nShield Monitor

Monitor v3.1.0 Install and User Guide

8 April 2024

© 2024 Entrust Corporation. All rights reserved.

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 . . . 4
    2.5. Accessing the User Guide . . . 6
3. License Installation . . . 8
    3.1. Overview . . . 8
    3.2. Installing a license . . . 8
4. Setup Wizard . . . 10
    4.1. Overview . . . 10
    4.2. Wizard . . . 10
    4.3. Setting up the network . . . 12
    4.4. Master Key Generation . . . 13
    4.5. Date/Time . . . 14
    4.6. Ready to Setup . . . 15
    4.7. Log In . . . 15
5. Configuration Logged in as Administrator . . . 17
    5.1. Overview . . . 17
    5.2. First-time setup . . . 17
    5.3. Edit Profile page . . . 20
    5.4. Configuration tab tasks . . . 23
6. Configuration Logged in as Group Manager . . . 47
    6.1. Overview . . . 47
    6.2. Edit Profile page . . . 47
    6.3. Managed entities . . . 48
    6.4. Group Alarm Thresholds . . . 53
    6.5. Group Event Notification . . . 55
7. Logs . . . 59
    7.1. Logs available to Group Managers . . . 59
    7.2. Logs available to Administrators . . . 60
    7.3. Log sorting . . . 61
    7.4. Log functionality . . . 62
8. Dashboard . . . 66
    8.1. Event List . . . 67
    8.2. nShield Performance . . . 69

8.3. Users . . . 74
8.4. nShield Monitor Status . . . 75
8.5. Unacknowledged Alarm Summary . . . 75
9. Views . . . 77
9.1. Logged in as Administrator . . . 77
9.2. Logged in as Group Manager . . . 77
9.3. View > Group > Group List . . . 81
9.4. Additional Views available to the Group Manager . . . 95
10. Reports . . . 121
10.1. Generate Reports . . . 121
10.2. Scheduled Reports . . . 123
11. Alarms . . . 126
11.1. General description . . . 126
11.2. Acknowledging alarms in bulk . . . 126
11.3. Acknowledging an individual alarm . . . 127
12. nShield CLI Commands . . . 129
12.1. GUI initialization . . . 129
12.2. Setting a password . . . 129
12.3. Master key status . . . 129
12.4. CLI setup wizard . . . 130
12.5. Welcome . . . 130
12.6. EULA . . . 130
12.7. Set User's Email . . . 131
12.8. Create Administrators . . . 131
12.9. Configure network . . . 132
12.10. Generate system key . . . 132
12.11. Configure date and time . . . 133
12.12. Initialize . . . 133
12.13. CLI commands . . . 134
12.14. Network commands . . . 135
12.15. Date-time commands . . . 137
12.16. System commands . . . 138
12.17. Email queue commands . . . 139
12.18. Troubleshooting commands . . . 140
12.19. Service commands . . . 141
13. Licensing . . . 142
13.1. Introduction . . . 142
14. Enterprise Firewall Settings . . . 143
15. Troubleshooting . . . 145

15.1. Global Troubleshooting Enhancement feature . . . 145
15.2. Network test tools . . . 146
15.3. Ping . . . 146
15.4. RouteDump . . . 148
15.5. TCPDump . . . 148
15.6. Traceroute . . . 149
15.7. No monitoring data received . . . 150
16. nShield Monitor Alarm Conditions . . . 151
17. nShield Monitor Backup and Restore . . . 157
18. Deploying nShield Monitor . . . 158
18.1. Centralized monitoring . . . 158
18.2. nShield Monitor multi-instance . . . 158
18.3. Distributed monitoring . . . 158
18.4. Deployment considerations . . . 159
19. Residual Risk . . . 161
19.1. User guidance . . . 161
19.2. Secure operation . . . 161
19.3. Risks . . . 161
19.4. Deployment and distribution . . . 161
19.5. Secure configuration . . . 162
19.6. Host machine . . . 162
20. Install OVA With VMware ESXi . . . 163
20.1. Introduction . . . 163
20.2. Install the nShield Monitor OVA . . . 163
20.3. Turn on the Virtual Machine . . . 164
20.4. Run the Virtual Machine . . . 165
21. Install OVA with VMware Workstation/Player . . . 166
21.1. Introduction . . . 166
21.2. Install the nShield Monitor OVA . . . 166
21.3. Run the Virtual Machine . . . 170
22. Create and manage Docker instances . . . 172
22.1. Prerequisites for using nShield Monitor with Docker . . . 172
22.2. Start an nShield Monitor Docker container . . . 173
22.3. Connect to the web UI for the nShield Monitor . . . 177
22.4. Assign a usable IP to a nShield Monitor container . . . 178
22.5. Troubleshooting container startup errors: . . . 179
23. Create and Manage Hyper-V Virtual Machines in Hyper-V Core . . . 181
23.1. Prerequisites for using nShield Monitor with Hyper-V virtual machines . . . 181
23.2. Install Hyper-V . . . 181

23.3. Configure a new virtual machine with Hyper-V 182

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.

Users connect to the nShield Monitor server via HTTP(s) using a configured IP address or through a user-friendly name. This is achieved using a standard web-browser (Internet Explorer, Chrome or Firefox). 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 inspect each device to determine status on a regular basis
- 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 respond to device hardware failures. For example, a failed 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
- Docker container

These 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 6.5
- vSphere ESXi 6.7
- vSphere ESXi 7.0
- 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

The Docker container can be deployed on either a physical machine or a virtualization platform which has hardware virtualization support enabled (VT-x or AMD-V).

2.1.2. Host server requirements

The host server should meet the following requirements:

- 64-bit host OS
- CPU: 2 core 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
- Disc space to download:
  - An OVA image (1.1 GB)
  - A Hyper-V image (3.3 GB)
  - A Docker container and its associated volumes (1.5 GB)
- Size on the hard drive:
  - 2.3 GB (OVA) / 3.3 GB (Hyper-V) / 1.5 GB (Docker container) (thin provisioned)
  - 326.0 GB (OVA) (thick provisioned)

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 (that is, more than one HSM), reduce data duplication 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. For example, due to regulatory issues.

2.3. Client workstation

The client workstation is any Apple or Microsoft Windows workstation that has network connections to nShield Monitor. A supported browser (WebUI access) or

SSH client (CLI access) that can access nShield Monitor is required.

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. This ensures 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 a Group Manager. This user is then able to perform tasks related to both the 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.

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:

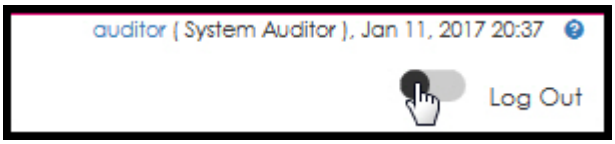
- The command instruction usage
- HSM utilization
- HSM health
- Event triggers in assigned groups
- Event logging and report generation in assigned groups
- Configuring event notification via email in assigned group

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.

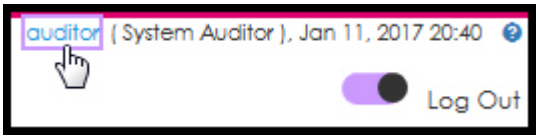
1. Log on as Administrator, Group Manager, or Auditor.
2. Locate the toggle switch in the upper-right corner of the screen.



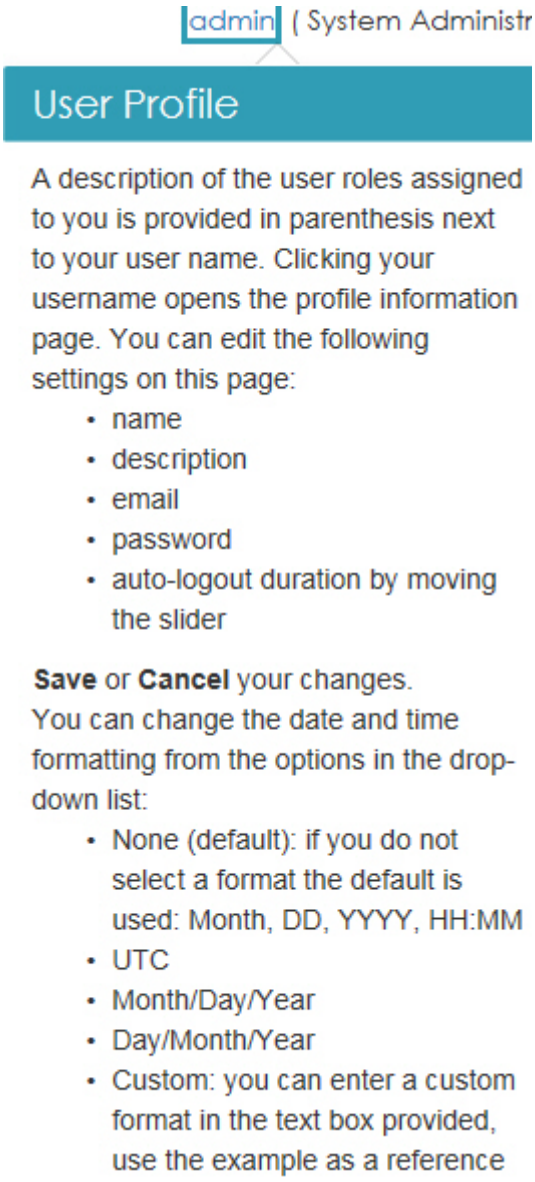
3. Slide the toggle switch to the right.

   Online Help is enabled.

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



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



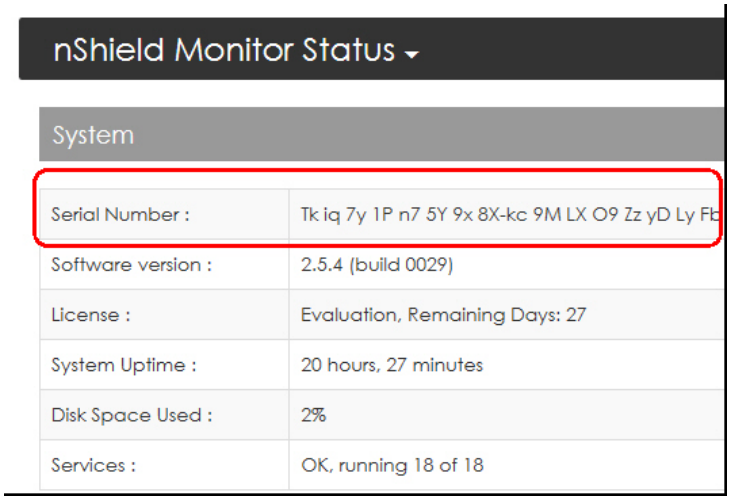
3. License Installation

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.

There are multiple license options available.

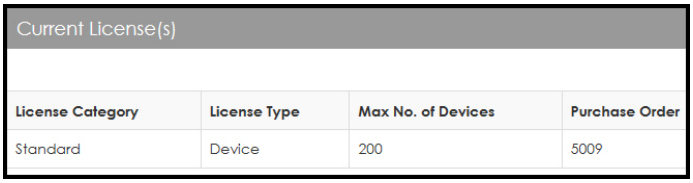
Contact Entrust Sales/Sales Support for prices and availability. Please have the serial number of the deployed nShield Monitor available in order to obtain a license. The serial number can be found on the dashboard page under the **nShield Monitor Status** tab.



3.2. Installing a license

1. Download the license that you received from Entrust to the local machine that is already 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.XXX.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.
   - Enter a new password.
3. Click **Change Password**.

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

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.

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

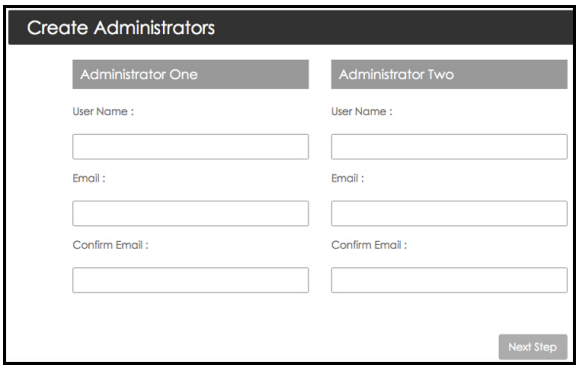
   The **Create Administrators** page opens.

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.

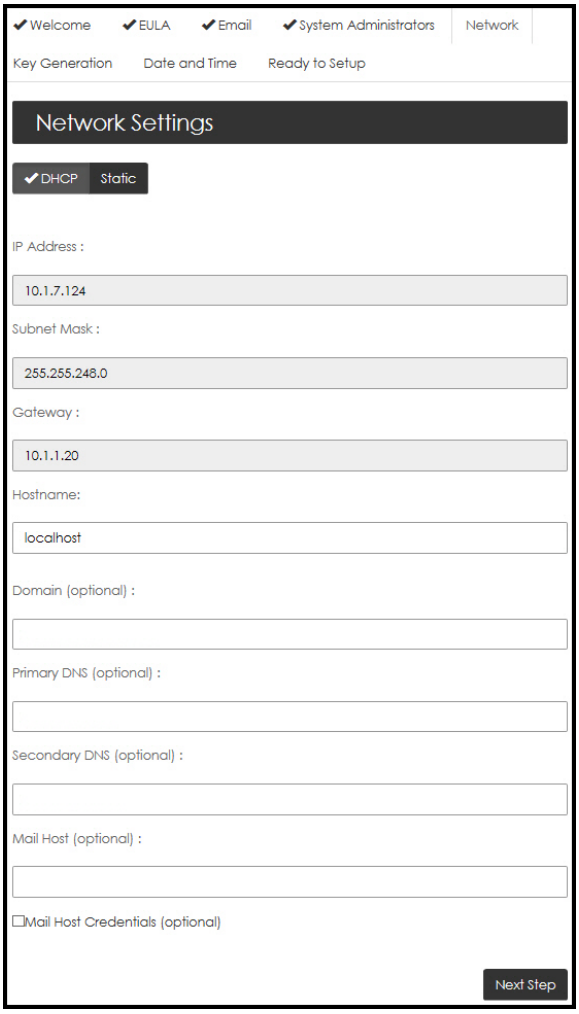
1. On the **Create Administrators** page, enter the **User Name** (for example, Admin1) and **Email** (and confirm email) for each **Administrator**.
2. Select **Next Step**.

   The **Create Administrators** page displays:



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

   The **Network Settings** page opens:



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.

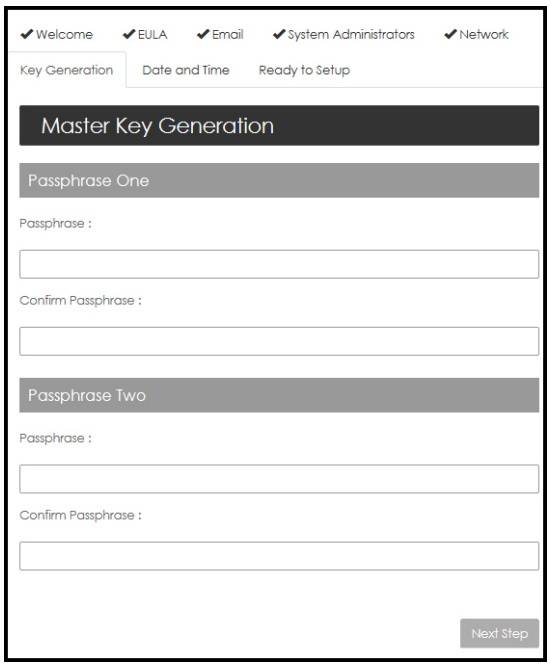
- IP Address
- Subnet
- Gateway
- Hostname
- Domain (optional)
- Primary DNS (optional)
- Secondary DNS (optional)
- Mail Host (optional)

- 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.



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.

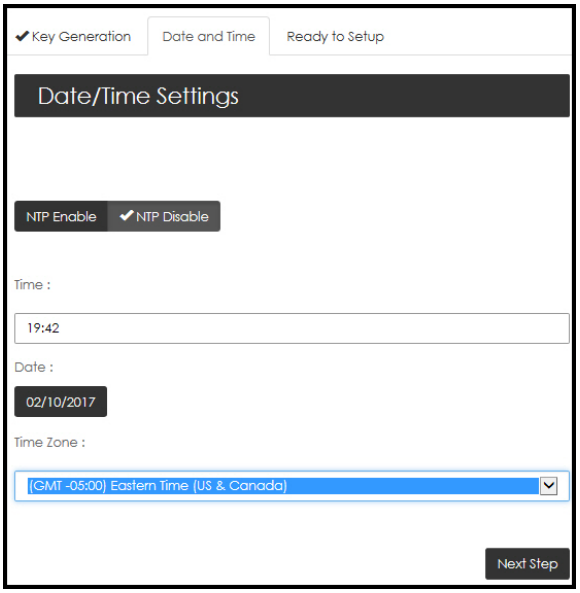
The master key is derived by using the two passphrases, using PBKDF2, that are input during the wizard configuration after the first boot and after every reboot.

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. On the **Master Key Generation** page, enter Passphrase One and Passphrase Two, and then re-enter both for confirmation.
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.

4.5.1. NTP Disabled

1. On the **Date/Time Settings** page, 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.

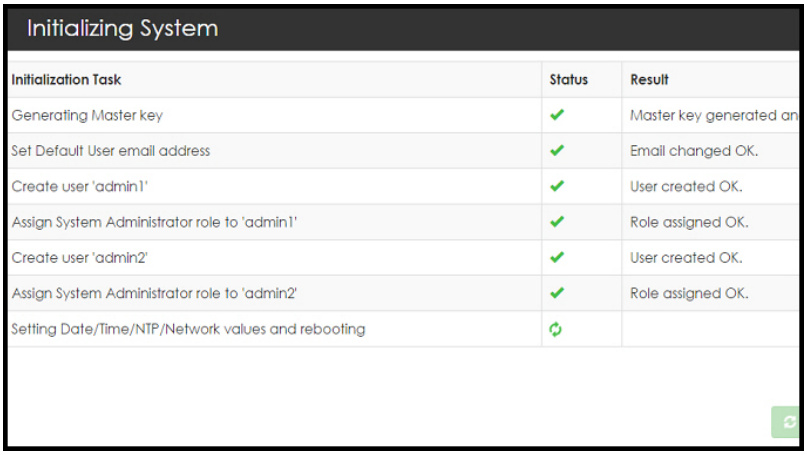
1. On the **Date/Time Settings** page, open the **Time Zone** menu.
2. Select the appropriate time zone.
3. Select **Next Step**.

   The **Ready to Setup** page opens.

4.6. Ready to Setup

1. Select **Initialize**.

   The initialization status page opens and tracks the process. For example:



   nShield Monitor reboots.

4.7. Log In

1. Enter your User ID and Password.
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.
5. Select **Load Master Key**.

   The GUI session disconnects and the following is reported:

   ```
   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.

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 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	Sets the period over which utilization statistics are collected. Must be set for 60 seconds.
UTILENABLE	Enables the collection of utilization data.
HEALTHENABLE	Enables the collection of health check counts.
SNMP	Enable provisioning of utilization and health check data via SNMP.
SNMPADD	Adds an SNMP community or user.

5.2.2. Configuring the nShield HSM

For instructions, see the *SNMP monitoring agent* appendix in the *User Guide* for your HSM(s).

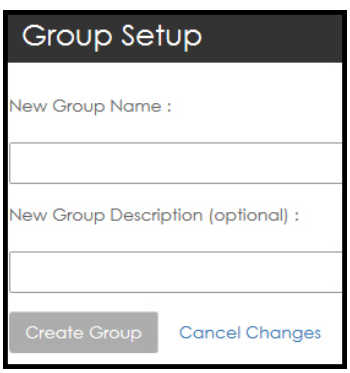
5.2.3. Step 1: Create groups

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**.

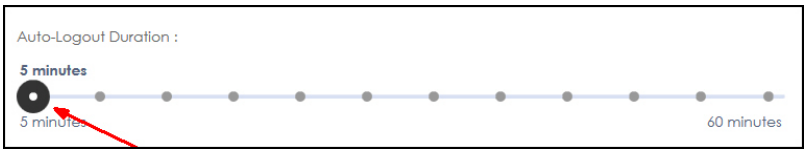
   The **Manage Users** page opens.

2. Select **Create User**.

   The **Create a New User** page opens.

3. Enter the new user data.

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



4. Complete the open fields appropriately and under **Assign Role(s) for this User**, select **Group Manager**.

   The **Assign User to Groups** window opens.

5. Associate the user to groups by selecting the group name (for example, Group 1).
6. When clicking on a Group name in the Available groups list, the group name moves to the **Member of** list.

7. Select **Create User**.

   The user is created and a reset link is sent to the email address associated with the username. The link will prompt the user to change the password before accessing their account. The reset link expires after 60 minutes.

5.2.5. Step 3: Group Manager enroll managed entities to groups

The Group Manager can add devices (that is, enroll entities) to be monitored into the groups. See Configuration Logged in as Group Manager.

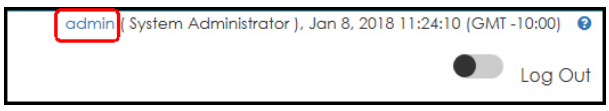
A Group Manager can be configured to access one group, a subset of all the groups or all of the groups in nShield Monitor.

It is usually best to assign to this role the personnel who are responsible for the day-to-day operation of the monitored devices.

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 your User ID located in the upper-right corner of the page. For example:



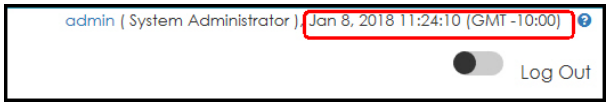
From this page, you can perform the following actions:

- 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:



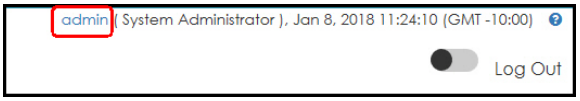
You can select **Use Browser Timezone for Exporting Events**, based on your preference.

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

To restore **Custom Date/Time Format** settings to the default, select the **admin's GUI Persistence Profile** tab, and then the **Reset to GUI Default** option.

5.3.1. Changing your password and email and set the auto-logout duration

1. Click on the username on the upper-right corner of main screen. For example, 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.

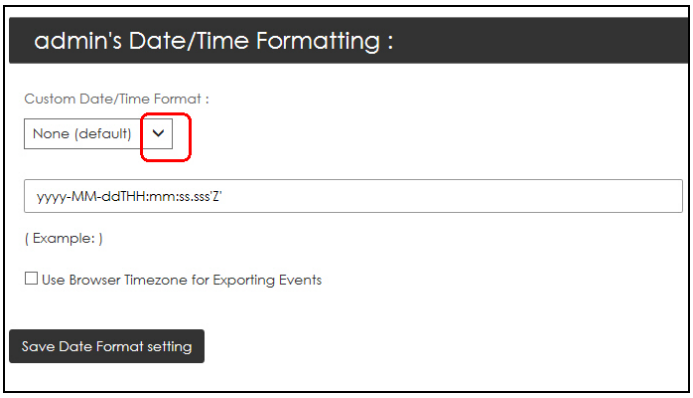
4. The Auto-Logout Duration is set to 60 seconds by default.

   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.



   The drop-down menu opens.

2. Select your preferred format.
3. Select **Use Browser Timezone for Exporting Events** 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, and so on.

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**:

- Select **Reset to GUI Default**.

  A confirmation message appears.

  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**.

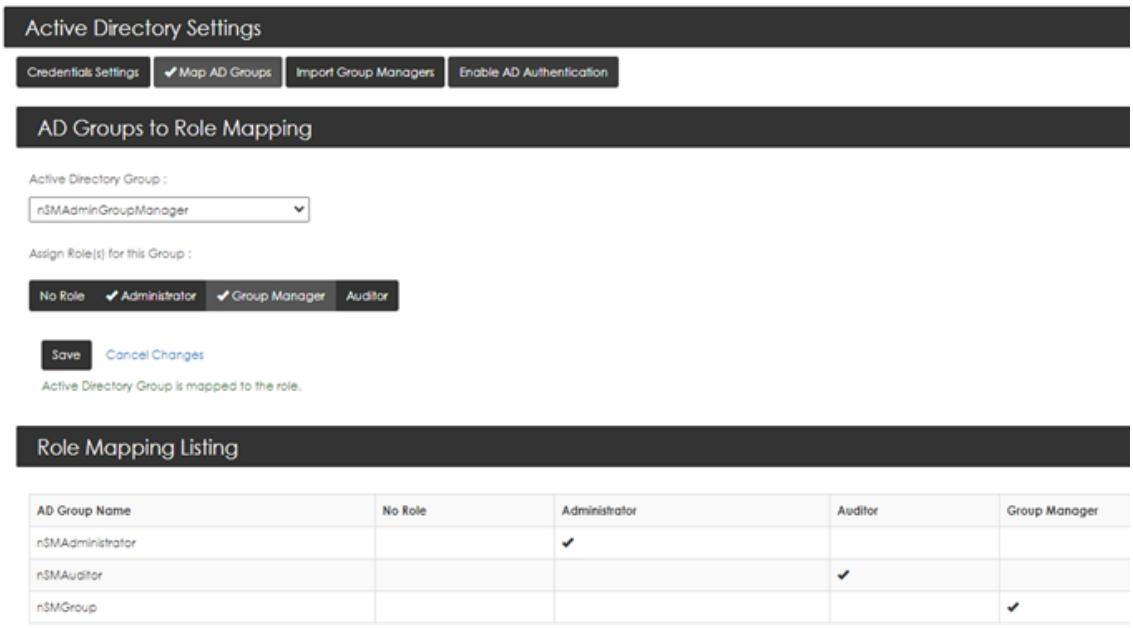
5.4.1. Active Directory authentication

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

To map Active Directory groups:

1. Sign in to nShield Monitor as an administrator.
2. Navigate to **Configuration** > **Active Directory** > **Map AD Groups**.
3. Select the **Active Directory Group** from the drop-down list and assign the appropriate role to it. (See the following table.)
4. **Save** your changes.

   The mappings appear in the **Role Mapping Listing** table at the bottom of the page.



Default Active Directory group to nShield Monitor role mappings:

AD group	nSM role
`nSMAdministrator`	**Administrator**
`nSMGroup`	**Group Manager**
`nSMAuditor`	**Auditor**

All nShield Monitor users are members of the `nSMUsers` group.

A typical nShield Monitor Active Directory user group structure:

- `nSMGroups`
  - `nSMAdministrator` (Administrator)
  - `nSMGroup` (Group manager)
  - `nSMAuditor` (Auditor)
- `nSMUsers` (All users)

For example:

- Forest name: `ldapnsm.com`
- Organizational Unit:

  An OU for each of the two parent folders, `nSMUsers` and `nSMGroups`.

  - `OU=NSMUsers,DC=ldapnsm,DC=com`
  - `OU=NSMGroups,DC=ldapnsm,DC=com`

- Security Group - Global:

  A Security Group for each of the three default nSM Active Directory groups.

  - `CN=NSMAuditor,OU=NSMGroups,DC=ldapnsm,DC=com`
  - `CN=NSMAdministrator,OU=NSMGroups,DC=ldapnsm,DC=com`
  - `CN=NSMGroup,OU=NSMGroups,DC=ldapnsm,DC=com`
- Users:
  - `CN=nsmauditoruser1,OU=NSMUsers,DC=ldapnsm,DC=com` (This user should belong to `nSMAuditor`.)
  - `CN=nsmadminuser,OU=NSMUsers,DC=ldapnsm,DC=com` (This user should belong to `nSMAdministrator`.)
  - `CN=nsmgroupmanager,OU=NSMUsers,DC=ldapnsm,DC=com` (This user should belong to `nSMGroup`.)
  - `CN=nsmcommonuser1,OU=NSMUsers,DC=ldapnsm,DC=com` (This user should belong to `nSMAdministrator` and `nSMGroup`.)

Notes on Active Directory configuration:

- Autologout is set to five minutes for Active Directory users. You cannot modify this setting.
- The content of the `mail` field of Active Directory user profiles must be populated. If this field is blank when a user is imported from Active Directory to nShield Monitor, the user will not be able to sign in to nShield Monitor with their Active Directory credentials. nShield Monitor does not use the field.
- If you create a new user in the `nSMUsers` hierarchy in Active Directory, the user must sign in to the Active Directory domain before they can use their Active Directory credentials in nShield Monitor.
- When Active Directory authentication is enabled in nShield Monitor, you must use Active Directory for all user management:
  - nShield Monitor-generated credentials (credentials not generated in Active Directory) 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. The **Forget password link** is disabled in the nShield Monitor UI.

5.4.1.1. Configuring Credentials for Active Directory

To configure credentials for Active Directory:

1. Login as Administrator.
2. Navigate to: **Configuration > Active Directory > Credentials Settings**.
3. On the **Credentials settings** tab, enter the following details:

Host or IP	The hostname or IP address of the AD server.
Port	The port on the AD server. Typically, port 389 is used for LDAP connections, and port 636 is used for secure LDAP.
Base DN	The point from where a server will search for users. For example: *dc=ivqq,dc=com*.
Username	The AD Administrator Bind DN. This enables the LDAP connection to gain access into the Active Directory. For example: *nSMserv*.
Password	The credentials to use with AD Administrator Bind DN.
AD Domain Name	The name of the AD domain. For example: *ivqq.com*.

4. If a secure LDAP connection is required:
   a. Select **Use Secure LDAP**.
   b. Ensure that a secure **Port** is selected. Typically, for secure LDAP connections, port 636 is used.
   c. Under **Choose certificate file**, click **Choose file** and select the required certificate file.

      Alternatively, paste the certificate text (in PEM format) into the window below the button. A valid AD Server Certificate starts with *-----BEGIN CERTIFICATE-----* and ends with *-----END CERTIFICATE-----*.

   d. Under **Choose key file**, click **Choose file** and select the required key file.

      Alternatively, paste the key (in PEM format) into the window below the button. A valid AD Server Key starts with *-----BEGIN PRIVATE KEY-----* and ends with *-----END PRIVATE KEY-----*.

5. Select **Save**.

   A confirmation message appears.

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, macOS, 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**.
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**.
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.

1. Select **Save**.

5.4.3. Events

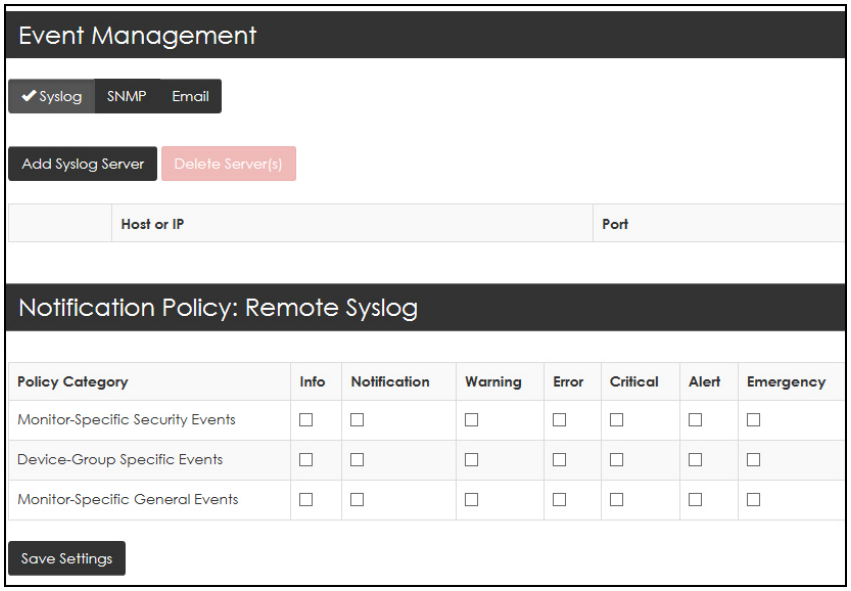
nShield Monitor provides the capability for event notification via:

- 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.



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 checkbox next to 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.

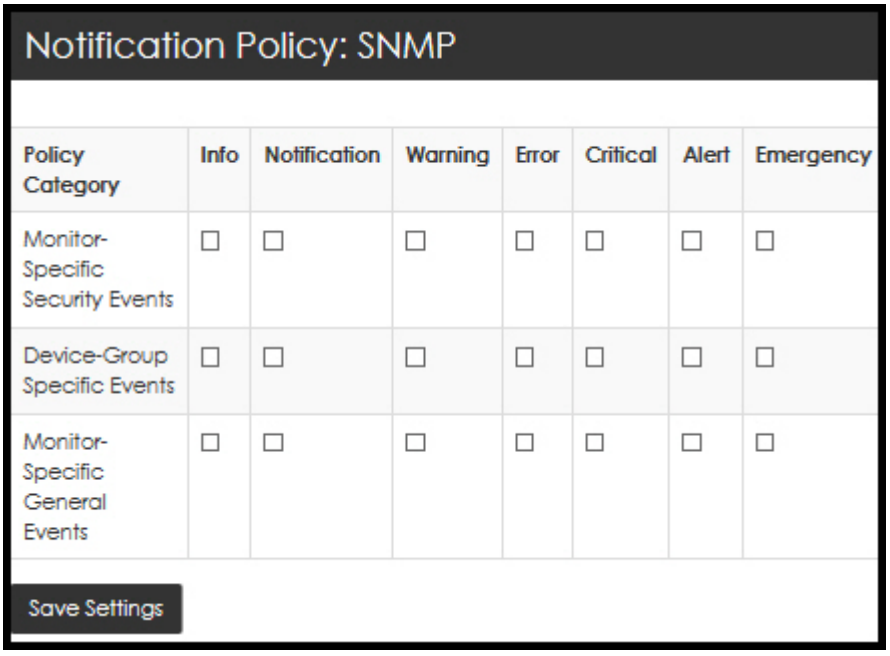
The following SNMP traps are supported:

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.

Trap ID	Name	Severity	Trigger Event
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.
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.

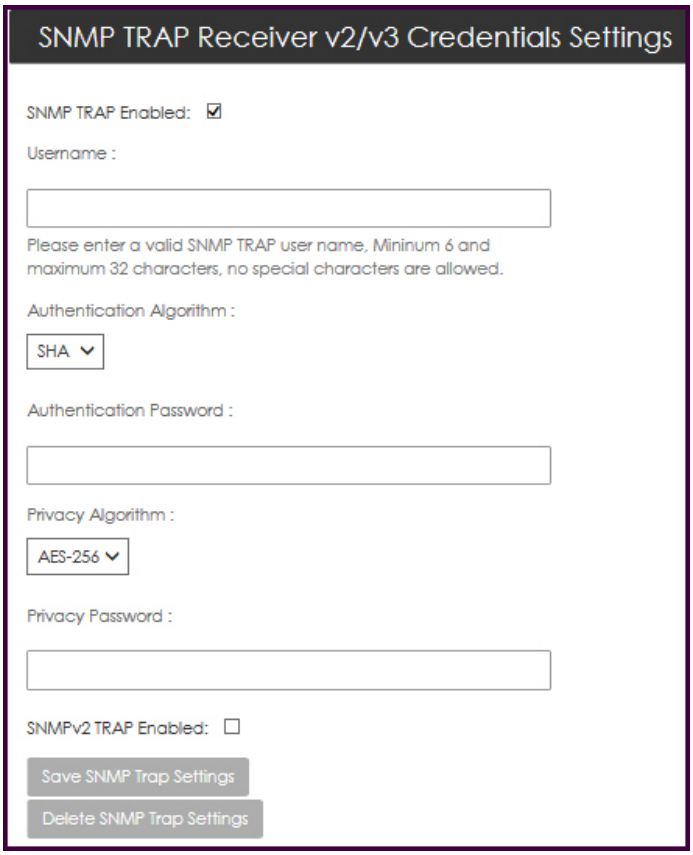


4. Select **Save Settings**.

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 SNMPv3 traps. `SNMPCMD_ARGS` are arguments that would be used for an equivalent `snmptrap` command. For example, to send an SNMPv3 trap 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:
   a. **Linux:** `/opt/nfast/etc/snmp`
   b. **Windows:** `c:\program files\nCipher\nfast\etc\snmp`
2. Stop the SNMP daemon:
   a. **Linux:** run `/opt/nfast/scripts/init.d/ncsnmpd stop`
   b. **Windows:** via Services, the name of the service is `nCipher SNMP Agent`
3. Add the `trapsess` commands 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:
   a. **Linux:** `/opt/nfast/scripts/init.d/ncsnmpd start`
   b. **Windows:** via Services, the name of the service is `nCipher SNMP Agent`

5.4.3.4.4. Delete SNMP Trap Credentials 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**.

   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**.

2. 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 all properties.

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

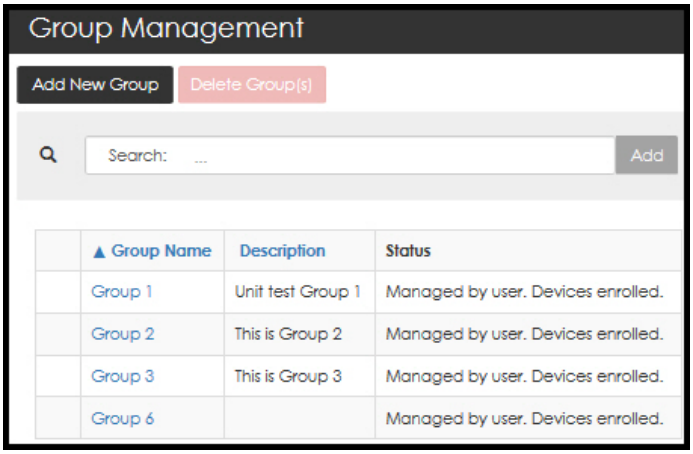
1. Navigate to: **Configuration** > **Events** > **Email**.
2. Select **Email Notification Enabled**.
3. Select the Policy Category and severity combination.
4. Select **Save Settings**.

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.

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**. That is:

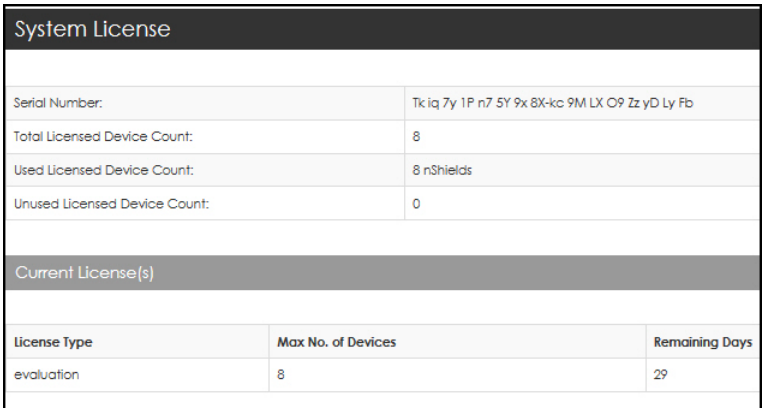
- the group is not managed by another user
- the group does not contain any enrolled devices
- there are no scheduled reports associated with this group.

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.



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 (that is, 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.

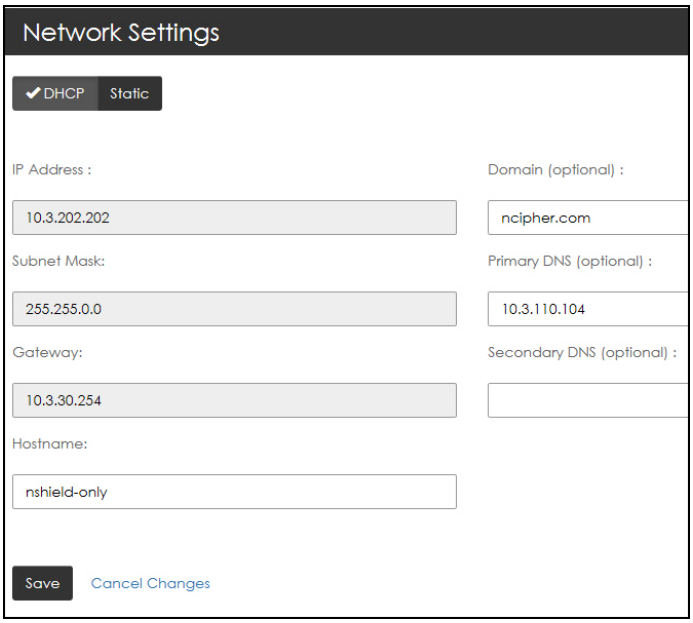
5.4.7. Network

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.



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

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 be 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**.

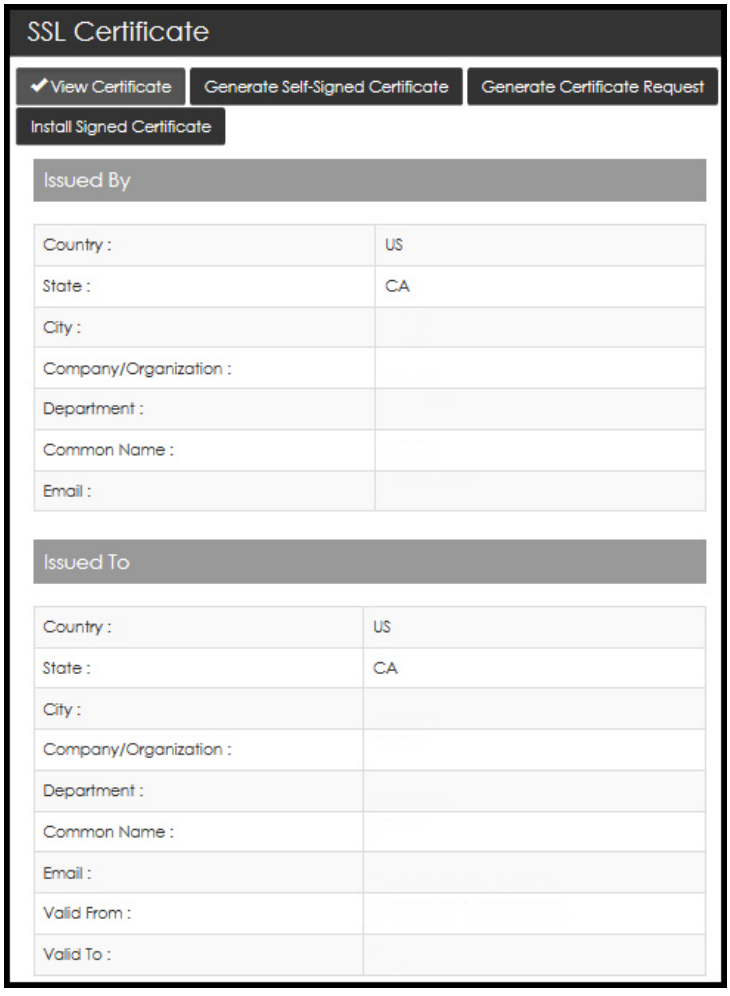
Please note that destroying the master key stops all device monitoring and renders all device credentials invalid. The system must be reset after this operation.

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, and so on.



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 (2 years).

3. Select **Generate Certificate**.

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

4. 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.
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 (that is, nShield Monitor certificate, signing CA, root CA).

The chain should consist of at least two certificates: * nShield Monitor certificate * Signing CA certificate.

The chain can have as many as seven certificates, including: * nShield Monitor certificate * Signing intermediate CA * 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**.
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.

   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.

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 one option remains clear (unblocked).

4. When a quorum approval is pending, one of three actions can happen next:
   a. The first administrator can cancel the quorum request by selecting **Cancel Change** and the system remains unchanged.
   b. The second administrator can deny the change by selecting Reject Change. This generates a log message indicating that a change was denied.
   c. 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.
3. Select **Save Password Settings**.

5.4.10. Upgrade

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

We recommend taking a backup before upgrading, see nShield Monitor Backup and Restore.

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.

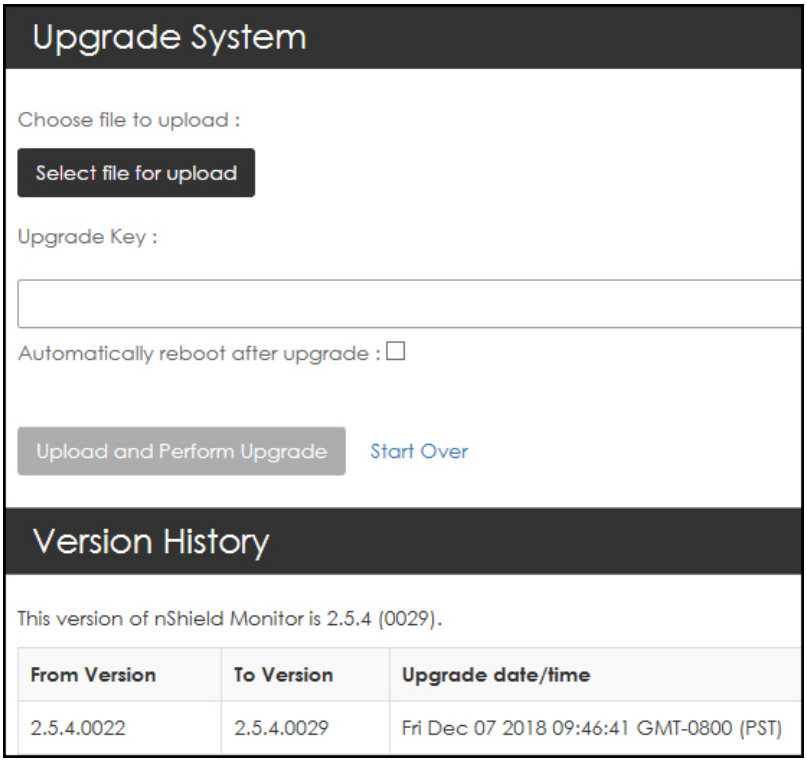
1. Send an email to Entrust nShield Support, https://nshieldsupport.entrust.com, and request an upgrade.

   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:



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.

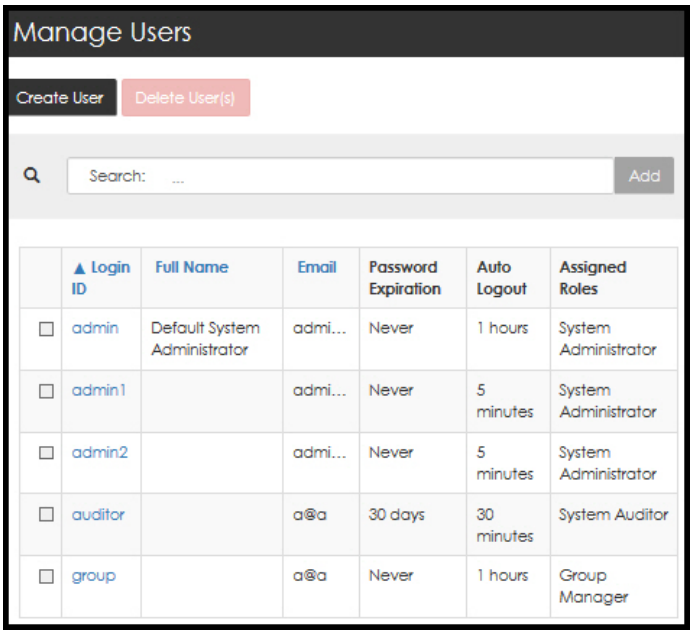
After three failed login attempts, the account is locked

To unlock an account, select **Forgot your Password** on the login page, enter your username, and then select **Request New Password**. An email containing a reset link will be sent to the email address associated with the username. The link will prompt the user to change the password before accessing their account.

