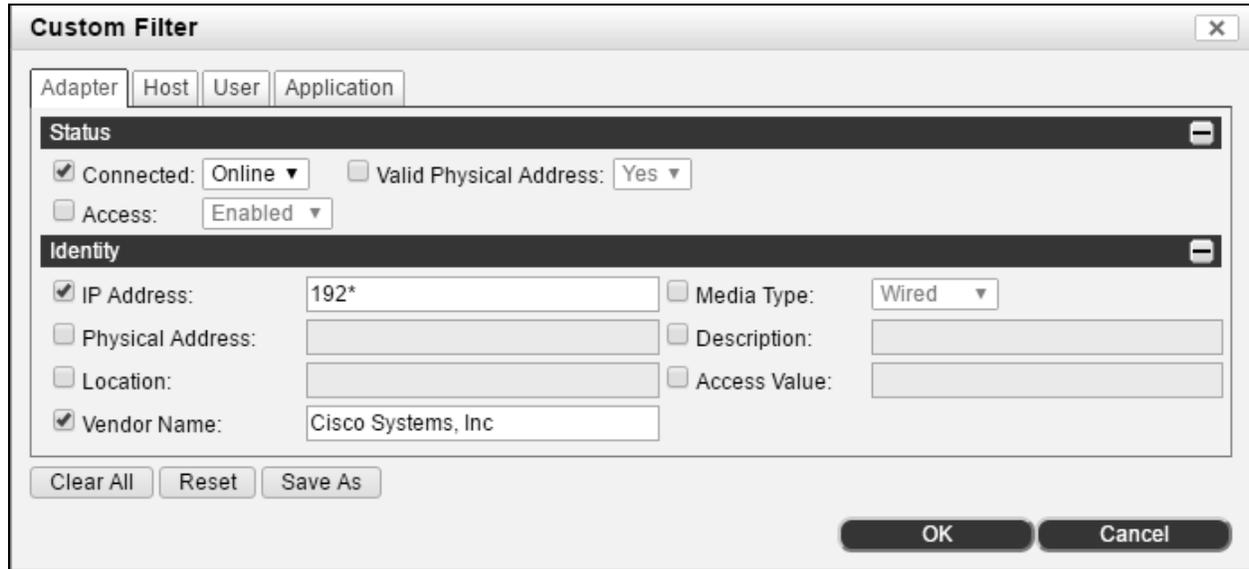


Figure 129: Custom Filter

**Note:** This dialog box is common to the Adapter, Host and User Views. Custom filter entries on any of these tabs will persist if you navigate between these views.

1. Once you have the Filter window displayed, enable the fields to be included in the filter by marking them with a check mark.
2. For each enabled field you must provide additional information. For example, if you select the Connected field, you must choose either On Line or Off Line.

3. For text fields, such as the IP Address field, you must enter the search data, such as 192.168.10.5. Wild cards can be used in these fields. See **Wild Cards** on page 317.
4. To erase all selections, click the **Clear All** button.
5. If you have opened a saved filter and started to modify it, use the **Reset** button to return the filter to its original settings.
6. Click **OK** to run the configured filter. If this filter was assigned a name, the settings will be saved.
7. Immediately after the filter is run, the filter name displays at the top of the view in the Quick Search field. To modify the filter, click the **Edit** link to the left of the Quick Search field. This modifies the filter whether it was saved or just configured and run one time.

### **Edit a Custom Filter**

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be edited and click the pencil or edit icon to the right of the filter name.
5. When the Filter window displays, modify the filter as needed.
6. Click **OK** to save your changes.

### **Delete a Custom Filter**

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be deleted and click the red X to the right of the filter name.
5. When the confirmation message displays, click **Yes**.

### **Export a Custom Filter**

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Export**.

5. In the Export Filters dialog, select the filters you want to export. Use Ctrl or Shift to select multiple filters.
6. Click **OK**.

The filters are downloaded to a .txt file to your default download directory.

### Import a Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Import**.
5. Click Choose File to find and select the .txt file containing the filters.
6. Click **OK** to import the filters.

The filters will appear in the list.

## Host View

The Host View is part of a window that includes menu options for Users, Adapters Hosts, and Applications. Use the Host View to add, delete, modify, locate and manage hosts connected to your network.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the adapters and their connection status on this host. Hover over the icon in the Status column to display a tool-tip with detailed information about this host. For field definitions see **Host View And Search Field Definitions** on page 327. For information on Status icons see the **Icon Key** on page 14.

The **Displayed** and **Total** fields in the title bar represent the number of records displayed versus the total number of records in the database. Data in some tables, such as Users, is refreshed periodically but is not re-sorted based on the new data until you close and reopen the view or click a column heading.

**Note:** If a host fails one scan and is denied access to the network, but passes another scan at a different time or location and is allowed access to the network, the host will still be marked At Risk because it failed the first scan. The host will continue to be marked At Risk until actions are taken to pass the failed scan.

Hosts - Displayed: 532 Total: 532

Servers: All Search \*

<< first < prev 1 2 next > last >> 500

Server	Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent	Host Created	Host Expires	Host Ina
qa217.bradfordnetworks.com		rmacintosh			Contractor		<input checked="" type="checkbox"/>	06/13/16 04:36 PM GMT-0400		
qa217.bradfordnetworks.com		rmacdonald			Contractor		<input checked="" type="checkbox"/>	06/13/16 04:27 PM GMT-0400		
qa217.bradfordnetworks.com		AP00EB-D510-37E0					<input checked="" type="checkbox"/>	09/06/16 02:41 PM GMT-0400	10/06/16 02:41 PM GMT-0400	10/20/16 0400
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	10/20/16 0400
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/06/16 06:03 PM GMT-0400	10/06/16 06:03 PM GMT-0400	
qa217.bradfordnetworks.com		SeahagIII				Windows Vista/7	<input checked="" type="checkbox"/>	09/07/16 07:55 AM GMT-0400	10/07/16 07:55 AM GMT-0400	
qa217.bradfordnetworks.com		BNLAPTOP-QA	a.lincoln		NAC-Default	Windows 7 Professional 6.1 Service Pack 1	<input checked="" type="checkbox"/>	09/09/16 01:34 PM GMT-0400		
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	
qa217.bradfordnetworks.com							<input checked="" type="checkbox"/>	09/11/16 06:11 PM GMT-0400	10/11/16 06:11 PM GMT-0400	

Export to:

Options Modify Delete Enable Disable

Figure 130: Host View

Host View Navigation, Menus, Options And Buttons

For information on selecting columns displayed in the Host View see **Configure Table Columns And Tool-tips** on page 313. Some menu options are not available for all hosts. Options may vary depending on host state.

Field	Definition
<b>Navigation</b>	<p>Across the top of the Hosts View are navigation tools that allow you to quickly move through large numbers of records. These tools include the following:</p> <p><b>&lt;&lt;first</b>—Takes you to the first page of records.</p> <p><b>&lt;prev</b>—Takes you back one page.</p> <p><b>Page Number</b>—Current page number is displayed.</p> <p><b>next&gt;</b>—Takes you forward one page.</p> <p><b>last&gt;&gt;</b>—Takes you to the last page.</p> <p><b>Drop-down Box</b>—Allows you to select the number of records to be displayed on each page.</p>
<b>Servers</b>	Select the server containing the hosts you want to view.
<b>Quick Search</b>	<p>Enter a single piece of data to quickly display a list of hosts. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters.</p> <p>If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.</p> <p>When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.</p>
<b>Right Mouse Click Menu Options</b>	
<b>Add Hosts To Groups</b>	Add the selected host(s) to one or more group(s). See <b>Add Hosts To Groups</b> on page 358.
<b>Delete Hosts</b>	Deletes the selected host(s) from the database. Deleting a host from the Host View that is also displayed in the Topology View, removes that host from both views. Deleting a host from the Topology View does not delete it from the Host View. See <b>Delete A Host</b> on page 349.
<b>Disable Hosts</b>	Disables the selected host(s) preventing them from accessing the network. See <b>Enable Or Disable Hosts</b> on page 350.
<b>Enable Hosts</b>	Enables the selected host(s) if they were previously disabled. Restores network access.
<b>Group Membership</b>	Displays groups in which the selected host is a member. See <b>Host Group Membership</b> on page 361.

Field	Definition
<b>Host Health</b>	Opens a dialog with the contents of the Host Health tab from the Host Properties view. See <b>Host Health And Scanning</b> on page 339.
<b>Host Applications</b>	Opens the Applications window for the selected host and lists installed applications. See Application Inventory.
<b>Host Properties</b>	Opens the Properties window for the selected host. See <b>Host Properties</b> on page 335.
<b>Modify Host</b>	Opens the Modify Host window. See <b>Modify a Host</b> on page 344.
<b>Policy Details</b>	Opens the Policy Details window and displays the policies that would apply to the selected host at this time, such as Endpoint Compliance Policies, Network Access Policies, Portal Policies or Supplicant Policies. See Policy Details on page 416.
<b>Register As Device</b>	Changes the selected host to a device in the Network Sentry database. See <b>Register A Host As A Device</b> on page 364.
<b>Register As Host</b>	Changes the selected Rogue host to a registered host. Displays the Modify Host window. See <b>Modify a Host</b> on page 344.
<b>Run Agentless Scanner</b>	Manually run an Agentless Scanner for selected hosts. Hosts must be Windows Hosts, members of the domain, have an IP Address and be connected to the network.
<b>Scan Hosts</b>	Evaluates the selected host with the scan that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Scan that most closely matches the host at the moment.
<b>Send Message</b>	Sends a text box message to the selected host(s). The host must be using the Persistent Agent or Bradford Mobile Agent for Android.
<b>Set Host Expiration</b>	Launches a tool to set the date and time for the selected host(s) to age out of the database. See <b>Set Host Expiration Date</b> on page 366.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Audting Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p> <p><b>Note:</b> Changes made to Hosts, Users, or Adapters are not displayed in the Admin Auditing Log. These changes are visible in the Audit Log on each server.</p>
<b>Set Host Role</b>	Assigns a role to the selected host.
<b>Show Events</b>	Displays the events for the selected host.

Field	Definition
<b>Go To Logged On User(s)</b>	Opens the Users tab and displays the users currently logged onto the selected hosts. The logged on user may not be the registered user for the selected host.
<b>Set Logged On User Expiration</b>	Launches a tool to set the date and time for the user currently logged on to the selected host to age out of the database. See <b>Set User Expiration Date</b> on page 425.
<b>Set Logged On User Role</b>	Assigns a role to the user currently logged on to the selected host. See <b>Role Management</b> on page 609.
<b>Go To Registered User(s)</b>	Opens the Users tab and displays the registered users for the selected hosts.
<b>Set Registered User Expiration</b>	Launches a tool to set the date and time for the registered user for the selected host to age out of the database. See <b>Set User Expiration Date</b> on page 425.
<b>Set Registered User Role</b>	Assigns a role to the registered user for the selected host. See <b>Role Management</b> on page 609.
<b>Collapse All</b>	Collapses all host records that have been expanded.
<b>Expand Selected</b>	Expands selected host records to display adapter information.
<b>Buttons</b>	
<b>Import/Export</b>	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats.
<b>Options</b>	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

### Host View And Search Field Definitions

The fields listed in the table below are displayed in columns on the Host View based on the selections you make in the Settings window. See **Configure Table Columns And Tool-tips** on page 313. These fields are also used in Custom Filters to search for hosts. See **Search And Filter Options For Hosts, Adapters, Users or Applications** on page 317. Additional fields that can be displayed on the Host View are fields for the user associated with the selected host. See **User View And Search Field Definitions** on page 400.

**Note:** You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

Filter
✕

Adapter
Host
User
Application

Status

 Connected: Online
 Access: Enabled
 Security: Pending at Risk
 Authenticated: Yes

Time

 Created Date: Before 2016-03-10 00:00:00
 Expiration Date: Next 30 Days
 Inactivity Date: Before 
 Last Connected: Before

Policy - Agent

Policy - Access

 Agent Version: 
 Persistent Agent: Yes
 Agent Platform: Windows
 Role: 
 Security Access & Value:

MDM

 Managed by MDM: Yes
 Compliant: Yes
 Passcode Enabled: Yes
 Data Encryption: Yes
 Compromised: Yes

Vulnerability Scan

 Status: Passed Scan
 Last Scanned Date: Before 2016-06-30 00:00:00

Misc

 Host Name: Host Has Norton
 Registered To: 
 Hardware Type: 
 Serial Number: 
 Asset Tag: 
 Passed Tests: 
 VPN Client: Yes
 Logged On User: 
 Device Type: 3D chart
 Operating System: 
 System UUID: 

Category: All

 Notes: 
 Type: Rogue
 Include IP Phones

OK
Cancel

Figure 131: Custom Filters - Host View

Field	Definition
<b>Agent Platform</b>	Distinguishes between Windows, Mac OSX, iOS and Android agents.
<b>Agent Version</b>	<p>The version number of the Persistent, Mobile or Dissolvable Agent installed on the Host machine.</p> <p><b>Note:</b> "None" is displayed if the Host has registered or been rescanned with a Dissolvable Agent version that is prior to V 2.1.0.X or if this Host is a type set to by-pass the agent scan in the Endpoint Compliance Configuration.</p>
<b>Allowed Hosts</b>	<p>The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total.</p> <p>If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single machine with up to five adapters counts as one host.</p> <p>If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one machine with two network adapters would be counted as two hosts.</p> <p>If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.</p>
<b>Applications</b>	Applications running on the host. Categories of applications include: Anti-virus, Anti-spyware, Hotfixes and Operating System.
<b>Asset Tag</b>	The Asset Tag of the host that is populated by the agent when the asset tag is readable by the agent. The asset tag is derived from the System Management BIOS (SMBIOS).
<b>Authenticated</b>	Indicates whether the host is authenticated.
<b>Delete Hosts When User Expires</b>	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click <b>Set</b> .

Field	Definition
<b>Device Type</b>	<p>If the Host is a pingable device that is being managed in Hosts view, this field indicates the specific type of device.</p> <p>The list includes:</p> <ul style="list-style-type: none"> <li>• Alarm System</li> <li>• Android</li> <li>• Apple iOS</li> <li>• Camera</li> <li>• Card Reader</li> <li>• Cash Register</li> <li>• Dialup Server</li> <li>• Environmental Control</li> <li>• Gaming Device</li> <li>• Generic Monitoring System</li> <li>• Health Care Device</li> <li>• Hub</li> <li>• IP Phone</li> <li>• IPS / IDS</li> <li>• Linux</li> <li>• Mobile Device</li> <li>• Network</li> <li>• PBX</li> <li>• Pingable</li> <li>• Printer</li> <li>• Registered Host</li> <li>• Server</li> <li>• StealthWatch</li> <li>• Top Layer IPS</li> <li>• Unix</li> <li>• UPS</li> <li>• Vending Machine</li> <li>• VPN</li> <li>• Windows</li> <li>• Wireless Access Point</li> <li>• Mac OS X</li> </ul>
<b>Container (Topology)</b>	Indicates whether this host is also displayed in the Topology View and shows the Container in which it is stored.
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>Email</b>	User's email address.
<b>Address</b>	User's physical address.
<b>City</b>	User's city.
<b>State</b>	User's state.
<b>Postal Code</b>	User's postal code.
<b>Phone</b>	User's phone number.
<b>Mobile Phone</b>	User's cell phone number.
<b>Mobile Provider</b>	User's mobile provider.
<b>Notes</b>	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.

Field	Definition
<b>Include IP Phones</b>	Appears when any option except Rogue is in the Host Type drop-down list. When selected, hosts that are IP Phones are included in the Host view.
<b>Hardware Type</b>	Type of Hardware, such as a PC.
<b>Created Date</b>	Date the Host record was created in the database.
<b>Expiration</b>	Controls the number of days a Host is authorized on the network. Host is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Inactivity Date</b>	Controls the number of days a Host is authorized on the network. Host is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Last Connected</b>	Date and time of the last communication with the Host.
<b>Host Name</b>	Machine name of the host.
<b>Host Notes</b>	Notes about this host.
<b>Host Role</b>	Role assigned to the Host. Roles are attributes of hosts and can be used as filters in a User/Host Profile. See <b>Role Management</b> on page 609.
<b>Host Security &amp; Access Value</b>	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used as a filter in a User/Host Profile, which in turn are used to assign Endpoint Compliance Policies, Network Access Policies and Supplicant EasyConnect Policies. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.  The access value is inherited from the user associated with this host.
<b>Last Modified By</b>	User name of the last user to modify the host.
<b>Last Modified Date</b>	Date and time of the last modification to this host.
<b>Logged On User</b>	Name of the user currently logged into the Host.
<b>Managed By MDM</b>	Host is managed by a Mobile Device Management system and data was retrieved from that system for registration.
<b>MDM Compliant</b>	Host is compliant with MDM policies. This data is retrieved directly from the MDM system.
<b>MDM Compromised</b>	MDM system has found this host to be compromised, such as Jailbroken or Rooted.
<b>MDM Data Encryption</b>	MDM system has detected that the host is using data protection.
<b>MDM Passcode</b>	MDM system has detected that the host is locked by a passcode when not in use.
<b>Operating System</b>	Host operating system, such as Mac OS X or Windows XP. This is usually determined based on the DHCP fingerprint of the device or is returned by an agent.

Field	Definition
<b>Passed Tests</b>	Shows passed scans.
<b>Persistent Agent</b>	Indicates whether the Persistent Agent is installed or not.
<b>Registered To</b>	User ID of the user to which this host is registered.
<b>Serial Number</b>	Serial number on the host.
<b>Server</b>	Select the server where the host is located.
<b>Status</b>	<p>Current or last known status is indicated by an icon. See <b>Icon Key</b> on page 14. Hover over the icon to display additional details about this Host in a tool tip.</p> <p><b>Connected</b> — Indicates whether host is online or offline.</p> <p><b>Access</b> — Indicates whether host is enabled or disabled.</p> <p><b>Security</b> — Indicates whether host is safe, at risk or pending at risk.</p> <p><b>Authentication</b> — Indicates whether or not the user associated with this host has been authenticated.</p> <p>When searching for a host based on Security, search results for Safe include Pending at Risk hosts. Those hosts are a sub-set of Safe hosts. Search results for Pending at Risk do not include Safe hosts.</p>
<b>System UUID</b>	The universal unique identifier used to identify the host.
<b>Title</b>	User's title, this could be a form of address or their title within the organization.
<b>Type</b>	<p>Select the type of host.</p> <p>Host types include:</p> <p><b>Rogue</b> — Unknown device that has connected to the network.</p> <p><b>Registered Host</b> — Device that is registered to a known user.</p> <p><b>Registered Device</b> — Device that is registered by its own Host Name and is not associated with a single user, such as a library computer or a shared workstation.</p> <p><b>Registered Host or Device</b> — Both devices that are registered to users and devices that are registered by host name.</p> <p><b>Registered Device In Host View</b> — Pingable device not associated with a user that is managed in the Host View, such as a printer.</p> <p><b>Registered Device In Host and Topology View</b> — Pingable device not associated with a user that displays in both the Host and Topology Views.</p>
<b>User Created</b>	Indicates when this record was created in the database.

Field	Definition
<b>User Expires</b>	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window.  To modify click <b>Set</b> . See <b>Set User Expiration Date</b> on page 425 for additional information.
<b>User Inactivity Date</b>	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit.  For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set.
<b>User Inactivity Limit</b>	Number of days the user must remain continuously inactive to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381.
<b>User Notes</b>	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
<b>User Role</b>	Role assigned to the user. Roles are attributes of users that can be used as filters in User/Host Profiles. See <b>Role Management</b> on page 609.
<b>User Security And Access Value</b>	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
<b>VPN Client</b>	Indicates whether the host connects to the network using a VPN connection.
<b>Vulnerability Last Scan</b>	The most recent time/date when Vulnerability scan results were processed for the host.
<b>Vulnerability Scan Status</b>	Indicates whether the host passed or failed the Vulnerability Scan.

Host Drill-Down

Use the arrow in the far left column of the Host View to expand a host and view adapter details. Expand or collapse multiple hosts by selecting them and using the right - mouse button or Options button. All adapters associated with a host are contained within the expanded section of the window. Adapters on the same host are considered siblings.

To copy an IP Address or Physical Address, click on the address to highlight it. Press Ctrl+C to copy it.

Status	Host Name	Host Role	Registered To	Logged On User	Operating System	Agent Platform
▼	AGENT-HP-WIN8	Test User	Test User		Windows 8.1 Pro 6.3	Windows
	<b>Status</b>	<b>IP Address</b>	<b>Physical Address</b>	<b>Media Type</b>	<b>Location</b>	<b>Actions</b>
		169.254.17.251	00:1C:BF:0B:31:DD	Wireless		⊗ [Icon] [Icon]
		fd5:e7c4:77f9:571a:3988:81fb:afee:7ddf	00:1A:4B:6C:84:BB	Wired	btrimby-switch [172.16.96.5] fa4	⊗ [Icon] [Icon]
		172.16.96.100				
		fd5:e7c4:77f9:571a:812b:5d49:325a:4591				
		fd5:e7c4:77f9:571a:dda2:375d:e731:45dd				
			00:1A:6B:EE:A2:D4	Wired		⊗ [Icon] [Icon]

Figure 132: Host - Expanded View

Field	Definition
<b>Status</b>	Status of the adapter. Options are Online or Offline and Enabled or Disabled. See <b>Icon Key</b> on page 14.
<b>IP Address</b>	IP address assigned to the adapter. If the adapter is offline, this is the last known IP address. Supports both IPv4 and IPv6 addresses.
<b>Physical Address</b>	MAC address of the adapter.
<b>Media Type</b>	Indicates whether the adapter is wired or wireless.
<b>Location</b>	The switch and port where the adapter last connected.
<b>Actions</b>	Use the action icons to do the following: <ul style="list-style-type: none"> <li>• Enable/Disable adapter</li> <li>• Access Adapter Properties</li> <li>• Access Port Properties for the port where the adapter last connected</li> <li>• Go to the Adapters tab and display the adapter for this host</li> </ul>

## Host Properties

The Host Properties view provides access to detailed information about a single host. From this view you can access the associated user's properties by clicking on the User option in the menu on the left or the associated adapter's by clicking on the adapter's physical address displayed in the Adapters tab at the bottom of the window.

### Access Host Properties:

1. Select **Hosts > Host View**.
2. Search for the appropriate Host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Host Properties**.

**General**

Host Name

Hardware Type

Operating System

Serial Number

Host Status      Enable  Disable

**Time**

Expiration Date      09/14/12 12:00 AM EDT     

Inactivity Date

Inactivity Limit      5 days

Created      08/30/12 08:59 AM EDT

Last Connected      08/29/12 12:22 AM EDT

**Policy Agent/Access**

Role     

Agent Version      2.2.5.4     

Security and Access Attribute Value

Adapters
Applications
Notes
Health
Patch Management
Logged In Users

Type	Name	Status	Actions
Admin	Guest No Access	<input style="border: 1px solid gray; width: 50px;" type="text" value="Initial"/>	
Agent	Agent_Install	<input style="border: 1px solid gray; width: 50px;" type="text" value="Success"/>	<input type="button" value="ReScan"/>
Agent	OS-Anti-Virus-Check	<input style="border: 1px solid gray; width: 50px;" type="text" value="Success"/>	<input type="button" value="ReScan"/>

Send Message

Groups

Apply

Reset

Figure 133: Host Properties

## Host Properties Field Definitions

Field	Definition
<b>General</b>	
<b>Host Name</b>	Machine name of the host.
<b>Hardware Type</b>	Type of machine such as workstation.
<b>Operating System</b>	Operating system installed on the host. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
<b>Serial Number</b>	Serial number of the host.
<b>Host Status</b>	Radio buttons indicating whether the host is Enabled or Disabled. To enable or disable the host, click the appropriate button and then click Apply.
<b>Time</b>	
<b>Created</b>	Indicates when this host record was created in the database. Options include Before, After, and Between.
<b>Expiration Date</b>	Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. If Never is displayed, this indicates that the host will not age out of the database. To modify click Set. See <b>Set Host Expiration Date</b> on page 366.
<b>Inactivity Date</b>	<p>Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. The date is continuously recalculated based on the number of days entered for Inactivity Limit.</p> <p>For example, if the host logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the host logs back in again, the Inactivity Date is blank until the next time it logs out. Then the value is recalculated again. To modify click Set.</p>
<b>Inactivity Limit</b>	Number of days the host must remain continuously inactive to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Last Connected</b>	Last time the host was heard on the network. Options include Before, After, Between, and Never.
<b>Policy Agent/Access</b>	
<b>Role</b>	Role assigned to the host. Use the drop-down list to select a new role.
<b>Agent Version</b>	<p>The version number of the Persistent or Dissolvable Agent installed on the host machine.</p> <p><b>Note:</b> "None" is displayed if the host has registered or been rescanned with a Dissolvable Agent version that is prior to V 2.1.0.X or if this host is part of a group with an Endpoint Compliance Policy set to by-pass the agent scan.</p>

Field	Definition
<b>Update Button</b>	Button only displays if the Persistent Agent is installed. Allows you to update this host to a different version of the Persistent Agent.
<b>Security And Access Attribute Value</b>	<p>The <b>value</b> of the attribute that can be used as a filter in User/Host Profiles. Data for this field can come from a guest template, can be entered automatically from an LDAP Directory based on attribute mappings or manually by typing a value in this field. If entered from a directory, the data is copied from the user record of the associated user. See <b>Add/Modify Directory - User Attributes Tab</b> on page 76.</p> <p>For example, if you have a policy for staff and a separate policy for executives, you could enter the word <b>staff</b> for each staff member and <b>executive</b> for each member of the executive group. Enter a matching word on the appropriate User/Host Profile to match the host to an Endpoint Compliance or Network Access Policy. See <b>Policies</b> on page 505.</p>
<b>Tabs</b>	
<b>Adapters</b>	Displays a list of adapters on this host by MAC address. Click on a MAC address to open the Adapter Properties.
<b>Applications</b>	Displays a list of applications installed on the device. This information is provided by the agent. Typically includes Anti-spyware, Anti-virus, Hotfixes and operating system. This information is updated with each successful scan.
<b>Notes</b>	Notes entered by the administrator. If this host is the registered host for a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
<b>Health</b>	Lists all the Scans and System scripts, and Administrative states for which the host machine has been scanned or had applied. Each scan the host is eligible for is shown along with the Name, Status, and Action. Click <b>Show History</b> for short-term historical data. See <b>Host Health And Scanning</b> on page 339.
<b>Patch Management</b>	Displays information on patches that have been applied to the host machine by its associated Patch Management server. The Patch Management Vendor name and the ID number of the most recent patch is displayed.
<b>Logged In Users</b>	User name of the user logged into this host.
<b>Buttons</b>	
<b>Send Message</b>	Opens the Send Message window and allows you to send a message to a host. If the host has the Persistent Agent or Bradford Mobile Agent for Android installed, the message can be sent to the host desktop.
<b>Groups</b>	Displays a list of available host groups. If the host is a member of a group the check box is selected. You may add or remove the host from one or more groups.
<b>Apply</b>	Saves changes to the Host Properties.
<b>Reset</b>	Resets the values in the Host Properties window to their previous settings. This option is only available if you have not clicked Apply.

## Host Health And Scanning

Host health is determined by the Endpoint Compliance Policies, System and Administrative states or scans run on the host. Each time a scan is run a record of that scan is stored in the database and displayed on the Health tab of the Host Properties window. Each scan and scan type the host is eligible for is shown along with the Name, Status, and Action. The Agent scan shown in bold text and highlighted with a gray bar indicates the scan that is currently applied to the host. Click **Show History** for short-term historical data.

When multiple scans exist in a host record in Host Health, the combination of the Status fields can affect whether or not the host is allowed on the network or is placed in remediation. In Network Sentry versions lower than Version 6.1, failing any scan would prevent the host from accessing the network, even if that scan no longer applied.

For example, assume an Administrator created an Endpoint Compliance Policy for all Accounting Staff and selected Scan A for that Policy. Accounting Staff would connect to the network, and be scanned using Scan A. Some hosts would fail and others would pass. If the Administrator then changed the scan associated with the Policy to Scan B, hosts that had failed Scan A would never be able to access the network even if they had passed Scan B. The failure of Scan A would prevent network access. In addition, those hosts would not be able to rescan for Scan A and it would remain a Failed scan permanently.

In Versions 6.1 and higher that is no longer true. Using the example above, the results of Scan A would no longer affect the host because the Endpoint Compliance Policy that now applies to the host uses Scan B. However, failing an Admin or System Scan would still prevent network access. Refer to the table below for the effects of the Status fields on network access in Version 6.1 and higher.

Scan Type/Status				Network Access
Admin	System	Agent Scan A	Agent Scan B*	
Initial	Initial	Failure	Initial	No. Must pass scan B.
Initial	Initial	Failure	Success	Yes
Failure	Initial	Failure	Success	No. Must pass Admin Scan.
Success	Failure	Failure	Success	No. Must pass System Scan.
Success	Success	Failure	Success	Yes

\*Agent Scan B is the scan that currently applies to the host in the example in the table.

### Access The Health Tab

1. Select **Hosts > Host View**.
2. Search for the appropriate Host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Host Properties**.
5. Click on the **Health** tab.

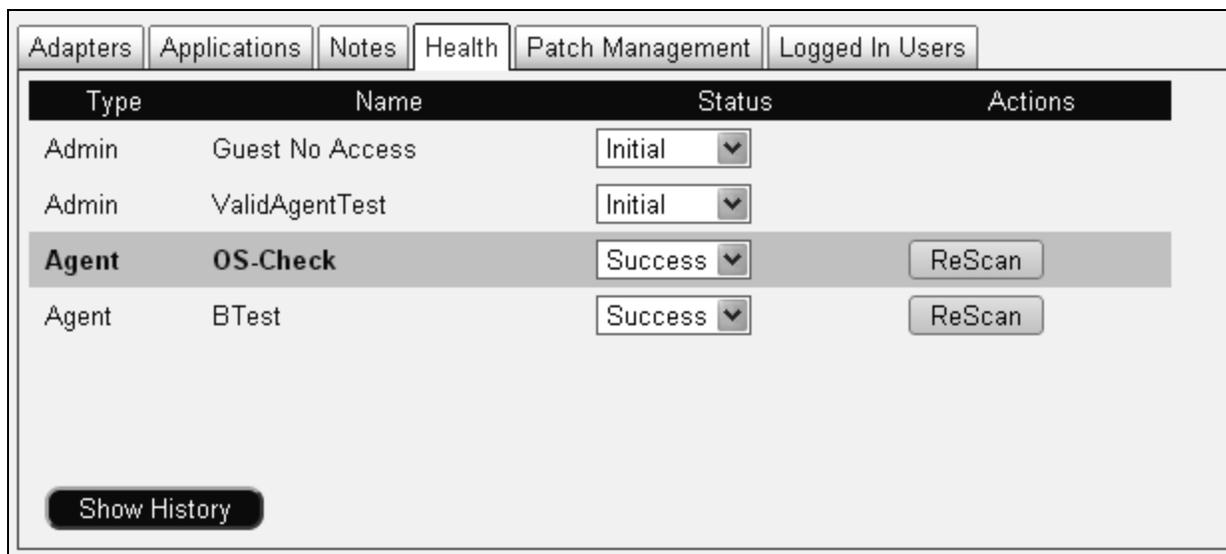


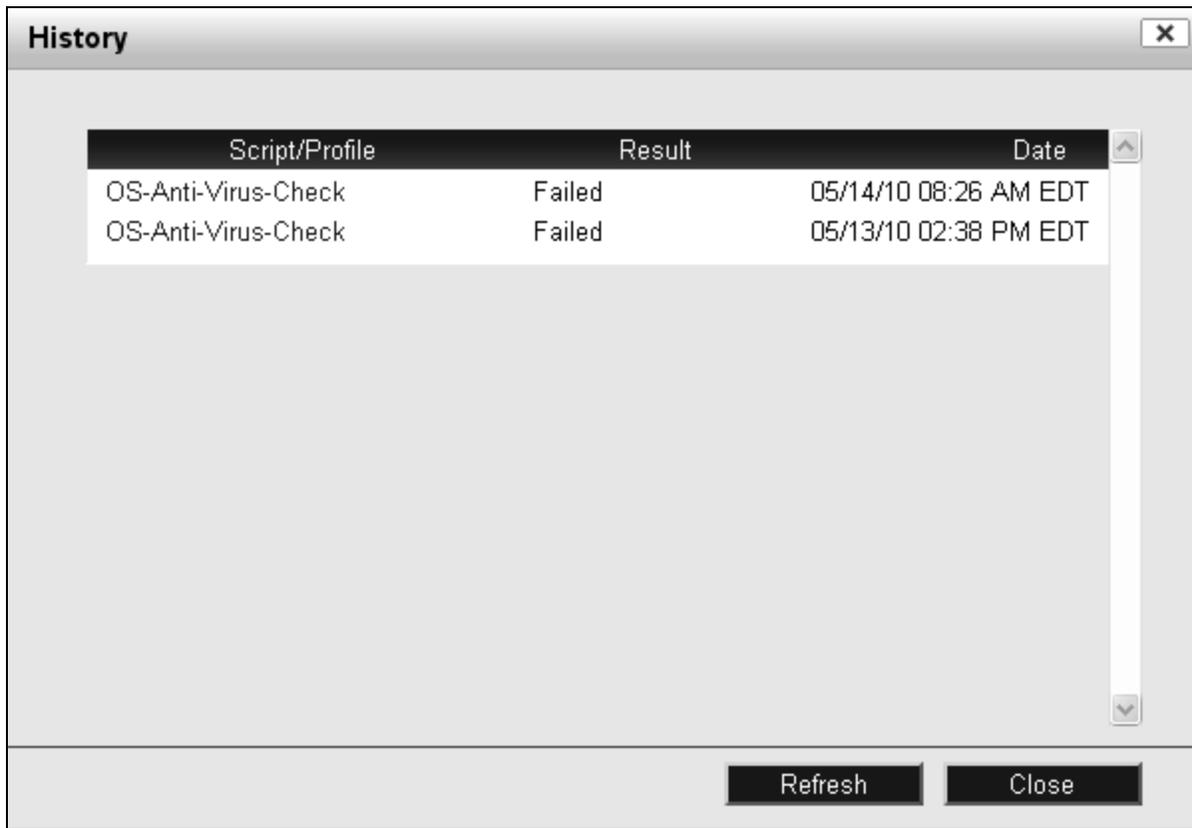
Figure 134: Host Properties - Health Tab

## Health Tab Field Descriptions

Option	Description
<b>Type</b>	<p><b>Admin</b> — Indicates the reason why a host was manually marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans can be used to mark hosts At Risk or Safe based on an alarm action triggered by an event. These scans can also be used to enable or disable access based on the time of day, for example to limit access for guests after 5:00 pm.</p> <p><b>System</b> — These scans run scripts on the Network Sentry platform.</p> <p><b>Agent</b> — Scans run by an agent installed on the host based on an Endpoint Compliance Policy or set of requirements with which the host must comply. The Agent scan listed in bold and highlighted by a gray bar indicates the scan that is currently applied to the host.</p>
<b>Name</b>	The Name of the scan. There may be more than one scan of a particular type that the host is eligible to be scanned against.
<b>Status</b>	<p><b>Initial</b>—Default setting indicating that the host has not been scanned, therefore it has neither passed nor failed. For Admin scans, manually setting the scan to Initial is the equivalent of Success. For other scan types, setting the status to Initial has no effect.</p> <p><b>Failure</b>—Indicates that the host has failed the scan. This option can also be set manually. When the status is set to Failure the host is marked "At Risk" for the selected scan.</p> <p><b>Failure Pending</b>—The host has been scanned and failed a scan that has the Delayed Remediation option enabled. The host is not placed in remediation and it is marked "Pending At Risk". See Delayed Remediation For Scanned Hosts on page 553 for additional information.</p> <p><b>Success</b>—Indicates that the host has passed the scan. This option can also be set manually. When the status is set to Success the host is marked "Safe" for the selected scan.</p>
<b>Actions</b>	<p>The ReScan button appears in the Actions column for Agent scans. Clicking the ReScan button places the host into the queue to be re-scanned.</p> <p>If Network Sentry cannot contact the host when the ReScan button is clicked, a message is displayed indicating that the host was not rescanned.</p>

**View History**

Displays a recent history of scans and details of each scan.



**Figure 135: Health Tab - History**

1. On the Host Properties Health tab, click **Show History**.
2. View the list of scans, results, and when the scan(s) were performed. Results are sorted with the most recent at the top of the list. Note that if there are no Admin, System, or Endpoint Compliance Policy scan results to display when you click History, the History window opens with the message, "There are no scan results for this host."
3. Inside the History window, click the **Script/Profile name** to view the details of the scan. The details view opens in a new browser window.

Date	05/14/10 08:26 AM EDT	Scan ID	171
Test Result	Failed	Host Name	dulcimer
Policy Name	OS-Anti-Virus-Check		
OS	Windows Vista (TM) Business 6.0 Service Pack 2		
Detected Physical Addresses			
Physical Address	ID		
00:19:D1:94:5C:06	Intel(R) 82566DM Gigabit Network Connection		
Test Results			
Category	Name	Result	
Anti-Spyware	Avast! Anti-Spyware (4.8 and Later)	Failed	
Anti-Spyware	AVG-8.0	Failed	
Anti-Spyware	AVG-8.0 Definitions	Failed	
Anti-Virus	AVG-8.0	Passed	
Anti-Virus	AVG-8.0 Definitions	Passed	
Operating-System	Windows Vista x64	Passed	
Operating-System	Vista x64 Service Pack	Passed	
Operating-System	Windows Vista x64 Edition	Passed	
Operating-System	Vista x64 Critical and Security Updates	Passed	
Operating-System	Windows Vista x64 AutoUpdates Label	Passed	

**Figure 136: Health Tab - History - Scan Details**

4. Close the scan details window.
5. Click **Refresh** on the History view to refresh the list with the most recent data.
6. Close the window when finished.

Modify a Host

Hosts records are created as hosts connect to the network and register. Hosts can be added by importing or by entering the data manually. Modify Host allows you to create new hosts or edit existing ones. Hosts added through this process are either registered to a user or registered as a device.

**Host Registered To A User**

A host registered to a user is associated with that user, inherits network access parameters from the user and contributes to the Allowed Hosts count for the user. Each registered device or host consumes one license when it is online. If the host is registered here, the user will not have to go through the registration process elsewhere, such as the captive portal.

**Modify Host**

Register Host to User     Register Host as Device

User ID:

Use Role From User     Specify Role:

Contractor

Host Name:     Hardware Type:

Serial Number:     Operating System:

Device Type:

Notes:

Security and Access Attribute Value:

Adapters		
Physical Address	Media Type	Description
00:EB:D5:10:37:E0	Unknown	

Figure 137: Modify Host - Register To User

**Note:** Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows or Mac.

### Host Registered As A Device

A host registered as a device can be displayed in the Host View. This type of host consumes license only when it is online. Typically hosts registered as devices are items such as IP phones, security cameras, alarm systems or printers.

**Modify Host**

Register Host to User
  Register Host as Device

Create in: Host View

Role:

Host Name: AP00EB-D510-37E0 Hardware Type:

Serial Number:  Operating System:

Device Type: Registered Host

Notes:

Security and Access Attribute Value:

Adapters		
Physical Address	Media Type	Description
00:EB:D5:10:37:E0	Unknown	

Add Modify Delete

OK Cancel

Figure 138: Modify Host - Register As Device

**Modify Host**

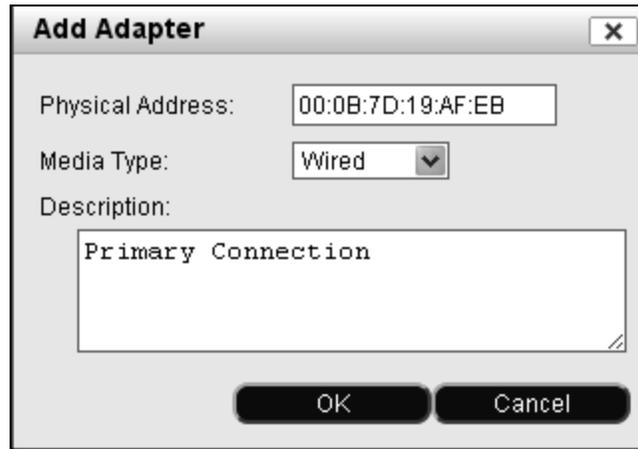
1. Select **Hosts > Host View**.
2. Use the search or filter mechanisms on the Host View to locate the appropriate host.
3. Click on the host to select it.
4. Click the **Modify** button.
5. See the field definitions table below for detailed information on each field.
6. Click **OK** to save your data.

**Modify Host - Field Definitions**

Field	Definitions
<b>Register Host To User</b>	
<b>User ID</b>	<p>ID of the user who owns this host. As you type a list of matching user IDs drops down. For example if you type ab, user IDs that start with ab are displayed. If the user ID does not exist in the database, but does exist in the directory used to authenticate users, the user is created at the same time. If the user does not exist either in the directory or in your database, you cannot save the host.</p> <p>If registering this host to a User exceeds the number of Allowed Hosts for that user, a message is displayed indicating that Allowed Hosts has been automatically incremented and the host is registered to the user.</p>
<b>Register Host As Device</b>	
<b>Create In</b>	Indicates where the device should be displayed. Options include Host View or Host View And Topology View.
<b>Container</b>	If the host is created in both Host View and Topology View, you must choose a Topology View container to contain the host. Containers in Topology are used to group devices.
<b>General</b>	
<b>Role</b>	<p>Roles are attributes of hosts and users that can be used as filters in User/Host Profiles.</p> <p>If the host is registered to a user, there are two options for selecting the host role.</p> <p><b>Use Role From User</b> — Indicates that the host role is inherited from the registered user associated with the host.</p> <p><b>Specify Role</b> — Indicates that the host role is manually selected. This enables a drop-down list of possible roles from which you can choose.</p> <p>If the host is registered as a device in Topology View only, its role is used to control network access or can be used to apply a CLI configuration. For example, a CLI configuration could be used to reduce the baud rate of a device when it connects to the network.</p>

Field	Definitions
<b>Host Name</b>	Machine name of the host being registered.
<b>Hardware Type</b>	Type of hardware such as Printer, Server or Workstation.
<b>Serial Number</b>	Serial number on the device. May be of assistance if the device is ever stolen.
<b>Operating System</b>	Operating system on the host, such as Windows XP or MAC OS X.
	<b>Note:</b> Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
<b>Device Type</b>	<p>Indicates the type of device being registered. When registering a host to a user this field defaults to Registered Host. It could also be set to a gaming or mobile device. When registering as a device, this might be set to devices that are not typically associated with an owner, such as a printer or an alarm system. An icon representing the device selected displays beside the Device Type field.</p> <p>If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.</p>
<b>Notes</b>	Free form notes entered by the Administrator.
<b>Security and Access Attribute Value</b>	This value can be included in a filter when determining the Security Policy that should scan this host when it connects to the network. If a directory is in use and a user is associated with this host, the value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
<b>Adapters</b>	<p>Lists the adapters or network interfaces that exist on this host. By listing all adapter's on the host here, you establish that these adapters are siblings. Number of adapters per host is limited to <b>five</b>. See Edit Adapters below.</p> <p><b>Physical Address</b> — MAC Address of the adapter</p> <p><b>Media Type</b> — Indicates whether the adapter is wired or wireless.</p>

### Edit Adapters



**Figure 139: Add Adapter**

1. Go to the Adapter section of the Add or Modify Host Window.
2. **To Add an Adapter:** Click the **Add** button and provide the **Physical Address** and the **Media Type**, such as wired or wireless.
3. **To Modify an Adapter:** Select an Adapter and click the Modify button. Change the Media Type as needed. To change the Physical Address you must delete the adapter and add it again.
4. **To Delete an Adapter:** Click on the Adapter to select it and click **Delete**.
5. Click **OK** to save.

**Note:** The number of adapters per host is limited to five.

## Delete A Host

This option deletes the selected host(s) from the Host View.

**Note:** Deleting a host from the Host View that is also displayed in the Topology View, removes that host from both views. Deleting a host from the Topology View does not delete it from the Host View.

**Note:** If a device has been detected as a Rogue host and then later manually entered as a device, the Rogue host record remains in the database. It is important to remove the corresponding Rogue host record so there is no conflict between the two records with the same MAC address.

1. Select **Hosts > Host View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Host(s).
3. Select the hosts to be deleted.
4. Click **Delete** at the bottom of the Host View.

### Enable Or Disable Hosts

Use this option to disable or enable hosts. A message window appears indicating the successful disabling or enabling of the host. When a host is disabled all of its adapters are disabled.

1. Select **Hosts > Host View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Host(s).
3. Select the hosts to be enabled/disabled.
4. Click either **Enable** or **Disable** at the bottom of the Host View.

Enabling and disabling hosts can be automated using events and alarm mappings. Specific events, such as, Possible MAC Address Spoof, can be mapped to an alarm that has the action "Disable Hosts" configured. See **Add or Modify Alarm Mapping** on page 497.

## Add IP Phones

IP phones can be added using one of the following methods:

- Connect your phones to the network and then convert the rogue hosts to IP phones using the Register As Device tool. See **Register A Host As A Device** on page 364.
- Connect your phones to the network and use the Device Profiler feature to automatically register them as IP Phones. See **Device Profiler** on page 189.
- Add a new host in the host view and choose Register As A Device in the Add window, then select IP Phone as the device type. See **Modify a Host** on page 344.

### Policy Details

Policy Details assesses the selected host or user and displays the specific profile and policies that apply to the host at the moment the dialog was opened. User/host profiles have a time component and hosts may be connected at different locations. Therefore, the profile and policy displayed in Policy Details now, may be different than the profile and policies that display tomorrow. Policies displayed in this view include: Network Access Policies, Endpoint Compliance Policies, Supplicant Policies and Portal Policies. Each type of policy is displayed in a separate tab that also contains a Debug Log. This log can be sent to Customer Support for analysis.

To access Policy Details from Host View:

1. Select **Hosts > Host View**.
2. Search for the appropriate Host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.

To access Policy Details from User View

1. Select **Users > User View**.
2. Search for the appropriate User.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.

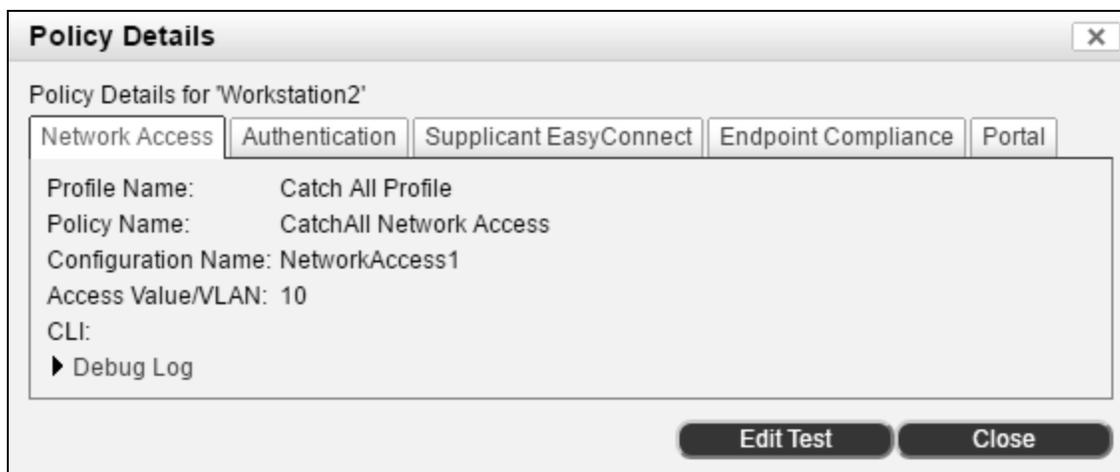


Figure 140: Policy Details - Network Access Tab

### Network Access Tab Field Definitions

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Network Access Policy that currently applies to the host.
<b>Configuration Name</b>	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host.
<b>Access Value/VLAN</b>	The specific network access that would be provided to the host, such as a VLAN ID or Name.
<b>CLI</b>	Name of the CLI Configuration that currently applies to this host or the connection port. This field may be blank.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

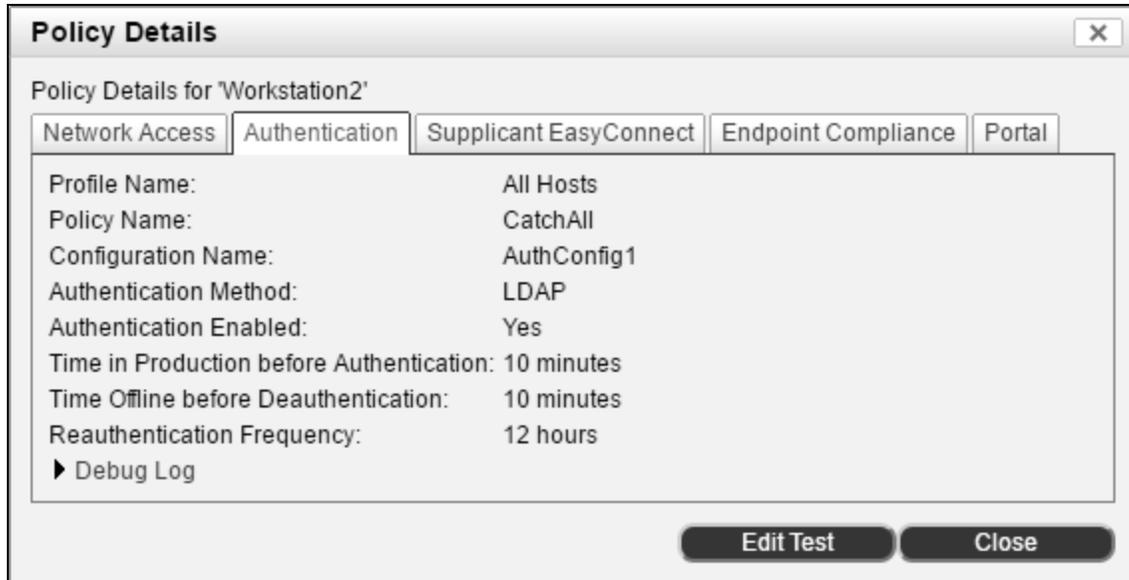


Figure 141: Policy Details - Authentication Tab

**Authentication Tab Field Definitions**

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Network Access Policy that currently applies to the host.
<b>Configuration Name</b>	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host.
<b>Authentication Method</b>	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
<b>Authentication Enabled</b>	Indicates whether Authentication is enabled. When enabled, the user is authenticated against a directory, the Network Sentry database, or a RADIUS server when logging on to access the network.
<b>Time in Production before Authentication</b>	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the Authentication VLAN.

Field	Definition
<b>Time Offline before Deauthentication</b>	Once the machine is offline, the user remains authenticated for this period of time. If the machine comes back online before the time period ends the user does not have to reauthenticate. If the machine comes back online after the time period ends, the user is required to re-authenticate.
<b>Reauthentication Frequency</b>	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

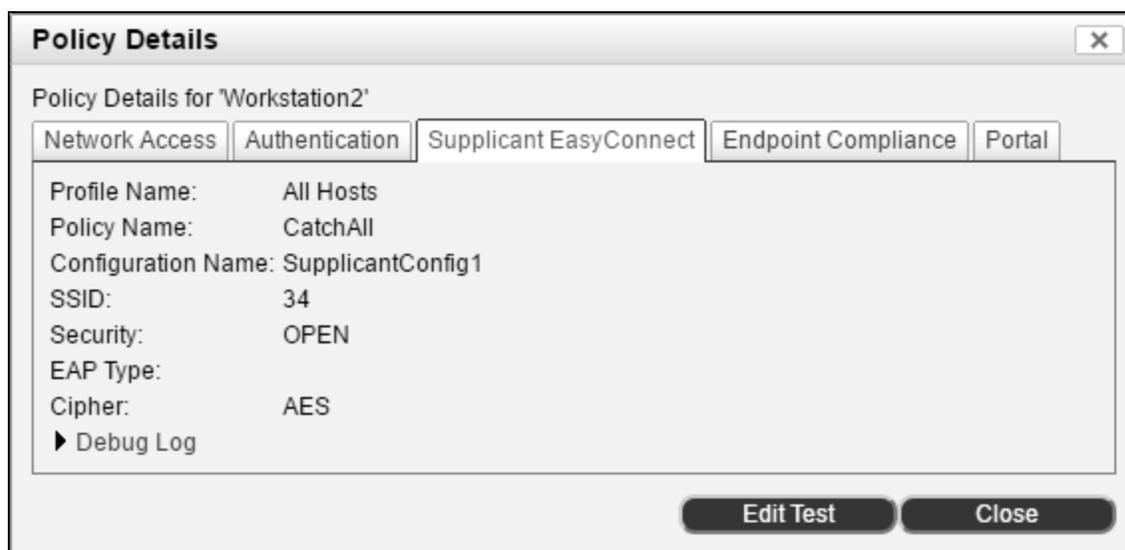


Figure 142: Policy Details - Supplicant EasyConnect Tab

### [Supplicant EasyConnect Tab Field Definitions](#)

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Supplicant Policy and Supplicant Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the most recent Supplicant Policy that currently applies to the selected host.
<b>Configuration Name</b>	Name of the configuration that applies to the selected host. This is the configuration for the supplicant on the host to allow access on a particular SSID.

Field	Definition
<b>SSID</b>	Name of the SSID for which the supplicant is being configured.
<b>Security</b>	Type of encryption that used for connections to this SSID, such as WEP or WPA.
<b>EAP Type</b>	Currently only PEAP is supported. Not always required. This field may be blank.
<b>Cipher</b>	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

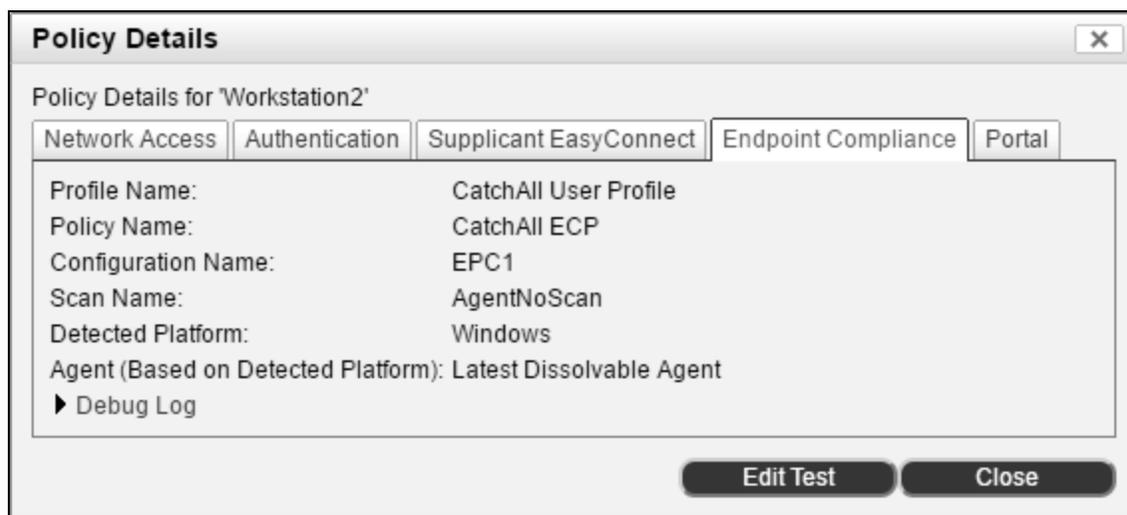


Figure 143: Policy Details - Host View - Endpoint Compliance Tab

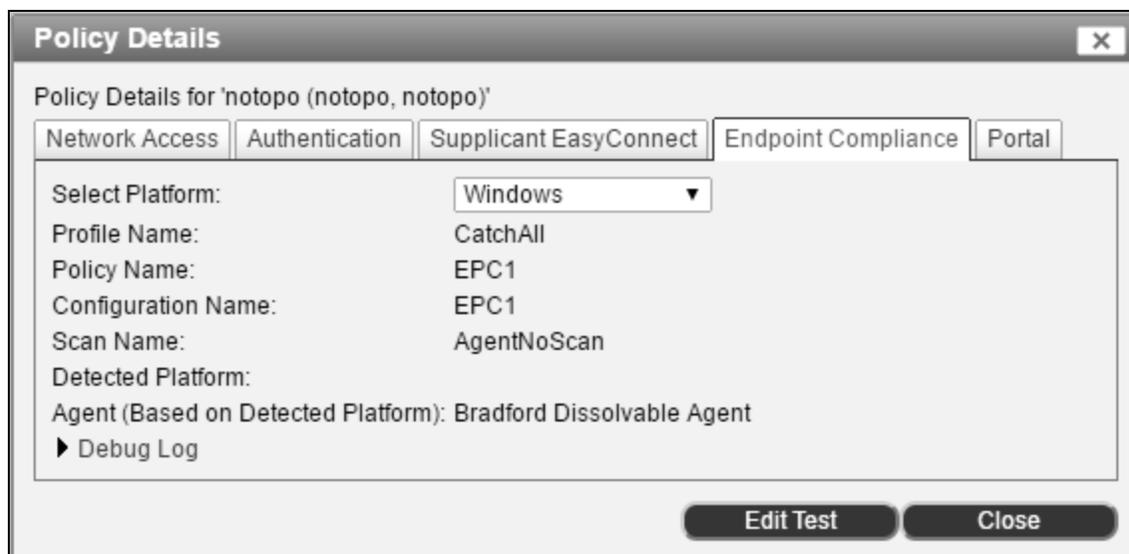


Figure 144: Policy Details - User View - Endpoint Compliance Tab

### Endpoint Compliance Tab Field Definitions

Field	Definition
<b>Select Platform</b>	<p>When the Policy Details option is selected from the User View, you must select the Platform of the device that the user anticipates connecting to the network. The platform is used to determine the agent that would be assigned to the host.</p> <p>Not all platforms are displayed here. Only the platforms that support the Persistent or Mobile Agents.</p>
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Endpoint Compliance Policy and Endpoint Compliance Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Endpoint Compliance Policy currently applies to the selected host. See Endpoint Compliance Policies on page 525.
<b>Configuration Name</b>	Name of the configuration that currently applies to the selected host. This is the configuration for the Scan and Agent for the host. See Endpoint Compliance Configurations on page 536.
<b>Scan Name</b>	Name of the scan that would be used to evaluate this host. See Scans on page 545.
<b>Detected Platform</b>	The device type, such as iPhone or Android, that Network Sentry thinks the host is, based on the information currently available in the system.
<b>Agent</b>	Agent setting that would be applied to the host. Determines whether or not an agent is used and which agent is required. Agent settings are selected in the Endpoint Compliance Configuration.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.



Figure 145: Policy Details - Portal Tab

**Portal Tab Field Definitions**

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location. Host connections that match the criteria within the User/Host Profile are assigned the associated Portal Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Portal Policy that was applied to the host.
<b>Configuration Name</b>	Name of the Portal Configuration that applied to the host.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

## Add Hosts To Groups

You can add selected host(s) to groups you have created. See **Groups View** on page 681 for detailed information on Groups and how they are used in Network Sentry. Only registered hosts can be added to groups.

IP phones have a special group type and can only be added to IP phone groups. If you select IP phones with other registered hosts you will not be allowed to use the **Add Hosts To Groups** option. Select IP Phones separately. Only IP Phone groups will be displayed.

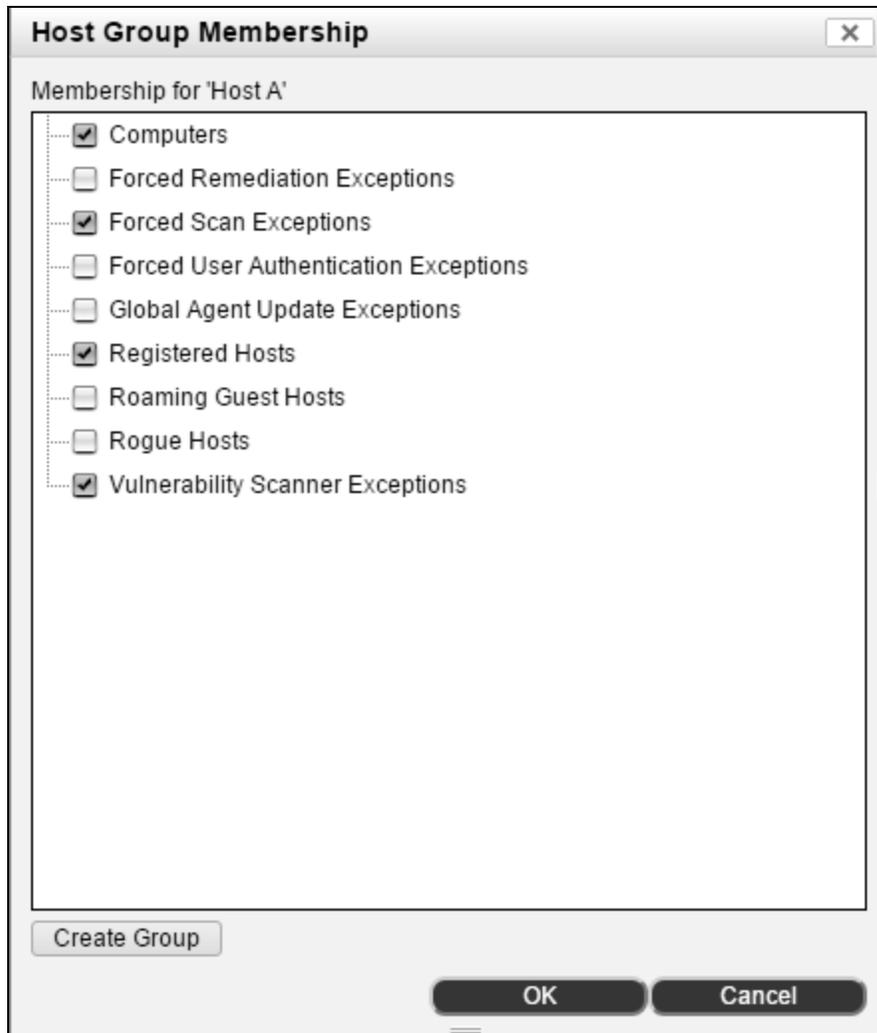


Figure 146: Add Hosts To Group

1. Select **Hosts > Host View**.
2. To select host(s) with specific parameters use the Custom Filter to set the criteria.
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the Options button and select **Add Hosts To Groups**.
5. The Group Membership view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups.
6. **To add the hosts to a group**, click the box next to the group name and then click **OK**.
7. **To create a missing group**, click the **Create Group** button.  
Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.

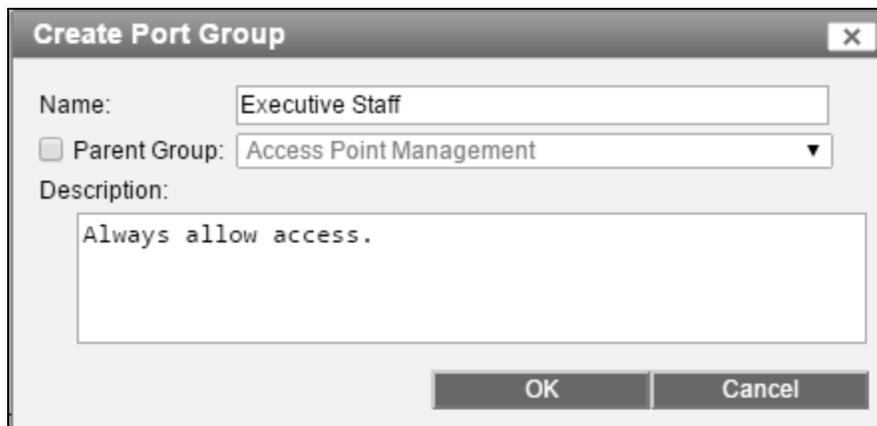


Figure 147: Create Port Group

8. Click **OK**.

## Host Group Membership

From the Host View window you can view or modify the group membership of an individual host. Use this option to open a window that displays a list of all groups to which the selected host belongs.

IP phones have a special group type and can only be added to IP phone groups. If you select an IP phone only IP Phone groups will be displayed.

1. Select **Hosts > Host View**.
2. To select host(s) with specific parameters use the Custom Filter to set the criteria.
3. Click on a host to select it.
4. Right-click or click the Options button and select **Group Membership**.

**Note:** The Group Membership option displays only for Registered Hosts.

5. The Group Membership view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this host is contained in that group.
6. **To add the host to a group**, click the box next to the group name and then click **OK**.
7. **To remove the host from a group**, click to uncheck the box next to the group name and then click **OK**.

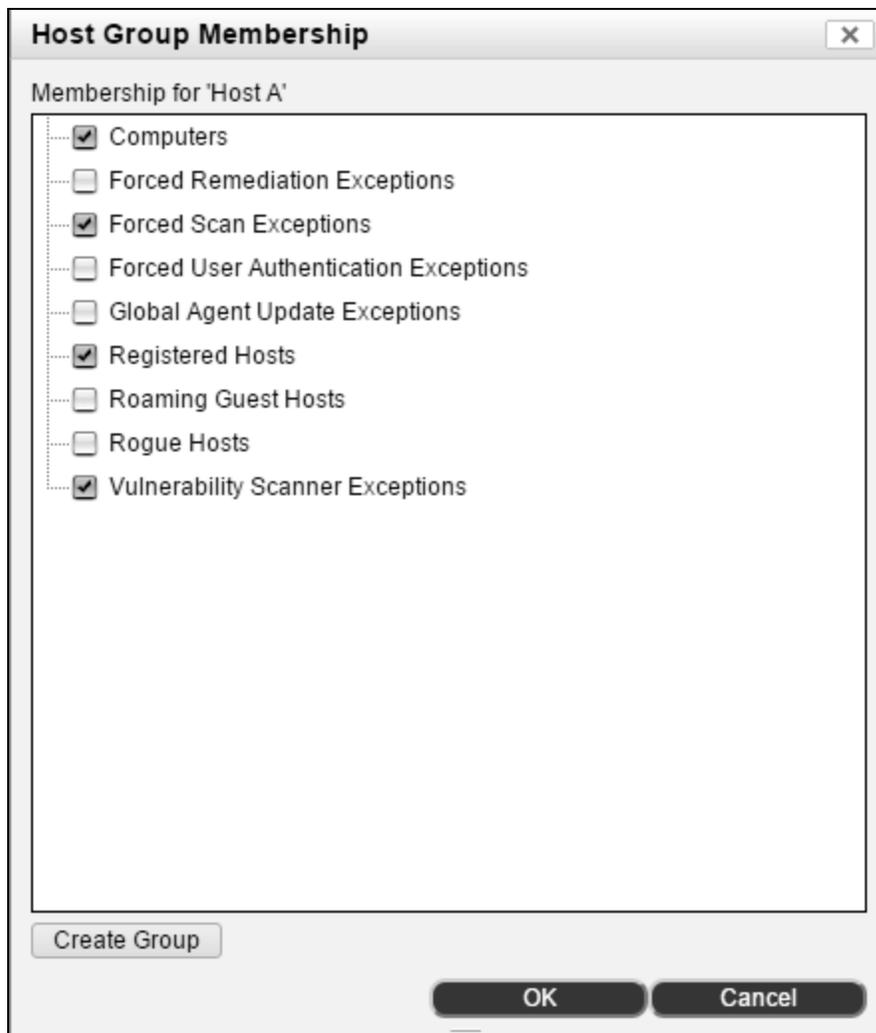


Figure 148: Group Membership View

8. **To create a missing group**, click the **Create Group** button.

Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.

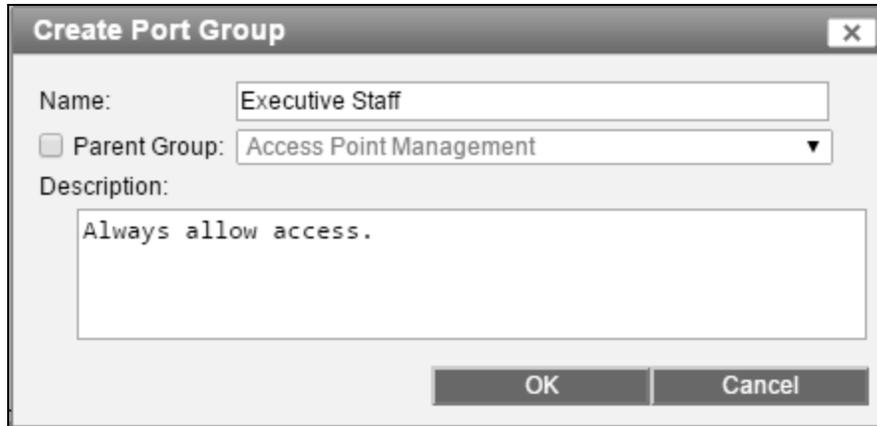


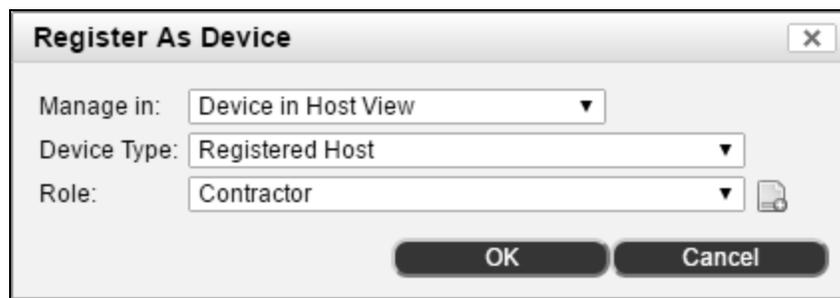
Figure 149: Create Port Group

9. Click **OK** to save your group selections.

## Register A Host As A Device

Devices such as printers, lab machines, and servers that have not been placed in the Topology but are connected to managed switches, are created as rogue hosts. If rogue hosts are denied access to the network, they are disabled. Use this option to prevent rogue hosts from being denied access to the network by registering them.

If you select more than one device on the Host View, the IP Address and Physical Address fields will not display on the Register As Device window. If multiple devices are selected and those devices do not have IP Addresses, you will not be able to place them in the Topology View using the Register As Device option. You can place those devices in the Host View using the Register As Device option.



**Figure 150: Register As Device**

A host can be registered as a device from the Host View based on the rogue host record or from the Adapter View based on the adapter record.

1. Select **Hosts > Host View** or **Hosts > Adapter View**.
2. Use the Quick Search or Custom Filter to locate the appropriate record.
3. Click the record to select it. Right-click or click Options and select **Register as Device**.
4. Click **Manage In** and select where this device should be placed. Options include:

**Device in Host View**—device is kept in Host View allowing you to track connection history and can be associated with a user.

**Device in Topology**—device is moved to Topology and removed from Host View. Device can be polled and contact status can be monitored.

**Device in Host View and Topology**—device is shown in both the Host View and Topology View. You can track connection history and it can be associated with a user, but it cannot be polled.

**Note:** If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.

5. Click **Device Type** and select a type from the drop-down list. The icon associated with the selected device type displays to the right of the drop-down list.
6. Click **Role** and select a role from the drop-down list. Roles are configured on the Roles View. See **Role Management** on page 609.
7. Select the **Container** for the device from the drop down list. This is where the device will display in the Topology view. This field is disabled if the device is not being managed in the Topology view.
8. Enter the **IP Address** for the device. IP Address is required for devices being managed in the Topology view.

This field does not display if the Manage In field is set to something other than Device In Topology or if you have selected more than one device. If you have selected more than one device and those devices do not already have IP Addresses you cannot add them to the Topology View.

9. The **Physical Address** field is read-only and displays only when one of the Topology View options is selected in the Manage In field.
10. Click **OK**.

Set Host Expiration Date

The expiration date on a host determines when it is automatically deleted or aged out of the database. Aging out of the database can be triggered by an expiration date, the amount of time the host has been inactive or both. There are many methods for setting an Expiration date. See **Aging Out Host Or User Records** on page 381 for information on other methods.

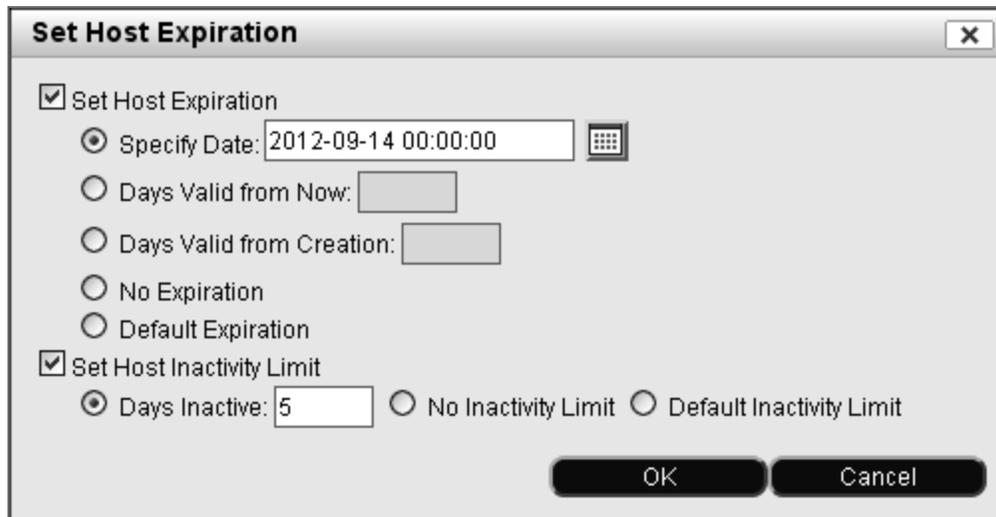


Figure 151: Set Host Expiration

The Set Host Expiration Date feature is used from the Host View.

1. Select **Hosts > Host View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Host(s).
3. Select the hosts to be modified.
4. Right-click or click Options and select **Set Host Expiration**.
5. Use the field definitions table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Set Host Expiration Field Definitions

Field	Definition
Set Host Expiration	Enables the expiration date option and corresponding calculation methods.

Field	Definition
<b>Specify Date</b>	<p>Allows you to select a specific date that the host will be aged out of the database.</p> <p><b>Note:</b> Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.</p>
<b>Days Valid From Now</b>	Enter the number of days from today that you would like the host to expire. The expiration date is calculated based on this number.
<b>Days Valid From Creation</b>	This is the number of days from the date the host record was created. The expiration date is calculated based on this number.
<b>No Expiration</b>	This host is never deleted from the database even if global or group aging options are added or modified.
<b>Default Expiration</b>	Defaults to the global aging settings configured in <b>System &gt; Settings &gt; User/Host Management &gt; Aging</b> .
<b>Set Host Inactivity Limit</b>	Enables the option to delete a host based on the number of days that it did not log onto the network.
<b>Days Inactive</b>	Number of consecutive days the host must be inactive to be aged out of the database. For example, if this is set to 4 days, and after 2 days the host connects to the network again, the counter is restarted.
<b>No Inactivity Limit</b>	With this option enabled, the host is never deleted from the database due to inactivity even if global or group aging options are added or modified.
<b>Default Inactivity Limit</b>	Defaults to the global aging settings configured in <b>System &gt; Settings &gt; User/Host Management &gt; Aging</b> .

## Adapter View

The Adapter View is part of a window that includes menu options for Users, Adapters, Hosts, and Applications. Use the Adapter View to locate and manage adapters connected to your network.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Hover over the icon in the Status column to display a tool-tip with detailed information about this adapter. For field definitions see **Adapter View And Search Field Definitions** on page 372. For information on Status icons see the **Icon Key** on page 14.

The **Displayed** and **Total** fields in the title bar represent the number of records displayed versus the total number of records in the database. Data in some tables, such as Users, is refreshed periodically but is not re-sorted based on the new data until you close and reopen the view or click a column heading.

The screenshot shows a window titled "Adapters - Displayed: 20 Total: 20". It features a search bar and a table with the following columns: Status, Server, Host Status, IP Address, Physical Address, All IPs, Location, Media, Access Value, and Vendor Name. The table contains 20 rows of data, each representing a network adapter. The status column contains icons, and the vendor name column lists various manufacturers like Intel, Cisco, and Dell.

