LogicVein

User's Manual

Contents

Revision history

Edition number	Date of issue	Revised content
Rev.1	9/27/2024	First edition issued
Rev.2	8/4/2019	Revised explanations and images as functions were added
Rev.3	10/9/2019	Revised explanations and images
Rev.4	3/9/2020	Add config backups
Rev.5	2/2022	Updated documentation for remediation and EOL/EOS
Rev.6	09/2022	Modified EOL/EOS
Rev.7	9/2023	Changes due to added functionality
Rev.7.6	05/2024	Changes due to added functionality
Rev 7.7	09/2024	Added new features – playbook/2FA/device groups/anomaly alert
Rev 7.8	01/2025	Added new features – playbook/2FA/device groups/anomaly alert
Rev 7.9	03/2025	Added multi-tenancy feature

1 Introduction

This document is a manual for the network fault monitoring software “ThirdEye.” This section explains various settings and operation methods for ThirdEye.

1.1 About ThirdEye

ThirdEye is a network fault monitoring tool that can be used in a wide range of environments, from small to large network environments. With ThirdEye, you can:

- Polling monitoring (ICMP Ping, SNMP polling)
- SNMP trap monitoring
- Threshold monitoring
- Incident management (severity, status, priority, assignee, event aggregation)
- Dashboard management (graph display of statistical information, customization of widgets)
- Inventory management (customize display, sort, search)
- Map management (hierarchical structure settings, map tree display, incident notification, automatic drawing of L2 map)
- Monitoring item set/template registration
- Export statistics
- Setting the non-monitoring period
- Trail management with terminal proxy
- Email notifications on incident updates
- Compiling private MIBs
- Configuration backup and generation management
- Change settings of network devices (router/switch/firewall, etc.)
- Syslog monitoring

1.2 About ThirdEye editions

ThirdEye is available in two editions: “Suite” and “Enterprise”. Available features vary depending on the edition. For functional differences between editions, please refer to the **Main function comparison table by edition** below. All functions in this document are explained based on the highest edition. Some “Suite” functions may not be available in “Enterprise”. Features that are only available in “Suite” are indicated with the following icon: Suite

- No icon: Available in all editions.
- Suite: Available only in “Suite”.

1.2.1 Main feature comparison table by edition

Function	ThirdEye	ThirdEye Suite
Discovery	✓	✓
Monitoring		
ICMP	✓	✓
SNMP	✓	✓
SNMP Trap	✓	✓
HTTP/HTTPS	✓	✓
TCP Port	✓	✓
vCenter	✓	✓
VMware Guest	✓	✓
VMware Host	✓	✓
Xen Server	✓	✓
Agent-D	✓	✓
Syslog Monitoring	✓	✓
Maintenance Windows		
Manual	✓	✓
Scheduled	✓	✓
Monitor Alert Actions		
Incident	✓	✓
Email	✓	✓
Command Execution	✓	✓
Trap Sending	✓	✓
Job Execution	✗	✓
Configuration Management		
Configuration Backup	✓	✓
Configuration History	✓	✓
Compare	✓	✓
Export	✓	✓
Configuration Change		
Smart Change	✗	✓
Restoration	✓	✓
Change Tools	✗	✓
Draft Configuration	✗	✓
Terminal Proxy		
Telnet/SSH Connection	✓	✓
Saving Operation History	✓	✓
Dashboard		

Function	ThirdEye	ThirdEye Suite
Addition	✅	✅
Share	✅	✅
Widget	✅	✅
Report	✅	✅
Incident	✅	✅
Job	✅	✅
Compliance	❌	✅
Report	✅	✅
MIB Compilation	✅	✅
Zero-Touch (Optional)	❌	✅
Playbooks	❌	✅

1.3 Environmental Settings

ThirdEye is available as a virtual appliance and supports the following platforms:

- VMware ESXi (version 7.0 or higher)
- Windows Hyper-V (Windows Server 2016 or later)
- Amazon Web Services*
- Nutanix AHV
- Linux KVM
- Microsoft Azure

The following environment is required for ThirdEye:

Item	Recommendation	Default	Minimum
Hard disk	HDD1: 2.5 GB HDD2: 50 GB or more	HDD1: 2.5 GB HDD2: 50 GB	HDD1: 2.5 GB HDD2: 50 GB
HDD provisioning	Thin or Thick	Thin or Thick	Thin or Thick
Memory	8 GB or more	16 GB	8 GB
CPU	8 cores or more	16 cores	4 virtual CPUs (cores)

*Both thin and thick HDD provisioning types are supported.

1.4 List of ports used

The ports that ThirdEye uses for communication are shown below. If you need to access your device through a firewall, change your firewall's communication settings to ensure the required ports are open.

Feature	**Port**	Protocol	UDP/TCP	Communication Direction
Zero-Touch	**67**	DHCP	UDP	ThirdEye ← Destination
	68	DHCP	UDP	ThirdEye → Destination
	80	HTTP	TCP	ThirdEye ← Destination
	69	TFTP	UDP	ThirdEye ← Destination
	-	ICMP	-	ThirdEye ← Destination
Auto-Discovery	**22, 23**	SSH, Telnet	TCP	ThirdEye → Destination
	161	SNMP	UDP	ThirdEye → Destination
	-	ICMP	-	ThirdEye → Destination
Restore Configuration	**22, 23**	SSH, Telnet	TCP	ThirdEye → Destination
	69	TFTP	UDP	ThirdEye ← Destination
	20, 21	FTP	TCP	ThirdEye ← Destination
Modify Configuration via Tools	**22, 23**	SSH, Telnet	TCP	ThirdEye → Destination
Send Trap	**162**	SNMP Trap	UDP	ThirdEye → Destination
SNMP Monitoring	**161**	SNMP	UDP	ThirdEye → Destination
Receive Trap	**162**	SNMP Trap	UDP	ThirdEye ← Destination
WMI/WinRM Monitoring	**5985**	HTTP	TCP	ThirdEye → Destination
	5986	HTTPS		
Real-Time Change Detection	**514**	Syslog	UDP	ThirdEye ← Destination
Backup*	**22, 23**	SSH, Telnet	TCP	ThirdEye → Destination
	161	SNMP	UDP	ThirdEye → Destination
	69	TFTP	UDP	ThirdEye ← Destination
	20, 21	FTP	TCP	ThirdEye ← Destination
Terminal Proxy	**2222, 443**	SSH or HTTPS	TCP	ThirdEye ← Client PC
	22, 23	SSH, Telnet	TCP	ThirdEye → Destination
Web Terminal	**443**	HTTPS	TCP	ThirdEye ← Client (GUI)
	22, 23	SSH, Telnet	TCP	ThirdEye → Destination
Client Access	**443**	HTTPS	TCP	ThirdEye ← Client (GUI)
External Authentication	**389**	LDAP	TCP	ThirdEye → Authentication server
	1812	RADIUS	UDP	ThirdEye → Authentication server

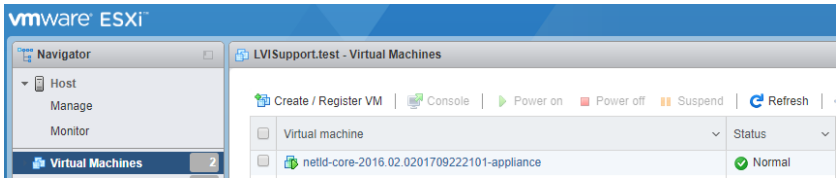
*The appropriate settings for the protocol you use will depend on the type of device you are using. For example, for IOS devices, "CLI (Telnet, SSH) only or both CLI and TFTP".

2 Installation

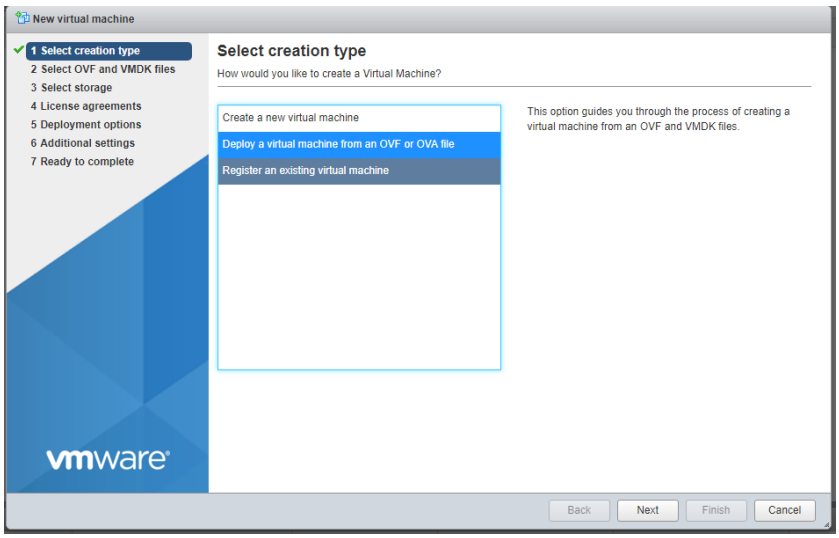
2.1 Deployment to VMware ESXi

This section describes the deployment procedure to VMware ESXi. Here we will explain using ESXi 6.5 as an example.

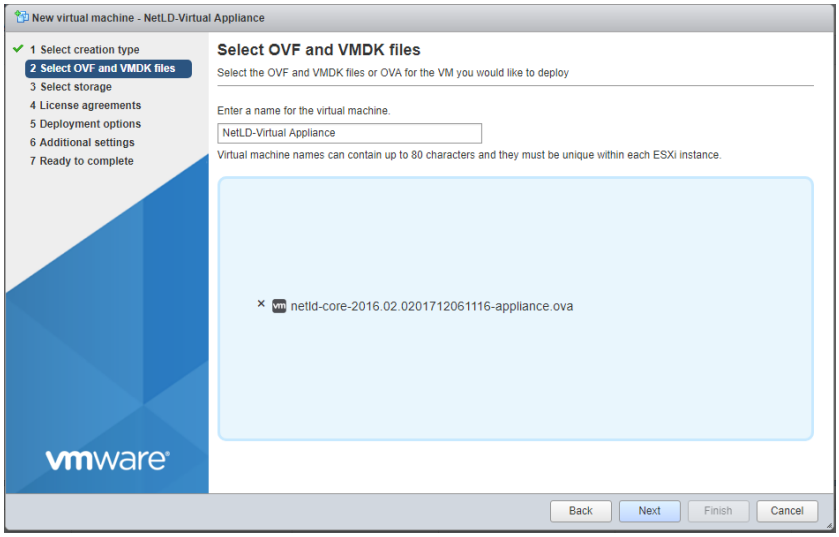
1. Log in to the Web UI and click [Create/Register Virtual Machine] from the virtual machine.



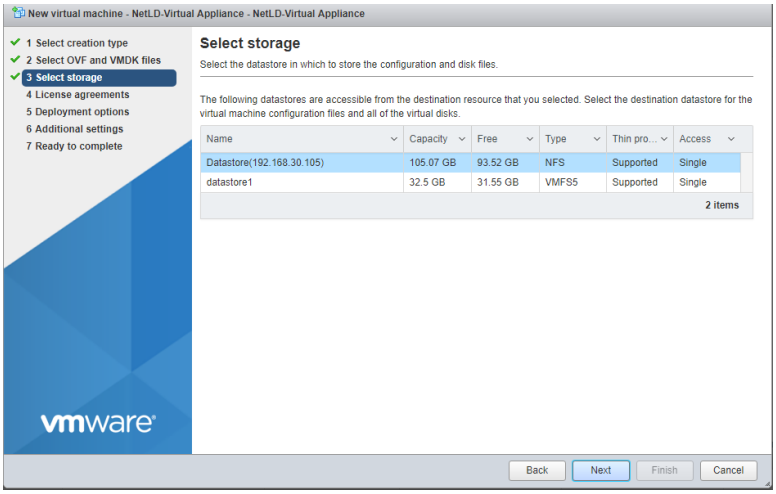
2. Select “Deploy a virtual machine from an OVF or OVA file” and click [Next].



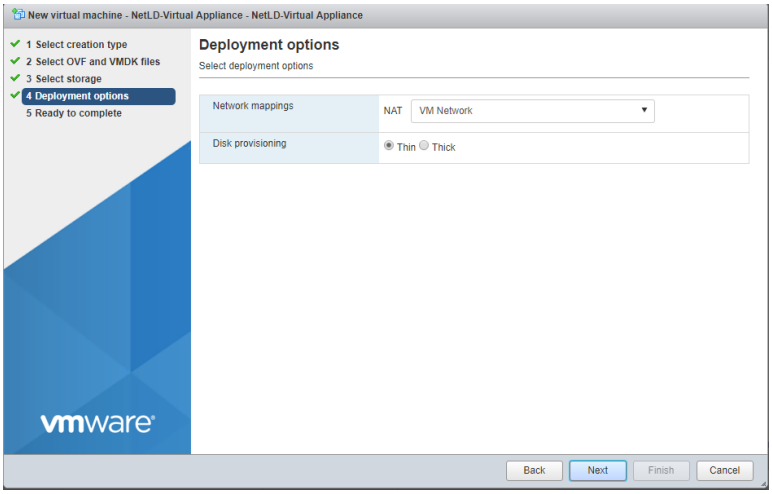
3. After entering the desired virtual machine name, drag and drop the OVA file “lvi-core-****-appliance.ova” and click [Next].



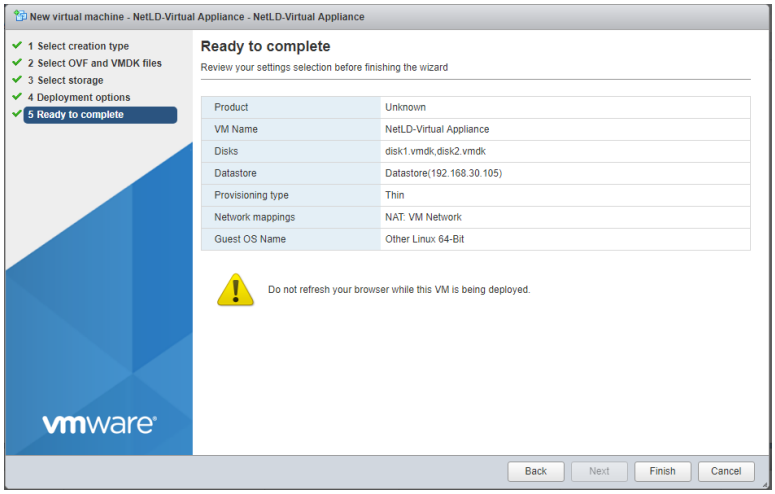
4. Select your storage and click [Next].



5. Select the network and disk provisioning you want to deploy and click [Next].



6. Click [Finish].



After deployment is completed, please start the new virtual machine.

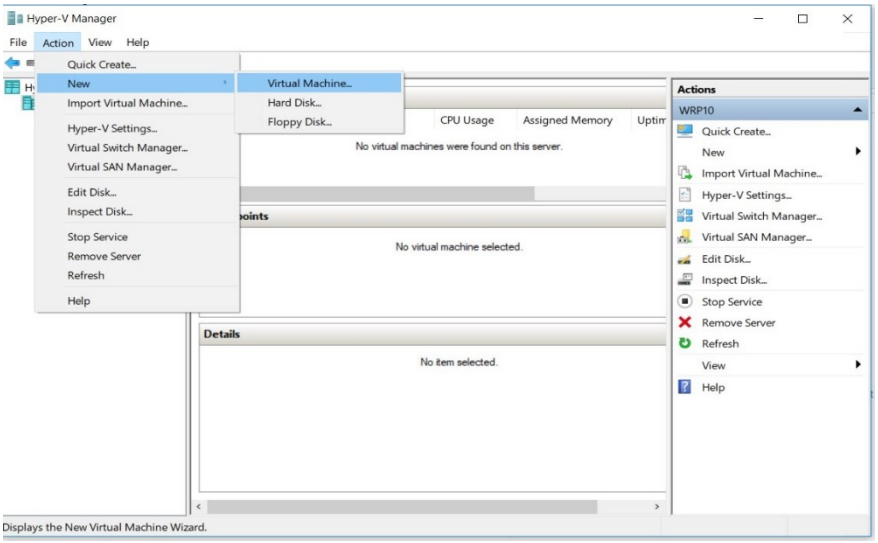
2.2 Deployment to Windows Hyper-V

This section describes the deployment procedure to Windows Hyper-V. Here we will explain using Windows Server 2016 as an example.

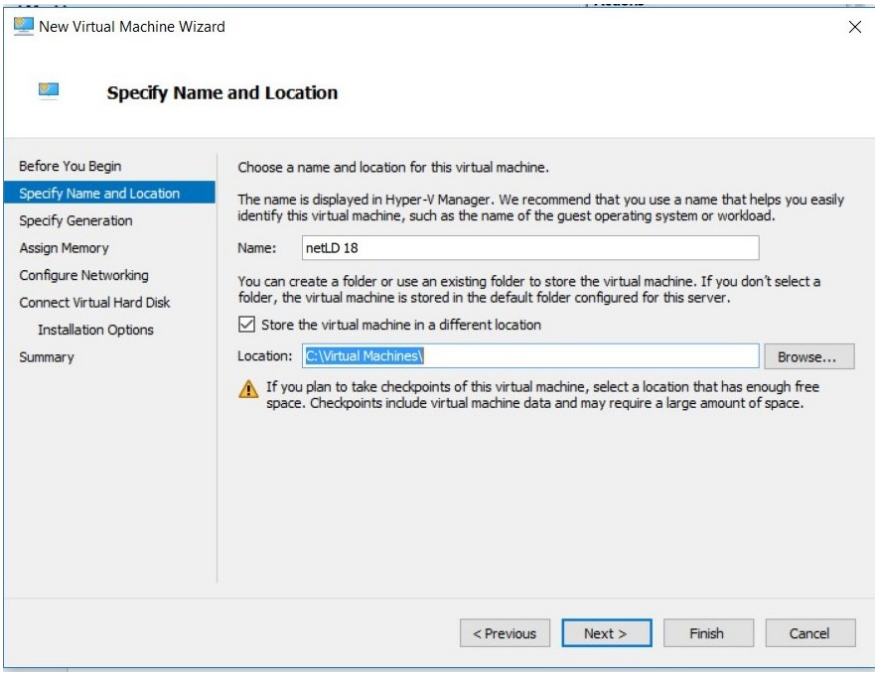
Prerequisites

- Hyper-V must be installed in Roles and Features.
- At least one virtual switch is required.

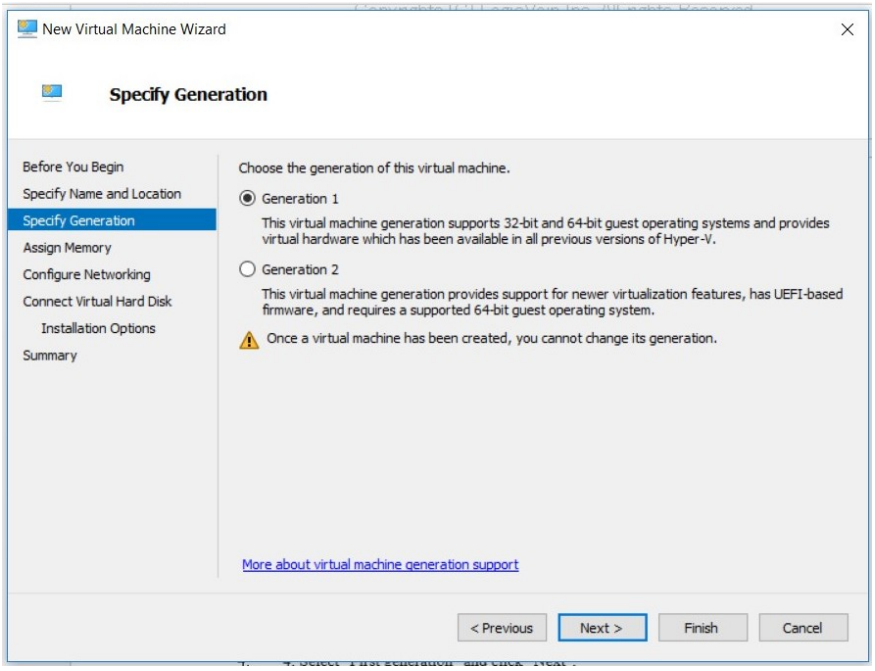
1. Start Hyper-V Manager and click [New] > [Virtual Machine].



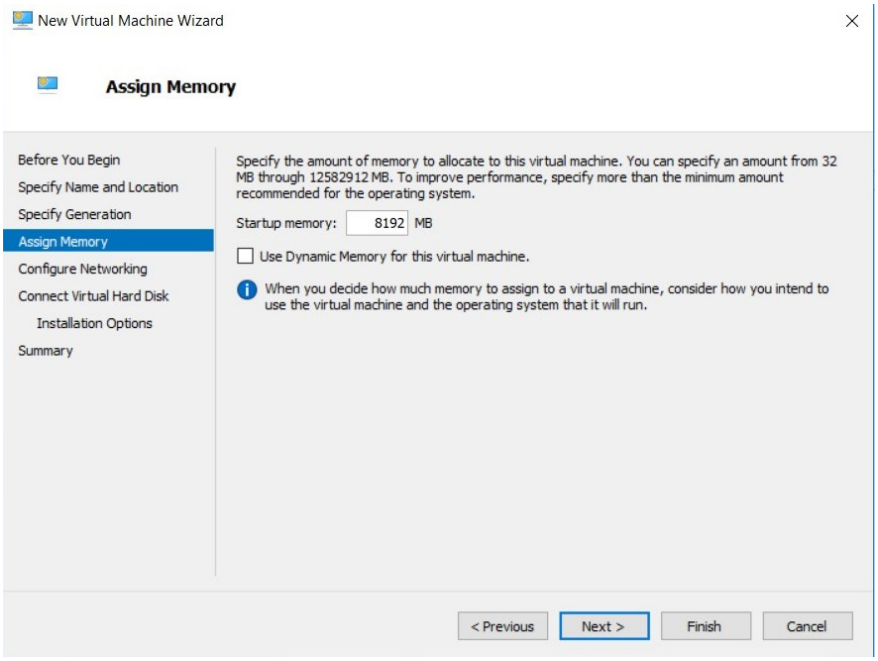
2. Enter a name for your virtual machine and click [Next].



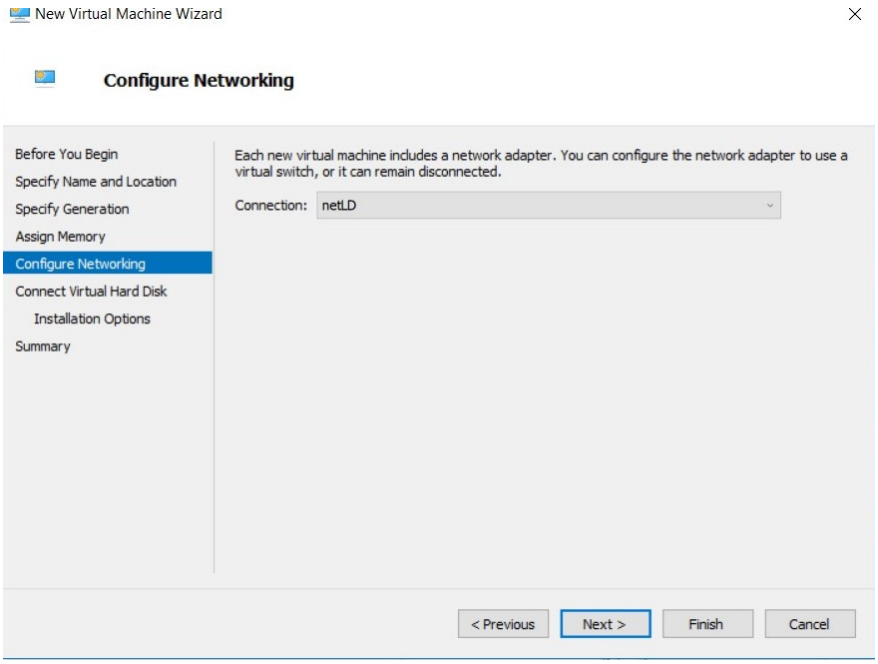
3. Select “Generation 1” and click [Next].