The reset link expires after 15 minutes.

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

   The **Manage Users** page opens.



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

   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.

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

   This will send a reset link to the email address associated with the username. The link will prompt the user to change the password before accessing their account. The reset link expires after 60 minutes.

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:

- The configuration of devices that are to be monitored.
- 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 your User ID located in the upper-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**.

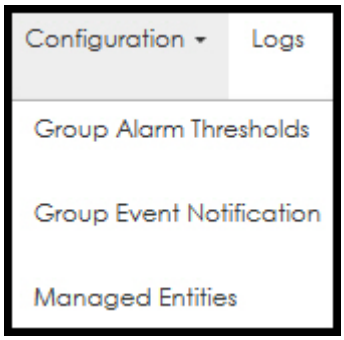
When you select a custom date format, the chosen format is associated with your user ID giving each user the option of selecting their preferred format. Once the format has been selected, it is consistently displayed in accordance with your selection.

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 algorithms during device enrollment.

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

   The **Manage Entity Settings** page opens.

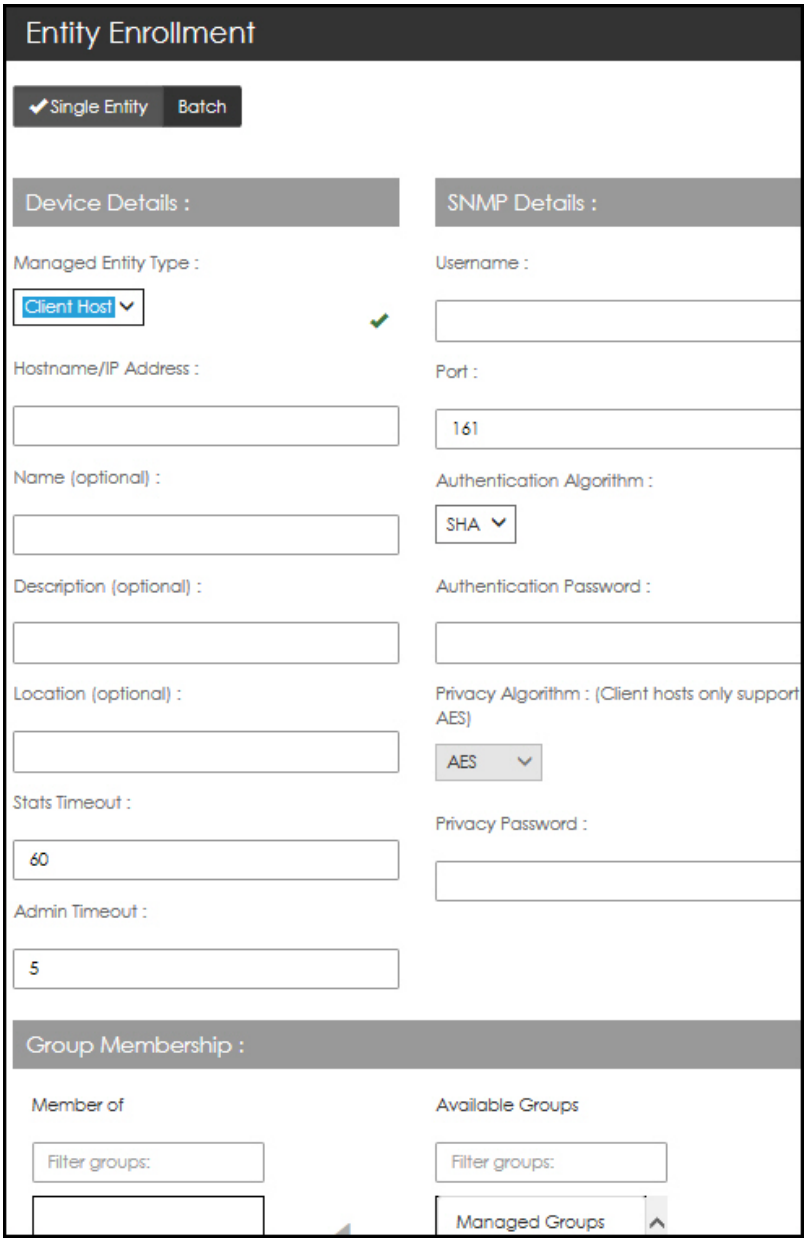
2. Select **Enroll Managed Entities**

   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 required **Managed Entity Type** from the drop-down menu.

4. Enter **Device Details**, **SNMP Details**, and **Group Membership** details.



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.
   - You can 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)
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 checkbox next to the device to be deleted.

Selecting the checkbox 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.

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

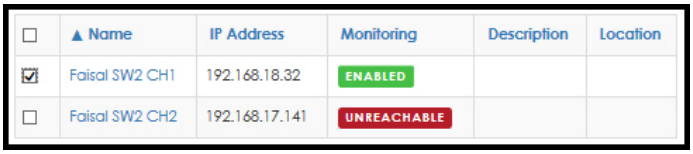
2. Enter the changes/make your selections.
3. Select **Save Changes**.

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.



   New action buttons appear:

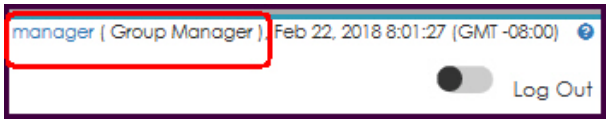
   > The Start Monitoring <device> is a toggle with Stop Monitoring <device>. When the device is being monitored, the **Stop Monitor** option is available. When the device is not being monitored, the **Start Monitor** option is available.

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

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

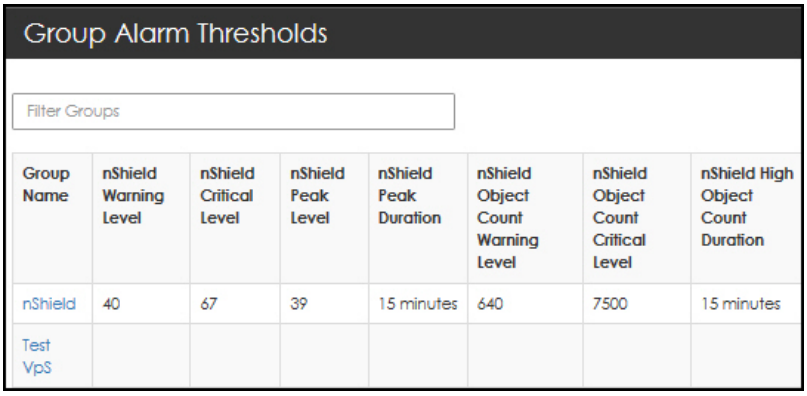
6.4. Group Alarm Thresholds

The Group Manager role can view and set alarm thresholds.



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

   The **Group Alarm Thresholds** page opens:



2. Select the Group that you would like to set.
3. Use the slide bars to set the thresholds.
4. Set the values in the **nShield High Object Count** fields based on your preferences.
5. 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:

- Every 10 minutes the alert detection will compute the previous 10-minute nShield utilization for each device in the group.
- If the utilization is over the Critical Threshold, a critical event is generated.
- If the utilization is 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

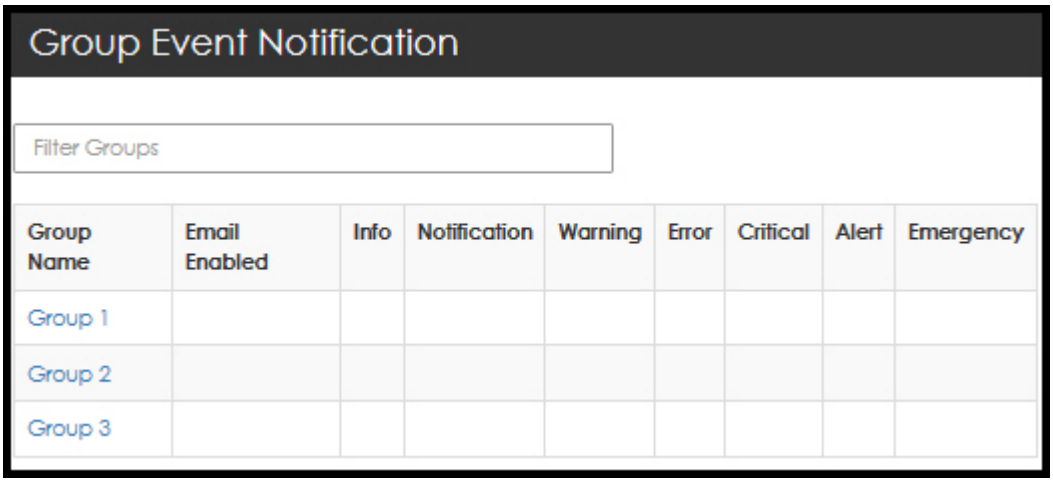
peaked above a selected percentage during a pre-configured amount of time in minutes.

Both sets of alerts are disabled by default.

6.5. Group Event Notification

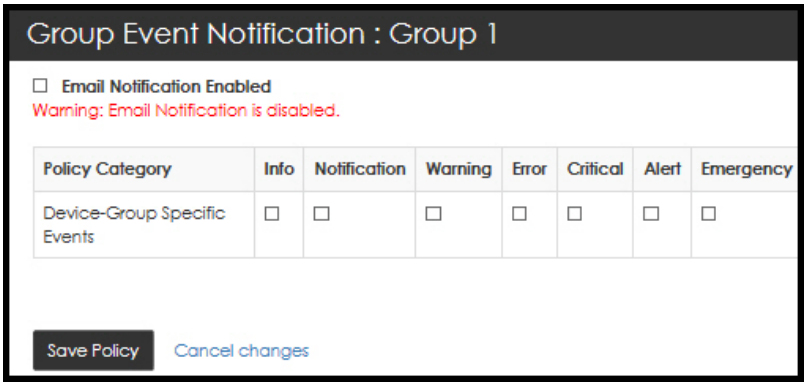
The group manager role has the capability to view and set group event notification via email.

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



2. Select the Group for notification.

   The Notification Warning message displays.



3. Select **Email Notification Enabled**.
4. Select the alert type.
5. Select **Save Policy**.

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

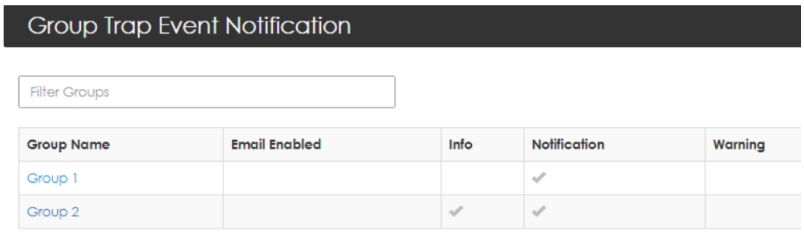
> device is enrolled and to which the manager has been assigned the Group Manager role.

6.5.1. Assign SNMP notification policies for groups

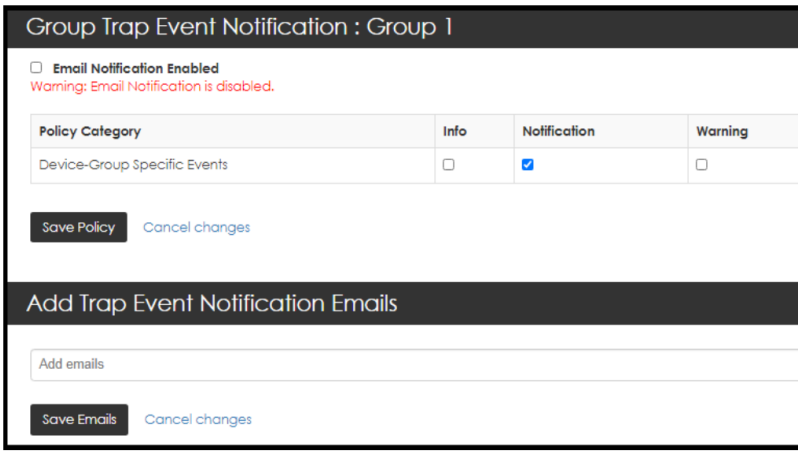
Group Managers manage which email addresses are sent notifications when a trap event occurs in the device group. For instructions on how to enable notifications by trap groups, see Assign SNMP Notification Policies for Trap Groups.

To assign Notification Policies for device groups:

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



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



   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

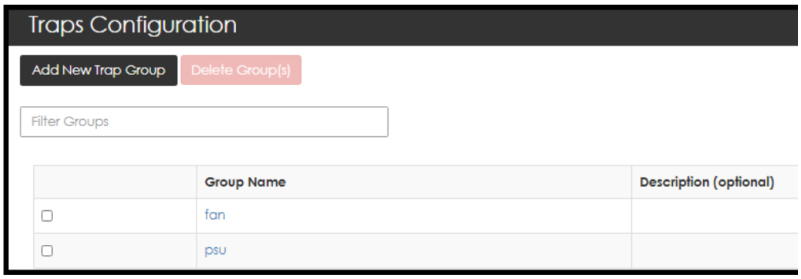
Group Managers create, edit, and manage trap groups that contain traps and a list of email addresses where notifications are sent when a trap event occurs.

For instructions on how to enable notifications by device groups, see Assign SNMP notification policies for groups.

To assign notification policies for trap groups:

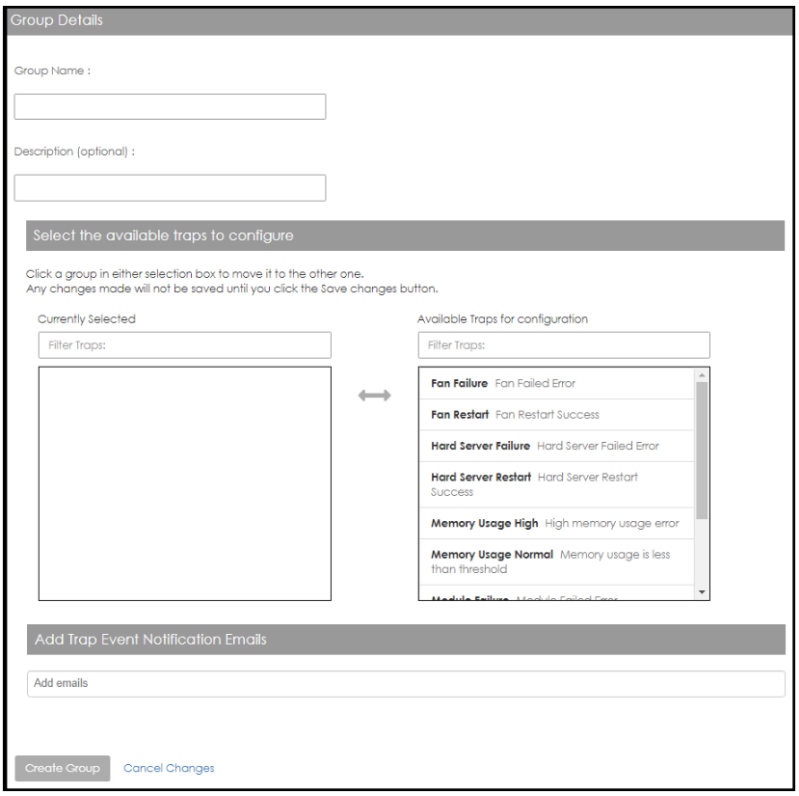
1. Navigate to: **Configuration** > **Trap Settings**.

    The **Trap Configuration** page is displayed.



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

    The **Group Details** page is displayed.

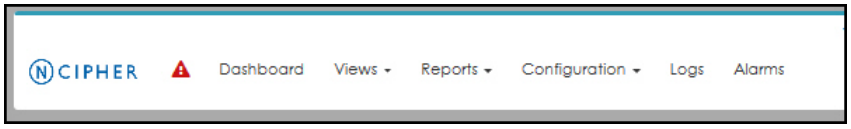


3. Enter a name for the new trap group.
4. Select traps from the list of **Available traps**. For traps supported in nShield Monitor, see Support for nCSNMP traps.
5. Add the email addresses to which the notifications should be sent when a trap event occurs. There is no limit on the number of emails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

   The **Trap Configuration** page is displayed.

7. Logs

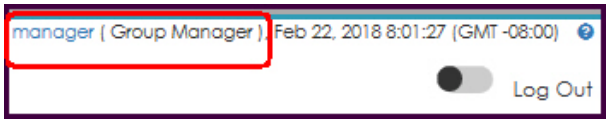
The logging capability of nShield Monitor provides a view of all ongoing events that occur in the system. Organizations can track all activities pertaining to their estate of HSMs and clients, and pro-actively evaluate a preventative maintenance strategy.

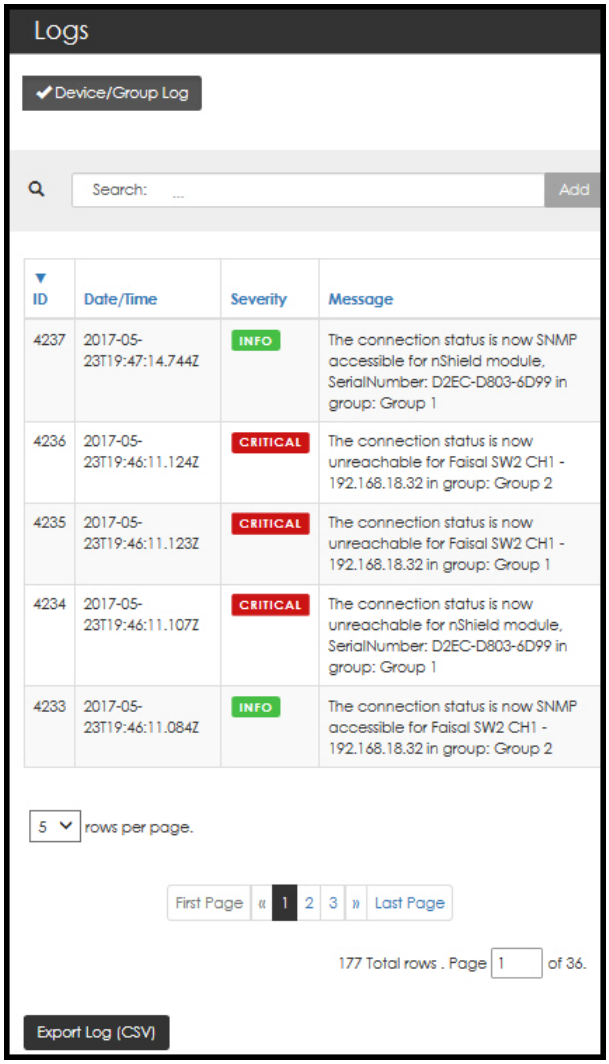


The default sorting is by sequence number.

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.



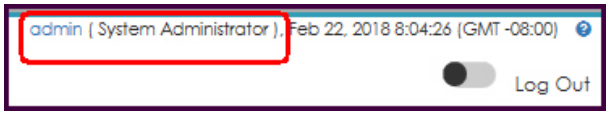


Logs can be exported via CSV format for further analysis.

7.2. Logs available to Administrators

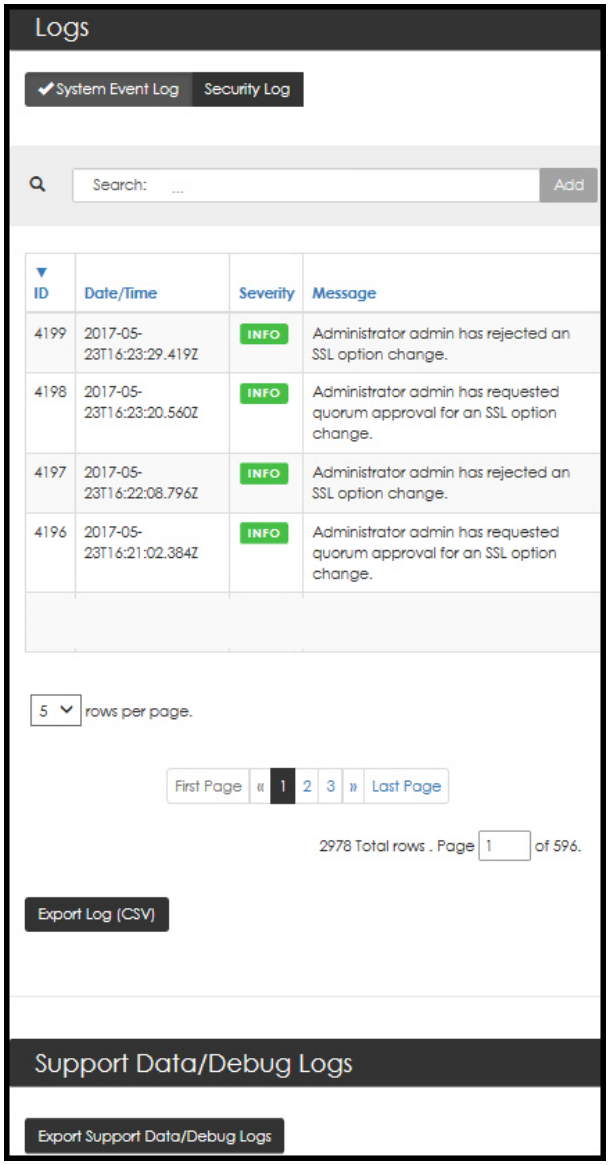
When logged in as an **Administrator**, the **Logs** tab on the main menu bar enables you to:

- View and sort system event logs
- View and sort security logs
- Export logs.



By default, the system sorts logs based on sequence. Clicking on the colored text (such as ID or Date/Time) toggles the order that

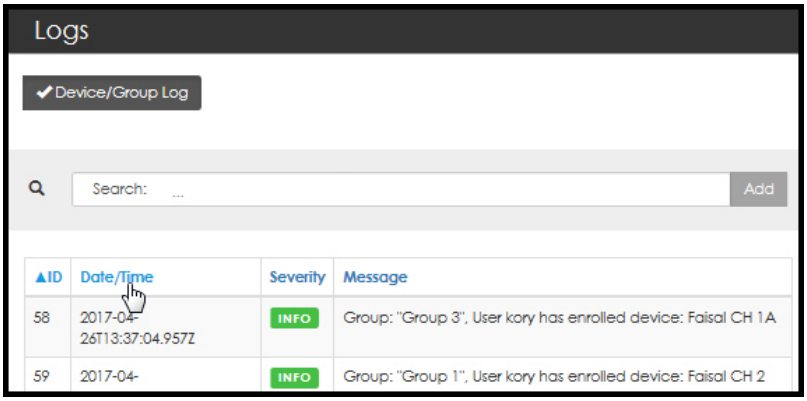
the data is displayed.



7.3. Log sorting

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

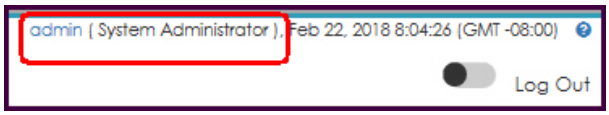
1. Click on the sort condition. For example, Date/Time.



The sorting icon displays as the content is sorted.

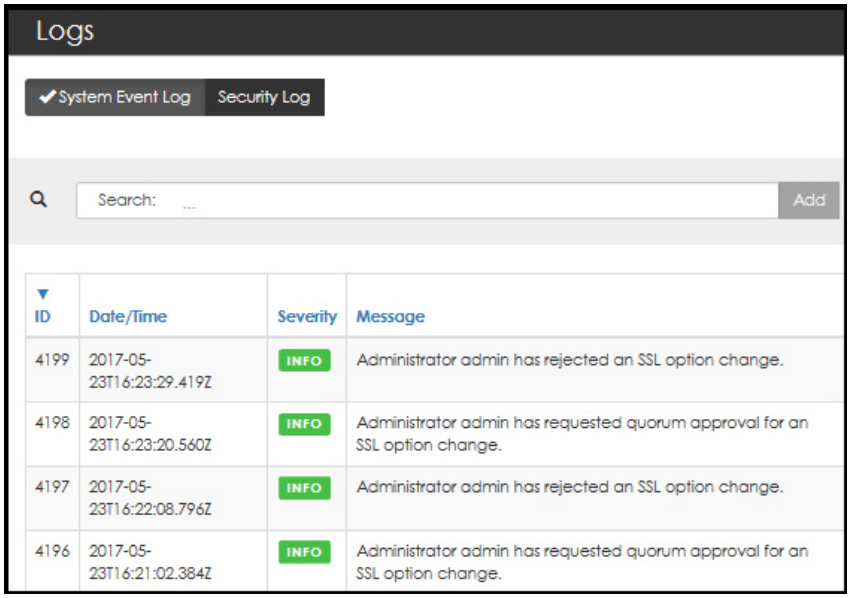
7.4. Log functionality

You are logged in as **Administrator**.



7.4.1. System event log

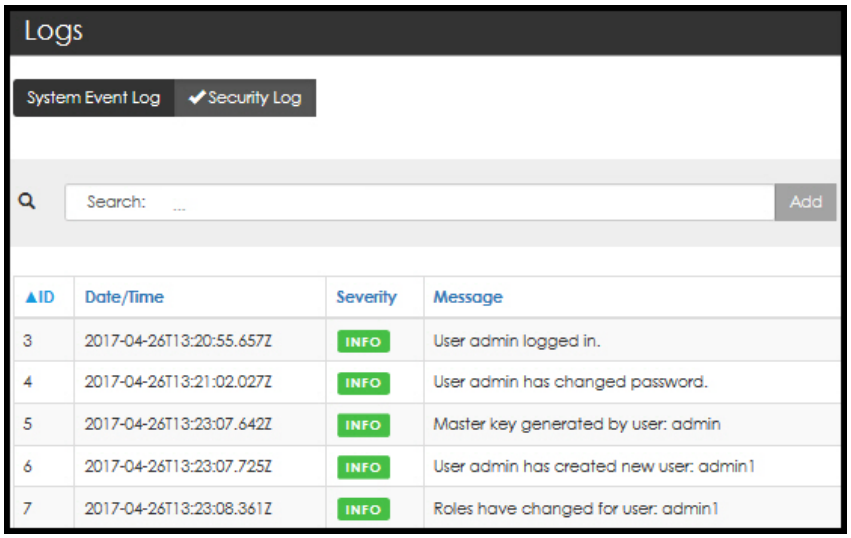
The system event log provides events that correspond to non-security related system events for nShield Monitor.



7.4.2. Security log

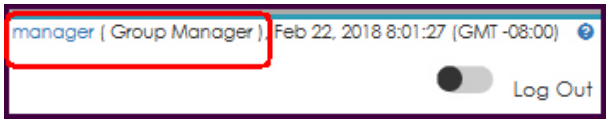
The security log shows events that are related to system level security events. Events such as master key password entry, master key destruction, certificate changes, and changes to other system level security information are noted.

The default for sorting is by sequence number.

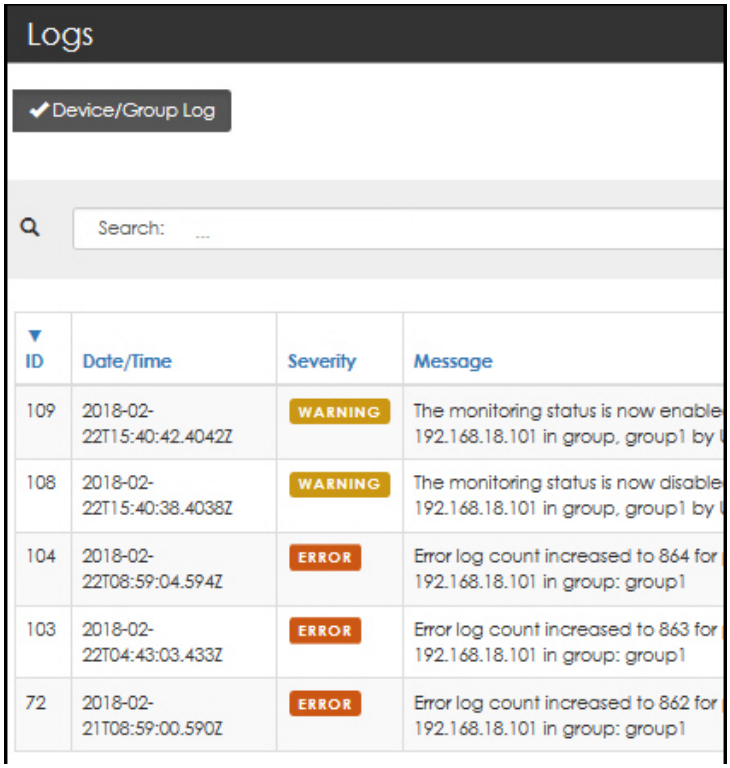


7.4.3. Device/group log

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.

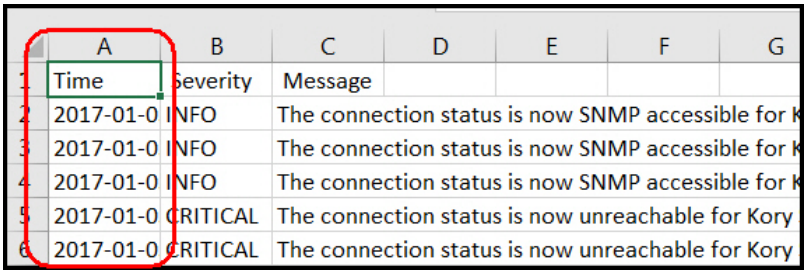


7.4.4. Exporting a log.csv file

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.



   - 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.

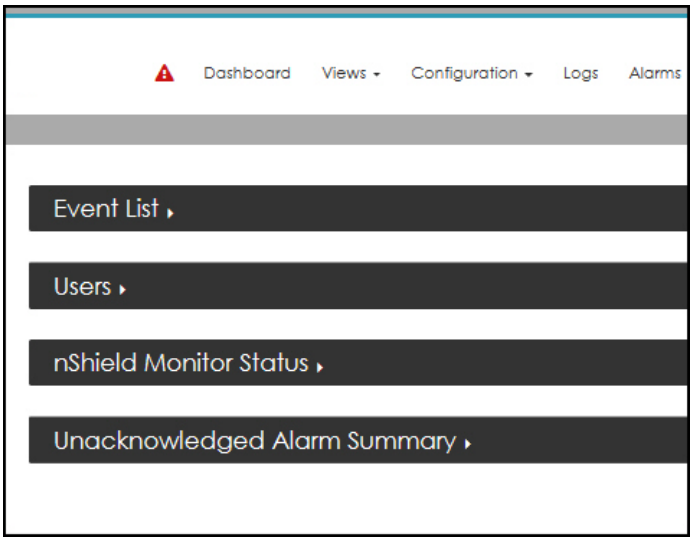
8. Dashboard

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

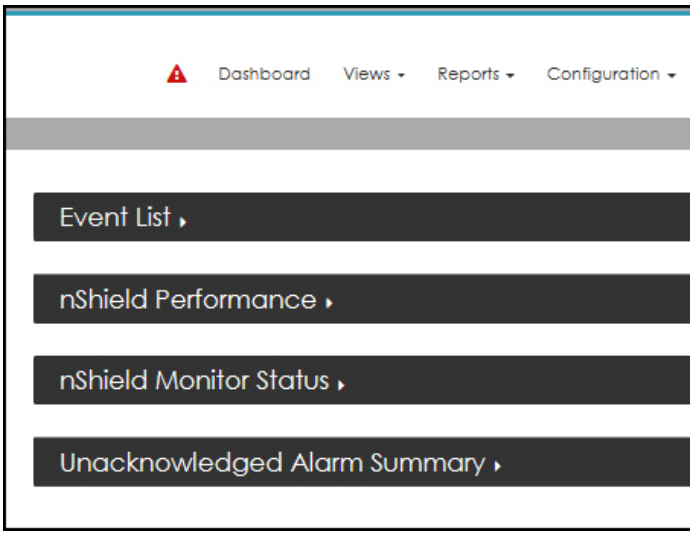
This view provides a snapshot of what is occurring with your estate and provides invaluable information for the day-to-day management of all your organization's HSMs.

The content of the dashboard depends on the login type:

- Logged on as **Administrator**.



- Logged in as **Group Manager**.



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

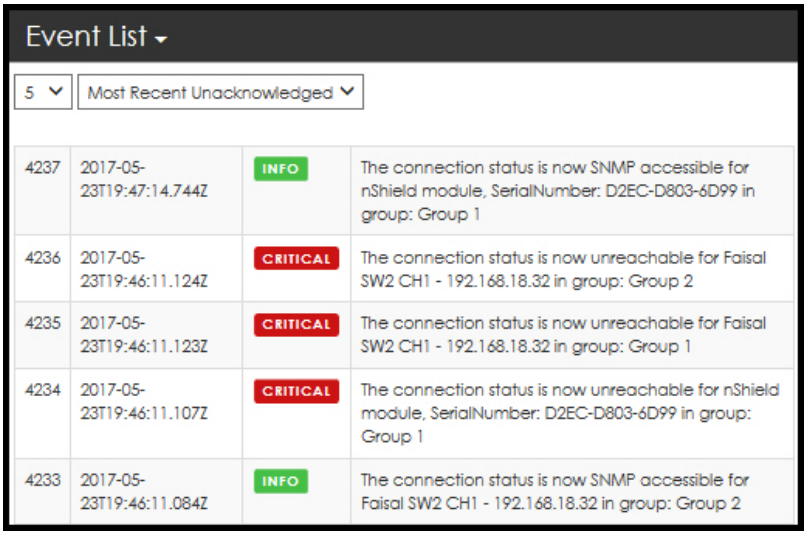
Dashboard views based on logon type

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

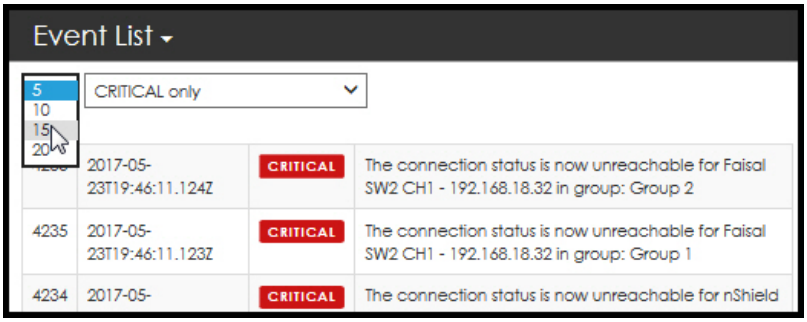
1. Select the **Event List** expansion arrow.



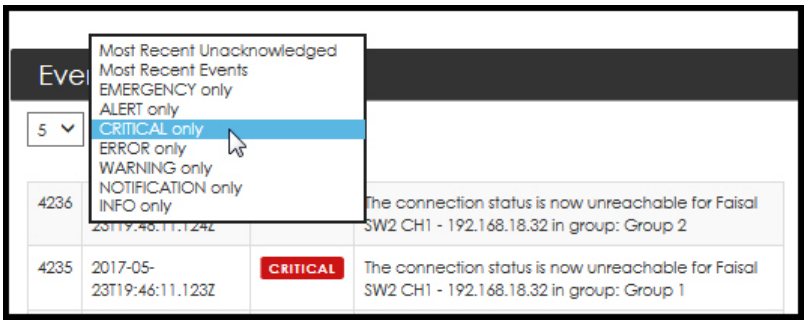
   From this window, you can specify the number of events (default value is 5) displayed and filter according to:

   - Most Recent Unacknowledged (default value)
   - Most Recent Events
   - Alarm level (That is, EMERGENCY ONLY, ALERT ONLY, and so on.)

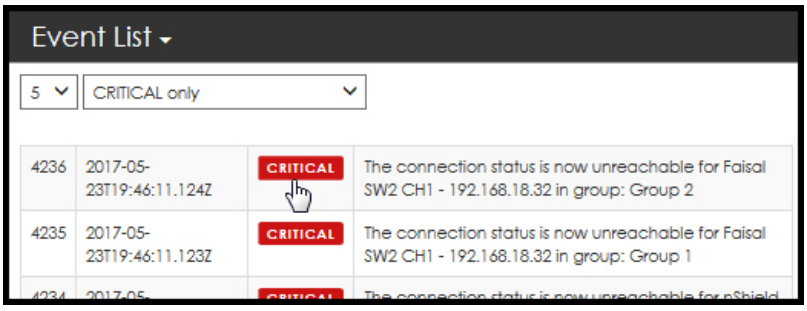
2. Select the drop-down arrow to change how many events are displayed.



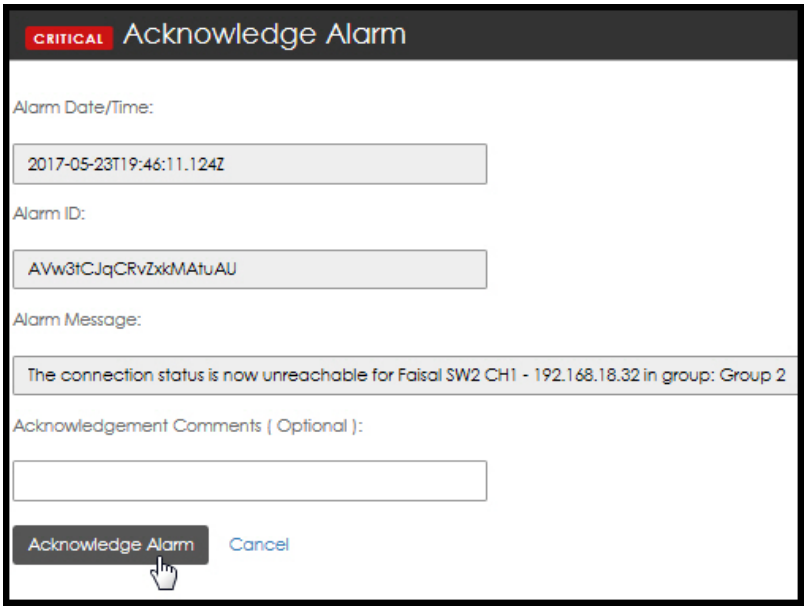
3. Select your preference.
4. Select the drop-down arrow to change which event types are displayed.



5. Select your preference (for example, **CRITICAL only**.)
6. Select the event by clicking on the event type. For example:



The **Acknowledge Alarm** page opens:

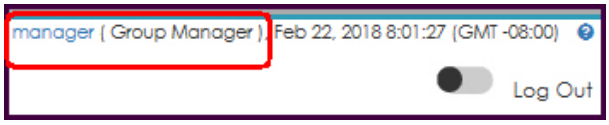


7. Enter Acknowledgment Comments, if needed.
8. Select **Acknowledge Alarm**.

> Selecting **Cancel** returns you to the Dashboard.

8.2. nShield Performance

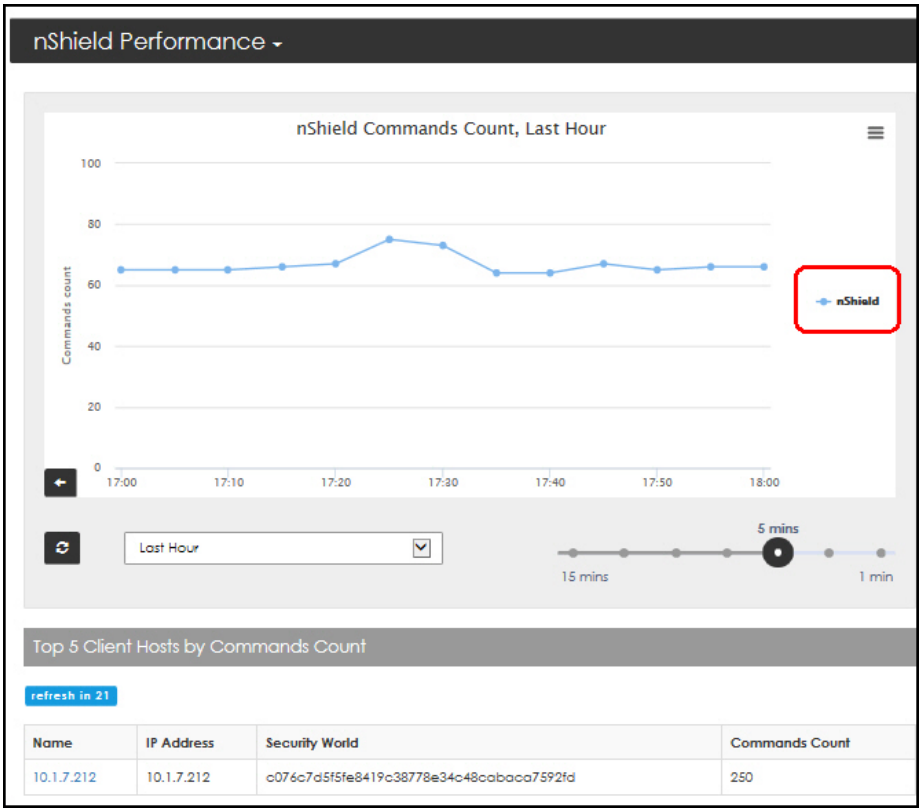
> You are logged in as a Group Manager.



1. Select the **nShield Performance** expansion arrow.

   Two windows open:

   - **nShield Performance**
   - **Top 5 Client Hosts by Command Count**



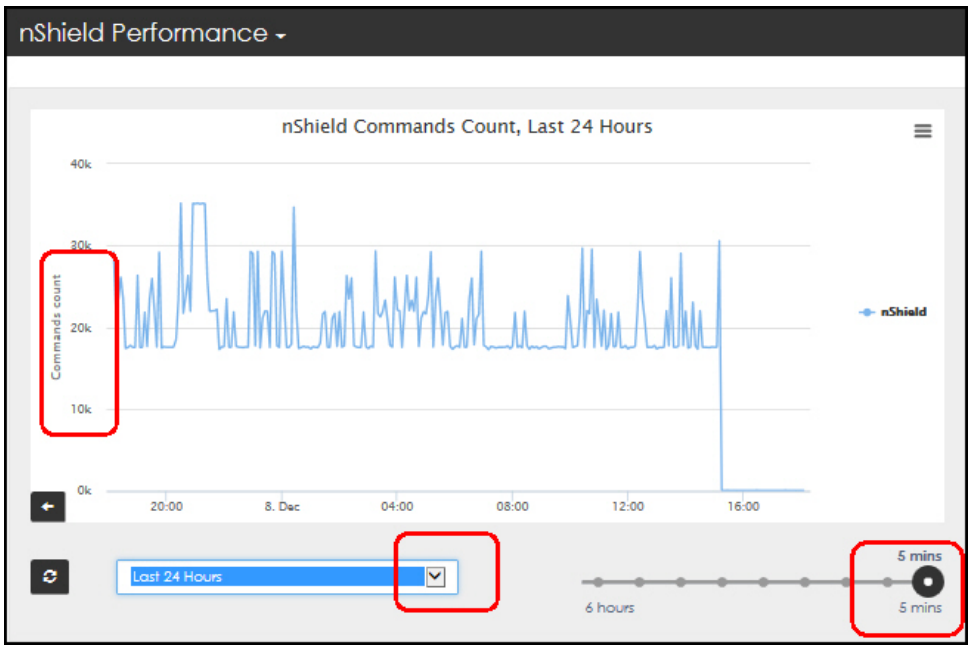
8.2.1. nShield performance window

The performance window provides a customizable graph.

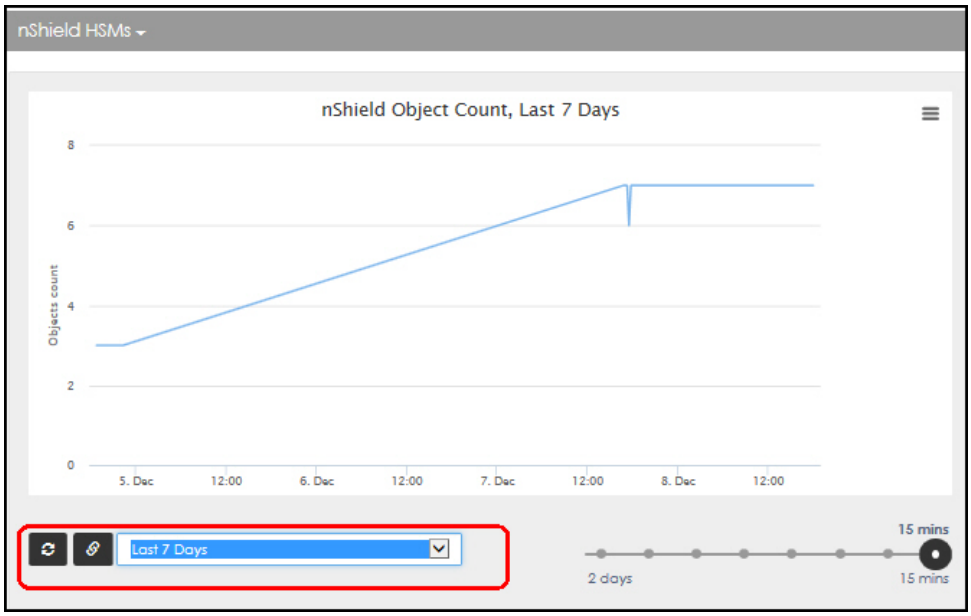
This section provides a basic overview on how to use the customization options. Refer to Client Host Detail Page for greater detail.

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. For example, the "nShield" group, circled in red above.



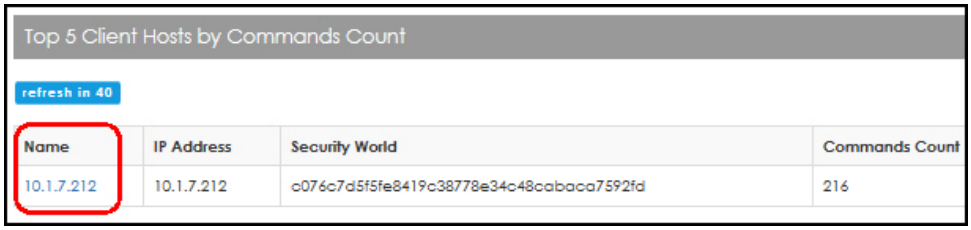
Clicking on Group 1's graph contents opens the **Group Detail For: Group 1** page.



Refer to Group Details for a full description of the **Group Details** page.

8.2.2. Top 5 Client Hosts by Commands Count

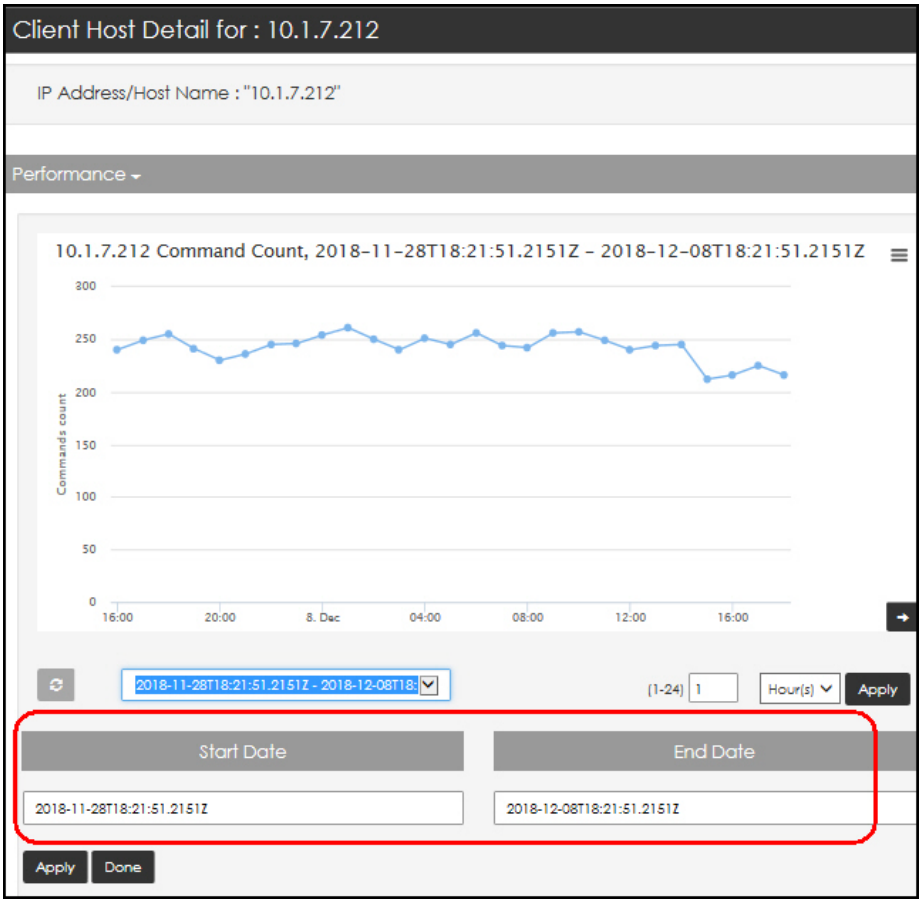
This window also contains a live count down until the next refresh. In the example below, the data will refresh in 24 seconds.



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

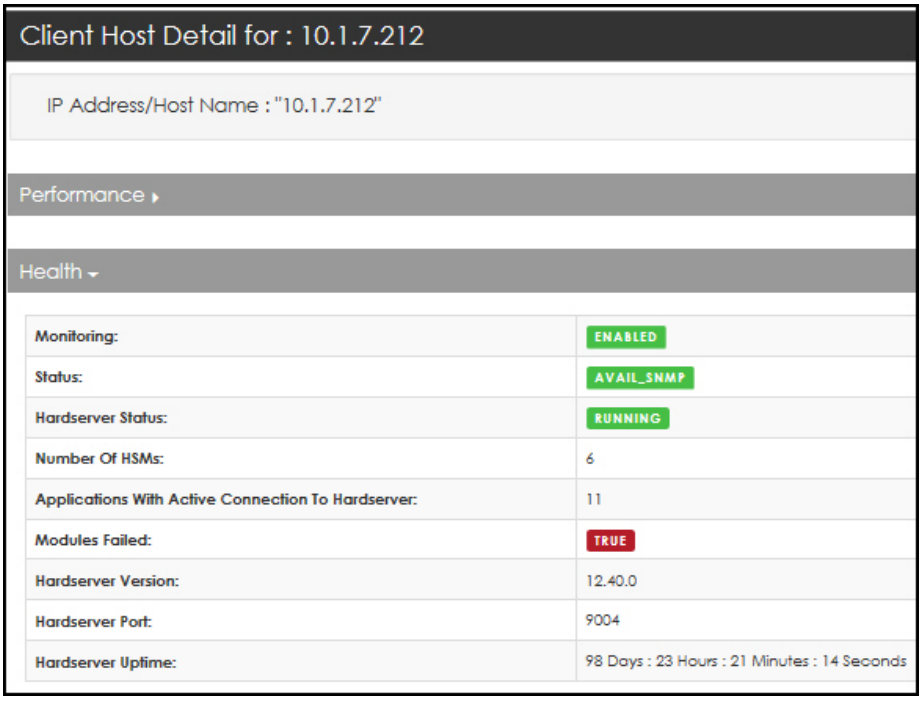
   The **Client Host Detail** page opens.

2. Select the **Performance** expansion arrow.

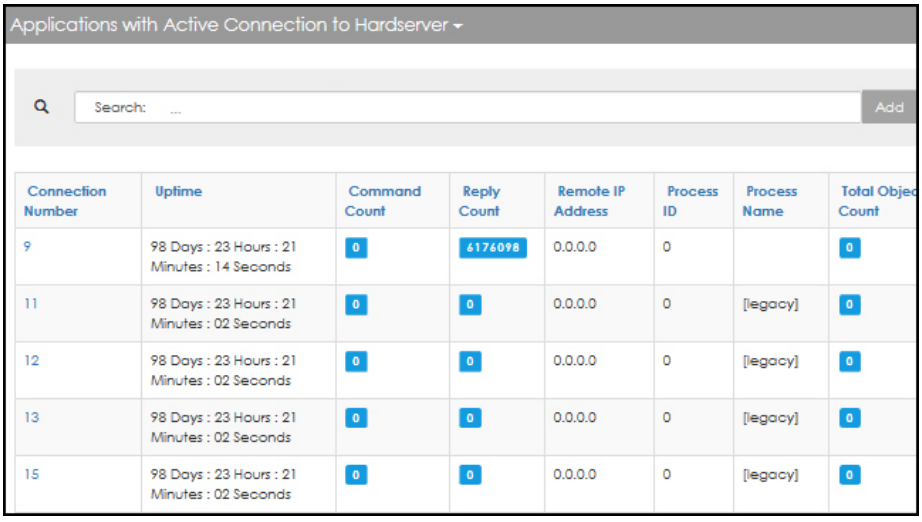


   The **Start Date** and **End Date** selection boxes appear when the custom date option is selected.

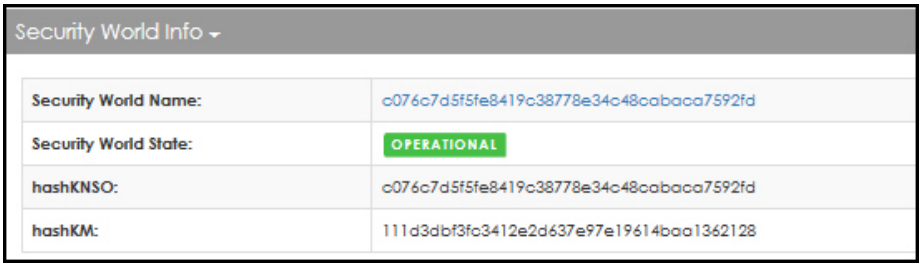
3. Scroll down and click on the **Health** expansion arrow.



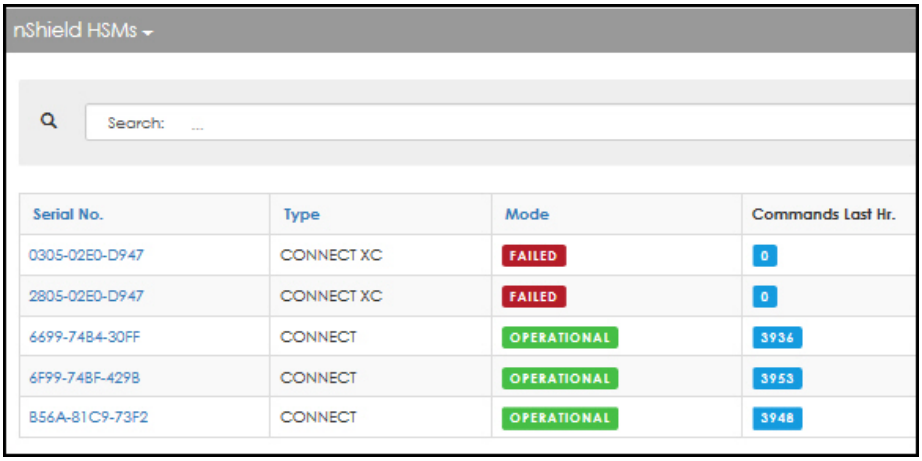
4. Scroll down and click on the **Applications with Active Connection to Hardserver** expansion arrow.



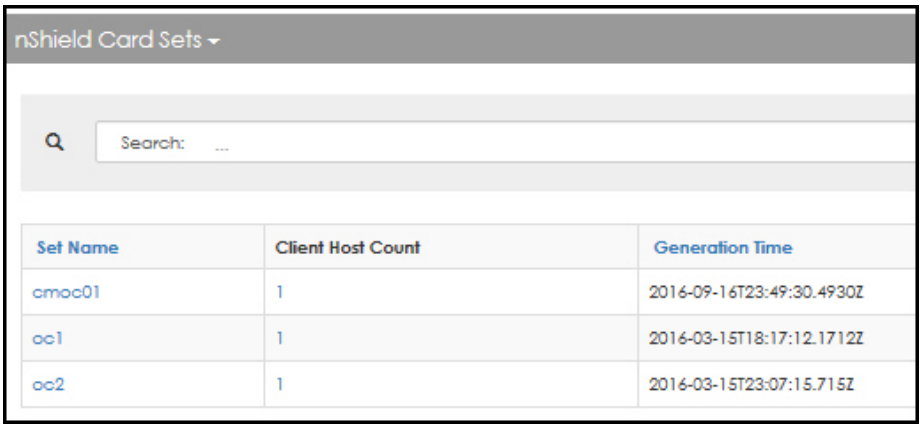
5. Scroll down and click on the **Security World** Info expansion arrow.



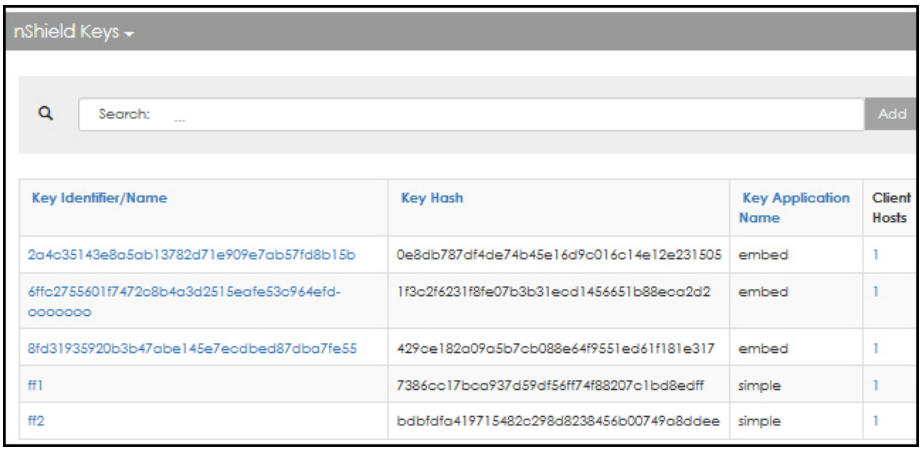
6. Scroll down and click on the **nShield HSMs** expansion arrow.



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



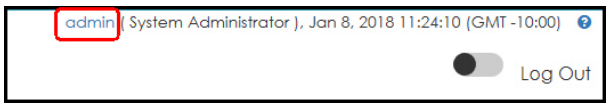
8. Scroll down and click on the **nShield Keys** expansion arrow.



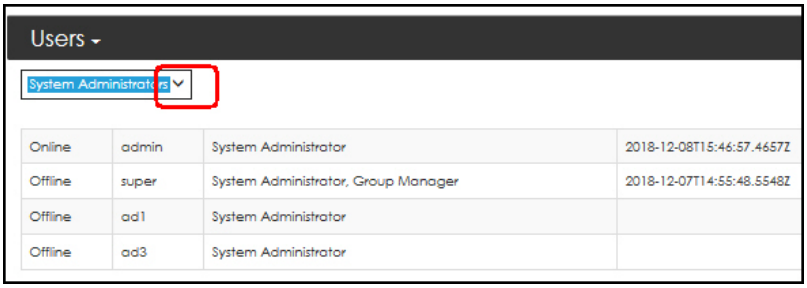
At any time, you can select **Back to Previous Page**.

8.3. Users

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



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



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**.

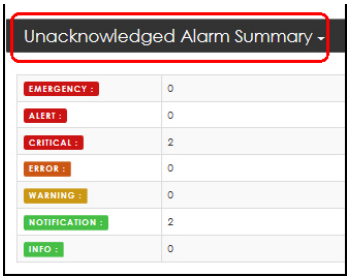
1. Select the **nShield Monitor Status** expansion arrow.

   The status data is displayed.

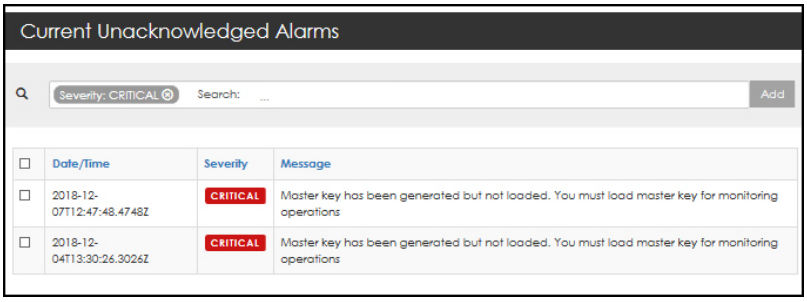
8.5. Unacknowledged Alarm Summary

You are logged in as an Administrator.

1. Select the **Unacknowledged Alarm Summary** expansion arrow.

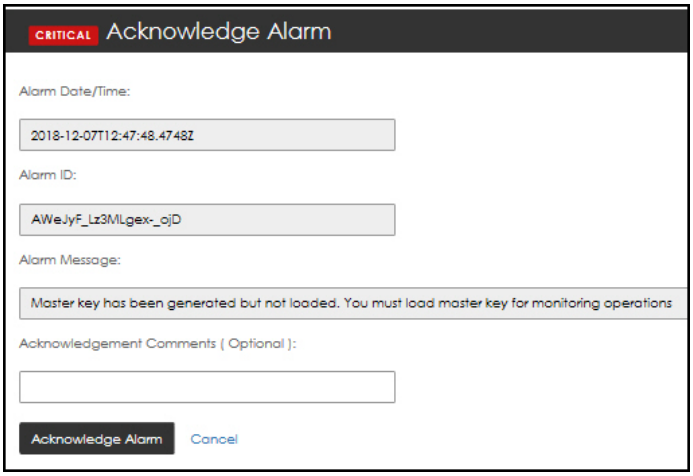


2. Select the alarm type. For example, click on **CRITICAL**. The **Current Unacknowledged Alarms** detail page opens.



3. Select the alarm for acknowledgment.
4. Enter **Acknowledgment Comments**, if required.
5. Select **Acknowledge Alarm**.

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



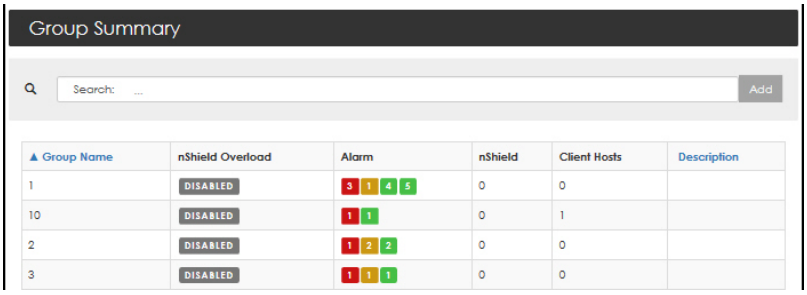
9. Views

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.

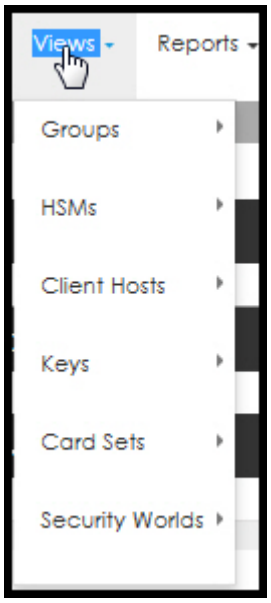


   On this page, you can **sort the display** order of the **Group Name** column and the **Description** column.

Refer to View > Group > Group List for additional information on Administrator options under Group List.

9.2. Logged in as Group Manager

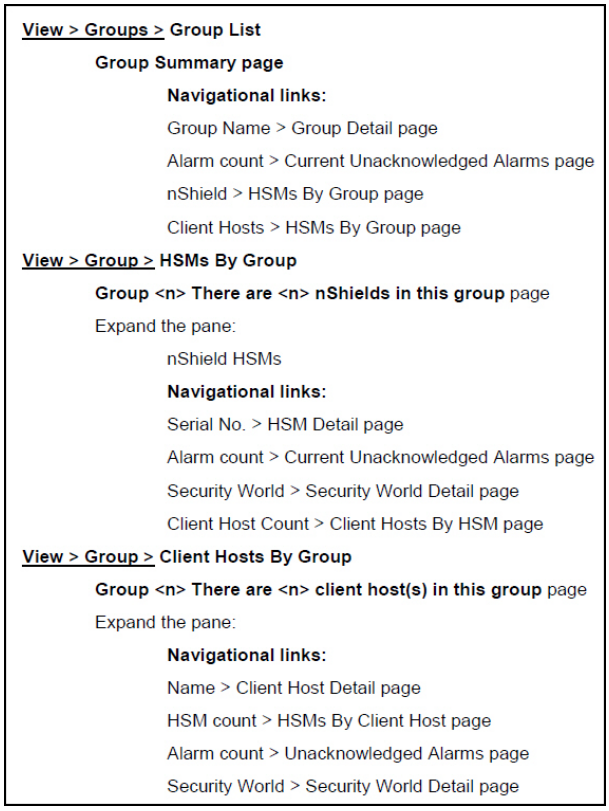
Logged on as Group Manager provides the following navigational options:



9.2.1. View > Groups

The **View > Groups** drop-down menu 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



9.2.2. View > HSMs