Status	Server	Host Status	IP Address	Physical Address	All IPs	Location	Media	Access Value	Vendor Name
[Icon]	primary.bradfordne	[Icon]		68:05:CA:40:A9:13					Intel Corporate
[Icon]	primary.bradfordne	[Icon]		00:05:1B:A1:E1:B5		switchbc6eb3 fa5		165	Magic Control Technology Corporation
[Icon]	primary.bradfordne	[Icon]		08:00:27:05:E0:61		switchbc6eb3 fa1		65	Cadmus Computer Systems
[Icon]	primary.bradfordne	[Icon]	192.168.65.1	00:13:1A:BC:48:73	192.168.65.1 (IPv4)	switchbc6eb3 fa1		65	Cisco Systems
[Icon]	primary.bradfordne	[Icon]		E0:D1:73:BC:6E:62		switchbc6eb3 fa1		65	Cisco Systems, Inc
[Icon]	primary.bradfordne	[Icon]		08:00:27:5C:C3:D5		switchbc6eb3 fa1		65	Cadmus Computer Systems
[Icon]	primary.bradfordne	[Icon]		B4:99:BA:C9:12:00		switchbc6eb3 fa1		65	Hewlett Packard
[Icon]	primary.bradfordne	[Icon]		00:22:90:5A:5F:D7		switchbc6eb3 fa1		65	Cisco Systems
[Icon]	primary.bradfordne	[Icon]		08:00:27:D1:41:D0		switchbc6eb3 fa1		65	Cadmus Computer Systems
[Icon]	primary.bradfordne	[Icon]		98:90:96:9E:55:A0		switchbc6eb3 fa1		65	Dell Inc.
[Icon]	primary.bradfordne	[Icon]		00:22:90:E6:CF:AC		switchbc6eb3 fa1		65	Cisco Systems
[Icon]	primary.bradfordne	[Icon]		C0:7B:BC:12:EC:D7		switchbc6eb3 fa1		65	Cisco Systems, Inc
[Icon]	primary.bradfordne	[Icon]	192.168.65.100	98:90:96:9E:17:55	192.168.65.100 (IPv4)	switchbc6eb3 fa1		65	Dell Inc.
[Icon]	primary.bradfordne	[Icon]		08:00:27:5E:B2:D3		switchbc6eb3 fa1		65	Cadmus Computer Systems
[Icon]	primary.bradfordne	[Icon]		00:05:1B:A1:E3:CE		switchbc6eb3 fa1		65	Magic Control Technology Corporation

Figure 152: Adapter View

## Adapter View Navigation, Menus, Options And Buttons

For information on selecting columns displayed in the Adapter View see **Configure Table Columns And Tool-tips** on page 313. Some menu options are not available for all adapters. Options may vary depending on adapter state.

Double-click on an adapter to display Adapter Properties.

Field	Definition
<b>Navigation</b>	<p>Across the top of the Adapters tab are navigation tools that allow you to quickly move through large numbers of records. These tools include the following:</p> <p><b>&lt;&lt;first</b>—Takes you to the first page of records.</p> <p><b>&lt;prev</b>—Takes you back one page.</p> <p><b>Page Number</b>—Current page number is displayed.</p> <p><b>next&gt;</b>—Takes you forward one page.</p> <p><b>last&gt;&gt;</b>—Takes you to the last page.</p> <p><b>Drop-down Box</b>—Allows you to select the number of records to be displayed on each page.</p>
<b>Quick Search</b>	<p>Enter a single piece of data to quickly display a list of adapters. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters.</p> <p>If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.</p> <p>When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.</p>
<b>Right Mouse Click Menu Options</b>	
<b>Adapter Properties</b>	Opens the Properties window for the selected adapter. See <b>Adapter Properties</b> on page 373.
<b>Disable Adapters</b>	Disables the selected adapter(s) preventing them from accessing the network. See <b>Enable Or Disable An Adapter</b> on page 377.
<b>Enable Adapters</b>	Enables the selected adapter(s) if they were previously disabled. Restores network access.
<b>Modify Adapter</b>	Opens the Modify Adapter window for the selected adapter. See <b>Modify An Adapter</b> on page 377.

Field	Definition
<p><b>Show Audit Log</b></p>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <hr/> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p> <hr/> <p><b>Note:</b> Changes made to Hosts, Users, or Adapters are not displayed in the Admin Auditing Log. These changes are visible in the Audit Log on each server.</p>
<p><b>Enable Hosts</b></p>	<p>Enables the host(s) associated with the selected adapter(s) if they were previously disabled. Restores network access.</p>
<p><b>Disable Hosts</b></p>	<p>Disables the host(s) associated with the selected adapter(s) and all of its other adapters preventing them from accessing the network. See <b>Enable Or Disable Hosts</b> on page 350.</p>
<p><b>Host Health</b></p>	<p>Opens a dialog with the contents of the Host Health tab from the Host Properties view. See <b>Host Health And Scanning</b> on page 339.</p>
<p><b>Host Applications</b></p>	<p>Opens the Applications window for the selected host and lists installed applications. See <b>Application View</b> on page 378.</p>
<p><b>Go To Host(s)</b></p>	<p>Opens the Hosts tab and displays the hosts associated with the selected adapters.</p>
<p><b>Modify Host</b></p>	<p>Opens the Modify Host window for the host associated with the selected adapter. Applies only to registered hosts.</p>
<p><b>Register As Device</b></p>	<p>Changes the host associated with the selected adapter to a device in the Network Sentry database. See <b>Register A Host As A Device</b> on page 364.</p>
<p><b>Register As Host</b></p>	<p>Changes the Rogue host associated with the selected adapter to a registered host. Displays the Modify Host window. See <b>Modify a Host</b> on page 344.</p>
<p><b>Scan Hosts</b></p>	<p>Scans the associated host with the Security Policy that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Security Policy that most closely matches the host at the moment.</p>
<p><b>Set Host Expiration</b></p>	<p>Launches a tool to set the date and time for the associated host(s) to age out of the database. See <b>Set Host Expiration Date</b> on page 366.</p>
<p><b>Set Host Role</b></p>	<p>Assigns a role to the associated host.</p>
<p><b>Go To User(s)</b></p>	<p>Opens the Users tab and displays the users associated with the selected adapters.</p>
<p><b>Set User Expiration</b></p>	<p>Launches a tool to set the date and time for the user associated with the selected adapter to age out of the database. See <b>Set User Expiration Date</b> on page 425.</p>
<p><b>Set User Role</b></p>	<p>Assigns a role to the user associated with the selected adapter. See <b>Role Management</b> on page 609.</p>
<p><b>Buttons</b></p>	

Field	Definition
<b>Import/Export</b>	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats.
<b>Options</b>	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

Adapter View And Search Field Definitions

The fields listed in the table below are displayed in columns on the Adapter View based on the selections you make in the Settings window. See **Configure Table Columns And Tool-tips** on page 313. These fields are also used in Custom Filters to search for adapters. See **Search And Filter Options For Hosts, Adapters, Users or Applications** on page 317. Additional fields that can be displayed on the Adapter View are fields for the user or the host associated with the selected adapter. See **Host View And Search Field Definitions** on page 327 and **User View And Search Field Definitions** on page 400.

Figure 153: Custom Filters - Adapter View

Field	Definition
<b>Access Value</b>	Name or number of the Network Access identifier given to this adapter based on the state of the host and the device to which the adapter is connected, such as VLAN ID, VLAN Name or Aruba Role.
<b>Description</b>	Free form notes entered by the Administrator about this adapter.
<b>IP Address</b>	The primary IP address assigned to this adapter that is used to communicate with Network Sentry. If the adapter is offline, this is the last known IP address for the adapter. Supports both IPv4 and IPv6 addresses.
<b>All IPs</b>	All IP addresses assigned to the adapter. Supports both IPv4 and IPv6 addresses. <ul style="list-style-type: none"> <li>• For IPv6, all addresses used for IPv6 communication will be displayed.</li> <li>• For IPv4, IP addresses used for registration, remediation, isolation, etc., will be displayed along with the production IP until a L3 poll determines the single IP being used.</li> <li>• Depending on the ARP cache aging of the L3 device itself and the poll interval that Network Sentry polls it, multiple production IP addresses may be displayed simultaneously for an adapter.</li> </ul>
<b>Location</b>	Name of the switch and port where this adapter is connected to the network. If the adapter is offline, this is the last known location where the adapter connected to the network.
<b>Media Type</b>	Indicates whether this is a wired or wireless adapter.
<b>Physical Address</b>	MAC address of the adapter.
<b>Status</b>	Current or last known status is indicated by an icon. See <b>Icon Key</b> on page 14. Hover over the icon to display additional details about this adapter in a tool tip. <p><b>Connected</b> — Indicates whether host is online or offline.</p> <p><b>Access</b> — Indicates whether host is enabled or disabled.</p> <p><b>Valid Physical Address</b> — Indicates whether or not the system knows the MAC address for the adapter that has connected to the network.</p>
<b>Vendor Name</b>	Name of the Vendor that matches the Vendor OUI for this device.

## Adapter Properties

The Adapter Properties view provides access to detailed information about a single adapter. From this view you can access the associated user's properties by clicking on the User tab or the associated host by clicking on the Host tab. Adapter properties also provides access to the Device Identity tab. See **Adapter Device Identity** on page 375.

### Access Adapter Properties:

1. Select **Hosts > Adapter View**.
2. Search for the appropriate Adapter.
3. Select the adapter and either right-click or click the **Options** button.
4. From the menu select **Adapter Properties**.

General	
IP Address	192.168.4.227
Physical Address	00:1C:BF:A9:46:98
Location	Concord_Cisco_1131-2.bradfordnetworks.com VLAN 4
Media Type	Wireless
Adapter Status	Enable <input checked="" type="radio"/> Disable <input type="radio"/>

Description	
Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler <u>Miniport</u>	

Apply      Reset

Figure 154: Adapter Properties

**Table 22: Adapter Properties Field Definitions**

<b>Field</b>	<b>Description</b>
<b>IP Address</b>	IP address assigned to the adapter.
<b>Physical Address</b>	MAC address of the adapter.
<b>Location</b>	Switch and port where the adapter is connected to the network.
<b>Media Type</b>	Indicates whether this is a wired or wireless adapter.
<b>Adapter Status</b>	Radio buttons indicating whether the adapter is Enabled or Disabled. To enable or disable the adapter, click the appropriate button and then click Apply.
<b>Description</b>	Free form notes section for the Administrator.
<b>Apply</b>	Saves changes to the Adapter Properties.
<b>Reset</b>	Resets the values in the Adapter Properties window to their previous settings. This option is only available if you have not clicked Apply.

## Adapter Device Identity

The Device Identity tab displays the Physical Address, Vendor Name, and DHCP fingerprint for selected Adapter. A separate record is added every time a new fingerprint is heard for a MAC. For example, if the adapter on a host is moved from a registration VLAN to a production VLAN and as a result requests a new IP address this creates a new record. If two records are displayed for the same MAC and port, but with different OSs, the host is most likely a dual-boot machine. This generates the Device Fingerprint Changed event. This view is informational only.

Physical Address	00:1C:23:41:14:EC								
Vendor Name	Dell Inc								
5 items found, displaying all items. 1									
Learned Time	Last Heard	Host Name	Option List	Parameter List	Vendor Class	Device Type	Message Type	Operating System	
Wed Apr 11 10:37:23 EDT 2012	Wed Apr 11 13:13:33 EDT 2012	Vista-1	53,116,61,12,60,55	1,15,3,6,44,46,47,31,33,121,249,43	MSFT 5.0	Windows	DISCOVER	Vista	
Wed Apr 11 11:16:03 EDT 2012	Wed Apr 11 11:18:33 EDT 2012	Vista-1	53,61,12,81,60,55	1,15,3,6,44,46,47,31,33,121,249,43	MSFT 5.0	Windows	REQUEST	Vista	
Wed Apr 11 11:18:45 EDT 2012	Wed Apr 11 13:26:45 EDT 2012					Windows	Passive	Windows XP/2000 (RFC1323+, w/+, tstamp-) [GENERIC]	
Wed Apr 11 13:13:32 EDT 2012	Wed Apr 11 14:05:10 EDT 2012	Vista-1	53,61,50,12,81,60,55	1,15,3,6,44,46,47,31,33,121,249,43	MSFT 5.0	Windows	REQUEST	Vista	
Wed Apr 11 13:13:34 EDT 2012	Wed Apr 11 13:13:34 EDT 2012	Vista-1	53,61,50,54,12,81,60,55	1,15,3,6,44,46,47,31,33,121,249,43	MSFT 5.0	Windows	REQUEST	Vista	
Export options: CSV   Excel   XML   PDF   RTF									

Figure 155: Adapter Properties - Device Identity Tab

Field	Definition
<b>Physical Address</b>	MAC address of the host interface or adapter.
<b>Vendor Name</b>	Manufacturer of the host. This is based on the Vendor OUI.
<b>Learned Time</b>	The first time a DHCP packet was heard by Network Sentry for this Physical address. This is not the time that the host connected to the network nor is it the time the host was created in the database.
<b>Last Heard</b>	The last time a DHCP packet was heard by Network Sentry for this host. Updated every time a DHCP packet with a matching identity is heard.
<b>Host Name</b>	The machine name for this host extracted from the DHCP packet.
<b>Option List</b>	Displays a list of option numbers from the DHCP packet used to provide information about the host.

<b>Field</b>	<b>Definition</b>
<b>Parameter List</b>	Combination of parameters contained in the DHCP packet that allows Network Sentry to infer the Operating System for this host.
<b>Vendor Class</b>	Vendor Class Identifier extracted from the DHCP packet. Allows the DHCP server to return specific information based on the host's hardware type.
<b>Device Type</b>	Indicates the type of hardware detected.
<b>Message Type</b>	DHCP message type, including  <b>DISCOVER</b> — Host broadcast initial DHCP request for an IP address.  <b>REQUEST</b> — DHCP server has responded. Host requests an IP address from a specific DHCP server.  <b>Passive</b> — Generated when something about the DHCP fingerprint has changed since the last message, such as a different Operating System.
<b>Operating System</b>	Operating system of the host. If more than one record is displayed with different operating systems, this host may be a dual boot machine.

## Enable Or Disable An Adapter

Use this option to disable or enable adapters. A message window appears indicating the successful disabling or enabling of the selected adapters. If a host has more than one adapter, only the selected adapter is disabled.

1. Select **Hosts > Adapter View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Adapter(s).
3. Select the adapters to be enabled/disabled.
4. Click either **Enable** or **Disable** at the bottom of the Adapter View.

## Modify An Adapter



**Figure 156: Modify Adapter**

1. Select **Hosts > Adapter View**.
2. Search for the appropriate Adapter.
3. Select the adapter and either right-click or click the **Options** button.
4. From the menu select **Modify Adapter**.
5. The **Physical Address** field cannot be modified.
6. Click in the **Media Type** field and select either Wired, Wireless or Unknown.
7. In the description field enter any notes on this adapter.
8. Click **OK** to save your changes.

## Application View

The Application View is part of a window that includes menu options for Users, Adapters, Hosts, and Applications.

Applications for scanned hosts connected to your network appear in the Application view. As hosts are scanned, the list of applications is updated.

**Note:** You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

Name	Threat Score	Version	Vendor	Operating System	Operating System Version	Source	Threat Override	Package Name	Success
Android Live Wallpapers		4.4.4-18	com.android.wallpaper	ANDROID	4.4.4	MOBILE_AGENT		com.android.wallpaper	
Android System		4.4.4-18	android	ANDROID	4.4.4	MOBILE_AGENT		android	
Basic Daydreams		4.4.4-18	com.android.dreams.basi	ANDROID	4.4.4	MOBILE_AGENT		com.android.dreams.basi	
Bluetooth Share		4.4.4-18	com.android.bluetooth	ANDROID	4.4.4	MOBILE_AGENT		com.android.bluetooth	
Bradford MA		4.4.4-18	com.bradfordnetworks.bm	ANDROID	4.4.4	MOBILE_AGENT		com.bradfordnetworks.bm	
Bradford Networks RTR Agent		1.0	com.bradfordnetworks.rtr	ANDROID	4.4.4	MOBILE_AGENT	Trusted	com.bradfordnetworks.rtr	
Bubbles		1.0	com.android.noisefield	ANDROID	4.4.4	MOBILE_AGENT		com.android.noisefield	
COATest		3.1.1	com.motorola.motocit	ANDROID	4.4.4	MOBILE_AGENT		com.motorola.motocit	
Calculator		4.4.4-18	com.android.calculator2	ANDROID	4.4.4	MOBILE_AGENT		com.android.calculator2	
Calendar		4.4.4-18	com.android.calendar	ANDROID	4.4.4	MOBILE_AGENT		com.android.calendar	
Calendar Storage		4.4.4-18	com.android.providers.cal	ANDROID	4.4.4	MOBILE_AGENT		com.android.providers.cal	
Camera		2.3.019 (1271679-30)	com.google.android.Goog	ANDROID	4.4.4	MOBILE_AGENT		com.google.android.Goog	
Cell Broadcasts		4.4.4-18	com.android.cellbroadcast	ANDROID	4.4.4	MOBILE_AGENT		com.android.cellbroadcast	
Certificate Installer		4.4.4-18	com.android.certinstaller	ANDROID	4.4.4	MOBILE_AGENT		com.android.certinstaller	
Chrome		36.0.1985.131	com.android.chrome	ANDROID	4.4.4	MOBILE_AGENT		com.android.chrome	
Clock		3.0.0	com.google.android.desk	ANDROID	4.4.4	MOBILE_AGENT		com.google.android.desk	
Cloud Print		0.9.10	com.google.android.apps	ANDROID	4.4.4	MOBILE_AGENT		com.google.android.apps	
ConfigUpdater		4.4.4-1215936	com.google.android.conf	ANDROID	4.4.4	MOBILE_AGENT		com.google.android.conf	
Contacts		4.4.4-18	com.android.contacts	ANDROID	4.4.4	MOBILE_AGENT		com.android.contacts	
Contacts Storage		4.4.4-18	com.android.providers.cor	ANDROID	4.4.4	MOBILE_AGENT		com.android.providers.cor	
Documents		4.4.4-18	com.android.documentsui	ANDROID	4.4.4	MOBILE_AGENT		com.android.documentsui	
Download Manager		4.4.4-18	com.android.providers.dow	ANDROID	4.4.4	MOBILE_AGENT		com.android.providers.dow	
Downloads		4.4.4-18	com.android.providers.dow	ANDROID	4.4.4	MOBILE_AGENT		com.android.providers.dow	
Drive		2.0.222.39	com.google.android.apps	ANDROID	4.4.4	MOBILE_AGENT		com.google.android.apps	
Earth		7.1.3.1255	com.google.earth	ANDROID	4.4.4	MOBILE_AGENT		com.google.earth	
Email		4.4.4-18	com.android.email	ANDROID	4.4.4	MOBILE_AGENT		com.android.email	

Figure 157: Applications View

The fields listed in the table below are displayed in columns on the Application view based on the selections you make in the Settings window. See **Configure Table Columns And Tool-tips** on page 390. Most of these fields are also used in Custom Filters. See **Search And Filter Options For Hosts, Adapters, Users, or Applications** on page 394.

Field	Definition
<b>Add Filter drop-down list</b>	<p>Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. Options include:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• OS</li> <li>• OS Version</li> <li>• Package Name</li> <li>• Source</li> <li>• Threat Override (RTR only) - Select Trusted or Untrusted</li> <li>• Threat Score (RTR only) - Enter a single number or a range of numbers (e.g., 8-10)</li> <li>• Vendor</li> <li>• Version</li> </ul> <p>See <b>Filters</b> on page 59.</p>
<b>Update button</b>	Displays the filtered data in the table.
<b>Security Events</b>	
<b>Name</b>	The name of the application.
<b>Threat Score</b>	<p>The threat score assigned to the application.</p> <p><b>Note:</b> This field appears only when the RTR license is enabled. You must have RTR enabled in your licensing package in order to use RTR features.</p>
<b>Version</b>	The version of the application being scanned. (This information may not be available.)
<b>Vendor</b>	The name of the vendor providing the application. (This information may not be available.)
<b>Operating System</b>	The operating system of the device containing the application.
<b>Operating System Version</b>	The operating system version for the device. (This information may not be available.)
<b>Source</b>	The agent that is used to scan the application.
<b>Threat Override</b>	<p>Indicates whether an application as Trusted or Untrusted according to the threat score.</p> <p><b>Note:</b> This field appears only when the RTR license is enabled. You must have RTR enabled in your licensing package in order to use RTR features.</p>
<b>Package Name</b>	The namespace in which the application is run. (This information may not be available.)

Field	Definition
<b>Submit Date</b>	The date when the application was last submitted to a Threat Analysis Engine.
	<b>Note:</b> This field appears only when the RTR license is enabled.
<b>Host Count</b>	The number of hosts that have the application.
<b>Buttons</b>	
<b>Export</b>	The Export option allows you to export a list of selected applications to CSV, Excel, PDF or RTF formats.
<b>Options</b>	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.
<b>Show Hosts</b>	Opens the Host View displaying the host(s) containing the application. Users can also right-click in the Applications table to access this option.
<b>Delete</b>	Deletes the selected application. Users can also right-click in the Applications table to access this option.
<b>Rescan</b>	Rescans the selected application for threat analysis. Users can also right-click in the Applications table to access this option.
	<b>Note:</b> This option appears only when the RTR license is enabled. You must have RTR enabled in your licensing package in order to use RTR features.
<b>Set Threat Override</b>	Marks an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none". Users can also right-click in the Applications table to access this option.
	<b>Note:</b> This option appears only when the RTR license is enabled. You must have RTR enabled in your licensing package in order to use RTR features.

### Show the Host(s) Containing an Application

1. Select **Hosts > Application View** to access the Application View.
2. Select an application in the table and click the **Show Hosts** button, or right-click an application and select **Show Hosts** from the menu.

The Host View is displayed showing the host(s) that contain the application.

### Set the Threat Override for an Application

Set Threat Override lets users mark an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none".

**Note:** You must have RTR enabled in your licensing package in order to use RTR features.

1. Select **Hosts > Application View** to access the Application View.
2. Select an application in the table and click the **Set Threat Override** button, or right-click an application and select **Set Threat Override** from the menu.
3. Select **Trusted** or **Untrusted** from the **Threat Override** drop-down menu.
4. Click **OK**.

## Aging Out Host Or User Records

Host and User records remain in the database indefinitely unless you set expiration dates for those records. There are several methods for setting expiration dates.

As new hosts, users or Administrative Users are added to the database, the **Expiration Date** and/or **Inactivity Date** are automatically populated based on settings elsewhere in Network Sentry. Aging settings are configured using the methods listed below. If no global settings have been established and hosts or users are added without Expiration or Inactivity dates, those dates can be added later by configuring the settings below.

**Note:** If you set age times for existing users or hosts, you may inadvertently cause them to be deleted from the database. If the expiration date calculated for those hosts or users is before today's date, those records will be removed from the database.

**Note:** Aging a large number of hosts or users at the same time can cause processing delays with Network Sentry if users attempt to re-register within a short period of time of each other. It is recommended that you stagger the aging times to reduce the number of possible re-registrations at any given time.

**Note:** Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.

**Directory**—If the **Time To Live** option is enabled in the Directory Attribute Mappings window, the value stored in the Directory is used to calculate the dates for Expiration Date and Inactivity Date. This is based on the user's record in the directory. For the user, only the Expiration Date is calculated. For the host, both the Expiration Date and the Inactivity Date are calculated. This may also apply to Administrative Users. The host must be associated with a user to inherit these settings. See **Add/Modify Directory - User Attributes Tab** on page 76.

**Group Aging**—You can create a host group and use Group Aging to populate the Expiration Date and/or the Inactivity Date fields for hosts in that group. All hosts in the group are modified even if they already have an age time set, except those set to Never Expire. See **Aging Hosts In A Group** on page 699.

**Host Aging**—You can enter or override aging values for individual hosts by clicking the Set button on the Host Properties window or using the Set Host Expiration Date option on the Host View. See **Set Host Expiration Date** on page 366.

**User Aging**—You can enter or override those values for individual users, including Administrative Users, by clicking the Set button on the User Properties window or using the Set User Expiration Date option on the User View. See **Set User Expiration Date** on page 425.

**Administrator User Aging**—Administrator users never age out of the database under any circumstances. These users must be removed from the database manually from the Admin Users View.

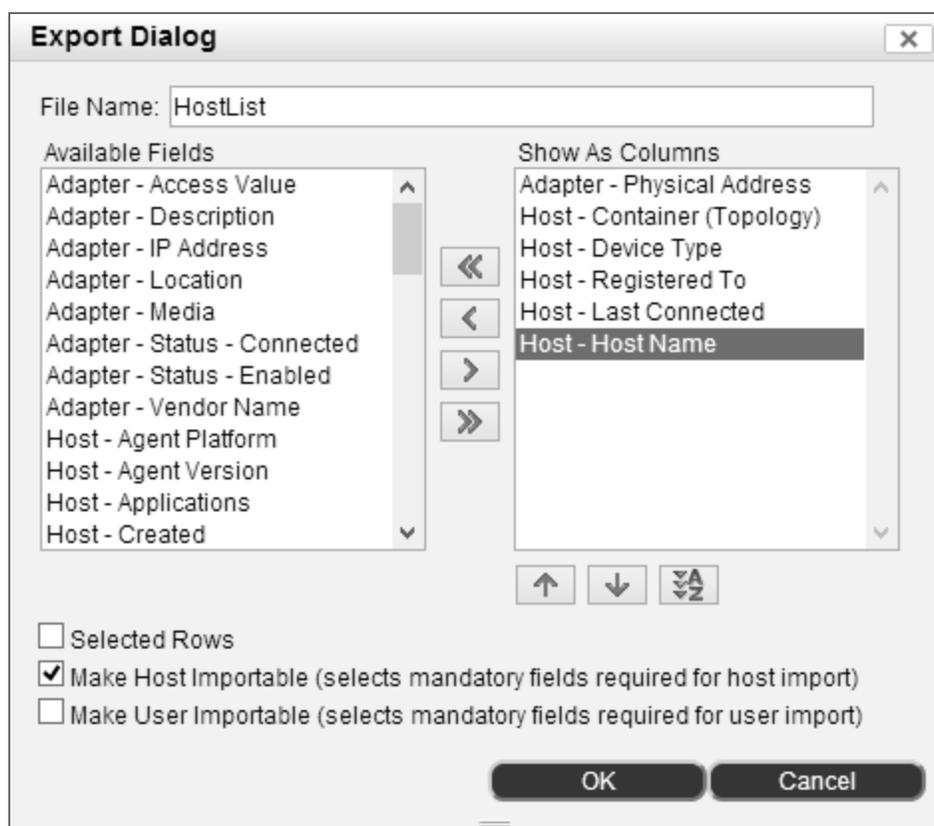
**Administrative User Aging**—Administrative Users (Operator, Help Desk) are treated like regular network users when aging settings are applied, depending on how they are added to the database. Below are ways to set the expiration date for an Administrative User:

- Manually give any Administrative User an expiration date by selecting the user on the Admin Users View and using the Set Expiration option. See **Set User Expiration Date** on page 425.
- When an Administrative User is added by converting an existing network user to an Administrative User, the new Administrative User can have aging set through any of the possible aging options.
- If you assign Admin User Profiles based on directory groups, there are circumstances in which an Administrative User would be assigned an expiration date.
  - If the user did not exist in the database as an Administrative User, registered a host through the captive portal and then a directory synchronization was run the user would be converted to an Administrative User but would have an expiration date based on the global aging settings.
  - If the user did not exist in the database as an Administrative User, another Admin User registered a host to someone in the directory from the Hosts View and then a directory synchronization was run the user would be converted to an Administrative User but would have an expiration date based on the global aging settings.

**Guest Aging** — A Guest user's expiration date is set based on the Account Duration entered in the Guest Template used to create the Guest. The host registered to the Guest inherits its expiration date from the Global Aging settings. When the Guest user's account expires, both the Guest user's account and the guest's registered host are automatically removed from the database. If the host's expiration date is earlier than the Guest user's expiration date, the host is removed from the database, but the Guest user account remains.

## Export Data

Export data to a CSV file, an Excel spreadsheet, a PDF document or an RTF document. Select from a list of possible fields and control the order of the data in the export. If you plan to re-import the same file after editing it, you must use a CSV file. See **Import Hosts, Users Or Devices** on page 294 for a list of fields that can be exported or imported and their definitions.



**Figure 158: Sample Export Dialog**

1. Navigate to a View with export options at the bottom, such as the Host View.
2. Use the Search or Filters to display a list of records.
3. Use Ctrl-click or Shift-click to select the records you wish to export. If you do not select specific records, all displayed records are exported. When the Export dialog is displayed, check the Selected Rows check box to export only selected records.
4. At the bottom of the window, click the icon for the type of export file needed, such as PDF.
5. In the File Name field, enter a name for the export file. Do not add an extension. It is added when you click OK based on the file type you selected in the previous step.

6. The fields contained in the Export Dialog vary based on the View from which you are exporting.
7. Select the field(s) you want to export and click the right-arrow to move the field to the Show As Columns list. Ctrl-click to select more than one field at a time.
8. Click the double-arrows to move all of the fields from one column to the other.
9. To remove fields from the export, select them in the Show As Columns list and click the left-arrow.
10. To reorder the fields in the **Show As Columns** list, click the field and then click the Up or Down arrows. The order displayed from top to bottom corresponds to the columns in the export from left to right. For example, if the first field at the top of the list is Last Name, that is the left most column in the export.
11. To sort fields alphabetically, click the **Sort** button labeled AZ.
12. Check the **Selected Rows** check box to export only the records selected in the View. If you leave this box unchecked, all the records in the View are exported.
13. A Header line consisting of the field names is inserted in the .csv file if you check either or both of the **Make Importable** check boxes. In addition, the fields required for import are automatically added to your export.

---

**Note:** When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

---

**Note:** Only the Export Dialog accessed from Users, Hosts or Adapters views includes two Make Importable check boxes because of the relationship between Users and their corresponding Hosts. The Export Dialog accessed from other views may have one Make Importable check box, such as, Admin Users, or no Make Importable check boxes, such as Connections.

---

14. Click **OK**.
15. Depending on your browser, the file is either generated and saved to a Downloads location or you may need to navigate to the **location** where the file is to be placed.

## Chapter 9: User View

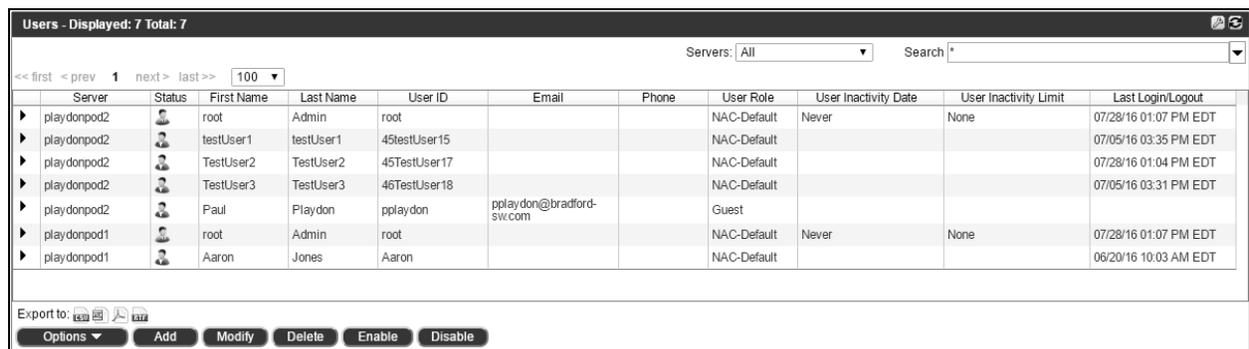
The User View is part of a four tabbed window that includes Adapters, Hosts, Users, and Applications. Use the User View to add, delete, modify, locate and manage users on your network. Users include network users, guest or contractor users and Administrator Users. Administrator users can also be managed from the Admin Users View. Administrator users are also network users, therefore, they are included in the Users View with a slightly different icon. See the **Icon Key** on page 14 for information on each icon.

If you have an LDAP or Active Directory configured, user information is added from the directory as users register on the network. The Network Sentry database is periodically synchronized with the directory to make sure that data is the same in both places. User information from the directory is matched to user information in the Network Sentry database based on User ID. If you manually create a user with an ID that is the same as a user in the directory, then directory data will overwrite your manually entered data.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a tabbed window, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters tab, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users tab to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the hosts associated with the selected user. Hover over the icon in the Status column to display a tool-tip with detailed information about this user. For field definitions see **User View And Search Field Definitions** on page 400.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.



Users - Displayed: 7 Total: 7

Servers: All Search \*

Server	Status	First Name	Last Name	User ID	Email	Phone	User Role	User Inactivity Date	User Inactivity Limit	Last Login/Logout
▶ playdonpod2		root	Admin	root			NAC-Default	Never	None	07/28/16 01:07 PM EDT
▶ playdonpod2		testUser1	testUser1	45testUser15			NAC-Default			07/05/16 03:35 PM EDT
▶ playdonpod2		TestUser2	TestUser2	45TestUser17			NAC-Default			07/28/16 01:04 PM EDT
▶ playdonpod2		TestUser3	TestUser3	46TestUser18			NAC-Default			07/05/16 03:31 PM EDT
▶ playdonpod2		Paul	Playdon	pplaydon	pplaydon@braadford-siw.com		Guest			
▶ playdonpod1		root	Admin	root			NAC-Default	Never	None	07/28/16 01:07 PM EDT
▶ playdonpod1		Aaron	Jones	Aaron			NAC-Default			06/20/16 10:03 AM EDT

Export to:

Options Add Modify Delete Enable Disable

Figure 159: User View

### User View Field Definitions

Field	Definition
<b>Address</b>	Users's street address.
<b>Allowed Hosts</b>	<p>The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total.</p> <p>If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single machine with up to five adapters counts as one host.</p> <p>If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one machine with two network adapters would be counted as two hosts.</p> <p>If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.</p>
<b>City</b>	User's city of residence.
<b>Created Date</b>	Date the user record was created in the database. Options include Before, After, and Between.
<b>Delete Hosts When User Expires</b>	Indicates whether hosts registered to this user should be deleted from the database when the user's record ages out of the database.
<b>Email</b>	User's email address.
<b>Expiration Date</b>	Controls the number of days a user is authorized on the network. Options include Before, After, Between, Never, and None. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Delete Hosts When User Expires</b>	Indicates whether hosts owned by this user should be deleted when the user ages out of the database. It is recommended that you set this to Yes.
<b>Inactivity Date</b>	Controls the number of days a User is authorized on the network. Options include Before, After, Between, Never, and None. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See <b>Aging Out Host Or User Records</b> on page 381 or <b>Set User Expiration Date</b> on page 425.
<b>Inactivity Limit</b>	Number of days the user must remain continuously inactive on the network to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381 or <b>Set User Expiration Date</b> on page 425.
<b>Last Login/Logout</b>	Date of the last time the user logged into or out of the network or the Network Sentry Admin UI. This date is used to count the number of days of inactivity. Options include Before, After, Between, and Never.
<b>Last Name</b>	User's last name.
<b>Mobile Number</b>	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the Mobile Provider to send SMS messages.

Field	Definition
<b>Mobile Provider</b>	Provider or carrier for user's mobile phone.
<b>Notes</b>	Notes about this user.
<b>Phone</b>	User's telephone number.
<b>User Role</b>	Role assigned to the user. Roles are attributes of users and are used as filters for User/Host Profiles. See <b>Role Management</b> on page 609.
<b>User Security &amp; Access Value</b>	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
<b>State</b>	User's state of residence.
<b>Status</b>	Current or last known status is indicated by an icon. See <b>Icon Key</b> on page 14. Hover over the icon to display additional details about this User in a tool tip.  <b>Access</b> — Indicates whether user is enabled or disabled.
<b>Title</b>	User's title, this could be a form of address or their title within the organization.
<b>Type</b>	Type of user. Allows you to differentiate between network users and guest-contractor users.
<b>User ID</b>	Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, Network Sentry assumes that this user is authenticating locally and asks you for a password.  When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the Network Sentry database is updated with the directory data.
<b>Postal Code</b>	User's zip code based on their state of residence.
<b>Last Modified By</b>	User name of the last user to modify the user.
<b>Last Modified Date</b>	Date and time of the last modification to this user.

User View Navigation, Menus, Options And Buttons

For information on selecting columns displayed in the User View see **Configure Table Columns And Tool-tips** on page 390. Some menu options are not available for all Users. Options may vary depending on user state.

Field	Definition
<b>Quick Search</b>	<p>Enter a single piece of data to quickly display a list of users. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters.</p> <p>If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.</p> <p>When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.</p>
<b>Right Mouse Click Menu Options</b>	
<b>User Properties</b>	Opens the Properties window for the selected user. See <b>User Properties</b> on page 404.
<b>Add Users To Groups</b>	Add the selected user(s) to one or more group(s). See <b>Add Users To Groups</b> on page 412.
<b>Delete Users</b>	Deletes the selected user(s) from the database. See <b>Delete A User</b> on page 411.
<b>Disable Users</b>	Disables the selected user (s) preventing them from accessing the network regardless of the host they are using.
<b>Enable Users</b>	Enables the selected user(s) if they were previously disabled. Restores network access.
<b>Group Membership</b>	<p>Displays groups in which the selected user is a member.</p> <p>Note: If the User is also an Admin User, separate options are displayed for Admin User Groups and User Groups. Options are labeled Group Membership (User) and Group Membership (Administrator).</p>
<b>Guest Account Details</b>	Displays account details for the selected guest record, such as User ID, Account Status, Sponsor, Account Type, Start and End dates, Availability, Role, Authentication, Security Policy, Account Duration, Reauthentication Period, Success URL and the guest's password. See <b>Guest User Account Details</b> on page 422.
<b>Modify User</b>	Opens the Modify User window. See <b>Modify A User</b> on page 408.
<b>Policy Details</b>	Opens the Policy Details window and displays the policies that would apply to the selected user at this time, such as Endpoint Compliance Policies, Network Access Policies or Supplicant Policies. See <b>Policy Details</b> on page 416.
<b>Set Expiration</b>	Launches a tool to set the date and time for the user to age out of the database. See <b>Set User Expiration Date</b> on page 425.
<b>Set Role</b>	Assigns a role to the selected user. See <b>Role Management</b> on page 609.

Field	Definition
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <hr/> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p> <hr/> <p><b>Note:</b> Changes made to Hosts, Users, or Adapters are not displayed in the Admin Auditing Log. These changes are visible in the Audit Log on each server.</p>
<b>Show Events</b>	Displays all events for the selected user.
<b>Collapse All</b>	Collapses all records that have been expanded.
<b>Expand Selected</b>	Expands selected user records to display host information.
<b>Buttons</b>	
<b>Import/Export</b>	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats. See <b>Import Hosts, Users Or Devices</b> on page 294 or <b>Export Data</b> on page 383.
<b>Options</b>	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.

## Configure Table Columns And Tool-tips

Use the configuration button on the User View, Adapter View, Host View, and Applications View to open the Settings window. The Settings window controls the columns displayed in each view and the details displayed in tool-tips when you hover over an icon.

### Configure Columns

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Columns** tab.
3. Mark the columns to be displayed in the table on the User, Adapter or Host View with a check mark and click **OK**.
4. These settings are saved for the logged in user.

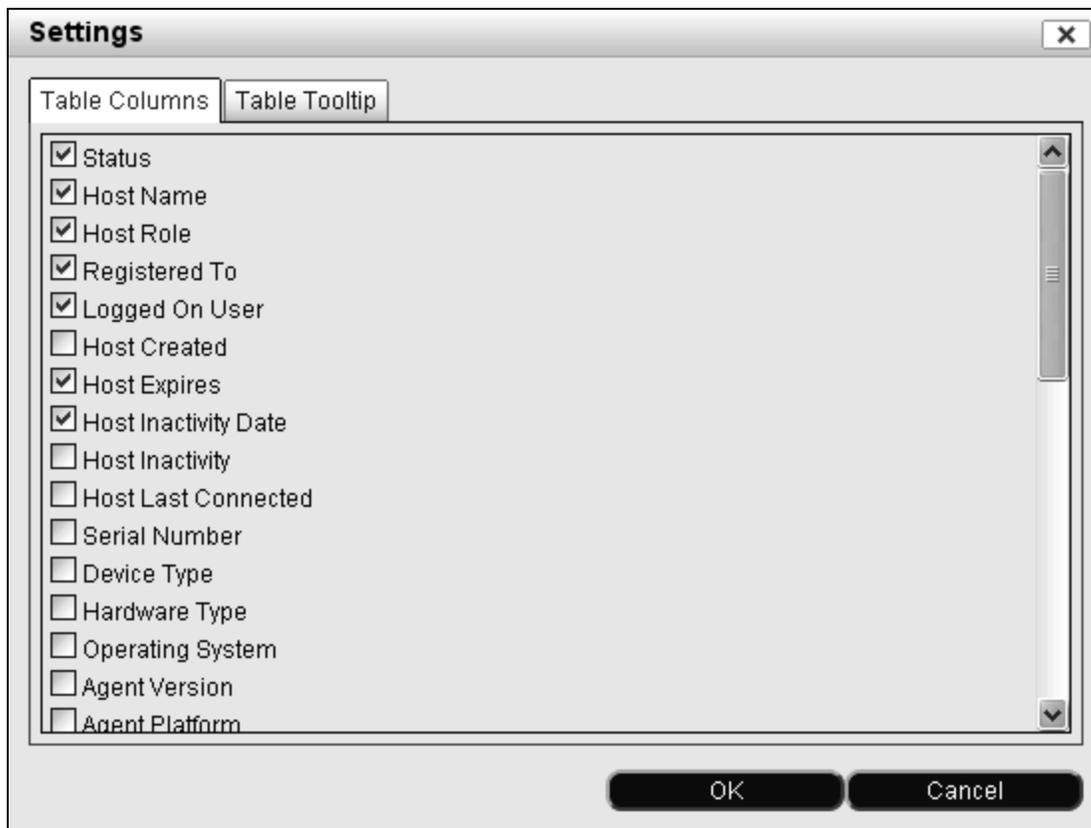


Figure 160: Configure Settings - Table Columns

### Configure Tool-Tips

Select the fields to be displayed in the tool-tip when you hover the mouse over the status icon of either a User, an Adapter or a Host. Available fields vary depending on which item you are configuring.

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Tooltip** tab.
3. The **Available Fields** column displays fields that can be displayed, but have not yet been selected. The Selected Fields column displays fields that will display in the tool-tip.
4. Use the arrows in the center of the window to move fields from one column to the other until the appropriate set of fields is displayed in the **Selected Fields** column.
5. Select a field in the Selected Fields column and use the up and down arrow buttons to change the order of display. Use the AZ button to sort fields alphabetically.
6. The **Hide Blank Fields** option is enabled by default. It reduces the size of the tool-tip when selected fields are blank for a particular item. For example, if you have selected Host Expires and the selected Host does not have an expiration date, then when the tool-tip for that host is displayed, the Host Expires field is hidden.
7. Click **OK** to save your changes. These settings are saved for the logged in user.

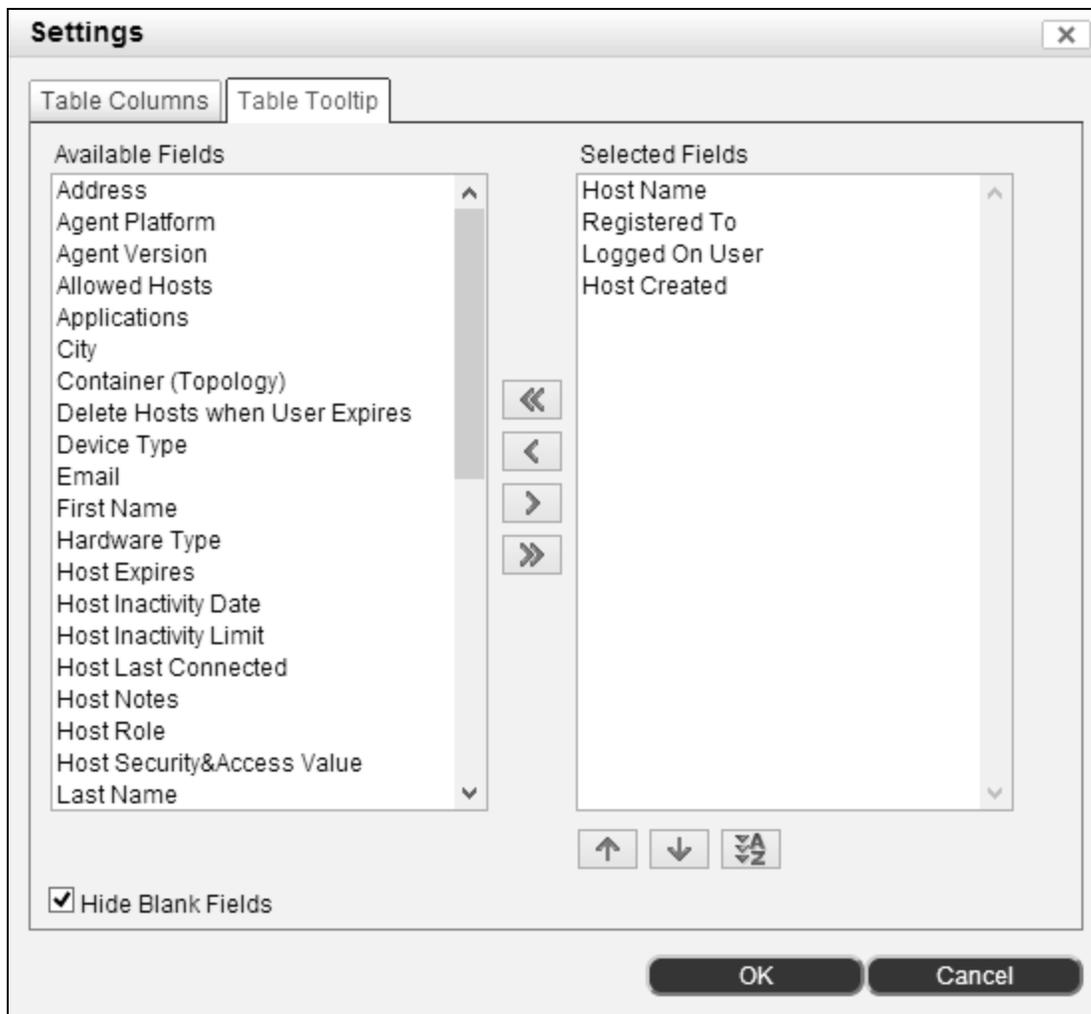
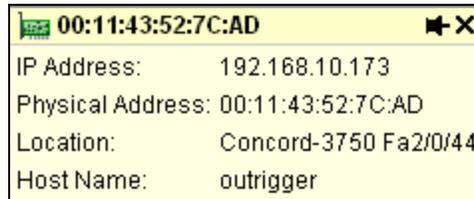


Figure 161: Configure Settings - Table Tool-tips

### Using Tool-Tips

Tool-tips are displayed when you hover the mouse over a status icon in the User, Adapter or Host views. Tool-tips details are configured using the Settings window shown in the previous section.



**Figure 162: Sample Tool-tip**

- When a tool-tip is displayed, click the Push Pin icon to anchor it to the screen. Now you can move the tool-tip around your desktop without it closing.
- High-light text in a tool-tip and press Ctrl-C to copy it. Press Ctrl-V to paste the text in a field.
- Open and anchor multiple tool-tips to quickly compare data.
- Hover over the status icon in the top left corner for text based status information.

## Search And Filter Options For Hosts, Adapters, Users, or Applications

There are several search and filter mechanisms used to locate Hosts, Adapters, Users or Applications. These four tabs share a single view and search mechanism. Options include: Quick Search and Custom Filters, which can be used once or saved for reuse.

When a search or filter is run, the search data or the name of the filter remains in the search field at the top of the window. If you then click on a different tab, that search is rerun in the context of the new tab.

### Wild Cards

When searching using a text field in a Custom Filter or the Quick Search field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP Address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records.  Any search field that starts and ends with square brackets "[" and has one or more commas "," is treated as a list of values.
!	!192. in the IP Address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).

### Quick Search

The Quick Search field at the top of the window allows you to search based on a single piece of data, such as IP Address, and display all matching records. The following fields are included in the Quick Search: IP Address, MAC Address, Host Name, User First Name, User Last Name, Registered User, Logged On User, and User ID. To search by MAC Address you must use one of the following formats:

```
xx:xx:xx:xx:xx:xx
xxxxxxxxxxxxxx
xx.xx.xx.xx.xx.xx
```

xx-xx-xx-xx-xx-xx

xxxx.xxxx.xxxx

Wild card searches can also be done. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5\*. Without the separators the search option cannot distinguish that it is a MAC address.

If you are searching by IP Address you enter 192.168.5.1\* and you get all records for IP addresses from 192.168.5.1 to 192.168.5.199. See **Wild Cards** on page 394.

The information displayed varies depending on the tab that is selected. As you click from tab to tab the search in the Quick Search field is applied automatically.

**Users Tab** — Displays all users associated with a device that matches the IP range.

**Hosts Tab** — Displays all hosts with an adapter that matches the IP range.

**Adapters Tab** — Displays all adapters that match the IP range

To broaden the search, enter less information, such as \*11\*. This returns any User Name, User ID, IP, MAC, or Host Name containing 11 depending on the tab you have selected.

To use the Quick Search option:

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts or Users Tab.
3. Enter a single piece data in the search field and press **Enter**. Wild card searches can be done.

## Custom Filter

The Custom Filter is the equivalent to an advanced search feature. It provides many fields that can be used in combination to narrow the list of Users, Adapters or Hosts displayed. A Custom Filter can be created and used just once or can be saved under a filter name. The new filter then displays in the drop-down menu accessed by clicking the arrow on the Quick Search field at the top of the window. Custom Filters can be modified, copied or deleted as needed. You can also export Custom Filters to a .txt file which allows Custom Filters to be imported and used by other Admin users.

Use your mouse to hover over a saved filter in the drop-down menu and display a tool-tip with details about that filter. There is currently only one default Custom Filter, Online Hosts, that displays a list of hosts that are connected to the network.

For filter field definitions refer to the following:

### Create and Save a New Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. From the drop-down menu select **New Filter**.
5. Enter the name of the new filter and click **OK**.
6. Continue with the topic below, Configure A Filter.



Figure 163: Add New Filter

## Configure a Filter

This window is used in two ways. First if you have selected New Filter from the menu off of the Quick Search drop-down, you can configure the filter and Network Sentry saves it for future use. Second, if you have selected Custom Filter from the menu off of the Quick Search, you can configure this filter and use it just one time.

**Figure 164: Custom Filter**

**Note:** This dialog box is common to the Adapter, Host and User Views. Custom filter entries on any of these tabs will persist if you navigate between these views.

1. Once you have the Filter window displayed, enable the fields to be included in the filter by marking them with a check mark.
2. For each enabled field you must provide additional information. For example, if you select the Connected field, you must choose either On Line or Off Line.

3. For text fields, such as the IP Address field, you must enter the search data, such as 192.168.10.5. Wild cards can be used in these fields. See **Wild Cards** on page 394.
4. To erase all selections, click the **Clear All** button.
5. If you have opened a saved filter and started to modify it, use the **Reset** button to return the filter to its original settings.
6. Click **OK** to run the configured filter. If this filter was assigned a name, the settings will be saved.
7. Immediately after the filter is run, the filter name displays at the top of the view in the Quick Search field. To modify the filter, click the **Edit** link to the left of the Quick Search field. This modifies the filter whether it was saved or just configured and run one time.

### Edit a Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be edited and click the pencil or edit icon to the right of the filter name.
5. When the Filter window displays, modify the filter as needed.
6. Click **OK** to save your changes.

### Delete a Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be deleted and click the red X to the right of the filter name.
5. When the confirmation message displays, click **Yes**.

### Export a Custom Filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Export**.

5. In the Export Filters dialog, select the filters you want to export. Use Ctrl or Shift to select multiple filters.
6. Click **OK**.

The filters are downloaded to a .txt file to your default download directory.

### **Import a Custom Filter**

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the **arrow** on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Import**.
5. Click Choose File to find and select the .txt file containing the filters.
6. Click **OK** to import the filters.

The filters will appear in the list.

User View And Search Field Definitions

The fields listed in the table below are displayed in columns on the User View based on the selections you make in the Settings window. See **Configure Table Columns And Tool-tips** on page 390. Most of these fields are also used in Custom Filters to search for hosts. See **Search And Filter Options For Hosts, Adapters, Users, or Applications** on page 394. Additional fields that can be displayed on the User View are fields for the host associated with the selected user. See **Host View And Search Field Definitions** on page 327.

**Note:** You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

The screenshot shows a 'Filter' dialog box with the following sections and options:

- Adapter | Host | User | Application** (User is selected)
- Status (Policy - Access)**
  - Access: Enabled
  - Type: Guest/Contractor
  - Role: [Empty]
  - Security Access & Value: [Empty]
- Time**
  - Created Date: Before 2016-03-10 00:00:00
  - Expiration Date: Next 30 Days
  - Inactivity Date: Before [Empty]
  - Last Login/Logout: Before [Empty]
- User Information**
  - First Name: [Empty]
  - Last Name: [Empty]
  - Notes: [Empty]
  - User ID: [Empty]
  - Title: [Empty]
- Address**
  - Address: [Empty]
  - City: [Empty]
  - State: [Empty]
  - Mobile Number: [Empty]
  - Zip/Postal Code: [Empty]
  - Phone: [Empty]
  - Email: [Empty]
  - Mobile Provider: [Empty]

Buttons: OK, Cancel

Figure 165: Custom Filters - User View

Field	Definition
<b>Access</b>	Indicates whether user is enabled or disabled
<b>Address</b>	Users's street address.
<b>City</b>	User's city of residence.
<b>Created Date</b>	Date the user record was created in the database. Options include Before, After, and Between.
<b>Email</b>	User's email address.
<b>Expiration Date</b>	Controls the number of days a user is authorized on the network. Options include Before, After, Between, Never, and None. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See <b>Aging Out Host Or User Records</b> on page 381.
<b>First Name</b>	User's first name.
<b>Inactivity Date</b>	Controls the number of days a User is authorized on the network. Options include Before, After, Between, Never, and None. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See <b>Aging Out Host Or User Records</b> on page 381 or Set User Expiration Date on page 425.
<b>Inactivity Limit</b>	Number of days the user must remain continuously inactive on the network to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381 or Set User Expiration Date on page 425.
<b>Last Login/Logout</b>	Date of the last time the user logged into or out of the network or the Network Sentry Admin UI. This date is used to count the number of days of inactivity. Options include Before, After, Between, and Never.
<b>Last Name</b>	User's last name.
<b>Mobile Number</b>	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the Mobile Provider to send SMS messages.
<b>Mobile Provider</b>	Provider or carrier for user's mobile phone.
<b>Notes</b>	Notes about this user.
<b>Phone</b>	User's telephone number.
<b>Role</b>	Role assigned to the user. Roles are attributes of users and are used as filters for User/Host Profiles. See <b>Role Management</b> on page 609.
<b>Security &amp; Access Value</b>	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
<b>Server</b>	Select the server where the user is located.

Field	Definition
State	User's state of residence.
Status	The icon indicates the level of user (network user or guest/contractor).
Title	User's title, this could be a form of address or their title within the organization.
Type	Type of user. Allows you to differentiate between network users and guest/contractor users.
User ID	<p>Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, Network Sentry assumes that this user is authenticating locally and asks you for a password.</p> <p>When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the Network Sentry database is updated with the directory data.</p>
Postal Code	User's zip code based on their state of residence.

### User Drill-down

Use the arrow in the far left column to expand a user and view host details. Expand or collapse multiple users by selecting them and using the right - mouse button or Options button. All hosts associated with a user are contained within the expanded section of the window.

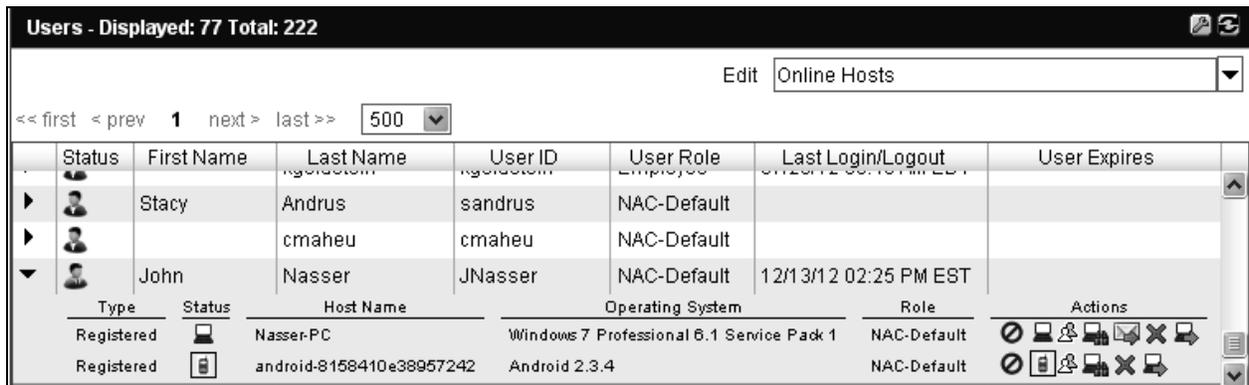


Figure 166: User - Expanded View

Field	Definition
Type	Type of host associated with this user. Types include: Registered
Status	Status of the host. See the <b>Icon Key</b> on page 14 for status information.

Field	Definition
<b>Operating System</b>	Operating system installed on the host.
<b>Role</b>	Role assigned to the host. Roles are attributes of hosts that can be used as filters in User/Host Profiles. See <b>Role Management</b> on page 609.
<b>Actions</b>	Use the action icons to do the following: <ul style="list-style-type: none"><li>• Enable/Disable a host.</li><li>• Access Host Properties</li><li>• View/Modify group membership</li><li>• Scan the host</li><li>• Send a message to the host (only hosts with the Persistent Agent installed)</li><li>• Delete host</li><li>• Go to host in the Host View</li></ul>

## User Properties

The User Properties view provides access to detailed information about a single user. From this view you can access the associated host by clicking on the adapter's physical address displayed in the Registered Hosts tab at the bottom of the window.

### Access User Properties:

1. Select **Users > User View**.
2. Search for the appropriate User.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **User Properties**.

General	
First Name	Alan
Last Name	Hackert
ID	hackert
Title	
Role	Administration <input type="button" value="v"/>
Security and Access Attribute Value	Accounting
User Status	Enable <input checked="" type="radio"/> Disable <input type="radio"/>
Allowed Hosts:	10
Address	
Address	162 Pembroke Rd.
City	Concord
State	NH
Zip/Postal Code	03301
Phone	603-555-1212
Email	hackert@sw.com

Figure 167: User Properties - General/Address

Time		
Expiration Date	08/15/13 09:59 AM EDT	<input type="button" value="Set"/>
Inactivity Date	05/27/12 10:05 AM EDT	
Inactivity Limit	30 days	
Last Login/Logout		
Delete Hosts upon Expiration	Yes	
Created	04/27/12 10:05 AM EDT	

Registered Hosts	Logged In Hosts	Notes
<p><b>Host Names</b></p> <p><i>Reagan hacker 00:19:E3:E8:82:DF</i></p> <p><i>hacker 00:24:A8:88:81:4E</i></p>		

Figure 168: User Properties - Time/Tabs

Table 23: User Properties Field Definitions

Field	Description
<b>General</b>	
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>ID</b>	<p>Unique alphanumeric ID for this user. Typically comes from the directory but if you are not using a directory, this field can be created manually. This field cannot be modified.</p> <p>When using a directory for authentication, fields such as name, address, and email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the Network Sentry database is updated with the directory data.</p>
<b>Title</b>	User's title, this could be a form of address or their title within the organization.
<b>Role</b>	Role assigned to the user. Roles are attributes of users that can be used as filters in User/Host Profiles. See <b>Role Management</b> on page 609.

Field	Description
<b>Security And Access Attribute Value</b>	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
<b>User Status</b>	Radio buttons indicating whether the user is Enabled or Disabled. To enable or disable the user, click the appropriate button and then click Apply.
<b>Allowed Hosts</b>	<p>The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total.</p> <p>If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single machine with up to five adapters counts as one host.</p> <p>If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one machine with two network adapters would be counted as two hosts.</p> <p>If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.</p>
<b>Time</b>	
<b>Expiration Date</b>	<p>Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window.</p> <p>To modify click <b>Set</b>. See <b>Set User Expiration Date</b> on page 425 for additional information.</p>
<b>Inactivity Date</b>	<p>Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit.</p> <p>For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set.</p>
<b>Inactivity Limit</b>	Number of days the user must remain continuously inactive to be removed from the database. See <b>Aging Out Host Or User Records</b> on page 381.
<b>Last Login/Logout</b>	Date of the last time the user logged into or out of the network or the Network Sentry Admin UI. This date is used to count the number of days of inactivity.
<b>Delete Hosts Upon Expiration</b>	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click <b>Set</b> .
<b>Created</b>	Indicates when this record was created in the database.
<b>Tabs</b>	
<b>Registered Hosts</b>	Displays a list of hosts, by the MAC address of their adapters, registered to this user. Click on a MAC address to open the Host Properties.

<b>Field</b>	<b>Description</b>
<b>Logged In Hosts</b>	List of hosts by host name registered to this user that are currently logged onto the network.
<b>Notes</b>	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
<b>Buttons</b>	
<b>Apply</b>	Saves changes to the User Properties.
<b>Reset</b>	Resets the values in the User Properties window to their previous settings. This option is only available if you have not clicked Apply.

## Modify A User

User records are created as users connect to the network and register. Users can be added by importing them in a file or by entering the data manually. See **Import And Export Data** on page 291. The Add or Modify User feature allows you to create new users or edit existing ones.

**Modify User** [X]

Asterisk (\*) indicates required fields.

**User Information**

\*User ID: a.lincoln

First Name:  \*Last Name:

\*Role:  [v] [icon]

Address:

City:  State:

Zip/Postal Code:  Phone:

Email:  Title:

Mobile Number:

Mobile Provider:  [v]

Allowed Hosts:  (Global Default: 1000)

Notes:

Security and Access Attribute Value:

Figure 169: Modify User

1. Select **Users > User View**.
2. Use the search or filter mechanisms on the User View to locate the appropriate user.
3. Select the user and click the **Modify** button.
4. See the field definitions table below for detailed information on each field.
5. Click **OK** to save your data.

## Modify User Field Definitions

Field	Definitions
<b>Required Fields</b>	
<b>User ID</b>	<p>Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, Network Sentry assumes that this user is authenticating locally and asks you for a password.</p> <p>When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the Network Sentry database is updated with the directory data.</p>
<b>Change Password</b>	Allows you to change the password for this user. Users who authenticate through the directory will not have a Change Password button. Only users who are locally authenticated by Network Sentry have a change password option.
<b>First Name Last Name</b>	User's name as it is retrieved from the directory. If you are using a directory, these fields are updated every time the directory is re-synchronized with the database. If you are not using a directory, enter the user's first and last name.
<b>Role</b>	Roles are attributes of users and can be used as filters in User/Host Profiles. These profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy is applied.
<b>Additional Info</b>	
<b>Address</b>	User's address of residence.
<b>City</b>	User's city of residence.
<b>State</b>	Two letter abbreviation for state of residence.
<b>Zip/Postal Code</b>	Postal code for the user's city and state of residence.
<b>Email</b>	User's email address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>Title</b>	This can be a form of address, such as Mr., or a title within the organization.
<b>Mobile Number</b>	Mobile Phone number used for sending SMS messages to guests and administrators.
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to guests and administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.

<b>Field</b>	<b>Definitions</b>
<b>Allowed Hosts</b>	<p>The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total.</p> <p>If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single machine with up to five adapters counts as one host.</p> <p>If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one machine with two network adapters would be counted as two hosts.</p> <p>If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.</p>
<b>Global Default</b>	<p>Default number of Allowed Hosts used if the Allowed Hosts field is empty. The default is set in <b>System &gt; Settings &gt; User/Host Management &gt; Allowed Hosts</b>.</p>
<b>Notes</b>	<p>Free form notes entered by the Administrator.</p>
<b>Security and Access Attribute Value</b>	<p>This value is an attribute of users and can be used as a filter in User/Host Profiles. These profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy is applied. If a directory is in use, the Security and Access Attribute value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.</p>

## Delete A User

When you delete a user, you have the option to delete hosts registered to this user or leave them in the database. It is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

1. Select **Users > User View**.
2. Use the Quick Search or Custom Filter to locate the appropriate User.
3. Select the user and click the **Delete** button.
4. A warning message is displayed asking if you would like to delete registered hosts associated with this user.

**To delete hosts**, enable the check box labeled **Delete Hosts Registered to User** and click **Yes**.

**To convert hosts to registered devices**, disable the check box labeled **Delete Hosts Registered to User** and click **Yes**.

To cancel the entire operation, click **Cancel**.

## Add Users To Groups

You can add selected users to groups you have created. See **Groups View** on page 681 for detailed information on Groups and how they are used in Network Sentry.



Figure 170: Add Users To Group

1. Select **Users > User View**.
2. Use the Quick Search or Custom Filter to locate the appropriate User(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the Options button and select **Add Users To Groups**.
5. The Add Users to Groups view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups.

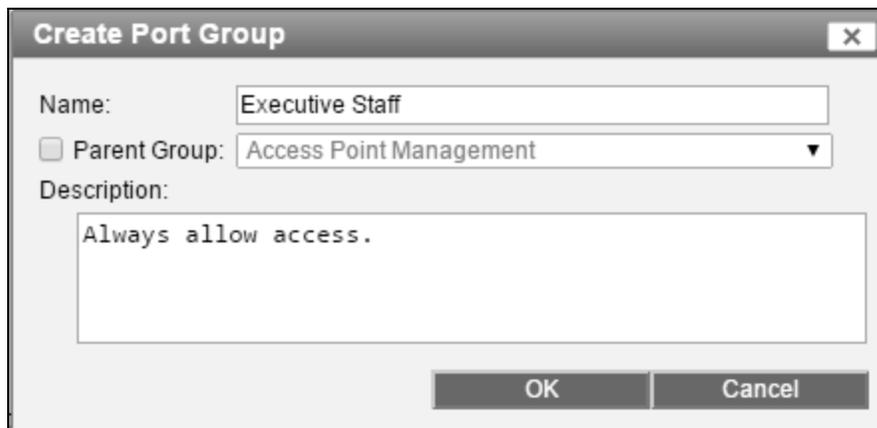
6. **To add the users to a group**, click the box next to the group name and then click **OK**.
7. **To create a missing group**, click the **Create Group** button.

Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.



The screenshot shows a dialog box titled "Create Port Group". It has a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "Executive Staff".
- Parent Group:** A checkbox labeled "Parent Group:" which is unchecked, followed by a dropdown menu currently showing "Access Point Management".
- Description:** A text area containing the text "Always allow access.".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 171: Create Port Group

8. Click **OK**.

## User Group Membership

From the User View window you can view or modify the group membership of an individual user. Use this option to open a window that displays a list of all groups to which the selected user belongs.



Figure 172: Group Membership View

1. Select **Users > User View**.
2. Use the Quick Search or Custom Filter to locate the appropriate User(s).
3. Click on a user to select it.
4. Right-click or click the Options button and select **Group Membership**.
5. The Group Membership view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this user is contained in that group.

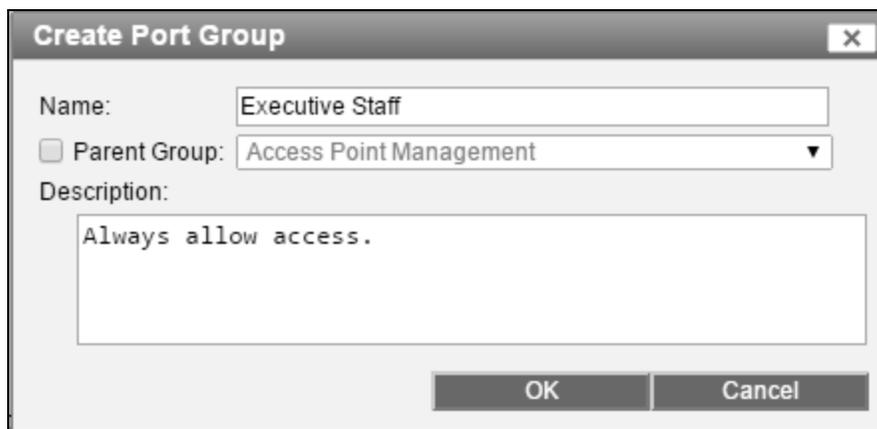
6. **To add the user to a group**, click the box next to the group name and then click **OK**.
7. **To remove the user from a group**, click to uncheck the box next to the group name and then click **OK**.
8. **To create a missing group**, click the **Create Group** button.

Enter a group name.

If the new group should be a sub-group of an existing group, enable the Parent Group option and select the appropriate group from the list.

Description is optional.

Click **OK** to save the new group.



The screenshot shows a dialog box titled "Create Port Group". It has a close button in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "Executive Staff".
- Parent Group:** A checkbox that is unchecked, followed by a dropdown menu currently showing "Access Point Management".
- Description:** A text area containing the text "Always allow access."
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 173: Create Port Group

### Policy Details

Policy Details assesses the selected host or user and displays the specific profile and policies that apply to the host at the moment the dialog was opened. User/host profiles have a time component and hosts may be connected at different locations. Therefore, the profile and policy displayed in Policy Details now, may be different than the profile and policies that display tomorrow. Policies displayed in this view include: Network Access Policies, Endpoint Compliance Policies, Supplicant Policies and Portal Policies. Each type of policy is displayed in a separate tab that also contains a Debug Log. This log can be sent to Customer Support for analysis.

To access Policy Details from Host View:

1. Select **Hosts > Host View**.
2. Search for the appropriate Host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.

To access Policy Details from User View

1. Select **Users > User View**.
2. Search for the appropriate User.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.

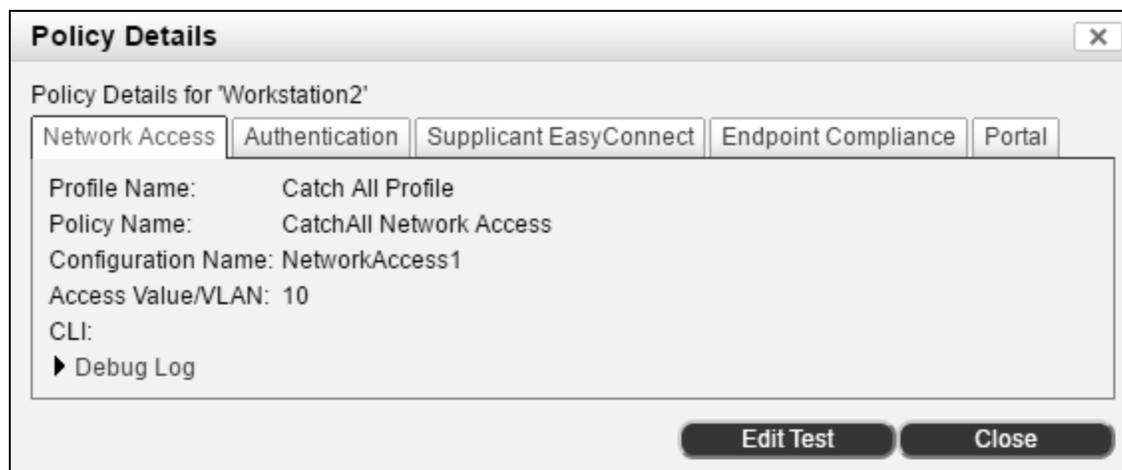


Figure 174: Policy Details - Network Access Tab

### Network Access Tab Field Definitions

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Network Access Policy that currently applies to the host.
<b>Configuration Name</b>	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host.
<b>Access Value/VLAN</b>	The specific network access that would be provided to the host, such as a VLAN ID or Name.
<b>CLI</b>	Name of the CLI Configuration that currently applies to this host or the connection port. This field may be blank.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

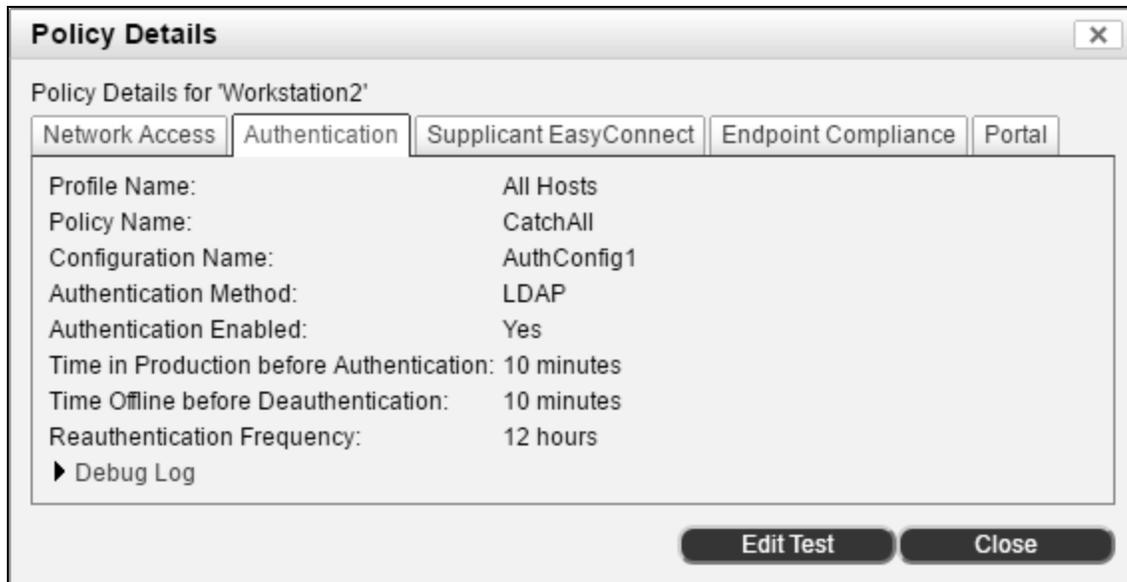


Figure 175: Policy Details - Authentication Tab

### Authentication Tab Field Definitions

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Network Access Policy that currently applies to the host.
<b>Configuration Name</b>	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host.
<b>Authentication Method</b>	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
<b>Authentication Enabled</b>	Indicates whether Authentication is enabled. When enabled, the user is authenticated against a directory, the Network Sentry database, or a RADIUS server when logging on to access the network.
<b>Time in Production before Authentication</b>	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the Authentication VLAN.

Field	Definition
<b>Time Offline before Deauthentication</b>	Once the machine is offline, the user remains authenticated for this period of time. If the machine comes back online before the time period ends the user does not have to reauthenticate. If the machine comes back online after the time period ends, the user is required to re-authenticate.
<b>Reauthentication Frequency</b>	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

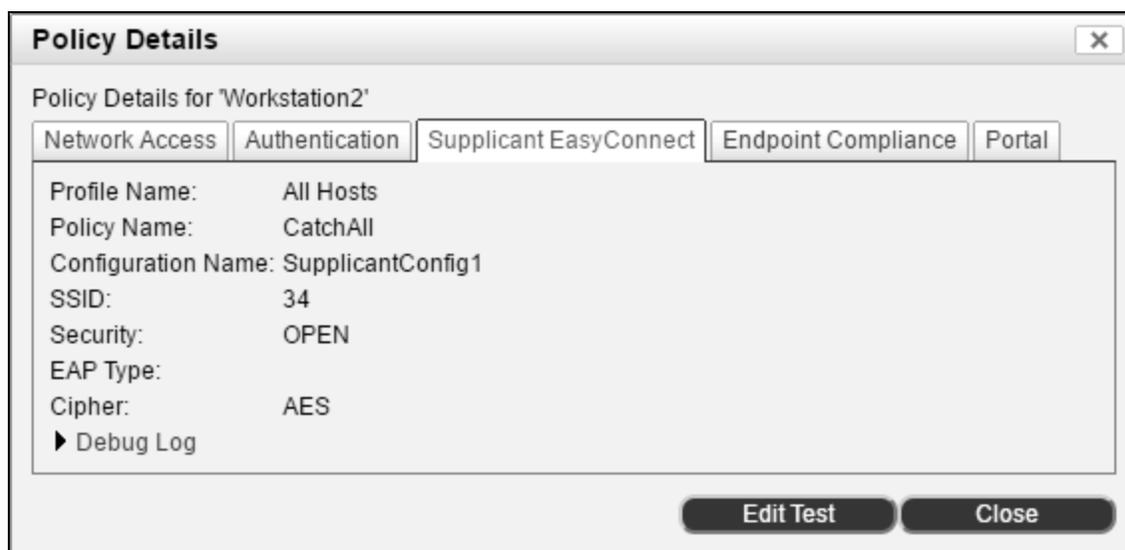


Figure 176: Policy Details - Supplicant EasyConnect Tab

### Supplicant EasyConnect Tab Field Definitions

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Supplicant Policy and Supplicant Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the most recent Supplicant Policy that currently applies to the selected host.
<b>Configuration Name</b>	Name of the configuration that applies to the selected host. This is the configuration for the supplicant on the host to allow access on a particular SSID.