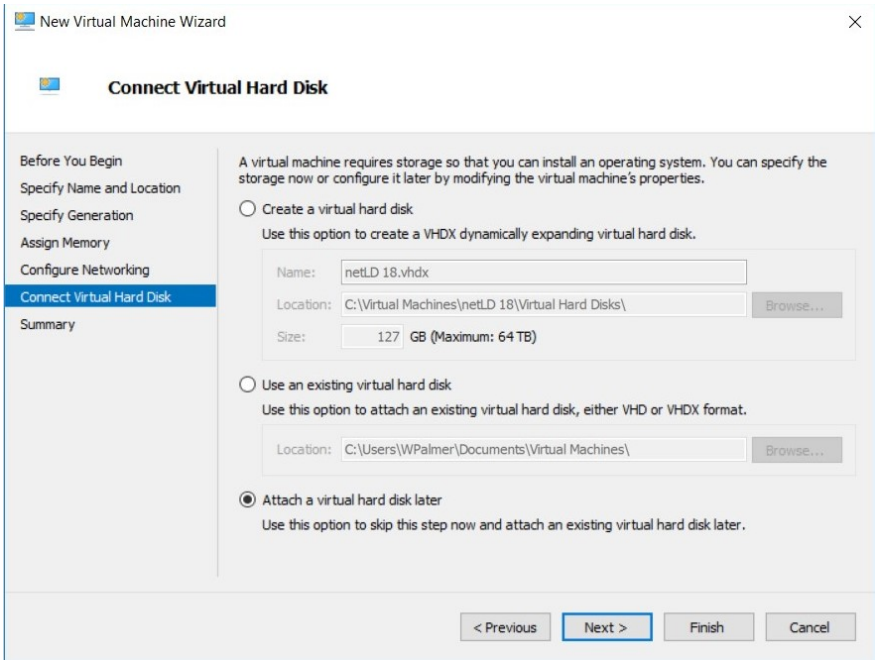
4. Set the startup memory and click [Next].



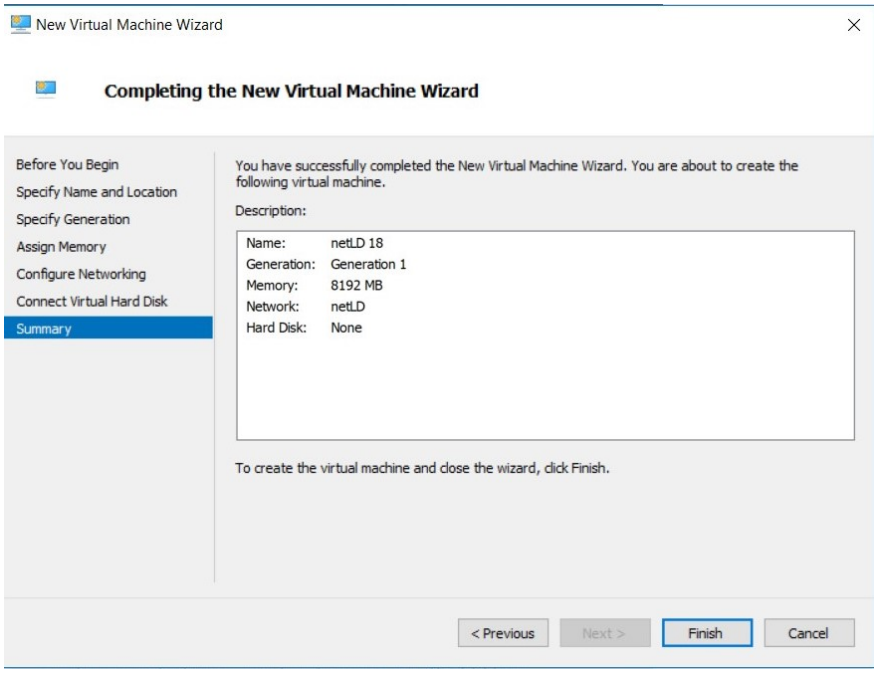
5. Select the virtual switch you want to connect to and click [Next].



6. Select “Attach a virtual hard disk later” and click [Next].



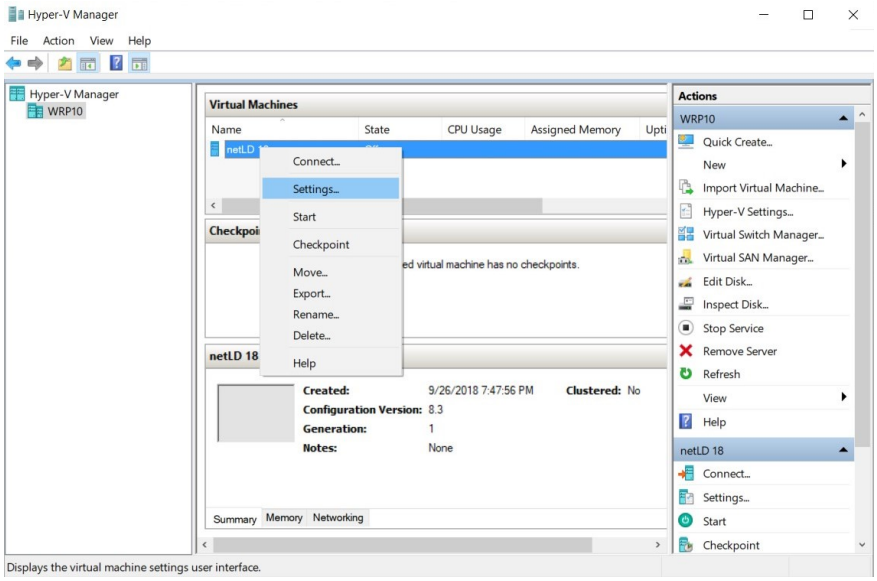
7. Click [Finish].



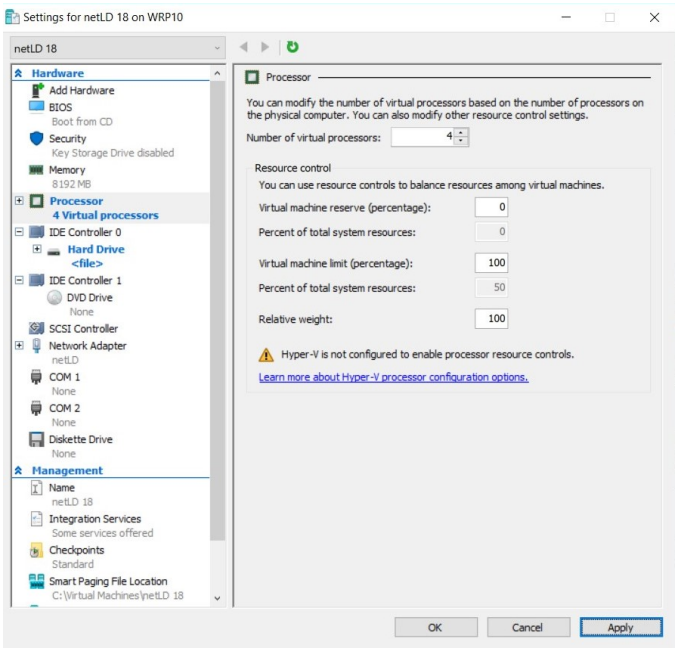
The virtual machine will now be created.

Next, assign the two VHDX files to the created virtual machine.

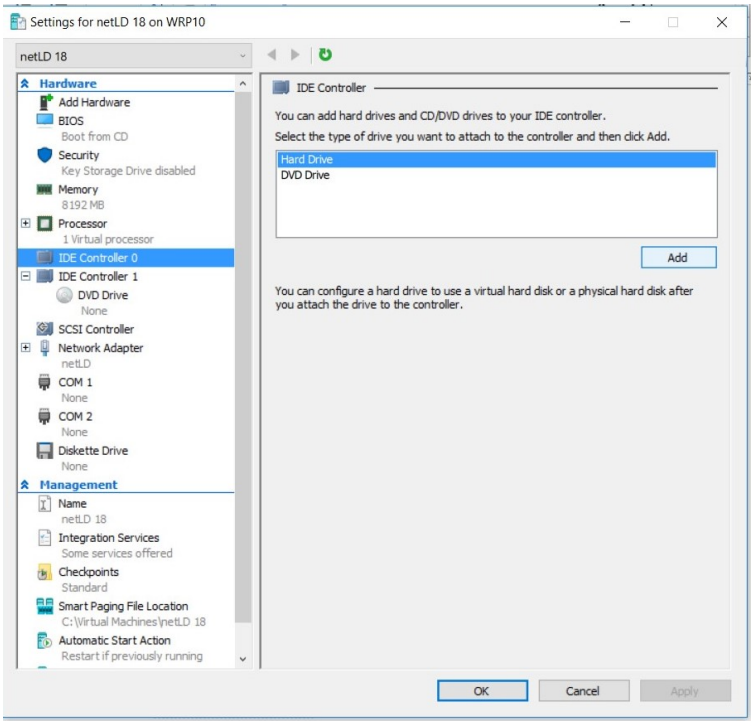
8. Right-click the virtual machine you created and click Settings.



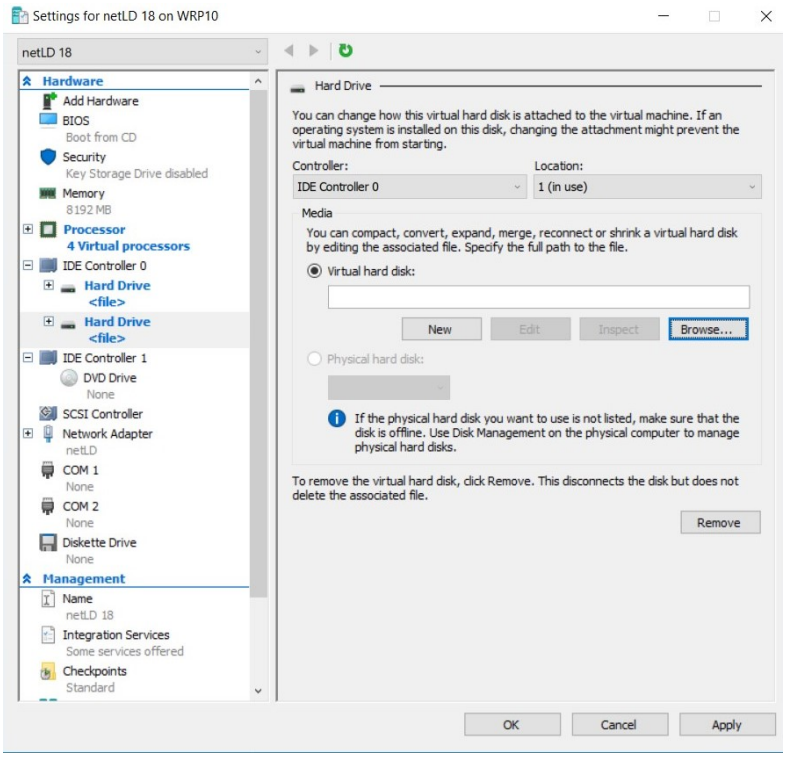
9. Select “Processor” and change [Number of virtual processors].



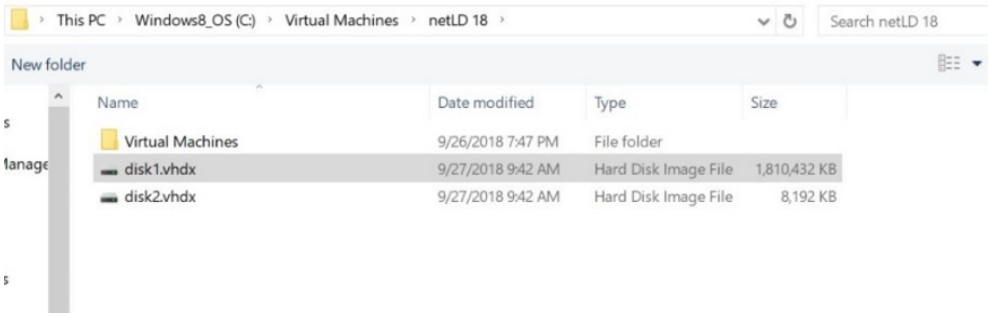
10. Select “IDE Controller 0” and click [Add].



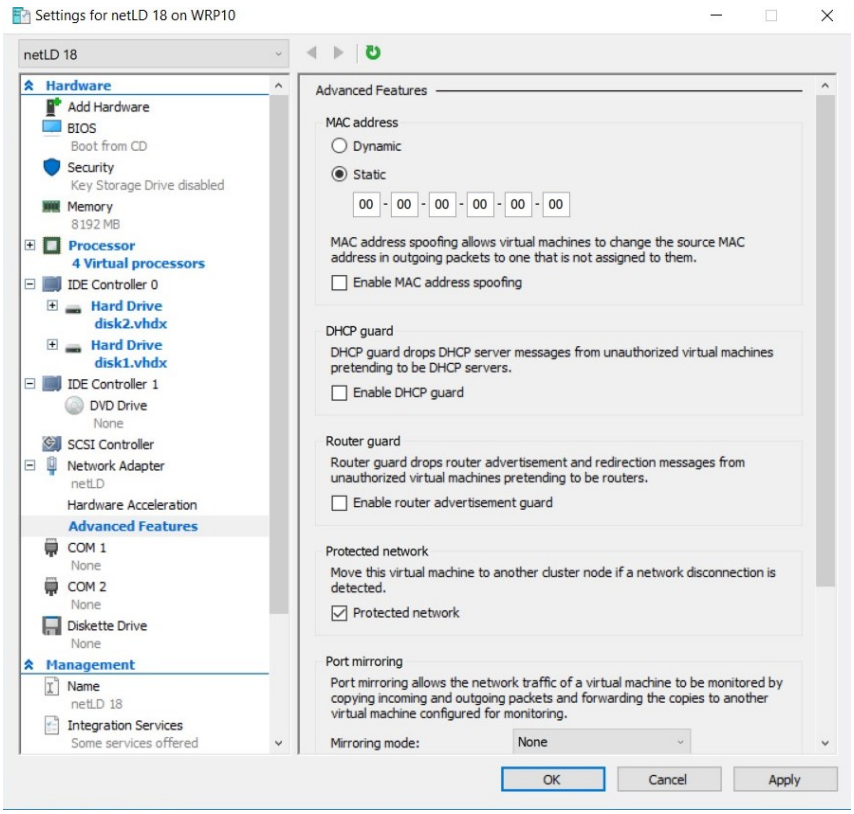
11. Click [Browse].



12. Add “disk1” and click [OK].



13. Repeat steps 8 to 12 to add “`disk2.vhdx`”.
14. Click [OK].



This completes the Windows Hyper-V deployment.

2.3 Deploying to Linux KVM

1. Save the qcow2 file in a directory of your choice.
2. Launch “Virtual Machine manager”.
3. From the file menu, click [New Virtual Machine].
4. Select “Import an existing disk image” and click [Next].
5. Specify the uploaded file in “Specify the path of the existing storage”.
6. In “select the operating system you want to install”, select “Generic or unknown OS”.
7. Enter the resources you want to assign and click [Next].
8. Enter a name for the virtual machine and check “Customize settings before installation”.
9. Open [Network Selection], select the device that matches your network environment and click [Finish].
10. Click on [IDE Disk1] and change the Disk Bus to “SCSI”.
11. Click on [Add Hardware] and add at least 50GB of storage.
12. Click [Begin Installation].

This completes the KVM deployment

2.4 Deploying to Nutanix AHV+

1. Login to Nutanix Prism and go to Settings from the pull-down menu at the top of the screen.
2. Click [image settings] from the menu on the left.
3. Click [upload image].
4. Enter a name and storage container
5. Specify the qcow2 file in “Upload a file” and click [Save].
6. Once the upload is complete, go to “Virtual Machines” from the drop-down menu at the top of the screen.
7. Click [Create Virtual Machine].
8. Enter the VM name and resource you want to allocate.
9. Click [Add new Disk].
10. Select [Clone from Image Service] from the Operation dropdown menu.
11. Select the image you created from the Image dropdown and add it.
12. Click [Add new Disk” again].
13. Set the size to at least 50GB and add it.
14. Add a NIC by clicking [Add New NIC].
15. Click [Save].

This completes the Nutanix deployment.

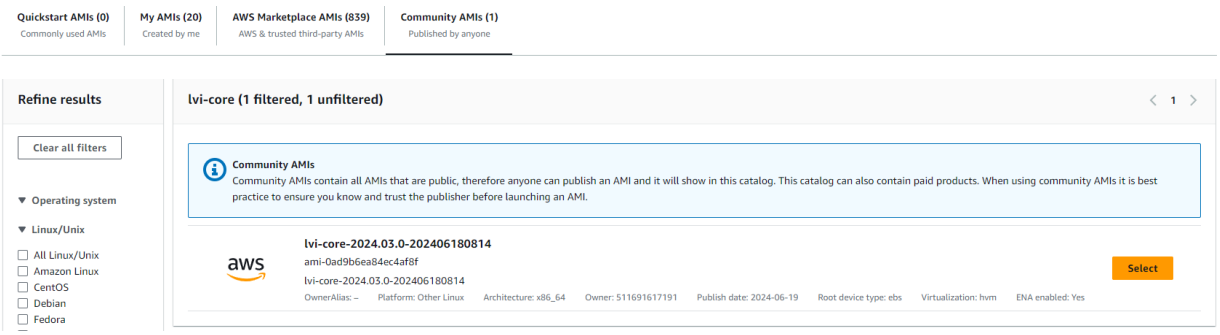
2.5 Deploy to Microsoft Azure

1. Log into Azure and go to the “Storage Accounts” service.
2. Click an existing storage account or click [Create] to create a storage account.
3. In the storage account menu, click [Data Storage] > [containers].
4. Click on an existing container or create a container from [containers].
5. Click [upload].
6. Select the VHD file you downloaded.
7. Open [Advanced settings] and change the Blob type to “Page blob”.
8. Click [Upload].
9. Once the upload is complete, go to the “disk” service.
10. Click [Create].
11. Select your subscription resource group and region.
12. Enter the disk name.
13. Change the source type to “Storage Blob” and select the file where you uploaded the source blob.
14. Change the OS type to “linux”
15. In the size section, click [change size].
16. Select the “storage type” that suits your environment (SSD is recommended).
17. Select the top 4GB and click [OK].
18. Click [Review and create].
19. Check the details and click [Create].
20. Once creation is complete, click [Go to Resource].
21. Click [Create VM].
22. Enter the virtual machine name.
23. Select the resources you want to allocate to the virtual machine by size.
24. Go to the disks tab.
25. in the Data Disk section, click [Create and connect a new disk].
26. In the Size section, click [change size].
27. Select the “storage type” that suits your environment (SSD is recommended).
28. 64GB or larger and add a data disk.
29. Verify that the host cache is “read/write”.
30. Go to the [Network] tab and configure the network settings to suit your Azure environment.
31. Click [Review].
32. Check the details and click [Create].

This completes the deployment on Azure.

2.6 Deploying to AWS

1. Login to AWS EC2 and click [launch Instance].
2. Give it a name and optionally set tags.
3. Click [Browse more AMI at Application and OS images] .
4. Select “Community AMIs”, enter `lvi-core` in the search field, and perform a search



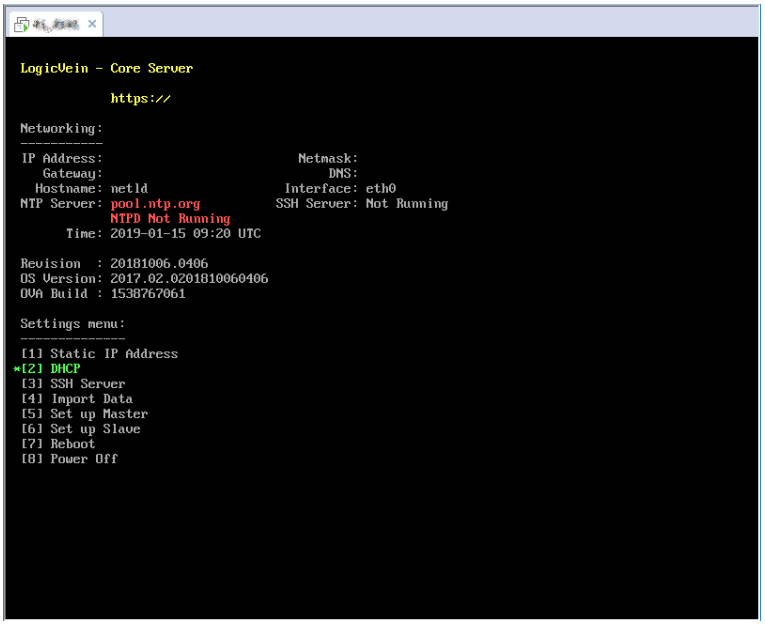
5. Select an instance type based on the sizing guidelines.
6. After creating a key pair in Key Pair (login), click [download key pair].
7. In the network settings, assign a group. You can choose an existing security group or create one. You can add a new security group.
8. [Under Configure Storage], click [add new volume] and set the size to at least 50GB.
9. Once configured, click [launch instance].

2.7 Configuring Network Settings

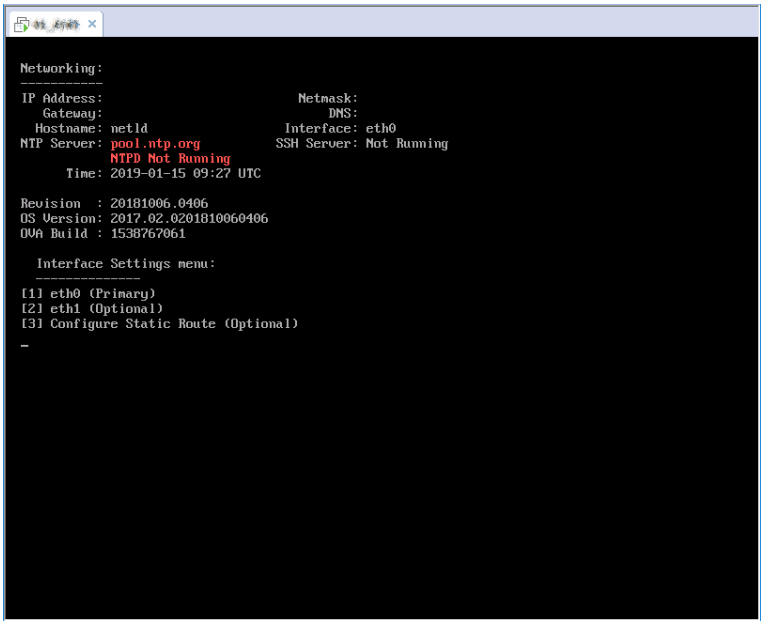
In the network settings, configure the host name and IP address to be given to ThirdEye. By default, the IP address etc. will be obtained from DHCP. In an environment without a DHCP server, perform various settings using the following steps.

Network settings are operated using the keyboard on the virtual machine console.

1. Press the [1] key on your keyboard to choose `Static IP Address`.



2. Press the [1] key on your keyboard to choose `eth0 (Primary)`.

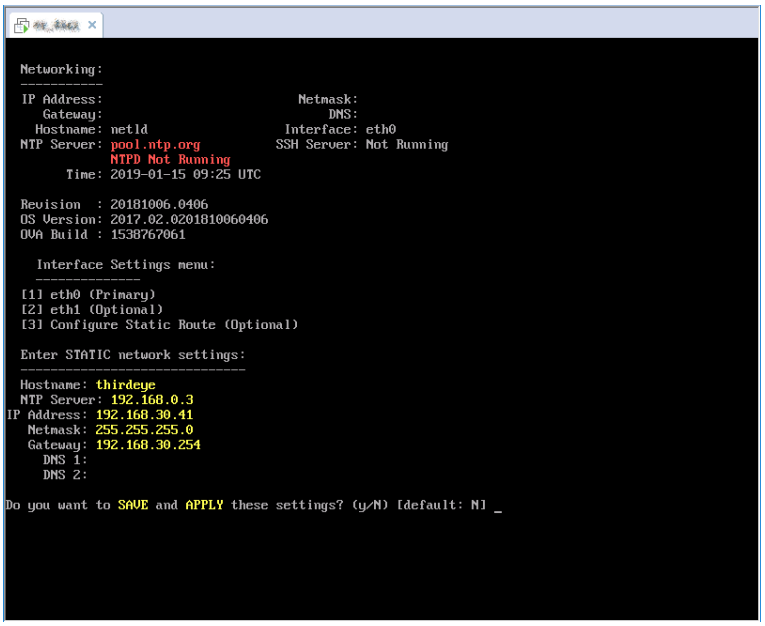


3. The following network setting items will be displayed in order.

Enter the value using the keyboard and press the [Enter] key to proceed.

