



ENTRUST

nShield Monitor

Monitor v2.9.0 Install and User Guide

9 April 2024

Table of Contents

1. Introduction	1
2. Requirements	2
2.1. General Requirements	2
2.2. Centralized Monitoring	3
2.3. Client Workstation	3
2.4. Role Based Access	3
2.5. Accessing the User Guide	6
3. License Installation	8
3.1. Overview	8
3.2. Installing a License	9
4. Setup Wizard	11
4.1. Overview	11
4.2. Wizard	11
4.3. Setting up the Network	17
4.4. Master Key Generation	18
4.5. Date/Time	19
4.6. Ready to Setup	21
4.7. Log In	22
5. Configuration Logged in as Administrator	24
5.1. Overview	24
5.2. First Time Setup	25
5.3. Edit Profile page	32
5.4. Configuration Tab tasks	36
6. Configuration Logged in as Group Manager	79
6.1. Overview	79
6.2. Edit Profile page	79
6.3. Managed Entities	80
6.4. Group Alarm Thresholds	90
6.5. Group Event Notification	93
7. Logs	98
7.1. Logs available to Group Managers	98
7.2. Logs available to Administrators	99
7.3. Log Sorting	101
7.4. Log Functionality	102
8. Dashboard	108
8.1. Event List	109
8.2. nShield Performance	112

8.3. Users	120
8.4. nShield Monitor Status	121
8.5. Unacknowledged Alarm Summary	122
9. Views	125
9.1. Logged in as Administrator	125
9.2. Logged in as Group Manager	125
9.3. View > Group > Group List	134
9.4. Additional Views available to the Group Manager	157
10. Reports	208
10.1. Generating Reports	208
10.2. Scheduled Reports	223
11. Alarms	228
11.1. General Description	228
11.2. Acknowledging Alarms in Bulk	228
11.3. Acknowledging an Alarm (individual basis)	229
12. nShield CLI Commands	231
12.1. GUI initialization	231
12.2. Setting Password	231
12.3. Master key status	231
12.4. CLI Setup Wizard	232
12.5. Welcome	232
12.6. EULA	233
12.7. Set User's Email	233
12.8. Create Administrators	234
12.9. Configure Network	234
12.10. Generate System Key	236
12.11. Configure Date & Time	237
12.12. Initialize	239
12.13. CLI Commands	240
12.14. Network commands	241
12.15. Date-time commands	243
12.16. System Commands	244
12.17. Email Queue Commands	246
12.18. Troubleshooting Commands	246
12.19. Service Commands	247
13. Licensing	248
13.1. Introduction	248
14. Enterprise Firewall Settings	249
15. Troubleshooting	250

15.1. Global Troubleshooting Enhancement feature	250
15.2. Network test tools	251
15.3. Ping	252
15.4. RouteDump	254
15.5. TCPDump	255
15.6. Traceroute	256
15.7. No Monitoring Data Received	256
16. nShield Monitor Alarm Conditions	257
17. nShield Monitor Backup and Restore	263
18. Deploying nShield Monitor	264
18.1. Centralized Monitoring	264
18.2. nShield Monitor Multi-Instance	264
18.3. Distributed Monitoring	264
18.4. Deployment Considerations	265
19. Residual Risk	267
19.1. User Guidance	267
19.2. Secure Operation	267
19.3. Risks	267
19.4. Deployment and Distribution	267
19.5. Secure Configuration	268
19.6. Host Machine	268
20. Install OVA With VMware ESXi	269
20.1. Introduction	269
20.2. Install the nShield Monitor OVA	269
20.3. Turn on the Virtual Machine	278
20.4. Run the Virtual Machine	279
21. Install OVA with VMware Workstation/Player	281
21.1. Introduction	281
21.2. Install the nShield Monitor OVA	281
21.3. Run the Virtual Machine	285
22. Create and Manage Hyper-V Virtual Machines in Hyper-V Core	287
22.1. Prerequisites for Using nShield Monitor with Hyper-V Virtual Machines	287
22.2. Install Hyper-V	287
22.3. Configure a New Virtual Machine with Hyper-V	288

1. Introduction

nShield® Monitor is a monitoring solution delivered in a virtual appliance environment. Designed to be both cost-effective and scalable, it delivers the level of security assurance expected of a Hardware Security Module (HSM) accessory supporting application.

Using a standard web-browser (Internet Explorer, Chrome (v 55.0) or Firefox), users connect to the nShield Monitor server via HTTP(s) using a configured IP address or through a user-friendly name. nShield Monitor provides a secure, authenticated connection allowing easy access to all monitored information.

nShield Monitor provides the following features:

- Able to monitor of estates composed of the nShield HSMs and client hosts
- Operates automatically in the background without human involvement
- Alerts users when investigation or intervention may be required
- Provides information relevant to each user based upon role and groups
- nShield Monitor provides the following benefits to an organization:
- Removes the need to pro-actively and regularly inspect each device to determine status
- Suitable to operate in "dark" data centers or in environments where physical access to devices is not possible
- Rapid and automatic notification of potential security issues
- Ability to react rapidly to device hardware failures (e.g., a power supply unit)
- Notification of unexpected changes to device configurations
- Immediate alerting of device overload
- General reporting of security, configuration, health and utilization of the estate of devices to support audit requirements

After the initial network setup and installation, the virtualized nShield Monitor server monitors HSMs and client hosts.

nShield Monitor provides a central repository of all information collected from your estate of devices and monitors information directly from the HSMs including device utilization, command information and HSM health. nShield Monitor also provides alarm and event notification (via syslog, SNMP, and email) as well as event logging and report generation from predefined templates.

2. Requirements

2.1. General Requirements

nShield Monitor is delivered in the following formats:

- Open Virtual Appliance (OVA)
- Microsoft Hyper-V

Both formats include:

- A 64-bit Linux-based OS
- Open VMware Tools (OVT)



By default, OVT service is DISABLED. A system administrator can choose to ENABLE OVT from the CLI. For details, refer to [Service Commands](#).

2.1.1. Hypervisor Compatibility

The OVA can be installed on the following virtual platforms:

- vSphere ESXi 6.0
- vSphere ESXi 6.5
- VMware Workstation 12
- VMware Workstation 14
- VMware Fusion 10
- Oracle VirtualBox 6.0

The Hyper-V image can be installed on the following virtual platforms:

- Microsoft Hyper-V
- Microsoft Azure

2.1.2. Server Requirements

- Must support 64 bit OS
- CPU: 2 cores of 2.0GHz multicore CPU (can be increased as needed)
- Memory: 8GB dedicated memory for nShield Monitor (can be increased)

- Network: Single network attached interface to bridged or physical network

Size on disk:

- Thin provisioned: 2.3 GB (OVA) / 3.3 GB (Hyper-V)
- Thick provisioned: 326.0 GB (OVA)

2.1.3. nShield Compatibility

nShield Monitor is compatible with the following nShield HSM models and software versions:

- nShield Edge, Solo+, Solo XC, Connect+, and Connect XC
- Security World software v12.40 and higher

2.2. Centralized Monitoring

When monitoring an estate of HSMs (i.e., more than one HSM), reduce duplicating data by keeping your data in as few places as possible.



Multiple instances of your data may be **required** due to your organization's external requirements (e.g., due to regulatory issues, etc.).

2.3. Client Workstation

The client workstation is any Apple or Microsoft Windows workstation that has network connections to nShield Monitor and a supported browser (WebUI access) or SSH client (CLI access) that can access nShield Monitor.

The client workstation can perform various configuration, administrative tasks or group management tasks based upon defined roles.

2.4. Role Based Access

nShield Monitor supports role-based access.

Each nShield Monitor user role is associated with a predefined set of tasks, ensuring that a user with a specific role can perform only those tasks that are allowed by that role. For example, if a user is assigned the role of group manager,

the user cannot perform administrative tasks, such as creating users. Role-based access adds a level of security to the configuration and administration of nShield Monitor.

The following credential schemes are supported:

- nShield Monitor’s own credential scheme, see [Creating Users](#).
- Active Directory credentials, see [Active Directory authentication](#).

Active Directory authentication is set up by mapping Active Directory groups to nShield Monitor roles.



For users whose credentials were imported from Active Directory, **Configuration > Security** shows their own credentials in and for nShield Monitor. Changes made to passwords in nShield Monitor are not ported back automatically to the Active Directory server.



Users who are Active Directory administrators have no access or visibility to the credentials of other Active Directory users through **Configuration > Security**.

2.4.1. User Roles

The nShield Monitor role based administration model has the following role type:

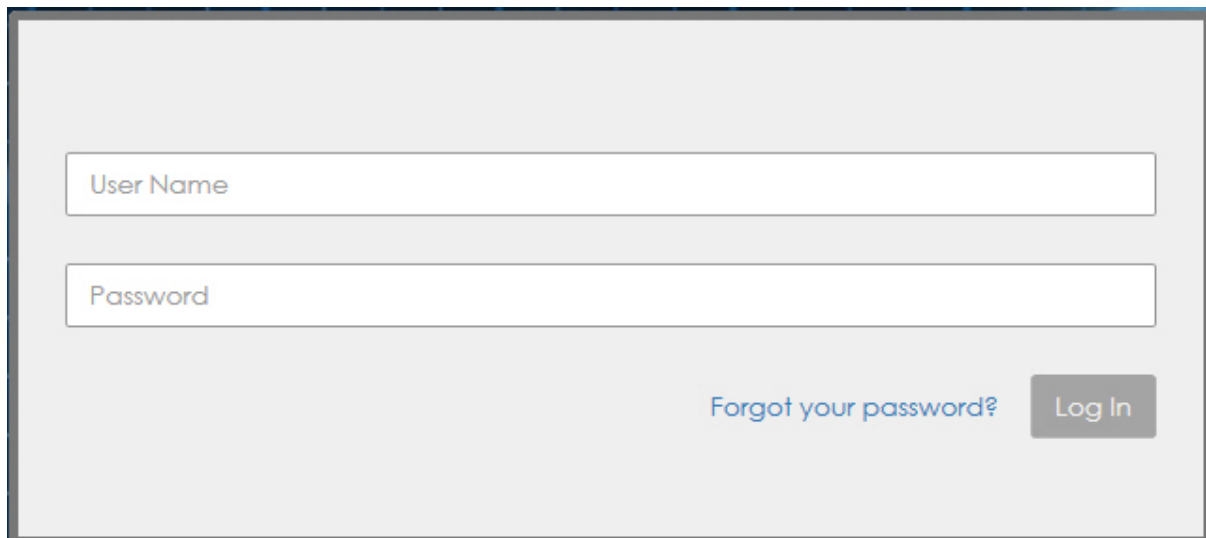
- Auditor
- Administrator
- Group Manager

Users can be assigned to more than one role. For example, a user could be both an Administrator and as a Group Manager. This user is then able to perform tasks related to both an administrator role and a group manager role.

For example, you could create users with the following combinations of permissions:

- User #1: administrator and group permissions
- User #2: auditor only
- User #3: group manager only

The nShield Monitor UI is role sensitive, and the pages displayed are dependent upon the role of the user.



The image shows a login interface with a light gray background. At the top, there is a white rectangular input field labeled 'User Name'. Below it is another white rectangular input field labeled 'Password'. To the right of the password field, there is a blue text link that says 'Forgot your password?'. Further to the right is a dark gray button with the text 'Log In' in white.

Figure 1.1: Login Prompts


2.4.1.1. Auditor

Auditors have complete visibility into nShield Monitor; however, they cannot modify any setting in nShield Monitor or on the HSMs.

 Auditors cannot be Administrators or Group Managers.

The auditor role is for visibility purposes.

2.4.1.2. Administrator

 Administrators are required to have sufficient knowledge of networks, various operating systems, and general system administration tasks such as configuring IP addresses, backing up systems, and using the console interface.

The Administrator is responsible for:

- User management, including creating new users, and deleting users who do not have any roles assigned to them
- Assigning administrator or group manager roles to users
- Network configuration
- System configuration
- Upgrading the system
- License management

- Security configuration
- Group management
- Event notification (syslog, SNMP and email) management
- Enabling the Open VMware Tools Service

2.4.1.3. Group Manager

Group Managers are required to have sufficient knowledge and understanding of:

- The importance of the data and devices that they manage
- Corporate policies with respect to data dissemination
- Corporate policies with respect to problem resolution

The Group manager is responsible for monitoring and understanding the following:

- The command instruction usage
- HSM utilization
- HSM health
- Event triggers in assigned groups
- Event logging and report generation in assigned groups
- Configuring event notification via email in assigned group

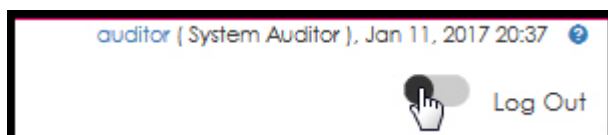
2.5. Accessing the User Guide

Online Help is available to all user role types.



While Online Help is enabled, you cannot perform any actions on the GUI.

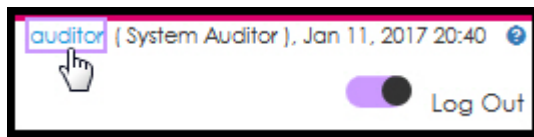
1. Log on as Administrator, Group Manager, or Auditor.
2. Locate the toggle switch in the upper right corner of the screen.



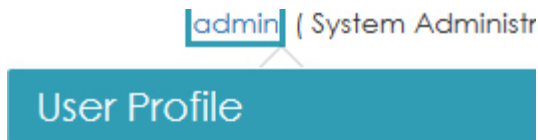
3. Slide the toggle switch to the right.

Online Help is enabled.

Fields surrounded by a **colored box** contain help.



4. Click a field to open the help text pop-up window.



A description of the user roles assigned to you is provided in parenthesis next to your user name. Clicking your username opens the profile information page. You can edit the following settings on this page:

- name
- description
- email
- password
- auto-logout duration by moving the slider

Save or **Cancel** your changes.

You can change the date and time formatting from the options in the drop-down list:

- None (default): if you do not select a format the default is used: Month, DD, YYYY, HH:MM
- UTC
- Month/Day/Year
- Day/Month/Year
- Custom: you can enter a custom format in the text box provided, use the example as a reference

3. License Installation

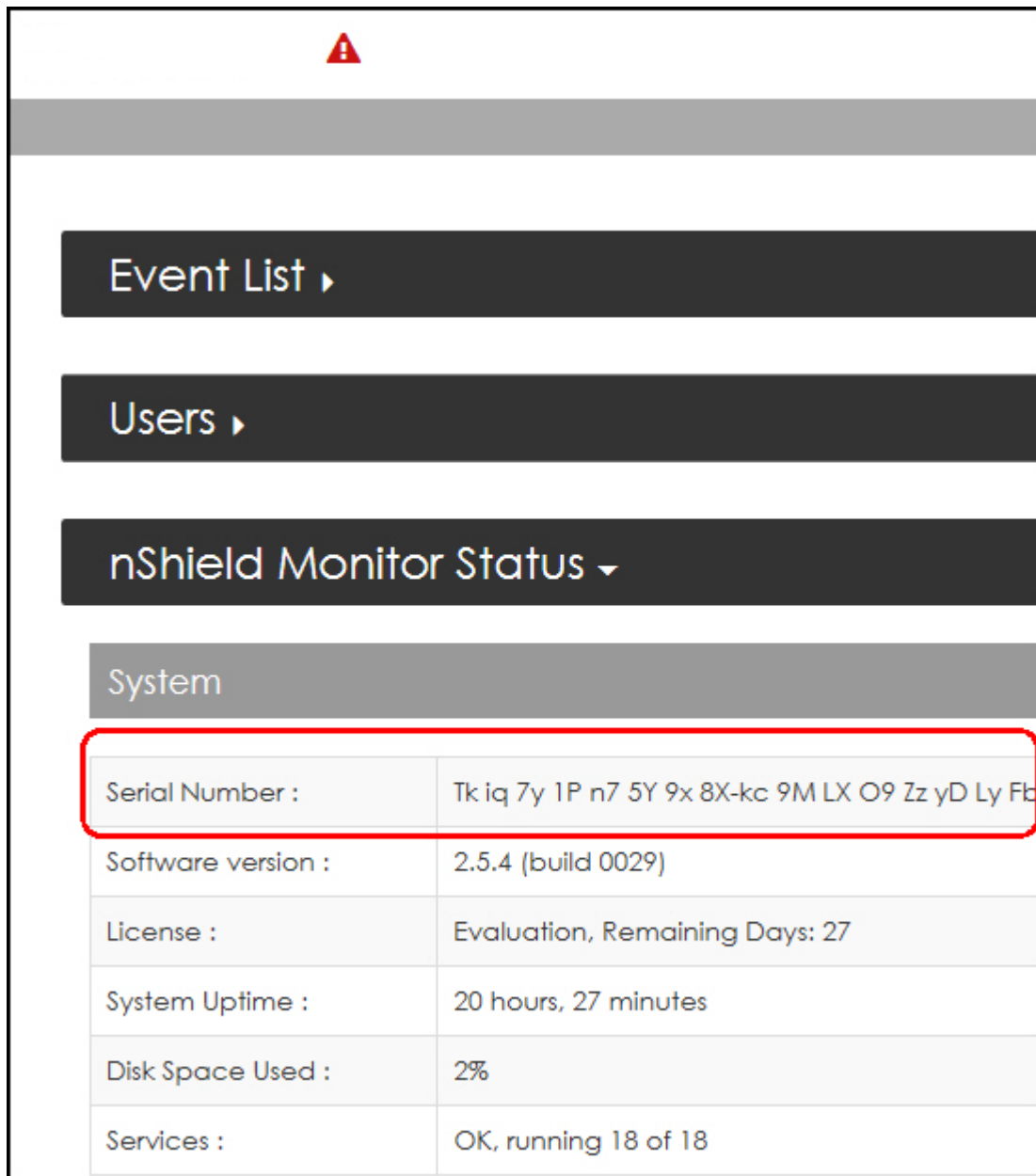
3.1. Overview

nShield Monitor is shipped with an evaluation license. This license allows for the Virtual Appliance to enroll and monitor up to eight devices for up to 30 days. After 30 days, the product automatically stops device monitoring and restricts user access to the administrator role only.

There are multiple license options available.



Contact Entrust Sales/Sales Support for prices and availability. Please have the serial number of the deployed nShield Monitor available in order to obtain a license. The serial number can be found on the dashboard page under the **nShield Monitor Status** tab.

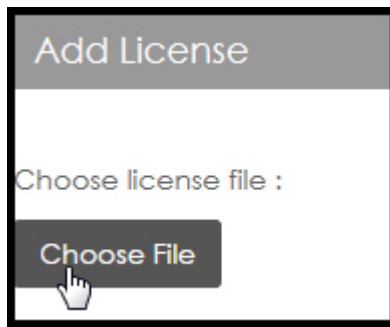


System

Serial Number :	Tk iq 7y 1P n7 5Y 9x 8X-kc 9M LX O9 Zz yD Ly Fb
Software version :	2.5.4 (build 0029)
License :	Evaluation, Remaining Days: 27
System Uptime :	20 hours, 27 minutes
Disk Space Used :	2%
Services :	OK, running 18 of 18

3.2. Installing a License

1. Download the license, provided by Entrust, to the local machine that is currently being used to access the nShield Monitor WebUI.
2. Log in as an **Administrator**.
3. Navigate to: **Configuration > License**
4. Click **Choose File**.



5. Browse to the license file.
6. Click **Open**.
7. Click **Install License**.

The license installs and details are viewable under the Current License(s) tab:

Current License(s)			
License Category	License Type	Max No. of Devices	Purchase Order
Standard	Device	200	5009



In addition to choosing the file, it is also possible to copy and paste the license code directly into the text box.

The Virtual Appliance is now ready to enroll and monitor devices up to the quantity of devices licensed.

4. Setup Wizard

4.1. Overview

nShield Monitor is delivered as an Open Virtual Appliance, OVA, format. The OVA includes a 64 bit Linux based OS. The nShield Monitor system can be accessed with a web browser.

Supported web browsers include:

- Firefox (Version 44 or higher)
- Internet Explorer (Version 11 or higher)
- Chrome (v 55.0)

4.2. Wizard

The initial setup of nShield Monitor upon first boot and login is done via a setup wizard. This setup wizard can be run both from the WebUI or the Command Line Interface (CLI). It is recommended that you use the WebUI Setup Wizard for initial setup of nShield Monitor.



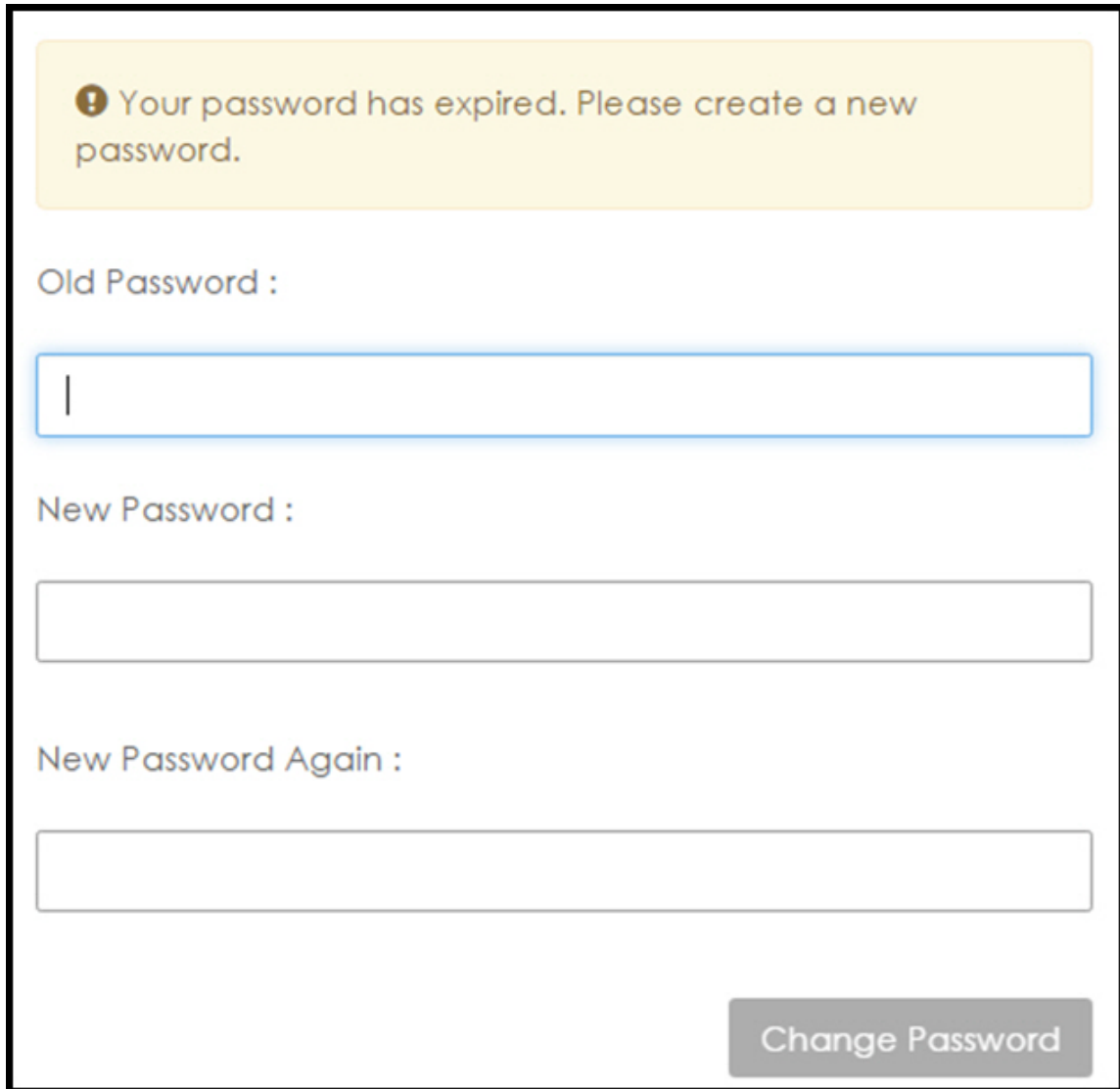
See [nShield CLI Commands](#) for details on how to setup using the CLI.

1. Access the Virtual Appliance from your Internet browser, go to:

```
https://XXX.XXX.X.XXX
```

(Use the IP address assigned in the CLI during the installation process.)

2. If the password was not changed during an initial OVA installation, via the CLI, enter the default admin username and password.
3. Followed by a new password.



! Your password has expired. Please create a new password.

Old Password :

New Password :

New Password Again :

Change Password

4. Click **Change Password**.

Once your password has changed (either using the CLI or the WebUI), the nShield Monitor Setup Wizard loads.

i | The Wizard prompts you through each tab.

1. Click **Start**.

The **EULA** page displays In order to continue to setup, you must accept the terms of the End User license Agreement (EULA) provided with the Virtual Appliance. If you decline the EULA, you will be automatically logged off.

2. Read through the entire EULA and then select **I Accept**.



The Email Setup page displays.

A screenshot of the 'Email Setup' page in a wizard. The page has a breadcrumb trail: 'Welcome', 'EULA', 'Email', 'System Administrators', 'Network', 'Key Generation', and 'Date and Time'. Below the breadcrumb is the text 'Ready to Setup'. The main heading is 'Set the Default User's Email Address'. There are two input fields: 'Email :' and 'Confirm Email :'. A 'Next Step' button is located in the bottom right corner.

3. Enter the email associated with the default user (admin).
4. Enter the email a second time to confirm and then click **Next Step**.

The **Create Administrators** page opens.

Welcome
 EULA
 Email
System Administrators
Network
Key Generation

Date and Time Ready to Setup

Create Administrators

Administrator One

User Name :

Email :

Confirm Email :

Administrator Two

User Name :

Email :

Confirm Email :

Next Step

4.2.1. Creating Administrators



nShield Monitor requires at least two administrators. During the setup, the system prompts to create two new Administrators (in addition to the default administrator which cannot be deleted during setup). The best practice recommendation is to come back and delete the default administrator, after you have successfully created your two official administrators, as described in the procedure below.

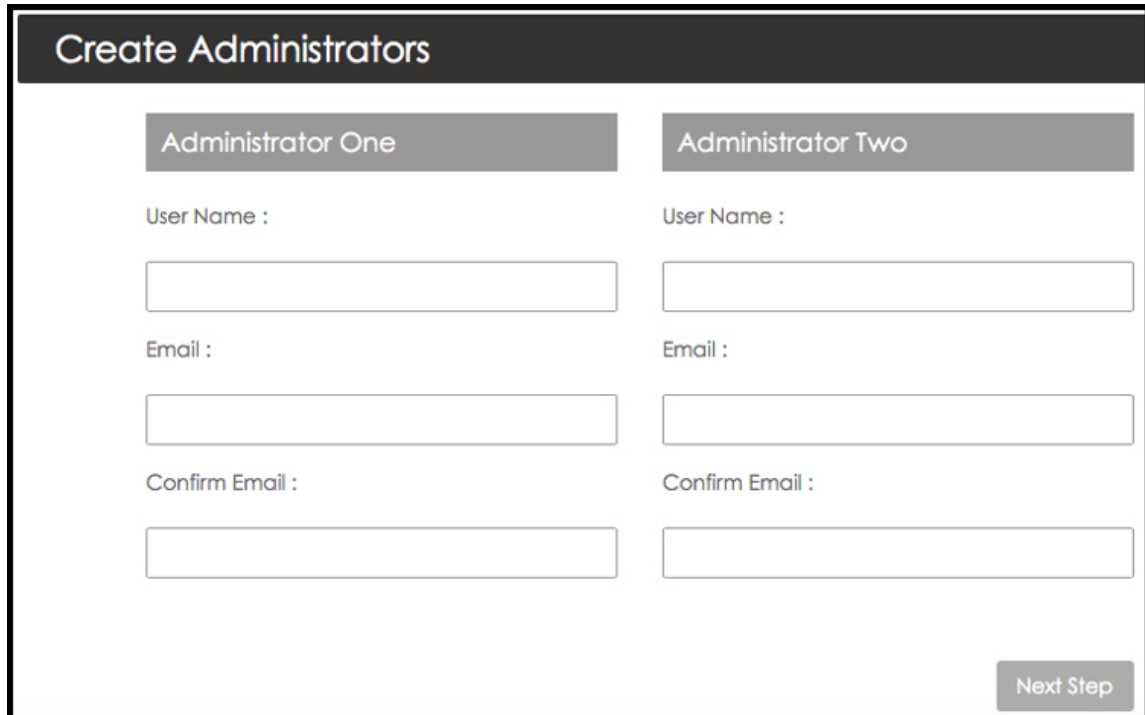
1. Enter the **User Name** (e.g., Admin1) and **Email** (and confirm email) for each

Administrator.

2. Select **Next Step**.

A one time password is automatically sent to the both Administrator email addresses.

The **Create Administrators** page displays:



The screenshot shows a web form titled "Create Administrators". The form is divided into two columns: "Administrator One" and "Administrator Two". Each column contains three input fields: "User Name", "Email", and "Confirm Email". A "Next Step" button is located at the bottom right of the form.

3. Complete the fields and then select **Next Step**.

The Network Settings page opens:

Welcome EULA Email System Administrators **Network**

Key Generation Date and Time Ready to Setup

Network Settings

DHCP Static

IP Address :

Subnet Mask :

Gateway :

Hostname:

Domain (optional) :

Primary DNS (optional) :

Secondary DNS (optional) :

Mail Host (optional) :

Mail Host Credentials (optional)

Next Step

4.3. Setting up the Network

To use nShield Monitor, you must setup a network.



Please do not change the following parameters without assistance from your IT support/infrastructure organization.

- IP Address
- Subnet
- Gateway
- Hostname
- Domain (optional)
- Primary DNS (optional)
- Secondary DNS (optional)
- Mail Host (optional)
- Master Key Generation



Mail Host Credentials are optional. Should you select the Mail Host Credentials box, a window opens prompting for **Mail Host User Name** and **Mail Host Password**.

1. On the **Network Settings** page, select **Next Step**.



The **Master Key Generation** page opens.

The screenshot shows a wizard interface for Master Key Generation. At the top, there are five progress indicators: 'Welcome', 'EULA', 'Email', 'System Administrators', and 'Network', all with checkmarks. Below these are three tabs: 'Key Generation' (active), 'Date and Time', and 'Ready to Setup'. The main heading is 'Master Key Generation'. The first section is 'Passphrase One', with a label 'Passphrase :' and an empty text input field. Below it is a label 'Confirm Passphrase :' and another empty text input field. The second section is 'Passphrase Two', with a label 'Passphrase :' and an empty text input field. Below it is a label 'Confirm Passphrase :' and another empty text input field. A 'Next Step' button is located in the bottom right corner.

4.4. Master Key Generation

The master key consists of an AES256 wrapping key and an HMAC-SHA-512 hash key that is used as the root of protection.

The master key is derived by using the two passphrases, using PBKDF2, that are input during the wizard configuration after the first boot and after every reboot.

The master key is never stored in persistent storage.

Please note to record each passphrase in a secure location as you will re-enter

them when nShield Monitor reboots.

1. Enter Passphrase One and Passphrase Two and then re-enter both for confirmation.

The screenshot shows a web-based setup wizard for nShield Monitor. At the top, there are three tabs: 'Key Generation' (selected with a checkmark), 'Date and Time', and 'Ready to Setup'. Below the tabs is a dark grey header with the text 'Master Key Generation'. The main content area is divided into two sections: 'Passphrase One' and 'Passphrase Two'. Each section contains a 'Passphrase :' label followed by a text input field with a green border and a green checkmark on the right, indicating successful entry. Below each input field is a 'Confirm Passphrase :' label followed by another text input field with a green border and a green checkmark. At the bottom right of the form is a dark grey button labeled 'Next Step'.

2. Record both phrases before continuing to the next step.
3. Select **Next Step**.

The **Date/Time Settings** page opens.

4.5. Date/Time

The Network Time Protocol (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit time to their client systems.



NTP Disable is the default setting. If you select NTP Enable, a new window opens and you are prompted to enter the NTP Server Address(es). You have the option of entering multiple servers, as long as you separate the entries with commas.

The screenshot shows the 'Date/Time Settings' window in the Setup Wizard. At the top, there are three tabs: 'Key Generation' (checked), 'Date and Time' (selected), and 'Ready to Setup'. Below the tabs is a dark header with the text 'Date/Time Settings'. Underneath, there are two radio buttons: 'NTP Enable' and 'NTP Disable' (which is selected with a checkmark). Below the radio buttons, there are three input fields: 'Time :', 'Date :', and 'Time Zone :'. The 'Time' field contains '19:42', the 'Date' field contains '02/10/2017', and the 'Time Zone' field is a dropdown menu showing '(GMT -05:00) Eastern Time (US & Canada)'. At the bottom right of the window is a 'Next Step' button.

4.5.1. NTP Disabled

1. Select **NTP Disable**.
2. Enter **Time**, **Date** and **Time Zone**.

The default setting is:

GMT Greenwich Mean Time.

3. Select **Next Step**.

The **Ready to Setup** page opens.

4. Continue to [Ready to Setup](#).

4.5.2. NTP Enabled

If NTP is enabled, you must indicate the NTP server that you want to use in the NTP Server Address field.



You can enter multiple servers, as long as you separate them using commas.

1. Use the drop down arrow to open the Time Zone drop down menu.
2. Select the appropriate **Time Zone**.
3. Select **Next Step**.

The **Ready to Setup** page opens.

4.6. Ready to Setup

1. Select **Initialize**.

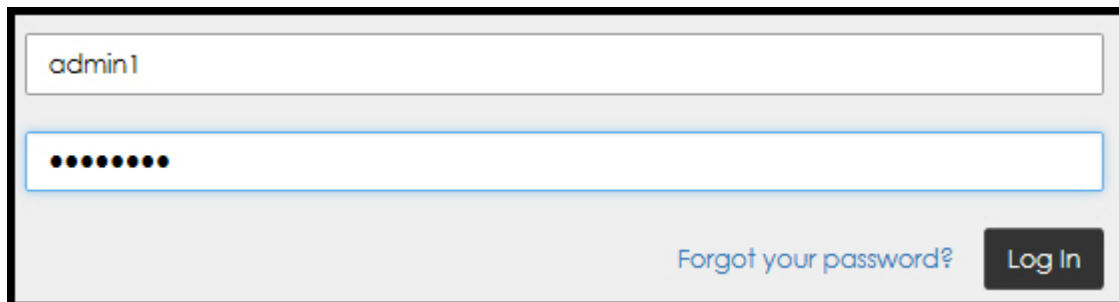
The initialization status page opens and tracks the process.

Initializing System		
Initialization Task	Status	Result
Generating Master key	✓	Master key generated an
Set Default User email address	✓	Email changed OK.
Create user 'admin1'	✓	User created OK.
Assign System Administrator role to 'admin1'	✓	Role assigned OK.
Create user 'admin2'	✓	User created OK.
Assign System Administrator role to 'admin2'	✓	Role assigned OK.
Setting Date/Time/NTP/Network values and rebooting	🔄	

nShield Monitor Reboots.

4.7. Log In

1. Enter your User ID and Password.



The image shows a login form with two input fields. The first field contains the text 'admin1'. The second field contains a series of black dots representing a password. To the right of the password field, there is a link that says 'Forgot your password?' and a dark button labeled 'Log In'.

2. Select **Log In**.

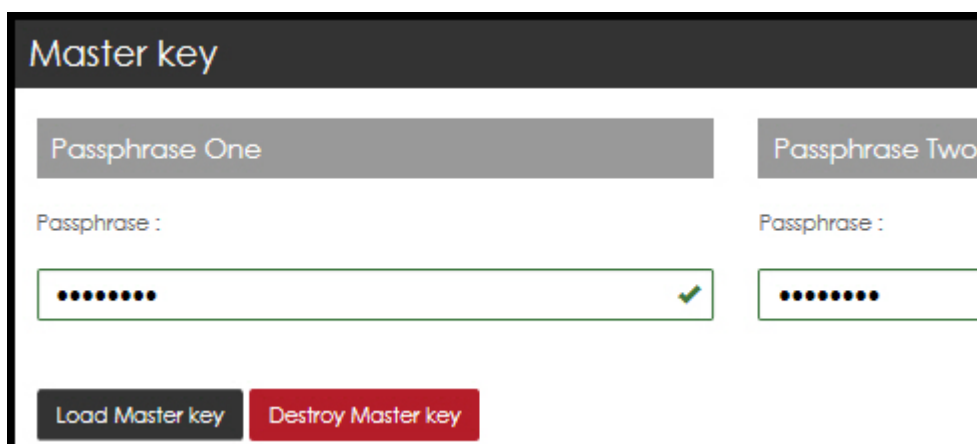
The Master Key needs to be reloaded every time that nShield Monitor is rebooted. After rebooting, you are prompted to enter the Master Key passphrase.



3. Select the message to initiate the Master Key load.

The Master Key / SSL Certificate and the User Interface SSL/TLS Options windows open.

4. Enter Passphrase One and Passphrase Two.



The image shows a 'Master key' configuration screen. It has two columns. The left column has a header 'Passphrase One' and a label 'Passphrase :'. Below it is an input field with black dots and a green checkmark icon. The right column has a header 'Passphrase Two' and a label 'Passphrase :'. Below it is an input field with black dots. At the bottom, there are two buttons: 'Load Master key' (dark grey) and 'Destroy Master key' (red).

5. Select **Load Master Key**.

The GUI session disconnects and the a pop-up reports:

Connection to nShield Monitor has been lost. If you have updated SSL Certificate, change the IP address or Hostname of nShield Monitor. You will need to open a new browser window to correct address. Attempting to reconnect.

6. After the system reconnects, log back on to the system.

The system is now ready to use.

5. Configuration Logged in as Administrator

5.1. Overview

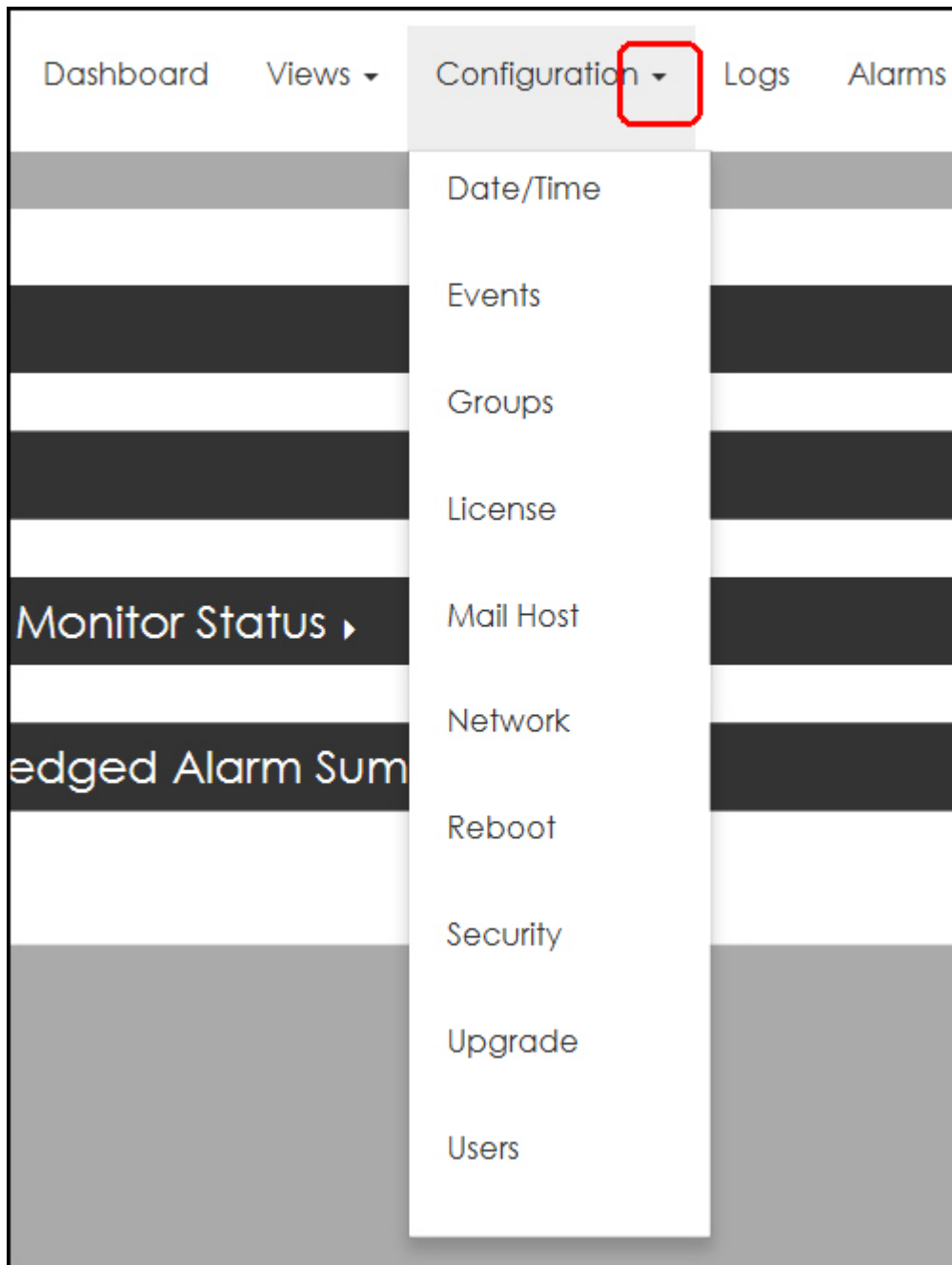
After setting up nShield Monitor, Administrators can modify the system setup via the **Configuration** tab.



To see the options available to a Group Manager, see [Configuration Logged in as Group Manager](#).

The Administrator is able to set date and time, events, create groups, update licenses, configure the network, reboot the system, set up security, perform upgrades, and set up users.

Logged on as an **Administrator**, the **Configuration** tab displays the following:



5.2. First Time Setup

In order to begin using nShield Monitor, several steps must be taken. These include:

- HSM configuration - verifying that the HSMs to be monitored are enabled for SNMP
- Installing the appropriate nShield Monitor License
- Creating groups and users in the nShield Monitor Virtual Appliance

- Enrolling devices to appropriate groups



Please note that a **device** can be assigned to **one group** or to **many separate groups**.

- Open firewall port settings

5.2.1. Configuring the nShield/Client Host

In order to properly manage your HSM estate with nShield Monitor, you must perform the following on each device:

- Enable SNMP and add SNMPv3 users
- Enable the collection of utilization data
- Set the period over which utilization statistics are to be collected to 60 seconds
- Enable the collection of health check counts

These tasks can be performed via the appropriate commands as follows:

- UTILCFG to set the period over which utilization statistics are to be collected.



Must be set for 60 seconds.

- UTILENABLE to enable the collection of utilization data
- HEALTHENABLE to enable collection of health check counts
- SNMP to enable provision of utilization and health check data via SNMP
- SNMPADD to add an SNMP community or user

5.2.2. Configuring the nShield HSM

Refer to the *SNMP V3 Agent for nShield Installation Guide* and to the *SNMPv3 Agent for nShield User Guide V3 User Guide* for the steps to follow in order to properly configure the nShield HSM.

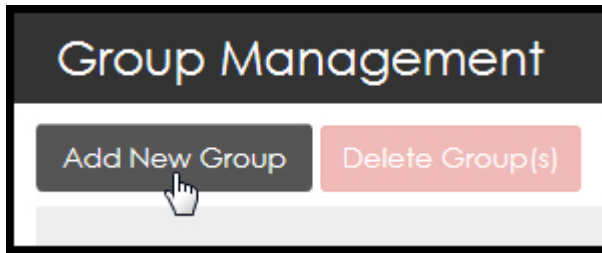
5.2.3. Step 1: Create Groups

In order to begin monitoring, the first required item is to create groups that will contain the monitored devices.

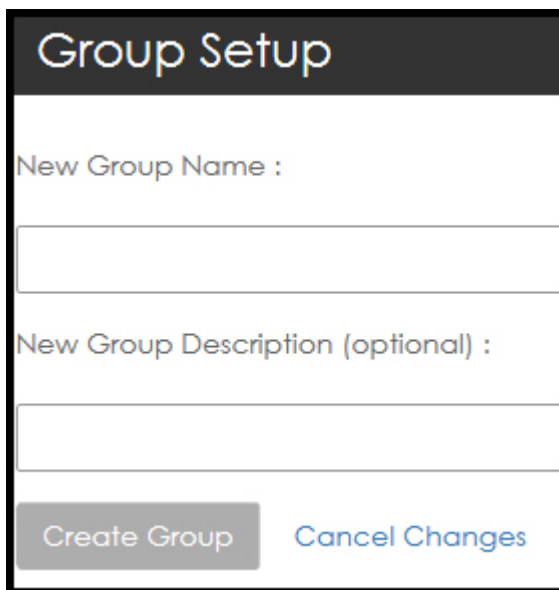


You must be logged in as an Administrator.

1. Navigate to **Configuration > Groups**.
2. Select **Add New Group**.



The **Group Setup** page opens.



3. Enter the **New Group Name** along with an optional description.
4. Select **Create Group**.



It is a best practice to never create more groups than the number required to manage the number of devices that you have.



nShield Monitor can support up to 32 groups.

5.2.4. Step 2: Configure the Group Manager Role

Once you have created your groups, you will need to configure one or more users with the Group Manager role.

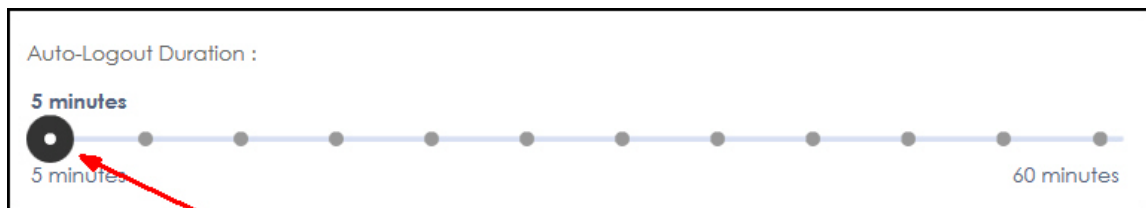


This procedure also includes how to associate a Group Manager with a group.

1. Navigate to: **Configuration > Users**.
2. The **Manage Users** page opens.
3. Select **Create User**.
4. The **Create a New User** page opens.
5. Enter the new user data.



You select the Auto-Logout Duration by sliding the circle to the right to increase the length of time.



Create a New User

User Name :

Full Name (optional) :

Description (optional) :

Email :

Confirm Email :

Auto-Logout Duration :

5 minutes

5 minutes 60 minutes

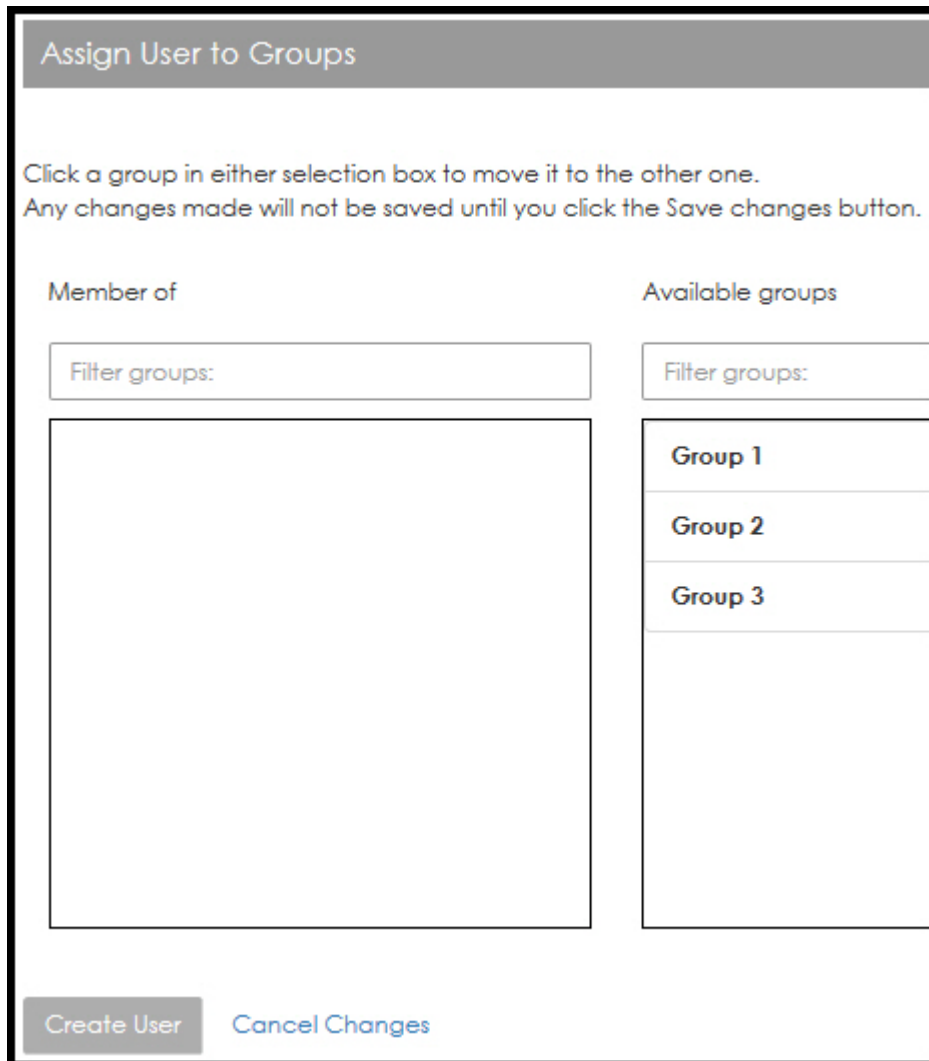
Password Expiration :

Monthly ▾

Assign Role(s) for this User :

No Role Administrator Group Manager Auditor

6. Complete the open fields appropriately and under **Assign Role(s) for this User**, select **Group Manager**.
7. The **Assign User to Groups** window opens.



Assign User to Groups

Click a group in either selection box to move it to the other one.
Any changes made will not be saved until you click the Save changes button.

Member of

Filter groups:

Available groups

Filter groups:

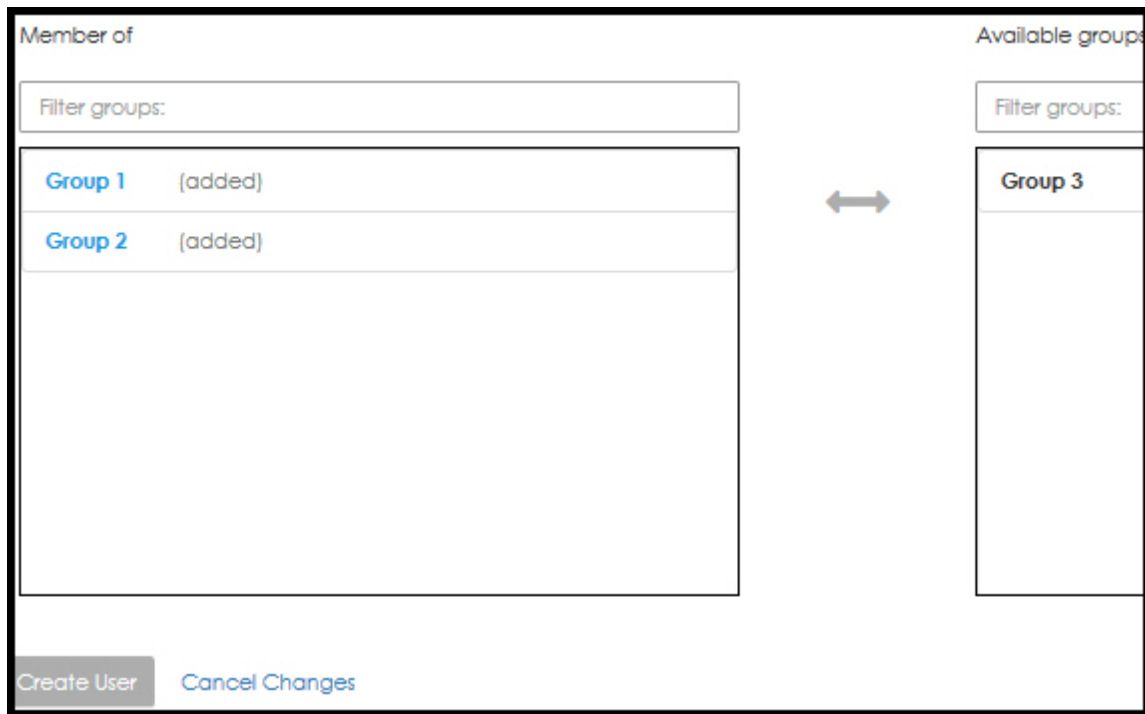
Group 1

Group 2

Group 3

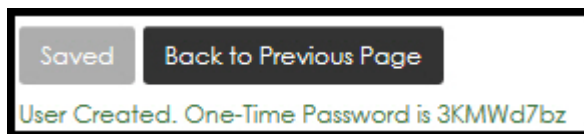
Create User Cancel Changes

8. Associate the user to groups by selecting the group name (e.g., Group 1).
9. When clicking on a Group name in the Available groups list, the group name moves to the **Member of** list.



10. Select **Create User**.

The User is created.



The one-time password is displayed on the screen and is emailed to the user.

5.2.5. Step 3: Group Manager Enroll Managed Entities to Groups

The Group Manager can add devices (i.e., enroll entities) to be monitored into the groups.

See [Configuration Logged in as Group Manager](#).

A Group Manager can be configured to access one group, a subset of all the groups or all of the groups in nShield Monitor.

Based on your current environment, the persons responsible for the day to day operations of the monitored devices are usually the appropriate persons to assign to this role.

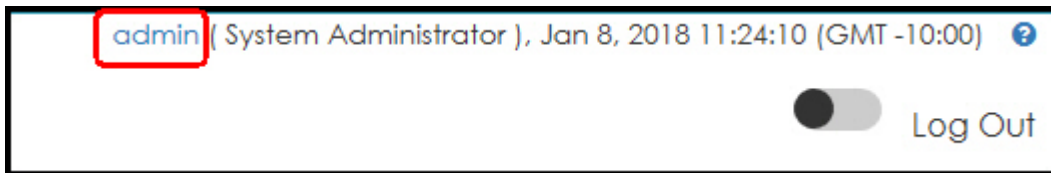


It is possible to assign a user to both Administrator and Group Manager roles. In doing so, operations and functions of both user

roles can be performed. You should refer to your organization's policy on whether a user with multiple roles is allowed to exist within your security management system.

5.3. Edit Profile page

The Edit Profile page is accessed by selecting (i.e., clicking on) your User ID located in the top right corner of the page.

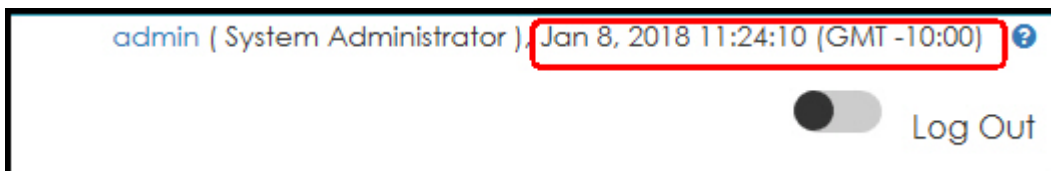


From this page, you can perform the following actions:

- Add a description
- Update the email address
- Change the password
- Set the Auto-Log duration
- Select a custom date format

When you select a custom date format, the chosen format is associated with your user ID giving each user the option of selecting their preferred format. Once the format has been selected, it is consistently displayed in accordance with your selection.

The only date format that will not change is the date in the User ID line, as shown below:



You can select the check box for **Use Browser Timezone for Exporting Events**, based on your preference.



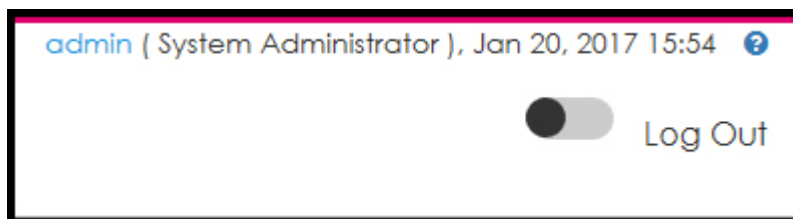
nShield Monitor keeps track of things like table column sort order, which sections of a page are collapsed/expanded, chart settings, etc., as part of your **GUI Persistence Profile**.

You are able to restore **Custom Date/Time Format** settings to the factory default through the **admin's GUI Persistence Profile** tab, **Reset to GUI Default** option.



5.3.1. Changing your Password and Email and set the Auto-Logout Duration

1. Click on the <user name> on the upper right hand corner of main screen, (e.g., click on **admin**).



The **Edit Profile** window displays:

2. To change the password:

Enter the old password in the **Change Password** field. As you type, the system will prompt.

As prompted, enter the new password once, and then again, to confirm.

3. To change your email:

Enter the new email in the **Email** field.

4. The Auto-Logout Duration is set to 60 seconds by default.

Use the slide to adjust this setting.

5. Select **Save User**.

5.3.2. Formatting the Admin Date and Time

1. Select the **Custom Date/Time Format** drop down arrow.

admin's Date/Time Formatting :

Custom Date/Time Format :

None (default) ▼

yyyy-MM-ddTHH:mm:ss.sss'Z'

(Example:)

Use Browser Timezone for Exporting Events

Save Date Format setting

The drop down menu opens.

admin's Date/Time Formatting :

Custom Date/Time Format :

None (default)
UTC
Month/Day/Year
Day/Month/Year
Custom Format

yyyy-MM-ddTHH:mm:ss.sss'Z'

(Example:)

Use Browser Timezone for Exporting Events

Save Date Format setting

2. Select your preferred format.
3. Select the **Use Browser Timezone for Exporting Events** check box to export logs/alarms using the same Date/Time format as that displayed on the web page.

Date/Time on all web pages display in the format configured in the User Profile.

By default, exported logs/alarms show Date/Time in GMT format.

4. Select **Save Date Format setting**.

5.3.3. Resetting the Admin GUI Persistence Profile

nShield Monitor keeps track of things like table column sort order, which sections of a page are collapsed/expanded, and chart settings, etc.

nShield Monitor also provides you with the means to reset Custom Date/Time Format settings for your profile.

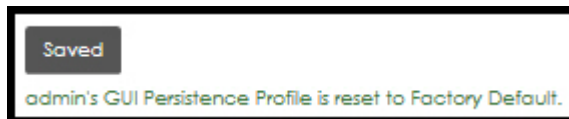


Selecting the **Reset to Factory Default** option **does not** affect nShield Monitor Configuration settings, but it does reset **Custom Date/Time Format settings** in your profile.

To return to the default for the **Date/Time format**:

1. Select **Reset to GUI Default**.

A confirmation message displays:



For more information, see [Managed entities](#).

5.4. Configuration Tab tasks

The nShield Monitor main menu page contains a **Configuration** tab. This tab provides quick links to individual pages. The following sections provide a brief discussion of actions available via the quick links.



For display purposes, the parameters displayed in this section are those found on the Configuration tab for the **Administrator user type**.

5.4.1. Active Directory authentication

Active Directory authentication is set up by mapping Active Directory groups to nShield Monitor roles.

Features of the integration between Active Directory and nShield Monitor:

- Auto-logout is set to five minutes for Active Directory users. This setting cannot be modified.
- Active Directory users under the **nSMUsers** hierarchy are tagged to **nSMGroups**. By default, three roles exist in **nSMGroups**. These roles map directly to the nShield Monitor user roles:

Active Directory	nShield Monitor
nSMAdministrator	Administrator
nSMGroup	Group Manager
nSMAuditor	Auditor

- The content of the **mail** field of Active Directory user profiles must be populated. nShield Monitor does not use the field. However, if it is empty when the user is imported from Active Directory to nShield Monitor, the user will not be able to log into nShield Monitor with their AD credentials.
- If a new user is created in the **nSMUsers** hierarchy in Active Directory, the user must log in to the Active Directory domain first, before being able to use the Active Directory credentials in nShield Monitor.
- When Active Directory authentication is enabled in nShield Monitor, user management is fully switched over to Active Directory:
 - nShield Monitor generated credentials, that is, non Active Directory credentials, cannot be used.
 - User creation and user editing is disabled in nShield Monitor.
 - Passwords cannot be updated from nShield Monitor. Passwords must be updated in Active Directory and the **Forget password link** is disabled in the nShield Monitor UI.

5.4.1.1. Configure Active Directory authentication

1. Save Active Directory server settings in nShield Monitor:
 - a. Navigate to: **Configuration > Active Directory > Credentials Settings**.
 - b. Enter the host name, the port number, the username and password for the Active Directory server.

For an LDAP connection, set the port to **636**, and import the certificate file and the private key on this tab.

c. Select **Save**.

2. Map Active Directory groups to nShield Monitor groups:

a. Navigate to: **Configuration > Active Directory > Map AD Groups**.

The list of Active Directory group is populated from the Active Directory server.

b. From the list, select a group, assign the relevant nShield Monitor roles to this group, then select **Save**.

c. Repeat the mapping step for each Active Directory group in the list.

Mappings that have been made between Active Directory groups and nShield Monitor roles are shown in a table at the bottom of the dialog.

3. Start the user import from the Active Directory with the group the users who will have the Group Manager role in nShield Monitor:

a. Navigate to: **Configuration > Active Directory > Import Group Managers**.

b. Select the Active Directory group that is to be mapped to the nShield Monitor Group Manager role, and select **Import**.

c. Assign nShield Monitor groups to each of these users. See [Editing users](#).



You must do all nShield Monitor user management activities at this point because user management will be fully switched over to Active Directory when Active Directory authentication is enabled. nShield Monitor's own user creation and user editing will be disabled.

4. After Active Directory users have been imported into nShield Monitor, finish the mapping of Active Directory users to nShield groups and users:

- Assign groups to the Group Manager role.
- Assign the Group Manager role to designated users.

5.4.1.2. Enable Active Directory authentication

1. Navigate to: **Configuration > Active Directory > Enable AD Authentication**.

2. Select **Use AD for Authentication**, then select **Save**.

3. Confirm the change.

The nShield Monitor UI restarts and Active Directory credentials can now be used for authentication.

5.4.1.3. Disable Active Directory authentication

To switch back to nShield Monitor's own authentication scheme:

1. Navigate to: **Configuration > Active Directory > Enable AD Authentication**.
2. Clear **Use AD for Authentication**, then select **Save**.
3. Confirm the change.

The nShield Monitor UI restarts and Active Directory credentials cannot be used for authentication. The nShield Monitor user management scheme is restored, including the ability to create, update, or delete users in nShield Monitor.

5.4.2. Date/Time

Navigate to: **Configuration > Date/Time**.

The **Date/Time Settings** window opens.

5.4.2.1. Date/Time - NTP Disabled

Most operating systems, including Windows, OS X, Linux, have an option to automatically synchronize the system clock periodically using a network time protocol (NTP) server. With nShield Monitor, you can toggle this option between disabled (off) and enabled (on).

This allows either manual configuration or setting up an NTP server to adjust time as needed.

1. Select **NTP Disabled**.

The screenshot shows the 'Date/Time Settings' configuration page. At the top, there are two radio buttons: 'NTP Disabled' (which is selected and highlighted with a red box) and 'NTP Enabled'. Below this, there are three input fields: 'Time' with the value '14:57', 'Date' with the value '12/05/2018', and 'Time Zone' with a dropdown menu showing '(GMT -08:00) Pacific Time (US & Canada); Tijuana'. At the bottom, there are two buttons: 'Save' and 'Cancel Changes'.

2. Enter data appropriately and select your Time Zone from the drop down menu.



The default Time Zone on nShield Monitor is GMT. Change it appropriately to match your organization's Time Zone.

3. Select **Save**.

5.4.2.2. Date/Time - NTP Enabled



Changing date, time, or NTP options will reboot nShield Monitor.

If NTP is enabled, you must indicate the NTP server that you want to use in the **NTP Server Address** field.

You can enter multiple servers, as long as you separate them using commas.

1. Select **NTP Enabled**.

Date/Time Settings

NTP Disabled **NTP Enabled**

NTP Server Address(es) :

0.us.pol.ntp.org ✓

Time :

14:57

Date :

12/05/2018

Time Zone :

(GMT -08:00) Pacific Time (US & Canada); Tijuana ▼

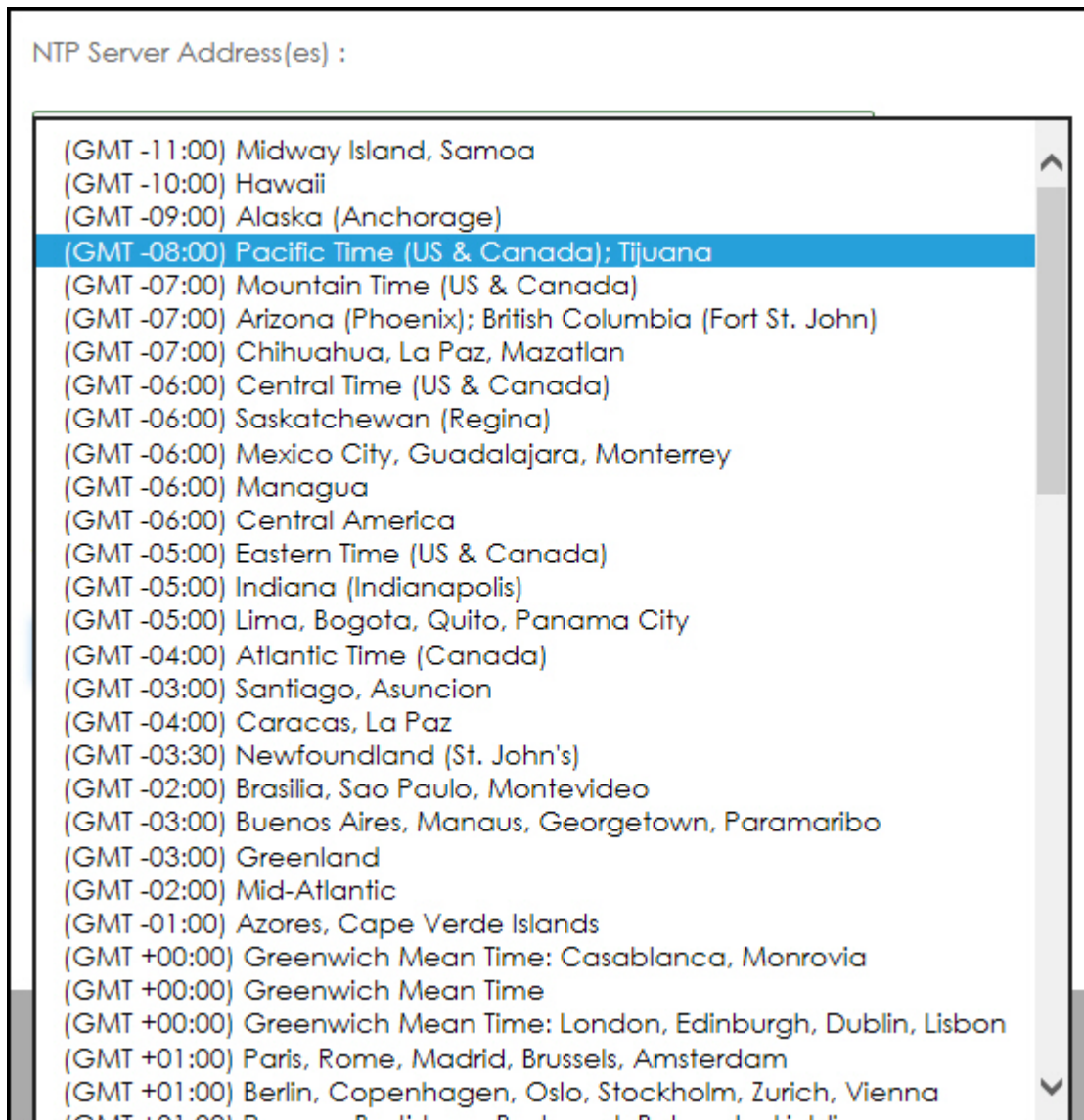
Save [Cancel Changes](#)

2. Enter the NTP Server Addresses (separated by commas).
3. Select the Time Zone drop down arrow to open your selections.



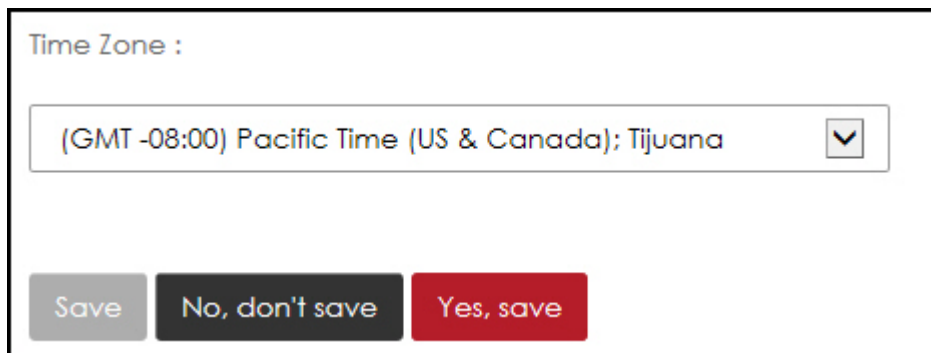
When NTP is enabled, the time and date field are already populated. You are not able to change them.