Field	Definition
<b>SSID</b>	Name of the SSID for which the supplicant is being configured.
<b>Security</b>	Type of encryption that used for connections to this SSID, such as WEP or WPA.
<b>EAP Type</b>	Currently only PEAP is supported. Not always required. This field may be blank.
<b>Cipher</b>	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

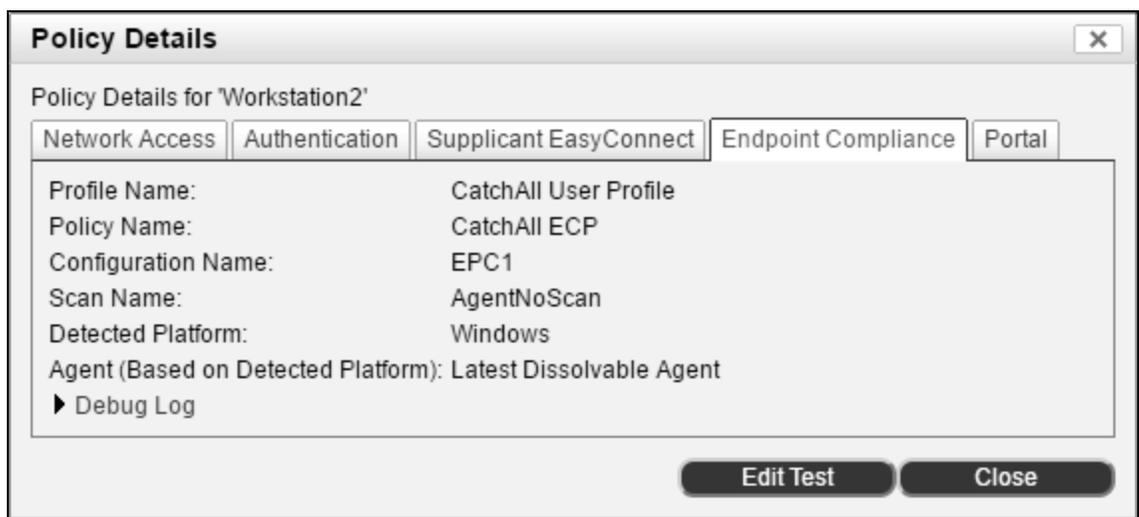


Figure 177: Policy Details - Host View - Endpoint Compliance Tab

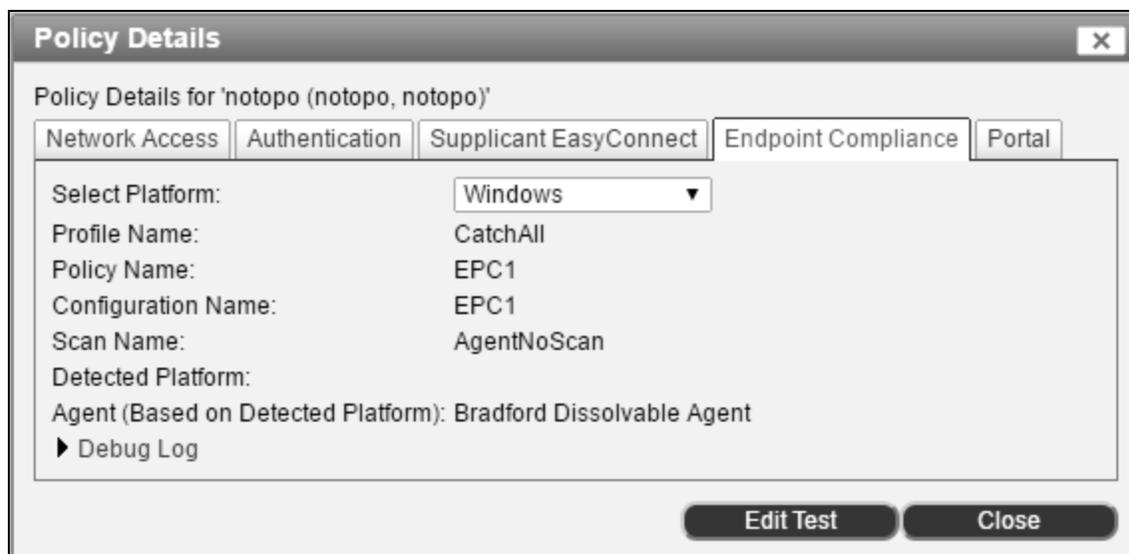


Figure 178: Policy Details - User View - Endpoint Compliance Tab

### Endpoint Compliance Tab Field Definitions

Field	Definition
<b>Select Platform</b>	When the Policy Details option is selected from the User View, you must select the Platform of the device that the user anticipates connecting to the network. The platform is used to determine the agent that would be assigned to the host.  Not all platforms are displayed here. Only the platforms that support the Persistent or Mobile Agents.
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Endpoint Compliance Policy and Endpoint Compliance Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Endpoint Compliance Policy currently applies to the selected host. See Endpoint Compliance Policies on page 525.
<b>Configuration Name</b>	Name of the configuration that currently applies to the selected host. This is the configuration for the Scan and Agent for the host. See Endpoint Compliance Configurations on page 536.
<b>Scan Name</b>	Name of the scan that would be used to evaluate this host. See Scans on page 545.
<b>Detected Platform</b>	The device type, such as iPhone or Android, that Network Sentry thinks the host is, based on the information currently available in the system.
<b>Agent</b>	Agent setting that would be applied to the host. Determines whether or not an agent is used and which agent is required. Agent settings are selected in the Endpoint Compliance Configuration.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.



Figure 179: Policy Details - Portal Tab

### Portal Tab Field Definitions

Field	Definition
<b>Profile Name</b>	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location. Host connections that match the criteria within the User/Host Profile are assigned the associated Portal Configuration. See User/Host Profiles on page 511.
<b>Policy Name</b>	Name of the Portal Policy that was applied to the host.
<b>Configuration Name</b>	Name of the Portal Configuration that applied to the host.
<b>Debug Log</b>	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

### Guest User Account Details

Guest User records created when Guest accounts are generated are displayed in the Users View with network and administrator users. The Guest Account Details window displays data from the Guest Template used to create the Guest User. To access Guest Account Details:

1. Select **Users > User View**.
2. Search for the appropriate User.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Guest Account Details**.

Guest Account Details	
User ID:	jjones@hotmail.com
Account Status:	Enabled
Sponsor:	root
Account Type:	Guest
Start Date:	05/24/12 01:24 PM EDT
End Date:	05/27/12 01:24 PM EDT
Login Availability:	Always
Role:	Guest
Authentication:	Local
Account Duration:	72 hours
Reauthentication Period:	48 hours
URL for Successful Landing Page:	http://www.cnn.com
URL for Acceptable Use Policy:	http://www.bbc.com
Password:	*****
<input type="button" value="Show Password"/>	
<input type="button" value="Close"/>	

Figure 180: Guest Account Details

Table 24: Guest Account Details - Field Definitions

Field	Description
<b>User ID</b>	Guest's email account which is used as the User ID at login.
<b>Account Status</b>	Indicates whether the guest account is enabled or disabled.
<b>Sponsor</b>	The administrator who created the guest account.
<b>Account Type</b>	<p>Guest account type. Types include:</p> <p><b>Guest</b>—A visitor to your facility with limited or Internet-only network access.</p> <p><b>Conference</b>—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days.</p> <p><b>Contractor</b>—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.</p>
<b>Start Date</b>	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
<b>End Date</b>	Date and time the account will expire.
<b>Login Availability</b>	Times during which the guest is permitted to access the network.

<b>Field</b>	<b>Description</b>
<b>Role</b>	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.
<b>Authentication</b>	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.
<b>Account Duration</b>	Amount of time this account will remain valid and usable.
<b>Reauthentication Period</b>	Number of hours the guest or contractor can access the network before reauthentication is required.
<b>URL for Successful Landing Page</b>	Directs the guest or contractor to a specific web page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.
<b>URL for Acceptable Use Policy</b>	Directs the guest or contractor to a specific web page that details the acceptable use policy for the network.
<b>Password</b>	The Guest's assigned password. Passwords are usually generated by the system unless the guests were bulk imported. Toggle the <b>Show Password/Hide Password</b> button to alternately display the password in plain text or as asterisks.

## Set User Expiration Date

The expiration date on a user determines when the user record is automatically deleted or aged out of the database. Administrator Users default to No Expiration. See **Aging Out Host Or User Records** on page 381 for information on other methods.

**Note:** Admin Users assigned the Administrator Profile cannot be aged out.

The screenshot shows a dialog box titled "Set User Expiration". It has a close button in the top right corner. The dialog contains the following options:

- Set User Expiration
  - Specify Date: [text box] [calendar icon]
  - Days Valid from Now: [text box with value 300]
  - Days Valid from Creation: [text box]
  - No Expiration
  - Default Expiration
- Set User Inactivity Limit
  - Days Inactive: [text box with value 30]
  - No Inactivity Limit
  - Default Inactivity Limit
- Delete Registered Hosts

At the bottom of the dialog are two buttons: "OK" and "Cancel".

**Figure 181: Set User Expiration**

The Set User Expiration Date feature can be accessed either from the User View or the Host View.

1. Select **Users > User View**.
2. Use the Quick Search or Custom Filter to locate the appropriate User(s).
3. Select the users to be modified.
4. Right-click or click Options and select **Set User Expiration**.
5. Use the field definitions table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Table 25: Set User Expiration - Field Definitions

Field	Definition
<b>Specify Date</b>	Allows you to select a specific date that the user will be aged out of the database.
<b>Days Valid From Now</b>	Enter the number of days from today that you would like the user to expire. The expiration date is calculated based on this number.
<b>Days Valid From Creation</b>	This is the number of days from the date the user record was created. The expiration date is calculated based on this number.
<b>No Expiration</b>	This user is never deleted from the database even if global or group aging options are added or modified.
<b>Default Expiration</b>	Defaults to the global aging settings configured in <b>System &gt; Settings &gt; User/Host Management &gt; Aging</b> .
<b>Set User Inactivity Limit</b>	Enables the option to delete a user based on the number of days that the user did not log onto the network or into the Admin UI.
<b>Days Inactive</b>	Number of consecutive days the user must be inactive to be aged out of the database. For example, if this is set to 4 days, and after 2 days the user connects to the network again, the counter is restarted.
<b>No Inactivity Limit</b>	With this option enabled, the user is never deleted from the database due to inactivity even if global or group aging options are added or modified.
<b>Default Inactivity Limit</b>	Defaults to the global aging settings configured in <b>System &gt; Settings &gt; User/Host Management &gt; Aging</b> .
<b>Delete Registered Hosts</b>	If enabled, hosts registered to the selected user are deleted when the user ages out of the database. It is recommended that you delete hosts with the user or they become registered devices when the user ages out of the database.





## Guest/Contractor Templates

Admin Users can be accessed from **Users > Guest/Contractor Templates**.

As an administrator, you control Guest, Contractor, Conference and Self-Registration accounts by creating templates for each account type. The templates include privileges you specify, such as account duration, and credential requirements. Each time a visitor account is created one of these templates must be applied.

The templates you define:

- Restrict or allow certain privileges for the sponsors who create guest, contractor, and conference accounts.
- Ensure that sponsors set up appropriate accounts for guests and contractors.
- Define the number of characters in the automatically generated passwords.
- Make sure data from the guest or contractor is provided to the sponsor.

You may grant sponsor privileges to an administrative user who uses the templates to create and manage temporary guest and contractor accounts. Sponsors may also provide account details to guests by email, sms message or printout. The entire process, from account creation to guest network access, is stored for audit and reporting.

From the Guest/Contractor Templates window you can add, delete, modify or copy templates.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Visitor Type	Authentication	Login Availability	Password Length	Password Exclusions	Account Duration	Reauth Period	Last Modified By
Yes	GuestSelfRegistration	Self Registered Guest	Local	Always	6	!@#%&'()*+~{} " '<>?-= [ \ /	24 hours		SYSTEM
Yes	GuestAccess	Guest	Local	Always	8	!@#%&'()*+~{} " '<>?-= [ \ /			SYSTEM
Yes	GuestConference	Conference	Local	Always	8	!@#%&'()*+~{} " '<>?-= [ \ /			SYSTEM

Figure 182: Create Guest/Contractor Template Window

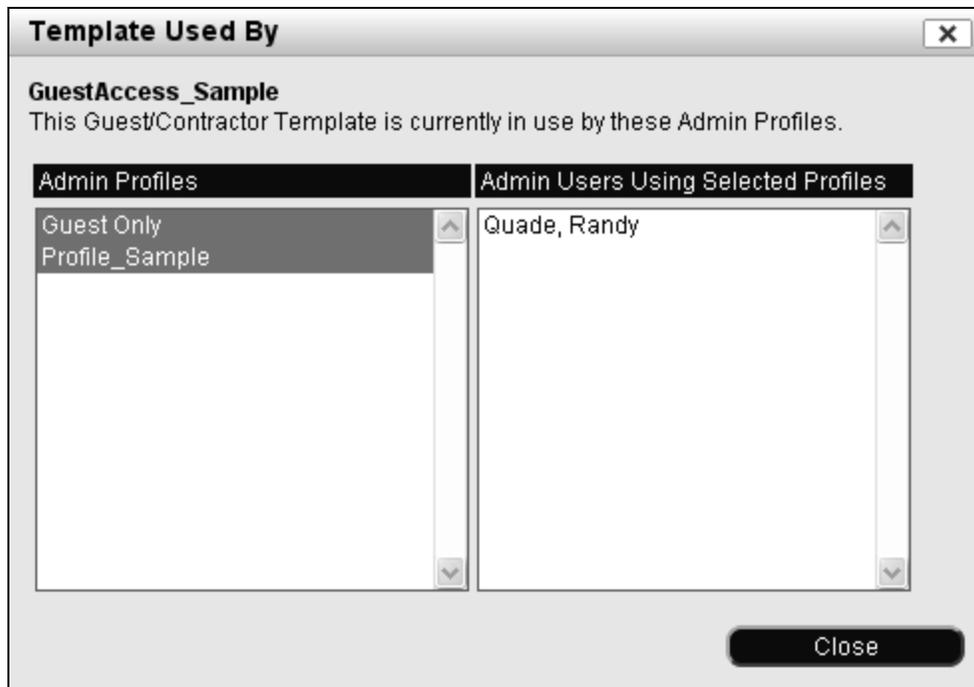
### Guest/Contractor Template Fields

Field	Definition
Global	

Field	Definition
<b>Name</b>	Descriptive name for the template. Sponsors use this name when they select a template to create accounts.
<b>Visitor Type</b>	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See <b>Guest Account Types Or Visitor Types</b> on page 631.
<b>Role</b>	<p>Role is an attribute added to the user and the host. Roles can be used in User-/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it.</p> <p>See <b>Guest Account Types Or Visitor Types</b> on page 631. For more on Roles see <b>Role Management</b> on page 609.</p>
<b>Authentication</b>	<p>Indicates type of authentication used for Guests or Contractors associated with this template. Options include:</p> <p><b>Local</b>—User name and password credentials are stored in the local database.</p> <p><b>Note:</b> For Conference accounts, authentication is Local only.</p> <p><b>LDAP</b>—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.</p> <p><b>RADIUS</b>—Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.</p>
<b>Login Availability</b>	<p>Indicates when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are:</p> <ul style="list-style-type: none"> <li>• Always</li> <li>• Time range</li> </ul> <p>Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.</p>
<b>Password Length</b>	Required length of guest or contractor passwords. Must be between 5 and 64 characters.

Field	Definition
<b>Account Duration</b>	<p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>
<b>Reauth Period (hours)</b>	Number of hours the guest or contractor can access the network before reauthentication is required.
<b>Security &amp; Access Value</b>	User specified text associated with guests created using this template that can be used as a filter. Used to assign a policy to a guest by filtering for this value.
<b>Password Exclusions</b>	List of characters that will not be included in generated passwords.
<b>Last Modified By</b>	User name of the last user to modify the template.
<b>Last Modified Date</b>	Date and time of the last modification to this template.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Import</b>	<p>Enables you to import information from the Network Sentry Server(s) to the FortiNac Control Managers so that during the next Global Synchronization (if enabled), the information will be written to other Network Sentry Servers in your network. This eliminates the need to manually enter the information on the FortiNac Control Manager. When it is imported to the FortiNac Control Manager, the information is treated as global information.</p> <p>The following describes some caveats to consider when importing items:</p> <p>If the name of an item that is being imported already exists on the FortiNac Control Manager, the item will not be imported.</p> <p>If an item being imported from a Network Sentry Server has a dependent item with the same name as a dependent item that already exists on the FortiNac Control Manager, the dependent item is not imported to the FortiNac Control Manager. The item will be imported and use the dependent item that already existed on the Network Sentry Control Manager.</p> <p>For example, if a User/Host Profile called "Student" exists on the FortiNac Control Manager and an Endpoint Compliance Policy is imported from a Network Sentry Server that also uses a User/Host Profile called "Student", the "Student" Profile (dependent item) that exists on the FortiNac Control Manager will not be imported. The Endpoint Compliance Policy will be imported and use the dependent item (User/Host Profile) that was already there. This results in the settings for the Network Sentry Control Manager's Endpoint Compliance Policy's User/Host Profile possibly differing from the Endpoint Compliance Policy's User/Host Profile on the FortiNac Control Manager.</p>

Field	Definition
<b>Export</b>	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Copy</b>	Copy the selected Template to create a new record.
<b>Delete</b>	Deletes the selected Template. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.
<b>Modify</b>	Opens the Modify Guest/Contractor Template window for the selected template.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446
	<b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Used By</b>	Display a list of users by Admin Profile that are associated with the selected template. Click on a specific Admin Profile to see the associated users. To select more than one profile use the Ctrl key.



**Figure 183: Guest/Contractor Template Used By**

---

## Guest Account Types Or Visitor Types

Guest Manager supports four basic types of accounts. They are identified on the Guest templates as Visitor types and are loosely defined as follows:

**Guest**—A visitor to your facility with limited or Internet-only network access. For example, a guest might be on the premises for a one-day sales call or a three-day presentation. Any number of guest accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

**Self-Registered Guest**—A visitor to your facility with limited or Internet-only network access who connects to your network on their own device to request a temporary account. The account request goes to a sponsor via e-mail. The sponsor can log into Network Sentry and approve or deny the request or, depending on your configuration, can approve or deny the request for the account directly from the e-mail. The account is created when the request is approved.

**Conference**—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. Conferences are often bulk accounts, in which attendees receive notification of the conference via, for example, email. Conference members may be given an identical generated user name and password that is specific to the conference—for example, *conference-1* or *training123*, individual passwords for individual attendees, or individual attendee names with a shared password. See **Conference Accounts** on page 673. When the conference members register they enter their email address. Once they have registered, they fill in their name and other information.

**Contractor**—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months. Any number of contractor accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

---

## Create Guest/Contractor Templates

Use this option to create multiple templates for each of the Guest, Contractor, Conference and Self-Registered Guest visitor types with a variety of permissions. Data fields allow you to collect data from your guests and store it in User Properties. If you are a Network Sentry administrator you have access to all templates and can assign any template of the correct type to any guest, contractor or conference user when you create their accounts. If you choose to create a sponsor user who is responsible for creating visitor accounts, the sponsor must be assigned a set of templates through the Admin Profile. When the sponsor creates visitor accounts, he can only choose templates from the list you have assigned.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Templates window appears. Click **Add**.
4. The **Add Guest/Contractor Template** window appears. Enter the information in the **Required Fields** tab as described in **Guest/Contractor Template Required Fields** on page 436.
5. Click the **Data Fields** tab to determine which fields will be required when a guest logs onto the network.
6. Click the **Note** tab to add a note to the printed access information to give the guest/contractor special login instructions or an SSID. See **Provide Account Information To Guest Or Contractor** on page 671.
7. Click **OK** to create the template and add it to the list of templates.

**Add Guest/Contractor Template** [X]

Required Fields | Data Fields | Note

Template Name:

Visitor Type:

Role:  Use a unique Role based on this template name  
 Select Role:

Security & Access Value:

Username Format:   Send Email  Send SMS

Password Length:

Password Exclusions:

Reauthentication Period:  (hours)

Authentication Method:   Account Duration:  (hours)

Login Availability:

URL for Acceptable Use Policy (optional)   IP Address of URL

[Portal Version 1 Settings](#)

**Figure 184: Guest/Contractor Template - Required Fields Tab**

---

## Guest/Contractor Template Required Fields

All possible fields are included in this table. The fields shown on your screen will vary depending on the Visitor Type you select.

Field	Definition
<b>Template Name</b>	Type a descriptive name for the template. Sponsors use this name when they select a template to create accounts.
<b>Visitor Type</b>	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See <b>Guest Account Types Or Visitor Types</b> on page 631.
<b>Use A Unique Role Based On This Template Name</b>	<p>Creates a role based on the template name and assigns that role to guests with accounts created using this template. Using the template name as a role allows you to limit network access based on the Guest Template by using the new role as a filter in a User/Host Profile. See User/Host Profiles on page 511.</p> <p>When using the Wireless Security feature to configure SSID mappings, the name of the Guest Template selected is used to create the appropriate User/Host Profile allowing you to limit SSID access based on Guest Template.</p>
<b>Select Role</b>	<p>Role is an attribute added to the user and the host. Roles can be used in User/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it.</p> <p>See <b>Guest Account Types Or Visitor Types</b> on page 631. For more on Roles see <b>Role Management</b> on page 609.</p>
<b>Security &amp; Access Value</b>	Enter a value, such as, Guest or Visitor. This field is added to each guest user account that is created based on this template and can be used as a filter. When creating User/Host Profiles, you can filter for the contents of the Security & Access Value field to control which Endpoint Compliance Policy is used to scan guest hosts.
<b>Send Email</b>	<p>For Conference accounts, email cannot be sent until a guest has registered or you have modified the account via the <b>User View &gt; Modify</b> option to enter an email address.</p> <p>Select this check box if you want a sponsor with this template to be able to send an e-mail confirmation to the guest's/contractor's email address. If not selected (default) guest or contractor credentials need to be printed or sent via SMS.</p> <p>For Self-Registered Guest accounts this option is automatically checked and cannot be disabled.</p>

Field	Definition
<b>Send SMS</b>	<p>For Guest or Contractor accounts, select this check box if you want a sponsor with this template to be able to send an SMS confirmation to the guest's/contractor's mobile phone. If not selected guest or contractor credentials need to be e-mailed or printed.</p> <p>For Self-Registered Guest accounts this option is automatically checked and cannot be disabled.</p> <p>Requires that the guest or contractor provide both a mobile number and the mobile provider. These fields default to Required in the Data Fields tab.</p>
<b>Max Number Of Accounts</b>	<p>Only available when Visitor Type is set to Conference. Typically used when generating a large number of accounts for a conference. Limits the total number of accounts that can be created on the Conference Account window when this template is selected.</p> <p>To limit accounts, enable the check box and enter the maximum number of accounts that can ever be created using this template.</p> <p>For an unlimited number of accounts, leave the check box empty.</p>
<b>Password Length</b>	<p>Between 5 and 64 characters. Passwords that are automatically generated by Guest Manager contain at least one capital letter, one lower case letter, one alphanumeric character, and one symbol. If you have characters listed in Password Exclusions, those characters will not be used.</p> <p>Note that for Conference accounts, once a template has been created, the sponsor may specify the individual different passwords for attendees when the sponsor creates the conference account. See <b>Conference Accounts</b> on page 673.</p> <p><b>Note:</b> Network Sentry does not recognize or restrict system-generated passwords that may be offensive.</p>
<b>Password Exclusions</b>	List of characters that will not be included in generated passwords.
<b>Use Mobile Friendly Exclusions</b>	<p>Removes any existing entries and then populates the Password Exclusions field with a list of symbols that are typically difficult to enter on a mobile device. Modify the list of characters as needed. Characters include:</p> <p>!@#\$\$%^&amp;*()_+~{} :"&lt;&gt;?.-=[]\';/</p>
<b>Reauthentication Period (hours)</b>	Specify the number of hours the guest or contractor can access the network before reauthentication is required. To specify a reauthentication period you must first select the check box. Next fill in the reauthentication period in hours. If you do not select this check box, you will not have to specify a reauthentication period for guests or contractor accounts created with this template.

Field	Definition
<b>Authentication Method</b>	<p>Specify where authentication occurs:</p> <p><b>Local</b>—User name and password credentials are stored in the local database.</p> <hr/> <p><b>Note:</b> For Conference accounts, authentication is Local only.</p> <hr/> <p><b>LDAP</b>—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.</p> <p><b>RADIUS</b>—Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access. PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from Network Sentry, such as the user name and password for the Validation Account used for communication between Network Sentry and the RADIUS server.</p> <p>If you are using an integrated RADIUS server and Authentication Method is set to RADIUS, single guest accounts created using this template will also generate a RADIUS User record in the RADIUS Users view.</p>
<b>Account Duration</b>	<p>Select the check box to specify the duration of the account in hours.</p> <p>For all guests except those with shared conference accounts: The duration governs how long from creation the account remains in the database, regardless of the end date that is entered when creating the guest account.</p> <p>For shared conference accounts: The duration governs how long from guest Login the account remains in the database, regardless of the end date that is entered when creating the conference.</p> <p>For Self-Registered Guest accounts this option is automatically checked and cannot be disabled. You must enter a duration.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

Field	Definition
<b>Propagate Hosts</b>	Controls whether the Propagate Hosts setting is enabled or disabled on the user record for guest users created with this template. If enabled, the record for the host owned by the guest user is copied to all managed Network Sentry appliances. This field is only displayed if the Network Sentry server is managed by a FortiNac Control Manager.
<b>Login Availability</b>	Select when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration.  The available options are: <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify Time: If you select this option, a window displays in which you specify the time range and select the days of the week. Click OK.</li> </ul> Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
<b>URL for Acceptable Use Policy</b>	Optional. Directs the guest or contractor to the page you specify with the network policies when they login.
<b>Resolve URL</b>	Click to acquire the IP addresses for the URLs for Acceptable Use Policy and Successful Landing page. If the URL is not reachable, specify the IP Address in the IP Address field.
<b>Portal Version 1 Settings</b>	
<b>URL for Successful Landing Page</b>	Directs the guest or contractor to a certain page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.  If you are using the portal pages included with Network Sentry and controlled by the Content Editor in the Portal Configuration, this field is ignored.

### [Login Availability Time For A Guest Template](#)

This option allows you to limit network access for a guest or contractor based on the time of day and the day of the week. Any guest associated with a template, can only access the network as specified in the Login Availability field for the template.

If you set times for Login Availability, Network Sentry periodically checks the access time for each guest associated with the template. When the guest is not allowed to access the network the host associated with the guest is marked "At Risk" for the Guest No Access admin scan. When the time is reached that the guest is allowed to access the network, the "At Risk" state is removed from the host. These changes in state occur on the guest host record whether the guest is connected to the network or not. If the guest host connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your Network Access has been disabled. You are outside of your allowed time window. To regain network access call the help desk."

Data Field	Guest/Contractor
First Name	Required ▼
Last Name	Required ▼
Address	Required ▼
City	Required ▼
State	Required ▼
Country	Required ▼
Zip/Postal Code	Required ▼
Email	Required
Phone	Required ▼
Mobile Number	Required ▼
Mobile Provider	Required ▼
Asset	Required ▼
Person Visiting	Required ▼
Reason	Required ▼

**Figure 185: Guest/Contractor Template - Data Fields Tab**

### **Guest/Contractor Data Fields**

Specify which pieces of data will appear on the form the guest or contractor will be required to fill out in the captive portal. For Self-Registered Guests this information is filled out with the request for an account. For Guests with an existing account, this information is filled out after they enter their user name and password on the login page. If the field has a corresponding database field, it is stored there and displayed on the User Properties window. If the field does not have a corresponding database field, it is stored and displayed in the Notes tab of the User Properties window and the Host Properties window. Hover over the field name to display a tool tip indicating where the data entered by the guest will be stored.

- **Required**—The data in this field must be entered in order for the guest or contractor to log in.
- **Optional**—Appears on the form, but is not required data from the guest or contractor.
- **Ignored**—Will not appear on the form.

The E-mail Field is required. The fields listed below are default fields that are included with the original setup of Guest Manager. Field names can be modified by typing over the original name. Therefore, the fields on your template window may not match any of the fields in this list. If you rename a field, the data entered into that field by the guest is still stored in its original location. For example, if you modify the title of the Last Name field to say Mother's Maiden Name, the data is still stored in the Last Name field on the User Properties window.

Original Field Name	Definition
<b>Last Name</b>	Maximum length 50 characters. Stored in the Last Name field.
<b>First Name</b>	Maximum length 50 characters. Stored in the First Name field.
<b>Address</b>	Maximum length 50 characters. Stored in the Address field.
<b>City</b>	Maximum length 50 characters. Stored in the City field.
<b>State (or Province/County)</b>	Standard two-letter state abbreviation, or up to 50 characters. Stored in the State field.
<b>Country</b>	Maximum length 50 characters. Stored on the Notes tab.
<b>Zip or Postal Code</b>	Maximum length of 16. Stored in the Zip Code field.
<b>Email</b>	Email address of the guest or contractor. Stored in the E-mail field.  <b>Important:</b> This field can be modified however Network Sentry expects the contents of the field to be an email address. This field tests for a valid email address and will not allow the user to proceed without one. If the label is something other than email and other types of data are entered, the guest account may not be able to be created.
<b>Phone</b>	Telephone number including international country codes (for example, +1, +44). Maximum length 16. Stored in the Phone field.
<b>Mobile Phone</b>	Mobile Telephone number. Maximum length 16. Stored in the Add/Modify User window.
<b>Mobile Provider</b>	The name of the company that provides the guest with Mobile service. The guest is provided with a list of possible providers. Stored in the Add/Modify User window.
<b>Asset</b>	Text field for computer serial numbers, manufacturer's name and model number, or any other asset identifier of the guest's or contractor's computing platform. Stored in the Serial Number field. Max.length 80 characters.

Original Field Name	Definition
<b>Reason</b>	The reason for the guest's or contractor's visit. Max. length 80 characters. Stored on the Notes tab.
<b>Person Visiting</b>	Maximum length 50 characters. Stored on the Notes tab.
<b>Buttons</b>	
<b>Add Field</b>	<p>Click to add new data fields to track additional guest or contractor data, such as license plate numbers or demo equipment details. Maximum length 80 characters.</p> <p>Type the name of the field in the pop-up window. Select whether to make the field required or optional.</p> <p>Once new fields have been added they are stored in the Notes tab of the user's account. To see these fields go to the User Properties window.</p>
<b>Delete Field</b>	Click this button to delete a data field from the list. Only those fields that have been created by an Admin user can be deleted. System fields can be set to ignore so they do not display, but cannot be deleted from the template.
<b>Reorder Fields</b>	Changes the order of the fields as they appear in the Guest or Contractor Form. Click this button to reorder account information fields. In the pop-up window, click Move Up or Move Down and OK.

### **Guest/Contractor Note**

The Notes tab on the template creation window allows you to provide additional information to guests and contractors. After you have created a Guest or Contractor account, you may want to provide that user with his login information. Login information can be printed, viewed on the screen, sent via text message to a mobile telephone or included in an e-mail. The text added on the Notes tab is appended to the guest information included in the printout, email or text message. See **Provide Account Information To Guest Or Contractor** on page 671 for additional information.

---

## Assign An Endpoint Compliance Policy To A Guest

Endpoint Compliance Policies and the agents that run associated scans are assigned based on the rules contained within the Policy. Network Sentry selects a scan and an agent by comparing guest and host data to the User/Host Profile in each policy beginning with the policy ranked number 1 until a match is found. When a match is found the scan and agent are assigned and the guest's computer is scanned. If you want to create a specific policy for guests, you must define a policy that searches for user data that only guests will match and place it at the beginning of the list of policies.

### **Example 1**

In this example the policy will apply to guests based on their Role. Create a policy that has the following settings:

#### **User/Host Profile**

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Role and enter the name of the Role assigned to guests. Typically the Role is named Guest, but you may have chosen to use a different role for Guests. Roles are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

#### **Scan**

- **Scan** — Create a scan to evaluate guest computers for compliance.

#### **Endpoint Compliance Configuration**

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

#### **Endpoint Compliance Policy**

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

---

## **Example 2**

In this example the policy will apply to guests based on their Security & Access Value. Create a policy that has the following settings:

### **User/Host Profile**

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Security & Access Value and enter the name of the Security & Access Value assigned to guests. These values are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

### **Scan**

- **Scan** — Create a scan to evaluate guest computers for compliance.

### **Endpoint Compliance Configuration**

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

### **Endpoint Compliance Policy**

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

---

## Modify Templates

To change information or parameters in a template, do the following:

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Modify**. Change the name of the template, or other information and parameters.

**Note:** Once the template has been modified the modifications will only apply to new accounts created from the template. All old accounts made from the template remain the same.

5. Click **OK**.

## Copy Templates

You may copy a template, save it under another name, and use it as the basis for a new template.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Copy**.
5. Change the name of the template, or other information and parameters.
6. Click **OK**.

## Delete Templates

You may delete a template at any time. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The **Guest/Contractor Template Management** window opens with a list of created templates.
4. Select the template and click **Delete**. A confirmation message is displayed. Click **Yes** to delete the template.

## Chapter 10: Admin Auditing

The Admin Auditing log tracks all changes made to an item in the system. Users with Admin Auditing permissions will see a change in the Admin Auditing log whenever data is added, modified, or deleted. Users can see what was changed, when the change was made, and who made the change.

**Note:** Changes made to Hosts, Users, or Adapters are not displayed in the Admin Auditing Log on the NCM. These changes are visible in the Admin Audit Log on each server.

Changes can be filtered by the name of the item that was changed, the action taken, the date when the change occurred, the user ID for the user who made the change, and the type of item that was changed.

**Note:** Similar to Events and Alarms, Admin Auditing archives and purges audits made to Hosts, Users, or Elements.

### Configuration

Users must have the Admin Auditing permissions in order to view the Admin Auditing log.

1. Click **Users > Admin Profiles**.
2. Select an admin profile from the list.
3. Click **Add** or select an admin profile and click **Modify**.
4. Select the **Access** check box next to **Admin Auditing**.
5. Click **OK**.

### Accessing the Admin Auditing Log

1. Click **Logs > Admin Auditing**.
2. Click a row to view the entire list of changes in Audit Details.

Filter (Not Applied)					
Date: Last 1 Days					
Add Filter: Select Update					
Admin Auditing - Total: 5					
<< first < prev 1 next > last >> 200					
Date	User ID	Action	Type	Name	Summary
10/11/16 11:34 AM GMT-0400	root	Add	Element		Request String set to: 192.168.65.122 Element Class set to: Network-Control-Server Status set to: Unknown Contact Status Polling Interval set to: 10 minutes More...
10/11/16 11:34 AM GMT-0400	root	Delete	Element	playdonpod2	Element playdonpod2 deleted
10/11/16 10:49 AM GMT-0400	root	Add	Element		Request String set to: 192.168.65.122 Element Class set to: Network-Control-Server Status set to: Unknown Contact Status Polling Interval set to: 10 minutes More...
10/11/16 10:47 AM GMT-0400	root	Delete	Element	playdonpod2	Element playdonpod2 deleted
10/11/16 09:48 AM GMT-0400	root	Add	Element		Request String set to: 192.168.65.122 Element Class set to: Network-Control-Server Status set to: Unknown Contact Status Polling Interval set to: 10 minutes More...
Export to:					
Audit Details					
Request String set to: 192.168.65.122 Element Class set to: Network-Control-Server Status set to: Unknown Contact Status Polling Interval set to: 10 minutes Contact Status Polling Enabled set to: true					

Figure 186: Admin Auditing Log

3. Click the name of the item that was changed to open a dialog displaying all changes that have been made to the item.

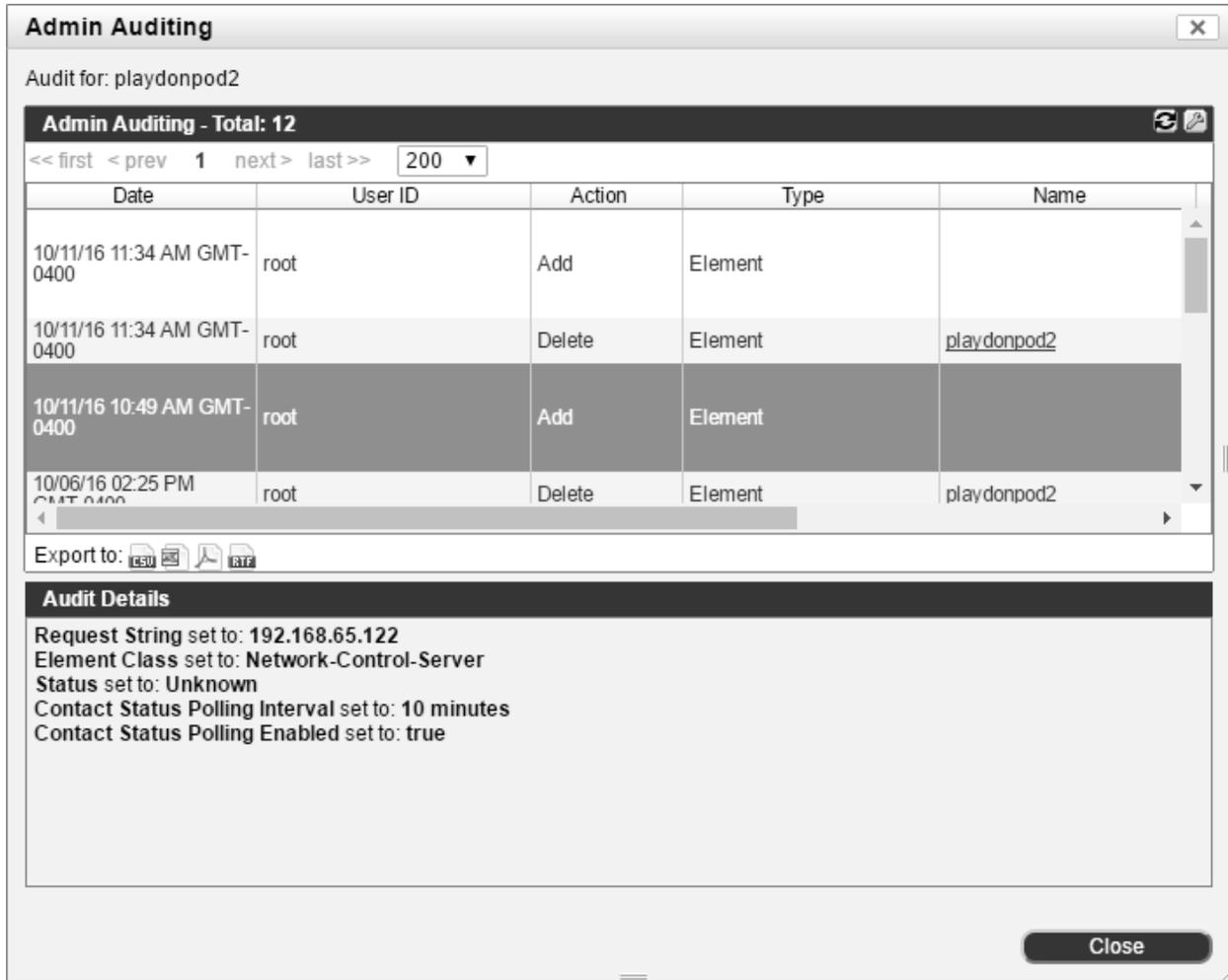


Figure 187: Admin Auditing Dialog - All Changes

**Admin Auditing Log Field Definitions**

Field	Definition
<b>Add Filter drop-down list</b>	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See <b>Filters</b> on page 59.
<b>Update button</b>	Displays the filtered data in the table.
<b>Admin Auditing</b>	
<b>Date</b>	The date and time when the change was made.

Field	Definition
<b>User ID</b>	The user ID of the user who made the change.
	<b>Note:</b> The user ID appears as "CLI Tool" when changes are made using CLI tools.
<b>Action</b>	Shows whether the change involved adding, modifying, or deleting information.
<b>Type</b>	The type of item that was changed.
<b>Name</b>	The name of the item that was changed. Click the name to view a dialog containing all changes that have been made to the area.
<b>Summary</b>	The first four lines of what was changed on the specified date.
<b>Audit Details</b>	Displays all details of the change made to the item on the specified date. This information appears when you click a row representing a change in the Admin Auditing table.
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.



# Chapter 11: Event Management

Event Management allows you to specify which events to generate and whether to log the event records on another server in addition to the local appliance. You can limit the number of events generated by selecting a group for each event. Event messages are only created when the event occurs within the specified group.

Specify threshold values for the Self-Monitoring Events by clicking the Event Thresholds button at the top of the view. These thresholds affect the Performance Summary Panel on the Dashboard. They can be edited here or from the Performance Summary Panel. See for additional information.

Some events are generated frequently and may not be necessary for day to day operations. Review the list of events and determine which ones to enable to provide you with the most useful feedback. You may choose to enable an event for a short period of time, such as to find a particular host when it connects to the network. See the example below for a scenario in which enabling a particular event might be useful.

## **Example: Finding A Stolen Device**

This is a scenario for locating a stolen or missing host machine:

1. Create a group that contains only the information for that host machine (including all wired and wireless sibling records).
2. Enable the Host Connected event for the new group. When the stolen machine connects to the network through the wired or wireless connection, a Host Connected event is generated.
3. Map the Host Connected event to an alarm to receive a notification that the machine has connected. You may also take an action against that host machine if you specified one in the mapping.
4. When you are notified that the stolen machine has connected to the network, use the Host View to determine the device and port to which this machine is connected.

Events are generated for all components, such as devices, hosts or ports, unless you reduce the output by selecting a specific group. See **Network Sentry Events And Alarms List** on page 469 for event definitions.

Events can be sent to an external log host. See **Log Events To An External Log Host** on page 458.

To access the Events View select **Logs > Event Management**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

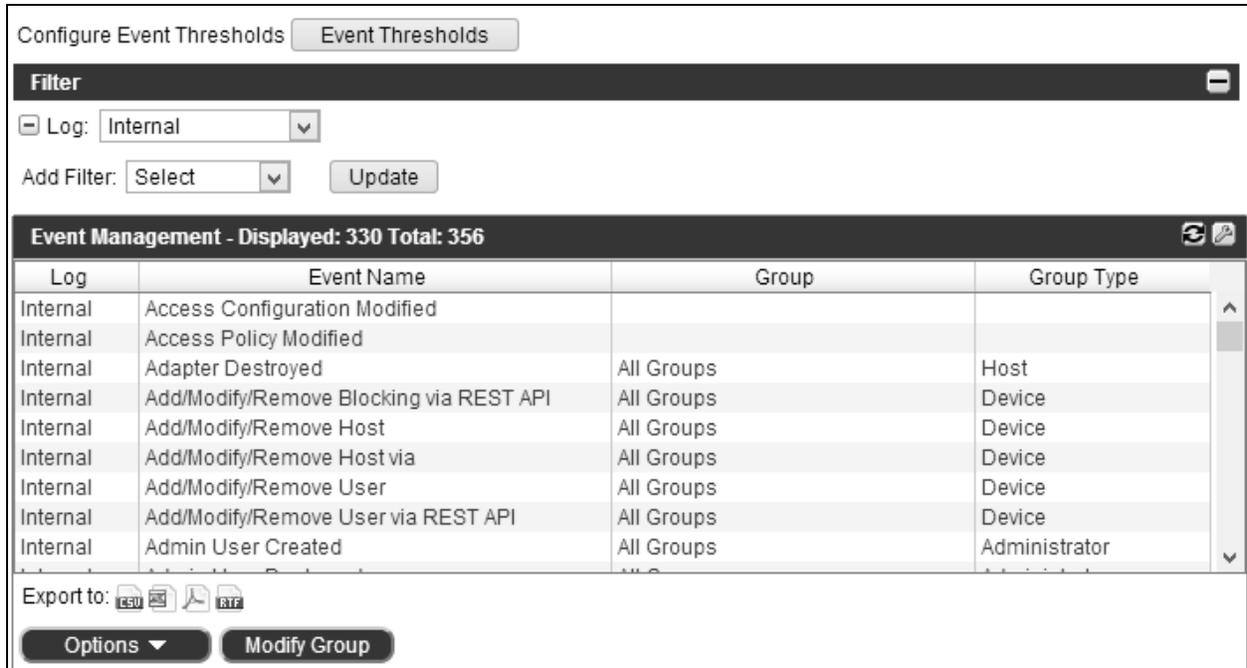


Figure 188: Event Management

**Event Management Field Definitions**

Fields used in filters are also defined in this table.

Field	Definition
<b>Event Thresholds</b>	Opens the Event Thresholds dialog to set thresholds to monitor license usage, memory usage, process thread counts, and disk space. Exceeding these thresholds generates specific events. See Event Thresholds on page 455.
<b>Events</b>	
<b>Log</b>	Indicates the state of the selected event and where it will be logged if it is generated. <b>Disabled</b> —Event is disabled and will not be generated or logged anywhere. <b>Internal</b> —Logs only to an internal events database. <b>External</b> —Logs only to an external host. <b>Internal &amp; External</b> —Logs both to an internal events database and an external host.
<b>Event Name</b>	Name of the event.

Field	Definition
<b>Group</b>	<p>Group name of a group of elements, such as, port group, device group or user group used to limit generation of the selected event to the items in the group.</p> <p>If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users.</p> <p>If no group is displayed, an event is generated for the system, and not a specific item.</p>
<b>Group Type</b>	Indicates whether this event applies to a group of ports, devices, hosts, users or administrators.
<b>Last Modified By</b>	User name of the last user to modify the event.
<b>Last Modified Date</b>	Date and time of the last modification to this event.
<b>Right Click Options</b>	
<b>Modify Group</b>	Opens the Modify Group window.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Disable Logging</b>	Disables the event is disabled. The event will not be generated or logged anywhere.
<b>Log Internal</b>	Logs the event only to an internal events database.
<b>Log External</b>	Logs the event only to an external host.
<b>Log Internal &amp; External</b>	Logs the event to both an internal events database and an external host.
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Options</b>	Allows you to change the log or group setting for one or more selected events.
<b>Modify Group</b>	Change the group setting for one or more selected events.

## Enable And Disable Events

Use the Event Management window to select which events will be logged.

### Events For The System

1. Click **Logs > Event Management**. The Event Management view appears.
2. Use the Filters to locate the appropriate event. Refer to **Event Management** on page 451 for Filter field definitions.
3. **To enable an event**, select one or more events and click the **Options** button. Select one of the following:
  - a. **Internal**—Logs only to an internal events database.
  - b. **External**—Logs only to an external host.
  - c. **Internal & External**—Logs both to an internal events database and an external host.

**Note:** Any event that is logged is enabled.

4. **To disable an event**, select one or more events and click the **Options** button. Select **Disable Logging**.

**Note:** To log events on an external log host, you must first add the log host to Network Sentry. See **Log Events To An External Log Host** on page 458 for instructions.

### Events For A Specific Group

Logging events for a specific group limits the number of times the event is generated. The event will only be generated for members of the selected group.

1. Click **Logs > Event Management**. The Event Management view appears.
2. Use the Filters to locate the appropriate event. Refer to **Event Management** on page 451 for Filter field definitions.
3. Select one or more events and click the **Options** button. Choose one of the logging options to enable the event.
4. Click the **Modify Group** button.
5. Click in the **Group** drop-down box and select the Group for which this event will be enabled.
6. Click **OK**.

## Event Thresholds

This option allows you to monitor license usage, memory usage, process thread counts, and disk space, and establish thresholds for the processes and hard drives. Each process type has its own thread count and maximum memory allocations. The percentages in the thresholds are not relative to the total memory available on the appliance; they are relative to the maximum amounts of memory that each loader process is allowed to consume.

View the memory allocated to each process in the Performance panel on the Dashboard. The number of threads used by the process is also contained in the panel. See .

When a threshold is exceeded, an event is generated. Each event has an associated alarm which is mapped by default. Each specific event or alarm mapping is configured so that multiple events for a specific process or threshold results in a single alarm. Modify the default mappings in Event to Alarm Mappings. You can also configure a specific action, such as email notification. See **Map Events To Alarms** on page 493 for details.

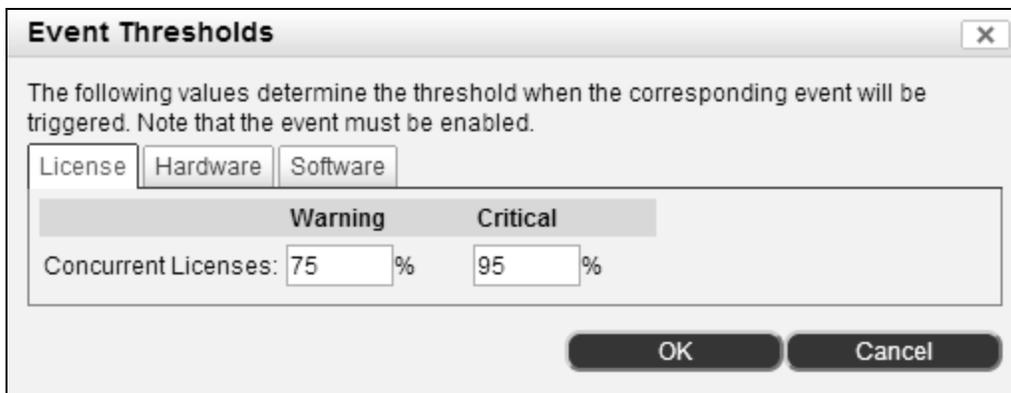
**Table 26: Threshold Field Definitions**

Threshold	Description
<b>License Thresholds</b>	
<b>Concurrent Licenses Warning/Critical</b>	Generated when the license usage threshold is reached. This threshold is a percentage of the total number of licenses configured. Default Warning = 75%. Default Critical = 95%.
<b>Hardware Thresholds</b>	
<b>Hard Disk Usage Warning / Critical</b>	Generated when the disk usage threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default Warning = 85%. Default Critical = 95%.
<b>Memory Usage Warning / Critical</b>	Generated when the memory usage threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.
<b>Network Topology Size Warning / Critical</b>	Generated when the system sizing tool detects that the appliance has reached the threshold for possible connections. This threshold is a percentage of the total connections that the appliance can manage. Default Warning = 85%. Default Critical = 95%.
<b>Software Thresholds</b>	

Threshold	Description
<b>Process Thread Count Warning / Critical</b>	Generated when the process thread count threshold is reached. This threshold is a specific number of threads the process is using. <ul style="list-style-type: none"> <li>• MasterLoader: Default Warning = 500. Default Critical = 575.</li> <li>• Nessus: Default Warning = 100. Default Critical = 125.</li> </ul>
<b>Process Memory Usage Warning / Critical</b>	Generated when the memory usage threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.

**Set Thresholds For Self-Monitoring Events**

1. Click **Logs > Event Management**.
2. Click the **Event Thresholds** button at the top of the window.
3. Click the **License Tab**. Enter the value for the warning and critical levels of the License usage.
4. Click the **Hardware Tab**. Enter the value for the warning and critical levels of the Hardware Thresholds for hard disk and memory usage.
5. Click the **Software Tab**. Enter the value for the warning and critical levels of the Software Thresholds for each system process.
6. Click **OK**.



**Figure 189: Event Management - Thresholds Tab - License Thresholds**

**Event Thresholds** ✕

The following values determine the threshold when the corresponding event will be triggered. Note that the event must be enabled.

License Hardware **Software**

	Warning	Critical
Hard Disk Usage:	85 %	95 %
Memory Usage:	85 %	95 %
Network Topology Size:	85 %	95 %

OK Cancel

Figure 190: Event Management - Thresholds Tab - Hardware Thresholds

**Event Thresholds** ✕

The following values determine the threshold when the corresponding event will be triggered. Note that the event must be enabled.

License Hardware **Software**

	Warning	Critical
MasterLoader/Principal Process Thread Count:	500	580
MasterLoader/Principal Process Memory Usage:	85 %	95 %
Nessus Process Thread Count:	100	125
Nessus Process Memory Usage:	85 %	95 %

OK Cancel

Figure 191: Event Management - Thresholds Tab - Software Thresholds

## Log Events To An External Log Host

To log events on an external log host, you must first add the log host to the Log Receivers View. Once you have added the log host server, configure the events to be logged externally on the Event Management View. The events will be sent as Syslog messages or SNMP Traps.

### Add Log Host Server

Figure 192: Add Log Host

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the IP Address of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Field	Definition
<b>Type</b>	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF).
<b>IP Address</b>	IP Address of the server that will receive Event and Alarm messages.
<b>Port</b>	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default =162

Field	Definition
<b>Facility</b>	<p>Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include:</p> <ul style="list-style-type: none"> <li>0 kernel messages</li> <li>1 user-level messages</li> <li>2 mail system</li> <li>3 system daemons</li> <li>4 security/authorization messages</li> <li>5 messages generated internally by syslogd</li> <li>6 line printer subsystem</li> <li>7 network news subsystem</li> <li>8 UUCP subsystem</li> <li>9 clock daemon</li> <li>10 security/authorization messages</li> <li>11 FTP daemon</li> <li>12 NTP subsystem</li> <li>13 log audit</li> <li>14 log alert</li> <li>15 clock daemon</li> <li>16 local use 0 (local0)</li> <li>17 local use 1 (local1)</li> <li>18 local use 2 (local2)</li> <li>19 local use 3 (local3)</li> <li>20 local use 4 (local4)</li> <li>21 local use 5 (local5)</li> <li>22 local use 6 (local6)</li> <li>23 local use 7 (local7)</li> </ul>
<b>Security String</b>	<p>Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.</p>

### Configure Events To Log Externally

1. Click **Logs > Event Management**.
2. Use the Filters to locate the appropriate event. Refer to **Event Management** on page 451 for Filter field definitions.
3. For each event that should be logged externally, select one or more events and click the **Options** button. Select one of the following:

**External**—Logs only to an external host.

**Internal & External**—Logs both to an internal events database and an external host.

**External Log Host Syslog Format**

The following is an example of a syslog message:

```
<37>Apr 10 11:42:16 : 2009/04/10 11:42:16 EDT,1,2587,Probe -
MAP IP To MAC Success,0,1127,,BuildingB-3750,192.168.10.1,,Suc-
cessfully read IP Address mappings from device BuildingB-3750
```

**Table 27: Syslog Format**

Column	Data From Example	Definition
1	<37>	Syslog category: This is the defined facility and the severity  Default Facility = 4 Security message  Severity = 5 Notice
2	Apr 10 11:42:16 :	Time of the syslog generation.
3	2009/04/10 11:42:16 EDT	Log time.
4	1	Log type:  1 Event  2 Alarm
5	2587	Database ID AlarmID or ElementID
6	Probe - MAP IP To MAC Success	Name of the event that generated the syslog message.
7	0	Severity:  0 Normal  1 Minor  2 Major  3 Critical
8	1127	Entity ID
9		Unique Identifier (User ID)
10	BuildingB-3750	Entity Name
11	192.168.10.1	Entity IP Address
12		Entity Physical Address
13	Successfully read IP Address mappings from device BuildingB-3750	Log Message

## External Log Host SNMP Trap Format

The following is an example of an SNMP message:

```
1.3.6.1.4.1.16856.1.1.5="2009/04/10 11:37:02 EDT",
1.3.6.1.4.1.16856.1.1.6=1, 1.3.6.1.4.1.16856.1.1.7=2585,
1.3.6.1.4.1.16856.1.1.8="Probe - MAP IP To MAC Success",
1.3.6.1.4.1.16856.1.1.9=0, 1.3.6.1.4.1.16856.1.1.10=1127,
1.3.6.1.4.1.16856.1.1.15=, 1.3.6.1.4.1.16856.1.1.11=BuildingB-
3750, 1.3.6.1.4.1.16856.1.1.12=192.168.10.1,
1.3.6.1.4.1.16856.1.1.13=, 1.3.6.1.4.1.16856.1.1.14-
4="Successfully read IP Address mappings from device BuildingB-
3750."
```

**Table 28: SNMP Format**

MIB Object	Data From Example	Definition
1.3.6.1.4.1.16856.1.1.5	"2009/04/10 11:37:02 EDT"	The log time stamp in the format YYYY/MM/DD hh:mm:ss z
1.3.6.1.4.1.16856.1.1.6	1	The type of log message 1 - Event message 2 - Alarm Message
1.3.6.1.4.1.16856.1.1.7	2585	The database identifier of the log message
1.3.6.1.4.1.16856.1.1.8	"Probe - MAP IP To MAC Success"	Name of the event that generated the syslog message.
1.3.6.1.4.1.16856.1.1.9	0	The log severity 0 - Normal 1 - Minor 2 - Major 3 - Critical
1.3.6.1.4.1.16856.1.1.10	1127	The database identifier of the log entity
1.3.6.1.4.1.16856.1.1.15		The unique identifier of the log entity "User ID"
1.3.6.1.4.1.16856.1.1.11	BuildingB-3750	The textual name of the log entity
1.3.6.1.4.1.16856.1.1.12	192.168.10.1	The IP address of the log entity. The format is 0.0.0.0"
1.3.6.1.4.1.16856.1.1.13		The Physical address of the log entity. The format is 00:00:00:00:00:00"

MIB Object	Data From Example	Definition
1.3.6.1.4.1.16856.1.1.14	"Successfully read IP Address mappings from device BuildingB-3750."	The textual log message

**External Log Host CEF (Common Event Format)**

Fields contained within a CEF syslog message include:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

**Example:**

```
<37>Jul 22 11:24:20 : CEF:0|Bradford Networks|NAC Control Server|4.1.1.219.P9|6111|Login Failure|1|rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa failed to login.
```

**Table 29: CEF Format**

Column Title	Data From Example	Definition
Facility	<37>	Syslog category: This is the defined facility and the severity  Default Facility = 4 Security message  Severity = 5 Notice  This is not part of the CEF format, but is contained within the syslog message.
Date/Time	Jul 22 11:24:20	Date and time the syslog message was generated.  This is not part of the CEF format but is contained within the syslog message.
CEF: Version	CEF:0	Version number defines the fields that are expected to follow this field.
Device Vendor	Bradford Networks	These fields uniquely identify the type of device sending the syslog message. In this case, the sending entity is Network Sentry.
Device Product	NAC Control Server	
Device Version	4.1.1.219.P9	
Signature ID	6111	Unique identifier per event type. This can be a string or an integer.
Name	Login Failure	Name of the event that generated the syslog message.

Column Title	Data From Example	Definition
Severity	1	Severity: 0 Normal 1 Minor 2 Major 3 Critical
Extension	rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa failed to log in.	Extension is a place holder for additional data. The extensions contained in this message include:  <b>rt</b> - receiptTime - Time stamp that indicates when the event was generated.  <b>cat</b> -category-Type of device sending the syslog message.  <b>msg</b> - message- Message giving more details about the event.

### Examples of Syslog Messages

Here are some examples of syslog messages that are returned from Network Sentry. In these examples, the Syslog server is configured as follows:

- Type: Syslog
- IP Address: a.b.c.d
- Port: 514
- Facility: Authorization

Event	Description	Syslog Message
Login Success	This is the event that is logged with a user logs into the Admin UI.	02-28-2014 08:16:04 Auth.Notice 192.168.34.31 Feb 27 22:16:14 : 2014/02/27 22:16:14 EST,1,545570,Login Success,0,12,,,,,User root logged in.

Event	Description	Syslog Message
Map IP To MAC Failure	This is a legacy event logged when a scheduled task runs (these are no longer used for IP-MAC) and the ARP is not read.	--
Probe - Map IP To MAC Failure	This is the event when we fail to poll and L3 device for IP->MAC (reading Arp Cache) L3 Polling	02-28-2014 09:00:14 Auth.Notice 192.168.34.31 Feb 27 23:00:24 : 2014/02/27 23:00:24 EST,1,545702,Probe - MAP IP To MAC Failure,0,28,,Switch,192.168.34.1,,Failed to read IP Address mappings from device Switch.
User Logged Out	This is the event that is logs when a user logs out of the Admin UI.	02-28-2014 08:48:55 Auth.Notice 192.168.34.31 Feb 27 22:49:04 : 2014/02/27 22:49:04 EST,1,545670,User Logged Out,0,12,,,,,User root Logged Out.
User Logged off Host	This event is logged when a user logs off a host	02-28-2014 08:44:25 Auth.Notice 192.168.34.31 Feb 27 22:44:34 : 2014/02/27 22:44:34 EST,1,545655,User Logged off Host,0,4155,,,,,"User Man, Bat logged off session 1 on host BRADSUPP7-LT"
User Logged onto Host	This event is logged when a user logs onto a host	02-28-2014 08:37:58 Auth.Notice 192.168.34.31 Feb 27 22:38:07 : 2014/02/27 22:38:07 EST,1,545633,User Logged onto Host,0,4155,,,,,"User Man, Bat logged onto session 1 on host BRADSUPP7-LT"
User Remotely Connected to Host	An event that is logged when a user remotely connected to a terminal session on a host using the PA	--
User Locked Session	This event is logged when a user locks his workstation	02-28-2014 08:49:53 Auth.Notice 192.168.34.31 Feb 27 22:50:03 : 2014/02/27 22:50:03 EST,1,545681,User Locked Session,0,4155,,,,,"User Man, Bat locked session 2 on host BRADSUPP7-LT"

Event	Description	Syslog Message
User Unlocked Session	This event is logged when a user unlocks his workstation	02-28-2014 08:52:07 Auth.Notice 192.168.34.31 Feb 27 22:52:16 : 2014/02/27 22:52:16 EST,1,545691,User Unlocked Session,0,4155,,,,,"User Man, Bat unlocked session 2 on host BRADSUPP7-LT"

## View Events Currently Mapped To Alarms

1. Select **Logs > Event to Alarm Mappings**.

The Event to Alarm Mappings view appears.

2. To add a new mapping see **Add or Modify Alarm Mapping** on page 497 for instructions.

## Events View

The Events View displays the contents of the events log. The events log is an audit trail of significant network and Network Sentry incidents. Events are logged when they are enabled in the Events Management View. See **Enable And Disable Events** on page 454.

To access the Events View select **Logs > Events**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

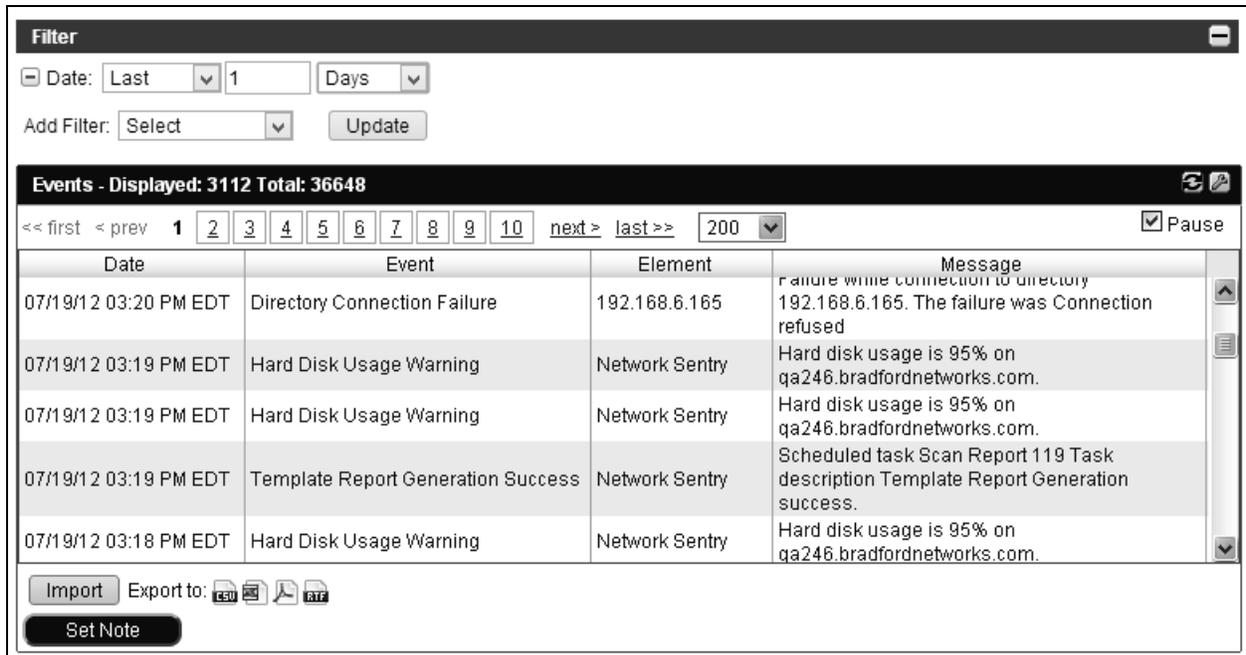


Figure 193: Events View

### Events View Field Definitions

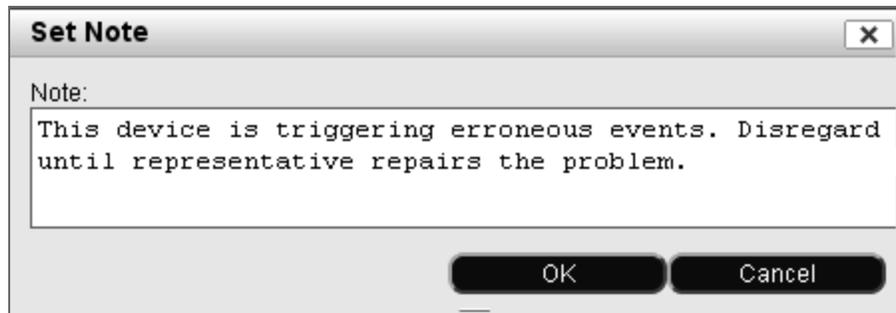
Fields used in filters are also defined in this table.

Field	Definition
<b>First Name</b>	First Name of the user associated with the event, such as the registered owner of a host or an admin user.
<b>Last Name</b>	Last Name of the user associated with the event.
<b>Login Name</b>	User name from the credentials of the user who was logged in and associated with the event.
<b>Element Name</b>	Name of the device, Admin User, server or process associated with the event.
<b>Element Type</b>	Type can be Device, Port, Container, Process, or All.

Field	Definition
<b>Group</b>	Group name of a group of elements, such as, port group, device group or user group.
<b>Pause</b>	If enabled, prevents the Events List from refreshing and adding new records to the screen. In an environment with a large number of events, you may need to pause the refresh in order to research an issue.
<b>Date</b>	Date and time that the event occurred.
<b>Event</b>	Event name. See <b>Network Sentry Events And Alarms List</b> on page 469.
<b>Element</b>	Element associated with the event, such as a user, Admin User, device, port, or process.
<b>Message</b>	A textual description of the selected entry.
<b>Note</b>	An area for user notes.
<b>Buttons</b>	
<b>Import</b>	Import historical events from an Archive file. See <b>Import Archived Data</b> on page 293.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Set Note</b>	Opens a notes window and allows you to add notes to the selected event. See <b>Event Notes</b> on page 468.

### Event Notes

You can add notes to an event entry to clarify why the event happened, track the resolution of a problem, or add general information.



**Figure 194: Set Event Note**

1. Select **Logs > Events**.
2. Use the Filters to locate the appropriate event. Refer to **Events View** on page 466 for Filter field definitions.
3. Select the event.
4. Click **Set Note**.
5. Enter the note text or modify the existing note.
6. Click **OK**.
7. The Note text appears on the Notes column on the Events View.

## Network Sentry Events And Alarms List

When events are enabled, they can be enabled for All Groups or for a single group. Depending on the event you may not want to enable it for all groups because the volume of events would be overwhelming. For example, if you enabled the Host Connected event for all groups, you would receive an event message every time someone connects to the network.

When you look at an event in the Event Viewer, additional information is provided about that occurrence of the event. It might include information such as, user name, IP address, MAC Address or location.

Each event has a corresponding alarm that can be configured. See **Map Events To Alarms** on page 493.

**Note:** Event names highlighted in gray are no longer used. However, they are still available in the Event Log to accommodate importing older data that may contain those events.

**Table 30: FortiNac Control Manager Events And Alarms**

Event	Description
<b>Admin User Created</b>	Network Sentry Admin user created. User types are not included in the event message.
<b>Admin User Destroyed</b>	Network Sentry Admin user deleted from the database.
<b>Admin User Logged Out</b>	Network Sentry admin user logged out of the user interface.
<b>Admin User Login Failure</b>	Network Sentry admin user failed to log into the user interface.
<b>Admin User Login Success</b>	Network Sentry admin user logged into the user interface.
<b>Admin User Timed Out</b>	Network Sentry Admin user was logged out of the User Interface based on the settings in <b>Users &gt; Admin Users &gt; Timeout Settings</b> in the Administrative Interface Inactivity Time (Minutes) field.
<b>Alarm Created</b>	Indicates that an event has caused an alarm.
<b>Appliance Weak Password</b>	Indicates that password for the appliance and/or the Admin UI are either a default factory password or are not complex enough. It is recommended that you modify the password. Otherwise, your network may be at risk for a security breach.
<b>Authentication Time-out Failure</b>	Forced authentication is enabled, the forced authentication time has expired, and the user has not authenticated.
<b>Authentication Failure</b>	A user fails to log in with a user ID and password via LDAP or RADIUS.
<b>Authenticated User</b>	A user succeeds in logging onto a device via LDAP or RADIUS.
<b>Certificate Expiration Warning</b>	A certificate is due to expire within 30 days.

Event	Description
<b>Certificate Expiration Warning (CRITICAL)</b>	A certificate is due to expire within 7 days.
<b>Certificate Expired</b>	A certificate has expired.
<b>Contact Established</b>	Contact with a device has been established.
<b>Contact Lost</b>	Contact with a device has been lost.
<b>Container Created</b>	New container has been created in the database. Containers are a grouping mechanism for devices that display in the Topology View.
<b>Container Destroyed</b>	Container has been deleted from the database. Deleting a container deletes all of the devices it contains.
<b>Database Archive/Purge Failure Database Archive/Purge Success</b>	Indicates whether the Archive/Purge scheduled task was successful.
<b>Database Backup Failure Database Backup Success</b>	Indicates whether the scheduled database backup was successful.
<b>Database Replication Error</b>	Occurs in a High Availability situation when the MasterLoader database is not replicating. Can also be triggered when the database on the secondary server is not running.
<b>Database Replication Succeeded</b>	Occurs in a High Availability situation when the MasterLoader database is successfully replicated to the secondary server.
<b>De-authenticated</b>	A user succeeds in logging off a device.
<b>De-authentication Failure</b>	A user fails to log out of a device.
<b>Device Created</b>	New managed device has been created in the database.
<b>Device Destroyed</b>	Managed device has been deleted from the database.
<b>Directory Connection Failure</b>	The connection to a directory, such as Active Directory or LDAP, failed. The directory could have refused the connection because the user name and password were incorrect. This event can be triggered when testing the connection to the directory with the Test button on the Directory Configuration window.
<b>Directory Group Enabled Directory Group Disabled</b>	Users can be disabled/enabled in a Directory such as LDAP based on Group membership. When the Network Sentry database synchronizes with the Directory, users that are members of the group are enabled. Users that are not members of the group are disabled. See <b>Add/Modify Directory - Group Attributes Tab</b> on page 80.
<b>Directory Synchronization Success Directory Synchronization Failure</b>	Indicates whether or not a directory, such as Active Directory or LDAP, synchronized with the user database. Could be caused if Network Sentry fails to connect to the directory. This synchronization is a one time task done when the Directory is configured.

Event	Description
<b>Directory User Enabled</b> <b>Directory User Disabled</b>	Users can be disabled/enabled in a Directory such as LDAP. When the Network Sentry database synchronizes with the Directory, users can be disabled/enabled based on their Directory setting.
<b>Incomplete User Found in Directory</b>	Network Sentry requires the Last name and ID fields for each user. If either of those fields is missing, the user record is incomplete.
<b>Management Established</b>	Generated when management of a device is established.
<b>Management Lost</b>	Generated when management of a device is lost.
<b>Maximum Concurrent Connections Critical</b>	Concurrent Connection licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
<b>Maximum Concurrent Connections Exceeded</b>	Concurrent Connection licenses in use has reached 100% of total licenses.
<b>Maximum Concurrent Connections Warning</b>	Concurrent Connection licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Operating System Is Up to Date</b>	Indicates that there are no new updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
<b>Operating System Status Check Failure</b>	Indicates that the Operating System update check failed due to multiple running checks. This may be caused by a configuration or network issue.
<b>Operating System Update Initiated</b>	Indicates that an Operating System Update was started from the Admin UI. See Operating System Updates on page 177.
<b>Operating System Updates Available</b>	Indicates that there are updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
<b>Policy Warning</b>	Host was scanned by an Endpoint Compliance Policy. The host does not meet all of the scan requirements, but the scan rules state that a warning be issued instead of making compliance a requirement.  Scan status "Warning" triggers this event.
<b>Secondary Contact Lost</b>	Event triggered when the primary loses contact with the secondary.
<b>Service Down - Tomcat Admin</b> <b>Service Down - Tomcat Portal</b> <b>Service Down -mysqlqld</b> <b>Service Down -sshd</b>	Event triggered when a specific service is no longer running. These services are required.  Network Sentry tries to restart the service every 30 seconds.  In a High Availability environment, failover occurs after the fourth failed restart attempt.  <b>Note:</b> If the primary is unable to communicate with the secondary to confirm it is running, service down will not trigger a fail-over.
<b>Service Started - Tomcat Admin</b> <b>Service Started - Tomcat Portal</b> <b>Service Started -mysqlqld</b> <b>Service Started -sshd</b>	Event triggered when one of the listed services is started. These services are required and must be running in order to use Network Sentry.

Event	Description
<b>Synchronize Users with Directory Success</b> <b>Synchronize Users with Directory Failure</b>	Indicates whether or not the Network Sentry user database has successfully synchronized with the selected directory such as LDAP or Active Directory. These events are triggered by the failure or success of the scheduled synchronization set up on the Directory Configuration window.
<b>System Automatically Restarted</b>	Server was restarted because a primary system process was down. Processes include: MasterLoader, IP to MAC, Communication and Nessus.  This event was System Restart in prior versions.
<b>System Backup Failure</b> <b>System Backup Success</b>	Indicates whether a system backup has succeeded. The system backup is run by a scheduled task. The system backup may succeed, but will still fail if remote backup is enabled and fails.  <b>Note:</b> It is recommended that you create an alarm action to send an email if system backup fails.
<b>System Power Off</b>	Indicates that the user specified in the event message powered off the Network Sentry server. See <b>Power Management</b> on page 163
<b>System Reboot</b>	Indicates that the user specified in the event message rebooted the Network Sentry server. See <b>Power Management</b> on page 163.
<b>Users Removed From Directory</b>	User has been removed directly from a Directory such as LDAP. When the Network Sentry user database is synchronized with the Directory this discrepancy triggers the event. If Remove User is selected on your Directory configuration, the missing user is removed from the Network Sentry database.
<b>Vendor OUI Added</b>	Generated when a new Vendor OUI has been added to the database.
<b>Vendor OUI Removed</b>	Generated when a Vendor OUI was removed from the database.

**Table 31: Network Sentry Events and Alarms (Standalone)**

Event	Definition
<b>Add/Modify/Remove Host</b>	Generated whenever a trap is received that adds, modifies or removes a host record in the database.
<b>Add/Modify/Remove User</b>	Generated when a trap is received that adds, modifies or removes a user record in the database.
<b>Admin User Created</b>	Network Sentry Admin user created. User types are not included in the event message.
<b>Admin User Destroyed</b>	Network Sentry Admin user deleted from the database.
<b>Admin User Logged Out</b>	Network Sentry admin user logged out of the user interface.
<b>Admin User Login Failure</b>	Network Sentry admin user failed to log into the user interface.
<b>Admin User Login Success</b>	Network Sentry admin user logged into the user interface.