Item	Explanation	Requirements
Hostname	Hostname used by the virtual appliance	required
NTP Server	Address of the NTP server used by the virtual appliance (IP address or hostname)	required
IP Address	IP address used by virtual appliance	required
Netmask	Subnet mask of the above IP address	required
Gateway	Gateway IP address	required
DNS 1/2	DNS server IP address	—

4. A confirmation message will be displayed. Press the [Y] key on your keyboard to save the settings.



Settings configuration is now complete, and the service will restart automatically.

2.8 Apply the license

Apply your license and activate your product.

1. Access ThirdEye by entering its address in your web browser:

`https://<Address>/`

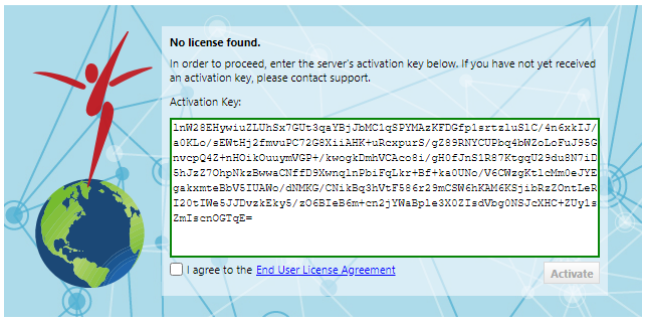
For `<Address>`, Specify the IP address or FQDN (Fully Qualified Domain Name).

The license authentication screen will be displayed.

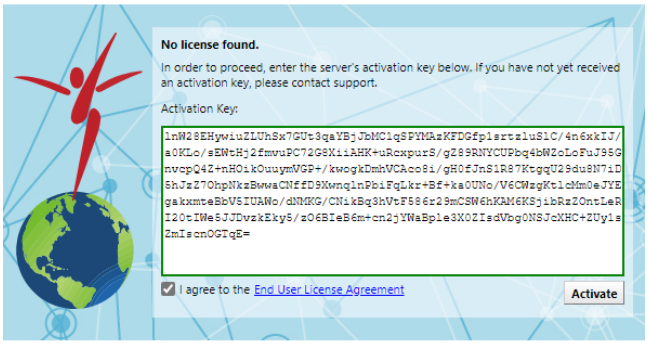
2. Copy and paste **Serial number** or **Activation key**.

If you **can** connect to the internet, use the **Serial number** (Number consisting of 25 alphanumeric characters).

If you **can't** connect to the internet, use the **Activation key**.



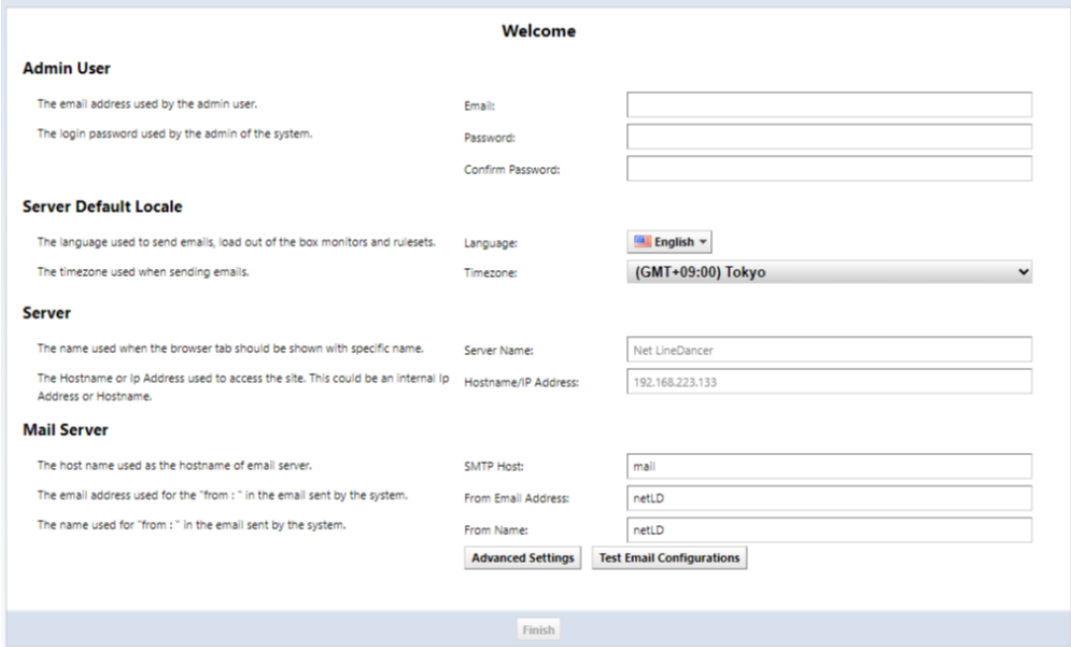
3. Check "I agree to the End User License Agreement", and click [Activate].



The service will restart automatically, and license application will be completed.

2.9 Initial settings (detailed settings)

After applying the license, the “Advanced Settings” screen will be displayed the first time you access it. On this screen, you can set the admin user’s password and mail server.



Setting	Explanation	Requirements
Admin User Settings	Admin user email address	—
	Admin user login password	required
Locale Settings	Language when sending email	—
	Time zone when sending email	—
Server Settings	Browser tab display name	—
	Host name or IP address used for link addresses in emails	—
Email Settings	SMTP server host name or IP address	—
	Email address when sending email	—
	Sender name when sending email	—

Note

To set a password, the following conditions must be met:

- Must be at least 8 characters
- Must not be a character string that is easy to guess (person’s name, proper noun, dictionary word, commonly used password)
- Character strings that do not repeat the same characters or are arranged in an easy-to-understand manner

After setting, click [Save] and proceed to the login screen.

3 Login/Logout

To log in/log out, please follow the steps below.

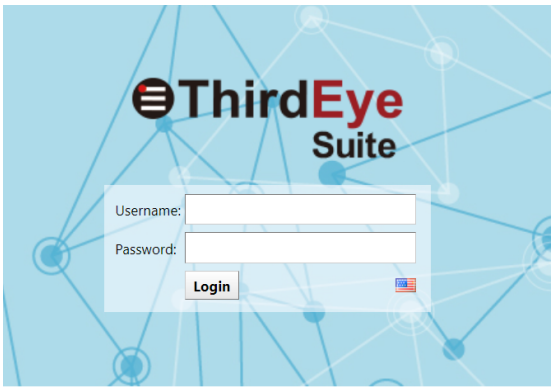
3.1 Log in

1. Access ThirdEye by entering its address in your web browser:

https://`Address`/

For `Address`, specify the IP address or FQDN (Fully Qualified Domain Name).

2. On the login screen, enter your username and password to log in.

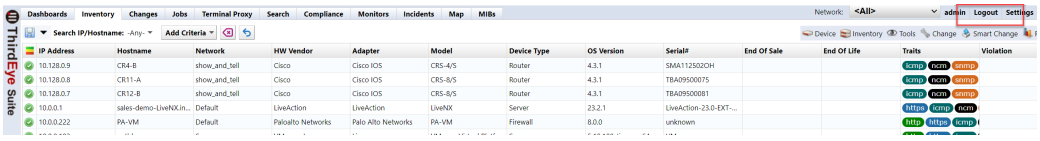


For a new installation, refer to the section **Installation > Initial settings (detailed settings)** to set the password for the admin user.

After logging in, the ThirdEye top screen will be displayed.

3.2 Log out

1. Click [Logout] at the top right of the screen.



After logging out, the ThirdEye login screen will be displayed.

4 HA (Active/Standby)

{{ProductName}} has supported HA feature (Active/Standby) since r20241218.0941. In this feature, we use active and standby as a role. For active server, ThirEye manages devices or monitor devices. For standby server, it receives transaction log (WAL) from active server and perform synchronization by recovering it. For HA configuration, we say primary server as active server. In case of attached file, it will be synchronized per 120 seconds with standby server.

4.1 Prerequisites

The HA feature uses eth1 to synchronize data because SSH is used, if there is a firewall between the active and standby servers, SSH communication from the standby server to the active server must be allowed. Also, the number of CPU cores, memory capacity, and disk size on both servers must be identical.

4.2 Restrictions

HA features have the following limitations. Please note that these features are not supported.

- Simultaneous use with Smart Bridge
- Using such as AWS and Azure in cloud environments
- Taking over Syslog data received on the active server
- Taking over system backup files obtained on the active server
- Taking over the settings to be configured in the OVA console

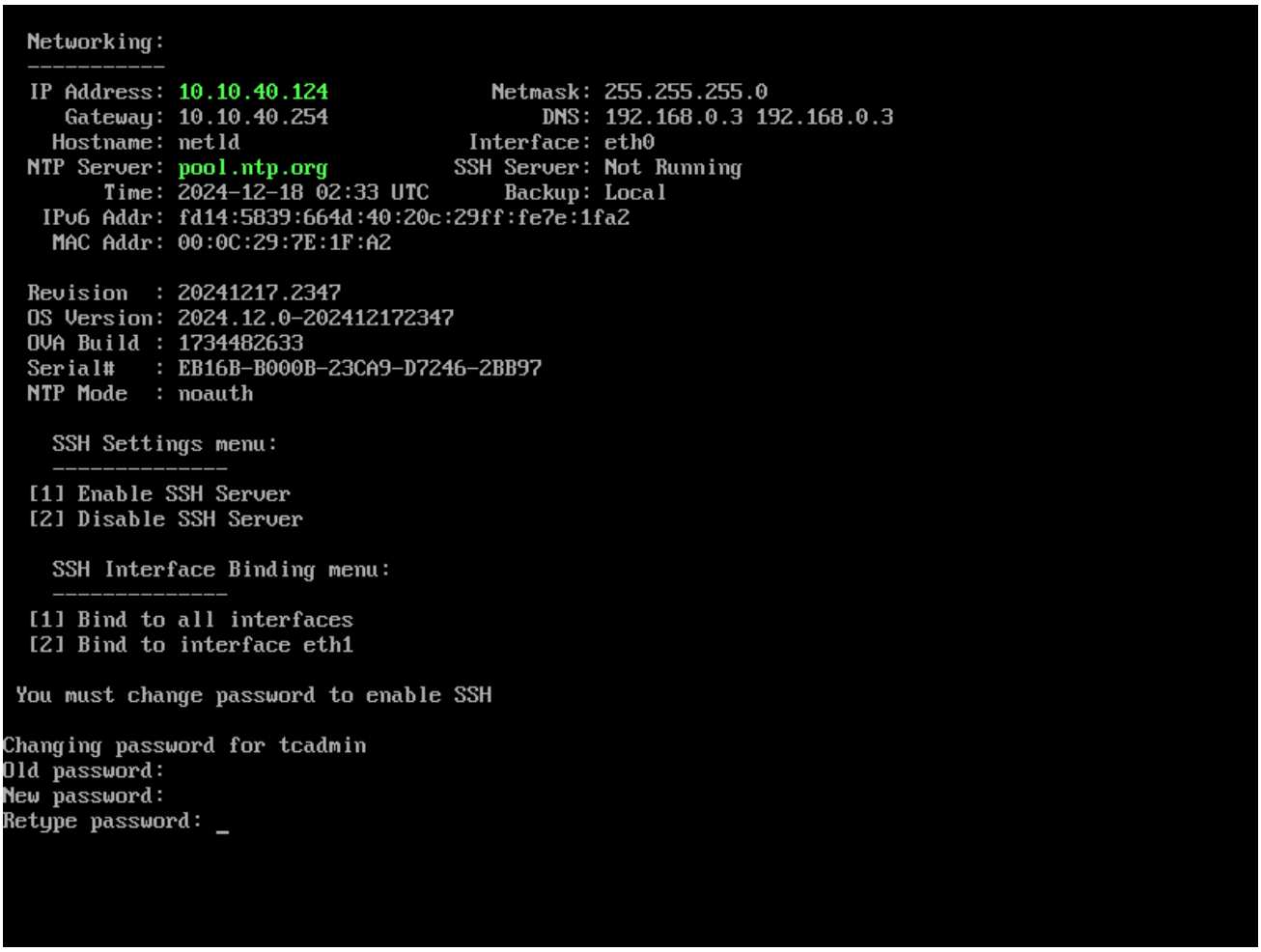
4.3 Settings

HA configuration is configured by using the OVA setting. To implement this configuration, user must have permission to operate VMware and Windows Hyper-V.

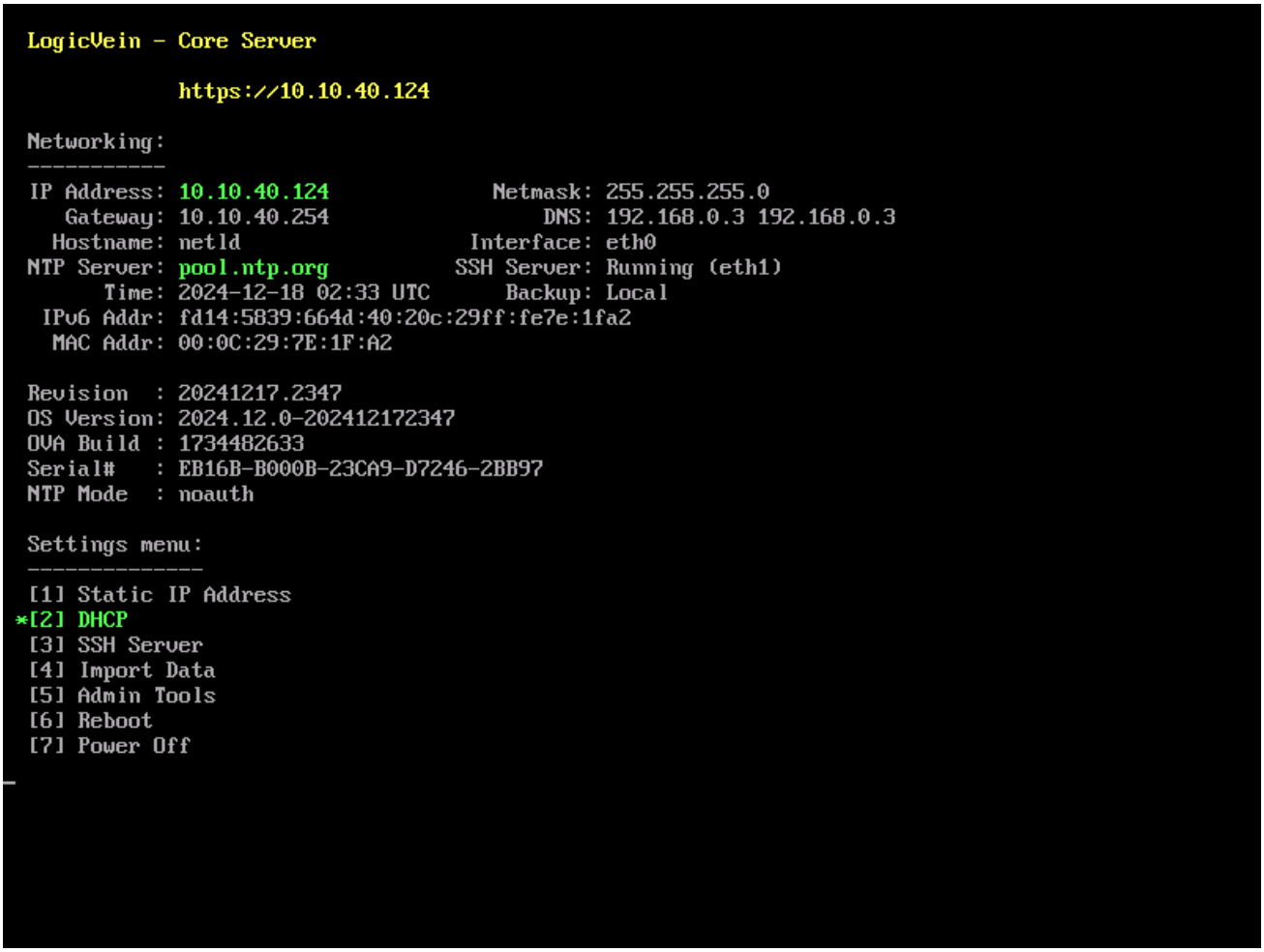
4.4 Procedure

Before configuring, set IP addresses on the eth1 interfaces of the primary and standby server so that communication is possible between eth1.

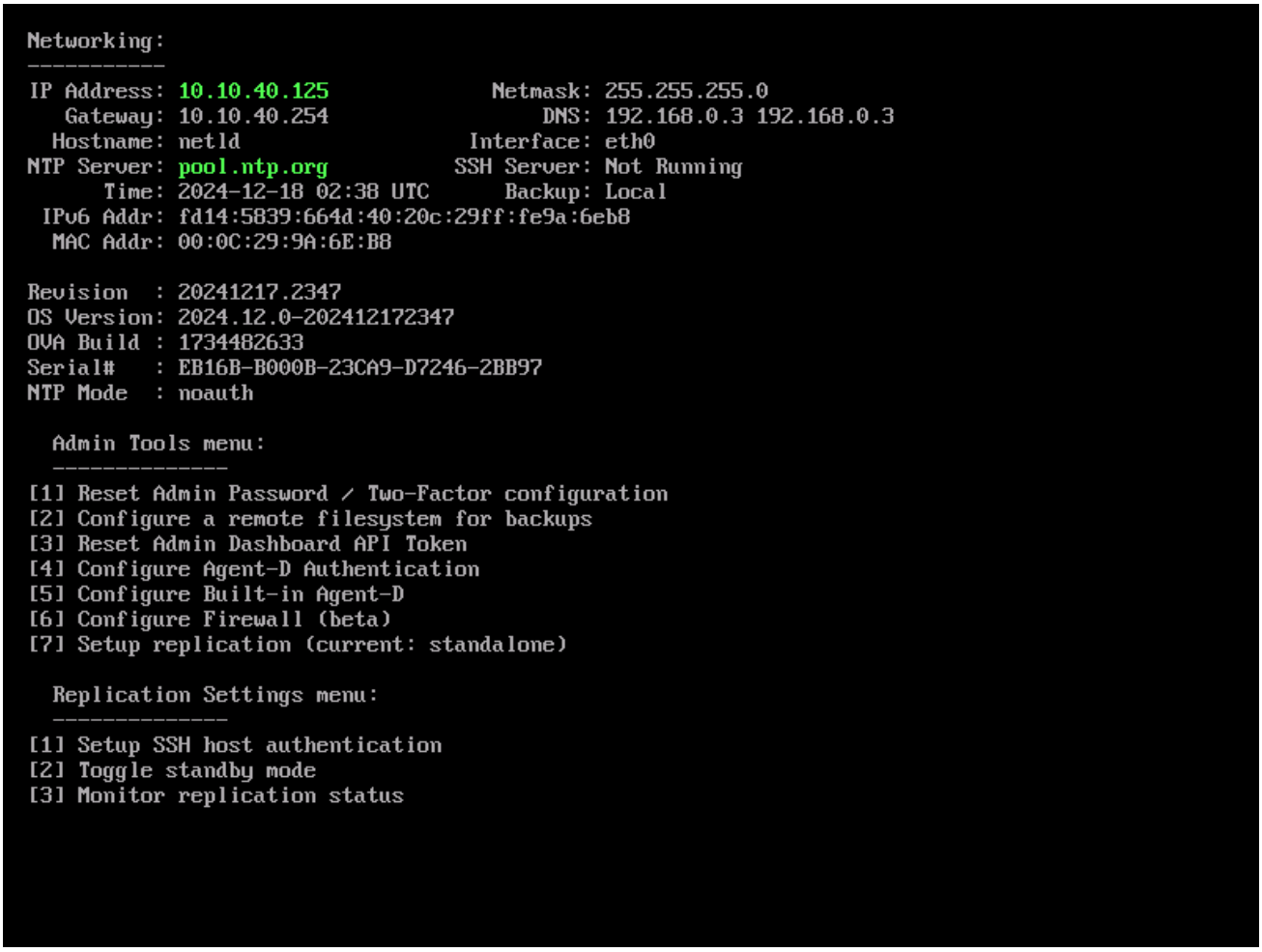
1. Connect to the OVA console on the primary server.
2. Enable SSH for eth1 by pressing [3] (SSH Server) > [1] (Enable SSH Server) > [2] (Bind to interface eth1) on the keyboard.



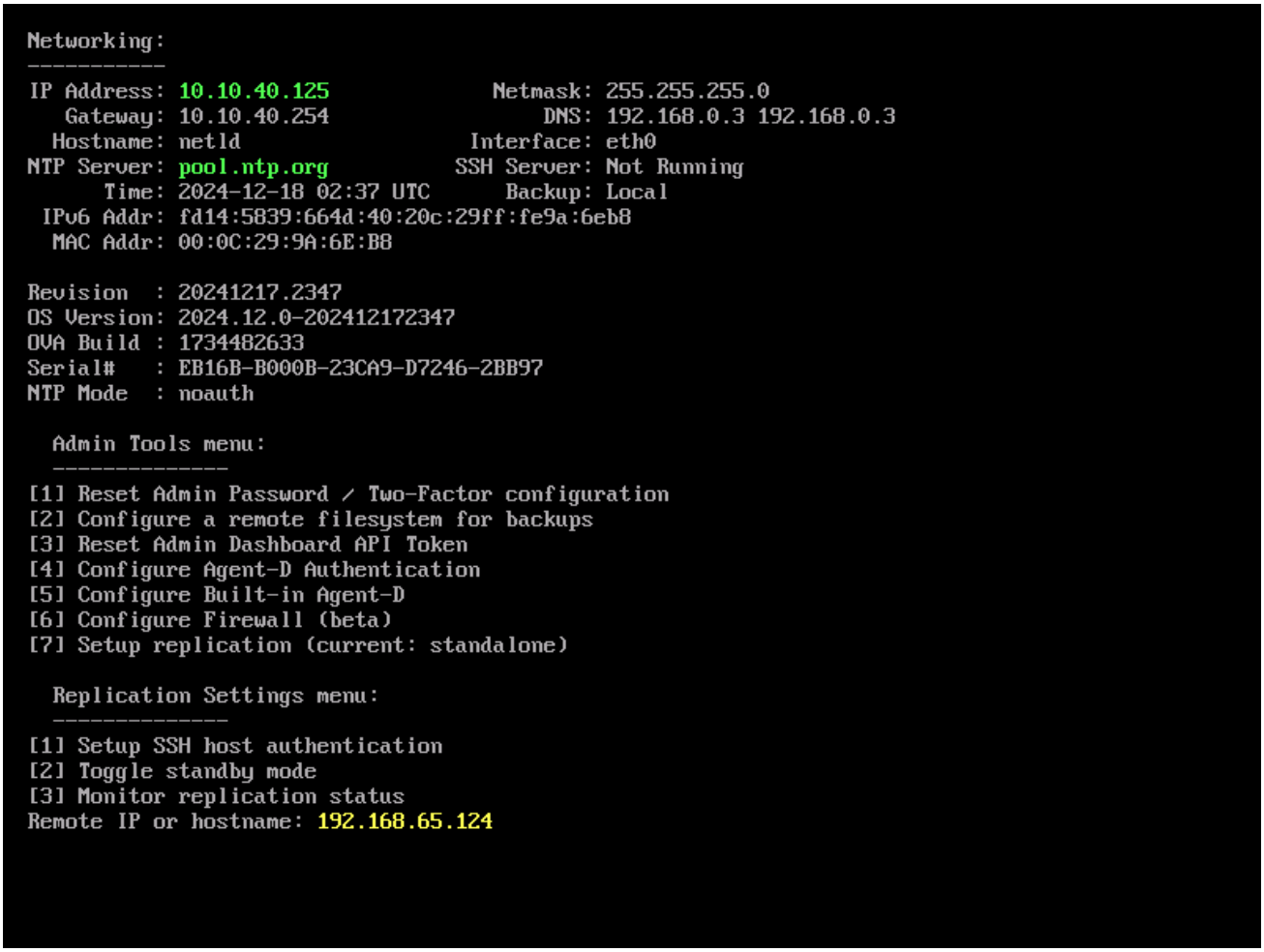
3. Confirm that the SSH Server is Running.