The default setting is: GMT Greenwich Mean Time.



4. Select your time zone.

The system prompts for confirmation:



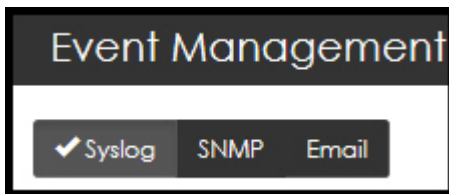
Changing date, time or NTP options **will reboot** nShield Monitor.

5. Select **Save**.

5.4.3. Events

nShield Monitor provides the capability for event notification via:

- Syslog
- SNMP and SNMP trap receiver
- Email



nShield Monitor can support up to 5 Syslog/SNMP servers at a time.

Navigate to: **Configuration > Events**.

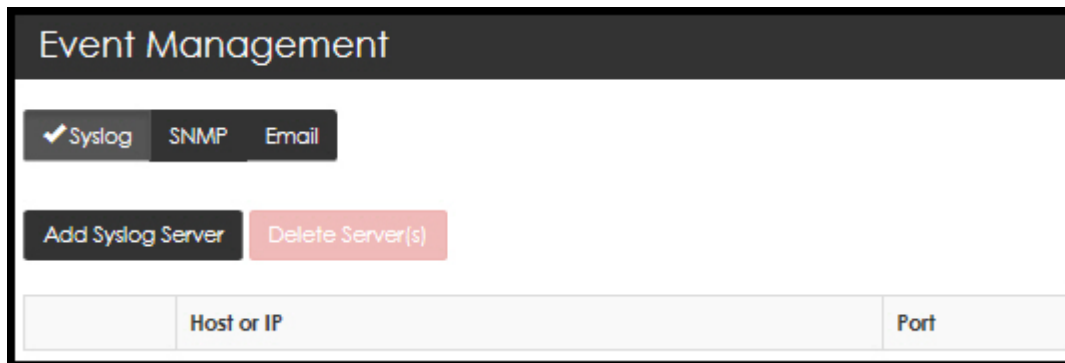
The **Event Management** page opens.

The screenshot shows the 'Event Management' configuration page. At the top, there are buttons for 'Syslog' (checked), 'SNMP', and 'Email'. Below these are 'Add Syslog Server' and 'Delete Server(s)' buttons. A table with columns 'Host or IP' and 'Port' is present but empty. A section titled 'Notification Policy: Remote Syslog' contains a table with columns for 'Policy Category' and notification levels: 'Info', 'Notification', 'Warning', 'Error', 'Critical', 'Alert', and 'Emergency'. All notification levels are currently unchecked. A 'Save Settings' button is at the bottom.

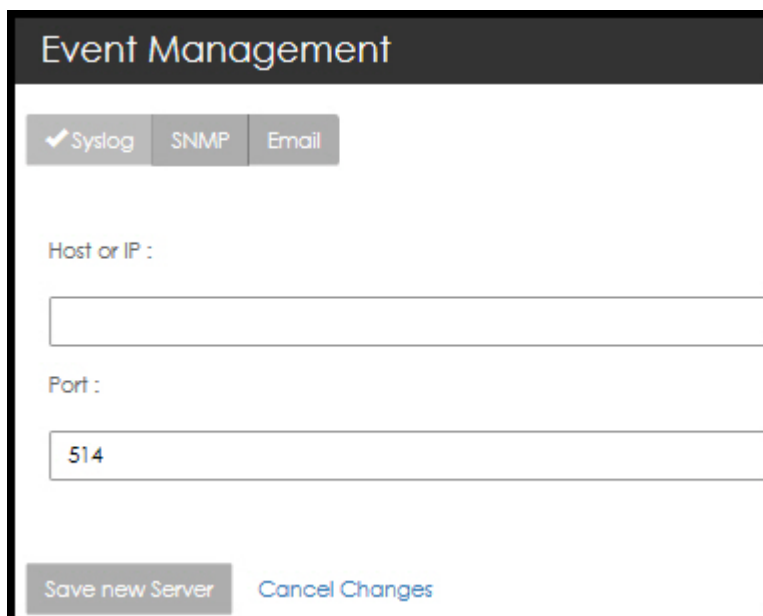
Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency
Monitor-Specific Security Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device-Group Specific Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitor-Specific General Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5.4.3.1. Adding a Syslog Server

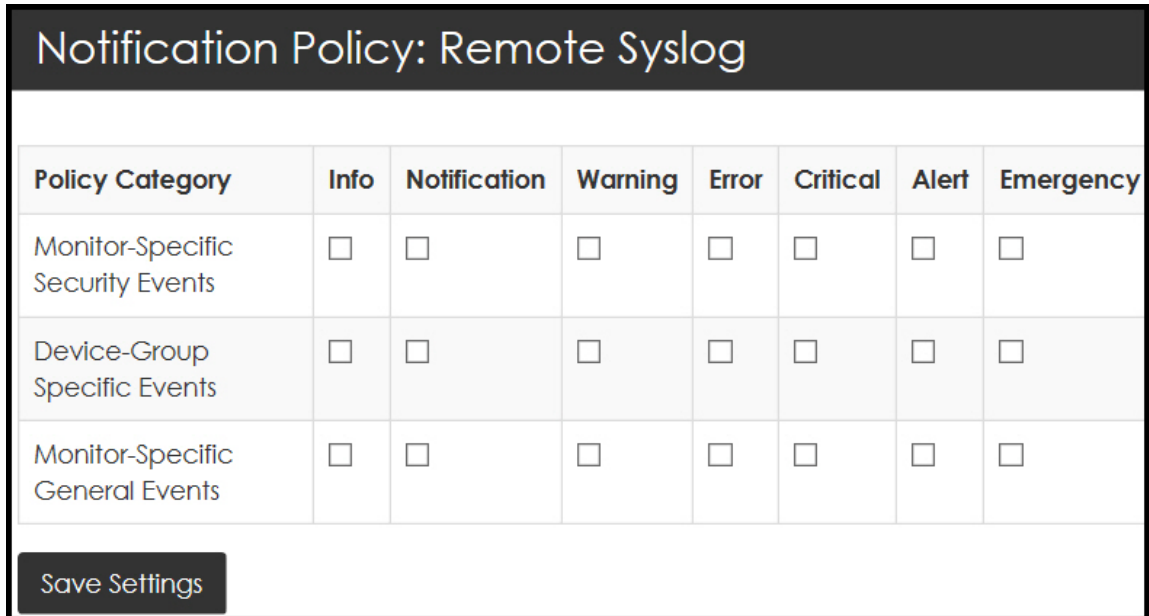
1. Navigate to: **Configuration > Events > Syslog.**



2. Click **Add Syslog Server.**



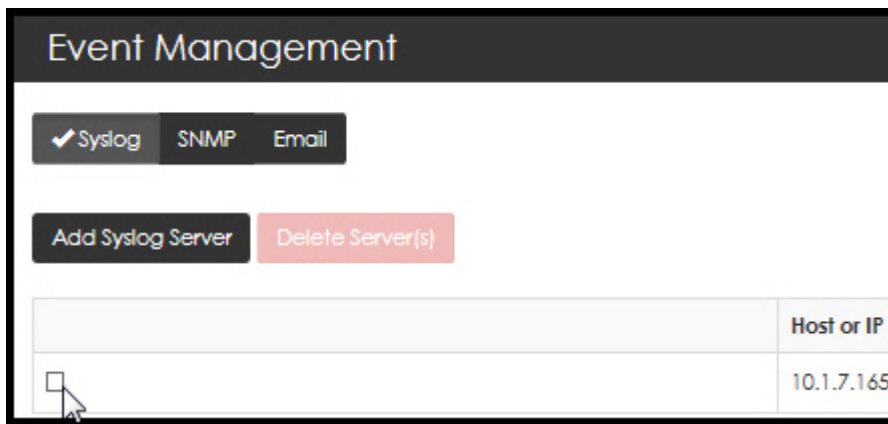
3. Enter the **Host or IP** of the syslog server.
4. Enter the **Port** number.
5. Click **Save new Server.**
6. Once the Syslog Server is configured, select the policy category and severity combination that you would like reported to the Syslog Server.



7. Select **Save Settings**.

5.4.3.2. Deleting a Syslog Server

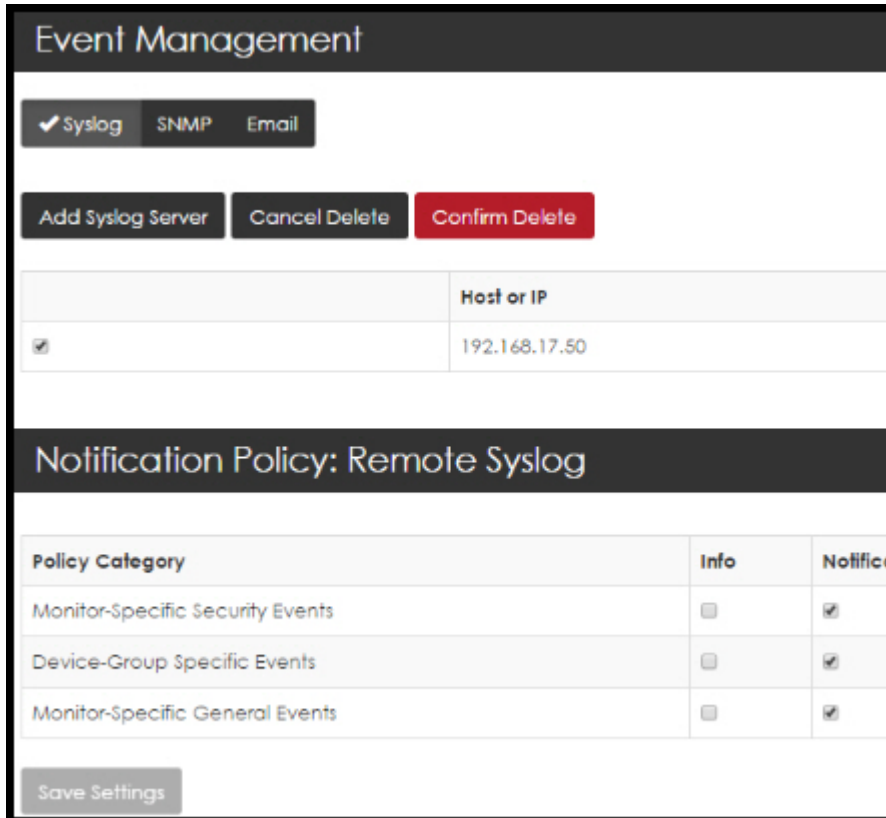
1. Select the check box associated with the HP or IP address of the Syslog server to be deleted.



The **Delete Server(s)** tab activates.

2. Select **Delete Server(s)**.

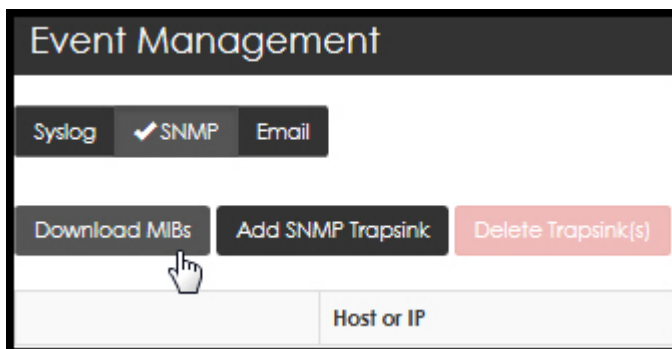
A confirmation page opens:



3. Select **Confirm Delete**.

5.4.3.3. Download MIBs

1. Navigate to: **Configuration > Events > SNMP**.
2. Select **Download MIBs**. The system prompts with the option to **Open**, **Save**, or **Cancel**.



3. Select your preference.

5.4.3.4. Support for nCSNMP traps

The nShield Monitor user interface provides event notifications for supported

nCipher SNMP (nCSNMP) traps on the Dashboard, Logs and Alarms pages.

- Policies can be set about the notification level, for example warning or emergency, for SNMP traps in general. These policies are managed by Administrators, [Assign Notification Policies for SNMP](#).
- Group Managers can associate these notification policies with device groups and trap groups:
 - [Assign SNMP Notification Policies for Groups](#).
 - [Assign SNMP Notification Policies for Trap Groups](#).

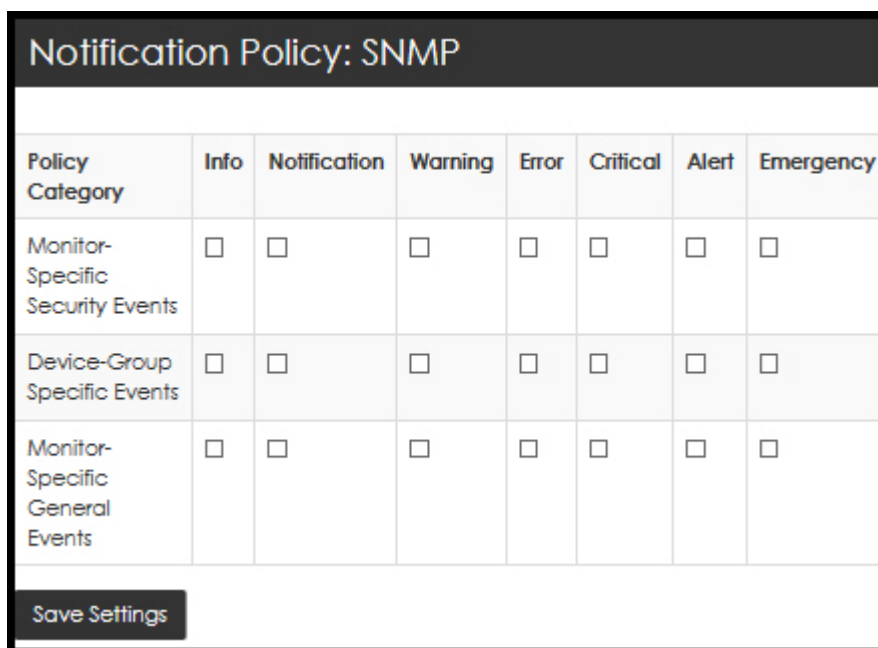
The following SNMP traps are supported:

Trap ID	Name	Severity	Trigger Event
hardserverAlert	Hard Server Failure	ERROR	The nShield host-side module control software failed
hardserverUnAlert	Hard Server Restart	NOTIFICATION	The nShield host-side module control software restarted after a previous failure event.
moduleAlert	Module Failure	ERROR	The nShield hardware failed.
moduleUnAlert	Module Restart	NOTIFICATION	The nShield hardware restarted after a previous failure event.
psuAlert	PSU Failure	ERROR	The power supply to an nShield Connect failed.
psuUnAlert	PSU Restart	NOTIFICATION	The power supply to an nShield Connect is now operational, after a previous failure event.
fanfailureAlert	Fan Failure	ERROR	The speed of an individual fan on the nShield Connect is zero.
fanfailureUnAlert	Fan Restart	NOTIFICATION	Fan speed is now non-zero, after a previous failure event.
memoryUsageHighAlert	Memory Usage High	ERROR	The HSM memory usage high threshold has been reached.

Trap ID	Name	Severity	Trigger Event
memoryUsageOkAlert	Memory Usage Normal	NOTIFICATION	The memory usage is below the HSM memory usage ok threshold.

5.4.3.4.1. Assign Notification Policies for SNMP

1. Sign in as Administrator.
2. Navigate to: **Configuration > Events > SNMP.**
3. Select your preferences for the Policy Categories.



4. Select **Save Settings.**

5.4.3.4.2. Assign SNMP Trap Settings

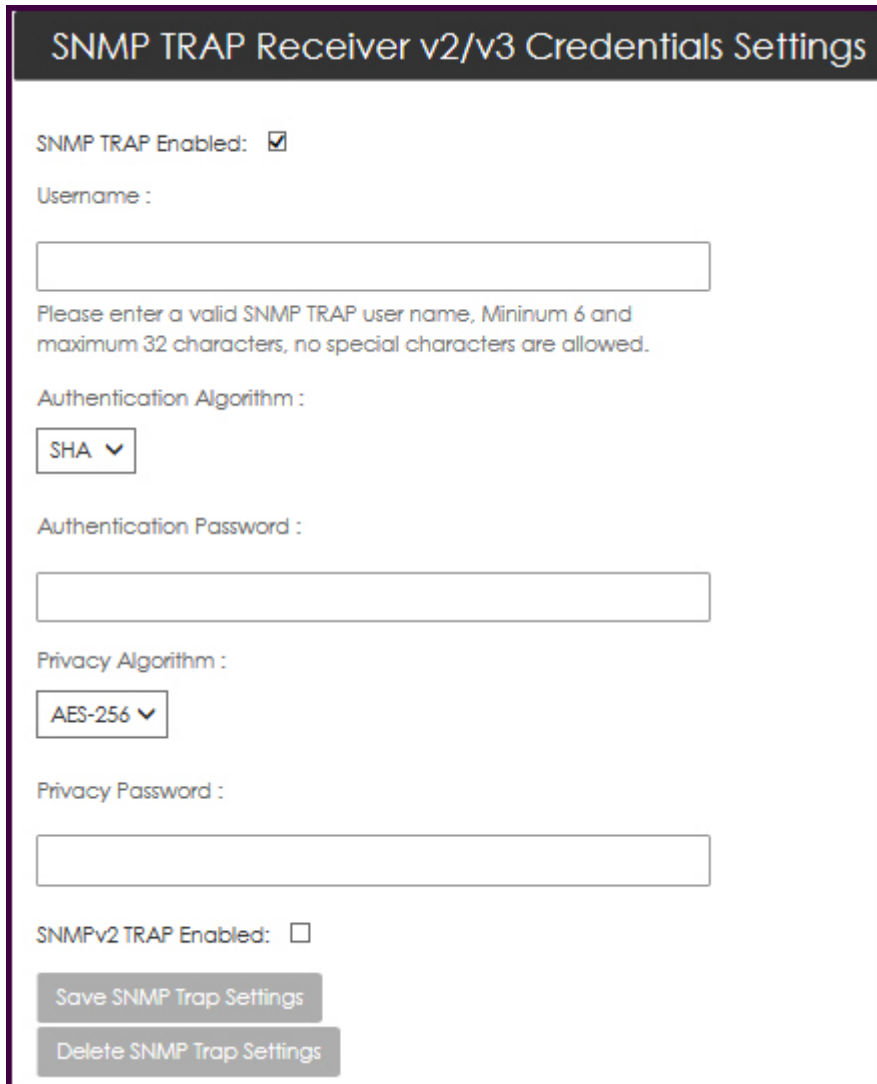


The settings need to match the SNMP trap settings on the devices.

1. Log in as Administrator.
2. Navigate to: **Configuration > Events > SNMP.**



3. Select the **SNMP TRAP Enabled** box. The **SNMP Trap Setting page** opens.



4. Populate the following data fields: **Username**, **Authentication Password**, and **Privacy Password**.
5. Select your **Authentication Algorithm** from the list.
6. Select your **Privacy Algorithm** from the list.



Client Hosts only support **AES**.

7. By default, SNMP traps are supported only for SNMP v3. Therefore, option **SNMPv2 Enabled** is not enabled by default.
8. Select **Save SNMP Trap Settings**.

5.4.3.4.3. Configure SNMPv3 Traps on the SNMP Daemon

`trapsess [SNMPCMD_ARGS] HOST` defines the configuration for a trap. This is the only way to define SNMPv3traps. `SNMPCMD_ARGS` are arguments that would be used for an equivalent `snmptrap` command. So, for example to send a SNMPv3trap as USM user `user1` with authentication and encryption, use `-v3 -u user1 -l priv`. For example:

```
trapsess -v3 -u user1 -l authpriv IP-address:port
```

To configure SNMPv3 traps on the SNMP daemon:

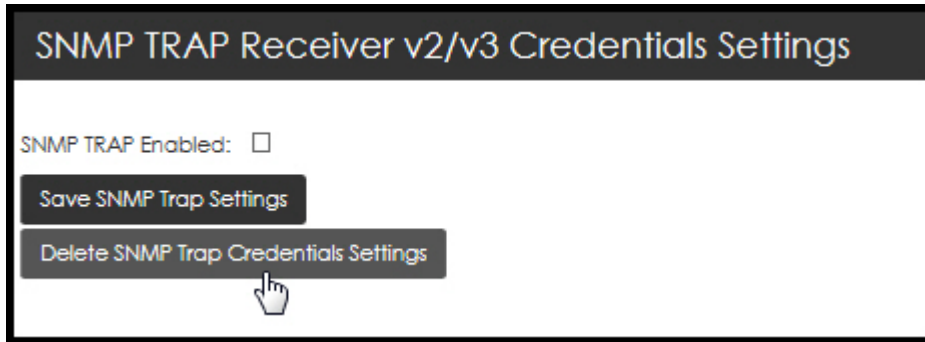
1. Navigate to the `snmp` folder:
 - **Linux:** `/opt/nfast/etc/snmp`
 - **Windows:** `c:\program files\nCipher\nfast\etc\snmp`
2. Stop the SNMP daemon:
 - **Linux:** run `/etc/init.d/nc_ncsnmpd stop`
 - **Windows:** via Services, the name of the service is `nCipher SNMP Agent`
3. Add the trapsess to the `snmpd.conf` file. Replace `<userRW>`, `<userRO>`, `<trapreceiverIP>`, and `port` with your values.

```
trapsess -v3 -u <userRW> -l authpriv <trapreceiverIP>:<port>
trapsess -v3 -u <userRO> -l authNopriv <trapreceiverIP>:<port>
```

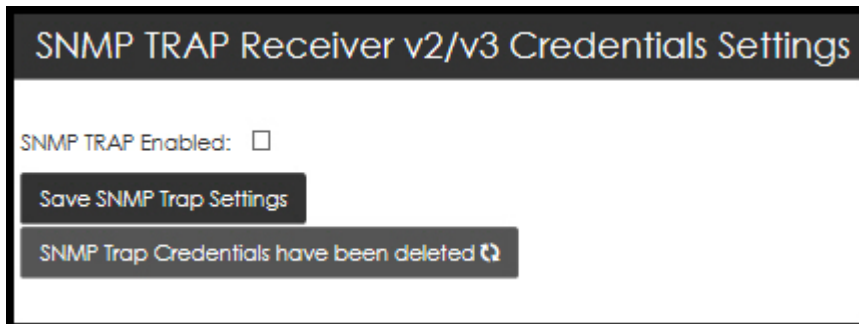
4. Restart the SNMP server:
 - **Linux:** `/etc/init.d/nc_ncsnmpd start`
 - **Windows:** via Services, the name of the service is `nCipher SNMP Agent`

5.4.3.4.4. Delete SNMP Trap Settings

1. Navigate to: **Configuration > Events > SNMP > SNMP Trap Receiver v2/v3 Credentials Settings**.

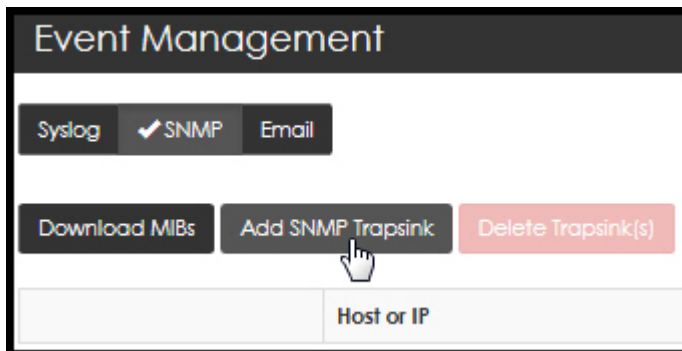


2. Select **Delete SNMP Trap Credentials Settings**. The system response confirms the deletion.



5.4.3.4.5. Add SNMP Trapsink

1. Navigate to: **Configuration > Events > SNMP > Add SNMP Trapsink**.



2. Two options are displayed, one for SNMP V2, and one for SNMP V3. By default, **SNMP V2** is selected, and the SNMP V2 settings are shown. To load the SNMP V3 settings, select **SNMP V3**.

Event Management

Syslog SNMP Email

SNMP V2 SNMP V3

Host or IP :

Port :

Community :

[Cancel Changes](#)

Event Management

Syslog SNMP Email

SNMP V2 **SNMP V3**

Host or IP :

Port :

162

Username :

Authentication Algorithm :

SHA-256

Authentication Password :

Privacy Algorithm :

AES-256

Privacy Password :

Save new Trapsink Cancel Changes

Configure the Trapsink:

For **SNMP V2**: Enter the Host or IP address of the SNMP device, the port number (default: 162), and the community.

For **SNMP V3**: Enter the Host or IP address of the SNMP device, the port number, the username, the authentication algorithm, the authentication password, the privacy algorithm, and the privacy password.

3. Select **Save new Trapsink**.

5.4.3.4.6. Delete the SNMP trap

1. Navigate to: **Configuration > Events > SNMP**
2. Select **Delete Trapsink(s)**.
3. Select the appropriate SNMP trap to delete.
4. Select **Save Settings**.

5.4.3.5. Request email notification

1. Navigate to: **Configuration > Events > Email**.

The screenshot shows the 'Event Management' configuration page for 'Email' notifications. At the top, there are three tabs: 'Syslog', 'SNMP', and 'Email' (which is selected). Below the tabs, there is a checkbox labeled 'Email Notification Enabled' which is checked. Underneath, there is a section titled 'Notification Policy: Email' containing a table with columns for 'Policy Category', 'Info', 'Notification', 'Warning', 'Error', 'Critical', 'Alert', and 'Emergency'. Two rows are visible in the table: 'Monitor-Specific Security Events' and 'Monitor-Specific General Events'. Each row has checkboxes under the 'Info', 'Notification', 'Warning', 'Error', 'Critical', 'Alert', and 'Emergency' columns. At the bottom of the page, there is a 'Save Settings' button.

Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency
Monitor-Specific Security Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitor-Specific General Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

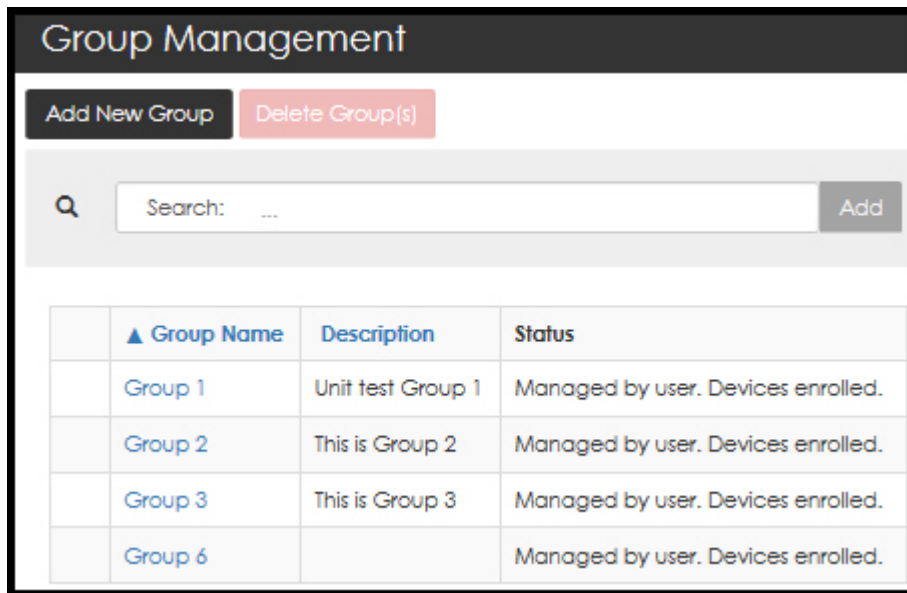
2. Select **Email Notification Enabled**.
3. Select the Policy Category and severity combination.
4. Select **Save Settings**.

5.4.4. Groups

Groups can be added, deleted and sorted.

1. Navigate to: **Configuration > Groups**.

The **Group Management** page opens.



5.4.4.1. Add a New Group

1. Select **Add New Group**.

The **Group Setup** window opens.

The screenshot shows the 'Group Setup' window. It contains two text input fields. The first is labeled 'New Group Name :' and the second is labeled 'New Group Description (optional) :'. At the bottom, there are two buttons: 'Create Group' (dark grey) and 'Cancel Changes' (blue).

2. Enter a **New Group Name** and optionally, a description.
3. Select **Create Group**.

5.4.4.2. Delete Groups

You can only delete a group if its status is **empty**, i. e.,

- the group is not managed by another user
- the group does not contain any enrolled devices
- there are no scheduled reports associated with this group.

5.4.5. License

From the License tab, users can:

- View general license data including license count
 - Add licenses
 - Install licenses
1. Navigate to: **Configuration > License.**

The **System License** page opens.

System License

Serial Number:	Tk iq 7y 1P n7 5Y 9x 8X-kc 9M LX O9 Zz yD Ly Fb
Total Licensed Device Count:	8
Used Licensed Device Count:	8 nShields
Unused Licensed Device Count:	0

Current License(s)

License Type	Max No. of Devices	Remaining Days
evaluation	8	29

Add License

Choose license file :

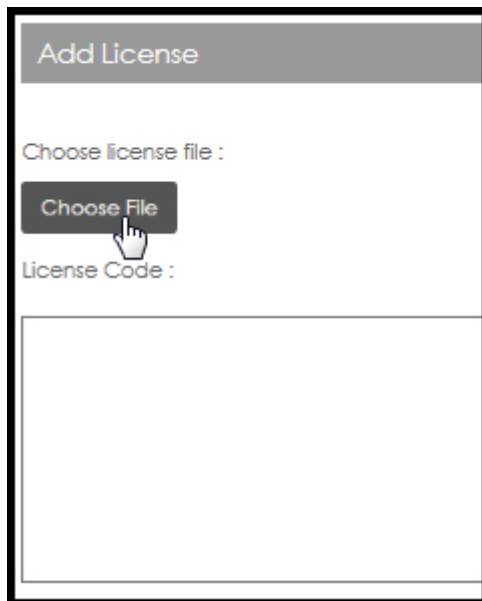
License Code :

Choose File

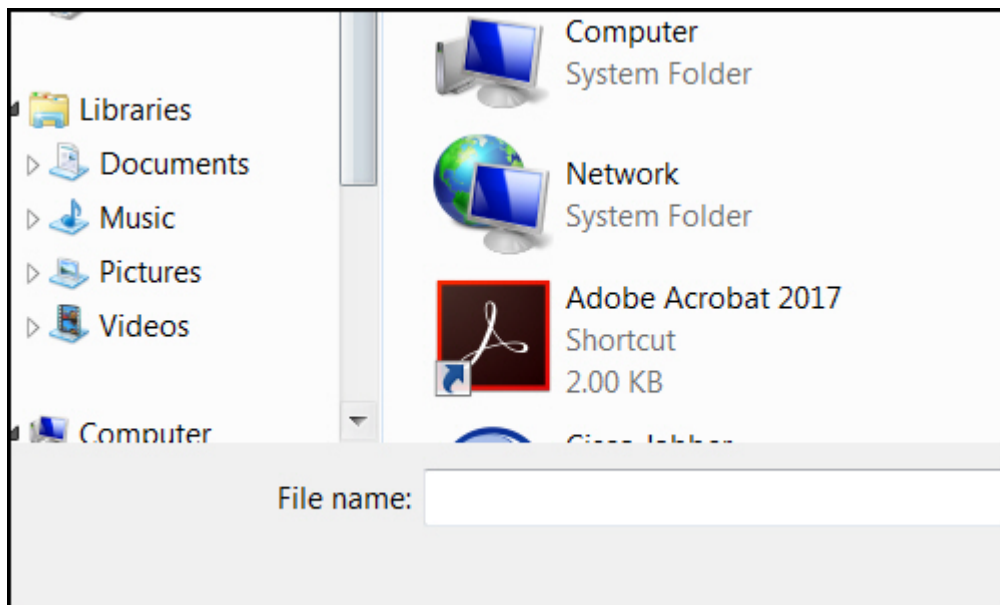
Install License

5.4.5.1. Add a License

1. Select **Choose File**.



The file browser window opens:



2. Navigate to the file location and select the file.
3. Select **Install License**.


5.4.5.2. License Warning Banner

When the number of enrolled devices exceeds the maximum number of managed devices, a warning banner displays on the top of the web page.

The highlighted message instructs you to reduce the number of managed devices.

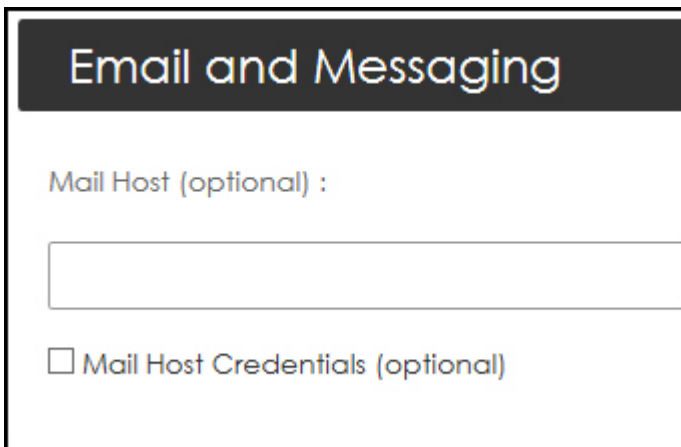
5.4.6. Mail Host

From here you can configure your nShield Monitor's outgoing email address, i.e., your "from" address, and you can send a test email.

 A mail host may be required in order to enable email.

1. Navigate to: **Configuration > Mail Host.**


The **Email and Messaging** page opens:



2. Enter your mail host.
3. Enter your **Email sender address.**
4. Select **Save.**
5. Enter your **Email ID for Sending Test Email.**
6. Select **Send Test e-mail.**
7. Locate the test email in your email In-box.

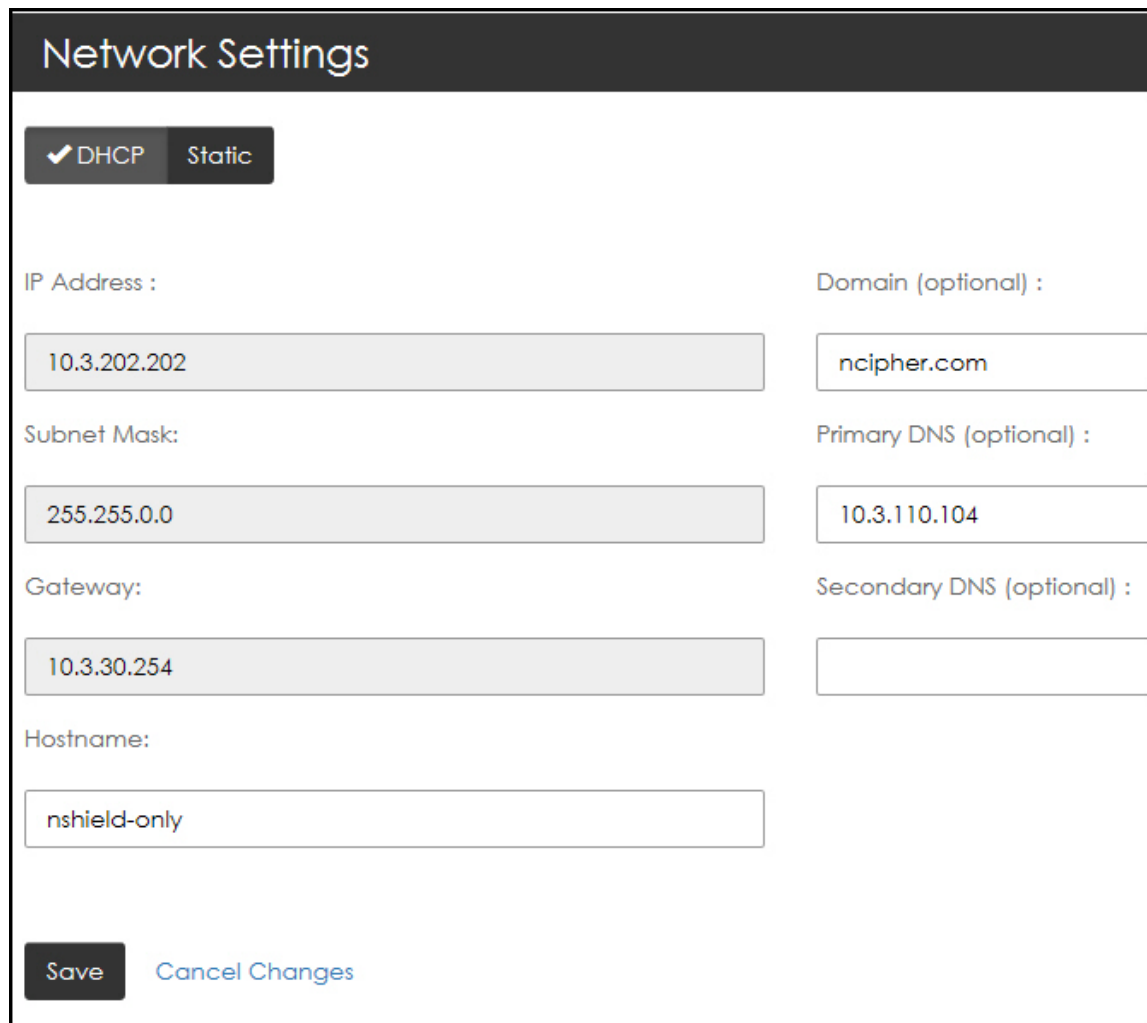
5.4.7. Network

The base network configuration including IP address, subnet mask and default gateway can all be changed via the **Network Settings** page.

 Changing any one of these settings requires that you close your browser and reconnect approximately 15 seconds **after you save** the new settings. If you change the IP address, you will have to redirect your web browser to the new IP address or host name.

1. Navigate to: **Configuration > Network**.

The **Network Settings** page opens.

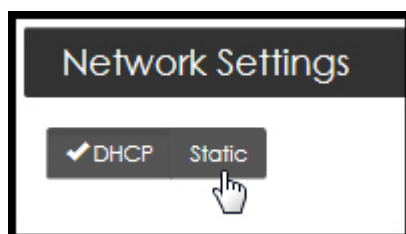


The screenshot shows the 'Network Settings' page with the following fields and values:

- IP Address :** 10.3.202.202
- Subnet Mask:** 255.255.0.0
- Gateway:** 10.3.30.254
- Hostname:** nshield-only
- Domain (optional) :** ncipher.com
- Primary DNS (optional) :** 10.3.110.104
- Secondary DNS (optional) :** (empty)

At the bottom, there are two buttons: **Save** and **Cancel Changes**.

2. Select your preference:
 - Dynamic Host Configuration Protocol (**DHCP**) IP addressing or
 - **Static** IP addressing



3. Select **Save**.

5.4.8. Reboot

Users with System Administrator privileges are able to reboot the nShield Monitor virtual appliance.

1. Navigate to: **Configuration > Reboot**.

The System Reboot page opens.

2. Select **Reboot Now**.

The system prompts for confirmation prior to initiating the reboot.

3. Select **Yes, reboot now** to continue the process.

5.4.9. Security

1. Navigate to: **Configuration > Security**.

The **Security** page opens.

Master key

✔ Master key is currently loaded.

Destroy Master key

SSL Certificate

✔ View Certificate
Generate Self-Signed Certificate
Generate Certificate Request
Install Signed Certificate

Issued By

Country :	
State :	
City :	
Company/Organization :	
Department :	
Common Name :	
Email :	

Issued To

Country :	
State :	
City :	
Company/Organization :	
Department :	
Common Name :	
Email :	
Valid From :	
Valid To :	

User Interface SSL/TLS Options

Denied Protocols:	Change Pending Approval:
<input checked="" type="checkbox"/> SSL v2 <input checked="" type="checkbox"/> SSL v3 <input checked="" type="checkbox"/> TLS v1 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> SSL v2 <input checked="" type="checkbox"/> SSL v3 <input checked="" type="checkbox"/> TLS v1 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.2
Save Options	Cancel Change

Password Settings

Global Password Expiration :

Monthly ▾

Disallow Password Reuse History Length :

Last password ▾

Minimum Password Length :

8

Password Complexity :

Lowercase Characters 1

Uppercase Characters

Numbers 1

Special Characters

Save Password Settings Cancel Password Settings Changes



For users whose credentials were imported from Active Directory, **Configuration > Security** shows their own credentials in and for nShield Monitor. Changes made to passwords in nShield Monitor are not ported back automatically to the Active Directory server.



Users who are Active Directory administrators have no access or visibility to the credentials of other Active Directory users through this dialog.

5.4.9.1. Master Key

The master key consists of an AES256 wrapping key and an HMAC-SHA-512 hash key that is used as the root of protection.

The master key is derived by using the two passphrases using PBKDF2, that are input during the wizard configuration after the first boot and after every reboot.

The master key is never stored in persistent storage.

Two passphrases are required for generation of the key. Enter by entering each passphrase twice.



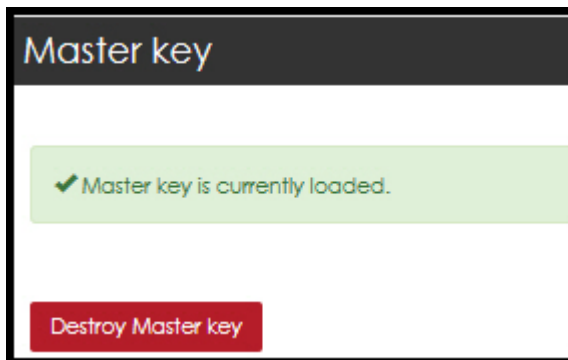
Please note to record each passphrase in a secure location as they are required to be reentered when nShield Monitor is rebooted.

To destroy a Master Key:

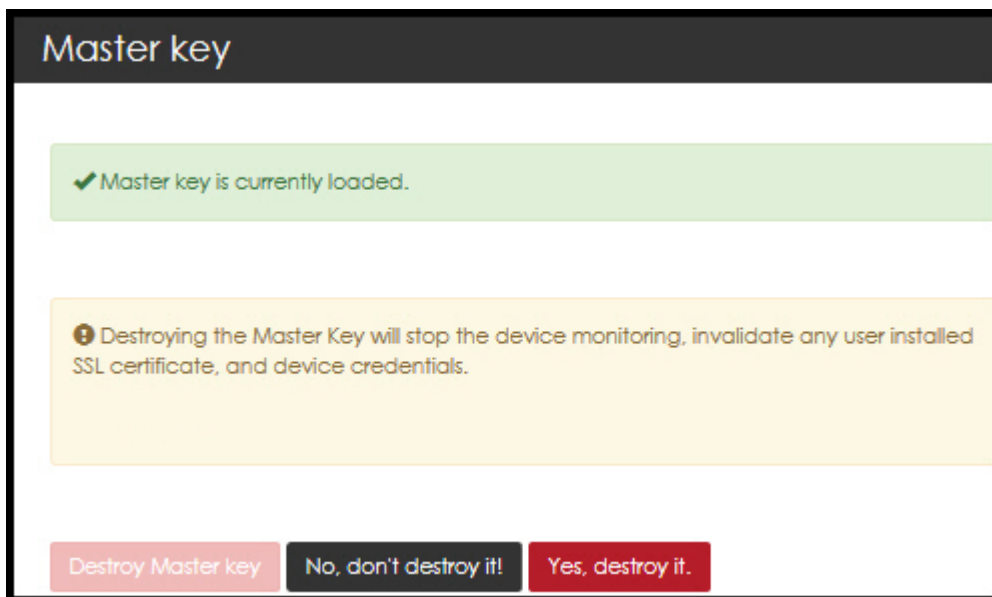


The Master Key can only be destroyed if all of the enrolled devices have been deleted.

1. Select **Destroy Master Key**.



2. Select **Yes, destroy it**.



Please note that destroying the master key stops all device monitoring and renders all device credentials invalid. The system must be reset after this operation.

To generate a new master key, enter the two passphrases as before.

5.4.9.2. View the SSL Certificate

By viewing the current SSL certificate, the administrator can determine what type of certificate is currently installed in the system.

By default, the system installs a self-signed SSL certificate with fixed values for common name, country state, city, etc.

SSL Certificate

✓ View Certificate
Generate Self-Signed Certificate
Generate Certificate Request

Install Signed Certificate

Issued By

Country :	US
State :	CA
City :	
Company/Organization :	
Department :	
Common Name :	
Email :	

Issued To

Country :	US
State :	CA
City :	
Company/Organization :	
Department :	
Common Name :	
Email :	
Valid From :	
Valid To :	

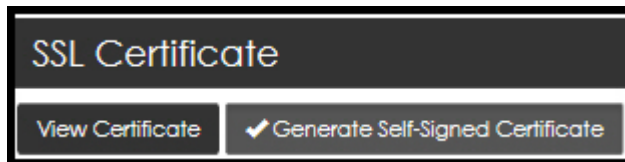


As a best practice, it is recommended that at least a new self-signed certificate be generated using the appropriate values. The default SSL certificate is valid for 30 days.

5.4.9.3. Generate a Self-Signed Certificate

With a self-signed certificate, you can customize certificate information by entering information that applies to your nShield Monitor deployment.

1. Select **Generate Self-Signed Certificate**.



2. Enter the requested data to complete each field.



The default value for the field **Certificate Validity in Days** is **730 (i.e., 2 years)**.

SSL Certificate

Country :

US - United States

State/Province :

City :

Company/Organization :

Department :

Common Name :

Email :

Number of Days Valid :

730

3. Select **Generate Certificate**.

This action requires restarting the web services so the new certificate can take effect.

You will need re-login into the WebUI.

The following message displays:

Self-Signed Certificate successfully created. System is restarting the web

service, please log in again.

5.4.9.4. Generate SSL Certificate Request

When a certificate must be signed by an organization's own Certificate Authority (CA) or a third party trusted CA, you must generate a certificate signing request.



The only difference between the fields in a self-signed certificate and a certificate signing request are the number of days of validity which will be determined by the signing CA.

1. Select **Generate Certificate Request**.



2. Enter the requested data to complete each field.

SSL Certificate

View Certificate
Generate Self-Signed Certificate
✓ Generate Certificate Request

Install Signed Certificate

Country :

US - United States
▼

State/Province :

City :

Company/Organization :

Department :

Common Name :

Email :

Generate Certificate Request
Clear all input

3. Select **Generate Certificate Request**.

The system prompts you to save a file that you will provide to your PKI team or third party CA provider to sign and return.



Private keys are not exported as part of the signing request.

5.4.9.5. Install Signed SSL Certificate

Once your PKI team or third party CA provider returns your signed certificate, you will need to install it in one of two fashions.



It is recommended that you ensure that the returned signed certificate includes the full chain of signers (e.g., nShield Monitor certificate, signing CA, root CA).

The chain should consist of at least two certificates (nShield Monitor certificate and signing CA) and as many as seven (includes nShield Monitor certificate, signing intermediate CA and intermediate CAs between signing CA and the root CA).



If you receive the file via email be sure to save it to a location where you can find it.

1. Select **Install Signed Certificate**.

SSL Certificate

View Certificate Generate Self-Signed Certificate Generate Certificate Request

✓ Install Signed Certificate

Choose local file :

Choose File

showing the certificate file contents, you can also paste the certificate contents to the window:

Install Certificate Clear all input

2. Select **Choose file** and browse to locate the file that contains the signed certificate and the associated signing chain.
3. Open the file and include the contents in the window.
4. Select **Install Certificate**. The signed certificate is installed.
5. Close your browser session (logout and close the tab) in order to connect using the new certificate properly.



You will be prompted to login again when you do so.

5.4.9.6. User Interface SSL/TLS Options

On this page, you can configure which protocols and cipher mechanisms nShield Monitor accepts.



This feature requires a quorum approval from a second administrator before changes made by the first administrator can be applied.

- By default, SSL v2 & v3, and TLS v1 protocols are disabled.
- By default, the AES256-SHA cipher suite is disabled.

User Interface SSL/TLS Options

Disabled Protocols:

- SSL v2
- SSL v3
- TLS v1
- TLS v1.1
- TLS v1.2

Disabled Cipher Suites:

- AES256-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-DSS-AES128-SHA256
- DHE-DSS-AES256-GCM-SHA384
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-SHA256
- ECDH-ECDSA-AES256-GCM-SHA384

Save Options

To change which protocols and cipher mechanisms are allowed:

1. Navigate to: **Configuration > Security**.
2. Select the protocols that the GUI server should deny.

3. Select **Save Options**.

This generates a warning that lists the protocol option changes that require approval.



There are protections that make sure at least one option is left unchecked (which means unblocked).

4. When a quorum approval is pending, one of three actions can happen next:

- The first administrator can cancel the quorum request by selecting **Cancel Change** and the system remains unchanged.
- The second administrator can deny the change by selecting **Reject Change**. This generates a log message indicating that a change was denied.
- The second administrator can approve the change by electing **Approve Change**. This generates a log message indicating that a change was approved, and the GUI server is restarted.

5. A restart is required for the new settings to take effect.



This is not a reboot, only a restart of the GUI server. However, any users that are logged on are sent back to the login page. They will need to log back in to the system.

5.4.9.7. Password Settings

1. Navigate to: **Configuration > Security**.

You may need to scroll down.

2. Set the parameters based on your organization's security policy.

- Global Password Expiration
 - Disable
 - Never
 - Monthly
 - Quarterly
 - Yearly
- Disallow Password Reuse History Length
 - Last password
 - Last 2 passwords

- Last <n> passwords (up to last 15 passwords)
- Minimum Password Length
- Password Complexity

Password Settings

Global Password Expiration :
Monthly

Disallow Password Reuse History Length :
Last password

Minimum Password Length :
8

Password Complexity :

Lowercase Characters 1

Uppercase Characters

Numbers 1

Special Characters

Save Password Settings Cancel Password Settings Changes

3. Select **Save Password Settings**.

5.4.10. Upgrade

nShield Monitor has the capability to be upgraded via a file provided by Entrust.

5.4.10.1. Upgrade from 1.1.X



The same firmware upgrade file works for all your nShield Monitor appliances. Additionally, the upgrade requires a password, or upgrade key.

The process to obtain an upgrade file for your virtual appliance follows.

1. Send an email to Entrust nShield Support, <https://nshieldsupport.entrust.com>, and request an upgrade.

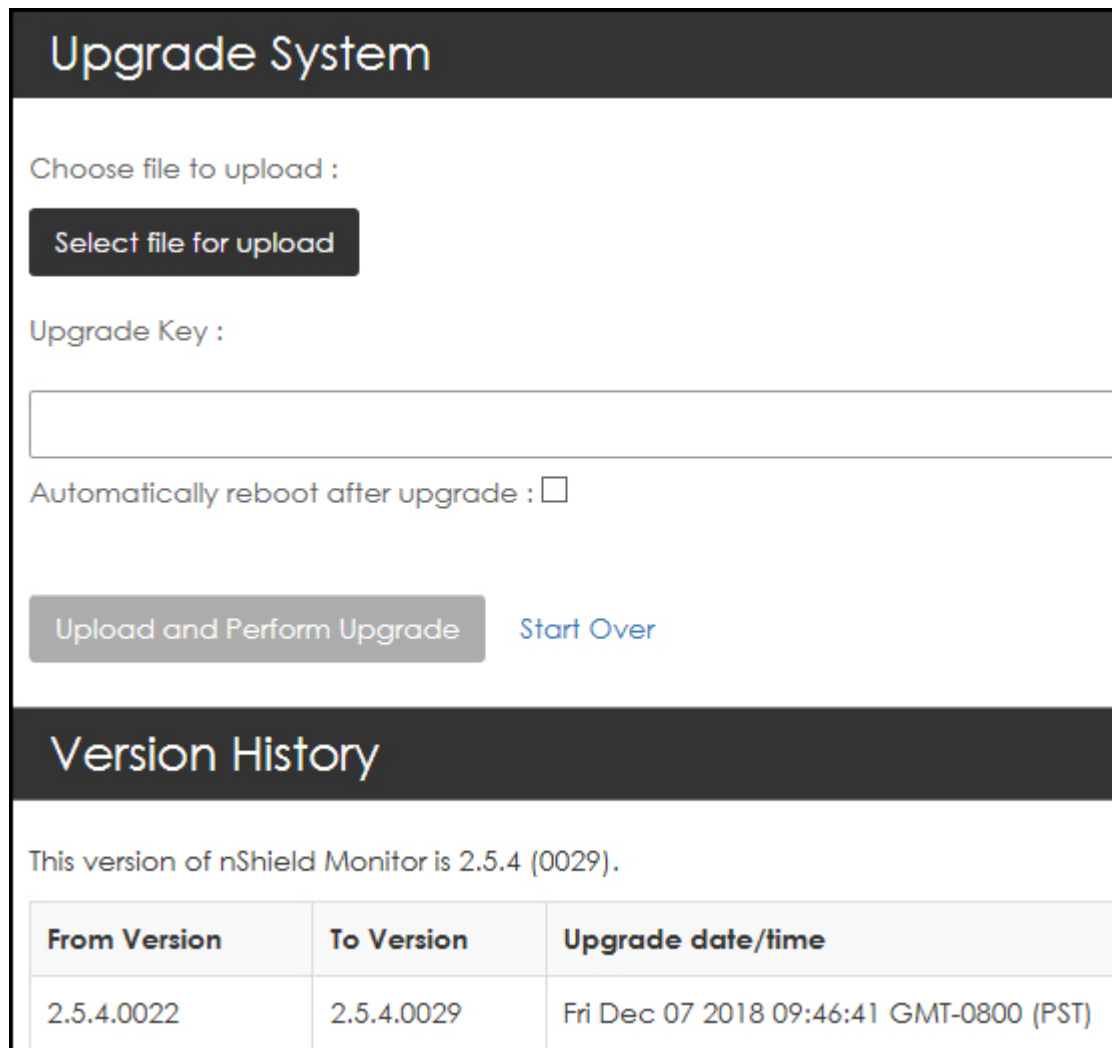
Support forwards a firmware upgrade file (with a .cmf file extension) along

with the upgrade key password.

2. Save the .cmf file to a convenient location. You are now ready to apply the upgrade.
3. Navigate to:

Configuration > Upgrade

The Upgrade System page opens:



Upgrade System

Choose file to upload :

Select file for upload

Upgrade Key :

Automatically reboot after upgrade :

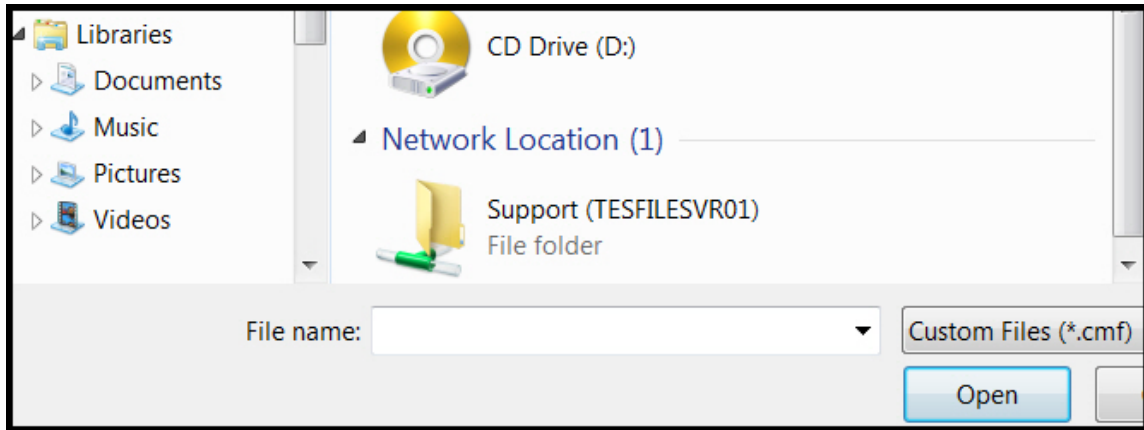
Upload and Perform Upgrade Start Over

Version History

This version of nShield Monitor is 2.5.4 (0029).

From Version	To Version	Upgrade date/time
2.5.4.0022	2.5.4.0029	Fri Dec 07 2018 09:46:41 GMT-0800 (PST)

4. Click **Select file for upload**.
5. Navigate to the upgrade file.

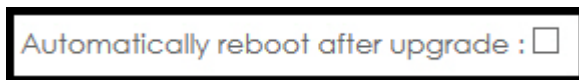


6. Select, and open the upgrade file that you just saved.
7. Enter the password, provided by Support, under **Upgrade Key**.



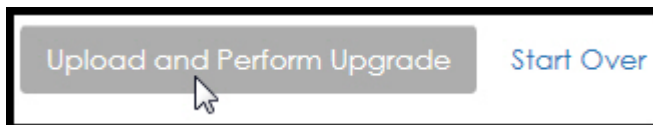
At this point, you can choose to have the system automatically reboot when the upgrade is complete by selecting **Automatically reboot after upgrade**. Otherwise, you will need to manually trigger a reboot once the upgrade process has completed. Either way, the system must be rebooted to complete the upgrade process.

8. Select **Automatically reboot after upgrade**.



If **Automatically reboot after upgrade** is not selected, you will need to manually trigger a reboot once the upgrade process has completed.

9. Select **Upload and Perform Upgrade**.



The system displays progress meters to indicate the status.



Please do not navigate away from the **Upload** page during the upload process. Should you navigate away, the upgrade automatically cancels.

If the system does not automatically reboot, select **Reboot Now** button and then confirm the action with a second click.

When the process completes, the system will either reboot automatically or you will need to select **Reboot Now** button and then confirm the action with a second click.



After the system reboots, the new software version is displayed on the **Dashboard** page, in the nShield Monitor Status window.

5.4.11. Creating Users



nShield Monitor can support up to 64 users.



A user with no role is not allowed to login.



After three failed login attempts, the account is locked

To unlock an account, select **Forgot your Password** on the login page. You will be emailed a onetime password (OTP). The first time you log in with the OTP, the account is unlocked and you are prompted to create a new password.

1. Navigate to: **Configuration > Users**.

The **Manage Users** page opens.

	▲ Login ID	Full Name	Email	Password Expiration	Auto Logout	Assigned Roles
<input type="checkbox"/>	admin	Default System Administrator	admi...	Never	1 hours	System Administrator
<input type="checkbox"/>	admin1		admi...	Never	5 minutes	System Administrator
<input type="checkbox"/>	admin2		admi...	Never	5 minutes	System Administrator
<input type="checkbox"/>	auditor		a@a	30 days	30 minutes	System Auditor
<input type="checkbox"/>	group		a@a	Never	1 hours	Group Manager

2. Select **Create User**.
3. Complete the open fields appropriately.

Create a New User

User Name :

Full Name (optional) :

Description (optional) :

Email :

Confirm Email :

Auto-Logout Duration :

5 minutes

5 minutes ●●●●●●●●●●● 60 minutes

Password Expiration :

Monthly ▼

Assign Role(s) for this User :

No Role Administrator Group Manager Auditor

Create User Cancel Changes



When creating a user with the Group Manager role, available groups must be assigned to the user.



At least **one group must be assigned** to all users assigned a Group Manager role.

A screenshot of a web interface. At the top, it says "Password Expiration" with a dropdown menu set to "Monthly". Below that, it says "Assign Role(s) for this User:" followed by a horizontal menu with four options: "No Role", "Administrator", "Group Manager", and "Auditor". The "Auditor" option is selected, indicated by a checkmark. At the bottom left, there is a "Create User" button, and at the bottom right, there is a "Cancel Changes" link.

4. After you have made your selections, select **Create User**.

5.4.12. Editing users

1. Navigate to: **Configuration > Users**.

The **Manage Users** page opens.

2. Select the Login ID associated with the user to edit. The **Edit this user** page opens.

When you are updating a user with the Group Manager role, available groups must be assigned to the user.



At least **one group must be assigned** to all users assigned a Group Manager role.

3. Under **Assign Roles for this User**, select the role to associate with the user, then select **Save User**.

5.4.13. Deleting Users

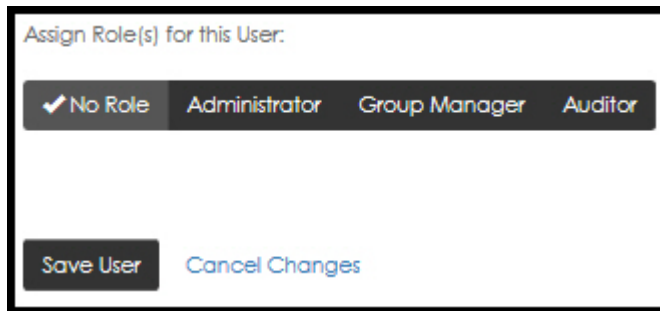
1. Navigate to: **Configuration > Users**.

The **Manage Users** page opens.

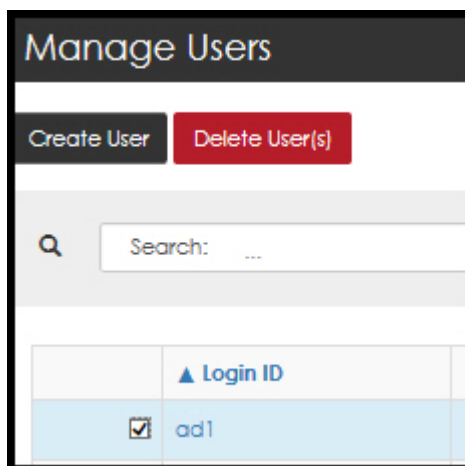


Only those users who have no role assigned can be deleted.

2. Select the Login ID associated with the user to be deleted. The **Edit this user** page opens.
3. Under **Assign Roles for this User**, select **No Role**.



4. Select **Save User**.
- The **Manage Users** page opens.
5. Select the box associated with the user.



6. Select **Delete User(s)**.
- The system prompts requesting a confirmation of the deletion.
7. Confirm the deletion.

6. Configuration Logged in as Group Manager

6.1. Overview

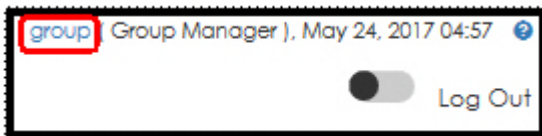
The Group Manager role is responsible for configuration of devices that are to be monitored and the day to day monitoring of health and statistics down to an individual HSM device level.

Group Managers are able to enroll devices, set group alarm thresholds, and configure group event notifications via email.

6.2. Edit Profile page

Both the Administrator and the Group Manager are able to edit their own profiles.

The **Edit Profile** page is accessed by selecting (i.e., clicking on) your User ID located in the top right corner of the page.

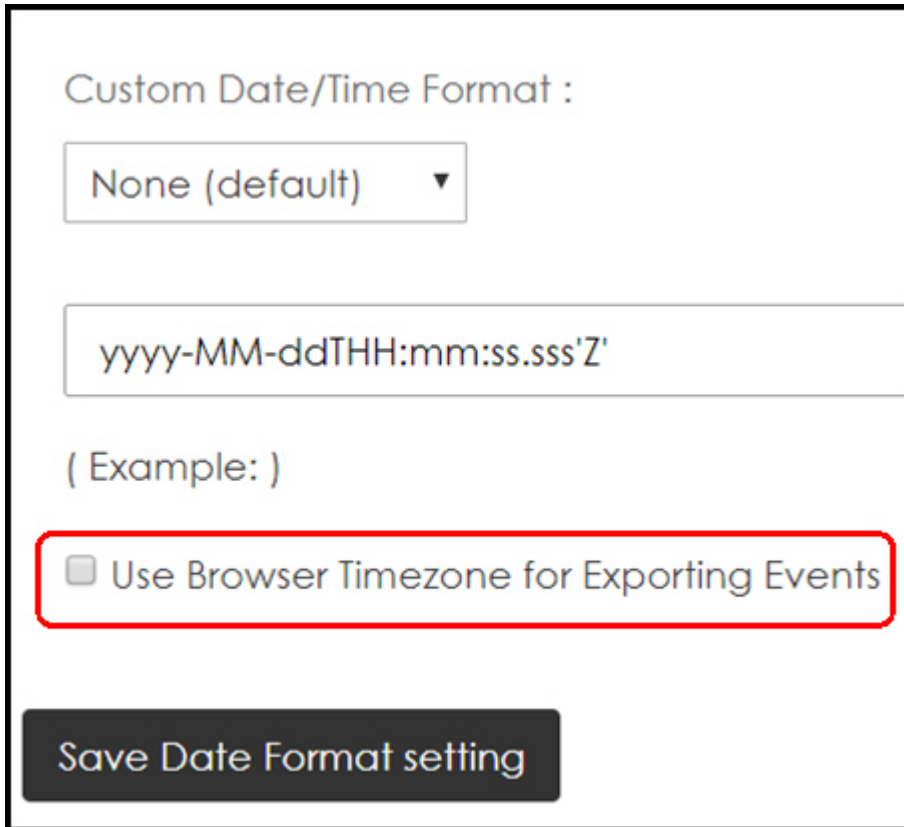


From this page, you can perform the following actions:

- Add a description
- Update the email address
- Change the password
- Set the Auto-Log duration
- Select a custom date format



When selecting a custom date format, you can also select: **Use Browser Timezone for Exporting Events.**



Custom Date/Time Format :

None (default) ▼

yyyy-MM-ddTHH:mm:ss.sss'Z'

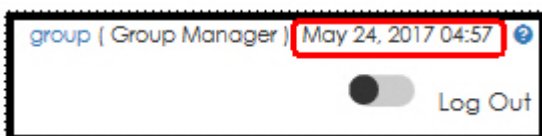
(Example:)

Use Browser Timezone for Exporting Events

Save Date Format setting

When you select a custom date format, the chosen format is associated with your user ID giving each user the option of selecting their preferred format. Once the format has been selected, it is consistently displayed in accordance with your selection.

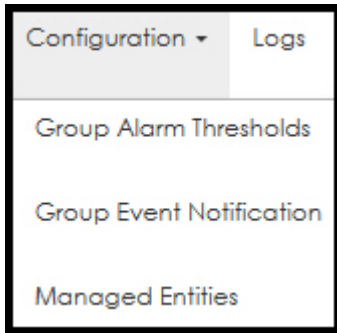
The only date format that will not change is the date in the User ID line, as shown below:



- Reset the GUI Persistence Profile.

6.3. Managed Entities

Logged on as a Group Manager, the Configuration tab displays the following:

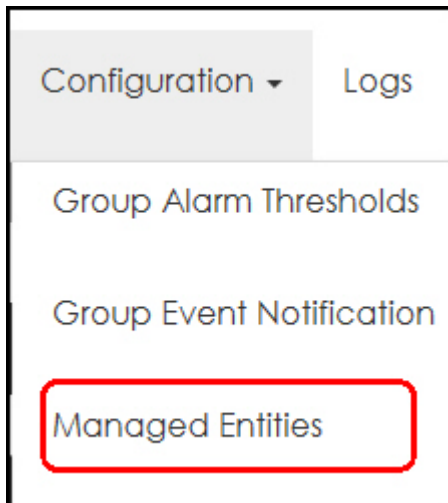


6.3.1. Enrolling Devices/Entities

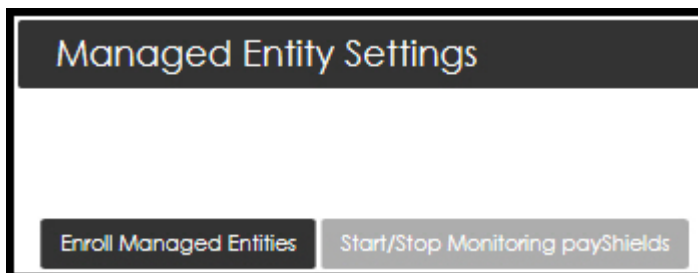


To enroll a device/entity, you must be logged on as a Group Manager. For enrolling a device you must configure SNMPV3 on the device with an authentication algorithm and a privacy algorithm, and use the same during device enrollment.

1. Navigate to: **Configuration > Managed Entities**.



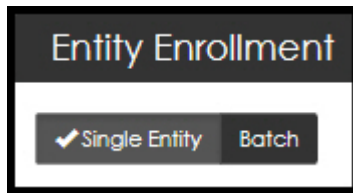
The **Manage Entity Settings** page opens.