Event	Definition
<b>Admin User Timed Out</b>	Network Sentry Admin user was logged out of the User Interface based on the settings in <b>Users &gt; Admin Users &gt; Timeout Settings</b> in the Administrative Interface Inactivity Time (Minutes) field.
<b>Administrative Status Success</b>	Network Sentry user has gone into Port Properties for an individual port and successfully turned the Admin Status on or off.
<b>Agent - Unrecognized Vendor OUI</b>	Generated when an agent scans a host and returns MAC addresses that have a Vendor OUI that is not included in the Vendor OUI Management list in Network Sentry.
<b>Agent Message Sent</b>	Message sent from Network Sentry user to one or more hosts. Only hosts running the Persistent Agent can receive messages. This event is not generated if the message fails to send.
<b>Alarm Created</b>	Indicates that an event has caused an alarm.
<b>Appliance Weak Password</b>	Indicates that password for the appliance and/or the Admin UI are either a default factory password or are not complex enough. It is recommended that you modify the password. Otherwise, your network may be at risk for a security breach.
<b>Application Server Contact Lost</b>	Generated when contact is lost to the Nessus plugin in a 1200/8200 pair. Requires contact to be established before contact can be lost.
<b>Application Violation</b>	Network Sentry can receive traps from external applications hosted on servers modeled in the Topology tree as Pingable or Server devices. This event is generated when a trap is received. Traps might be used to indicate intrusion or that a threshold has been exceeded.  A Host Application Violation event can be generated at the same time. See <b>Host Application Violation</b> on page 478 in this list.
<b>Application Violation Reset</b>	Generated based on a trap sent from an external application. Indicates that the condition that caused the Application Violation event is no longer happening and operations can return to normal. For example, if hosts have been marked at risk, they can now be marked safe and can access the network.  A Host Application Violation Reset can be generated at the same time with host specific information. See <b>Host Application Violation Reset</b> on page 478 in this list.
<b>Authentication Time-out Failure</b>	Forced authentication is enabled, the forced authentication time has expired, and the user has not authenticated.
<b>Authentication Failure</b>	A user fails to log in with a user ID and password via LDAP or RADIUS.
<b>Authenticated User</b>	A user succeeds in logging onto a device via LDAP or RADIUS.
<b>Certificate Expiration Warning</b>	Generated when a certificate is due to expire within 30 days.
<b>Certificate Expiration Warning (CRITICAL)</b>	Generated when a certificate is due to expire within 7 days.

Event	Definition
<b>Certificate Expired</b>	Generated when a certificate has expired.
<b>cipSecTunnelStop</b>	Generated when VPN connection IPsec Phase-2 Tunnel becomes inactive.
<b>Communication Lost with Palo Alto User Agent</b>	<p>Palo Alto User Agent is a component of the Palo Alto Firewall. If configured Network Sentry sends User ID and IP Address to the Palo Alto User Agent each time a host connects to the network.</p> <p>Event indicates that the Palo Alto User Agent modeled in the Topology View cannot be reached.</p>
<b>Communication Lost with RADIUS/SSO Agent</b>	<p>Fortinet SSO Agent is a component of the Fortigate Firewall. If configured Network Sentry sends User ID and IP Address to the Fortinet SSO Agent each time a host connects to the network.</p> <p>Event indicates that the Fortinet SSO Agent modeled in the Topology View cannot be reached.</p>
<b>Conference Created</b>	Using Guest/Contractor Accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.
<b>Contact Established</b>	Contact with a device has been established.
<b>Contact Lost</b>	Contact with a device has been lost.
<b>Container Created</b>	New container has been created in the database. Containers are a grouping mechanism for devices that display in the Topology View.
<b>Container Destroyed</b>	Container has been deleted from the database. Deleting a container deletes all of the devices it contains.
<b>DHCP Host Name Changed</b>	Generated when a known host connects to the network and its host name is different. Indicates that the host name in the database associated with the MAC address and existing DHCP finger print for that host is different.
<b>Database Backup Failure Database Backup Success</b>	Indicates whether or not the scheduled database backup was successful.
<b>Database Replication Error</b>	Occurs in a High Availability situation when the MasterLoader database is not replicating. Can also be triggered when the database on the secondary server is not running.
<b>Database Replication Succeeded</b>	Occurs in a High Availability situation when the MasterLoader database is successfully replicated to the secondary server.
<b>De-authenticated</b>	A user succeeds in logging off a device.
<b>De-authentication Failure</b>	A user fails to log out of a device.
<b>Deleted Host Successfully</b>	Host or Network Sentry user has been successfully deleted from the database. If multiple records are deleted at once, a separate event is generated for each record.

Event	Definition
<b>Device Cold Start</b>	Device was restarted using the power switch.
<b>Device Created</b>	New managed device has been created in the database.
<b>Device Destroyed</b>	Managed device has been deleted from the database.
<b>Device Fingerprint Changed</b>	<p>Host is using a different operating system than the one with which the machine was registered. This could occur on a machine with a dual-boot. For example, the machine registers with a Windows operating system. The user later boots the machine using Linux and tries to access the network. That change would trigger this event. An upgrade within a family of operating systems would not normally trigger this event, such as from Windows XP to Windows Vista.</p> <p>Operating system is determined by the DHCP fingerprint.</p>
<b>Device Identity</b>	No longer used.
<b>Device Link</b>	A device has linked to port X on the network.
<b>Device Link Down</b>	A device link goes down on a specific port because a device was disconnected from the port.
<b>Device Link Up</b>	Generated when a device link goes up on a specific port.
<b>Device Profile</b>	Generated whenever device profiling updates a rogue.
<b>Device Rule Confirmation Failure</b> <b>Device Rule Confirmation Success</b>	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.
<b>Device Profile Rule Match</b>	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
<b>Device Profiling Automatic Registration</b>	A rogue host has been registered by device profiling based on a device profiling rule.
<b>Device Profiling Rule Missing Data</b>	Indicates that Device Profiler cannot compare a rogue against a rule because Network Sentry does not have enough information about the rogue, such as a DHCP fingerprint. If Device Profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
<b>Device Warm Start</b>	Device was restarted from the command line interface.
<b>Directory Connection Failure</b>	The connection to a directory, such as Active Directory or LDAP, failed. The directory could have refused the connection because the user name and password were incorrect. This event can be triggered when testing the connection to the directory with the Test button on the Directory Configuration window.

Event	Definition
<b>Directory Group Disabled</b> <b>Directory Group Enabled</b>	Users can be disabled/enabled in a Directory such as LDAP based on Group membership. When the Network Sentry database synchronizes with the Directory, users that are members of the group are enabled. Users that are not members of the group are disabled. See <b>Add/Modify Directory - Group Attributes Tab</b> on page 80.
<b>Directory Synchronization Failure</b> <b>Directory Synchronization Success</b>	Indicates whether or not a directory, such as Active Directory or LDAP, synchronized with the user database. Could be caused if Network Sentry fails to connect to the directory. This synchronization is a one time task done when the Directory is configured. See <b>Schedule Directory Synchronization</b> on page 83
<b>Directory User Disabled</b> <b>Directory User Enabled</b>	Users can be disabled/enabled in a Directory such as LDAP. When the Network Sentry database synchronizes with the Directory, users can be disabled/enabled based on their Directory setting. See <b>Add/Modify Directory - User Attributes Tab</b> on page 76.
<b>Disable Host Failure</b> <b>Disable Host Success</b>	Generated when a user manually disables a host on the Host View. Indicates whether or not the host was successfully disabled.
<b>Disable Hosts Failure</b> <b>Disable Hosts Success</b>	Indicates whether or not hosts in a group were successfully disabled using a scheduled task.
<b>Disable Port Failure</b> <b>Disable Port Success</b>	Indicates whether or not a particular port was disabled by an alarm action.
<b>Disable Ports Failure</b> <b>Disable Ports Success</b>	Indicates whether or not ports in a particular group were disabled by a scheduled task.
<b>Disable User Success</b>	Indicates that a user selected from the User View was successfully disabled.
<b>Discovery Completed</b>	The device discovery process that adds new devices to Network Sentry has completed. IP address range is included in the completion message.
<b>Duplicate Physical Address</b>	No longer used.
<b>Duplicate Users Found in Directory</b>	Two users with the same last name and/or ID were found in the Directory. Network Sentry is case in-sensitive. For example, two users with last names listed as SMITH and smith are treated as if they were the same person. The newer of the two users is ignored.
<b>Email Failure</b>	Alarms can be configured to send E-mail Notifications to Network Sentry Admin users. If the Admin user has no e-mail address or the e-mail fails in any other way, this event is generated.
<b>Enable Host Failure</b> <b>Enable Host Success</b>	Indicates whether or not a host selected from the Host View was successfully enabled.
<b>Enable Hosts Failure</b> <b>Enable Hosts Success</b>	Indicates whether or not hosts in a group were successfully enabled using a scheduled task.
<b>Enable Port Failure</b> <b>Enable Port Success</b>	Indicates whether or not a particular port has been enabled by an alarm action in response to a previous event.

Event	Definition
<b>Enable Ports Failure</b> <b>Enable Ports Success</b>	Indicates whether or not ports in a particular group were enabled by a scheduled task.
<b>Enable User Success</b>	Indicates that a user selected from the User View was successfully enabled.
<b>Enterasys Dragon Violation</b>	Enterasys Dragon is an Intrusion Protection/Detection System. An event is generated when an intruder is detected.
<b>Failed to Disable Adapters</b>	Attempted to disable hosts using an Alarm Action. Hosts failed to be disabled.
<b>Failed to Disable HP Port Security</b>	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
<b>Failed to Enable Adapters</b>	Attempted to enable hosts using an Alarm Action. Hosts failed to be enabled.
<b>Failed to Enable HP Port Security</b>	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
<b>Found Ignored MAC Address</b>	A host or device has connected with a MAC address that is in the MAC Address Exclusions list. This connection is not being managed by Network Sentry and the host or device has access to the production network.
<b>Found Microsoft LLTD or Multicast Address</b>	A host or device has connected with a MAC address in the Microsoft LLTD or Multicast Address range. Those ranges are managed in the MAC Address Exclusion list. Network Sentry ignores these MAC addresses for 48 hours after the first one is seen and then treats them as rogues unless the configuration is updated on the MAC Address Exclusion list.
<b>Gaming Device Registration</b>	A gaming device was registered by a user.
<b>Group Does Not Exist for Scan</b>	Network Sentry attempted to perform a scan or scheduled task for a particular group and the group no longer exists in the database. Either recreate the group or remove the scan or scheduled task.
<b>Guest/Contractor Pre-allocation Critical</b>	No longer used.  If you are setting up Guest/Contractor users in advance, an event can be generated if you set up more Guest/Contractor users than you have licenses.
<b>Guest/Contractor Pre-allocation Warning</b>	No longer used.  If you are setting up Guest/Contractor users in advance, an event can be generated if you set up enough Guest/Contractor users to use 75% of the available licenses.
<b>Guest Account Created</b>	New guest account is created.
<b>Guest Account Deleted</b>	Guest account is deleted.

Event	Definition
<b>Hard Disk Usage Critical</b>	Generated when the disk usage critical threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 95%
<b>Hard Disk Usage Warning</b>	Generated when the disk usage warning threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 85%
<b>Host Aged Out</b>	Host has been removed from the database based on the time or expiration date on the associated Host Properties window. See <b>Host Properties</b> on page 335.
<b>Host Application Violation</b>	Generated against a Network Sentry host based on the IP, MAC, or ID information contained within an Application Violation trap. If IP, MAC, or User ID match any records in the Network Sentry database, this event is generated. See <b>Application Violation</b> on page 473 in this list.
<b>Host Application Violation Reset</b>	Generated against a Network Sentry host based on the IP, MAC, or User ID information contained within an Application Violation Reset trap. If IP, MAC, or User ID match any records in the Network Sentry database, an event is generated. The reset event occurs when the host is no longer in violation. See <b>Application Violation</b> on page 473 in this list.
<b>Host At Risk</b>	An Admin user marked a selected host At Risk or the host failed a scan.
<b>Host At Risk Failure</b> <b>Host At Risk Success</b>	Indicates whether an alarm action triggered by an At Risk host succeeded or failed.
<b>Host CLI Task Success</b> <b>Host CLI Task Failure</b>	Indicates whether or not the CLI commands associated with host/adaptor based ACLs have been successful.
<b>Host Copied From NCS</b>	In an environment where multiple Network Sentry appliances are managed by a FortiNac Control Manager, hosts and their corresponding information can be copied from one appliance to another based on settings in the FortiNac Control Manager under <b>System &gt; Settings &gt; Network Control Manager &gt; Server Synchronization</b> . When hosts are copied from one appliance to another this event is generated.
<b>Host Identity Changed</b>	Indicates that a registered host's name or operating system has changed since the last time it was read by the Persistent or Dissolvable Agent, and that it is possibly a dual boot device. This could also indicate MAC spoofing. An operating system change, such as an upgrade could also trigger this event.

Event	Definition
<b>Host Pending At Risk</b>	A host failed a scan for an Endpoint Compliance Policy. The policy was configured for delayed remediation indicating that hosts that fail the scan are not sent to remediation for x number of days. The event is generated when the host is marked Pending At Risk. See <b>Network Sentry Events And Alarms List</b> on page 469 in this list.  Scan status "Failure Pending" triggers this event.
<b>Host Registration Failure Host Registration Success</b>	Host has gone to the Registration page and the user attempted to register the host. Indicates whether the registration succeeded or failed.
<b>Host Rejected - No MAC</b>	Host rejected because it is missing a MAC address.
<b>Host Rejected - No VLAN</b>	Host rejected because there is no VLAN defined for current state.
<b>Host Safe</b>	Generated when a user goes to <b>System &gt; Settings &gt; Control &gt; Quarantine</b> . On the Quarantine view there is a button that allows the user to mark all hosts as Safe. If this button is clicked the event is generated for each host that was affected.
<b>Host Safe Failure Host Safe Success</b>	Indicates whether or not an alarm action associated with marking a host as safe has failed. See <b>Host Safe</b> on page 479 in this list.
<b>Host Session Logged On Host Session Logged Off</b>	Agent has detected that the user has logged on or off the host. Applies only to Windows hosts.
<b>Incomplete User Found in Directory</b>	Network Sentry requires the Last name and ID fields for each user. If either of those fields is missing, the user record is incomplete.
<b>Interface Status Failure Interface Status Success</b>	Indicates whether or not the Update interface status scheduled task was successful. The task reads and updates the interface status for each port on the devices in the associated groups.
<b>Internal Scheduled Task Failure Internal Scheduled Task Success</b>	Indicates whether or not a scheduled task has failed. The name of the task is provided.
<b>Invalid Physical Address</b>	The MAC Address of the specified host or device is not recognized by Network Sentry because the corresponding Vendor OUI is not in the Network Sentry database. Update the Vendor OUI database either manually or by using Auto-Def Updates. See <b>Add A Vendor OUI</b> on page 106 and Schedule Auto-Definition Updates.
<b>L2 Poll Failed L2 Poll Succeeded</b>	Indicates whether or not Network Sentry successfully contacted the device to read the list of connected hosts.
<b>L3 Poll Failed L3 Poll Succeeded</b>	Indicates whether Network Sentry successfully read IP Address mappings from a device.
<b>Load In Limit Exceeded</b>	No longer used.  Max % In setting on the Bandwidth window has been met or exceeded.

Event	Definition
<b>Load In Limit Rearmed</b>	No longer used. After the first “Load In Limit Exceeded” event occurs the server does not generate a “Load In Limit Rearmed” event until the percentage of bandwidth bytes in falls below Rearm % In value.
<b>Load Out Limit Exceeded</b>	No longer used. Max % Out setting on the Bandwidth window has been met or exceeded.
<b>Load Out Limit Rearmed</b>	No longer used. After a “Load Out Limit Exceeded” event occurs the server creates a “Load Out Limit Rearmed” event once the percentage of bytes out falls below this the Rearm % Out value.
<b>MAC Learned</b>	Switch has learned the MAC address of a host that has connected and has added that address to its forwarding table.
<b>MAC Removed</b>	Switch has removed the MAC address of a host who has disconnected from its forwarding table.
<b>MAC change event on uplink</b>	Host has been moved to a new VLAN.
<b>Management Established</b>	Generated when management of a device is established.
<b>Management Lost</b>	Generated when management of a device is lost.
<b>Map IP to MAC Failure</b> <b>Map IP to MAC Success</b>	No longer used. Mapping IP addresses to physical addresses for a selected group using a scheduled task failed or succeeded.
<b>Maximum Blacklist Clear Attempts Reached</b>	Maximum number of attempts to remove a host from a controller's blacklist have been reached and the host remains on the blacklist.
<b>Maximum Concurrent Physical Address Warning</b>	No longer used. Generated when host connections exceed 6000 or 12000 depending on the size of the appliance.
<b>Maximum Concurrent Connections Critical</b>	Concurrent Connection licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable. See <b>Event Thresholds</b> on page 455.
<b>Maximum Concurrent Connections Exceeded</b>	Concurrent Connection licenses in use has reached 100% of total licenses.
<b>Maximum Concurrent Connections Warning</b>	Concurrent Connection licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable. See <b>Event Thresholds</b> on page 455.
<b>Maximum Guest/Contractor Critical</b>	No longer used. Guest Manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.

Event	Definition
<b>Maximum Guest/Contractor Exceeded</b>	No longer used. Guest Manager licenses in use has reached 100% of total licenses.
<b>Maximum Guest/Contractor Warning</b>	No longer used. Guest Manager licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Maximum Hosts Critical</b>	No longer used. Access Manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
<b>Maximum Host Warning</b>	No longer used. Access Manager licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Maximum Hosts Exceeded</b>	No longer used. Access Manager licenses in use has reached 100% of total licenses. No new accounts can be created.
<b>Maximum Known Device Critical</b>	No longer used. Device Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
<b>Maximum Known Device Warning</b>	No longer used. Device Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Maximum Known Devices Exceeded</b>	No longer used. Device Tracker licenses in use has reached 100% of total licenses.
<b>Maximum User Critical</b>	No longer used. Shared Access Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
<b>Maximum User Warning</b>	No longer used. Shared Access Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
<b>Maximum Users Exceeded</b>	No longer used. Shared Access Tracker licenses in use has reached 100% of total licenses.
<b>Maximum Blacklist Clear Attempts Reached</b>	Generated when the maximum number of attempts to remove a MAC address from a device's black list has been exceeded. Currently the maximum is set to 3 attempts.

Event	Definition
<b>Memory Usage Critical</b>	Generated when the memory usage critical threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 95% Threshold is configurable. See <b>Event Thresholds</b> on page 455.
<b>Memory Usage Warning</b>	Generated when the memory usage warning threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 85% Threshold is configurable. See <b>Event Thresholds</b> on page 455.
<b>Message</b>	Cabletron/Enterasys Event Log Message OID = 1.3.6.1.4.1.52.1280
<b>Multi-Access Point Detected</b>	Generated when multiple MAC addresses are detected on a port. However, if the port is in the Authorized Access Points group an event is not generated.
<b>NAT Device Registered</b>	Generated when a NAT Device (router) is registered.
<b>Nitro Security Violation Nitro Threat Level 1 - 6</b>	Generated based on traps received from the NitroGuard Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
<b>No CDP Announcement</b>	Generated when a device that has sent at least one CDP announcement has stopped sending those announcements. This is based on the polling time set for the device. For example if the poll time is one hour, a new event message is sent each time the hour elapses with no message from the device.
<b>Operating System Is Up to Date</b>	Indicates that there are no new updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
<b>Operating System Status Check Failure</b>	Indicates that the Operating System update check failed due to multiple running checks. This may be caused by a configuration or network issue.
<b>Operating System Update Initiated</b>	Indicates that an Operating System Update was started from the Admin UI. See Operating System Updates on page 177.
<b>Operating System Updates Available</b>	Indicates that there are updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
<b>Packeteer Configuration Failure Packeteer Configuration Success</b>	Indicates whether or not communication has been established with the Packeteer PacketShaper software after Packeteer has been modeled in the Topology View.
<b>Packeteer Monitor</b>	If Packet Shaper has been configured to generate threshold violation events and if a threshold violation occurs, the event triggers an SNMP trap from PacketShaper to Network Sentry. This trap causes Network Sentry to generate a Packeteer Monitor event.
<b>Packeteer Monitor 2</b>	If a Packeteer product has been configured to generate events for OID 13.6.1.3.6.1.4.1.2334.1.1 and the event triggers an SNMP trap from the Packeteer to Network Sentry. This trap causes Network Sentry to generate a Packeteer Monitor 2 event.

Event	Definition
<b>Policy Warning</b>	Host was scanned by an Endpoint Compliance Policy. The host does not meet all of the scan requirements, but the scan rules state that a warning be issued instead of making compliance a requirement.  Scan status "Warning" triggers this event.
<b>Poll For Hosts Failure Poll For Hosts Success</b>	No longer used.  Indicates whether a scheduled task to poll switches for hosts has succeeded or failed. Switches are contained in a device group and that group is polled.
<b>Port CLI Task Failure Port CLI Task Success</b>	Indicates whether a CLI configuration applied to a port ran and failed or succeeded.
<b>Port Link Down Port Link Up</b>	Trap received from the switch each time there is a link up or a link down on a port. Link up and link down happen each time a host is switched from one VLAN to another.
<b>Port Security Incomplete</b>	Maximum number of users on a port has been reached.
<b>Port Segmented</b>	Trap received from an Enterasys or Cabletron switch indicating that a link is down. This port may have been logically disconnected due to an excessive collision level or it may be physically disconnected.
<b>Port in Authorized Access Points Group</b>	Scheduled task for a port in the Authorized Access Points group failed.
<b>Possible MAC Address Spoof</b>	Indicates that the same MAC address has been detected for more than five minutes on two different devices simultaneously. One is possibly spoofing the other's MAC address.
<b>Possible NAT Device, MAC Spoofed</b>	This event has been replaced with NAT Device Registered. It remains visible to allow you to restore an old backup and view occurrences of this event. See <b>NAT Device Registered</b> on page 482 in this list.
<b>Possible NAT User</b>	Generated on each host. One per MAC address on the NATd machine. For example, if a host has both a wired and wireless connection, an event is generated for each.
<b>Process Memory Usage Critical</b>	Generated when the memory usage critical threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 95%
<b>Process Memory Usage Warning</b>	Generated when the memory usage warning threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 85%
<b>Process Thread Count Critical</b>	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 200  This event is disabled by default.

Event	Definition
<b>Process Thread Count Warning</b>	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 175  This event is disabled by default.
<b>Profile Modified</b>	Generated when a user modifies a User/Host Profile. Event message contains user information for the user who made the change, whether the change was an add, remove or replace, and the complete profile after the changes.
<b>RADIUS Rate Exceeded</b>	Generated when the 60 requests-per-second threshold is exceeded.  This event is disabled by default.
<b>RADIUS Time Threshold</b>	Indicates that the time threshold for a response from the RADIUS server has been exceeded. This threshold is not configurable.
<b>Remote Access Excessive Session Process Time</b>	Generated when the time to process the remote client exceeds a threshold (set through the "MaxClearTime" attribute on the ASA device).
<b>Reports Purged</b>	Lists the file names of all reports that were deleted when reports were purged from the /home/cm/reports directory.
<b>SNMP Failure</b>	Generated when Network Sentry receives an SNMP failure during communication with a SNMP enabled Network Device. This includes any error message received from the SNMP packet.
<b>SNMP Read Error</b>	Did not receive all data when reading a switch using SNMP. Device name and error code are included in the event message.
<b>Scan Does Not Exist For Scheduler Task</b>	Network Sentry has attempted to run a scan using a scheduled task. The scan referred to in the task no longer exists in the database. You must either recreate the scan or remove the scheduled task from the scheduler.
<b>Secondary Contact Lost</b>	Event triggered when the primary loses contact with the secondary.
<b>Service Down - Tomcat Admin</b> <b>Service Down - Tomcat Portal</b> <b>Service Down -dhcpd</b> <b>Service Down -httpd</b> <b>Service Down -mysqld</b> <b>Service Down -named</b> <b>Service Down -sshd</b>	<p>Event triggered when a specific service is no longer running. These services are required.</p> <p>Network Sentry tries to restart the service every 30 seconds.</p> <p>In a High Availability environment, failover occurs after the fourth failed restart attempt.</p> <p>For the httpd service: After the system confirms that the httpd service is running, the system also attempts to connect to ports 80 and 443. If the system fails to connect to either port, the httpd service is restarted.</p> <hr/> <p><b>Note:</b> If the primary is unable to communicate with the secondary to confirm it is running, service down will not trigger a fail-over.</p>

Event	Definition
<b>Service Started - Tomcat Admin</b> <b>Service Started - Tomcat Portal</b> <b>Service Started -dhcpd</b> <b>Service Started -httpd</b> <b>Service Started -mysqld</b> <b>Service Started -named</b> <b>Service Started -sshd</b>	Event triggered when one of the listed services is started. These services are required and must be running in order to use Network Sentry.
<b>Set Default VLAN Failure</b> <b>Set Default VLAN Success</b>	When a host disconnects from a port, the port can be set to return to its default VLAN. Indicates whether or not the port successfully returns to the default VLAN.
<b>Sophos AntiVirus: Virus Found</b>	Sophos AntiVirus can be configured to send traps to Network Sentry when a virus is found on a host machine. Host information is included in the trap. If a Sophos Trap is received, this event is generated.
<b>Sourcefire Error</b> <b>Sourcefire IPS Action</b> <b>Sourcefire IPS High Violation</b> <b>Sourcefire IPS Low Violation</b> <b>Sourcefire IPS Medium Violation</b>	<p>Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.</p> <p><b>Sourcefire IPS Action</b>—Indicates that an action has been triggered by a syslog message from Sourcefire.</p>
<b>StealthWatch</b>	SNMP trap has been sent from a StealthWatch device OID = 1.3.6.1.4.1.8712
<b>StealthWatch Email Rejects</b>	Host is receiving a significant number of rejected mail attempts.
<b>StealthWatch Email Relay</b>	Host is operating as an email relay.
<b>StealthWatch High Concern</b>	A host has exceeded the Concern Index threshold set for it. This usually means that an inside host is no longer operating as it was during the tuning period and should be examined for possible compromise, misuse, or policy violations. An external host with a High Concern index is often attempting to violate your network integrity.
<b>StealthWatch High File Sharing</b>	Host is transferring files.
<b>StealthWatch High Volume Email</b>	Host is infected with an email worm.
<b>StealthWatch Max Flows Initiated</b>	Host has had an excessive number of total flows active.
<b>StealthWatch New Flows</b>	Indicates that a host exceeds a total number of new flows in a 5-minute period.
<b>StealthWatch Port Flood</b>	The host has attempted to connect on an excessive number of ports on the Target IP. This may indicate a DoS attack or an aggressive scan by the source IP.
<b>StealthWatch SYN Flood</b>	The host has sent an excessive number of TCP connection requests (SYN packets) in a 5-minute period. This may indicate a DoS attack or non-stealthy scanning activity

Event	Definition
<b>StealthWatch Suspect Long Flow</b>	Host has a long duration flow.
<b>StealthWatch Worm Activity</b>	A host has scanned and connected on a particular port across more than one subnet. The details section of this alarm specifies the port on which the activity was observed.
<b>StealthWatch Worm Propagation</b>	Host has scanned and connected on port 5 across more than 1 subnet.
<b>StealthWatch Zone Violations</b>	Host has connected to a server in a zone that it is not allowed to access.
<b>StoneGate IPS High Violation StoneGate IPS Low Violation StoneGate IPS Medium Violation</b>	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
<b>StoneGate Violation</b>	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
<b>Success Disabling Port Security Success Enabling Port Security</b>	Generated when the Enable or Disable HP/NT Port Security scheduled task runs successfully. This task enables or disables port security configuration on all HP/NT devices in the selected group. Port Security is used to disable hosts if DeadEnd VLANs are not used on the network.
<b>Synchronize Users with Directory Failure Synchronize Users with Directory Success</b>	Indicates whether or not the Network Sentry user database has successfully synchronized with the selected directory such as LDAP or Active Directory. These events are triggered by the failure or success of the scheduled synchronization set up on the Directory Configuration window. See <b>Directory Configuration</b> on page 71.
<b>Syslog Error</b>	Generated when the Network Sentry server receives an inbound syslog message for a host that is not currently managed by Network Sentry.
<b>System Backup Failure System Backup Success</b>	Indicates whether a system backup has succeeded. The system backup is run by a scheduled task. The system backup may succeed, but will still fail if remote backup is enabled and fails.  <b>Note:</b> It is recommended that you create an alarm action to send an email if system backup fails.
<b>System Created Uplink</b>	If Uplink Mode on a Port's properties is set to Dynamic, Network Sentry converts the port to an uplink port when the number of MAC addresses on the port exceeds the System Defined Uplink count and generates this event.
<b>System Fail Over</b>	In a High Availability environment, this event indicates that the primary server has failed and the secondary has taken over.
<b>System Power Off</b>	Indicates that the user specified in the event message powered off the Network Sentry server. See Power Management on page 163.
<b>System Reboot</b>	Indicates that the user specified in the event message rebooted the Network Sentry server. See Power Management on page 163.

Event	Definition
<b>System Automatically Restarted</b>	Server was restarted because a primary system process was down. Processes include: MasterLoader, IP to MAC, Communication and Nessus.  This event was System Restart in prior versions.
<b>TippingPoint SMS High Violation TippingPoint SMS Low Violation TippingPoint SMS Medium Violation</b>	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
<b>Top Layer IPS High Violation Top Layer IPS Low Violation Top Layer IPS Medium Violation</b>	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
<b>Unauthorized SSID/VLAN</b>	Reserved for future use. This event is not generated at this time.
<b>Unknown User in Group</b>	No longer used.
<b>Unsupported Trap</b>	Generated when Network Sentry receives a trap that it cannot interpret from a device. The device's OID is included in the event.
<b>Update SSID Failure Update SSID Success</b>	SSID assignment scheduled task maps VLAN IDs to SSIDs. Event indicates whether or not the task succeeded.
<b>Update VLAN ID Failure Update VLAN ID Success</b>	Indicates that the user specified in the event message powered off the Network Sentry server. See Power Management on page 163.  Update Default VLAN Values scheduled task sets the Default VLAN value for the port in Network Sentry device model to the value entered in the scheduled task. Event indicates whether or not the task succeeded.
<b>User Aged Out</b>	Indicates that the user specified in the event message rebooted the Network Sentry server. See Power Management on page 163.  User has been aged out of the database based on the data stored in the Age Time section of the User Properties view.
<b>User Created User Destroyed</b>	Network user created in or deleted from the database. This is a non-administrative user.
<b>User not NATd</b>	This event is generated on each host that had been previously NATd but are not any longer. One per MAC address on the NATd machine. For example, if a host has both a wired and wireless connection, an event is generated for each.
<b>Users Removed From Directory</b>	User has been removed directly from a Directory such as LDAP. When the Network Sentry user database is synchronized with the Directory this discrepancy triggers the event. If Remove User is selected on your Directory configuration, the missing user is removed from the Network Sentry database.
<b>Valid DHCP Server</b>	Generated when has verified that the DHCP server is running a valid DHCP server application.
<b>Vendor OUI Added</b>	Generated when a new Vendor OUI has been added to the database.

<b>Event</b>	<b>Definition</b>
<b>Vendor OUI Removed</b>	Generated when a Vendor OUI was removed from the database.
<b>VLAN Switch Failure</b>	VLAN failed to change for port X.
<b>VLAN Switch Success</b>	VLAN was changed successfully for X port.
<b>Vulnerability Scan Failed</b>	The host failed the Vulnerability scan.
<b>Vulnerability Scan Finished</b>	Generated when the Vulnerability rescan has finished.
<b>Vulnerability Scan Ignored</b>	Indicates that Vulnerability has not run the scan.
<b>Vulnerability Scan Incomplete</b>	Generated when the scan is configured in Network Sentry but the Vulnerability scanner has not run the scan.
<b>Vulnerability Scan Passed</b>	The host passed the Vulnerability Scan.
<b>Vulnerability Scan Removed</b>	Generated when a Vulnerability scan that was added to Network Sentry was removed from the vendor.
<b>Vulnerability Scan Started</b>	Generated when the Vulnerability rescan has started.
<b>Vulnerability Scanner Connection Failure</b>	Generated when the connection to the Vulnerability Scanner has failed.
<b>Vulnerability Scanner Deleted</b>	Generated when a Vulnerability scanner was deleted from Network Sentry.
<b>Vulnerability Scan Skipped</b>	Generated when the Vulnerability scanner has not run the scan since the previous poll, so Network Sentry skipped the scan during processing.

## Chapter 12: Alarms View

Use the Alarms View to view and manage the contents of the alarm log. The alarm log is a list of all current alarms. The Severity column indicates how serious the alarm is. Severity levels include: Critical, Minor, Warning, Informational.

The state of an alarm is either acknowledged or not acknowledged. The event-to-alarm mapping determines the behavior and characteristics of the alarm. The event-to-alarm mapping feature gives you the option of sending alarms to an external log host. See **Map Events To Alarms** on page 493 for details.

You can remove alarms from the log in two ways:

- Manually, when you select and clear the alarm
- Automatically, when the *clear event* defined in alarm mapping occurs

To access the Alarms View select **Logs > Alarms**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

The screenshot shows the Alarms View interface. At the top, there is a 'Filter' section with a 'Date' dropdown set to 'Last' and a value of '100' days. Below this is an 'Add Filter' dropdown set to 'Select' and an 'Update' button. The main area is titled 'Alarms - Displayed: 26 Total: 26' and includes navigation controls like '<< first < prev 1 next > last >>' and a '200' dropdown. A 'Pause' checkbox is also present. The central table lists alarms with the following columns: Severity, Date, Alarm, Element, and Trigger Rule. The bottom of the interface features an 'Import' button, an 'Export to:' section with icons for CSV, PDF, and RTF, and three large buttons: 'Acknowledge', 'Clear', and 'Show Details'.

Severity	Date	Alarm	Element	Trigger Rule
Critical	02/24/14 01:41 AM EST	L2 Poll Failed	RAC_1301RN1	All Events to One Alarm
Critical	02/24/14 01:11 AM EST	L2 Poll Failed	MeruController	All Events to One Alarm
Critical	02/24/14 01:09 AM EST	L2 Poll Failed	rfs6000-D86A33	All Events to One Alarm
Critical	02/24/14 01:08 AM EST	L2 Poll Failed	XR2023Lab	All Events to One Alarm
Critical	02/21/14 01:36 PM EST	Contact Lost	RuckusAP_Bradford_Lab	
Warning	02/19/14 02:45 PM EST	DHCP Host Name Changed	DELL INC.	
Warning	02/19/14 02:35 PM EST	DHCP Host Name Changed	DELL INC.	
Critical	02/18/14 11:44 AM EST	No Response from DHCP Server	MegaTech	

Figure 195: Alarms View

### Alarms View Field Definitions

Fields used in filters are also defined in this table.

Field	Definition
<b>First Name</b>	First Name of the user associated with the alarm, such as the registered owner of a host or an admin user.
<b>Last Name</b>	Last Name of the user associated with the alarm.
<b>User ID</b>	User name from the credentials of the user who was logged in and associated with the alarm.
<b>Element Name</b>	Name of the device, Admin User, server or process associated with the alarm.
<b>Element Type</b>	Type can be Device, Port, Container, Process, or All.
<b>Group</b>	Group name of a group of elements, such as, port group, device group or user group.
<b>Pause</b>	If enabled, prevents the Alarms List from refreshing and adding new records to the screen. In an environment with a large number of alarms, you may need to pause the refresh in order to research an issue.
<b>Severity</b>	<p>Category indicating how serious the alarm is. Options include: Critical, Minor, Warning and Informational</p> <p>Critical - </p> <p>Minor - </p> <p>Warning - </p> <p>Informational - </p>
<b>Date</b>	Date and time the alarm was triggered.
<b>Alarm</b>	Alarm name. See Network Sentry Events And Alarms List on page 469.
<b>Element</b>	Element associated with the alarm entry, such as a user name, a host name, a switch name or an application name.
<b>Trigger Rule</b>	<p>Rule that determine the conditions under which an alarm is triggered based on an event. Options include:</p> <p><b>One Event to One Alarm</b>—Every occurrence of the event generates a unique alarm.</p> <p><b>All Events to One Alarm</b>—The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm.</p> <p><b>Event Frequency</b>—Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm.</p> <p><b>Event Lifetime</b>—Duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm.</p>
<b>Acknowledged Date</b>	Indicates the date the alarm was acknowledged. If this field is blank, it indicates that the alarm was never acknowledged.
<b>Buttons</b>	

Field	Definition
<b>Import</b>	Import historical records from an Archive file. See <b>Import Archived Data</b> on page 293.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Acknowledge</b>	Acknowledges the selected alarm but does not clear it. The Alarm remains in the displayed until you clear it. A date is displayed in the Acknowledged column when the alarm is acknowledged.
<b>Clear</b>	Clears the selected alarm and removes it from the list.
<b>Show Details</b>	Displays the Details Panel for the selected alarm. See <b>Show/Hide Alarm Details</b> on page 491.

## Show/Hide Alarm Details

The Alarm Details panel launched from the Alarms View displays a detailed narrative about the cause of the selected alarm and the event that triggered it. For example, if there is an alarm indicating that an L2 Poll failed, the possible causes are displayed indicating that the security string may be incorrect or the telnet credentials are incorrect. This gives the administrator two things to verify when trying to correct the problem.

The screenshot shows the Alarm Details interface. At the top, there is a 'Filter' section with a 'Date' dropdown set to 'Last' and a value of '100' days. Below this is an 'Add Filter' dropdown set to 'Select' and an 'Update' button. The main area displays a table of alarms with the following columns: Severity, Date, Alarm, Element, and Trigger Rule. The table contains 8 rows of data. At the bottom of the interface, there are buttons for 'Import', 'Export to:' (with icons for CSV, Excel, PDF, and RTF), 'Acknowledge', 'Clear', and 'Show Details'.

Severity	Date	Alarm	Element	Trigger Rule
Critical	02/24/14 01:41 AM EST	L2 Poll Failed	RAC_1301RN1	All Events to One Alarm
Critical	02/24/14 01:11 AM EST	L2 Poll Failed	MeruController	All Events to One Alarm
Critical	02/24/14 01:09 AM EST	L2 Poll Failed	rfs6000-D86A33	All Events to One Alarm
Critical	02/24/14 01:08 AM EST	L2 Poll Failed	XR2023Lab	All Events to One Alarm
Critical	02/21/14 01:36 PM EST	Contact Lost	RuckusAP_Bradford_Lab	
Warning	02/19/14 02:45 PM EST	DHCP Host Name Changed	DELL INC.	
Warning	02/19/14 02:35 PM EST	DHCP Host Name Changed	DELL INC.	
Critical	02/18/14 11:44 AM EST	No Response from DHCP Server	MegaTech	

**Figure 196: Alarm Details**

1. Select **Logs > Alarms**.
2. Use the Filters to locate the appropriate alarm. Refer to **Alarms View** on page 489 for Filter field definitions.

3. Select the alarm.
4. Click **Show Details**.
5. Review the details displayed.
6. Click **Hide Details** to close the panel.

## Map Events To Alarms

An event indicates that something significant has happened within Network Sentry. All events that are generated are logged in the event log. If an event is mapped to an alarm, you are immediately informed by the alarm notification system. Some events are mapped to alarms by default.

To view events that are mapped to alarms select **Logs > Event to Alarm Mappings**. For a list of possible alarms see **Network Sentry Events And Alarms List** on page 469.

**Note:** If an event is disabled, the associated Alarm Mapping is grayed out and has a line through it. To enable the event, right click on the Alarm Mapping and select one of the Enable options.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

### Enable/Disable Alarm Mappings

When mapping events to alarms, you have the option to disable an alarm mapping to prevent the generation of alarms when the selected event occurs. This may be useful during periods you know will generate many events. An example of this is during the repair of a modeled network device. You may want to block the Device Contact Lost and Established events from getting to the system since they will be expected. Another example is to block the Rogue User Detected event during an Open House when many rogues will be detected. Use the Enable and Disable buttons at the top of the view to enable and disable selected Alarm Mapping records.

Event To Alarm Mappings - Total: 61				
Enable: <input checked="" type="checkbox"/> <input type="checkbox"/>				
Enabled	Event	Alarm	Severity	Trigger Rule
<input type="checkbox"/>	Appliance Weak Password(s)	Appliance Weak Password(s)	Critical	One Event to One Alarm
<input checked="" type="checkbox"/>	Authentication Time-out Failure	Authentication Time-out Failure	Critical	One Event to One Alarm
<input checked="" type="checkbox"/>	Communication lost with BigFix Server Database	Patchlink Server Communication Lost.	Critical	One Event to One Alarm
<input checked="" type="checkbox"/>	Communication lost with PatchLink Server	Patchlink Server Communication Lost.	Critical	One Event to One Alarm
<input checked="" type="checkbox"/>	Contact Lost	Contact Lost	Critical	One Event to One Alarm
<input checked="" type="checkbox"/>	DHCP Host Name Changed	DHCP Host Name Changed	Warning	One Event to One Alarm
<input checked="" type="checkbox"/>	Database Backup Failure	Database Backup Failure	Critical	All Events to One Alarm
<input checked="" type="checkbox"/>	Database Replication Error	Database Replication Error	Critical	Frequency - 3 within 2 minutes
<input checked="" type="checkbox"/>	Device Fingerprint Changed	Device Fingerprint Changed	Warning	One Event to One Alarm
<input checked="" type="checkbox"/>	Device-Link-Up	Device-Link-Up	Critical	Frequency - 20 within 1 minute

Export to:

Options

Figure 197: Event To Alarm Mappings

**Alarm Mapping Field Definitions**

Refer to **Add or Modify Alarm Mapping** on page 497 for additional information on each field.

Field	Definition
<b>Enable Buttons</b>	Enables or disables the selected Alarm Mappings. Disabled mappings do not trigger an alarm when the associated event is generated.
<b>Enabled</b>	A green check mark indicates that the mapping is enabled. A red circle indicates that the mapping is disabled.
<b>Event</b>	Name of the Event that triggers this alarm.
<b>Alarm</b>	Name of the Alarm that is mapped to the event.
<b>Clear Event</b>	Name of the event that must be generated to clear the alarm mapped in this Alarm and Event combination.
<b>Severity</b>	<p>Critical -</p> <p>Minor - </p> <p>Warning - </p> <p>Informational - </p> <p>Only the text of the severity is displayed. Severity icons do not display in the Alarm Mappings table.</p>
<b>Notify Users</b>	Indicates who will be notified if this alarm is triggered, such as, All Management Group.
<b>Trigger Rule</b>	<p>Rules that determine when the alarm is triggered. Options include:</p> <p><b>One Event to One Alarm</b>—Every occurrence of the event generates a unique alarm.</p> <p><b>All Events to One Alarm</b>—The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm.</p> <p><b>Event Frequency</b>—Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm.</p> <p><b>Event Lifetime</b>—Duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm.</p>

Field	Definition
<b>Apply To</b>	<p>Elements to which this alarm mapping applies. Options include:</p> <p><b>All</b>—Applies this mapping to all elements.</p> <p><b>Group</b>—Applies this mapping to a single group of elements.</p> <p><b>Specific</b>—Applies this mapping to an element that you select from a list.</p>
<b>Action</b>	<p>If an Action is enabled in the mapping, displays the action that will be taken when this alarm is triggered. Options include:</p> <p><b>Host Access Action</b>—Host is disabled and then re-enabled after the specified time has passed.</p> <p><b>Host Role</b>—The host's role is changed and then set back to the original role after the specified time has passed.</p> <p><b>Host Security Action</b>—Host is set At Risk and then set to Safe after the specified time has passed.</p> <p><b>Command Line Script</b>—You can specify a particular command line script to be executed as an alarm action.</p> <p><b>Email User Action</b>—An email is sent to the user associated with the host.</p> <p><b>SMS User Action</b>—An SMS Message is sent to the user associated with the host.</p> <p><b>Port State Action</b>—Port is disabled and then re-enabled after the specified time has passed.</p> <p><b>Send Message to Desktop</b>—Send a text message to the desktop of a host(s) with the Persistent Agent or Bradford Mobile Agent for Android installed.</p>
<b>Send To External Log Hosts</b>	<p>Indicates whether this alarm is sent to an external log host when the trigger event occurs, select this check box. Default = No.</p>
<b>Send To Custom Script</b>	<p>Name of the command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts. Scripts are stored on the server in the following directory:</p> <p><code>/home/cm/scripts</code></p>
<b>Event Logging</b>	<p>Indicates where the event is being logged or if logging has been disabled. Options include:</p> <p><b>Disabled</b>—Event is disabled and will not be generated or logged anywhere.</p> <p><b>Internal</b>—Logs only to an internal events database.</p> <p><b>External</b>—Logs only to an external host.</p> <p><b>Internal &amp; External</b>—Logs both to an internal events database and an external host.</p>
<b>Event Logging Group</b>	<p>Group name of a group of elements, such as, port group, device group or user group used to limit generation of the selected event to the items in the group. If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users.</p>

Field	Definition
<b>Last Modified By</b>	User name of the last user to modify the mapping.
<b>Last Modified Date</b>	Date and time of the last modification to this mapping.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Delete</b>	Deletes selected mappings from the database.
<b>Modify</b>	Opens the Modify dialog and allows you to modify the selected mapping.  When multiple mappings are selected, opens a limited Modify dialog and allows you to modify Severity and Notification settings. See Bulk Modify Alarm Mappings on page 502.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item.  For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446  <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Enable</b>	Enables the selected mappings.
<b>Disable</b>	Disables the selected mappings.
<b>Event Logging - Disable</b>	Disables the events associated with the selected mappings.
<b>Event Logging - Internal</b>	Enables the events associated with the selected mappings and logs to an internal events database.
<b>Event Logging - External</b>	Enables the events associated with the selected mappings and logs to an external host.
<b>Event Logging - Internal &amp; External</b>	Enables the events associated with the selected mappings and logs to both an internal events database and an external host.
<b>Export</b>	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

## Add or Modify Alarm Mapping

**Add Event to Alarm Mapping**

Enabled

Trigger Event: Host At Risk

Alarm To Assert: Host At Risk

Severity: Critical

Clear on Event: Host Safe

Send Alarm to External Log Hosts

Send Alarm to Custom Script: AgentlessScanRegisterClient

Apply To: Group Forced Remediation Exceptions

Notify Users: All Management Group

Send Email  Send SMS

Trigger Rule: Event Frequency 2 events occurring within 2 Hours

Action: Email User Action

**Email User Action**

Send an Email message to the user associated with the host.

Email Message: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: %event%

%host%  
%event%

OK Cancel

Figure 198: Add Mapping

1. Select **Logs > Event to Alarm Mappings**.
2. Click **Add** or double-click on an existing mapping to modify it.
3. Refer to the field definitions table below for detailed information about each field.
4. The new mapping is enabled by default. If you wish to disable it, remove the check mark from the **Enabled** check box.
5. In the **Apply To** section, select the element affected by this mapping. You can apply mappings to all elements, a single group of elements, or specific elements.

**Note:** Available selections vary depending upon the selected Trigger Event.

6. Click the box and select an element from the drop-down list.
7. If you choose to Apply To a Group, you can select a group from the list or use the icons next to the group field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See **Add Groups** on page 684 for additional information.
8. Select the **Notify Users** settings.

9. If you choose to Notify Users, you can select an Admin Group from the list or use the icons next to the Group field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See **Add Groups** on page 684 for additional information.
10. Select the **Trigger Rule** for the event from the drop-down list. Rules determine when an Event triggers the creation of an Alarm.
11. If you enable the Action option, select the **Action** to take when the event occurs and the alarm is asserted. These are basic actions that Network Sentry executes on a given alarm.
12. Action parameters display. Select the **Primary Task** from the drop-down list.
13. For some actions there is a secondary task. If desired, click the **Enable** box in the **Run Secondary Task section**, select **Min, Hr, or Day** and enter the corresponding **value**.
14. Click **OK**. The new mapping is saved and appears in the Event/Alarm Map View.

**Table 32: Add/Modify Alarm Mapping Field Definitions**

Field	Definition
<b>Alarm Definition</b>	
<b>Enabled</b>	If checked, the alarm mapping is enabled. Default = Enabled.
<b>Trigger Event</b>	Event that causes the alarm. Whenever this event occurs, its associated alarm is generated. The alarm is automatically listed when you select the event.
<b>Alarm to Assert</b>	The alarm generated when the event occurs.
<b>Severity</b>	Sets the severity of the alarm. Select one of the values from the drop-down list: Critical, Informational, Minor, and Warning. This value may be changed for existing Alarm and Event mappings.
<b>Clear on Event</b>	To automatically clear the alarm when a specific event occurs, select this check box. Select the event that, when generated, causes this alarm to be removed.  If you leave the check box unchecked, you must manually clear the alarm.  Default = Unchecked (Disabled)
<b>Send Alarm to External Log Hosts</b>	The alarm is sent to an external log host when the trigger event occurs, select this check box. See <b>Log Receivers</b> on page 127 for details on configuring an external log host.  Default = Unchecked (Disabled)

Field	Definition
<b>Send Alarm to Custom Script</b>	<p>You can specify a particular command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts.</p> <p>First, write the script that is to be used as the alarm action. Store the script in this directory:</p> <pre>/home/cm/scripts</pre> <p>If there are no scripts in the directory, this field is not available. Click the check box to enable the option and select the correct script from the drop-down list.</p> <p>The arguments that are automatically passed to the script are as follows:</p> <ul style="list-style-type: none"> <li>• <b>type</b> — EndStation. User or Network Device</li> <li>• <b>name</b> — name of element</li> <li>• <b>ip</b> — IP address</li> <li>• <b>mac</b> — MAC address</li> <li>• <b>user</b> — userID</li> <li>• <b>msg</b> — email message from alarm</li> </ul>
<b>Apply To</b>	<p><b>All</b>—Applies this mapping to all elements.</p> <p><b>Group</b>—Applies this mapping to a single group of elements.</p> <p><b>Specific</b>—Applies this mapping to the element that you select from a list.</p>
<b>Notify Users</b>	
<b>Notify</b>	If checked, the administrators in the selected group are notified when an alarm occurs.
<b>Send Email</b>	If checked, the administrators in the selected group are sent an email when the alarm occurs. Administrators must have an email address configured in the Modify User dialog to receive this email.
<b>Send SMS</b>	If checked, the administrators in the selected group are sent an SMS message when an alarm occurs. Administrators must have a Mobile Number and Mobile Provider configured to receive this SMS message.
<b>Trigger Rules</b>	
<b>One Event to One Alarm</b>	Every occurrence of the event generates a unique alarm.
<b>All Events to One Alarm</b>	<p>The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur.</p> <p>When the alarm clears, the next occurrence of the event generates another unique alarm.</p>

Field	Definition
<b>Event Frequency</b>	<p>The number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. Settings are updated when the Action is configured. Example:</p> <p>Assume the “Host Connected” event is mapped to an alarm and the frequency is set to 3 times in 10 minutes.</p> <ul style="list-style-type: none"> <li>• Host A connects 3 times in 10 minutes and the alarm is triggered.</li> <li>• Host A connects 2 times and host B connects 2 times, there are 4 connections in 10 minutes. No alarm is generated because the hosts are different.</li> <li>• Host A connects at minutes 1, 8 and 12. No alarm is triggered because the host did not connect 3 times in 10 minutes.</li> <li>• Host A connects at minutes 1, 8, 12, and 14. An alarm is triggered because connections at minutes 8, 12 and 14 fall within the 10 minute sliding window.</li> </ul>
<b>Event Lifetime</b>	<p>The duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm. Example: Event A occurs. If Event B (clear event) does not occur within the specified time, an alarm is generated.</p>
<b>Actions</b>	
<b>Action</b>	<p>If checked, the selected action is taken when the alarm mapping is active and the alarm is asserted.</p>
<b>Host Access Action</b>	<p>Host is disabled and then re-enabled after the specified time has passed.</p>
<b>Host Role</b>	<p>The host's role is changed and then set back to the original role after the specified time has passed. Roles are attributes of the host and are used as filters in User-/Host Profiles. Those profiles determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy to apply.</p> <p>Note: If roles are based on a user's attribute from your LDAP or Active Directory, this role change is reversed the next time the directory and the Network Sentry database resynchronize.</p>
<b>Host Security Action</b>	<p>Host is set At Risk and then set to Safe after the specified time has passed.</p>
<b>Command Line Script</b>	<p>You can specify a particular command line script to be executed as an alarm action. These command line scripts are for advanced use, such as administrator-created Perl scripts.</p> <p>First, write the script that is to be used as the alarm action. Store the script in this directory:</p> <pre>/home/cm/scripts</pre> <p>The IP and MAC address arguments that are automatically passed to the script are in the format shown in this example:</p> <pre>/home/cm/scripts/testScript 192.168.10.1 00:00:00:00:00:00</pre>

Field	Definition
<b>Email User Action</b>	<p>An email is sent to the user associated with the host. The text of the email is entered in the Email Host Action dialog box.</p> <p>HTML tags may be added to text within the content of the email in order to format the text, convert the text to a link, etc.</p> <p>For example, you can add the &lt;b&gt; and &lt;/b&gt; tags to text in the Email message window to bold the selected text in the recipient's email message.</p>
<b>SMS User Action</b>	<p>An SMS Message is sent to the user associated with the host. The text of the message is entered in the SMS User Action dialog box. The recipient must have a Mobile Number and Mobile Provider configured.</p>
<b>%host%</b>	<p>Allows you to include information specific to the non-compliant host in the email or SMS alert message.</p> <p>For example, this message:</p> <p style="padding-left: 40px;">The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue. %host%</p> <p>is displayed as:</p> <p style="padding-left: 40px;">The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue:</p> <p style="padding-left: 80px;">Host:</p> <p style="padding-left: 120px;">Host Name: TestUser-MacBook-Pro-2</p> <p style="padding-left: 120px;">OS: Mac OS X 10.7.5</p> <p style="padding-left: 120px;">Network Adapters:</p> <p style="padding-left: 160px;">Connected 3C:07:54:2A:88:6F,192.168.10.143,Concord-3750 Fa3/0/46</p> <p style="padding-left: 160px;">Disconnected 60:C5:47:8F:B1:66,192.168.4.70,Concord_Cisco_1131.bradfordnetworks.com VLAN 4</p>

Field	Definition
%event%	<p>Allows you to include information specific to the event in the email or SMS alert message.</p> <p>For example, this message:</p> <p>The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: %event%</p> <p>is displayed as:</p> <p style="padding-left: 40px;">The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue:</p> <p style="padding-left: 80px;">Host failed Test-Host</p> <p style="padding-left: 80px;">Tests:</p> <p style="padding-left: 120px;">Failed :: Anti-Virus :: ClamXav</p> <p style="padding-left: 120px;">MAC Address: 3C:07:54:2A:88:6F</p> <p style="padding-left: 120px;">Last Known Adapter IP: 192.168.10.143</p> <p style="padding-left: 120px;">Host Location: Concord-3750 Fa3/0/46</p> <p style="padding-left: 80px;">. Remediation Delayed.</p>
Port State Action	The port is disabled and then re-enabled after the specified time has passed.
Send Message to Desktop	Send a text message to the desktop of a host(s) with the Persistent Agent or Bradford Mobile Agent for Android installed.

### Bulk Modify Alarm Mappings

This option displays on the right-click menu only when multiple mappings are selected in the Event to Alarm Mappings View. It provides a limited Modify dialog with options to modify Severity and Notification settings.

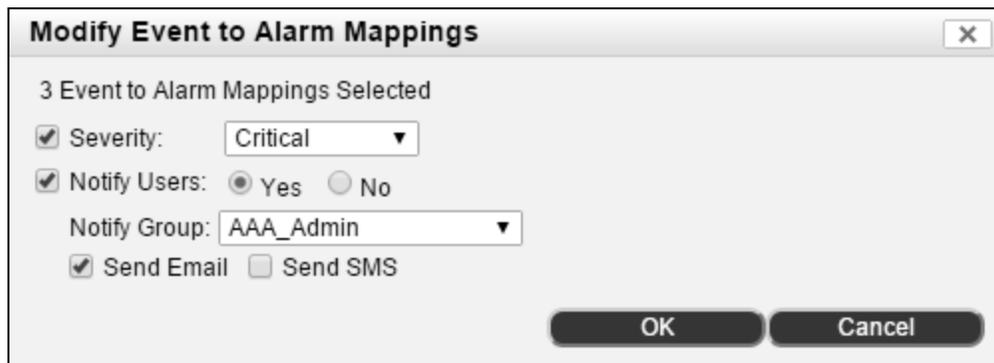


Figure 199: Bulk Modify Event To Alarm Mappings

1. Select **Logs > Event to Alarm Mappings**.
2. Use Ctrl or Shift to select multiple Alarm Mappings.

3. Right-click on the selected records and choose **Modify** from the pop-up menu.
4. Use the field definitions in the table below to modify the selected mappings.
5. Click OK to save your changes.

Field	Definition
<b>Severity</b>	Enables the Severity drop-down. The severity level of the alarm. Options include: Critical, Informational, Minor and Warning.
<b>Notify Users</b>	Enables the Notify Users settings.
<b>Notify Group</b>	Drop-down list of Admin groups. Use this to determine who will be notified when this alarm is triggered. The default is the All Management Group which contains all Admin users.
<b>Send Email</b>	If enabled, Admin Users in the selected group receive an email when this alarm is triggered.
<b>Send SMS</b>	If enabled, Admin Users in the selected group receive a text message when this alarm is triggered. Admin Users must have a mobile phone number and a mobile provider listed on their user records to receive SMS messages.

### Delete Alarm Mapping

1. Select **Logs > Event to Alarm Mappings**.
2. Select the appropriate mapping record from the list displayed.
3. Click **Delete**.
4. At the prompt, click **OK**.



## Chapter 13: Policies

Policies are assigned to hosts based on the User/Host Profile associated with each policy. User/Host Profiles allow you to select one or more pieces of user or host data to match with users and hosts and determine which policy is applied to that host. Policies are ranked in priority starting with number 1. When a host requires a particular service, the host and user data are compared to the User/Host Profile in each policy starting with the first policy in the list. If the host and user do not match criteria in the first policy, the next one is checked until a match is found.

Policies that are created on the FortiNac Control Manager are Global and cannot be modified at the server(s).

**Table 33: Policy Types**

Policy	Definition
<b>Endpoint Compliance Policy</b>	Maps scans and agents to hosts to evaluate the host from a security perspective.

Types of data used to determine whether or not the host/user is a match include the following:

<b>Data</b>	<b>Definition</b>
<b>Where (Location)</b>	One or more port or device groups. A User/Host Profile can include more than one port or device group, however the connection location only needs to be contained in one of the selected groups. If the Location field is empty it is set to Any, indicating that location is not being used as criteria for the match, therefore any host connection location would be a match. .
<b>Who/What by Group</b>	One or more user or host groups. If the host or user is in at least one of the groups listed, then the host is considered a match. If this field is empty, it is set to Any, indicating that the Groups field is not used as criteria for the match, therefore any host is a match.
<b>Who/What by Attribute</b>	Allows you to create matches based on Adapter, Host or User data. A single filter can contain checks for multiple pieces of data, however the host, user and adapter must be an exact match to all of that data. If more than one filter is used, the host, user and adapter need only match the contents of one filter to be a match for the policy. See User/Host Profile Filter Example on page 517 for additional information on filters.
<b>When</b>	Allows you to create matches based on the current time. If Always is selected, then time of day is not used. If Specify Time is selected, then the current time must be within the days and times included in the list to be a match for the host.

The host/user must match at least one item in each field that contains criteria other than Any. If the host/user does not match something in all fields, the policy is not selected and the next policy is checked.

---

**Note:** A host that has had a policy applied based on time of day, may be moved to a different policy when the window of time in the current policy has passed. For example, the host may be moved to another VLAN or disconnected from the network when the window of time in the applied Endpoint Compliance Policy has passed. Hosts are re-evaluated frequently, such as, when the device where they are connected is polled or when the Persistent Agent contacts the server. If another Policy exists that applies to this host, the host will be provided with configuration parameters from that new policy.

---

**Note:** There may be more than one Policy that is match for this host/user, however, the first match found is the one that is used.

---

**Note:** Policy assignments are not permanent. Each time a host is re-evaluated by Network Sentry, the User/Host Profile data is re-evaluated and a Policy is selected.

---

## Policy Assignment

Policies are applied to hosts by comparing user and host data to the User/Host Profile contained in the each policy until a match is found. The example below demonstrates this process.

**Figure 200: User/Host Profile**

**Table 34: Sample Policy Types**

Policy Type	Location	Groups	Attributes	Time	Host Notes
<b>Location Based</b>	One or more Port or Device Groups	Any	None	Always	Host connects to a port or device in one of the selected groups and is assigned this policy.
<b>Role Based</b>	Any	Any	User Role = (Role Name)	Always	Host connects to the network. If the logged in user has the selected role, the host is assigned this policy.

Policy Type	Location	Groups	Attributes	Time	Host Notes
<b>Role Based</b>	Any	Any	Host Role = (Role Name)	Always	Host connects to the network. If the host has the selected role, it is assigned this policy.
<b>Security and Access Attribute Value</b>	Any	Any	User SaaV = (Attribute Value)	Always	Host connects to the network. If the logged in user has the selected Security and Access Value, the host is assigned this policy.
<b>Group Based</b>	Any	User Group1 User Group2	None	Always	Host connects to the network. If the logged in user is a member of either one of the selected groups, the host is assigned this policy.
<b>Group Based</b>	Any	Host Group1 Host Group2	None	Always	Host connects to the network. If the host is a member of either one of the selected groups, it is assigned this policy.
<b>Guest</b>	Any	Any	Guest Role = Role Name	Always	Host connects to the network. If the Guest has the selected role, the host is assigned this policy.
<b>Registration</b>	Any	Any	Host = Rogue	Always	Host connects to the network. If the host is a rogue, it is assigned this policy.
<b>Remediation</b>	Any	Any	Host State = At Risk	Always	Host connects to the network. If the host state is At Risk, it is assigned this policy.
<b>VPN</b>	Any	Any	Host = VPN Client	Always	Host connects to the network. If the host is a VPN Client, it is assigned this policy.
<b>Time of Day</b>	Any	Any	None	Monday - Friday 9 am to 5 pm	Host connects to the network. If the connection time is on any day Monday through Friday and between 9 am and 5 pm, it is assigned this policy.
<b>Default or Catch All</b>	Any	Any	None	None	This policy will match ALL hosts and users. Host connects to the network. If the host does not match any other policy, it is assigned this policy. When this policy is reached, no other policies after it will be considered.

**Example:**

The example below outlines how Network Sentry would choose an Endpoint Compliance Policy for a specific host.

Assume the Host has the following characteristics:

- Connects on a port that is contained within the Library Ports group.
- Host is a member of the Accounting Group and the Finance Group.
- Host is running a Persistent Agent.
- Logged in user has a Role called Management.
- Logged in user has a Security and Access Attribute value of Accounting.

Rank	Policy	Location	Groups	Attributes	Process
1	Policy A	Port Group = Lobby Ports	Accounting	Filter1=User Role "Staff"	<p><b>Location</b> - Not a match</p> <p><b>Group</b> - Matches</p> <p><b>Attribute1</b> - Not a Match</p> <p>Go to the next policy.</p>
2	Policy B	Port Group = Library Ports	Accounting	<p>Filter1=User Role "Management" and User Security and Access Value "Human Resources"</p> <p>Filter2=User Role "Staff"</p>	<p><b>Location</b> - Matches</p> <p><b>Group</b> - Matches</p> <p><b>Filter1</b> - Does not match both pieces of data.</p> <p><b>Filter2</b> - Does not match.</p> <p>Go to the next policy.</p>

Rank	Policy	Location	Groups	Attributes	Process
3	Policy C	Port Group1 = Lobby Ports Port Group2 = Second Floor Ports	Finance Admin	Filter1=User Role "Staff" and User Security and Access Value "Accounting"  Filter2=User Role "Management" and Host has Persistent Agent	<p><b>Location</b> - Not a match for either location.</p> <p><b>Group</b> - Matches Finance group</p> <p><b>Filter1</b> - Does not match both pieces of data.</p> <p><b>Filter2</b> - Matches all data.</p> <p>In this case, the fact that the neither location matches prevents the host from getting this policy. In the Group field, the host or user need only match one group. In the filter field, the host or user need only match one filter as long as it matches all parts of the filter.</p> <p>Go to the next policy.</p>
4	Policy D	Any	Finance Admin	Filter1=User Role "Management" and Host has Persistent Agent  Filter2=User Role "Executives" and Host has Persistent Agent	<p><b>Location</b> - No location selected so this field is not used.</p> <p><b>Group</b> - Matches Finance group</p> <p><b>Filter1</b>=Matches all data</p> <p><b>Filter2</b>=Does not match both pieces of data</p> <p>This policy is selected for the host because Location is irrelevant, one group matches and one filter matches.</p>

Rank	Policy	Location	Groups	Attributes	Process
5	Policy E	Port Group1 = Library Ports  Port Group2 = Second Floor Ports	Finance  Admin	Filter1=User Role "Management" and Host has Persistent Agent  Filter2=User Role "Executives" and Host has Persistent Agent	<b>Location</b> - Matches Port Group1  <b>Group</b> - Matches Finance group  <b>Filter1</b> =Matches all data  <b>Filter2</b> =Does not match both pieces of data  This policy is not selected because policies are checked in order by rank. The policy in rank 4 has already been selec- ted even though this policy matches on more points. You must be careful about the order of the policies to ensure that the correct policy is applied to a host.

## User/Host Profiles

User/Host Profiles are used to map sets of hosts and users to Network Access Policies, Endpoint Compliance Policies, Supplicant EasyConnect Policies, Portal Polices, or Security Rules (RTR must be enabled. User/Host Profiles can be reused across many different policies.

For example, Network Access Policies are used to assign the VLAN in which a host is placed. Each Network Access Policy has a specific User/Host profile and a Network Access Configuration containing a VLAN, CLI Configuration or VPN Group. When a host requires network access, Network Sentry looks at the Network Access Policies starting with the first policy in the list and checks that the User/Host profile is a match. If it is not, the next Network Access Policy is checked until a match is found.

User/Host Profiles are combinations of User/Host data. A host's or user's profile is not fixed but can change based on the user/host being moved to a different group, having a new attribute applied, connecting to the network in a different place or the current time of day. Users/hosts are only classified at the time that they need a service, such as a Network Access Policy. When Network Sentry evaluates a host connection, the data for the user and host are prioritized as follows:

- Logged in User and Host
- Registered User and Host
- Registered Host

**Important:** If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

User/Host Profiles can be accessed from **Policy > Policy Configuration > User/Host Profiles** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > User/Host Profiles**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Where (Location)	Who/What by Group	Who/What by Attribute	When
Yes	Administration	Any	Any	No	Sa 12:00 AM - 11:59 PM
Yes	Matches All Users	Any	Any	No	Su 12:00 AM - 11:59 PM

Figure 201: User/Host Profiles View

**User/Host Profiles View Field Definitions**

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Name</b>	Each profile must have a unique name.

Field	Definition
<b>Where (Location)</b>	Location on the network where the host is connected. This field lists groups of ports, SSIDs or devices. Hosts are checked to determine whether they have connected to the network via one of the selected devices, ports or SSIDs. Host must connect on one of the items contained within one of the selected groups to match this profile. When set to Any, this field is a match for all hosts or users.
<b>Who/What By Group</b>	Host or User groups where the host or user must be a member to match this profile. Host or user must be in at least one of the groups listed. When set to Any, this field is a match for all hosts or users.
<b>Who/What By Attribute</b>	Indicates whether or not attribute filters have been created for this Profile. Filters are based on Adapter, Host and User data. A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. See User/Host Profile Filter Example on page 517.
<b>When</b>	If the host is on the network during the specified time frame, it matches this profile. Time options include Always or a specific set of days of the week and times of the day.
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry.
<b>Last Modified By</b>	User name of the last user to modify the profile.
<b>Last Modified Date</b>	Date and time of the last modification to this profile.
<b>Right Mouse Click Menu - Options Button Menu</b>	
<b>Copy</b>	Copy the selected Profile to create a new record.
<b>Delete</b>	Deletes the selected Profile. Profiles that are currently in use cannot be deleted.
<b>In Use</b>	Indicates whether or not the selected Profile is currently being used by any other Network Sentry element. See User/Host Profiles In Use on page 524.
<b>Modify</b>	Opens the Modify Profile window for the selected Profile.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446
	<b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Buttons</b>	
<b>Import</b>	Allows you to import information from the Network Sentry Server(s) to the NCM. This eliminates the need to manually enter the information on the NCM. When it is imported to the NCM, the information is global.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export Data on page 383.

## Add/Modify A User Or Host Profile

You are not required to complete all of the fields when creating a User/Host Profile. If you leave a field blank, it is set to Any or is left blank. When set to Any or blank, the field is a match for all hosts or users. You can create a profile with only location, only a group, only an attribute filter, only a time range or any combination of those options.

Figure 202: Add User/Host Profile

1. Select **Policy > Policy Configuration**.
2. In the menu on the left, **User/Host Profiles** should be selected.
3. Click the **Add** button or select an existing Profile and click **Modify**.
4. Click in the **Name** field and enter a name for this Profile.
5. Click the **Select** button next to the **Where (Location)** field. This opens the Select Location window.

Choose one or more device, port or SSID groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column.

---

**Note:** In the Select Location window, you can click **Add Group** to create a group, or click **Modify Group** to modify the selected group.

Click **OK** to continue.

6. Click the **Select** button next to the **Who/What by Group** field. This opens the Select Groups window.

Choose one or more Host, User, or Administrator groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column.

---

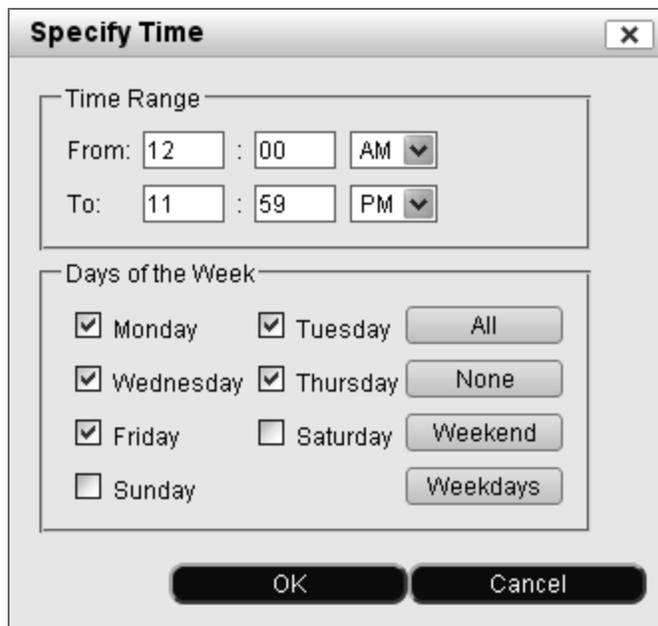
**Note:** In the Select Groups window, you can click **Add Group** to create a group, or click **Modify Group** to modify the selected group.

Click **OK** to continue.

7. **To add a filter**, click the **Add** button next to the **Who/What by Attribute** field. These filters narrow the number of hosts to which this Profile applies.

The Adapter, Host, User, Application Filter window displays allowing you to select one or more pieces of data to use as a filter. See **Host View And Search Field Definitions** on page 327, **Adapter View And Search Field Definitions** on page 372, **User View And Search Field Definitions** on page 400, and **Application View** on page 378 for detailed descriptions of the fields on the Filter window.

8. Click in the drop-down menu next to the **When** field. Select either **Always** or select **Specify Time**. **Always** indicates that there is no time criteria to match this Profile. **Specify Time** allows you to choose days and times to be used as criteria for connecting hosts. Hosts must connect to the network during the selected times to match this profile.
9. **To specify a time**, select **Specify Time** in the drop-down to display the Specify Time dialog.



**Figure 203: Specify Time**

In the **Time Range** section enter the **From** and **To** times for the time of day that devices should be able to access the network.

In the **Days of the Week** section select the days during which these devices should be allowed to access the network.

Click **OK**.

10. Click **OK** to save your data.

## User/Host Profile Filter Example

User/Host Profiles contain filters to narrow the group of hosts or users that match a particular profile. This allows you to create special profiles for certain hosts or users and filter by host, adapter or user criteria. For example, if you had hosts that were running on different operating systems, you might want to have a special profile for each operating system. By filtering for the operating system, you could provide different treatment for each type of host without having to create and maintain special host groups.

### **Filter Examples**

Filters are based on Host, Adapter or User attributes and can be applied such that the host or user must meet all criteria or only some criteria. Within the Who/What by Attribute filter, the user/host must match all of the data specified. If there are multiple Who/What by Attribute filters, the user/host must match all of the data specified in only one of the filters.

Assume that you want to create User/Host Profile A to handle rogue hosts by Operating System. In this case, the host must meet the following criteria to match User/Host Profile A:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = Running a Windows operating system and is a Rogue (not registered).

**Add User/Host Profile**

Name: Windows Rogue Hosts

Where (Location): Device Group A

Who/What by Group: Any

Who/What by Attribute: Host [Operating System: Windows, Type: Rogue]

When: Always

Note:

**Figure 204: User/Host Profile - One Host Filter**

In the second example, the User/Host Profile contains two options under Who/What by Attribute. The first filter requires that the host state be Safe and Authenticated. The second filter requires that the host be a VPN client. In this case the host must meet the following criteria to match the User/Host Profile:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = One of the following sets of options from the filters
  - Host must be Safe and Authenticated
 or
  - Host must be a VPN Client

**Modify User/Host Profile** [X]

Name:

Where (Location):

Who/What by Group:

Who/What by Attribute:

- Host [Security Status: Safe, Authenticated: Yes]
- Host [VPN Client: Yes]

When:  [v]

Note:

Not currently in use

**Figure 205: User/Host Profile - Two Host Filters**

### User/Host Profile Example

Assume that you are running a network at a University. You have Students and Faculty that must be allowed on the network. Due to the volume of traffic you determine that you will have four VLANs. This division of network users requires a mechanism for matching them to the appropriate VLANs. To accomplish this task you must do the following:

- Determine how you are going to divide your network users into four groups. In this case you decide that you will break up users as follows:
  - Students that connect to devices in Dorm A
  - Students that connect to devices in Dorm B
  - Faculty running Windows
  - Faculty running Mac OS X
- Make sure that Students are in a group labeled Students and Faculty are in a group labeled Faculty.
- Make sure that you have two device groups, one for devices in Dorm A and another for devices in Dorm B.
- Based on the divisions you have selected, you must create four User/Host Profiles. You need one Profile for each combination of data that defines a set of users, such as Students that connect to devices in Dorm A.
- Create four Network Access Configurations to configure the VLANs for your four groups of users.
- Create four Network Access Policies to map the four User/Host Profiles to the appropriate VLANs.

## User/Host Profiles

Create four User/Host Profiles that have the following settings:

Name	Where (Location)	Who/What by Group	Who/What by Attribute	Time
<b>Students Dorm A</b>	Device Group = Dorm A Devices	User Group = Students	None	Always
<b>Students Dorm B</b>	Device Group = Dorm B Devices	User Group = Students	None	Always
<b>Faculty Windows</b>	Any	User Group = Faculty	Host OS = Windows	Always
<b>Faculty Mac OS X</b>	Any	User Group = Faculty	Host OS = Mac OS X	Always

**Modify User/Host Profile**

Name:

Where (Location):

Who/What by Group:

Who/What by Attribute:

When:

Note:

Not currently in use

Figure 206: User/Host Profile Example

### Network Access Configurations

Create a Network Access Configuration for each of the four VLANs that you wish to assign. For this example we will create configurations for VLANS 10, 20, 30 and 40.