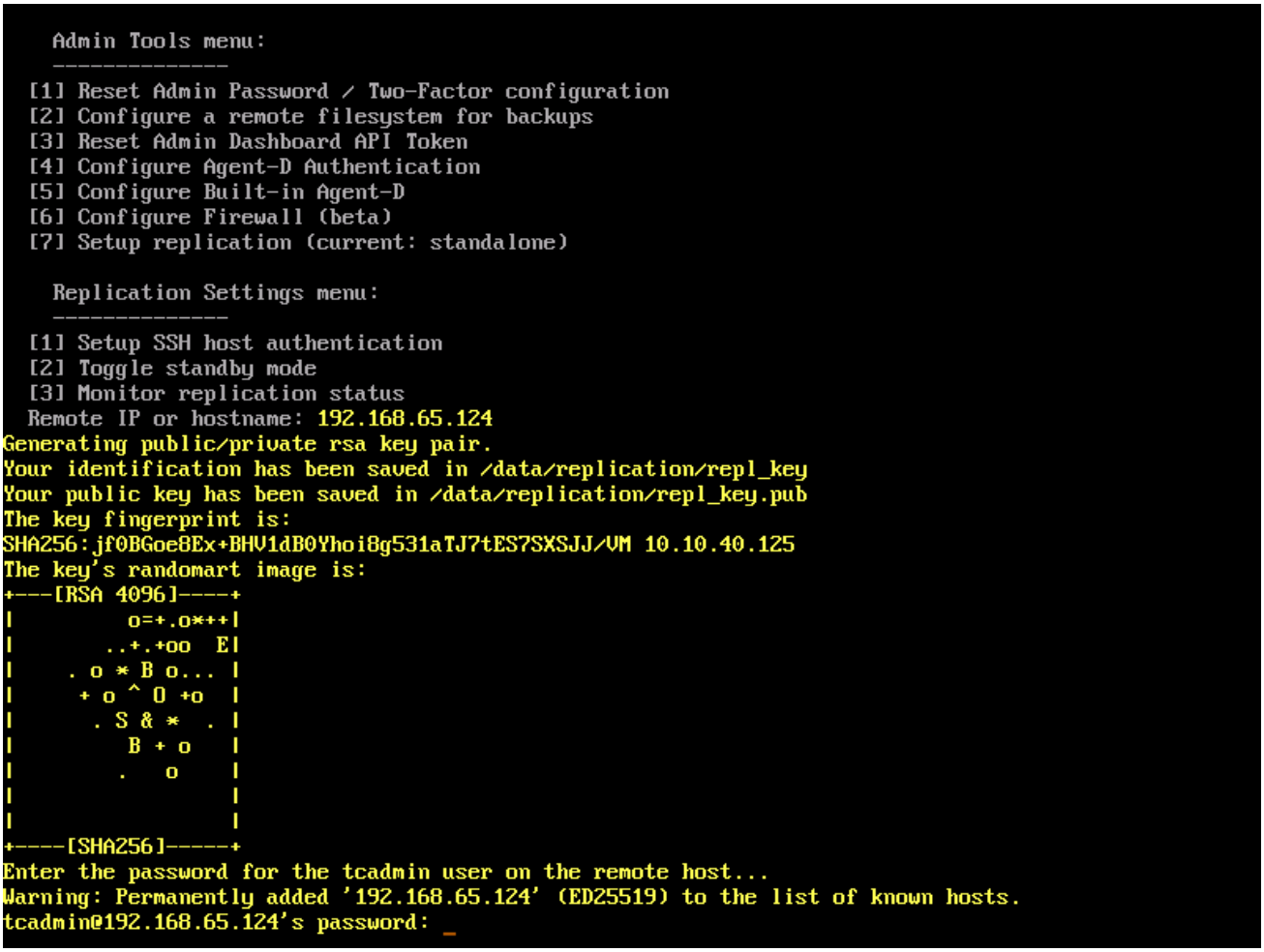
4. Connect to the OVA console of the standby server.
5. Press [5] (Admin Tools) > [7] (Setup replication) > [1] (Setup SSH host authentication) on the keyboard to configure SSH host authentication settings for the primary server.



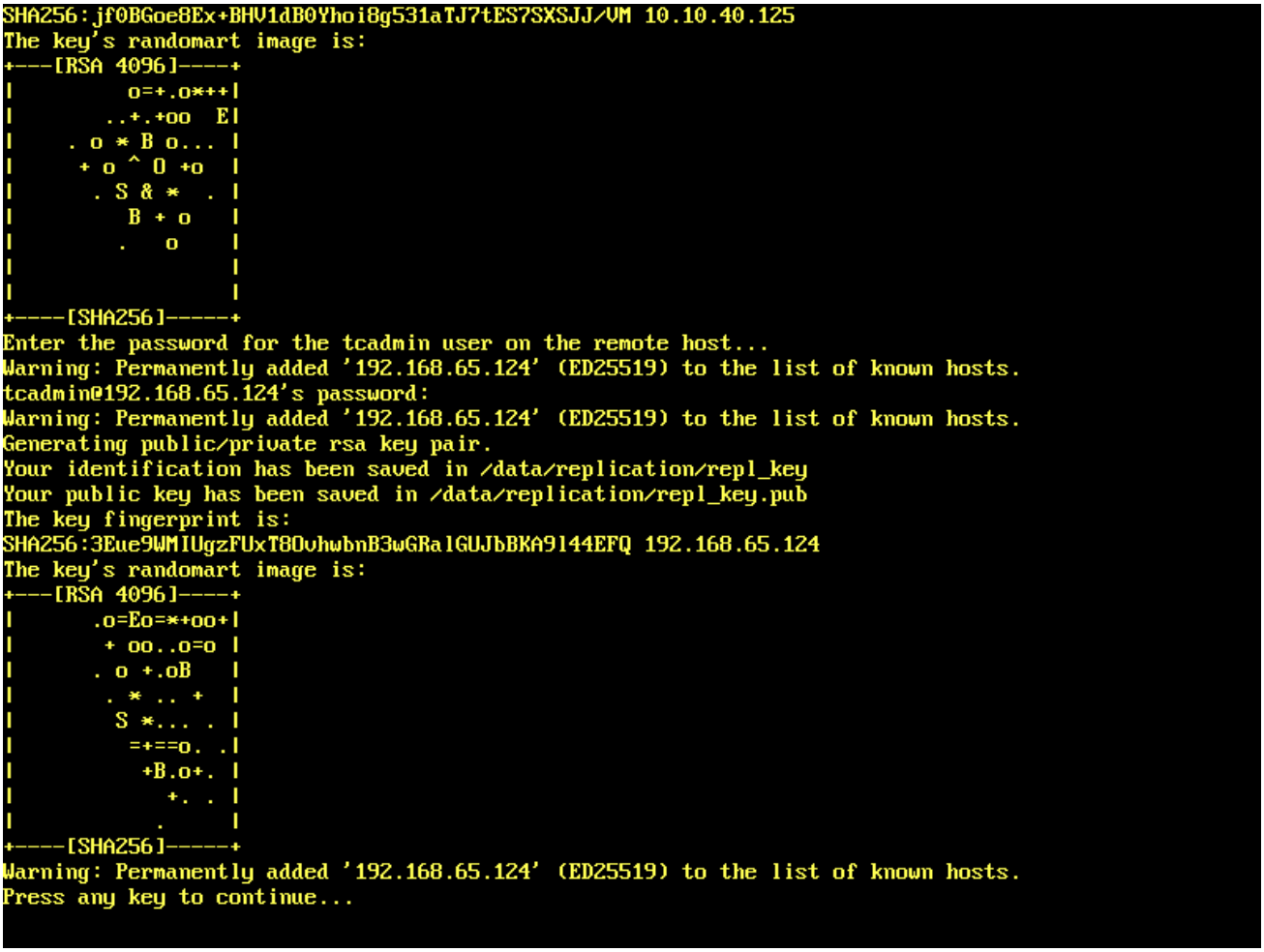
6. Enter the eth1 IP address of the primary server.



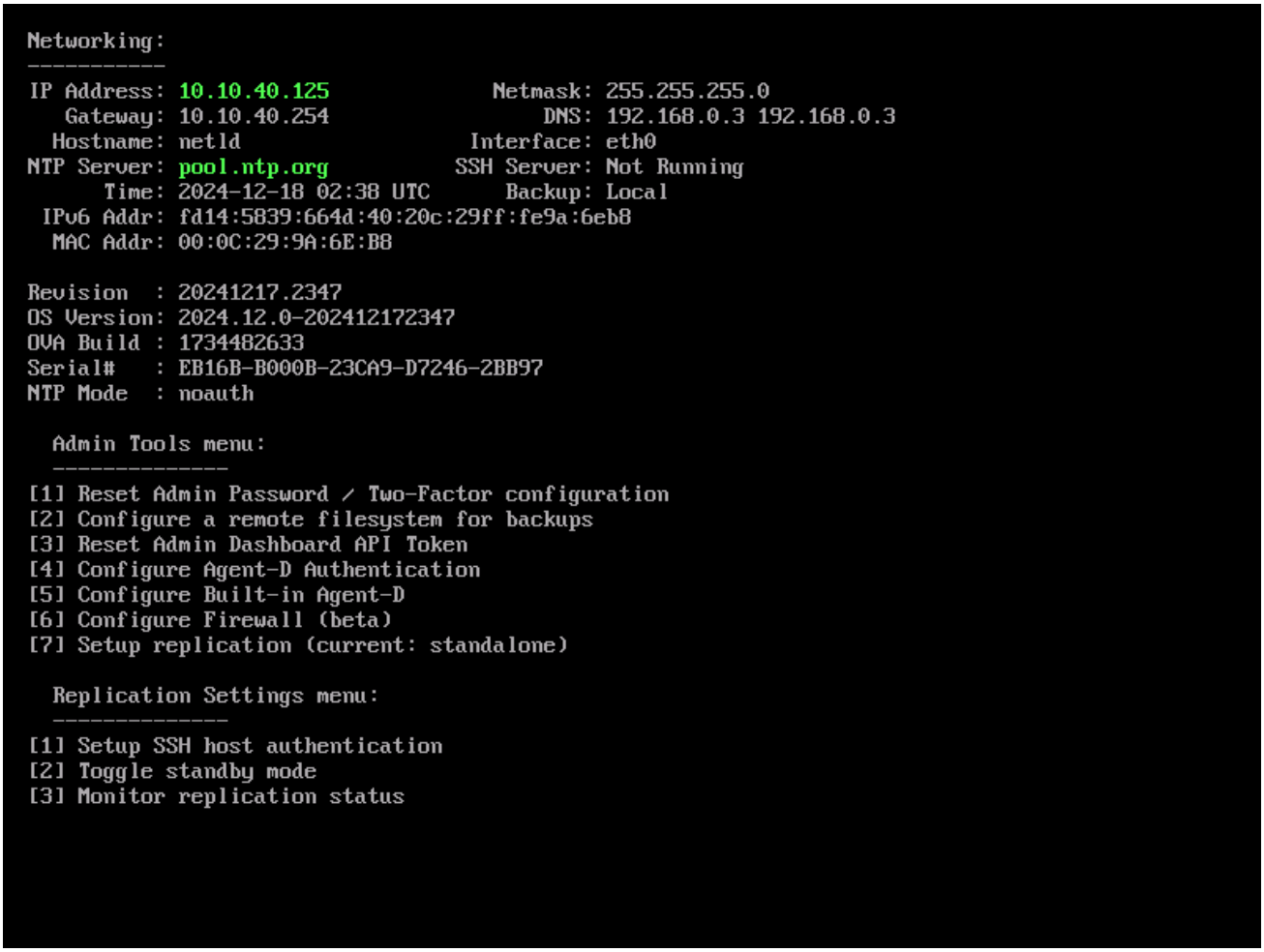
7. Enter the password for SSH to the primary server.



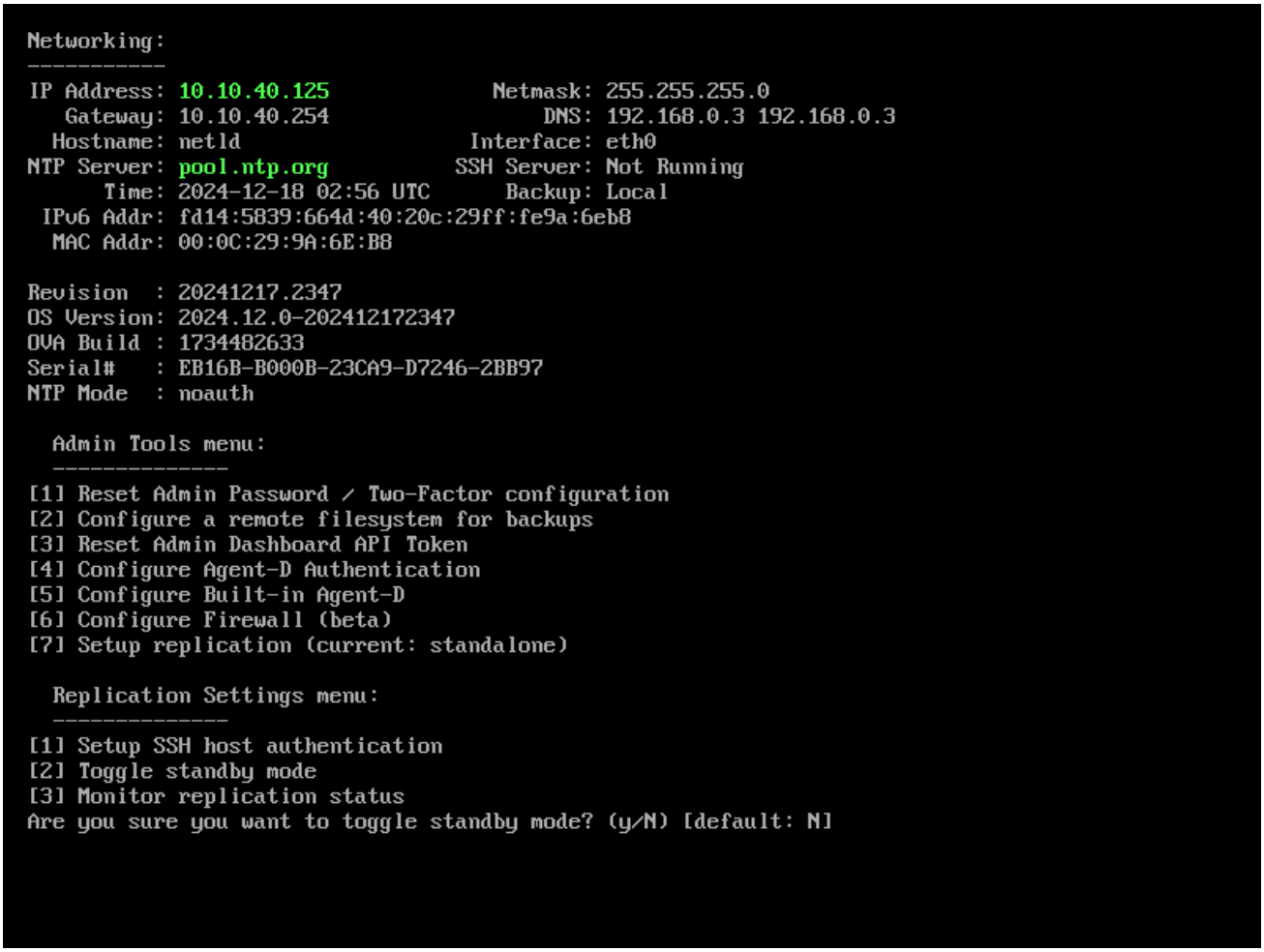
8. Press any key, such as the [Enter] key.



9. Press [5] (Admin Tools) > [7] (Setup replication) > [2] (Toggle standby mode) on the keyboard to change the standby server from active to standby server role.



10. Press [Y].

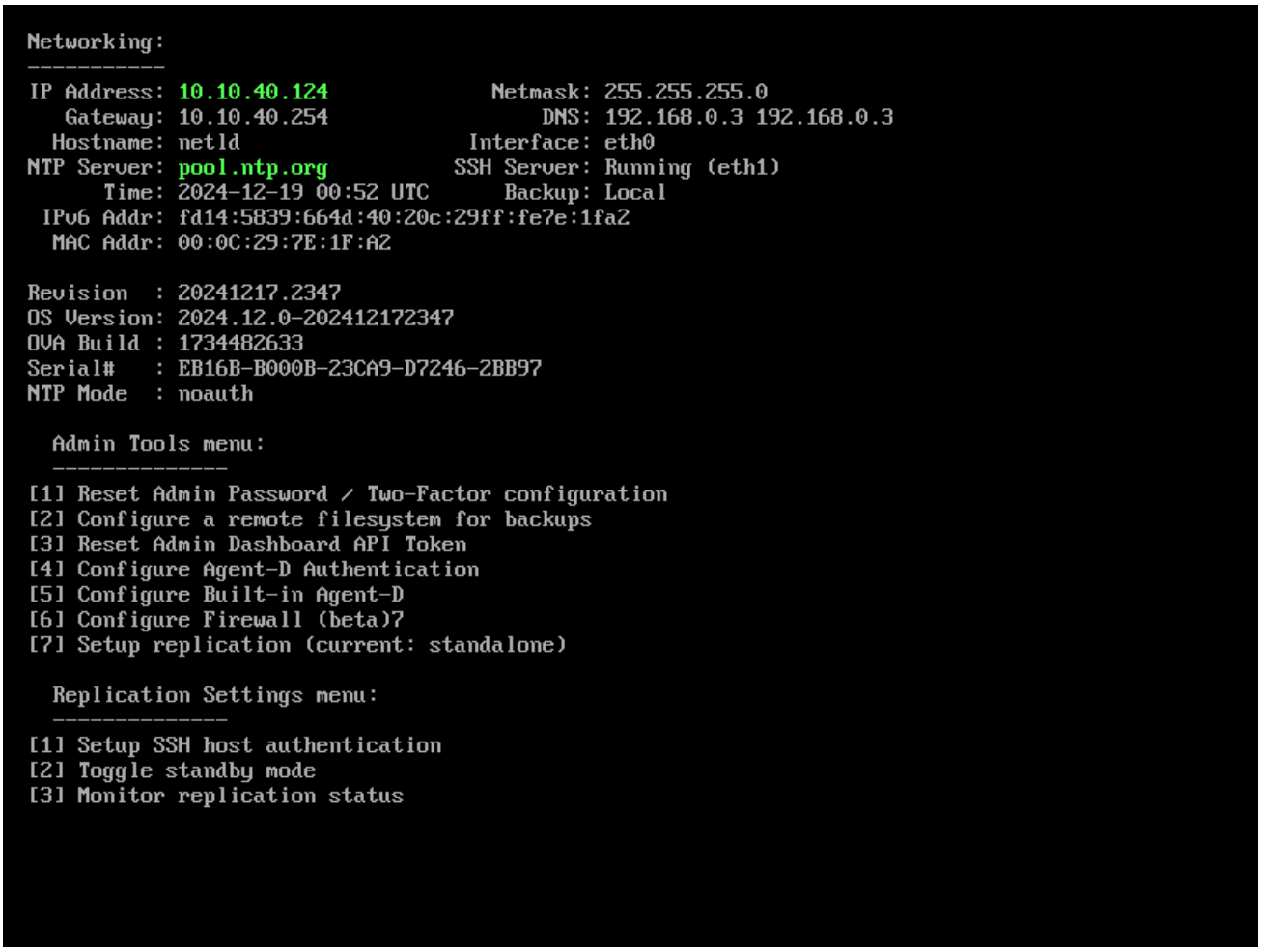


11. Press [Y] to automatically restart the standby server.

4.5 Confirm status

The status of HA feature can be checked from the OVA console screen.

1. Connect to the OVA console of the primary server.
2. Press [5] (Admin Tools) > [7] (Setup replication) > [3] (Monitor replication status) on the keyboard to check the status.

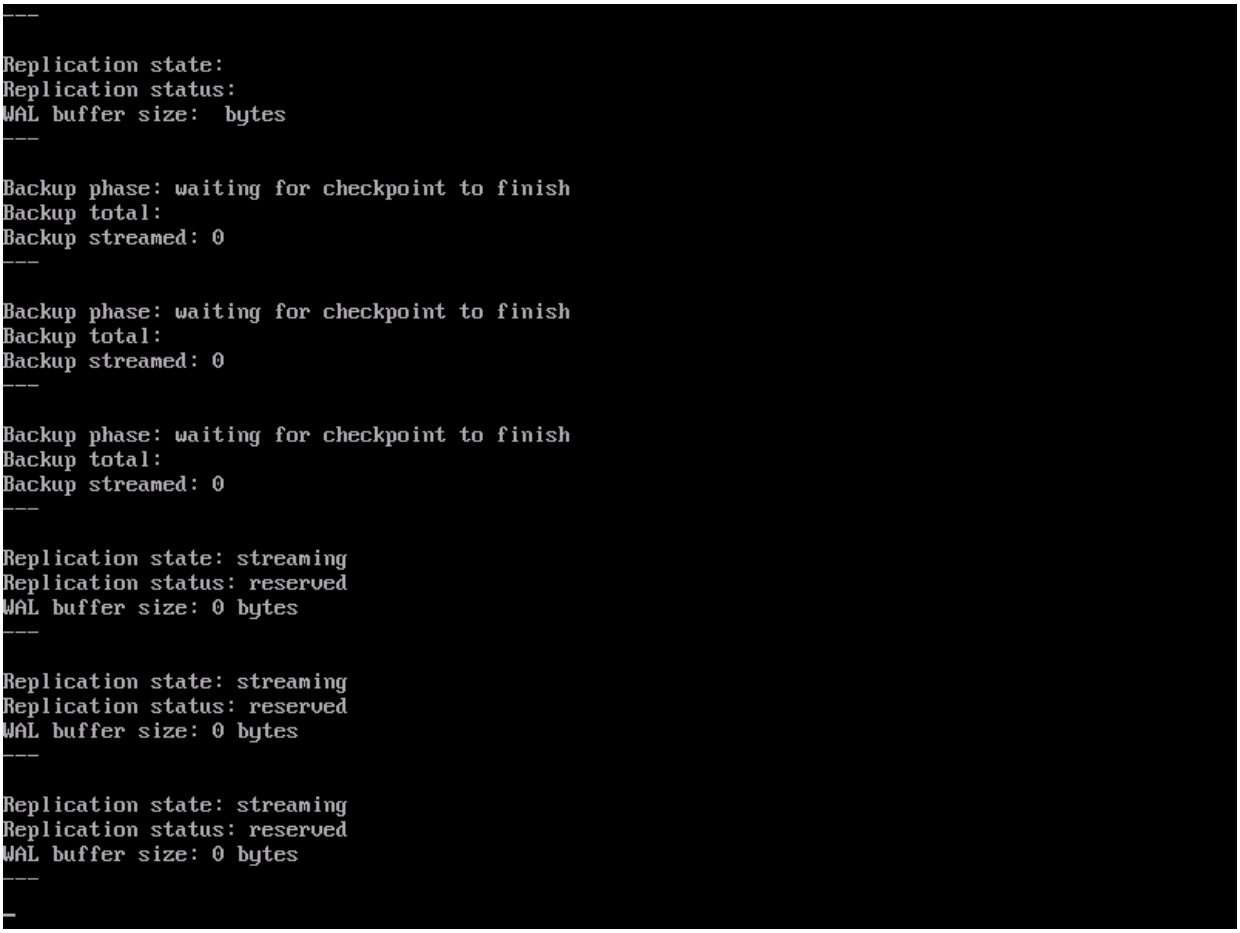


The status will be updated automatically when it is displayed. To close the status screen, press [Ctrl+C].

Once the HA configuration is set up, the backup phase is initiated first. During the backup phase, the initial data is copied from the primary server to the standby server.

```
---

Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
---

Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
---

Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
---

Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
---

Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
---

Backup phase: streaming database files
Backup total: 106565120
Backup streamed: 89051136
---

Replication state: streaming
Replication status: reserved
WAL buffer size: 0 bytes
---
```

Once the backup phase is complete, data streaming will begin. Once started, a screen similar to the one below will appear. After setting, confirm that “Replication state: streaming” is displayed.



4.6 Cases for Reconfiguration

In the following cases, the HA function must be configured again:

- When restoring a system backup on the primary server
- To restore the original state after failover.