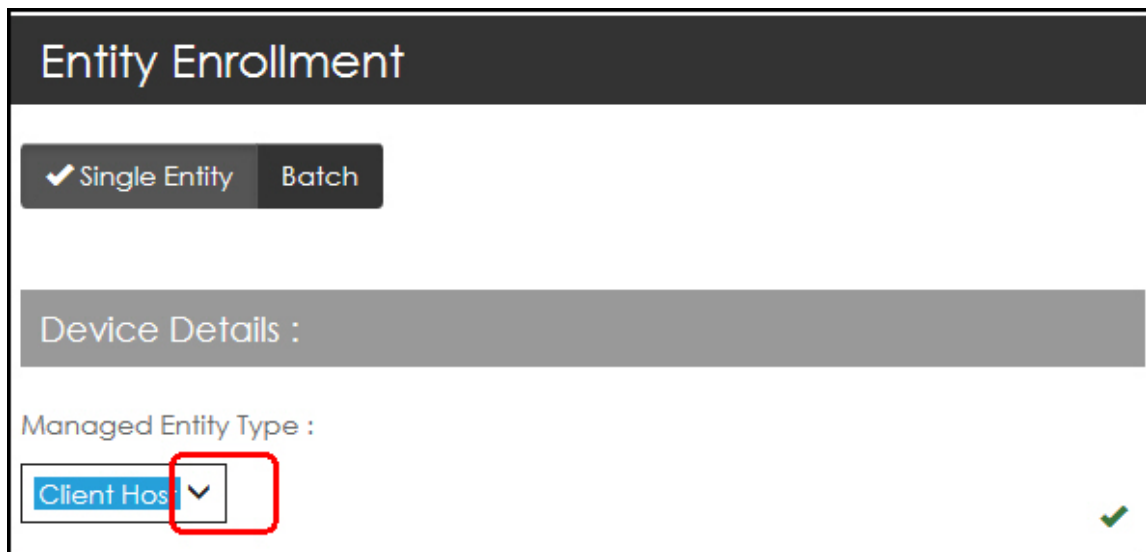
2. Select **Enroll Managed Entities**

The Entity Enrollment options are displayed.

You can choose to enroll an entity one at a time or you can use a Batch file. The default is set to enroll a Single Entity.



3. Select the **Managed Entity Type** from the drop down menu.



4. Enter the details information into the appropriate fields, i.e., device details, SNMP details, and Group Membership details.

Entity Enrollment

✓ Single Entity
Batch

Device Details :

Managed Entity Type :

Client Host ▼

✓

SNMP Details :

Username :

Hostname/IP Address :

Port :

Name (optional) :

Authentication Algorithm :

SHA ▼

Description (optional) :

Authentication Password :

Location (optional) :

Privacy Algorithm : (Client hosts only support AES)

AES ▼

Stats Timeout :

Privacy Password :

Admin Timeout :

Group Membership :

Member of

Filter groups:

Available Groups

Filter groups:

Managed Groups
▲



Both the Authentication Algorithm and the Privacy Algorithm require a selection from a drop down.



Client hosts only support AES Privacy Algorithms.

5. Click **Enroll Device** to complete the enrollment process:



6. Select **Yes, test connection** to test the connection.
 - If you would like to skip the test, select **No, skip Test**.
 - If you would like to cancel the data that you just entered, select **Cancel Changes**.
 - If you choose to test your connection and the test is successful are returned to the **Managed Entities** page.



If you test the connection and the test is not successful, you will receive an error message. Correct the error condition and re-enter the device information.

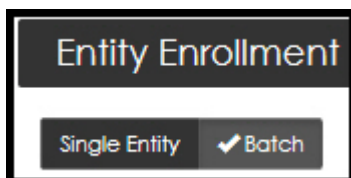
ATTENTION: Devices/entities can be assigned to multiple groups.

- A device/entity can be assigned to groups not associated with the current manager role; however, this is a one way function.
- In order to make changes or delete a device/entity in a group, the user must be a Group Manager for that group.
- A device/entity can be associated into multiple groups during enrollment.
- The same device/entity can be associated to more groups by editing the device.

ATTENTION: All HSMs being monitored must be configured to support SNMPv3 with nShield Monitor.

6.3.2. Option: Enrolling using a Batch File

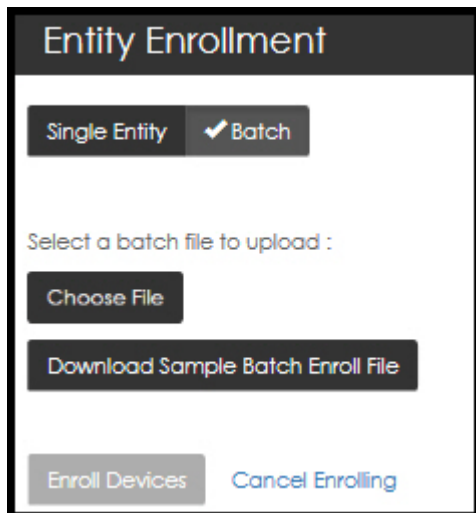
1. From the **Entity Enrollment** page, select **Batch**.



The **Entity Enrollment** page opens.



To see a sample batch file, select **Download Sample Batch Enroll File**.



2. Select either **Choose File** or **Download Sample Batch Enroll File**.

- Enrolling multiple devices at one time requires a comma separated variable (CSV) file containing all the device information and SNMP information.
- It is possible to create a file without passwords but you will need to still leave a space where the passwords would go in the file.



Devices can be assigned to multiple groups. A device can be assigned to groups not associated with the current manager role; however, this is a one way function. In order to make changes or delete a device in a group, the user must be the Group Manager. A device can be associated into multiple groups during enrollment. The same device can be associated to more groups by editing the device.

Device/Entity Batch Entry CSV Fields

CSV File Field Name	Notes
Group Name	Required (string) [multiple groups in square brackets]
Device Host name	Optional if IP address present (string)
Device IP address	Optional if hostname present (IPv4 address - 123.45.67.89)
Device Name	Optional (string)
Description	Optional (string)

CSV File Field Name	Notes
Location	Optional (string - cannot use commas to separate city from state)
SNMP User Name	Required (string)
SNMP Authentication Algorithm	Required (one of [MD5 SHA])
SNMP Authentication Password	Required (string)
SNMP Privacy Algorithm	Required (one of [DES AES 3DES AES-192 AES-256])
SNMP Privacy Password	Required (string)
SNMP Port	Optional (string) default is 161
Device type	Optional (string)
Admin Timeout	Optional (string)
Stats Timeout	Optional (string)

- Each entity must be listed in a single row and all fields must be separated by commas.
- For the optional fields, if you do not want to specify a value, leave the field blank. Both blank lines and comment lines are ignored.
- Example with all fields specified:

```
Group1, Device1, 192.168.18.101, Device 1, Device description 1, Location 1, User1, SHA, authpassword1, DES, privacypassword1
```

- Example with optional fields not specified - Note that those field are left empty:

```
Group2, , 192.168.18.102, Device 2, , , User2, SHA, authpassword2, DES, privacypassword2
```

- Example with optional fields not specified - Note that those field are left empty:

```
Group2, , 192.168.18.102, Device 2, , , User2, SHA, authpassword2, DES, privacypassword2
```

3. After loading the batch file, select **Enroll Devices**.



4. Select **Yes, test connection** to test the connection.
 - If you would like to skip the test, select **No, skip Test**.
 - If you would like to cancel the data that you just entered, select **Cancel Changes**.
 - If you choose to test your connection and the test is successful, you are returned to the **Device Listing** page.



If you test the connection and the test is not successful, you will receive an error message. Correct the error condition and re-enter the device information.

6.3.2.1. Deleting Enrolled Devices



You can only delete devices from groups that you have been assigned the manager role. When a device is associated with multiple groups, deleting a device from a group removes the association of the device **from that group only**. The device **does not get deleted from other groups** that it is associated with. A device gets deleted from nShield Monitor only when it does not have any association with any other group.

1. Navigate to: **Configuration > Managed Entities**.
2. Select the check box next to the device to be deleted.



Selecting the check box at the header level automatically selects all the devices in the Group.

3. Select **Delete <device>**.

6.3.2.2. Editing Enrolled Devices

1. Single click on <device name> of the device to be edited.

The **Edit Device Details** page opens.

Edit Device Details

Device Details :	SNMP Details :
Managed Entity Type : <input type="text" value=""/>	Username : <input type="text" value="vpsuser"/>
Hostname/IP Address : <input type="text" value="192.168.19.255"/>	Port : <input type="text" value="161"/>
Name (optional) : <input type="text" value="VpS-003"/>	Authentication Algorithm : <input type="text" value="SHA"/>
Description (optional) : <input type="text" value="VpS"/>	Authentication Password : <input type="text" value="....."/>
Location (optional) : <input type="text" value="esx5"/>	Privacy Algorithm : <input type="text" value="DES"/>
	Privacy Password : <input type="text" value="....."/>

Group Membership :

Member of	Available Groups							
<input type="text" value="Filter groups:"/> <table border="1"><tr><td>Group 1</td></tr><tr><td>Group 2</td></tr><tr><td>Group 3</td></tr><tr><td> </td></tr></table>	Group 1	Group 2	Group 3		<input type="text" value="Filter groups:"/> <table border="1"><tr><td>Managed Groups</td></tr><tr><td>Other Groups</td></tr><tr><td> </td></tr></table>	Managed Groups	Other Groups	
Group 1								
Group 2								
Group 3								
Managed Groups								
Other Groups								



The **Group Membership** window displays two assignments: **Member of** and **Available Group**. You are able to toggle membership between the two.

2. Enter the changes/make your selections.
3. Select **Save Changes**.



6.3.2.3. Starting and Stopping Device Monitoring

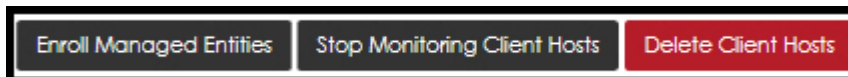
1. Navigate to: **Configuration > Managed Entities**.

The **Managed Entity Setting** page opens.

2. Select the box associated with the device to have monitoring started/stopped.

<input type="checkbox"/>	▲ Name	IP Address	Monitoring	Description	Location
<input checked="" type="checkbox"/>	Faisal SW2 CH1	192.168.18.32	ENABLED		
<input type="checkbox"/>	Faisal SW2 CH2	192.168.17.141	UNREACHABLE		

New action buttons appear:

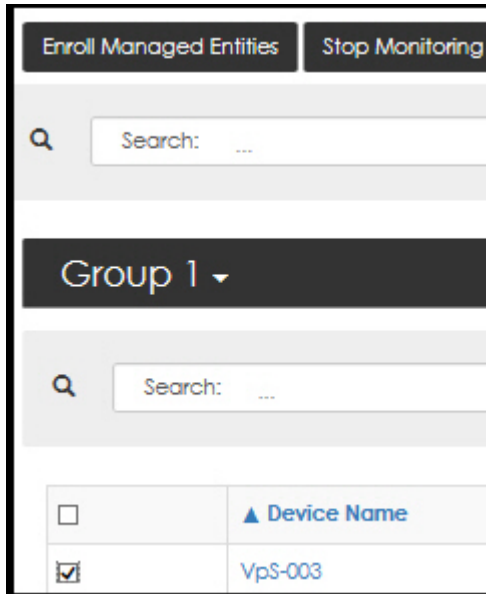


The Start Monitoring <device> is a toggle with Stop Monitoring <device>. When the device is being monitored, the **Stop Monitor** option is available. When the device is not being monitored, the **Start Monitor** option is available.

3. Select the check box next to the device to stop/start monitoring.



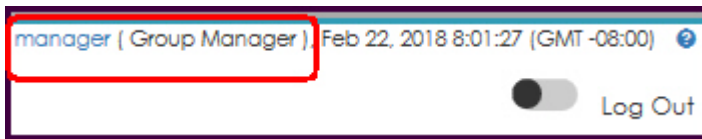
All selected devices must be either **enrolled** or **unenrolled** for the button to be enabled.



4. Select <Stop><Start> **Monitoring** <device/entity>.

6.4. Group Alarm Thresholds

The Group Manager role can view and set alarm thresholds.



1. Navigate to: **Configuration > Group Alarm Thresholds.**

The **Group Alarm Thresholds** page opens:

Group Alarm Thresholds							
Filter Groups							
Group Name	nShield Warning Level	nShield Critical Level	nShield Peak Level	nShield Peak Duration	nShield Object Count Warning Level	nShield Object Count Critical Level	nShield High Object Count Duration
nShield	40	67	39	15 minutes	640	7500	15 minutes
Test VpS							

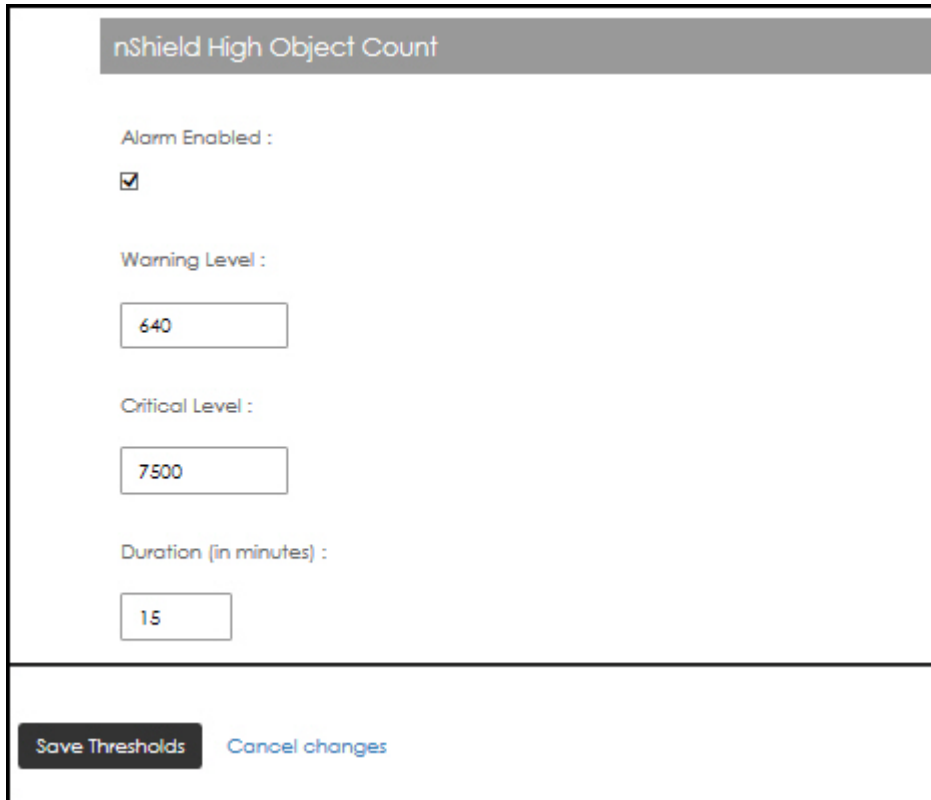
2. Select (i.e., click on) the Group that you would like to set.

3. Utilize the slide bars to set the thresholds.

The screenshot displays the nShield configuration interface with three sections:

- Utilization Overload:**
 - Alarm Enabled:
 - Warning Level: 40% (slider from 0% to 100%)
 - Critical Level: 67% (slider from 0% to 100%)
- Utilization Peak Event:**
 - Alarm Enabled:
 - Utilization Level: 39% (slider from 0% to 100%)
 - Duration (in minutes): 15 (input field)
- nShield High Object Count:**
 - Alarm Enabled:
 - Warning Level: 640 (input field)

4. Continue to scroll down the screen.

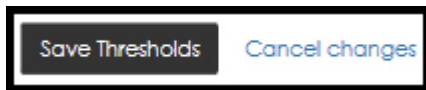


The screenshot shows a configuration window titled "nShield High Object Count". It contains the following fields and controls:

- Alarm Enabled :** A checkbox that is checked.
- Warning Level :** A text input field containing the value "640".
- Critical Level :** A text input field containing the value "7500".
- Duration (in minutes) :** A text input field containing the value "15".

At the bottom of the form, there are two buttons: "Save Thresholds" (a dark button with white text) and "Cancel changes" (a light blue button with dark blue text).

5. Set the values in the **High Object Count** fields based on your preferences.
6. Select **Save Thresholds**.



Alarms must be enabled to receive alerts and must be programmed for each group you wish to see alerts for.

Utilization overload thresholds have two levels:

- The first level is a Warning Threshold used to generate a Warning Severity Event.
- The second level is Critical Threshold used to detect a Critical Severity Event.

When the group utilization overload alarm is enabled, and both thresholds are configured, then every 10 minutes the alert detection will compute the last 10-minute nShield utilization for each device in the group.

If the utilization is over the Critical Threshold, a critical event is generated; if it's less than the Critical Threshold, but over the Warning Threshold, a warning event is generated. Otherwise, there is no alert event.

The Utilization Peak Event provides a warning level threshold if the utilization peaked above a selected percentage during a pre-configured amount of time in

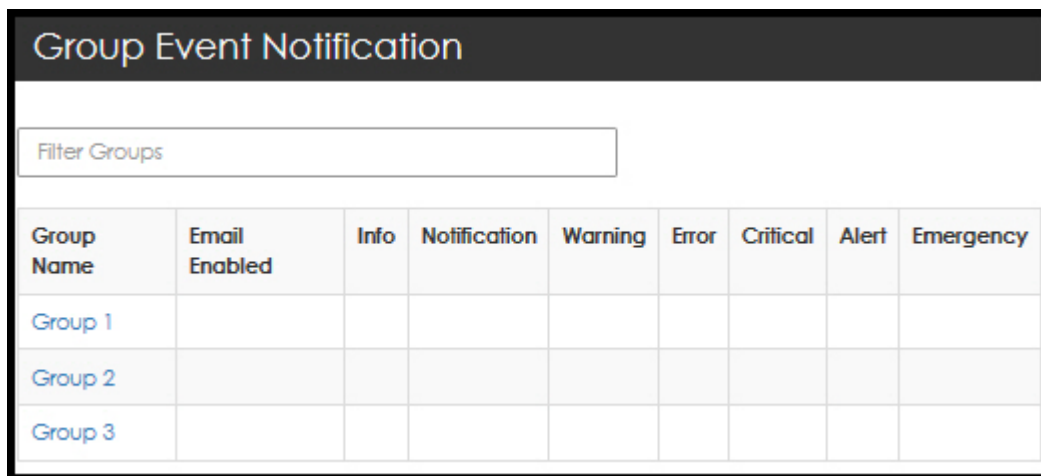
minutes.

Both sets of alerts are disabled by default.

6.5. Group Event Notification

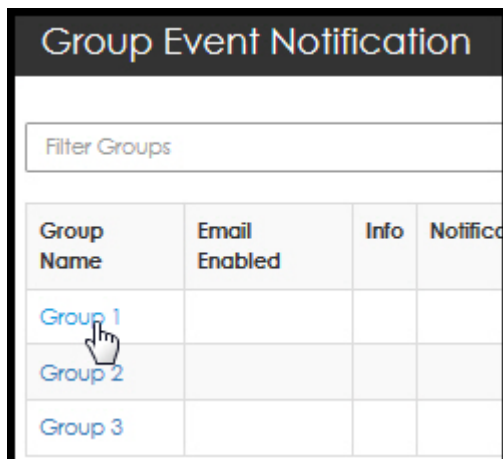
The group manager role has the capability to view and set group event notification via email.

1. Navigate to: **Configuration > Group Event Notification.**



Group Name	Email Enabled	Info	Notification	Warning	Error	Critical	Alert	Emergency
Group 1								
Group 2								
Group 3								

2. Select the Group for notification.



Group Name	Email Enabled	Info	Notific
Group 1			
Group 2			
Group 3			

The Notification Warning message displays.

Group Event Notification : Group 1

Email Notification Enabled
 Warning: Email Notification is disabled.

Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency
Device-Group Specific Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Policy [Cancel changes](#)

3. Select **Email Notification Enabled**.

Group Event Notification : Group 1

Email Notification Enabled

Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency
Device-Group Specific Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Policy [Cancel changes](#)

4. Select the alert type.

5. Select **Save Policy**.

Group Event Notification : Group 1

Email Notification Enabled

Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency
Device-Group Specific Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Policy [Cancel changes](#)



If a device is enrolled in multiple groups, the Group Manager receives event notification emails for all groups to which the device is enrolled and to which the manager has been assigned

the Group Manager role.

6.5.1. Assign SNMP Notification Policies for Groups

Group Managers manage which email addresses are sent notifications when a trap event occurs in the device group. For instructions on how to enable notifications by trap groups, see [Assign SNMP Notification Policies for Trap Groups](#).

To assign Notification Policies for device groups:

1. Navigate to: **Configuration > Group Trap Settings**.
2. In the **Group Name** column, select the link of the device group for which you want to configure email notifications.

Group Trap Event Notification								
Filter Groups								
Group Name	Email Enabled	Info	Notification	Warning	Error	Critical	Alert	Emergency
Group 1			✓		✓			
Group 2		✓	✓		✓	✓		

3. Select your preferences for the **Group Trap Event** policy categories and configure the trap emails for the group.

Group Trap Event Notification : Group 1								
<input type="checkbox"/> Email Notification Enabled Warning: Email Notification is disabled.								
Policy Category	Info	Notification	Warning	Error	Critical	Alert	Emergency	
Device-Group Specific Events	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Save Policy"/> <input type="button" value="Cancel changes"/>								
Add Trap Event Notification Emails								
Add emails								
<input type="button" value="Save Emails"/> <input type="button" value="Cancel changes"/>								

- a. To enable email notification, select the **Enable Email Notification Enabled** option.
- b. To specify for which trap events to send email notifications, select the relevant options.
- c. Select **Save Policy**.

The **Group Trap Event Notification** page is displayed.

4. Configure the email notifications.
 - a. In the **Group Name** column, select the link of the group for which you

want to configure email notifications.

- b. Add the email addresses to which the notifications should be sent when a trap event occurs. There is no limit on the number of emails that you can add to the list.
- c. Select **Save Emails**.

6.5.2. Assign SNMP Notification Policies for Trap Groups

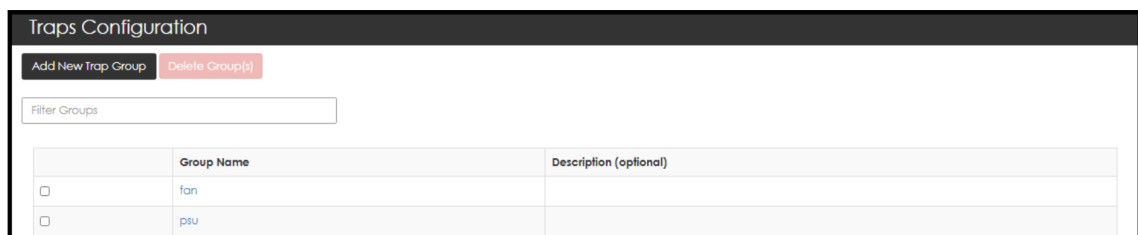
Group Managers create, edit, and manage trap groups that contain traps and a list of email addresses where notifications are sent when a trap event occurs.

For instructions on how to enable notifications by device groups, see [Assign SNMP Notification Policies for Groups](#).

To assign notification policies for trap groups:

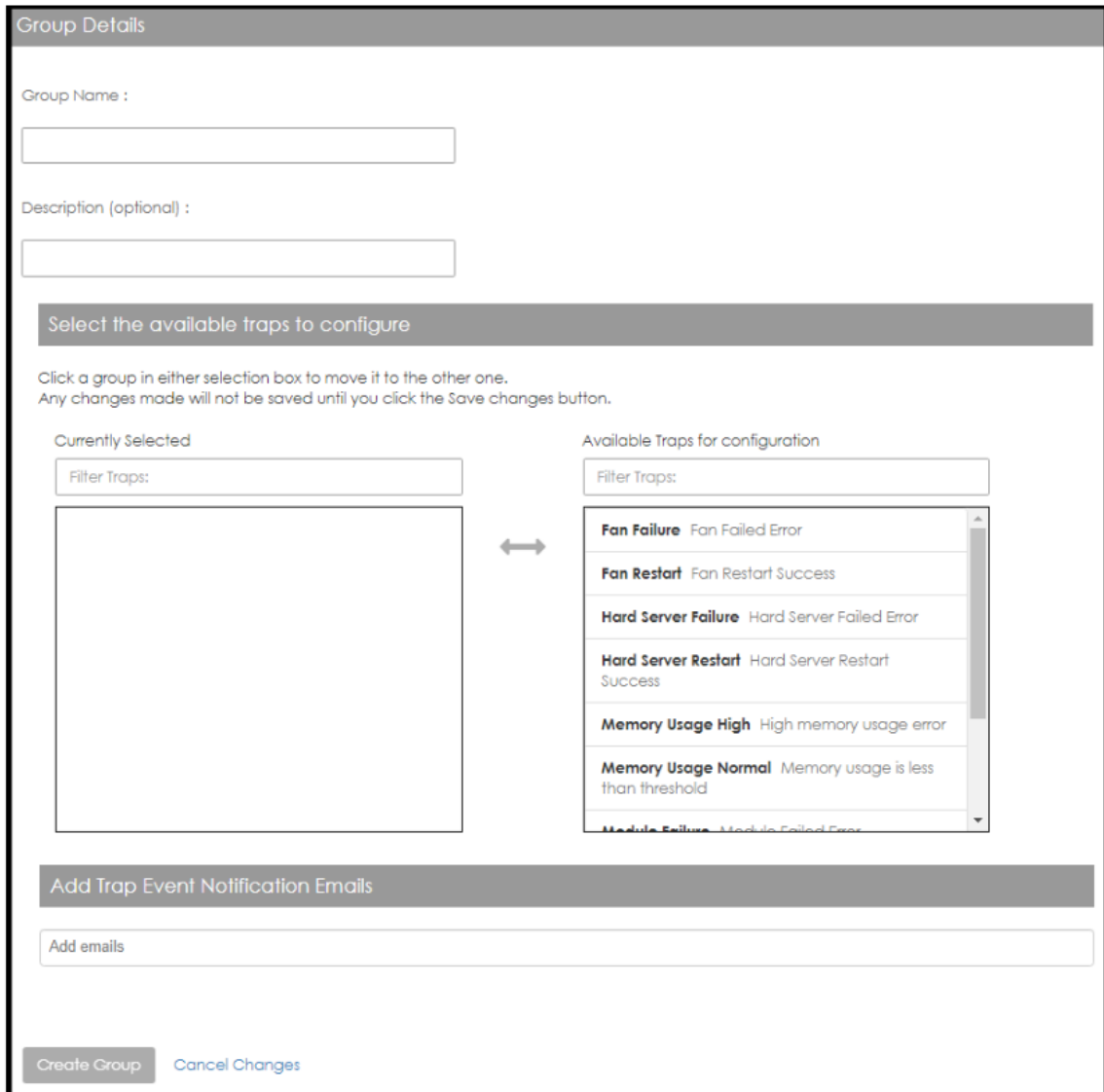
1. Navigate to: **Configuration > Trap Settings**.

The **Trap Configuration** page is displayed.



2. Select **Add New Trap Group**.

The **Group Details** page is displayed.

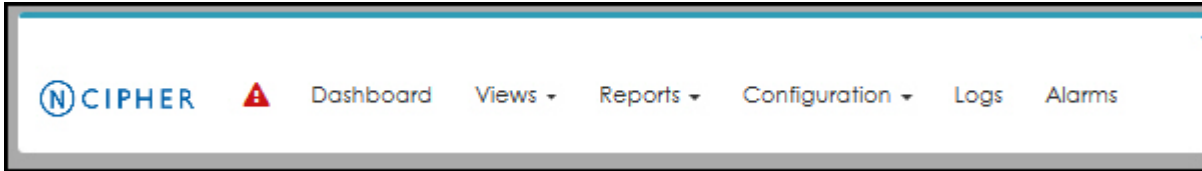


3. Enter a name for the new trap group.
4. Select traps from the list of **Available traps**. For traps supported in nShield Monitor, see [Support for nCSNMP traps](#).
5. Add the email addresses to which the notifications should be sent when a trap event occurs. There is no limit on the number of emails that you can add to the list.
6. Select **Create Group**.

The **Trap Configuration** page is displayed.

7. Logs

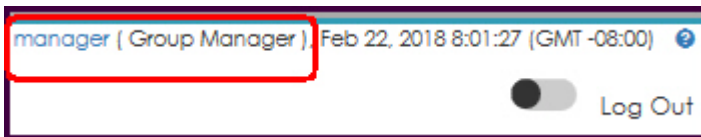
The logging capability of nShield Monitor provides a view of all ongoing events that occur in the system. Organizations can track all activities pertaining to their estate of HSMs and clients, and pro-actively evaluate a preventative maintenance strategy.



The default sorting is by sequence number.

7.1. Logs available to Group Managers

When logged in as a **Group Manager**, the logs tab provides the ability to view, sort device and filter group logs.



Logs

✓ Device/Group Log

Q Search: Add

▼ ID	Date/Time	Severity	Message
4237	2017-05-23T19:47:14.744Z	INFO	The connection status is now SNMP accessible for nShield module, SerialNumber: D2EC-D803-6D99 in group: Group 1
4236	2017-05-23T19:46:11.124Z	CRITICAL	The connection status is now unreachable for Faisal SW2 CH1 - 192.168.18.32 in group: Group 2
4235	2017-05-23T19:46:11.123Z	CRITICAL	The connection status is now unreachable for Faisal SW2 CH1 - 192.168.18.32 in group: Group 1
4234	2017-05-23T19:46:11.107Z	CRITICAL	The connection status is now unreachable for nShield module, SerialNumber: D2EC-D803-6D99 in group: Group 1
4233	2017-05-23T19:46:11.084Z	INFO	The connection status is now SNMP accessible for Faisal SW2 CH1 - 192.168.18.32 in group: Group 2

5 rows per page.

First Page « 1 2 3 » Last Page

177 Total rows . Page 1 of 36.

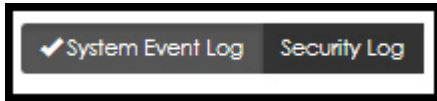
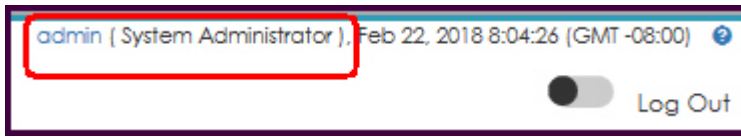
Export Log (CSV)

Logs can be exported via CSV format for further analysis.

7.2. Logs available to Administrators

When logged in as an **Administrator**, the Logs tab on the main menu bar provides the ability to view and sort system event logs, security logs, and the ability to

export the logs.



By default, the system sorts logs based on sequence. Clicking on the colored text (e.g., ID, Date/Time) toggles the order that the data is displayed.

Logs

System Event Log
 Security Log

ID	Date/Time	Severity	Message
4199	2017-05-23T16:23:29.419Z	INFO	Administrator admin has rejected an SSL option change.
4198	2017-05-23T16:23:20.560Z	INFO	Administrator admin has requested quorum approval for an SSL option change.
4197	2017-05-23T16:22:08.796Z	INFO	Administrator admin has rejected an SSL option change.
4196	2017-05-23T16:21:02.384Z	INFO	Administrator admin has requested quorum approval for an SSL option change.

rows per page.

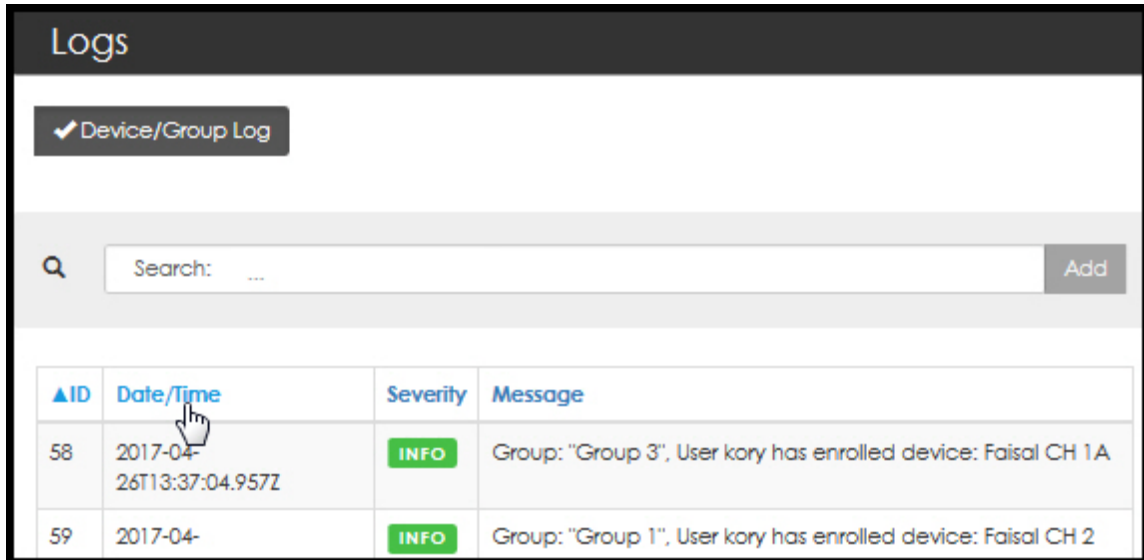
2978 Total rows . Page of 596.

Support Data/Debug Logs

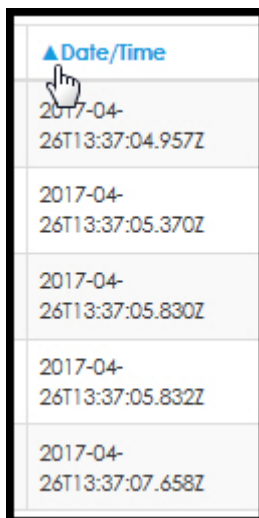
7.3. Log Sorting

nShield Monitor provides the ability to filter logs by ID, date/time, severity, and message.

1. Click on the sort condition, e.g., Date/Time

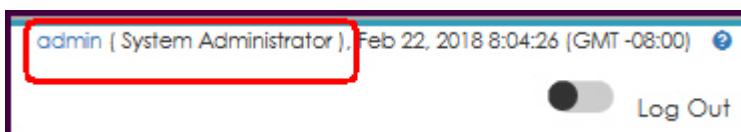


The sorting icon displays as the content is sorted.

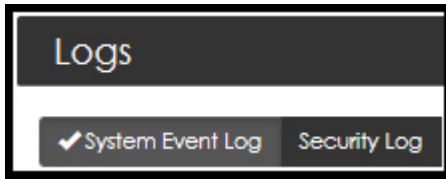


7.4. Log Functionality

 You are logged in as **Administrator**.



7.4.1. System Event Log

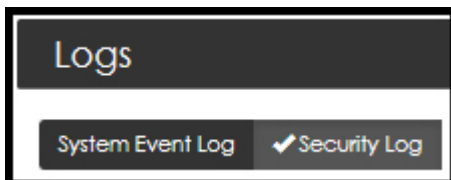


The system event log provides events that correspond to non-security related system events for nShield Monitor.

 A screenshot of the 'Logs' interface showing a list of system event log entries. The interface includes a search bar and an 'Add' button. The log entries are displayed in a table with columns for ID, Date/Time, Severity, and Message.

ID	Date/Time	Severity	Message
4199	2017-05-23T16:23:29.419Z	INFO	Administrator admin has rejected an SSL option change.
4198	2017-05-23T16:23:20.560Z	INFO	Administrator admin has requested quorum approval for an SSL option change.
4197	2017-05-23T16:22:08.796Z	INFO	Administrator admin has rejected an SSL option change.
4196	2017-05-23T16:21:02.384Z	INFO	Administrator admin has requested quorum approval for an SSL option change.

7.4.2. Security Log



The security log shows events that are related to system level security events. Events such as master key password entry, master key destruction, certificate changes, and changes to other system level security information are noted.



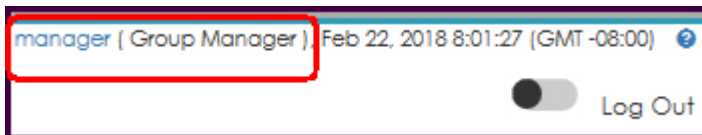
The default for sorting is by sequence number.

The screenshot shows a 'Logs' interface with two tabs: 'System Event Log' and 'Security Log' (which is selected). Below the tabs is a search bar with the text 'Search: ...' and an 'Add' button. A table displays the following log entries:

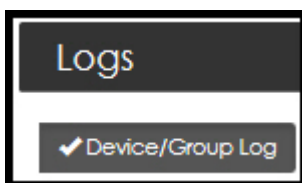
ID	Date/Time	Severity	Message
3	2017-04-26T13:20:55.657Z	INFO	User admin logged in.
4	2017-04-26T13:21:02.027Z	INFO	User admin has changed password.
5	2017-04-26T13:23:07.642Z	INFO	Master key generated by user: admin
6	2017-04-26T13:23:07.725Z	INFO	User admin has created new user: admin1
7	2017-04-26T13:23:08.361Z	INFO	Roles have changed for user: admin1

7.4.3. Device/Group Log

 You are logged on as Group Manager.



The device/group log lists events and alerts that relate to the groups for which a group manager has management rights.



Group event entries are displayed in sequential order from newest to oldest.

Logs

✓ Device/Group Log

Search: ...

ID	Date/Time	Severity	Message
109	2018-02-22T15:40:42.404Z	WARNING	The monitoring status is now enable 192.168.18.101 in group, group1 by l
108	2018-02-22T15:40:38.4038Z	WARNING	The monitoring status is now disable 192.168.18.101 in group, group1 by l
104	2018-02-22T08:59:04.594Z	ERROR	Error log count increased to 864 for 192.168.18.101 in group: group1
103	2018-02-22T04:43:03.433Z	ERROR	Error log count increased to 863 for 192.168.18.101 in group: group1
72	2018-02-21T08:59:00.590Z	ERROR	Error log count increased to 862 for 192.168.18.101 in group: group1

5 rows per page.

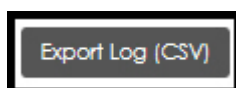
First Page « 1 2 3 » Last Page

37 Total rows .

Export Log (CSV)

7.4.4. Exporting a log.csv file

1. Select **Export Log (CSV)**.



The system prompts to open or save the **logs.csv** file.

2. Select **Open**. The log.csv file is imported into Microsoft Excel.

	A	B	C	D	E	F	G
1	Time	Severity	Message				
2	2017-01-0	INFO	The connection status is now SNMP accessible for K				
3	2017-01-0	INFO	The connection status is now SNMP accessible for K				
4	2017-01-0	INFO	The connection status is now SNMP accessible for K				
5	2017-01-0	CRITICAL	The connection status is now unreachable for Kory				
6	2017-01-0	CRITICAL	The connection status is now unreachable for Kory				

- Logs can be exported in their entirety or filtered. This includes both actions on or by a monitored system. They can also include changes in security of a given device as needed such as a tamper, changes to device SNMP credentials, or the addition of a new device. Changes in the device contact status are also displayed in the group event log and on the alarms screen.
- The default for sorting is by sequence number.
- By default, the Time format is Date/Time in GMT format. Refer to [Formatting the Admin Date and Time](#) for additional information regarding date formatting.

3. Save the Excel file, if needed.

7.4.5. Debug Log Export and Upload

A debug log export may be required to be given to Support for investigating issues. This log will need to be exported which can take several minutes to generate and export. Once exported it will need to be sent to Support.

The file does not contain any security information but does contain information related to actions taken by nShield Monitor such as polling devices, system status events, and code execution information.

The debug logs are a system for assisting in troubleshooting issues that may arise with the virtual appliance during day-to-day operation. Logs are provided on a First in First out (FIFO) basis, so if requested, the logs need to be exported as soon as possible after an issue has occurred.

Only one user can export the debug log at a time, and only administrators and auditors have the ability to perform this function.



The debug logs are not readable by users, and are to be sent to Support for analysis. Exporting large debug files requires that

| the auto logout value be set to 60 minutes.

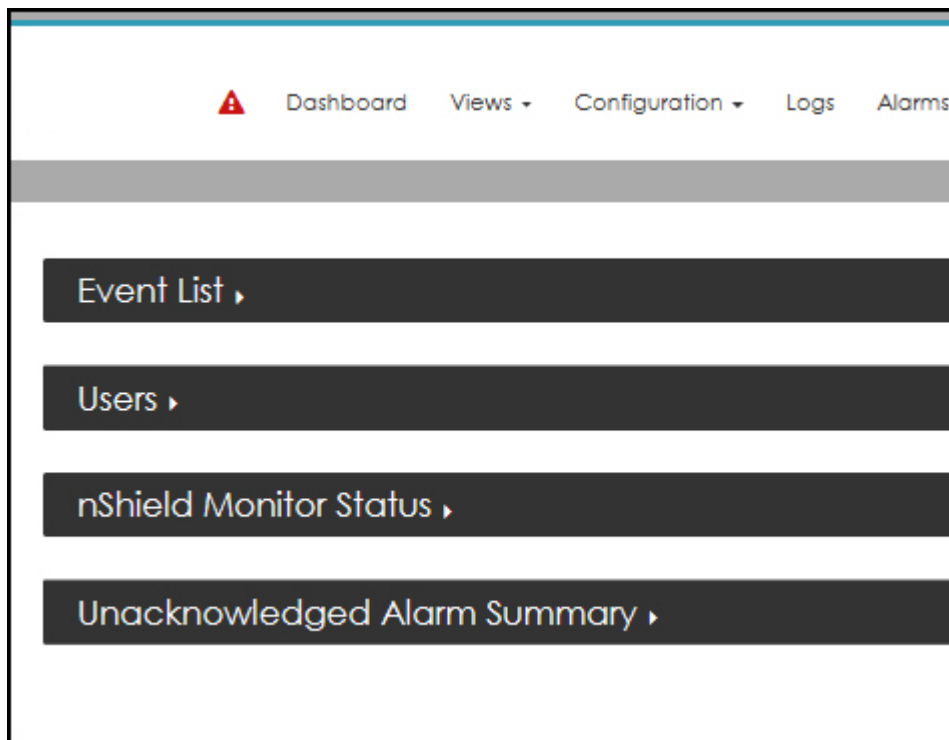
8. Dashboard

nShield Monitor provides a dashboard view when you first log on to the system.

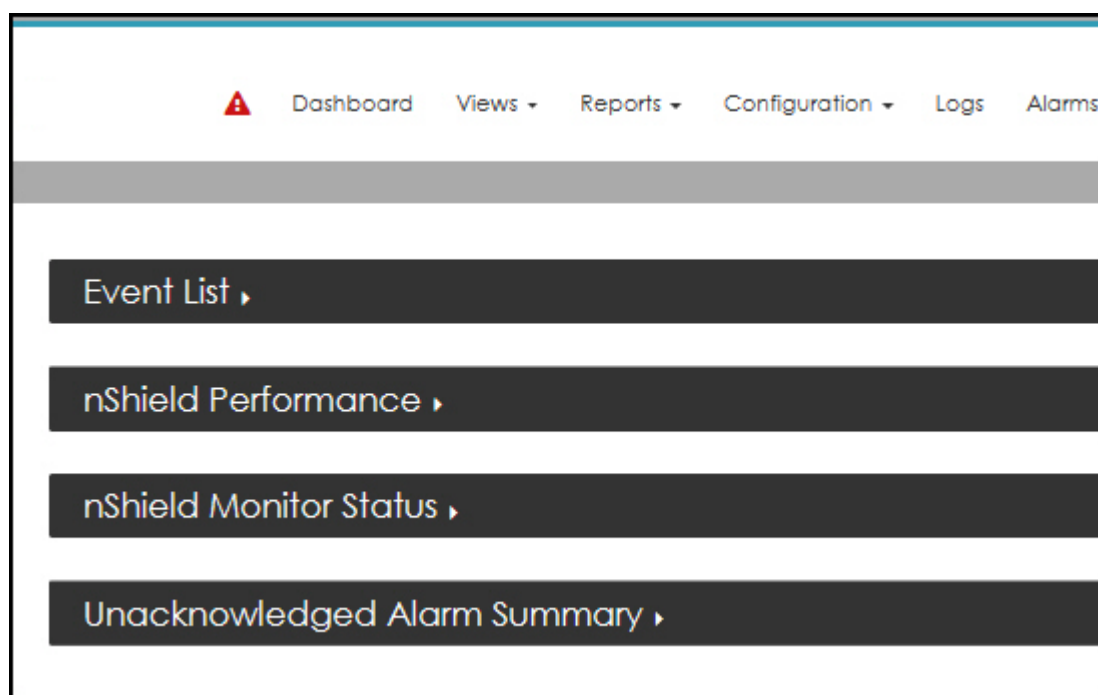
This view provides a snapshot of what is occurring with your estate and provides invaluable information for the day-to-day management of all your organization's HSMs.

The contents of the dashboard depends upon logon type:

- Logged on as **Administrator**.



- Logged in as **Group Manager**.



The following table summarizes the views based on log-on type:

Dashboard Views based on Log-on Type

Dashboard Views	Administrator logon required	Group Manager logon required
Event List	X	X
nShield Performance		X
Users		X
nShield Monitor Status	X	X
Unacknowledged Alarm Summary	X	X



The sections that follow examine each of the Dashboard Views (as identified in the table above).

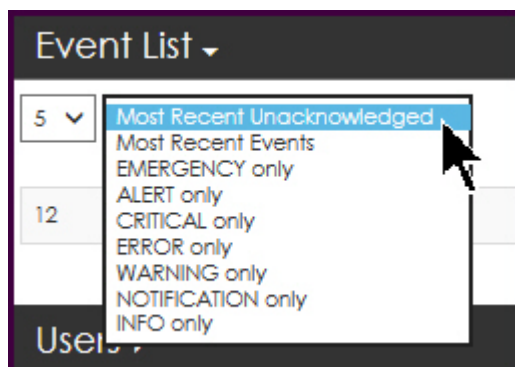
8.1. Event List

1. Select the **Event List** expansion arrow.

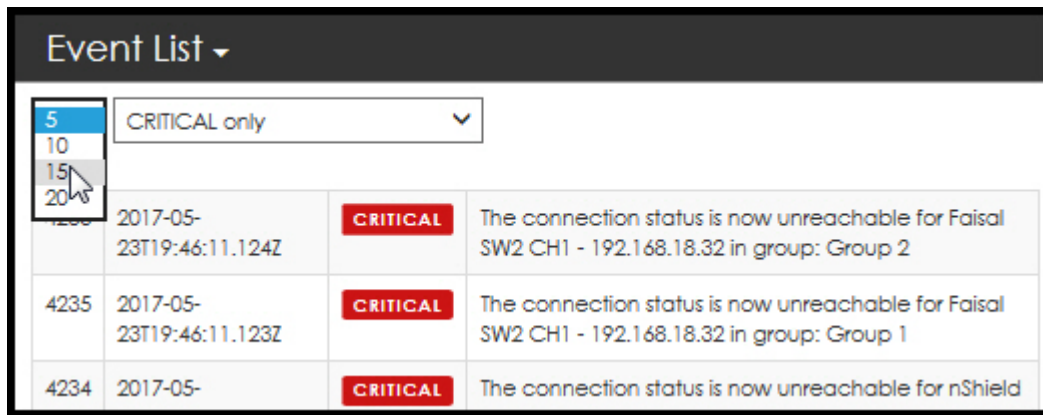
Event List ▾			
5 ▾	Most Recent Unacknowledged ▾		
4237	2017-05-23T19:47:14.744Z	INFO	The connection status is now SNMP accessible for nShield module, SerialNumber: D2EC-D803-6D99 in group: Group 1
4236	2017-05-23T19:46:11.124Z	CRITICAL	The connection status is now unreachable for Faisal SW2 CH1 - 192.168.18.32 in group: Group 2
4235	2017-05-23T19:46:11.123Z	CRITICAL	The connection status is now unreachable for Faisal SW2 CH1 - 192.168.18.32 in group: Group 1
4234	2017-05-23T19:46:11.107Z	CRITICAL	The connection status is now unreachable for nShield module, SerialNumber: D2EC-D803-6D99 in group: Group 1
4233	2017-05-23T19:46:11.084Z	INFO	The connection status is now SNMP accessible for Faisal SW2 CH1 - 192.168.18.32 in group: Group 2

From this window, you can specify the number of events (default value is 5) displayed and filter according to:

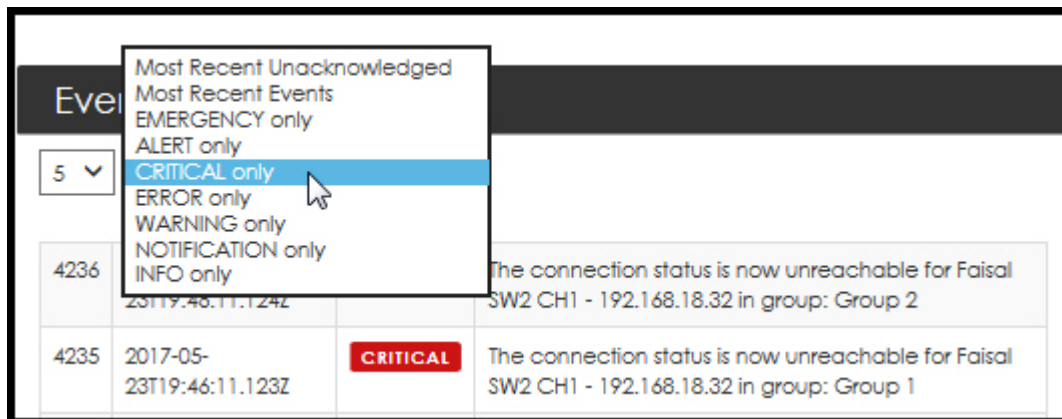
- Most Recent Unacknowledged (default value)
- Most Recent Events
- Alarm level (i.e., EMERGENCY ONLY, ALERT ONLY, etc.)



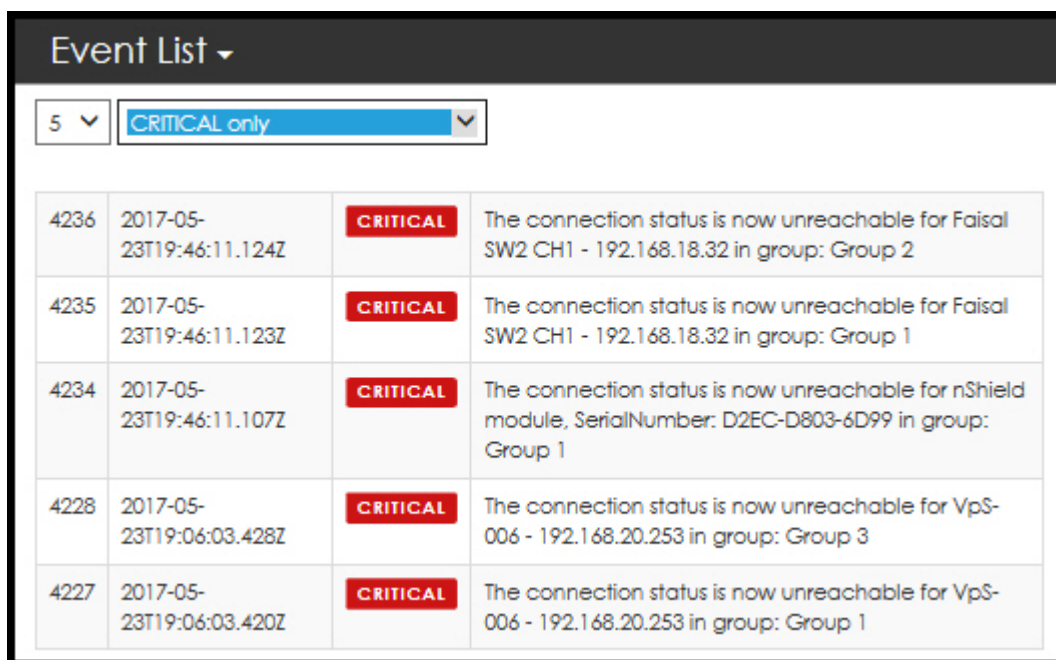
2. Select the drop down arrow to expand your choices for number of events displayed.



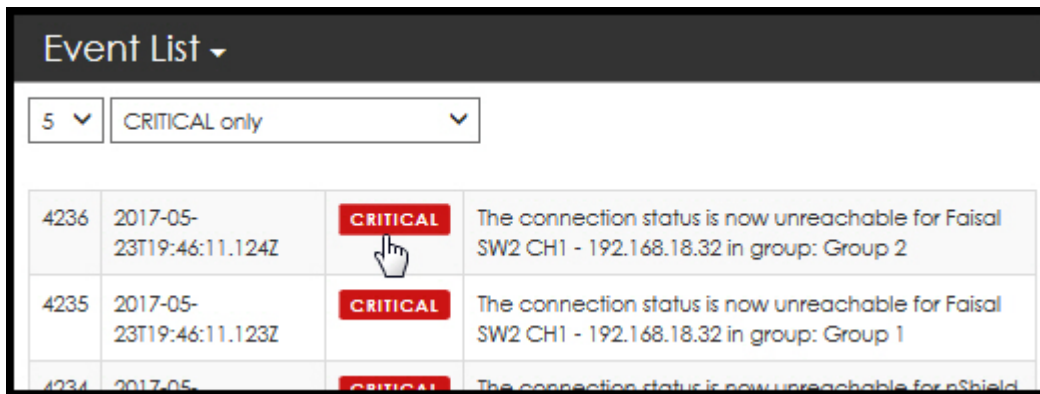
3. Select your preference.
4. Select the drop down arrow to expand your choices for event types.



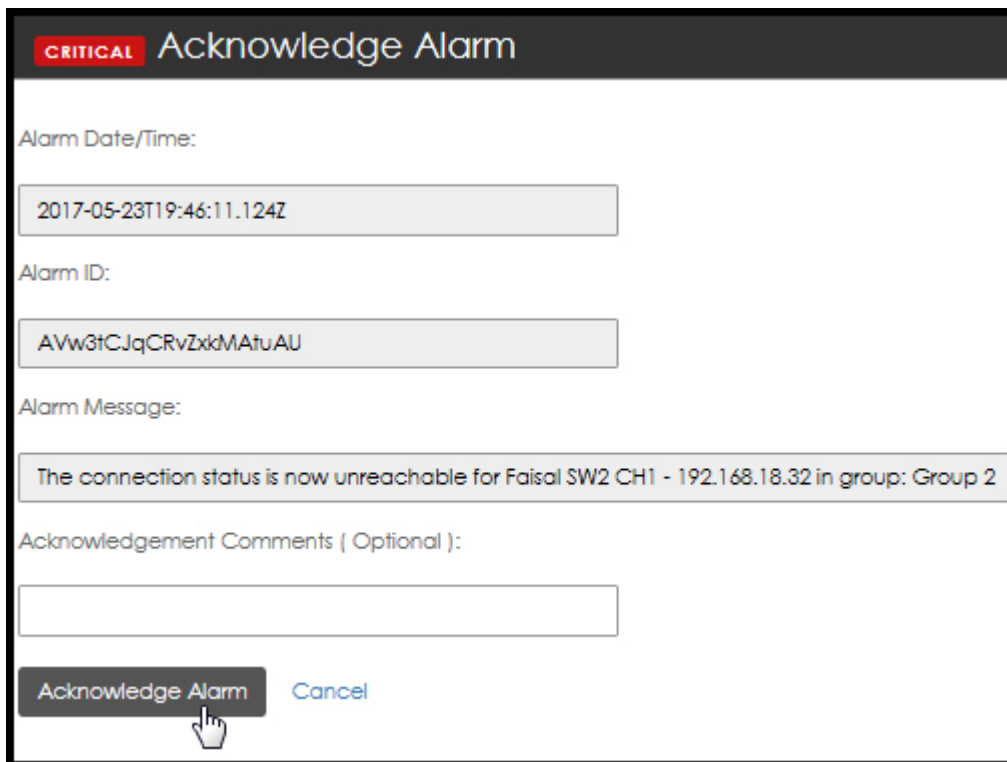
5. Select your preference, e.g. **CRITICAL only**.



6. Select the event by clicking on the event type.



The **Acknowledge Alarm** page opens:



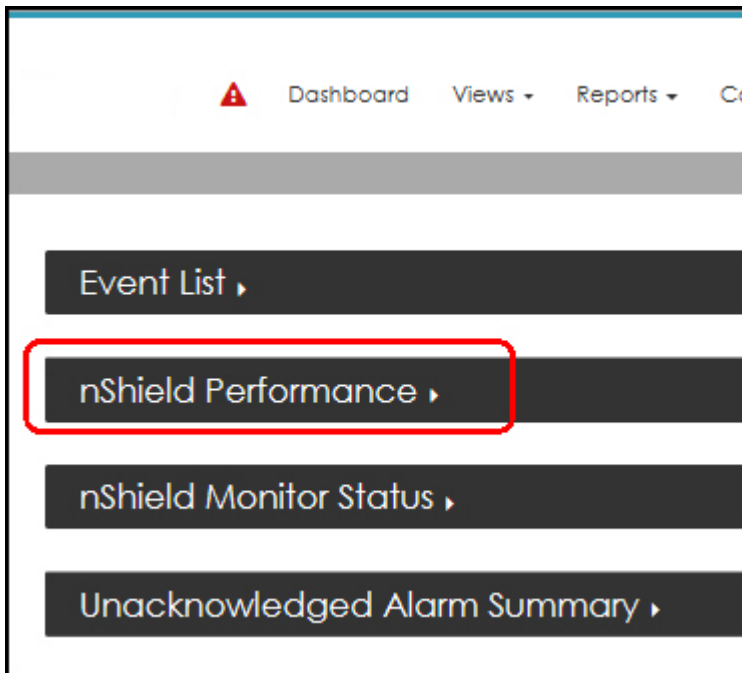
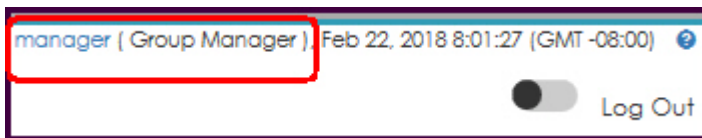
7. Enter Acknowledgment Comments, if needed.

8. Select **Acknowledge Alarm**.

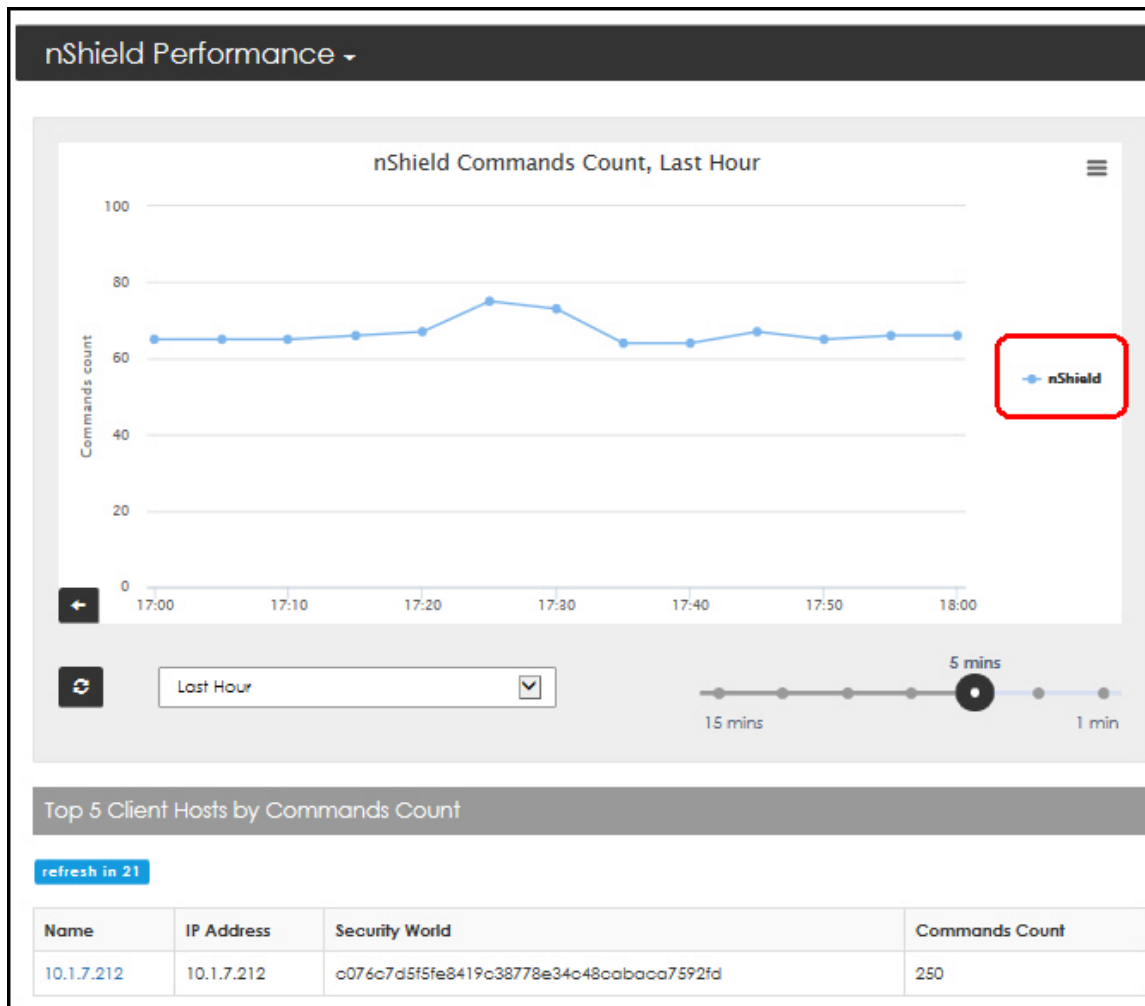
i | Selecting **Cancel** returns you to the Dashboard.

8.2. nShield Performance

i | You are logged in as a Group Manager.



1. Select the **nShield Performance** expansion arrow. Two windows open:
 - nShield Performance
 - **Top 5 Client Hosts by Command Count**



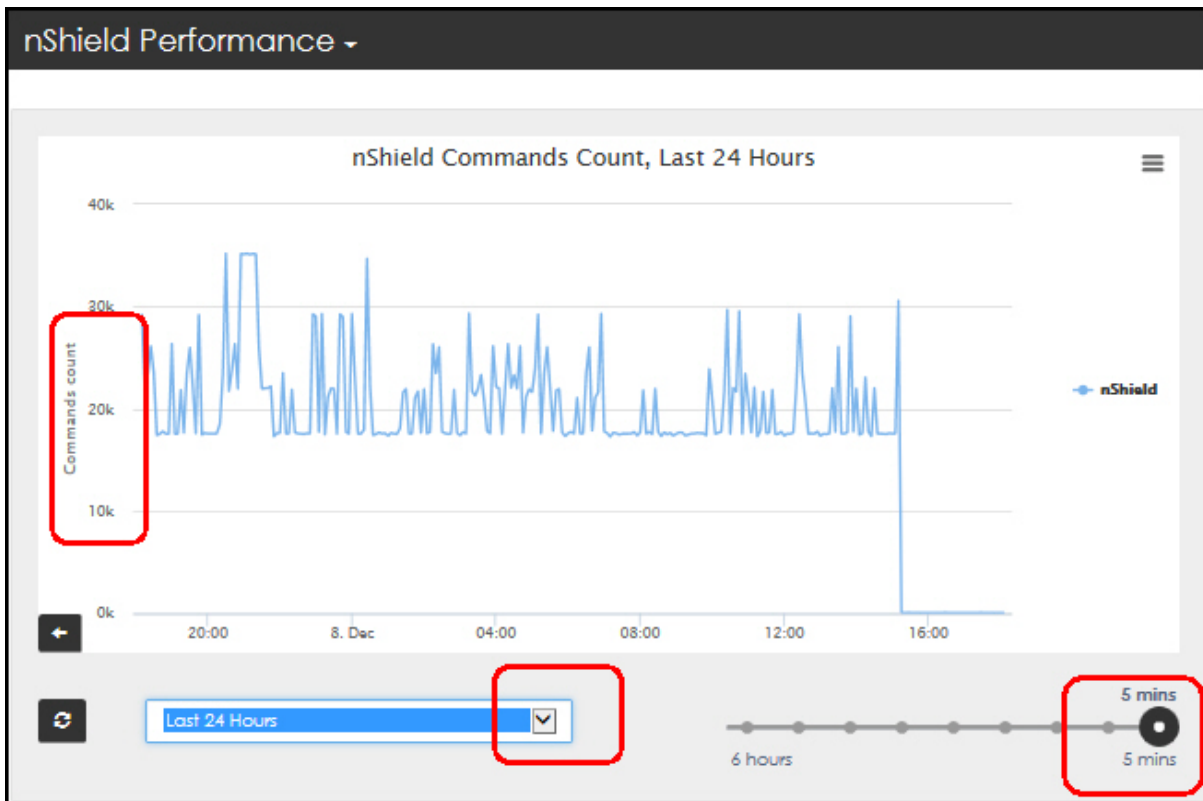
8.2.1. nShield Performance window

The performance window provides a customizable graph.

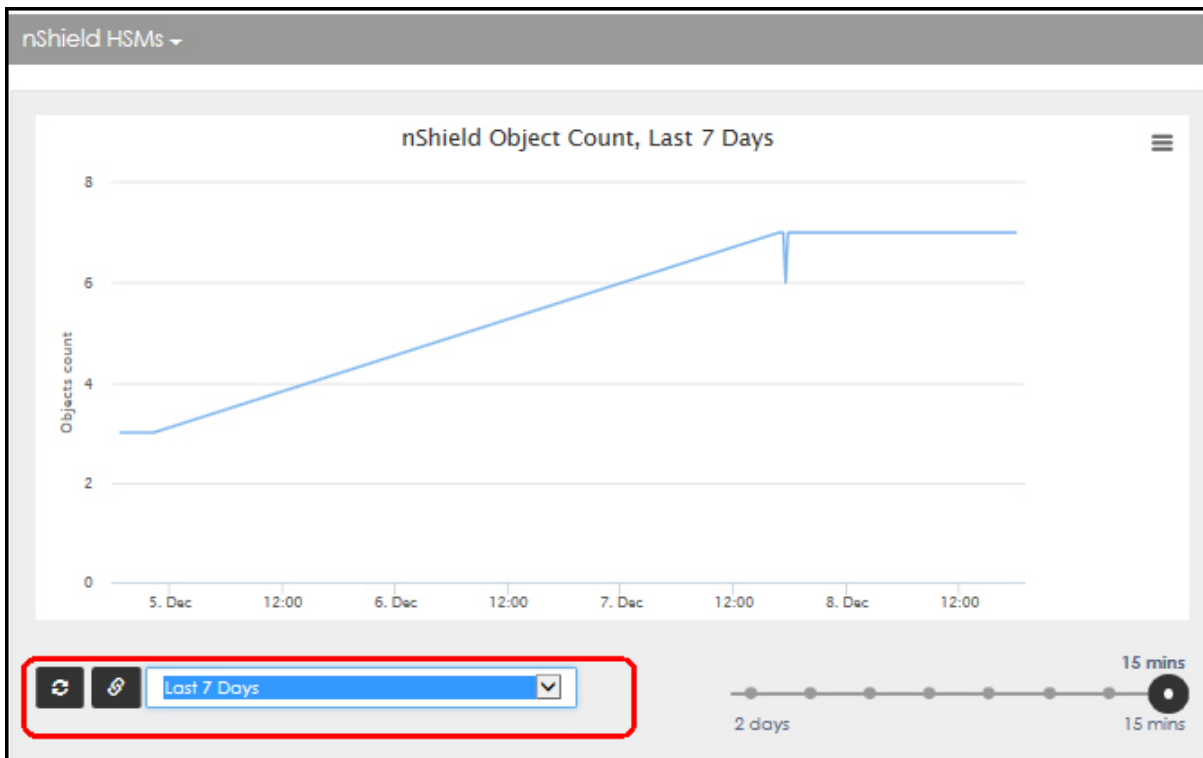
This section provides a basic overview on how to use the customization options. Refer to [Client Host Detail Page](#) for greater detail.

8.2.1.1. Navigate to a Group's Detail page

At any time, you can open a specific group's **Detail** page. A color key on the right side of the graph contains Group color line assignments, e.g., "nShield" group - circled in red above.



Clicking on Group 1's graph contents opens the **Group Detail For: Group 1** page.



Refer to [Group Details](#) for a full description of the **Group Details** page.

8.2.2. Top 5 Client Hosts by Commands Count

This window also contains a live count down until the next refresh. In the example below, the data will refresh in 24 seconds.

Top 5 Client Hosts by Commands Count			
refresh in 40			
Name	IP Address	Security World	Commands Count
10.1.7.212	10.1.7.212	c076c7d5f5fe8419c38778e34c48cabaca7592fd	216

1. Select an entry in the name list to navigate to additional windows of data.

The detail page opens.