The **View > HSMs** drop-down menu 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
- Utilization information
- Host command information
- Overload information
- Alarm information
- Descriptive information.

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

The options in the **View** drop-down menu are directly tied to your logon.

- Administrator
- Group Manager
- Auditor

The Auditor has the same views (that is, drop-down menu options) as the Group Manager. However, the Auditor has no ability to perform any actions. For example, an Auditor cannot acknowledge alarms or enter comments.

9.3.1. Group List > Group Summary - Administrator

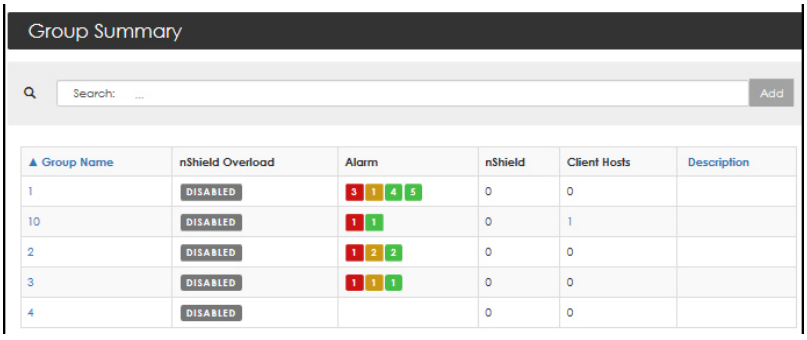
The **Group Summary** page updates every 60 seconds as information is polled.

1. Navigate to:

   Views > Groups > Group List

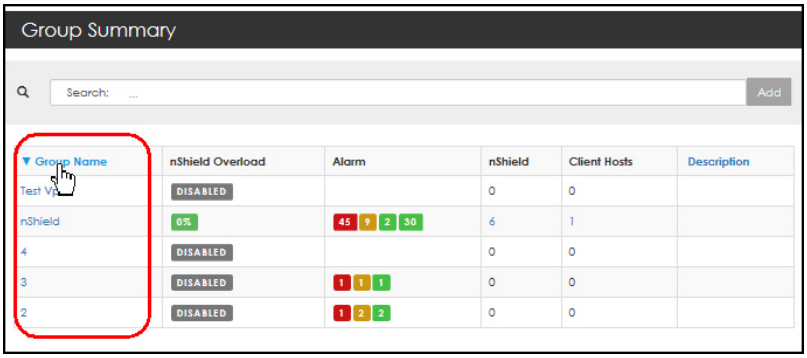
   The **Group Summary** page opens.

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

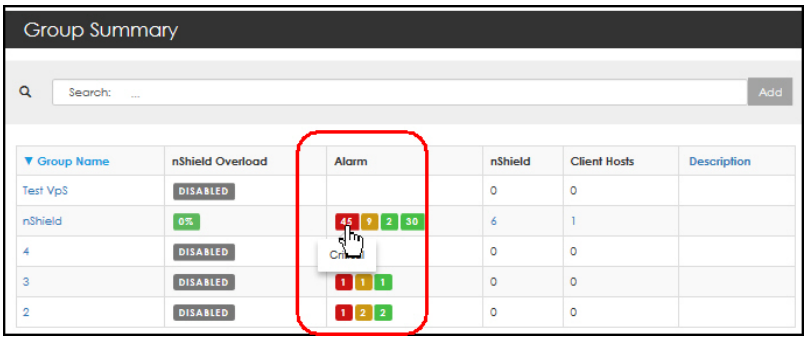


As an **Administrator**, you are able to sort the data displayed.

Blue column headers indicate that the contents of the column can be sorted. Black column headers indicate that the contents of the column **cannot** be sorted.



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



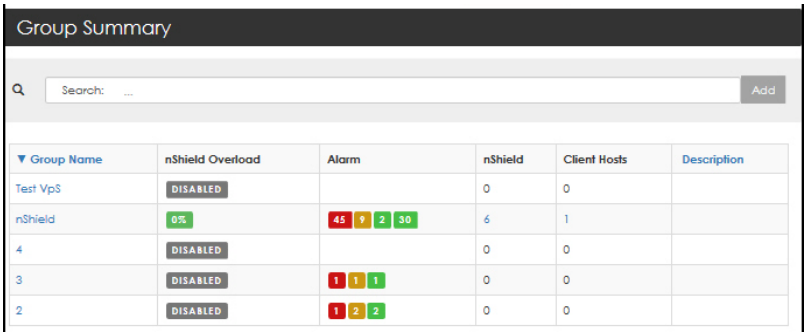
9.3.2. Group List > Group Summary - Group Manager

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.

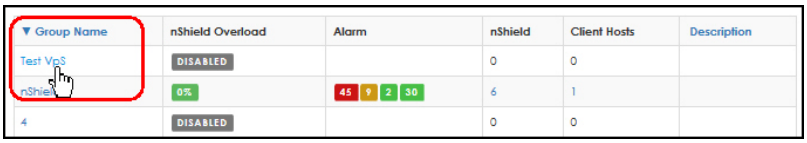


9.3.3. Group Summary page - Navigation options

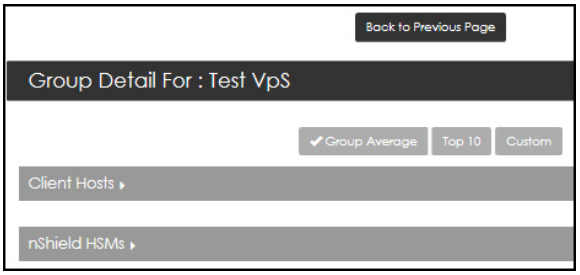
The **Group Summary** contains three navigation points.

Selecting any one of the following opens a new page:

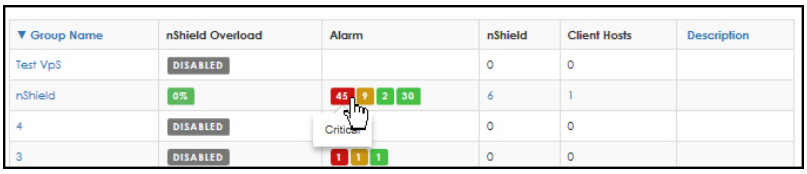
- A specific **Group Name**



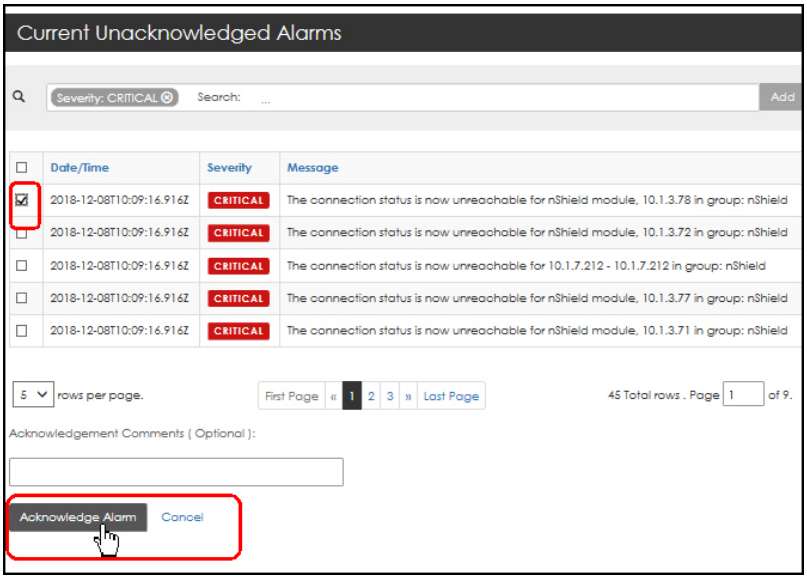
The **Group Detail** page opens.



- A specific **Alarm**

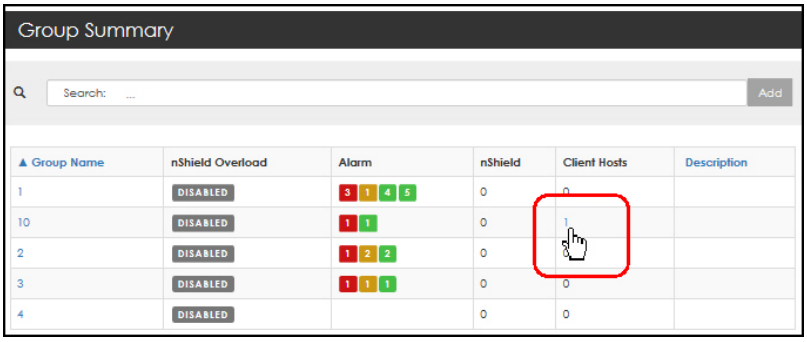


The **Current Unacknowledged Alarms** page opens.

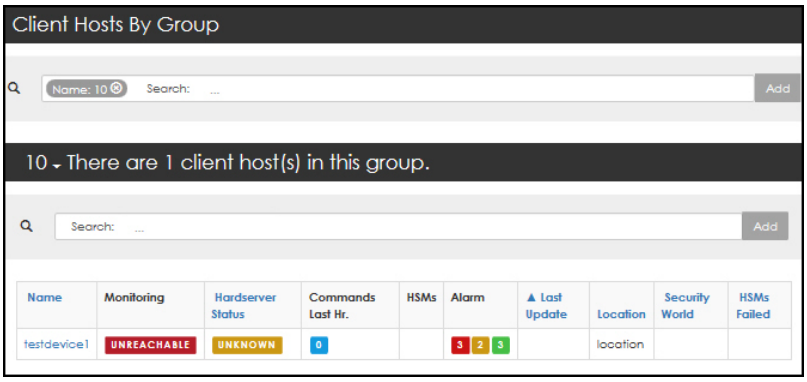


You can acknowledge the alarm by checking the box to open the **Acknowledge Alarm** page.

- A specific entity



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

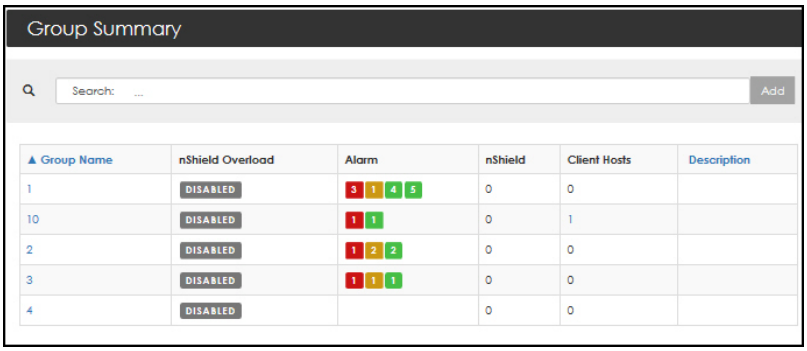


9.3.3.1. Alarms Acknowledgment Views

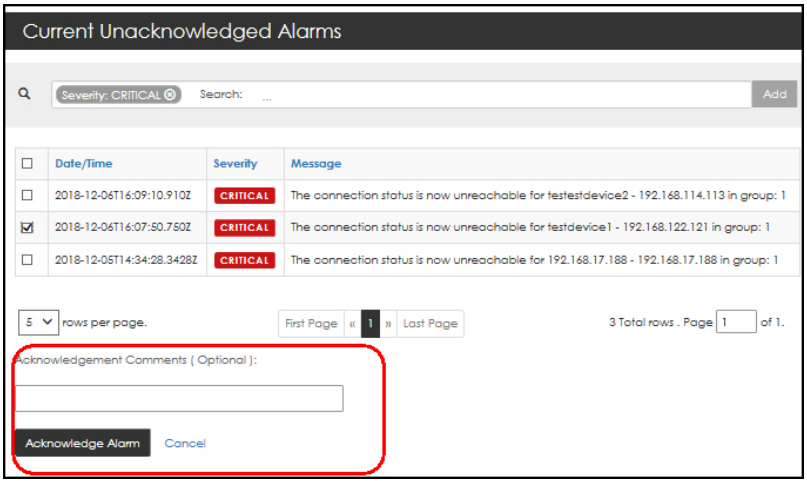
1. Navigate to:

   View > Groups > Group List

   The **Group Summary** page opens.

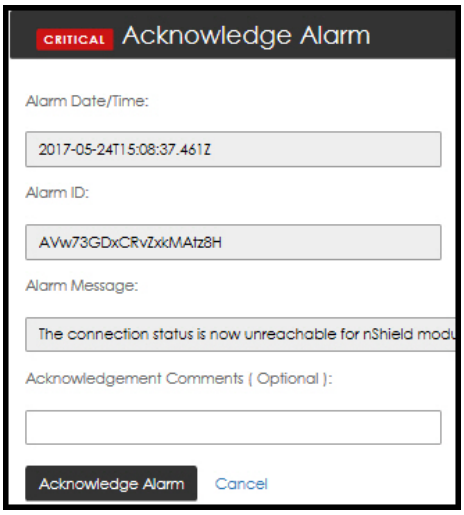


2. Select any number in the **Alarm** column.
3. After **Current Unacknowledged Alarms** page opens, optionally enter a comment and then select **Acknowledge Alarm**.



Selecting multiple boxes allows you to simultaneously acknowledge multiple alarms.

If you click directly on the Alarm Severity (for example, click directly on **CRITICAL**), the **Acknowledge Alarm** page opens.



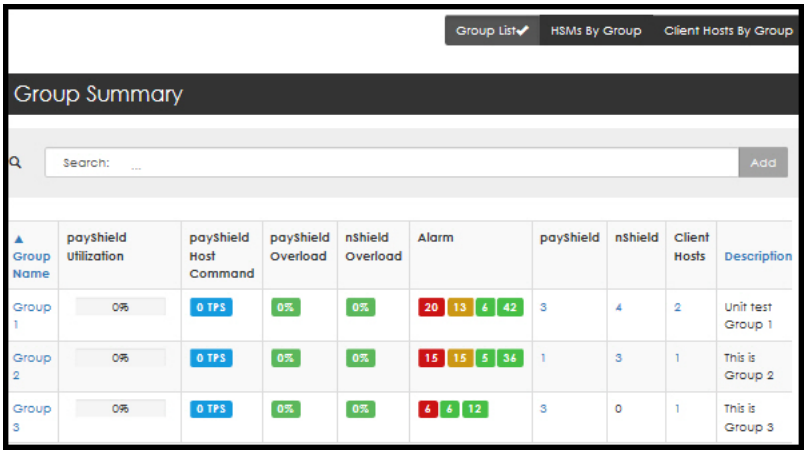
4. Enter comments (optionally) and then select **Acknowledge Alarm**.

9.3.3.2. Navigating to the Group Detail page

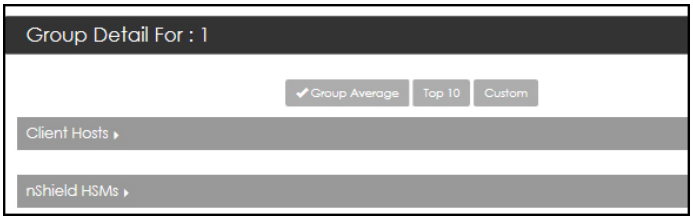
1. To get to the **Group Detail** page, navigate to:

   View > Groups > Group List

   The **Group Summary** page opens.

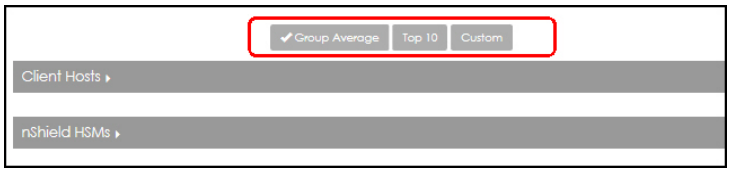


2. From the **Group Name** column, select a group. The **Group Detail** page for the selected group appears. For example:



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

Each window on the **Group Detail** page can be filtered based on Group Average, Top 10, or based on a Custom list of devices. For example:



Each of these views shows the average of the data collected for the interval period selected (5 minutes, 15 minutes, and so on).

Line colors in the chart are used to designate a specific device. Click on the items in the color index, (for example, 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.

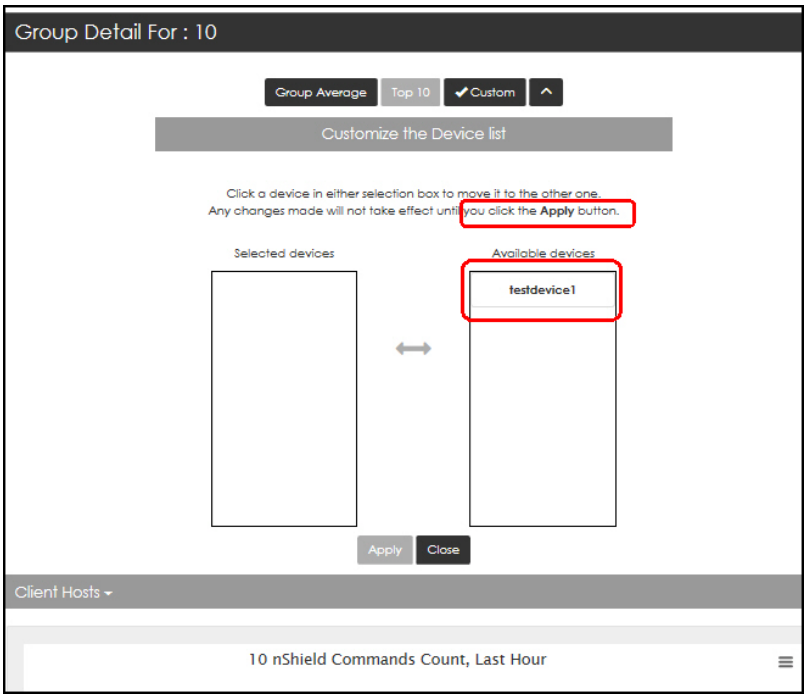
- Select the drop-down arrow on the time period bar to modify the time period

to view.

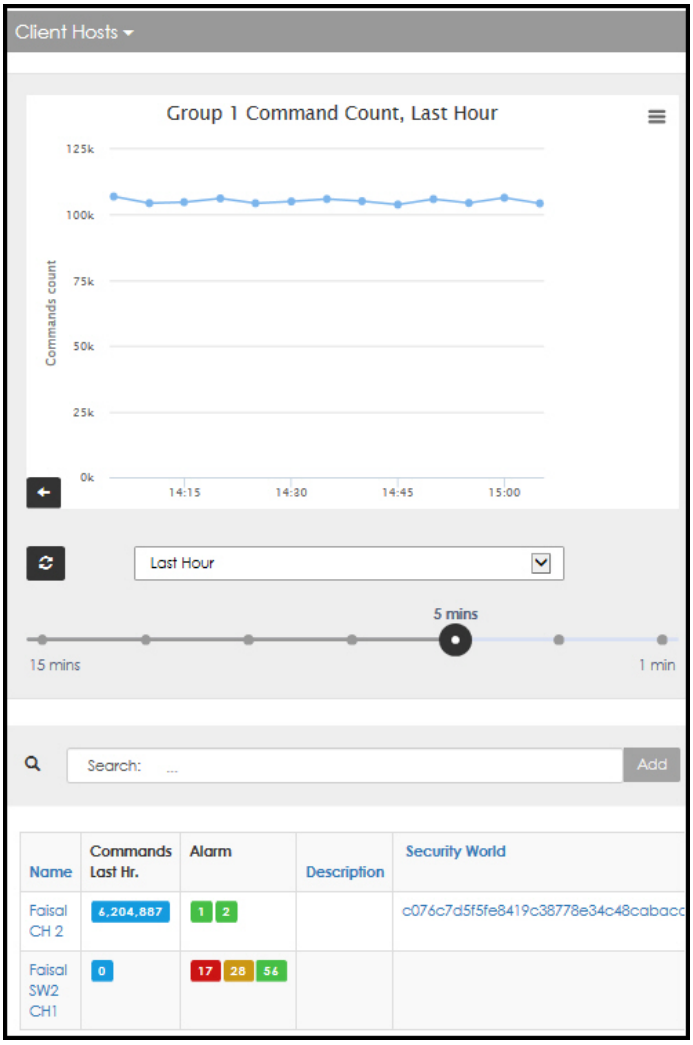
The Custom Range selections are in the UTC time zone.

- Use the sliding mechanism to change the intervals.

Example of **Custom**:



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

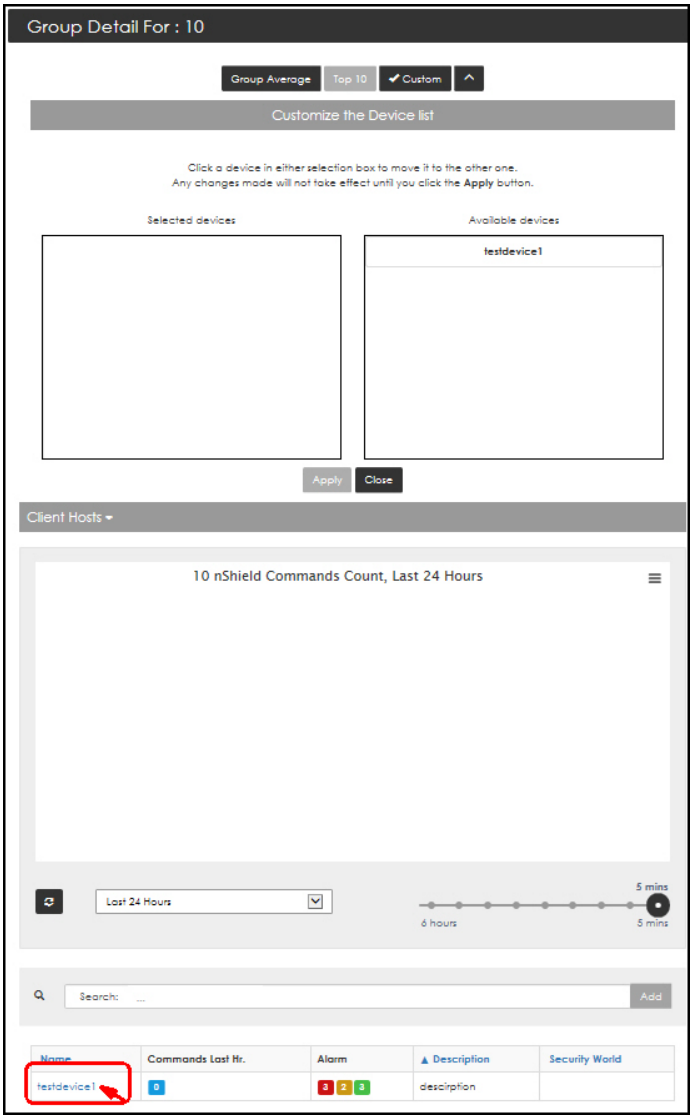


Each graph can be printed or exported in CSV.

9.3.3.4. Group Detail page - Client Hosts

The **Client Hosts** window displays:

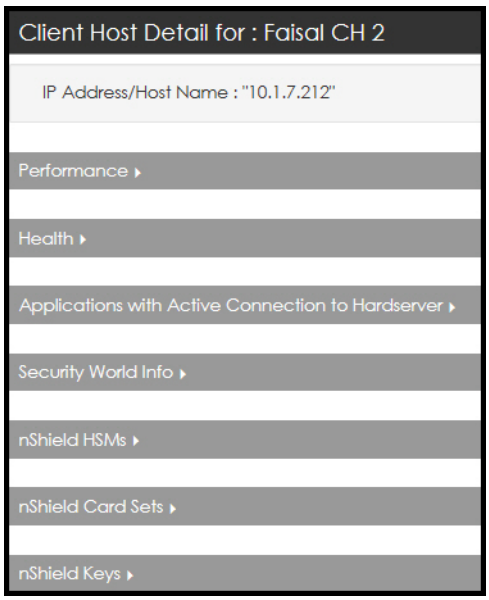
- **Graphed** command count based on command count per time block:



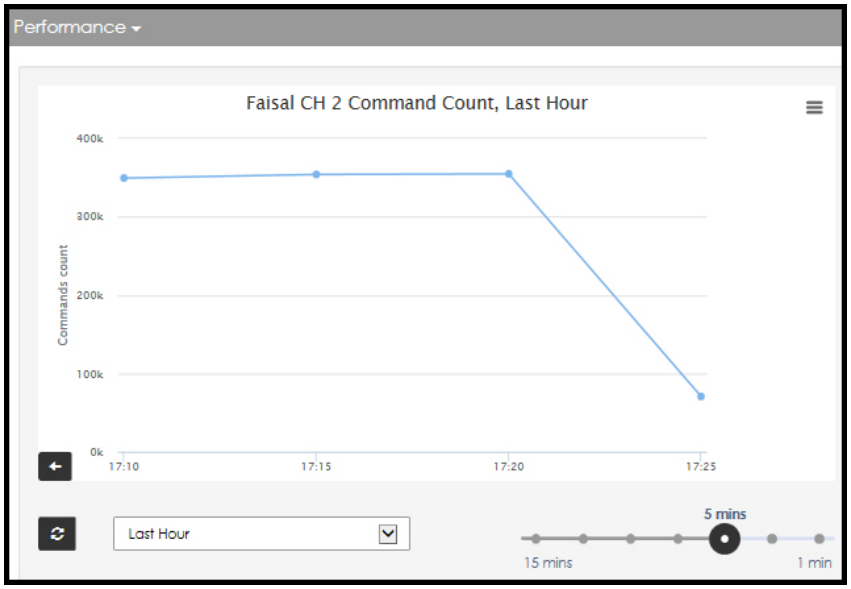
- Clicking on the device name opens the **Client Host Detail** page for that device.

9.3.3.5. Client Host Detail page - Overview

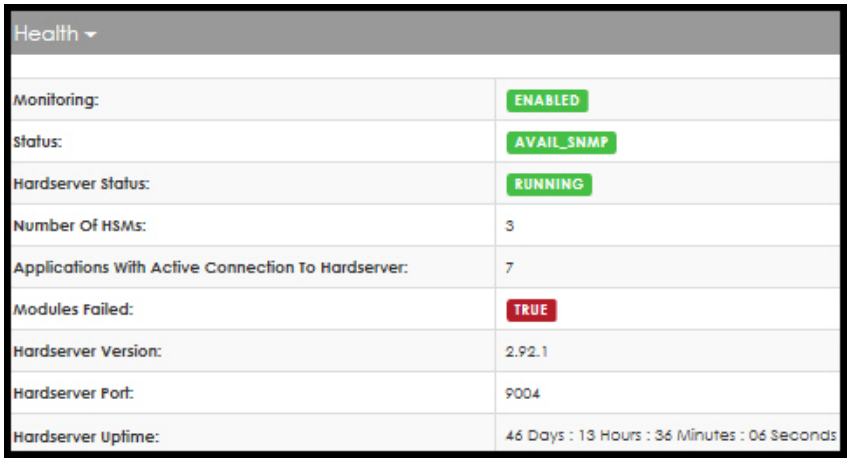
Select the expansion arrow to open the windows.



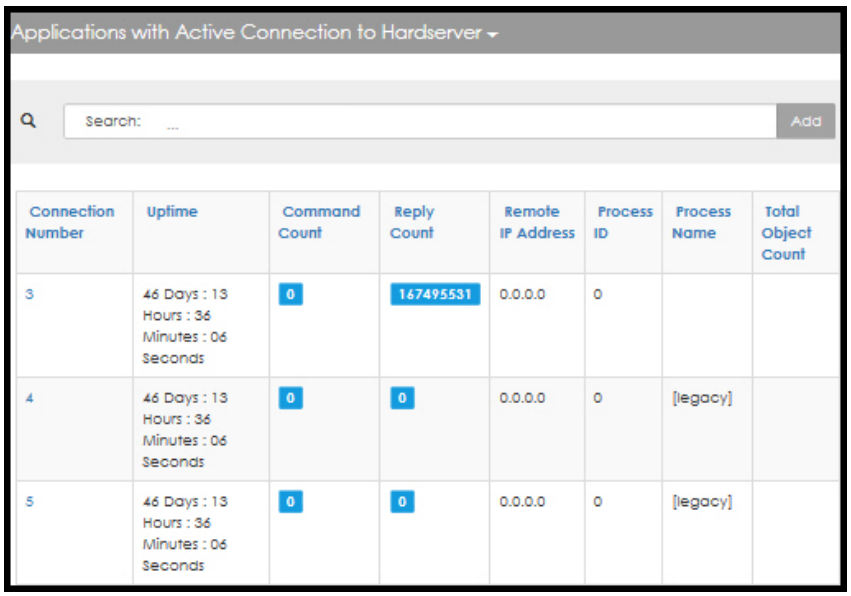
9.3.3.6. Client Host - Performance window



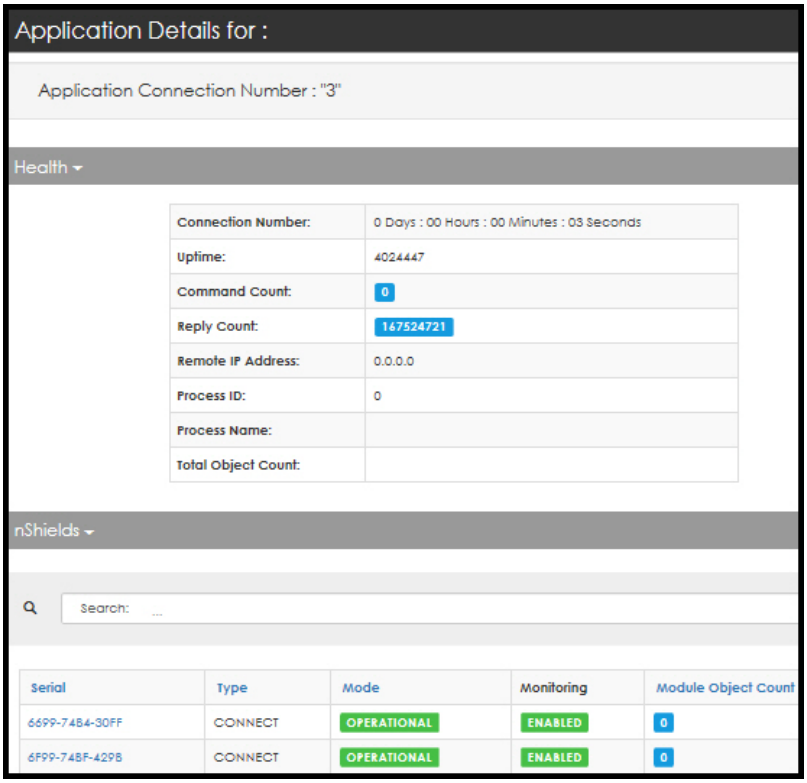
9.3.3.7. Client Host - Health window



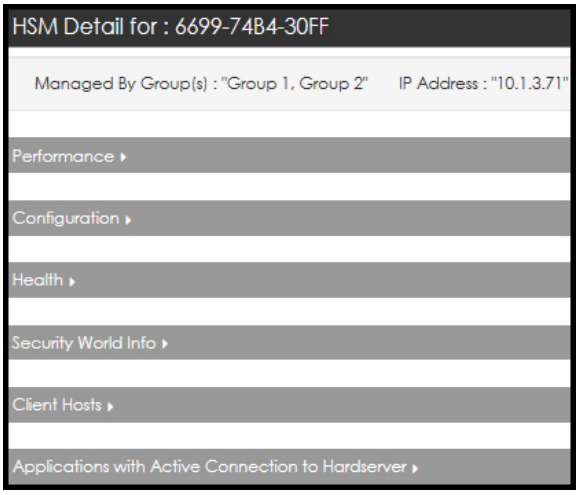
9.3.3.8. Client Host - Applications with Active Connection window



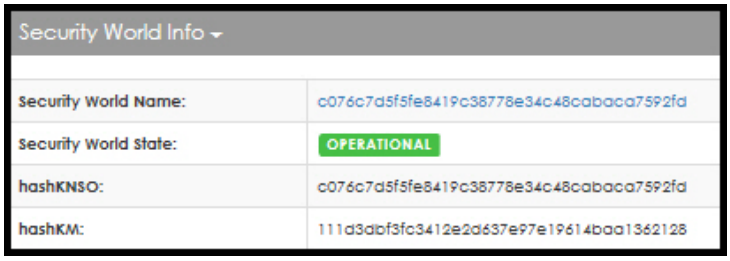
- Click on the blue columns to reverse the sort order, based on preference.
- Select a specific **Connection Number** to open the connection's **Application Details** page.



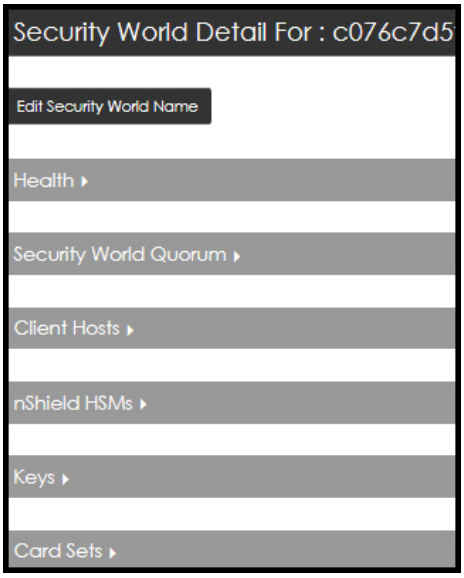
- Select a specific Serial number to open the **HSM Detail** page.



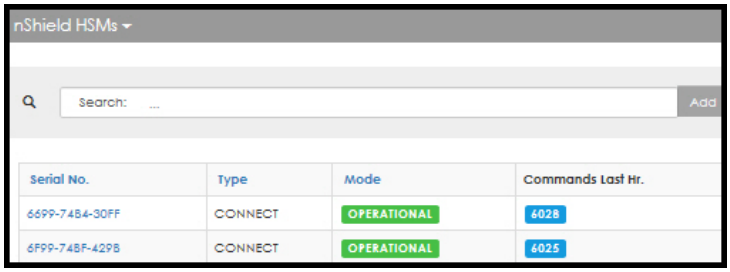
9.3.3.9. Client Host - Security World Info window



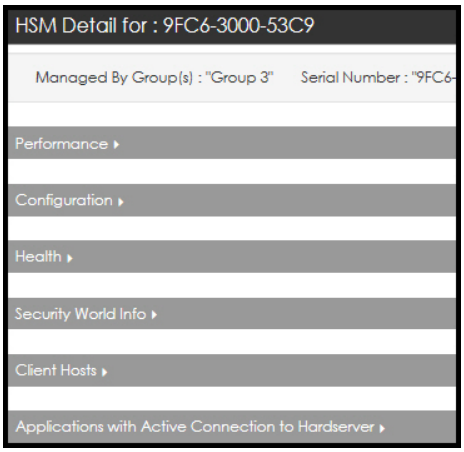
- Select the Security World identifier to open the **Security World Detail** page.



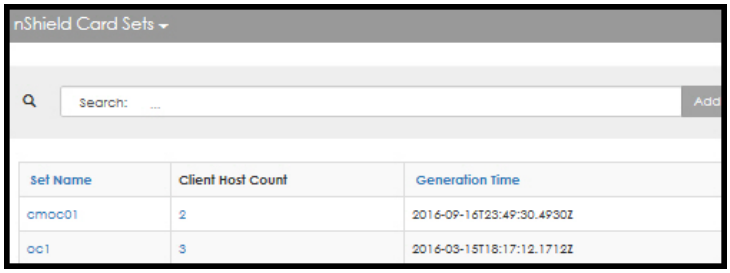
9.3.3.10. Client Host - nShield HSMs window



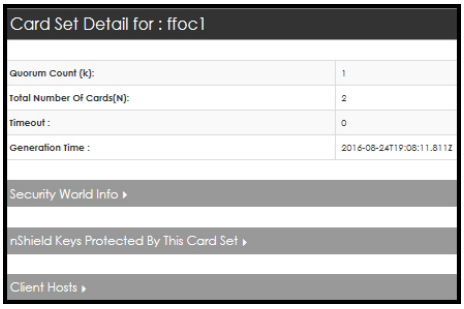
- Select a specific Serial Number to open the **HSM Detail** page.



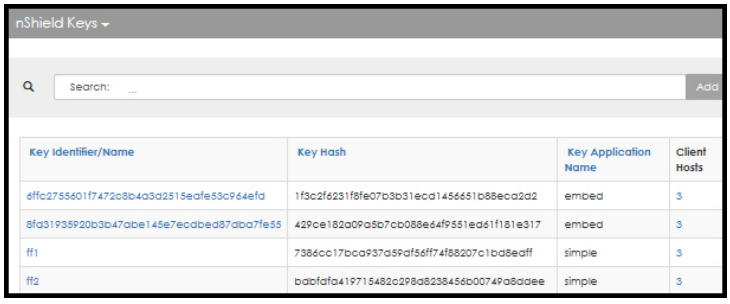
9.3.3.11. Client Host - nShield Card Sets window



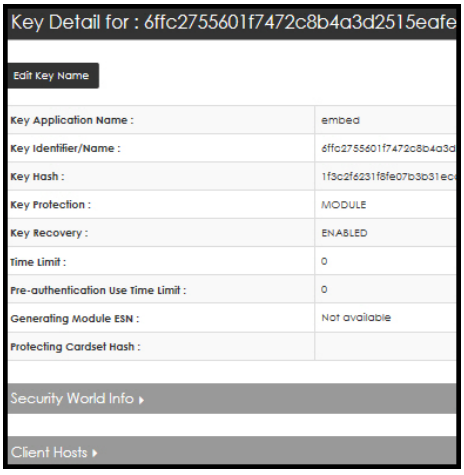
- Select a specific Set Name to open the **Card Set Detail** page.



9.3.3.12. Client Host - nShield Keys window



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



9.4. Additional Views available to the Group Manager

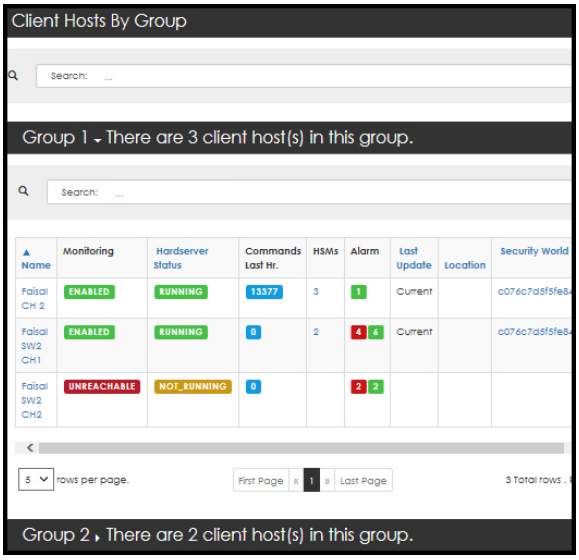
The **View** drop-down menu provides options that are not offered to the Administrator:

- 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**.

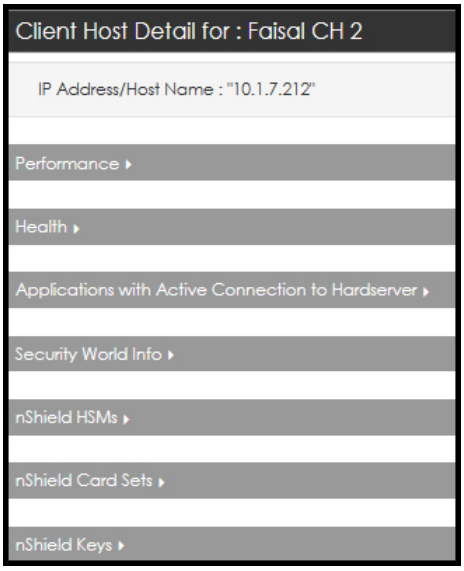
   The **Client Hosts By Groups** page opens.



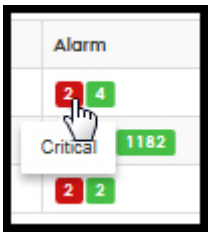
The **Client Hosts By Group** page contains three navigation points. Selecting any one of the following opens a new page:

- A specific **device name**.

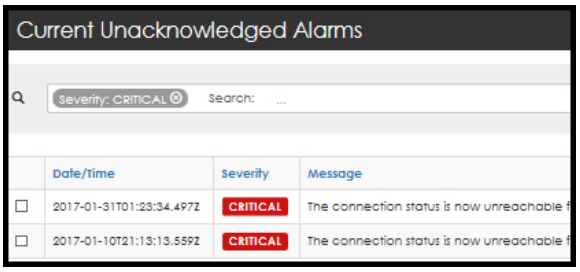
  The **Client Host Detail** page opens.



- A specific **Alarm**



The **Current Unacknowledged Alarms** page opens.



- A specific Security World

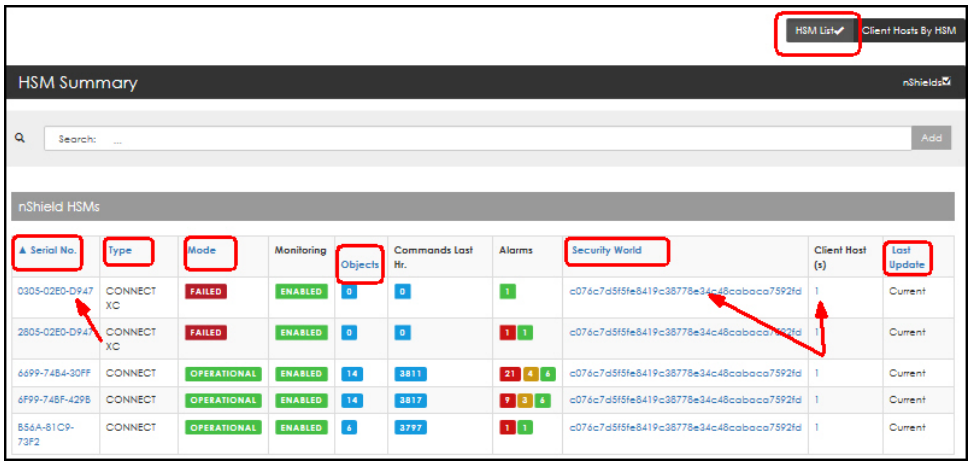
The **Security World Detail** page opens.

9.4.2. View > HSMs > HSM List

1. Navigate to **Views > HSMs > HSM List**.
2. Select **HSM List**.

   The **HSMs Summary** page opens.

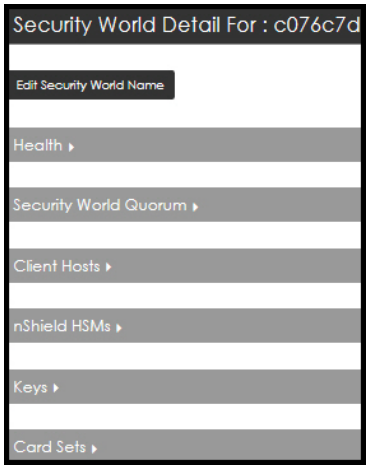
With the HSM Summary page open, you can toggle between views by selecting **Client Hosts by HSM**. See the upper-right corner of the screen.



On this screen:

- A colored column heading indicates that filtering is available.
- A blue icon or blue text indicates that an action is available.
- You can select individual devices to open new windows.

For example, select a security world to display the **Security World Detail** page.

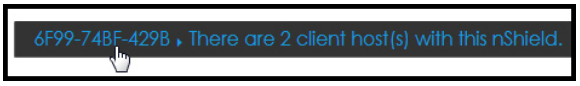


9.4.3. View > HSMs > Client Hosts by HSM

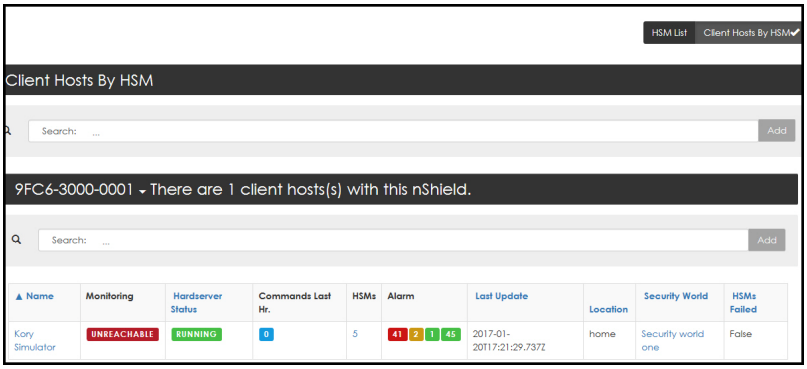
1. Navigate to **Views > HSMs > Client Hosts by HSM**.

   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.

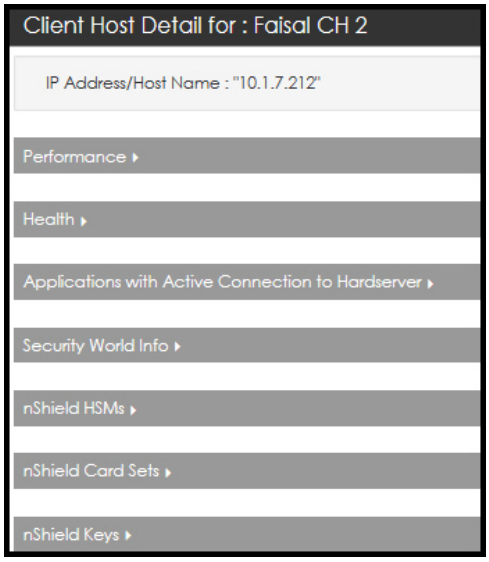
Links on the Details window

Clicking	Opens this page	Notes
Name	See Client Host Detail page	

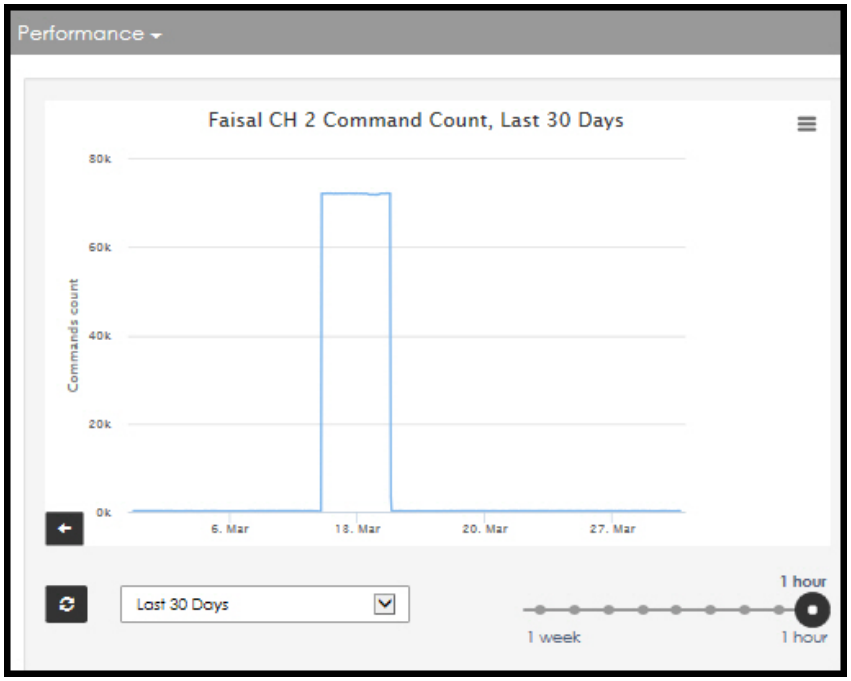
HSMs count	nShield HSMs page. This page lists all the **HSMs by Serial Number**	The nShield HSMs page also contains a link under the Security World column. Clicking on the Security World identifier opens the **Security World Detail** page.
Alarm (hover over the colored alarm total box in the Alarm column, then click.)	Current Unacknowledged Alarm	Select the box associated with the alarm to open the **Acknowledge Alarm** window.
Security World (name or Hash of the K_{NSO})	Security World Detail page.	

9.4.3.1. Client Host Detail page

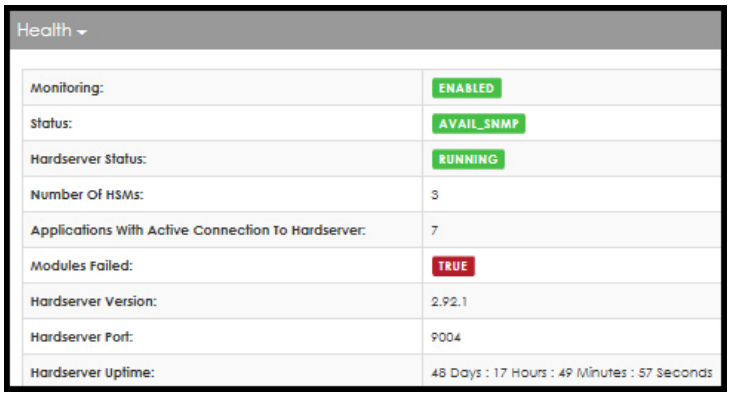
Select the expansion arrows to open additional windows.



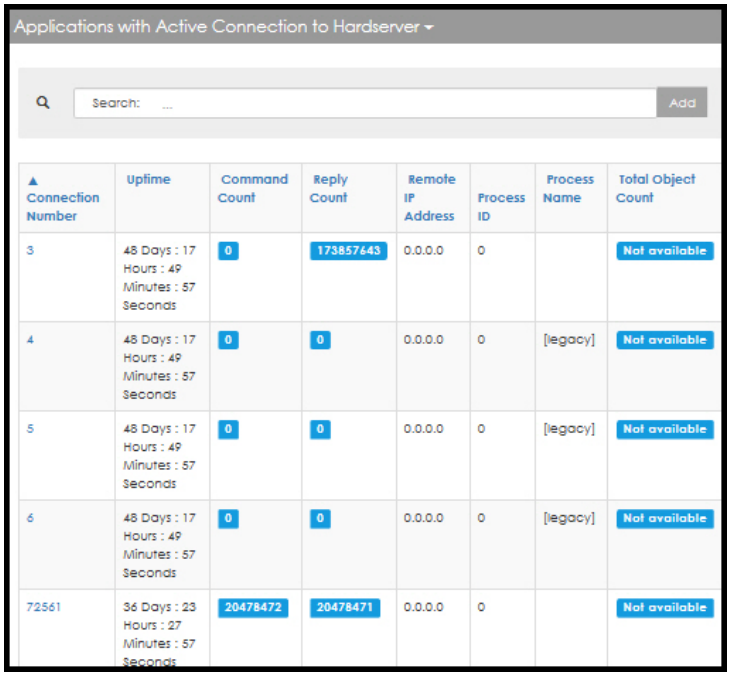
Performance window:



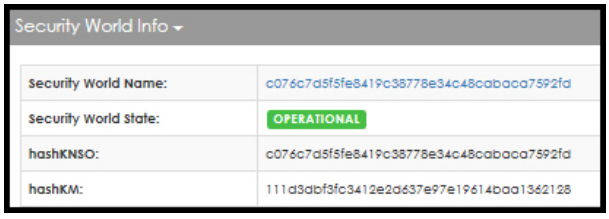
Health window:



Applications with Active Connection to Hardserver window:

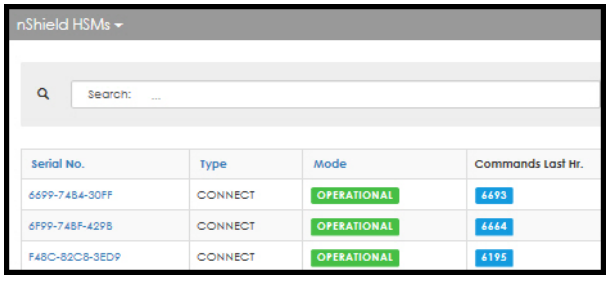


Security World Info window:

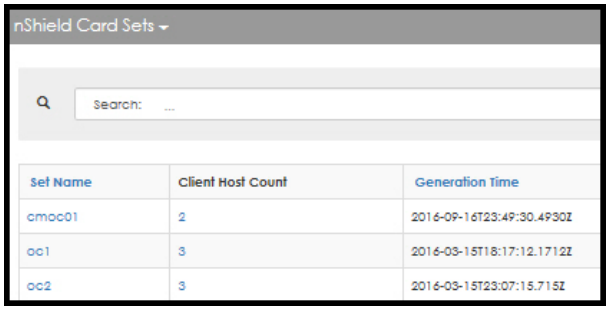


Clicking on the Security World identifier (for example, c076cd... .), opens the **Security World Detail** page.

nShield HSMs window:

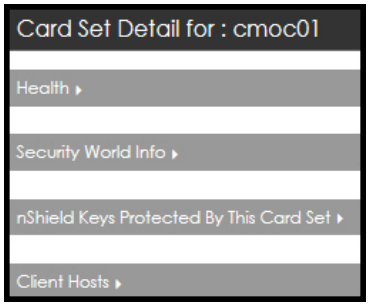


nShield Card Sets window:



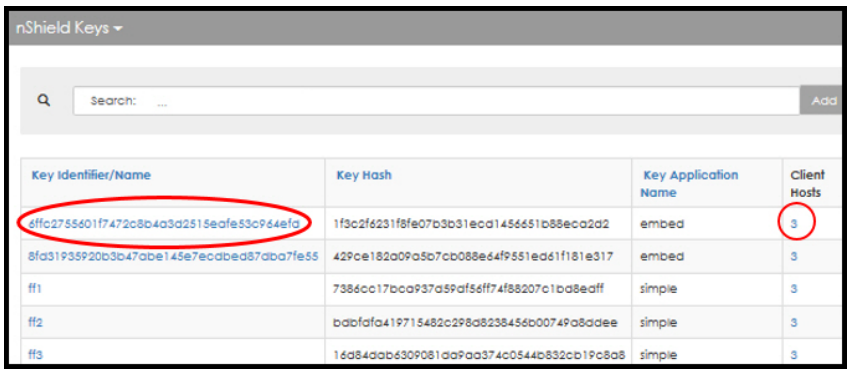
Selecting a set name, opens the **Card Set Detail** page.

Card Set Detail page:



Select the expansion arrows to open additional windows.

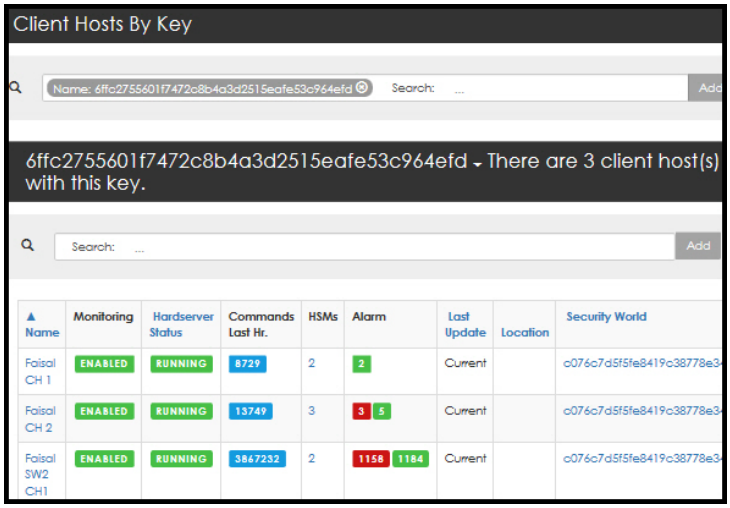
nShield Keys window:



This window has two navigational links.

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

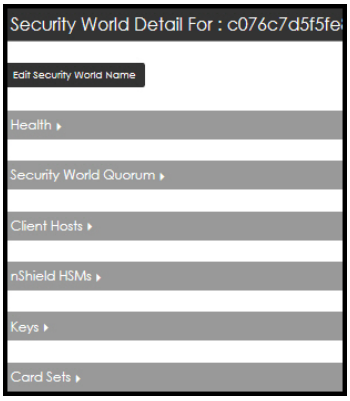
Selecting the Client Hosts number opens the **Client Hosts By Key** page.



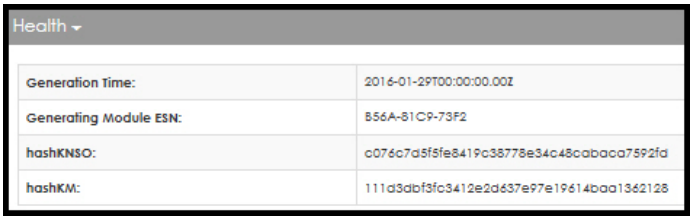
9.4.3.2. Navigating to the Security World Detail page

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

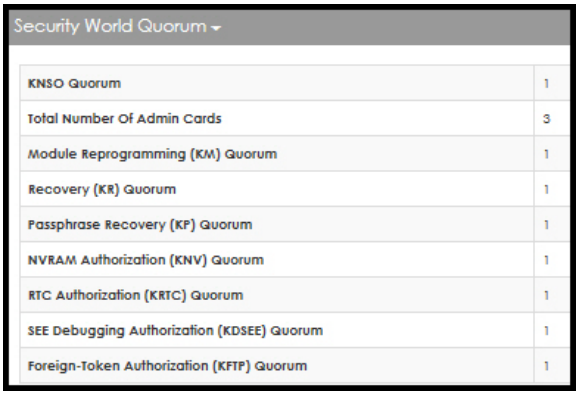
   Security World Detail page opens.



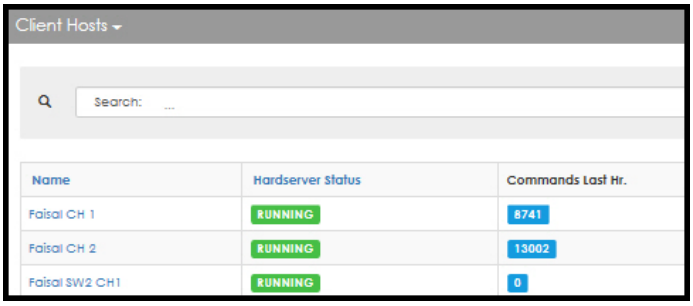
2. Select the **Health** expansion arrow.



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



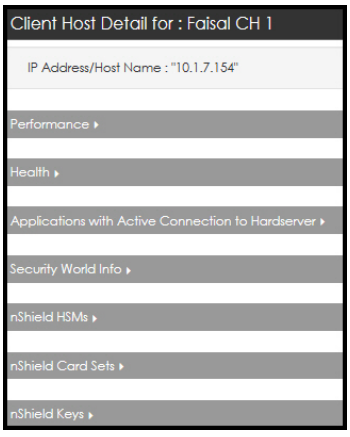
4. Select **Client Hosts**.



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

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

The **Client Host Detail** page opens:

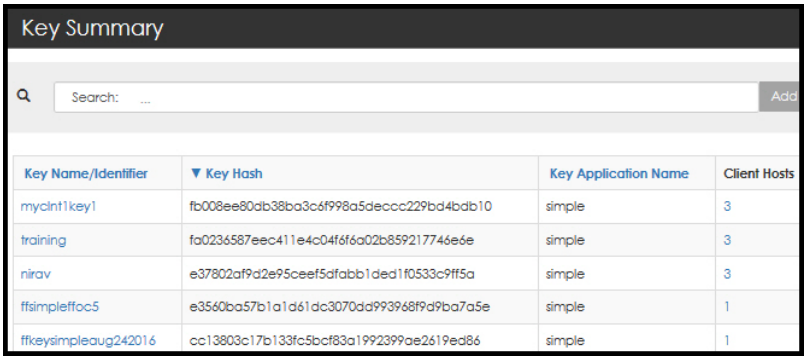


9.4.4. View > Keys

9.4.4.1. Key > Key List

1. Navigate to **Views > Keys**.
2. Select **Key List**.

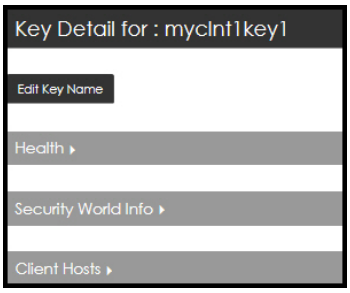
The **Key Summary** page opens.



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.

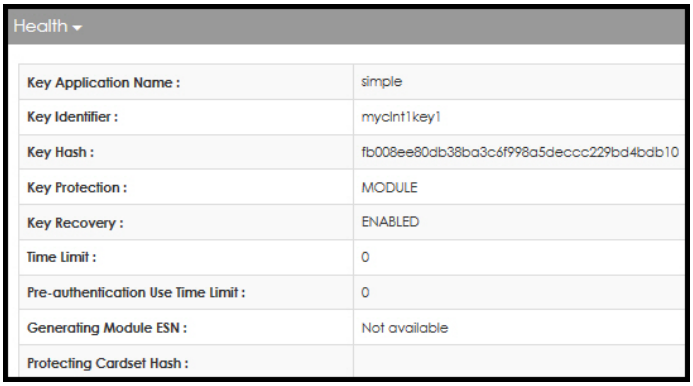


Should you need to Edit the Key Name, Select **Edit Key Name**, rename the key and then select **Save**.

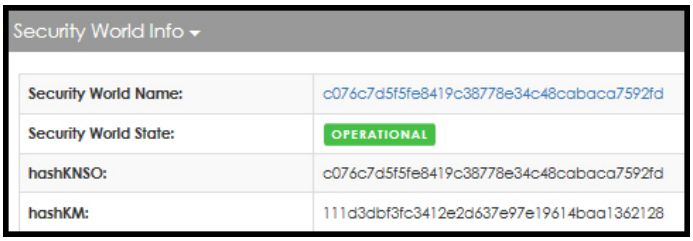
4. Select the expansion arrows to open the windows.

Blue font indicates that the text is a link. Click on the blue text to drill deeper. For example, click on Faisal CH 1 to open the **Client Host Detail** page.

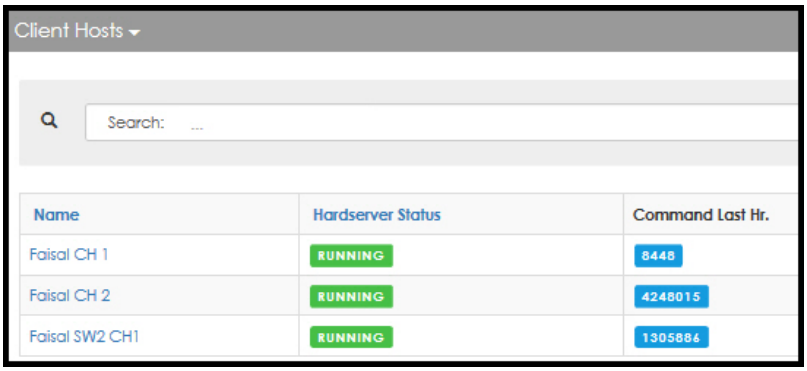
Health:



Security World Info:



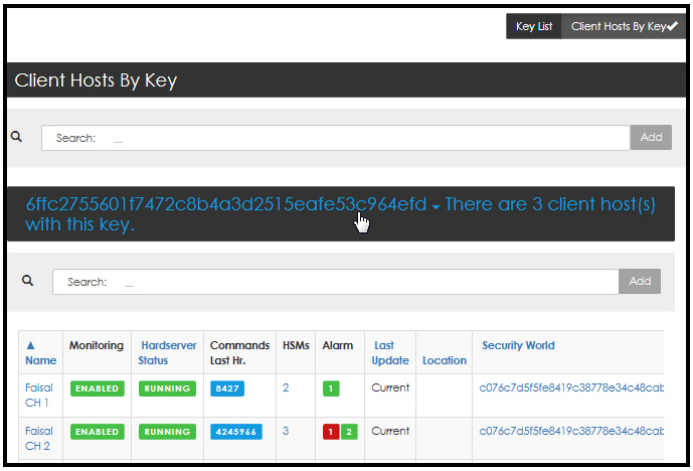
Client Hosts:



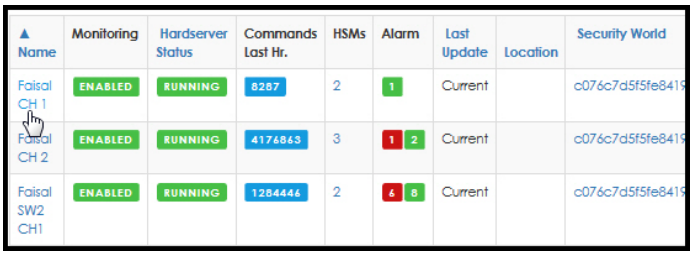
9.4.4.2. Keys > Client Hosts By Key

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

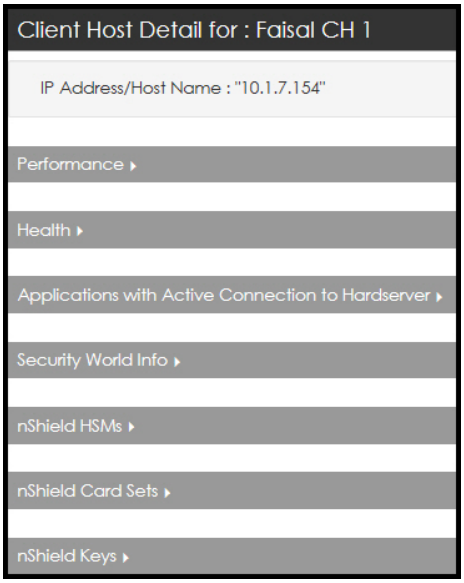
   The **Client Hosts By Key** page opens.



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

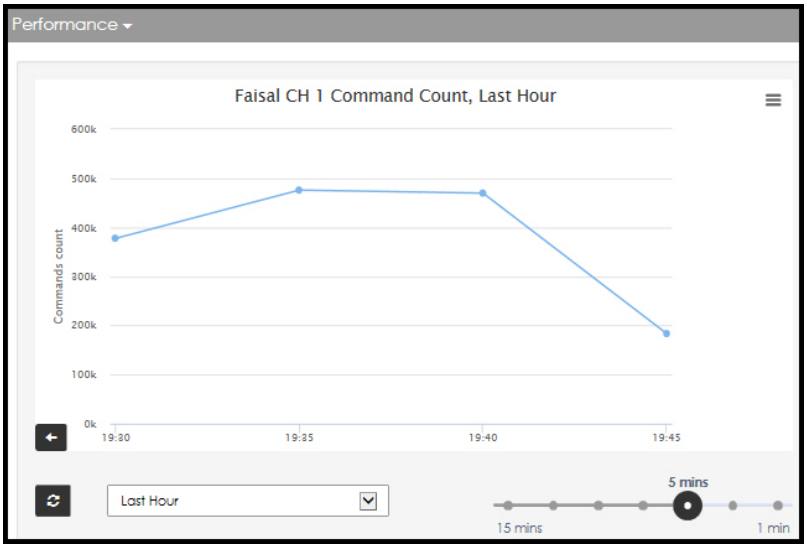


The **Client Host Detail** page opens.

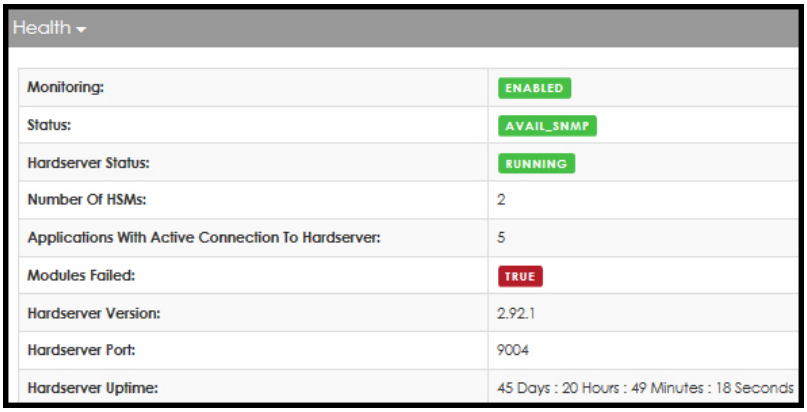


4. Select the expansion arrows to open the windows.

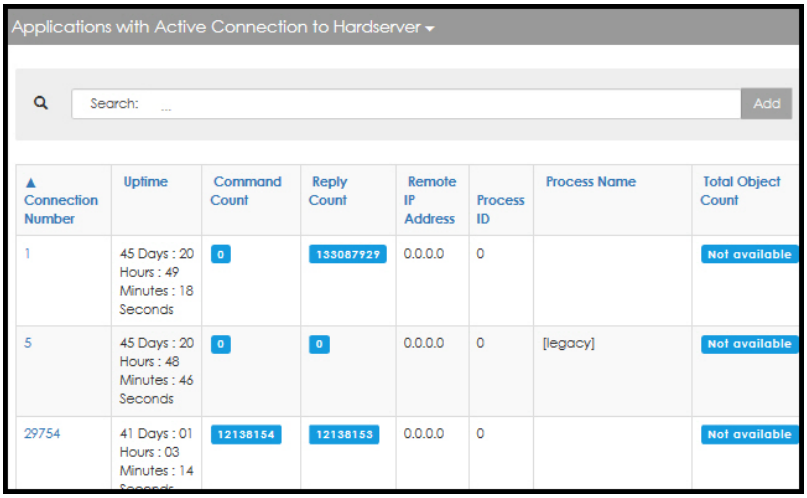
   Performance:



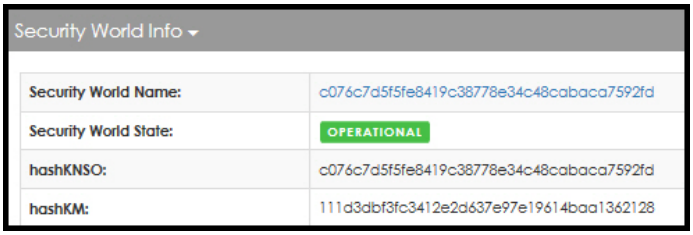
Health:



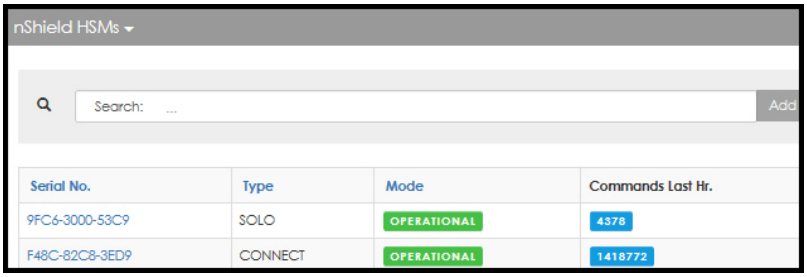
Applications with Active Connection to Hardserver:



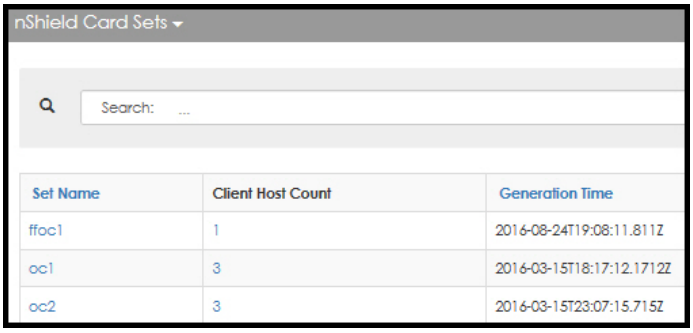
Security World Info:



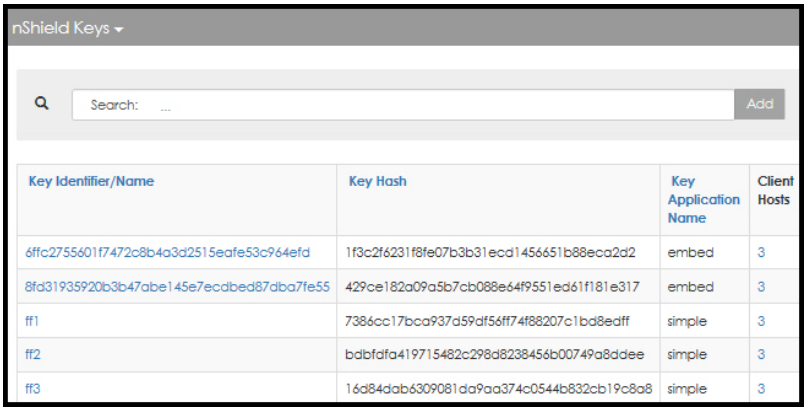
nShield HSMs



nShield Card Sets:



nShield Keys:



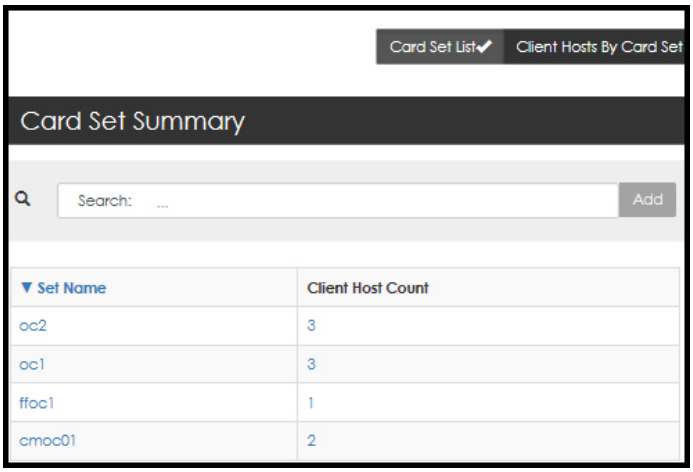
9.4.5. Card Sets

1. Navigate to **Views > Card Sets**.

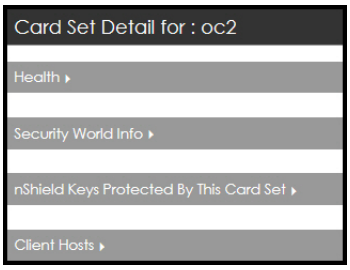
9.4.5.1. View > Card Set > List

1. Navigate to **Views > Card Sets > Card Set List**.

   The **Card Set Summary** page opens.

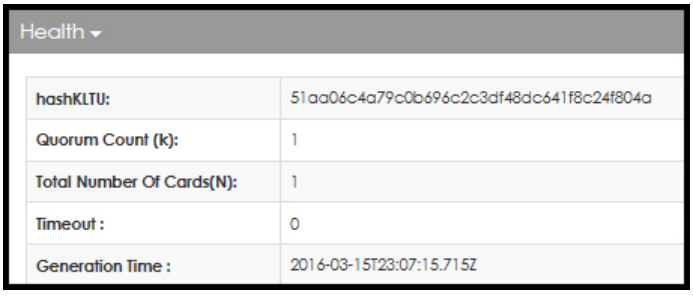


2. Select a **Set Name** to open a specific **Card Set Detail** page.

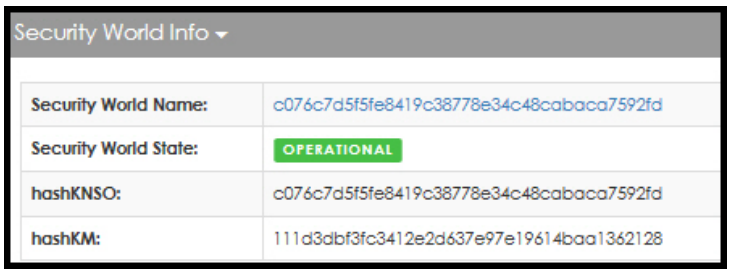


3. Select the expansion arrow to open the windows.

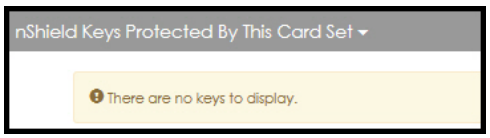
   Health:



Security World Info:

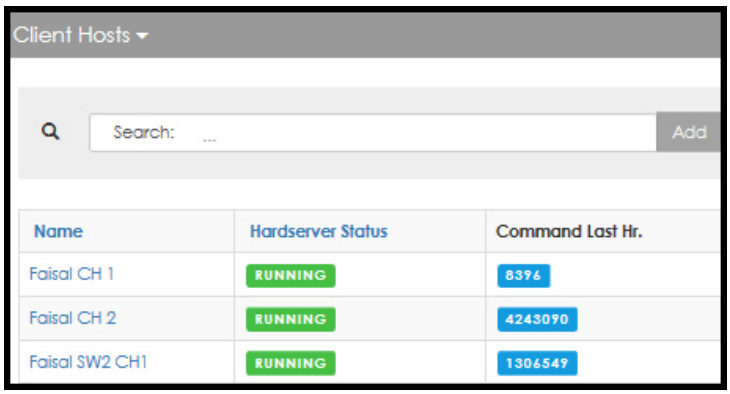


nShield Keys Protected By This Card Set:



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

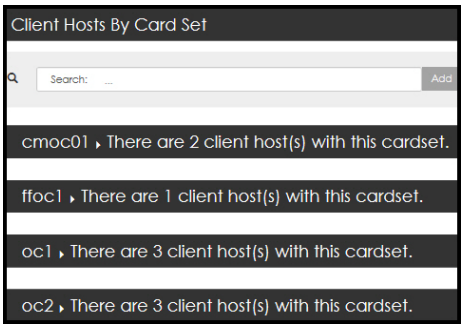
Client Hosts:



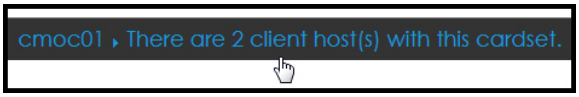
9.4.5.2. View > Card Sets > Client Hosts By Card Set

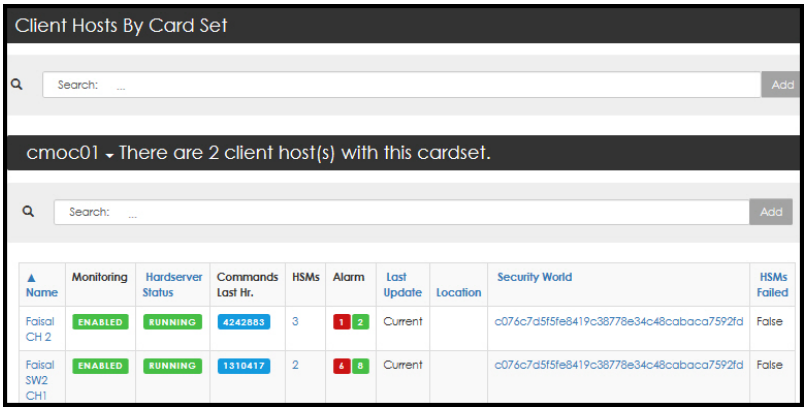
1. Navigate to **Views > Card Sets > Client Hosts By Card Set**.

   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.

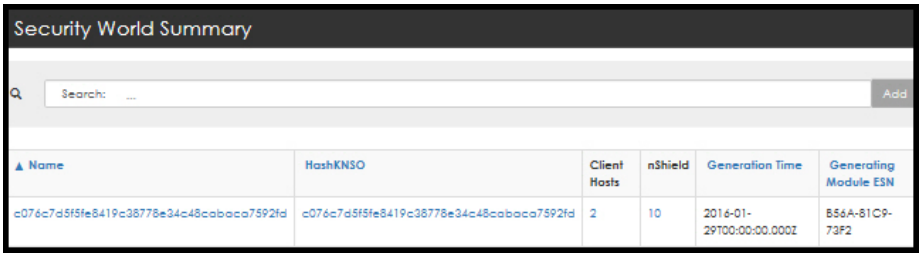
For example, clicking on the Security World identifier opens the **Security World Detail** page:

9.4.6. Security Worlds

9.4.6.1. Views > Security Worlds > Security World List

1. Navigate to **Views > Security Worlds > Security World List**.

   The **Security World Summary** page opens.



2. Click on the blue text to drill deeper.

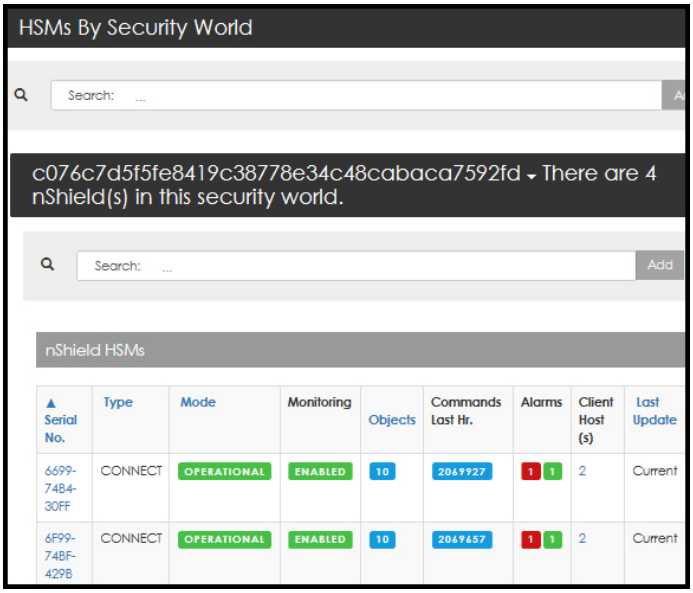
For example, clicking on the Security World HashKNSO opens the **Security World Detail** page.

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