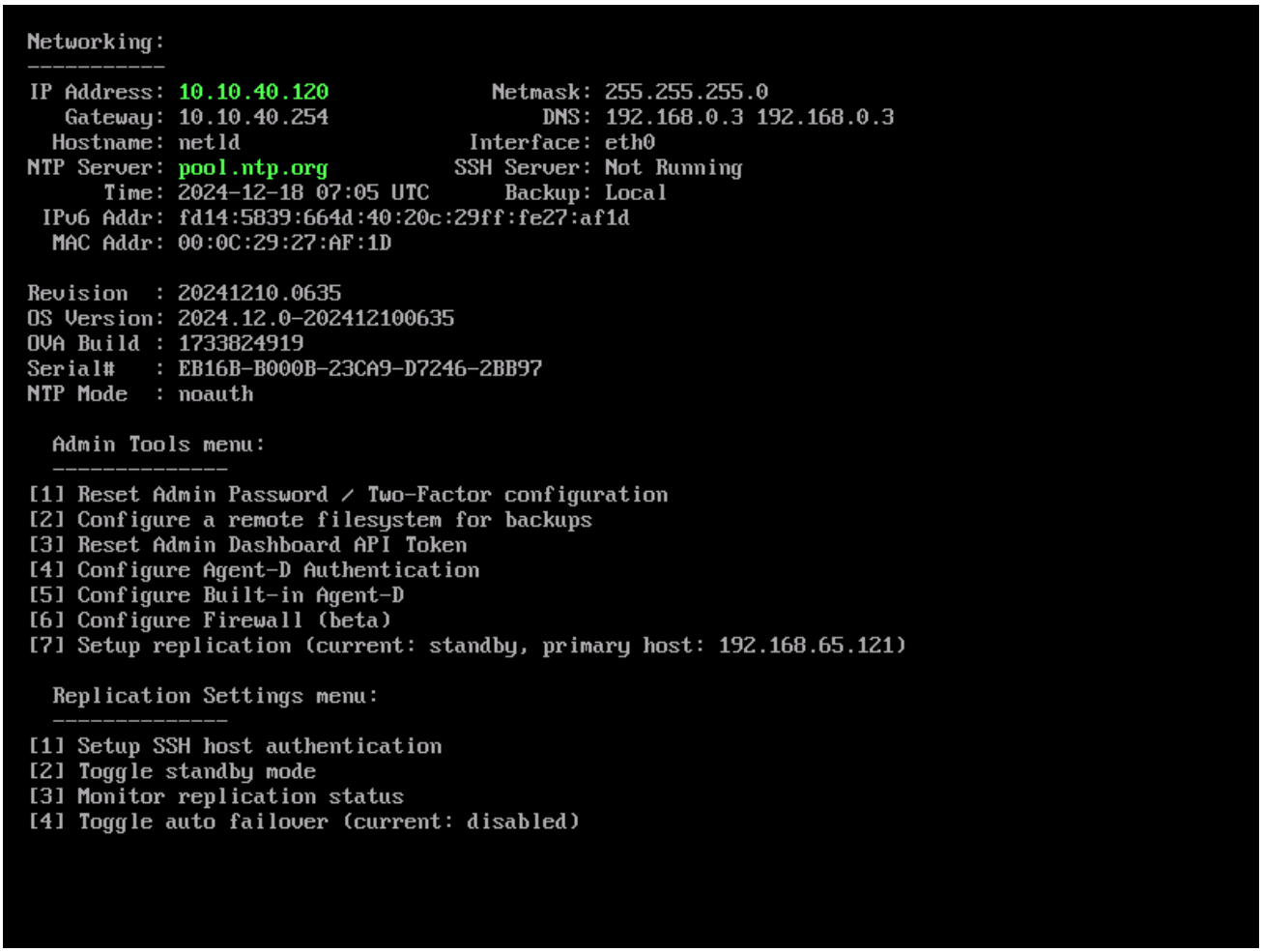
4.7 Failover

Failover refers to the process of automatically switching to a redundant or standby system when the primary system fails, ensuring minimal downtime and continuous operation.

4.7.1 Manual failover

To monitor on an active server, change the role from standby to active. The change procedure is as follows.

1. Connect to the OVA console of the standby server.
2. Press [5] (Admin Tools) > [7] (Setup replication) > [2] (Toggle standby mode) on the keyboard to change the standby server from standby to primary server role.



3. Press [Y].

Press [Y] to automatically restart the standby server. After restarting, please log in from a web browser.

4.7.2 Auto failover

When auto failover is enabled, the standby server will automatically change its role from standby to primary and take over monitoring if there is an unintended communication breakdown between the primary and standby servers for more than 60 seconds. If the user restarts/shuts down the primary server or successfully reconnects within 60 seconds, the switchover does not take place.

By default, auto failover is disabled. To have the standby server automatically take over monitoring if the primary server fails, follow these steps to enable auto failover.

1. Connect to the OVA console of the standby server.
2. Press [5] (Admin Tools) > [7] (Setup replication) > [4] (Toggle auto failover) on the keyboard to enable auto failover.

3. After pressing [4] , the screen will automatically return to the first screen. Again, go to [5] (Admin Tools) > [7] (Setup replication) and confirm that the Toggle auto failover current is “enabled”.

5 Smart Bridges (Optional)

{{ProductName}} supports two modes for the connection of Smart Bridges to the core server:

- **Bridge-to-Server**
- **Server-to-Bridge**

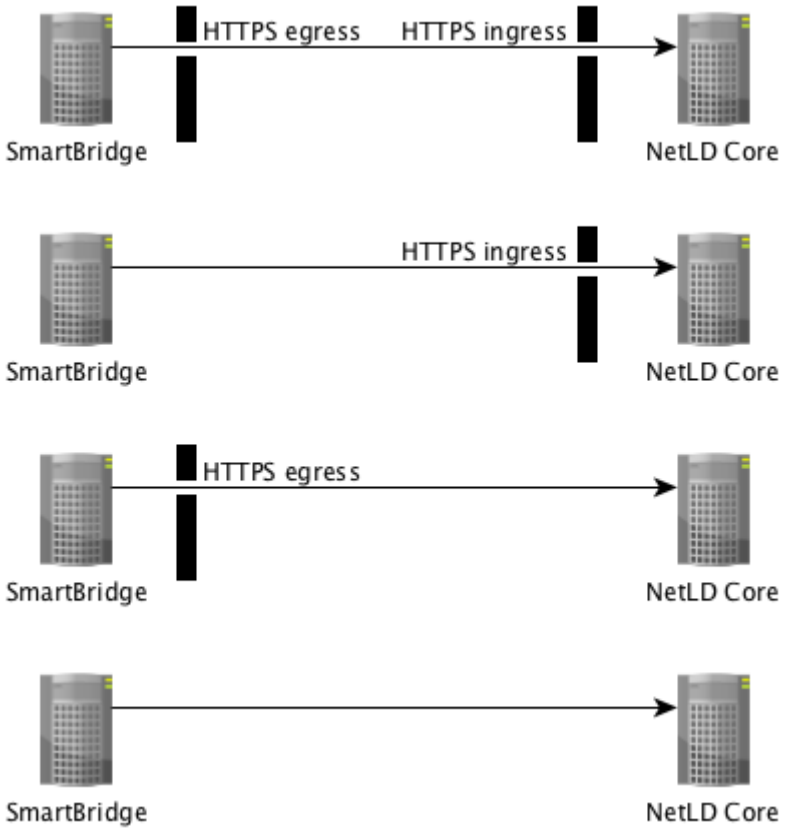
All connections are via HTTPS, so wire traffic is encrypted end-to-end.

5.1 Bridge-to-Server

This is the new default connection mode. In this mode, the SmartBridge will initiate contact with the core server; the core server will never initiate connections to the SmartBridge. The SmartBridge is commonly running in a remote network, sometimes over public infrastructure, and often behind a firewall. Corporate security groups are hesitant to open holes in the corporate firewall for in-bound connections, and rightfully so.

The Bridge-to-Server connection mode removes the necessity for the creation of a hole in the firewall in the SmartBridge network, as long as the firewall allows *egress* (out-bound) HTTPS traffic. No involvement by firewall administrators is required.

The following diagram shows various scenarios in which firewalls are present in one network, in both networks, or absent.

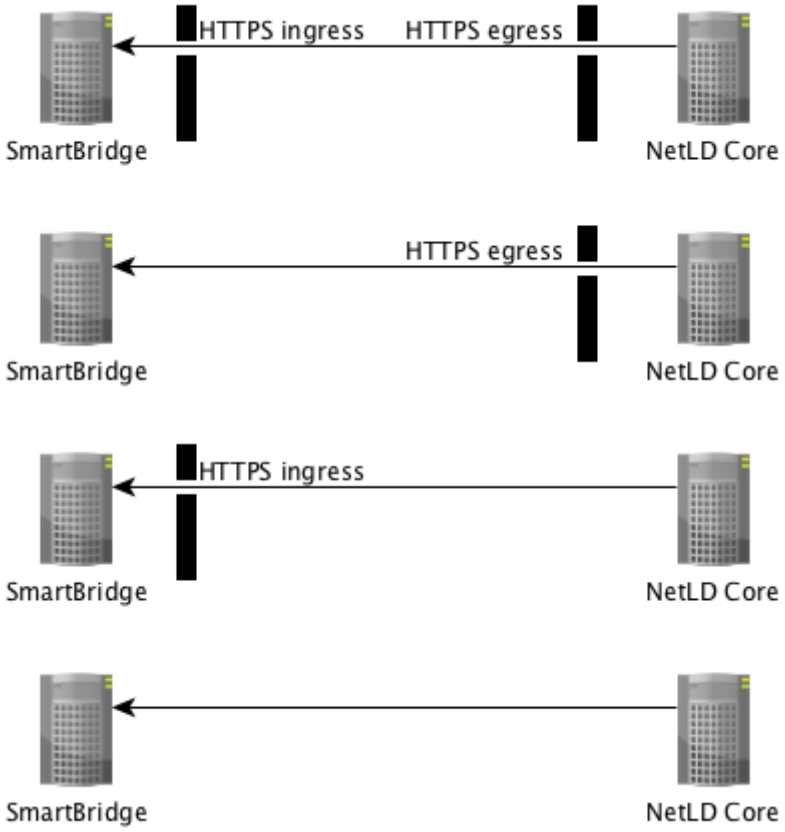


5.2 Server-to-Bridge

This connection mode is *primarily* useful for internal networks (LAN/WAN) in which there are no intervening firewalls between the core server and the SmartBridge. In this mode, the core server will initiate contact with the SmartBridge; the SmartBridge will never initiate connections to the core server.

If the there is a firewall between the SmartBridge and the core server, then a hole must be punched in the firewall to allow *ingress* (in-bound) HTTPS connection initiation from the core server.

The following diagram shows various scenarios in which firewalls are present in one network, in both networks, or absent.



5.3 Connection Token

LogicVein introduces the concept of a *Connection Token*. A unique token is generated for a SmartBridge at the time that the SmartBridge is first configured on the core server.

If a SmartBridge is configured to use **Bridge-to-Server** mode, then the core server will not accept an in-bound connection from a SmartBridge unless it first presents its unique token. This prevents random or malicious connections to the core server.

If SmartBridge is configured to use **Server-to-Bridge** mode, users can choose not to use Tokens. However, we recomend using Connection Tokens for security reasons.

5.4 SmartBridge Installation

The installation of SmartBridge is almost identical to the installation of the Core Server, the only difference being the files used for the installation.

Example:

Core server file name: `lvi-core-2024.03.0-202406180814-appliance.ova`

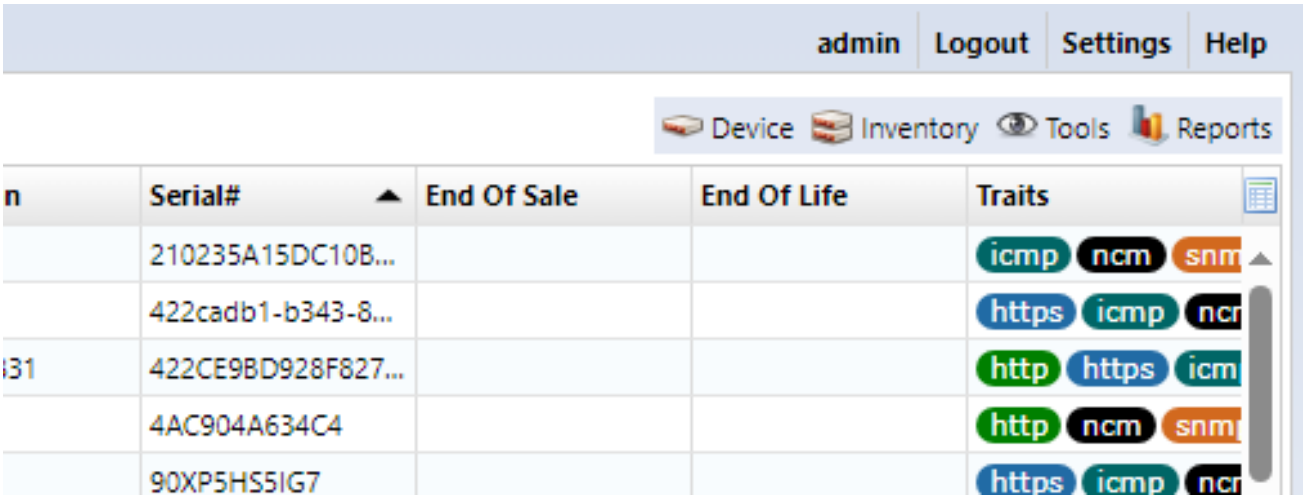
Smart bridge file name: `lvi-bridge-2024.03.0-202406180814-appliance.ova`

After installation, you can configure the network by referring to the **Installation** > **Configuring Network Settings** section.

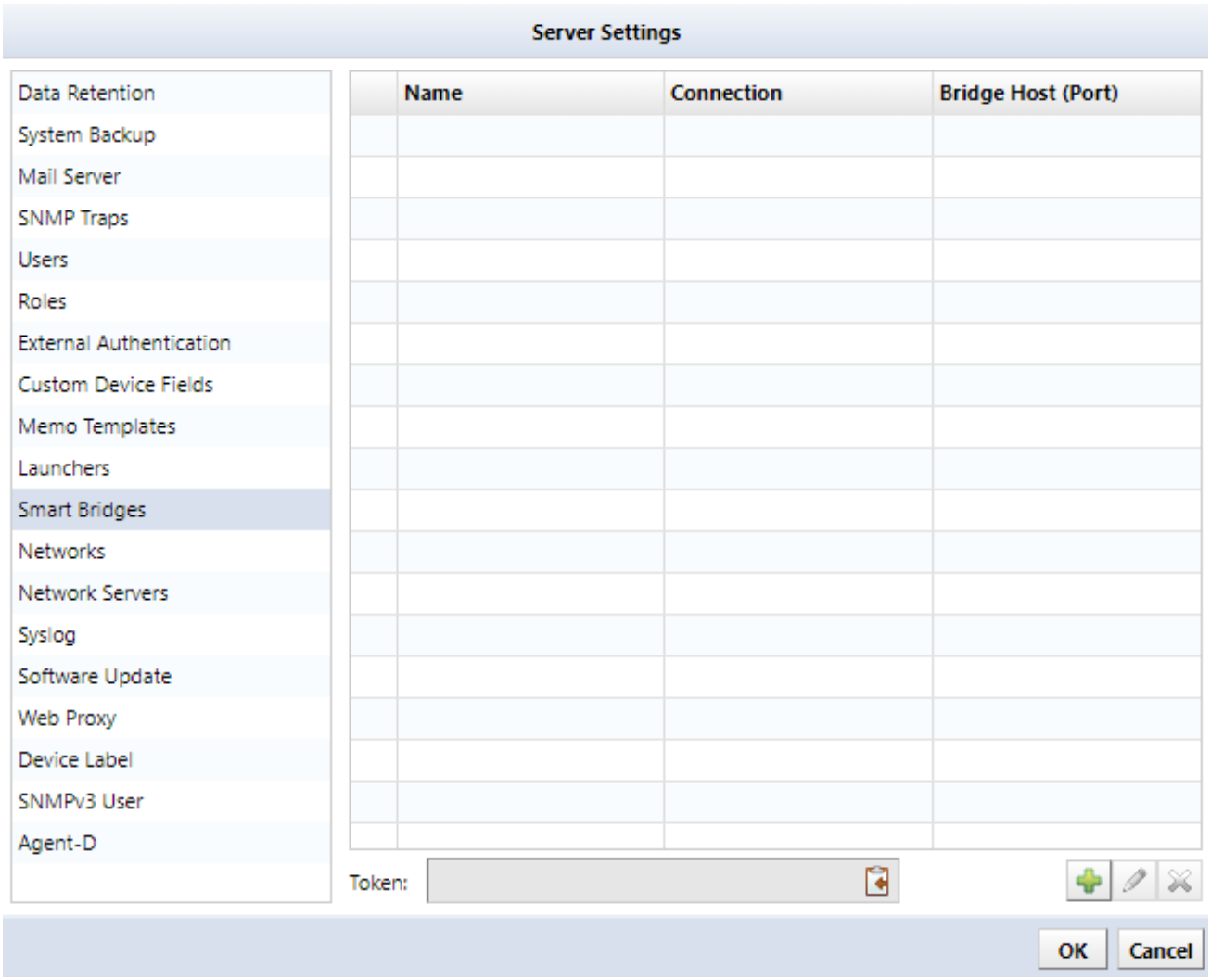
5.5 Add SmartBridge to core server

Register SmartBridge on the core server. After registering SmartBridge, a token will be automatically generated.

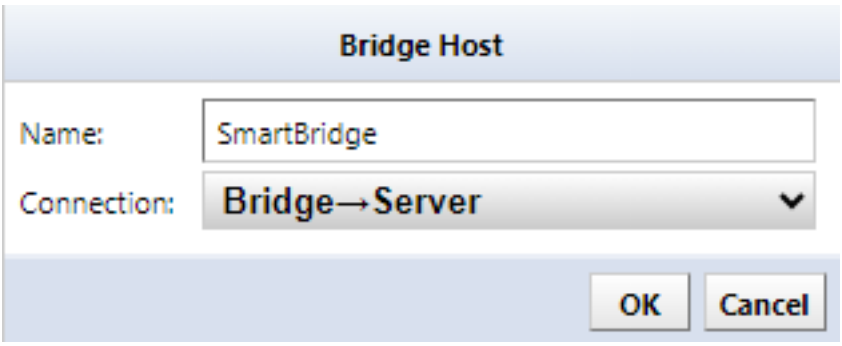
1. Login to the core server as an Administrator and click [Settings] in the Global Menu.



2. Select the [Smart Bridges] category in the left sidebar of the [Server Settings] window, and click the button to add a new Smart Bridge.

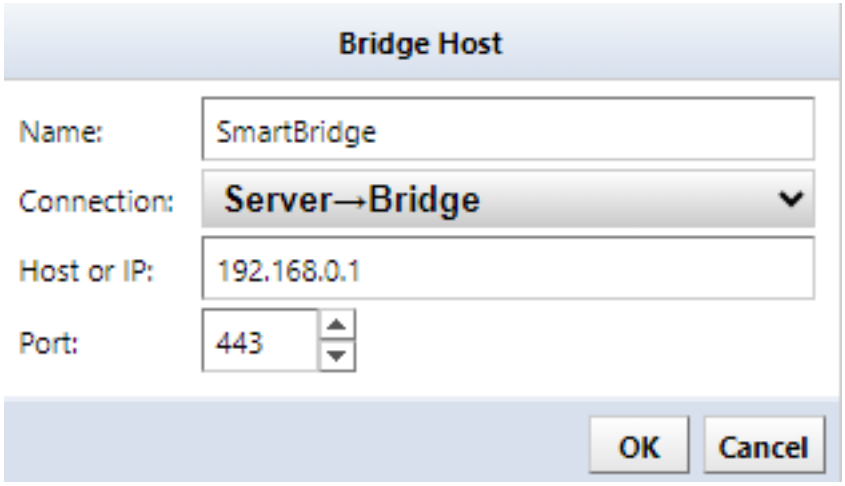


3. Enter the name for the Smart Bridge



4. Click [Connection].

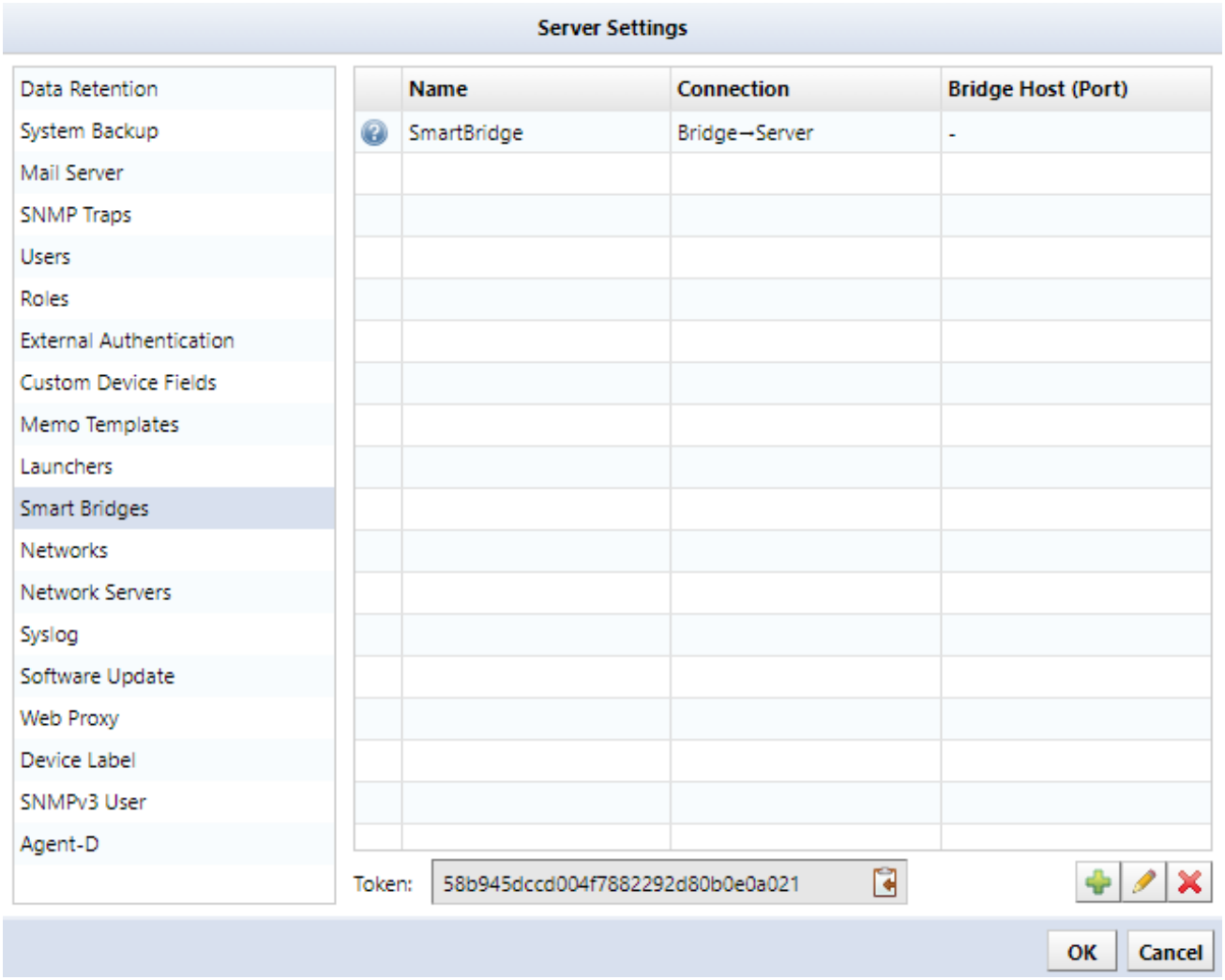
When you select [Server to Bridge], you have to enter a “Host or IP” address and “Port” for the bridge.



5. Click [OK].

6. Copy token.

The new Smart Bridge will appear in the table, and below the table you will find the Connection Token.