Name	Access Value
Students Dorm A VLAN	10
Students Dorm B VLAN	20
Faculty Windows VLAN	30
Faculty Mac OS X VLAN	40

The screenshot shows a dialog box titled "Modify Network Access Configuration". It contains the following fields and controls:

- Name:** A text input field containing "Student Dorm A VLAN".
- Access Value/VLAN:** A text input field containing "10".
- Access Value is an alias:** An unchecked checkbox.
- CLI Configuration:** A dropdown menu set to "Disable", with a "Print" icon and a "Refresh" icon to its right.
- Note:** A large empty text area.
- In use in 1 location:** A text label with a link icon.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 207: Network Access Configuration Example

## Network Access Policies

Now you must map the User/Host Profiles to the Network Access Configurations you created. That will tie the different types of users to the appropriate VLAN. Create four Network Access Policies that contain the following data:

Name	User/Host Profile	Network Access Configuration
Students Connecting in Dorm A	Students Dorm A	Students Dorm A VLAN
Students Connecting in Dorm B	Students Dorm B	Students Dorm B VLAN
Faculty running Windows	Faculty Windows	Faculty Windows VLAN
Faculty running Mac OS X	Faculty Mac OS X	Faculty Mac OS X VLAN

**Add Network Access Policy** [X]

Name:

User/Host Profile:  [v] [i] [c]

Network Access Configuration:  [v] [i] [c]

Note:

OK Cancel

Figure 208: Network Access Policy Example

### User/Host Profiles In Use

To find the list of Network Sentry features that reference a specific User/Host Profile, select the Profile from the User/Host Profiles View and click the **In Use** button. A message is displayed indicating whether or not the Profile is associated with any other features. If the Profile is referenced elsewhere, a list of each feature that references the Profile is displayed.



**Figure 209: Profile In Use**

### Delete A User/Host Profile

If a profile is in use by another configuration or feature in Network Sentry, it cannot be deleted. A dialog displays with a list of the configurations in which the profile is used. Remove the association between the profile and other configurations before deleting the profile.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left, **User/Host Profiles** should be selected.
3. Select the profile to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the profile.

## Endpoint Compliance Policies

Endpoint Compliance Policies are used to assess hosts and determine if they are safe. An Endpoint Compliance Policy is composed of building blocks, including: a User/Host Profile and an Endpoint Compliance Configuration. Refer to **Endpoint Compliance Implementation** on page 529 for information on the entire Endpoint Compliance feature.

When a host is evaluated and Network Sentry determines that the host requires an Endpoint Compliance Policy, the host and user are compared to the User/Host Profiles within each Endpoint Compliance Policy starting with the first policy in the list. When a match is found, the Endpoint Compliance Policy is applied. Once a policy is selected as a match for the host or user, the Endpoint Compliance Configuration within the policy determines the treatment that the host receives. An Endpoint Compliance Configuration specifies whether or not an agent is required and the scan parameters for scanning the host.

**Note:** Endpoint Compliance policies created on the Network Sentry server will be ranked above global Endpoint Compliance Policies created on the NCM. The rank of a local Endpoint Compliance Policy can be adjusted above or below another local Endpoint Compliance Policy, but cannot be ranked below a global Endpoint Compliance Policy. The rank for a global Endpoint Compliance Policy cannot be modified from the Network Sentry server.

**Note:** If the user/host does not match any policy, it is allowed to register with no scan and no policy.

**Note:** There may be more than one Endpoint Compliance Policy that is a match for this host/user, however, the first match found is the one that is used.

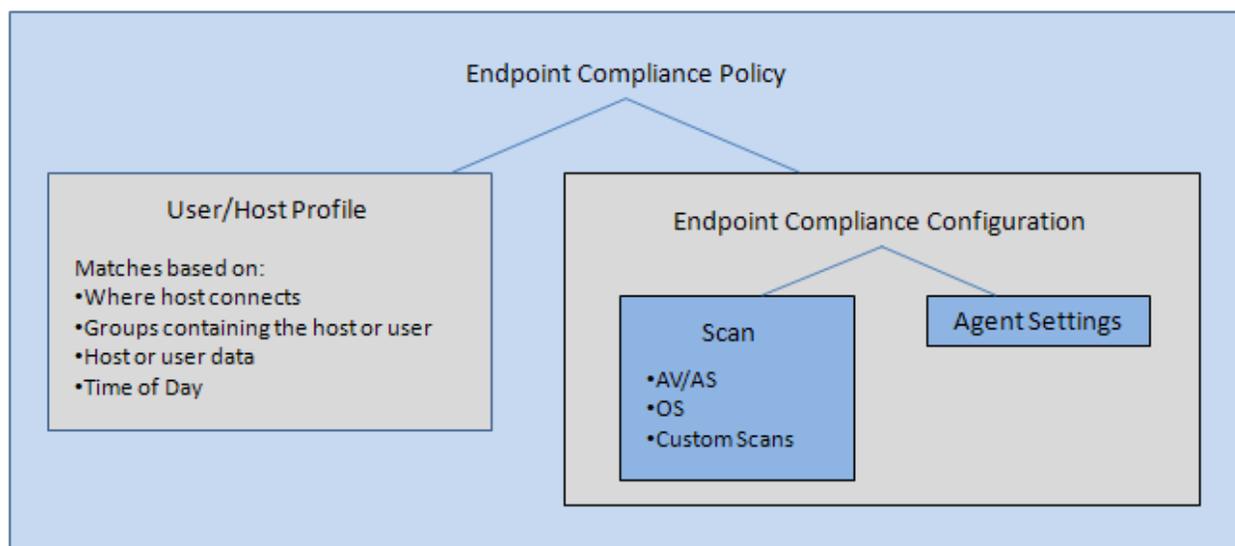


Figure 210: Endpoint Compliance Policy Components

**Important:** If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Endpoint Compliance Policies can be accessed from **Policy > Policy Configuration > Endpoint Compliance**, however configuration steps point you to **Policy > Policy Configuration > Endpoint Compliance**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Rank	Name	Endpoint Compliance Configuration	User/Host Profile	Note	Last Modified By	Last Modified Date
Yes	1	Executive Policy	General Configuration	Administration		root	09/02/16 01:36 PM EDT
Yes	2	General Policy	General Configuration	Matches All Users		root	09/02/16 01:36 PM EDT

Figure 211: Endpoint Compliance Policies View

**Endpoint Compliance Policies Field Definitions**

An empty field in a column indicates that the option has not been set.

Field	Definition
<b>Rank Buttons</b>	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.
<b>Set Rank Button</b>	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies this process is faster than using the up and down Rank buttons.
<b>Table Columns</b>	

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Rank</b>	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
<b>Name</b>	User defined name for the policy.
<b>Endpoint Compliance Configuration</b>	Contains the configuration for the Agent and Scan parameters that will be assigned if this Policy matches the connecting host and user. See Endpoint Compliance Configurations on page 536.
<b>User/Host Profile</b>	Contains the required criteria for a host or user, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Endpoint Compliance Configuration. See User/Host Profiles on page 511.
<b>Where (Location)</b>	The connection location specified in the User/Host Profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
<b>Who/What by Group</b>	User or Host group or groups specified in the User/Host Profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users.
<b>Who/What by Attribute</b>	User or Host attributes specified in the selected User/Host Profile. The connecting host or user must have the attributes to be a match. See User/Host Profile Filter Example on page 517.
<b>When</b>	The time frame specified in the selected User/Host Profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry.
<b>Last Modified By</b>	User name of the last user to modify the policy.
<b>Last Modified Date</b>	Date and time of the last modification to this policy.
<b>Right Mouse Click Menu Options</b>	
<b>Delete</b>	Deletes the selected Endpoint Compliance Policy.
<b>Modify</b>	Opens the Modify Endpoint Compliance Policy window for the selected policy.

Field	Definition
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446
	<b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

## Endpoint Compliance Implementation

Endpoint Compliance allows you to create security policies and use those policies to scan network users' computers for compliance with your organization's network usage rules. The implementation of this feature set can vary widely from one organization to another based on how restrictive or open you choose to make it. You can simply monitor hosts for non-compliance or go so far as to completely block network access. You can institute scans based on simple options included in Network Sentry or create your own custom scans. This section of the documentation discusses the implementation in the approximate order in which it should be done. It also details optional features that you may or may not choose to implement. As the options are discussed, links to additional information are provided.

**Note:** Before implementing Endpoint Compliance, it is recommended that you notify all users about your network usage requirements. This helps users anticipate the changes and reduces calls to your IT Staff.

### Endpoint Compliance Policy

When you have determined the agent or agents to be used, you are ready to begin configuring your Endpoint Compliance Policies.

- Create User/Host Profiles to determine which users/hosts will match a policy. See **User/Host Profiles** on page 511.
- Create Endpoint Compliance Policies to evaluate the hosts connecting to your network. See **Endpoint Compliance Policies** on page 525.
- Policies contain Scans that rely on having up-to-date information about Anti-Virus, Anti-Spyware and Operating Systems. In order to ensure that you have the latest information at all times you should configure a schedule for and run the Auto Def Updates. See **Schedule Auto-Definition Updates**.
- If you plan to use Custom Scans, you must create them first and then associate them with a Scan. This can be done at any time you feel that a custom scan is necessary. New custom scans can be associated with existing Scans. See **Custom Scans Overview** on page 578.
- For each Scan that you create, decide how often to rescan hosts assigned to that policy. Setup a rescan schedule. See **Schedule A Scan** on page 570.
- If you are using the Dissolvable Agent and you want to allow hosts to rescan at their convenience, enable Proactive scanning. See **Add Proactive Scanning To A Scheduled Scan** on page 573.
- When a host fails a scan the user sees a web page with a list of reasons for the failure. To comply with your organization's requirements, that host may need access to certain web sites. For example, if the host failed because virus definitions were not up to date, that host needs to access the anti-virus software

manufacturer's web page to download new virus definitions. Network Sentry has a list of web sites that are made accessible even when a host has failed a scan. Make sure that the web sites for the software you require are included in that list on the Network Sentry server(s).

- To understand what determines the policy that is assigned to a host, see **Policy Assignment** on page 507.

### Events & Alarms

- Make sure the **Security Risk Host** event is enabled, so that an event is generated any time a host fails a scan. The event message provides you with information about the host and why they failed. This is optional, but may be helpful in troubleshooting. See **Enable And Disable Events** on page 454.
- You can view the list of events that have been generated by going to the Events View. See **Events View** on page 466.
- If you would like to be notified that a host has failed a scan, map the **Security Risk Host** event to an alarm. Within the alarm configuration you can specify that you would like to be notified via email or you can use the Alarm Panel on the dashboard. This alarm notifies you when a host has failed a scan and helps you trouble shoot any problems. You can also set up e-mail notification for users so they are aware that their host failed a scan. See **Map Events To Alarms** on page 493 and Alarm Panel.
- Make sure that your administrator e-mail address and your e-mail server have been configured or Network Sentry will not be able to send e-mail notifications. See **Email Settings** on page 125.

### Scan Hosts Without Enforcing Remediation - Optional

To scan hosts without placing "at risk" hosts in remediation you can enable one or more options. See **Scan Hosts Without Enforcing Remediation** on page 551 for more details.

- Disable Quarantine VLAN switching to scan hosts but not mark them "at risk".
- Enable the Audit Only option on an Endpoint Compliance Policy. Hosts that fail when scanned with that policy are not marked "at risk" .
- Add hosts to the Forced Remediation Exceptions Group. Hosts in this group are scanned with the policy that corresponds to them. Hosts that fail the scan are marked "at risk" but are not forced into remediation.

### Delayed Remediation For Scanned Hosts - Optional

Allows you to scan hosts, notify the users of hosts that fail the scan of any pending issues, but not place the host in Remediation for a specified number of days. See **Delayed Remediation For Scanned Hosts** on page 553

- Enable the Delayed Remediation setting on one or more Endpoint Compliance Policies by entering the number of days for the delay.

### Authentication

- If you are using the Persistent Agent, you must set the method for authenticating your users in the Credential Configuration and in Portal Configuration in the Network Sentry Server(s). The authentication method selected must be the same in both places.

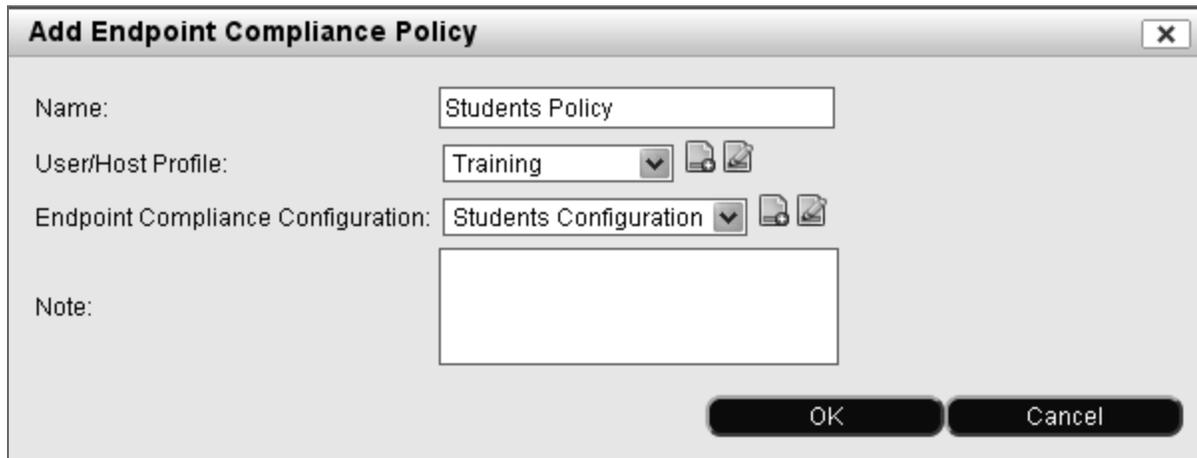
### Monitoring

- Use the Health Tab under Host Properties to view detailed scan information for an individual host. See **Host Health And Scanning** on page 339.

### Testing

It is recommended that you spend considerable time testing your Endpoint Compliance Policies, web pages and VLAN switching before fully implementing Endpoint Compliance. Use your own host machines and go through as many failure scenarios as possible to make sure that hosts are being managed correctly.

## Add/Modify An Endpoint Compliance Policy



**Add Endpoint Compliance Policy**

Name:

User/Host Profile:   

Endpoint Compliance Configuration:   

Note:

OK Cancel

Figure 212: Add Endpoint Compliance Policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Endpoint Compliance**.
3. Click the **Add** button or select an existing Policy and click **Modify**.
4. Click in the **Name** field and enter a name for this Policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Endpoint Compliance Configuration specified in the next step. See **Add/Modify A User Or Host Profile** on page 514.
6. Select an **Endpoint Compliance Configuration** from the drop-down menu. You can use the icons next to the Endpoint Compliance Configuration field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See **Add/Modify An Endpoint Compliance Configuration** on page 539.
7. The **Note** field is optional.
8. Click **OK** to save your Policy.

### Delete An Endpoint Compliance Policy

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Endpoint Compliance**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

### Determining Host Operating System

Network Sentry uses the information configured in the Endpoint Compliance Policy and information received from the connecting host to determine if an agent is required and which agent should be offered to a host. If the operating system or host type is one for which there is no agent, Network Sentry can allow or deny network access based on the settings in the Endpoint Compliance Policy.

The host operating system is detected based on the information contained in the User-Agent string. When a host connects to a Network Sentry web page, its browser sends the user-agent string to the Network Sentry Server or Application Server. This string indicates which browser the host is using, its version number, and details about the host, such as operating system and version. The chart below outlines the criteria Network Sentry uses to determine the host operating system.

Operating system is considered unsupported unless it meets one of the following criteria:

Criteria	OS/Device
UserAgent contains "linux" and "android"	Android
User Agent contains "linux" only	Linux
User Agent contains "mac os x"	Mac OS X
User Agent contains "Macintosh" and "Silk"	Android
User Agent contains "Macintosh" and "Cloud9"	Android
User Agent contains "linux", "android" and "silk"	Kindle
User Agent contains any one of the following: "KFOT", "KFTT", "KFJWI", "KFJWA", "KFSOWI", "KFTHWI", "KFTHWA", "KFAPWI" or "KFAPWA"	Kindle Fire
User Agent contains "mac os x" and "mobile" and "ipod"	iOS for iPod
User Agent contains "mac os x" and "mobile" and "iphone"	iOS for iPhone
User Agent contains "mac os x" and "mobile" and "ipad"	iOS for iPad
User Agent contains "mac os x" and "mobile"	Apple iOS
UserAgent contains "windows nt"	Windows
UserAgent contains "windows phone"	Windows Phone
UserAgent contains "windows nt" and "ARM"	Windows RT
UserAgent contains "freebsd"	Free BSD
UserAgent contains "openbsd"	Open BSD
UserAgent contains "netbsd"	Net BSD

<b>Criteria</b>	<b>OS/Device</b>
UserAgent contains "solaris" or "sunos"	Solaris
UserAgent contains "symbianos" or "symbos"	Symbian
UserAgent contains "webos"	Web OS
UserAgent contains "windows ce"	Windows CE
UserAgent contains "blackberry"	Blackberry OS
UserAgent contains "BB10" and "Mobile"	BlackBerry 10 OS
UserAgent contains "RIM Tablet OS"	RIM Tablet OS
UserAgent contains "CrOS"	Chrome OS

## Endpoint Compliance Configurations

Endpoint Compliance Configurations define agent and scan parameters for hosts and users. Hosts can be required to download an agent and undergo a scan, permitted access with no scan or denied access. The Endpoint Compliance Configuration that is used for a particular host is determined by the pairing of an Endpoint Compliance Configuration and a User/Host Profile within an Endpoint Compliance Policy.

When a host is evaluated, the host, user and connection location are compared to each Endpoint Compliance Policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the User/Host Profile in the policy, that policy is assigned. The Endpoint Compliance Configuration contained within that policy determines the security treatment received by the host.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Scan	Note	Collect Applications	Last Modified By	Last Modified Date	Agent-Windows
Yes	Employee Configuration	<a href="#">AgentNoScan</a>		✓	root	09/02/16 01:56 PM EDT	Latest Dissolvable Agent
Yes	General Configuration	<a href="#">AgentNoScan</a>		✓	root	09/02/16 01:35 PM EDT	Latest Dissolvable Agent
Yes	Guest	<a href="#">PodLocalScan</a>		✓	root	09/02/16 01:56 PM EDT	Latest Dissolvable Agent

Figure 213: End Point Compliance Configurations View

## Endpoint Compliance Configurations Field Definitions

An empty field in a column indicates that the option has not been set.

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Name</b>	User defined name for the Configuration.
<b>Scan</b>	Name of the scan used to evaluate a connecting host.
<b>Note</b>	User specified note field. This field may contain notes regarding the conversion from a previous version of Network Sentry.
<b>Collect Applications</b>	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
<b>Last Modified By</b>	User name of the last user to modify the record.
<b>Last Modified Date</b>	Date and time of the last modification to this configuration.
<b>Agent - OS</b>	An Agent column is displayed for each operating system supported. The column contains the agent that will be used or treatment that applies to hosts with that operating system when the scan is applied. Some operating systems do not have agents and those hosts can only be allowed or denied access to the network. See the Field Definitions in Add/Modify An Endpoint Compliance Configuration on page 539 for information on the agent options for each operating system.
<b>Right Mouse Click Menu Options</b>	
<b>Delete</b>	Deletes the selected Endpoint Compliance Configuration.
<b>In Use</b>	Indicates whether or not the selected configuration is currently being used by any other Network Sentry element. See Endpoint Compliance Configurations In Use on page 544.
<b>Modify</b>	Opens the Modify Endpoint Configuration window for the selected configuration.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Buttons</b>	

Field	Definition
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

## Add/Modify An Endpoint Compliance Configuration

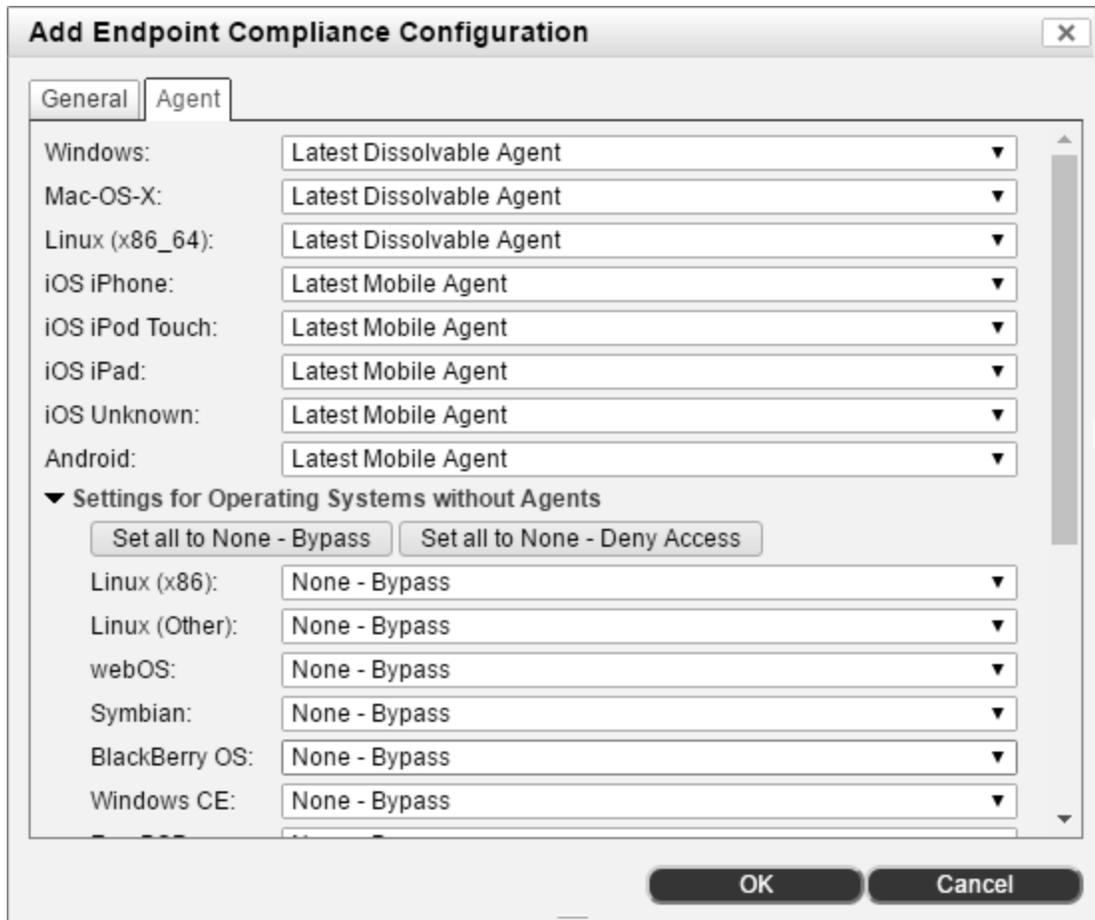
The screenshot shows a dialog box titled "Add Endpoint Compliance Configuration" with a close button (X) in the top right corner. The dialog has two tabs: "General" (selected) and "Agent".

Under the "General" tab, the following fields are visible:

- Name:** A text input field containing "Employee PCs".
- Scan:** A dropdown menu set to "Employee", with a small icon to its right.
- Collect Application Inventory**
- Note:** A large, empty text area for additional information.

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

**Figure 214: Add Endpoint Compliance Configuration - General Tab**



**Figure 215: Add Endpoint Compliance Configuration - Agent Tab**

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance**.
3. From the menu on the left select **Configuration**.
4. On the Endpoint Compliance Configurations window, click the **Add** button or select an existing Configuration and click **Modify**.
5. On the **General** tab click in the **Name** field and enter a name for this Configuration.
6. Select a **Scan** from the drop-down menu. You can use the icons next to the Scan field to add a new scan or modify the scan shown in the drop-down menu. Note that if you modify this scan, it is modified for all features that make use of it. See **Add/Modify A Scan** on page 556.
7. If you would like to add a list of installed applications to the host record, enable the **Collect Application Inventory** check box. This only applies to hosts that are assigned an agent. An application inventory cannot be generated for hosts unless an agent is in use.

8. The **Note** field is optional.
9. Click the **Agent** tab to select it.
10. Select an agent for each operating system. You may choose not to use an agent for a particular operating system, however, scans can only be applied via an agent.
11. No agent exists for some operating systems. In those cases select either **None-Deny Access** or **None-Bypass**. Refer to the table below for information on each field.
12. Click **OK** to save the Endpoint Compliance Configuration.

### Add Endpoint Compliance Configuration - Field Definitions

Field	Definition
<b>General Tab</b>	
<b>Name</b>	User specified name for this configuration.
<b>Scan</b>	Select the scan to be associated with this configuration. Hosts that match the Endpoint Compliance Policy containing this configuration will be scanned with the selected Scan.
<b>Collect Application Inventory</b>	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
<b>Note</b>	User specified note field. This field may contain notes regarding the conversion of policies from a previous version of Network Sentry.
<b>Agent Tab</b>	

Field	Definition
<p>Windows</p> <p>MAC OSX</p> <p>Linux</p>	<p>Allows you to select a separate agent or treatment for each operating system. For example, a host with a Windows operating system may be scanned by the Persistent Agent while a host with a Mac operating system may be scanned with the Dissolvable Agent. See <b>Determining Host Operating System</b> on page 534.</p> <p>The names of all the agent versions and types available on the appliance are included in the list. The .exe is recommended for user-interactive installation. The .msi is recommended for use for a managed install by a non-user-interactive means.</p> <p>Agent options include:</p> <p><b>Persistent Agent:</b> Hosts with this operating system are required to download and install the selected version of the Persistent Agent.</p> <p><b>Dissolvable Agent:</b> Hosts with this operating system are required to download and run the selected version of the Dissolvable Agent.</p> <p><b>Latest Persistent Agent:</b> Hosts with this operating system are required to download and install the highest version of the Persistent Agent available on the Network Sentry Application server. Using the Latest Persistent Agent option prevents you from having to update Policies each time a new Agent is released and loaded onto your server.</p> <p><b>Legacy Persistent Agent:</b> Hosts with this operating system are required to download and install the highest version of the Persistent Agent within the 2.X series. The Version 2.X agents do not require that a certificate be installed on the portal in order to run.</p> <p><b>Latest Dissolvable Agent:</b> Hosts with this operating system are required to download and run the highest version of the Dissolvable Agent available on the Network Sentry Application server. Using the Latest Dissolvable Agent option prevents you from having to update Policies each time a new Agent is released and loaded onto your server.</p> <p><b>Legacy Dissolvable Agent:</b> Hosts with this operating system are required to download and install the highest version of the Dissolvable Agent that is lower than V3.1.0. Dissolvable Agents with version numbers lower than Version 3.1.0 do not require that a certificate be installed on the portal in order to run.</p> <p><b>None-Deny Access:</b> No agent is assigned and hosts are denied access to the network if they have the matching operating system.</p> <p><b>None-Bypass:</b> No agent is assigned but hosts are allowed to access the network.</p> <p><b>Note:</b> If you select None - Bypass, hosts can register only if their IP Address has been determined by Network Sentry. If IP Address information has not been determined Network Sentry cannot determine the Physical Address and will not allow that host on the network. Users see the following message: "Registration Failed - Physical Address not Found" .</p>

Field	Definition
<p>iOS...</p> <p>Android</p>	<p>The drop-downs for iOS and Android operating systems will contain None-Deny Access, None-Bypass and Latest Mobile Agent.</p> <p><b>None-Deny Access:</b> No agent is assigned and hosts are denied access to the network if they have the matching operating system.</p> <p><b>None-Bypass:</b> No agent is assigned but hosts are allowed to access the network if they have the matching operating system.</p> <p><b>Bradford Mobile Agent:</b> Mobile devices detected running the iOS or Android operating system are required to download and install the Mobile Agent. These devices are automatically directed to the Mobile Agent Download page in the captive portal where the host is prompted to download the Mobile Agent from Apple App Store (iOS) or Google Play (Android).</p> <p><b>Latest Mobile Agent:</b> Hosts with this operating system are required to download and install the highest version of the Mobile Agent available. For iOS operating systems the Mobile Agent is downloaded from the Apple Apps Store. For Android operating system the Mobile Agent is downloaded from Google Play.</p>
<p><b>Settings For Operating Systems Without Agents</b></p>	<p>This section provides a list of additional operating systems and allows you to select treatment for each one. For example, iPod devices could be set to None-Bypass indicating that no agent is necessary and allowing that device to connect to the network. Options for additional platforms include:</p> <p><b>None-Deny Access:</b> No agent is assigned and hosts are denied access to the network if they have the matching operating system.</p> <p><b>None-Bypass:</b> No agent is assigned but hosts are allowed to access the network if they have the matching operating system.</p> <p>Use the <b>Set all to None-Bypass</b> or <b>Set all to None-Deny Access</b> buttons to modify settings for all additional platforms at once.</p> <p>The last platform labeled Other is used as a catch-all for devices with new or unsupported operating systems. Any platform not listed in the Policy, is treated as specified by the setting associated with Other.</p>

### Endpoint Compliance Configurations In Use

To find the list of Network Sentry features that reference a specific Endpoint Compliance Configuration, select the Configuration from the Endpoint Compliance Configurations View and click the **In Use** button. A message is displayed indicating whether or not the Configuration is associated with any other features. If the Configuration is referenced elsewhere, a list of each feature that references the Configuration is displayed.



**Figure 216: Endpoint Compliance Configuration In Use**

### Delete An Endpoint Compliance Configuration

If a configuration is in use by another feature in Network Sentry, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Endpoint Compliance**.
3. Click on the **+** sign next to **Endpoint Compliance** to open it.
4. Select **Configuration** from the menu on the left.
5. Select the Endpoint Compliance Configuration to be removed.
6. Click **Delete**.
7. Click **OK** to confirm that you wish to remove the configuration.

## Scans

The Scans View allows you to configure network scans or sets of rules that are used to scan hosts for compliance. Scans are included in Endpoint Compliance Configurations that are paired with User/Host Profiles, which form Endpoint Compliance Policies. When a host is evaluated and requires an Endpoint Compliance Policy, Network Sentry goes through the list of policies and compares user and host information to the associated User/Host Profile. When a match is found, the Endpoint Compliance Configuration inside the policy is applied to the host. That configuration contains the scan and agent information used to evaluate the host.

Scans typically consist of lists of permitted operating systems and required anti-virus and anti-spyware software. In addition, Custom Scans can be created for more detailed scanning such as, searching the registry for particular entries, searching the hard drive for specific files, or verifying that hotfixes have been installed. Individual scans can be scheduled to run at regular intervals if your organization requires frequent rescans.

**Note:** For a list of supported operating systems, anti-virus software and anti-spyware software, use the Interoperability Search in the Resource Center on our web site.

The results of a scan are stored on the Host Health tab in the Host Properties view. Refer to **Host Health And Scanning** on page 339 for additional information.

### Scanning With Agent 2.X

If your hosts are scanned by an Agent prior to Agent version 3.0, the agent tests every single item in the scan and presents extensive scan results. In some cases those items may not be relevant. For example, if Windows XP is required and that operating system is not installed, the agent will still test to see if the updates have been installed. In the scan results, the host fails for not having the operating system AND for not having the updates.

The opposite is also true. In some cases if an item is unchecked and therefore is not required, the host passes for that item and can pass the scan. See the example below:

OS/AV	Anti-Virus 1	Anti-Virus 2	Anti-Virus 3
Operating System 1	Unchecked	Unchecked	Checked
Operating System 2	Unchecked	Checked	Checked
Operating System 3	Checked	Checked	Checked

If the scan is set to Any indicating that any combination is acceptable, the goal of these scan settings would be as follows:

- Operating System 1 requires Anti-Virus 3
- Operating System 2 requires either Anti-Virus 1 or Anti-Virus 2.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3.

However, this is not supported because the agent tests for each combination. The actual process is as follows:

- Operating System 1 requires either no Anti-Virus 1 or no Anti-Virus 2 or Anti-Virus 3. Host passes if it does not have Anti-Virus 1 or 2 because those are unchecked, and the agent tests for that combination. It also passes if it has Anti-Virus 3.
- Operating System 2 requires either no Anti-Virus 1 or Anti-Virus 2 or Anti-Virus 3. Host passes if it does not have Anti-Virus 1 because that one is unchecked, and the agent tests for that combination. It also passes if it has Anti-Virus 2 or 3.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3. Host passes if it has any one of the three Anti-Viruses installed.

### **Scanning With Agent 3.X And Higher**

If your hosts are scanned using Agent version 3.0 or higher, the agent first checks to see if a required item is installed and then proceeds to scan for additional details about that item. For example, if the host is required to run Windows XP and that operating system is not installed, the agent does not check to see if the updates have been installed. Scan results, therefore, are reduced because needless scans are minimized. In the scan results, the host fails only for not having the operating system.

Using the example from the table shown above, Agent 3.X ignores items that are not checked or selected. With this agent, you would achieve the following results.

- Operating System 1 requires Anti-Virus 3. The agent does not test to see that Anti-Virus 1 and 2 are not installed, therefore, the host cannot pass the scan unless it has Operating System 1 with Anti-Virus 3.
- Operating System 2 requires either Anti-Virus 1 or Anti-Virus 2. The agent does not test for Anti-Virus 1.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3.

## Scans View Navigation

Scans can be accessed from **Policy > Policy Configuration > Endpoint Compliance** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > Endpoint Compliance**. See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Scans - Total: 5								
Global	Name	Remediation	Scan On Connect	Renew IP	Jailbreak Detection	Root Detection	Scan Failure Link Label	Agent Order of Operations
Yes	AgentNoScan	On Failure	⊘	⊘	⊘	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Yes	MyEndpointComplianceScanWithv	On Failure	⊘	⊘	⊘	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Yes	OS-Anti-Virus-Check	On Failure	⊘	⊘	⊘	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Yes	OS-Check	On Failure	⊘	⊘	⊘	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Yes	Pod2LocalScan	On Failure	⊘	✓	⊘	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate

Import | Export to:

Options ▾ Add Modify Delete In Use Custom Scans

Figure 217: Scans View

## Scans View Field Definitions

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Scan Name</b>	Each scan must have a unique name.
<b>Remediation</b>	<p>Indicates when the host is moved to Remediation. Options include:</p> <p><b>On Failure</b> — Host is moved to remediation immediately after failing a scan.</p> <p><b>Delayed</b> — Host is moved to remediation after a user specified delay if the reason for the scan failure has not been addressed.</p> <p><b>Audit Only</b> — Host is scanned and a failure report is generated, but the host is never moved to remediation.</p>

Field	Definition
<b>Scan On Connect</b>	<p>Indicates whether this option is enabled or disabled. Scan On Connect forces a rescan every time the host assigned this scan connects to the network. See <b>Scan On Connect</b> on page 550.</p> <p>This option only affects hosts running the Persistent Agent.</p>
<b>Renew IP (Supported by Dissolvable Agent Only)</b>	<p>Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP Address of the host after it has completed its scan. The Renew IP option is only supported on the following systems that use the Dissolvable agent:</p> <ul style="list-style-type: none"> <li>- Windows: All Dissolvable Agent Versions</li> <li>- Mac-OS-X: Dissolvable Agent Versions 3.3.0.56+</li> </ul>
<b>Scan Failure Link Label</b>	<p>Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.</p>
<b>Agent Order Of Operations Remediation = On Failure</b>	<p>This set of options is available only when <b>Remediation</b> is set to <b>On Failure</b>.</p> <p>Determines the order in which the agent performs its tasks. Choose one of the following:</p> <p><b>Scan Before Registering:</b> The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following:</p> <ol style="list-style-type: none"> <li>1. <b>Do not Register, Remediate:</b> Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting.</li> <li>2. <b>Register and mark At Risk:</b> The host is registered immediately after the scan and then moved to Quarantine.</li> </ol> <p><b>Note:</b> Persistent Agent ALWAYS registers and marks at risk.</p> <p><b>Register, then Scan (if the scan fails, Remediate):</b> The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned.</p>
<b>Agent Order Of Operations Remediation = Delay or Audit Only</b>	<p>The option below is available only when <b>Remediation</b> is set to <b>Delay</b> or <b>Audit Only</b>.</p> <p><b>If scan fails - Register or Remediate:</b> If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user.</p> <p>If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan.</p> <p>If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.</p>

Field	Definition
<b>Patch URL</b>	URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page.
<b>Jailbreak Detection</b>	Indicates whether this option is enabled or disabled. If enabled, jailbroken mobile devices are not allowed to register.  The Mobile Agent for iOS devices determines whether or not a device has been jailbroken. iOS jailbreaking is the process of removing limitations imposed by Apple on devices running the iOS operating system through the use of hardware/software exploits.
<b>Root Detection</b>	Indicates whether this option is enabled or disabled. If enabled, rooted mobile devices are not allowed to register.  Mobile Agent for Android devices determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.
<b>Last Modified By</b>	User name of the last user to modify the scan.
<b>Last Modified Date</b>	Date and time of the last modification to this scan.
<b>Right Mouse Click Menu - Options Button Menu</b>	
<b>Copy</b>	Copy the selected Scan to create a new record.
<b>Delete</b>	Deletes the selected Scan. Scans that are currently in use cannot be deleted.
<b>In Use</b>	Indicates whether or not the selected Scan is currently being used by any other Network Sentry element. See <b>Scans In Use</b> on page 569.
<b>Modify</b>	Opens the Modify Scan window for the selected Scan.
<b>Schedule</b>	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See <b>Schedule A Scan</b> on page 570.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item.  For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446  <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Buttons</b>	
<b>Custom Scans</b>	Opens the Custom Scan Configuration window which allows you to add, remove or modify Custom Scans. Custom scan can be added to policies for more detailed host scans. See <b>Custom Scans Overview</b> on page 578.
<b>Schedule</b>	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See <b>Schedule A Scan</b> on page 570.

### Scan On Connect

Network Sentry allows you to configure Scans that scan hosts each time they connect to the network. The Scan on Connect option is enabled on individual Scans. You may have hosts that are scanned each time they connect and hosts with a different Scan that are scanned periodically.

**Note:** Scan on Connect can only be used on registered hosts that have the Persistent Agent installed. If you are using the Dissolvable Agent, this option is ignored.

When a host connects to the network, Network Sentry determines which Endpoint Compliance Policy should be applied to this host based on the criteria in the associated User/Host Profile. If a registered host has the Persistent Agent installed and Scan on Connect is enabled for the Scan that applies to this host, then the host is scanned. When the host disconnects from the network, the Persistent Agent modifies that host's Scan on Connect status to indicate that the host should be scanned again the next time it connects. If the host has more than one interface, such as wired and wireless, the host is scanned regardless of which one is used.

**Note:** A rescan happens any time Network Sentry detects that the host has come online and the agent has communicated with the server, such as when a switch sends a linkdown/linkup trap.

To enable Scan on Connect you must go to the Scans window, select the appropriate Scan and enable the option. See **Add/Modify A Scan** on page 556 for step-by-step instructions on creating a Scan and enabling Scan on Connect.

## Scan Hosts Without Enforcing Remediation

Hosts who are in Remediation are denied network access until they comply with the requirements of the Scan used to evaluate them. Network Sentry can scan hosts on the network without placing them in Remediation. This allows the administrator to determine host state or test new Endpoint Compliance Policies without interrupting network users as they work. To scan hosts without enforcing remediation you can disable the Quarantine switching option in Network Sentry Properties. Disabling Quarantine VLAN switching affects all hosts. However, you may need to scan selected hosts with no repercussions.

Two options have been provided to allow you to scan selected hosts without forcing "at risk" hosts into Remediation, Audit Only and Forced Remediation Exceptions group. You can use either one or both of these options. They work independently of each other. Audit Only controls remediation based on the scan applied. The Forced Remediation Exceptions group controls remediation based on group membership regardless of the scan used to evaluate the hosts.

### **Audit Only**

When the Audit Only option on a scan is enabled, hosts are scanned and the results of the scan are stored. Hosts that fail the scan are never marked "at risk" and therefore are not forced into Remediation or Quarantine. Administrators can then review all of the scan results and address issues of non-compliance without blocking users from the network.

Audit Only affects only those hosts evaluated by the scan in which Audit Only is enabled. If you have other scans with Audit Only disabled, hosts evaluated by those scans who fail are forced into Remediation. Using this option you can decide to force some groups of hosts into remediation while leaving others on the network. For example, you could have a scan for your executive staff that has Audit Only enabled and a different scan for administrative staff that has Audit Only disabled. Executives that fail a scan would continue to work without disruption, while administrative staff that fail a scan would be forced to remediate.

To enable the Audit Only option:

1. Select **Policy > Policy Configuration**.
2. In the menu on the left, click the + symbol next to **Endpoint Compliance** to open it.
3. Click **Scans**.
4. Select an existing Scan to modify or create a new one.
5. On the **Add or Modify Scan** window go to the Scan Settings section and enable **Audit Only** under the Remediation drop-down.

See **Add/Modify A Scan** on page 556 for additional information.

### **Forced Remediation Exceptions Group**

When hosts are placed in this group, they are evaluated by the scan that corresponds to them. See **Policy Assignment** on page 507. Results of the scan are stored and hosts who fail are marked "at risk". Hosts in this group are never forced into remediation no matter which scan they fail. To prevent selected hosts from being forced to remediate, add them to this group.

The Forced Remediation Exceptions group is a system group that has already been created. System groups cannot be removed only modified. See **System Groups** on page 700 and **Modify A Group** on page 695.

## Delayed Remediation For Scanned Hosts

The Delayed Remediation scan feature allows you to scan hosts on your network, notify the user if the host has failed the scan and delay placing the host in the remediation VLAN for a specified number of days. This process gives the host's owner time to rectify the issues that triggered the failed scan and rescan without being removed from the network. If the user does not take care of the issues that caused the failure and successfully rescan the host by the time the specified delay has elapsed, the host is placed in remediation and cannot access the network.

### Implementation

To implement Delayed Remediation, first implement the settings for Endpoint Compliance. See **Endpoint Compliance Implementation** on page 529.

- This feature works with any agent (Passive, Persistent or Dissolvable\*). If you choose to use this feature with the Dissolvable Agent, note the following:
  - Using the Dissolvable Agent, Delayed Remediation can only be implemented during the registration process where the host is provided a link to the Dissolvable Agent. If the host fails, it is marked as Pending - At Risk, but can register and move to the production VLAN. The Dissolvable Agent remains on the host until all issues have been resolved and the host has been rescanned.
  - If you set up scheduled rescans for hosts, using Delayed Remediation does not prevent the scheduled rescan from marking the host "At Risk" at the scheduled interval. Therefore, it is recommended that you use Proactive Scanning with the Dissolvable Agent instead of Delayed Remediation. Proactive Scanning allows a user to rescan a host prior to a scheduled required rescan and if the host fails it is not marked "at risk" until the date of the scheduled rescan. See **Add Proactive Scanning To A Scheduled Scan** on page 573 and **Schedule A Scan—Proactive Scanning** on page 573.

To rescan the user must open a browser and navigate to the following:

```
https://<Server or Application Server>/remediation
```

The Network Sentry Server or Application Server in the URL can be either the IP Address or Name of the server that is running the captive portal.

- Modify existing scans or create new ones and set the Delayed Remediation option for the number of days the host should be allowed to continue on the network after failing a scan. The default setting for Delayed Remediation is 0 days or no delay. See **Add/Modify A Scan** on page 556.
- If a host has already failed a scan with a Delayed Remediation setting and the delay setting is changed on the Scan, it does not change the delay for the associated host. For example, if Host A is scanned, fails Scan A and is assigned a delay of 2 days, changing Scan A to a delay of 5 days does not alter the delay for Host A. It remains 2 days.

- Configure events and alarms to notify you when a host is affected by the Delayed Remediation setting. See **Enable And Disable Events** on page 454. Events include:
  - **Host Pending At Risk** — Indicates that a host has failed a scan that has a Delayed Remediation set and has been set to Pending At Risk.
  - **Host Security Test - Delayed Failure** — A host has failed a scan and the scan has been set to Failure Pending in the Host Properties Health Tab.

### **Process**

Below is a sample of the process Network Sentry goes through when Delayed Remediation is enabled.

1. A host connects to the network and is scanned by an agent with Scan A that has a 3 day delay configured.
2. The host fails the scan for Anti-Virus.
3. A failure page indicating the reason for the failure is displayed on the host.
4. A Delayed Remediation record is created for this host and Scan A, which was used to scan the host.
5. The host's status is set to Pending At Risk.
6. On the Host Properties - Health Tab the scan for Scan A is set to Failure Pending.
7. The host remains on the production network and is not sent to the remediation VLAN.
8. After one day the host connects in the Library and is scanned by an agent with Scan B that has a 5 day delay configured.
9. The host fails the scan for Anti-Spyware.
10. A failure page indicating the reason for the failure is displayed on the host.
11. A second Delayed Remediation record is created for this host and Scan B.
12. The host status remains Pending At Risk.
13. On the Host Properties - Health Tab the scan for Scan B is set to Failure Pending.
14. The user corrects the Anti-Virus issue and rescans with Scan A.
15. The Delayed Remediation record for this host and Scan A is removed.
16. On the Host Properties - Health Tab the scan for Scan A is set to Success.
17. The host's status remains Pending At Risk because the user has not corrected the Anti-Spyware issue and rescanned for Scan B.
18. Five days elapse and the user still has not corrected the Anti-Spyware issue and rescanned for Scan B.

19. The host is marked At Risk but it is not moved to the Remediation VLAN because Scan B is not the scan that currently applies to the host. Scan B will apply to the host if the host ever reconnects in the Library.
20. On the Host Properties - Health Tab the scan for Scan B is set to Failure.
21. The Delayed Remediation record for this host and Scan B is removed.
22. The host continues on the production network.
23. If the host ever reconnects in the Library, the host will be placed in Remediation. The User will have to resolve the Anti-Spyware issue and rescan the host for Scan B.

---

**Note:** Each host failure and delay record is treated individually. Passing one scan and associated delay, does not remove failures for other scans and corresponding delays. However, if a failed scan does not apply to the host, the host will not be sent to Remediation. Refer to **Host Health And Scanning** on page 339.

---

## Add/Modify A Scan

Use the Add or Modify Scan dialog to configure scan settings. Field definitions are divided into two tables. The first table details the fields on the General tab and the second details the Categories available under the remaining tabs.

Figure 218: Add Scan - General Tab

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. On the Scans View, click **Add** to add a new Scan or select an existing Scan and click **Modify**.
5. Enter data in the fields as needed. See the **Scan Configuration Field Definitions** table below for information on each field.

6. For each **operating system** tab, there is a drop-down menu of categories that can be set, such as, anti-virus or anti-spyware settings. Instructions for configuring each category are contained in the Scan Configuration Field Definitions - Categories table.
7. The **Summary** tab provides an overview of the entire scan configuration for your review.
8. Click **OK** to save the Scan.

### Scan Configuration Field Definitions - General Tab

Field	Definition
<b>Scan Name</b>	Each scan must have a unique name.
<b>Scan Settings</b>	
<b>Scan On Connect (Persistent Agent Only)</b>	<p>Forces a rescan every time the host assigned this scan connects to the network.</p> <p>This option only affects hosts running the Persistent Agent.</p> <p>See <b>Scan On Connect</b> on page 550.</p>
<b>Renew IP (Supported Dissolvable Agent Only)</b>	<p>Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP address of the host after it has completed its scan. The Renew IP option is only supported on the following systems that use the Dissolvable agent:</p> <ul style="list-style-type: none"> <li>- Windows: All Dissolvable Agent Versions</li> <li>- Mac-OS-X: Dissolvable Agent Versions 3.3.0.56+</li> </ul>
<b>Jailbreak Detection (iOS Agent Only)</b>	<p>The Mobile Agent for iOS devices determines whether or not a device has been jailbroken. iOS jailbreaking is the process of removing limitations imposed by Apple on devices running the iOS operating system through the use of hardware/software exploits.</p> <p>If enabled, jailbroken mobile devices are not allowed to register.</p> <p>If disabled, devices suspected of being jailbroken are allowed to register and (Jailbroken) is appended to the operating system information displayed in the Host View.</p> <p>If the agent detects that device has been altered, a <b>Potential Jailbroken Device</b> event is generated.</p>

Field	Definition
<p><b>Root Detection (Android Agent Only)</b></p>	<p>The Mobile Agent for Android devices determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.</p> <p>If enabled, rooted mobile devices are not allowed to register.</p> <p>If disabled, devices suspected of being rooted are allowed to register and (Rooted) is appended to the operating system information displayed in the Host View.</p> <p>If the agent detects that device has been altered, a <b>Potential Rooted Device</b> event is generated.</p>
<p><b>Remediation - On Failure</b></p>	<p>If enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, the user must resolve all of the issues for which the host failed and rescan before being allowed on the network.</p> <p><b>Agent Order Of Operations:</b></p> <p>This set of options is available only when Remediation is set to On Failure.</p> <p>Determines the order in which the agent performs its tasks. Choose one of the following:</p> <p><b>Scan Before Registering:</b> The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following:</p> <ol style="list-style-type: none"> <li>1. <b>Do not Register, Remediate:</b> Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting.</li> <li>2. <b>Register and mark At Risk:</b> The host is registered immediately after the scan and then moved to Quarantine.</li> </ol> <p><b>Note:</b> Persistent Agent ALWAYS registers and marks at risk.</p> <p><b>Register, then Scan (if the scan fails, Remediate):</b> The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned.</p>

Field	Definition
<b>Remediation - Delayed</b>	<p>Hosts who fail this scan are set to Pending at Risk for the number of days indicated in the Remediation Delay field. Hosts set to Pending at Risk are not placed in remediation until the number of days indicated has elapsed. The user is notified of the failure immediately.</p> <p>Changes to this setting do not affect hosts that are already marked as Pending At Risk. If a host was set to a delay of 3 days and you change the Remediation Delay field to 5 days, the host remains at a delay of 3 days. Hosts scanned after the change will use the 5 day setting.</p> <p><b>Agent Order Of Operations:</b></p> <p><b>If scan fails - Register or Remediate:</b> If the host fails a scan, the Persistent Agent displays a message stating that the host is at risk. Click the message to display information about the scan. The host is automatically registered.</p> <p>The Dissolvable Agent displays the results of the scan. You can choose to rescan or register.</p> <p>When the host is registered, the host is placed in production. The user can correct all of the issues and re-run the Agent.</p>
<b>Remediation - Audit Only</b>	<p>If enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, it is not marked "at risk". Therefore, it is not forced into Remediation and can continue using the network. The administrator can review the scan results and take corrective action without disrupting users on the network.</p> <p><b>Agent Order Of Operations:</b></p> <p><b>If scan fails - Register or Remediate:</b> If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user.</p> <p>If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan.</p> <p>If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.</p>
<b>Portal Page Settings</b>	
<b>Label For Scan Failure Link</b>	<p>Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.</p>
<b>Instructions For Scan Failure</b>	<p>If a host has failed a scan, the user must remedy the issue and rescan. This field allows you to provide the user with a brief set of instructions.</p>

Field	Definition
<b>Patch URL For Dissolvable Agent Re-Scan</b>	<p>URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page.</p> <p>Set this to /remediation</p> <p>To rescan the user must open a browser and navigate to the following:</p> <p><code>https://&lt;Server or Application Server&gt;/remediation</code></p> <p>The Network Sentry Server or Application Server in the URL can be either the IP Address or Name of the server that is running the captive portal.</p>
<b>In use by/Not currently in use</b>	Indicates whether the scan is being used in User/Host Profile(s). When the scan is in use, click the link to view the User/Host Profile(s).

**Scan Configuration Field Definitions - Categories**

For each operating system there is a Category drop-down that allows you to configure specific settings for categories such as anti-spyware or anti-virus. The table below outlines these settings.

**Note:** Default parameter values for individual anti-virus, anti-spyware and operating systems packages are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

**Note:** Removing a check mark from a selected option causes any underlying changes to be lost. For example, if you modified settings for AVG antivirus and then unselected it, those changes are lost.

Field	Definition
<b>Anti-Spyware</b>	
<b>Validation Options</b>	<p><b>Any</b> — Any one of the selected items must be present on the host machine to pass the scan.</p> <p><b>All</b> — All of the selected items must be present on the host machine to pass the policy.</p>

Field	Definition
Anti-Spyware List	<p>New anti-spyware software is continuously being created and sold. As new anti-spyware software becomes available, parameters for that software are made available as quickly as possible in Network Sentry. The default values for anti-spyware are entered automatically by the scheduled Auto-Def Updates feature and normally do not require any changes. You should not need to modify these.</p>
	<p><b>Note:</b> Anti-Spyware settings apply only to Windows operating systems.</p>
	<p>Select each Anti-Spyware package that should be included in the scan. To set custom parameters for any of the selected Anti-Spyware programs, click the name of the program. A parameters window opens and displays all of the advanced options that can be set. See Anti-Spyware Parameters on page 746 for details on individual settings.</p>
Preferred	<p>Select the <b>Preferred</b> Anti-Spyware from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.</p>
<b>Anti-Virus</b>	
Validation Options	<p><b>Any</b> — Any one of the selected items must be present on the host machine to pass the scan.</p> <p><b>All</b> — All of the selected items must be present on the host machine to pass the scan.</p>
Anti-Virus List	<p>New anti-virus software is continually being created. As new anti-virus software becomes available, parameters for that software are made available as quickly as possible in Network Sentry. The default values for each anti-virus program are entered automatically by the scheduled Auto-Def Updates feature. You should not need to modify these.</p> <p>Select one or more types of <b>Anti-virus software</b> to check for on the host machine. To set additional parameters for any of the selected Anti-Virus programs, click the name of a program. A parameters window opens and displays all of the advanced options that can be set. Enter the custom parameter values for the selected program and click <b>OK</b>. See Anti-Virus Parameters - Windows on page 751 or Anti-Virus Parameters - Mac OS X on page 756 for details on each parameter.</p>
Preferred	<p>Select the <b>Preferred</b> Anti-Virus from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.</p>
<b>Custom Scans</b>	

Field	Definition
<b>Custom Scans List</b>	<p>Custom scans are user created scans that have been configured to scan hosts for things such as specific files, registry entries or programs. Custom scans must be created and saved before they can be included as part of a Security Policy. See <b>Custom Scans Overview</b> on page 578.</p> <p>When a Custom scan is added to a regular scan the custom scan is used across the board no matter what other options have been selected for the policy. Any host that is scanned with the regular scan is also scanned based on the Custom Scan. See <b>Custom Scans Options - Scan Level</b> on page 562.</p> <p>Custom scans can be added within a category, such as Anti-Virus or Anti-Spyware. For example, any host that has AVG Anti-Virus will be scanned using an associated custom scan. In this case, the Custom Scan is being used to enhance the scan for AVG Anti-Virus and it is not run on every host. See <b>Custom Scans Options Within A Category Level</b> on page 564.</p>
<b>Operating Systems</b>	
<b>Selection Options</b>	<p><b>All</b> — Marks every operating system with a check mark.</p> <p><b>None</b> — Removes the check mark from every operating system check box.</p>
<b>Operating Systems List</b>	<p>Scans for required or prohibited operating systems on host machines. Operating systems that are selected are required. See <b>Operating System Parameters - Windows</b> on page 758</p> <p><b>Important:</b> The Windows-2003-Server-x64 product has been removed. Use the Windows 2003 Server and Windows XP x64 products.</p>
<b>Preferred</b>	<p>Select the <b>Preferred</b> Operating System from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.</p>
<b>Monitors</b>	
<b>Scan List</b>	<p>Allows you to run a custom scan with greater frequency than the regular scan with which it is associated. For example, the original scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire scan policy every half an hour you can choose to run only a custom scan. See <b>Monitor Custom Scans</b> on page 565.</p> <p>Select a custom scan and enter the frequency with which it should run.</p> <p><b>WARNING:</b> Performance degradation may occur if you select an interval less than every five (5) minutes. It is recommended that monitoring intervals be set to five (5) minutes or more.</p>

### **Custom Scans Options - Scan Level**

Custom scans can be enabled for a regular scan. When a host is checked for compliance with the regular scan, the custom scan is also checked. Before adding a Custom Scan to a security scan you must create the custom scan. See **Create Custom Scans For Windows**

on page 579, **Create Custom Scans For Mac-OS-X** on page 594, or **Create Custom Scans for Linux** on page 600.

To enable a Custom scan for a security scan:

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the scan that will use this custom scan.
5. Click either the **Windows**, the **Mac OS X**, or the **Linux** tab.
6. Select **Custom** from the drop-down menu at the top of the window.
7. Select the check box next to the Custom Scan for the security scan.
8. Click **OK** to save your changes.

**Custom Scans Options Within A Category Level**

Custom scans can be enabled for various categories within a security scan such as the anti-virus, anti-spyware or operating system requirements. When a host is checked for compliance with the security scan and one of the products within a category has a custom scan enabled, the custom scan is also used for hosts with the selected product. For example, if the security scan checks for the existence of AVG Anti-Virus and a Custom Scan has been associated with AVG, then hosts with AVG will also be scanned using the Custom Scan.

Before adding a Custom Scan to a security scan you must create the custom scan. See **Create Custom Scans For Windows** on page 579 or **Create Custom Scans For Mac-OS-X** on page 594.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the security scan that will use this custom scan.
5. Click either the **Windows**, the **Mac OS X**, or the **Linux** tab.
6. Click the **Category** drop-down on the Modify Scan view and select: anti-virus, anti-spyware, operating system, etc.
7. Click the specific item within the sub-category (i.e. product name).
8. Click the **Custom Scans** tab and click next to the **Custom Scan** name to be applied to this sub-category.
9. Click **OK** to save the selected custom scan.
10. Click **OK** to save changes to the security scan.

## Monitor Custom Scans

This feature allows you to run a custom scan with greater frequency than the security scan with which it is associated. For example, the original security scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire security scan every half an hour you can choose to run only a custom scan.

Use the monitor feature to periodically test for a specific status on host machines running the Persistent Agent. Monitors use Custom Scans to check the host machine. A monitor you configure as part of a scan can be the same or different for each scan. Configure monitors for each platform (Windows, Mac OS X, or Linux) separately.

Host machines associated with the security scan are checked at the interval period set in the monitor. The agent on the host sends a message to the server after each time period has passed, indicating whether the host has passed or failed the scan. If several monitors are set to 1 minute intervals, traffic to the server is increased. For example, if there are 10 monitors running every minute on 5,000 hosts, the server might see up to 50,000 messages a minute.

**Important:** Even though monitors use custom scans which can be set to warning, monitors will not send warnings to hosts. Monitors can only pass or fail. Hosts that fail are marked at risk and placed in remediation.

Enabling a monitor for a custom scan automatically enables the custom scan. However, disabling a monitor will not disable the associated custom scan.

For example, you have created Custom Scan A but have not selected it within any security scan. When you select Custom Scan A in the Monitor list select a time period, the custom scan is enabled.

**Important:** Monitors ignore the severity flag of a custom scan.

### Monitor Example

All users have been notified that peer-to-peer software is not tolerated on the network. A web page explaining this policy is located in the remediation area where the host is moved after failing the scan.

#### Actions taken:

- A custom scan for a prohibited process has been created to check for LimeWire, a peer-to-peer software program, running on the host machine. The custom scan includes the URL of the web page where the host browser will be directed if the host fails the custom scan.
- The monitor is set to 10 minutes for the custom scan.

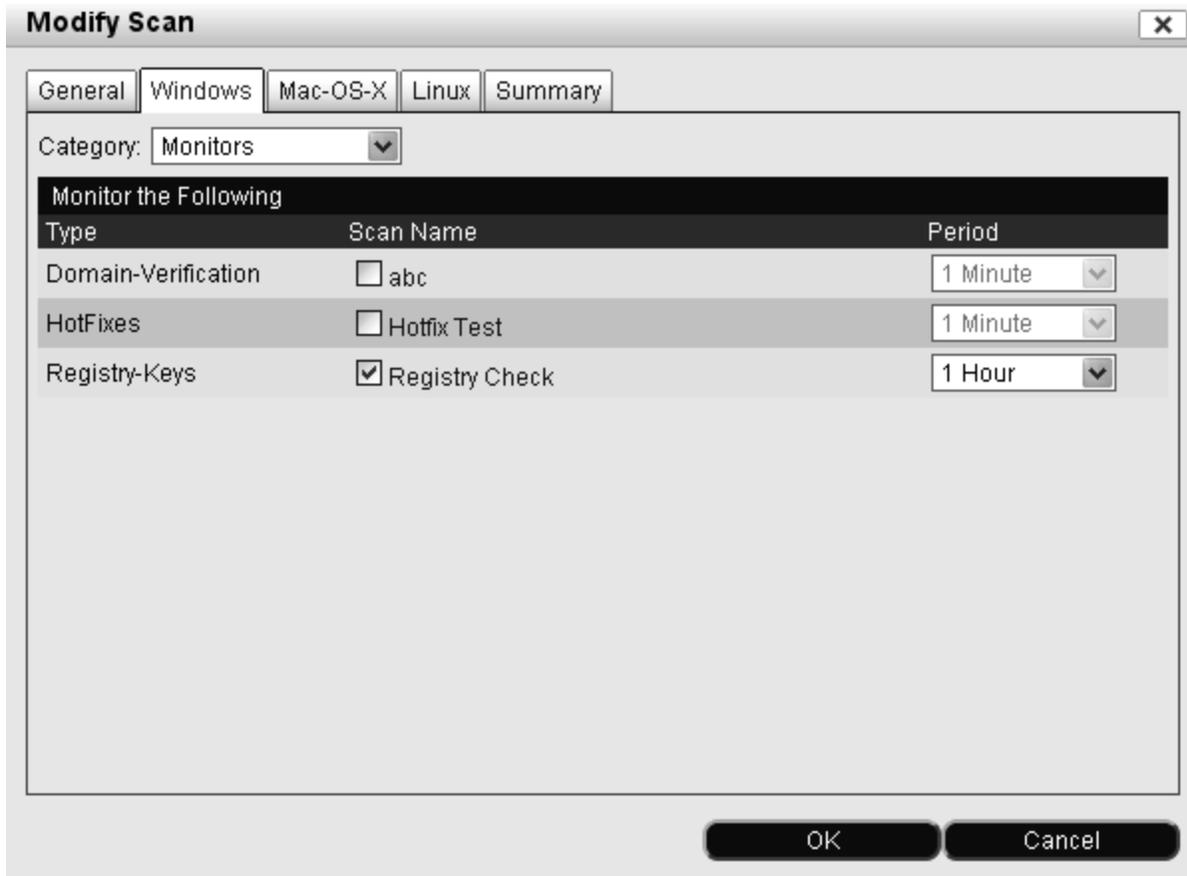
### Results:

- Every 10 minutes the agent checks the host machine to determine if LimeWire is running.
  - If LimeWire is not running, the agent sends a message to the server indicating that the host has passed the security scan.
  - If LimeWire is running, the agent sends a message to the server indicating that the host has failed the scan. The host machine is immediately moved to the quarantine VLAN and the browser redirected to the web page specified in the Custom Scan.

### Set Up A Custom Scan Monitor

Before adding a Custom Scan to a security scan you must create the custom scan. See **Create Custom Scans For Windows** on page 579 or **Create Custom Scans For Mac-OS-X** on page 594.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Click the security scan name and click **Modify**. If the security scan does not exist, it needs to be added. See **Scans** on page 545 for details on adding scans.
5. Click either the **Windows**, the **Mac OS X**, or the **Linux** tab.
6. Click the **Category** drop-down and select **Monitors**.



**Figure 219: Configure Monitors**

7. Select the check box for the type of Custom Scan.
8. Select the time period that the agent waits before checking the host for compliance with the custom scan settings. The available intervals are every 15 seconds up to and including 1 minute, and every 5 minutes up to and including 1 hour.

**WARNING:** Performance degradation may occur if you select a very short interval or if you select a large number of monitors. It is recommended that monitoring intervals be set to five (5) minutes or more.

9. Click **OK**.

### Reset Default Anti-Virus Or Anti-Spyware Values

Anti-Virus and Anti-Spyware parameters contained in Network Sentry are updated weekly using the Auto-Def updates feature. This ensures that new version numbers and bug definition files for Anti-Virus and Anti-Spyware software that you require are taken into account when users' computers are scanned.

If you have manually edited any parameters associated with a particular Anti-Virus or Anti-Spyware software the Auto-Def update does not override your settings for that software. To reset Anti-Virus Or Anti-Spyware to the default values and allow the Auto-Def updates feature to update parameters do the following:

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Select a Scan and click **Modify**.
5. Click either **Windows** or **Mac**, whichever applies.
6. Select **Anti-Virus** or **Anti-Spyware** from the Categories drop-down.
7. Uncheck the checkbox for the software for which you have modified settings.
8. Click **OK**.
9. Open the same Scan again and navigate back to the software you unchecked.
10. Check the checkbox for the previously modified settings and click **OK**.
11. Repeat this process for each Anti-Virus or Anti-Spyware software that needs to be reset to defaults.
12. The next time the Auto-Def updates feature retrieves and installs an update, the Anti-Virus or Anti-Spyware software that you reset will accept the updated parameters.

## Delete A Scan

If a Scan is in use by another feature in Network Sentry, it cannot be deleted. A dialog displays with a list of the features in which the scan is used. Remove the association between the scan and other features before deleting the scan.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the Scans option to select it.
4. Click the scan to be removed.
5. Click **Delete**.
6. Click **OK** to remove the scan.

**Note:** Deleting a scan automatically removes scheduled tasks for that scan.

## Scans In Use

To find the list of Network Sentry features that reference a specific Scan, select the Scan from the Scans View and click the **In Use** button. A message is displayed indicating whether or not the Scan is associated with any other features. If the Scan is referenced elsewhere, a list of each feature that references the Scan is displayed.

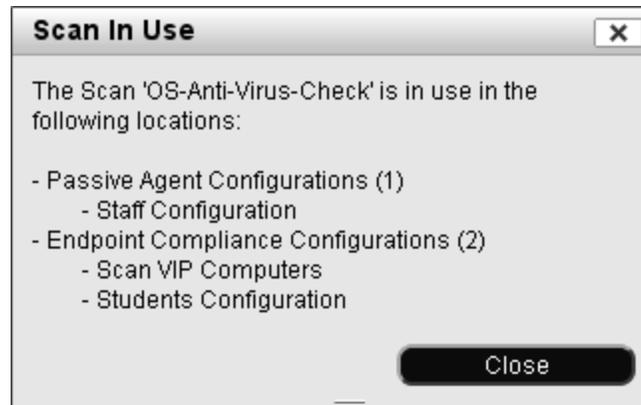


Figure 220: Scan In Use

## Schedule A Scan

When hosts that use the Persistent Agent or the Dissolvable Agent connect to the network, they are checked against an Endpoint Compliance Policy. Network Sentry maintains a list of hosts that have passed the scan within the policy. When hosts that previously passed the scan connect to the network, they are given access.

To recheck the hosts and ensure continued compliance, schedule the scan to be run at specific intervals. The hosts are rechecked the next time the scheduled task for the scan runs. Only hosts that have a valid operating system listed in Host Properties are rescanned. Valid operating systems include Windows and Mac.

You can add more than one scheduled task for each scan to check different groups of network hosts at various times. This prevents an excessive load on the system. These groups are subgroups of the original group targeted by the scan. For example, if the original scan was set to scan all staff in the Building A group, the scheduled scan could target staff in subsets of the Building A group. Subsets would be created by placing staff from the Building A group into smaller groups. Then, the 1st floor group could be scanned on Mondays, the 2nd floor group could be scanned on Tuesdays, etc.

**Note:** If Network Sentry has lost contact with the host's Persistent Agent, the host cannot be scanned.

To add schedule tasks for a policy:

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Click the scan to be scheduled.
5. Click **Schedule**.

The Schedule Rescan of Agents window opens. Any existing scheduled tasks appear in the window.

Scheduled Tasks For Scan A Scan

Rescan Scan A

Add

Modify

Remove

Figure 221: Schedule Rescan

6. Click **Add**.

Specify the types of agents and host group this scheduled policy scan will target. Indicate the interval and time for the scheduled task. Use Proactive Scanning to extend the expiration time for hosts which have already passed scans in the recent history interval, instead of marking them at risk.

Task

Scan Name	Scan A	
Scheduled Task Name	<input style="width: 90%;" type="text" value="Rescan Scan A"/>	
Target Agent Types	<input style="width: 90%;" type="text" value="ALL"/>	
<input checked="" type="checkbox"/> Host Group	<input style="width: 90%;" type="text" value="Training Users"/>	
<input type="checkbox"/> Security and Access Attribute Value	<input style="width: 90%;" type="text"/>	

Schedule

Schedule Interval	<input style="width: 90%;" type="text" value="2"/>	<input style="width: 90%;" type="text" value="Days"/>
Next Scheduled Time	<input style="width: 90%;" type="text" value="5/21/12 1:27 PM"/>	
	MM/DD/YY Hour: Mins AM/PM	
Pause	<input type="checkbox"/>	

Proactive Scanning

Proactive Scanning	<input style="width: 90%;" type="text" value="Off"/>	
--------------------	--	--

Apply

Reset

Figure 222: Schedule Scan

7. Use the information in the table below to configure your Scan schedule.

Field	Definition
<b>Task</b>	
<b>Scan Name</b>	Name of the Scan that will be used to rescan hosts.
<b>Schedule Task Name</b>	Each task for the selected scan must have a unique name.
<b>Target Agent Types</b>	Type of agent the hosts are using: ALL, Dissolvable, or Persistent.
<b>Host Group</b>	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See <b>Groups View</b> on page 681 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original scan.
<b>Security And Access Attribute</b>	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group of must be the same as or a subset of the group targeted in the original scan.
<p><b>Note:</b> If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.</p>	
<p><b>Note:</b> If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original scan are scanned.</p>	
<p><b>Note:</b> Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.</p>	
<b>Schedule</b>	
<b>Schedule Interval</b>	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
<b>Next Scheduled Time</b>	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
<b>Pause</b>	When selected, the scheduled task is paused and will not run automatically. Go to the Scheduler View and run the task manually. See the <b>Scheduler View</b> on page 705 for more information.
<b>Proactive Scanning</b>	
<b>Proactive Scanning</b>	See <b>Schedule A Scan—Proactive Scanning</b> on page 573 for additional information.

8. You can run the scheduled task automatically or manually. To manually run the scheduled task from the Scheduler View, click **Pause** to prevent the scheduled task from running. Otherwise, leave the **Pause** check box empty and the task will run at the next scheduled interval and time.
9. Click **Apply**.

### **Add Proactive Scanning To A Scheduled Scan**

Within Network Sentry you can schedule scans to run automatically. Hosts using the Dissolvable Agent can initiate a rescan on the production network. When a rescan is successful, the host has extended the time before another scan is required.

For example, assume the schedule is set to rescan every Sunday. The user rescans his host at his convenience on Friday and passes the scan. When Sunday comes, Network Sentry checks the scan history and determines that this host has had a successful scan. This host is not forced to rescan nor is it marked at risk.

If the host fails the scan, the user is presented with a list of reasons for the failure. The host is not marked at risk at this time. If the user resolves the issues and rescans before the scheduled scan date, the host is never marked at risk and is not forced to rescan on Sunday. If the user does not resolve the issues and rescan, when the scheduled scan date arrives the host is either marked at risk or aged out of the database. The host cannot access the network until it has been successfully scanned or until the host is reregistered and then is successfully scanned.

To rescan the user must open a browser and navigate to the following:

```
https://<Server or Application Server>/remediation
```

The Network Sentry Server or Application Server in the URL can be either the IP Address or Name of the server that is running the captive portal.

Proactive scanning is enabled on the Schedule Rescan window. To provide your hosts access to the dissolvable agent, you can create a web page accessible from your network to download the dissolvable agent.

Scan results are central to Network Sentry's ability to determine when a host was last scanned. Scan results are removed based on the archive and purge schedule set up in Network Sentry properties. When configuring the archive and purge schedule be sure to make the interval long enough to allow the scan results to be used for Proactive Scanning. If the interval is too short, scan results will be purged too soon forcing all hosts to rescan regardless of when their last scan occurred. See **Database Archive** on page 147 for information on archive and purge settings.

### **Schedule A Scan—Proactive Scanning**

Users can proactively rescan their computers to re-assess their system with or without any impact to their At Risk status. This feature helps to decrease the load around the re-registration process or rescan intervals.

To rescan the user must open a browser and navigate to the following:

```
https://<Server or Application Server>/remediation
```

The Network Sentry Server or Application Server in the URL can be either the IP Address or Name of the server that is running the captive portal.

**Note:** The time extension capability can not change a guest record's age-out time; time extensions only apply to standard hosts.

Use the options in the **Schedule Rescan** window to specify whether to apply a time extension if there is a successful scan history within the interval, and what actions to take if there is no scan history. For example if a host does not rescan proactively, the registered host can be set to age-out or be marked At Risk.

Once you have created a policy, do the following to configure the proactive scanning and specify subsequent actions.

### **Add Proactive Scanning To A Scan Schedule**

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Select the scan to be scheduled.
5. Click **Schedule**.

The Schedule Rescan of Agents window opens. Any existing scheduled tasks for the scan appear in the window.

6. Click **Add**.
7. For **Target** select **Dissolvable**. Only hosts using the Dissolvable Agent can do a proactive scan.
8. For the **Proactive Scanning Option**, select **On**. See the Schedule Policy Rescan Of Agent Fields section field definitions.
9. Click **Apply**.

In the figure shown below, the **Scan History Interval** is set to one week. If hosts have successfully passed a scan during the week prior to the time and date specified in the **Next Scheduled Time** field, their expiration time is extended by one week and they will remain on their production network. If they do not have a successful scan within the previous week, they are marked at risk and moved to remediation to be rescanned.

Specify the types of agents and host group this scheduled policy scan will target. Indicate the interval and time for the scheduled task. Use Proactive Scanning to extend the expiration time for hosts which have already passed scans in the recent history interval, instead of marking them at risk.

Task	
Scan Name	Scan A
Scheduled Task Name	<input type="text" value="Rescan Scan A"/>
Target Agent Types	<input type="text" value="ALL"/>
<input checked="" type="checkbox"/> Host Group	<input type="text" value="DistGroup"/>
<input type="checkbox"/> Security and Access Attribute Value	<input type="text"/>
Schedule	
Schedule Interval	<input type="text" value="5"/> <input type="text" value="Days"/>
Next Scheduled Time	<input type="text" value="5/21/12 2:28 PM"/> MM/DD/YY Hour:Mins AM/PM
Pause	<input type="checkbox"/>
Proactive Scanning	
Proactive Scanning	<input type="text" value="On"/>
Scan History Interval (previous)	<input type="text" value="1"/> <input type="text" value="Weeks"/>
No Scan History Found	<input type="text" value="Mark At Risk"/>
Scan History Found	<input type="text" value="Extend Time"/>
Extend Expiration Time	<input type="text" value="1"/> <input type="text" value="Weeks"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 223: Schedule Rescan

**Schedule Rescan Fields**

Field	Definition
<b>Task</b>	
<b>Scan Name</b>	Name of the Scan that will be used to rescan hosts.
<b>Schedule Task Name</b>	Each task for the selected policy must have a unique name.
<b>Target Agent Types</b>	Type of agent the hosts are using: ALL, Dissolvable, or Persistent.
<b>Host Group</b>	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See <b>Groups View</b> on page 681 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original policy.
<b>Security And Access Attribute</b>	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group of must be the same as or a subset of the group targeted in the original policy.
<b>Note:</b> If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.	
<b>Note:</b> If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original policy are scanned.	
<b>Note:</b> Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.	
<b>Schedule</b>	
<b>Schedule Interval</b>	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
<b>Next Scheduled Time</b>	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
<b>Pause</b>	When selected, the scheduled task is paused and will not run automatically. Go to the Scheduler View and run the task manually. See the <b>Scheduler View</b> on page 705 for more information.
<b>Proactive Scanning</b>	
<b>Proactive Scanning</b>	Select <b>On</b> . If you select Off, the hosts are placed in Quarantine when the scheduled task runs.
<b>Scan History Interval (previous)</b>	Interval of time the previous scan history is considered valid.