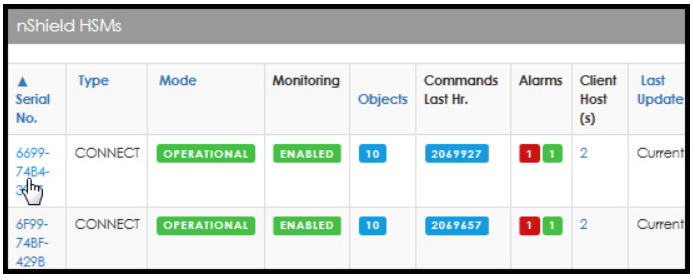
9.4.6.2. Security Worlds > HSMs By Security World

1. Navigate to **Security Worlds > HSMs By Security World**.

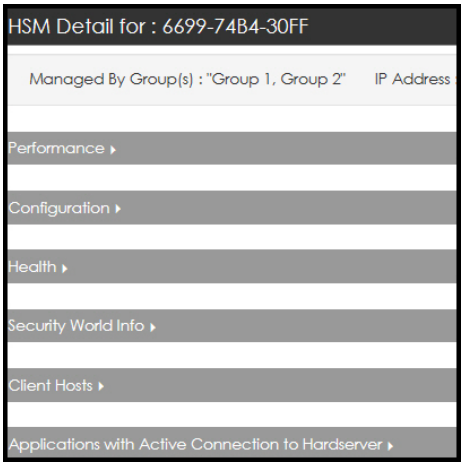
   The **HSMs By Security World** page opens.



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



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



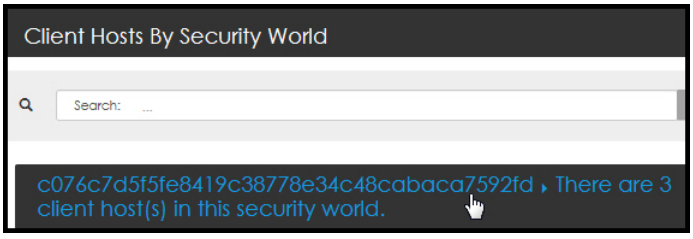
4. Select the expansion arrows to open additional windows.

9.4.6.3. Security Worlds > Client Hosts By Security World

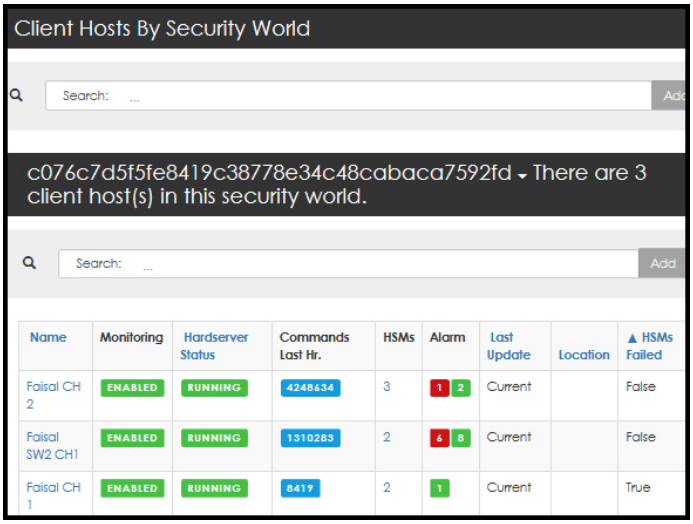
1. Navigate to **Security Worlds > Client Hosts By Security World**.

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

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



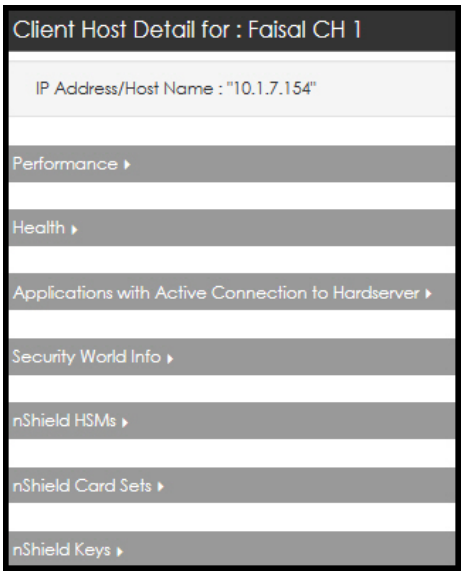
   The page expands:



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

3. Select a specific **Name**. For example, click on **Faisal CH 2**.

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

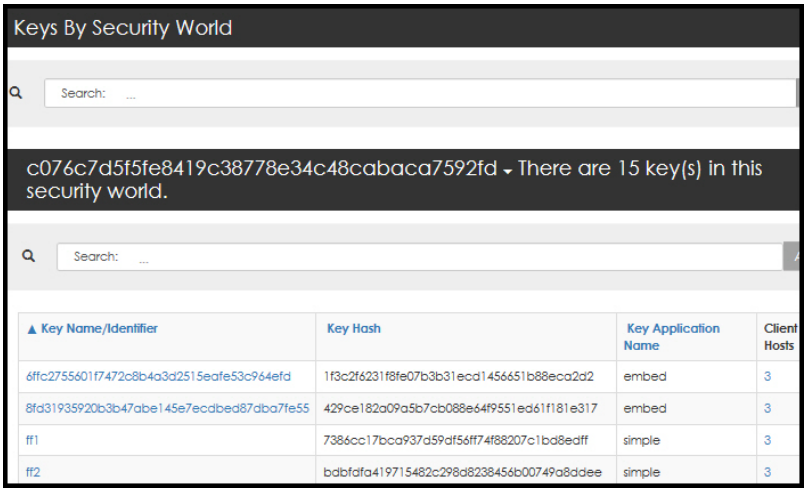


4. Select the expansion arrows to open additional windows.
5. Continue to click on the blue text to drill deeper.

9.4.6.4. Security Worlds > Keys By Security World

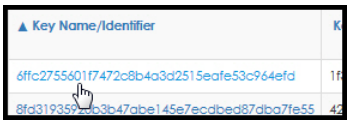
1. Navigate to **Security Worlds > Keys By Security World**.

   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**.



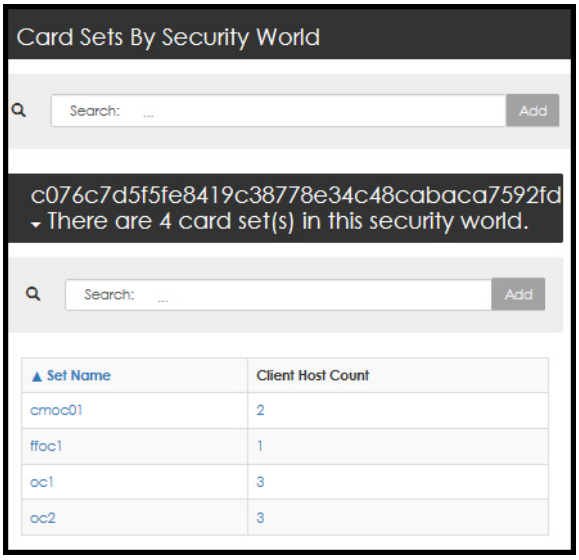
The **Key Detail** page opens.

3. Select the expansion arrows to open additional windows.
4. Continue to click on the blue text to drill deeper.

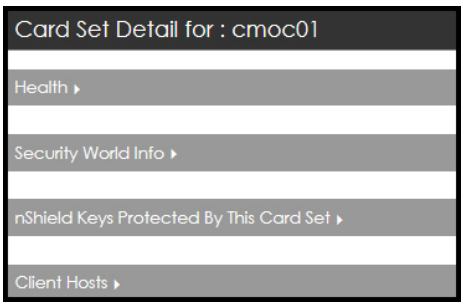
9.4.6.5. Security Worlds > Card Sets By Security World

1. Navigate to **View > Security Worlds > Card Sets By Security World**.

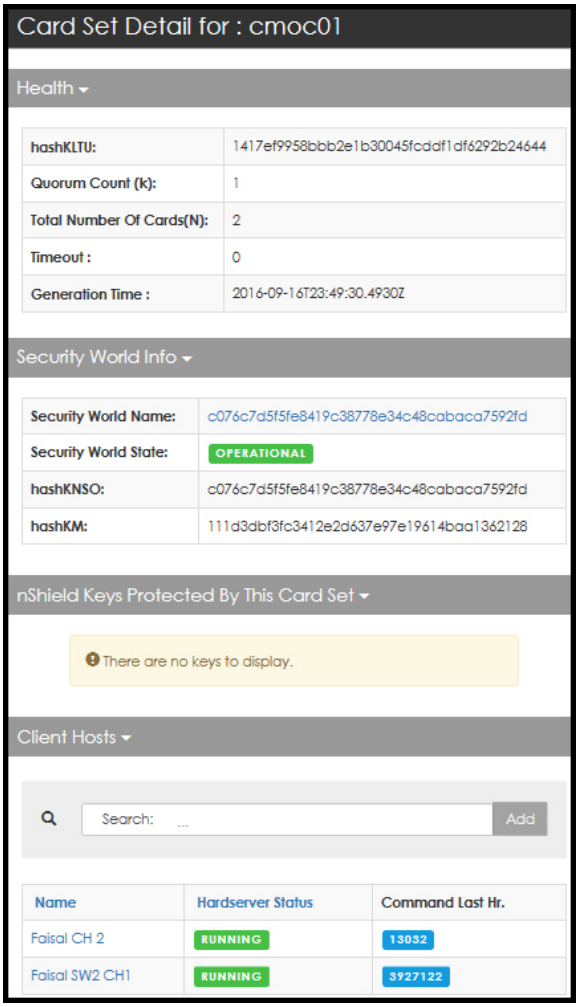
   The **Card Sets By Security World** page opens.



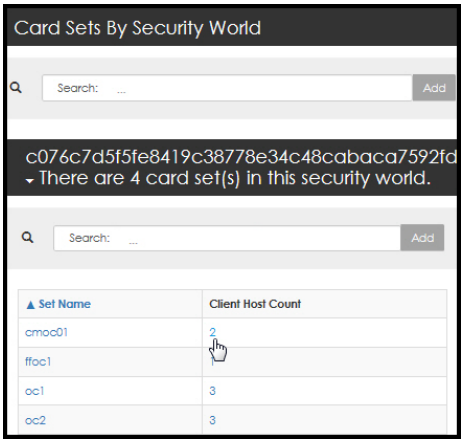
2. Select a **Set Name** to open the **Card Set Detail** page.



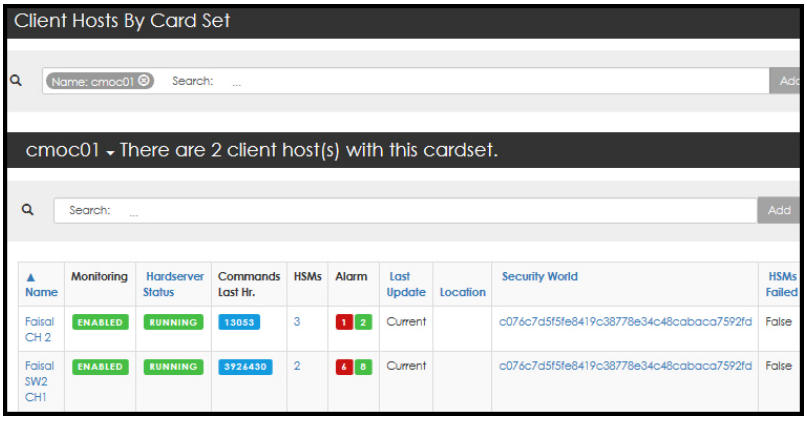
3. Select the expansion arrows to open the windows.



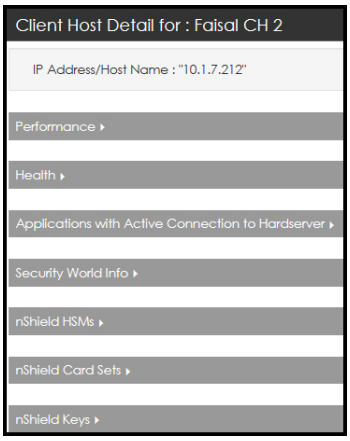
4. Select the **Client Host Count** (from the **Card Sets By Security World** page).



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. Generate 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**

   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.

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

10.1.2. Device Report

1. Select **Device Report**.
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.

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.
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.
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**

The Client Host Cross-HSM device report supports 2,500 nShield keys. That is, 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.

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.

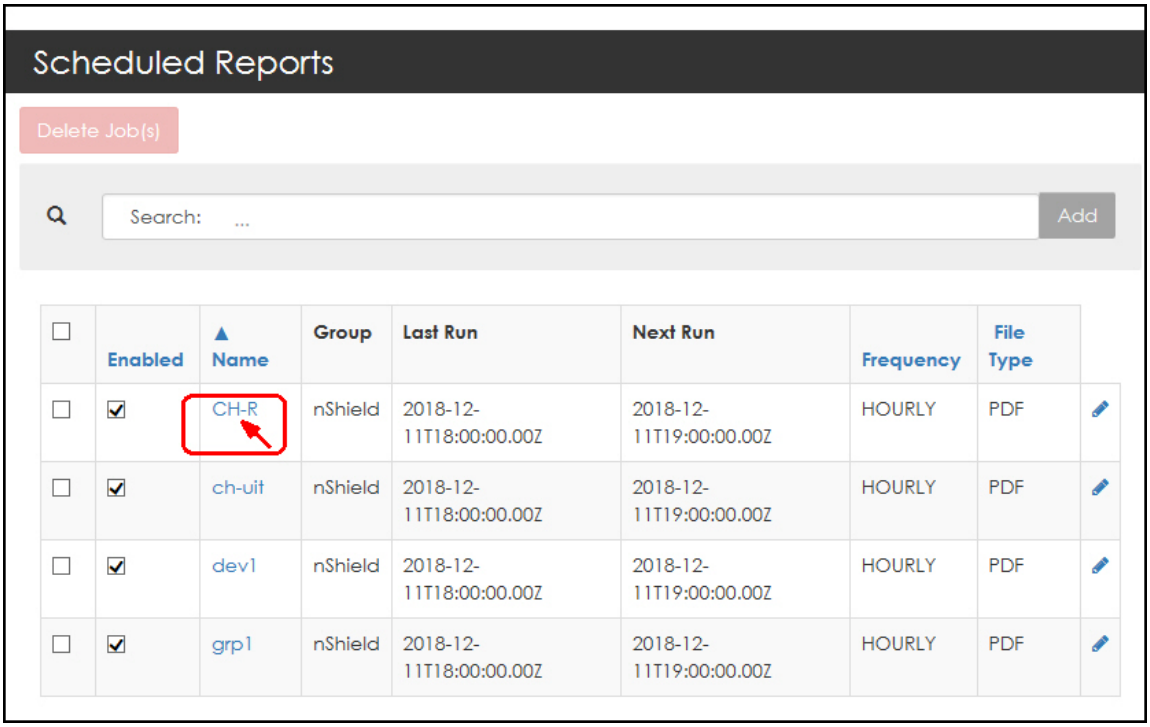
3. Select the expansion arrows to open the **Report Configuration** window.
4. Enter a report name and select the drop-down arrows to display additional selections.
5. Select your preferences.
6. Select the expansion arrow to open the **Loading Trends Options** window.
7. Set your thresholds.
8. Select **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**.

   You can open the downloaded report or save the report in a specific folder.

10.2.2. Downloading reports in bulk

Selecting **Bulk Download** uses a toggle:

1. Select the checkbox 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 checkbox can also be used to clear your selections.

   Conversely, you can click specific checkboxes to customize the download. The checkbox selection can be toggled.

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

   You can open the zip file containing the selected reports or save the zip file in a specific folder.

10.2.3. Delete Reports

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

   Once the checkbox 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:

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**.

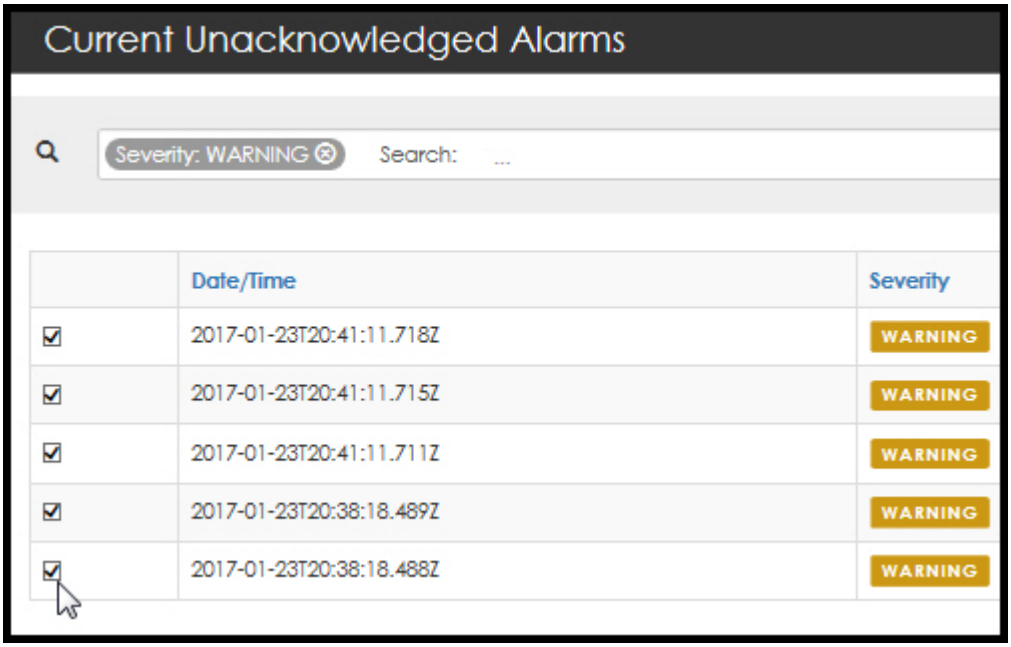
Alarms can always be exported, by selecting Export Alarm History (CSV) from the **Alarm History** page.

11.2. Acknowledging alarms in bulk

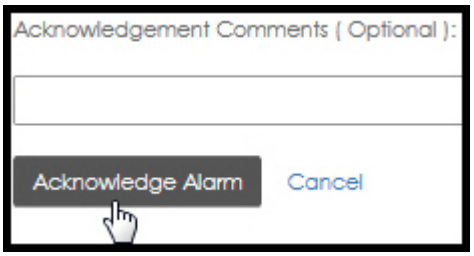
1. From any Alarm count column, select the alarm total.

The **Current Unacknowledged Alarms** page opens.

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



3. Select **Acknowledge Alarm**.



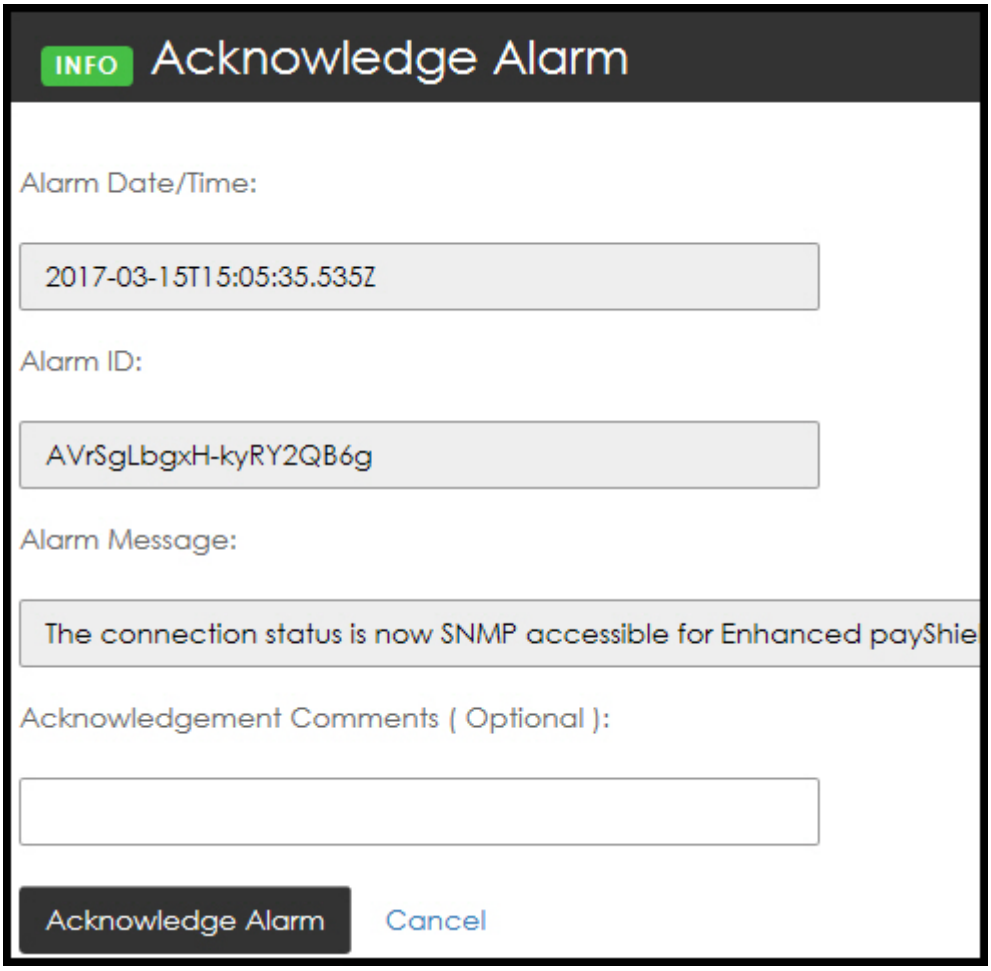
11.3. Acknowledging an individual alarm

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

   The **Alarm History** page opens.

2. Select (that is, single click) on the alarms severity level.

The **Acknowledgment Alarm** page opens.



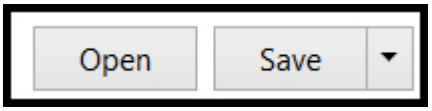
3. Enter any Acknowledgment Comments in, if needed.
4. Select **Acknowledge Alarm**.

   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.



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 a 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 letters
- 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 may be prompted. This occurs 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. Log in 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.

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 to the bottom of the page, which will automatically close the EULA
6. Select **y** to agree to the terms of the EULA.

   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

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

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

The wizard will show the current network configuration.

1. Select the network configuration.
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.

    The system prompts to configure date and time.

12.11. Configure date and time

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).
   - 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)
2. Follow the prompts to complete the configuration:
   - 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

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.

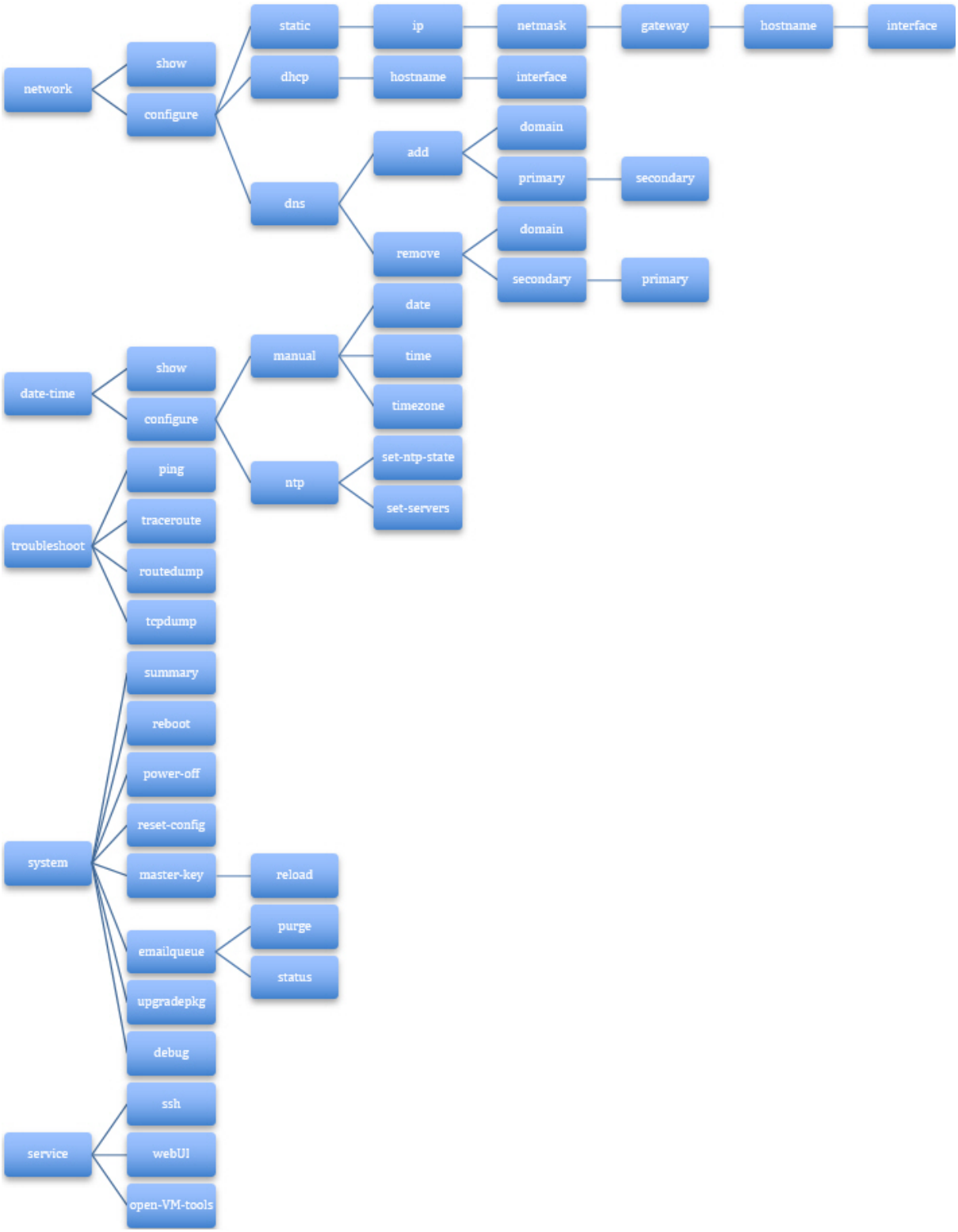
- Set NTP (on/off). Configure date, time and timezone and/or NTP servers.

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	`> network show`
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	`> network configure dhcp hostname <hostname> interfacename <interface>`
Output	Hostname is optional. Interface is optional

Action	Configure static network
Input	`> network configure static hostname <hostname> ip <ip> netmask <netmask> gateway <gateway> interfacename <interface>`
Details	All parameters are mandatory. Interface is optional

Action	Add/overwrite DNS parameters
Input	`> network configure dns add domain <domain name> primary <primary dns> secondary <secondary dns> interfacename <interface>`
Details	Commands to set domain name and primary DNS/secondary DNS can be performed separately or together in one command. Only prompt for secondary if primary is entered to ensure that primary DNS is not left blank. Interfacename is optional

Action	Remove DNS parameters
Input	`> network configure dns remove domain <domain name> primary <primary dns> secondary <secondary dns> interfacename <interface>`

Details	Commands to remove domain name and primary DNS/secondary DNS can be performed separately or together in one command. Only prompt for primary if secondary is entered, to ensure that primary DNS is not left blank. If the domain name is removed, it will be replaced by « localdomain ». Interface name is optional.

12.15. Date-time commands

Date-time configuration triggers system reboot if configuration has succeeded.

Action	Show date and time configuration
Input	`> date-time show`
Output	NTP enabled : <yes/no> Date/time Timezone Day light saving status : <yes/no> NTP server list (if any)

Action	Switch NTP on or off
Input	`> date-time configure ntp set-ntp-state <on/off>`
Details	set-ntp-state is mandatory. Set it to « on » to enable NTP and set it to « off » to disable NTP. If enabled, NTP will try synchronizing with NTP servers. If it fails, it will remain disabled. Note: check with « date-time show » command if any servers were configured.

Action	Set NTP servers
Input	`> date-time configure ntp set-servers <"list of servers">`
Details	This command removes all previous servers (if any) sets the new list of servers. In CLI, provide the list of servers between double quotes. If there is only one server then there is no need for quotes. Examples : date-time configure ntp set-servers us.pool.ntp.org date-time configure ntp set-servers "us.pool.ntp.org time.nist.gov"

Action	Configure date and time manually

Input	`> date-time configure manual date <date> time <time> timezone <select from list>`
Details	NTP has to be disabled to perform this operation. Commands to set date, time and timezone can be performed separately or together in one command.

12.16. System commands

Action	Power off the system
Input	`> system power-off`
Details	This operation can take up to 60 seconds

Action	Reboot the system
Input	`> system reboot`
Details	This operation can take up to 60 seconds

Action	Reset the system to factory settings
Input	`> system reset-config`
Details	This operation can take up to 60 seconds

Action	Show the summary of system information
Input	`> system summary`
Details	SSH state indicates only the user's configuration for SSH through the CLI (« service ssh enable/disable » command.) * `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	`> system master-key reload`
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	`> system debug show`
Details	Show current state of debug

Action	Enable logging of debug message
Input	`> system debug configure set-debug-state on`
Details	Enable debug logging

Action	Disable logging of debug message
Input	`> system debug configure set-debug-state off`
Details	Disable debug logging

12.17. Email queue commands

Action	Disable logging of debug message
Input	`> system debug configure set-debug-state off`
Details	Disable debug logging

Action	Show the outstanding emails queued up in the system
Input	`> system emailqueue status`
Output	EMAIL QUEUE SUMMARY Pending mail requests.....: nn

Action	Purge system email queue
Input	`> system emailqueue purge`
Output	EMAIL QUEUE PURGE STATUS Mail purge status .....: success

12.18. Troubleshooting commands

Action	Ping host name or IP address
Input	`> troubleshoot ping <ip address/hostname>`

Action	Traceroute host name or IP address
Input	`> troubleshoot traceroute <ip address/hostname>`
Details	This operation may take up to 450 seconds (7.5 min)

Action	Show routing tables
Input	`> troubleshoot routedump`

Action	Dump traffic on the network to a file
Input	`> troubleshoot tcpdump <on/off>`
Details	The file is overwritten every time tcpdump is turned on

Action	Export debug logs through SCP
Input	`> troubleshoot export_logs server <IP> username <name> dest_dir <destination path> port <optional_port_number>`
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	`> service ssh <enable/disable>`
Details	By default, it is disabled as well as after each reboot

Action	Enable/Disable webUI
Input	`> service webUI <enable/disable>`

Action	Enable/Disable OVT
Input	`> service open-vm-tools enable` `This will enable Open VMware Tools. Proceed? [y/n]`

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 or endpoints by a firewall, you must configure the firewall to allow passage of the appropriate IP protocols. For example:

- Services, such as NTP, DNS, or SMTP server.
- Endpoints, such as user devices.

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
SMTP	TCP	465	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)

Protocol	Transport	Port	Direction	Description
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. This is 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 nShield Monitor users in various time zones, to select and view nShield Monitor Log and Alarms in a common 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. That is, 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 sign in, the time zone is reset to '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, and so on. 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 Montor > 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 result:
 PING 10.1.1.14 (10.1.1.14) from 10.1.2.22 eth0: 56(84) bytes of data.
64 bytes from 10.1.1.14: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 10.1.1.14: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 10.1.1.14: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 10.1.1.14: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 10.1.1.14: icmp_seq=5 ttl=64 time=0.054 ms
64 bytes from 10.1.1.14: icmp_seq=6 ttl=64 time=0.055 ms
64 bytes from 10.1.1.14: icmp_seq=7 ttl=64 time=0.057 ms
64 bytes from 10.1.1.14: icmp_seq=8 ttl=64 time=0.054 ms
64 bytes from 10.1.1.14: icmp_seq=9 ttl=64 time=0.057 ms
64 bytes from 10.1.1.14: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.1.1.14: icmp_seq=11 ttl=64 time=0.058 ms

--- 10.1.1.14 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 9999ms
rtt min/avg/max/mdev = 0.029/0.051/0.058/0.011 ms

************************************************************
```