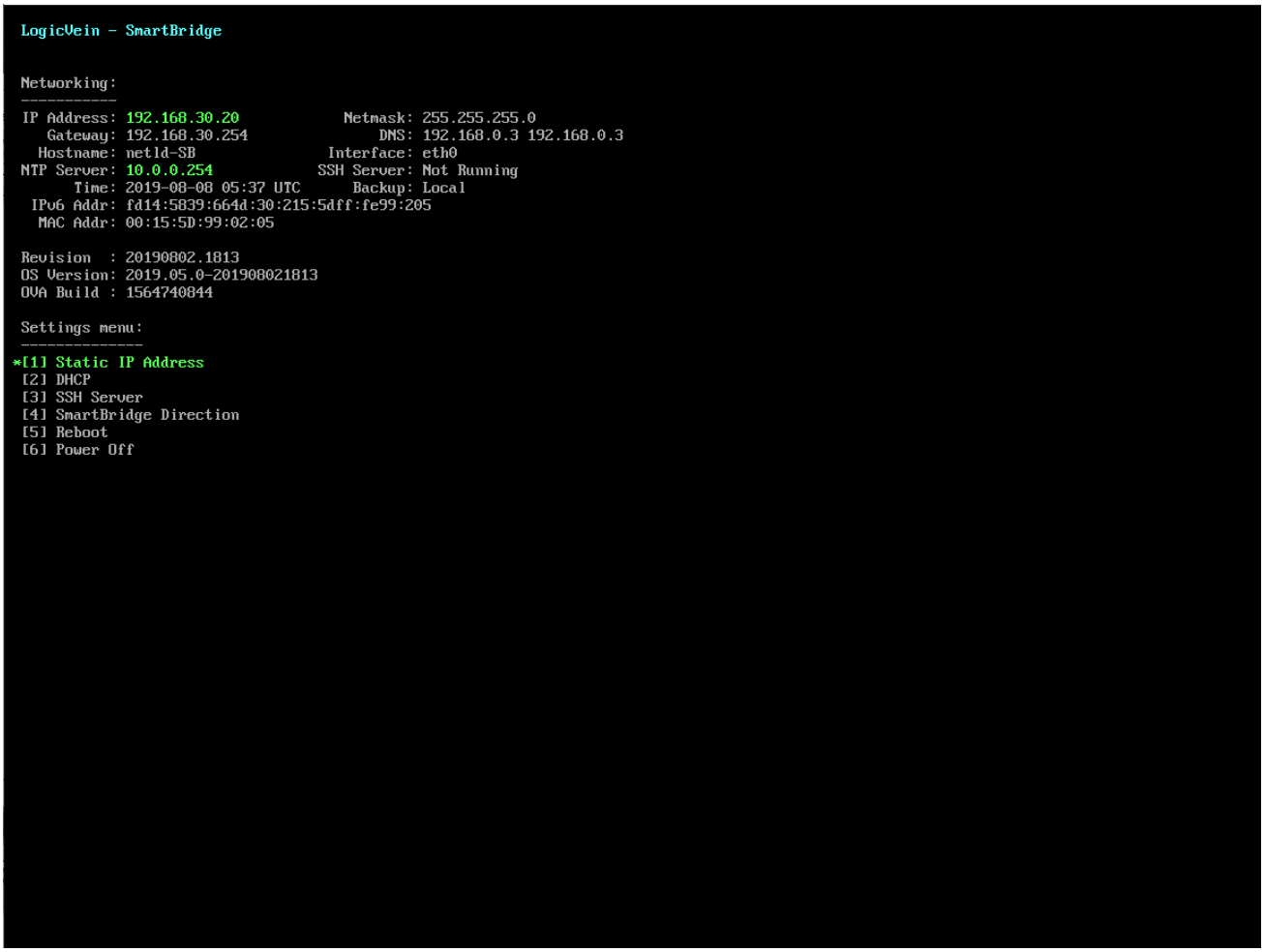
7. Click [OK].

Now that SmartBridge is registered with the core server, you need to provide the core server information and token to SmartBridge.

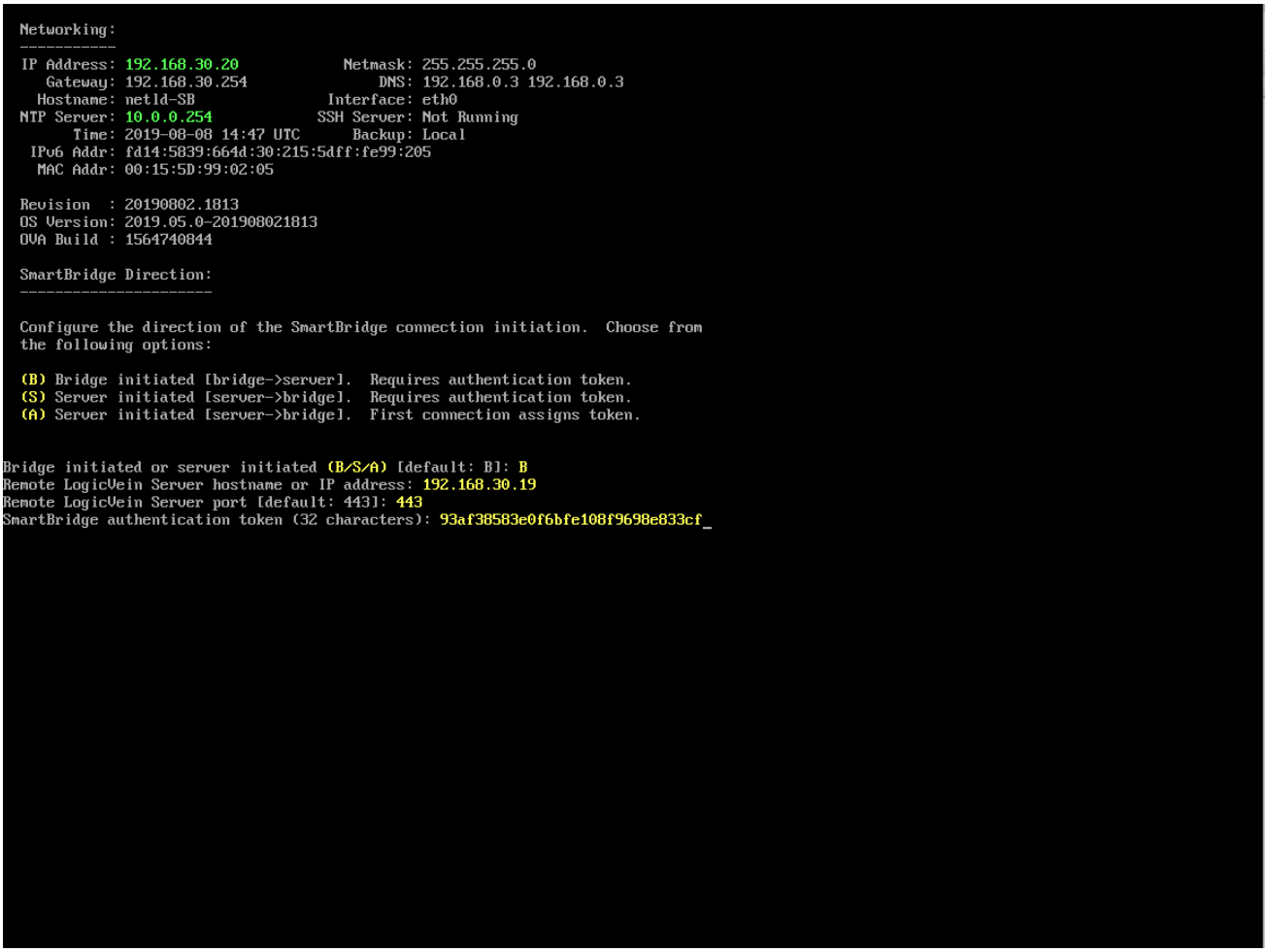
5.6 SmartBridge Settings

Set the core server information and token in SmartBridge. SmartBridge does not have a web console, so you will need to use the OVA console.

1. Press [4] on the keyboard to select [SmartBridge Direction].



2. Enter the values for the following items using the keyboard and press the [Enter] key to proceed.



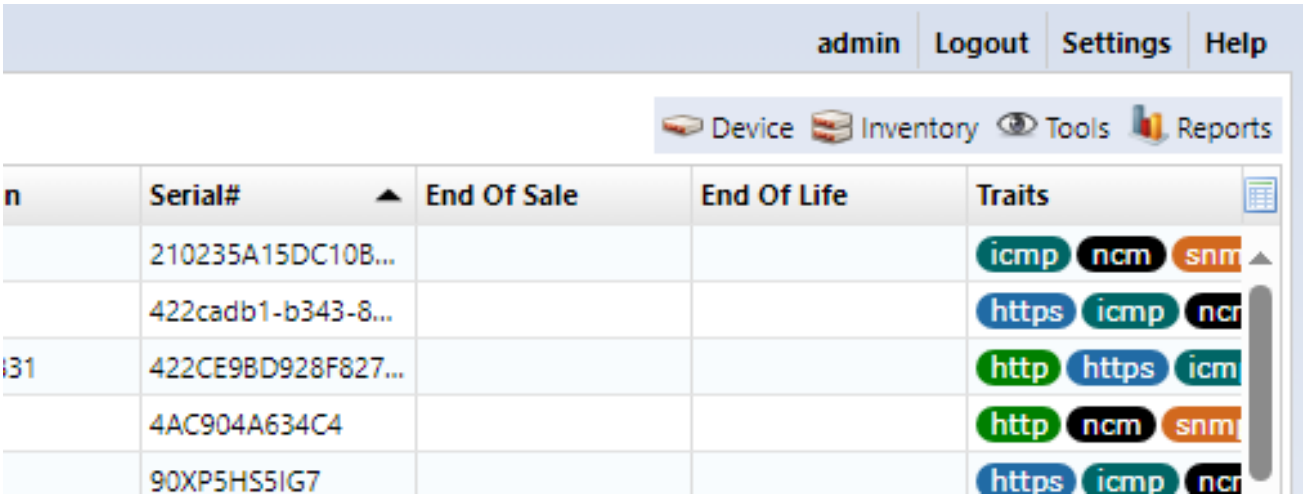
Project	Explanation	Keyboard Selction
Connection Initiation	Connection direction	
	Connect from Bridge to Server (with token)	[B]
	Connect from Server to Bridge (with token)	[S]
	Connect from Server to Bridge (without token)	[A]
Hostname or IP address	Core server (ThirdEye) IP address	`192.168.30.19`
Port	Core server (ThirdEye) HTTPS port	`443`
Token	Token generated during SmartBridge registration	

After the settings are made, the service will be automatically restarted, and you will be returned to the initial screen.

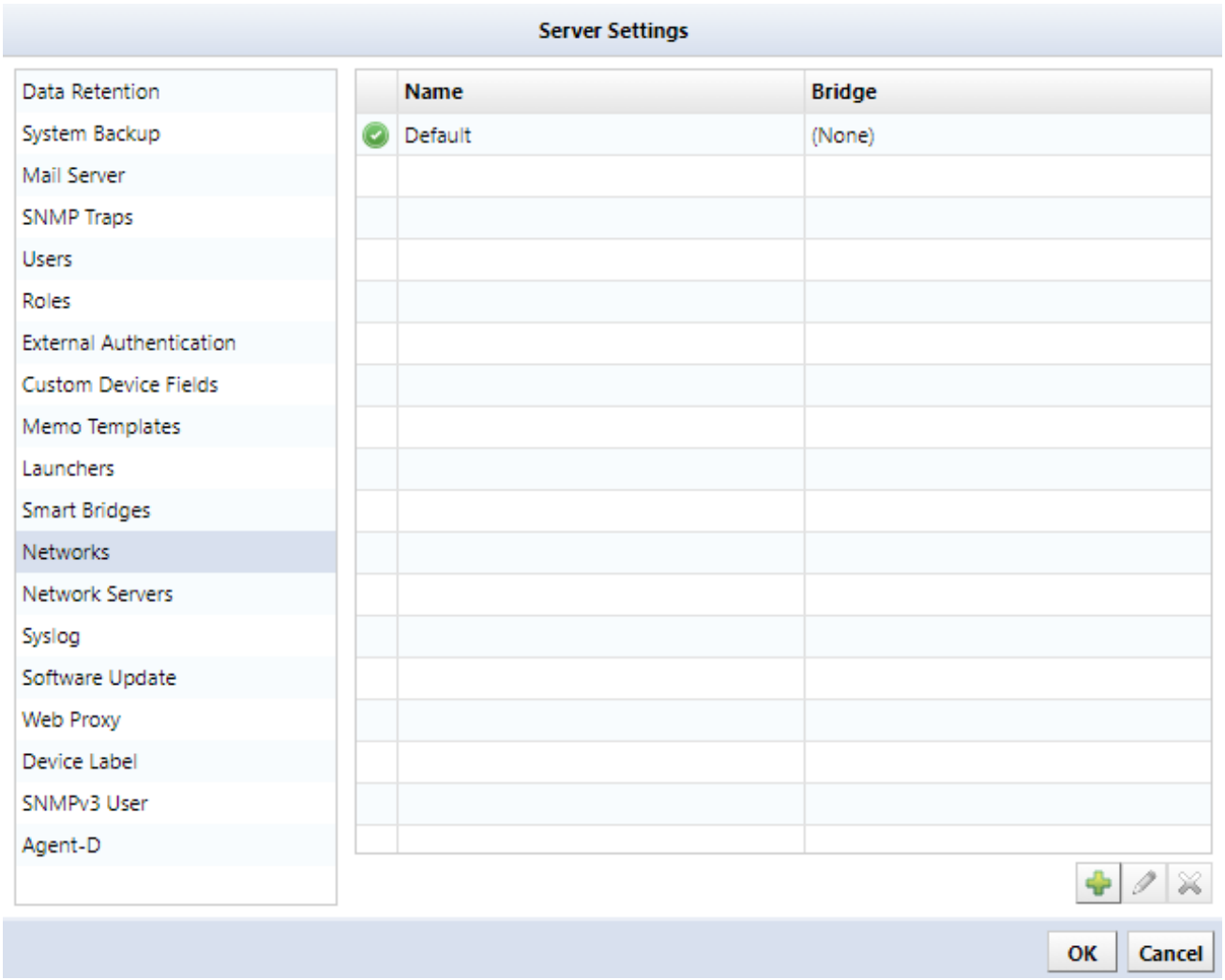
5.7 Managing Devices via SmartBridge

When you want to manage devices with SmartBridge, you will use the Network feature, any devices added to that network will be monitored/managed via SmartBridge.

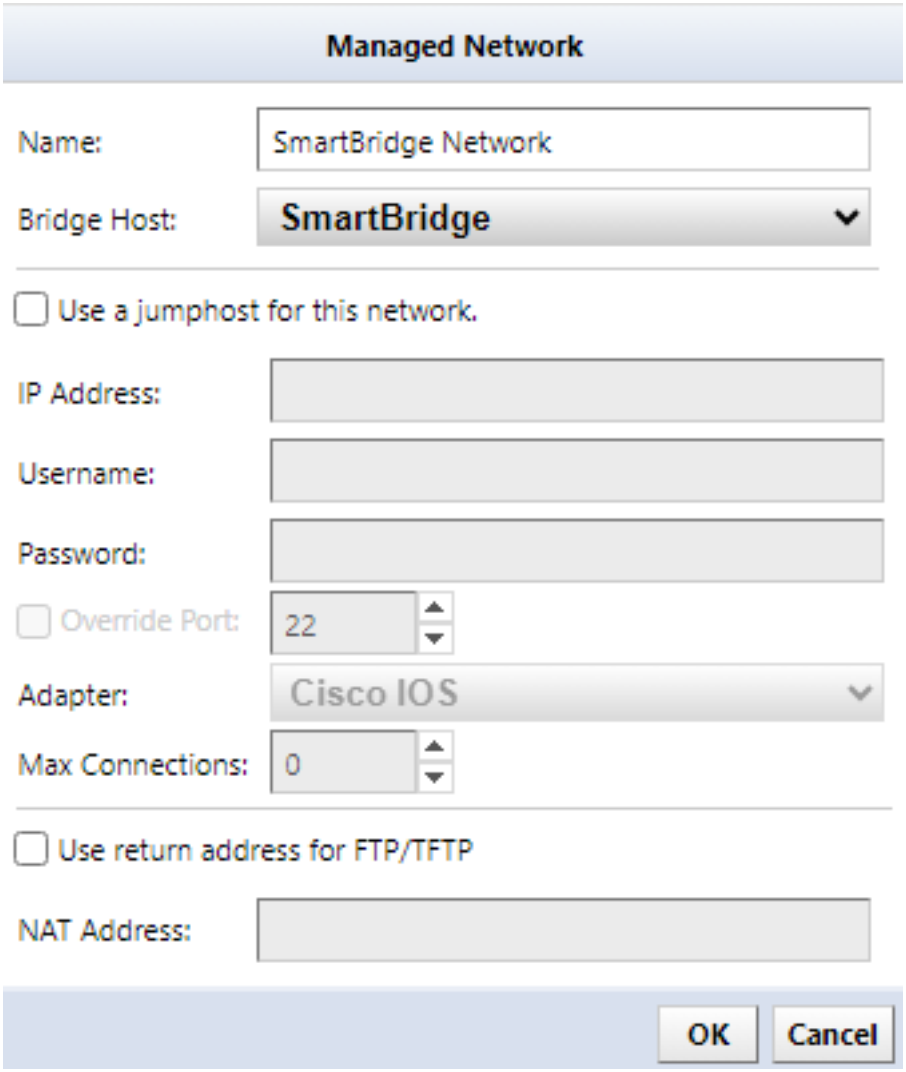
1. Click Settings.



2. Select the Networks category on the settings dialog and click the button to add a new network.

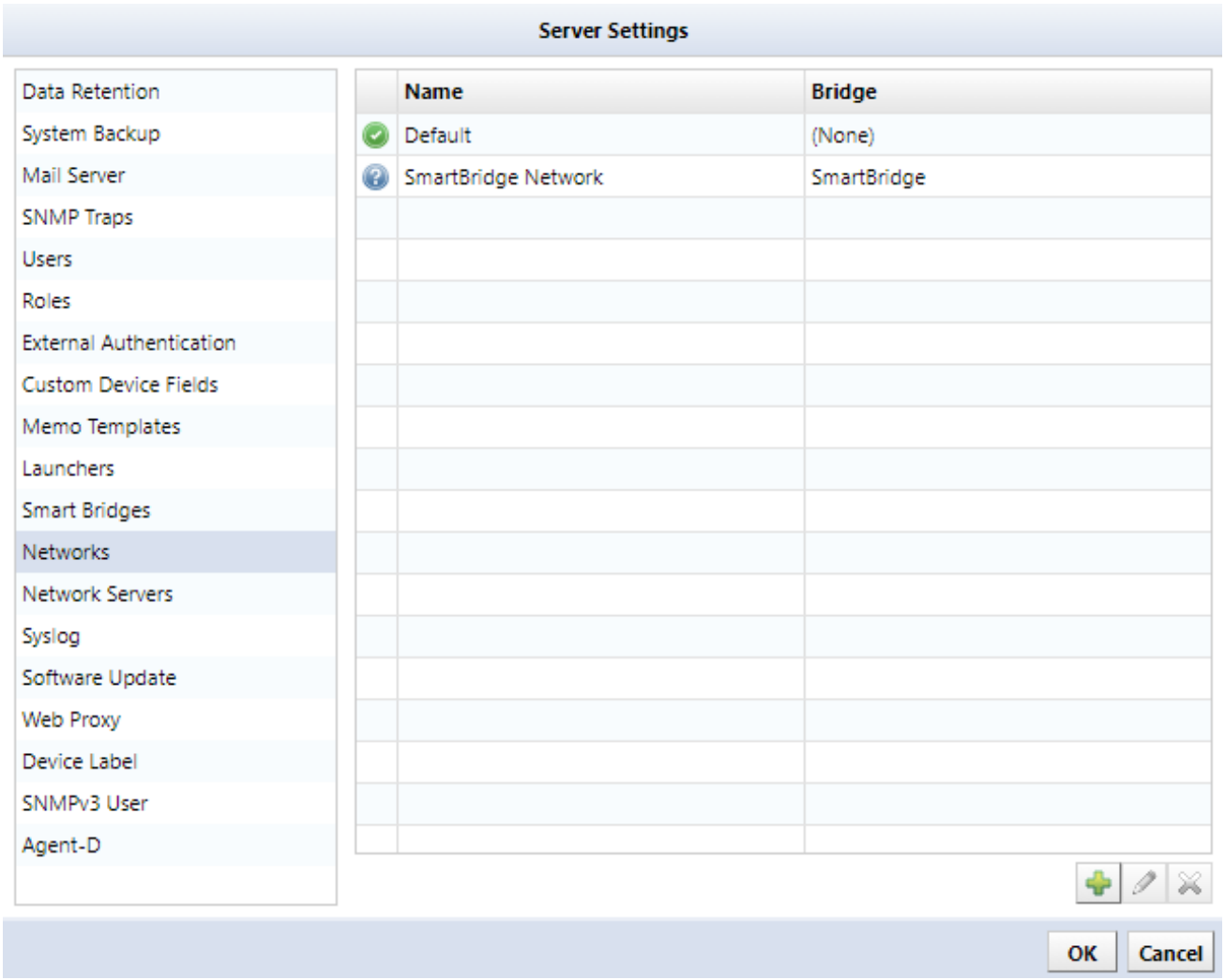


3. Enter a name for your network and select [Smart Bridge] in the “Bridge Host” field.

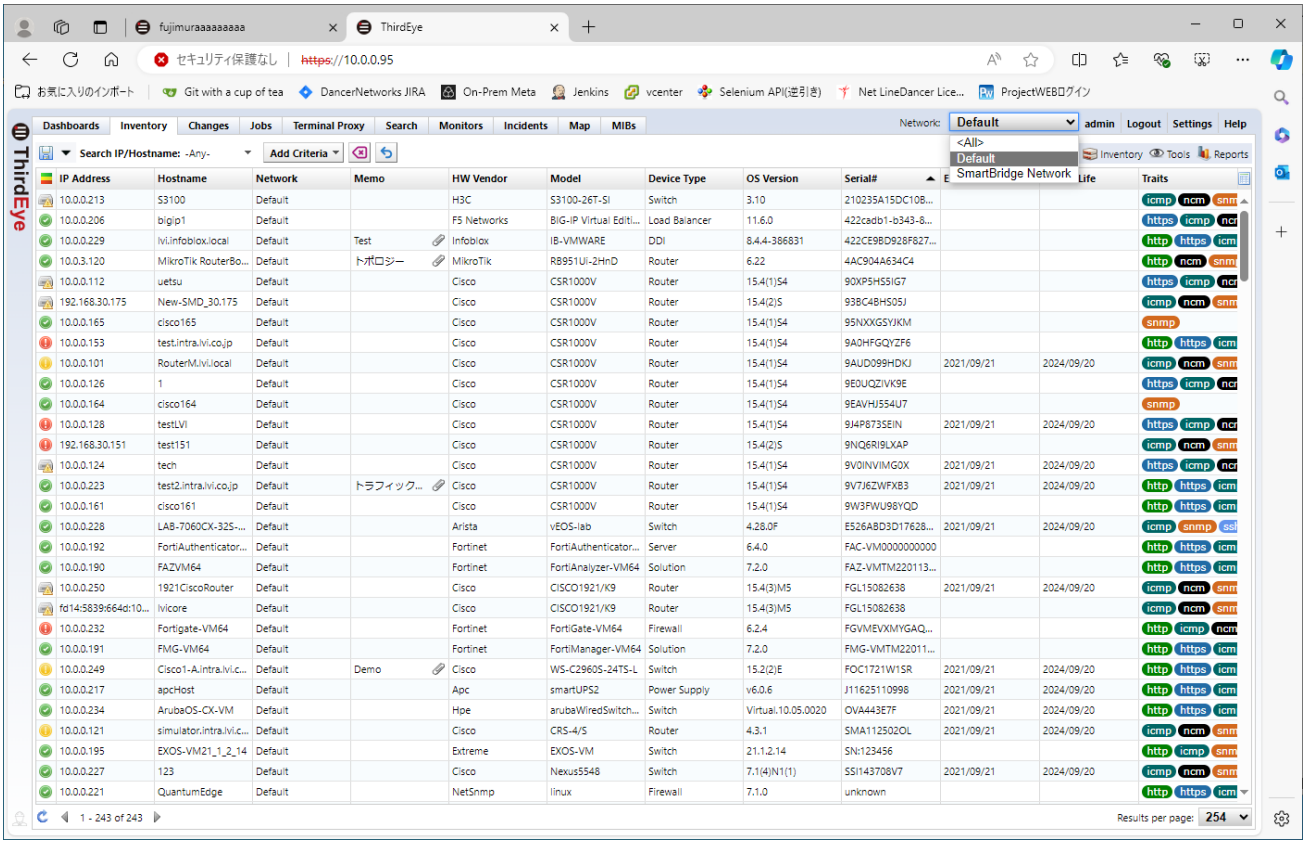


4. Click [OK]

The network has now been added, click [OK] to save the settings.



Once the settings are saved, the network will be added to the top left. Select the added network from the pull-down menu to display a blank table. The devices registered here will be monitored/managed via the selected SmartBridge.