Client Host Detail for : 10.1.7.212

IP Address/Host Name : "10.1.7.212"

Performance ▶

Health ▶

Applications with Active Connection to Hardserver ▶

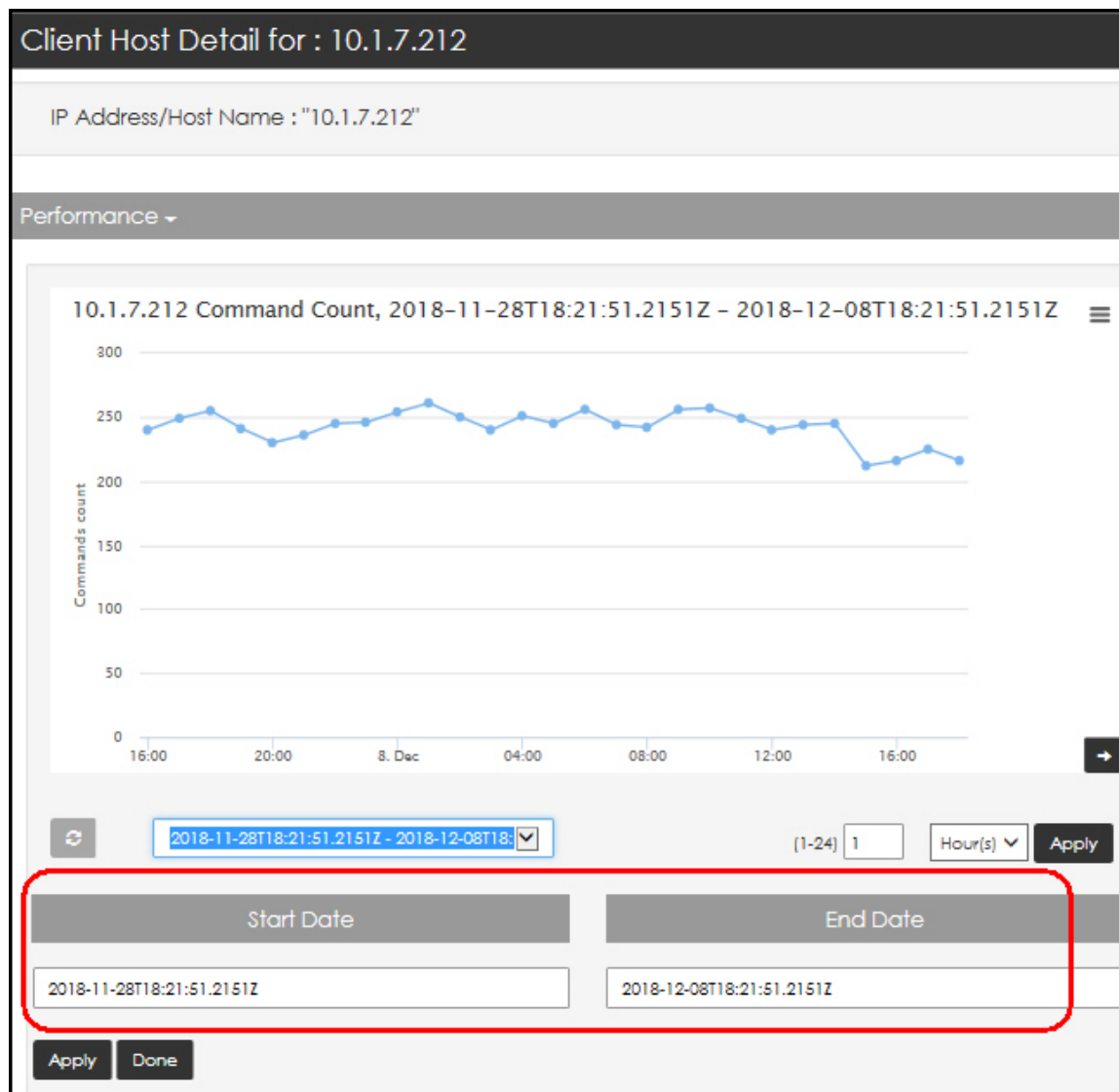
Security World Info ▶

nShield HSMs ▶

nShield Card Sets ▶

nShield Keys ▶

2. Select (i.e., click on) the **Performance** expansion arrow.



The **Start Date** and **End Date** selection boxes appear when the custom date option is selected.

3. Scroll down and click on the **Health** expansion arrow.

Client Host Detail for : 10.1.7.212

IP Address/Host Name : "10.1.7.212"

Performance ▶

Health ▼

Monitoring:	ENABLED
Status:	AVAIL_SNMP
Hardserver Status:	RUNNING
Number Of HSMs:	6
Applications With Active Connection To Hardserver:	11
Modules Failed:	TRUE
Hardserver Version:	12.40.0
Hardserver Port:	9004
Hardserver Uptime:	98 Days : 23 Hours : 21 Minutes : 14 Seconds

4. Scroll down and click on the **Applications with Active Connection to Hardserver** expansion arrow.

Applications with Active Connection to Hardserver ▼

Q Search: ... Add

Connection Number	Uptime	Command Count	Reply Count	Remote IP Address	Process ID	Process Name	Total Object Count
9	98 Days : 23 Hours : 21 Minutes : 14 Seconds	0	6176098	0.0.0.0	0		0
11	98 Days : 23 Hours : 21 Minutes : 02 Seconds	0	0	0.0.0.0	0	[legacy]	0
12	98 Days : 23 Hours : 21 Minutes : 02 Seconds	0	0	0.0.0.0	0	[legacy]	0
13	98 Days : 23 Hours : 21 Minutes : 02 Seconds	0	0	0.0.0.0	0	[legacy]	0
15	98 Days : 23 Hours : 21 Minutes : 02 Seconds	0	0	0.0.0.0	0	[legacy]	0

5. Scroll down and click on the **Security World** Info expansion arrow.

Security World Info ▾	
Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

6. Scroll down and click on the **nShield HSMs** expansion arrow.

nShield HSMs ▾			
<input type="text" value="Search: ..."/>			
Serial No.	Type	Mode	Commands Last Hr.
0305-02E0-D947	CONNECT XC	FAILED	0
2805-02E0-D947	CONNECT XC	FAILED	0
6699-74B4-30FF	CONNECT	OPERATIONAL	3936
6F99-74BF-429B	CONNECT	OPERATIONAL	3953
B56A-81C9-73F2	CONNECT	OPERATIONAL	3948

7. Scroll down and click on the **nShield Card Sets** expansion arrow.

nShield Card Sets ▾		
<input type="text" value="Search: ..."/>		
Set Name	Client Host Count	Generation Time
cmoc01	1	2016-09-16T23:49:30.4930Z
oc1	1	2016-03-15T18:17:12.1712Z
oc2	1	2016-03-15T23:07:15.715Z

8. Scroll down and click on the **nShield Keys** expansion arrow.

nShield Keys ▾

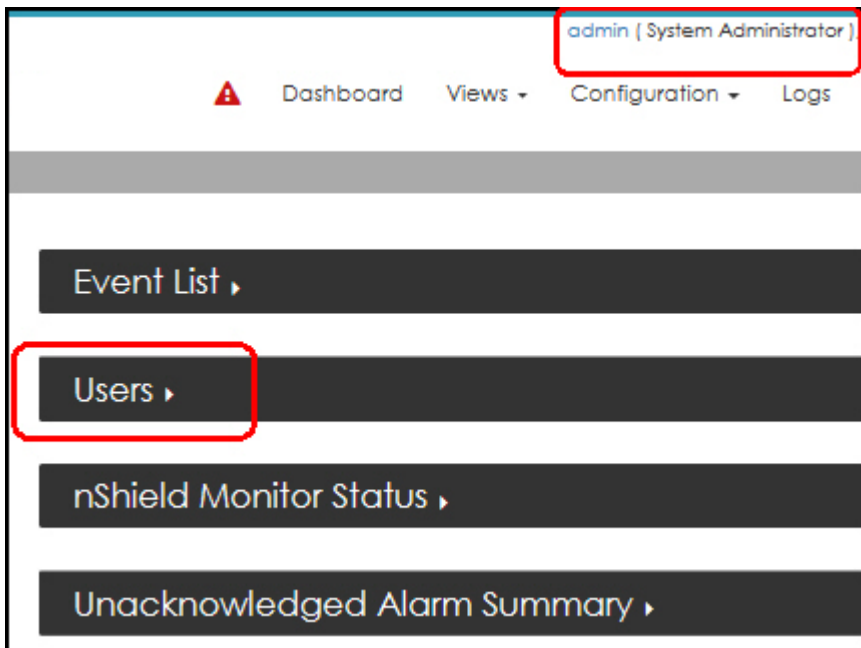
Search: ... Add

Key Identifier/Name	Key Hash	Key Application Name	Client Hosts
2a4c35143e8a5ab13782d71e909e7ab57fd8b15b	0e8db787df4de74b45e16d9c016c14e12e231505	embed	1
6ffc2755601f7472c8b4a3d2515eafe53c964efd- oooooooo	1f3c2f6231f8fe07b3b31ecd1456651b88eca2d2	embed	1
8fd31935920b3b47abe145e7ecdbed87dba7fe55	429ce182a09a5b7cb088e64f9551ed61f181e317	embed	1
ff1	7386cc17bca937d59df56ff74f88207c1bd8edff	simple	1
ff2	bdbfdfa419715482c298d8238456b00749a8ddee	simple	1

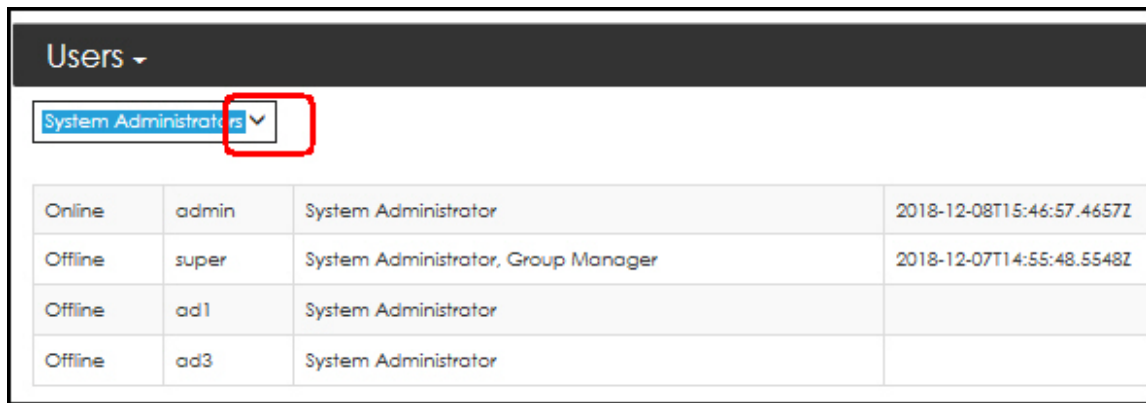
i | At any time, you can select **Back to Previous Page**.

8.3. Users

i | You are logged in as an **Administrator**.



1. Click the Users expansion arrow.
2. Select the drop down arrow to open the filtering options.



The screenshot shows a dashboard titled 'Users' with a dropdown menu for filtering. The selected option is 'System Administrators', which is highlighted with a red box. Below the dropdown is a table with four rows of user data.

Status	Username	Role	Last Login
Online	admin	System Administrator	2018-12-08T15:46:57.4657Z
Offline	super	System Administrator, Group Manager	2018-12-07T14:55:48.5548Z
Offline	ad1	System Administrator	
Offline	ad3	System Administrator	

3. Select your preferred view. Filters include:

- System Administrators
- Group Managers
- System Auditors
- Last 5 login
- Locked Out

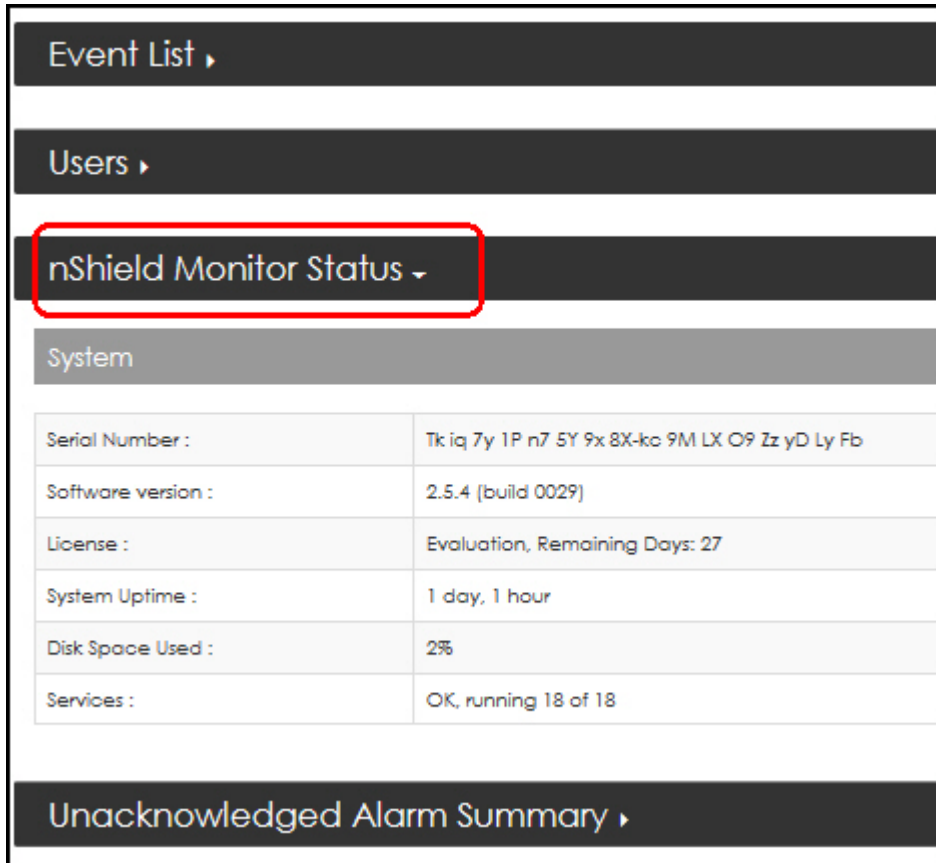
The display reflects your selected filter option.

8.4. nShield Monitor Status



You are logged in as an **Administrator**.

1. Select the **nShield Monitor Status** expansion arrow.



The screenshot shows a dashboard with several menu items: 'Event List', 'Users', 'nShield Monitor Status' (highlighted with a red box), 'System', and 'Unacknowledged Alarm Summary'. The 'System' section contains a table with the following data:

Serial Number :	Tk iq 7y 1P n7 5Y 9x 8X-ko 9M LX O9 Zz yD Ly Fb
Software version :	2.5.4 (build 0029)
License :	Evaluation, Remaining Days: 27
System Uptime :	1 day, 1 hour
Disk Space Used :	2%
Services :	OK, running 18 of 18

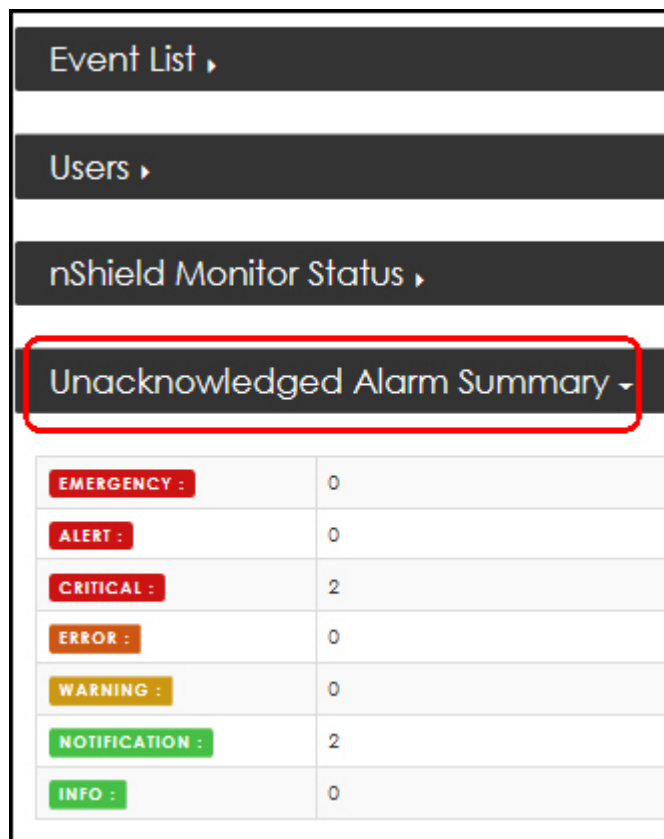
The status data is displayed.

8.5. Unacknowledged Alarm Summary



You are logged in as an Administrator.

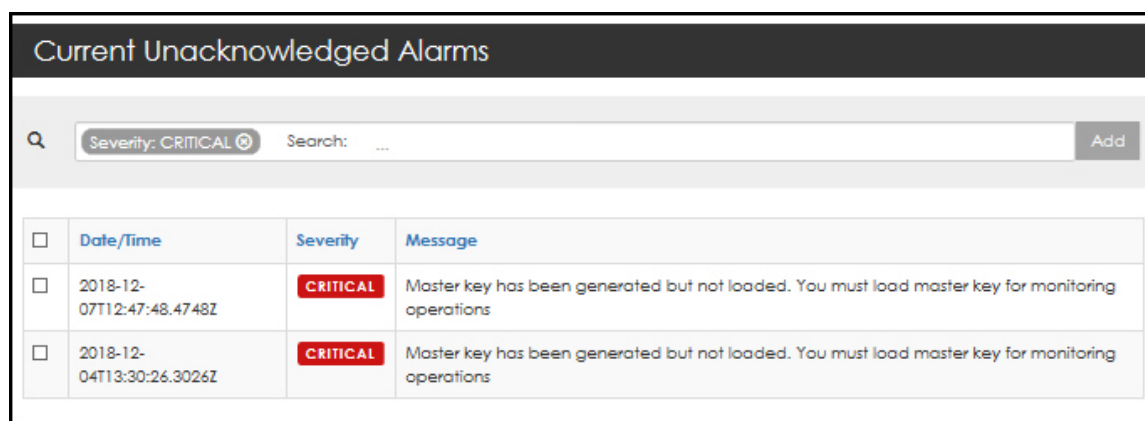
1. Scroll down, if needed, and select the **nUnacknowledged Alarm Summary** expansion arrow.



The screenshot shows a vertical navigation menu with the following items: 'Event List', 'Users', 'nShield Monitor Status', and 'Unacknowledged Alarm Summary'. The 'Unacknowledged Alarm Summary' item is highlighted with a red rectangular box. Below the menu is a table showing the counts for various alarm types.

EMERGENCY :	0
ALERT :	0
CRITICAL :	2
ERROR :	0
WARNING :	0
NOTIFICATION :	2
INFO :	0

2. Select the alarm type, e.g., click on **CRITICAL**. The **Current Unacknowledged Alarms** detail page opens.



The screenshot shows the 'Current Unacknowledged Alarms' detail page. It features a search bar with a filter set to 'Severity: CRITICAL' and an 'Add' button. Below the search bar is a table with two columns: 'Date/Time' and 'Severity'. The table contains two rows of data, both with a 'CRITICAL' severity.

<input type="checkbox"/>	Date/Time	Severity	Message
<input type="checkbox"/>	2018-12-07T12:47:48.4748Z	CRITICAL	Master key has been generated but not loaded. You must load master key for monitoring operations
<input type="checkbox"/>	2018-12-04T13:30:26.3026Z	CRITICAL	Master key has been generated but not loaded. You must load master key for monitoring operations

3. Select the alarm for acknowledgment.

4. Enter Acknowledgment Comments, if needed.
5. Select **Acknowledge Alarm**.



From the **Current Unacknowledged Alarms** window, you can also click on the severity type (e.g., click on **CRITICAL**), to open the **Acknowledge Alarm** window.

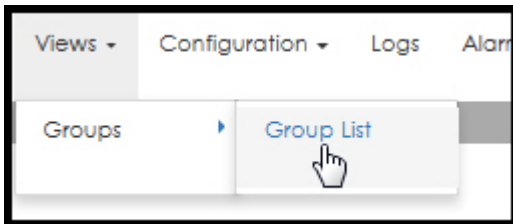
9. Views

User login type determines which options are displayed.

9.1. Logged in as Administrator

1. Navigate to:

Views > Groups > Group List



The **Group Summary** page opens.

 A screenshot of the 'Group Summary' page. The page has a search bar and an 'Add' button. Below is a table with the following data:

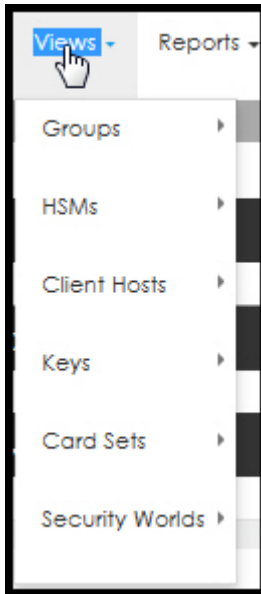
▲ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
1	DISABLED	3 1 4 5	0	0	
10	DISABLED	1 1	0	1	
2	DISABLED	1 2 2	0	0	
3	DISABLED	1 1 1	0	0	
4	DISABLED		0	0	

On this page, you can **sort the display** order of the **Group Name** column and the **Description** column.

Refer to [View > Group > Group List](#) for additional information on Administrator options under Group List.

9.2. Logged in as Group Manager

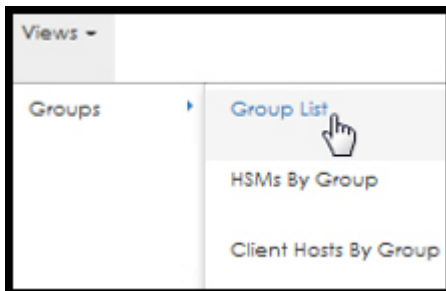
Logged on as Group Manager provides the following navigational options:



9.2.1. View > Groups

View **Groups** drop down has three destinations:

- Group List. Refer to [View > Group > Group List](#), for additional information on Group Manager options under Group List.
- HSMs By Group
- Client Hosts By Group



View > Groups > Group List

Group Summary page

Navigational links:

Group Name > Group Detail page

Alarm count > Current Unacknowledged Alarms page

nShield > HSMs By Group page

Client Hosts > HSMs By Group page

View > Group > HSMs By Group

Group <n> There are <n> nShields in this group page

Expand the pane:

nShield HSMs

Navigational links:

Serial No. > HSM Detail page

Alarm count > Current Unacknowledged Alarms page

Security World > Security World Detail page

Client Host Count > Client Hosts By HSM page

View > Group > Client Hosts By Group

Group <n> There are <n> client host(s) in this group page

Expand the pane:

Navigational links:

Name > Client Host Detail page

HSM count > HSMs By Client Host page

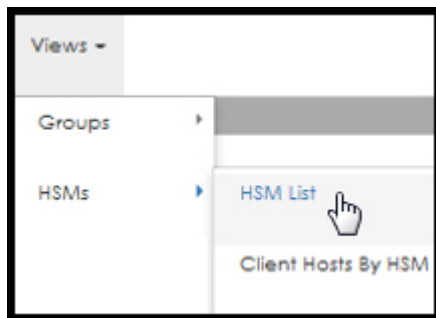
Alarm count > Unacknowledged Alarms page

Security World > Security World Detail page

9.2.2. View > HSMs

View **HSMs** drop down has two destinations:

- HSM List
- Client Hosts By HSM



View > HSMs > HSM List

HSM Summary page

nShield HSMs

Navigational links:

Serial No. > HSM Detail page

Alarm count > Current Unacknowledged Alarms page

Security World > Security World Detail page

Client Host(s) count > Client Hosts By HSM page

View > HSMs > Client Hosts By HSMs

There are <n> client host(s) in this nShield page

Expand the pane:

Navigational links:

Name > Client Host Detail page

HSMs count > HSMs By Client Host page

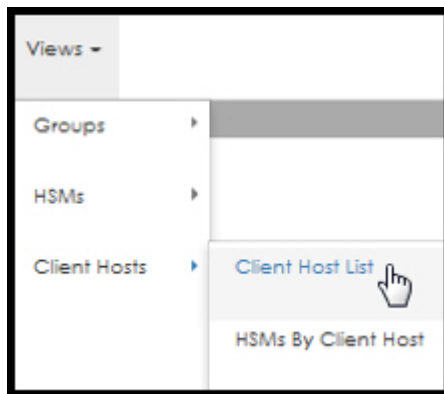
Alarm count > Current Unacknowledged Alarms page

Security World > Security World Detail page

9.2.3. View > Client Hosts

View **Client Hosts** has two destinations:

- Client Host List
- HSMs By Client Hosts



View > Client Hosts > Client Hosts List

Client Host Summary page

Navigational links:

Name > Client Host Detail page

HSMs count > HSMs By Client Host page

Alarm count > Unacknowledged Alarms page

Security World > Security World Detail page

View > Client Hosts > HSMs By Client Hosts

There are <n> nShield(s) in this client host page

Expand the pane:

Navigational links:

Serial No. > HSM Detail page

Alarm count > Current Unacknowledged Alarm page

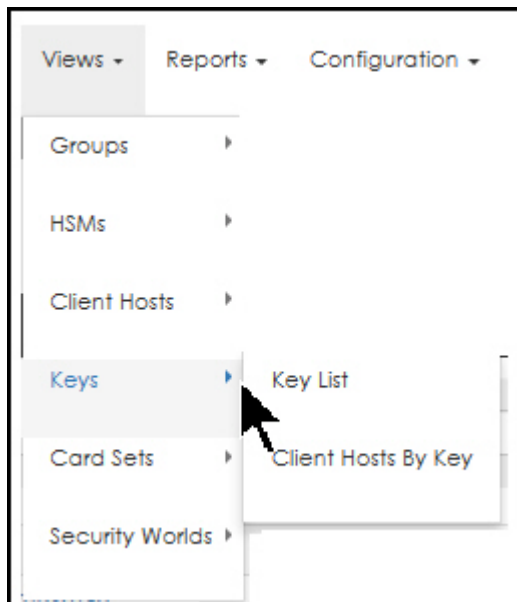
Security World > Security World Detail page

Client Host(s) count > Client Hosts By HSM page

9.2.4. View > Keys

View Keys has two destinations:

- Key List
- Client Hosts By Key



View > Keys > Key List

Key Summary page

Navigational links:

Key Name/Identifier > Key Detail page

Client Hosts > Client Hosts By Key page

View > Keys > Client Hosts By Key

Key Summary page

There are <n> client host(s) with this key page

Expand the pane:

Navigational links:

Name > Client Host Detail page

HSMs > HSMs by Client Host page

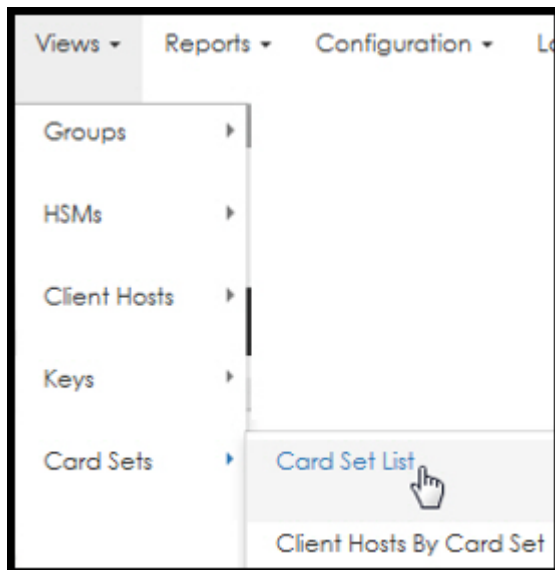
Alarm count > Current Unacknowledged Alarms page

Security World > Security World Detail page

9.2.5. View > Card Sets

View Card Sets has two destinations:

- Card Set List
- Client Hosts By Card Set



View > Card Sets > Card Set List

Card Set Summary page

Navigational links:

Set Name > Card Set Detail page

Client Host count > Client Hosts By Card Set page

View > Card Sets > Client Hosts By Card Set

There are <n> client host(s) with this cardset page

Expand the pane:

Navigational links:

Name > Client Host Detail page

HSMs > HSMs By Client Host page

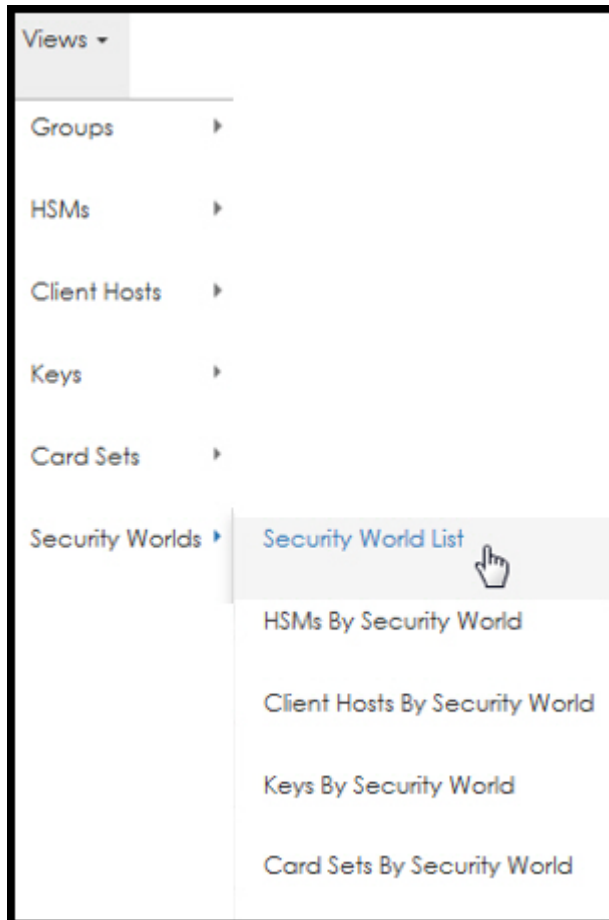
Alarm count > Current Unacknowledged Alarms page

Security World > Security World Detail page

9.2.6. View > Security Worlds

View Security Worlds has five destinations:

- Security World List
- HSMs By Security World
- Client Hosts By Security World
- Keys By Security World
- Card Sets By Security World



View > Security Worlds > Security World List

Security World Summary page

Navigational links:

Name > Security World Detail page

HashKNSO > Security World Detail page

Client Hosts count > Client Hosts By Security World page

nShield count > HSMs By Security World page

View > Security Worlds > HSMs By Security World

There are <n> nShields in this security world page

Expand the pane:

Navigational links:

Serial No. > HSM Detail page

Alarm count > Current Unacknowledged Alarms page

Client Host(s) count > Client Hosts By HSM page

View > Security Worlds > Client Hosts By Security World

There are <n> client host(s) in this security world page

Expand the pane:

Navigational links:

Name > Client Host Detail page

HSMs count > HSMs By Client Host page

Alarm count > Unacknowledged Alarms page

View > Security Worlds > Keys By Security World

There are <n> keys(s) in this security world page

Expand the pane:

Navigational links:

Key Name/Identifier > Key Detail page

Client Hosts count > Client Hosts By Key page

View > Security Worlds > Card Sets By Security World

There are <n> card set(s) in this security world page

Expand the pane:

Navigational links:

Set Name > Card Set Detail page

Client Hosts count > Client Hosts By Card Set page

9.3. View > Group > Group List

From the View tab, whether logged in as an Administrator or as a Group Manager (or Auditor), you are able to navigate to the **Group List** page.

The **Group List** page provides a group summary listing of groups configured in the virtual appliance as well as utilization information, host command information, and overload, alarm information, and a column for descriptive information.



When logged on as a Group Manager, you can navigate through the View menu to **acknowledge alarms**.

The options provided in the View drop down menu is directly tied to your logon.

- Administrator
- Group Manager
- Auditor

The Auditor has the same views (i.e., menu drop downs) as the Group Manager; however, the auditor has no ability to perform any actions. For example, an Auditor can not acknowledge alarms or enter comments, etc.

9.3.1. Group List > Group Summary - Administrator

The **Group Summary** page provides an easy to use view that updates every 60 seconds as information is polled.

1. Navigate to:

Views > Groups > Group List

The **Group Summary** page opens.



When logged in as an Administrator, you can only **view** all groups. You **can not perform** any other actions on these groups.

The screenshot shows the 'Group Summary' page with a navigation bar at the top containing 'Group List' (highlighted with a red box), 'HSMs By Group', and 'Client Hosts By Group'. Below the navigation bar is a search bar with the text 'Search: ...' and an 'Add' button. The main content is a table with the following data:

▲ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
1	DISABLED	3 1 4 5	0	0	
10	DISABLED	1 1	0	1	
2	DISABLED	1 2 2	0	0	
3	DISABLED	1 1 1	0	0	
4	DISABLED		0	0	



As an **Administrator**, you are able to sort the data displayed.



Black column headers indicate that the contents of the column can **not** be sorted while blue column headers indicate that the contents of the column can be sorted.

The screenshot shows the 'Group Summary' page with the 'Group Name' column header highlighted by a red box. The table data is as follows:

▼ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
Test V...	DISABLED		0	0	
nShield	0%	45 9 2 30	6	1	
4	DISABLED		0	0	
3	DISABLED	1 1 1	0	0	
2	DISABLED	1 2 2	0	0	

2. Toggle the sort, if needed.
3. Hover over an alarm total in the **Alarm** column to view the **severity pop-up**.

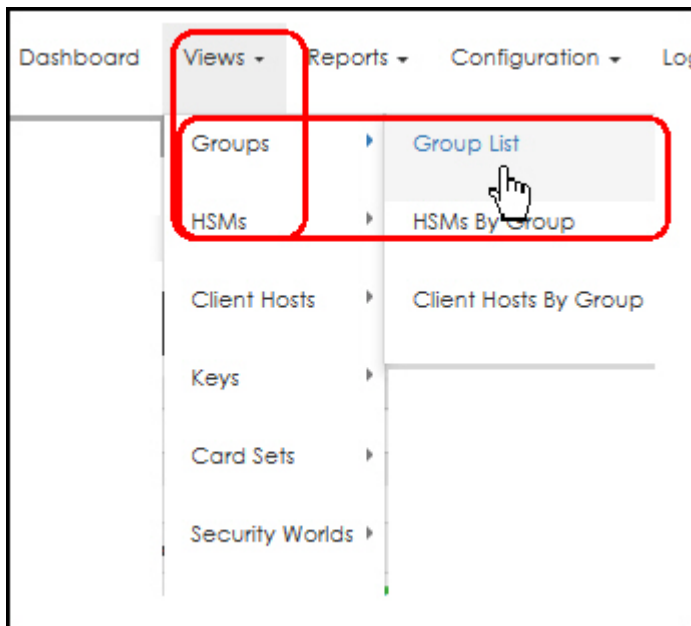
Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
Test VpS	DISABLED		0	0	
nShield	0%	45 9 2 30 Critical	6	1	
4	DISABLED		0	0	
3	DISABLED	1 1 1	0	0	
2	DISABLED	1 2 2	0	0	

9.3.2. Group List > Group Summary - Group Manager

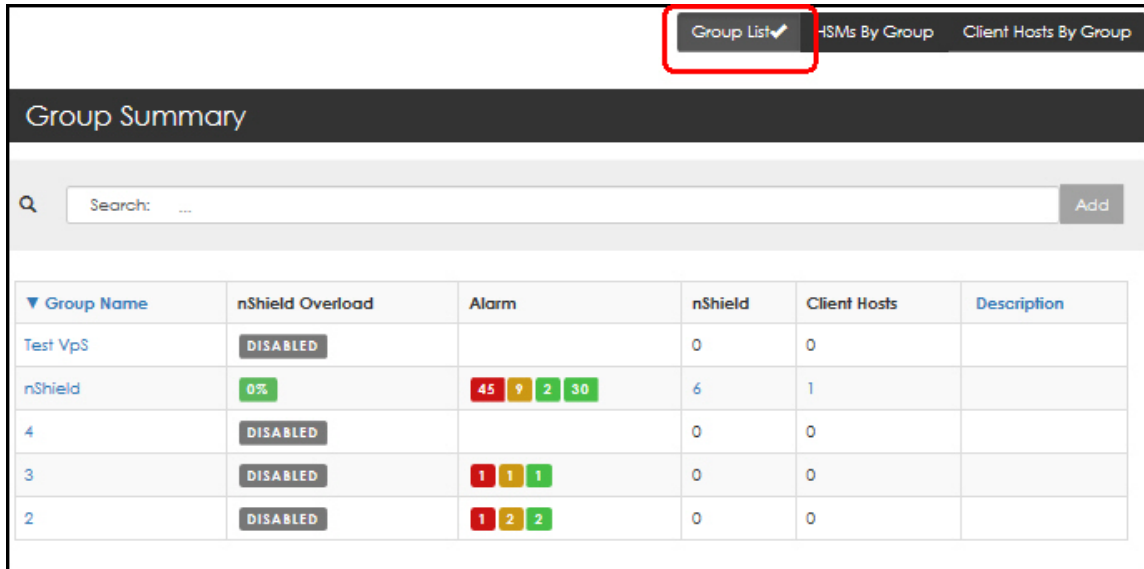
When logged in as Group Manager, all groups assigned to you are listed.

1. Navigate to:

Views > Groups > Group List



The **Group Summary** page opens.

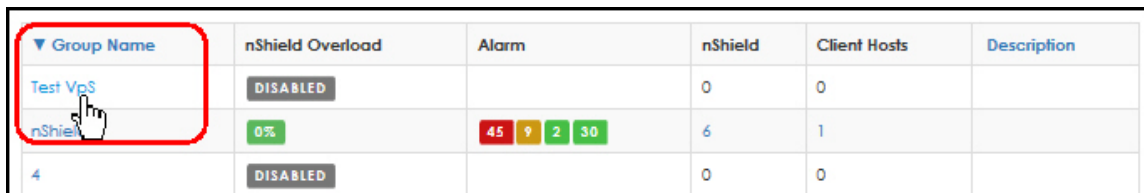


9.3.3. Group Summary page - Navigation options

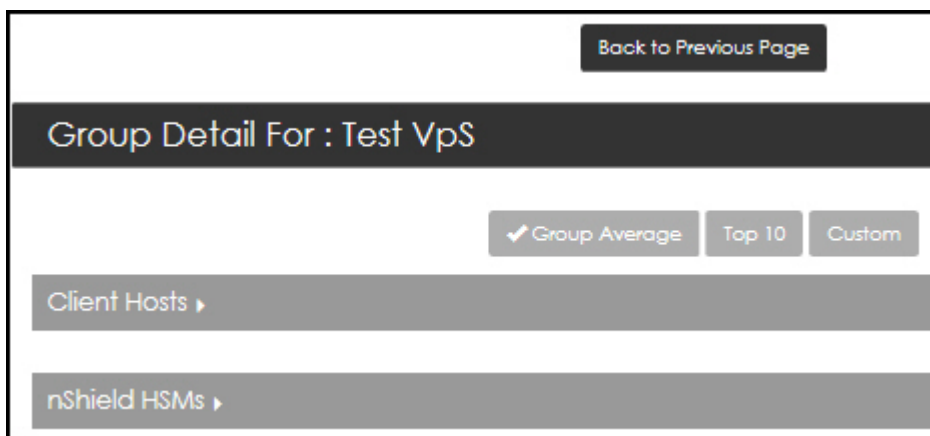
The **Group Summary** contains three navigation points.

Selecting any one of the following opens a new page:

- A specific **Group Name**



The **Group Detail** page opens.



- A specific **Alarm**

▼ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
Test VpS	DISABLED		0	0	
nShield	0%	45 9 2 30 Critical	6	1	
4	DISABLED		0	0	
3	DISABLED	1 1 1	0	0	

The **Current Unacknowledged Alarms** page opens.

Current Unacknowledged Alarms

Q Severity: CRITICAL Search: Add

<input type="checkbox"/>	Date/Time	Severity	Message
<input checked="" type="checkbox"/>	2018-12-08T10:09:16.916Z	CRITICAL	The connection status is now unreachable for nShield module, 10.1.3.78 in group: nShield
<input type="checkbox"/>	2018-12-08T10:09:16.916Z	CRITICAL	The connection status is now unreachable for nShield module, 10.1.3.72 in group: nShield
<input type="checkbox"/>	2018-12-08T10:09:16.916Z	CRITICAL	The connection status is now unreachable for 10.1.7.212 - 10.1.7.212 in group: nShield
<input type="checkbox"/>	2018-12-08T10:09:16.916Z	CRITICAL	The connection status is now unreachable for nShield module, 10.1.3.77 in group: nShield
<input type="checkbox"/>	2018-12-08T10:09:16.916Z	CRITICAL	The connection status is now unreachable for nShield module, 10.1.3.71 in group: nShield

5 rows per page.
First Page « 1 2 3 » Last Page
45 Total rows . Page 1 of 9.

Acknowledgement Comments (Optional):

Acknowledge Alarm
Cancel

You can acknowledge the alarm by checking the box to open the Acknowledge Alarm page.

- A specific entity

Group Summary

Q Search: ... Add

▲ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
1	DISABLED	3 1 4 5	0	0	
10	DISABLED	1 1	0	1	
2	DISABLED	1 2 2	0	0	
3	DISABLED	1 1 1	0	0	
4	DISABLED		0	0	

The **Client Hosts By Group** page opens.

Client Hosts By Group

Q Name: 10 Search: ... Add

10 - There are 1 client host(s) in this group.

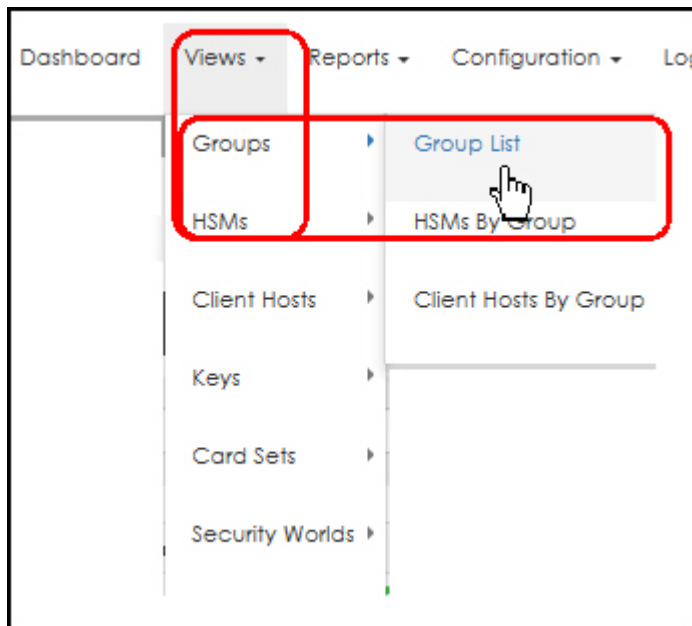
Q Search: ... Add

Name	Monitoring	Hardserver Status	Commands Last Hr.	HSMs	Alarm	▲ Last Update	Location	Security World	HSMs Failed
testdevice1	UNREACHABLE	UNKNOWN	0		3 2 3		location		

9.3.3.1. Alarms Acknowledgment Views

1. Navigate to:

View > Groups > Group List



The **Group Summary** page opens.

Group Summary					
<input type="text" value="Search: ..."/> Add					
▲ Group Name	nShield Overload	Alarm	nShield	Client Hosts	Description
1	DISABLED	3 1 4 5	0	0	
10	DISABLED	1 1	0	1	
2	DISABLED	1 2 2	0	0	
3	DISABLED	1 1 1	0	0	
4	DISABLED		0	0	

2. Select (i.e., click) any number in the **Alarm** column.
3. After **Current Unacknowledged Alarms** page opens, optionally enter a comment and then select **Acknowledge Alarm**.

Current Unacknowledged Alarms

Severity: CRITICAL Search: ... Add

<input type="checkbox"/>	Date/Time	Severity	Message
<input type="checkbox"/>	2018-12-06T16:09:10.910Z	CRITICAL	The connection status is now unreachable for testestdevice2 - 192.168.114.113 in group: 1
<input checked="" type="checkbox"/>	2018-12-06T16:07:50.750Z	CRITICAL	The connection status is now unreachable for testdevice1 - 192.168.122.121 in group: 1
<input type="checkbox"/>	2018-12-05T14:34:28.3428Z	CRITICAL	The connection status is now unreachable for 192.168.17.188 - 192.168.17.188 in group: 1

5 rows per page. First Page « 1 » Last Page 3 Total rows . Page 1 of 1.

Acknowledgement Comments (Optional):

Acknowledge Alarm Cancel

<input type="checkbox"/>	Date/Time	Severity	Message
<input checked="" type="checkbox"/>	2017-01-20T17:24:54.2454Z	CRITICAL	The connec
<input type="checkbox"/>	2017-01-19T00:06:59.659Z	CRITICAL	The connec
<input type="checkbox"/>	2017-01-17T19:06:16.616Z	CRITICAL	The connec
<input type="checkbox"/>	2017-01-17T16:33:47.3347Z	CRITICAL	The connec
<input type="checkbox"/>	2017-01-12T16:42:49.4249Z	CRITICAL	The connec

5 rows per page. First Page

Acknowledgement Comments (Optional):

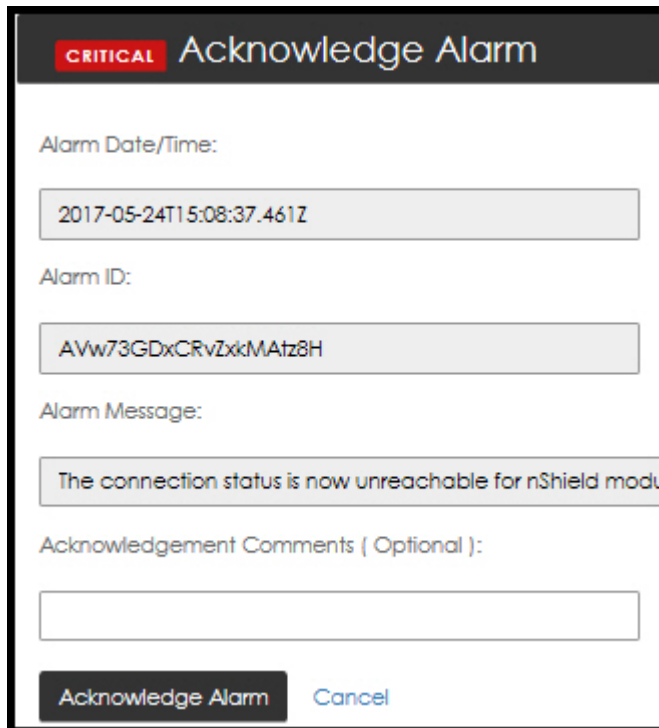
Acknowledge Alarm Cancel



Selecting multiple boxes allows you to simultaneously acknowledge multiple alarms.



If you click directly on the Alarm Severity, i.e., directly on **CRITICAL**, the **Acknowledge Alarm** page opens.



4. Enter comments (optionally) and then select **Acknowledge Alarm**.

9.3.3.2. Navigating to the Group Detail page

1. To get to the **Group Detail** page, navigate to:

View > Groups > Group List

The **Group Summary** page opens.

Group Name	payshield Utilization	payshield Host Command	payshield Overload	nshield Overload	Alarm	payshield	nshield	Client Hosts	Description
Group 1	0%	0 TPS	0%	0%	20 13 6 42	3	4	2	Unit test Group 1
Group 2	0%	0 TPS	0%	0%	15 15 5 36	1	3	1	This is Group 2
Group 3	0%	0 TPS	0%	0%	6 6 12	3	0	1	This is Group 3

2. From the **Group Name** column, select **Group <n>**.

Group Detail For : 1

Group Average
 Top 10
 Custom

Client Hosts ▶

nShield HSMs ▶

9.3.3.3. Filtering Group Detail - Group Average, Top 10, or Custom

Each window on the Group Detail page, i.e., Client Hosts, nShield HSMs, can be filtered based on Group Average, Top 10, or based on a Custom list of devices.

Example: Filtering a **Utilization Chart** based on:

Group Average, Top 10, or Custom list of devices

Group Average
 Top 10
 Custom

Client Hosts ▶

nShield HSMs ▶

Each of these views shows the average of the data collected for the interval

period selected (5 minutes, 15 minutes, etc.).



Line colors in the chart are used to designate a specific device. Click on the items in the color index, (e.g., specifically on **"MAX"**, and/or on **"Group 1"**) to toggle the display options.



nShield Monitor can provide the maximum data point that occurred in a selected interval period. The utilization chart provides a red line to show a maximum data point as well as a time stamp to show when that maximum utilization occurred.

- Select the drop down arrow on the time period bar to modify the time period being viewed.

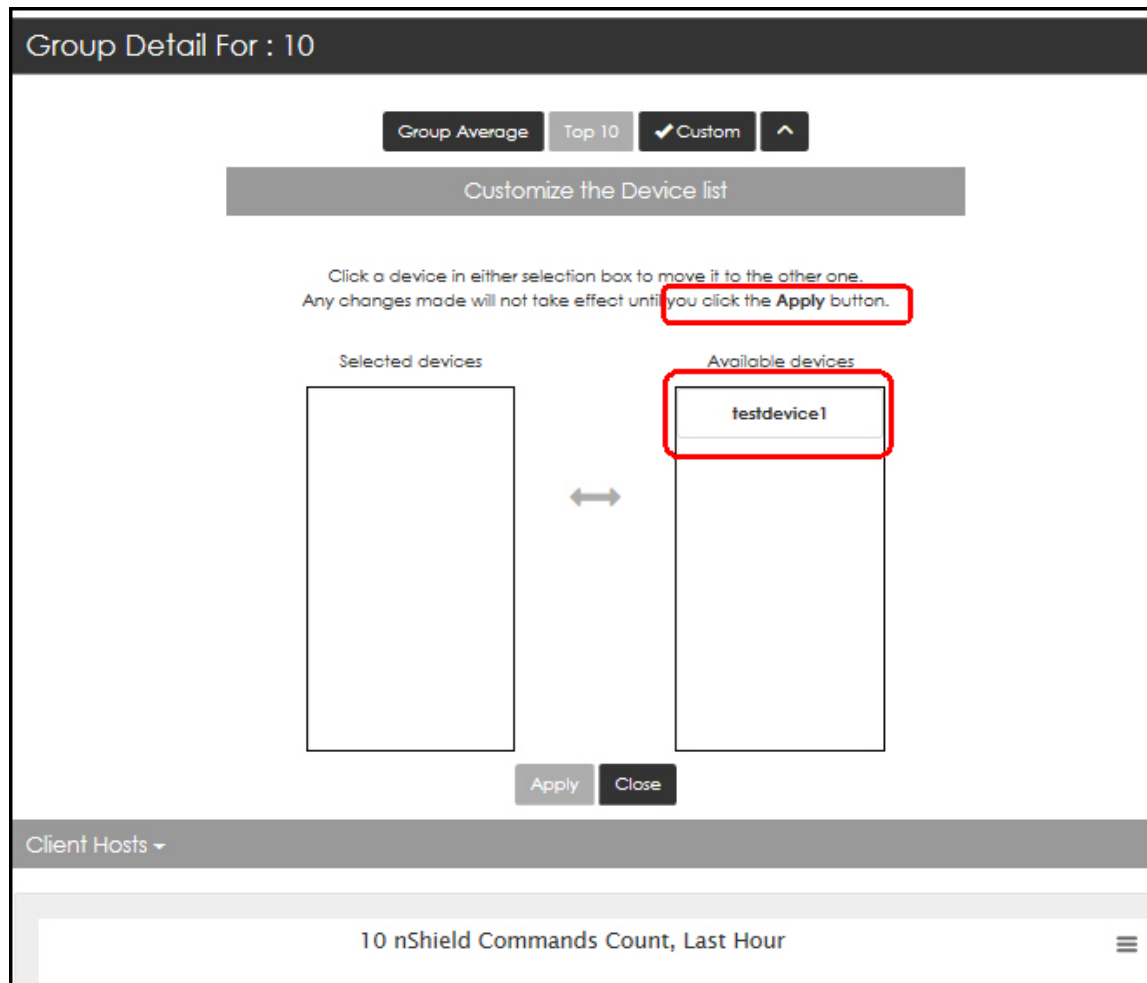


The Custom Range selections are in the UTC time zone.

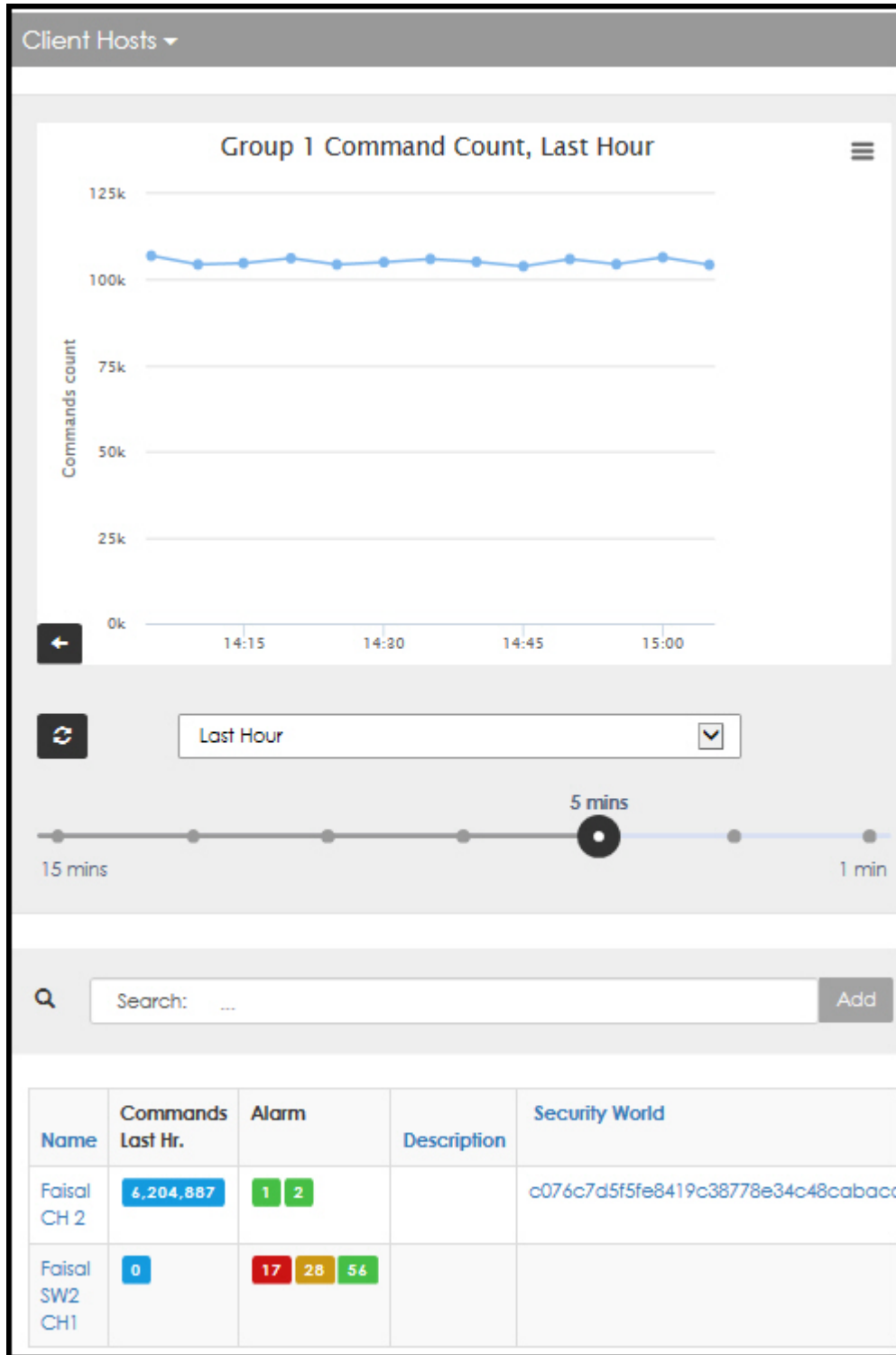
- Use the sliding mechanism to change the intervals.



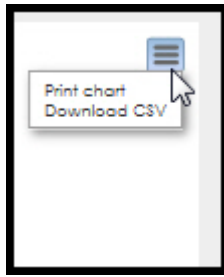
Example of **Custom**:



- Select (i.e., click on a device) in the selection box to move it from one box to the other.
- Select **Apply** to confirm the change.
- Select **Close** to return the to **Group Detail** page.
- Select the expansion arrow to open a **Group Detail** page, as needed.



i | Each graph can be printed or exported in CSV.



9.3.3.4. Group Detail page - Client Hosts

The **Client Hosts** window displays:

- **Graphed** command count based on command count per time block:



Group Detail For : 10

Group Average
Top 10
✓ Custom
^

Customize the Device list

Click a device in either selection box to move it to the other one.
 Any changes made will not take effect until you click the **Apply** button.

Selected devices

Available devices

testdevice1

Apply
Close

Client Hosts ▾

10 nShield Commands Count, Last 24 Hours ☰

↻

Last 24 Hours ▾

6 hours
5 mins

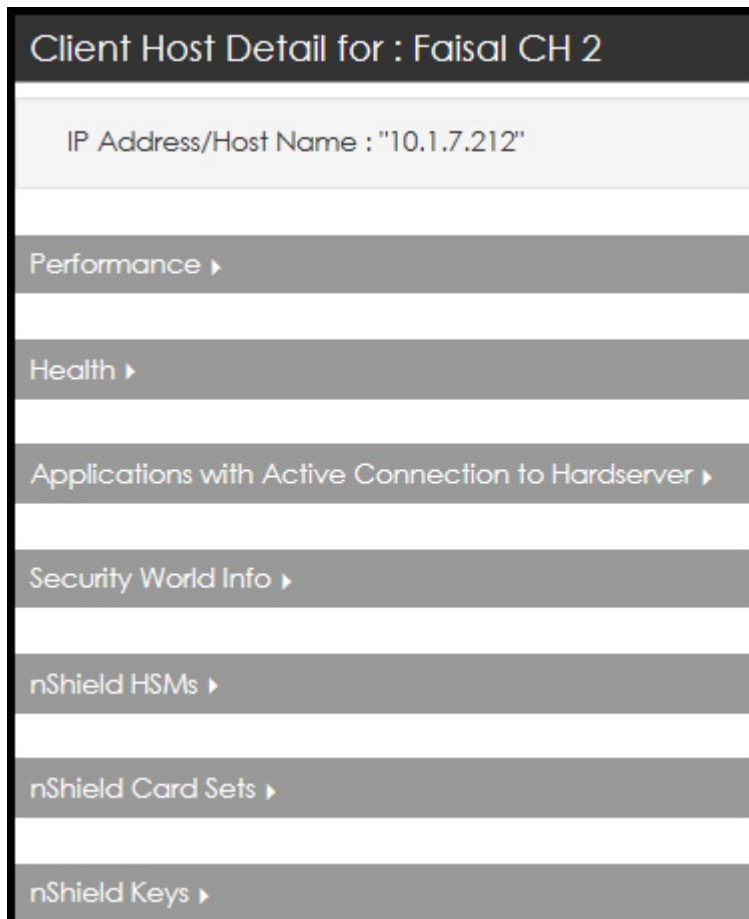
🔍 Search: Add

Name	Commands Last Hr.	Alarm	Description	Security World
testdevice1	0	3 2 3	description	

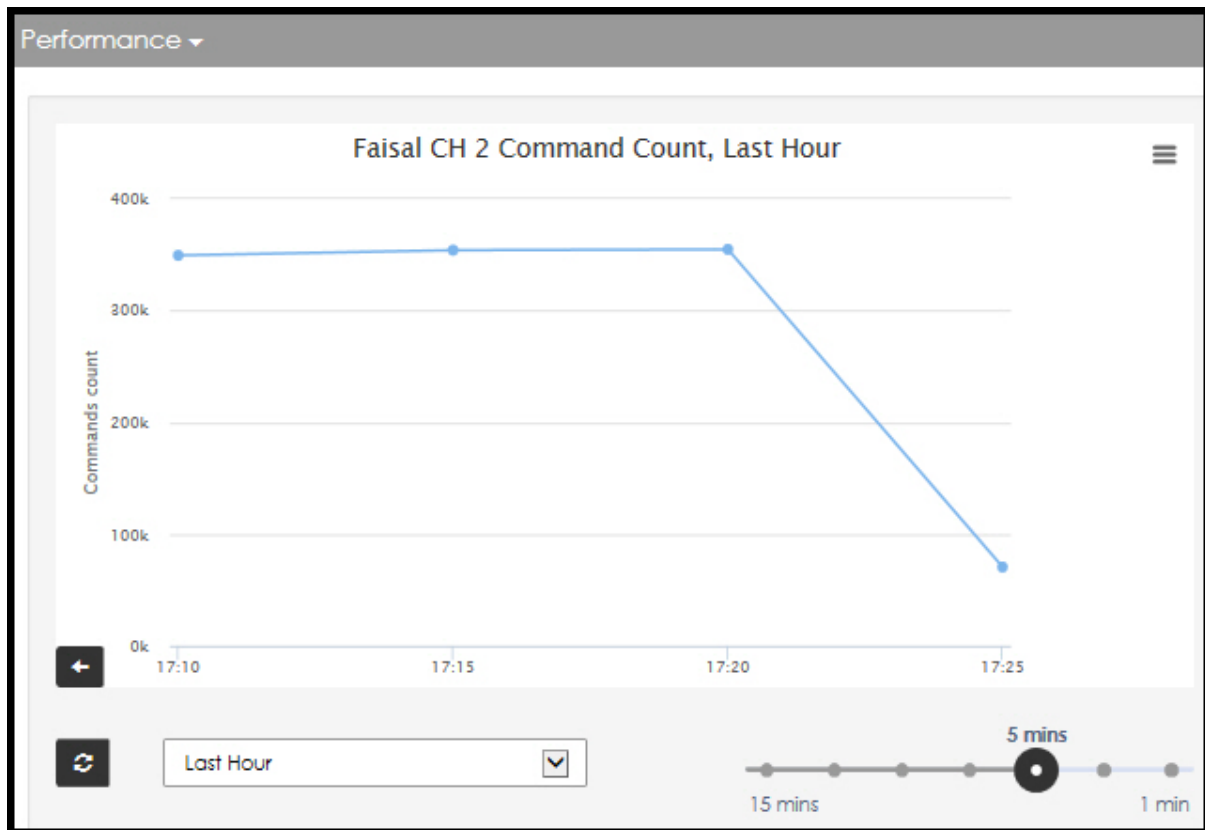
- Clicking on the device name opens the **Client Host Detail** page for that device.

9.3.3.5. Client Host Detail page - Overview

Select the expansion arrow to open the windows.



9.3.3.6. Client Host - Performance window



9.3.3.7. Client Host - Health window

Health	
Monitoring:	ENABLED
Status:	AVAIL_SNMP
Hardserver Status:	RUNNING
Number Of HSMs:	3
Applications With Active Connection To Hardserver:	7
Modules Failed:	TRUE
Hardserver Version:	2.92.1
Hardserver Port:	9004
Hardserver Uptime:	46 Days : 13 Hours : 36 Minutes : 06 Seconds

9.3.3.8. Client Host - Applications with Active Connection window

Applications with Active Connection to Hardserver ▾

Q Search: ... Add

Connection Number	Uptime	Command Count	Reply Count	Remote IP Address	Process ID	Process Name	Total Object Count
3	46 Days : 13 Hours : 36 Minutes : 06 Seconds	0	167495531	0.0.0.0	0		
4	46 Days : 13 Hours : 36 Minutes : 06 Seconds	0	0	0.0.0.0	0	[legacy]	
5	46 Days : 13 Hours : 36 Minutes : 06 Seconds	0	0	0.0.0.0	0	[legacy]	

- Click on the blue columns to reverse the sort order, based on preference.
- Select (i.e., click on) a specific **Connection Number** to open a the connection's **Application Details** page.

Application Details for :

Application Connection Number : "3"

Health ▾

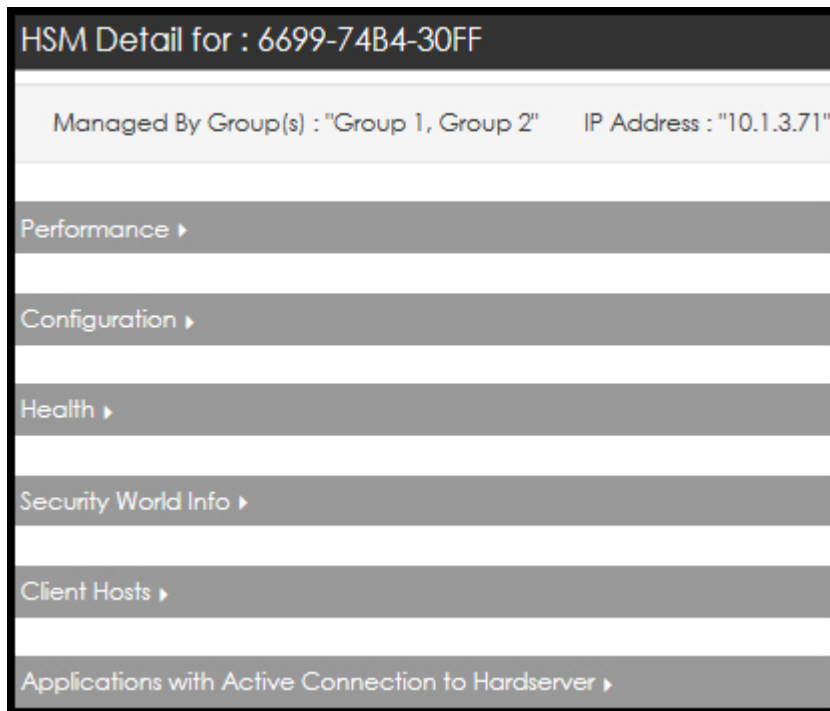
Connection Number:	0 Days : 00 Hours : 00 Minutes : 03 Seconds
Uptime:	4024447
Command Count:	0
Reply Count:	167524721
Remote IP Address:	0.0.0.0
Process ID:	0
Process Name:	
Total Object Count:	

nShields ▾

Q Search: ...

Serial	Type	Mode	Monitoring	Module Object Count
6699-7484-30FF	CONNECT	OPERATIONAL	ENABLED	0
6F99-748F-429B	CONNECT	OPERATIONAL	ENABLED	0

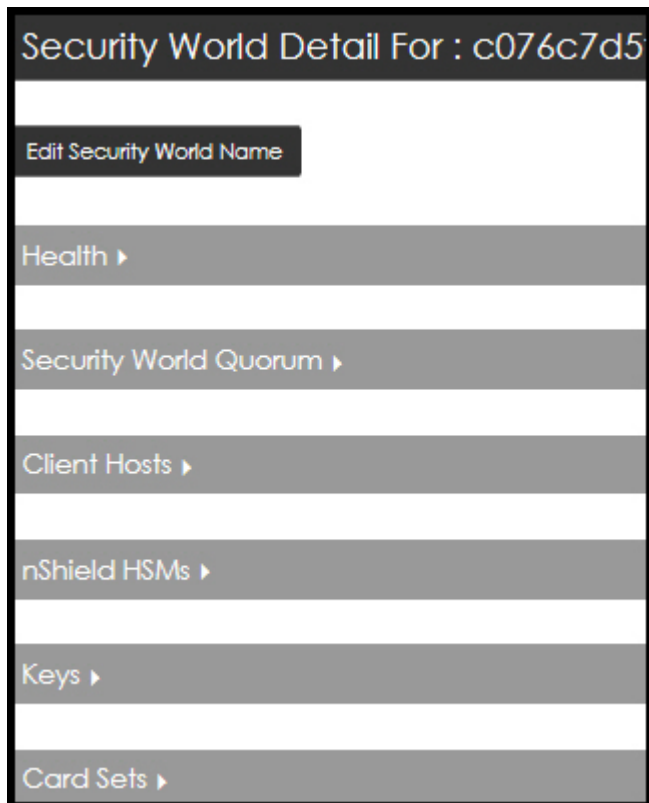
- Select a specific Serial number to open the **HSM Detail** page.



9.3.3.9. Client Host - Security World Info window

Security World Info ▼	
Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World state:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

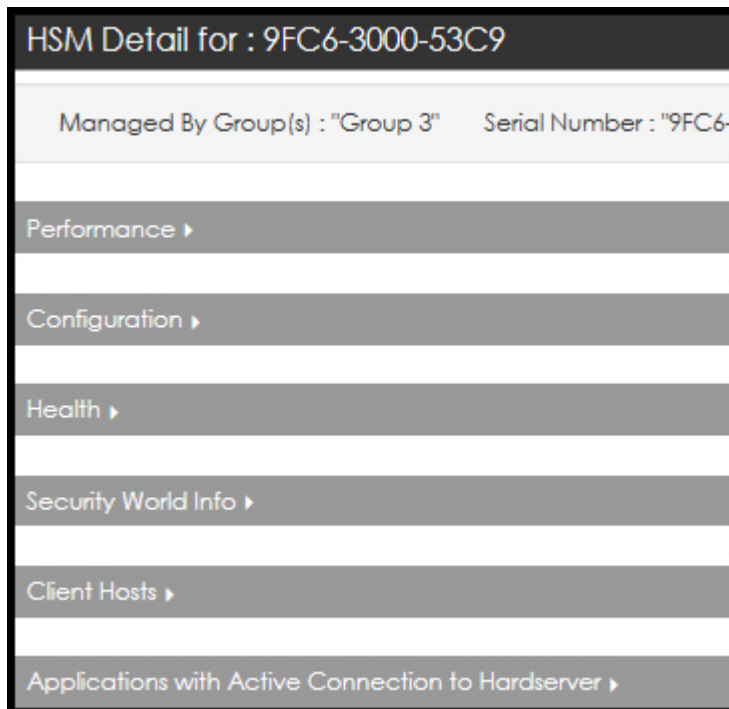
- Select the Security World identifier to open the **Security World Detail** page.