Field	Definition
<b>No Scan History Found</b>	<p>If the host has not been successfully scanned within the scan history interval, you have the option of marking the host at risk or aging the record.</p> <p>If you select <b>At Risk</b>, the host is moved to Quarantine to be rescanned.</p> <p>If you select <b>Age Record</b>, the host is deleted and must be re-registered to regain network access.</p>
<b>Scan History Found</b>	<p>If the most recent scan in the scan history is a successful scan for the host and is within the scan history interval, you have the option of selecting No Action or Extend Time.</p> <p>Select <b>No Action</b> to let the account remain with the existing expiration date and time. If the system takes no action, the host is forced to rescan when the expiration date and time are met even if the host has a successful scan prior to the expiration date and time.</p> <p>Select <b>Extend Time</b> to specify a period in Extend Expiration Date (the next field).</p>
<b>Extend Expiration Time</b>	<p>If Extend Time is selected and the host has had a successful scan within the Scan History Interval, the host's expiration time is extended by this amount.</p>

## Custom Scans Overview

Scans are configured to evaluate hosts connecting to the network. These scans search the host computer for things such as anti-virus software, anti-spyware software or a particular version of an operating system. The categories within which the scan can search are fairly broad. To scan for very specific items, such as a file on the hard drive or a patch, you must create Custom Scans and then link Custom Scans to a general Scan.

The severity level set in the Custom Scan determines how the host is treated when it fails a Custom Scan. Levels can be set to deny the host access to the network or to just send a warning. See **Custom Scans Severity Level** on page 606 for additional details.

Custom Scans that are associated with a Scan can be configured to run at more frequent intervals than the Scan itself by setting up a Monitor in the Scan. This requires that the host have the Persistent Agent installed. See **Monitor Custom Scans** on page 565.

In addition to running a Custom Scan on any host that is evaluated by the associated Scan, you can use Custom Scans to refine or enhance other Scans. For example, if you have set up a Scan to check hosts for one of the following anti-virus programs: AVG 8.5, Kaspersky, or Norton. Within the Kaspersky setting you can add a Custom Scan to search for a version that must be installed. This Custom Scan will not be run for hosts using AVG 8.5 or Norton. It will be run for hosts using Kaspersky.

Custom Scans are created differently depending on the operating system on which they will run. You must create separate Custom Scans for each operating system. For instructions on creating Custom Scans see the following:

**Create Custom Scans For Windows** on page 579

**Create Custom Scans For Mac-OS-X** on page 594

**Create Custom Scans for Linux** on page 600

When hosts fail a Custom Scan, they are redirected to the web page designated within the Custom Scan configuration. These web pages are not provided as part of the Portal Configuration. They must be created and stored on your Network Sentry appliance in the following directory:

```
/bsc/Registration/registration/site
```

Within the directory listed above there are other web pages that might serve as a template for the custom scans web pages. One option is to copy the `antivirus.jsp` file to a new name and edit the text within that file to accommodate your custom scans.

---

**Note:** User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma` you do not need to move them to the new directory, they will continue to display to hosts as needed.

---

## Create Custom Scans For Windows

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A Windows Custom Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or delete the scans at any time. When a scan is modified it affects any existing Scan that use that Custom Scan.

**Note:** User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma` you do not need to move them to the new directory, they will continue to display to hosts as needed.

### Add A Windows Custom Scan

**Add Custom Scan**

Operating System: Windows ▼

Scan Type: Cert-Check ▼

Scan Name:

Property Name	Value
Label	<input type="text"/>
Web Address	<input type="text"/>
Severity	Required ▼
CRL Revocation Checking	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Extended Key Usage Restrictions.	Disabled ▼

See RFC 5820, section 4.2.1.11 for more information.  
Examples:  
Server Authentication: 1.3.6.1.5.5.7.3.1  
Client Authentication: 1.3.6.1.5.5.7.3.2  
Both: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1

OK Cancel

Figure 224: Add Custom Scans

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.

3. Click the **Scans** option to select it.
4. At the bottom of the window click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **Windows** from the Operating System drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Review the table of field definitions for the Windows Custom Scan to be configured.

Scan Type	Description
<b>Cert-Check</b>	Test for a valid certificate on the host.  Note: Requires Agent Version 3.5 or higher. See <b>Cert-Check -Field Definitions</b> on page 581
<b>Domain-Verification</b>	Test for the domain joined by the host. See <b>Domain-Verification Scan - Field Definitions</b> on page 591.  Note: Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.
<b>File</b>	Test for the existence and version of a specific file. If the file exists and is an executable the program can be forced to run. See <b>File Scan - Field Definitions</b> on page 582.
<b>HotFixes</b>	Test for the existence of specific HotFixes for the specified Operating systems. See <b>HotFixes Scan - Field Definitions</b> on page 586.
<b>Processes</b>	Test for the existence of a specific process name for the indicated Windows operating system. See <b>Processes Scan - Field Definitions</b> on page 589.
<b>Prohibited - Domain-Verification</b>	Test for the domain joined by the host. See <b>Prohibited-Domain-Verification Scan - Field Definitions</b> on page 592.  Note: Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.
<b>Prohibited-Processes</b>	Test for the existence of a specific prohibited process for the indicated Windows operating system(s). See <b>Prohibited Processes Scan - Field Definitions</b> on page 590.
<b>Registry-Keys</b>	Test for a specific registry key and its associated data. See <b>Registry-Keys Scan - Field Definitions</b> on page 584.
<b>Registry-Version</b>	Test for a specific program and its version. The program can be required for specific versions of the Windows Operating System. See <b>Registry-Version Scan - Field Definitions</b> on page 587.
<b>Service</b>	Test the state of a service running on the operating system. See <b>Service Scan - Field Definitions</b> on page 592.  Note: Requires Agent Version 3.5 or higher.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.

10. Click **OK**.
11. The name of the Custom Scan displays in the Custom Scans section for each scan. You can select the Custom Scan to be part of the creation or modification of scan parameters.

### Cert-Check -Field Definitions

To create a custom scan for a Cert-Check, enter the information shown in the table below into the custom scan window after selecting the Cert-Check scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information about this cert-check. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>
<b>Severity</b>	The severity of the failure if the certificate is not on the host machine. If you select Required and the certificate does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>CRL Revocation Checking</b>	<p>If enabled, CRL Revocation Checking ensures the certificate has not been revoked by the Certificate Authority (CA). If the certificate is revoked, the host fails the custom scan.</p> <p><b>Note:</b> The application server must have access to the web server. When CRL Verification is enabled, the server reads the CRL Distribution point URIs from the client certificate. The application server will directly download a CRL from an "http://" URI, or indirectly download a CRL from a "ldap://" URI through your configured LDAP servers.</p>

Scan Parameter	Description
<b>Extended Key Usage Restrictions</b>	<p>If enabled, determines how the private key may be used. Multiple extensions must be comma-separated.</p> <p><b>Disabled</b> - There are no restrictions on key usage extensions.</p> <p><b>All of</b> - The certificate must include all of the specified extensions (e.g., if you select this option and enter "1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1", the certificate must include both 1.3.6.1.5.5.7.3.2 and 1.3.6.1.5.5.7.3.1 in order to be verified).</p> <p><b>Exactly</b> - The certificate must include only the specified extensions (e.g., if you select this option and enter "1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2" the certificate may only include 1.3.6.1.5.5.7.3.1 and 1.3.6.1.5.5.7.3.2 to be verified).</p> <p><b>One or More of</b> - The certificate must have at least one of the specified extensions (e.g., if you select this option and enter "1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1", the certificate must include at least one these extensions to be verified).</p> <p><b>None of</b> - The certificate must exclude the specified extensions (e.g., if you select this option and enter "1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1", a certificate that includes either of these extensions will not be verified).</p>

**File Scan - Field Definitions**

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Severity</b>	The severity of the failure if the file is not on the host machine. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>File Name</b>	The name of the file being checked.
<b>File Contains String</b>	<p>Enter the content that must be present within the file in order for the host to pass the scan (e.g., the version number of a product in a configuration file). When the information is found, the host passes the scan. If the information is not found, the host fails the scan.</p> <hr/> <p><b>Note:</b> Requires Agent 4.0.4 or greater.</p> <hr/> <p><b>Note:</b> Requires AV/AS Definition Updates as of May 2, 2016.</p>

Scan Parameter	Description
<b>Registry Key</b>	<p>To speed up the search for a file you can first check the registry to determine the folder in which the file is installed. In this field you would enter the section of the registry where the information about the file you seek resides.</p> <p>For example, if you want to make sure that Windows Messenger is installed on the machine, the scan needs to look for <b>msmsgs.exe</b>. Enter the registry key that points to the Value Name containing the location of msmsgs.exe, such as:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService</p>
<b>Registry Value Name</b>	<p>The Value Name that contains the path to the file the custom scan is seeking.</p> <p>To continue the example above, the Registry Key listed in the previous field tells the custom scan the part of the registry to access to determine where msmsgs.exe is installed. Once the custom scan is looking in the correct section, it needs to know the specific "container" or Value Name in the registry that has the path to msmsgs.exe, such as:</p> <p>InstallationDirectory</p> <p>The custom scan can begin its search in the directory specified in the "InstallationDirectory" Value Name, such as:</p> <p>"C:\Program Files\Messenger"</p>
<b>Execute</b>	Default = No. Select Yes to run the file when it is located.
<b>Command-Line Options</b>	Command line options to be used when executing the file.
<b>Wait for Execution to Complete Before Continuing</b>	Default = No. If set to Yes, the scan waits until the execution of the program is complete before continuing.
<b>File Version (&gt;=)</b>	The version number of the file has to be greater than or equal to the version number entered here.
<b>Web Address</b>	<p>The URL of the page with information about this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p>/bsc/Registration/registration/site</p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p>site/pagename.jsp</p>
<b>Windows OS</b>	<p>Select the check box next to the version(s) of Windows OS for which this key is required.</p> <p>Select the OS within the Custom Scan to apply the custom scan to host machines with that OS.</p> <p>If you do not select an OS in the Custom Scan, and the host machine has that OS, the host automatically passes the general scan.</p>
<b>Prohibit this product</b>	<p>If the file is found and this is set to true, the host fails the scan for a prohibited product.</p> <p>Default = false.</p>

### Registry-Keys Scan - Field Definitions

To create a custom scan for a specific Registry key, enter the information shown in the table below into the custom scan window after selecting the Registry-Keys scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information about this registry key. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>
<b>Severity</b>	The severity of the failure if the key is not on the host machine. If you select Required and the registry key does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Hive</b>	<p>The name of the hive to be searched. Supported hives are:</p> <ul style="list-style-type: none"> <li>• HKEY_CLASSES_ROOT</li> <li>• HKEY_CURRENT_USER</li> <li>• HKEY_LOCAL_MACHINE</li> <li>• HKEY_USERS</li> <li>• HKEY_CURRENT_CONFIG</li> </ul> <p><b>Note:</b> Scanning for registry keys in the HKEY_CURRENT_USER hive will not be successful because the user running Persistent Agent differs from the user logged on to the host.</p>
<b>Key Name</b>	Name of the Registry Key that contains the value being located.
<b>Value Name</b>	The Value Name to be located.
<b>Type</b>	<ul style="list-style-type: none"> <li>• REG_SZ</li> <li>• REG_DWORD</li> </ul> <p><b>Note:</b> You must enter the REG_DWORD setting as a decimal value, not hexadecimal.</p>
<b>Data</b>	The data to be contained in the selected type.

Scan Parameter	Description
<b>Action</b>	<p>Select an action from the drop-down list:</p> <p><b>Match Value Exactly</b>—The <b>Value Name</b> is used as a path to find the specified <b>Key Name</b> in the tree. <b>Data</b> listed in the scan is compared to the data on the key. If the value and data in the key are exact matches to the specified entries, the scan passes. Otherwise, it fails.</p> <p><b>Search keys and values</b>—The <b>Key Name</b> is used as a starting point. The search is for whatever is contained in <b>Data</b>. The data must be found in a key name, a Value name, or the data of all sub-keys of the key entered.</p> <p><b>Value contains Data</b>—The <b>Value Name</b> is used as a path to find the specified <b>Key Name</b> in the tree. <b>Data</b> listed in the scan is compared to the data in the value. If the contents in the value contains the data, the scan passes. Otherwise, it fails.</p> <p><b>Key has a value</b>—The <b>Value Name</b> is used as a path to find the specified <b>Key Name</b> in the tree. If the key is found by using the name in the value and the data is not empty, the scan passes. Otherwise, it fails.</p> <p><b>Sets the value (Use Caution)</b>— When checked, this scan ALWAYS PASSES. The scan checks to see if the key exists in the registry key. If it does, the scan overwrites the key to have the specified data. If it does not exist, the scan creates the key and sets the data as specified.</p> <hr/> <p><b>Note:</b> When the Type is <b>REG_DWORD</b>, the only actions available are <b>Match Value</b> and <b>Sets the value (Use Caution)</b>.</p> <p><b>Example:</b></p> <p><b>Hive Name</b> HKEY_LOCAL_MACHINE</p> <p><b>Key Name</b> SOFTWARE\Widgets\Setup</p> <p><b>Value Name</b> Version</p> <p><b>Data</b> 1.0</p>
<b>DWORD Comparison Operation</b>	<p>This field is enabled only when <b>Type</b> is set to REG_DWORD and <b>Action</b> is set to Match Value. The operator selected here is used in the comparison of the value in the <b>Data</b> field to the Data value in the registry. For example, if this field is set to = then both values must match exactly. If the operator is set to &gt;= the Data value in the host registry must be greater than or equal to the Data value in the custom scan.</p>
<b>Prohibit</b>	<p>If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product.</p> <p>Default = False.</p>
<b>Require for Windows...</b>	<p>Select the check box next to the version(s) of Windows OS for which this key is required.</p> <p>You must select the OS within the Custom Scan to apply the scan to host machines with the selected OS.</p> <p>If you do not select an OS in the Custom Scan and the host machine has that OS, the host automatically passes the general scan.</p>

**HotFixes Scan - Field Definitions**

You can create a custom scan for a specific HotFix. Enter the information shown in the table below into the custom scan window after selecting the HotFix scan type.

**WARNING:** As a best practice, add HotFix custom scans to a particular operating system within a general Scan. If you enable the HotFix custom scan at the Scan level, every host that is evaluated by the scan is also scanned for the HotFix. Since HotFixes are operating system specific you could inadvertently deny access to the network to many hosts.

Scan Parameter	Description
<b>Label</b>	Label in the Results page information identifying which scan the host failed.
<b>Web Address</b>	The URL of the page with information about this HotFix. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  /bsc/Registration/registration/site  When completing this field you must enter part of the path for the page not just the page name, such as:  site/pagename.jsp
<b>Severity</b>	The severity of the failure if the hotfix is not on the host machine. If you select Required and the hotfix does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>HotFix ID</b>	The name of the HotFix, such as, KB123456.
<b>Bypass Service Pack (&gt;=)</b>	Select the Bypass Service Pack check box to display a text field. Enter the numeric value for the Service Pack level in this field.  The host must have the specified hotfix (HotFix ID above) OR a service pack level equal to or greater than the set value to pass the scan.
<b>Require for Windows...</b>	Select the check box next to the version(s) of Windows OS for which this key is required.  You must select the OS within the Custom Scan to apply the scan to host machines with the selected OS.  If you do not select an OS in the Custom Scan and the host machine has that OS, the host automatically passes the general scan.

### Registry-Version Scan - Field Definitions

Create a custom scan to verify that a specific version of an application, such as Internet Explorer, is installed on the host machine. Enter the information shown in the table below into the custom scan window after selecting the Registry-Version scan type. When the scan runs, the registry is checked to see if the installed application has the required version.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information about this registry version. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>
<b>Severity</b>	The severity of the failure if the file is not on the host machine. If you select Required and the version of the application does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Hive</b>	<p>The name of the Hive to be searched. Supported hives are:</p> <ul style="list-style-type: none"> <li>• HKEY_CLASSES_ROOT</li> <li>• HKEY_CURRENT_USER</li> <li>• HKEY_LOCAL_MACHINE</li> <li>• HKEY_USERS</li> <li>• HKEY_CURRENT_CONFIG</li> </ul>
<b>Key Name</b>	Name of the Registry Key that contains the value being searched for.
<b>Value Name</b>	The Value Name that must be in the key entry.
<b>Version</b>	The Version that must be in the key entry.
<b>Operation</b>	<p>Select an Operator for the version number:</p> <p>&gt;</p> <p>=</p> <p>&gt;=</p>

<b>Scan Parameter</b>	<b>Description</b>
<b>Prohibit</b>	If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product.  Default = False.
<b>Version Delimiter</b>	The character used to identify the delimiter.
<b>Require for Windows...</b>	Select the check box next to the version(s) of Windows OS for which this key is required.  You must select the OS within the Custom Scan to apply the scan to host machines with the selected OS.  If you do not select an OS in the Custom Scan and the host machine has that OS, the host automatically passes the general scan.

### Processes Scan - Field Definitions

Create a custom scan for a specific process. Process names for various applications may differ between operating systems. Enter the process name for each OS if this is the case. Enter the process name(s) information into the custom scan window for Processes.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code>  When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
<b>Severity</b>	The severity of the failure if the process is not running on the host machine. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name for ...</b>	Enter the name of the process that is required for the specific Operating System(s).

**Note:** If you do not want to scan for a process on a particular Operating System, leave the corresponding field blank. When you click **Apply** Network Sentry fills each blank field with the word SYSTEM. This indicates that the corresponding Operating System should be passed for this scan.

### Prohibited Processes Scan - Field Definitions

Create a custom scan to prohibit a specific process on a host machine with selected Operating System(s). Process names for various applications may differ between operating systems. Enter the process name for each OS if this is the case. Enter the process name(s) information into the custom scan window for Prohibited-Processes.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <pre>/bsc/Registration/registration/site</pre> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <pre>site/pagename.jsp</pre>
<b>Severity</b>	The severity of the failure if the prohibited process is running on the host machine. If you select Required and the process does exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name for ...</b>	Enter the name of the process that is prohibited for the specific Operating System (s).

### Domain-Verification Scan - Field Definitions

Create a custom scan to verify that a host machine has joined the appropriate domain when it connected to the network. Domain names may differ between operating systems. Enter a comma separated list of domain names for each OS. Attach this custom scan to any Policies that require domain verification. A host will pass this scan if it is joined with any domain contained in the list for the host's operating system.

**Note:** Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information regarding domain verification. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>
<b>Severity</b>	The severity of the failure if the host is not part of any of the domains specified. If you select Required and the host is not in the correct domain, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Domain Names for ...</b>	Enter a comma separated list of the NetBIOS domain names that are required or permitted for the specific Operating System(s).

**Prohibited-Domain-Verification Scan - Field Definitions**

Create a custom scan to verify the domain a host is attempting to join and prohibit access to the network based on that domain. Domain names may differ between operating systems. Enter a comma general scan to prevent access based on domain verification. A host will fail this scan if it is joined with any domain contained in the list for the host's operating system.

**Note:** Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	The URL of the page with information regarding domain verification. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  /bsc/Registration/registration/site  When completing this field you must enter part of the path for the page not just the page name, such as:  site/pagename.jsp
<b>Severity</b>	The severity of the failure if the host is part of any of the domains specified. If you select Required and the host is not in the correct domain, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Domain Names for ...</b>	Enter a comma separated list of the NetBIOS domain names that are prohibited for the specific Operating System(s).

**Service Scan - Field Definitions**

You can create a custom scan to check the status of a Windows Service. Enter the information shown in the table below into the custom scan window after selecting the Service scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.

Scan Parameter	Description
<b>Severity</b>	The severity of the failure if the service is not in the desired state on the host. If you select Required and the service is not in the desired state, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Service Name</b>	The name of the service on the Windows OS. To retrieve the service name, open the Microsoft Management Console Local Services view. See Find the Service Name below for information on how to locate the Service Name on your system.
<b>Desired State</b>	Select the the state of the service on the host to be scanned. Select Running to indicate the host must be running the service. Select Stopped to indicate the host must not be running the service.
<b>Web Address</b>	The URL of the page with information about this service. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  /bsc/Registration/registration/site  When completing this field you must enter part of the path for the page not just the page name, such as:  site/pagename.jsp

### **Find the Service Name**

1. Open Microsoft Management Console on your system.
2. Navigate to the Local Services view.
3. Right-click the process you want to create the custom scan for, and click **Properties**.
4. Find the service name in the Properties view and enter it in the **Service Name** field of the custom scan.

## Create Custom Scans For Mac-OS-X

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A Mac OS X Custom Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a Custom Scan is modified it affects any existing general Scans that use that Custom Scan.

**Note:** User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma` you do not need to move them to the new directory, they will continue to display to hosts as needed.

### Add A Mac OS X Custom Scan

The screenshot shows a dialog box titled "Add Custom Scan". It contains the following fields and options:

- Operating System: Mac-OS-X (dropdown)
- Scan Type: File (dropdown)
- Scan Name: Mac Only (text input)
- Label: (empty text input)
- Severity: Required (dropdown)
- File Name: (empty text input)
- Starting Path: /Applications (text input)
- Web Address: (empty text input)
- Prohibit this product:  true  false

Buttons: OK, Cancel

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.

4. At the bottom of the window click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **Mac-OS-X** from the Operating System drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Review the table of field definitions for the type to be configured.

Scan Type	Description
<b>File</b>	Test for the existence of a specific file on the host machine. See <b>File Scan - Field Definitions</b> on page 595.
<b>Package</b>	Test for a existence of a specific installer package on the host machine. An inclusive range of Mac OS X Versions can be specified for this scan. See <b>Package Scan - Field Definitions</b> on page 596.
<b>Processes</b>	Test for the existence of a specific process. See <b>Processes Scan - Field Definitions</b> on page 598.
<b>Prohibited-Processes</b>	Test for the existence of a specific prohibited process. See <b>Prohibited Processes Scan - Field Definitions</b> on page 599.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.
11. The name of the Custom Scan will now appear in the Custom Scans section for each Mac OS X scan and can be selected as part of the creation or modification of the general scan parameters.

### File Scan - Field Definitions

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Severity</b>	The severity of the failure if the file is not on the host machine. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>File Name</b>	The name of the file being checked for on the host machine.

Scan Parameter	Description
<b>Starting Path</b>	The search for the file starts with the directory indicated here and includes all sub-directories and files.  <b>Important:</b> Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).
<b>Web Address</b>	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  <code>/bsc/Registration/registration/site</code>  When completing this field you must enter part of the path for the page not just the page name, such as:  <code>site/pagename.jsp</code>
<b>Prohibit this product</b>	If the file is found and this is set to true, the host fails the scan for a prohibited product.  Default = false.

### Package Scan - Field Definitions

To create a custom scan for a specific installer package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host machine.

**Note:** If the package name is installed on a machine with an OS version outside the range, the host machine will pass the scan.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Severity</b>	The severity of the failure if the package is not on the host machine. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Package Name</b>	<code>name.pkg</code>  The name of the installer package being searched for on the host machine. The custom scan searches the /Library/Receipts directory for install receipts.
<b>Minimum Mac OS X Version</b>	The inclusive minimum version of the MAX-OS software.

---

Scan Parameter	Description
<b>Maximum Mac OS X Version</b>	The inclusive maximum version of the MAX-OS-X software.
<b>Web Address</b>	<p>The URL of the page with information regarding this installer package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>

**Processes Scan - Field Definitions**

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
<b>Severity</b>	The severity of the failure if the process is not running on the host machine. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name</b>	The name of the process being scanned for on the host machine. This name is seen when you use <code>ps</code> at the command line. This is not necessarily the name in the Activity Monitor list. For example, <code>iChat</code> , <code>iChatAgent</code> , <code>iTunes</code> , <code>iTunesHelper</code> .

### Prohibited Processes Scan - Field Definitions

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	<p>The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>
<b>Severity</b>	The severity of the failure if the prohibited process is running on the host machine. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name</b>	Name of the prohibited process being scanned for on the host machine.

## Create Custom Scans for Linux

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A Linux Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a Custom Scan is modified it affects any existing general Scans that use that Custom Scan.

**Note:** User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma` you do not need to move them to the new directory, they will continue to display to hosts as needed.

### Add A Linux Custom Scan

The screenshot shows a dialog box titled "Add Custom Scan" with a close button in the top right corner. The dialog contains the following fields and controls:

- Operating System: Linux (dropdown menu)
- Scan Type: File (dropdown menu)
- Scan Name: Employee Scan (text input field)
- Label: (empty text input field)
- Severity: Required (dropdown menu)
- File Name: (empty text input field)
- Starting Path: /home (text input field)
- Web Address: (empty text input field)
- Prohibit this file:  true  false

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.

4. At the bottom of the window click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **Linux** from the Operating System drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Review the table of field definitions for the type to be configured.

Scan Type	Description
<b>File</b>	Test for the existence of a specific file on the host machine. See <b>File Scan - Field Definitions</b> on page 601.
<b>Package</b>	Test for a existence of a specific rpm/deb packages on the host machine. See <b>Package Scan - Field Definitions</b> on page 603.
<b>Processes</b>	Test for the existence of a specific process. See <b>Processes Scan - Field Definitions</b> on page 604.
<b>Prohibited-Processes</b>	Test for the existence of a specific prohibited process. See <b>Prohibited Processes Scan - Field Definitions</b> on page 604.
<b>Script</b>	Allows users to upload a script to Network Sentry to be executed on the host machine. See <b>Script - Field Definitions</b> on page 605.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.
11. The name of the Custom Scan will now appear in the Custom Scans section for each Linux scan and can be selected as part of the creation or modification of the general scan parameters.

### **File Scan - Field Definitions**

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Severity</b>	The severity of the failure if the file is not on the host machine. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.

<b>Scan Parameter</b>	<b>Description</b>
<b>File Name</b>	The name of the file being checked for on the host machine.
<b>Starting Path</b>	The search for the file starts with the directory indicated here and includes all sub-directories and files. <b>Important:</b> Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).
<b>Web Address</b>	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  <code>/bsc/Registration/registration/site</code>  When completing this field you must enter part of the path for the page not just the page name, such as:  <code>site/pagename.jsp</code>
<b>Prohibit this product</b>	If the file is found and this is set to true, the host fails the scan for a prohibited product.  Default = false.

### Package Scan - Field Definitions

To create a custom scan for a specific rpm or deb package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host machine.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Severity</b>	The severity of the failure if the package is not on the host machine. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Package Name</b>	The name of the rpm or deb package being searched for on the host machine. The custom scan runs rpm or dpkg commands to search for installed packages.
<b>Version</b>	The inclusive minimum version of the Linux software.
<b>Web Address</b>	<p>The URL of the page with information regarding this rpm or deb package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>

### Processes Scan - Field Definitions

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  <code>/bsc/Registration/registration/site</code>  When completing this field you must enter part of the path for the page not just the page name, such as:  <code>site/pagename.jsp</code>
<b>Severity</b>	The severity of the failure if the process is not running on the host machine. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name</b>	The name of the process being scanned for on the host machine. This name is seen when you use ps at the command line.

### Prohibited Processes Scan - Field Definitions

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Web Address</b>	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:  <code>/bsc/Registration/registration/site</code>  When completing this field you must enter part of the path for the page not just the page name, such as:  <code>site/pagename.jsp</code>

Scan Parameter	Description
<b>Severity</b>	The severity of the failure if the prohibited process is running on the host machine. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See <b>Custom Scans Severity Level</b> on page 606 for more details.
<b>Process Name</b>	Name of the prohibited process being scanned for on the host machine.

### Script - Field Definitions

To create a custom scan for a specific script, enter the information shown in the table below into the custom scan window after selecting the Script scan type.

Scan Parameter	Description
<b>Label</b>	This label appears in the Results page information to identify which scan the host failed.
<b>Upload Script</b>	Users can select a script to upload to Network Sentry. The name of the uploaded script appears in the text field.
<b>Return Value</b>	The value that the script must return after the agent executes the script.
<b>Web Address</b>	<p>The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:</p> <p><code>/bsc/Registration/registration/site</code></p> <p>When completing this field you must enter part of the path for the page not just the page name, such as:</p> <p><code>site/pagename.jsp</code></p>

## Custom Scans Severity Level

You can configure custom scans with a Severity Level setting. The Severity Level controls whether a host loses access to the network or only receives a warning when it is not in compliance with the scan. When the host fails a custom scan with a severity level set to warning, the experience varies, depending on the type of security agent that is being used.

### **Setting Severity Level To Required**

When a custom scan severity level is set to Required, if the host fails the scan, the host is set to At Risk. The browser is redirected to a web page that contains details about the requirements the host failed. The host self-remediates (corrects the issues causing the failure) and rescans until it meets all requirements. When the host passes the requirements, it is moved to the production network.

The Scan Results section of the Health Tab on the Host Properties window shows a Failed or Passed result. See **Host Health And Scanning** on page 339.

### **Setting Severity Level To Warning**

When the host fails a custom scan with a severity level set to Warning, the experience will vary depending on the type of security agent that is being used.

#### **Dissolvable Agent**

When a host fails the scan, the browser is redirected to a web page that contains details about the requirements the host failed. The web page is divided into two sections. One section contains Required severity level items the host failed; the other contains Warning severity level items the host failed.

If the host failed only Warning severity level items, a **Register Now** button is available on the web page. The user clicks the button and is moved to the Success web page.

If the host failed Required and Warning severity level items, the host must self-remediate until all items in the Required section are corrected. When only Warning level items are listed in the Warning section of the web page, the **Register Now** button becomes available. The user clicks the button and is moved to the Success web page. The host is not fully compliant with the Endpoint Compliance Policy, but is allowed on the production network.

#### **Persistent Agent**

If the host fails the scan for only items with the severity level set to Warning, a **Warning** message is sent to the host and the host is moved to the production network.

If the host fails items with severity levels set to Required and Warning, the host is moved to the remediation network. The browser is redirected to a web page containing details about the requirements the host failed. The web page is divided into

two sections. One section contains Required severity level items the host failed; the other contains Warning severity level items the host failed.

The host must self-remediate until all items in the Required section are corrected. When the only items listed are in the section containing the failures for severity level set to Warning, the user receives a warning message that his computer is not fully compliant with the Endpoint Compliance Policy. The host is then allowed on the production network.

The Scan Results section of the Health Tab on the Host Properties window shows a Warning result. See **Host Health And Scanning** on page 339.

### Custom Scans - Use Case

The company network rules prohibit registered hosts on the network from having LimeWire installed on the host machine. Host machines are required to have a Persistent Agent and are scanned daily to maintain compliance. If LimeWire is installed, the host will receive three warnings before being removed from the network.

To set up a custom scan to enforce this rule:

1. Create a custom scan for Registry Key, enter the details for LimeWire, set Prohibit to True, and set the Severity level to Warning. See **Add A Windows Custom Scan** on page 579 or **Add A Mac OS X Custom Scan** on page 594.
2. Create a regular Scan and enable the custom scan within that scan. See **Add/Modify A Scan** on page 556.
3. Schedule the regular Scan to be rerun daily. See **Schedule A Scan** on page 570.
4. Create an Endpoint Compliance Policy that contains the regular Scan. See **Endpoint Compliance Policies** on page 525.
5. Map the Security Risk Host event to an alarm that will take action on the third occurrence of the event, and set the host At Risk and Send a message. See **Add or Modify Alarm Mapping** on page 497.
6. Configure the web page that the host will be redirected to when moved to Remediation. The web page used is created outside the program. In order to keep this page from being overwritten during an upgrade, it should be stored in `/bsc/Registration/registration/site`. Then, return to your custom scan and modify it to contain the new web address.

If the host fails the scan, the first two times, the Warning message is sent. On the third failure, the host is sent the Warning message, is marked At Risk, and moved to Remediation. The web page informs the user about the failure to meet policy requirements. The host self-remediates and rescans. When the host passes the policy, the host is moved back to the production network.

## Chapter 14: Role Management

Roles are used in two different ways in Network Sentry. Roles assigned to hosts managed in the Host View or Users are attributes of those elements. In this case the role is another way to group users and hosts. Roles can be used in User/Host Profiles to filter for specific Users or Hosts when applying Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.

For devices or hosts managed in the Topology View, Roles are used to determine the network access given to those elements based on their connection location. In this case Roles are used with Network Device Roles. The Role is simply a name or identifier that is assigned to the host or device. The Network Device Role maps the connection location with device, port or SSID groups to a specific Role. For example, when a device connects to the network with Role A on Switch 1, Network Sentry searches through the Network Device Roles for a record with Role A that has a connection location containing Switch 1. The first matching Network Device Role is used. The configuration of this Network Device Role can place the device in a specific VLAN or can apply a CLI Configuration.

Role Management relies on the configuration of both Roles and Network Device Roles. The Roles View contains the list of possible Role names and controls assigning roles to users and hosts based on group membership. Roles for hosts managed in the Host View and Users do not need a corresponding Network Device Role. Network access for those hosts and users is handled by Network Access Policies. Roles for devices or hosts managed in Topology View require a corresponding Network Device Role to control network access. See **Roles** on page 615.

**Note:** If a role has more than one mapping for the same device or port group, the order of precedence is determined by the order of the role mappings on the Network Device Roles View. Starting from the top of the list, the first mapping match found is used.

See **Set Up Role Management** on page 614 for an overview of setup requirements.

## Assigning Roles

Roles can be assigned to users, hosts, network devices and ports. Each one of these entities has a role field on its corresponding Properties window. Assignment of roles is accomplished by setting the role field for the user, host, device or port either manually or using one of the options listed in the table.

**Note:** When a user and a host have different roles, the user role is applied if the user logs into the host. In the case of a gaming device that the user does not log into, it has its own role that may or may not be the same as the user's.

In the event that multiple methods are used to set a role, the order of precedence is determined by the order of the roles on the Roles View. Starting from the top of the list, the first role match found is used. For example, assume you have assigned roles to hosts based on groups. Later you add the host to a new group, if that group is associated with a role that is ranked above the host's original role, the host's role will be changed.

**Note:** Roles created on the Network Sentry server will be ranked above global roles created on the NCM. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the Network Sentry server.

In the event that multiple methods are used to assign a role to a host, a hierarchy determines which role to assign. Roles assigned through Portal pages (typically for gaming), have the lowest precedence and will be overwritten by a role determined by any other method. Roles assigned by Directory Attributes have the highest precedence and will overwrite a role that is assigned by any other method. Roles assigned by Group Membership have the middle level of precedence, overwriting roles assigned through Portal Pages, but being overwritten by roles assigned via Directory Attributes. Roles assigned via Group Membership will change when the host's group membership changes. When this occurs, the roles are ranked, with low-numbered ranks having the highest precedence.

Roles	Definition
User Roles	

Roles	Definition
<p><b>User Roles Based On Groups</b></p>	<p>Users can be assigned roles by placing them in a group and then associating that group with a role on the Role View. See <b>Add A Role</b> on page 618 for additional information on adding roles. Once the group of users has been created and you have assigned them a role, you must associate that role with a device group or a port group and a corresponding VLAN or CLI configuration.</p> <p>User groups can also be created based on groups in the Directory. These groups are treated the same as groups created manually within Network Sentry. If a user is a member of more than one group the group that is found first when matching users to roles determines the role assigned to the user.</p> <p><b>Note:</b> When assigning Roles to users, the use of Directory attributes over Directory groups is recommended. Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the Network Sentry server and could be out-dated.</p>
<p><b>User Roles Based On A Directory Field</b></p>	<p>Network users can be assigned a role based on a field in LDAP or Active Directory. For example, you might choose to have roles based on a field in the directory called Department. The data within the Department field would be the name of the role, such as, Accounting or Customer Service. In a university environment a user might have a role based on whether he is a Student or Faculty.</p> <p>To assign roles based on a field in a directory you must indicate which field in the directory is to be used as a role. See <b>Add/Modify Directory - User Attributes Tab</b> on page 76 to map the role field.</p> <p>Users in the directory with matching data in this field constitute a group, even though the group is not shown anywhere. For example, users with Accounting in their department field are treated as an Accounting group for the purpose of assigning roles.</p> <p>Next, you must create a Role with the exact same name as the data contained in the directory field. For example, if the user's role in the directory is Accounting, you must create a Role on the Role View that is named Accounting.</p> <p>When a user registers, the role field in User Properties is set to match the data in that user's role field in the directory.</p>
<p><b>User Roles Based On Fields In Captive Portal</b></p>	<p>When registering a host through the Captive Portal, if the user fields on the portal page have a role set, that role is assigned to the user, such as during registration or authentication.</p>
<p><b>Individual User Roles</b></p>	<p>In some situations you may want to assign a role to a single user. First create the role on the Roles View. Then, navigate to the User Properties window and modify the Role field.</p>
<p><b>Host Roles</b></p>	

Roles	Definition
<p><b>Host Roles Inherited From Users</b></p>	<p>When registering a rogue to a user on the Host View, you have the option to use the user's role or to select a different role for the device. See <b>Modify a Host</b> on page 344.</p> <p>When registering a host through the Captive Portal, if the portal does not have a role set, the host inherits the role of the user.</p> <p>If the users role changes, regardless of how it is changed, any host registered to that user that has the same role will be changed also.</p> <p><b>Example:</b></p> <p>John Doe is a student and has two registered hosts.</p> <ul style="list-style-type: none"> <li>• John Doe's Role: <b>Student</b></li> <li>• John Doe's Host 1 Role: <b>Student</b></li> <li>• John Doe's Host 2 Role: <b>Gaming</b></li> </ul> <p>John Doe graduates and becomes faculty, so the University makes the change in AD and runs a Directory Sync. John's role is changed to Faculty.</p> <ul style="list-style-type: none"> <li>• John Doe's Role: <b>Faculty</b></li> <li>• John Doe's Host 1 Role: <b>Faculty</b></li> <li>• John Doe's Host 2 Role: <b>Gaming</b></li> </ul> <p>Host 2 did not match John's original role of Student, so it is not changed.</p>
<p><b>Host Roles Assigned Through Captive Portal</b></p>	<p>When registering a host through the Captive Portal, if the portal page has a role set, that role is assigned to the host during registration. If the role field is blank, the host inherits the role of the user.</p>
<p><b>Host Roles Based On Groups</b></p>	<p>Hosts can be assigned roles by placing them in a group and then associating that group with a role on the Roles View. See <b>Add A Role</b> on page 618 for additional information on adding roles.</p>
<p><b>Host Roles Assigned Manually</b></p>	<p>This would typically be used to assign a role to hosts, such as a medical device that connects to the network.</p> <p>To register rogues and set their role: Select one or more rogues on the Host View. Right-click on the selected records and choose Register as Device from the menu. On the registration pop-up you can select device type and role. See <b>Register A Host As A Device</b> on page 364.</p> <p>To set roles for registered devices: Select one or more devices on the Host View. Right-click on the selected records and choose Set Host Role. Select the new role from the drop-down list in the pop-up window.</p>

Roles	Definition
<b>Host Roles Assigned By Device Profiler</b>	<p>This would typically be used to assign a role to hosts, such as a medical device that connects to the network. Devices that are hosts, such as, medical devices, gaming devices, or printers can be assigned a role and a device type based on Device Profiling Rules.</p> <p>If you are using the Device Profiler feature, you can create or use default rules that allow Network Sentry to determine the device type and assign the device to a role. When a new host device connects to the network it becomes a rogue because it is unknown. Network Sentry compares information received from the device with the Device Profiling Rules in its database until it comes up with a match. Based on the parameters defined in the rule, the device is assigned a type and a role. See <b>Device Profiler</b> on page 189 and <b>Device Profiling Rules</b> on page 192.</p> <p>Note: The role assigned by Device Profiler takes precedence over any role associated with the Vendor OUI.</p>

## Set Up Role Management

1. Determine which device(s) will be used to support a specific role.
2. Configure the device(s) with the VLAN or Interface ID information for the role.
3. Create a device group and add the device(s) for each set of devices that will be used for roles. For example, you might have a group of devices that provide network access in Building A. That group of devices will provide different types of access than the devices in Building B, therefore you would create two separate device groups. See **Groups View** on page 681 for information on groups.
4. If only some ports on a device or devices will be used for Role Management, you can place just the required ports in a Port group specifically for roles. First, determine which ports will participate in Role Management and place those ports in the Role Based Access Group. Ports that are not in this group cannot apply roles. Once ports are in the Role Based Access group, place them in groups that will be associated with roles. See **Groups View** on page 681 for information on groups.

**Note:** Ports that are assigned roles are typically included in the Role Based Access Group. If a port is assigned a role but is not included in the Role Based Access Group, devices connecting to that port are placed in the default VLAN entered on the Model Configuration window for that device. They are not placed on the VLAN defined for the role. However, if the role is used as a filter for any policy, that policy is still used.

5. Create a list of Roles. See **Roles** on page 615.
6. Determine which hosts or users will be identified by the role.
7. Associate the hosts or users with the role. See **Assigning Roles** on page 610.

**Important:** Use only one method to associate a host or a user with a role. If more than one method is used, the role is assigned based on the ranking of roles and the first piece of data that matches.

**Note:** Roles are only applied to hosts that are registered.

8. Once roles have been created, configure Network Device Roles. Network Device Roles indicate the actions to be taken when a device in that role connects to a group of devices or ports. There can be multiple mappings for a single role. For example, Role A can have a mapping for Port/Device Group A and a different mapping for Port/Device Group B. Select the Device or Port group and enter the Network Access IDs.

## Roles

This view allows you to setup Role Names. Roles are assigned to Users, Hosts and Devices. For hosts managed in the Host View and users roles are attributes that are used in User/Host Profiles as filters. For devices and hosts managed in Topology View, such as a printer, roles are used to control network access based on where they connect. If you are using roles to control network access for hosts and devices you must also configure Network Device Roles to provide a set of connection instructions for role and device or port group combinations.

For example, if Role A is assigned to all of the printers in the Accounting Department, then when a printer connects to a port in the accounting office, the Network Device Role for accounting office ports is configured to move them to VLAN 10.

In the case of a host managed in the Host View, if Role B is assigned to that host, then when the host connects to a port in the accounting office, Network Sentry reviews the Network Access Policies until it finds a policy for a host with Role B connected to accounting ports based on the User/Host Profile in the policy.

Roles can be assigned in many different ways. In the case of the Roles View, roles are assigned based on directory groups or Network Sentry groups. When a user or a host is added to a group, Network Sentry searches the list of roles for a match starting with the role ranked number 1. When a match is found, the role is assigned to the user or the host. In the case of directory attributes, when a user is registered and Network Sentry checks the list of roles, a role with a name that exactly matches the attribute will be assigned to the user if it is the first piece of data about the user that matches the role criteria.

---

**Note:** Roles created on the Network Sentry server will be ranked above global roles created on the NCM. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the Network Sentry server.

---

For additional information on all methods for role assignment, see **Assigning Roles** on page 610.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Roles - Total: 8						
Rank	Name	Groups	Note	Last Modified By	Last Modified Date	
1	GuestSelfRegistration	None		SYSTEM	08/18/14 12:37 PM EDT	
2	GuestAccess	None		SYSTEM	08/18/14 12:37 PM EDT	
3	GuestConference	None		SYSTEM	08/18/14 12:37 PM EDT	
4	Guest	None	Converted from existing role Guest. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT	
5	Contractor	None	Converted from existing role Contractor. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT	
6	NAC-Default	None	Converted from existing role NAC-Default. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT	
7	Sponsor_Template	None		SYSTEM	08/22/14 11:28 AM EDT	
8	GuestTemplate3	None		SYSTEM	01/13/15 03:10 PM EST	

Export to:

Options Add Modify Delete In Use

Figure 225: Roles View

Roles View Field Definitions

Field	Definition
<b>Rank Buttons</b>	Moves the selected role up or down in the list. Users and hosts are compared to roles in order by rank.
<b>Set Rank Button</b>	Allows you to type a different rank number for a selected role and immediately move the role to that position. In an environment with a large number of roles, this process is faster than using the up and down Rank buttons.
<b>Name</b>	Name of the role. If you are assigning roles based on the directory attribute specified in Attribute Mappings in the Role field, the name of the role in the Roles View must match the data in the user's directory attribute. For example, if the directory attribute is department and the user's field is set to Accounting, then the role name must be Accounting in order to match. See <b>Add/Modify Directory - User Attributes Tab</b> on page 76.
<b>Groups</b>	One or more groups whose members will be assigned to this role. List includes Groups both in Network Sentry and in the Directory, if one is being used with Network Sentry.  If no groups are selected, None is displayed in this field. This effectively disables the role for group assignment. However, the role can still be assigned manually, by Device Profiler or through the Captive Portal.
<b>Note</b>	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of Network Sentry.
<b>Last Modified By</b>	User name of the last user to modify the role. SYSTEM indicates that the role was modified by Network Sentry itself.
<b>Last Modified Date</b>	Date and time of the last modification to this role
<b>Right Mouse Click Menu - Options Button Menu</b>	
<b>Export</b>	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

Field	Definition
<b>Copy</b>	Copy the selected Role to create a new record.
<b>Delete</b>	Deletes the selected Role. Roles that are currently in use cannot be deleted.
<b>In Use</b>	Indicates whether or not the selected role is currently being used by any other Network Sentry element. See <b>Role In Use</b> on page 620.
<b>Modify</b>	Opens the Modify Role window for the selected role.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446 <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243

### Add A Role

Once you have created and configured the host, user and device groups, create the roles associated with these groups.



The screenshot shows a dialog box titled "Add Role". It has a close button in the top right corner. The dialog contains three text input fields: "Name" with the text "Accounting", "Groups" with the text "DistGroup", and "Note" with the text "Group of district owned hosts.". To the right of the "Groups" field is a "Select..." button. At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 226: Add Role

1. Select **Policy > Roles**.
2. Click **Add** at the bottom of the Roles View.
3. In the **Name** field, enter a name for the new role. If this role corresponds to an LDAP attribute value, the spelling of the role name must be an exact match for the data contained in the user's directory record and you do not need to select a group in the Groups field.
4. Click the **Select** button next to the Groups field. Choose one or more user or host groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.  

If you are creating a role that you do not want to have automatically assigned, but wish to assign manually or through the captive portal, then do not enter any groups.
5. Click in the **Note** field to add any user defined information needed for this role.
6. Click **OK** to save the role.
7. If this role will be used to control network access for hosts managed in Topology View and devices, go to the Network Device Roles View and configure the role mapping there.

### Modify Or Delete Role From Database

You can modify the role settings as needed. All devices, users and hosts in the database are required to have a role. You cannot remove a role from these elements. You can only change the role to something else. If no role is specified devices, users and hosts default to the NAC Default role.

If a role is in use by a Device Profiling Rule, Guest Template or assigned to a Host, User, or Device, the role cannot be removed from the database. If a role is simply mapped to a device based on the device's membership in a group and not assigned specifically to the device, the role can be removed.

1. Select **Policy > Roles**.
2. Select the role from the list.
3. **To remove the role from the database**, click the **Delete** button.
4. On the confirmation window, click **Yes** to remove the role.
5. If the role is in use, a warning message is displayed and the role is not deleted. Click the **In Use** button for a complete list of places where this role is referenced.
6. **To modify the role**, click the **Modify** button.
7. Modify settings as needed and click **OK** to save.

## Role In Use

To find the list of Network Sentry features that reference a role, select the role from the Roles View and click the **In Use** button. A message is displayed indicating whether or not the role is associated with any other features. If the role is referenced elsewhere, a list of each feature that references the configuration is displayed. A role can be used in the following locations:

- Network Device Roles
- Hosts
- Users
- Devices
- Device Profiling Rules
- Vendor OUIs
- Guest Templates
- Scheduled Tasks with an action of "Role Assignment"
- Event to Alarm Mappings with an Action of "Host Role Action"

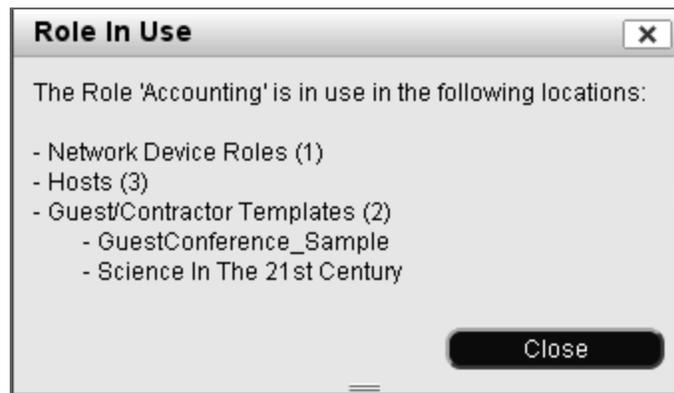


Figure 227: Role In Use





## Chapter 15: Guest Manager

Your enterprise may occasionally need to augment staff with contractors for short term projects. More often, you need to provide controlled network access for guests or remote attendees of conferences. Guest Manager meets these demands by providing you with a set of tools to create limited network accounts for Guests and Contractors that are secure, role-based and provide access for a specified time period. Guest Manager allows you to:

- Control the point of access for guests and contractors.
- Manage guest and contractor authorization.
- Ensure that guests and contractors receive the appropriate network resources for the amount of time the services are needed.
- Provide IT staff with control and tracking capabilities.
- Provide administrative accounts that allow non-IT staff to create accounts and manage accounts for visiting users.

You must have a license for the Guest Manager feature. You must be sure to have enough Concurrent Licenses to provide a connection to the network for each guest. When a host connects to the network it uses one Concurrent license. The license is released as soon as that host disconnects from the network. See **License Types And Usage** on page 8 for additional information.

**Important:** If you have not purchased a Guest Manager license you will not be able to create Guest/Contractor accounts.

When guests or contractors enter their temporary user name, password, and other required information, Guest Manager checks the credentials against the guest or contractor account. Guest Manager denies access if the credentials do not match the entries in the Guest Manager database or LDAP directory, depending on which is being used for guest or contractor authentication. In addition, guests and contractors can be scanned to ensure that they have up-to-date anti-virus software and pose no threat to the network.

## Guest Manager Implementation

Guest Manager is implemented at several levels. The initial setup is done by a Network Sentry administrator. Guest and Contractor Accounts are created and managed by an administrative user called a sponsor. Finally, Guests and Contractors themselves follow a login process. The initial setup of Guest Manager can be done using the Quick Start wizard under System > Quick Start. This section of the documentation outlines the implementation process in the order in which it should be done if you are implementing Guest Manager without using the wizard or enabling additional features not configured by the wizard.

**Important:** If you have not purchased a Guest Manager license you will not be able to create Guest/Contractor accounts.

### Administrator

Administrators have full rights to all parts of the Network Sentry system and can fully implement Guest Manager without needing a sponsor user to create accounts. However, in most organizations these responsibilities are divided up.

- Make sure that e-mail settings for your Network Sentry server or control server have been configured. If they are not configured you will not be able to send email to guests with their account credentials. See **Email Settings** on page 125.
- If you intend to use Endpoint Compliance Policies and scan guest/contractor's computers, set up the policies before creating templates. See **Assign An Endpoint Compliance Policy To A Guest** on page 641 and **Endpoint Compliance Policies** on page 525.
- Each guest account that is created must be associated with a template that controls configuration details about that account, such as, how long the account is valid or when the guest can access the network. Guest account types include Guest, Contractor, Conference and Self-Registered Guest. See **Guest/Contractor Templates** on page 626.
- Guest Manager templates allow you to limit guest access to the network based on time of day or day of week. During the time that the guest is not allowed to access the network it is marked "At Risk" for the Guest No Access admin scan. If you choose to implement this feature for any template, the following requirements must be met:
  - You must have a quarantine or remediation VLAN on your network.
  - Ports through which a guest would connect must be in the Forced Remediation Group (applies only to wired ports). See **Groups View** on page 681.
  - The Model Configuration for all switches to which guests connect must have an entry for the Quarantine VLAN. This applies to both wired and wireless switches and access points.

- Admin User Profiles control what administrative users can do when they are working in Network Sentry. If you intend to have an administrative user create and manage guest accounts you must create an Admin User Profile to provide that user with the appropriate permissions. Sponsors profiles determine whether the sponsor can manage Guest accounts, Kiosk Accounts or Self-Registered Guest accounts. See **Administrative User Profiles For Guest Manager** on page 644.
- Create any administrative users or sponsors that will be responsible for creating and managing guests. See **Add An Admin User For Guest Manager** on page 653. Administrative users can also be created and associated with an Administrative User Profile automatically based on users and groups in your Directory. See **Set Admin Privileges Based On Directory Groups**.
- To force guests and contractors to register and/or authenticate when they connect to the network, the ports to which they connect must be in a controlled access group such as Forced Registration.
- When guests or contractors connect to the network they are presented with a registration page. This page can be set up either by editing the existing registration pages directly (Portal V1) or using the Portal Configuration Content Editor (Portal V2). If you plan to use the Guest Self-Registration feature, you must use the portal pages distributed with Network Sentry (Portal V2).
- If you would like to provide guests with badges containing their login credentials, you must make sure the printer is set up correctly. See **Printer Settings For Guest Contractor Badges** on page 656.
- If you would like to send guests their login credentials via an SMS message, enable any necessary Mobile Providers. See **Mobile Providers** on page 130. For guest account type Self-Registered Guest, SMS messages are enabled by default and requires that you enable Mobile Providers.
- If you decide to use Network Access Policy features of Network Sentry you must configure User/Host Profiles that correspond to guests. Then map a User/Host Profile to a Network Access Configuration using a Network Access Policy.

### **Sponsor**

Sponsors have the following responsibilities. Administrators can perform these functions also.

- When all of the preliminary setup steps have been completed, either the Sponsor or the Administrator can create guest/contractor accounts. See **Guest Or Contractor Accounts** on page 660.
- If Self-Registration Requests permission has been granted, sponsors can also approve or deny account requests for accounts from guests using the Self-Registration feature.
- To facilitate your guests connection to the network you must give them information about their login credentials. See **Provide Account Information To Guest Or Contractor** on page 671.
- If you are managing a large group of guests or contractors, you can use the Locate feature to find and manage guests. See **Locate Hosts/Users** on page 49.

Sponsors with management permissions in their Admin Profile can locate guests, contractors, registered hosts, and other sponsors.

Sponsors who are limited in their Admin User Profile to managing their own hosts, can not search for any other hosts. See **Administrative User Profiles For Guest Manager** on page 644. The Sponsor field in the Locate screen is automatically filled in with the sponsor's name and can not be changed.

### **Guest/Contractor**

- **Guest Or Contractor Login** on page 679

### **Other Guest Manager Features**

- Guest Self- Registration
- Guest Manager Reports
- **Guest Manager Events And Alarms** on page 657

### **Guest/Contractor Templates**

Admin Users can be accessed from **Users > Guest/Contractor Templates**.

As an administrator, you control Guest, Contractor, Conference and Self-Registration accounts by creating templates for each account type. The templates include privileges you specify, such as account duration, and credential requirements. Each time a visitor account is created one of these templates must be applied.

The templates you define:

- Restrict or allow certain privileges for the sponsors who create guest, contractor, and conference accounts.
- Ensure that sponsors set up appropriate accounts for guests and contractors.
- Define the number of characters in the automatically generated passwords.

- Make sure data from the guest or contractor is provided to the sponsor.

You may grant sponsor privileges to an administrative user who uses the templates to create and manage temporary guest and contractor accounts. Sponsors may also provide account details to guests by email, sms message or printout. The entire process, from account creation to guest network access, is stored for audit and reporting.

From the Guest/Contractor Templates window you can add, delete, modify or copy templates.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Visitor Type	Authentication	Login Availability	Password Length	Password Exclusions	Account Duration	Reauth Period	Last Modified By
Yes	GuestSelfRegistration	Self Registered Guest	Local	Always	6	!@#%&'()*_+-{} ~"':;<=>?`-:=	24 hours		SYSTEM
Yes	GuestAccess	Guest	Local	Always	8	!@#%&'()*_+-{} ~"':;<=>?`-:=			SYSTEM
Yes	GuestConference	Conference	Local	Always	8	!@#%&'()*_+-{} ~"':;<=>?`-:=			SYSTEM

Figure 228: Create Guest/Contractor Template Window

### Guest/Contractor Template Fields

Field	Definition
<b>Global</b>	
<b>Name</b>	Descriptive name for the template. Sponsors use this name when they select a template to create accounts.
<b>Visitor Type</b>	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See <b>Guest Account Types Or Visitor Types</b> on page 631.
<b>Role</b>	<p>Role is an attribute added to the user and the host. Roles can be used in User-/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it.</p> <p>See <b>Guest Account Types Or Visitor Types</b> on page 631. For more on Roles see <b>Role Management</b> on page 609.</p>

Field	Definition
<b>Authentication</b>	<p>Indicates type of authentication used for Guests or Contractors associated with this template. Options include:</p> <p><b>Local</b>—User name and password credentials are stored in the local database.</p> <p><b>Note:</b> For Conference accounts, authentication is Local only.</p> <p><b>LDAP</b>—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.</p> <p><b>RADIUS</b>—Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.</p>
<b>Login Availability</b>	<p>Indicates when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are:</p> <ul style="list-style-type: none"> <li>• Always</li> <li>• Time range</li> </ul> <p>Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.</p>
<b>Password Length</b>	<p>Required length of guest or contractor passwords. Must be between 5 and 64 characters.</p>
<b>Account Duration</b>	<p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>
<b>Reauth Period (hours)</b>	<p>Number of hours the guest or contractor can access the network before reauthentication is required.</p>
<b>Security &amp; Access Value</b>	<p>User specified text associated with guests created using this template that can be used as a filter. Used to assign a policy to a guest by filtering for this value.</p>
<b>Password Exclusions</b>	<p>List of characters that will not be included in generated passwords.</p>
<b>Last Modified By</b>	<p>User name of the last user to modify the template.</p>

Field	Definition
<b>Last Modified Date</b>	Date and time of the last modification to this template.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Import</b>	<p>Enables you to import information from the Network Sentry Server(s) to the FortiNac Control Managers so that during the next Global Synchronization (if enabled), the information will be written to other Network Sentry Servers in your network. This eliminates the need to manually enter the information on the FortiNac Control Manager. When it is imported to the FortiNac Control Manager, the information is treated as global information.</p> <p>The following describes some caveats to consider when importing items:</p> <p>If the name of an item that is being imported already exists on the FortiNac Control Manager, the item will not be imported.</p> <p>If an item being imported from a Network Sentry Server has a dependent item with the same name as a dependent item that already exists on the FortiNac Control Manager, the dependent item is not imported to the FortiNac Control Manager. The item will be imported and use the dependent item that already existed on the Network Sentry Control Manager.</p> <p>For example, if a User/Host Profile called "Student" exists on the FortiNac Control Manager and an Endpoint Compliance Policy is imported from a Network Sentry Server that also uses a User/Host Profile called "Student", the "Student" Profile (dependent item) that exists on the FortiNac Control Manager will not be imported. The Endpoint Compliance Policy will be imported and use the dependent item (User/Host Profile) that was already there. This results in the settings for the Network Sentry Control Manager's Endpoint Compliance Policy's User/Host Profile possibly differing from the Endpoint Compliance Policy's User/Host Profile on the FortiNac Control Manager.</p>
<b>Export</b>	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.
<b>Copy</b>	Copy the selected Template to create a new record.
<b>Delete</b>	Deletes the selected Template. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.
<b>Modify</b>	Opens the Modify Guest/Contractor Template window for the selected template.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Used By</b>	Display a list of users by Admin Profile that are associated with the selected template. Click on a specific Admin Profile to see the associated users. To select more than one profile use the Ctrl key.

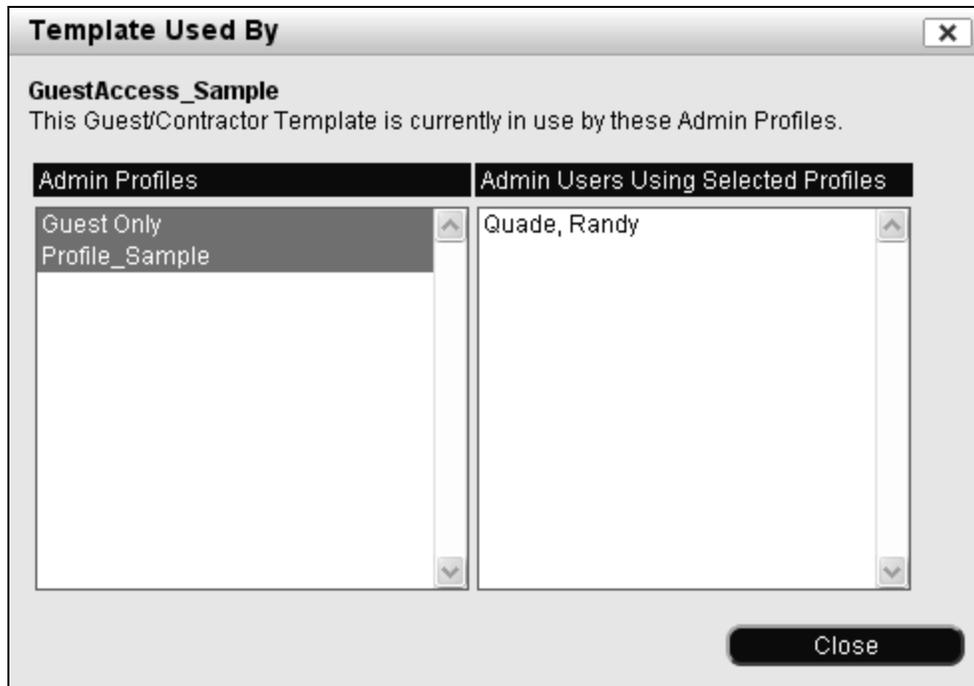


Figure 229: Guest/Contractor Template Used By

## Guest Account Types Or Visitor Types

Guest Manager supports four basic types of accounts. They are identified on the Guest templates as Visitor types and are loosely defined as follows:

**Guest**—A visitor to your facility with limited or Internet-only network access. For example, a guest might be on the premises for a one-day sales call or a three-day presentation. Any number of guest accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

**Self-Registered Guest**—A visitor to your facility with limited or Internet-only network access who connects to your network on their own device to request a temporary account. The account request goes to a sponsor via e-mail. The sponsor can log into Network Sentry and approve or deny the request or, depending on your configuration, can approve or deny the request for the account directly from the e-mail. The account is created when the request is approved.

**Conference**—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. Conferences are often bulk accounts, in which attendees receive notification of the conference via, for example, email. Conference members may be given an identical generated user name and password that is specific to the conference—for example, *conference-1* or *training123*, individual passwords for individual attendees, or individual attendee names with a shared password. See **Conference Accounts** on page 673. When the conference members register they enter their email address. Once they have registered, they fill in their name and other information.

**Contractor**—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months. Any number of contractor accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

### Create Guest/Contractor Templates

Use this option to create multiple templates for each of the Guest, Contractor, Conference and Self-Registered Guest visitor types with a variety of permissions. Data fields allow you to collect data from your guests and store it in User Properties. If you are a Network Sentry administrator you have access to all templates and can assign any template of the correct type to any guest, contractor or conference user when you create their accounts. If you choose to create a sponsor user who is responsible for creating visitor accounts, the sponsor must be assigned a set of templates through the Admin Profile. When the sponsor creates visitor accounts, he can only choose templates from the list you have assigned.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Templates window appears. Click **Add**.
4. The **Add Guest/Contractor Template** window appears. Enter the information in the **Required Fields** tab as described in **Guest/Contractor Template Required Fields** on page 634.
5. Click the **Data Fields** tab to determine which fields will be required when a guest logs onto the network.
6. Click the **Note** tab to add a note to the printed access information to give the guest/contractor special login instructions or an SSID. See **Provide Account Information To Guest Or Contractor** on page 671.
7. Click **OK** to create the template and add it to the list of templates.

**Add Guest/Contractor Template** ✕

Required Fields | Data Fields | Note

Template Name:

Visitor Type:  ▼

Role:  Use a unique Role based on this template name  
 Select Role:  ▼

Security & Access Value:

Username Format:   Send Email  Send SMS

Password Length:

Password Exclusions:

Reauthentication Period:  (hours)

Authentication Method:  ▼  Account Duration:  (hours)

Login Availability:  ▼

URL for Acceptable Use Policy (optional)   IP Address of URL

[Portal Version 1 Settings](#)

Figure 230: Guest/Contractor Template - Required Fields Tab

**Guest/Contractor Template Required Fields**

All possible fields are included in this table. The fields shown on your screen will vary depending on the Visitor Type you select.

Field	Definition
<b>Template Name</b>	Type a descriptive name for the template. Sponsors use this name when they select a template to create accounts.
<b>Visitor Type</b>	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See <b>Guest Account Types Or Visitor Types</b> on page 631.
<b>Use A Unique Role Based On This Template Name</b>	Creates a role based on the template name and assigns that role to guests with accounts created using this template. Using the template name as a role allows you to limit network access based on the Guest Template by using the new role as a filter in a User/Host Profile. See User/Host Profiles on page 511.  When using the Wireless Security feature to configure SSID mappings, the name of the Guest Template selected is used to create the appropriate User/Host Profile allowing you to limit SSID access based on Guest Template.
<b>Select Role</b>	Role is an attribute added to the user and the host. Roles can be used in User-/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it.  See <b>Guest Account Types Or Visitor Types</b> on page 631. For more on Roles see <b>Role Management</b> on page 609.
<b>Security &amp; Access Value</b>	Enter a value, such as, Guest or Visitor. This field is added to each guest user account that is created based on this template and can be used as a filter. When creating User/Host Profiles, you can filter for the contents of the Security & Access Value field to control which Endpoint Compliance Policy is used to scan guest hosts.
<b>Send Email</b>	For Conference accounts, email cannot be sent until a guest has registered or you have modified the account via the <b>User View &gt; Modify</b> option to enter an email address.  Select this check box if you want a sponsor with this template to be able to send an e-mail confirmation to the guest's/contractor's email address. If not selected (default) guest or contractor credentials need to be printed or sent via SMS.  For Self-Registered Guest accounts this option is automatically checked and cannot be disabled.

Field	Definition
<b>Send SMS</b>	<p>For Guest or Contractor accounts, select this check box if you want a sponsor with this template to be able to send an SMS confirmation to the guest's/contractor's mobile phone. If not selected guest or contractor credentials need to be e-mailed or printed.</p> <p>For Self-Registered Guest accounts this option is automatically checked and cannot be disabled.</p> <p>Requires that the guest or contractor provide both a mobile number and the mobile provider. These fields default to Required in the Data Fields tab.</p>
<b>Max Number Of Accounts</b>	<p>Only available when Visitor Type is set to Conference. Typically used when generating a large number of accounts for a conference. Limits the total number of accounts that can be created on the Conference Account window when this template is selected.</p> <p>To limit accounts, enable the check box and enter the maximum number of accounts that can ever be created using this template.</p> <p>For an unlimited number of accounts, leave the check box empty.</p>
<b>Password Length</b>	<p>Between 5 and 64 characters. Passwords that are automatically generated by Guest Manager contain at least one capital letter, one lower case letter, one alphanumeric character, and one symbol. If you have characters listed in Password Exclusions, those characters will not be used.</p> <p>Note that for Conference accounts, once a template has been created, the sponsor may specify the individual different passwords for attendees when the sponsor creates the conference account. See <b>Conference Accounts</b> on page 673.</p> <p><b>Note:</b> Network Sentry does not recognize or restrict system-generated passwords that may be offensive.</p>
<b>Password Exclusions</b>	List of characters that will not be included in generated passwords.
<b>Use Mobile Friendly Exclusions</b>	<p>Removes any existing entries and then populates the Password Exclusions field with a list of symbols that are typically difficult to enter on a mobile device. Modify the list of characters as needed. Characters include:</p> <p>!@#\$\$%^&amp;*()_+~{ :"&lt;&gt;?.-=[]\';/</p>
<b>Reauthentication Period (hours)</b>	Specify the number of hours the guest or contractor can access the network before reauthentication is required. To specify a reauthentication period you must first select the check box. Next fill in the reauthentication period in hours. If you do not select this check box, you will not have to specify a reauthentication period for guests or contractor accounts created with this template.

Field	Definition
<p><b>Authentication Method</b></p>	<p>Specify where authentication occurs:</p> <p><b>Local</b>—User name and password credentials are stored in the local database.</p> <hr/> <p><b>Note:</b> For Conference accounts, authentication is Local only.</p> <p><b>LDAP</b>—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor’s credentials are accepted and they are granted access.</p> <p><b>RADIUS</b>—Checks your RADIUS server for the email address (required) in the user’s created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor’s credentials are accepted and they are granted access. PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from Network Sentry, such as the user name and password for the Validation Account used for communication between Network Sentry and the RADIUS server.</p> <p>If you are using an integrated RADIUS server and Authentication Method is set to RADIUS, single guest accounts created using this template will also generate a RADIUS User record in the RADIUS Users view.</p>
<p><b>Account Duration</b></p>	<p>Select the check box to specify the duration of the account in hours.</p> <p>For all guests except those with shared conference accounts: The duration governs how long from creation the account remains in the database, regardless of the end date that is entered when creating the guest account.</p> <p>For shared conference accounts: The duration governs how long from guest Login the account remains in the database, regardless of the end date that is entered when creating the conference.</p> <p>For Self-Registered Guest accounts this option is automatically checked and cannot be disabled. You must enter a duration.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

Field	Definition
<b>Propagate Hosts</b>	Controls whether the Propagate Hosts setting is enabled or disabled on the user record for guest users created with this template. If enabled, the record for the host owned by the guest user is copied to all managed Network Sentry appliances. This field is only displayed if the Network Sentry server is managed by a FortiNac Control Manager.
<b>Login Availability</b>	Select when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration.  The available options are: <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify Time: If you select this option, a window displays in which you specify the time range and select the days of the week. Click OK.</li> </ul> Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
<b>URL for Acceptable Use Policy</b>	Optional. Directs the guest or contractor to the page you specify with the network policies when they login.
<b>Resolve URL</b>	Click to acquire the IP addresses for the URLs for Acceptable Use Policy and Successful Landing page. If the URL is not reachable, specify the IP Address in the IP Address field.
<b>Portal Version 1 Settings</b>	
<b>URL for Successful Landing Page</b>	Directs the guest or contractor to a certain page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.  If you are using the portal pages included with Network Sentry and controlled by the Content Editor in the Portal Configuration, this field is ignored.

### Login Availability Time For A Guest Template

This option allows you to limit network access for a guest or contractor based on the time of day and the day of the week. Any guest associated with a template, can only access the network as specified in the Login Availability field for the template.

If you set times for Login Availability, Network Sentry periodically checks the access time for each guest associated with the template. When the guest is not allowed to access the network the host associated with the guest is marked "At Risk" for the Guest No Access admin scan. When the time is reached that the guest is allowed to access the network, the "At Risk" state is removed from the host. These changes in state occur on the guest host record whether the guest is connected to the network or not. If the guest host connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your Network Access has been disabled. You are outside of your allowed time window. To regain network access call the help desk."

**Add Guest/Contractor Template**

Required Fields | Data Fields | Note

Data Field	Guest/Contractor
First Name	Required ▼
Last Name	Required ▼
Address	Required ▼
City	Required ▼
State	Required ▼
Country	Required ▼
Zip/Postal Code	Required ▼
Email	Required
Phone	Required ▼
Mobile Number	Required ▼
Mobile Provider	Required ▼
Asset	Required ▼
Person Visiting	Required ▼
Reason	Required ▼

Add Field | Delete Field | Reorder Fields

OK | Cancel

**Figure 231: Guest/Contractor Template - Data Fields Tab**

### Guest/Contractor Data Fields

Specify which pieces of data will appear on the form the guest or contractor will be required to fill out in the captive portal. For Self-Registered Guests this information is filled out with the request for an account. For Guests with an existing account, this information is filled out after they enter their user name and password on the login page. If the field has a corresponding database field, it is stored there and displayed on the User Properties window. If the field does not have a corresponding database field, it is stored and displayed in the Notes tab of the User Properties window and the Host Properties window. Hover over the field name to display a tool tip indicating where the data entered by the guest will be stored.

- **Required**—The data in this field must be entered in order for the guest or contractor to log in.
- **Optional**—Appears on the form, but is not required data from the guest or contractor.
- **Ignored**—Will not appear on the form.

The E-mail Field is required. The fields listed below are default fields that are included with the original setup of Guest Manager. Field names can be modified by typing over the original name. Therefore, the fields on your template window may not match any of the fields in this list. If you rename a field, the data entered into that field by the guest is still stored in its original location. For example, if you modify the title of the Last Name field to say Mother's Maiden Name, the data is still stored in the Last Name field on the User Properties window.

Original Field Name	Definition
<b>Last Name</b>	Maximum length 50 characters. Stored in the Last Name field.
<b>First Name</b>	Maximum length 50 characters. Stored in the First Name field.
<b>Address</b>	Maximum length 50 characters. Stored in the Address field.
<b>City</b>	Maximum length 50 characters. Stored in the City field.
<b>State (or Province/County)</b>	Standard two-letter state abbreviation, or up to 50 characters. Stored in the State field.
<b>Country</b>	Maximum length 50 characters. Stored on the Notes tab.
<b>Zip or Postal Code</b>	Maximum length of 16. Stored in the Zip Code field.
<b>Email</b>	Email address of the guest or contractor. Stored in the E-mail field.  <b>Important:</b> This field can be modified however Network Sentry expects the contents of the field to be an email address. This field tests for a valid email address and will not allow the user to proceed without one. If the label is something other than email and other types of data are entered, the guest account may not be able to be created.
<b>Phone</b>	Telephone number including international country codes (for example, +1, +44). Maximum length 16. Stored in the Phone field.
<b>Mobile Phone</b>	Mobile Telephone number. Maximum length 16. Stored in the Add/Modify User window.
<b>Mobile Provider</b>	The name of the company that provides the guest with Mobile service. The guest is provided with a list of possible providers. Stored in the Add/Modify User window.
<b>Asset</b>	Text field for computer serial numbers, manufacturer's name and model number, or any other asset identifier of the guest's or contractor's computing platform. Stored in the Serial Number field. Max.length 80 characters.

Original Field Name	Definition
<b>Reason</b>	The reason for the guest's or contractor's visit. Max. length 80 characters. Stored on the Notes tab.
<b>Person Visiting</b>	Maximum length 50 characters. Stored on the Notes tab.
<b>Buttons</b>	
<b>Add Field</b>	<p>Click to add new data fields to track additional guest or contractor data, such as license plate numbers or demo equipment details. Maximum length 80 characters.</p> <p>Type the name of the field in the pop-up window. Select whether to make the field required or optional.</p> <p>Once new fields have been added they are stored in the Notes tab of the user's account. To see these fields go to the User Properties window.</p>
<b>Delete Field</b>	Click this button to delete a data field from the list. Only those fields that have been created by an Admin user can be deleted. System fields can be set to ignore so they do not display, but cannot be deleted from the template.
<b>Reorder Fields</b>	Changes the order of the fields as they appear in the Guest or Contractor Form. Click this button to reorder account information fields. In the pop-up window, click Move Up or Move Down and OK.

### **Guest/Contractor Note**

The Notes tab on the template creation window allows you to provide additional information to guests and contractors. After you have created a Guest or Contractor account, you may want to provide that user with his login information. Login information can be printed, viewed on the screen, sent via text message to a mobile telephone or included in an e-mail. The text added on the Notes tab is appended to the guest information included in the printout, email or text message. See **Provide Account Information To Guest Or Contractor** on page 671 for additional information.

## Assign An Endpoint Compliance Policy To A Guest

Endpoint Compliance Policies and the agents that run associated scans are assigned based on the rules contained within the Policy. Network Sentry selects a scan and an agent by comparing guest and host data to the User/Host Profile in each policy beginning with the policy ranked number 1 until a match is found. When a match is found the scan and agent are assigned and the guest's computer is scanned. If you want to create a specific policy for guests, you must define a policy that searches for user data that only guests will match and place it at the beginning of the list of policies.

### Example 1

In this example the policy will apply to guests based on their Role. Create a policy that has the following settings:

#### User/Host Profile

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Role and enter the name of the Role assigned to guests. Typically the Role is named Guest, but you may have chosen to use a different role for Guests. Roles are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

#### Scan

- **Scan** — Create a scan to evaluate guest computers for compliance.

#### Endpoint Compliance Configuration

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

#### Endpoint Compliance Policy

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

### **Example 2**

In this example the policy will apply to guests based on their Security & Access Value. Create a policy that has the following settings:

#### **User/Host Profile**

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Security & Access Value and enter the name of the Security & Access Value assigned to guests. These values are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

#### **Scan**

- **Scan** — Create a scan to evaluate guest computers for compliance.