6 Global Menu

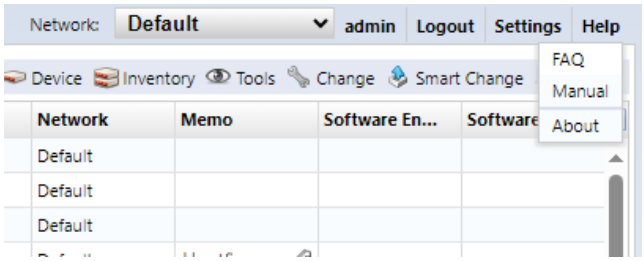
The Global Menu is the fixed menu that is always visible to the right of the main tabs:

Global Menu Item	Explanation
Network	The currently selected Managed Network. (This option is not visible when the logged in user only has access to a single Managed Network, or if no Managed Networks are configured.)
User name	The current login user name is displayed.
Logout	Log out of ThirdEye.
Setting	The Server Settings screen will be displayed.
Help	The [Help] menu contins the following links: **FAQ** - a link to frequently asked questions on the LogicVein website at https://logicvein.com/faqs **Manual** - a link to downloadable ThirdEye (and NetLD) PDF manuals at https://logicvein.com/manual **About** - Information about about ThirdEye

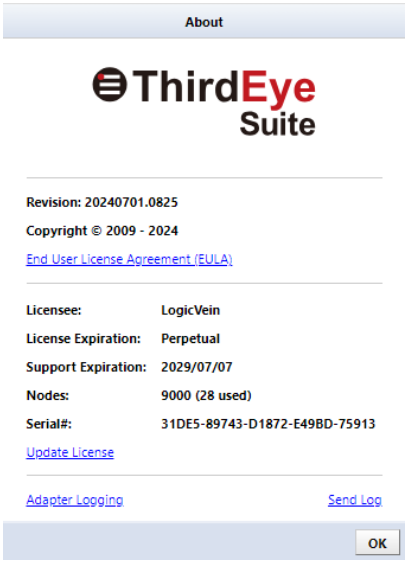
6.0.0.1 Update license If you update support, or increase the number of license nodes, you will need to update the applied license. You can update the license from [Help] > [About].

This task can only be performed by a user with administrator privileges.

1. Click [Help] > [Version Information] on the Global Menu.

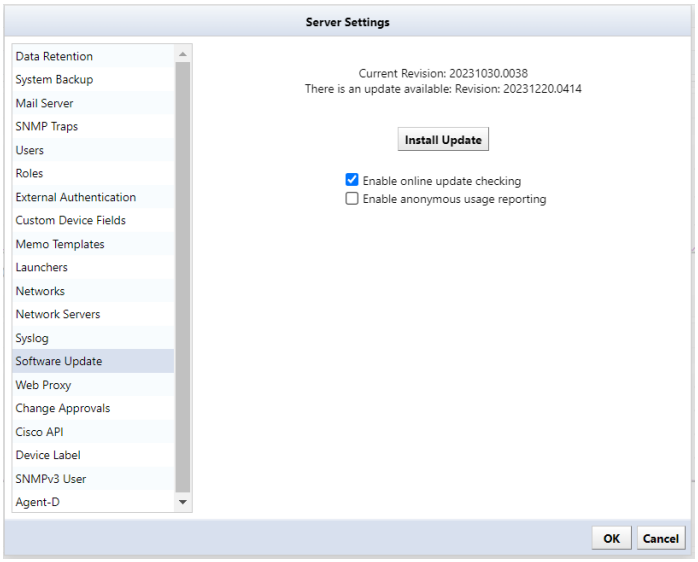


2. Click Update License.



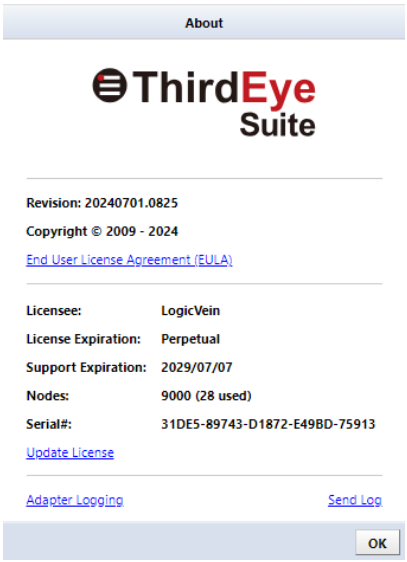
In the online environment, the license will be updated automatically. If you are in an offline environment, a screen to enter the activation key will be displayed. Please prepare the activation key in advance and update.

6.0.0.2 Update online The ThirdEye software version can be updated online via [Software update]. Software update settings only work when you are connected to the Internet.

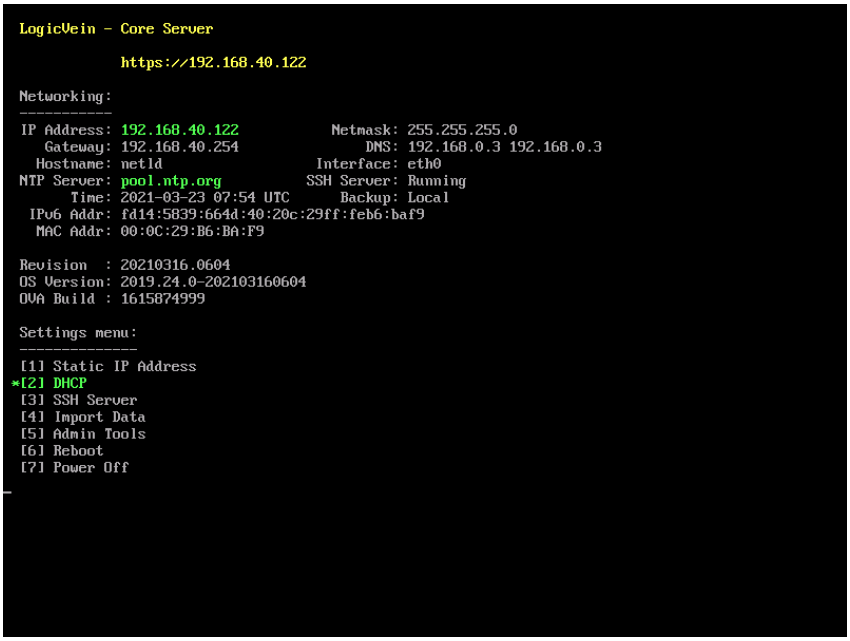


Setting	Explanation
Check for updates	Click Check for Updates to check online for updates.
Enable online update checking	If [Enable online update check] is checked, the machine will periodically check to see if updates are available. (Initial value: Enabled)
Enable anonymous usage reporting	If Enable Anonymous Usage Reporting is checked, usage data will be sent anonymously.

6.0.0.3 Check revisions To check the revision you are currently using, select [About] from the [Help] menu.

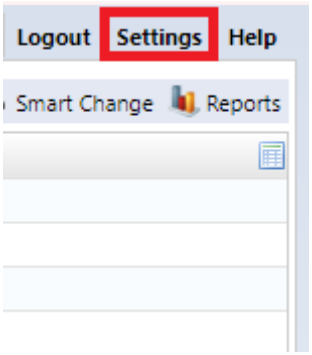


You can also check from the virtual machine console.

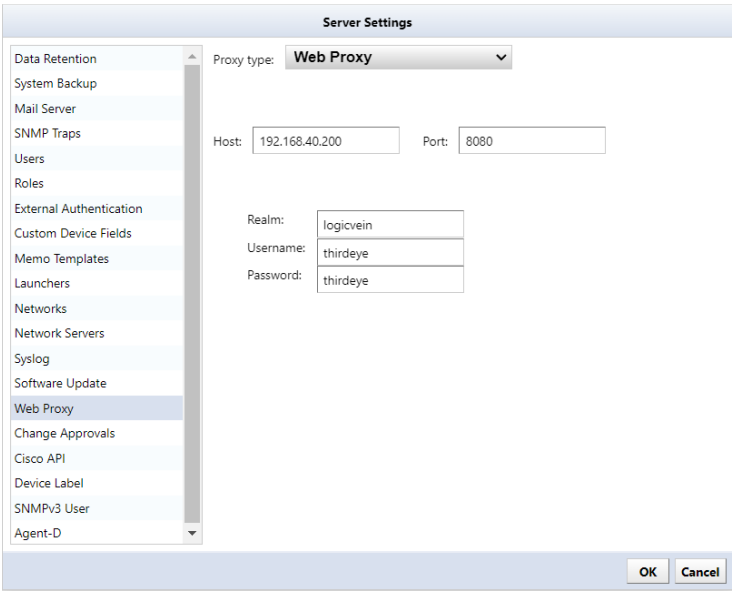


6.0.0.4 Use a proxy server If you want to use software updates and license updates online via a proxy server, set the proxy server information.

1. Click Settings on the Global Menu.



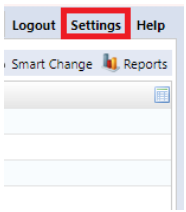
2. Click [Web Proxy] and enter the proxy server information.



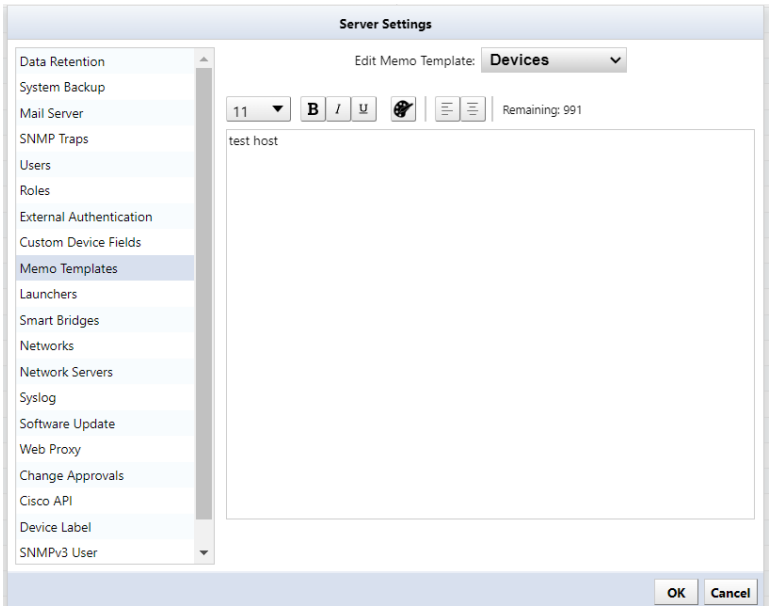
Item	Explanation
Proxy type	Select the proxy server type from the following: (Initial value: None) “None”, “Web Proxy”, “SOCKS4 Proxy”, “Secure Web Proxy”
Host	Specify the IP address or host name of the server to use as a proxy.
Port	Specify the port number on the proxy server. (Initial value: 8080)
Realm	Specifies the authentication realm for the proxy. If you do not need a realm, do not specify a value.
Username	Specify the username to send to the proxy server.
password	Specify the password to send to the proxy server.

6.0.0.5 Edit a memo template [Memo template] allows you to set a template that will be automatically inserted when creating a new Device Memo in the [Memo] column of the Inventory.

1. Click Settings on the Global Menu.



2. Click [Memo Template] in the left sidepanel.

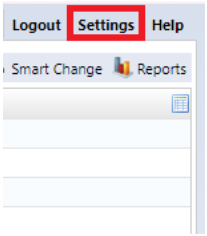


Item	Explanation
Font size	Change font size.
Bold	Change the specified text to bold.
Italic	Change to italic.
Underline	Underline.
Text color	Change the font color.
Left alignment	Set the string alignment to left alignment.
Centered	Set text alignment to center.
Number of input characters	Number of characters remaining that can be entered. All characters are counted as one character, regardless of whether they are full-width or half-width.

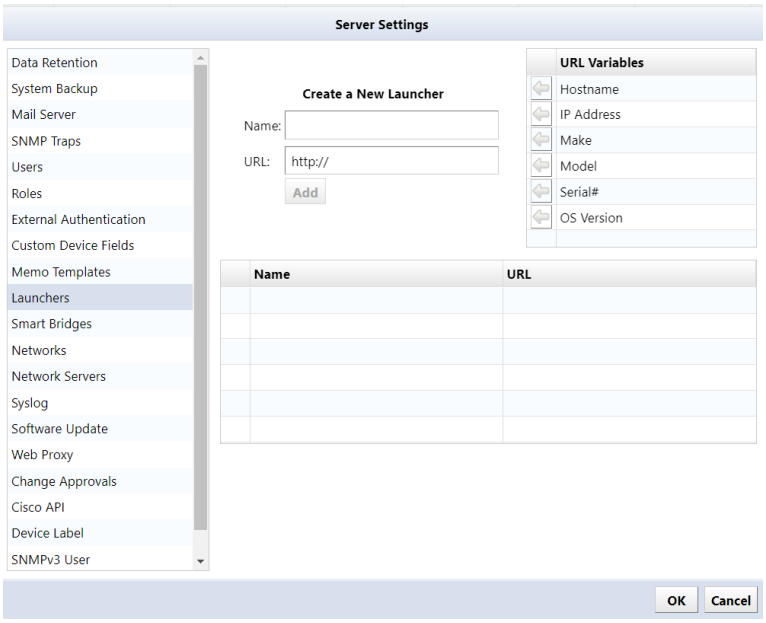
3. click [OK].

6.0.0.6 Add specific URL to right-click menu URL Launcher is a shortcut feature that allows you to easily access specific pages. By registering the URL, you will be able to access the page from the right-click menu.

1. Click Settings on the Global Menu.



2. Click [Launcher] in the left sidepanel.



3. Enter a name and specify the URL.

The name will be displayed as the menu name in the right-click menu.

URL variable explanation:

Items: Manufacturer

Explanation: Quoting the manufacturer name obtained during configuration backup.

Example: `http://{device.hardwareVendor}`

Items: Model

Explanation: Quoting the model name obtained from the configuration backup.

Example: `http://{device.model}`

Items: Serial number

Explanation: Quoting the serial number obtained during configuration backup.

Example: `http://{device.assetIdentity}`

Items: OS version

Explanation: Quoting the software version obtained by config backup.

Example: `http://{device.osVersion}`

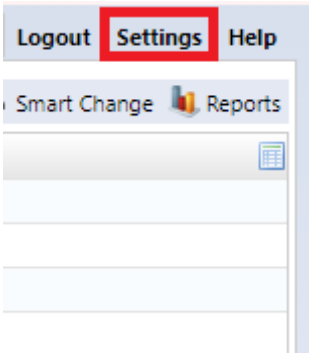
4. click [OK].

6.0.1 Set up mail server

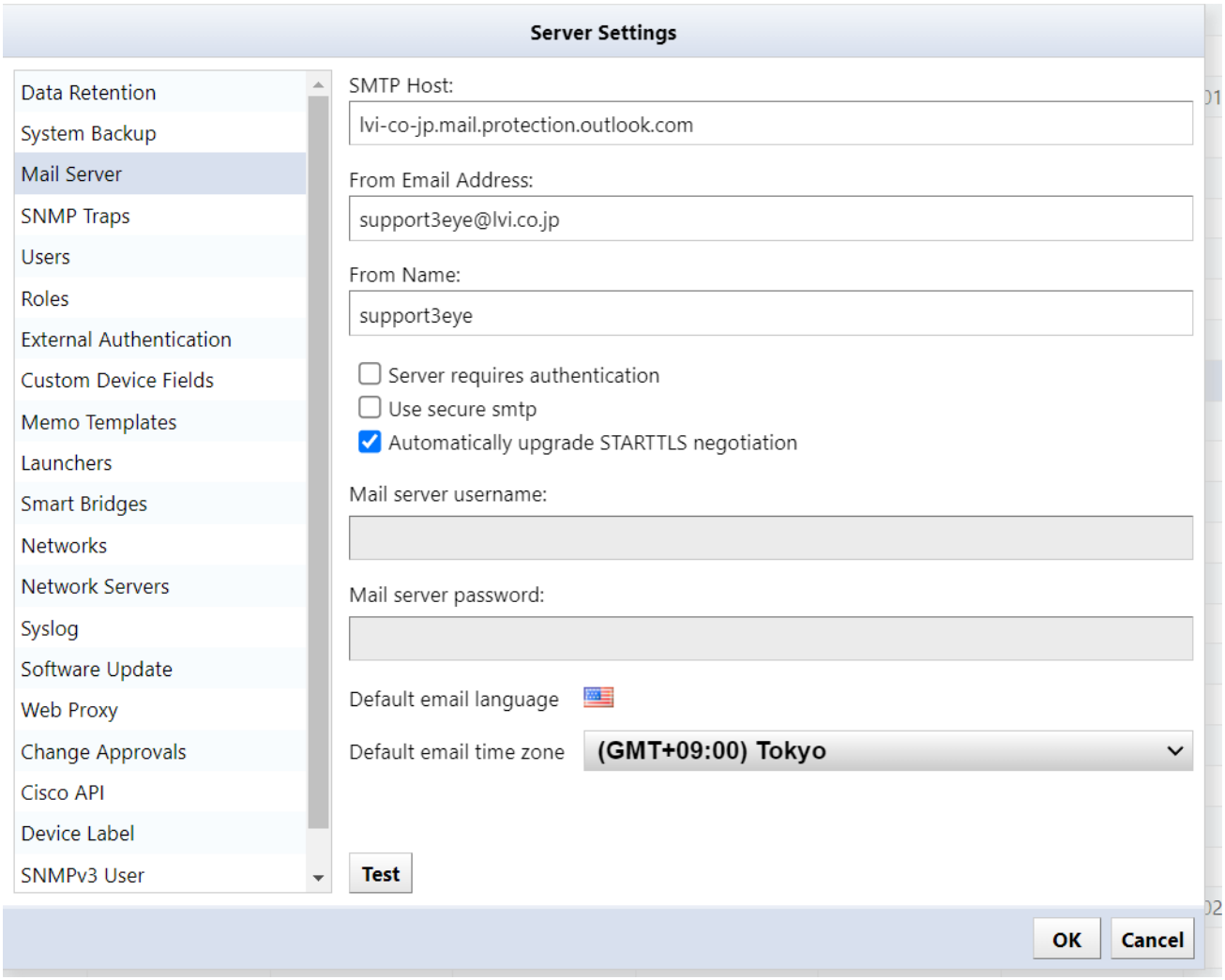
Enter the SMTP server information for Email Server notifications from {{ProductName}}.

> **Note**
>
> If you want to send an email or a dashboard report in the event of a failure, you need to make settings in advance.

1. Click Settings on the Global Menu.



2. Click [Mail Server], and enter the SMTP server information.



Field	Explanation
SMTP Host	Specify the host name or IP address of the mail server. (Initial value: `mail`)
From Email Address	Specify the email address that will be displayed as the sender (sender) of the email. (Initial value: `netLD`)
From Name	Specify the name that will be displayed as the email sender's name (sender). (Initial value: `netLD`)
Server requires authentication	Configure mail server authentication. If SMTP authentication is required, check the box and configure the following items. (Initial value: `disabled`) Mail server username… Authentication ID Mail server password… Authentication password
Use secure smtp	Enable TLS.
Automatically upgrade STARTTLS negotiation	Automatically upgrade to secure connections using TLS or SSL.

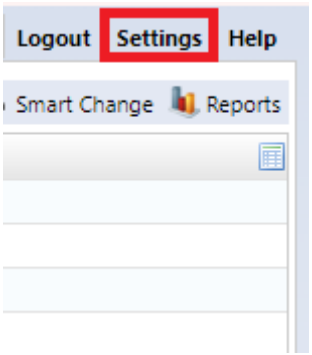
Field	Explanation
Default email language	Set the email display language.
Default email time zone	Set the email time zone.
Root Certificate	Set the trusted CA certificate.

3. Click [OK].

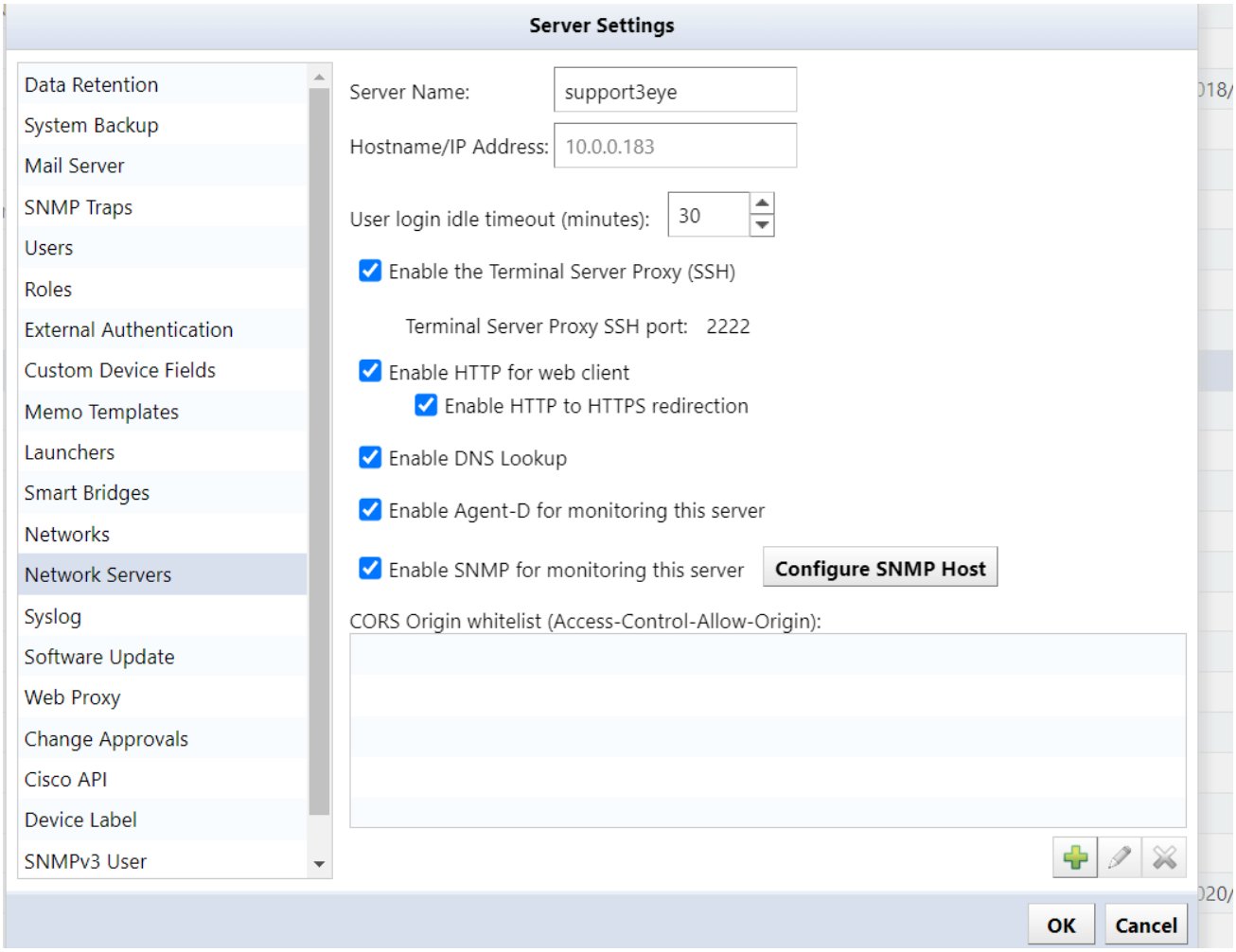
6.0.2 Use sysName for hostname

{{ProductName}} retrieves the hostname from your DNS server and displays it in the [Devices] tab. To use the host name (`sysName`) 7on the device, use the following settings.