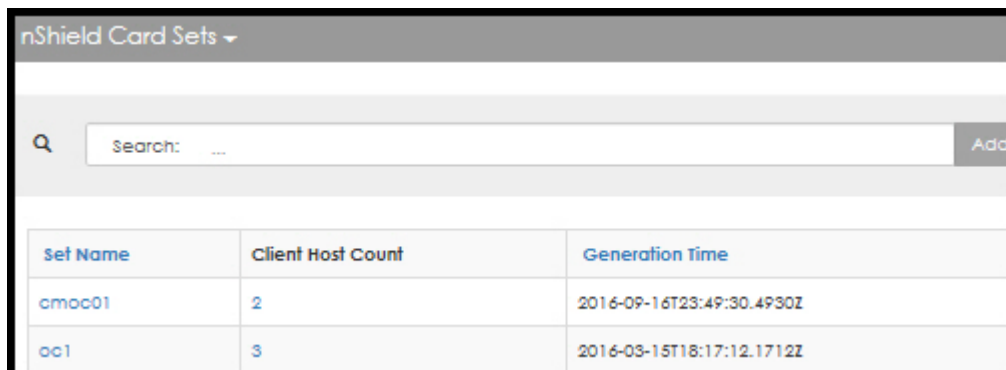
9.3.3.10. Client Host - nShield HSMs window

Serial No.	Type	Mode	Commands Last Hr.
6699-7484-30FF	CONNECT	OPERATIONAL	6028
6F99-748F-429B	CONNECT	OPERATIONAL	6025

- Select a specific Serial Number to open the **HSM Detail** page.



9.3.3.11. Client Host - nShield Card Sets window



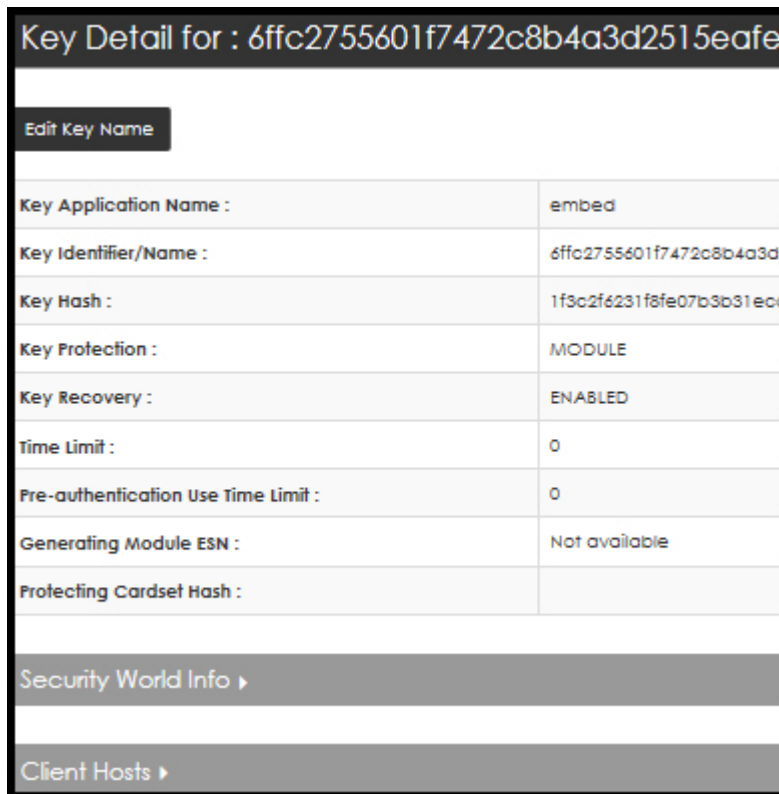
- Select a specific Set Name to open the **Card Set Detail** page.

Card Set Detail for : ffoc1	
Quorum Count (k):	1
Total Number Of Cards(N):	2
Timeout :	0
Generation Time :	2016-08-24T19:08:11.811Z
Security World Info ▶	
nShield Keys Protected By This Card Set ▶	
Client Hosts ▶	

9.3.3.12. Client Host - nShield Keys window

nShield Keys ▼			
<input type="text" value="search: ..."/> Add			
Key Identifier/Name	Key Hash	Key Application Name	Client Hosts
6ffc2755601f7472c8b4a3d2515eafe53c964efd	1f3c2f6231f8fe07b3b31ecd1456651b88eca2d2	embed	3
8fd31935920b3b47abe145e7ecdbed87dba7fe55	429ce182a09a5b7cb088e64f9551ed61f181e317	embed	3
ff1	7386cc17bca937d59df56ff74f88207c1bd8edff	simple	3
ff2	babfafa419715482c298d8238456b00749a8ddee	simple	3

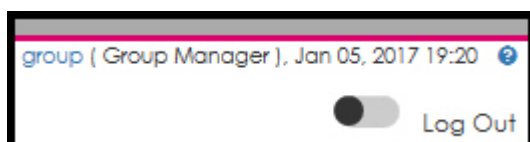
- Select a specific Key Identifier/Name to open the **Key Detail** page.

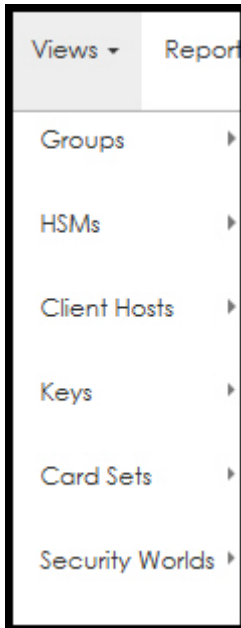


9.4. Additional Views available to the Group Manager

The View drop down menu provides several additional options that are not offered to the Administrator, i.e.,

- Groups
- HSMs
- Client Hosts
- Keys
- Card Sets
- Security Worlds

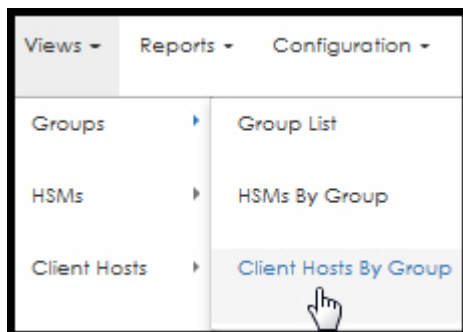




9.4.1. Groups

1. Navigate to:

View > Groups > Client Hosts By Group



2. Select **Client Hosts By Groups**.

The **Client Hosts By Groups** page opens.

Client Hosts By Group

Search: ...

Group 1 ▾ There are 3 client host(s) in this group.

Search: ...

▲ Name	Monitoring	Hardserver Status	Commands Last Hr.	HSMs	Alarm	Last Update	Location	Security World
Faisal CH 2	ENABLED	RUNNING	13377	3	1	Current		c076c7a5f5fe84
Faisal SW2 CH1	ENABLED	RUNNING	0	2	4 6	Current		c076c7a5f5fe84
Faisal SW2 CH2	UNREACHABLE	NOT_RUNNING	0		2 2			

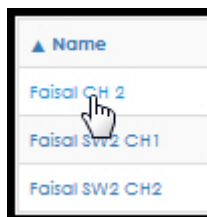
<

5 rows per page. First Page « 1 » Last Page 3 Total rows

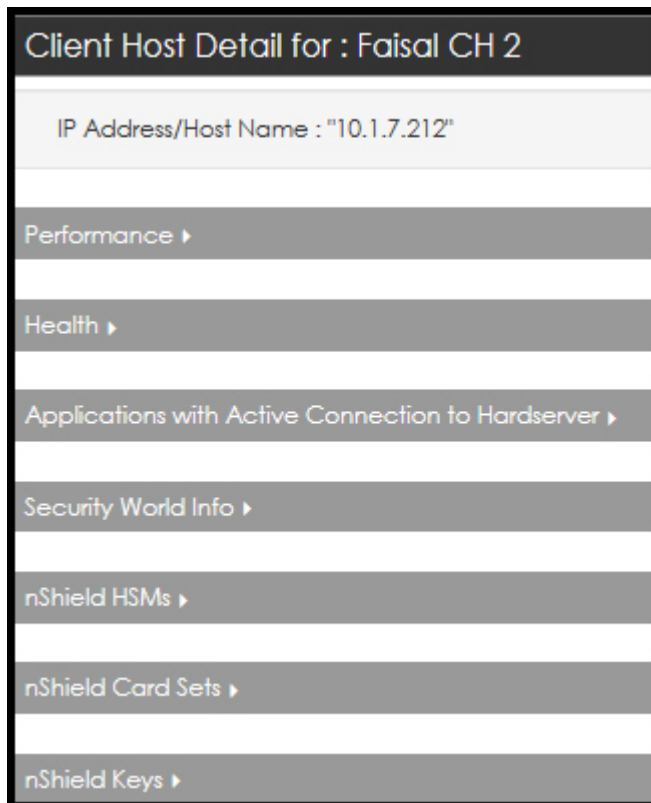
Group 2 ▾ There are 2 client host(s) in this group.

The **Client Hosts By Group** page contains three navigation points. Selecting any one of the following opens a new page;

- A specific **device name**



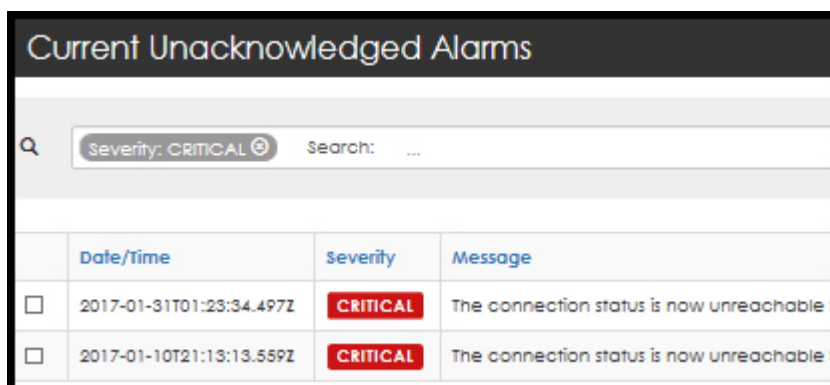
The **Client Host Detail** page opens.



- A specific **Alarm**



The **Current Unacknowledged Alarms** page opens.



- A specific Security World



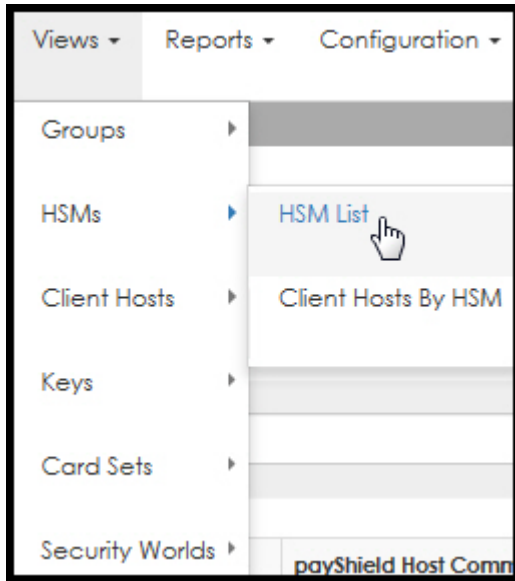
The **Security World Detail** page opens.



9.4.2. View > HSMs > HSM List

1. Navigate to:

Views > HSMs > HSM List



2. Select **HSM List**.

The **HSMs Summary** page opens.

9.4.2.1. HSM Summary Page



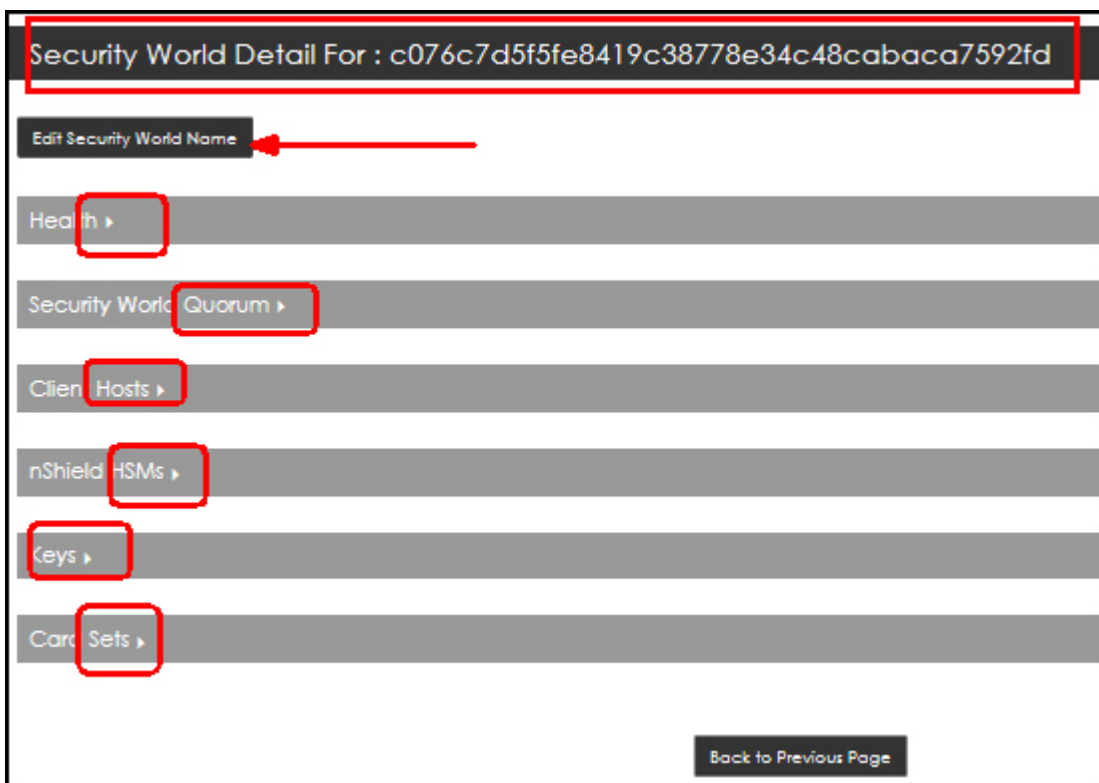
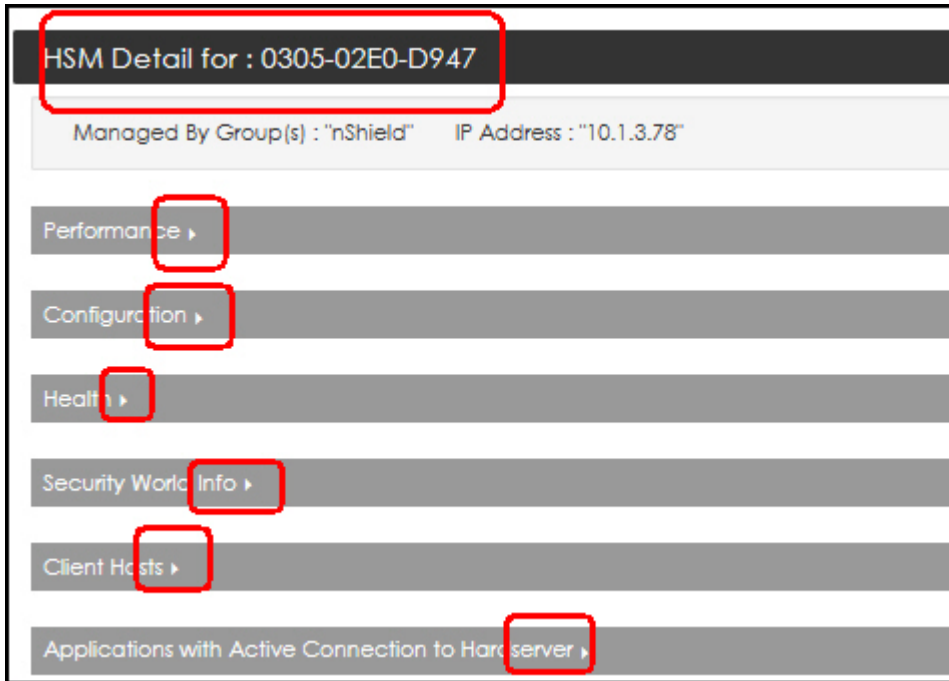
With the HSM Summary page open, you can toggle between views by selecting **Client Hosts by HSM**. See the upper right hand corner of the screen.

A screenshot of the 'HSM Summary' page. At the top right, there are two view toggle buttons: 'HSM List' (selected) and 'Client Hosts By HSM'. Below the header is a search bar. The main content is a table titled 'nShield HSMs'. The table has columns for Serial No., Type, Mode, Monitoring, Objects, Commands Last Hr., Alarms, Security World, Client Host (s), and Last Update. Red boxes highlight the 'Serial No.', 'Type', 'Mode', 'Objects', 'Security World', and 'Last Update' columns. Red arrows point from the 'Serial No.' and 'Security World' columns to the 'Client Host (s)' column.

Serial No.	Type	Mode	Monitoring	Objects	Commands Last Hr.	Alarms	Security World	Client Host (s)	Last Update
0305-02E0-D947	CONNECT XC	FAILED	ENABLED	0	0	1	c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current
2805-02E0-D947	CONNECT XC	FAILED	ENABLED	0	0	1 1	c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current
6699-74B4-30FF	CONNECT	OPERATIONAL	ENABLED	14	3811	21 4 6	c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current
6F99-74BF-429B	CONNECT	OPERATIONAL	ENABLED	14	3817	9 3 6	c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current
856A-81C9-73F2	CONNECT	OPERATIONAL	ENABLED	6	3797	1 1	c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current

Colored font indicates that filtering is available. Additionally, you can select individual devices to open new windows.

Examples:



9.4.2.2. Navigation Example - nShield HSMs window

Serial No.	Type	Mode	Monitoring	▲ Objects	Commands Last Hr.	Alarms	Security World	Client Host (s)	Last Update
F48C-82C8-3E1R	CONNECT	OPERATIONAL	ENABLED	5	6315	10	c076c7d5f5fe8419c38778e34c48cabaca7592fd	2	Current
9FC6-3000-53C9	SOLO	OPERATIONAL	ENABLED	5	4391		c076c7d5f5fe8419c38778e34c48cabaca7592fd	1	Current

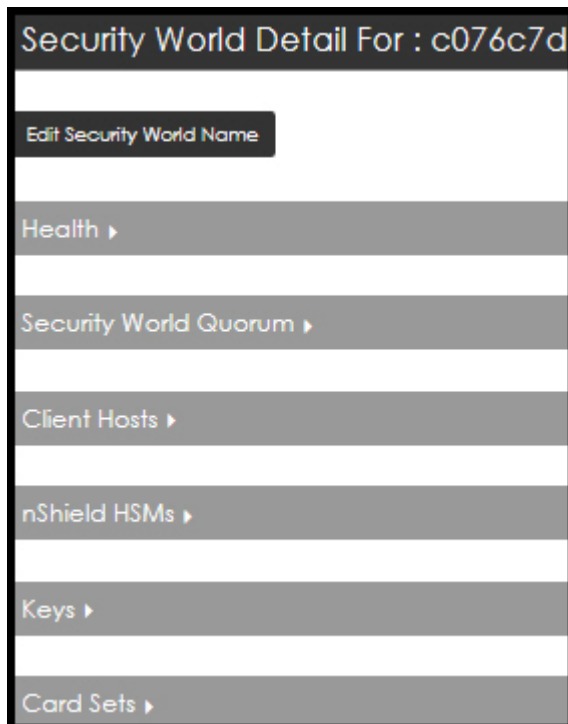


Blue icons and blue text indicate action available, e.g., selecting a specific Security World, opens the **Security World Summary** page.

Examples follow:



- Select the **Security World** identifier. The **Security World Detail** page opens.



- Select **Edit Security World Name** to edit the name:

- Enter the new name and select **Save**.



Select **Clear** to close this dialog box without saving an edit.

- **Health** window

Health ▾	
Generation Time:	2016-01-29T00:00:00.000Z
Generating Module ESN:	B56A-81C9-73F2
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

- **Security World Quorum** window

Security World Quorum ▾	
KNSO Quorum	1
Total Number Of Admin Cards	3
Module Reprogramming (KM) Quorum	1
Recovery (KR) Quorum	1
Passphrase Recovery (KP) Quorum	1
NVRAM Authorization (KNV) Quorum	1
RTC Authorization (KRTC) Quorum	1
SEE Debugging Authorization (KDSEE) Quorum	1
Foreign-Token Authorization (KFTP) Quorum	1

- **Client Hosts** window

Client Hosts ▾

Search: ... Add

Name	Hardserver Status	Commands Last Hr.
Faisal CH 1	RUNNING	8726
Faisal CH 2	RUNNING	13083
Faisal SW2 CH1	RUNNING	11505

- Select the client host name to open the **Client Host Detail** page.

Client Host Detail for : Faisal CH 1

IP Address/Host Name : "10.1.7.154"

Performance ▶

Health ▶

Applications with Active Connection to Hardserver ▶

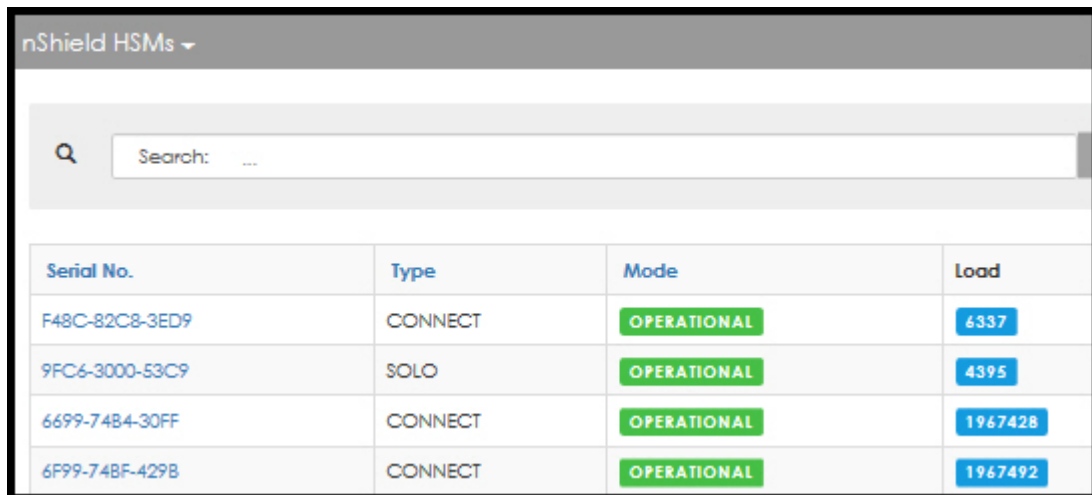
Security World Info ▶

nShield HSMs ▶

nShield Card Sets ▶

nShield Keys ▶

- **nShield HSMs window**

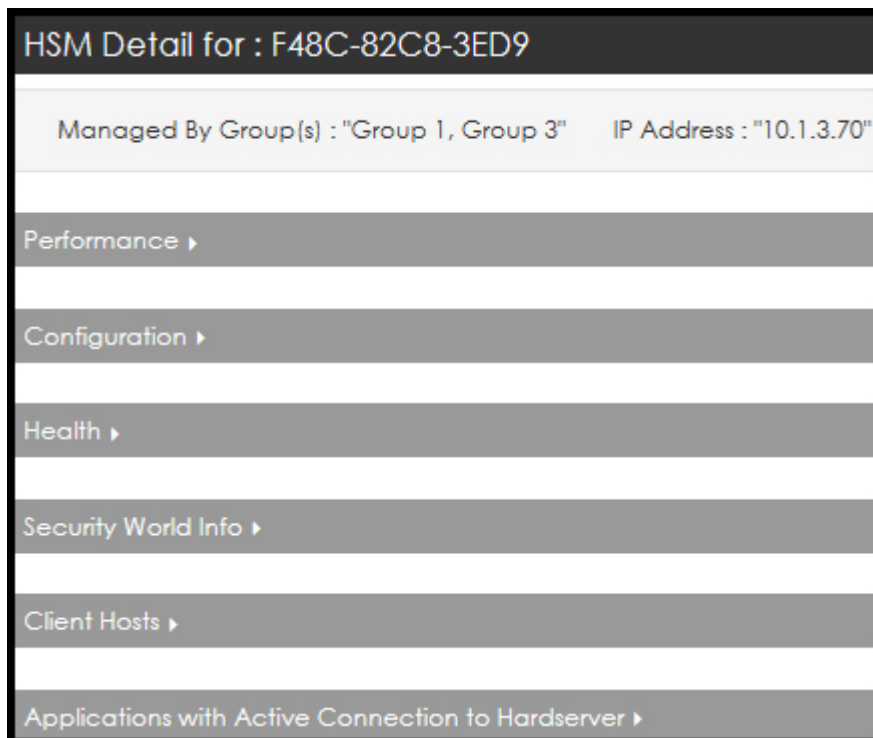


nShield HSMs

Search: ...

Serial No.	Type	Mode	Load
F48C-82C8-3ED9	CONNECT	OPERATIONAL	6337
9FC6-3000-53C9	SOLO	OPERATIONAL	4395
6699-74B4-30FF	CONNECT	OPERATIONAL	1967428
6F99-74BF-429B	CONNECT	OPERATIONAL	1967492

- Select a Serial No. (e.g., click **F48C-82C8-3ED9**) to open the **HSM Detail** page.



HSM Detail for : F48C-82C8-3ED9

Managed By Group(s) : "Group 1, Group 3" IP Address : "10.1.3.70"

Performance ▶

Configuration ▶

Health ▶

Security World Info ▶

Client Hosts ▶

Applications with Active Connection to Hardserver ▶

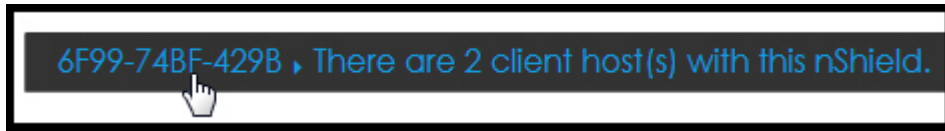
9.4.3. View > HSMs > Client Hosts by HSM

1. Navigate to:

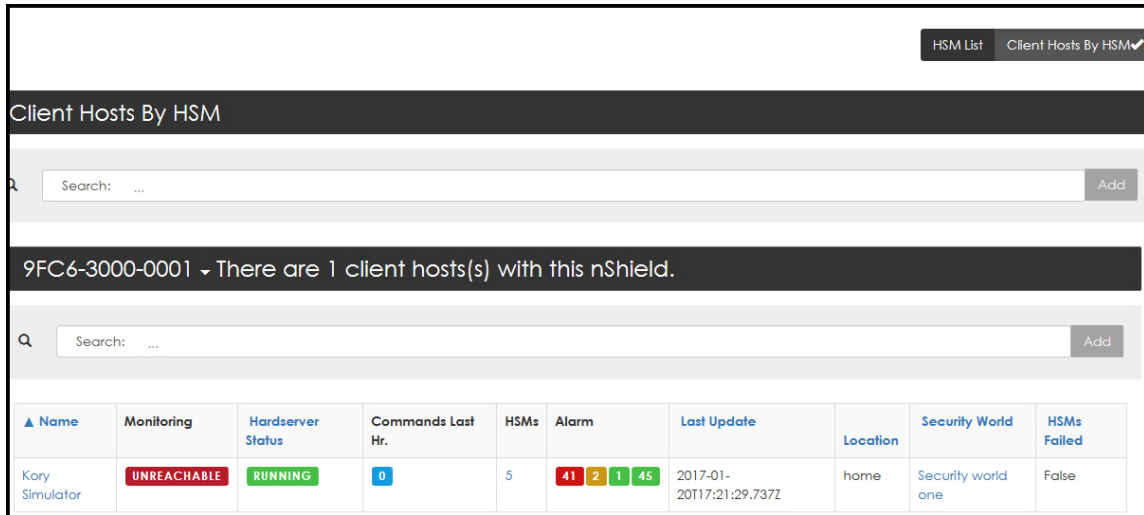
Views > HSMs > Client Hosts by HSM

The **Client Host by HSM** page opens.

2. When hovering over the text turns the text blue, click to expand.



A details window opens:



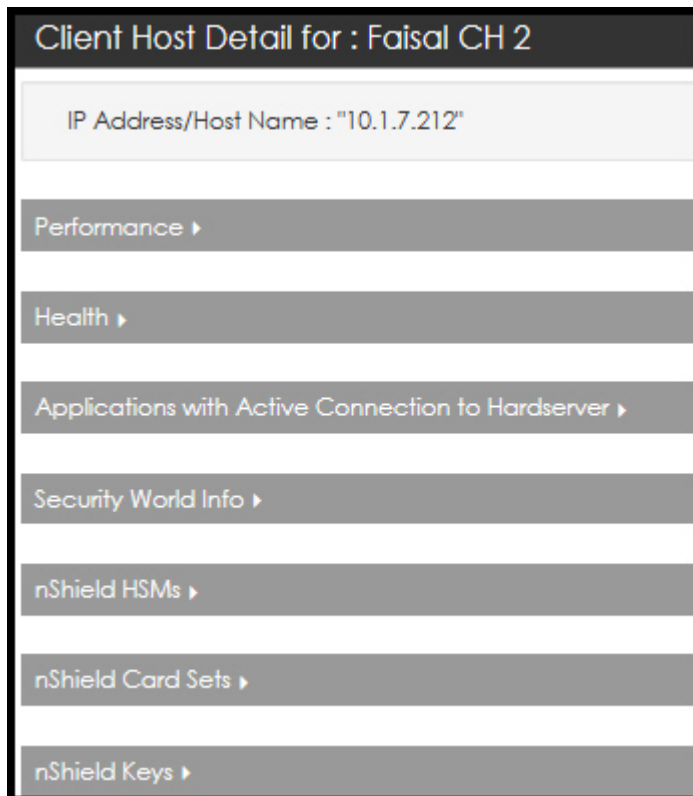
This detail window has **4 navigation links** as summarized in the following table.

Links on the Details window

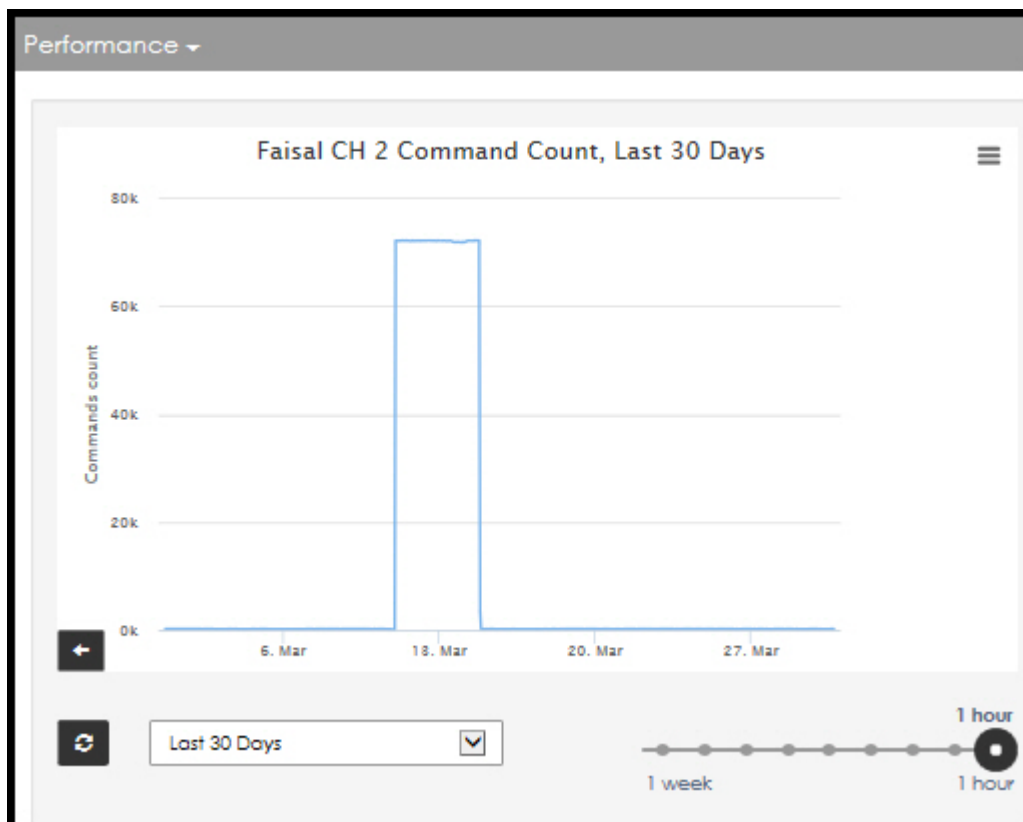
Clicking	Opens this page	Notes
Name	See Client Host Detail page	
HSMs count	nShield HSMs page. This page lists all the HSMs by Serial Number	The nShield HSMs page also contains a link under the Security World column. Clicking on the Security World identifier opens the Security World Detail page .
Alarm (hover over the colored alarm total box in the Alarm column, then click.)	Current Unacknowledged Alarm	Select the box associated with the alarm to open the Acknowledge Alarm window.
Security World (name or HashKNSO)	Security World Detail page.	

9.4.3.1. Client Host Detail page

Select the expansion arrows to open additional windows.



Performance window:



Health window:

Health ▾	
Monitoring:	ENABLED
Status:	AVAIL_SNMP
Hardserver Status:	RUNNING
Number Of HSMs:	3
Applications With Active Connection To Hardserver:	7
Modules Failed:	TRUE
Hardserver Version:	2.92.1
Hardserver Port:	9004
Hardserver Uptime:	48 Days : 17 Hours : 49 Minutes : 57 Seconds

Applications with Active Connection to Hardserver window:

Applications with Active Connection to Hardserver ▾							
<input type="text" value="Search: ..."/> Add							
▲ Connection Number	Uptime	Command Count	Reply Count	Remote IP Address	Process ID	Process Name	Total Object Count
3	48 Days : 17 Hours : 49 Minutes : 57 Seconds	0	173857643	0.0.0.0	0		Not available
4	48 Days : 17 Hours : 49 Minutes : 57 Seconds	0	0	0.0.0.0	0	[legacy]	Not available
5	48 Days : 17 Hours : 49 Minutes : 57 Seconds	0	0	0.0.0.0	0	[legacy]	Not available
6	48 Days : 17 Hours : 49 Minutes : 57 Seconds	0	0	0.0.0.0	0	[legacy]	Not available
72561	36 Days : 23 Hours : 27 Minutes : 57 Seconds	20478472	20478471	0.0.0.0	0		Not available

Security World Info window:

Security World Info	
Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128



Clicking on the Security World identifier (e.g, c076cd...), opens the **Security World Detail** page.

nShield HSMs window:

nShield HSMs			
Search: ...			
Serial No.	Type	Mode	Commands Last Hr.
6699-74B4-30FF	CONNECT	OPERATIONAL	6693
6F99-74BF-429B	CONNECT	OPERATIONAL	6664
F48C-82C8-3ED9	CONNECT	OPERATIONAL	6195

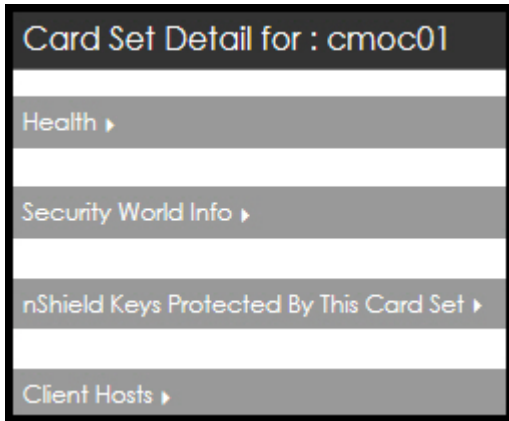
nShield Card Sets window:

nShield Card Sets		
Search: ...		
Set Name	Client Host Count	Generation Time
cmoc01	2	2016-09-16T23:49:30.4930Z
oc1	3	2016-03-15T18:17:12.1712Z
oc2	3	2016-03-15T23:07:15.715Z



Selecting a set name, opens the **Card Set Detail** page.

Card Set Detail page:



Select the expansion arrows to open additional windows.

nShield Keys window:

nShield Keys ▾

Search: ... Add

Key Identifier/Name	Key Hash	Key Application Name	Client Hosts
6ffc2755601f7472c8b4a3d2515eafe53c964efd	1f3c2f6231f8fe07b3b31ecd1456651b88eca2d2	embed	3
8fa31935920b3b47abe145e7ecdbed87aba7fe55	429ce182a09a5b7cb088e64f9551ed61f181e317	embed	3
ff1	7386cc17bca937d59af56ff74f88207c1bd8edff	simple	3
ff2	babfafa419715482c298d8238456b00749a8ddee	simple	3
ff3	16d84dab6309081da9aa374c0544b832cb19c8a8	simple	3

This window has two navigational links.

Selecting the Key Identifier opens the **Key Detail** page:



Selecting the Client Hosts number opens the **Client Hosts By Key** page.

Client Hosts By Key

Q Name: 6ffc2755601f7472c8b4a3d2515eafe53c964efd © Search: ... Add

6ffc2755601f7472c8b4a3d2515eafe53c964efd ▾ There are 3 client host(s) with this key.

Q Search: ... Add

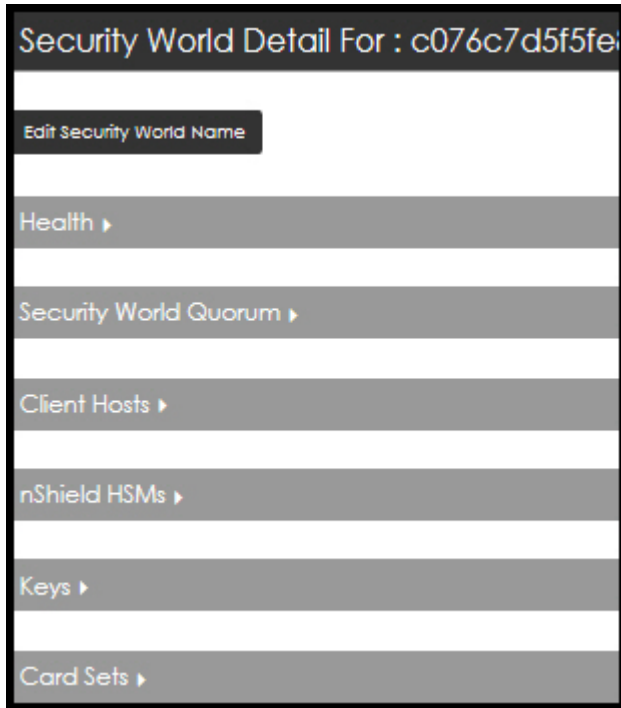
▲ Name	Monitoring	Hardserver Status	Commands Last Hr.	HSMs	Alarm	Last Update	Location	Security World
Faisal CH 1	ENABLED	RUNNING	8729	2	2	Current		c076c7d5f5fe8419c38778e3...
Faisal CH 2	ENABLED	RUNNING	13749	3	3 5	Current		c076c7d5f5fe8419c38778e3...
Faisal SW2 CH1	ENABLED	RUNNING	3867232	2	1158 1184	Current		c076c7d5f5fe8419c38778e3...

9.4.3.2. Navigating to the Security World Detail page

1. Select a **Security World** name.



Security World Detail page opens.



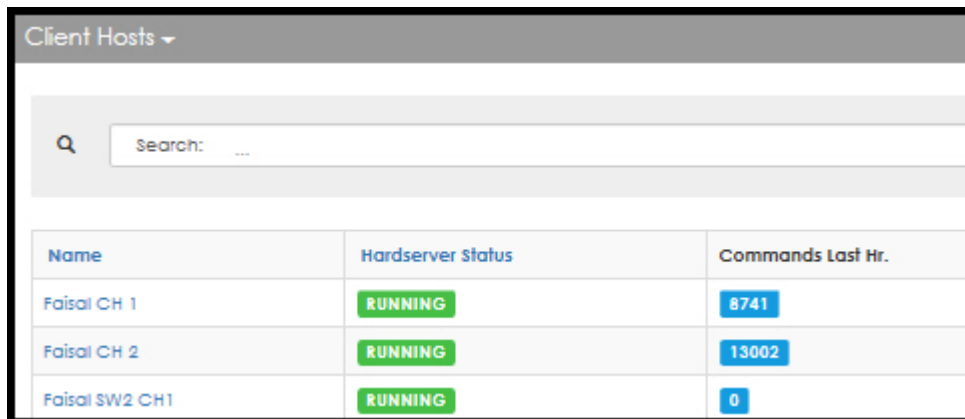
2. Select the **Health** expansion arrow.

Health	
Generation Time:	2016-01-29T00:00:00.00Z
Generating Module ESN:	B56A-81C9-73F2
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

3. Select the **Security World Quorum** expansion arrow.

Security World Quorum	
KNSO Quorum	1
Total Number Of Admin Cards	3
Module Reprogramming (KM) Quorum	1
Recovery (KR) Quorum	1
Passphrase Recovery (KP) Quorum	1
NVRAM Authorization (KNV) Quorum	1
RTC Authorization (KRTC) Quorum	1
SEE Debugging Authorization (KDSEE) Quorum	1
Foreign-Token Authorization (KFTP) Quorum	1

4. Select **Client Hosts**

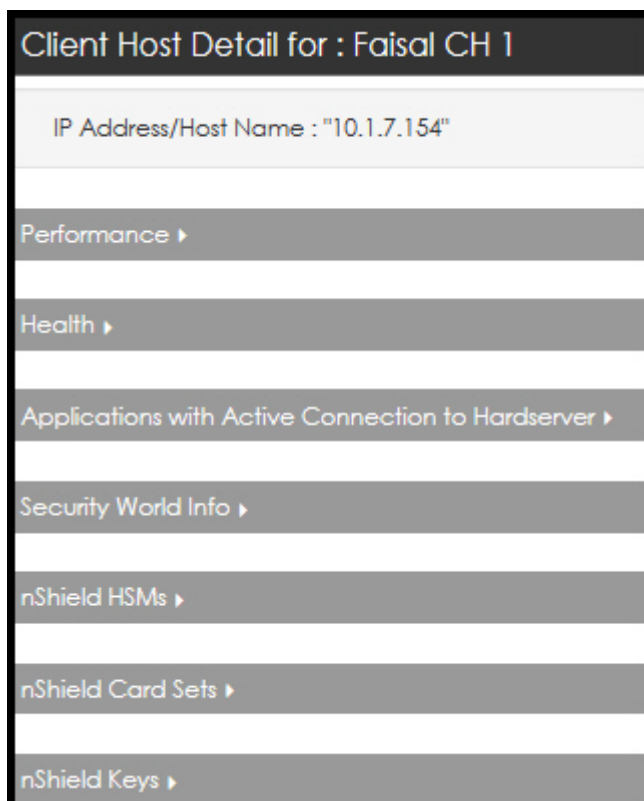


Name	Hardserver Status	Commands Last Hr.
Faisal CH 1	RUNNING	8741
Faisal CH 2	RUNNING	13002
Faisal SW2 CH1	RUNNING	0

The **Client Hosts** window has one navigational link.

5. Select a name from the **Name** column (e.g., click on **Faisal CH 1**)

The **Client Host Detail** page opens:



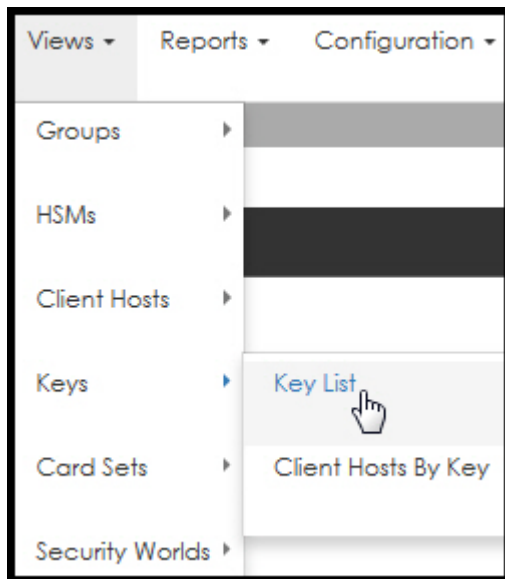
Client Host Detail for : Faisal CH 1	
IP Address/Host Name : "10.1.7.154"	
Performance ▶	
Health ▶	
Applications with Active Connection to Hardserver ▶	
Security World Info ▶	
nShield HSMs ▶	
nShield Card Sets ▶	
nShield Keys ▶	

9.4.4. View > Keys

9.4.4.1. Key > Key List

1. Navigate to:

Views > Keys



2. Select **Key List**.

The **Key Summary** page opens.

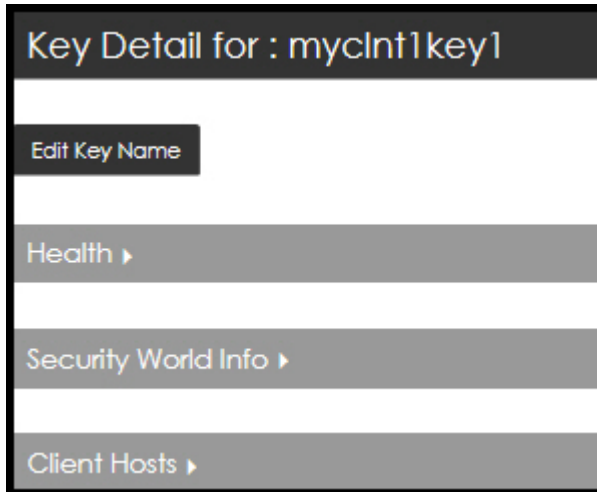
 A screenshot of the 'Key Summary' page. At the top, there is a search bar with a magnifying glass icon on the left and an 'Add' button on the right. Below the search bar is a table with four columns: 'Key Name/Identifier', 'Key Hash', 'Key Application Name', and 'Client Hosts'. The table contains five rows of data.

Key Name/Identifier	Key Hash	Key Application Name	Client Hosts
myclnt1key1	fb008ee80db38ba3c6f998a5deccc229bd4bdb10	simple	3
training	fa0236587eec411e4c04f6f6a02b859217746e6e	simple	3
nirav	e37802af9a2e95ceef5dfabb1ded1f0533c9ff5a	simple	3
ffsimpleffoc5	e3560ba57b1a1d61dc3070dd993968f9d9ba7a5e	simple	1
ffkeysimpleaug242016	cc13803c17b133fc5bcf83a1992399ae2619ed86	simple	1

The **Key Summary** page has two navigation links:

- Key Name/Identifier
- Client Hosts

3. Select a **Key Name** to open the **Key Detail** for page.



Should you need to Edit the Key Name, Select **Edit Key Name**, rename the key and then select **Save**.

4. Select the expansion arrows to open the windows.



Blue font indicates that the text is a link. Click on the blue text to drill deeper (e.g., click on Faisal CH 1 to open the Client Host Detail for: Faisal CH1 page.)

Health:

Health ▾	
Key Application Name :	simple
Key Identifier :	mycInt1key1
Key Hash :	fb008ee80db38ba3c6f998a5deccc229bd4bdb10
Key Protection :	MODULE
Key Recovery :	ENABLED
Time Limit :	0
Pre-authentication Use Time Limit :	0
Generating Module ESN :	Not available
Protecting Cardset Hash :	

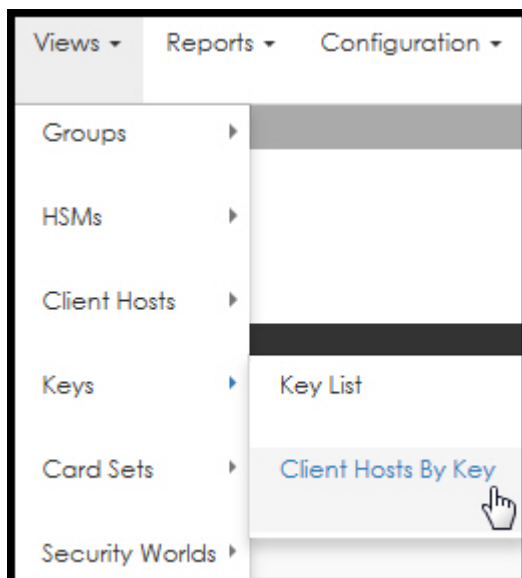
Security World Info:

Security World Info	
Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

Client Hosts:

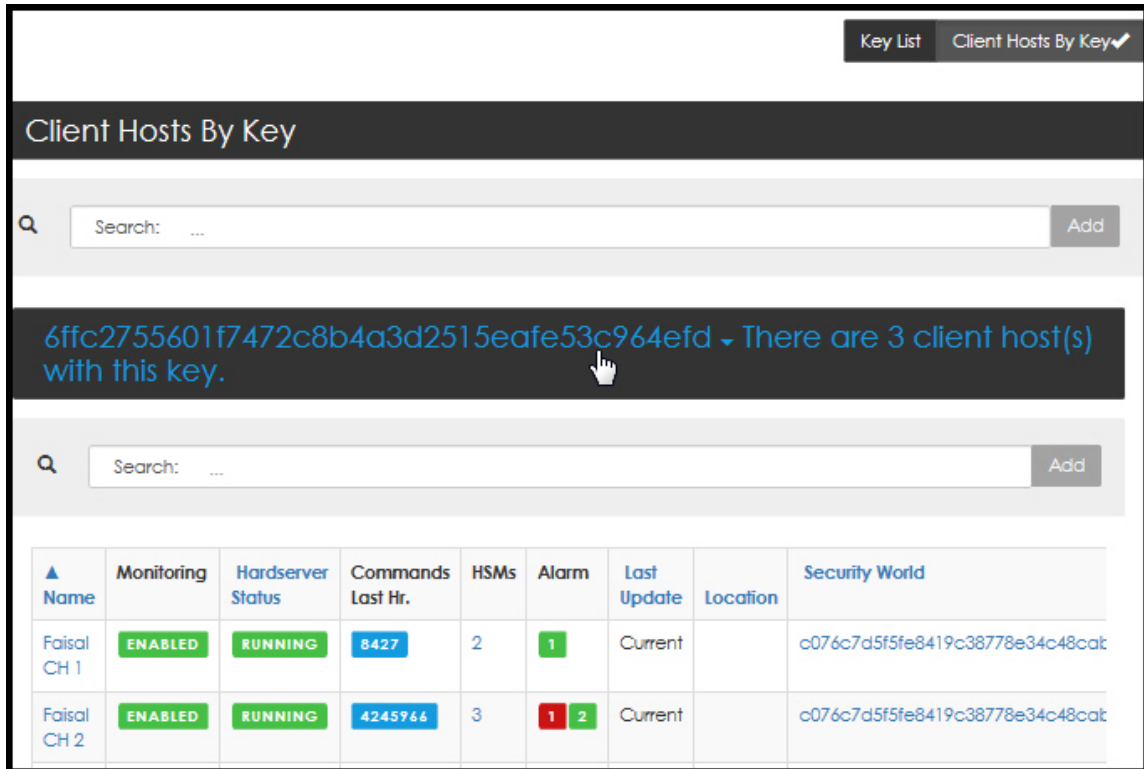
Client Hosts		
<input type="text" value="Search: ..."/>		
Name	Hardserver Status	Command Last Hr.
Faisal CH 1	RUNNING	8448
Faisal CH 2	RUNNING	4248015
Faisal SW2 CH1	RUNNING	1305886

9.4.4.2. Keys > Client Hosts By Key

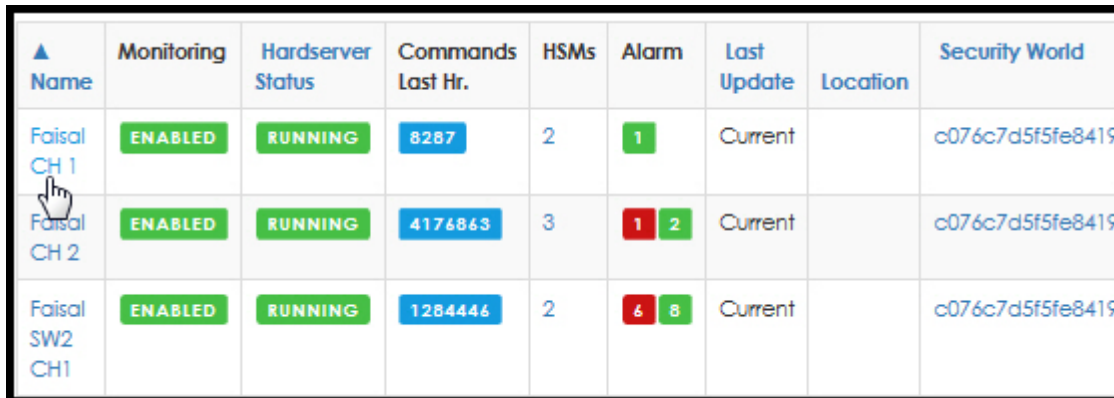


1. Select **Client Hosts By Key**.

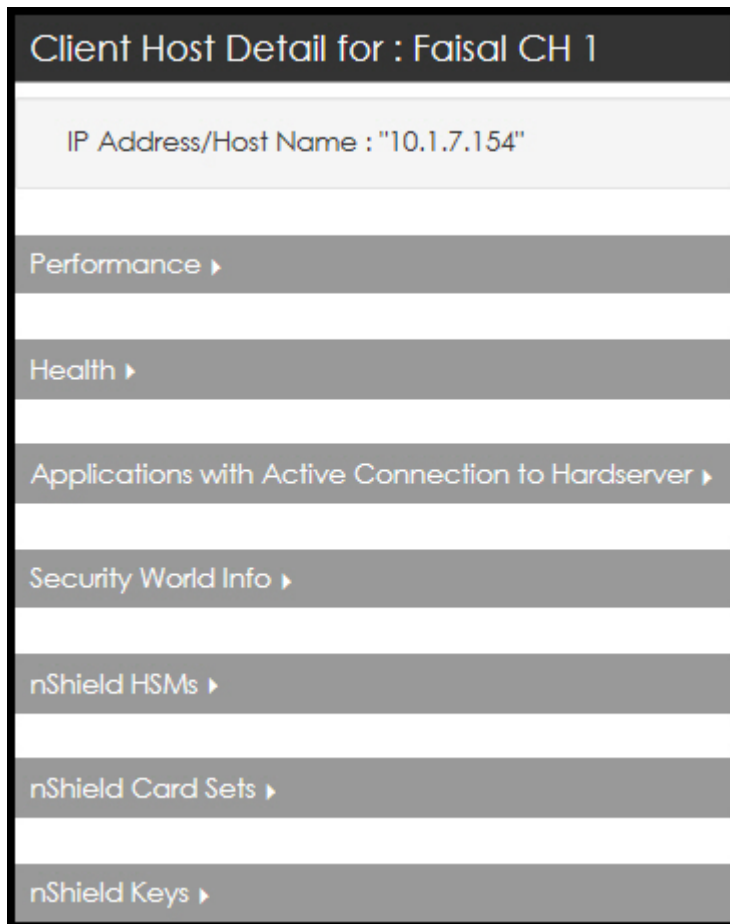
The **Client Hosts By Key** page opens.



2. When hovering over the text turns the text blue, click to expand.
3. Select a device.

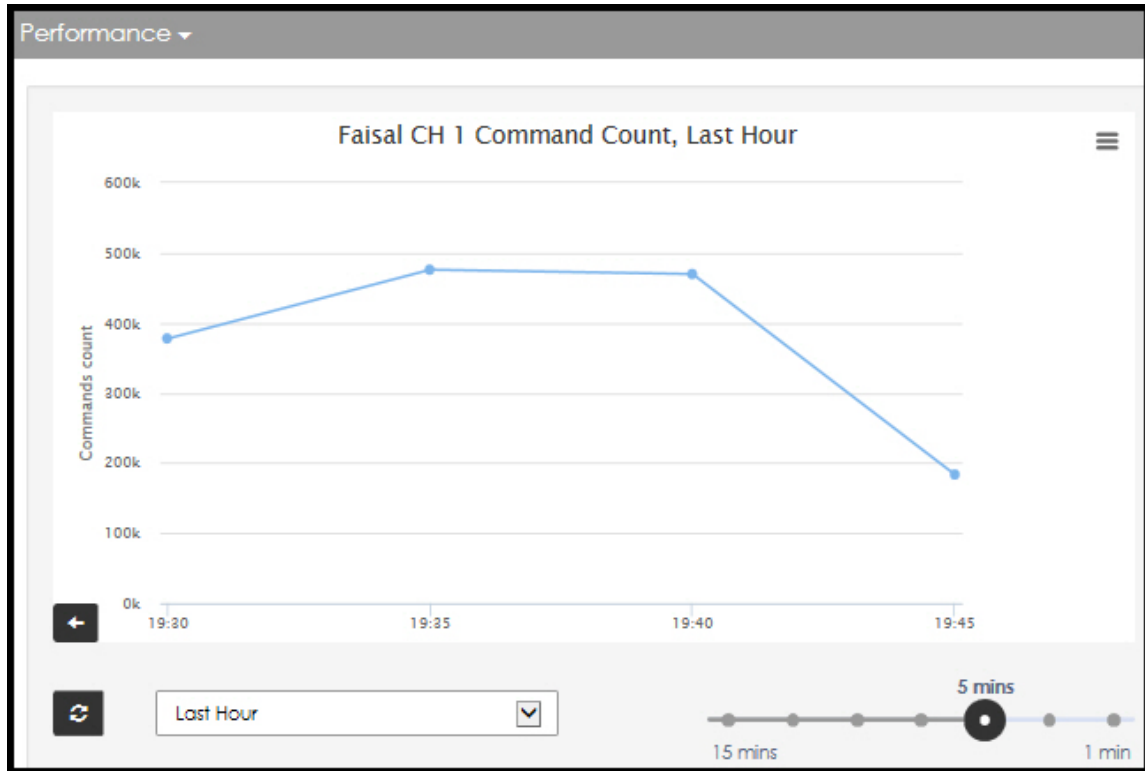


The **Client Host Detail** page opens.



4. Select the expansion arrows to open the windows.

Performance:



Health:

Health	
Monitoring:	ENABLED
Status:	AVAIL_SNMP
Hardserver Status:	RUNNING
Number Of HSMs:	2
Applications With Active Connection To Hardserver:	5
Modules Failed:	TRUE
Hardserver Version:	2.92.1
Hardserver Port:	9004
Hardserver Uptime:	45 Days : 20 Hours : 49 Minutes : 18 Seconds

Applications with Active Connection to Hardserver:

Applications with Active Connection to Hardserver ▾

Search: Add

▲ Connection Number	Uptime	Command Count	Reply Count	Remote IP Address	Process ID	Process Name	Total Object Count
1	45 Days : 20 Hours : 49 Minutes : 18 Seconds	0	133087929	0.0.0.0	0		Not available
5	45 Days : 20 Hours : 48 Minutes : 46 Seconds	0	0	0.0.0.0	0	[legacy]	Not available
29754	41 Days : 01 Hours : 03 Minutes : 14 Seconds	12138154	12138153	0.0.0.0	0		Not available

Security World Info:

Security World Info ▾

Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

nShield HSMs

nShield HSMs ▾

Search: Add

Serial No.	Type	Mode	Commands Last Hr.
9FC6-3000-53C9	SOLO	OPERATIONAL	4378
F48C-82C8-3ED9	CONNECT	OPERATIONAL	1418772

nShield Card Sets:

nShield Card Sets		
<input type="text" value="Search: ..."/>		
Set Name	Client Host Count	Generation Time
ffoc1	1	2016-08-24T19:08:11.811Z
oc1	3	2016-03-15T18:17:12.1712Z
oc2	3	2016-03-15T23:07:15.715Z

nShield Keys:

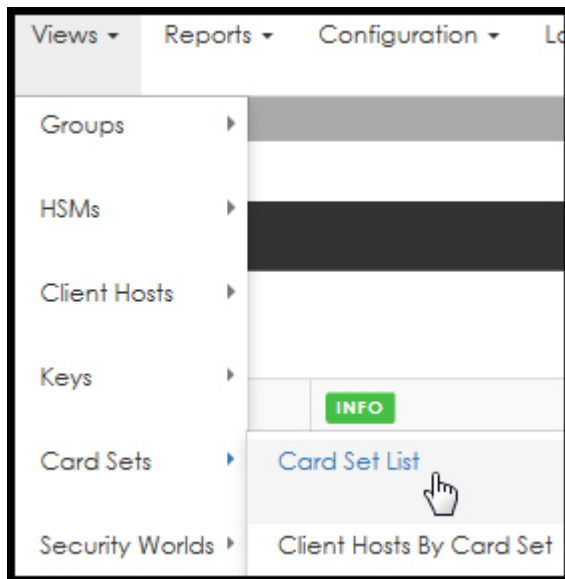
nShield Keys			
<input type="text" value="Search: ..."/> Add			
Key Identifier/Name	Key Hash	Key Application Name	Client Hosts
6ffc2755601f7472c8b4a3d2515eafe53c964efd	1f3c2f6231f8fe07b3b31ecd1456651b88eca2d2	embed	3
8fd31935920b3b47abe145e7ecdbed87dba7fe55	429ce182a09a5b7cb088e64f9551ed61f181e317	embed	3
ff1	7386cc17bca937d59df56ff74f88207c1bd8edff	simple	3
ff2	bdbfdfa419715482c298d8238456b00749a8ddee	simple	3
ff3	16d84dab6309081da9aa374c0544b832cb19c8a8	simple	3

9.4.5. Card Sets

1. Navigate to:

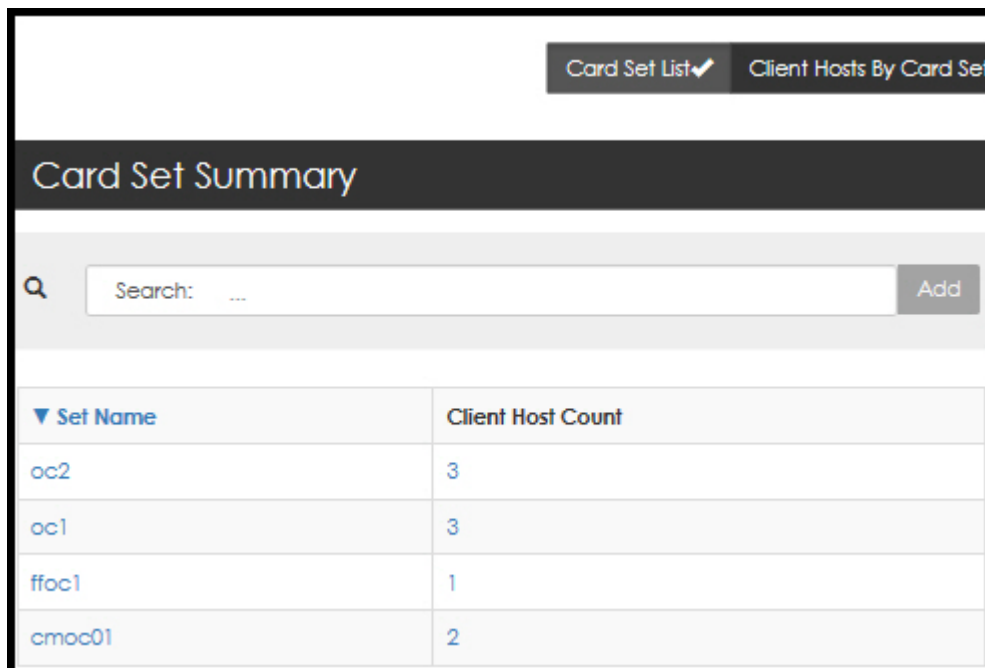
Views > Card Sets

9.4.5.1. View > Card Set > List



1. Select **Card Set List**.

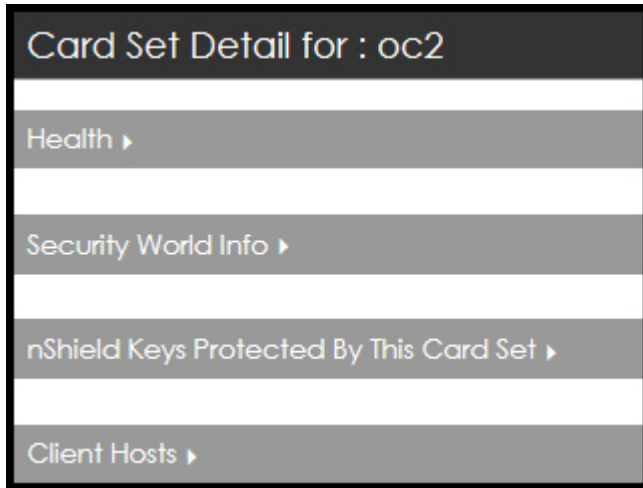
The **Card Set Summary** page opens.



The screenshot shows the 'Card Set Summary' page. At the top, there are two tabs: 'Card Set List' (selected) and 'Client Hosts By Card Set'. Below the tabs is a search bar with the text 'Search: ...' and an 'Add' button. The main content is a table with two columns: 'Set Name' and 'Client Host Count'.

Set Name	Client Host Count
oc2	3
oc1	3
ffoc1	1
cmoc01	2

2. Select a **Set Name** to open a specific **Card Set Detail** page.



3. Select the expansion arrow to open the windows.

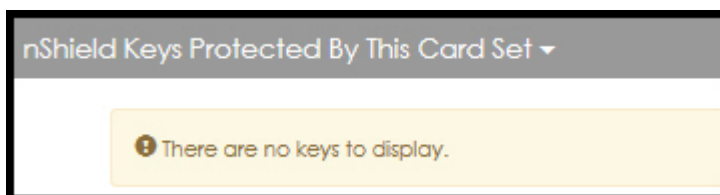
Health:

Health ▾	
hashKLTU:	51 aa06c4a79c0b696c2c3df48dc641f8c24f804a
Quorum Count (k):	1
Total Number Of Cards(N):	1
Timeout :	0
Generation Time :	2016-03-15T23:07:15.715Z

Security World Info:

Security World Info ▾	
Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

nShield Keys Protected By This Card Set:



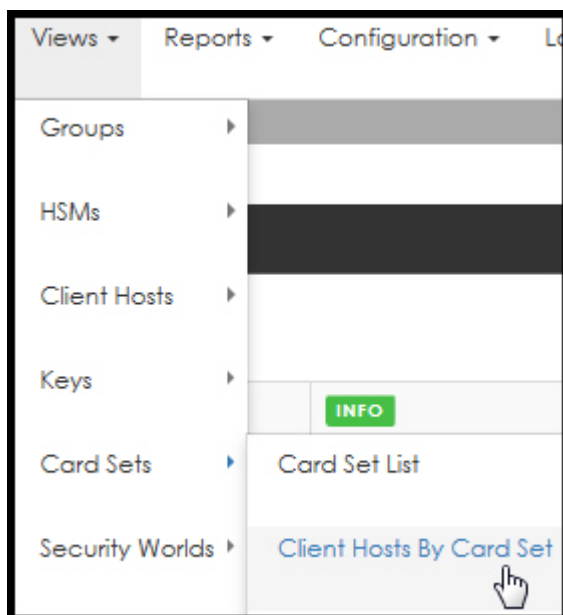


When there are no keys to display, the system indicates such.

Client Hosts:

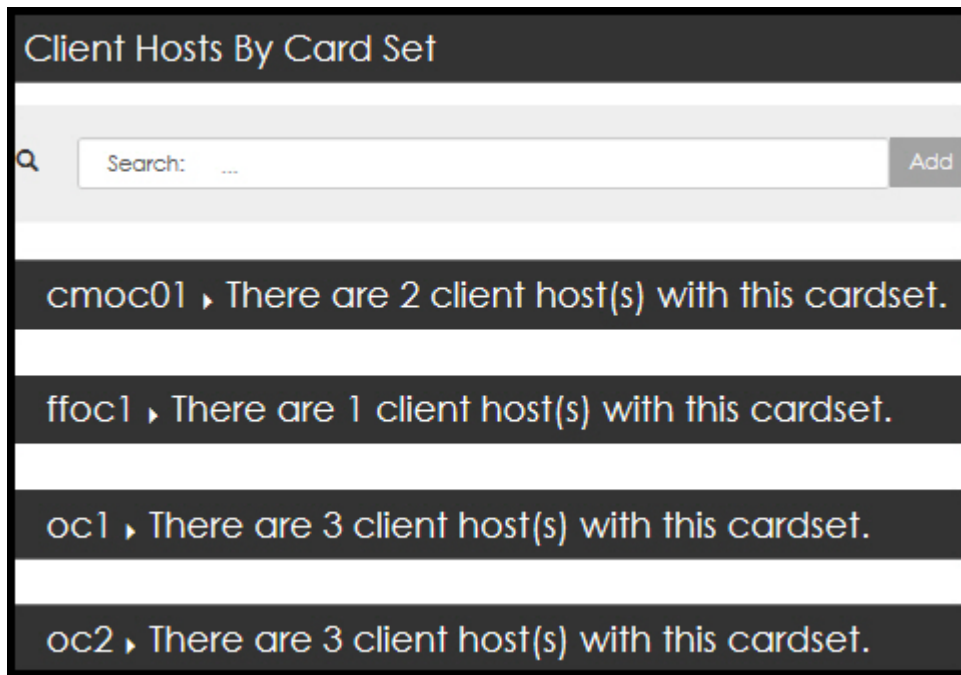
Name	Hardserver Status	Command Last Hr.
Faisal CH 1	RUNNING	8396
Faisal CH 2	RUNNING	4243090
Faisal SW2 CH1	RUNNING	1306549

9.4.5.2. View > Card Sets > Client Hosts By Card Set

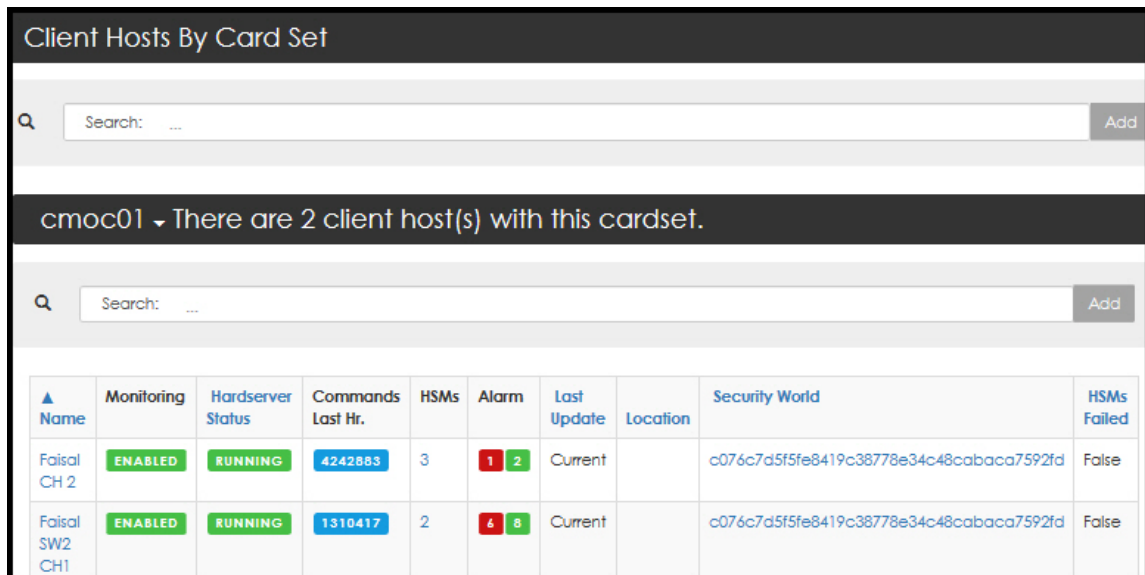
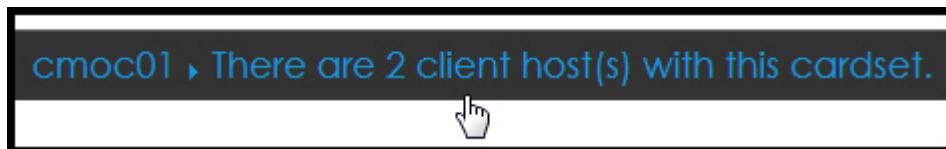


1. Select **Client Hosts By Card Set**.

The **Client Hosts By Card Set** page opens.