   Example: Not Successful

```
************************************************************
    PING result:
 PING 10.1.1.131 (10.1.1.131) from 10.1.2.22 eth0: 56(84) bytes of data.
64 bytes from 10.1.2.22: icmp_seq=1 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=2 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=3 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=4 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=5 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=6 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=7 Destination Host Unreachable
64 bytes from 10.1.2.22: icmp_seq=8 Destination Host Unreachable
```

```
--- 10.1.1.131 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 7000ms
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. It enables users 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 scop 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. A CRITICAL alert will be sent out on 29th day and an EMERGENCY alert will be sent out on 30th day. An 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	System Alarm - nShield Monitor 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. Add storage space by expanding the virtual hard disk.
nShield Monitor Security Related Alarm Warning when Master key has not been generated and Critical when Master key is not loaded	WARNING CRITICAL	Security Alarm - nShield Monitor 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.
nShield Monitor Security Related Alarm User: has enabled/disabled Service	INFO	Security Alarm - nShield Monitor If SSH, WebUI or Open VMTool services are enabled or disabled.
nShield Monitor Security Related Alarm	WARNING CRITICAL	Security Alarm - nShield Monitor It is a security alarm regarding master key not being generated or not being loaded. If the key is not generated a WARNING message is generated and a CRITICAL message is generated when a master key is not loaded. The Administrator needs to take appropriate action by configuring the same on the Security page.
The license features have been changed for Device	INFO	Device Alarm - nShield 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.

Alarm Condition	Alarm Severity	Notes
The nShield device temperature change alerts	WARNING / CRITICAL	Device Alarm - nShield System reports device temperature change WARNING message when exceeds lower configured threshold value and CRITICAL above upper threshold value.
Hard Server failure in Client Host	WARNING	Device Alarm - nShield A WARNING message would be generated when hard server program fails. Follow Remote Administrator Client User Guide for further investigation.
Module count is Zero for Client Host	WARNING	Device Alarm - nShield When Client host discovers no nShield HSMs attached to enrolled Client Host. Follow up with nShield User Guide.
The software base release updated, revision, build number, core API version, performance model update, crypto algorithm host command update and optional license update	INFO	Device Alarm - nShield 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, and so on. No action needed.

Alarm Condition	Alarm Severity	Notes

License count exceeded
 	
`Device count license Exceed - NOTIFICATION`
 	
`Install new License - NOTIFICATION`
 	
`Device count license exceeds for <N> days - WARNING`
 	
`Device count license exceeds for <0> days - ALERT`
	NOTIFICATION / WARNIING / ALERT / CRITICAL	System Alarm - nShield Monitor
		
		When nShield Monitor detects more nShield HSMs connected to ClientHost than the permitted “nShield Monitor” License count, nShield Monitor generates this event.
		
		When the License count is exceeded, a new license (with more HSM count) should be installed within 30 days. If this does not occur, ONLY Administrator privilege users of nShield Monitor will be allowed to login.
		
		Group Manager Privileged Users won’t be allowed to login to nShield Monitor.
		
		After 30 days, nShield Monitor will still continue to monitor the detected nShield HSMs in the background. Once the new “nShield Monitor” license with a sufficient HSM count is installed, Group Manager Privileged Users are allowed to login.

Client Host does not belong to a security world	WARNING	Device Alarm – nShield When the Client host is not configured with correct Security World information but is enrolled for monitoring. WARNING message gets generated. Refer to Remote Administrator Client User Guide.
Solo XC fan speed down to zero	CRITICAL	Device Alarm - nShield This CRITICAL alarm generates when the fan speed for Solo goes down to zero or is not functioning. Refer to nToken Installation Guide if needed.
Power Supply failed for nShield module	WARNING	Device Alarm - nShield This WARNING alarm generates when power supply to nShield module fails. Refer to nToken Installation and Solo installation guide if needed.
Number of nShield discovered by nShield Monitor	INFO	Device Alarm - nShield nShield Monitor generates alarms when client host start discovering nShield configured to it.

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	Device Alarm - nShield Monitor Enrolled device WARNING and/or CRITICAL notifications 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. The alert indicates: • The threshold value • The HSM hostname and IP address (or the HSM ESN if hostname and IP address are not present) • The group that the HSM belongs to.
SNMP Trap Notification	NOTIFICATION / ALERT / CRITICAL	Device Alarm - nShield Monitor Enrolled device nShield Monitor generates alerts and notifications when the SNMP TRAP state changes. ALERT when the state changes to offline or unavailable. NOTIFICATION when the state changes to secure or online. CRITICAL when the connection status is unreachable.

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 possible. This may be subject to external requirements such as network connectivity, regulatory control or other issues.

The best-case scenarios are a single nShield Monitor instance that poll all HSMs in an estate. This provides a complete set of statistics for all HSMs in the estate from a single login. This is based on access rights and role/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 for the user who is 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. For example, 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

A single nShield Monitor virtual appliance is all that is required to monitor an HSM estate. However, it is possible to utilize multiple nShield Monitor virtual appliances simultaneously as insurance in case of an outage. By distributing nShield Monitor virtual appliances across multiple locations, polling is maintained to all devices in the event of a network outage, other than to a single site. It is possible to ensure that, even during a single location network failure, only a minimal number of devices will be unmonitored until the issue is resolved.

18.3. Distributed monitoring

There are cases where multiple monitors are required due. For example:

- Network connectivity via firewalls
- Potential regulatory compliance requirements
- Scenarios 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, central distribution of alerts using SIEM or email services is recommended. This enables proactive notifications to be sent to the persons who are responsible for an nShield Monitor instance or for a 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. 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. These may 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. For example, 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.

A distributed model of nShield Monitor can still provide the ability to distribute proactive alerts and event information to centralized tools. This can be 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. This includes 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 because they are directly relevant to mitigating the outlined risks to nShield Monitor and they can be modified by the user who is operating the virtual machine.

- Secure virtual machines as you would secure physical servers. Antivirus, 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.
- 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 6.5
- vSphere ESXi 6.7
- vSphere ESXi 7.0

Access to a DVD or the nShield Monitor OVA file from the machine that has the vSphere software running is required for proper installation of the Virtual Appliance.

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 are required.

20.2. Install the nShield Monitor OVA

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:

   a. **Select template**.

      Enter the URL to the OVF template or **Browse** to a local OVF file, then select **Next**.

   b. **Select name and location**.

      Enter a name for the OVF and select the deployment location, then select

Next.

c. **Select a resource**.

Select the host on which to run the deployment template, then select **Next**.

d. **Review details**.

Verify the template details, then select **Next**.

e. **Accept license agreements**.

Review the agreement. You can scroll through it by selecting **Next**, then select **Accept**.

f. **Select storage**.

Select where the files for the deployed template will be stored, then select **Next**.

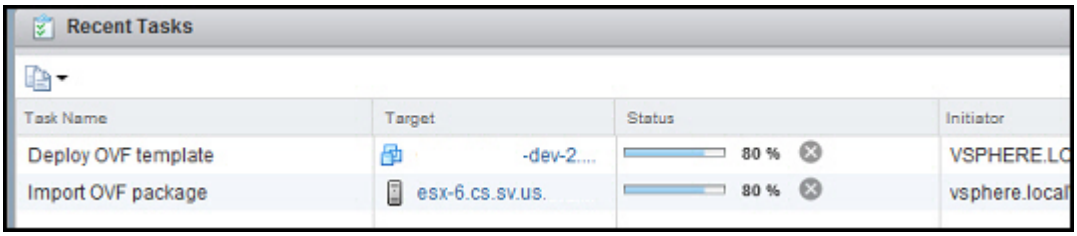
g. **Select networks**.

Select a destination network for each source network, then select **Next**.

h. **Ready to complete**.

Review the configuration data, then select **Finish**.

4. You can follow the deployment status:



5. 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.

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.

20.4.2. Familiar with VMware ESXI

If you can determine the IP address assigned to the new VM, record your new password and IP address. Then, provide this information to the appropriate personnel.

In most organizations the information technology or infrastructure group will accomplish the setup of the OVA. However, 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.

The nShield Monitor virtual appliance does not have VMware Tools installed. As a result, 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.

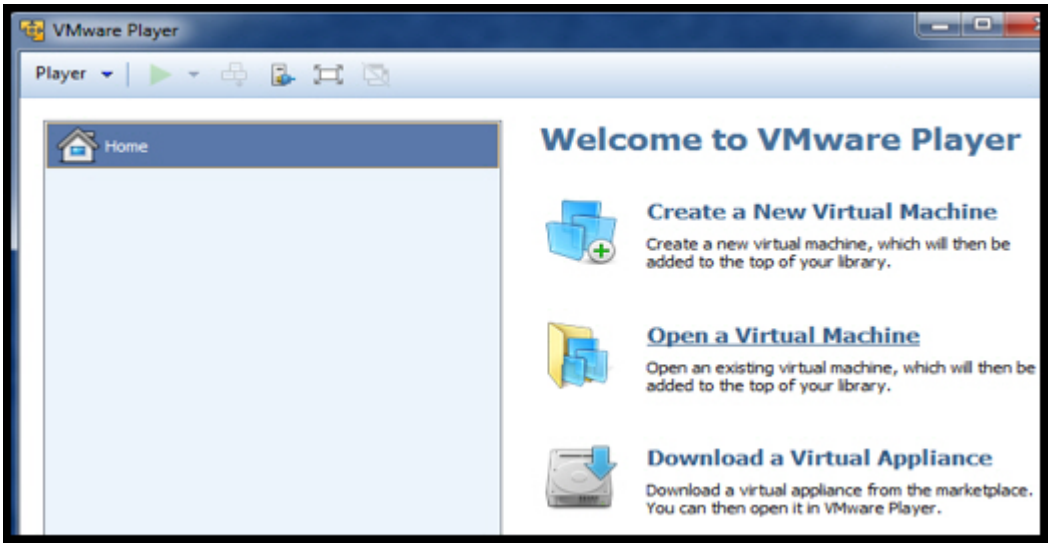
Note: If you are going to be running nShield at full capacity with 500 devices, a recommended precaution is to increase the 250GB disk in vCenter to 350GB after deploying the OVA but before powering it on. Once the OVA has been powered on the disk size cannot be changed.

21.2. Install the nShield Monitor OVA

Run the VMware Player or Workstation software.

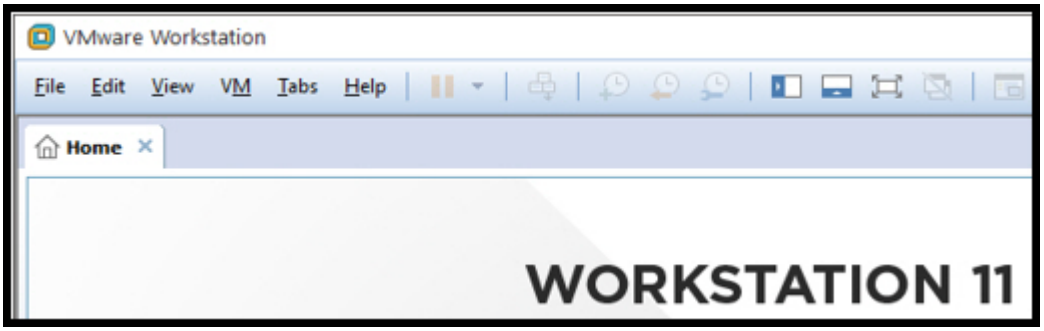
The steps that follow apply for both the VMware Player and the VMware Workstation.

1. Select Open a Virtual Machine from the Home tab.

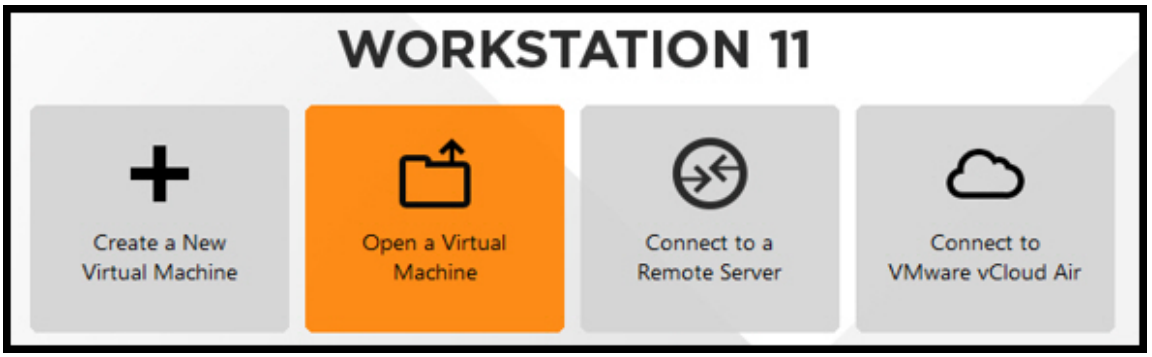


From the menu bar you can also select **File** (Alt + F) and **Open** (Ctrl + O). On VMware Workstation, this is the first option on the menu bar. For VMware Player, it is found under the **Player** drop-down menu.

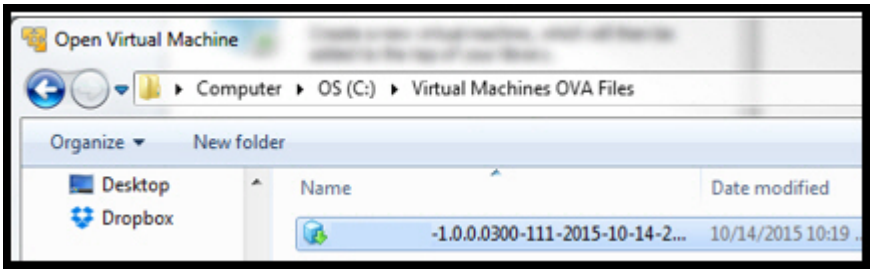
VMware Player and Workstation versions vary on the home screen, so please refer to the documentation for the version that you plan to use.



2. Select **Open a Virtual Machine**.

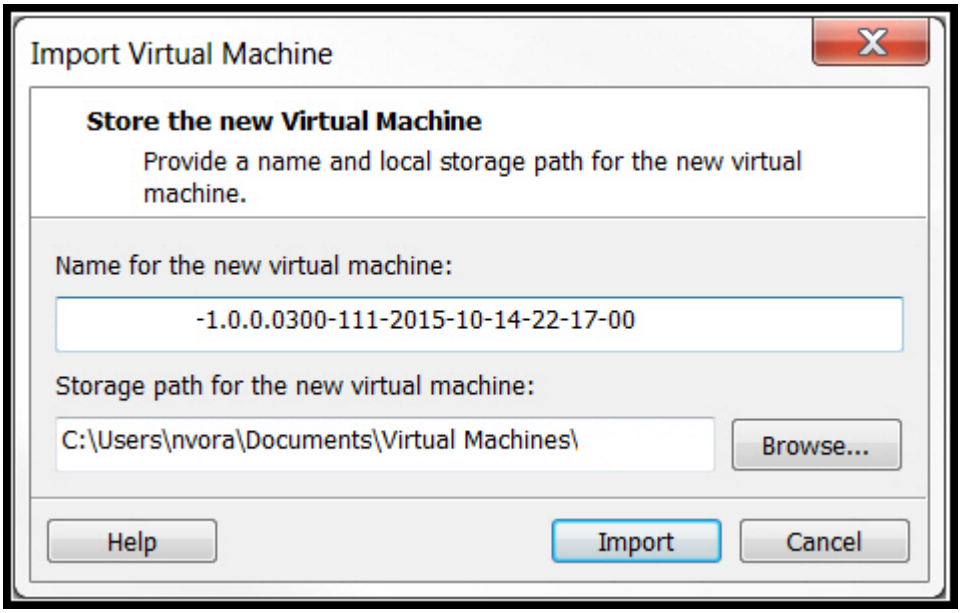


The **Open Virtual Machine** page opens.



3. Select the OVA file to be installed.
4. Select **Open**.

   The Import Virtual Machine dialog box opens.



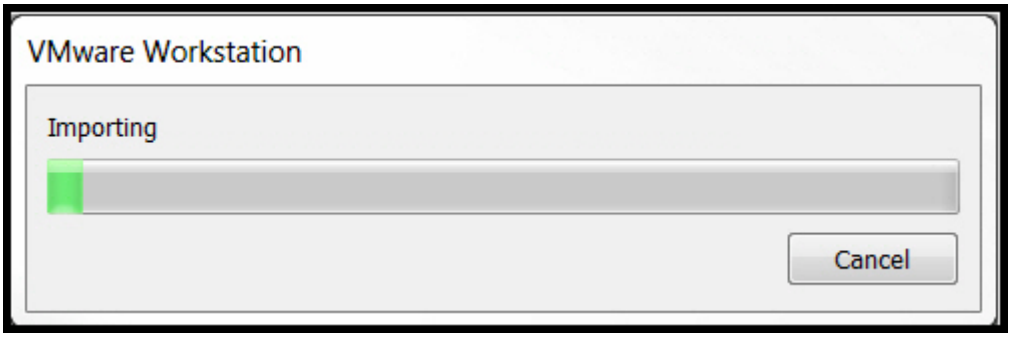
5. Enter a name and path for the VM to be stored.
6. Select **Import**.

   The **End User License Agreement (EULA)** page opens.

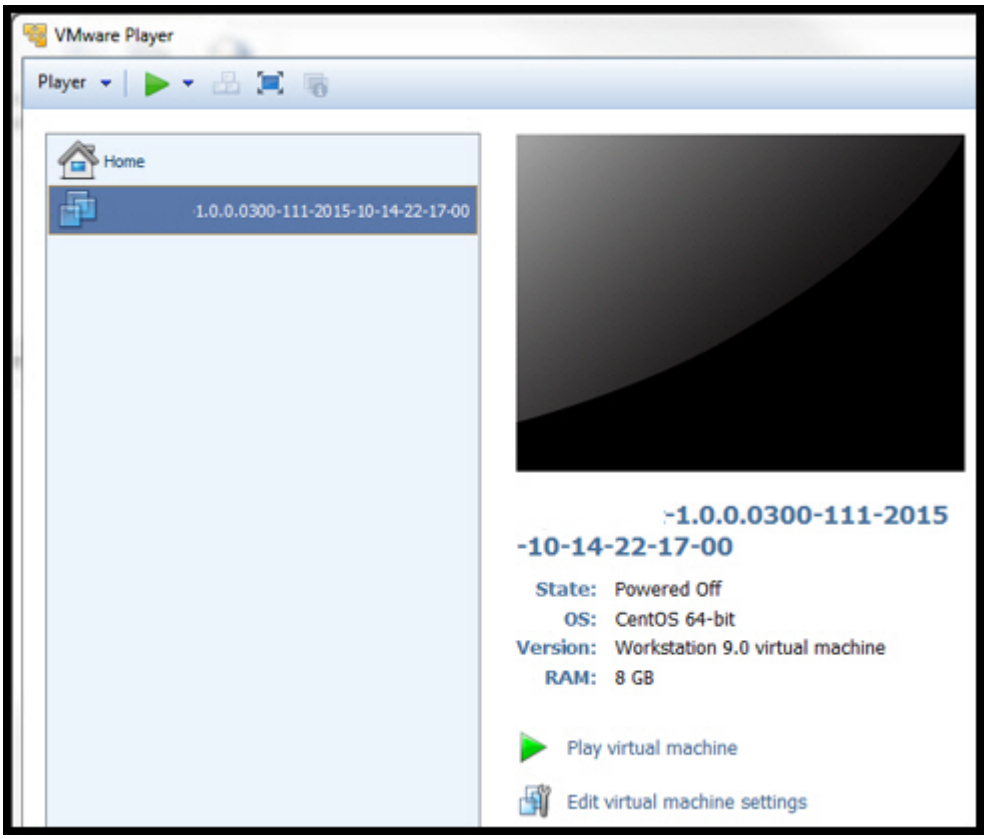
7. Read the EULA.
8. Select **Accept**.

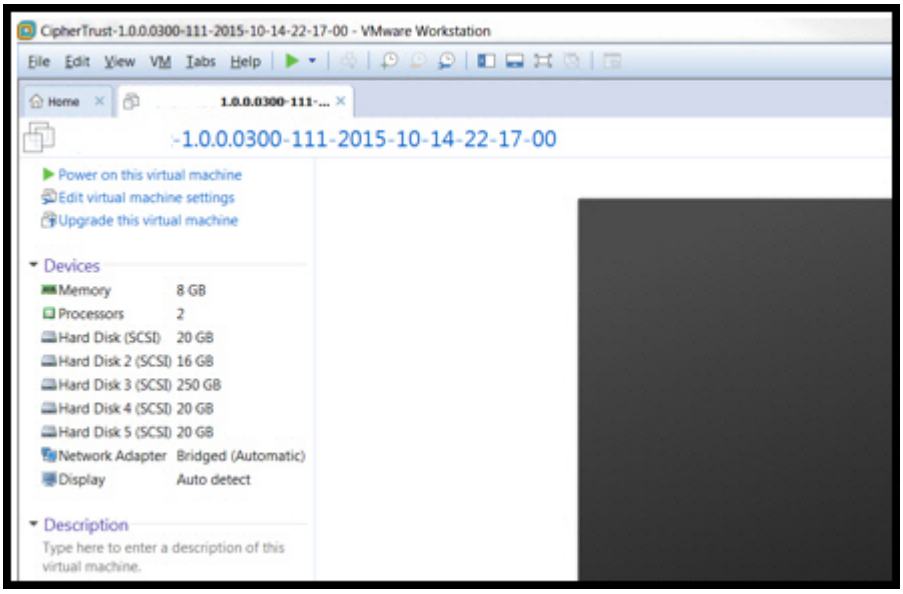
   If you decline the EULA, you will be unable to proceed with the installation.

   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.

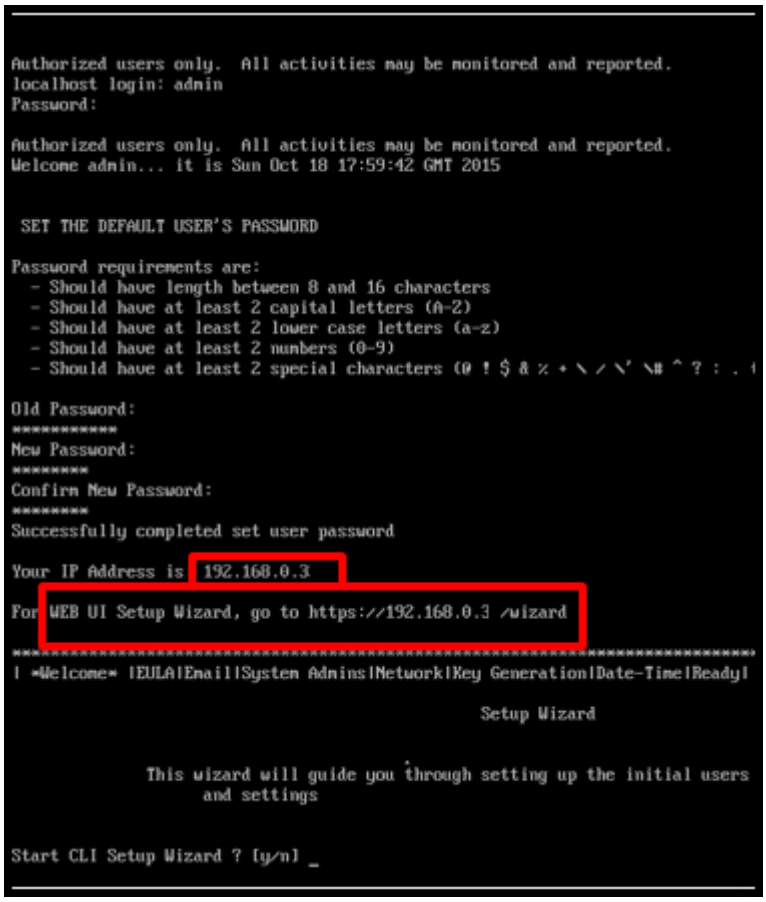
21.3. Run the Virtual Machine

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.



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 Docker instances

22.1. Prerequisites for using nShield Monitor with Docker

22.1.1. Docker container setup

The nShield Monitor Docker container ships as a `.tar.gz` file, for example `nShieldMonitor-x.x.x.xxxx.tar.gz`.

Before you can use the container, you must load it into a private Docker repository using:

```
docker load < nShieldMonitor-x.x.x.xxxx.tar.gz
```

22.1.2. Virtualization

The machine running nShield Monitor as a Docker container must have virtualization support (VT-x or AMD-V) enabled in its processor settings. To check if the processor has virtualization support, open a terminal and run:

```
LC_ALL=C lscpu | grep Virtualization
```

If the command does not return a response, then the processor does not support hardware virtualization. This means you need to enable virtualization support in the BIOS of the Docker host. The procedure for doing this depends on whether the machine is a physical or virtual machine and the virtualization technology it uses.

22.1.3. Docker volume files

You must have copied the following Docker volume files from the installation source to their permanent location on the Docker host for data to persist during the lifecycle of the nShield Monitor instance:

- `nsmvolume1`
- `nsmvolume2`
- `nsmvolume3`

- `nsmvolume4`
- `nsmvolume5`

22.2. Start an nShield Monitor Docker container

You must be a privileged user to use Docker.

You can start the nShield Monitor Docker container using either `docker compose` or `docker run`.

`docker compose` uses a YAML file to specify the parameters for the Docker container. With `docker run`, you specify the parameters in a single command in the console.

22.2.1. docker compose

`docker compose` uses the `docker-compose.yml` file to start up the nShield Monitor Docker container. Specify all the parameters for the container in the `docker-compose.yml` file.

To start an nShield Monitor Docker container using `docker compose`, in a privileged command-prompt, run:

```
docker compose up
```

To specify the parameters, set out the `docker-compose.yml` file as illustrated by the following example. All sections and parameters are mandatory unless otherwise stated.

```
version: '3.3'
services:
  nsm:
    privileged: true
    environment:
      - CPU=4 ①
      - RAM=4096 ②
      - HDA=/tmp/1 ③
      - HDB=/tmp/2
      - HDC=/tmp/3
      - HDD=/tmp/4
      - HDE=/tmp/5
    devices:
      -/dev/kvm
    volumes: ③
      -'<path to volumes>/nsmvolume1:/tmp/1'
      -'<path to volumes>/nsmvolume2:/tmp/2'
      -'<path to volumes>/nsmvolume3:/tmp/3'
      -'<path to volumes>/nsmvolume4:/tmp/4'
      -'<path to volumes>/nsmvolume5:/tmp/5'
```

```
    -'<path to bridge.conf>:/etc/qemu'
  ports: ④
    -'446:443'
    -'16166:16163'
    -'166:161/udp'
    -'167:162/udp'
    -'57:53'
    -'126:123'
    -'517:514'
    -'29:25'
    -'465:465'
    -'28:21'
  image:'<nsrepo>/nsm:x.x.x' ⑤
  stdin_open: true
  tty: true
```

① The number of CPU cores to be allotted to the container. This parameter is optional.

② The RAM, in bytes, to be allocated to the container. This parameter is optional. If you do not specify a value, it defaults to 2096 MB.

③ The `environment` variables `HDA` to `HDE` must correspond to the `volumes`. For example:

`nsmvolume1`, mounted as `/tmp/1`, is assigned to `HDA`. `nsmvolume2`, mounted as `/tmp/2`, is assigned to `HDB`, and so on.

④ Ports are declared in `x:y` pairs, where `x` denotes the port on the Docker host machine and `y` denotes the corresponding port on the nShield Monitor Docker machine.

Ensure the host port numbers are not used by other applications.

⑤ Change `<nsrepo>` for the repository where nShield Monitor resides.

22.2.1.1. Connect to the nShield Monitor container

After starting the nShield Monitor instance using `docker compose`, identify the container ID and connect to it using `docker attach`:

1. Retrieve the container IDs of the available nShield Monitor instances:

   ```
   docker ps
   ```

2. Note the `CONTAINER ID` of the required nShield Monitor instance from the output:

   ```
   CONTAINER ID   IMAGE                  COMMAND            CREATED      STATUS         PORTS NAMES
   88c61c1eb5d1   nsmrepo/nsm:x.x.x      "nShieldMonitor"   8 days ago   Up 7 seconds   ...   nsm2
   e7055016fb53   684a666d22ee           "nShieldMonitor"   9 days ago   Up 9 days      ...   nsm3
   ```

3. Using the `CONTAINER ID` from the previous step, connect to the container console:

   ```
   docker attach <CONTAINER ID>
   ```

   For example:

   ```
   docker attach 88c61c1eb5d1
   ```

After connecting to a console, continue using nShield Monitor in the same console.

22.2.2. docker run

`docker run` enables you to specify all parameters in a single command line at the console instead of using a `docker-compose.yml` file. You must be logged in as a privileged user to run this command.

After running the command, you can access nShield Monitor in the same console. There might be a delay between running the command and nShield Monitor being accessible.

```
docker run --privileged --device=/dev/kvm:/dev/kvm --device=/dev/net/tun:/dev/net/tun --cap-add NET_ADMIN  -it
--rm --device /dev/kvm --name mynet -v <path to volumes>/nsmvolume1:/tmp/1 -v <path to volumes>/nsmvolume2:/tmp/2
-v <path to volumes>/nsmvolume3:/tmp/3 -v <path to volumes>/nsmvolume4:/tmp/4 -v <path to
volumes>/nsmvolume5:/tmp/5 -e HDA=/tmp/1 -e HDB=/tmp/2 -e HDC=/tmp/3 -e HDD=/tmp/4 -e HDE=/tmp/5 -e BOOT=c -e
CPU=4 -e RAM=4096 -v <path to bridge.conf>:/etc/qemu -p 44:443 -p 16163:16163 -p 166:161/udp -p 167:162/udp -p
57:53 -p 126:123 -p 517:514 -p 29:25 -p 465:465 -p 28:21 nsrepo/nsm:x.x.x
```

Or:

```
docker run --privileged --device=/dev/kvm:/dev/kvm --device=/dev/net/tun:/dev/net/tun --cap-add NET_ADMIN -e
"AUTO_ATTACH=yes" -it --rm --device /dev/kvm --name ns37 --mount type=bind,source=<path to
volumes>/nsmvolume1,target=/tmp/1 --mount type=bind,source=<path to volumes>/nsmvolume2,target=/tmp/2 --mount
type=bind,source=<path to volumes>/nsmvolume3,target=/tmp/3 --mount type=bind,source=<path to
volumes>/nsmvolume4,target=/tmp/4 --mount type=bind,source=<path to volumes>/nsmvolume5,target=/tmp/5 -e
HDA=/tmp/1 -e HDB=/tmp/2 -e HDC=/tmp/3 -e HDD=/tmp/4 -e HDE=/tmp/5 -v <path to bridge.conf>:/etc/qemu -p 83:80 -p
443:443 -p 16163:16163 -p 161:161/udp -p 162:162/udp -p 54:53 -p 123:123 -p 514:514 -p 26:25 -p 465:465 -p 21:21
nsrepo/nsm:x.x.x
```

All parameters passed in the command are mandatory unless otherwise specified in the following table:

Parameter	Details
`--privileged`	Runs the nShield Monitor container in privileged mode.

Parameter	Details

`--device=/dev/kvm`
 	
`--device=/dev/net/tun`
	Both devices must exist on the host.

`--cap-add NET_ADMIN`	This is a necessary capability for the container.
`--it`	Enables interactive mode.
`--rm`	Removes the container on exit. Data persists in the volumes. Optional
`--name <container-name`	Specifies the container to use. Optional

`-v /root/ns2/nsmvolume<x>:/tmp/<x>`
 	
and
 	
`-e HD<X>=/tmp<x>`
	Creates volume to environment variable mapping.
	
	The volumes (`-v`) must correspond to the environment variables (`-e`) from `HDA` to `HDE`. For example, `-v <path to volumes>/nsmvolume1:/tmp/1` corresponds with `-e HDA=/tmp/1`, and `-v <path to volumes>/nsmvolume2:/tmp2` with `-e HDB=/tmp/2`.

`-e CPU=4`	Specifies the number of cores to allot to the Docker container. Optional
`-e RAM=4096`	Specifies the amount of RAM to allot to the Docker container. Optional. If you do not specify a value, it defaults to 2096 MB.
`-v <path to bridge.conf>:/etc/qemu`	The location of the `bridge.conf` file, which must contain the line: `allow all`.
`-p <x>:<y>`	Ports (`-p`) are declared in `x:y` pairs, where `x` denotes the port on the Docker host machine and `y` denotes the corresponding port on the nShield Monitor Docker machine. Ensure the host port numbers are not used by other applications.

Parameter	Details
`nsrepo/nsm:x.x.x`	Specifies the Docker repository where nShield Monitor resides. Ensure you change `nsrepo` for the name of the repository in use.

22.3. Connect to the web UI for the nShield Monitor

To access the nShield Monitor web UI from a browser on a machine that is not the Docker host, use the Docker host IP address followed by the host port that is mapped to port `443` on the container (https://<docker-host-ip>:<host-port>/login). This port mapping was specified in either the `docker-compose.yml` file or in the `docker run` command, depending on how you started it.

To access the web UI from the Docker host machine, you need to inspect the container's settings to determine the IP address assigned to it. Docker manages the network settings of a container.

1. Retrieve the container IDs of the available nShield Monitor instances:

   ```
   docker ps
   ```

2. Note the `CONTAINER ID` of the required nShield Monitor instance.

   ```
   CONTAINER ID   IMAGE                  COMMAND            CREATED      STATUS         PORTS NAMES
   88c61c1eb5d1   nsmrepo/nsm:x.x.x      "nShieldMonitor"   8 days ago   Up 7 seconds   ...   nsm2
   e7055016fb53   684a666d22ee           "nShieldMonitor"   9 days ago   Up 9 days      ...   nsm3
   ```

3. Using the `CONTAINER ID`, inspect the network settings of the container console:

   ```
   docker inspect <CONTAINER ID>
   ```

4. Use the `IPAddress` in the output to access the container.
   - If you used `docker run` to start the nShield Monitor container, the output appears as follows:

     ```
     "NetworkSettings": {
               "Gateway": "172.17.0.1",
               "IPAddress": "172.17.0.3",
               "Networks": {
                    "bridge": {
                        "Gateway": "172.17.0.1",
                        "IPAddress": "172.17.0.3",
                    }
                }
     ```

```
}
```

In this example, you would access the container via https://172.17.0.3/login.

If a port other than 443 was mapped, the access URL changes to https://172.17.0.3:<host_port>/login, for example https://172.17.0.3:444/login.

- If you used `docker compose` to start the nShield Monitor container, the output appears as follows:

```
"NetworkSettings": {
           "Gateway": "",
           "IPAddress": "",
           "Networks": {
                "ns2_default": {
                    "Gateway": "172.23.0.1",
                    "IPAddress": "172.23.0.2",
                }
            }
}
```

In this example, you would access the container Web UI via https://172.23.0.2:<host_port>/login.

22.4. Assign a usable IP to a nShield Monitor container

To change the Web UI access IP for the container:

1. List the available networks:

```
docker network ls
```

2. From the list, note the name of the network in which you started the container, for example:

```
NETWORK ID     NAME          DRIVER    SCOPE
a9cd9ed46e6b   bridge        bridge    local
6af6b576d8a3   host          host      local
42d390a3fdb1   none          null      local
240d738c0a8b   ns2_default   bridge    local
```

If you started with `docker run`, the network is the default `bridge` network. If you started with `docker compose`, the network is a specific `bridge` network that has the same name

> as the container, for example `ns2_default`.

3. Inspect the network relevant to the container, for example:

```
docker network inspect bridge
```

or

```
docker network inspect ns2_default
```

4. Note the `Subnet` and `Gateway` settings displayed in the output:

```
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.17.0.0/16",
                    "Gateway": "172.17.0.1"
                }
            ]
        },
```

5. If required, use this information to reconfigure the container in the nShield Monitor CLI.

> This is an advanced configuration. You must specify all parameters correctly for the Docker container to be accessible on the network. For more information on using these commands, see Network commands.

   a. Configure the network with DHCP configuration inside the nShield Monitor Docker container, because Docker uses it to assign unique IP addresses to each container.

```
network configure dhcp
```

   b. If you assign a specific IP address to the container, make sure that the parameters fall within the subnet that the earlier `docker inspect` command returned:

```
network configure static
```

22.5. Troubleshooting container startup errors:

22.5.1. Port binding errors

Rerun the command and specify a different host port in the `docker compose` or `docker run` command.

22.5.2. Write lock errors

You must assign a unique set of volumes to each container. Containers cannot share the same set of volumes. Copy a new set of the provided Docker volumes to launch a new instance of an nShield Monitor Docker container. After starting the container, you can access it using `docker attach`.

22.5.3. Formatting and directory errors

Ensure that the volumes are present at the location specified by the `docker run` or `docker compose` syntax and that they are regular files.

23. Create and Manage Hyper-V Virtual Machines in Hyper-V Core

23.1. 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-3.1.0-1.vhd`
- `nShieldMonitor-3.1.0-2.vhdx`
- `nShieldMonitor-3.1.0-3.vhdx`
- `nShieldMonitor-3.1.0-4.vhdx`
- `nShieldMonitor-3.1.0-5.vhdx`

23.2. 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.

23.2.1. 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.

23.2.2. 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**.

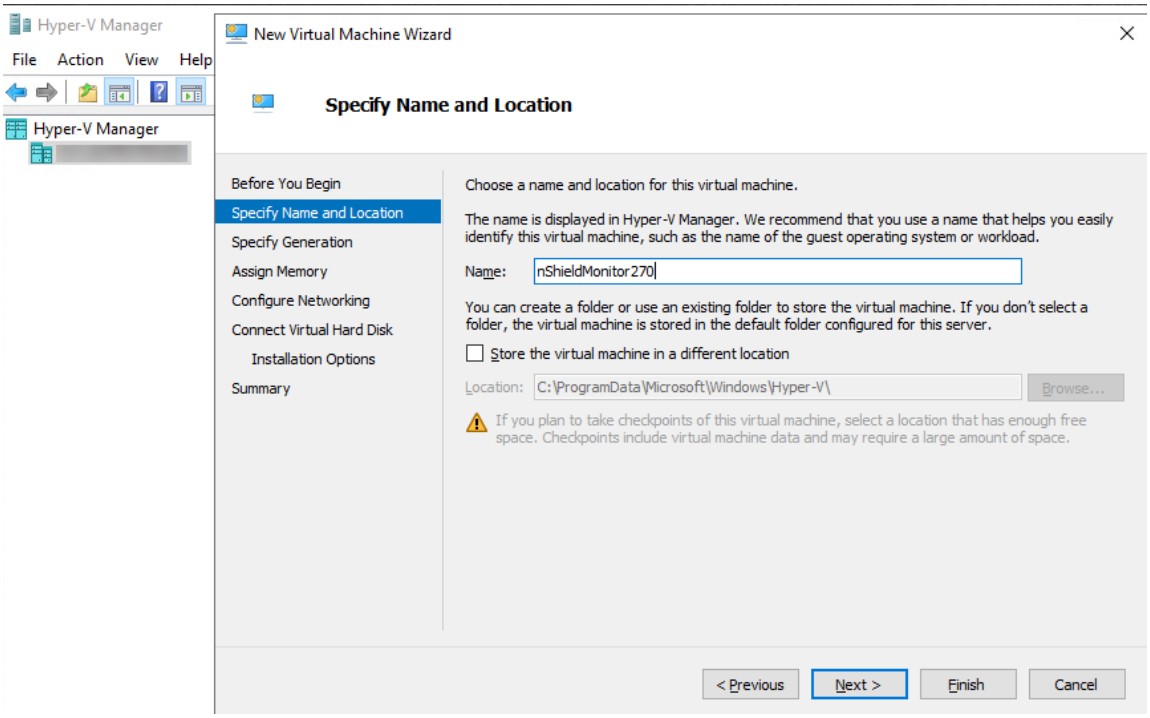
Windows Admin Center will calculate the dependencies of role and feature installations and then prompt you to proceed with the installation, including automatic reboot options.

3. When Windows Server has rebooted, check in **Server Manager > Roles and Features** that the **State** for the Hyper-V role is **Installed**.

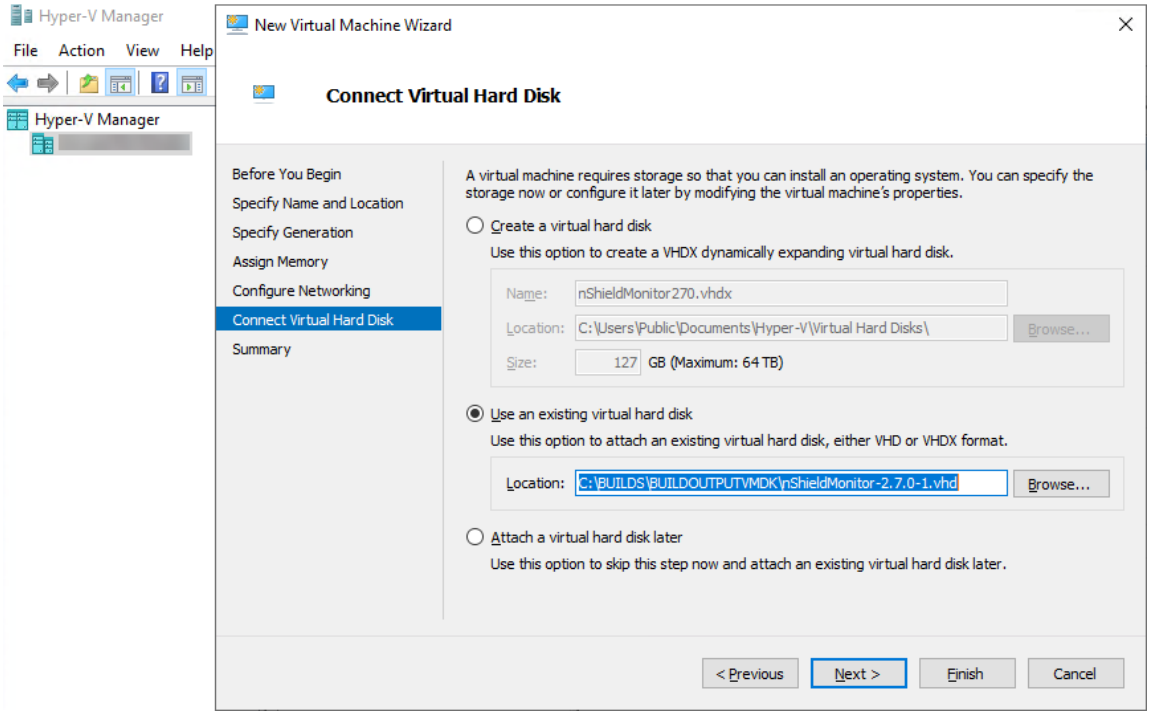
23.3. Configure a new virtual machine with Hyper-V

1. In Windows Admin Center, select **Server Manager**, then launch **Hyper-V Manager**.
2. Select **New > Virtual Machine**.

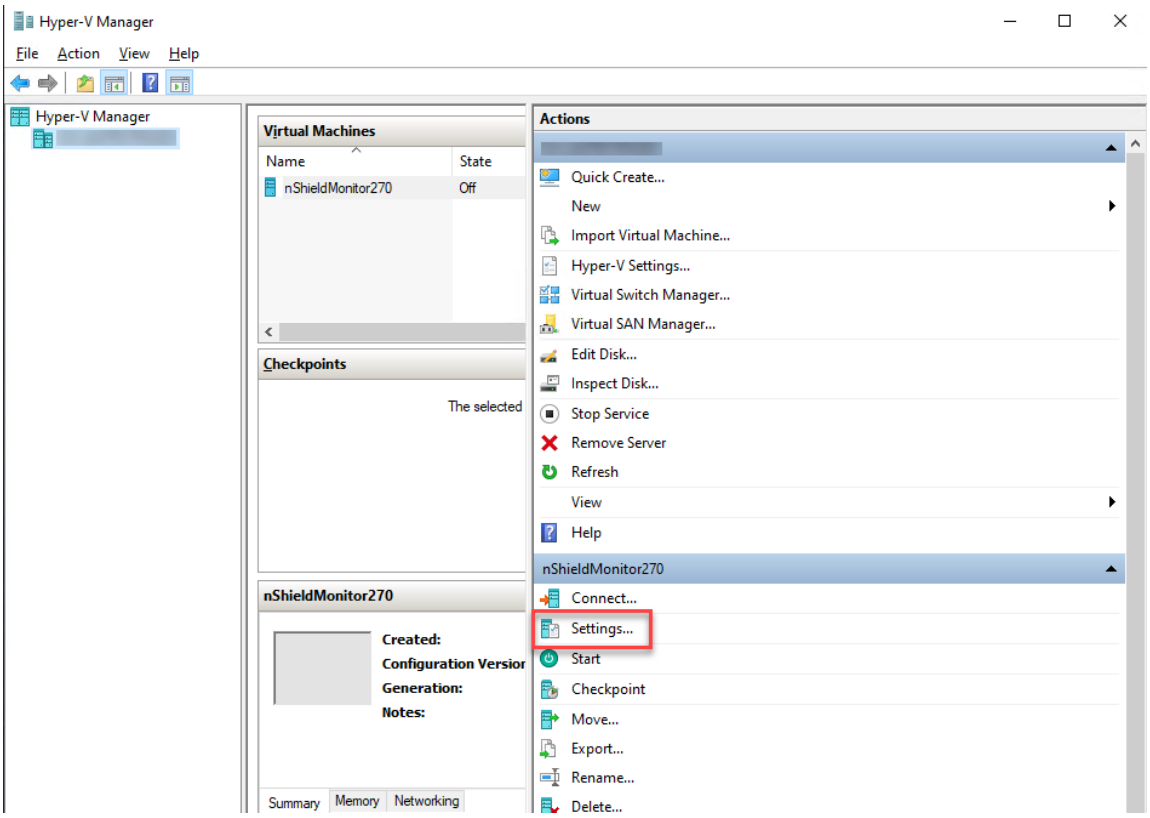
   The **New Virtual Machine Wizard** opens.



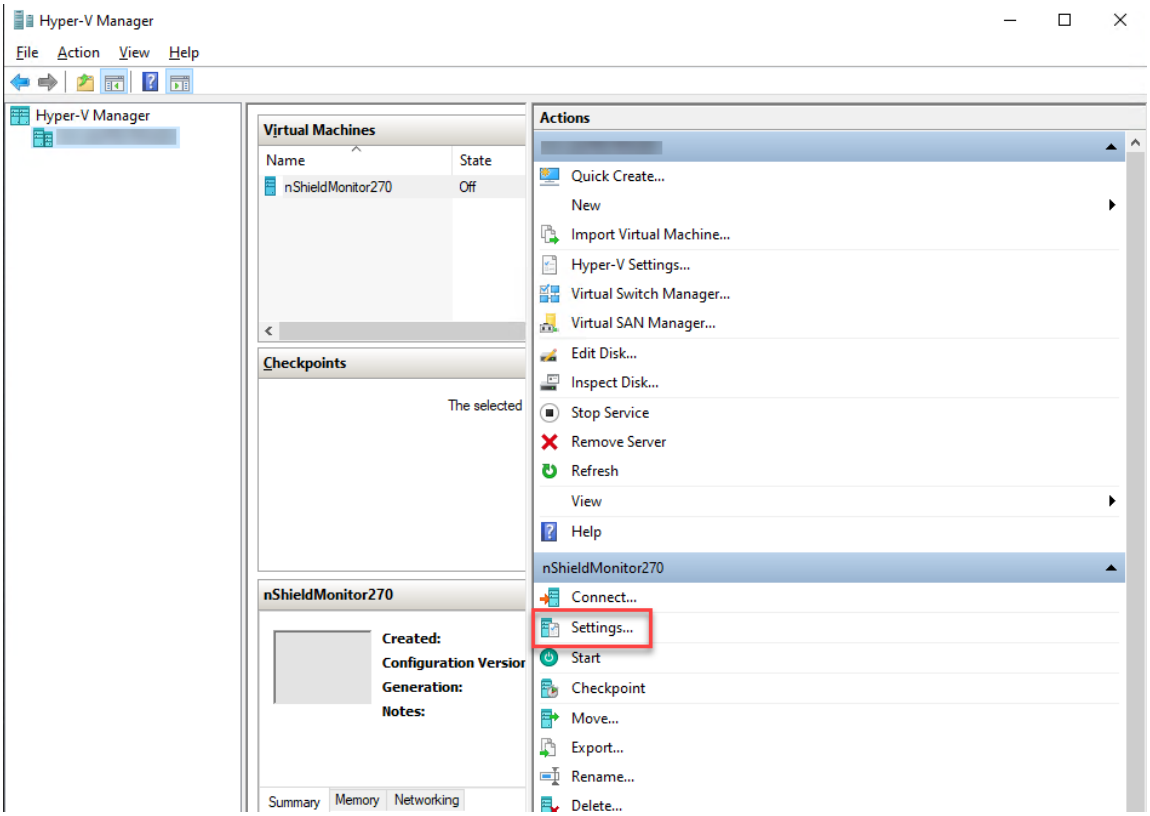
3. Specify the **Name** and **Location** of the virtual machine, then select **Next**.
4. Select **Generation 1**, then select **Next**.
5. Set the **RAM Size**, then select **Next**.
6. Set the **Connection** to **Default Switch**, then select **Next**.
7. Attach the boot hard disk (VHD file) for nShield Monitor.



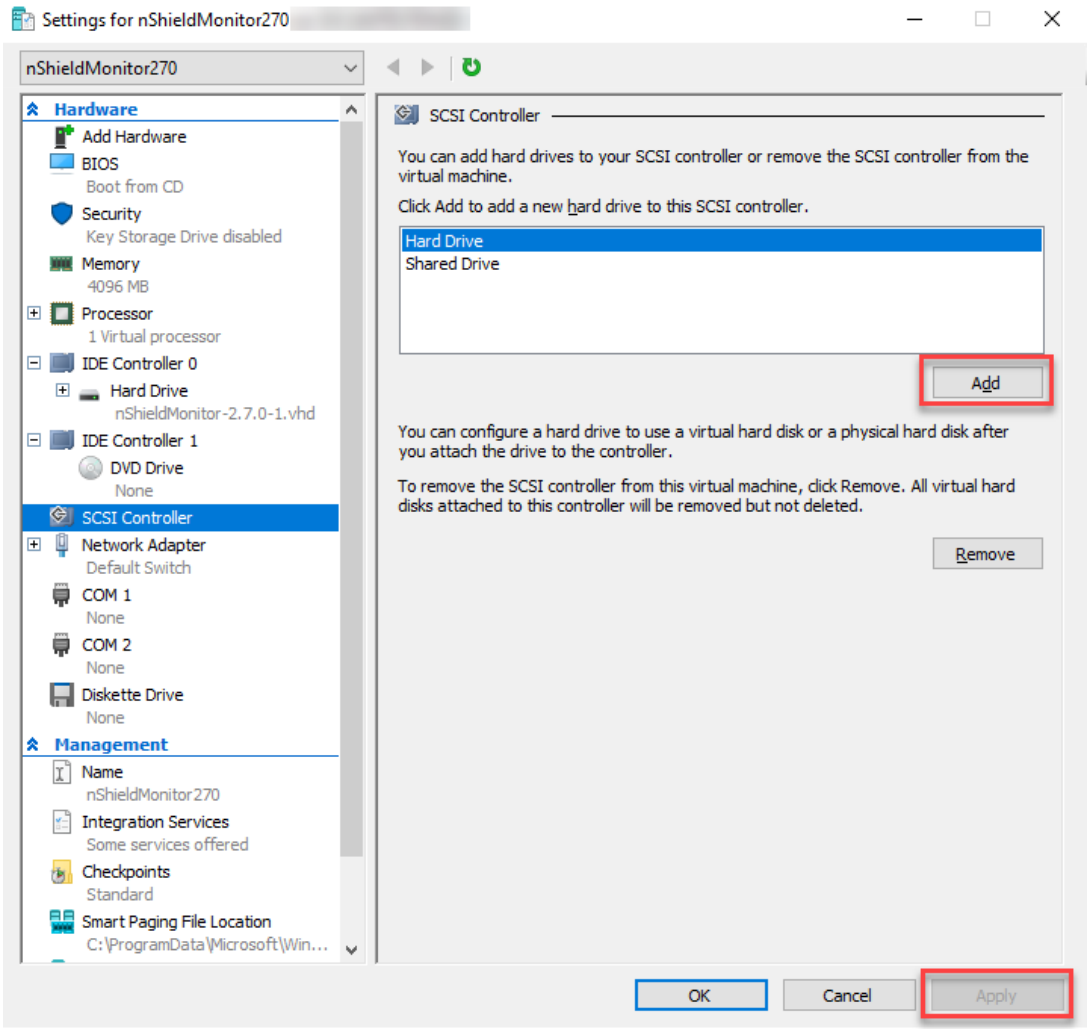
8. Select **Next**, then select **Finish**.
9. In the new machine, select **Settings**.



10. Select **SCSI Controller**, then add the remaining four hard drives of nShield Monitor.



a. Select **Hard Drive**, then select **Add**.

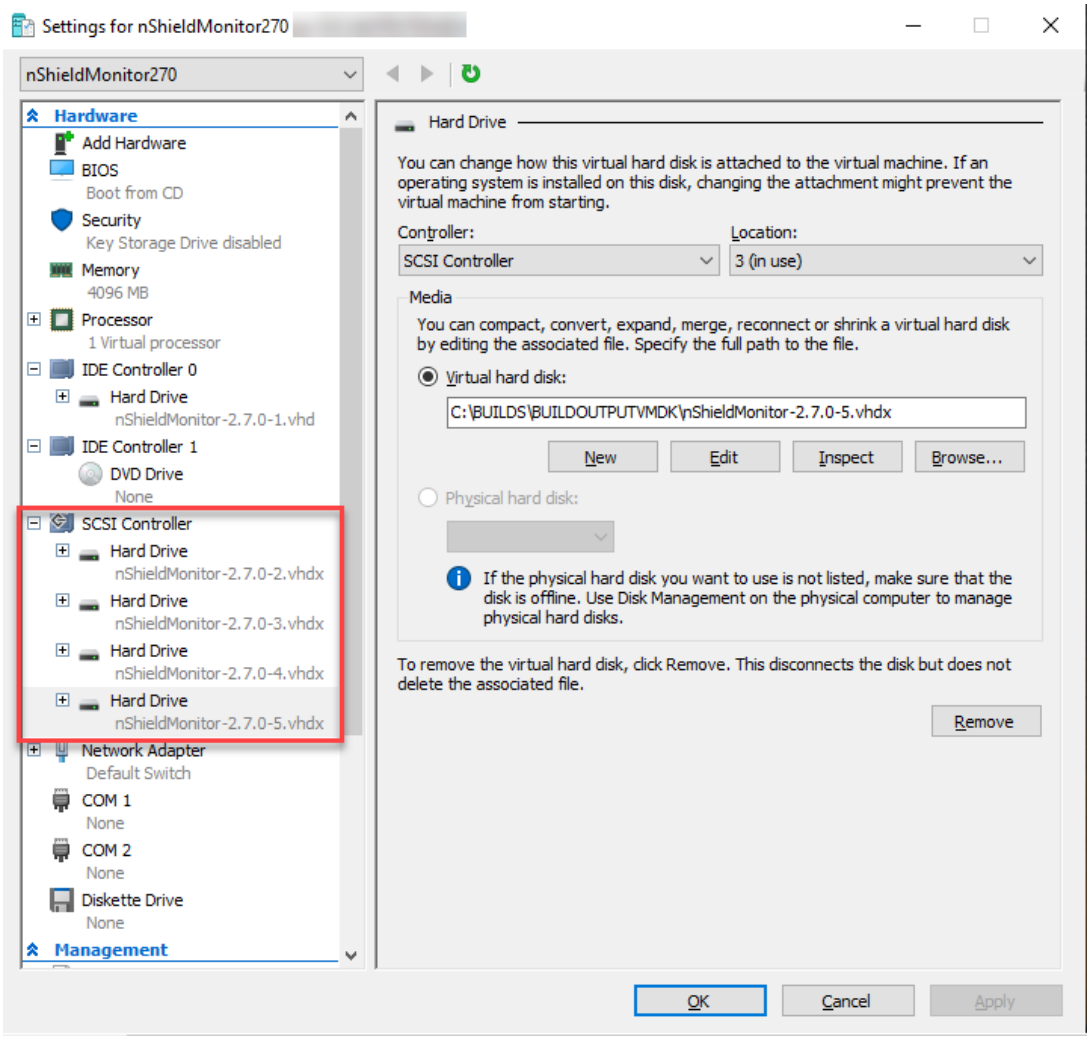


b. In the **New Virtual Hard Disk Wizard**, select **Copy the contents of the specified virtual hard disk**, browse to the **-2.vhdx** file, and add it.

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.