#### **Endpoint Compliance Configuration**

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

#### **Endpoint Compliance Policy**

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

## Modify Templates

To change information or parameters in a template, do the following:

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Modify**. Change the name of the template, or other information and parameters.

**Note:** Once the template has been modified the modifications will only apply to new accounts created from the template. All old accounts made from the template remain the same.

5. Click **OK**.

## Copy Templates

You may copy a template, save it under another name, and use it as the basis for a new template.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Copy**.
5. Change the name of the template, or other information and parameters.
6. Click **OK**.

## Delete Templates

You may delete a template at any time. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.

1. Log into your Administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The **Guest/Contractor Template Management** window opens with a list of created templates.
4. Select the template and click **Delete**. A confirmation message is displayed. Click **Yes** to delete the template.

## Administrative User Profiles For Guest Manager

In Network Sentry, you can create an administrative user and give that user an Admin Profile that contains special permissions for the Guest/Contractor feature set. These privileges are designed to restrict this user to certain parts of the program. See **Admin Profiles And Permissions** on page 219.

For Guest Manager, this type of user is referred to as a Sponsor in documentation because that person sponsors incoming guests and contractors. Creating a Sponsor Admin Profile allows the user to manage guest, contractor, conference or Self-Registered Guest accounts. For more information on the types of accounts, see **Guest Account Types Or Visitor Types** on page 631.

Guest Manager supports multiple UPN formats (for example, @gcs.xyztech.com) so sponsors do not have to type their full user login name. As administrative users create guest or contractor accounts, their administrative login name within Guest Manager is added as a part of the guest or contractor record for reporting purposes.

Additional permissions can be given to Sponsors based on the parameters of their responsibilities. Create one or more Admin Profiles for these types of users. Sponsor Admin User Profiles determine whether the sponsor can manage Guest accounts, Kiosk Accounts or Self-Registered Guest accounts. See the following for additional information:

**Add A Guest Manager Admin User Profile** on page 645

**Add A Kiosk Admin Profile** on page 648

**Add A Guest Self Registration Admin Profile** on page 651

## Add A Guest Manager Admin User Profile

This procedure describes how to create a specific Admin User Profile for an administrative user with permissions for Guest Manager. As a sponsor, the administrative user can create guest or contractor accounts. For details on all of the options that can be include in an Admin User Profile see **Add An Admin Profile** on page 243.

If an Admin User Profile has Kiosk Mode enabled, the corresponding user can only log into the Kiosk computer to make it available to arriving guests. That user cannot create accounts. You may need to create a sponsor who can manage accounts and a second sponsor to use for the self-service Kiosk. See **Add A Kiosk Admin Profile** on page 648

**Figure 232: Add Admin Profile - Manage Guests Tab**

To create an Admin User Profile you must first be logged into your Administrator account. Follow the steps below to add an Admin User Profile for an Administrative User that is considered a Sponsor for incoming guests:

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Guest Sponsor.

4. Under **Manage Hosts and Ports** select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
7. The minimum that this sponsor must have is the **Guest/Contractor Accounts** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Guest/Contractor permission set, the Landing Page field defaults to Guest Contractor Accounts.
9. In addition you may want include Self Registration Requests, which allow a Sponsor to Allow or Deny guest access to a user who has registered through the captive portal. This is not required.
10. The Manage Guests tab is enabled when Custom is selected for the Guest/Contractor Accounts permission set. Click on the **Manage Guests** tab.
11. Use the field definitions below to configure the Guest Manager specific fields.
12. Click **OK** to save.

### Custom Manage Guests Tab Fields

Field	Definition
<b>Guest Account Access</b>	<p>You can give Administrative Users with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts.</p> <p>The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports.</p> <p><b>No</b>—Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts.</p> <p><b>Own Accounts</b>—Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts.</p> <p><b>All Accounts</b>—User can see all Guest accounts in the database, send credentials to guests and modify or delete any guest accounts.</p>
<b>Account Types</b>	<p><b>Individual</b>—Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it.</p> <p><b>Bulk</b>—Sponsors may create multiple accounts with unique passwords by importing a bulk account file.</p> <p><b>Conference</b>—Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.</p>
<b>Create Accounts Days in Advance (Maximum)</b>	<p>The maximum number of days in advance this sponsor is allowed to create accounts.</p>
<b>Create Accounts Active For Days (Maximum)</b>	<p>Determines the length of time the guest account remains active in the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

Field	Definition
<b>Allowed Templates</b>	Indicates whether the Administrative User can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include:  <b>All Templates</b> —Profile gives the Administrative User access to all templates in the database when creating guest accounts.  <b>Specify Templates</b> —Profile gives the Administrative User access to the templates listed in Selected Templates.
<b>Specify Templates</b>	Allows you to select guest/contractor templates available for Administrative Users with this Admin User Profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column.  If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
<b>Available Templates</b>	Shows the templates that have not been selected to be included in this Admin User Profile.
<b>Selected Templates</b>	Shows the templates selected to be included in this Admin User Profile.
<b>Add Icon</b>	Click this button to create a new Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.
<b>Modify Icon</b>	Click this button to modify the selected Guest/Contractor template.  For information on templates, see <b>Create Guest/Contractor Templates</b> on page 632.

### Add A Kiosk Admin Profile

A kiosk allows visitors to your facility to create their own account. Guests have a maximum of 24 hours of access to your network, which may be only during certain hours of the day, or a pre-defined number of hours from when they log on. Guests may simply be queried for pre-defined contact data. In any case, at 11:59 PM each day, or after the allowed number of hours has elapsed, kiosk guest accounts expire.

**Note:** All other profile options are disabled if Kiosk Mode is enabled, because guests creating their own accounts would not need access to other options.

For added security, sponsors should use a kiosk browser. Kiosk browsers block users from accessing other programs on the machine or other web sites.

This procedure describes how to create a profile that gives a sponsor permission to manage a kiosk. A sponsor with Kiosk Mode enabled cannot access any of the regular Network Sentry windows. That user can log in to display the Guest Login web page and make it available on the Kiosk PC.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Kiosk Sponsor.
4. Use the table of field definitions below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Click on **Enable Guest Kiosk** to mark it with a check mark.
7. In the **Kiosk Template** field select a Guest/Contractor Account template. All guest accounts created through the Kiosk will use this template.
8. In the **Kiosk Welcome Text** field type the message that a guest will see when they create a guest account through the Kiosk.
9. Click **OK** to save.

The screenshot shows a dialog box titled "Add Admin Profile" with a close button (X) in the top right corner. The "General" tab is selected. The fields are as follows:

- Name: Kiosk Sponsor
- Logout After: 60 minutes of inactivity
- Login Availability: Always
- Manage Hosts and Ports: All
- Note: (empty text area)
- Enable Guest Kiosk
- Kiosk Template: Art Fair
- Kiosk Welcome Text: Welcome to the Art Fair! Click Start to create your guest account.

At the bottom right, there are "OK" and "Cancel" buttons.

Figure 233: Add Kiosk Profile

### Admin Profile Fields For Kiosk Sponsors

Field	Definition
<b>Name</b>	Enter a name that describes the profile, such as Kiosk Sponsor.
<b>Logout After</b>	User is logged out after this amount of time has elapsed without any activity in the user interface.
<b>Login Availability</b>	Specify when this sponsor can log into the network: <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify time</li> </ul> <p>The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.</p>
<b>Manage Hosts And Ports</b>	Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users. <p>Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in Network Sentry. Typically, this type of user would ONLY have the Manage Hosts &amp; Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All.</p> <p><b>All</b>—All groups containing hosts and ports can be accessed.</p> <p><b>Restrict By Groups</b>—Enables the restriction of Administrative Users to specific hosts and ports.</p> <p>For an overview and additional setup information see Limit Admin Access With Groups on page 282.</p>
<b>Note</b>	User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry for an existing Admin Profile record.
<b>Enable Guest Kiosk</b>	If you enable this mode, sponsors can log into Network Sentry to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. <p>Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.</p>
<b>Kiosk Template</b>	Select a Kiosk template for this sponsor. All visitors who use the self-service Kiosk when this sponsor is logged in will be assigned this template.
<b>Kiosk Welcome Message</b>	Enter the message that will appear when the kiosk user creates a guest account.

## Add A Guest Self Registration Admin Profile

Guest Self-Registration allows visitors to request a temporary or guest account from their own device. A sponsor receives an email indicating that a request has been received from a guest. The sponsor responds to the request by approving or denying it. Sponsors with the Guest Self Registration Admin Profile or with a Guest Manager Admin Profile and Administrators can respond to a Self-Registration request from a guest.

Anyone in your organization can be a sponsor for Guest Self-Registration. They must be entered into Network Sentry as an Administrative User and that user account must have a Guest Self-Registration Admin Profile applied. You can quickly create Sponsors by using Directory Groups.

Guests can access your network for the length of time specified by the Account Duration. Availability can be 24 hours a day or limited to specific hours during the day.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Self-Registered Guest Sponsor.
4. Use the table of field definitions below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Leave the defaults for the remaining fields and click on the **Permissions** tab.
7. On the Permissions tab note that some permissions are dependent on each other. Refer to the **Permissions List** on page 230 for additional information.
8. The minimum that this sponsor must have is the **Self Registration Requests** permission set. Select all of the check boxes for this set.
9. When you select the Self Registration Requests permission set, the **Landing Page** field defaults to Self Registration Requests.
10. Click **OK**.

### Admin Profile Fields For Self Registered Guest Sponsors

Field	Definition
<b>Name</b>	Enter a name that describes the profile, such as Kiosk Sponsor.
<b>Logout After</b>	User is logged out after this amount of time has elapsed without any activity in the user interface.

Field	Definition
<p><b>Login Availability</b></p>	<p>Specify when this sponsor can log into the network:</p> <ul style="list-style-type: none"> <li>• Always</li> <li>• Specify time</li> </ul> <p>The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.</p>
<p><b>Manage Hosts And Ports</b></p>	<p>Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users.</p> <p>Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in Network Sentry. Typically, this type of user would ONLY have the Manage Hosts &amp; Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All.</p> <p><b>All</b>—All groups containing hosts and ports can be accessed.</p> <p><b>Restrict By Groups</b>—Enables the restriction of Administrative Users to specific hosts and ports.</p> <p>For an overview and additional setup information see Limit Admin Access With Groups on page 282.</p>
<p><b>Note</b></p>	<p>User specified note field. This field may contain notes regarding the data conversion from a previous version of Network Sentry for an existing Admin Profile record.</p>
<p><b>Enable Guest Kiosk</b></p>	<p>Do not enable this field for the Self Registered Guest Admin User Profile.</p> <p>If you enable this mode, sponsors can log into Network Sentry to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser.</p> <p>Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.</p>

## Administrative Users For Guest Manager

When you create or modify an administrative user, you must attach an Admin User Profile to the account. Before adding Administrative Users to manage guests, create an Admin User Profile that contains the set of permissions that allow the administrative user to sponsor guest, contractor, or conference accounts. The profile limits the administrative user's access to Network Sentry features.

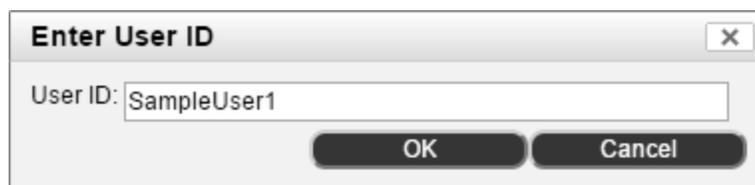
When an administrative user with an Admin Profile logs into Network Sentry, the system presents the views available based on the user's default permissions. You can configure administrative accounts to authenticate locally or externally via RADIUS or LDAP. If the administrative user cannot be authenticated, an error message specifying the problem displays.

### Add An Admin User For Guest Manager

If you are creating Admin Users to manage guests or devices, you must create an Administrative User who has the appropriate Admin User Profile associated. See **Admin Profiles And Permissions** on page 219.

1. Select **Users > Admin Users**.
2. Click the **Add** button.
3. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

This allows you to give a network user administrator privileges to help with some administrative tasks.



**Figure 234: Enter User ID**

4. Use the table of field definitions below to complete the information in the Add User dialog.
5. Click **OK** to save the new user.

**Add User** [X]

Asterisk (\*) indicates required fields.

**User Information**

\*Authenticate Type: Local [v]  
\*Admin Profile: Device Manager [v] [icon] [icon]  
\*User ID: johndoe \*Password: [password field]  
First Name: John \*Last Name: Doe  
Address: 55 Main Street  
City: Concord State: NH  
Zip/Postal Code: 03301 Phone: 603-555-1212  
Email: jdoe@bnetworks.com Title: Mr.  
Mobile Number: 603-848-1111  
Mobile Provider: Sprint (xxxxxxxxx@sprintpaging.com) [v]  
Notes: Works in Building B  
 User Never Expires

OK Cancel

Figure 235: Add Admin User

## Admin User Field Definitions

Field	Definition
<b>Authentication Type</b>	<p>Authentication method used for this Admin user. Types include:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> — Validates the user to a database on the local FortiNac appliance.</li> <li>• <b>LDAP</b> — Validates the user to a directory database. Network Sentry uses the LDAP protocol to communicate to an organization's directory.</li> <li>• <b>RADIUS</b> — Validates the user to a RADIUS server. If an integrated RADIUS server has been added under RADIUS Settings and the Authentication Type field is set to RADIUS, a RADIUS User record is automatically added to the RADIUS User's view for this user.</li> </ul> <p><b>Note:</b> Authentication of Admin Users via RADIUS is not currently available, however, Admin Users can still be created with the RADIUS authentication type for use on NetworkSentry pods.</p>
<b>Admin Profile</b>	<p>Profiles control permissions for administrative users. See Admin Profiles And Permissions on page 219.</p> <p><b>Add</b> — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window.</p> <p><b>Modify</b> — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.</p>
<b>User ID</b>	Unique alphanumeric ID for this user.
<b>Password</b>	<p>Password used for local authentication.</p> <p><b>Note:</b> If you authenticate users through LDAP, the password field is disabled and the user must log in with their LDAP password.</p>
<b>First Name</b>	User's first name.
<b>Last Name</b>	User's last name.
<b>Address</b>	Optional demographic information.
<b>City</b>	
<b>State</b>	
<b>Zip/Postal Code</b>	
<b>Phone</b>	
<b>E-mail</b>	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
<b>Title</b>	User's title, such as Mr. or Ms.

Field	Definition
<b>Mobile Number</b>	Mobile Phone number used for sending SMS messages to administrators.
<b>Mobile Provider</b>	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
<b>Notes</b>	Free form notes field for additional information.
<b>User Never Expires</b>	If enabled, Admin users are never aged out of the database. The default is enabled.  <b>Note:</b> Admin Users assigned the Administrator Profile cannot be aged out.

## Printer Settings For Guest Contractor Badges

In Guest Manager, administrative users you designate as sponsors can access guests' account credentials that show the user name, password, and access start time and end time. Sponsors may print the account details, e-mail them or send them via an SMS message directly to guests after account creation.

If sponsors managing guest kiosks or conferences need to print badges, contact your IT Manager to assure that printer settings are optimized for badge creation:

- Make sure the label printer is the default printer for kiosks.
- In the Printer Properties, Paper Options settings, set the paper label size to a minimum of 2" x 2-3/4" (5.1 cm x 7 cm).
- In the Page Handling Settings, make sure that Auto-Rotate is enabled to automatically adjust the orientation to fit the label's orientation on the sheet.
- Test to make sure that text is centered and fits on each label.

## Guest Manager Events And Alarms

Certain actions within Guest Manager generate events that appear in the Event Log. Examples of Guest Manager events are listed in the following table.

Event	Definition
<b>Conference Created</b>	Using Guest/Contractor Accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.
<b>Guest Account Created</b>	New guest account is created.
<b>Guest Account Deleted</b>	Guest account is deleted.

If certain event conditions occur, you are immediately informed of the condition through the alarm notification system. You can define and map additional events to alarms.

For more information on events and alarms, e-mail notifications, and how to map events to alarms see **Map Events To Alarms** on page 493.

## Use Guest Manager As A Sponsor

As a Guest Manager sponsor, you must log into Network Sentry to create guest or contractor accounts. Once logged in, the permissions defined by your administrator in your sponsor's Admin Profile are applied. Depending on the permissions, you could be presented with a **Locate** tab, a **Guest/Contractor Accounts** tab, a **View Reports** tab, or all three.

### Log Into Guest Manager As A Sponsor

You can access the sponsor privileges assigned to you only when you log into your account. As a sponsor, you can:

- Create and manage Guest, Contractor, and Conference accounts.
- Locate guests, contractors, and other sponsors.
- Sign-in to the kiosk you are in charge of to allow guests to create their own accounts for network access.

**Note:** Guest Sponsor users who sign in to the kiosk to prepare it for arriving guests have very limited permissions. If you are responsible for both the kiosk and managing Guest, Contractor and Conference accounts, you will need to have separate logins for each responsibility.

1. To log into Guest Manager, bring up a web browser and the following type in the URL:

```
http://<Hostname>:8080
```

This opens the Administrative User login screen.

2. Enter the username and password that was given to you by the administrator.
3. A screen with the end-user license agreement opens. To access your sponsor account, read the agreement and press **Accept**.
4. Based on your privileges, this screen will show a **Bookmarks** drop-down menu. From this menu you can select **Guest/Contractor Accounts** or **Locate** to locate hosts and users.

|

**Figure 236: Sponsor Account**

- To search for host or user records, click the **Locate** tab to open the **Locate** screen. See **Locate Hosts/Users** on page 49.
- As a sponsor you will typically want to create accounts for guest, contractors, and conference members before they arrive. To create and manage accounts, click **Bookmarks > Guest/Contractor** to open the **Create** screen. See **Guest Or Contractor Accounts** on page 660, **Create Bulk Or Multiple Accounts** on page 667, or **Conference Accounts** on page 673.
- To view reports of guest or contractor accounts and registrations, click the **View Reports** link at the top of the Guest/Contractor Accounts view. See View Guest Or Contractor Reports.

In addition to these privileges, Guest Manager Sponsor users may also have permission to manage a self-serve **kiosk** or to manage guest self-registration. The kiosk allows guests to create their own accounts for network access. The guest self-registration option allows guests to send a request for network access which can be approved or denied by the Sponsor. A Sponsor with permissions to manage a self-serve kiosk or guest self-registration, does not have permission to manage Guest, Contractor and Conference accounts. A user who is responsible for all of these types of guest account creation, must have a separate login for the Kiosk.

A kiosk is unique within Guest Manager. Once the sponsor's credentials for the kiosk have been entered, guests use the kiosk computer to create their own accounts. Network access is limited and there are generally time constraints.

## Guest Or Contractor Accounts

Guest Accounts allows you to create and manage guest or contractor accounts. To initially set up the accounts, access the Add Guest option and select a template set up by your administrator. Include the e-mail addresses of the guests or contractors as you create their accounts. You can then notify them of start times, required class materials, or other relevant information.

You may enter data specified as *Required* in the guest or contractor registration form, or you can let the guests and contractors enter the data themselves when they log into the portal. At that time, the required fields must be completed in order for the guest or contractor to log into the system.

Passwords are automatically generated when guest or contractor accounts are created. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the upper case letter I (eye), zero, upper or lower-case letter O. For Conference Accounts with shared passwords you have the option of creating your own password or generating one.

---

**Note:** Network Sentry does not recognize or restrict system-generated passwords that may be offensive.

---

If you have account management privileges in your Sponsor Admin Profile, you may change or remove information in an account. Depending on your privileges, you may be allowed to manage all created accounts or only your own accounts.

Guests also display on the User View. See **User View** on page 385 and **Guest Account Details** on page 676.

Guest/Contractor Accounts can be accessed from **Users > Guest/Contractor Accounts** or from **System > Quick Start > Authentication Settings**, however configuration steps point you to **Users > Guest/Contractor Accounts**.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

|

**Figure 237: Guest/Contractor Accounts Window**

### [Guest/Contractor Account Field Definitions](#)

Fields used in filters are also defined in this table.

Field	Definition
<b>View Reports</b>	Opens the Guest Accounts Report view. This option displays only when Guest/Contractor accounts is accessed from the Users menu. See View Guest Or Contractor Reports.
<b>Table Columns</b>	
<b>Enabled</b>	Indicates Guest account status. The account is either enabled (check mark) or disabled (x).
<b>Sponsor</b>	User name of the Administrator or Sponsor that created the guest account.
<b>Account Type</b>	<p>Guest account type. Types include:</p> <p><b>Guest</b>—A visitor to your facility with limited or Internet-only network access.</p> <p><b>Conference</b>—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days.</p> <p><b>Contractor</b>—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.</p>
<b>Name</b>	Guest's first and last name.
<b>User</b>	Guest's email account which is used as the User ID at login.
<b>Starting Start Date</b>	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
<b>Ending End Date</b>	Date and time the account will expire.
<b>Login Availability</b>	Times during which the guest is permitted to access the network.
<b>Role</b>	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.
<b>Authentication</b>	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.
<b>Security &amp; Access Value</b>	Attribute assigned to a guest that can be used as a filter. Common values are Guest, Contractor or Visitor.

Field	Definition
<b>Account Duration</b>	<p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>
<b>Reauth Period</b>	Number of hours the guest or contractor can access the network before reauthentication is required.
<b>Last Modified By</b>	User name of the last user to modify the guest account.
<b>Last Modified Date</b>	Date and time of the last modification to this guest account.
<b>Right Mouse Click Menu Options &amp; Buttons</b>	
<b>Delete</b>	To delete an account, select the account and click <b>Delete</b> . The account is deleted and will no longer show up in the created accounts window.
<b>Modify</b>	<p>Change information in an existing guest or contractor account. This option also allows you to reset the information and reenter it.</p> <p>To modify an account select the account you want to change and click <b>Modify</b>.</p> <p><b>Note:</b> Conference accounts cannot be modified.</p>
<b>Reset Password</b>	To reset an account password select the account and click <b>Reset Password</b> . The account password is automatically changed.
<b>View</b>	View additional account information such as passwords and guest or contractor phone numbers. Select an account and click <b>View</b> . This displays the Print, Send e-mail and Send SMS options for the selected account(s).
<b>Send Email</b>	Sends email to the selected guests containing their login information.
<b>Send SMS</b>	Sends a text message to the selected guests' mobile telephone containing their login information.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Select All</b>	Selects all guest accounts displayed in the table.

Field	Definition
<b>Enable/Disable</b>	Select the account and click <b>Enable/Disable</b> . The account status is changed. This is used to enable a Guest account if a guest were to arrive earlier than expected.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. This option displays only when Guest/Contractor accounts is accessed from the Users menu. See <b>Export Data</b> on page 383.

## Create Single Guest Or Contractor Accounts

Guest Manager allows Administrative Users with Sponsor Admin Profiles to create and manage guest or contractor accounts. This helps to:

- Free IT staff from the daily burden of creating accounts for visiting users.
- Ensure that guest and contractor accounts get created ahead of time so they do not have to wait for their accounts to be created when they arrive.

To set up accounts for guests or contractors before they arrive at your organization:

1. Log into your Sponsor account.
2. The Guest/Contractor Accounts window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add** to open a new screen.
4. Click **Single Account**. Enter the information described below in **Single Account Field Definitions** on page 664.

**Note:** E-mail address, start and end dates are required. Additional personal information about the guest or contractor is optional. If the additional personal information is blank, the guest or contractor is prompted to fill in those fields before logging into the network.

**Note:** If Send SMS is enabled in the template, then Mobile Number and Mobile Provider are also required to allow you to send a message to the guest's mobile telephone.

5. Click **OK**. The View Accounts screen opens with the account information in it. See **Provide Account Information To Guest Or Contractor** on page 671.
6. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See **Create Guest/Contractor Templates** on page 632.

Guests also display on the User View. See **User View** on page 385.

|

**Figure 238: Single Account**

### Single Account Field Definitions

Field	Definition
<b>Template</b>	Click the down arrow on the Template box and select the type of template you want to use for the account.
<b>Information Required to Create Account</b>	
<b>E-mail</b>	Enter the E-mail address of the guest or contractor. This is the only personal information you are required to enter.
<b>Password</b>	<p>A password is automatically generated for this guest. Click Generate Password to generate a new password if necessary or enter a password manually. Password must meet the minimum length designated in the selected Guest Template.</p> <p><b>Note:</b> Network Sentry does not recognize or restrict system-generated passwords that may be offensive.</p> <p><b>Note:</b> If LDAP is specified as the authentication method in the selected Guest Template, the Password field is not displayed.</p>
<b>Account Start Date</b>	Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will become active for the guest or contractor.

Field	Definition
<b>Account End Date</b>	<p>Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will expire. At that time, the guest or contractor will no longer be able to access the network.</p> <p>This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the guest template. If this field is empty, no account duration has been entered in the guest template. Admin Users that have an admin profile with custom Guest/Contractor Account permissions will be restricted to choosing an end date that is within the bounds of the "Create accounts active for days (maximum)" setting as defined in the admin profile. For example, if your admin profile has a "Create accounts active for days" set to 20, you will not be able to choose an end date that is more than 20 days ahead of the chosen start date.</p> <p>This date sets the user expiration date for the guest. The host registered to this guest inherits the setting for registered hosts in Global Aging. When the user expires, both the user and host are removed from the database. If the host expires first, then only the host is removed from the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>
<b>Additional Account Information</b>	
<b>First Name</b>	<p>The guest or contractor's required personal data and the fields below may be entered by the sponsor before the arrival of the guests, or may be left for the individual guests to fill out themselves.</p> <p>The Required Fields under the Additional Account Information heading are designated with an asterisk (*). These fields must be filled in before the guest or contractor will be granted network access.</p>
<b>Last Name</b>	
<b>Address</b>	
<b>City</b>	
<b>State</b>	
<b>Country</b>	
<b>Zip/Postal Code</b>	
<b>Phone</b>	
<b>Asset</b>	<p>The computer serial number, manufacturer's name, and model number, or any other asset identifier of the guest or contractor's computing platform. There may be other Administrator-defined fields here as well, such as license plate. This field has a maximum length of 80.</p>

Field	Definition
Reporting To	In this example, these fields were added when the template was created and marked as Required.
Department	

## Create Bulk Or Multiple Accounts

Depending on permissions, as a Guest Manager Sponsor you may be able to create and manage multiple guest or contractor accounts at one time. The process for creating bulk accounts is similar to that for creating single accounts.

|

**Figure 239: Bulk Accounts Creation Screen**

To simultaneously create multiple guest or contractor accounts:

1. Log into your Sponsor account.
2. The **Guest/Contractor Accounts** window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.

**Table 35: Bulk Account Fields**

Field	Definition
<b>Template</b>	Choose either a Guest or Contractor Template.
<b>Import Passwords</b>	<p>Enable this check box if you want to manually specify a password for each guest. the Password must be the last field in each record. If enabled you must specify a password for every guest account being imported.</p> <p>If the check box is disabled, Network Sentry generates a password for each guest account as it is imported.</p> <p><b>Note:</b> Network Sentry does not recognize or restrict system-generated passwords that may be offensive.</p>
<b>Account Information</b>	<p>You must create a separate record for each account you are creating. Type field place holders for data that you would like the guest to enter. Press <b>Enter</b> after each record to indicate that a new record has been started.</p> <p>You also have the option of importing from a text file.</p> <p>Required information for account creation. Use a comma to separate each field. You may choose to enter additional user information if it is available, but it is not required at this time. The guest or contractor will be prompted to fill in the missing fields before they can log into the network. If there is missing information, enter a comma in its place.</p> <p>If you intend to provide login credentials to guests via SMS messages sent to their mobile telephones, you must include mobile number and mobile provider name in the account list of fields. See <b>Mobile Providers</b> on page 130for instructions on accessing the list of names.</p>

Field	Definition
<b>Import File From</b>	If you have a CSV or text file of the user record information, click <b>Import From File</b> to import the text into the Account Information window. See Bulk Guest Account Import File below for more information.
<b>Account Start Date</b>	The day the account becomes active. You can start the account only on one of the days defined in your profile.
<b>Account End Date</b>	<p>The date the accounts become inactive.</p> <p>This date sets the User Expiration date for each Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

5. Click **OK**. The View Accounts screen opens with the account information in it. See **Provide Account Information To Guest Or Contractor** on page 671.
6. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See **Create Guest/Contractor Templates** on page 632.

Guests also display on the User View. See **User View** on page 385.

### Bulk Guest Account Import File

If you need to create many guest accounts simultaneously, you can create Conference accounts or Bulk accounts. Conference accounts are generated by the system and don't allow you to provide any additional guest information, thus preventing you from e-mailing credentials to attendees. Bulk accounts use data that you supply either by typing it into the Bulk Account screen or by importing it from a CSV or text file.

The fields used in the file vary depending on the template selected to create the accounts. When a Guest Account Template is created you indicate the fields that will be required, optional or ignored for guests. E-mail address is the only field that is absolutely required for all guests and must be included in the file. Other fields, such as first name or last name, may be required but this does not mean that they have to be in the import file. It means that the guest cannot log onto the network unless this information is supplied, either by you in the import file or by the guest when they fill out a web form during the login process.

### **Create Guest Accounts Using A CSV Or Text File**

1. Log into Network Sentry.
2. The **Guest/Contractor Accounts** window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.
5. Select the template that will be used to create these bulk accounts.
6. To manually enter passwords as part of the import file, enable **Import Passwords**. If you prefer that the system generate the passwords, disable this option. If Import Passwords is enabled, it is a required field for each guest. Without this data you cannot import the file.
7. Once the template has been selected you can see the fields that can be imported in a list across the screen. E-mail is bolded indicating that it is required for import. Fields that are preceded by an asterisk are required prior to login but are not necessarily required for import. Therefore, including them in your CSV or text file is optional. Note that if you intend to send login information to guests via SMS, Mobile Provider and Mobile Number fields must be included both in the template and in the import file.
8. For this example, assume that the list of fields on the Bulk Account window is as follows:

**First Name, Last Name, Address, City, State, Zip, Email, Phone**

9. Based on the list of fields shown above, the CSV file could look like this:
 

```
Ana,Bahr,44 Bow St,Pittsfield,NH,03263,asbahr@yahoo.com,603-523-7676
,,,,,jjones@yahoo.com,
James,Smith,,,,,jsmith@aol.com,
```
10. Requirements:
  - Do not include a header row
  - You must have a comma for each possible field
  - You must have a carriage return at the end of each record.

- E-mail is mandatory because you must have a way to forward credentials to your guests
  - If Import Passwords is enabled the password is mandatory and it must be the last field in the row of data
  - If the template is set to send SMS messages to guests, you must include Mobile Number and Mobile Provider
  - Other fields may be required for the guest to enter but are optional for the CSV file
11. Save the file as .csv or .txt and make note of its location on your hard drive.
  12. On the Bulk Accounts window, click **Import From File**.
  13. On the Import From File window, click **Choose File**. Browse to your CSV file, select it and click **Open**.
  14. The contents of the file display in the Bulk Accounts window. Click **OK**.
  15. The View Accounts screen opens with the account information in it. See **Provide Account Information To Guest Or Contractor** on page 671.
  16. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See **Create Guest/Contractor Templates** on page 632.

## Provide Account Information To Guest Or Contractor

After you have created a Guest or Contractor account, you may want to provide that user with his login information. This information can be printed, viewed on the screen, included in an e-mail or sent to a mobile phone via an SMS message. To include additional text with the account information sent to the guest, you must add the text to the Guest Account template under the Note tab prior to creating the account. See the Guest Template Note section in **Create Guest/Contractor Templates** on page 632.

**Note:** Guests who use the self-registration option in the portal receive their credentials automatically. You do not need to send account information to those guests unless they lose the information.

For information on printer settings for guest badges, see **Printer Settings For Guest Contractor Badges** on page 656.

1. Make sure you are on the **Guest/Contractor Accounts** view. Admin users select **Users > Guest/Contractor Accounts**.
2. The list of Guest/Contractor Accounts is displayed.
3. Select one or more accounts for which you wish to view additional information.
4. Click the **View** button.
5. Do the following:
  - Click **Print** to print the guest/contractor account information on a full (8.5 X 11) page.
  - Click **Print Badge** to print out the badge containing the guest/contractor account information.
6. Click **Send Email** to send account information to the e-mail account listed.
7. Click **Send SMS** to send account information to the mobile phone number listed in the guest's account.
8. Click **Close** to close the window.

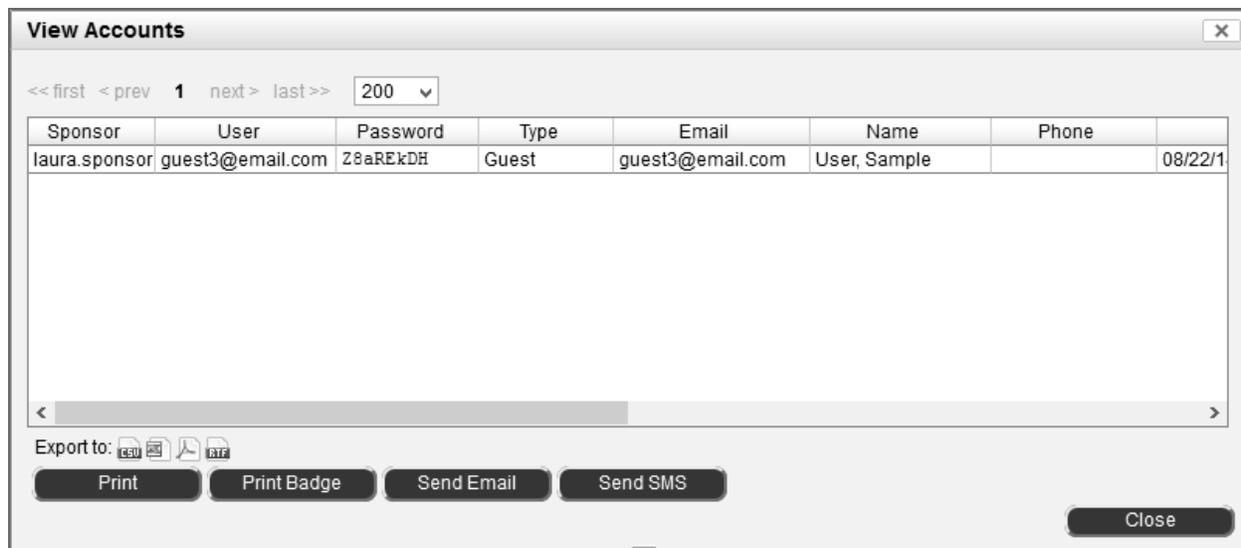


Figure 240: View Accounts Window

|

Figure 241: Guest Email

## Conference Accounts

As a Sponsor, if you have been granted permission in your Admin Profile, you may create Conference accounts, which are bulk accounts in which the account information may be the same for all attendees, or unique to each conference attendee. Conference accounts ensure that attendees have the information they need to access the conference account ahead of time.

Before you create the conference account, determine how you want to manage attendee names and passwords. You may specify:

- Individual names and passwords
- The same name and password for all attendees (for example Seminar1, seminar123)
- Individual attendee names and the same password for all.

If you select Individual Passwords, they will be generated by Guest Manager. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the uppercase letter I (eye), zero, upper or lowercase letter O. In addition, the template used to create the Conference accounts may have specific characters to be excluded from passwords.

### Create Conference Accounts

**Note:** Conference Accounts cannot be modified. The only change that can be made is to Reset Passwords. To modify Conference Accounts you must delete the accounts and create new ones.

To create multiple accounts for a conference at one time:

1. Log into your Sponsor account.
2. The Guest/Contractor Accounts window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. On the Add Account screen click **Conference**.
5. Fill in the fields as needed. See **Conference Account Field Definitions** on page 675 for additional details.
6. Click **OK**. The View Accounts screen opens with the account information in it. See **Provide Account Information To Guest Or Contractor** on page 671.
7. Click **Print** to print out account and password information, or **Close**. These options are visible to you depending on the privileges you have in your profile.

**Note:** E-mail cannot be sent to these conference attendees unless you enter an e-mail address for each attendee to whom you would like to send e-mail using the Modify User option on the User View.

**Note:** SMS messages cannot be sent to these conference attendees unless you enter a mobile number and mobile provider using the Modify User option on the User View.

Guests also display on the User View. See **User View** on page 385.

|

**Figure 242: Conference Account**

## Conference Account Field Definitions

Field	Definition
<b>Template</b>	Select a conference template.
<b>Data Fields</b>	
<b>Conference Type</b>	<p>The selection you make from the pull-down menu determines how user names and passwords are managed for the conference. If you click the <b>Generate Password</b> button, the Password field is automatically populated. The length of the password is determined by the length requirement specified in the Conference template.</p> <p>The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Individual User Names/Individual Passwords:</b> Individual passwords are generated for each attendee. Conference members are required to enter their name and unique password.</li> <li>• <b>Individual User Names/Shared Password:</b> Enter a password in the Password field, or click <b>Generate Password</b>. Conference members are required to enter their name and the password that is shared among all conference attendees.</li> <li>• <b>Shared User Name/Shared Passwords:</b> Enter a password in the Password field, or click <b>Generate Password</b>. All conference attendees are required to enter the shared name and password.</li> </ul> <p><b>Note:</b> Network Sentry does not recognize or restrict system-generated passwords that may be offensive.</p>
<b>Conference Name</b>	<p>Enter the name of the conference. Note that the name of the conference appears as the User Name (conference attendee name) in the list of attendees created when you click Apply on this window.</p> <p>This cannot be modified after the account is created. You must delete the account and create new conference accounts with a new name.</p>
<b>Password</b>	Click Generate Password to generate a password or enter a password manually. Password must meet the minimum length designated in the selected Guest template. See the Conference Types listed above for additional details on generating Passwords.
<b>Number of Attendees</b>	Enter the maximum number of attendees who need network access.
<b>Conference Start Date</b>	Enter a date and time or click the Calendar icon.

Field	Definition
<p><b>Conference End Date</b></p>	<p>Enter date and time that attendees will no longer need network access. This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the template. For example, if the template Account Duration is set to 72 hours, the end date can be less than three days but it cannot be more than three days.</p> <p>If this field is empty, no Account Duration has been entered in the template and you can choose any end date.</p> <p>This date sets the User Expiration date for the Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database.</p> <p>There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.</p> <p><b>Account Duration (Hours)</b>— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week</p> <p><b>Account End Date</b>— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.</p>

**Guest Account Details**

Guest User records created when Guest accounts are generated are displayed in the Users View with network and administrator users. The Guest Account Details window displays data from the Guest Template used to create the Guest User. To access Guest Account Details:

1. Select **Users > User View**.
2. Search for the appropriate User.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Guest Account Details**.

Guest Account Details	
User ID:	jjones@hotmail.com
Account Status:	Enabled
Sponsor:	root
Account Type:	Guest
Start Date:	05/24/12 01:24 PM EDT
End Date:	05/27/12 01:24 PM EDT
Login Availability:	Always
Role:	Guest
Authentication:	Local
Account Duration:	72 hours
Reauthentication Period:	48 hours
URL for Successful Landing Page:	http://www.cnn.com
URL for Acceptable Use Policy:	http://www.bbc.com
Password:	*****
<input type="button" value="Show Password"/>	
<input type="button" value="Close"/>	

Figure 243: Guest Account Details

Table 36: Guest Account Details - Field Definitions

Field	Description
<b>User ID</b>	Guest's email account which is used as the User ID at login.
<b>Account Status</b>	Indicates whether the guest account is enabled or disabled.
<b>Sponsor</b>	The administrator who created the guest account.
<b>Account Type</b>	<p>Guest account type. Types include:</p> <p><b>Guest</b>—A visitor to your facility with limited or Internet-only network access.</p> <p><b>Conference</b>—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days.</p> <p><b>Contractor</b>—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.</p>
<b>Start Date</b>	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
<b>End Date</b>	Date and time the account will expire.
<b>Login Availability</b>	Times during which the guest is permitted to access the network.

<b>Field</b>	<b>Description</b>
<b>Role</b>	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.
<b>Authentication</b>	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.
<b>Account Duration</b>	Amount of time this account will remain valid and usable.
<b>Reauthentication Period</b>	Number of hours the guest or contractor can access the network before reauthentication is required.
<b>URL for Successful Landing Page</b>	Directs the guest or contractor to a specific web page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.
<b>URL for Acceptable Use Policy</b>	Directs the guest or contractor to a specific web page that details the acceptable use policy for the network.
<b>Password</b>	The Guest's assigned password. Passwords are usually generated by the system unless the guests were bulk imported. Toggle the <b>Show Password/Hide Password</b> button to alternately display the password in plain text or as asterisks.

## Guest Or Contractor Login

The portal defaults to a guest or contractor login link which opens the default guest authentication page. To log into the network, guests and contractors must enter the required data fields on their account.

### Login Procedure

Guests and contractors log in so they can access the network.

1. From the Guest or Contractor Login page, the guest clicks the **Start** link to open the Welcome screen.

#### Figure 244: Guest/Contractor Registration Screen

2. Guests enter the Username and the Password that was provided to them by a printout, e-mail or SMS message.
3. Guests click **Download** or **Register** to open the Registration screen.

#### Figure 245: Registration Screen

4. The fields that appear in the Registration screen are those that were defined in the Guest/Contractor template. Fields with an asterisk indicate to the guest that this information must be entered in order to register.
5. The guest clicks **Acceptable Use Policy** to read, accept, and exit the Acceptable Use Policy page.
6. The guest clicks **Continue** button. If the machine passes the Endpoint Compliance Policy requirements, the successful landing page is displayed.
7. If the machine does not pass the Endpoint Compliance Policy requirements, a remediation web page appears and directs the guest to correct the problems that inhibited opening his account.

## Manage Guests In A FortiNac Control Manager Environment

When using Guest Manager in an environment where two or more Network Sentry appliances are managed by a central FortiNac Control Manager appliance, guest accounts are not centrally located. Guest accounts can be created on any Network Sentry appliance, but are not replicated to other Network Sentry appliances. When guests arrive, they may connect to the network in a location managed by an appliance other than the one where their accounts were created. When a guest connects to the network and tries to register, the Network Sentry appliance to which the guest is connected checks its own database for the guest's account. If the guest account exists on that Network Sentry appliance, the guest can proceed with the registration process. If the guest account does not exist, the FortiNac Control Manager checks the other Network Sentry appliances it manages until it finds the guest account. The FortiNac Control Manager copies the guest account from the appliance on which it was created to the appliance where the guest is attempting to connect to the network. Then the guest can continue the registration process.

Since guest records are copied and are not centrally located there are some limitations.

- Guest accounts are only copied from one appliance to another as needed and are not synchronized at any time.
- If a guest account is manually deleted on one Network Sentry appliance, it is not deleted from all appliances automatically.
- Because all appliances are not kept in sync, Guest reports on Network Sentry appliance A may not show the same information as a guest report on Network Sentry appliance B. The guest may have been created on appliance A, but registered and authenticated on appliance B. A report on appliance A will not reflect the changes made to appliance B.
- Guest accounts cannot be limited to a particular appliance or set of appliances, which would subsequently limit access to a subset of the network.
- There is no central location where all guest records can be viewed. A best practice would be to use the same Network Sentry appliance to create all guest accounts.
- If the FortiNac Control Manager is not running, guests will not be able to register on any appliance that does not already contain their guest accounts.

## Chapter 16: Groups View

Groups allow you to put like items together. By creating groups you eliminate the need to configure and control items within the group individually. For example, if you put a set of ports in a group, you can modify the group settings and affect all of the ports simultaneously. Groups can contain other groups.

All Groups (except Admin User Groups) on the NCM are only used in the construction of other global objects. You can modify the sub-groups of these groups on the NCM, but not the members (Admin User Groups are the exception and you can modify the members of these groups on the NCM since they can be used on the NCM, for example to assign to an Event to Alarm Mapping to send email to for an Alarm).

With Global groups on the Network Sentry Servers, you can modify the members, but cannot modify the group structure (sub-groups).

Use the Groups View to add, modify, and delete groups within FortiNac Control Manager. FortiNac Control Manager comes with some standard groups over which it maintains ownership. These are marked as System groups. Create groups to group admin users on the FortiNac Control Manager. Associate these groups with scheduled tasks to perform a variety of functions.

Groups can be used to assign Policies or Roles to Hosts or Users.

If there are more than 2000 Groups in the database, the groups are not automatically displayed. Instead, a confirmation dialog is shown asking if you would like to continue. Note that large numbers of records may load very slowly if not filtered. Choose Yes to display all Groups or No to reduce the number displayed by using the filters.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

Global	Name	Type	Owner	Members	Days Valid	Days Inactive	Description	Last Modified By	Last Modified Date
Yes	All Management Group	Administrator	System	2			Administrative users with all management access rights.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Authorized Access Points	Port	System				Ports that have authorized access points connected. Examples would be dumb hubs or wireless units.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Device Interface Status	Device	System				Devices that participate in the updating of device interface status.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Forced Authentication	Port	System				Ports that participate in forced authentication VLAN switching when hosts connect.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Forced Registration	Port	System				Ports that participate in forced registration when unregistered hosts connect.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Forced Remediation	Port	System				Ports that participate in forced remediation VLAN switching when hosts connect.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Forced Remediation Exceptions	Host	System				Hosts that do not participate in forced remediation.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Forced Scan Exceptions	Host	System				Host machines that do not participate in forced scans.	SYSTEM	03/16/17 12:22 PM EDT
Yes	L2 Network Devices	Device	System				Devices that support the SNMP bridging MIB.	SYSTEM	03/16/17 12:22 PM EDT
Yes	L2 Wired Devices	Device	System				Wired devices that support the SNMP bridging MIB.	SYSTEM	03/16/17 12:22 PM EDT
Yes	L2 Wireless Devices	Device	System				Wireless devices that support the SNMP bridging MIB.	SYSTEM	03/16/17 12:22 PM EDT
Yes	L3 (IP->MAC)	Device	System				Devices that participate in mapping IP addresses to physical addresses.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Physical Address Filtering	Device	System				Devices that participate in the enabling and disabling of physical addresses.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Registered Hosts	Host	System				Group of all registered hosts.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Reset Forced Default	Port	System				Ports that will return to the default VLAN when hosts disconnect.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Reset Forced Registration	Port	System				Ports that will return to Registration when hosts disconnect.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Roaming Guest Hosts	Host	System				Roaming guest hosts (eduroam).	SYSTEM	03/16/17 12:22 PM EDT
Yes	Roaming Guest Interfaces	Port	System				Interfaces that participate in the Roaming guest feature (eduroam).	SYSTEM	03/16/17 12:22 PM EDT
Yes	Roaming Guest Users	User	System				Roaming guest users (eduroam).	SYSTEM	03/16/17 12:22 PM EDT
Yes	Rogue Hosts	Host	System				Group of all rogue hosts.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Unmanaged Access Points	Device	System				Wireless Access Points whose connected clients should not be managed.	SYSTEM	03/16/17 12:22 PM EDT
Yes	Vulnerability Scanner Exceptions	Host	System				Hosts that will never be marked as failed for a vulnerability scan.	SYSTEM	03/16/17 12:22 PM EDT

Figure 246: Groups View

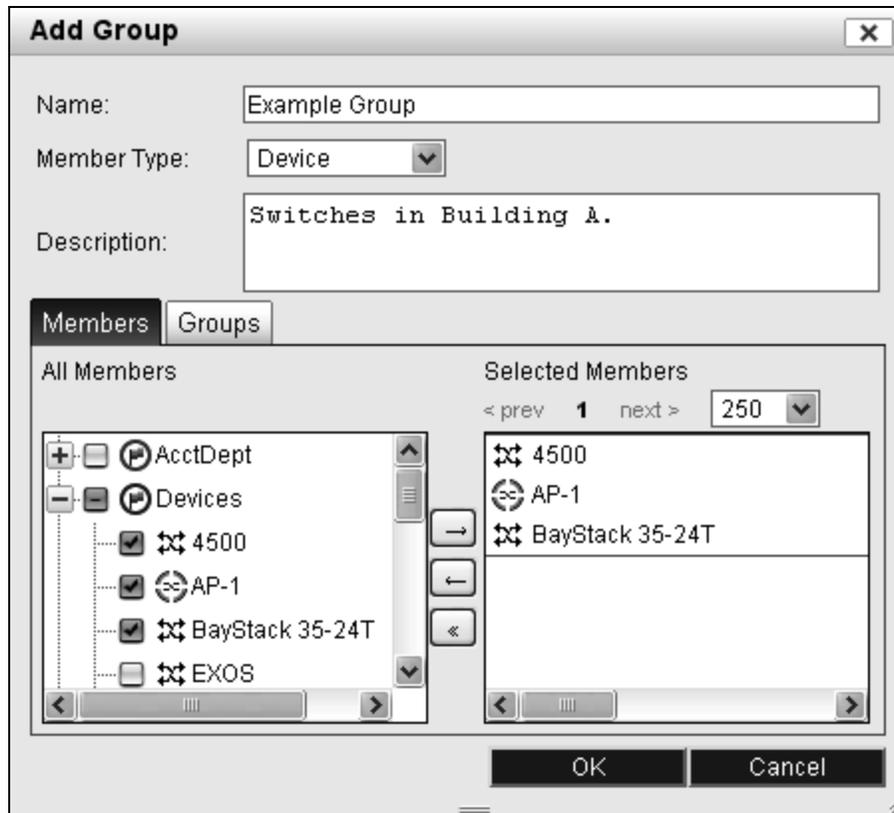
### Groups View Field Definitions

Field	Definition
<b>Global</b>	<p>The Global column always displays "Yes" on the FortiNac Control Manager, and indicates which information will be synchronized with a Network Sentry Server upon manual or automatic synchronization. This information is read-only on the Network Sentry Server. Upon synchronization, the information is overwritten on the Network Sentry Server. See <b>Server Synchronization</b> on page 111 for more information.</p> <p>Global information with a rank will always be ranked first on a Network Sentry Server. The rank of any item on a Network Sentry Server cannot be modified if it would result in changing the rank of a global item.</p> <p>You can only modify or delete global information from the FortiNac Control Manager.</p>
<b>Name</b>	Name used to identify the group.
<b>Type</b>	Indicates whether this is a group of ports, devices, IP phones, hosts, users or administrators.
<b>Owner</b>	Creator of the group. <b>System</b> indicates that the group was created by Network Sentry. <b>User</b> indicates that an administrative user created the group.
<b>Members</b>	<p>The number of items contained within the group. For example, if this is a host group, this number indicates the total number of hosts in the group. If this group contains sub-groups, the number includes those items in each sub-group.</p> <p><b>Note:</b> Only the Administrator group type will display the number of members in the group. The Members column will appear blank for all other group types because members cannot be added to these groups on the NCM.</p>
<b>Days Valid</b>	This column only applies to Host groups. The Expiration Date for hosts in this group is calculated using the number of days valid. For example, if a host is added to the group on 01/01/2011 and days valid is set to 30, the host's Expiration Date is set to 01/31/2011. The Expiration Date is set when a host is added to the group or when the Days Valid is edited. See <b>Aging Hosts In A Group</b> on page 699 for more information.
<b>Days Inactive</b>	This column only applies to Host groups. The number of days of network inactivity after which hosts in this group are removed from the database. For example, if this is set to three and a host in this group has not connected to the network for three days, the host record is removed from the database. See <b>Aging Hosts In A Group</b> on page 699 for more information.
<b>Description</b>	User specified description for the selected group.
<b>Last Modified By</b>	User name of the last user to modify the group.
<b>Last Modified Date</b>	Date and time of the last modification to this group.
<b>Right Mouse Click Menu - Options Button Menu</b>	
<b>Copy Group</b>	Creates a copy of the selected group.
<b>Delete</b>	Deletes the selected group.

Field	Definition
<b>Group Member Of</b>	Displays groups in which this group is a member. A group can be a sub-group of another group of the same type. See <b>Groups - Group Membership</b> on page 696.
<b>In Use</b>	Provides a list of other features that reference this group, such as a Policy Mapping or a Scheduled Task. See <b>Group In Use</b> on page 698.  <b>Note:</b> System-owned groups will not be displayed as "In Use", even though they are in use by the system.
<b>Manages</b>	Applies only to Administrator groups. Administrator groups can be designated to manage groups of devices or hosts. See <b>Limit User Access With Groups</b> on page 693.
<b>Modify</b>	Opens the Modify Group window. See <b>Modify A Group</b> on page 695.
<b>Set Aging</b>	Allows you to set Days Valid and Days Inactive for the selected Host group. Days Valid and Days Inactive are used to calculate the date when the host is aged out of the database. Date is set when a host is added to the group or when Days Valid or Days Inactive fields are modified. See <b>Aging Hosts In A Group</b> on page 699.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item.  For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446  <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF.
<b>Show Members</b>	Opens the Group Members window and displays a list of all of the items within the group. Indicates whether the item is a member of the main group or a sub-group. See <b>Show Group Members</b> on page 697.

## Add Groups

Create additional groups to logically group elements that require network resources.



**Figure 247: Group Creation Dialog**

1. Select **System > Groups**.
2. From the Group view, click **Add**.
3. Enter a **Group Name**
4. Select a **Member Type**, which indicates the types of items that will be included in the group.

Member Type	Description
<b>Administrator</b>	Admin Users that access Network Sentry.
<b>Hosts</b>	Hosts that access the network.
<b>Devices</b>	Devices such as switches, computers, or printers.
<b>Ports</b>	Ports on switches on the network.

---

Member Type	Description
IP Phones	Internet phones that are connected to the network.
Users	Users that log onto the network.

5. For Host groups you have options for **Days Valid** and **Days Inactive**. These fields are used to calculate the Expiration Date used to age hosts out of the database. They are optional and should not be set if you have another mechanism that sets the Expiration date. See **Aging Out Host Or User Records** on page 381 before you set these fields.
6. Enter a **Group Description**.
7. In the **All Members** pane select one or more items to be included in the group, then click the right arrow to move them to the **Selected Members** pane. For lists that do not include check boxes, select multiple items by holding down the **Ctrl** key while clicking.
8. To remove an object from the group, click on it and then click the left arrow.
9. To add subgroups to a group, select the **Groups** tab and select one or more groups to add as subgroups.
10. Click **OK** to save the new group.

Administrator

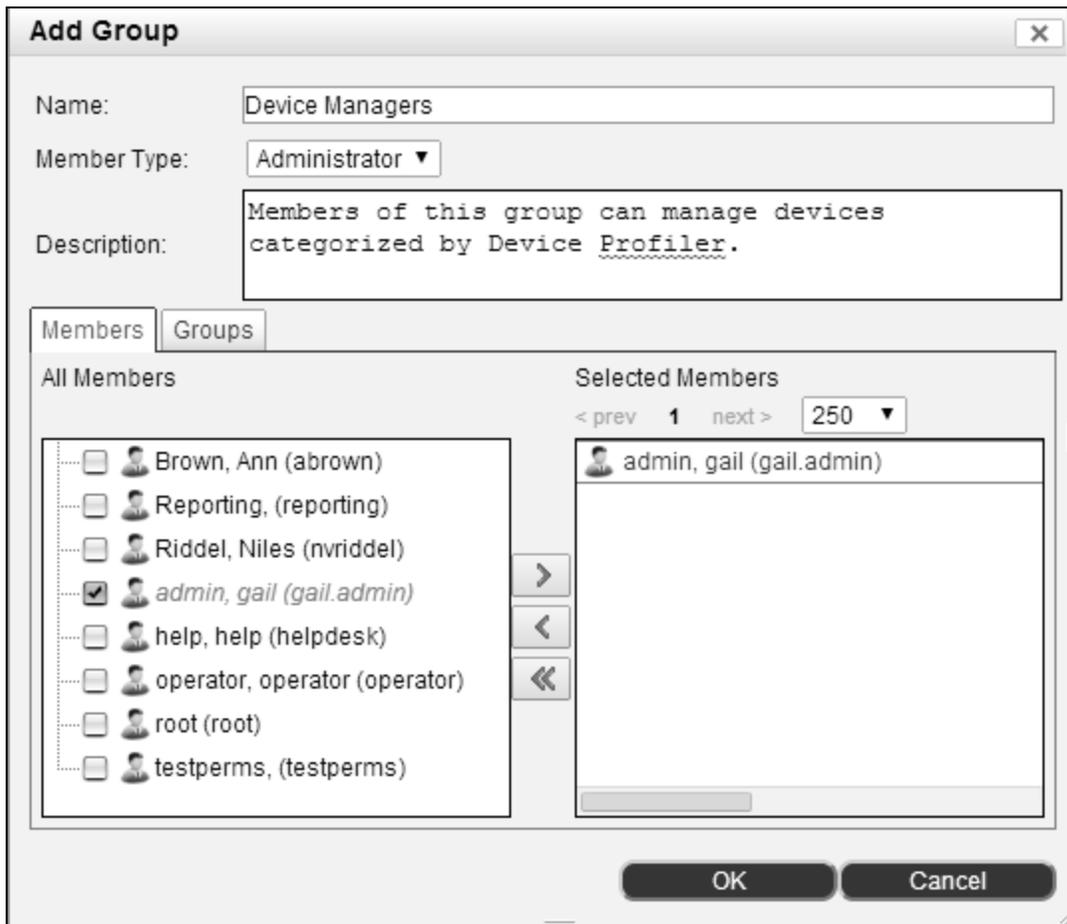


Figure 248: Add Administrator Group

Host

**Add Group**

Name: Hosts In Accounting Dept.

Member Type: Host

Days Valid: 120 Days Inactive:

Description: Desktop, portable units, alarm system in Accounting

Members Groups

All Members Selected Members

< prev 1 next > 250 < prev 1 next > 250

00:0C:29:19:0B:4E  
00:0D:ED:38:AB:58  
+ 00:1C:23:29:B2:CD  
00:1D:45:24:AA:A2  
5C:59:48:4F:96:F0

00:0D:ED:38:AB:58  
00:1D:45:24:AA:A2  
5C:59:48:4F:96:F0  
Jessicas-iphone 8C:58:77:33:EC

OK Cancel

Figure 249: Add Host Group

Device

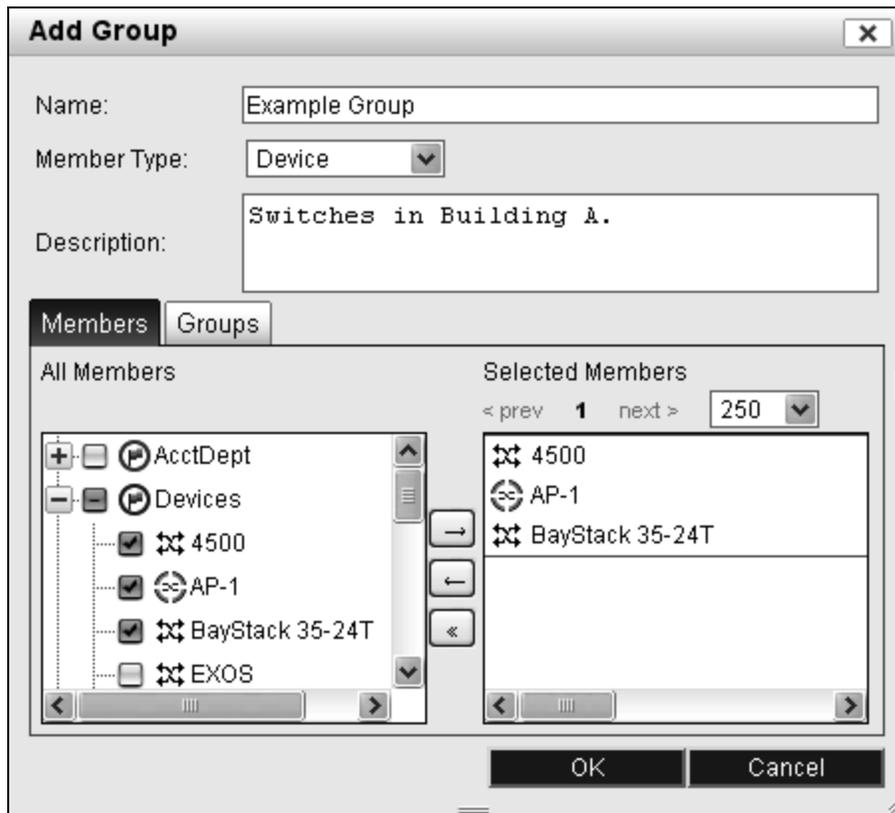
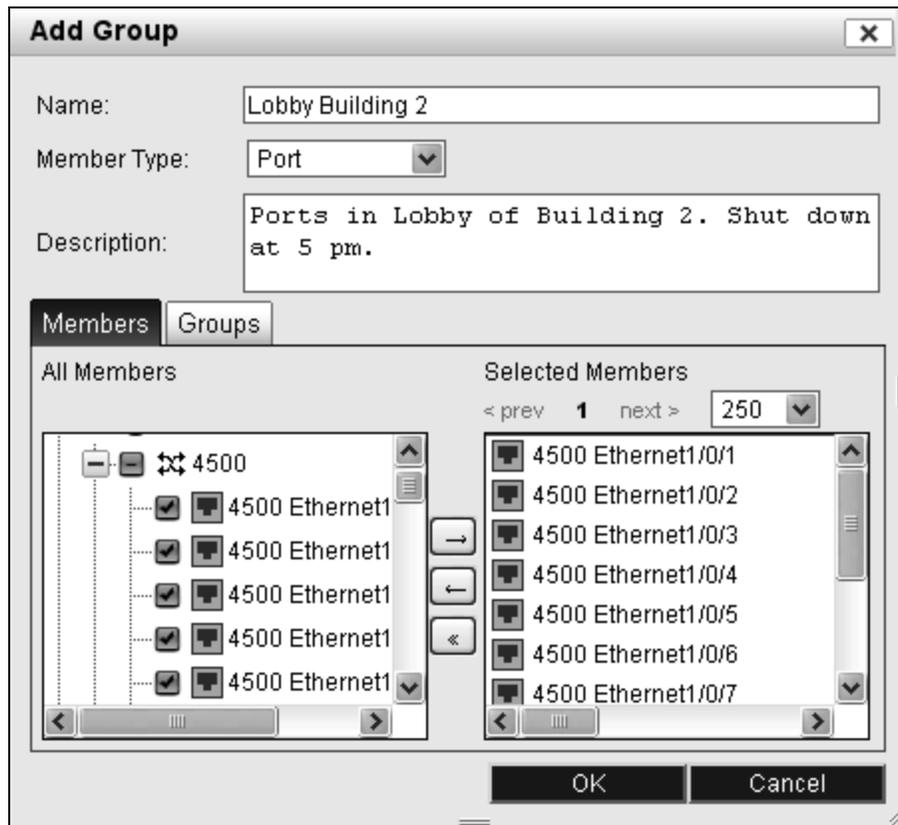


Figure 250: Add Device Group

**Port****Figure 251: Add Port Group**

**IP Phone**



**Figure 252: Add IP Phone Group**

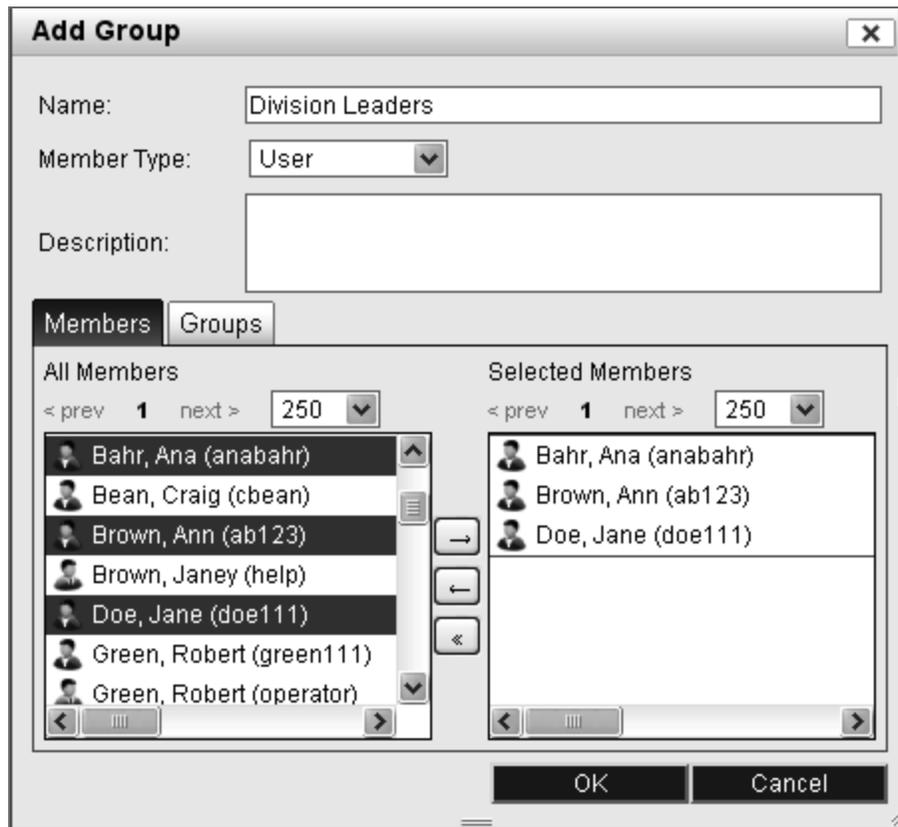
[User](#)

Figure 253: User Selection

## Copy A Group

1. Select **System > Groups**.
2. Locate the group to be copied.
3. Right-click on the group and select **Copy Group**.
4. Enter a **name** for the new group and click **OK**.
5. The new group appears in the Groups View. This group is owned by the user and not Network Sentry.

## Delete A Group

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Delete** to remove the group from the list.
4. Click **Yes** to confirm that you wish to delete the group.

## Limit User Access With Groups

To control which hosts and ports Admin users can access you can place those Admin users in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

### Example:

Assume you have two Administrative Users that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two Administrative Users in a special Administrator Group.
- Assign these two Administrative User to a profile with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the General Tab of the profile is set to **Restrict by Groups**.
- Set the Administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two Administrative Users from the All Management Group or they will have access to all hosts and ports.

When those Administrative Users log into the Admin user interface, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.

**Note:** Make sure to remove affected Administrative Users from the All Management group or they will continue to have access to all hosts and ports.

**Note:** Administrative Users can still view all hosts and users from the Locate View if their Admin Profile gives them permission for that view, but they can only modify those that are in the group they are managing.

1. Create the group of hosts or ports. See **Add Groups** on page 684 for instructions.
2. Create an Admin Profile for with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the General Tab of the profile is set to **Restrict by Groups**. See **Add Administrative Users** on page 274
3. Create an Administrator group that contains the Administrative Users responsible for the devices or ports.
4. Remove the Administrative Users from the All Management group. See **Modify A Group** on page 695 for instructions.
5. Right-click on the Administrator group of Administrative Users and select **Manages**.

6. On the Manages window select the group(s) to be managed by marking them with a check mark.
7. Click **OK**.

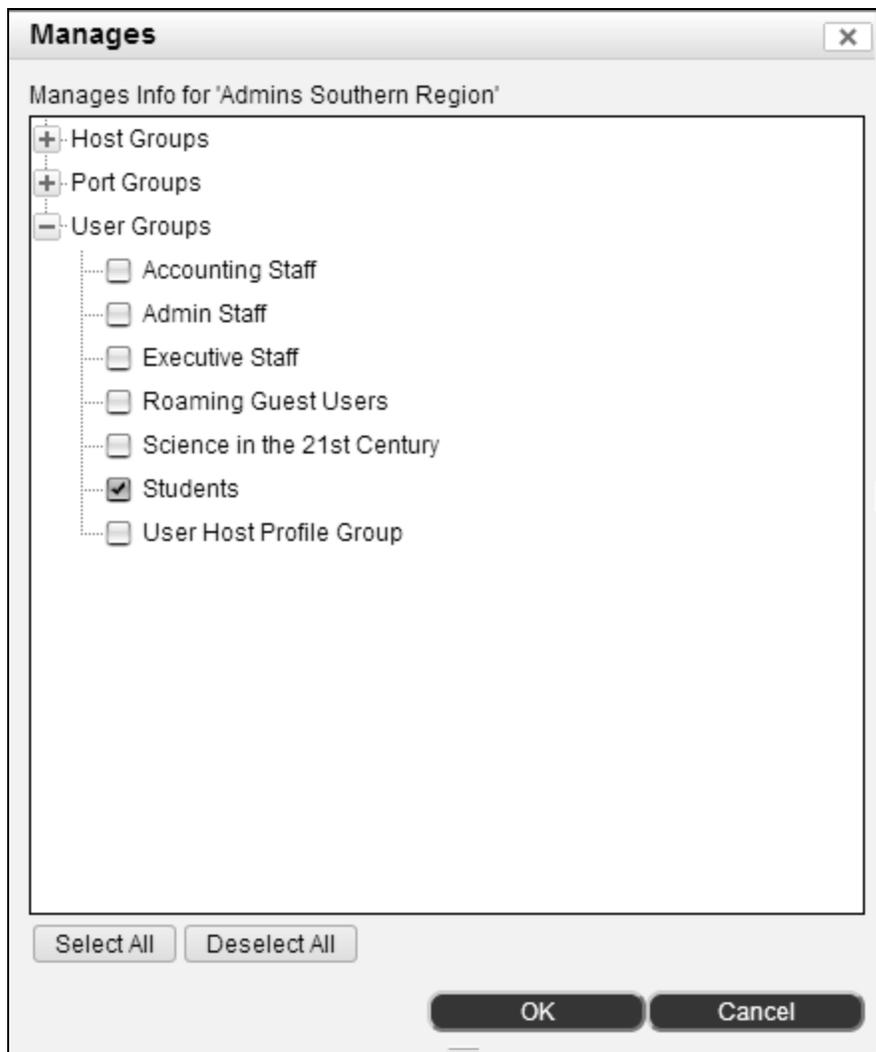


Figure 254: Group Management Dialog

## Modify A Group

Modify a group by adding additional items to the group or removing members from the group. Group description, Days Valid and Days Inactive can also be modified.

1. Select **System > Groups**.
2. Select the group.
3. Click the **Modify** button at the bottom of the window.
4. If this is a Host Group, Days Valid and Days Inactive can be modified. See **Aging Out Host Or User Records** on page 381 before modifying these numbers.
5. **To remove items from the group**, Ctrl-click items in the **Selected Members** panel, then click the left arrow button.
6. **To modify subgroups**, click the Groups tab and check or uncheck groups in the displayed list.
7. **To add members to the group**, Ctrl-click items in the **All Objects** panel, then click the right arrow button.
8. When you have selected all the members that are to be part of the group, click **OK**.

### Groups - Group Membership

Displays the groups that contain the selected group and allows you to modify group membership. For example, if you had a group called Staff, you might want to further subdivide that by department, therefore you could have sub-groups such as Accounting or Human Resources within Staff. Selecting Human Resources from the Groups View and opening the Group Membership window would show that hierarchy. In addition the selected group can be added to or removed from other groups.

To access Group Membership:

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Group Member Of** to display the groups that contain the selected group.
4. Modify the groups as needed and click **OK** to save your changes.



Figure 255: Group Membership

## Show Group Members

This option displays a list of all of the items within the selected group. Indicates whether the item is a member of the main group or a sub-group.

1. Select **System > Groups**.
2. Select the group and click **Show Members** to display the list of items within the group.
3. Use the Find: field to search for a particular item by typing in any part of its name and clicking Next or Previous. This field is case sensitive.

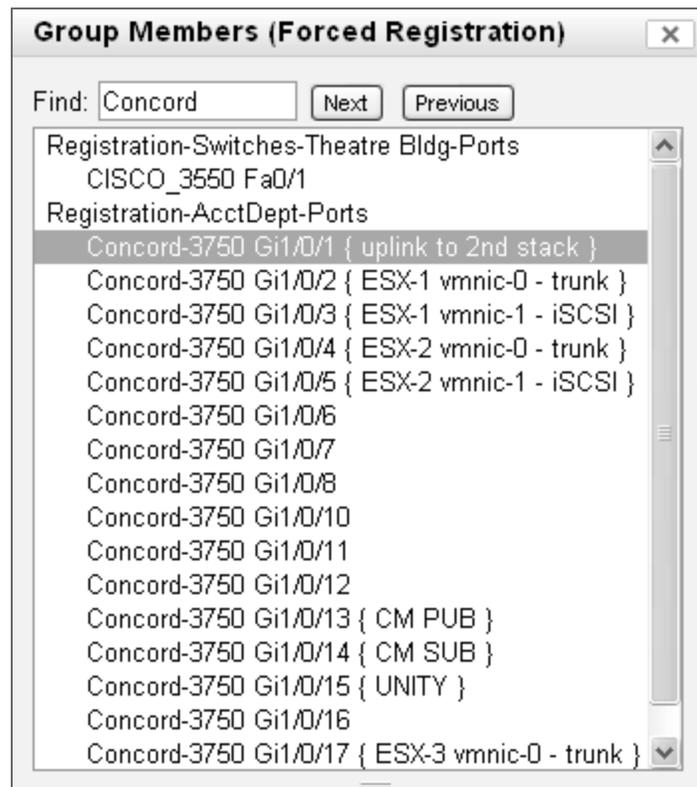


Figure 256: Show Group Members

### Group In Use

To find the list of Network Sentry features that reference a group, select the group from the Groups View and click the **In Use** button. A message is displayed indicating whether or not the group is associated with any other features. If the group is referenced elsewhere, a list of each feature that references the group is displayed.

**Note:** System-owned groups will not be displayed as "In Use", even though they are in use by the system.

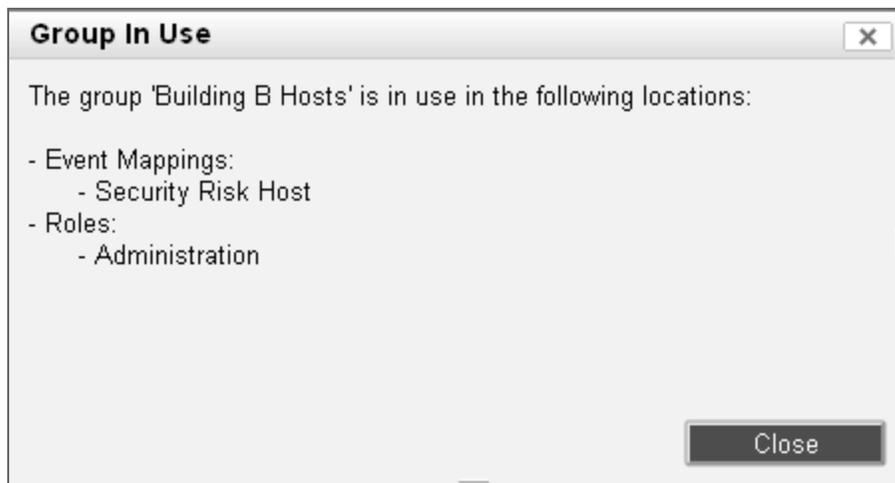


Figure 257: Group In Use

## Aging Hosts In A Group

Use the Set Aging window to set aging for the hosts in a selected Host group. Using the Aging feature populates the Expiration Date and the Inactivity Date fields on the Host Properties window. Hosts with existing age times are modified. This option is only valid for Host groups. If a host is a member of more than one group, the aging time is applied based on the last group to which the host was added or the last group whose aging times were modified.

Adding age times to existing hosts can cause some hosts to be removed from the database immediately depending on the creation date of the host record. If, for example, the creation date is 01/01/2010, today's date is 02/02/2010 and Days Valid is set to 5, then the Expiration Date calculated is 01/06/2010. The record is deleted immediately.

If hosts have been manually set to Never Expire, the Expiration Date and Inactivity Date fields for those hosts will not be modified by adding those hosts to a group with aging settings. See **Host Properties** on page 335, **Set Host Expiration Date** on page 366 and **Aging Out Host Or User Records** on page 381 for additional information.

1. Select **System > Groups**.
2. Right-click on the Host group and select **Set Aging**.
3. Enter a number for Days Valid or Days Inactive. The number in Days Valid is used to calculate the Expiration Date for each host in the group. The number in Days Inactive is used to calculate the Inactivity Date for each host.
4. Click **OK**.

## System Groups

The groups listed below are default system groups that exist within the Network Sentry database. They cannot be deleted. System groups are global and not server-specific.