2. When hovering over the text turns the text blue, click to expand.



3. Continue to click on the blue text to drill deeper.

For example, clicking on the Security World identifier opens the **Security World Detail** page:

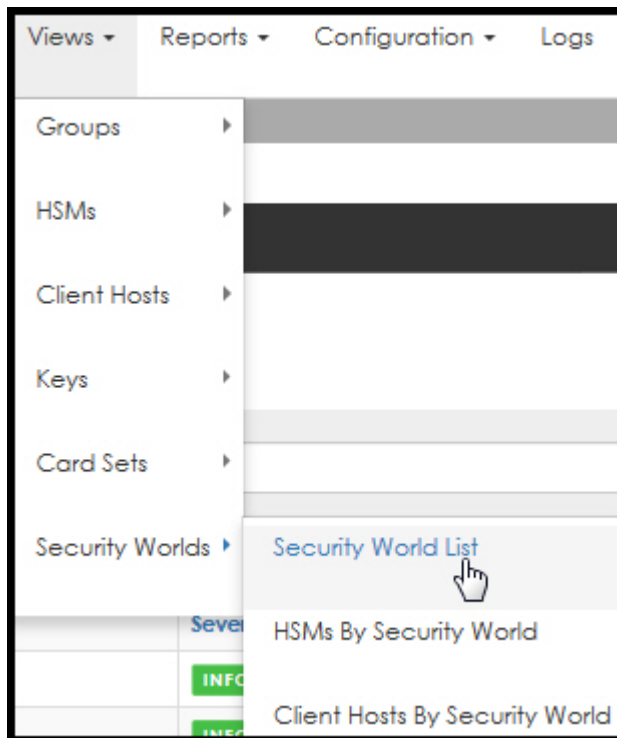


9.4.6. Security Worlds

9.4.6.1. Views > Security Worlds > Security World List

1. Navigate to:

Views > Security Worlds > Security World List



2. Select **Security World List**.

The **Security World Summary** page opens.

A screenshot of the 'Security World Summary' page. At the top, there is a search bar with the text 'Search: ...' and an 'Add' button. Below the search bar is a table with the following data:

Name	HashKNSO	Client Hosts	nShield	Generation Time	Generating Module ESN
c076c7d5f5fe8419c38778e34c48cabaca7592fd	c076c7d5f5fe8419c38778e34c48cabaca7592fd	2	10	2016-01-29T00:00:00.000Z	B56A-81C9-73F2

3. Click on the blue text to drill deeper.

A close-up screenshot of the table row from the previous image. The 'Name' column contains the value 'c076c7d5f5fe8419c38778e34c48cabaca7592fd' and the 'HashKNSO' column contains the same value. A mouse cursor is clicking on the 'HashKNSO' value.

Name	HashKNSO
c076c7d5f5fe8419c38778e34c48cabaca7592fd	c076c7d5f5fe8419c38778e34c48cabaca7592fd

For example, clicking on the Security World HashKNSO opens the **Security World Detail** page.

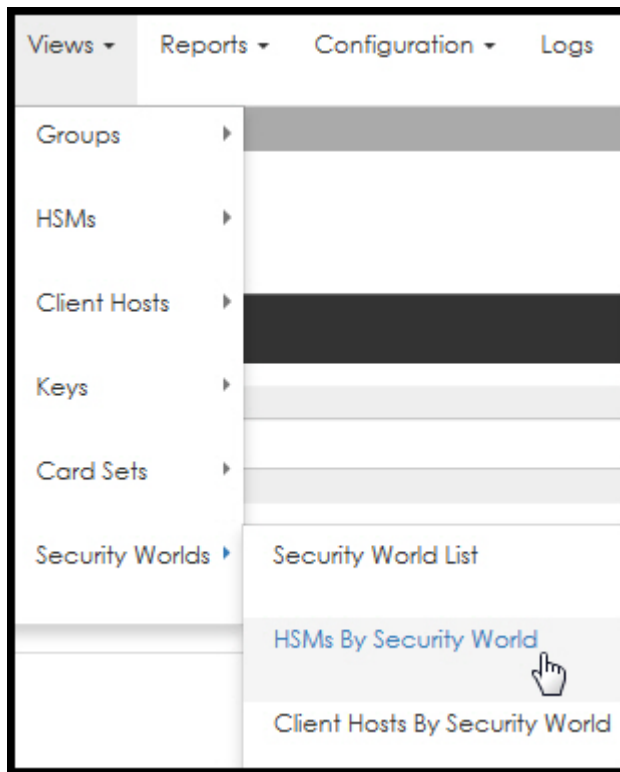


4. Click on the expansion arrows to open additional windows.

9.4.6.2. Security Worlds > HSMs By Security World

1. Navigate to:

Security Worlds > HSMs By Security World



2. Select **HSMs By Security World**.

The **HSMs By Security World** page opens.

HSMs By Security World

Search: ...

c076c7d5f5fe8419c38778e34c48cabaca7592fd ▾ There are 4 nShield(s) in this security world.

Search: ... Add

nShield HSMs

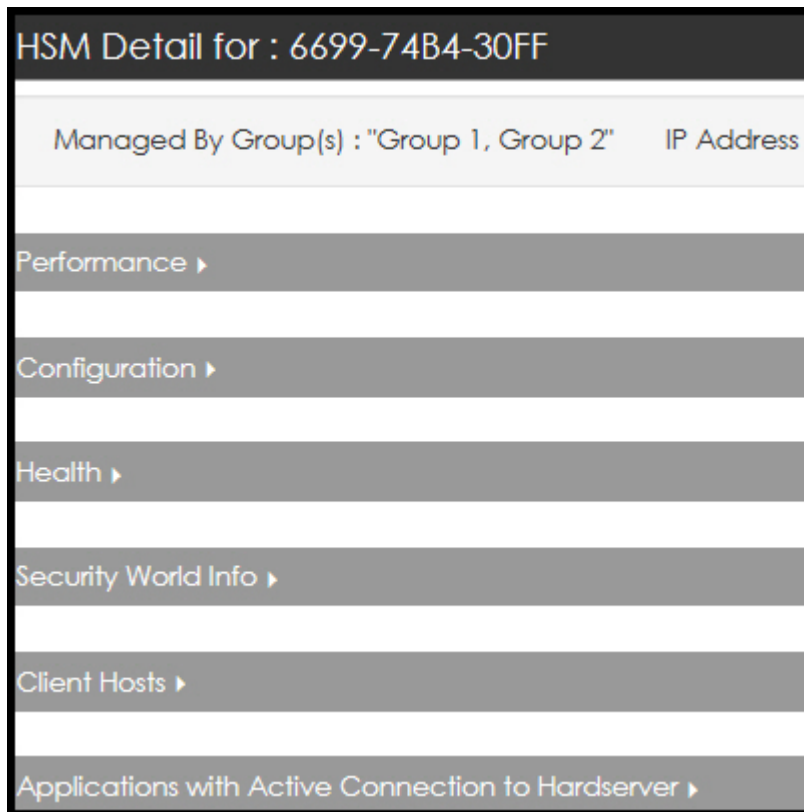
▲ Serial No.	Type	Mode	Monitoring	Objects	Commands Last Hr.	Alarms	Client Host (s)	Last Update
6699-74B4-30FF	CONNECT	OPERATIONAL	ENABLED	10	2069927	1 1	2	Current
6F99-74BF-429B	CONNECT	OPERATIONAL	ENABLED	10	2069657	1 1	2	Current

3. When hovering over the text turns the text blue, click to expand.

nShield HSMs

▲ Serial No.	Type	Mode	Monitoring	Objects	Commands Last Hr.	Alarms	Client Host (s)	Last Update
6699-74B4-30FF	CONNECT	OPERATIONAL	ENABLED	10	2069927	1 1	2	Current
6F99-74BF-429B	CONNECT	OPERATIONAL	ENABLED	10	2069657	1 1	2	Current

4. Select a **Serial Number** to open the **HSM Detail** page.

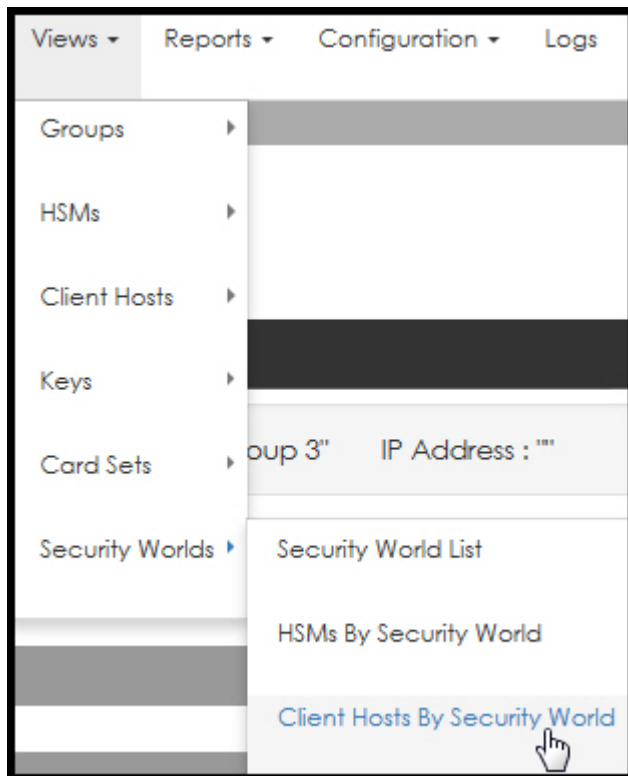


5. Select the expansion arrows to open additional windows.

9.4.6.3. Security Worlds > Client Hosts By Security World

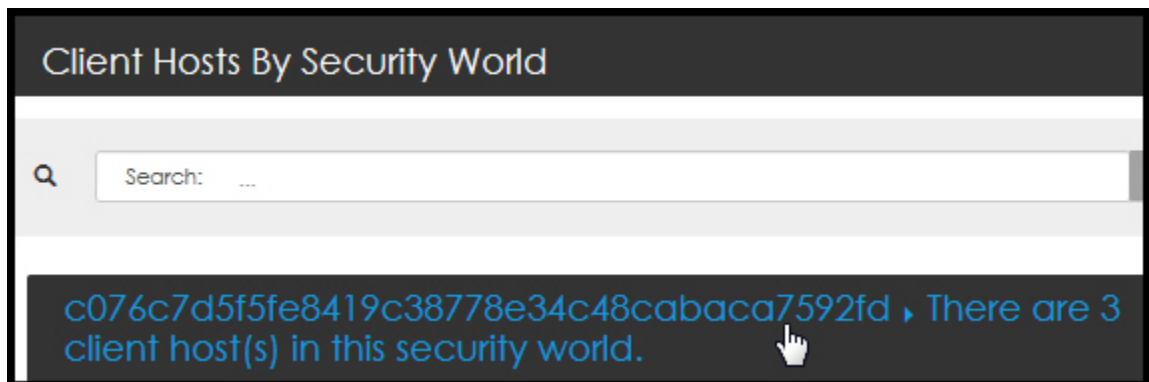
1. Navigate to:

Security Worlds > Client Hosts By Security World



The **Client Hosts By Security World** page opens.

2. When hovering over the text, the font turns blue, click to expand.



The page expands:

Client Hosts By Security World

Search: ... Add

c076c7d5f5fe8419c38778e34c48cabaca7592fd ▾ There are 3 client host(s) in this security world.

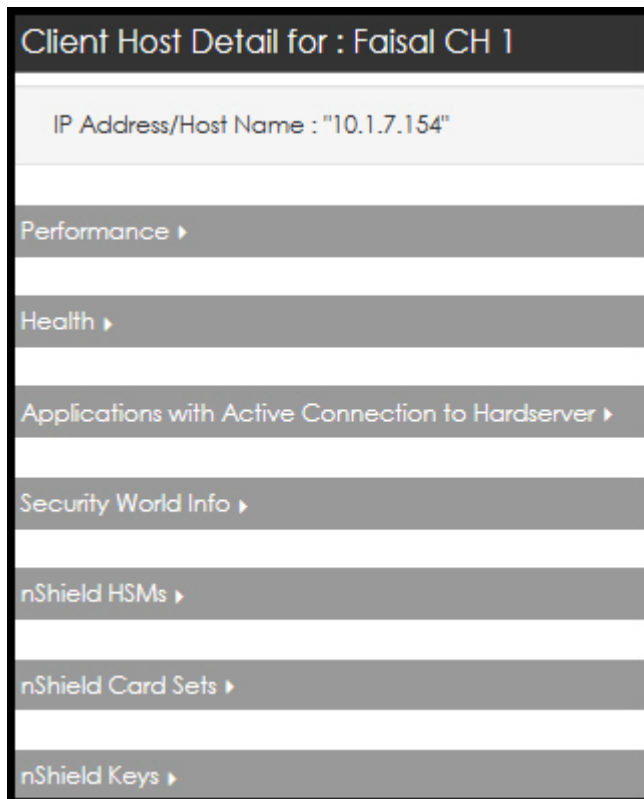
Search: ... Add

Name	Monitoring	Hardserver Status	Commands Last Hr.	HSMs	Alarm	Last Update	Location	▲ HSMs Failed
Faisal CH 2	ENABLED	RUNNING	4248634	3	1 2	Current		False
Faisal SW2 CH1	ENABLED	RUNNING	1310283	2	6 8	Current		False
Faisal CH 1	ENABLED	RUNNING	8419	2	1	Current		True

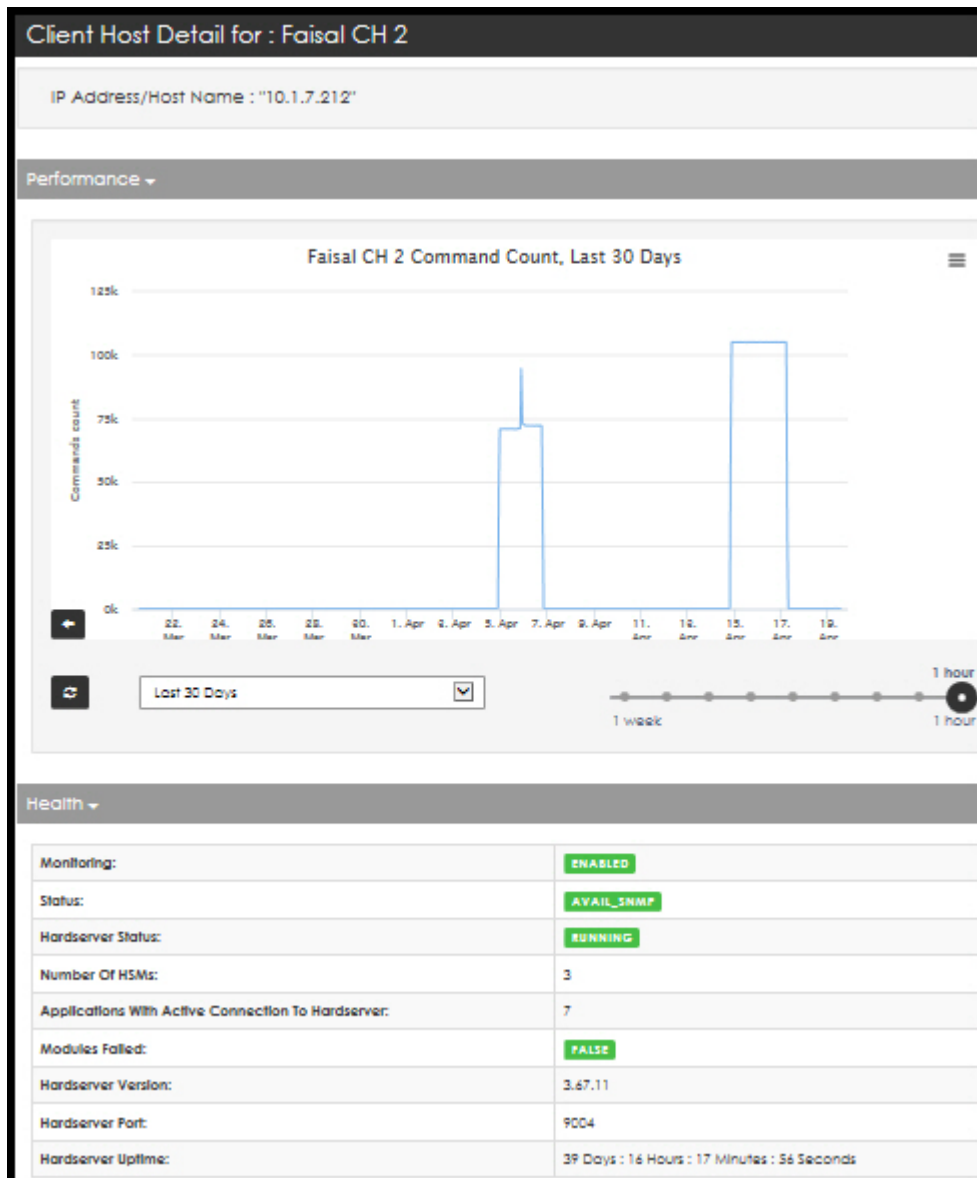
The blue font indicates that there are two links on this page, i.e., data in the name column, and count total in the HSMs column.

3. Select a specific **Name**, e.g., click on **Faisal CH 2**.

The **Client Host Detail for: Faisal CH 2** page opens.



4. Select the expansion arrows to open additional windows.



Applications with Active Connection to Hardserver ▾

Q Search: ... Add

Connection Number	Uptime	Command Count	Reply Count	Remote IP Address	Process ID	Process Name	Total Object Count
3	39 Days : 16 Hours : 17 Minutes : 54 Seconds	0	128670655	0.0.0.0	0		0
4	39 Days : 16 Hours : 17 Minutes : 54 Seconds	0	0	0.0.0.0	0	[legacy]	0
5	39 Days : 16 Hours : 17 Minutes : 54 Seconds	0	0	0.0.0.0	0	[legacy]	0
6	39 Days : 16 Hours : 17 Minutes : 54 Seconds	0	0	0.0.0.0	0	[legacy]	0
160619	13 Days : 15 Hours : 20 Minutes : 39 Seconds	11986380	11986379	0.0.0.0	0		0

5 rows per page. First Page 1 2 Last Page 7 Total rows . Page 1 of 2

Security World Info ▾

Security World Name:	c076c7d5f5fe8419c38778e34c48cab0ca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cab0ca7592fd
hashKM:	111a3dbf3fc3412e2d637e97e19614baa1362128

nShield HSMs ▾

Q Search: ... Add

Serial No.	Type	Mode	Commands Last Hr.
6699-7484-30FF	CONNECT	OPERATIONAL	4519
6F99-748F-429B	CONNECT	OPERATIONAL	4512
F48C-82C9-3ED9	CONNECT	OPERATIONAL	4520

5 rows per page. First Page 1 Last Page 3 Total rows . Page 1 of 1

nShield Card Sets ▾

Q Search: ... Add

Set Name	Client Host Count	Generation Time
amoc01	2	2016-09-16T23:49:30.000Z
oc1	3	2016-09-15T18:17:12.000Z
oc2	3	2016-09-15T23:07:15.000Z

3 rows per page. First Page | 1 | Last Page 3 Total rows . Page 1 of 1

nShield Keys ▾

Q Search: ... Add

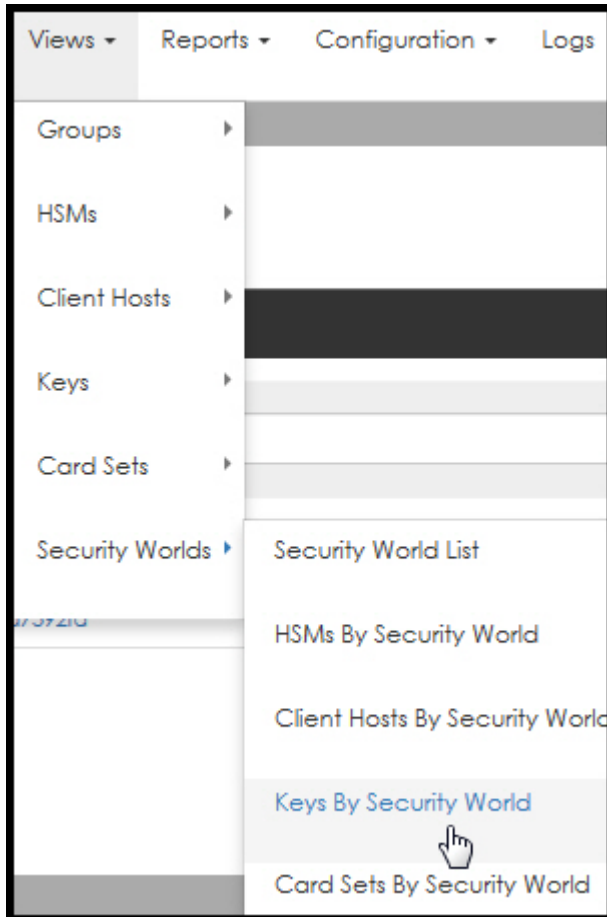
Key Identifier/Name	Key Hash	Key Application Name	Client Hosts
6ffa275560117472c8b4a3d2515eafe53c964e1d	1f3c216231f81e07b3b31e0d1456651b88eca2d2	embed	3
8fd31935920b3b47abe145e7eacdbed87d0a71e55	429ce182a09a9b7cb088e64f9551ed611181e317	embed	3
#1	7386cc17bca937a59af56ff74f88207c1ba8edff	simple	3
#2	bbbf0fa419715482c298d8238456b00749a8ddee	simple	3
#3	16d84dab6309081da9aa374c0544b832cb19a8a8	simple	3

5. Continue to click on the blue text to drill deeper.

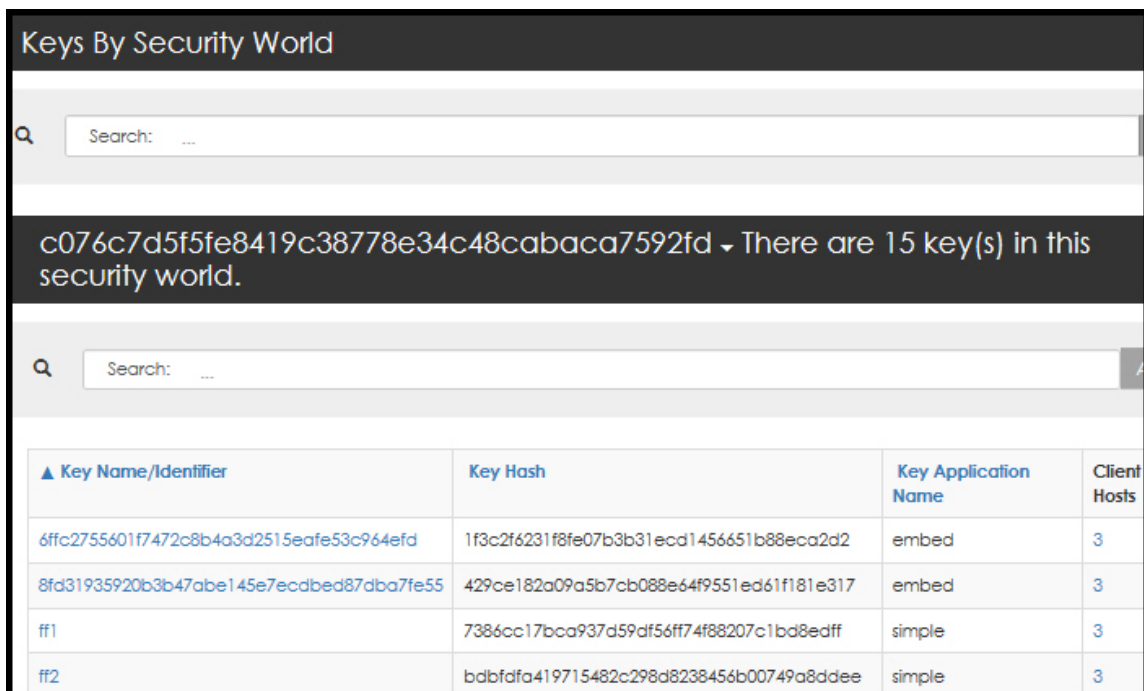
9.4.6.4. Security Worlds > Keys By Security World

1. Navigate to:

Security Worlds > Keys By Security World



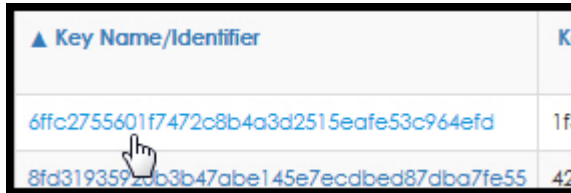
The **Keys By Security World** page opens.



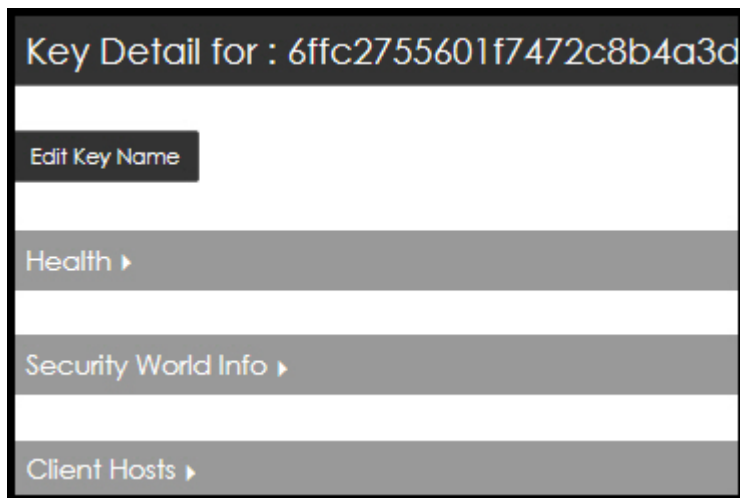
Both the Key Name/Identifier and the Client Host columns contain blue font. Blue font indicates an active link. For

example purposes, the following step selects the Key Name/Identifier.

2. Select the **Key Name/Identifier**.



The **Key Detail** page opens.



3. Select the expansion arrows to open additional windows.

Health ▾

Key Application Name :	embed
Key Identifier :	6ffc2755601f7472c8b4a3d2515eafe53c964efd
Key Hash :	1f3c2f6231f8fe07b3b31ecd1456651b88eca2d2
Key Protection :	MODULE
Key Recovery :	ENABLED
Time Limit :	0
Pre-authentication Use Time Limit :	0
Generating Module ESN :	Not available
Protecting Cardset Hash :	

Security World Info ▾

Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

Client Hosts ▾

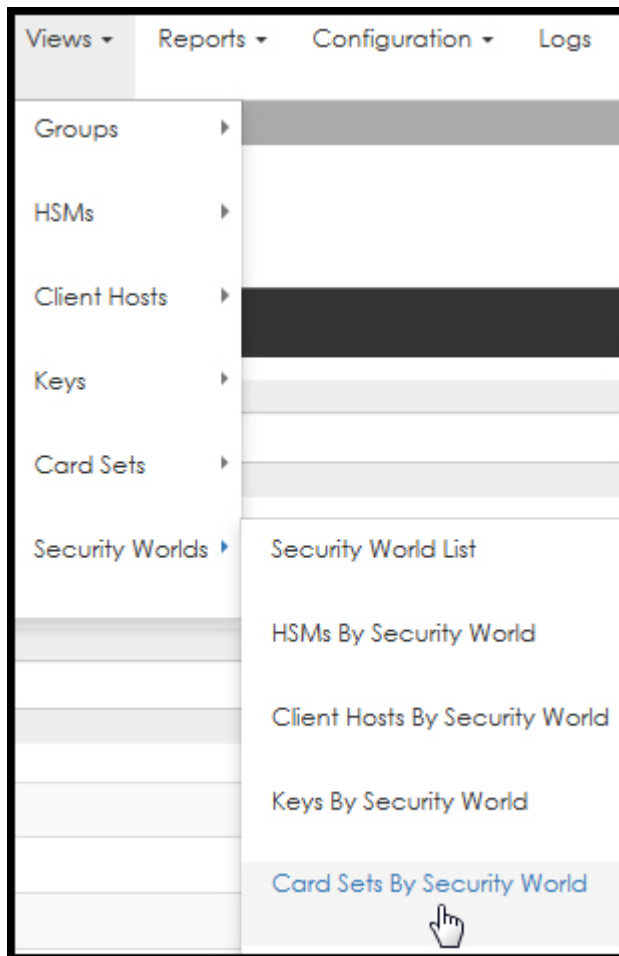
Name	Hardserver Status	Command Last Hr.
Faisal CH 1	RUNNING	8334
Faisal CH 2	RUNNING	4246414
Faisal SW2 CH1	RUNNING	1310280

4. Continue to click on the blue text to drill deeper.

9.4.6.5. Security Worlds > Card Sets By Security World

1. Navigate to:

View > Security Worlds > Card Sets By Security World



The **Card Sets By Security World** page opens.

Card Sets By Security World

Search: ... Add

c076c7d5f5fe8419c38778e34c48cabaca7592fd
 ▾ There are 4 card set(s) in this security world.

Search: ... Add

▲ Set Name	Client Host Count
cmoc01	2
ffoc1	1
oc1	3
oc2	3

2. Select a **Set Name** to open the **Card Set Detail** page.

Card Set Detail for : cmoc01

Health ▶

Security World Info ▶

nShield Keys Protected By This Card Set ▶

Client Hosts ▶

3. Select the expansion arrows to open the windows.

Card Set Detail for : cmoc01

Health ▾

hashKLTU:	1417ef9958bbb2e1b30045fcdcf1df6292b24644
Quorum Count (k):	1
Total Number Of Cards(N):	2
Timeout :	0
Generation Time :	2016-09-16T23:49:30.4930Z

Security World Info ▾

Security World Name:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
Security World State:	OPERATIONAL
hashKNSO:	c076c7d5f5fe8419c38778e34c48cabaca7592fd
hashKM:	111d3dbf3fc3412e2d637e97e19614baa1362128

nShield Keys Protected By This Card Set ▾

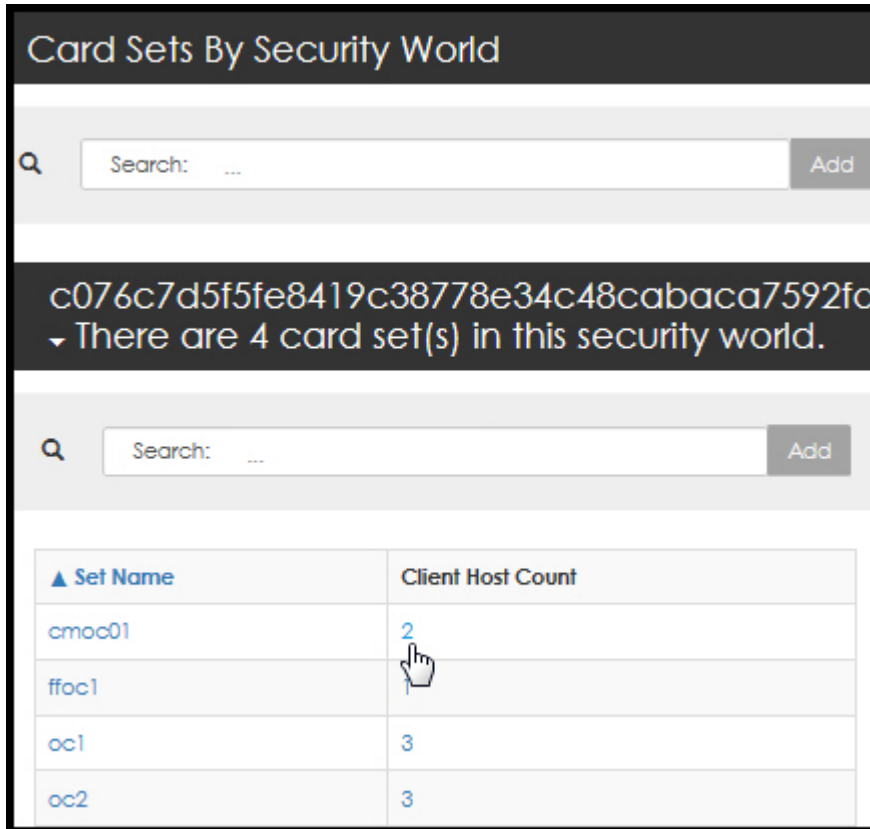
! There are no keys to display.

Client Hosts ▾

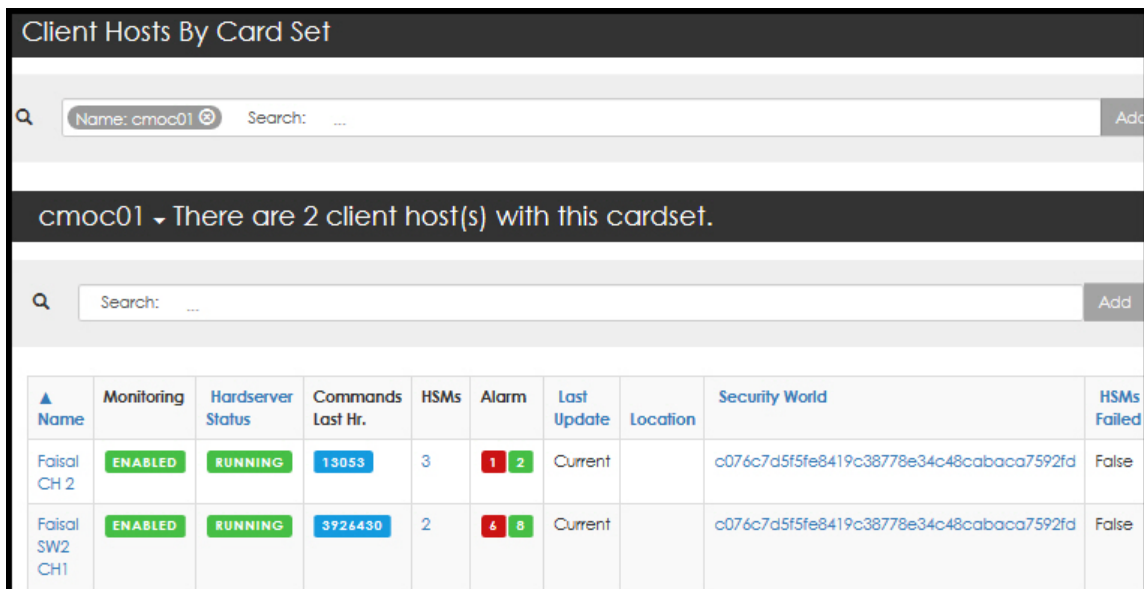
Search: Add

Name	Hardserver Status	Command Last Hr.
Faisal CH 2	RUNNING	13032
Faisal SW2 CH1	RUNNING	3927122

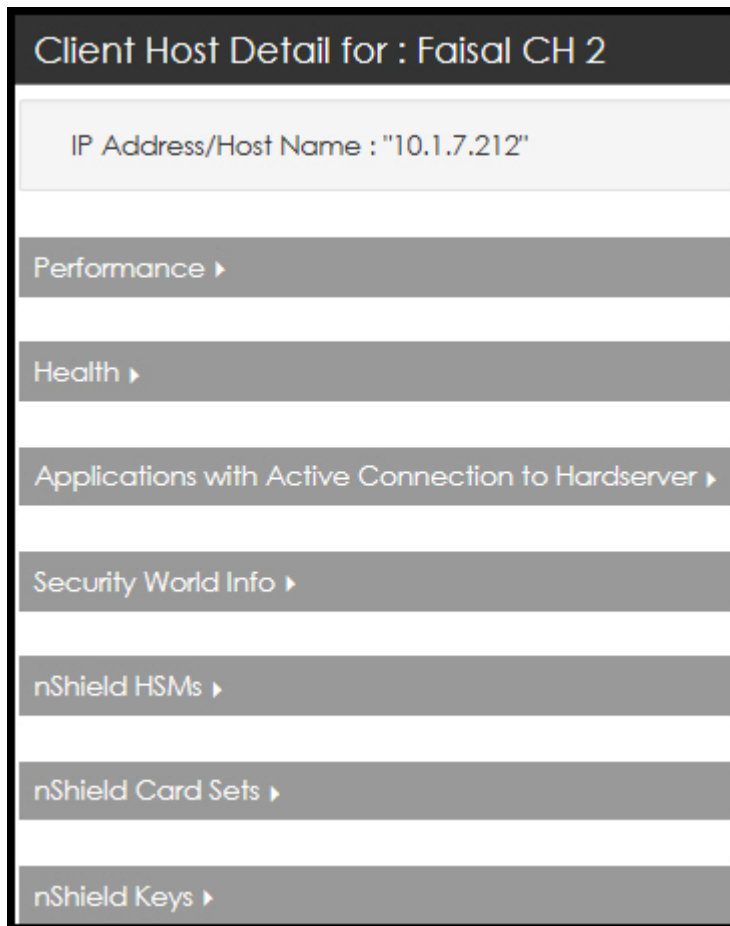
4. Select the **Client Host Count** (from the Card Sets By Security World page).



The **Client Hosts By Card Set** page opens.



5. Select **Name** to open the **Client Host Detail** page.



6. Select the expansion arrows to open the windows.

10. Reports

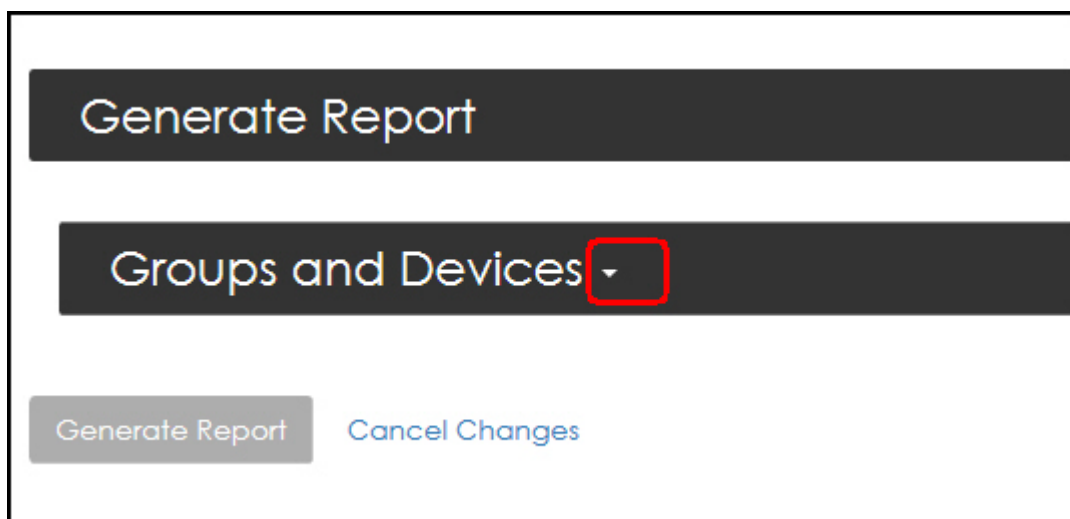
With nShield Monitor, you can create pre-generated reports and send them to a PDF file or export them to a CSV file. These reports can provide valuable information pertaining to a specific HSM or group in near real time. You can also schedule a report to periodically track a group or a specific HSM over time.

With the Reports feature you can track device utilization and loading trends, as well as cross HSM (details per HSM as selected).

10.1. Generating Reports

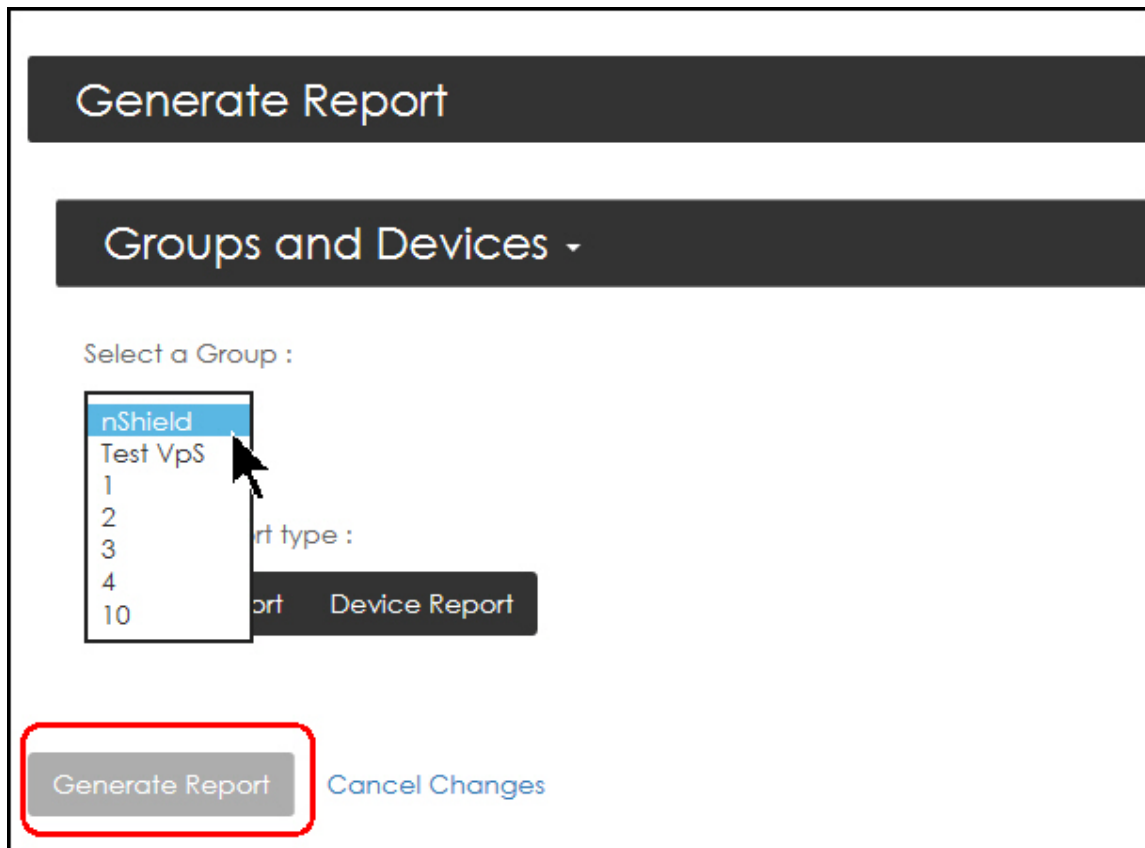
1. Navigate to: **Reports > Generate Reports**

The **Generate Report** page opens.



2. Select the **Groups and Devices** drop down arrow.

The down menu opens.



3. Select a Group. (In the example above, the Group is titled "nShield".)

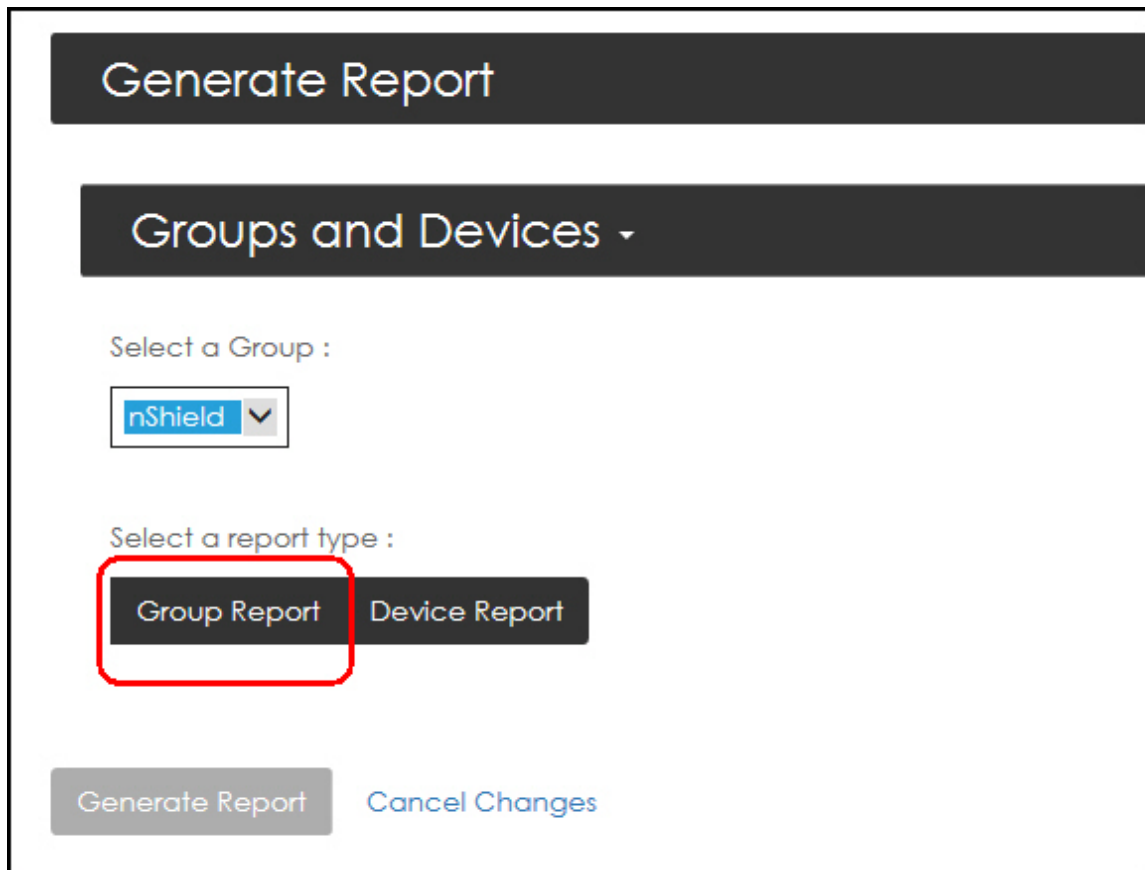
The **Group Report** and **Device Report** options display.



Follow this link to see the Device Report menus/options:
[Device Report.](#)

10.1.1. Group Report

1. Select **Group Report**



Generate Report

Groups and Devices ▾

Select a Group :

nShield ▾

Select a report type :

Group Report Device Report

Generate Report Cancel Changes

The **Generate Report** page opens.

2. Optionally, select **Show Top 10 Devices** to limit the report to the top 10 devices.



You may need to scroll down the screen to access the expansion arrows.

3. Select the **Report Configuration** expansion arrows.

The **Report Configuration** window opens.

Generate Report

Groups and Devices ▾

Select a Group :

nShield ▾

Select a report type :

Group Report ✓

Device Report

(optional) Show Top 10 Devices.

Report Configuration ▾

Enter the report name :

Select a report type :

Utilization and Loading Trends ▾

Select an output format :

PDF ▾

Select a schedule :

One-Time ▾

Select a time/date range :

Last 24 Hours ▾

Select a delivery method :

Save to File ▾

Select a report orientation :

Portrait Landscape

Utilization and Loading Trends Options ▾

Generate Report

Cancel Changes

4. Enter a report name.
5. Expand the drop down arrows and use the radio button to set your report's specifications.
6. Scroll to the **Utilization and Loading Trends Options** window.
7. Expand the drop down arrow.

Utilization and Loading Trends Options ▾

Client Host Options

High Command Count Threshold :

Low Command Count Threshold :

nShield Options

High Command Count Threshold :

Low Command Count Threshold :

High Object Count Threshold :

Low Object Count Threshold :

8. Modify the default settings, based on preference.
9. Select **Generate Report**.

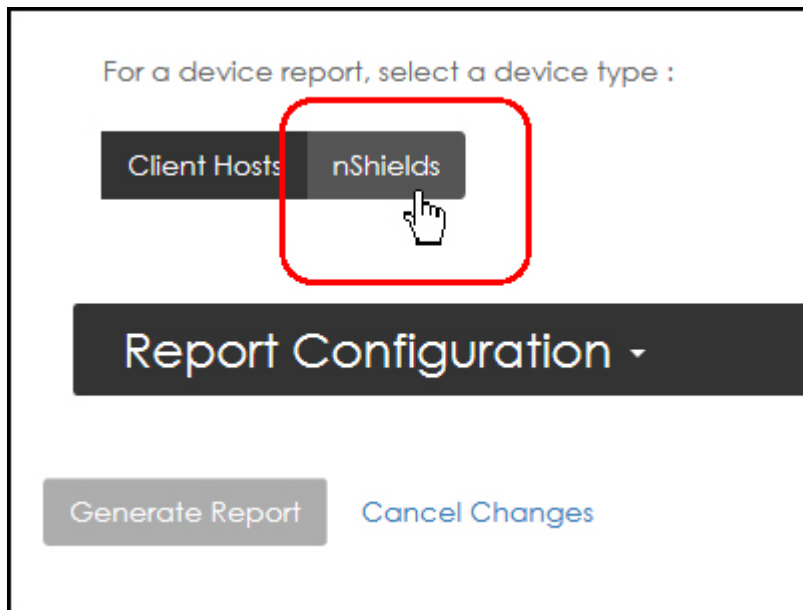
10.1.2. Device Report

1. Select **Device Report**.

The screenshot shows a web interface for generating reports. At the top is a dark header with the text "Generate Report". Below this is another dark header labeled "Groups and Devices" with a downward arrow. The main content area contains the following elements:

- A label "Select a Group :" followed by a dropdown menu showing "nShield" with a downward arrow.
- A label "Select a report type :" followed by two buttons: "Group Report" and "Device Report". The "Device Report" button is selected, indicated by a checkmark and a red rectangular highlight.
- A label "For a device report, select a device type :" followed by two buttons: "Client Hosts" and "nShields".
- A dark footer bar with the text "Report Configuration" and a downward arrow.
- At the bottom, there are two buttons: "Generate Report" (disabled) and "Cancel Changes" (active).

2. Select a device type.



To see the flow for device type **Client Hosts**, go to: [Device report for Client Hosts](#).

The device selection window opens.

Groups and Devices ▾

Select a Group :

Select a report type :

For a device report, select a device type :

Click a device in either selection box to move it to the other one.

Search:

Selected Devices
 Remaining Devices: 15

Available Devices

0305-02E0-D947 (10.1.3.78) (CONNECT XC)
2805-02E0-D947 (10.1.3.77) (CONNECT XC)
6699-74B4-30FF (10.1.3.71) (CONNECT)
6F99-74BF-429B (10.1.3.72) (CONNECT)
B56A-81C9-73F2 (10.1.5.49) (CONNECT)
F48C-82CB-3ED9 (10.1.3.70) (CONNECT)

Report Configuration ▾

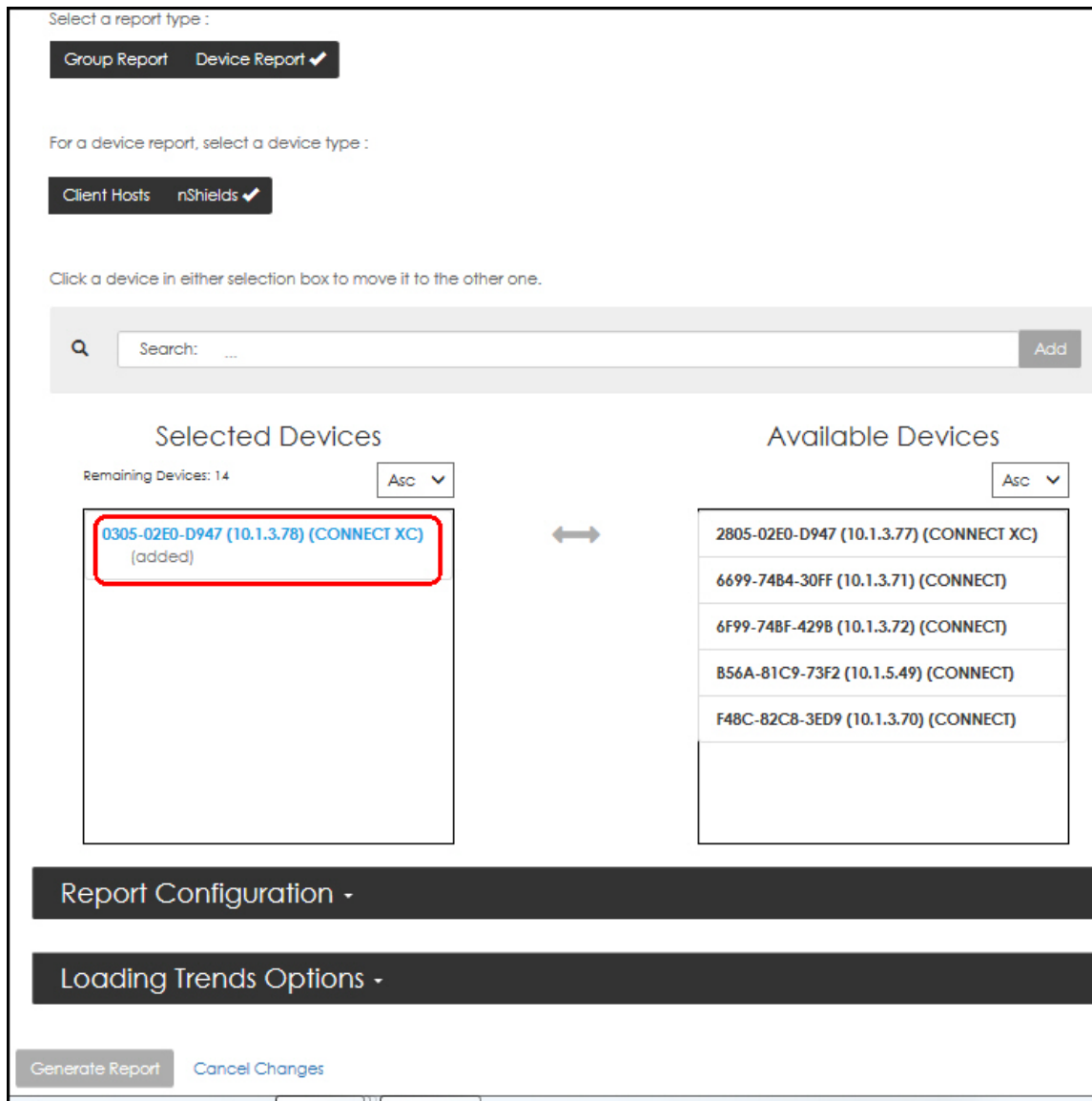
Loading Trends Options ▾

3. Select, by single clicking, the devices from the **Available Devices** window for inclusion in your report.



The click will toggle the device between the **Selected Devices** window and the **Available Devices** window.

The selected device moves to the **Selected Devices** window.



You may need to scroll down to access the expansion arrows for additional views.

4. Select the expansion arrow to open the **Report Configuration** window.

Report Configuration ▾

Enter the report name :

Select a report type :

Loading Trends ▾

Select an output format :

PDF ▾

Select a delivery method :

Save to File ▾

Select a report orientation :

Portrait Landscape

Select a schedule :

One-Time ▾

Select a time/date range :

Last 24 Hours ▾

5. Enter the report name and select the drop down arrows to display additional selections.
6. Select your preferences.
7. Select the expansion arrow to open the **Utilization and Loading Trends Options** window.

Loading Trends Options ▾

nShield Options

High Command Count Threshold :

Low Command Count Threshold :

High Object Count Threshold :

Low Object Count Threshold :

Generate Report Cancel Changes

8. Set your preferences.
9. Select **Generate Report**.

10.1.3. Device report for Client Hosts

1. Navigate to: **Generate Report > Groups and Devices > Device Report > Client Hosts**

Generate Report

Groups and Devices ▾

Select a Group :

nShield ▾

Select a report type :

Group Report Device Report ✓

For a device report, select a device type :

Client Hosts ✓ nShields



The Client Host Cross-HSM device report supports 2,500 nShield keys, i.e., the report limits the number of keys to 2,500 even if there are more keys on the client host.

2. Select, by single clicking, the devices in the **Available Devices** window to move the device into the **Selected Devices** window.

Select a report type :

Group Report Device Report ✓

For a device report, select a device type :

Client Hosts ✓ nShields

Click a device in either selection box to move it to the other one.

Q Search: ... Add

Selected Devices

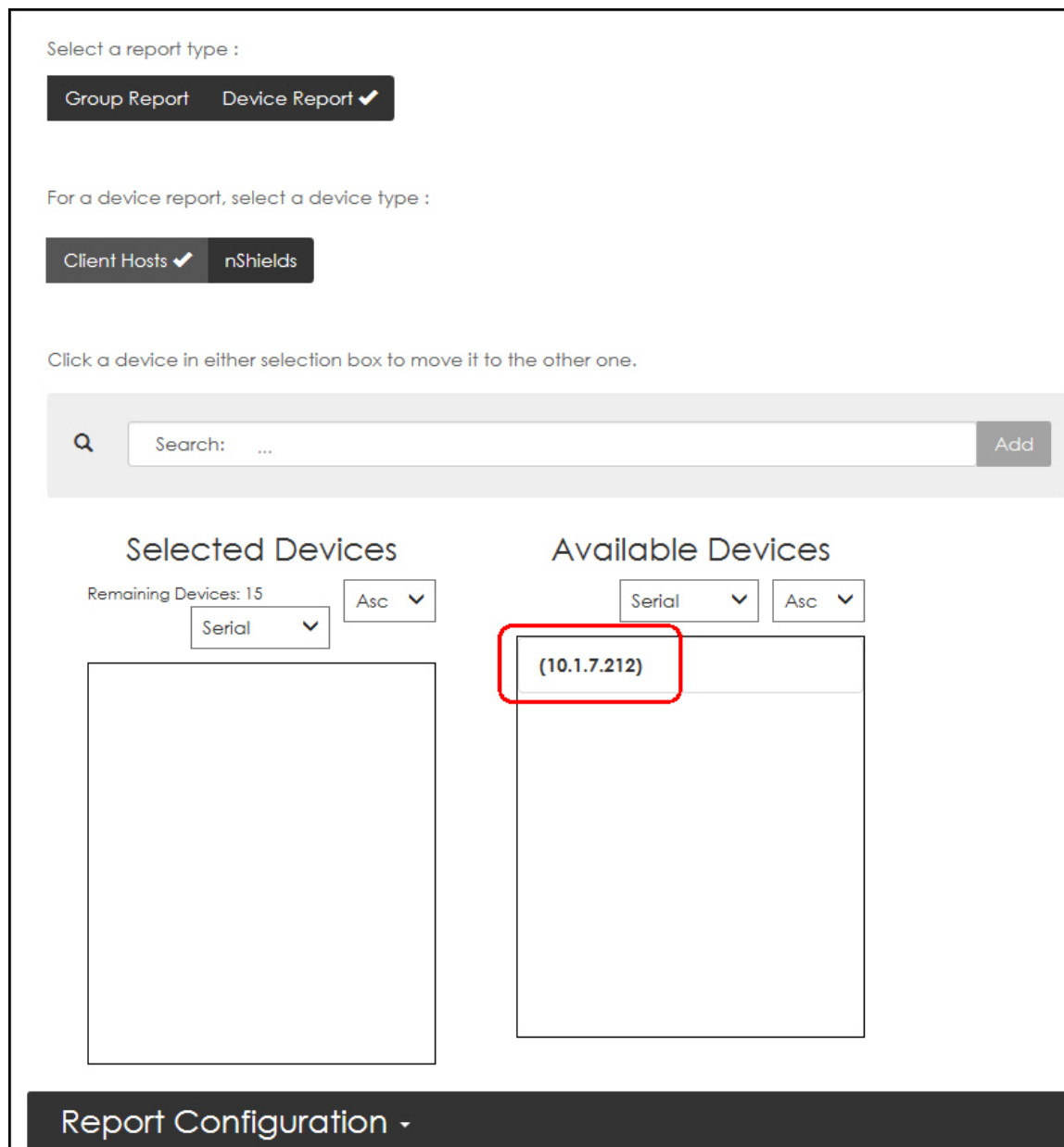
Remaining Devices: 15 Serial Asc ▼

Available Devices

Serial Asc ▼

(10.1.7.212)

Report Configuration ▾



The click will toggle the device between the **Selected Devices** window and the **Available Devices** window.



You may need to scroll down to access the expansion arrows for additional views.

3. Select the expansion arrows to open the **Report Configuration** window.

Report Configuration ▾

Enter the report name :

Select a report type :

Loading Trends ▾

Select an output format :

PDF ▾

Select a delivery method :

Save to File ▾

Select a report orientation :

Portrait Landscape

Select a schedule :

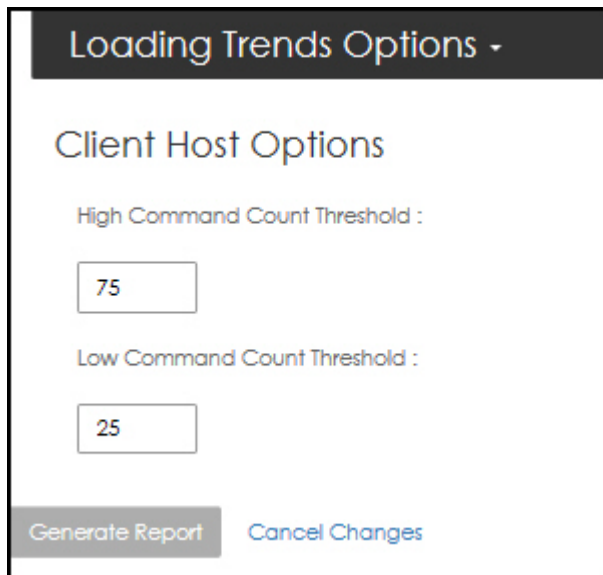
One-Time ▾

Select a time/date range :

Last 24 Hours ▾

Loading Trends Options ▾

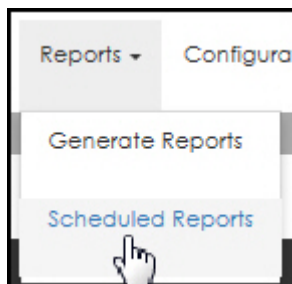
4. Enter a report name and select the drop down arrows to display additional selections (i.e., choices).
5. Select your preferences.
6. Select the expansion arrow to open the **Loading Trends Options** window.



7. Set your thresholds.
8. Select **Generate Report**.

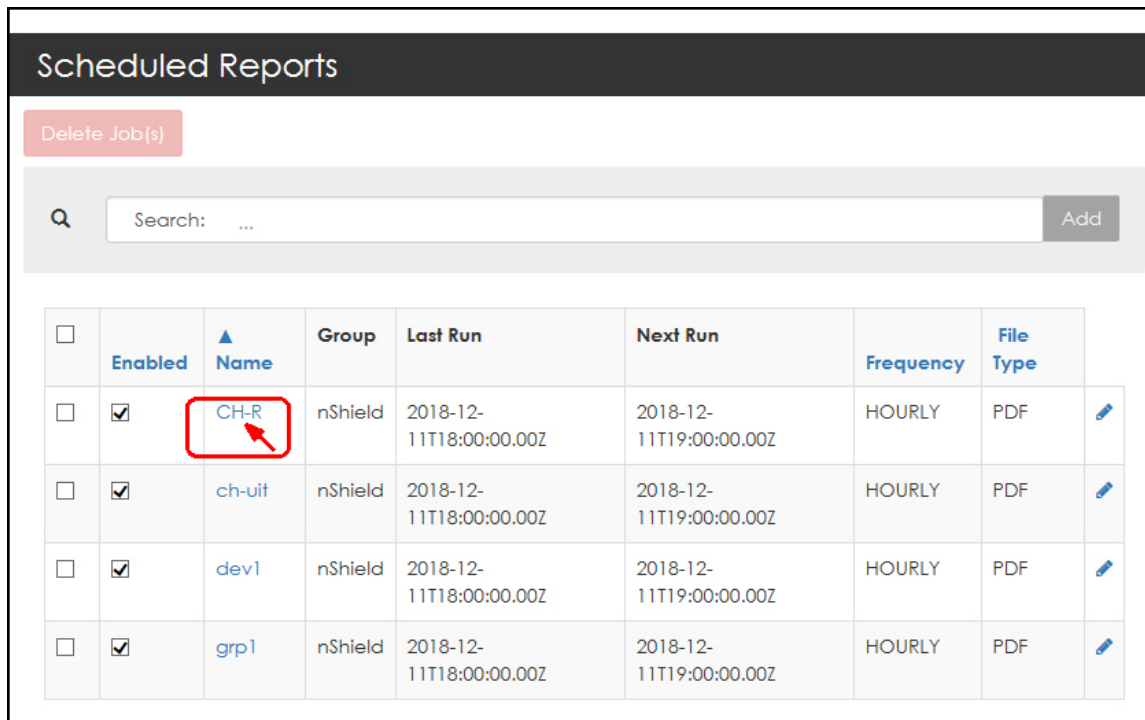
10.2. Scheduled Reports

1. Navigate to: **Reports > Scheduled Reports**

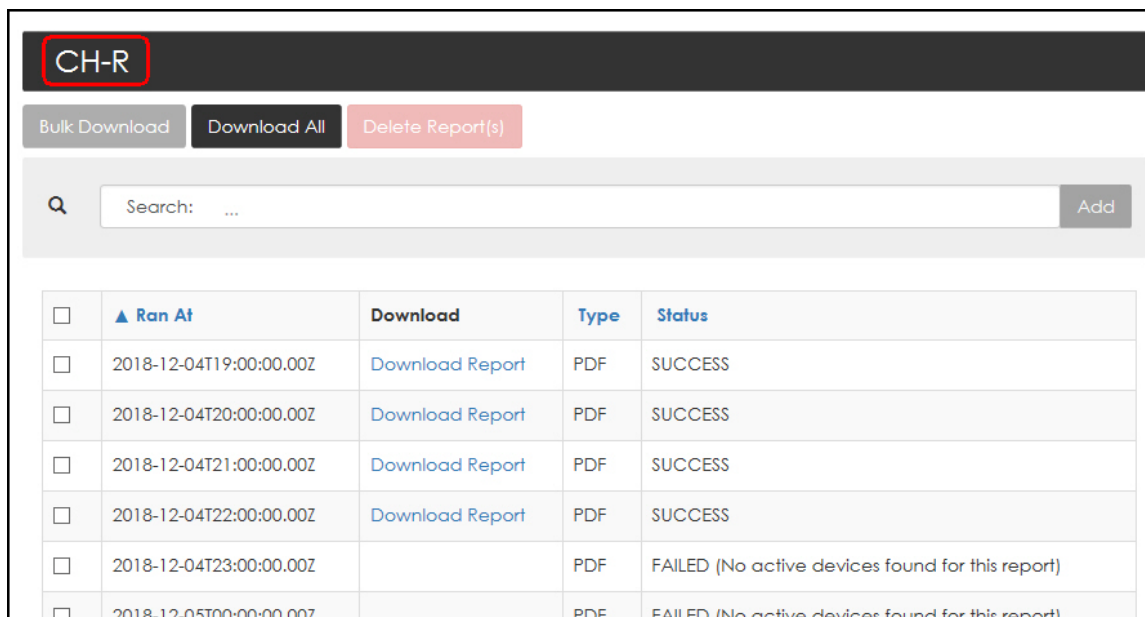


The **Scheduled Reports** page opens.

2. Select the report name.

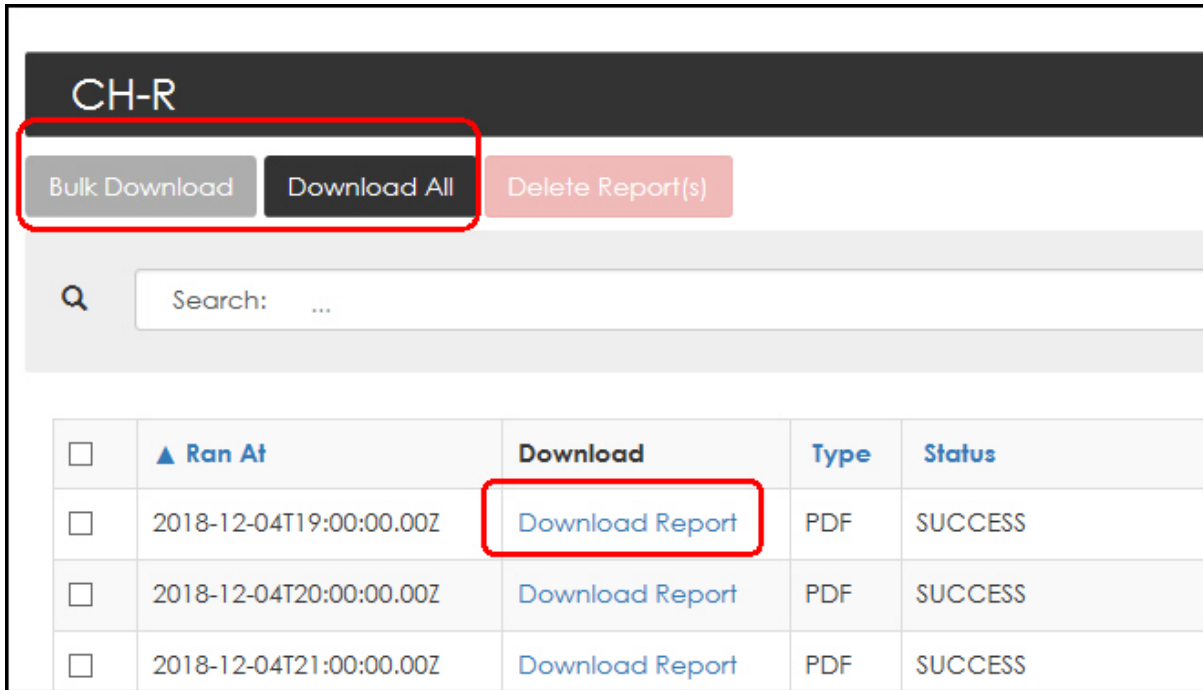


The report page opens.



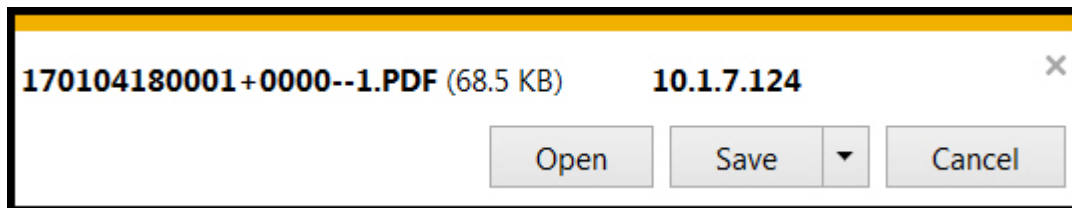
10.2.1. Downloading Individual Reports

The report page also provides download links.



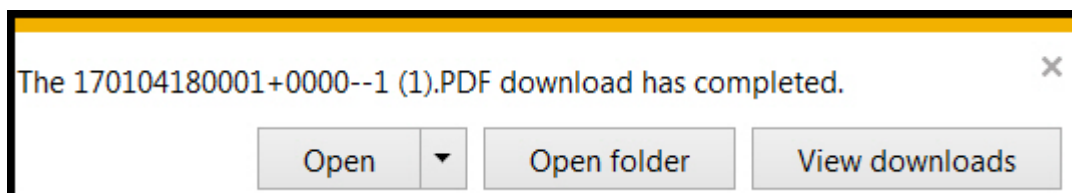
1. Select **Download Report**.

The system prompts:



2. Select **Open** or **Save**.

When Save is selected, the system prompts:



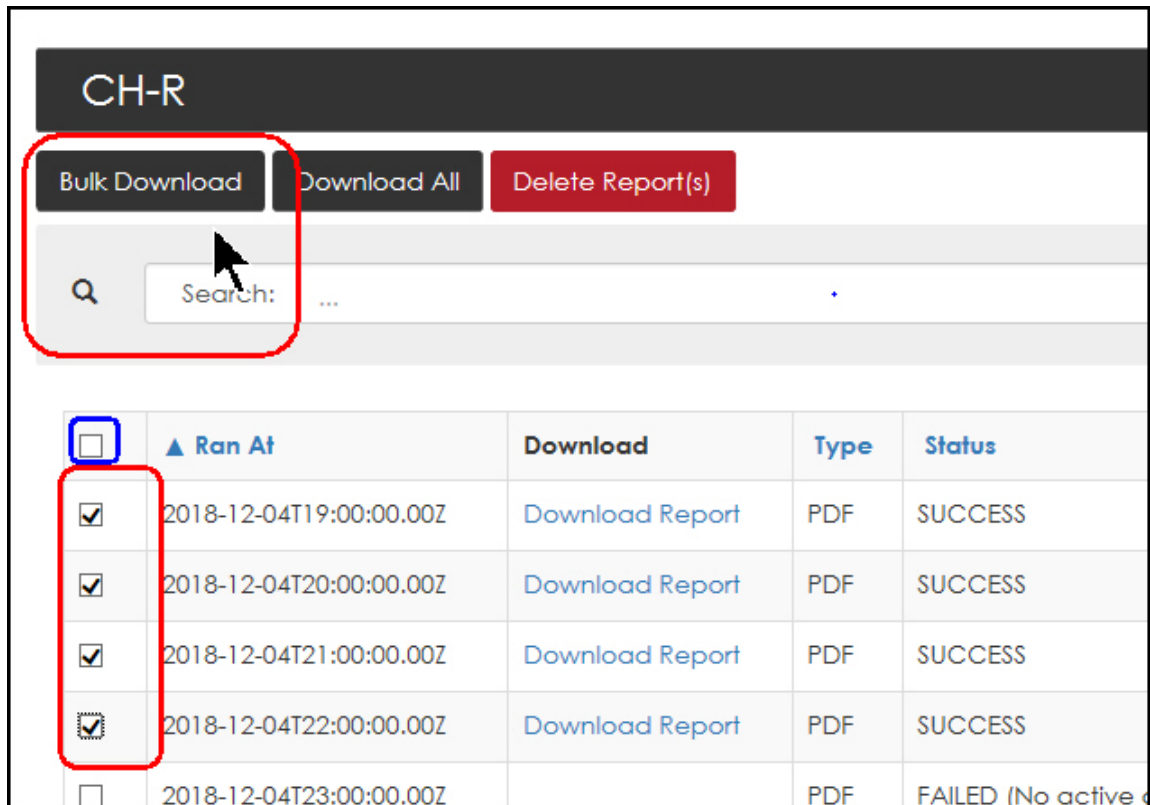
3. Select your preference.

10.2.2. Downloading Reports in Bulk

Selecting **Bulk Download** uses a toggle:

1. Select the check box of the first report to download.

The **Bulk Download** and **Delete Report** tabs activate as soon as you have selected a report.



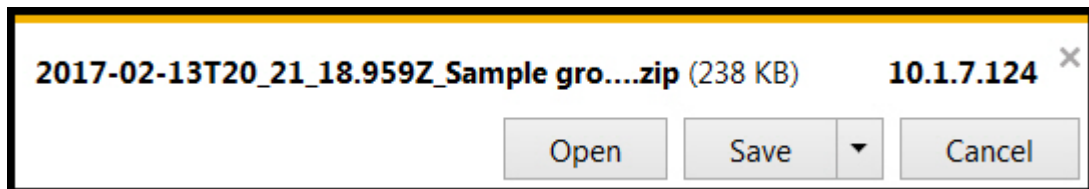
To activate the Select All feature, select the box at the header. This check box can also be used to clear you selections.



Conversely, you can click specific check boxes to customize the download. The check box selection can be toggled.

2. Select **Bulk Download** to initiate the download.

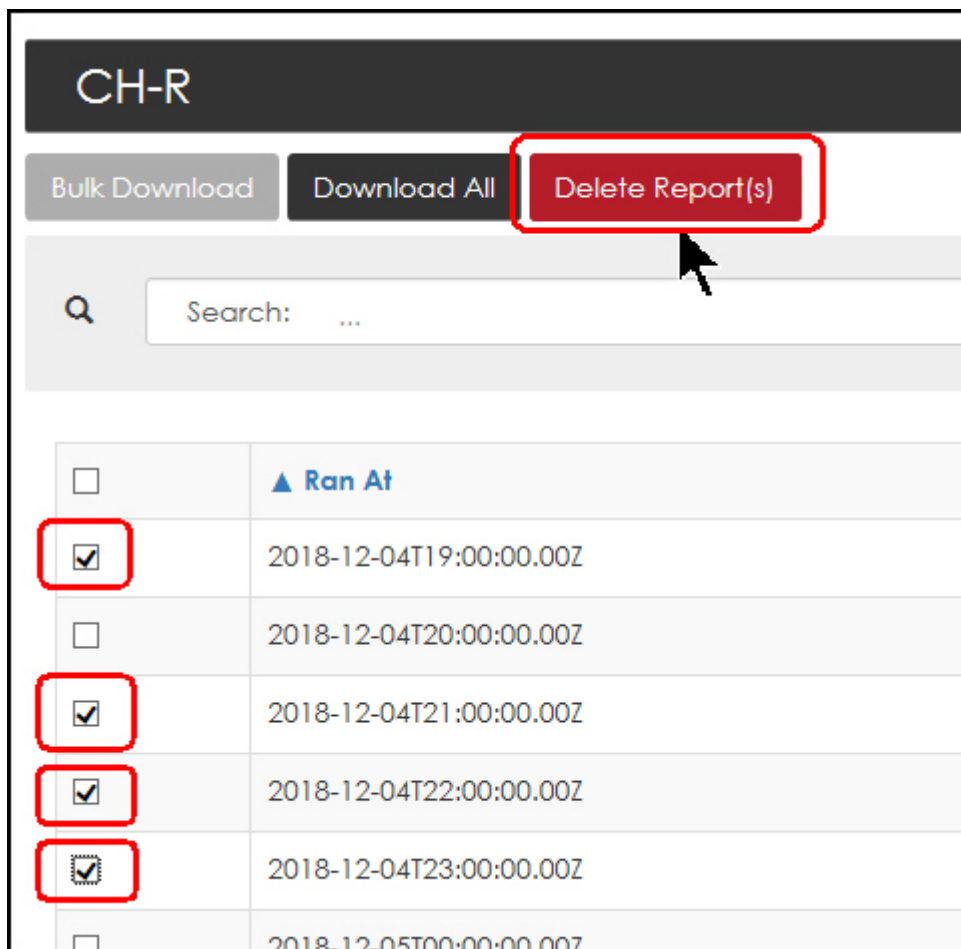
The system prompts with (example):



3. Select your preference.

10.2.3. Deleting Reports

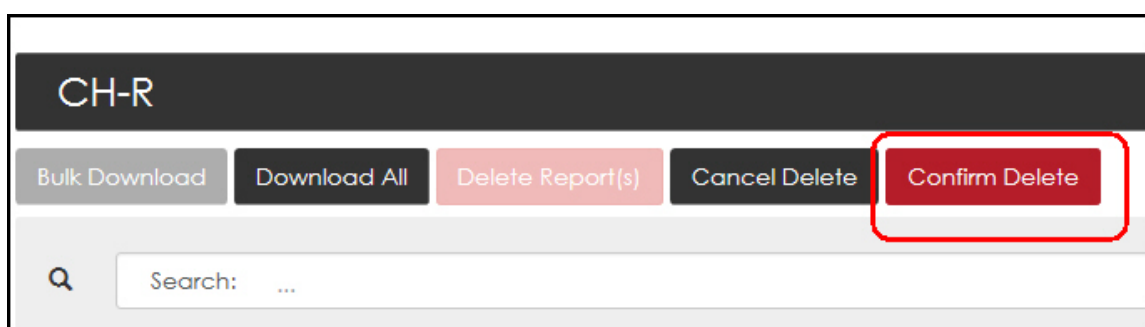
1. Select the report(s) to be deleted.



Once the check box is selected the **Delete Report(s)** option activates.

2. Select **Delete Report(s)**.

The system prompts for confirmation.



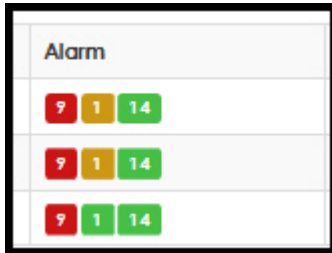
3. Select **Confirm Delete**.

11. Alarms

11.1. General Description

Alarms events must be acknowledged before they can be cleared. Until an alarm is acknowledged it remains reported in the alarm totals.

For example:



Alarm		
9	1	14
9	1	14
9	1	14

Alarms can be monitored actively and historically.

Active alarms (unacknowledged alarms) appear on the main menu by clicking on the icon that looks like an exclamation.



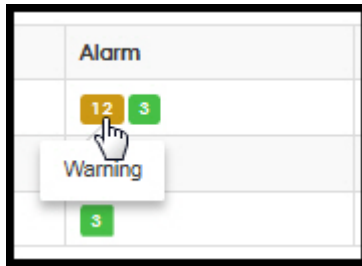
When there are any active alarms, this icon changes color to indicate the highest alarm active.

Select the **Alarms** tab, in the main menu, to view **Alarm History**.

Alarms can always be exported, by selecting Export Alarm History (CSV) from the Alarm History page.

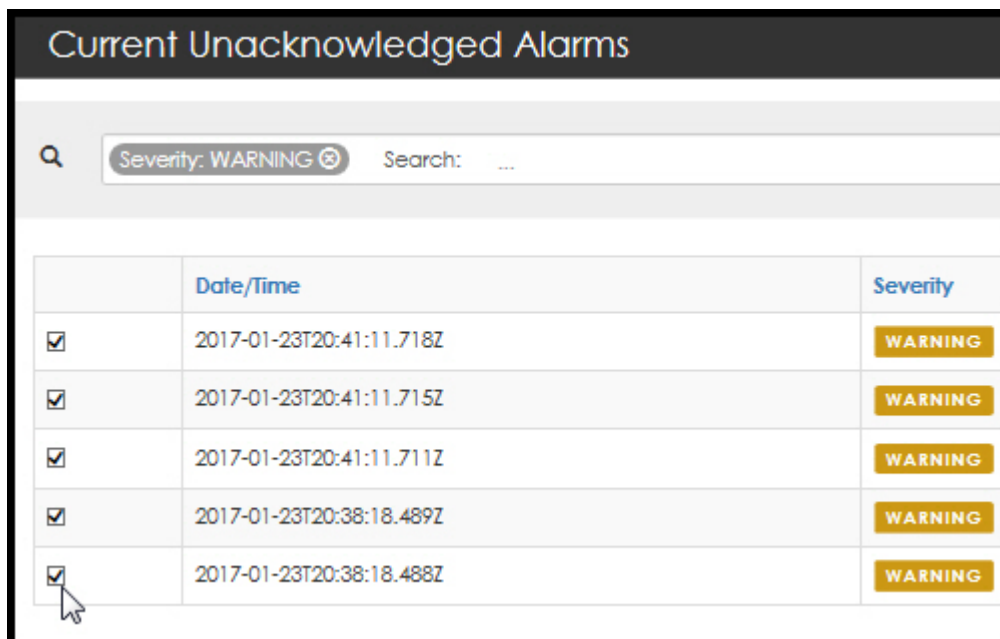
11.2. Acknowledging Alarms in Bulk

1. From any Alarm count column, select (i.e., click on) the alarm total.

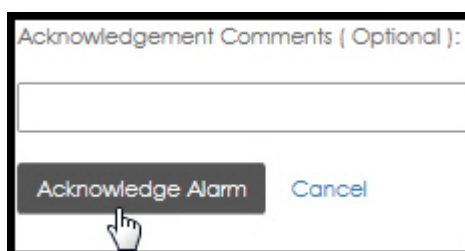


The **Current Unacknowledged Alarms** page opens.

2. Select all the alarms that you want to acknowledge.



3. Select **Acknowledge Alarm**.



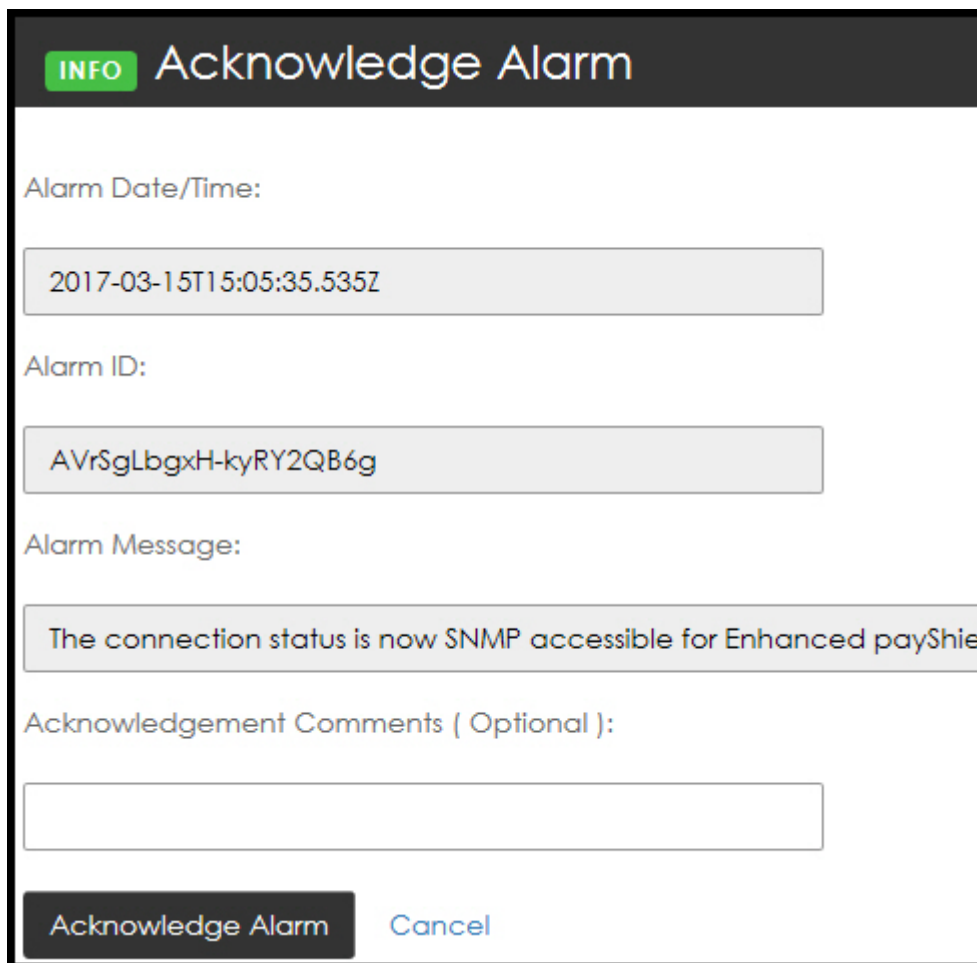
11.3. Acknowledging an Alarm (individual basis)

1. Navigate to: **Alarms > Alarm History**

The **Alarm History** page opens.

2. Select (i.e., single click) on the alarms severity level.

The **Acknowledgment Alarm** page opens.



INFO Acknowledge Alarm

Alarm Date/Time:
2017-03-15T15:05:35.535Z

Alarm ID:
AVrSgLbgxH-kyRY2QB6g

Alarm Message:
The connection status is now SNMP accessible for Enhanced payShie

Acknowledgement Comments (Optional):

Acknowledge Alarm Cancel

3. Enter any Acknowledgment Comments in, if needed.
4. Select **Acknowledge Alarm**.

The **Alarm History** page opens.

5. Select Export Alarm History (CSV). The file can now be saved or opened.

The system prompts asking if you would prefer to Open or Save the .csv file.

6. Select your preference.



Open Save ▼

12. nShield CLI Commands

12.1. GUI initialization

Upon the startup of the nShield Monitor Virtual Appliance, the CLI will wait for the GUI to finish initializing (at the first boot and every reboot). This operation can take up to 60 seconds. If GUI initialization is not completed by then, the user is logged out and asked to log back in later.

12.2. Setting Password

If you are using the One Time Password (OTP), you will be asked to change it after logging in and before accessing any of the CLI operations.

You are prompted with the following password requirements:

- Length should be between eight and sixteen characters
- Should contain at least two capital letters
- Should contain at least two lower case letter,
- Should contain at least two digits
- Should contain at least two special characters

1. Enter the old password.
2. Enter the new password.



The new password is checked for the requirements above and compared with the old password. If it fails to comply with the requirements or if the new password is the same as the old one, the user is prompted with the associated error and/or the requirements and is directed back to step 2.

3. Enter the password confirmation.

The only check that is performed is whether the two passwords match.

If it fails, it will prompt the error and start from step 2 above.

If it is successful, you will proceed to the CLI commands of the wizard.

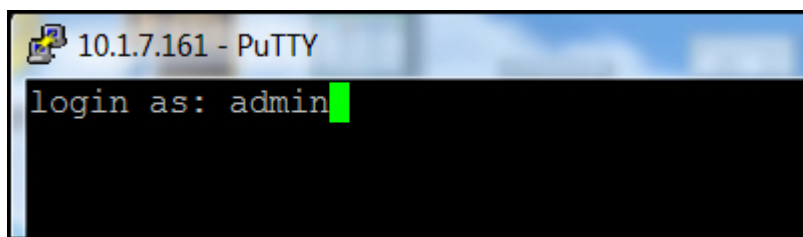
12.3. Master key status

After the setup wizard has run and the mandated passwords have been entered, a status message for the master key is prompted if the master key needs to be reloaded, or generated and loaded.

12.4. CLI Setup Wizard

12.4.1. Log in

1. Connect to the IP address.
2. Login as administrator.



The CLI Setup Wizard initializes at the first boot. It will only initialize if the entire wizard setup has not yet run, or if the following steps of the wizard failed: **Set User Email**, or **Create Administrators**.

The wizard prompts you to perform the following operations:

- Set the user's email
- Create two administrators
- Configure the network
- Configure the date and time
- Set two passwords for system key

Once the user logs in, the CLI verifies if the Virtual Machine (VM) has an IP address. If it does, it will prompt the user with the IP address and the URL to launch the wizard from a web browser.




If the Virtual Machine (VM) does not have an IP address, the CLI will prompt the user to set the static network configuration before running the Wizard. Until the IP address is set, the user will not be able to run the Wizard.

12.5. Welcome

1. Select **y** to start the CLI Setup Wizard.

```
Start CLI Setup Wizard ? [y/n] █
```

 | Select **n** if you need to exit and logout.

12.6. EULA

The EULA is displayed one page at a time.

1. Navigate the EULA:
2. Scroll up and down the page using up and down arrows
3. Select **Enter** to scroll down the page
4. Enter **q** to quit EULA at any time
5. Scroll all the way down the page, which will automatically closes the EULA
6. Select **y** to agree to the terms of the EULA.

```
Agree with the terms ? [y/n]
```

 | Select **n** if your need to exit and logout (after 5 seconds).

The system prompts to set the default user email.

12.7. Set User's Email

```
*****  
|Welcome|EULA| *Email* |System Admins|Network|Key  
  
SET THE DEFAULT USER'S EMAIL  
  
Email:  
█
```

The requirements for an email address are:

- Alphanumeric characters and < - or _ or .>@<alphanumeric characters and < - or .>
- The two parts before and after the "@" cannot start or end with a non-

alphanumeric character.

- The email cannot contain successive dots, dashes or underscores.
1. Enter your email address.
 2. Re-enter your email address to confirm.

The system prompts to create your Administrators.

12.8. Create Administrators

```
CREATE ADMINISTRATORS
* Administrator One *
User Name:
█
```

1. Enter the User Name for Administrator One.
2. Enter the first administrator's email address; verify that the email address is valid.
3. Enter the first administrator's email address confirmation; verify that the email addresses match.
4. Repeat steps 1 through 3 above to create second administrator.

Once the administrators are created, the system prompts for network configuration.

12.9. Configure Network

```

*****
|Welcome|EULA|Email|System Admins| *Network* |Key Generat
*****

      NETWORK SETTING

configuration ..: dhcp
ip .....: 192.168.17.197
netmask .....: 255.255.248.0
gateway .....: 192.168.16.20
hostname .....: localhost
primary DNS ...: 192.168.17.79
secondary DNS ..: 192.168.17.80
domain name ...: localdomain
interface.....: eth0

```

The wizard will show the current network configuration.

1. Select the network configuration.

```

*****
|Welcome|EULA|Email|System Admins| *Network* |Key Generation|
*****

      NETWORK SETTING

configuration ..: dhcp
ip .....: 192.168.17.197
netmask .....: 255.255.248.0
gateway .....: 192.168.16.20
hostname .....: localhost
primary DNS ...: 192.168.17.79
secondary DNS ..: 192.168.17.80
domain name ...: localdomain
interface.....: eth0

Select the type of network configuration.
1) DHCP
2) Static
3) Keep the current configuration

Type number corresponding to configuration type: _

```

2. If DHCP, enter:

- hostname (optional)
- mail host (optional)
- Interface (optional)



Interface can be skipped by pressing enter (system defaults)

| to eth0).

3. If Static, enter:

- hostname (mandatory)
- IP (mandatory)
- netmask (mandatory)
- gateway (mandatory)
- domain (optional)
- primary DNS (optional)
- secondary DNS (optional)
- mail host (optional)
- Interface (optional)



Interface can be skipped by pressing enter (system defaults to eth0).

4. To Keep the current configuration, enter: mail host(optional)

The system continues with Master Key Generation and prompts you to create Passphrase One.

12.10. Generate System Key

1. Enter Passphrase One and then re-enter to confirm.

The system prompts for Passphrase Two.

2. Enter Passphrase Two and then re-enter to confirm.

```

Password requirements are:
- Should have length between 8 and 16 characters
- Should have at least 2 capital letters (A-Z)
- Should have at least 2 lower case letters (a-z)
- Should have at least 2 numbers (0-9)
- Should have at least 2 special characters (@ ! $ & % +
[ ] ( ) - _ ` ~ * = | ; " , < >)

Passphrase One: █

```

The system prompts to configure date and time.

12.11. Configure Date & Time

```
*****
|Welcome|EULA|Email|System Admins|Network|Key Generation|
DATE/TIME SETTINGS

ntp enabled.....: no
date/time.....: Thu 2017-06-08 17:41:59 GMT
timezone.....: GMT
day light saving status..: n/a

Select type of date and time configuration.
1) NTP (dynamic configuration)
2) Manually configure date, time and timezone.

Enter number corresponding to configuration type: █
```

1. Choose between NTP and NTP Disable (manual configuration).
 - Enter **1** or **2** based on your preference:
 - Enter: **1** for dynamic configuration (NTP enabled)

Follow the prompts to complete the configuration.
2. Enter servers (this is only optional if a server is already configured, otherwise this is mandatory).

```

|Welcome|EULA|Email|System Admins|Network|Key Generation|
DATE/TIME SETTINGS

ntp enabled.....: no
date/time.....: Thu 2017-06-08 17:41:59 GMT
timezone.....: GMT
day light saving status..: n/a

Select type of date and time configuration.
1) NTP (dynamic configuration)
2) Manually configure date, time and timezone.

Enter number corresponding to configuration type: 1

NTP Servers:
Use quotes for adding several servers.
Eg.: "server.one server.two"
2
Do you want to set the timezone ? [y/n] 

```

- Check for server regular expression.
- Select timezone (optional).



Each parameter is checked. If a failure occurs, you are prompted to re-enter the parameter.

1. Enter **2** for manual configuration (NTP disabled)

```

DATE/TIME SETTINGS

ntp enabled.....: no
date/time.....: Mon 2017-05-01 18:29:43 GMT
timezone.....: GMT
day light saving status..: n/a

Select type of date and time configuration.
1) NTP (dynamic configuration)
2) Manually configure date, time and timezone.

Enter number corresponding to configuration type: 2

Date (optional): [YYYY-MM-DD]

```

2. Follow the prompts to complete the configuration:

```
Type number corresponding to search type:2
 2) Search by region
1) Africa          5) Atlantic        9) Europe
2) America         6) Atlantic Time   10) GMT
3) Australia       7) Central Time    11) Mountain Time
4) Asia            8) Eastern Time    12) Pacific

Invalid entry - please select from available list of region(s)
 2) Search by region
1) Africa          5) Atlantic        9) Europe
2) America         6) Atlantic Time   10) GMT
3) Australia       7) Central Time    11) Mountain Time
4) Asia            8) Eastern Time    12) Pacific
```

- Enter date (optional)
- Enter time (optional)
- Select timezone (optional)



Each parameter is checked. If a failure occurs, you are prompted to re-enter the parameter.

The system now prompts for initialization.

12.12. Initialize

```
*****
|Welcome|EULA|Email|System Admins|Network|Key Ger
*****
          READY TO SETUP

Initialize to complete the setup process and laur
ication.
When the configuration is complete, the CipherTru
eboot.
Initialize ? [y/n]
```

1. Select **y** to start performing all operations.



Select **n** if you need to log out.

The initialization process is performed in the following order:

- Generate and load master key.

- Set user's email (if this fails, it will log out after five seconds).
- Create administrators (if this fails, it will log out after five seconds).
- Set mailhost.
- Configure network.
- Set NTP (on/off). Configure date, time and timezone and/or NTP servers.

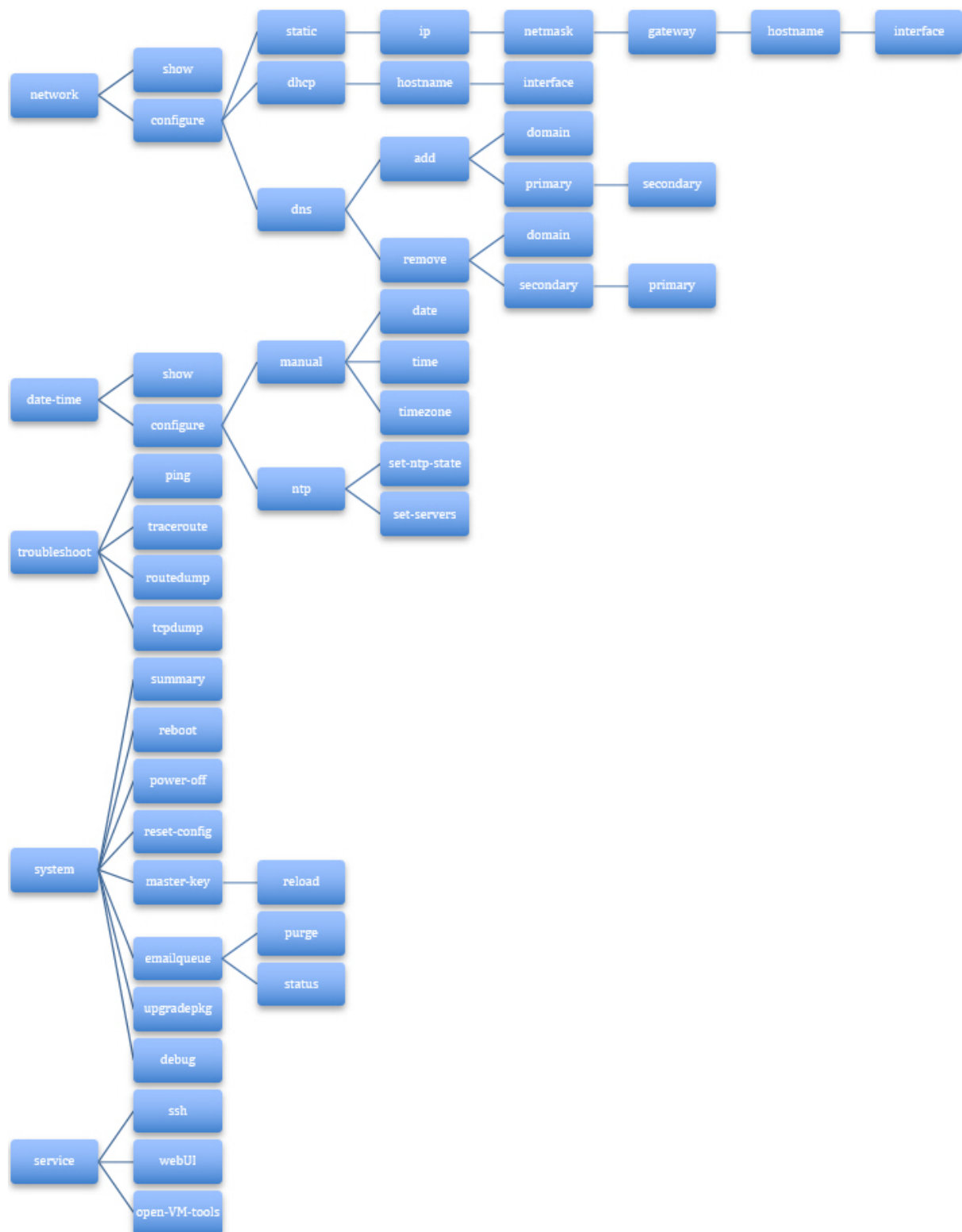
If the date-time configuration is successful, a reboot is triggered.



You can log back in and restart the wizard if:

- Initialization failed
- Initialization was interrupted before setting **Date/Time** and **Network**
- You logged out before initialization.

12.13. CLI Commands



12.14. Network commands

Action	Show current network configuration.
Input	<code>> network show</code>
Output	Mode (dhcp or static) IP address Netmask Gateway Host Name Primary DNS IP Secondary DNS IP Domain Name Mail Host (if any) Interface (if any)

Action	Configure dynamic network.
Input	<code>> network configure dhcp hostname <hostname> interfacename <interface></code>
Details	Hostname is optional. Interface is optional.

Action	Configure static network.
Input	<code>> network configure static hostname <hostname> ip <ip> netmask <netmask> gateway <gateway> interfacename <interface></code>
Details	All parameters are mandatory. Interface is optional.

Action	Add/overwrite DNS parameters.
Input	<pre>> network configure dns add domain <domain name> primary <primary dns> secondary <secondary dns> interfacename <interface></pre>
Details	<p>Commands to set domain name and primary DNS/secondary DNS can be performed separately or together in one command.</p> <p>Only prompt for secondary if primary is entered to ensure that primary DNS is not left blank.</p> <p>Interfacename is optional</p>

Action	Remove DNS parameters.
Input	<pre>> network configure dns remove domain <domain name> primary <primary dns> secondary <secondary dns> interfacename <interface></pre>
Details	<p>Commands to remove domain name and primary DNS/secondary DNS can be performed separately or together in one command.</p> <p>Only prompt for primary if secondary is entered to ensure that primary DNS is not left blank.</p> <p>If the domain name is removed, it will be replaced by « localdomain »</p> <p>Interface name is optional.</p>

12.15. Date-time commands

Date-time configuration triggers system reboot if configuration has succeeded.

Action	Show date and time configuration.
Input	<pre>> date-time show</pre>
Output	<pre>NTP enabled : <yes/no> Date/time Timezone Day light saving status : <yes/no> NTP server list (if any)</pre>

Action	Switch NTP on or off.
Input	<code>> date-time configure ntp set-ntp-state <on/off></code>
Details	<p>set-ntp-state is mandatory. Set it to « on » to enable NTP and set it to « off » to disable NTP.</p> <p>If enabled, NTP will try synchronizing with NTP servers. If it fails, it will remain disabled.</p> <p>Note: check with « date-time show » command if any servers were configured.</p>

Action	Set NTP servers.
Input	<code>> date-time configure ntp set-servers <"list of servers"></code>
Details	<p>This command removes all previous servers (if any) sets the new list of servers.</p> <p>In CLI, provide the list of servers between double quotes. If there is only one server then there is no need for quotes.</p> <p>Examples :</p> <pre>date-time configure ntp set-servers us.pool.ntp.org date-time configure ntp set-servers "us.pool.ntp.org time.nist.gov"</pre>

Action	Configure date and time manually.
Input	<code>> date-time configure manual date <date> time <time> timezone <select from list></code>
Details	<p>NTP has to be disabled to perform this operation.</p> <p>Commands to set date, time and timezone can be performed separately or together in one command.</p>

12.16. System Commands

Action	Power-off the system.
Input	<code>> system power-off</code>
Details	This operation can take up to 60 seconds.

Action	Reboot the system.
Input	<code>> system reboot</code>
Details	This operation can take up to 60 seconds.

Action	Reset the system to factory settings.
Input	<code>> system reset-config</code>
Details	Stop database services. Remove data. This operation can take up to 60 seconds.

Action	Show summary of system information.
Input	<code>> system summary</code>
Details	SSH state indicates only the user's configuration for SSH through the CLI (« service ssh enable/disable » command.) <ul style="list-style-type: none"> • 'enable': if user configured SSH using « service ssh enable » • 'disable': if user configured SSH using « service ssh disable »
Output	Serial Number Software Version System Uptime Disk Usage Services status License Type : Evaluation/Product. If evaluation then show remaining days. Upgrade history (if any) SSH state Web UI state

Action	Reload Master Key.
Input	<code>> system master-key reload</code>
Details	Reload master key when master key is generated but not loaded. Master key has to be reloaded after each reboot.

Action	Show current state of debug.
Input	<code>> system debug show</code>
Details	Show current state of debug

Action	Enable logging of debug message
Input	<code>> system debug configure set-debug-state on</code>
Details	Enable debug logging

Action	Disable logging of debug message
Input	<code>> system debug configure set-debug-state off</code>
Details	Disable debug logging

12.17. Email Queue Commands

Action	Show the out standing emails queued up in the system
Input	<code>> system emailqueue status</code>
Output	EMAIL QUEUE SUMMARY Pending mail requests : nn
Action	Purge system email queue
Input	<code>> system emailqueue purge</code>
Output	EMAIL QUEUE PURGE STATUS Mail purge status : success

12.18. Troubleshooting Commands

Action	Ping host name or IP address
Input	<code>> troubleshoot ping <ip address/hostname></code>

Action	Traceroute host name or IP address
Input	<code>> troubleshoot traceroute <ip address/hostname></code>
Details	This operation may take up to 450seconds (7.5min)

Action	Show routing tables.
Input	<code>> troubleshoot routedump</code>

Action	Dump traffic on the network to a file.
Input	<code>> troubleshoot tcpdump <on/off></code>
Details	The file is overwritten everytime tcpdump is turned on.

Action	Export debug logs through SCP.
Input	<pre>> troubleshoot export_logs server <IP> username <name> dest_dir <destination path> port <optional_port_number></pre>
Optional	port and debug_db_data are optional parameters
Details	This command is used to export debug logs using SCP. The users should have valid access to SCP server with username and destination directory. Port number is optional and the default SCP port would be used if not provided. User is prompted to enter correct password after executing the command.

12.19. Service Commands

Action	Enable/Disable SSH.
Input	<pre>> service ssh <enable/disable></pre>
Details	By default, it is disabled as well as after each reboot.

Action	Enable/Disable webUI.
Input	<pre>> service webUI <enable/disable></pre>

Action	Enable/Disable OVT
Input	<pre>> service open-vm-tools enable This will enable Open VMware Tools. Proceed? [y/n]</pre>



CLI access is restricted to Administrator accounts only. Manager accounts cannot access the CLI. A proper error message will be displayed.

13. Licensing

13.1. Introduction

The nShield Monitor Virtual Appliance offers several license options as listed below.

License Options

Order Code	Description
nShield Monitor monitoring software licenses for installation onto customer-supplied workstation or PC.	
NT-SW-V2S	nShield Monitor software license - single
NT-SW-V2D	nShield Monitor software license - dual
NT-SW-V2E	nShield Monitor software license - Enterprise
NT-LIC-ADD50	Adds additional 50 endpoints
nShield (endpoints) to be monitored. A maximum of 500 endpoints per monitoring software license is available.	
NT-LIC-ADD5	nShield Monitor endpoint license - 5 additional
NT-LIC-ADD10	nShield Monitor endpoint license - 10 additional
NT-LIC-ADD20	nShield Monitor endpoint license - 20 additional
NT-LIC-ADD50	nShield Monitor endpoint license - 50 additional
NT-LIC-ENTERPRISE	nShield Monitor endpoint license - Enterprise (500 endpoints valid for NTM 2.5 and later, 300 endpoints for NTM 2.4.1 and earlier)
Post-installation upgrades	
NT-DVD-V2	nShield Monitor installation image on DVD
NT-LICU-S2D	Upgrade from single to dual license
NT-LICU-S2E	Upgrade from single to Enterprise license
NT-LICU-D2E	Upgrade from dual to Enterprise license

14. Enterprise Firewall Settings

If the nShield Monitor appliance is separated from any of its services (for example, NTP, DNS, SMTP server) or endpoints (for example, users devices) by a firewall, you must configure the firewall to allow passage of the appropriate IP protocols.

The table in this section lists the ports that, at a minimum, you must configure to support connectivity.

Port Configurations

Protocol	Transport	Port	Direction	Description
Echo1	N/A	N/A	Both	Echo/ICMP Pings
SSH	TCP/UDP	22	Inbound	nShield Monitor Remote Console Management
HTTPS	TCP	443	Both	nShield Monitor Web UI & firmware upgrade
DNS	TCP/UDP	53	Outbound	nShield Monitor Web UI & firmware upgrade DNS
NTP	UDP	123	Outbound	nShield Monitor utilization of Network Time Protocol
SNMP	UDP	161	Outbound	Monitoring devices via SNMPV3
SNMP	UDP	162	Outbound	SNMPV3 Notification
System Log	UDP	514	Outbound	Remote system log alerts
SMTP	TCP	25	Outbound	nShield Monitor sending email alerts
FTP	TCP	21	Both	nShield Monitor firmware upgrade option
HTTP	TCP/UDP	80	Outbound	nShield Monitor firmware upgrade option
Echo Reply			Both	ICMP Response (code 0)
Echo Request			Both	ICMP Request (code 8)

15. Troubleshooting

This appendix describes nShield Monitor troubleshooting information.

15.1. Global Troubleshooting Enhancement feature

15.1.1. Overview

HSMs, nShield Monitor (NM) Servers, and nShield Monitor users can be globally dispersed crossing multiple time zones. nShield Monitor stores all collected HSM events in Greenwich Mean Time (also referred to as nShield Monitor Server time). Users who remotely log into nShield Monitor see NM information displayed in the local time zone of their browser.

The Global Troubleshooting Enhancement feature allows users, logged into nShield Monitor from various time zones around the world, to select and view nShield Monitor Log and Alarms in a common agreed upon Timezone. This ability is helpful during global troubleshooting discussions.

15.1.2. Procedure

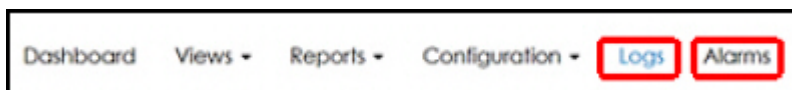
Prerequisite:

You are logged into nShield Monitor.



Just for the duration of a special global collaboration work-session, a logged in user can choose a SELECTED time zone for viewing Logs and Alarms on their browser connected to nShield Monitor.

1. Navigate to either the **Logs** tab or the **Alarms** tab.



2. Go to the Date/Time drop down.



3. Select your preferred time zone.

Notes:

- The setting applies to both Alarms and Logs tabs (i.e., you only have to select the time zone once).
- ONLY the time zone displayed in these two tabs will be affected by this selection (nShield Monitor displays on the other nShield Monitor tabs are NOT affected).
- The default time zone in Logs and Event pages are browser 'Local Time' unless the Date/Time Format is set to UTC in User Profile, and in such case, the default time zone is GMT.
- The time zone change is NOT persisted across user logout/login. The time zone change is temporary. The next time that you login, the time zone is reset to the default 'Local Time' which is the default (or UTC if the Date/Time Format is UTC in the login User Profile).
- The Time Zone customization in Logs/Alarms pages does NOT affect Date/Time in other WebUI pages, including Charts, Export Logs, etc. All other WebUI pages display Date/Time in 'Local Time' Time Zone (or UTC if the Date/Time Format is UTC in the login User Profile).

15.2. Network test tools

Event logs provide additional information about security and operations issues.

The following networking test tools are available through the CLI to facilitate nShield Monitor inter-networking tests.

- Ping
- RouteDump
- TCPDump
- Traceroute

To run the nShield Monitor Network test tools:

1. Log into the CLI as an **Administrator**.
2. Enter the command: **troubleshoot**
3. Press **Enter** or **Tab** to display available options as follows:

```
nShield Monitor > troubleshoot
ping routedump tcpdump traceroute
```

```
nShield Monitor > troubleshoot
```

4. Type one of the four options to run the appropriate test tool.

15.3. Ping

Ping is a pass-fail continuity test that determines the accessibility of a target IP address on an IP network. It sends ICMP echo request packets from the selected nShield Monitor Management Interface to the specified target IP address and waits for an ICMP response.

15.3.1. Using Ping

1. Log into the CLI as an **Administrator**.
2. Enter the command:

```
troubleshoot ping <Hostname or IP Address to ping>
```

3. Press **Enter**.

Ping output is displayed directly on the CLI screen. If the ping returns successfully, the network statistics and properties display appear. If the ping does not return, a failure message appears.

Example: Success case


```
*****
PING:
PING 10.1.1.14 (10.1.1.14) from 10.1.2.122 eth0: 56(84) bytes of data
64 bytes from 10.1.1.14: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 10.1.1.14: icmp_seq=2 ttl=255 time=0.273 ms
64 bytes from 10.1.1.14: icmp_seq=3 ttl=255 time=0.319 ms
64 bytes from 10.1.1.14: icmp_seq=4 ttl=255 time=0.287 ms
64 bytes from 10.1.1.14: icmp_seq=5 ttl=255 time=0.259 ms
64 bytes from 10.1.1.14: icmp_seq=6 ttl=255 time=0.197 ms
64 bytes from 10.1.1.14: icmp_seq=7 ttl=255 time=0.257 ms
64 bytes from 10.1.1.14: icmp_seq=8 ttl=255 time=0.256 ms
--- 10.1.1.14 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7000ms
rtt min/avg/max/mdev = 0.197/0.264/0.319/0.038 ms
*****
```

Example: Not Successful

```
*****
PING:
PING 10.1.1.131 (10.1.1.131) from 10.1.2.122 eth0: 56(84) bytes of data
From 10.1.2.122 icmp_seq=1 Destination Host Unreachable
From 10.1.2.122 icmp_seq=2 Destination Host Unreachable
From 10.1.2.122 icmp_seq=3 Destination Host Unreachable
From 10.1.2.122 icmp_seq=4 Destination Host Unreachable
From 10.1.2.122 icmp_seq=5 Destination Host Unreachable
From 10.1.2.122 icmp_seq=6 Destination Host Unreachable
From 10.1.2.122 icmp_seq=7 Destination Host Unreachable
From 10.1.2.122 icmp_seq=8 Destination Host Unreachable
--- 10.1.1.131 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 700
pipe 4
*****
```

15.4. RouteDump

RouteDump displays routing information used by nShield Monitor.

15.4.1. Using RouteDump

1. Log into the CLI as an **Administrator**.
2. Enter the command: `troubleshoot routedump`
3. Press **Enter**.

The routing information for nShield Monitor is displayed on the screen.

```

*****
ROUTEDUMP:
default via 10.1.1.20 dev eth0 proto static metric 1024
10.1.0.0/21 dev eth0 proto kernel scope link src 10.1.2.122
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Re
Use Iface
default          10.1.1.20      0.0.0.0         UG    1024  0
0 eth0
10.1.0.0         0.0.0.0        255.255.248.0  U     0      0
0 eth0
*****

```

15.5. TCPDump

TCPDump is a common packet analyzer that allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

Using the CLI commands `tcpdump on` and `tcpdump off`, the utility can be turned on and off.

15.5.1. Using TCPDump

1. Log into the CLI as an **Administrator**.
2. Turn on TCPDump.
3. Enter the command:

```
troubleshoot tcpdump on
```

4. Press **Enter**.

The utility starts capturing.

Each Interface TCPDump capture generates a trace file. The TCPDump trace file can only be exported as part of exporting debug logs.



Restarting the TCPDump capture overwrites any previously captured data.

15.6. Traceroute

Traceroute determines network response time, displays route (path) information from an IP source to an IP destination address, and measures the associated transit delays of packets across the network. It operates by sending a sequence of ICMP packets from a specified source IP address to a specified destination IP address, and uses responses to determine the intermediate routers traversed.

15.6.1. Using Traceroute

1. Log into the CLI as an **Administrator**.
2. Enter the command:

```
troubleshoot traceroute <Hostname or IP Address>
```

3. Press **Enter**.

Traceroute output is displayed directly on the CLI. The last Traceroute operation performed can also be exported as part of the debug logs.

```
*****
It may take up to 450 seconds to complete the operation.
Ctrl-c to stop the process.
TRACEROUTE:
  traceroute to 172.26.0.10 (172.26.0.10), 30 hops max, 60 byte
packets
 1  10.1.1.20 (10.1.1.20)  0.750 ms  0.801 ms  0.865 ms
 2  172.26.0.10 (172.26.0.10)  0.510 ms  0.529 ms  0.527 ms
*****
```

15.7. No Monitoring Data Received

If no Monitoring Data is received or if a device is not reachable, verify that:

- SNMP is enabled
- SNMPv3 user is configured
- Utilization and health collection is enabled.

16. nShield Monitor Alarm Conditions

nShield Monitor provides the following alert conditions for monitoring and tracking system and device level conditions:

Alarm Condition	Alarm Severity	Notes
Device is added or removed	Added: INFO Deleted: Warning	System Alarm - nShield Monitor Alarm gets generated by nShield Monitor when a device gets enrolled or deleted from the system. Add operation will create an INFO alarm and delete of enrolled device reported as WARNING.
When the nShield Monitor average CPU usage is higher than 95%	ERROR	System Alarm - nShield Monitor This is a health alert for nShield Monitor, when the average CPU usage is higher than 95%. nShield Monitor will not shut down. Send debug logs to your Support organization.
nShield Monitor License Expiry alerts	WARNING CRITICAL EMERGENCY	System Alarm - nShield Monitor nShield Monitor will keep sending alerts with different severity a few days before expiration. A WARNING alert message will be sent out every day from 23rd day to 28th day. CRITICAL alert will be sent out on 29th day and EMERGENCY alert will be sent out on 30th day. Emergency alert is the final alert before the evaluation license expires. User needs to install valid license at this point for nShield Monitor to monitor the devices.
When the nShield Monitor Memory is over 90% full	ERROR	System Alarm - nShield Monitor This Alarm gets generated when system memory gets 90% full. At this point, nShield Monitor does not stop monitoring or shut down. The system will continue with normal operation.

Alarm Condition	Alarm Severity	Notes
When the nShield Monitor disk is over 90% full	ERROR	<p>System Alarm - nShield Monitor</p> <p>This Alarm gets generated when system disk gets 90% full. At this point nShield Monitor does not stop monitoring or shut down. The system will continue with normal operation. Follow this link to find disk size recommendations Server Requirements.</p> <p>Add storage space by expanding the virtual hard disk.</p>
nShield Monitor Security Related Alarm Warning when Master key has not be generated and Critical when Master key is not loaded	WARNING CRITICAL	<p>Security Alarm - nShield Monitor</p> <p>It is a security alarm regarding master key not being generated or not being loaded. If key is not generated a WARNING message and CRITICAL when MK is not loaded. Administrator needs to take appropriate action by configuring the same on Security page.</p>
nShield Monitor Security Related Alarm User: has enabled/disabled Service	INFO	<p>Security Alarm - nShield Monitor</p> <p>If SSH, WebUI or Open VMTool services are enabled or disabled.</p>
nShield Monitor Security Related Alarm	WARNING CRITICAL	<p>Security Alarm - nShield Monitor</p> <p>It is a security alarm regarding master key not being generated or not being loaded.</p> <p>If the key is not generated a WARNING message is generated and a CRITICAL message is generated when a master key is not loaded.</p> <p>The Administrator needs to take appropriate action by configuring the same on the Security page.</p>
The license features have been changed for Device	INFO	<p>Device Alarm - nShield</p> <p>There are optional feature licenses for the nShield HSM. At a later date, when you require a new feature, you can order it from Sales and install the new License. Change in those featured licenses are going to be monitored by nShield Monitor and notified by an event.</p>

Alarm Condition	Alarm Severity	Notes
The nShield device temperature change alerts	WARNING / CRITICAL	<p>Device Alarm - nShield</p> <p>System reports device temperature change WARNING message when exceeds lower configured threshold value and CRITICAL above upper threshold value.</p>
Hard Server failure in Client Host	WARNING	<p>Device Alarm - nShield</p> <p>A WARNING message would be generated when hard server program fails.</p> <p>Follow Remote Administrator Client User Guide for further investigation.</p>
Module count is Zero for Client Host	WARNING	<p>Device Alarm - nShield</p> <p>When Client host discovers no nShields attached to enrolled Client Host.</p> <p>Follow up with nShield User Guide.</p>
The software base release updated, revision, build number, core API version, performance model update, crypto algorithm host command update and optional license update	INFO	<p>Device Alarm - nShield</p> <p>This is an nShield monitored Event. Event is logged for audit purposes. A Security World software upgrade operation would update revision, build number, core API versions and optional licensing update information etc. No action needed.</p>

Alarm Condition	Alarm Severity	Notes
<p>License count exceeded</p> <div data-bbox="199 331 587 416" style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> Device count license Exceed - NOTIFICATION </div> <div data-bbox="199 456 587 519" style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> Install new License - NOTIFICATION </div> <div data-bbox="199 560 587 645" style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> Device count license exceeds for <N> days - WARNING </div> <div data-bbox="199 685 587 770" style="border: 1px solid gray; padding: 5px;"> Device count license exceeds for <0> days - ALERT </div>	<p>NOTIFICATION / WARNING / ALERT / CRITICAL</p>	<p>System Alarm - nShield Monitor</p> <p>When nShield Monitor detects more nShields (connected to ClientHost) than the permitted “nShield Monitor” License count, nShield Monitor generates this event.</p> <p>When the License count is exceeded, and if a new license (with more HSM count) is not installed after 30 days, ONLY Administrator privilege users of nShield Monitor will be allowed to login.</p> <p>Group Manager Privileged Users won't be allowed to login to nShield Monitor.</p> <p>After 30 days, nShield Monitor will still continue to monitor the detected nShields in the background. Once the new “nShield Monitor” license with a sufficient HSM count is installed, Group Manager Privileged Users are allowed to login.</p>
<p>Client Host does not belong to a security world</p>	<p>WARNING</p>	<p>Device Alarm - nShield</p> <p>When the Client host is not configured correctly with correct security world information, and enrolled for monitoring. WARNING message gets generated. Refer to Remote Administrator Client User Guide.</p>
<p>SoloXC fan speed down to zero</p>	<p>CRITICAL</p>	<p>Device Alarm - nShield</p> <p>This CRITICAL alarm generates when Fan speed for Solo Down to zero or not functioning any more. Refer to nToken Installation Guide if needed.</p>
<p>Power Supply failed for nShield module</p>	<p>WARNING</p>	<p>Device Alarm - nShield</p> <p>This WARNING alarm generates when power supply to nShield module fails.</p> <p>Refer to nToken Installation and Solo installation guide if needed.</p>
<p>Number of nShield discovered by nShield Monitor</p>	<p>INFO</p>	<p>Device Alarm - nShield</p> <p>nShield Monitor generates alarms when client host start discovering nShield configured to it.</p>

Alarm Condition	Alarm Severity	Notes
HSM module hard failure	CRITICAL	Device Alarm - nShield It's an nShield/ClientHost module hard failure event. Customer needs to investigate on Client Host about module failure and refer to Remote Administrator Client User guide suggest how to restart it.
Device State changed to offline	ALERT	Device Alarm - nShield An ALERT alarm is generated when the Device State changes to offline.
Device State changed to online	NOTIFICATION	Device Alarm - nShield A NOTIFICATION alarm is generated when the device state changes to online.
Device State changed to unavailable	ALERT	Device Alarm - nShield An ALERT alarm is generated when the device state changes to unavailable.
Device State changed to secure	NOTIFICATION	Device Alarm - nShield A NOTIFICATION alarm is generated when the device state changes to unavailable.
Device information Modified	NOTIFICATION	System Alarm - nShield Monitor Enrolled device nShield Monitor enrolled device information has been modified. Device Details include Hostname, HostIP, Description, Location; SNMP Details include username, port, Authentication algorithm/password or Privacy algorithm/password or Group membership information.
Device Monitoring Enable/Disable	WARNING	Device Alarm - nShield Monitor Enrolled device WARNING message gets generated when administrator disables or enables monitoring option for enrolled devices.

Alarm Condition	Alarm Severity	Notes
Object Count Notification	INFO / WARNING / CRITICAL	<p>Device Alarm - nShield Monitor Enrolled device</p> <p>WARNING and/or CRITICAL otifications are raised if the object count of any HSM in a defined group exceeds one of the thresholds for a pre-configured period. INFO message gets generated when the object count for that device falls back under the lower threshold value for a pre-configured period.</p> <p>The alert indicates the threshold value, the HSM hostname and IP address or the HSM ESN (if hostname and IP address are not present) and the group that the HSM belongs to.</p>
SNMP Trap Notification	NOTIFICATION / ALERT / CRITICAL	<p>Device Alarm - nShield Monitor Enrolled device</p> <p>nShield Monitor generates alerts and notifications when the SNMP TRAP state changes.</p> <p>ALERT when the state changes to offline or unavailable.</p> <p>NOTIFICATION when the state changes to secure or online.</p> <p>CRITICAL when the connection status is unreachable.</p>

17. nShield Monitor Backup and Restore

To protect against data loss, nShield Monitor should be backed up using native VMware capabilities for protecting virtual machines.

Both manual and scheduled backup operations can be used, as follows:

- After nShield Monitor is installed, setup and configured, a manual backup should be completed.
- Before a nShield Monitor software upgrade is performed, a manual backup should be completed.
- A scheduled backup program should also be setup to provide ongoing protection against loss of monitored data collected.

For details of VMware virtual machine backup and restore capabilities please refer to VMware the Virtual Machine Backup guide and the vSphere Virtual Machine Administration manual.

Please also note the following:

- For your security, Master Key is not persisted in nShield Monitor - you must remember the passwords used for establishment of the Master Key.
- Don't invoke the nShield Monitor backup operation while a nShield Monitor upgrade is in process.

18. Deploying nShield Monitor

18.1. Centralized Monitoring

When monitoring an estate of HSMs, it is recommended to keep all the data in as few instances as allowed by external requirements such as network connectivity, regulatory or other issues.

The best case scenarios are a single nShield Monitor instance that poll all HSMs in an estate. This provides for a complete set of statistics for all HSMs in the estate from a single login based on access rights and role or roles assigned within the nShield Monitor server.

18.1.1. Single Instance Monitoring

By collecting statistics in a single window it allows views of all groups of HSMs including events and alerts from a single browser when logged in as Administrator.

This configuration allows historical reporting for any and all HSMs in the estate as needed, again based on assigned rights or roles.

There may be additional requirements when monitoring must be continuous such that more than one instance of a central nShield Monitor virtual appliance is required in order to ensure monitoring is continuous and non-stop.

18.2. nShield Monitor Multi-Instance

While a single nShield Monitor virtual appliance is all that is required to monitor an HSM estate, it is possible to utilize multiple nShield Monitor virtual appliances simultaneously as insurance in case of an outage. By having more than one nShield Monitor virtual appliance distributed across multiple locations, it is possible to ensure that even in the event of a network outage other than to a single site, polling is maintained to all devices. In fact, it is possible to ensure that even in the event of a single location network failure, at most, only a minimal number of devices will lose the ability to be monitored until such time as the issue is resolved.

18.3. Distributed Monitoring

There are cases where multiple monitors are required due to one or more reasons ranging from network connectivity via firewalls, potential regulatory compliance requirements or some other reason where one or more central nShield Monitor virtual appliances cannot poll specific HSM devices.

18.3.1. Multiple nShield Monitor Instances

In this case, multiple regional or local nShield Monitor instances may be required in order to provide coverage and continuous monitoring of HSM estates.

Even in this case, it is still recommended that a central distribution of alerts using SIEM or email services so that proactive notifications can be sent to the appropriate person or persons responsible for a given nShield Monitor or specific group of devices.

18.4. Deployment Considerations

When looking into how to deploy nShield Monitor, there are some specific items that need to be considered prior to implementation.

18.4.1. User Access Requirements

nShield Monitor has included provisions to address user access requirements by providing the ability to limit which portions of HSM estates any given user can view. This is done by only assigning a specific group or portion of the total configured groups to a user with the group manager role assigned. These requirements may affect both centralized and distributed configurations and a thorough examination of the environment in question will need to be performed prior to implementing nShield Monitor.

There may also be regional requirements for monitoring encryption devices that require regional or local users to be the only authorized persons to access specific portions of the estate due to geographic location.

18.4.2. Network Connectivity

Multiple instances of nShield Monitor may be required on a per region or location basis. This is mainly due to firewalling or other forms of limited network access to the local HSM estates. In this case, individual nShield Monitor systems will have to

be configured individually to achieve full coverage and notification of failures per region or location.

18.4.3. Regulatory Compliance Requirements

nShield Monitor does not have any regulatory impact or requirements around it at this time. However, due to potential regional requirements for the HSM estates, you may be required to have individual nShield Monitor servers deployed regionally in order to access the management ports of the HSMs to be monitored.

To this end, a distributed model of nShield Monitor can still provide the ability to distribute proactive alerts and event information to centralized tools based on configuration at the virtual appliance or HSM group level.

19. Residual Risk

19.1. User Guidance

Deploying organizations should consider these guidelines for secure operation of their systems.

19.2. Secure Operation

This section highlights residual risks that are not completely covered by the technical solution and that may require additional operational or procedural controls.



Refer to Security Hardening: VMWare Infrastructure 3 (VMware ESX 3.5 and VMware VirtualCenter 2.5) (<http://www.vmware.com>) for recommendations for security hardening VMware infrastructure, including virtual machines and virtual machines files and settings.

Deploying organizations may wish to implement additional measures based on their assessment and risk appetite.

19.3. Risks

- Malicious Host
- Misconfiguration
- Data Aggregation
- Data Ex-filtration

19.4. Deployment and Distribution

- Keys and for communication with clients and other Critical Security Parameters (CSPs) such as TLS and SSH certificates are protected in software only and are embedded on the virtual machine.
- Audit data accumulated from monitored clients is only protected by software mechanisms on the virtual instance.
- Virtual machine instances must be managed carefully (including auditing use

and distribution of the virtual instances and controlling access to the host machines).

- Cloning virtual machines with nShield Monitor is not recommended for new deployments (a fresh installation via distribution of the OVA image and reconfiguration is always recommended).

19.5. Secure Configuration

The manual, Security Hardening: VMWare Infrastructure 3 (VMware ESX 3.5 and VMware VirtualCenter 2.5), covers these measures in more depth.

They are repeated here since they are directly relevant to mitigating the outlined risks to nShield Monitor Monitor and can be modified by user operating the virtual machine.

- Secure virtual machines as you would secure physical servers. Anti-Virus, Anti spyware, intrusion detection and other protection must be enabled for the virtual machine. All security measures must be kept up to date including applying appropriate patches.
- Disable Automatic Mounting of USB Devices. This measure is required to prevent introduction of malware to the virtual environment and exfiltration of data.
- Ensure Unauthorized Devices are Not Connected.
- Strictly Control Root Privileges.
- Disable Technical Support Mode.
- Disable Copy and Paste Operations Between the Guest Operating System and Remote Console.

19.6. Host Machine

Must be sanitized as per the deploying organizations policy. Best practices for OS and application security controls are recommended on the host machine to minimize the risks outlined above.

20. Install OVA With VMware ESXi

20.1. Introduction

The nShield Monitor OVA can be installed on a VMware ESXi hypervisor including the following versions:

- vSphere ESXi 6.0
- vSphere ESXi 6.5

For installation of the VMware ESXi hypervisor it may be necessary to involve your vSphere management team if you plan to install this system in a corporate VMware environment and you do not have access/authority to create and manage virtual machines (administrative rights will be required).

It will be required to have access to a DVD or the nShield Monitor OVA file from the machine that has the vSphere software running for proper installation of the Virtual Appliance.



The nShield Monitor OVA has been digitally signed with a signature based on the SHA-256 algorithm. Legacy VMware software, such as the platform-native vCenter client, only supports signatures based on the deprecated SHA-1 algorithm and cannot directly deploy the nShield Monitor OVA. To deploy nShield Monitor to VMware ESXi 5.5 or later, use the vCenter web client.

20.2. Install the nShield Monitor OVA

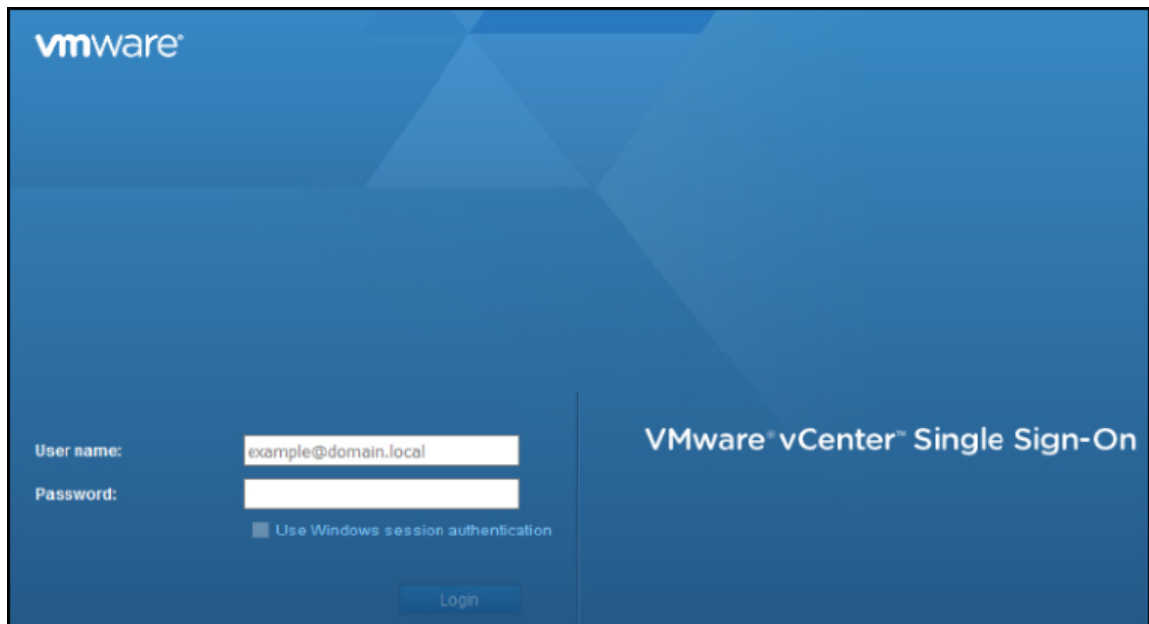


Screen views are based upon vSphere ESXi 6.5.

Run the vSphere software.