Group	Definition
<b>Administrator</b>	
<b>All Management</b>	<p>Network Sentry administrative users with all management access rights. Initially contains only <i>Admin</i>, <i>root</i>. New Administrator and Administrative Users are added to this group automatically. This is the default group for e-mail notifications triggered by alarms.</p> <p>Add users to your own specific Administrator groups to give them privileges to manage (disable and enable) specific hosts and ports. If you place a user into your own Administrator group, be sure to remove that user from the All Management group. See <b>Limit User Access With Groups</b> on page 693.</p>
<b>Port</b>	
<b>Access Point Management</b>	Ports with authorized access points connected and Network Sentry serving DHCP. Examples are dumb hubs or wireless units. Network Sentry provides management of hosts connecting through these access points.
<b>Authorized Access Points</b>	<p>Ports that have authorized access points connected. Access points that connect to these ports do not generate Multi Access Point Detected events or alarms and the port is not switched to another VLAN during, for example, Forced Registration or Role Management VLAN Switching.</p> <p>Access points that connect to ports that are not in this group do generate an event or alarm.</p> <p>Add switch ports that connect to hubs and wireless access points to this group.</p>
<b>Forced Authentication</b>	Ports that participate in forced authentication when unauthenticated users connect. If you have a port in this group, when a host connects to this port and is unauthenticated, the port is put into isolation VLAN and the host is forced to authenticate.
<b>Forced Registration</b>	<p>Ports that participate in forced registration when unregistered hosts connect.</p> <p>Add switch ports that participate in forced registration when an Unregistered Host connects to the Forced Registration port group. Only ports that participate have their VLAN ID set to the Registration VLAN when an Unregistered Host connects.</p>
<b>Forced Remediation</b>	Ports that participate in forced remediation VLAN switching when hosts connect.
<b>Reset Forced Default</b>	Ports that return to the default VLAN when hosts disconnect.
<b>Reset Forced Registration</b>	Ports that return to Registration when hosts disconnect.

Group	Definition
<b>Role-Based Access</b>	<p>Ports that participate in role-based access and switch VLANs, based on the role of network devices, such as printers, when they connect.</p> <p>Add switch ports that participate in VLAN switching. Ports that participate have their VLAN ID set to the role specified for the connected network device.</p> <p><b>Example:</b></p> <p>A printer is set up with the role "Accounting". When the printer connects to a port in this group, the printer is switched to the VLAN associated with the "Accounting" role.</p>
<b>System DHCP Port</b>	The port used to discover unauthorized DHCP servers and validate authorized DHCP servers.
<b>Device</b>	
<b>Authorized DHCP Servers</b>	Servers that are authorized to serve DHCP on the network.
<b>Bridging Devices</b>	<p>Devices that support the SNMP bridging MIB.</p> <p><b>Note:</b> This group has been replaced by the L2 Network Devices Group.</p>
<b>Device Interface Status</b>	Devices created through Discovery or created manually are automatically added to this group. Use this group in conjunction with the task scheduler to periodically update the interface status for each device in the group.
<b>L2 Network Devices</b>	Devices that support the Standard 802.1d Bridge Table. This group is also used for filtering the list of devices displayed on the L2 Network Devices window. As new L2 devices are discovered they are added automatically to this group and to either L2 Wired Devices or L2 Wireless Devices.
<b>L2 Wired Devices</b>	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wired Devices are added to this group automatically as they are discovered.
<b>L2 Wireless Devices</b>	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wireless Devices are added to this group automatically as they are discovered.
<b>L3 (IP--&gt;MAC)</b>	This group must be populated manually with your L3 devices. The L3 group can be used for filtering on the L3 Polling window.
<b>Physical Address Filtering</b>	<p>Devices that participate in the enabling and disabling of hosts.</p> <p>Add switches that participate in host disabling to this group. If a host is connected to a switch that is not in the Physical Address Filtering group, and that host is disabled through Network Sentry, the host remains connected to the network and is displayed as in violation. Add the switch regardless of whether a host is disabled through a Dead End VLAN, or through MAC address security.</p>
<b>Host</b>	
<b>Forced Scan Exceptions</b>	Host machines that do not participate in forced scans.

Group	Definition
<b>Forced User Authentication Exceptions</b>	Host machines that do not participate in forced user authentication.
<b>Forced Remediation Exceptions</b>	Host machines are scanned and can be marked "at risk", but are never put into remediation. Scan results are stored allowing the administrator to review the results and take corrective action without disrupting users on the network.
<b>Global Agent Update Exceptions</b>	Host machines in this group are excluded from automatic Persistent Agent Updates. Updates are controlled by MAC Address. If a host has more than one MAC Address, as long as any one of its MAC Addresses is listed in this group the host is not updated.
<b>Registered Hosts</b>	Group of all registered hosts.
<b>Rogue Hosts</b>	<p>This group has a special property that controls whether or not rogue hosts can access the network. Under Group Properties for this group, the Access field can be set to either Deny or Allow.</p> <p><b>Deny</b>—If the Access field is set to Deny, rogue hosts in this group are denied network access until they register and any new unregistered hosts are automatically put into the group as they connect to the network.</p> <p><b>Allow</b>— If the Access field is set to Allow, rogue hosts in this group are permitted to access the network and any new unregistered hosts are not added to the group.</p> <p>Devices that are not in the Topology View but are connected to managed switches are created as rogue hosts.</p> <p>If rogue hosts are denied access to the network, they are disabled. To prevent this from causing problems with new devices such as printers, lab machines or servers, you must register those machines as devices or as hosts. See <b>Register A Host As A Device</b> on page 364 or <b>Modify a Host</b> on page 344 for detailed instructions.</p>

## Customer Defined Groups

User-owned groups are typically created to associate devices, ports, IP phones or hosts. You can associate these groups with scheduled actions to perform a variety functions. Typical groups include the following:

Customer Groups	Notes
<b>Ports</b>	<p>Port groups can be used for a variety of purposes. Use the Fixed Day Task option in the Scheduler with the Disable Ports and Enable Ports actions to disable or enable ports on a date or time schedule.</p> <p>You can nest port groups to make it easier to add ports to the Network Sentry owned groups, such as Forced Registration groups.</p>
<b>Departments, Staff, Divisions</b>	<p>You can use Host groups for a variety of purposes. Use Disable Hosts and Enable Hosts on a date or time schedule with the Fixed Day Task option in the Network Sentry Scheduler.</p> <p>Nest host groups to make it easier to control access over large groups of students.</p> <p>Create host groups for each grade level to control each group through its own scheduled task. You can also create a host group that contains each grade level and schedule it to disable or enable the entire student population with a single task.</p>
<b>Administrator</b>	<p>This group contains Administrative Users who can manage (disable and enable) ports or hosts contained in the associated port or host groups.</p> <p>For example, place Administrative User "John Smith" in the Northeast Admins group. Set the Northeast Admins group to manage the "Department 1 Ports" and the "Department 1 hosts". When John Smith logs in to Network Sentry, he can find and disable any host or port in those groups. See <b>Limit User Access With Groups</b> on page 693.</p>



## Chapter 17: Scheduler View

Use the Scheduler View to add, modify and delete scheduled tasks within Network Sentry. A task is an action that is scheduled to occur at a specified time and is usually associated with a specific group.

There are two types of scheduling, Fixed Day and Repetitive. A Fixed Day Task is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. A Repetitive Task is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. You can set the repetition rate to any number of minutes, hours, or days.

See **Navigation** on page 54 and **Filters** on page 59 for information on common navigation tools and data filters.

The screenshot shows the Scheduler View interface. At the top, there is a 'Filter' section with an 'Add Filter: Select' dropdown and an 'Update' button. Below this is a header for 'Scheduled Activities - Displayed: 9 Total: 9' with a 'Refresh: Manual' dropdown and a refresh icon. The main area contains a table with columns: Name, Action, Group, Enabled, Schedule, Last Scheduled Time, and Next Scheduled Time. The table lists several tasks, some of which are disabled (indicated by a crossed-out checkmark). At the bottom, there is an 'Export to:' section with icons for CSV, PDF, and HTML, and a row of buttons: Add, Modify, Delete, Copy, and Run Now.

Name	Action	Group	Enabled	Schedule	Last Scheduled Time	Next Scheduled Time
Auto-Definition Synchronizer	Auto-Definition Synchronizer		✓	7 Days	11/24/13 12:01 AM EST	12/01/13 12:01 AM EST
Database BackUp	Database Backup		✓	M_12:01AM	11/25/13 12:01 AM EST	12/02/13 12:01 AM EST
FailAllClients - Group - Training Users	Security Rescan		⊗	1 Days	06/10/13 03:48 PM EDT	11/25/13 02:48 PM EST
Guest No Access - All Registered	Security Rescan		⊗	100 Days	06/10/13 03:46 PM EDT	12/27/13 02:46 PM EST
Guest Report	Report Generation		⊗	7 Days		11/25/13 02:54 PM EST

Figure 258: Scheduler View

### Scheduler View Field Definitions

Fields used in filters are also defined in this table.

Field	Definition
<b>Enable Disable Buttons</b>	Enables or disables the selected task.
<b>Name</b>	User created name for the task.
<b>Action</b>	Action being performed by the scheduler.
<b>Group</b>	Action is limited to the group listed.
<b>Enabled</b>	Indicates whether the task is enabled or disabled. Disabled tasks do not execute.
<b>Schedule</b>	Days and times that this task is scheduled to run.
<b>Last Scheduled Time</b>	Last time the task was executed by the scheduler.
<b>Next Scheduled Time</b>	Next time the task will execute.
<b>Description</b>	User specified description of the scheduled task.
<b>Last Modified By</b>	User name of the last user to modify the scheduled task.
<b>Last Modified Date</b>	Date and time of the last modification to this scheduled task.
<b>Right Mouse Click Menu Options</b>	
<b>Copy</b>	Copy the selected task to create a new record.
<b>Delete</b>	Deletes the selected task.
<b>Disable</b>	Disables the selected task.
<b>Enable</b>	Enables the selected task.
<b>Modify</b>	Opens the Modify Scheduled Activity window for the selected rule.
<b>Show Audit Log</b>	<p>Opens the Admin Auditing Log showing all changes made to the selected item.</p> <p>For information about the Admin Auditing Log, see <b>Admin Auditing</b> on page 446</p> <p><b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>Add An Admin Profile</b> on page 243</p>
<b>Run Now</b>	Executes the selected task immediately.
<b>Buttons</b>	
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> on page 383.

## Add A Task Within The Scheduler

**Add Activity**

Enabled

Name:

Description:

Action Type:

Action:

Group:

Schedule Type:

Sunday 1 : 00 AM

Monday 6 : 00 AM

Tuesday 1 : 00 AM

Wednesday 1 : 00 AM

Thursday 1 : 00 AM

Friday 1 : 00 AM

Saturday 1 : 00 AM

**Figure 259: Scheduler - Add Task**

1. Select **System > Scheduler**.
2. From the **Scheduler** view, click **Add**.
3. The **Enabled** check box is selected by default. Uncheck it if you want this task to be disabled.
4. Enter a **Name** for the task and an optional description.
5. In the **Action Type** field select either System or CLI. System actions are pre-defined tasks that you can choose to execute. CLI actions are sets of command line instructions that are created in the CLI Configuration View and saved to be executed elsewhere in the program.

6. Select the **Action** from the list of System or CLI actions. Refer to the Actions table below the instructions for more information.
7. From the **Group** drop down list, select the group that the action will be performed on. The list contains only the group types specific to that Action.
8. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
9. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
  - a. Click the **box** next to the day(s) to select the day.
  - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
  - c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
  - d. To remove all settings click the **Clear All** button.
10. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.

**Note:** A repetition rate of zero causes the task to run only once.

- a. Enter the **Repetition Rate** using whole numbers.
- b. Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
- c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

**Important:** The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

- d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.

11. Click **OK**.

**Table 37: Actions**

Actions	Group Type	Description
Agentless Host Scanning	Host	Scans hosts with the Agentless Scanner.

Actions	Group Type	Description
<b>Certificate Expiration Monitor</b>	None	Generates a warning, critical warning, and expiration events for the certificates listed in Certificate Management. See <b>Certificate Management</b> on page 116
<b>Custom Script</b>	None	Executes the selected command line script located in /home/cm/scripts.
<b>Database Archive and Purge</b>	None	Archives and purges Event, Connection, and Alarm records that are older than 7 days. The number of days is configurable in the Event And Alarm Age Time field on the Network Sentry Properties window. See Database Archive on page 147.
<b>Database Backup</b>	None	Back up the Network Sentry database. The database backup files are stored on the local appliance at  /bsc/campusMgr/master_loader /mysql/backup.  See <b>Backup To Remote Server</b> on page 165 for more information on configuring backups to a remote server.
<b>Disable Adapters</b>	Hosts	Prohibits network access to all adapters in the associated host group. Disables the adapters but not the host itself.
<b>Disable HP/NT Port Security</b>	Devices	Disables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.
<b>Disable Ports</b>	Port	Administratively disables all ports in the associated group.
<b>Enable Adapters</b>	Hosts	Allows network access to all hosts in the associated group.
<b>Enable HP/NT Port Security</b>	Devices	Enables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.
<b>Enable Ports</b>	Port	Administratively enables all ports in the associated group.
<b>Integrated RADIUS Database Backup</b>	None	Back up the RADIUS settings and users when there is a RADIUS server configured.  The default configuration is "Disabled".  The RADIUS Database backup files are stored on the RADIUS server at  /bsc/campusMgr/master_loader /mysql/backup
<b>Modify Device VLAN Values</b>	Ports	Writes the indicated VLAN value to the switch and changes only the Current VLAN value in the Network Sentry device model. You must specify the VLAN value.

Actions	Group Type	Description
<b>Purge Remediation Output Files (Reports)</b>	None	Purges the output files from all the Nessus scans performed since the last purge.
<b>Resynchronize Device</b>	Devices	Allows you to sync a device with Network Sentry after making a change to the device (e.g., adding a VLAN, role or SSID for a wireless device).
<b>Role Assignment</b>	Hosts	Modifies the Role for the associated group of hosts or users. You must specify the new role.
<b>SSID Assignment</b>	Devices	Maps VLAN IDs to SSIDs. You must specify the both the VLAN ID and the SSID.
<b>System Backup</b>	None	Back up the Network Sentry system files. The system backup files are stored on the local appliance at  <code>/bsc/backups/&lt;server name&gt;</code>  See <b>System Backups</b> on page 170.
<b>Update Default VLAN Values</b>	Ports	Sets the Default VLAN value for the port in Network Sentry device model to the value entered in the scheduled task. You must specify the VLAN value.
<b>Update Interface Status</b>	Devices	Reads and updates the interface status for each port on the devices in the associated groups.
<b>Update Remediation Center</b>	None	Connects to Nessus.org and updates the Nessus server with the scan IDs for the version running on the application server. Also connects to Fortinet and updates the server with the latest scan profiles.  Note: If you create scan profiles with Nessus Wx, you must run this task to ensure that those scan profiles will work properly.  <b>Note:</b> Nessus Servers and scans are no longer supported.

## Copy a Task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Copy**.
5. Enter a **name** for the new task.
6. Modify other fields as needed.
7. Click **OK**.
8. The new task appears in the Scheduler.

## Modify A Task

You can change a task from a Repetitive task to a Fixed Day task by changing the task's date, time, and repetition rate. You can also change the group associated with the task and the name of the task . For field definitions see **Add A Task Within The Scheduler** on page 707.

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Modify**.
5. Modify the data as needed.
6. Click **OK**.

## Delete A Task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Delete**.
5. Click **Yes** to delete the task.

## Run Task Now

To run a scheduled action at any time:

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Run Now**.

## Chapter 17: Send SMS Messages

Network Sentry has the ability to send SMS messages to administrators, guests or users. These messages are used to provide guests with user names and passwords, to notify administrators when an alarm has been triggered or to notify a user when an alarm has been triggered based on his host. Network Sentry sends SMS messages by sending email to a mobile phone number through a special email address provided by the mobile provider. For example, if you have a guest who is a Verizon Wireless customer and you need to send him an SMS message, the message is sent to xxxxxxxxxxx@vtext.com (where xxxxxxxxxxx is the guest's cell phone number).

**Note:** Both the Mobile Number and Mobile Provider must be entered into the guest, administrator or user record. SMS messages are sent via email. Without provider information Network Sentry cannot send SMS messages.

**Note:** Long SMS messages might be divided up into multiple messages or truncated depending on how the Mobile Provider and the mobile telephone process long messages.

## Implementation

To enable the SMS Messaging feature you must configure the following:

### General

- Configure a connection to an out bound email server to send your SMS messages. See **Email Settings** on page 125 for instructions.
- Review the list of Mobile Providers. Enable the providers that should be available to assign to guests, users, and administrators. The list is long so you may not want to enable them all. Add any providers that are not included in the list. Providers can be modified as needed. See **Mobile Providers** on page 130.

### SMS For Guests

- Modify your current guest templates or create new ones to include **Send SMS message** as an option. Two new data fields have been added to the Data Fields tab on the Add/Modify Template dialog to accommodate Mobile Number and Mobile Provider. Make sure you do not remove these fields or guests will not have a place to provide their mobile information when they register. See **Create Guest/Contractor Templates** on page 632.
- If you have existing guests that you would like to send messages to you must delete their guest records and recreate them using a template that has the Send SMS option enabled. Make sure to add Mobile Number and Mobile Provider for these guests.
- When guest accounts are created, you have the option to select one or more accounts from the list and send those guests an email and/or an SMS message

containing their user name and password. See **Provide Account Information To Guest Or Contractor** on page 671.

- Mapping events to alarms and setting an SMS user notification action allows Network Sentry to send an SMS message to a guest. For example, if you want to send guests a message when their host is marked at risk and their network access is disabled, you can map the Host At Risk event to an alarm and send a message. The guest account must be associated with a template that has Send SMS enabled and the guest must have a Mobile Number and Provider entered on the Add/Modify User dialog. See **Add or Modify Alarm Mapping** on page 497.

### **SMS For Administrators**

- Add a Mobile phone number and Mobile provider to each admin user that should receive SMS messages. See **Add Administrative Users** on page 274. This information can also be added by exporting Admin Users and re-importing them with their Mobile information. See **Import Admin Users** on page 304.
- Admin users that should receive SMS messages based on alarm mappings must be in one or more Administrator groups. Add Admin users to the appropriate Administrator groups either from the Groups View or from the Admin Users View. See **Admin User Group Membership** on page 287.
- Mapping events to alarms, enabling options for notification and sending SMS messages to an Administrator group allows Network Sentry to send an SMS message to every Admin user in the group. For example, if you want to send Admin users a message if the database backup fails, map the Database Backup Failure event to an alarm and send an SMS message notifying Admin users about the problem. See **Add or Modify Alarm Mapping** on page 497.

### **SMS For Users**

- Add a Mobile phone number and Mobile provider to each user that should receive SMS messages. See **Modify A User** on page 408.
- Mapping events to alarms allows Network Sentry to send an SMS message to a user. For example, if you want to send a user a message if their host has been disabled, map the Host Disabled Success event to an alarm and send an SMS message notifying the user about the problem. See **Add or Modify Alarm Mapping** on page 497.





## Chapter 18: Scan Management

**Important:** The Scan Management view will be deprecated in a future release. The Scans view in Policy Configuration will enable you to manage security scans. Go to **Policy > Policy Configuration > Scans** to add, modify, copy, and delete security scans. See **Scans** on page 545 for more information.

Use Scan Management to access security scans on the appliances you are managing with FortiNac Control Manager or to copy security scans from one appliance to another.

Scans are used to scan hosts on your network to make sure they adhere to your security requirements. If you have many appliances with hosts who move from one appliance to another, it is beneficial to have the same scans on all appliances. The Scan Management view allows you to copy scans from one appliance to several appliances.

**Note:** Scan History is not copied from one appliance (server) to a different appliance if the host moves. This means that if you connect to a different appliance, your Scan History from the previous appliance will not be available.

### Manage Scans

**Important:** The Scan Management View will be deprecated in a future release. The Scans view in Policy Configuration will enable you to manage security scans. Go to **Policy > Policy Configuration > Scans** to add, modify, copy, and delete security scans. See **Scans** on page 545 for more information.

This option allows you to access the Security Scans on appliances running Network Sentry that are managed by FortiNac Control Manager.

Select a server and press Manage or Copy Scan

Manage Copy Scan

Select	Name	Status	Policies
<input type="radio"/>	qa244.bradfordnetworks.com	Established	OS-Anti-Virus-Check, qa244Policy, qa249Policy, OS-Check,
<input type="radio"/>	qa249.bradfordnetworks.com	Established	OS-Anti-Virus-Check, qa249Policy, OS-Check,

**Figure 260: Policy Management Tab**

1. Select **Policy > Scan Management**.
2. Select a server from the server list and click **Manage**.
3. The FortiNac Control Manager Scans window for the selected server is displayed. This is opened in a separate tab.

Scans - Total: 6					
Name	Remediation	Scan On Connect	Renew IP	Scan Failure Link Label	Agent Order of Operations
MAC-Only	Delayed: 5 Days	<input type="radio"/>	<input type="radio"/>	Use Scan Name	If scan fails, Register or Remediate
OS-Anti-Virus-Check	Audit Only	<input type="radio"/>	<input type="radio"/>	Use Scan Name	If scan fails, Register or Remediate
OS-Check	On Failure	<input checked="" type="radio"/>	<input type="radio"/>	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Roles-Only	On Failure	<input type="radio"/>	<input type="radio"/>	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Scan A	On Failure	<input type="radio"/>	<input type="radio"/>	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate
Test	On Failure	<input type="radio"/>	<input type="radio"/>	Click here for more information	Scan before Registering - Scan Fail: Do not Register, Remediate

Options ▾
Add
Modify
Delete
In Use
Custom Scans
Schedule

Figure 261: Security Scans

4. You can now manage scans on the selected server using its Scans window with the buttons across the bottom of the screen.
5. Click Help for detailed instructions on Scan options or consult your *Network Sentry Administration and Operation* document.
6. See **Copy A Scan** on page 719 for instructions on copying policies from one Network Sentry server to another.

## Copy A Scan

**Important:** The Scan Management view will be deprecated in a future release. The Scans view in Policy Configuration will enable you to manage security scans. Go to **Policy > Policy Configuration > Scans** to add, modify, copy, and delete security scans. See **Scans** on page 545 for more information.

This option allows you to access the Scans on appliances running Network Sentry that are managed by FortiNac Control Manager and copy them from one server to another.

When a Scan is copied there are several issues that must be noted. If a scan with the same name exists on a receiving server, it is replaced with the scan being copied.

If the original scan is modified at a later time, those changes are not sent to the copied scans on other appliances. The scan must be copied again or all versions of the scan must be modified individually.

Certain pieces of data must be kept in mind when copying Scans. Scans require a mechanism to assign them. After copying the scan to the receiving appliance you must configure an Endpoint Compliance Profile and an Endpoint Compliance Configuration that include the scan.

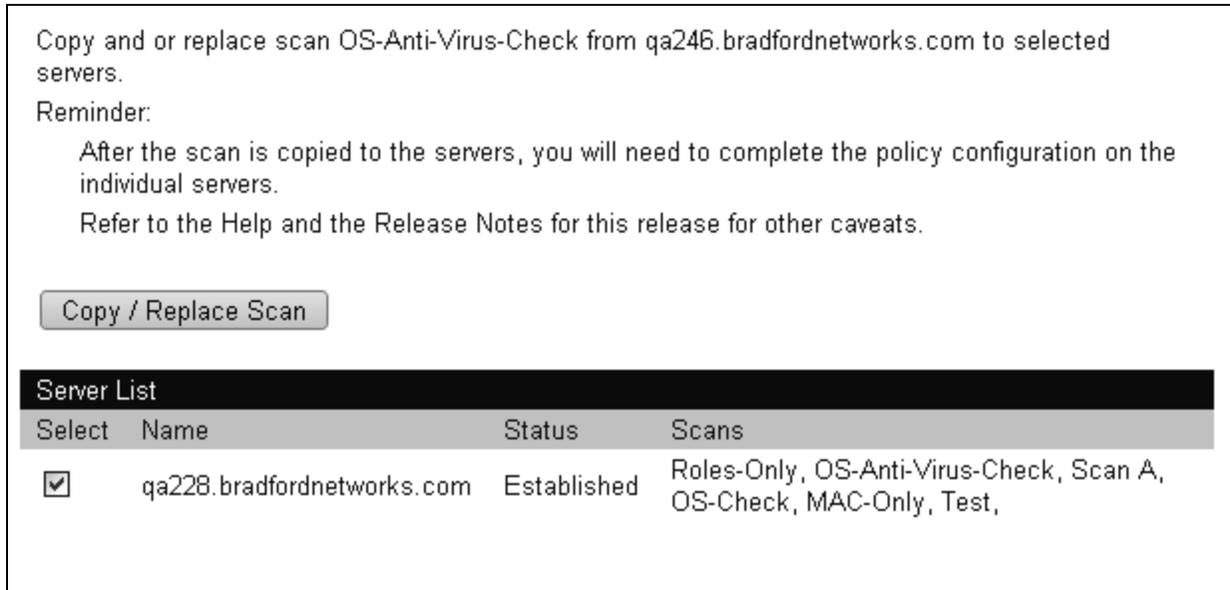


Figure 262: Copy/Replace Window

1. Select **Policy > Scan Management**.
2. Select the server from which you would like to copy a scan and click **Copy**.
3. Select the policy to be copied from the drop-down list displayed and click **OK**.
4. The Copy/Replace window is displayed.
5. Select one or more servers to receive the Scan.
6. Click the **Copy/Replace Scan** button.

**Note:** If a scan with the same name exists on a receiving server, it is replaced with the scan being copied.

7. If the scan has been successfully copied, a success page is displayed.

## Chapter 19: High Availability Overview

The Network Sentry High Availability solution consists of a common management process, supporting scripts, and configuration and monitoring options in the Admin user interface. High Availability can be used to ensure redundancy for FortiNac Servers, FortiNac Control Server and Application Server pairs, and FortiNac Control Manager appliances.

The High Availability management process provides messaging between the primary and secondary appliances. The process mirrors critical information, controls services, and performs system maintenance functions on all appliances. The management process also manages and determines which server is in control. It starts the secondary appliances in the event of a failover.

Supporting scripts determine whether the database replication is working. These scripts are also used to restore the database and/or files from the secondary to the primary and restart the primary server.

Database synchronization is handled by MySQL replication to provide complete data integrity. For additional information on the MySQL replication see <http://dev.mysql.com/doc/refman/4.1/en/replication.html>.

The High Availability diagrams shown below define two possible High Availability configurations using FortiNac Control Server and Application Server pairs. The first diagram illustrates the use of a shared IP address or host name that is moved between appliances during a failover and recovery. This provides the administrator with a single point of management access regardless of which appliance is in control. To use a shared IP address all of the appliances must be in the same subnet on the network. See **HA Configuration Using A Shared IP Address (Layer 2)** on page 725.

The second diagram displays a High Availability setup in which the appliance are on different subnets. To leverage High Availability with appliances on separate subnets do not include a shared IP as part of the High Availability configuration. If you are using a Control Server and Application Server pair and you are not using a shared IP address, during failover both appliances will failover to their corresponding secondary appliances regardless of which one actually failed. If you are using a shared IP address only the appliance that failed will failover to the secondary. See **HA Configuration With Servers On Different Subnets (Layer 3)** on page 727.

---

**Note:** In a High Availability configuration eth1 on the server is disabled until that server is in control. For example, eth1 on the secondary server is disabled until the primary server fails over and the secondary takes control.

---

**Note:** It is recommended that you use a Shared IP address in your High Availability configuration whenever possible. This prevents the Administrator from having to use separate IP Addresses to manage the servers that are in control and alleviates communication issues with the Persistent Agent.

**Note:** If your Primary and Secondary servers are on different subnets, make sure that communication between the subnets is configured in advance.

### FortiNac Control Server And Application Server Communication

#### **Shared IP - Same Subnet**

In a FortiNac Control Server and FortiNac Application Server configuration that uses a shared IP, the FortiNac Application Server appliances are separate standbys from the FortiNac Control Server appliances.

For example:

- If the primary FortiNac Control Server fails, the secondary FortiNac Control Server communicates with whichever FortiNac Application Server is in control (either the primary or the secondary).
- If the primary FortiNac Application Server fails, the primary FortiNac Control Server communicates whichever FortiNac Application Server is in control.

#### **No Shared IP - Different Subnets**

In a FortiNac Control Server and FortiNac Application Server configuration that does not use a shared IP, the FortiNac Application Server and FortiNac Control Server appliances failover in pairs.

For example:

- If the primary FortiNac Control Server fails the primary FortiNac Application server is also brought down and the Secondary pair of appliances take control.
- If the primary FortiNac Application Server fails, the primary FortiNac Control Server is also brought down and the Secondary pair of appliances take control.

High Availability Diagrams

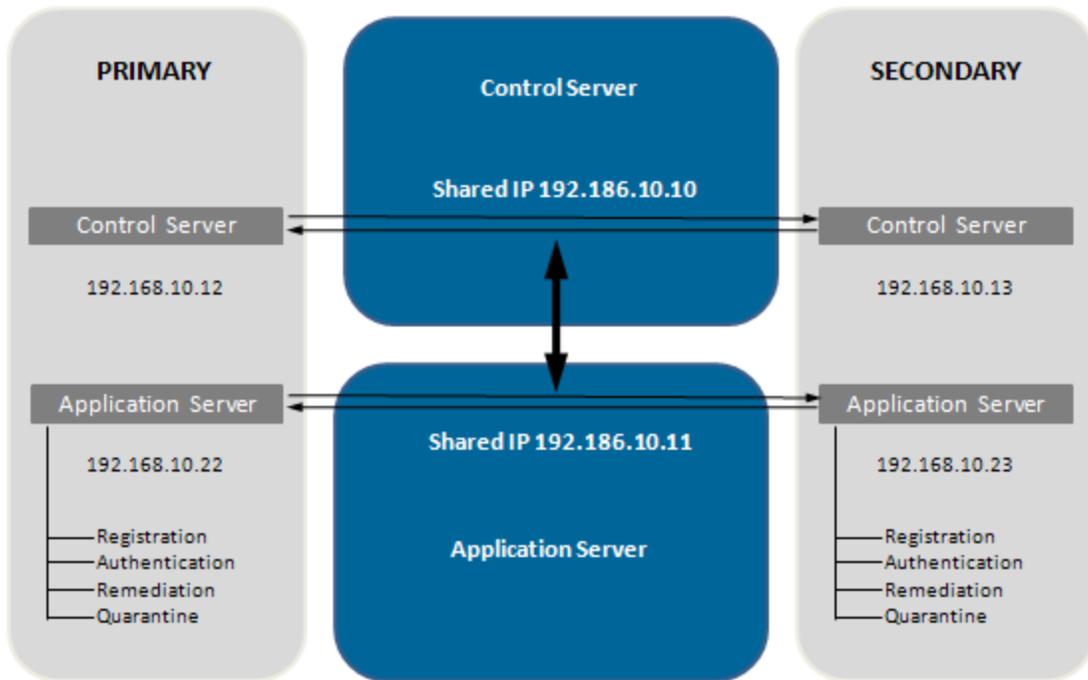


Figure 263: Shared IP Configuration - Servers On Same Subnet (L2)

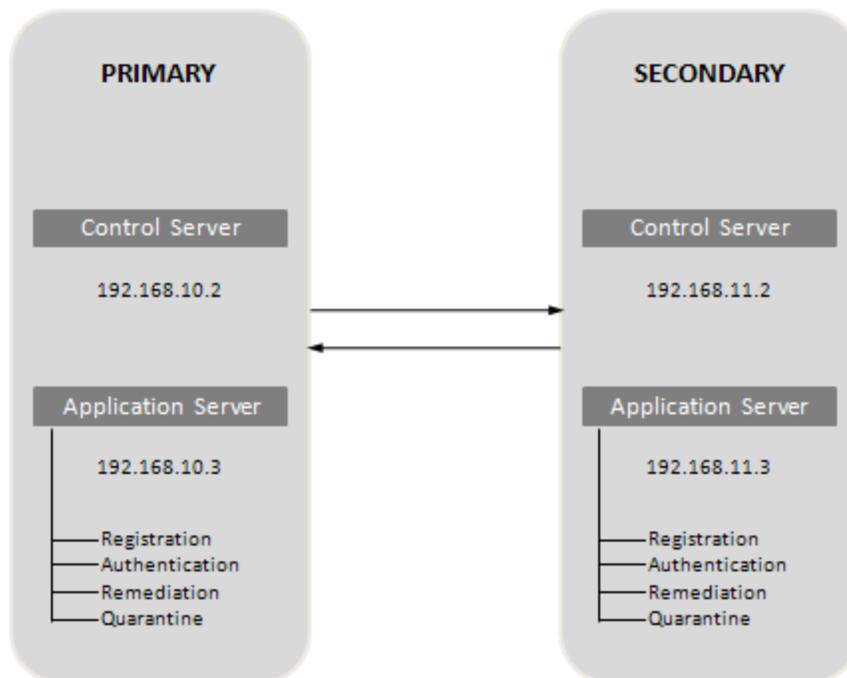


Figure 264: No Shared IP - Servers On Different Subnets (L3)

### High Availability Terminology

Term	Definition
<b>Primary</b>	The active server or servers of the high availability pair that is in control by default. Sometimes referred to as the Master.
<b>Secondary</b>	The "backup" server or servers that takes control when the primary fails. Sometimes referred to as the Slave.
<b>Management Process</b>	The process which manages and determines which server is in control.
<b>Idle</b>	High Availability state in which the management process is functional, but the secondary server will not take control even if connectivity is lost with the primary server.

## HA Configuration Using A Shared IP Address (Layer 2)

### Network Infrastructure

- Configure all network devices to send traps to both the primary and secondary Network Sentry server IP Addresses.
- Configure RADIUS servers to use both the primary and secondary addresses.
- If you are setting up Network Sentry as the RADIUS server for a device in a Bradford High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your Network Sentry appliances can be reached. This would allow users to access the network, but they would not be controlled by Network Sentry.
- If the primary and secondary servers are running on the same subnet and use a shared IP address, make sure that the Persistent Agent and all other features use the shared IP or host name. Refer to the Help on Persistent Agent Properties.
- In a High Availability configuration changes to the database on the primary server are replicated immediately to the secondary server. If the latency is too long and/or the bandwidth between redundant servers is not sufficient, the secondary may not have all of the database changes made on the primary when a failover occurs.

Latency and bandwidth recommendations are as follows:

- latency between remote data nodes must not exceed 20 milliseconds
- bandwidth of the network link must be a minimum of 4.8 Mbps

### Appliance Configuration

- Make sure all appliances have a license key that includes High Availability and that all appliances have matching licenses.
- Use the Configuration Wizard to configure each of the appliances. Refer to the Appliance Installation Guide that comes with the appliances for information on using the Configuration Wizard.
- Establish the address to use as the Shared IP Address (optional) and the IP addresses for the primary and secondary appliances. This enables communication with the other appliances in the High Availability configuration.

- Go to the Administration - High Availability Tab and configure IP addresses and communication between appliances. See **Network Sentry Primary And Secondary Configuration** on page 730.
- Apply the configuration to restart your appliances. This replicates the database on the Secondary and copies any necessary files. Portal pages are copied every 10 minutes.

**Important:** If you are using DHCP Management in a High Availability environment, the ports to which the DHCP Interfaces connect must be added to the System DHCP Port group. Refer to Help on Modifying a Group. In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

- Ensure that the DHCP plugins on both the Primary and Secondary are configured.

## HA Configuration With Servers On Different Subnets (Layer 3)

**Important:** In a High Availability environment with an L3 configuration where redundant Network Sentry servers are on different subnets and do not use a shared IP address, you must select the Layer 3 network option in the Configuration Wizard. L3 High Availability configurations are not supported with Layer 2 Isolation settings.

### Network Infrastructure

- If your Primary and Secondary servers are on different subnets, a Shared IP address cannot be used. Make sure that communication between the subnets is configured in advance.
- Configure two DHCP Helpers (eth1 on the Primary and eth1 on the Secondary) for isolation VLANs. Network Sentry returns two DNS servers (eth1 on the Primary and eth1 on the Secondary) for isolation VLANs.  
Upon failover the isolated hosts will have two DNS entries for use. Should the host stay in isolation longer than the DHCP time to live, then the host will fail to renew its IP from the primary. It will redo DHCP discovery and get an IP address from the secondary application server. The secondary application server will have responded with two DNS servers (secondary eth1 and primary eth1).
- If you are using high availability for a FortiNac Control Server and Application Server pair, when failover occurs both servers failover. See **Recovery** on page 739.
- Configure all network devices to send traps to both the primary and secondary Network Sentry server IP Addresses.
- Configure RADIUS servers to use both the primary and secondary addresses.
- If you are setting up Network Sentry as the RADIUS server for a device in a Bradford High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your Network Sentry appliances can be reached. This would allow users to access the network, but they would not be controlled by Network Sentry.
- If your primary and secondary servers are running on different subnets and do not use a shared IP address, make sure that the Persistent Agent and all other features use the individual IP addresses or host names of the primary and secondary servers. Refer to the Help on Persistent Agent Properties.

- If you are using the Guest Self-Registration feature, you must configure settings to generate the correct links in the emails sent to Sponsors when a guest requests access.
- In a High Availability configuration changes to the database on the primary server are replicated immediately to the secondary server. If the latency is too long and/or the bandwidth between redundant servers is not sufficient, the secondary may not have all of the database changes made on the primary when a failover occurs.

Latency and bandwidth recommendations are as follows:

- latency between remote data nodes must not exceed 20 milliseconds
- bandwidth of the network link must be a minimum of 4.8 Mbps

### Appliance Configuration

- Make sure all appliances have a license key that includes High Availability and that all appliances have matching licenses.
- Use the Configuration Wizard to configure each of the appliances. Refer to the Appliance Installation Guide that comes with the appliances for information on using the Configuration Wizard.

**Important:** You must run the Configuration Wizard on both the Primary and Secondary servers and make sure that the necessary Route scopes are filled in for both servers. If you do not enter scopes on both servers, the High Availability configuration will be incomplete and will not work correctly.

- Go to the Administration - High Availability Tab and configure IP addresses and communication between appliances. See **Network Sentry Primary And Secondary Configuration** on page 730.
- Apply the configuration to restart your appliances. This replicates the database on the Secondary and copies any necessary files. Portal pages are copied every 10 minutes.

**Important:** If you are using DHCP Management in a High Availability environment, the ports to which the DHCP Interfaces connect must be added to the System DHCP Port group. See Modifying a Group in the Network Sentry Administration and Operation documentation for additional information. In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

- Ensure that the DHCP plugins on both the Primary and Secondary are configured.

## Connectivity Configuration

To access the Admin user interface that is available through a web browser, the appliances use the "nac" alias to identify which IP Address/hostname will be allowed in the URL.

In High Availability configurations entries for the "nac" alias are entered automatically in the `/etc/hosts` file for your FortiNac Server appliances. Each of the appliances in the High Availability configuration must be resolvable in the DNS or you must enter them in the `hosts` file of your administration PC. Make sure the entries contain the IP address, the fully qualified domain name (FQDN), and the short name.

### Example:

```
192.168.10.1 ApplianceName.Subdomain ApplianceName
```

Consider the following for the nac alias:

- If the appliance is a FortiNac Control Manager there should be no nac alias entry in the `/etc/hosts` file. Use either the shared or individual IP address to access this server.
- If the High Availability appliances are being managed by the FortiNac Control Manager, verify that none of the appliances have an entry for nac alias in the `/etc/hosts` file. Using nac alias in this configuration would stop the FortiNac Control Manager from accessing the appliances it manages. To access the managed appliances use either the direct or shared IP address.
- If the High Availability appliances are **not** being managed by the FortiNac Control Manager use these guidelines:
  - If the appliance is a FortiNac Server, verify that the nac alias is mapped nac alias to the shared IP address. Use the shared IP address (or shared host name) in the URL.
  - If the appliance is the FortiNac Control Server or FortiNac Control Manager, verify that the nac alias has been removed from the `/etc/hosts` file and use the shared or the individual IP addresses (or host names) in the URL.

**Note:** The 'nac' alias must not be included in DNS. For example, do not use an alias like "nac.-abc.def.com" anywhere in DNS.

## Network Sentry Primary And Secondary Configuration

Configure the High Availability appliances through the High Availability tab on the Administration view.

**Note:** It is recommended that you use a Shared IP address in your High Availability configuration whenever possible. This prevents the Administrator from having to use separate IP Addresses to manage the servers that are in control and alleviates communication issues with the Persistent Agent.

**Note:** If your Primary and Secondary servers are on different subnets, a Shared IP address cannot be used. Make sure that communication between the subnets is configured in advance.

To access the High Availability configuration view on FortiNac Server or Control Server appliances:

1. Click **System > Settings > System Management > High Availability**.
2. Additional information is available in the Network Sentry documentation or see **High Availability** on page 730.

To access the High Availability tab on FortiNac Control Manager appliances:

1. Log into FortiNac Control Manager.
2. Select the **Management View** tab.
3. Click the **Administration** button.
4. Click the **High Availability** tab.
5. Additional information is available in the FortiNac Control Manager documentation or see **High Availability** on page 730.

**Note:** When you click Apply on the Administration High Availability Tab, the primary server tries to communicate with the secondary to ensure that the database will be replicated. If the primary server cannot communicate with the secondary, it continues to try until communication is established.

### **High Availability**

The information you enter into the view is written to files on all of the appliances involved, configures the ssh keys for all the specified appliances and configures mysql for replication. All appliances in the configuration are restarted and placed into High Availability mode when you click Apply and acknowledge the success message.

**WARNING:** Use the High Availability tab for all changes to the configuration. If you manually edit the files on the appliance, values in the files will not be reflected on the High Availability tab.

Table 38: High Availability Fields

Field	Description
<b>Shared IP Configuration</b>	
<b>Use Shared IP Address</b>	<p>Enables the use of a shared IP address in the High Availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual machine IP address.</p> <p>If your primary and secondary servers are not in the same subnet, do not use a shared IP address.</p>
<b>Shared IP Address</b>	The shared IP address for the High Availability configuration. Added to the <code>/etc/hosts</code> file when the configuration is saved.
<b>Shared Subnet Mask (bits)</b>	The shared subnet mask in bits. For example, <code>255.255.255.0 = 24</code> bits. If you are using a Shared IP Address, this field is required.
<b>Shared Host Name</b>	Part of the an entry in the <code>/etc/hosts</code> file for the shared IP address. Admin users can access the UI using either the Shared IP address or the shared host name.
<b>Server Configuration</b>	
<b>Primary Appliance</b>	<p><b>IP Address</b>—IP address assigned to eth0 for the primary.</p> <p><b>Gateway IP Address</b>—IP address pinged by the appliances to determine if network connectivity is still available.</p> <p><b>CLI/SSH root Password [User:root]</b>—root password on the appliance itself. Allows settings to be written to the appliance.</p> <p><b>Retype root CLI/SSH Password [User:root]</b>—retype the password entered in the CLI/SSH root Password field for confirmation.</p>
<b>Secondary Appliance</b>	<p><b>IP Address</b>—IP address assigned to eth0 for the secondary.</p> <p><b>Host Name</b> — Name assigned to the secondary.</p> <p><b>Gateway IP Address</b>—IP Address that pinged by the appliances to determine if network connectivity is still available.</p> <p><b>CLI/SSH root Password [User:root]</b>—root password on the appliance itself. Allows settings to be written to the appliance.</p> <p><b>Retype root CLI/SSH Password [User:root]</b>—retype the password entered in the CLI/SSH root Password field for confirmation.</p>

### High Availability

Apply these settings to configure Primary and Secondary appliances for High Availability.  
 Warning: Saving changes to this configuration restarts both the Primary and Secondary servers.

#### Shared IP Configuration

The Shared IP Address(es) are recommended when the primary and the secondary are in the same subnet. This allows you to fail each server over separately and to use a single IP for administrative use. If they are not in the same subnet and separated by a router, then you will not be able to use a Shared IP Address and will be require to fail both appliances over together. The IP address(es) of the individual appliances will need to be used for administrative use.

Use Shared IP Address

Network Sentry Control Server	Network Sentry Application Server
Shared IP Address: 192.168.6.104	Shared IP Address: 192.168.6.105
Shared Subnet Mask(bits): 24	Shared Subnet Mask(bits): 24
Shared Host Name: qa6-104	Shared Host Name: qa6-105

#### Network Sentry Control Server Configuration

Primary Appliance	Secondary Appliance
IP Address: 192.168.6.100	IP Address: 192.168.6.102
Gateway IP Address: 192.168.6.1	Host Name: qa6-102
CLI/SSH root Password [User:root]: ***** Show	Gateway IP Address: 192.168.6.1
	CLI/SSH root Password [User:root]: ***** Show

#### Network Sentry Application Server Configuration

Primary Appliance	Secondary Appliance
IP Address: 192.168.6.101	IP Address: 192.168.6.103
Gateway IP Address: 192.168.6.1	Host Name: qa6-103
CLI/SSH root Password [User:root]: ***** Show	Gateway IP Address: 192.168.6.1
	CLI/SSH root Password [User:root]: ***** Show

**Save Settings**

Figure 265: High Availability Configuration

## Update Software In A High Availability Environment

To update your servers in a High Availability environment note the following:

- The Primary server must be running and in control in order to update the system.
- The Secondary server(s) must be running.
- The Primary server must be able to communicate with the Secondary server(s).
- The Primary server automatically updates the Secondary server(s).
- If the Secondary server(s) is in control, Network Sentry prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.

Update the Primary server following the instructions for a regular system update in the Network Sentry Admin UI. See **Settings > Updates > System Update** in the Help for update instructions.

If you have a FortiNac Control Manager that manages your Network Sentry servers, you can run the update from the FortiNac Control Manager and select all managed servers to propagate the update throughout your environment.

## High Availability Concepts

The concepts of High Availability configurations include the startup and control sequences as well as the communication for both the primary and secondary servers.

### Startup High Availability

#### **Primary Server Startup**

1. The management process starts up.
2. The condition of the secondary server is checked.
3. If the secondary is **in control**, the secondary retains control until a manual recovery is performed to return control to the primary server. See **Recovery** on page 739.
4. If the secondary is **not in control**, the startup of the primary continues and the primary is in control.

**Note:** If any of the following processes does not start, the appliance is not in control: httpd, dhcpd, named, mysqld, sshd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

#### **Secondary Server Startup**

1. The management process starts up.
2. The condition of the primary server is checked.
3. If the primary is **in control**, database replication is started on the FortiNac Server, FortiNac Control Server, or FortiNac Control Manager. Other processes are not started on the secondary.
4. If the primary is **not in control** and the secondary is not idle then the startup of the secondary continues.
5. The secondary remains in control until you manually perform the recovery that returns control to the primary server.

#### **Management Process**

The Management process starts when the appliance is booted up or by running the following command:

```
startupCampusMgr
```

If the appliance is in control the appropriate processes are started.

**Note:** If any of the following processes does not start, the appliance is not in control: httpd, dhcpd, named, mysqld, sshd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

## Monitor High Availability

### **Monitoring Current Status**

**Important:** These events are not generated for the FortiNac Control Manager.

The status of your High Availability appliances can be viewed on the Dashboard in a Summary panel.

The High Availability appliances also write to a date stamped log file named

`output.processManager.<datestamp>`

located in this directory: `/bsc/logs/processManager`

The file shows current status as well as debug output.

### **Process Down Events**

**Important:** These events are not generated for the FortiNac Control Manager.

Network Sentry generates events and alarms whenever any of the required processes fails or does not start as expected. Network Sentry tries to restart the process every 30 seconds. In a High Availability environment failover occurs after the fourth failed restart attempt. These events are enabled by default and each event has a corresponding alarm.

Events for failed processes include:

- Service Down - Tomcat Admin
- Service Down - Tomcat Portal
- Service Down -dhcpd
- Service Down -httpd
- Service Down -mysqld
- Service Down -named
- Service Down -sshd

### **Process Started Events**

**Important:** These events are not generated for the FortiNac Control Manager.

Network Sentry generates events whenever any of the required processes is started. These events are enabled by default and each event has a corresponding alarm. Alarms for process started events are not typically enabled. They can be enabled manually using Alarm Mappings.

In the Event View, event messages for started processes include the name of the process and the IP address of the machine where the process started. For example, if the **named** process started you would see the following message associated with the event.

```
A critical service (/bsc/services/named/sbin/named) on
192.168.5.228 was not running and has been started.
```

Events for started processes include:

- Service Started - Tomcat Admin
- Service Started - Tomcat Portal
- Service Started -dhcpd
- Service Started -httpd
- Service Started -mysql
- Service Started -named
- Service Started -sshd

### **Other High Availability Events**

**Important:** These events are not generated for the FortiNac Control Manager.

An Event appears in the Events view and can have an alarm configured to send email to you when it occurs.

- **Database Replication Error** — This event is generated if the database on the secondary appliance is not replicating.
- **System Failover** — This event is generated when a failover occurs.

## Control Sequence

**Required Processes**

In a High Availability environment the primary fails over to the secondary when certain processes don't start or fail while running. If any process listed in the table below fails on the primary, then the secondary attempts to take control. Depending on the appliance and platform being used, different processes are required. See the table below for additional information.

Required Process	FortiNac Control Manager	FortiNac Control Server	FortiNac Application Server	FortiNac Server
mysql	X	X		X
sshd	X	X	X	X
dhcpcd			X	X
httpd			X	X
named			X	X
tomcat-admin	X	X		X
tomcat-portal			X	X

**Determining Whether The Secondary Needs To Take Control**

The secondary server pings the primary server every 30 to 60 seconds depending on the time spent "validating" the connection to determine whether the primary is still in control.

If the secondary receives no response from the primary after five attempts, the secondary pings the gateway configured in the High Availability Tab and the default gateway for the appliance. See **Network Sentry Primary And Secondary Configuration** on page 730.

- If the gateway is reachable, after 30 seconds the secondary takes control, since the primary is assumed to be isolated from the network.
- If the gateway is not reachable, the secondary will not take control since the secondary is assumed to be isolated from the network and the primary could be functioning properly.

**Important:** If the secondary is Idle, it does not take control. For example, the secondary can be set to Idle when Reboot and Shutdown commands are run on the primary.

### CLI Control Scripts

The following scripts are used by Network Sentry to control the server and are located in `/bsc/campusMgr/bin`

Script	Description
<b>hsIsSlaveActive</b>	Determines if the secondary SQL server is performing replication.
<b>hsRestartCMMaster</b>	Executed on the Primary FortiNac Server, FortiNac Control Server, or FortiNac Control Manager appliance to recover after a failover. It copies the database and other files from the secondary appliance. Also resets the process states back to the master and restarts both servers.
<b>hsRestartCMRCMaster</b>	Executed on the primary FortiNac Application Server to recover after a failover. It copies all the required files from the secondary FortiNac Application Server. Also resets the process states back to the master and restarts both servers.

## Recovery

If high availability has been implemented and a failover has occurred, you must correct the reason for the failover before restarting your Primary Server.

### **Restart The Primary Server**

Use the **Resume Control** button on the Dashboard Summary panel to start the primary again. When the Resume Control button is clicked, critical files are copied from the secondary back to the primary and control is returned to the primary. On the FortiNac Server, FortiNac Control Server and FortiNac Control Manager appliances, the database is also copied.

If you are using high availability for a FortiNac Control Server and Application Server pair and this configuration does not use a shared IP address, when failover occurs both servers failover. To return control to the primary pair, click the **Resume Control** button on the Dashboard Summary panel for either of the two servers in the pair. This causes both the FortiNac Control Server and Application Server in the primary pair to start again and control is returned to both servers in the primary pair.

**Note:** If for any reason the database was not replicated correctly on the secondary before failover, the recovery process gives you the option of retaining the older database located on the primary.

1. Click **Bookmarks > Dashboard**.
2. Scroll to the **Summary** panel.
3. Click the **Resume Control** button for the server that should resume control.
4. The primary server restarts. Database and configuration files are copied from the secondary to the primary. Processes are started on the primary. Then the secondary server relinquishes control.

**Note:** This process may take a few moments while the data is synchronized between the two servers.

To restart the primary manually see the table of **CLI Scripts** on page 740.

**Manually Restart, Stop Or Force A Failover**

The scripts in the table below allow you to control High Availability from the CLI. Scripts to restart the primary servers vary depending on the configuration implemented. For configuration options see **Network Sentry Primary And Secondary Configuration** on page 730.

**Table 39: CLI Scripts**

Server Type	Primary Recovery	Shutdown Without Failover	Shutdown With Failover
<b>HA Configuration - Shared IP Address</b>			
FortiNac Server	hsRestartCMMaster	shutdownCampusMgr	shutdownCampusMgr -kill
FortiNac Control Server			
FortiNac Control Manager			
FortiNac Application Server	hsRestartCMRCMaster	shutdownNessus	shutdownNessus -kill
<b>HA Configuration - No Shared IP Address</b>			
FortiNac Control Server	hsRestartPair (restarts both servers in the pair)	shutdownCampusMgr	shutdownCampusMgr -kill
FortiNac Application Server	hsRestartPair (restarts both servers in the pair)	shutdownNessus	shutdownNessus -kill

## Stop The Primary Server

To stop the processes on the primary Server *without* causing a failover (for example, for routine maintenance and quick restart), use this command: `shutdownCampusMgr`. When you use the `shutdownCampusMgr` command on the primary, the management process tells the secondary not to take control by setting the secondary state to Idle. This prevents a failover from occurring.

When the command listed below is run on the primary server, it stops the `campusMgr` processes and causes a failover to the secondary Server.

```
shutdownCampusMgr -kill
```

Refer to the **CLI Scripts** on page 740 table for additional scripts.

### Troubleshooting Tips

**Note:** Prior to configuring High Availability, ensure that all appliances are able to communicate (i.e. firewall is not blocking communication).

Use these troubleshooting tips to:

- If you have implemented High Availability using a Shared IP address, determine which appliance has the shared IP.
- Determine the status of your appliances including:
  - which is primary/secondary
  - which has control
  - is secondary idle
- Confirm that replication of the database is occurring.
- Verify whether the license key is configured for High Availability.

### Determine Which Appliance Has The Shared IP

Enter `ip addr sh dev eth0` at the command prompt and look at the output to determine which `eth0` interface has the Shared IP Address (`eth0` of the primary or `eth0` of the secondary):

```
root@host name:/bsc/campusMgr/bin
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast
qlen 100
link/ether 00:30:48:79:62:24 brd ff:ff:ff:ff:ff:ff
inet 192.168.5.231/24 brd 192.168.5.255 scope global eth0
inet 192.168.5.230/24 scope global secondary eth0
```

In this example the Shared IP Address is 192.168.5.230. The `eth0` on the secondary has the Shared IP Address.

**Note:** Using a Shared IP address in your High Availability configuration is optional.

### Determine Appliance Status

The Summary panel on the Dashboard indicates the status of all appliances, which appliance has control and if an appliance is idle. To access this panel select **Bookmarks > Dashboard** and scroll to the Summary panel.

## Confirm Database Replication

When the primary server is started it attempts to communicate with the secondary. It continues to attempt communication until it connects to the secondary and can begin replicating the database.

When you make a change in the database of the primary, the database replication process makes the same change in the database of the secondary.

Navigate to the `/bsc/campusMgr/bin/` directory on the Secondary. Run the following script:

```
hsIsSlaveActive
```

You should receive a response that is similar to the following:

```
root@Host Name:/bsc/campusMgr/bin
> hsIsSlaveActive
Host Host Name
SQL version 5.0.18,
slave is inactive
```

If the response contains the line `slave is inactive`, database replication is not active. If the response contains the line `slave is active`, database replication is active.

**Note:** If for any reason the database is not replicated correctly on the secondary before failover, the recovery process gives you the option of retaining the older database located on the primary.

## Verify License Key Configuration

The license key on both the Primary and Secondary appliances must be configured to be High Availability capable. The steps below provide verification that the key is configured correctly.

1. Navigate to the `/bsc/campusMgr/bin` directory.
2. Enter the following at the command prompt:
 

```
RunClient DumpKey.class
```
3. Look for Plugins: Hot-Standby-Capable
4. If this line is not displayed, the license key does not support High Availability. A new key is required.



## Appendix A: Scan Parameters

Endpoint Compliance Policies used to scan your hosts for compliance, have many variables for which the host machine can be scanned. For the anti-virus, anti-spyware and operating system variables, you can narrow the scan by setting custom parameters. For example, when scanning for a particular operating system you can require that the operating system be at Service Pack 4 or higher.

Any parameter that you modify will no longer be updated by the Auto-Def Updates scheduled task. That task updates the list of anti-spyware, anti-virus and operating systems for which you can scan. It also modifies parameters associated with each of those items to force hosts to use the most recent definitions for anti-virus and anti-spyware and to have installed the latest updates to the operating system.

This section provides details about each type of variable and the detailed parameters within that can be set to narrow your scan further. Detailed lists include the following:

**Anti-Spyware Parameters** on page 746

**Anti-Virus Parameters - Windows** on page 751

**Anti-Virus Parameters - Mac OS X** on page 756

**Operating System Parameters - Windows** on page 758

**Operating Systems Parameters - Mac OS X** on page 1

## Anti-Spyware Parameters

The option to scan for Anti-Spyware applies only to hosts with a Windows operating system. Separate anti-spyware products are not available on the market for other operating systems. Those products are typically bundled with an anti-virus product.

The table below provides an alphabetical list of all of the possible parameters that can be configured for anti-spyware software. Only some of these parameters are used for any given anti-spyware program.

### Parameter Definitions

**Important:** \*\* Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.

**Note:** Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Parameter	Description	Typical Options
<b>Check for available Engine updates Live (No install).</b>	Select to check if any available Engine updates. The update will not be installed.	Check or Uncheck
<b>Check for available Signature updates Live (No install).</b>	Select to check if any available Signature updates. The update will not be installed.	Check or Uncheck
<b>Client Security Antimalware Service must be running</b>	Select a setting.	Enabled or Disabled
<b>Client Security State Assessment Service must be running</b>	Select a setting.	Enabled or Disabled
<b>Custom Scans</b>	Select the custom scans that you want to implement for the product.	Custom Scans
<b>Definitions Date</b>	The date of the required definition files.	**
<b>Definitions Label</b>	Enter the label for the Definitions Web Address. When a host fails the scan this label appears in the Failed Scan Results view.	Text entry

Parameter	Description	Typical Options
<b>Definitions Web Address</b>	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded.  When a host fails the scan this URL appears in the Failed Scan Results view.	URL
<b>Engine Version</b>	Required engine version number of the program.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	** > = >=
<b>Engine Version Label</b>	The label for the Engine Version web address.	Text entry
<b>Engine Version Web Address</b>	URL for the web page where the Microsoft Windows defender engine version information can be located. The administrator supplies either a local or Internet URL. This URL is displayed on the Failed Scan Results view if the host fails the scan.	URL
<b>Force Scan</b>	Forces anti-spyware to run.	Yes or No
<b>Label</b>	Enter a label. This label appears on the Results panel to identify which scan the host failed.	Text entry
<b>Operational Label</b>	Enter a label. This label will appear on the Results panel if the host fails the scan because the product operational state did not meet the requirement.	Text entry
<b>Operational Web Address</b>	Enter the URL of the web page that displays information about the failure cause if the host fails the scan.	URL
<b>Product Version</b> <b>Program Version</b>	The required version.  Select the operator that will apply to the version value found on the host machine: greater than, equal to, or both.	** > = >=
<b>Products to Detect</b>	Select which products you wish to include in the scan. All products are selected by default.  <b>Note:</b> Scan results show the group name (label) only, not the specific AV/AS product. The scan will either pass or fail for the group (label).	
<b>Program Version Label</b>	Enter the label for the Program Version.  When a host fails the scan for not having the required program version this label appears in the Failed Scan Results view.	Text entry

<b>Parameter</b>	<b>Description</b>	<b>Typical Options</b>
<b>Program Version Web Address</b>	Enter the URL of the web page where the required program version can be located and downloaded.  When a host fails the scan for not having the required program version this URL appears in the Failed Scan Results view.	URL
<b>Prohibit this Product</b>	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
<b>Protection Updates</b>	The required Protection Updates number. Format varies by product.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Protection Updates Label</b>	The label for the Protection Updates web address.	Text entry
<b>Protection Updates Web Address</b>	The URL for the web page where the Protection Updates information can be located. The administrator supplies either a local or Internet URL. This URL will be displayed on the Failed Scan Results view if the host fails the scan.	URL
<b>Run Update Command</b>	Forces the Update command to run when the host is checked.	Yes or No
<b>Scan Arguments</b>	Command line arguments that will be automatically entered when the program runs.	Command line arguments
<b>Signature Label</b>	The label for the Spyware Signatures address. This label will appear on the Results panel.	Text entry
<b>Spyware Definition</b>	Used to identify the Spyware definition version installed. May be the name of the definition file, the date of the file, a version number, etc.  Select the operator to apply to the definition value found on the host machine: more than, equal to, or both.	**  > = >=
<b>Spyware Pattern</b>	The number for the required pattern definition files. Format varies by product.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=

Parameter	Description	Typical Options
<b>Spyware Signatures Address</b>	The URL for the web page where the information for the Spyware Signatures can be located. The administrator supplies either a local or Internet URL. This URL will be displayed on the Failed Scan Results view if the host fails the scan.	URL
<b>Spyware Signatures Label</b>	The label for the Spyware Signatures address.	Text entry
<b>Spyware Signatures (Version)</b>	The required spyware signature version.  Select the operator that will apply to the version value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Stand-Alone Product Version</b>	The required version for the stand-alone product. Format varies by product.	**
<b>Stand-Alone Spyware Definition</b>	The required definition number if using the stand-alone product.	**
<b>Virus Definition</b>	Used to identify the definition version installed. May be the name of the definition file, the date of the file, a version number, etc.  Select the operator that will apply to the definition value found on the host machine (greater than, equal to, or both.)	**  > = >=
<b>Web Address</b>	Enter the URL of the web page that displays information about the product when the host fails the scan.	URL
<b>Windows Operating System</b>	Select any or all Windows Operating Systems required for the selected product.	
<b>Software Specific Parameters</b>		
<b>AVG Anti-Spyware 7.5 must be running</b>	Indicates whether the product must be running on the host machine for the scan to pass.	Enabled or Disabled
<b>CA-Pest Control Spyware Definition v5</b>	The date of the required definition files for version 5.	YYYY-MM-DD
<b>PCTools -Spyware - Doctor Spyware Definition 5.0+</b>	Date of the required Spyware Definition 5.0+ files.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	YYYY-MM-DD  > = >=

## Appendix A: Scan Parameters

---

Parameter	Description	Typical Options
<b>Sophos</b>	Virus definition settings are configured in the product.	
<b>Virus Definition</b>	Use Windows Explorer to go to <code>Windows/Anti-Virus/Sophos</code> and configure the product.	

## Anti-Virus Parameters - Windows

The table below provides an alphabetical list all of the possible parameters that can be configured for anti-virus software for Windows. Only some of these parameters are used for any given anti-virus program.

### Parameter Definitions

**Important:** \*\* Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.

**Note:** Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Parameter	Description	Typical Options
<b>AntiVirus definition Date</b>	The date of the required AntiVirus definition files.	YYYY-MM-DD
<b>AntiVirus Engine</b>	The version number of the required AntiVirus Engine.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=
<b>Client Security Antimalware Service must be running</b>	Select a setting.	Enabled or Disabled
<b>Client Security State Assessment Service must be running</b>	Select a setting.	Enabled or Disabled
<b>Custom Scans</b>	Select the custom scans that you want to implement for the product.	Custom Scans
<b>Daily Virus Definition</b>	The version of the required daily definition files.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=
<b>Definitions Label</b>	Enter the label for the Definitions Web Address.	Text entry

## Appendix A: Scan Parameters

Parameter	Description	Typical Options
<b>Definitions Web Address</b>	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Definitions Version</b>	The version of the required definition files.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=
<b>Engine Version</b>	The number of the required engine version.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=
<b>Engine Version Label</b>	Enter the label for the Engine Version Web Address.	Text entry
<b>Engine Version Web Address</b>	Enter the URL for the web page where the updated engine version for the selected product can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Label</b>	Enter a label. This label will appear on the Results panel to identify which scan the host failed.	Text entry
<b>Macro Definition</b>	The date of the required macro definition files.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	YYYY-MM-DD  >  =  >=
<b>Main Virus Definition</b>	The version of the required main definition files.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=

Parameter	Description	Typical Options
<b>Minimum Engine Version</b>	Minimum engine version required to pass the scan.	**
<b>Operational Label</b>	Enter a label. This label will appear on the Results panel to identify that an operational state did not meet the requirement.	Text entry
<b>Operational Web Address</b>	Enter the URL of the web page that displays information about the product when the host fails the scan because the Client Security State Assessment or Antimalware Service operational state did not meet the requirement.	URL
<b>Operator (applies to all)</b>	The Engine version and definition (Virus and Spyware) values found on the host machine must be either greater than, equal to, or both than the value(s) entered.	> = >=
<b>Products to Detect</b>	Select which products you wish to include in the scan. All products are selected by default.  <b>Note:</b> Scan results show the group name (label) only, not the specific AV/AS product. The scan will either pass or fail for the group (label).	
<b>Program Version</b>	The version number of the program.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Program Version Label</b>	Enter the label for the Program Version Web Address.	Text entry
<b>Program Version Web Address</b>	Enter the URL for the web page where the required version can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Prohibit this Product</b>	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
<b>Protection Updates</b>	The date of the required Protection Updates file.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	YYYYMMDD  > = >+
<b>Protection Updates Label</b>	Enter the label for the Protection Updates Web Address.	Text entry

## Appendix A: Scan Parameters

Parameter	Description	Typical Options
<b>Protection Updates Web Address</b>	Enter the URL for the web page where the Production Updates can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Signature Version</b>	The build number or date and build number of the required signature file.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Signature Version Label</b>	Label for the Signature Version Web Address.	Text entry
<b>Signature Version Web Address</b>	Enter the URL for the web page where the required signature version can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Spyware Definition</b>	Number of the required spyware definition file.	**
<b>Version</b>	The number of the required virus definition file.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Version Label</b>	Enter the label for the Version Web Address.	Text entry
<b>Version Web Address</b>	Enter the URL for the web page where the required version can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Virus Definition</b>	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number, etc.  Select the operator that will apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=

Parameter	Description	Typical Options
<b>Virus Definition</b>		
<b>VDF</b> <b>Label</b>	The label for the VDF web address.	Text entry
<b>Virus Definition</b> <b>VDF</b> <b>Web Address</b>	The URL for the web page where updated definitions can be located and downloaded. Supply a local or Internet URL. This URL will be displayed on the Failed Policy Results view if the host fails the scan.	URL
<b>Virus Signature</b>	The date of the required virus signature.	YYYY-MM-DD
<b>Web Address</b>	Enter the URL of the web page that displays information about the product if the host fails the scan.	URL
<b>Windows Operating System</b>	Select any or all Windows Operating Systems required for the selected product.	
<b>Software Specific Parameters</b>		
<b>Eset-NOD32</b> <b>Minimum Scanner Version (nod32.exe)</b>	The number of the required scanner version of the file nod32.exe.	**

## Anti-Virus Parameters - Mac OS X

The table below provides an alphabetical list all of the possible parameters that can be configured for anti-virus software for Mac OS X. Only some of these parameters are used for any given anti-virus program.

### Parameter Definitions

**Important:** \*\* Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.

**Note:** Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Parameter	Description	Typical Options
<b>Definitions Label</b>	Enter the label for the Definitions Web Address.	Text entry
<b>Definitions Web Address</b>	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Engine Version Web Address</b>	Enter the URL of the web page where information about the engine version is displayed if the host fails the scan.	URL
<b>Engine Version Label</b>	Enter the label for the Engine Version Web Address.	Text entry
<b>Label</b>	Enter a label. This label appears in the Results page information to identify which scan the host failed.	Text entry
<b>Program Version</b>	The number of the required version.  Select the Operator to apply to the definition value found on the host machine: greater than, equal to, or both.	**  >  =  >=
<b>Program Version Label</b>	Enter the label for the Program Version Web Address.	Text entry
<b>Program Version Web Address</b>	Enter the URL for the web page where the required program version can be located and downloaded.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL

Parameter	Description	Typical Options
<b>Prohibit this Product</b>	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
<b>Version Label</b>	Enter the label for the Version Web Address.	Text entry
<b>Virus Definition</b>	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number, etc.  Select the operator to apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=
<b>Version Web Address</b>	Enter the URL for the web page where information about the version is displayed when the scan is failed.  When a host fails the scan this URL appears in the Failed Policy Results view.	URL
<b>Web Address</b>	Enter the URL of the web page where information about the product is displayed in case the scan fails.	URL
<b>Software Specific Parameters</b>		
<b>Clam Engine Version</b>	The number of the required engine version.  Select the Operator to apply to the definition value found on the host machine: greater than, equal to, or both.	**  > = >=

## Operating System Parameters - Windows

The table below contains an alphabetical list of possible Configuration Parameters that can be used when setting up scans for Windows Operating Systems. A subset of these parameters is available for each version of this operating system.

### Parameter Definitions

**Important:** Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Parameter	Description
<b>Allowed Editions</b>	Select the allowed editions. Options are Home Basic, Home Premium, Business, Enterprise, Ultimate, and Starter.
<b>Critical / Security Updates Label</b>	The Critical / Security Updates Label that displays on the results page.
<b>Critical / Security Updates Web Address</b>	The URL for the web page where Windows-Server-2008 Critical / Security Updates information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
<b>Custom Scans</b>	Any custom scans that have been created are shown.
<b>Disable Bridging</b>	When selected, disables bridging on the host machine.
<b>Disable Internet Connection Sharing</b>	When selected Internet Connection Sharing is disabled on the machine.
<b>Edition Label</b>	Enter a label. This label appears in the Results page information to identify which scan the host failed.
<b>Edition Web Address</b>	The URL for the web page where the specific edition information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
<b>Enable Automatic Updates</b>	See <b>Enable Automatic Updates Parameters</b> on page 760 table.
<b>Enable Windows Firewall</b>	When selected, the Windows Firewall is enabled.
<b>Force DHCP</b>	Requires write access to the registry if done through the dissolvable agent.  <b>Note:</b> Do not enable Force DHCP on policies that will be used for VPN clients. Enabling this setting can cause the host to continuously lose its VPN connection.
<b>Label</b>	Enter a label. This label appears in the Results page information to identify which scan the host failed.

Parameter	Description
<b>Prohibit Home Edition</b>	When selected, prohibits Windows-XP Home Edition.
<b>Require All Critical Updates</b>	When selected, all Critical Updates are required for the host machine.
<b>Require Critical Updates</b>	When selected, Require Critical Updates must be enabled on the host machine.
<p><b>Note:</b> Network Sentry leverages the Windows Update tool to check for Critical Updates and Security Updates during an operating system scan. The host must be able to connect to the Microsoft Windows Update web site and any other associated sites.</p>	
<b>Require Security Updates</b>	When selected will Require Security Updates to be enabled on the host machine.
<b>Require Service Pack</b>	When the checkbox labeled "Require Service Pack" is selected a text field displays. Enter the numeric value for the Service Pack Level.
<b>Service Pack Label</b>	The Service Pack Label that displays on the results page.
<b>Service Pack Level</b>	The required Service Pack Level. Enter the numeric value. Select the Operator to apply to the definition value found on the host machine: greater than, equal to, or both.
<b>Service Pack Web Address</b>	URL for the web page where Service Pack information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.
<b>Trigger SCCM Evaluation</b>	When selected, an upgrade is forced on the host from the SCCM controller. This ensures all hosts on the network are up-to-date.  <b>Note:</b> This option is available for Windows 7, 8, 10, Windows-Server-2012, Windows-Server-2008-R2, and Windows-Server-2012-R2.
<b>Updates Label</b>	The Updates Label that displays on the results page.
<b>Validate Edition</b>	When enabled, only those editions of Windows that are selected in Network Sentry are permitted. When disabled, all/any edition of the selected Windows operating systems will be allowed, such as Windows Vista N or Windows Vista K.
<b>Web Address</b>	The URL for the web page where Windows operating system information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.

### Enable Automatic Updates Parameters

When this option is checked for the selected operating system, it enables Automatic Updates on the host machine by modifying the registry. Additional configuration options appear once the box is selected. Use CAUTION when changing any of the Auto Update Settings. It is recommended that you are familiar with these options before you make any changes.

Auto Update Web Address	<input type="text" value="sma/windowsupdates.js"/>
Apply as a Policy (users can't modify)	<input type="radio"/> False <input checked="" type="radio"/> True
RescheduleWaitTime	<input type="text" value="4"/>
NoAutoRebootWithLoggedOnUsers	<input checked="" type="radio"/> False <input type="radio"/> True
NoAutoUpdate	<input type="text" value="0"/>
AUOptions	<input type="text" value="4"/>
AUState	<input type="text" value="2"/>
ScheduledInstallDay	<input type="text" value="0"/>
ScheduledInstallTime	<input type="text" value="3"/>
UseWUServer	<input checked="" type="radio"/> False <input type="radio"/> True
WUServer	<input type="text"/>
WUStatusServer	<input type="text"/>

Figure 266: Enable Automatic Updates Parameters Options

Parameter	Description
<b>Auto Update Web Address</b>	Web address used for Windows update. The default is sma/windowsupdates.jsp.
<b>Apply as a Policy (users can't modify)</b>	<p>Select True or False. Default = True.</p> <p>If this option is enabled, users of host machines running the selected version of Windows can no longer set Windows Update Parameters for their own machines. Registry keys for those settings are set by Network Sentry and are locked. Changing this option to False does not remove the lock from the registry keys. The keys must be deleted to restore user access to Windows Update settings. Keys are as follows:</p> <pre>SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate</pre> <pre>SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU</pre>
<b>RescheduleWaitTime</b>	<p>Time to wait between the time Automatic Updates starts and the time it begins installations, where the scheduled times have passed. The time is set in minutes from 1 to 60, representing 1 minute to 60 minutes).</p> <p><b>Note:</b> Note: This setting only affects host behavior after the hosts have updated to the SUS SP1 client version or later.</p>
<b>NoAuto RebootWithLoggedOnUsers</b>	<p>Select True or False. Default = False.</p> <p>If set to true, Automatic Updates does not automatically restart a computer while users are logged on. Note: This setting affects host behavior after the hosts have updated to the SUS SP1 host version or later.</p>
<b>NoAutoUpdate</b>	<p>0 = Automatic Updates is enabled.</p> <p>1 = Automatic Updates is disabled.</p> <p>Default = 0</p>
<b>AUOptions</b>	<p>1 = Keep my computer up to date has been disabled in Automatic Updates.</p> <p>2 = Notify of download and installation.</p> <p>3 =Automatically download and notify of installation.</p> <p>4 = Automatically download and schedule installation.</p>

Parameter	Description
<b>AUState</b>	<p>0 = Initial 24-hour timeout (Automatic Updates doesn't run until 24 hours after it first detects an Internet connection.)</p> <p>1 = Waiting for the user to run Automatic Updates</p> <p>2 = Detection pending</p> <p>3 = Download pending (Automatic Updates is waiting for the user to accept the pre-downloaded prompt.)</p> <p>4 = Download in progress</p> <p>5 = Install pending</p> <p>6 = Install complete</p> <p>7 = Disabled</p> <p>8 = Reboot pending (Updates that require a reboot were installed, but the reboot was declined. Automatic Updates will not do anything until this value is cleared and a reboot occurs.)</p>
<b>ScheduledInstallDay</b>	<p>0 = Every day.</p> <p>1 - 7 = The days of the week from Sunday (1) to Saturday (7).</p>
<b>ScheduledInstallTime</b>	The time of day in a 24-hour format (0-23).
<b>UseWUServer</b>	<p>Select True or False</p> <p>Use or not use a server that is running Software Update Services instead of Windows Update.</p>
<b>WUServer</b>	<p>http://&lt;server&gt;</p> <p>This value sets the SUS server by HTTP name (for example, http://IntranetSUS).</p>
<b>WUStatusServer</b>	<p>http://&lt;server&gt;</p> <p>This value sets the SUS statistics server by HTTP name (for example, http://IntranetSUS).</p>

**Important:** If you configure the scan to enable Automatic Updates and an error occurs (for example, a network or permission error) so that the scan cannot perform the update, then the scan might fail.





Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.