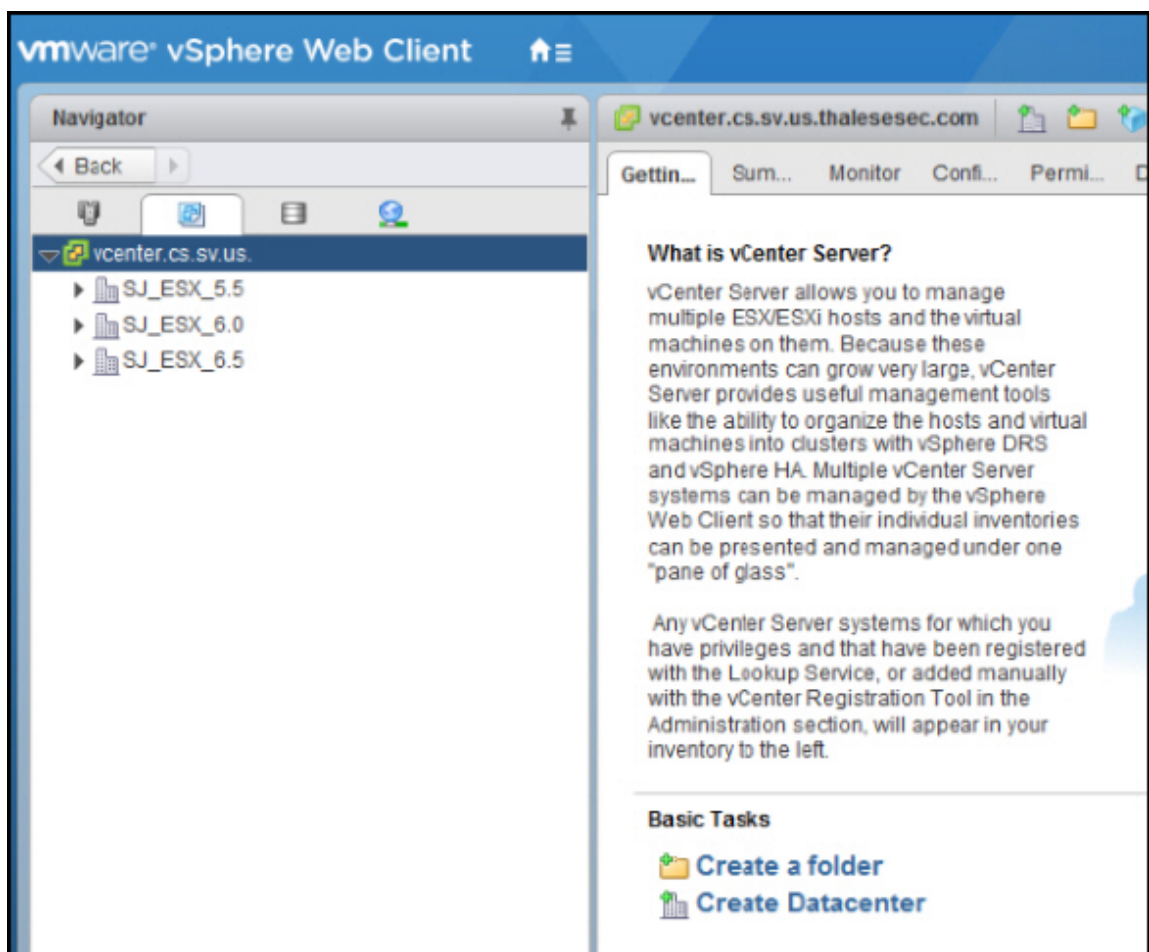
1. Log into the web client.

The initial VMware page opens.

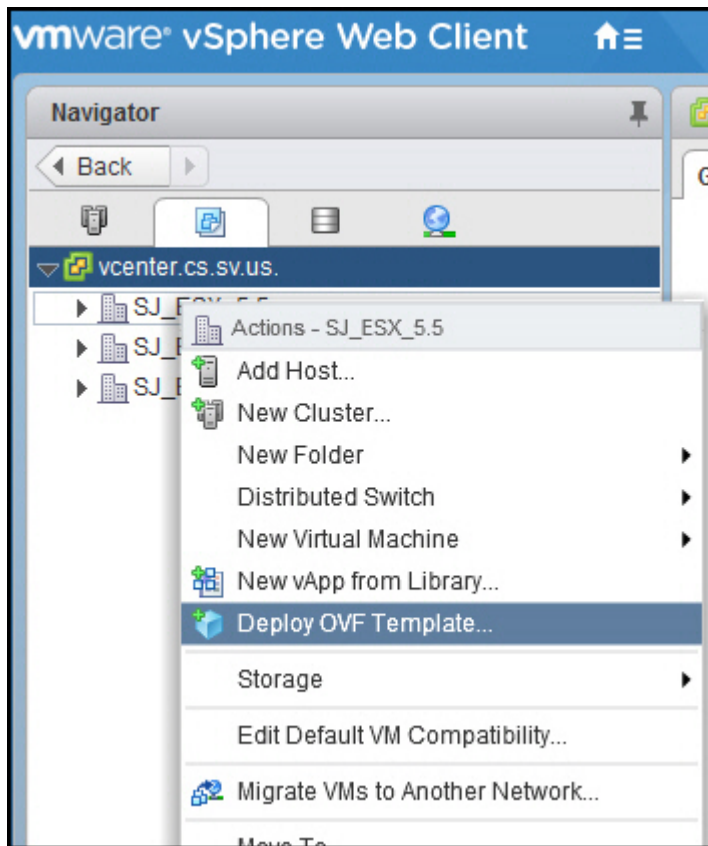


The web client is ready to be deployed.

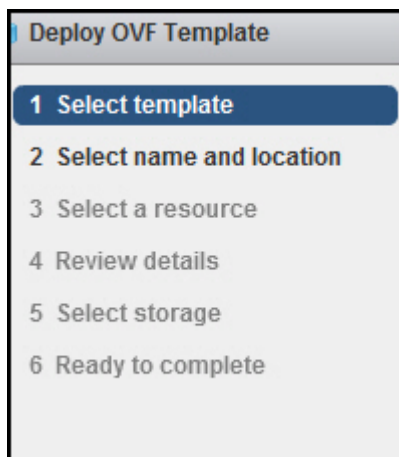
2. Select your version.



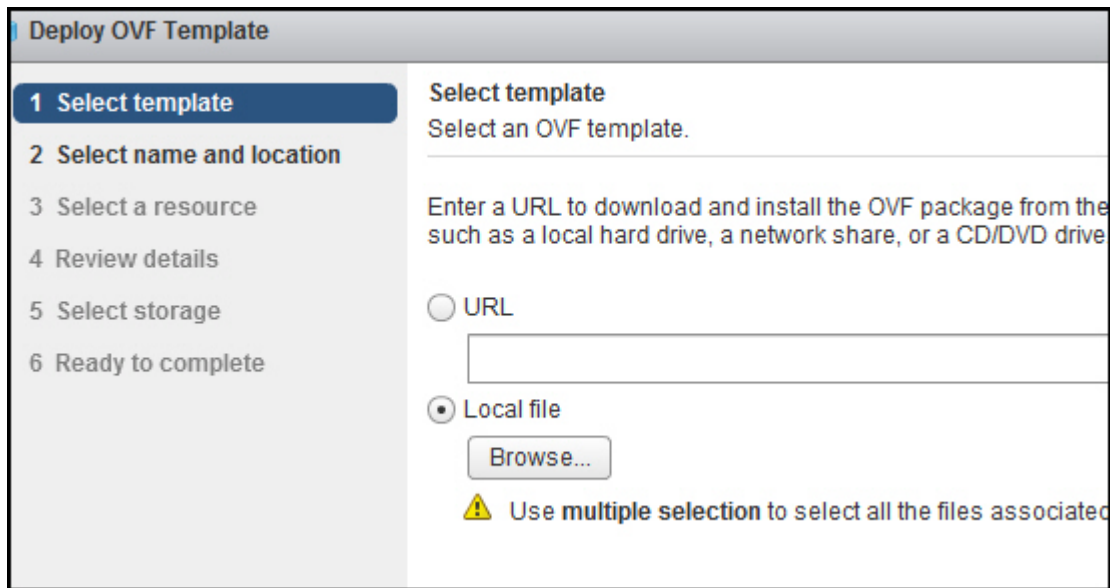
3. Navigate to **Deploy OVF Template**.



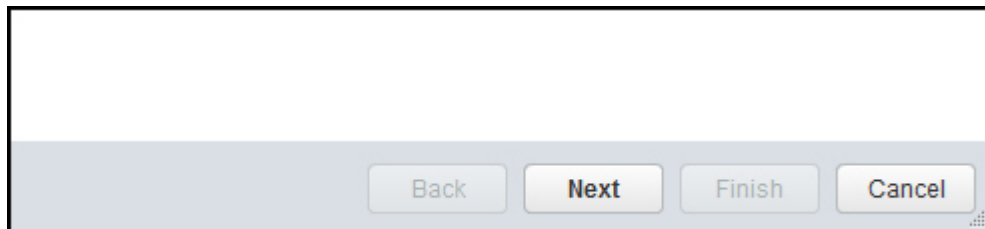
You will be prompted through the process:



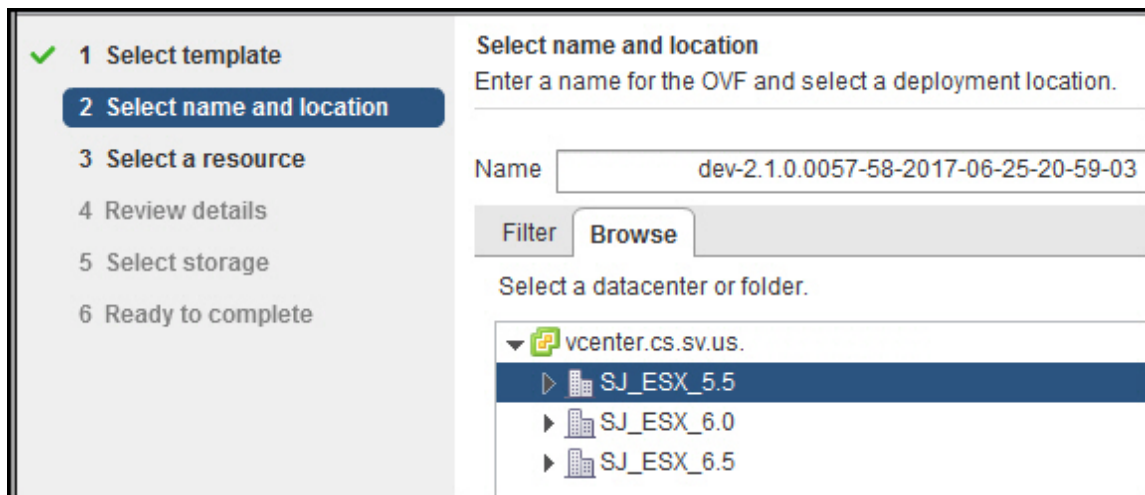
4. Select template.
5. Enter the file location or select **Browse** and navigate to the location.



6. Select **Next**.

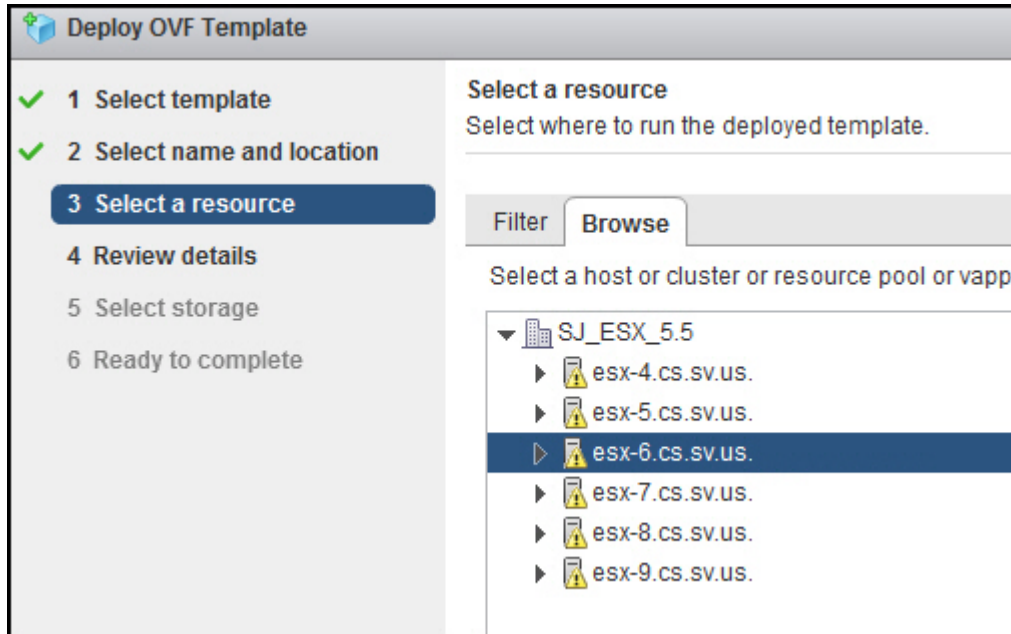


7. Select name and location.

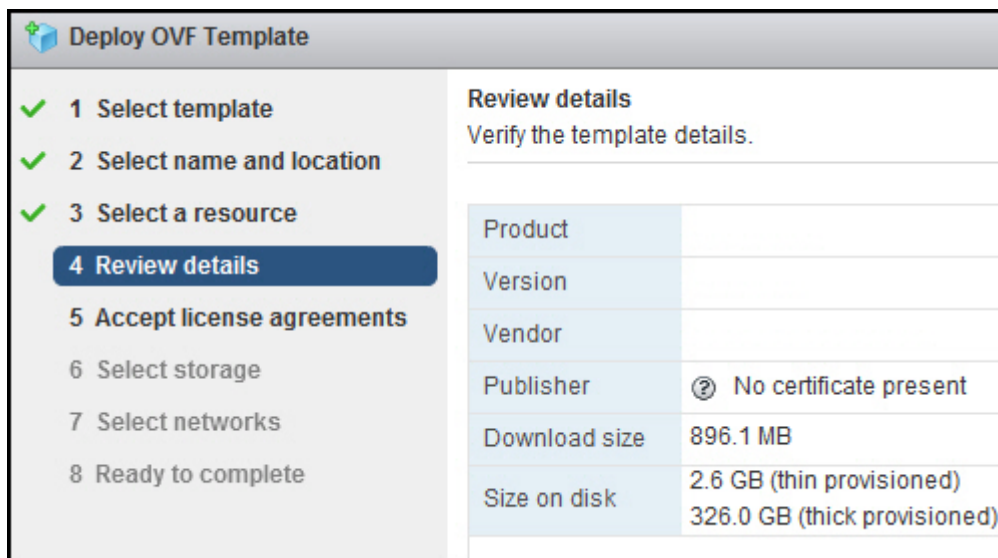


8. Select **Next**.

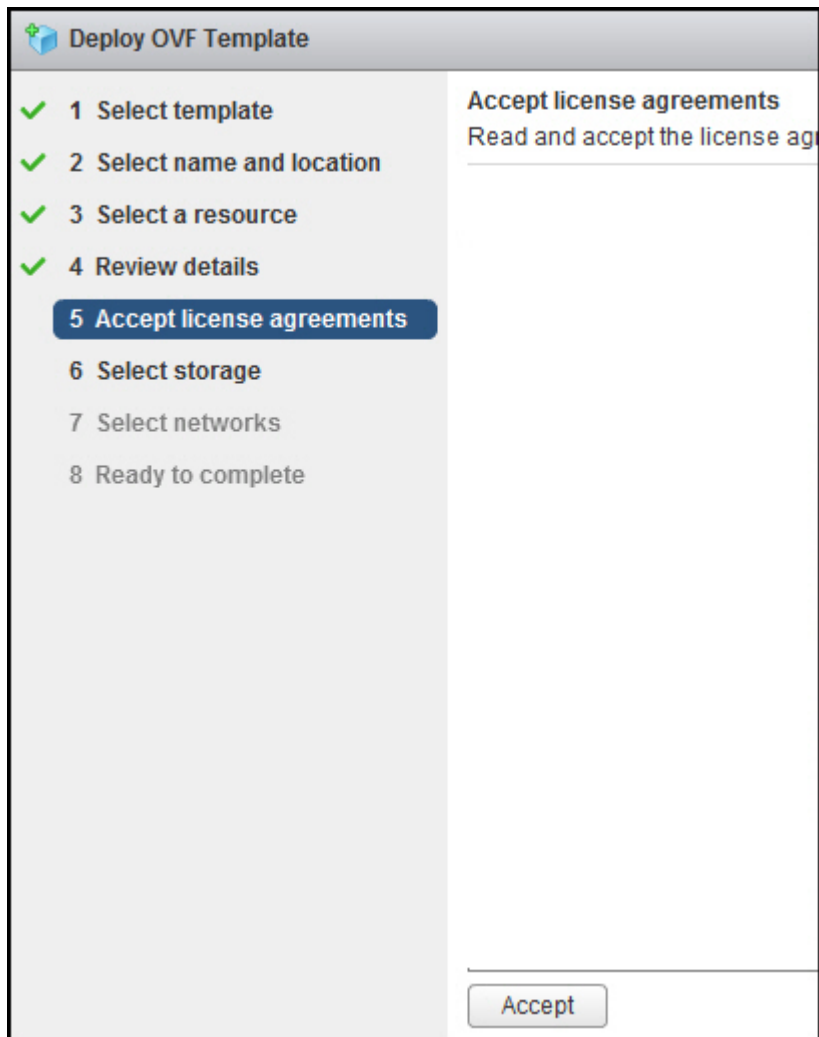
9. Select a resource (i.e., host).



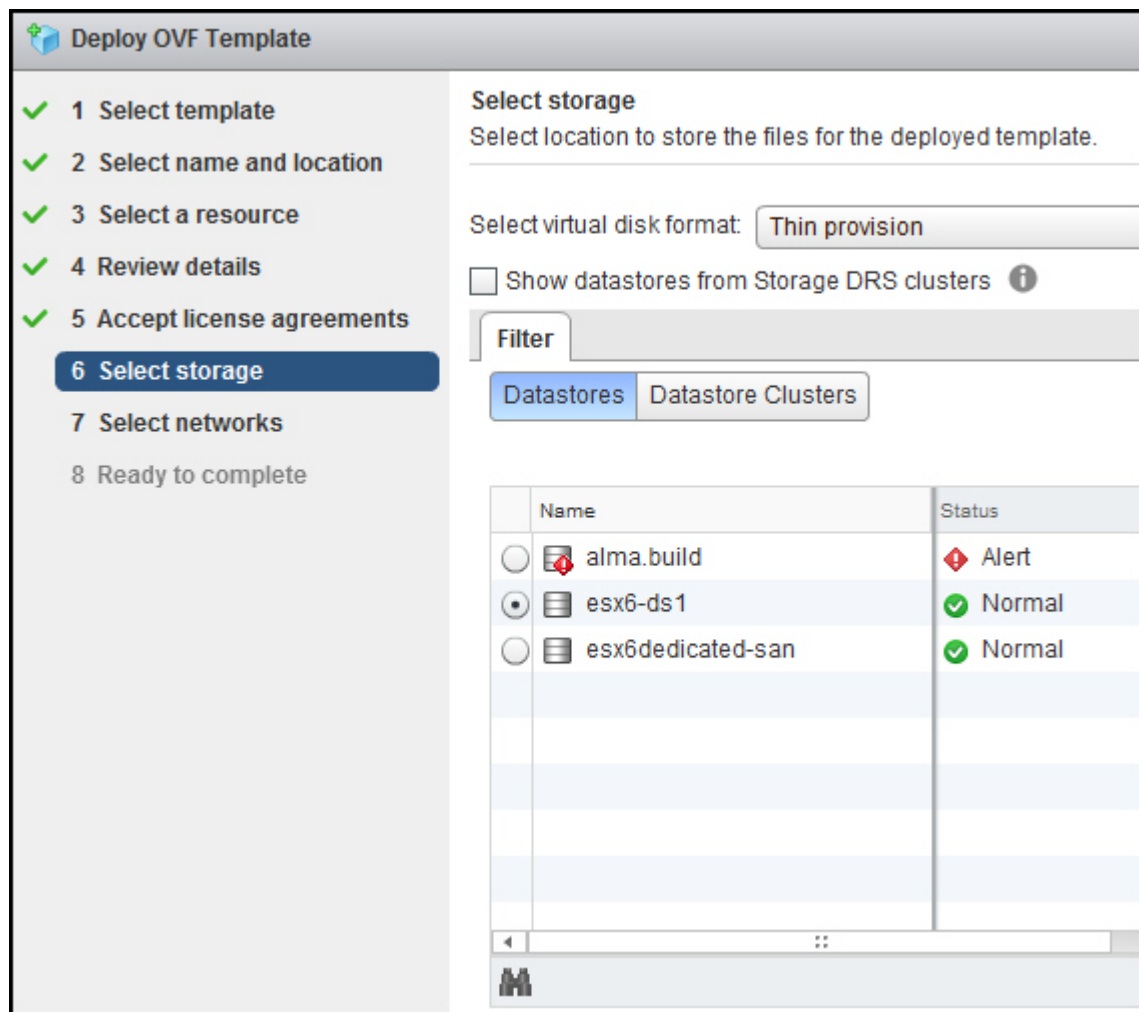
10. Select **Next**.
11. Review the details.



12. Select **Next**.
13. Review the Agreement, (selecting **Next** to scroll through the Agreement).
14. Select **Accept**.

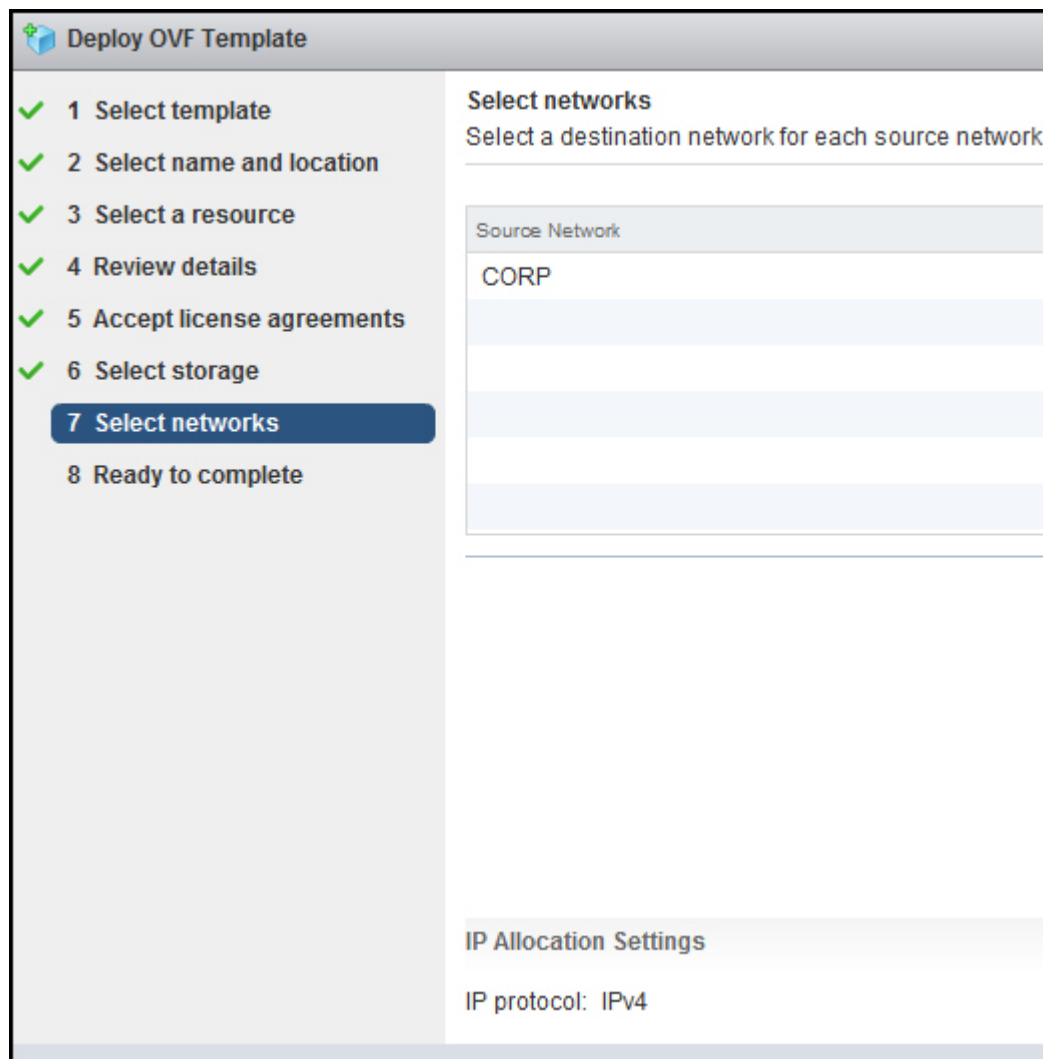


15. Select storage.

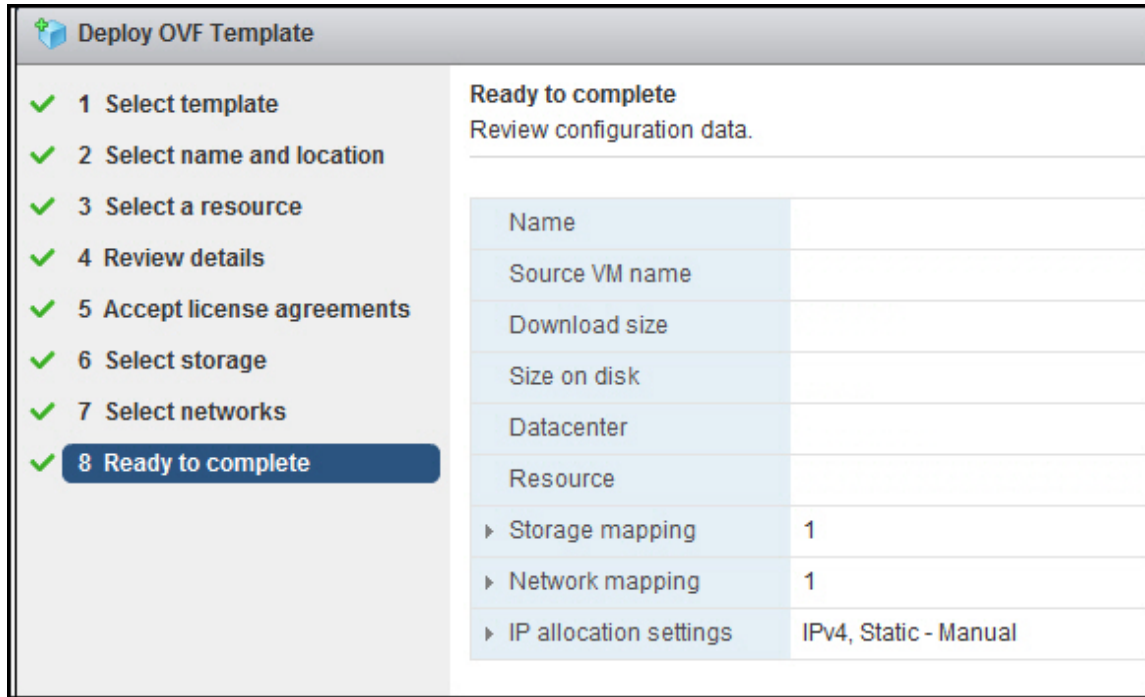


16. Select **Next**.

17. Select your network.



18. Select **Next**.
19. Review the configuration data.

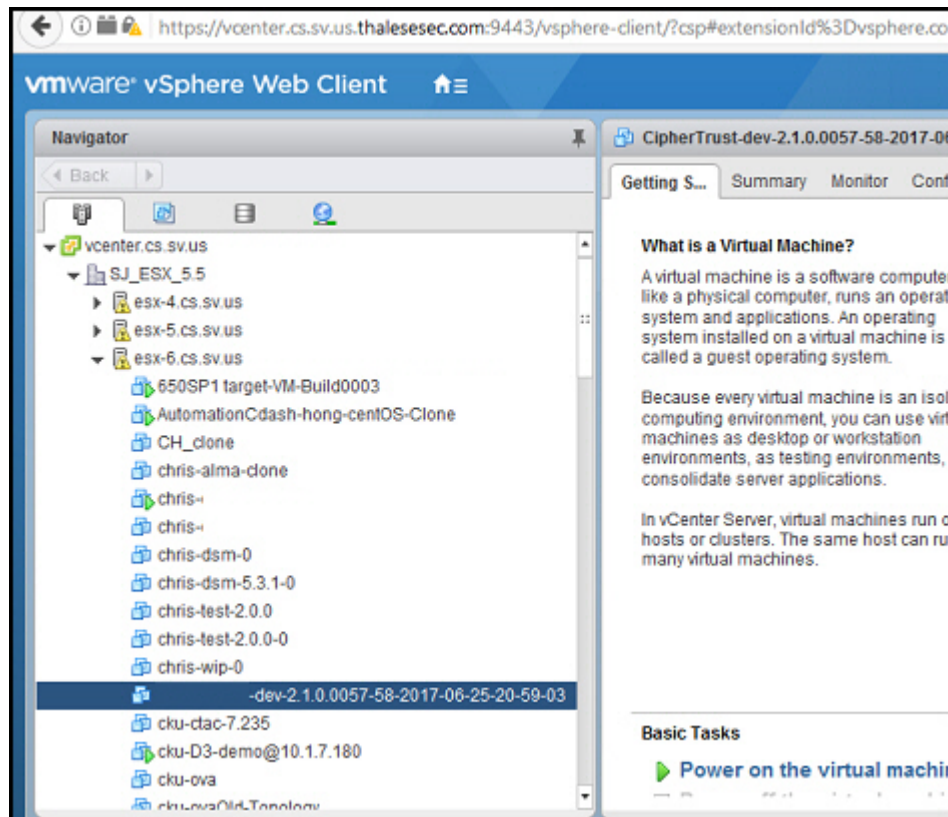


20. Select **Finish**.

21. You can follow the status.

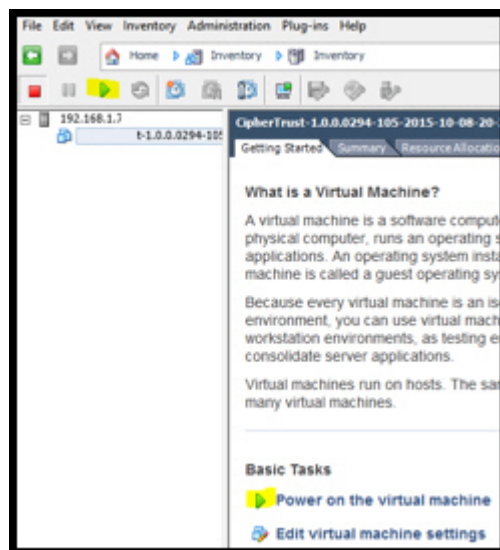


22. You are now ready to power on.



20.3. Turn on the Virtual Machine

1. Click on the VM that you just created.
2. Select the **Getting Started** tab.
3. Select **Power on the virtual machine**.

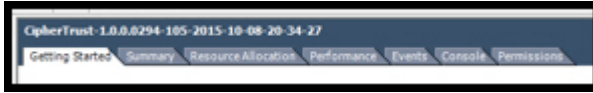


4. Allow five minutes for the virtual appliance to load.

20.4. Run the Virtual Machine

20.4.1. Unfamiliar with VMware ESXi

1. Select the **Console** tab, if you are unfamiliar with VMware ESXi and cannot determine the IP Address of the nShield Monitor VM that you just created:



2. The login prompt displays.
3. Login to the system using the default user ID and password:
 - Default user id: admin
 - Default password: password123

The system will prompt you to change the password.

4. Change the password to one that meets the same minimum requirements those for a user on the nShield.

After the first login from the CLI, the system prompts you to start the **CLI Setup Wizard**.

Entrust recommends using the WebUI set up wizard. If you would like to use the WebUI for setup, then answer "no" to the prompt for starting the CLI setup wizard.



Entering the wrong password 3 or more times will lock the user out of system and a re-install of OVA is required.

```

Authorized users only. All activities may be monitored and reported.
localhost login: admin
Password:

Authorized users only. All activities may be monitored and reported.
Welcome admin... It is Sun Oct 18 17:59:42 GMT 2015

SET THE DEFAULT USER'S PASSWORD

Password requirements are:
- Should have length between 8 and 16 characters
- Should have at least 2 capital letters (A-Z)
- Should have at least 2 lower case letters (a-z)
- Should have at least 2 numbers (0-9)
- Should have at least 2 special characters ( @ ! $ % & * + \ / \ ' \# ^ ? : ; . , )

Old Password:
*****
New Password:
*****
Confirm New Password:
*****
Successfully completed set user password

Your IP Address is 192.168.0.3
For WEB UI Setup Wizard, go to https://192.168.0.3 /wizard
*****
| *Welcome* |EULA|Email|System Admins|Network|Key Generation|Date-Time|Ready|
*****
                                Setup Wizard

This wizard will guide you through setting up the initial users
and settings

Start CLI Setup Wizard ? (y/n) _

```

20.4.2. Familiar with VMware ESXi

If you are familiar with VMware ESXi and can determine the IP address assigned to the new UI VM, record your new password and the IP Address listed, and provide information to the appropriate personnel.

In most organizations the information technology or infrastructure group will accomplish the setup of the OVA, while the installation and operation of the nShield Monitor Virtual Appliance will be performed by a different functional group.

If you are to perform both tasks (nShield Monitor OVA install and nShield Monitor setup), record your new password and the IP Address listed above.

Proceed to [Setup Wizard](#) for instructions on using the WebUI Setup Wizard for setting up and configuring the nShield Monitor Virtual Appliance.

21. Install OVA with VMware Workstation/Player

21.1. Introduction

The nShield Monitor OVA can be installed on a VMware Workstation/Player hypervisor including the following versions:

- VMware Player or Player Professional 6
- VMware Player or Player Professional 7
- VMware Workstation 11
- VMware Workstation 12.



The VMware Workstation and Player installation must be local to the machine nShield Monitor is being installed on.

Please be aware that the nShield Monitor virtual appliance does not have VMware Tools installed; thus copy and paste operations are not supported from the host or other guest OS to the virtual appliance console.

You should ensure that the machine that you install nShield Monitor on runs 24X7 throughout the duration. You may need to reboot at some point at which point you will have to enter passwords to re-establish the master key.

Note: If you are going to be running nShield at full capacity with 500 devices, a recommended precaution is to increase the 250GB disk in vCenter to 350GB after deploying the OVA but before powering it on. Once the OVA has been powered on the disk size cannot be changed.

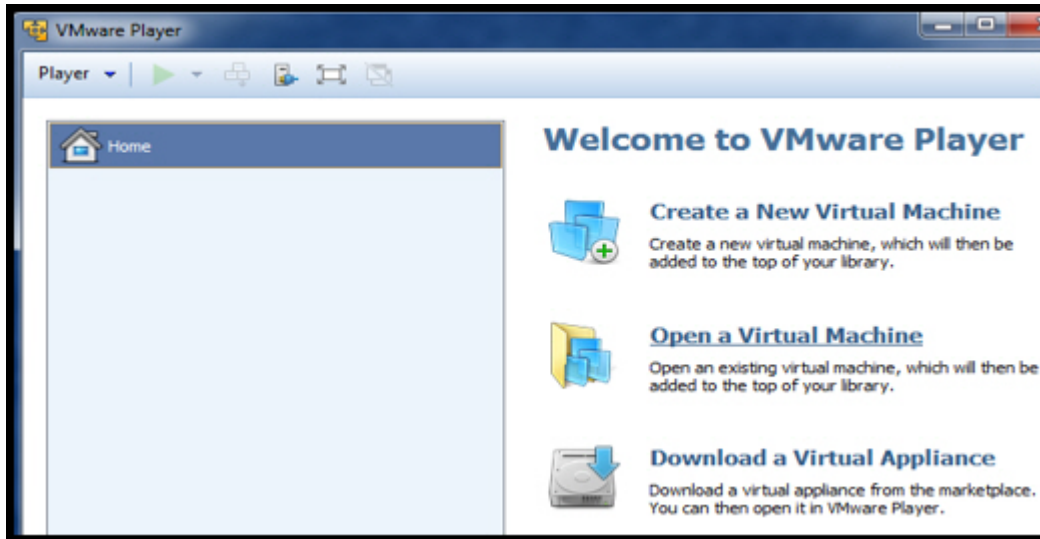
21.2. Install the nShield Monitor OVA

Run the VMware Player or Workstation software.



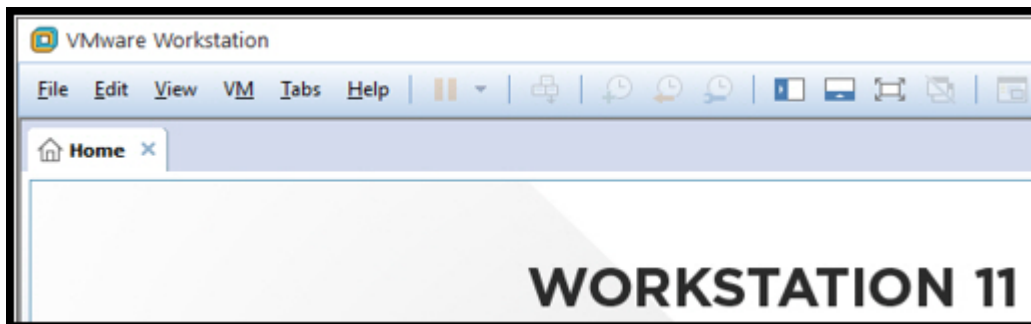
The steps that follow apply for both the VMware Player and the VMware Workstation.

1. Select Open a Virtual Machine from the Home tab.

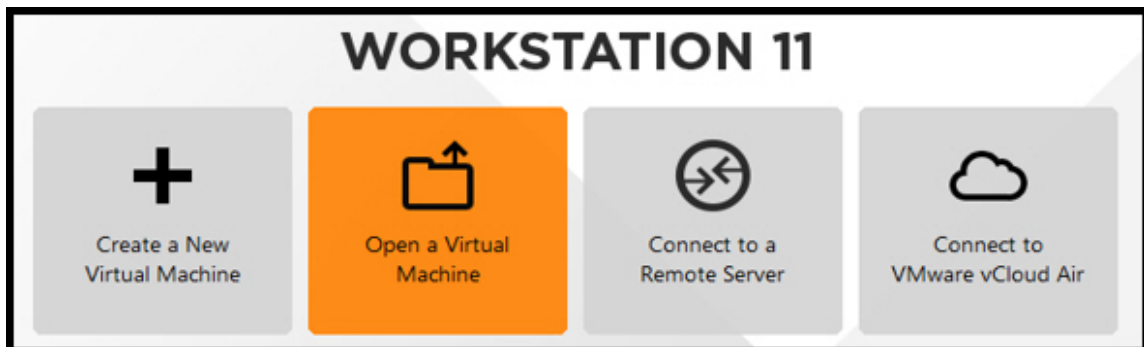


From the menu bar you can also select **File** (Alt + F) and **Open**(Ctrl + O). On VMware Workstation, this is the first option on the menu bar. For VMware Player, it is found under the **Player** drop down menu.

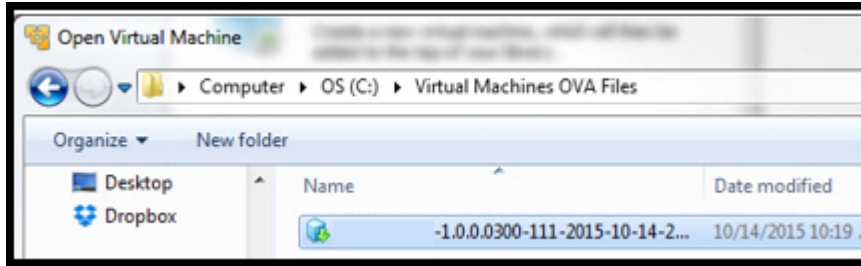
VMware Player and Workstation versions vary on the home screen, so please refer to the documentation for the version that you plan to use.



2. Select **Open a Virtual Machine**.

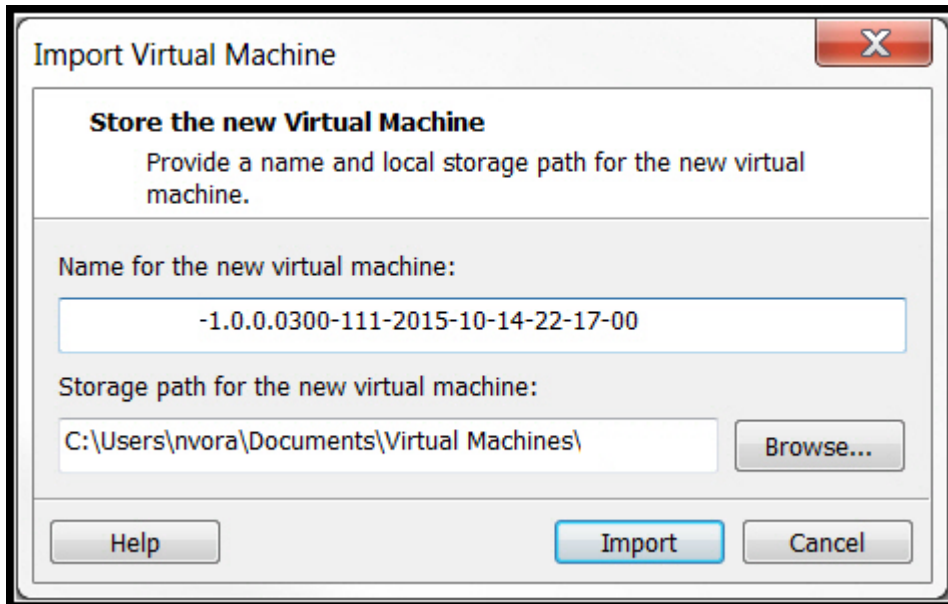


The Open Virtual Machine page opens.



3. Select the OVA file to be installed.
4. Select **Open**.

The Import Virtual Machine dialog box opens.



5. Enter a name and path for the VM to be stored.
6. Select **Import**.

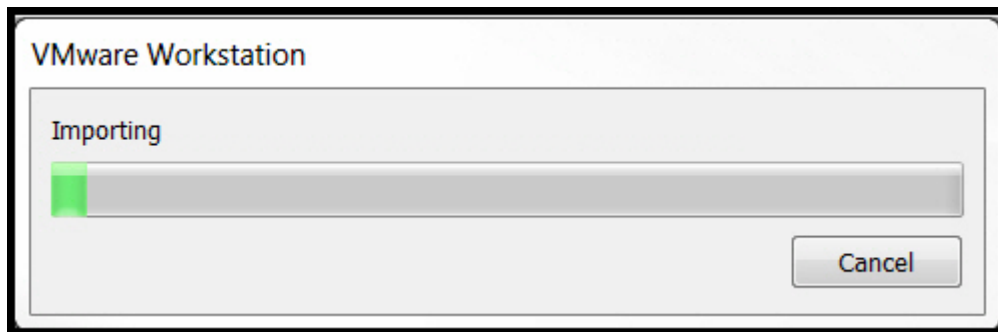
The End User License Agreement (EULA) page opens.

7. Read the EULA.
8. Select **Accept**.

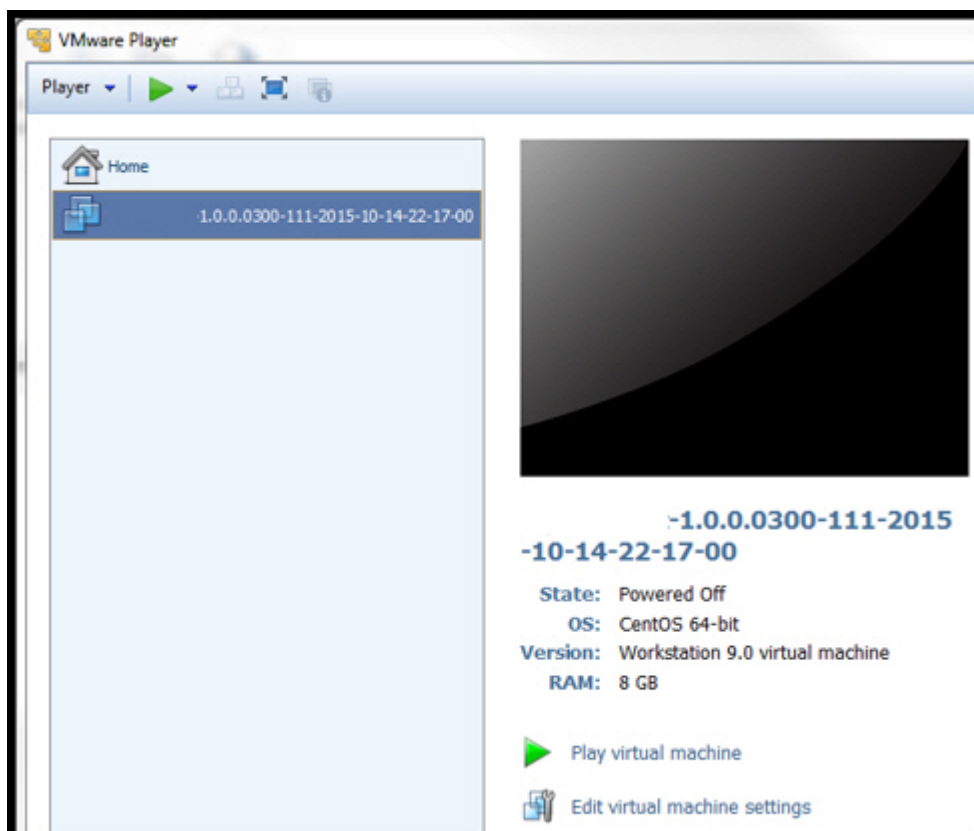


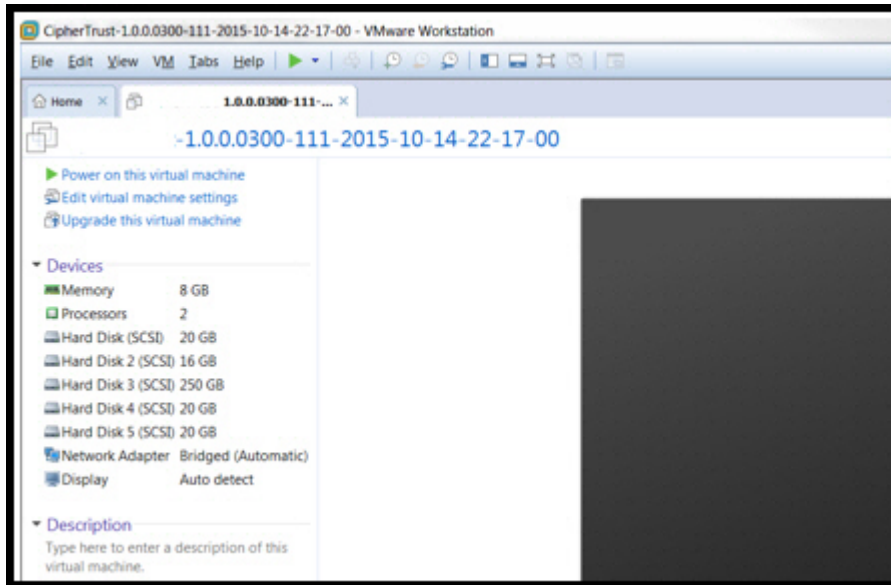
If you decline the EULA, you will be unable to proceed with the installation.

The Import Progress page opens.



Once nShield Monitor is installed you will be looking at the nShield Monitor VM (VMware Player) / VMware Workstation.





After deployment of OVA is finished, the installation of the nShield Monitor OVA is now complete.

9. On the VMware Player and Workstation screens, click the green right arrow button to power on nShield Monitor.

Please allow five minutes for the Virtual Appliance to boot.

The login prompt displays.

21.3. Run the Virtual Machine

1. At the login prompt, enter the default user ID and password:
 - Default user id: admin
 - Default password: password123
 - The system will prompt you to change the password.
2. Change the password to one that meets the same minimum requirements those for a user on the nShield.
3. Record your new password and the IP Address listed and provide information to appropriate personnel.

After the first login from the CLI, the system prompts you to start the **CLI Setup Wizard**.

It is recommended that you use the WebUI set up wizard. If you would like to use the WebUI for setup, then answer "no" to the prompt for starting the CLI setup wizard.



Entering the wrong password 3 or more times will lock the user out of system and a re-install of OVA is required.

```

Authorized users only. All activities may be monitored and reported.
localhost login: admin
Password:

Authorized users only. All activities may be monitored and reported.
Welcome admin... It is Sun Oct 18 17:59:42 GMT 2015

SET THE DEFAULT USER'S PASSWORD

Password requirements are:
- Should have length between 8 and 16 characters
- Should have at least 2 capital letters (A-Z)
- Should have at least 2 lower case letters (a-z)
- Should have at least 2 numbers (0-9)
- Should have at least 2 special characters (0 ! $ & % + \ / \ ' \# ^ ? : . , )

Old Password:
*****
New Password:
*****
Confirm New Password:
*****
Successfully completed set user password

Your IP Address is 192.168.0.3
For WEB UI Setup Wizard, go to https://192.168.0.3 /wizard

*****
| *Welcome* |EULA|Email|System Admins|Network|Key Generation|Date-Time|Ready|
*****

                                Setup Wizard

This wizard will guide you through setting up the initial users
and settings

Start CLI Setup Wizard ? [y/n] _

```



In most organizations, the information technology or infrastructure group will accomplish the setup of the OVA, while the installation and operation of the nShield Monitor Virtual Appliance will be performed by a different functional group. If you are to perform both tasks (nShield Monitor OVA install and nShield Monitor setup), record your new password and the IP Address listed above and proceed to [Setup Wizard](#).

22. Create and Manage Hyper-V Virtual Machines in Hyper-V Core

22.1. Prerequisites for Using nShield Monitor with Hyper-V Virtual Machines

It is recommended to have at least 8 GB main memory when using Hyper-V Manager with nShield Monitor. The following Hyper-V image files are required:

- `nShieldMonitor-2.7.0-1.vhd`
- `nShieldMonitor-2.7.0-2.vhdx`
- `nShieldMonitor-2.7.0-3.vhdx`
- `nShieldMonitor-2.7.0-4.vhdx`
- `nShieldMonitor-2.7.0-5.vhdx`

22.2. Install Hyper-V

With Windows Server Core installations, you can install Hyper-V using the following applications:

- The legacy Hyper-V Manager.
- Windows Admin Center.

22.2.1. Install Hyper-V on Windows Server Core with PowerShell

At the PowerShell command prompt, run:

```
Install-WindowsFeature -Name Hyper-V -IncludeAllSubFeature -Restart
```

Windows Server Core will install the Hyper-V role and restart automatically.

22.2.2. Add the Hyper-V Role Using Windows Admin Center

1. Connect your Windows Admin Center Gateway Server to your Windows Server Core installation.
2. In Windows Admin Server, select **Server Manager > Roles and Features > Install**, then select **Hyper-V**.

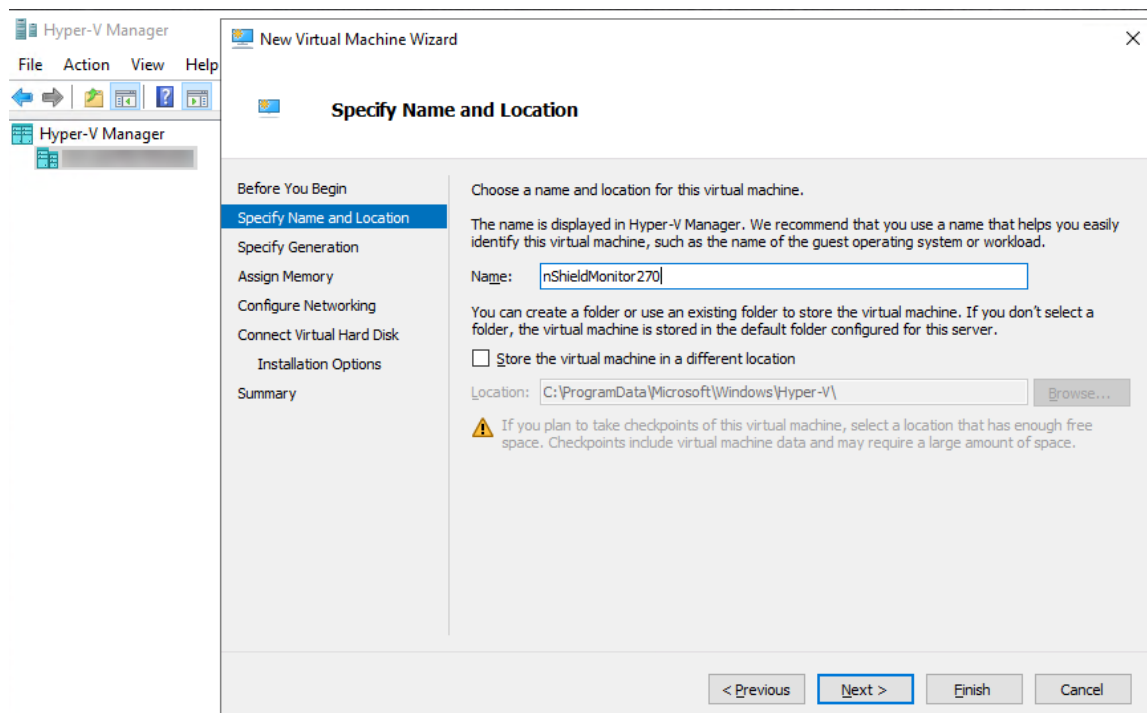
Windows Admin Center will calculate the dependencies of role and feature installations and then prompt you to proceed with the installation, including automatic reboot options.

3. When Windows Server has rebooted, check in **Server Manager > Roles and Features** that the **State** for the Hyper-V role is **Installed**.

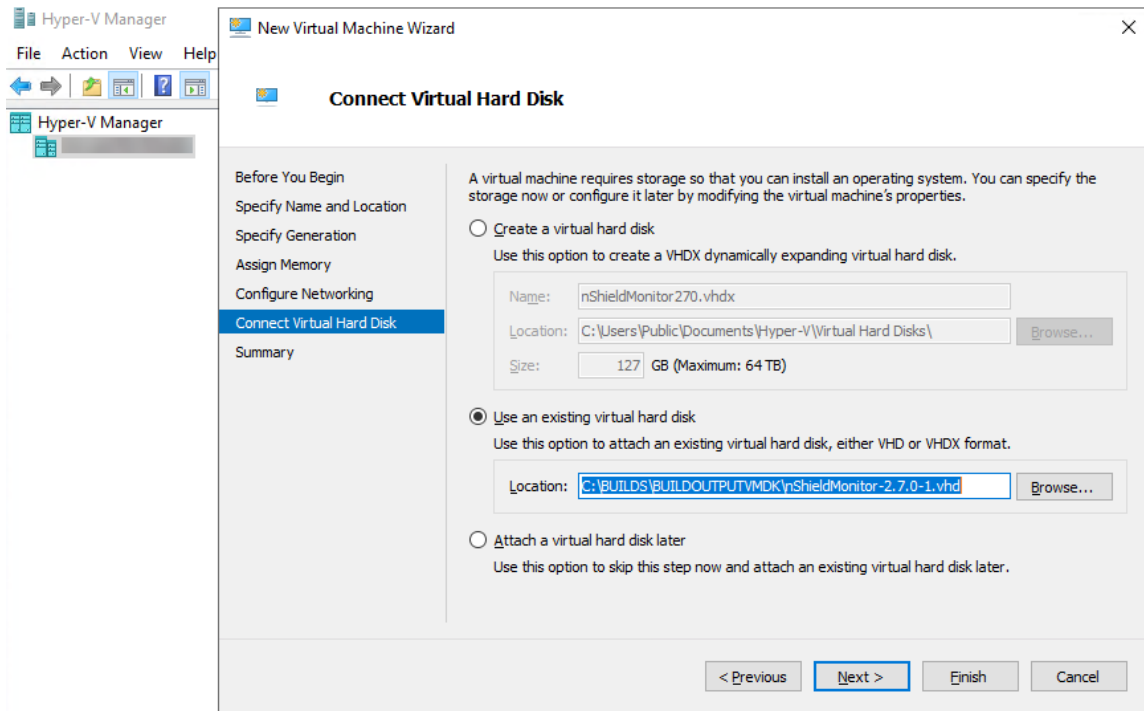
22.3. Configure a New Virtual Machine with Hyper-V

1. In Windows Admin Center, select **Server Manager**, then launch **Hyper-V Manager**.
2. Select **New > Virtual Machine**.

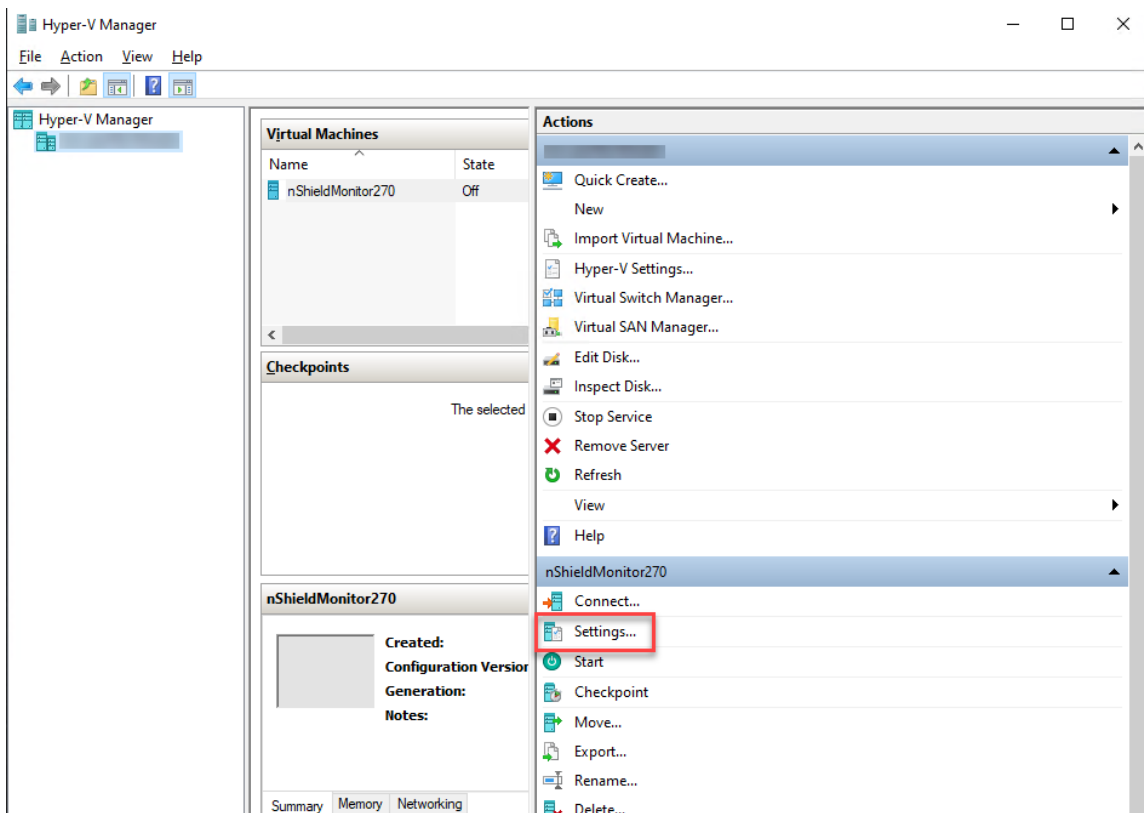
The **New Virtual Machine Wizard** opens.



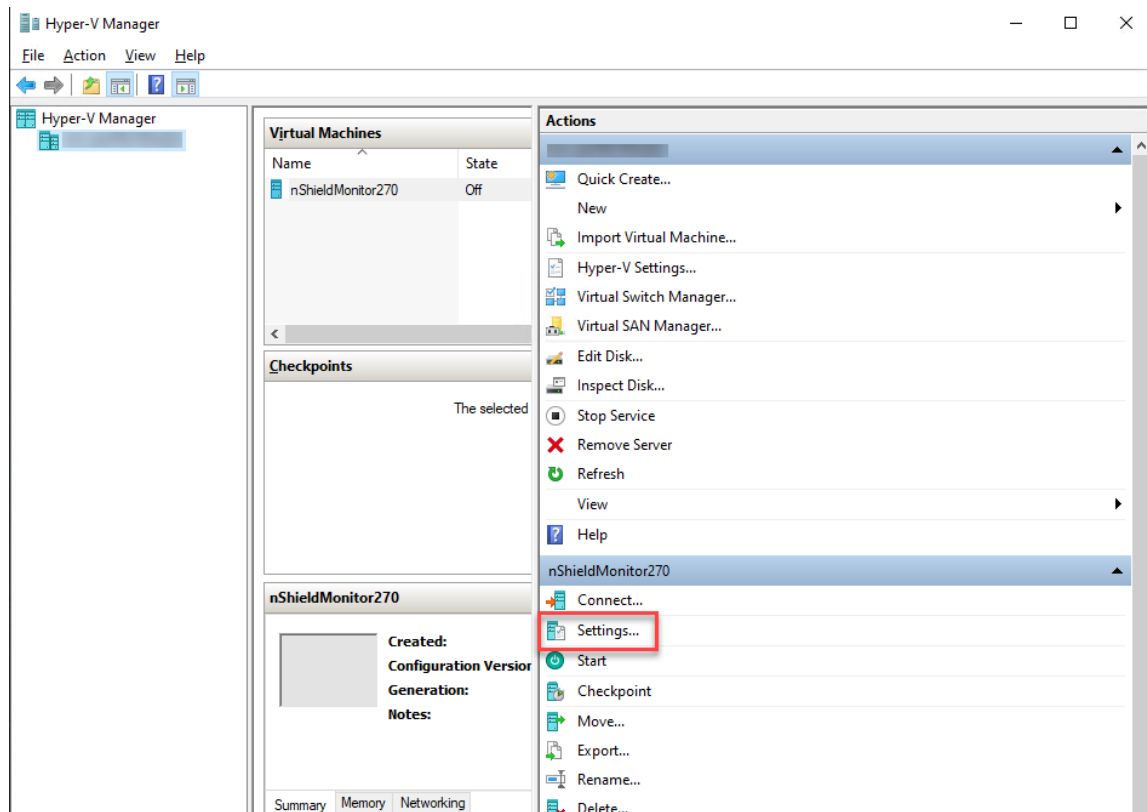
3. Specify the **Name** and **Location** of the virtual machine, then select **Next**.
4. Select **Generation 1**, then select **Next**.
5. Set the **RAM Size**, then select **Next**.
6. Set the **Connection** to **Default Switch**, then select **Next**.
7. Attach the boot hard disk (VHD file) for nShield Monitor.



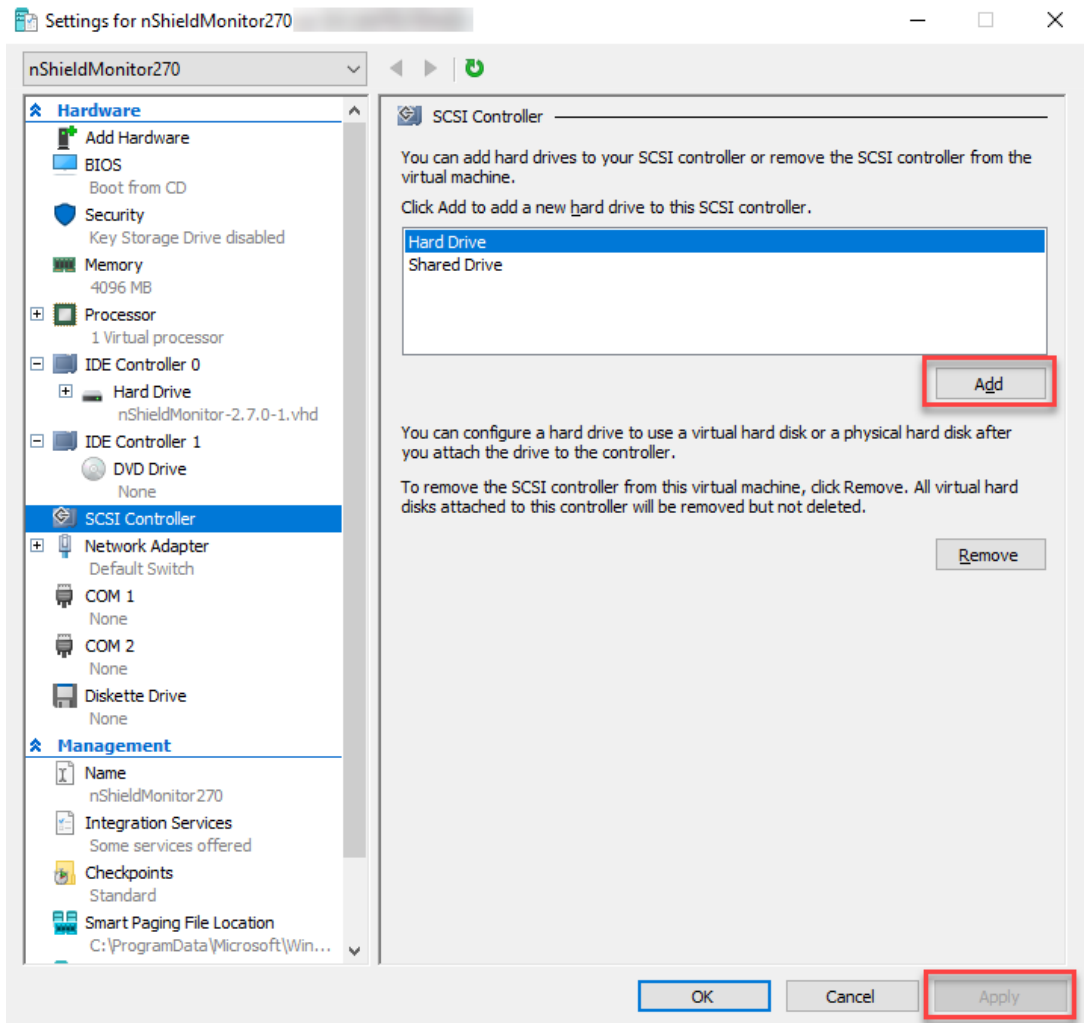
8. Select **Next**, then select **Finish**.
9. In the new machine, select **Settings**.



10. Select **SCSI Controller**, then add the remaining four hard drives of nShield Monitor.

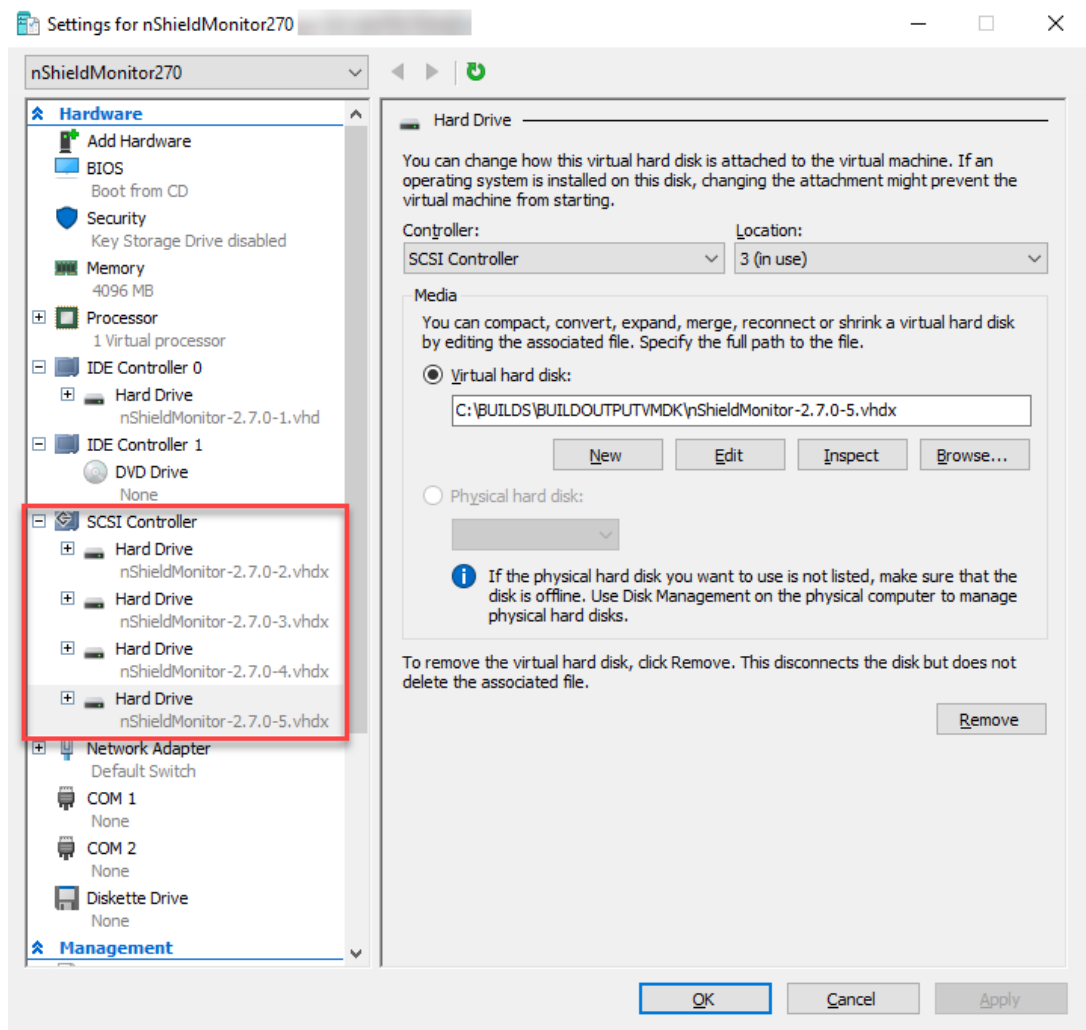


- a. Select **Hard Drive**, then select **Add**.



- b. In the **New Virtual Hard Disk Wizard**, select **Copy the contents of the specified virtual hard disk**, browse to the **-2.vhdx** file, and add it.
- c. Back on the **SCSI Controller** page, select **Apply**.
- d. Add the other three virtual hard disk files (**-3.vhdx**, **-4.vhdx**, and **-5.vhdx**), repeating steps a-c for each of them.

All four virtual hard disk files added to the SCSI Controller:



11. From **Hyper-V Manager**, select **Start** and **Connect** to see the nShield Monitor image running.