1. Click Settings on the Global Menu.



2. Click [Network Server] in the left side panel, and uncheck “Enable DNS Lookup”.

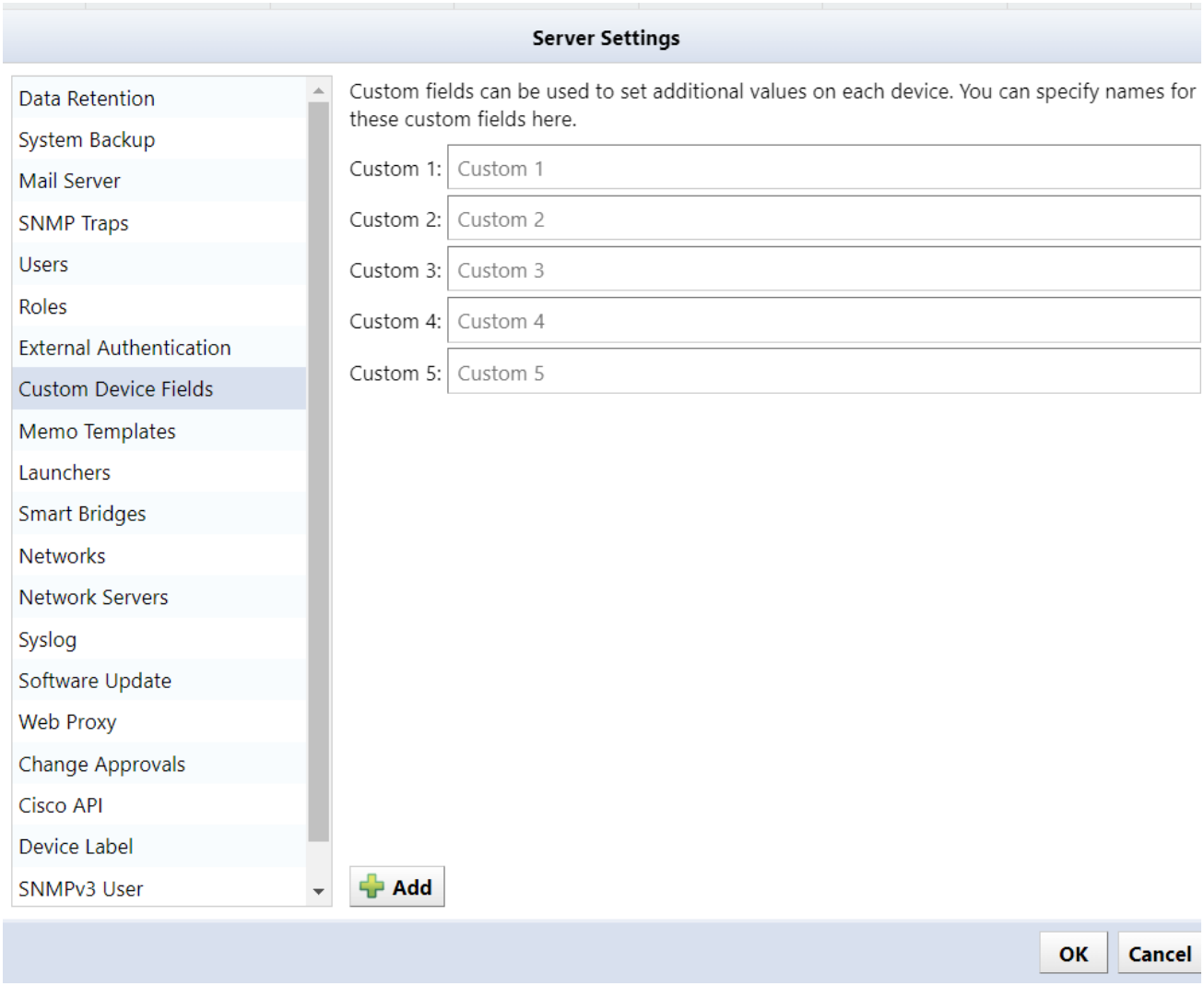


3. Click [OK].

6.0.3 Add columns/change column names for custom device fields

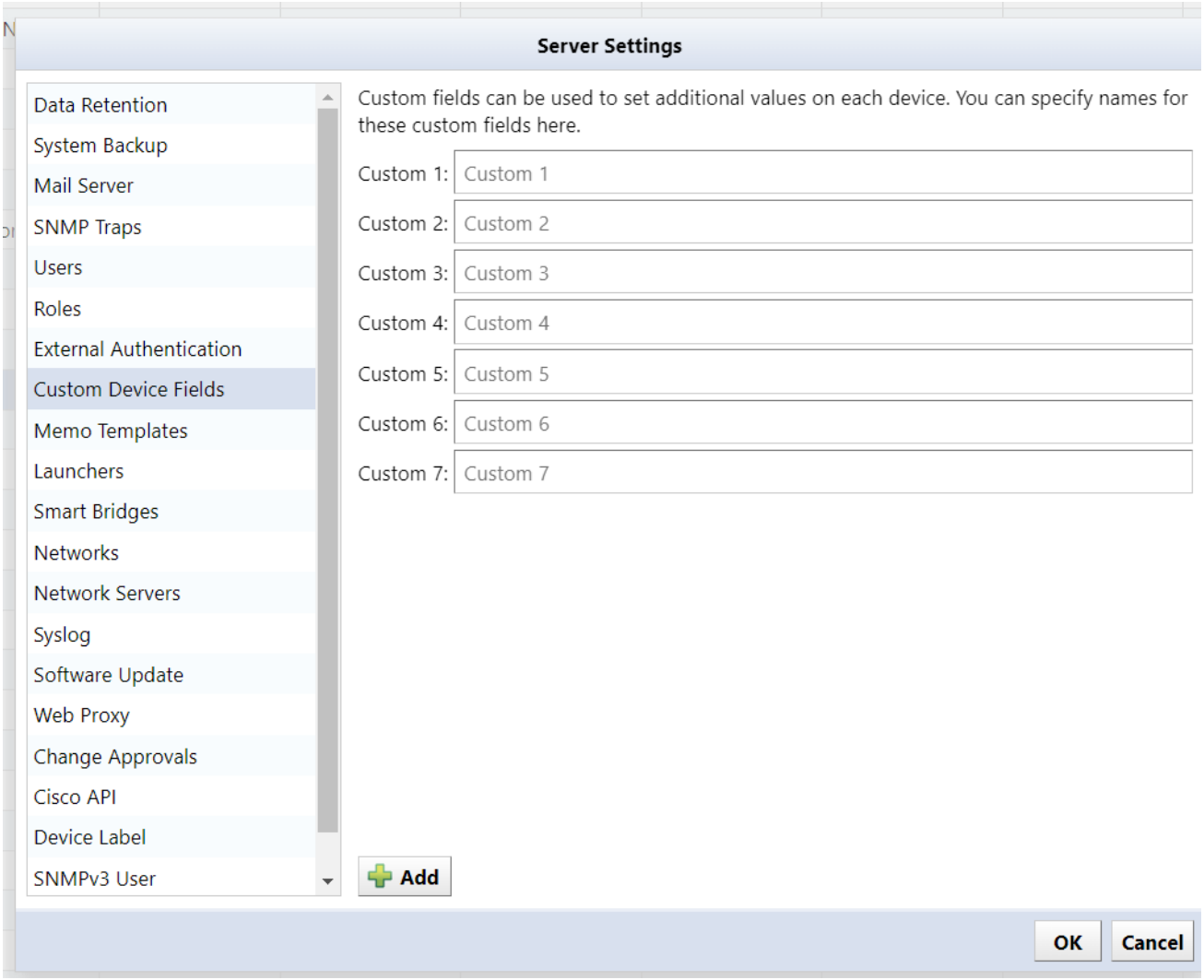
The custom device field allows you to set the name of a custom column to be used in device tabs and searches.

1. Click Settings on the Global Menu.
2. Click [Custom Device Field].



3. Set the desired display name in the input field to change the column name(s).

4. To add a column, click the button to add a column.



Note

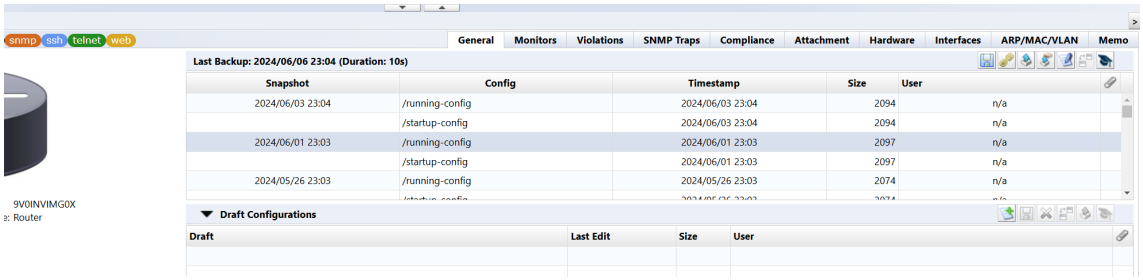
Once a custom device field is added, it cannot be deleted.

6.0.4 Draft configuration Suite

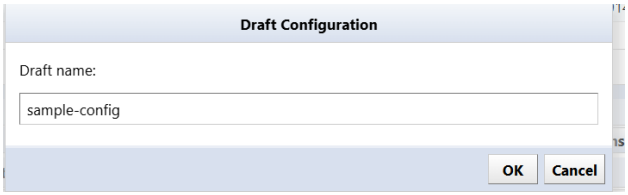
A draft configuration is a configuration that is saved independently from the backup history. Its nature is almost the same as a normal backed up configuration history, but with some additional elements. For example, each can be given a name, saved externally in plain text, and imported. This feature is useful if you want to reuse the same device configuration several times.

6.0.4.1 Creating a draft configuration Draft configurations can be created by copying from an existing configuration history.

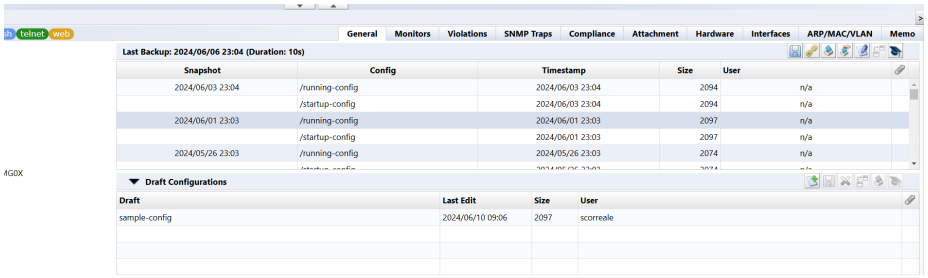
1. Doubleclick the target device to open the configuration history.
2. Select the one you want to base your draft configuration on and click the following button.



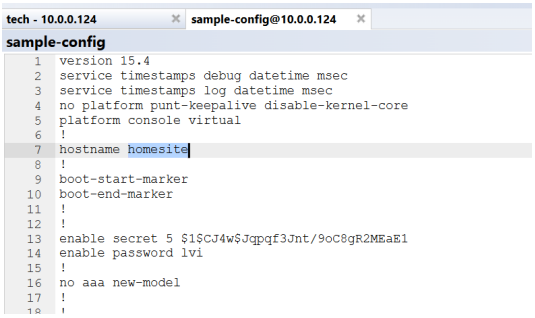
3. Enter a name for your draft configuration and click [OK].



4. Doubleclick the created draft configuration.

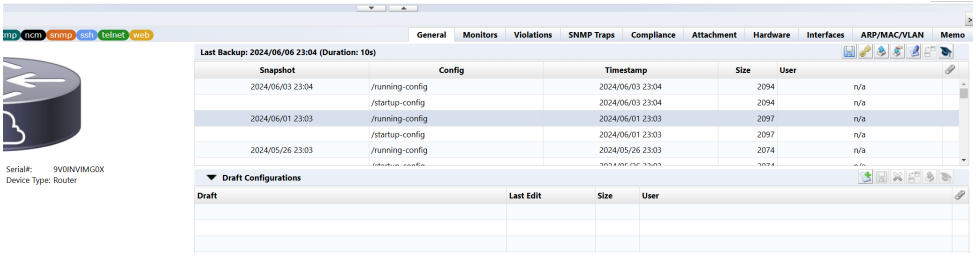


5. Edit the configuration and click button.

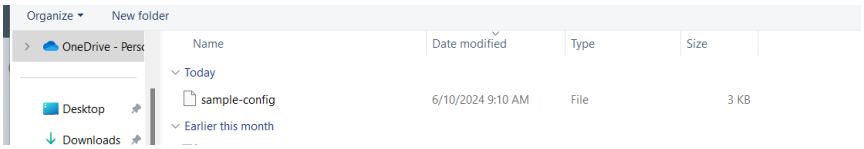


6.0.4.2 Import draft configuration from plain text You can create a draft configuration by importing a configuration edited with a text editor, etc. First, doubleclick the target device in the device view to display the configuration history.

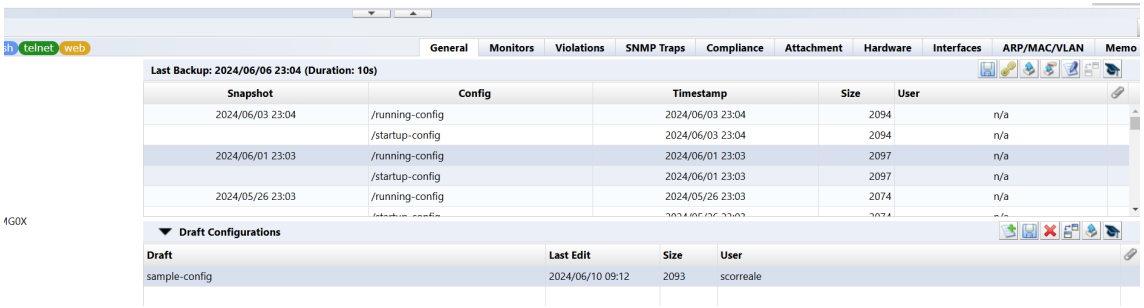
1. In the status panel, click the  button.



2. Select the file you want to import and click Open.



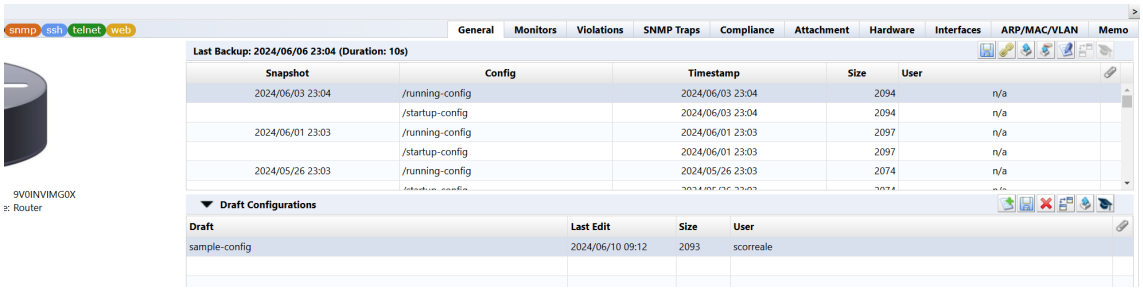
The contents of the text file are imported and a draft configuration is created.



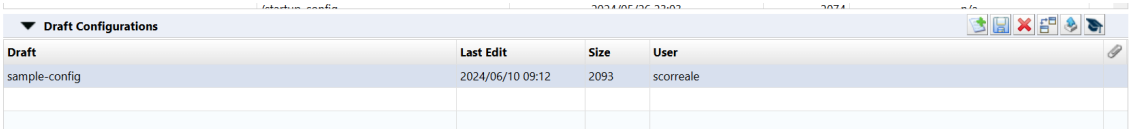
6.0.4.3 Export the draft To export, click the  button.

6.0.4.4 Delete draft To delete, click the  button.

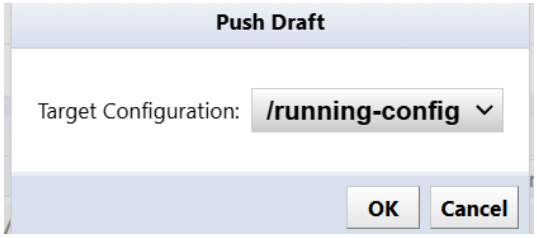
6.0.4.5 Comparison of drafts To compare configurations, click the button. You can use the same comparison functions in draft configurations as in regular configurations.



6.0.4.6 Apply draft configuration to devices Similar to comparing drafts, applying drafts can be done using the same procedure as applying (restoring) backup configurations. However, there is one difference. Select the draft configuration to upload, click the button.



Please select which one you would like to upload to. This is the only difference from history upload. (When uploading history,running-config ,startup-config will be uploaded respectively.)

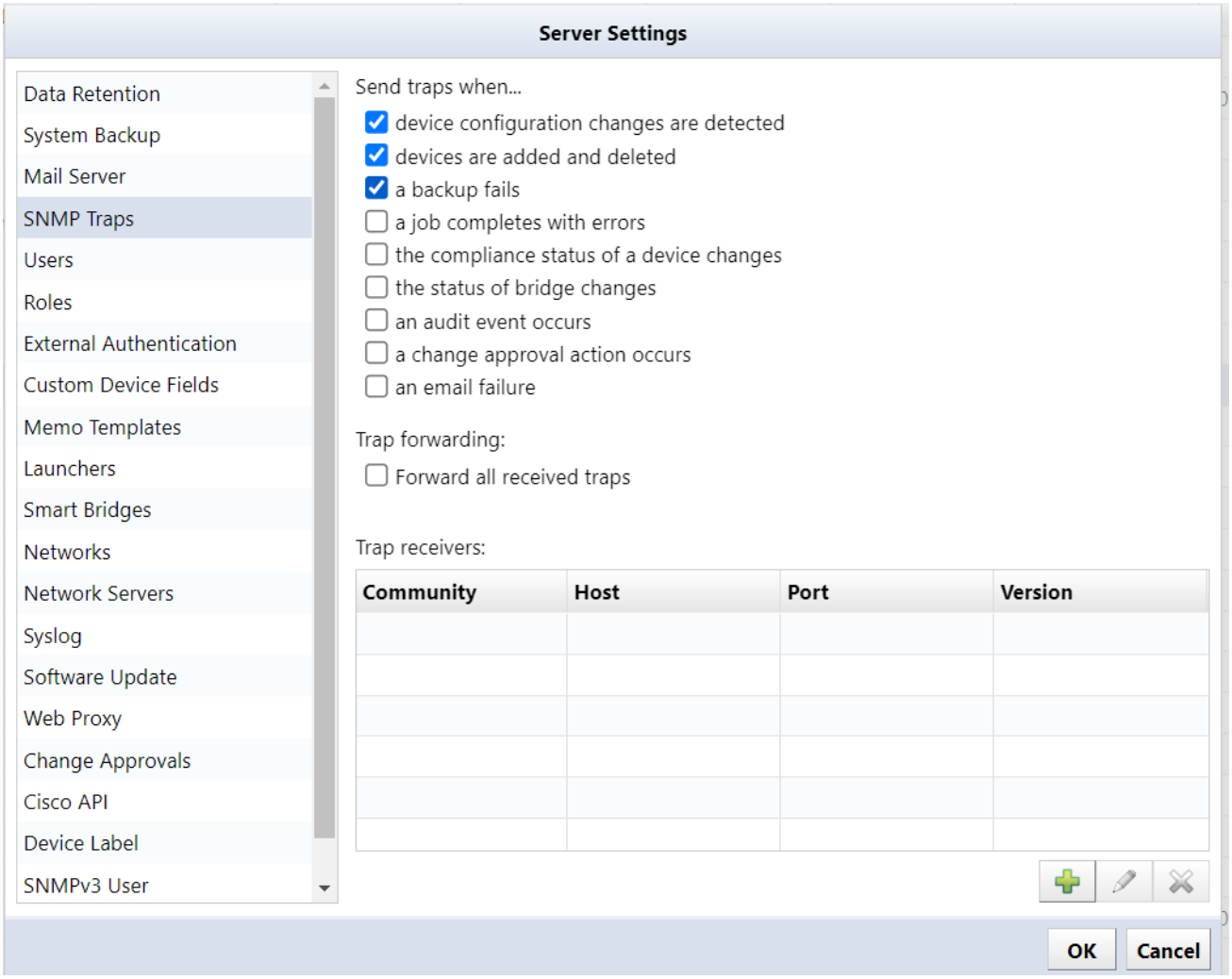


Press [OK] to start uploading.

6.0.5 Configure SNMP trap sending

You can configure SNMP Trap Settings configures settings for sending SNMP traps from {{Product-Name}}. Set the conditions for sending traps and the trap destination.

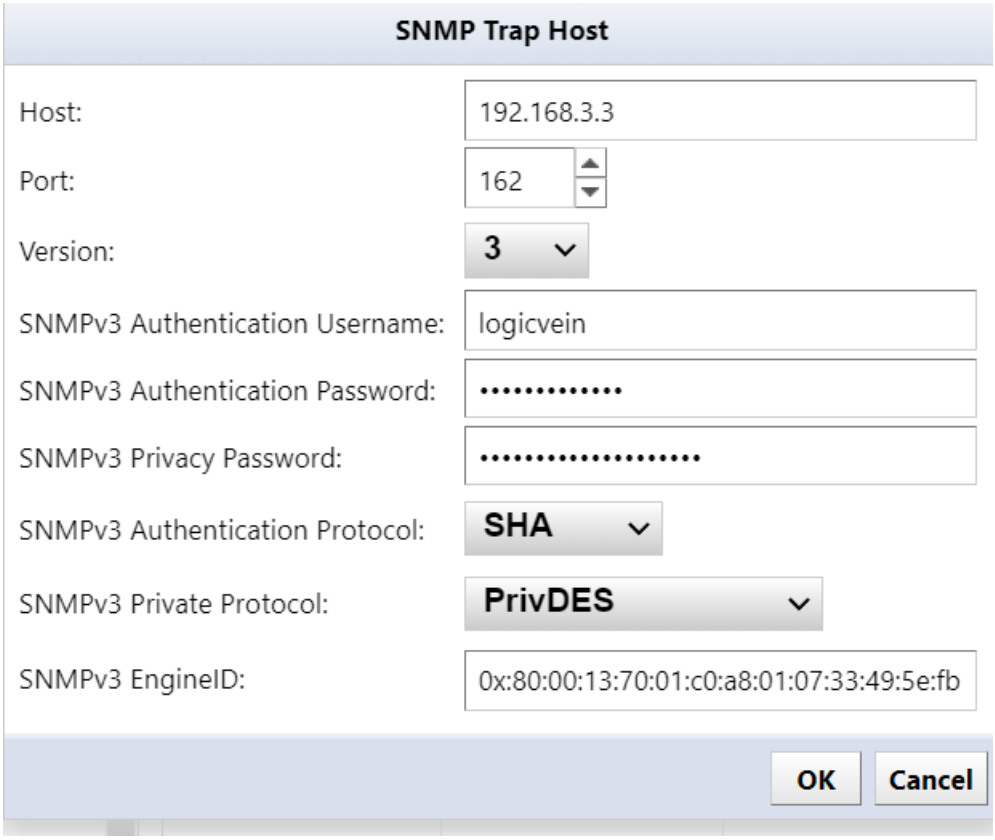
1. Click Settings on the Global Menu.
2. Click SNMP Trap Settings and select the events to be sent.



Event Trigger	SNMP Trap Action
Device configuration changes are detected	Sends an SNMP trap when it detects that the device configuration has changed since the last backup.
Devices are added and deleted	Sends SNMP traps when devices are added/removed.
A backup failure	Sends an SNMP trap if configuration backup fails.
A job completes with errors	Sends an SNMP trap if job execution fails.
The compliance status of a device changes	Sends SNMP traps when compliance status changes.

Event Trigger	SNMP Trap Action
The status of bridge changes	Sends an SNMP trap when the connection status between the smart bridge and core server changes. (*Displayed only when the optional license is valid)
An audit event occurs	Sends an SNMP trap when a user logs in/logs out.
A change approval action occurs	Sends an SNMP trap when a job approval event occurs.
An email failure	If email sending fails, an SNMP trap will be sent.

3. Click the button.
4. Enter the trap destination information and click [OK].



Items	Explanation
Host	Enter the IP address or host name of the trap destination.
Port	Specify the trap destination port. (Initial value: `162`)
Version	Specify the trap version from the following: `2c`, `3`
SNMP Community String	Enter the trap community name. (When selecting 1 or 2c at Version)

Items	Explanation
(SNMPv3) Authentication Username	Enter the username used for user authentication.
(SNMPv3) Privacy Password	Enter your encryption password.
(SNMPv3) Authentication Protocol	Specify the authentication protocol from the following: `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
(SNMPv3) Private Protocol	Specify the encryption protocol from the following: `PrivDES`, `PrivAES128`, `PrivAES192`, `PrivAES256`, `Priv3DES`, `PrivAES256-3DES`, `PrivAES192-3DES`
(SNMPv3) EngineID	Enter if you want to change the engine ID. (It will be filled in automatically)

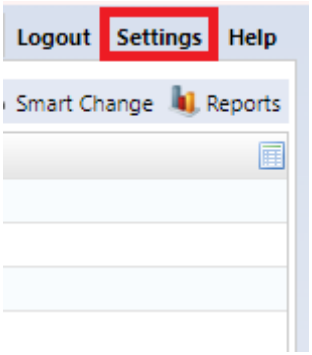
7 Manage Users

7.1 Create User Account

Create a user to log in to {{ProductName}}.

By assigning privileges to users, you can restrict the operations that users can perform. {{ProductName}} allows you to specify detailed permissions by combining multiple permissions.

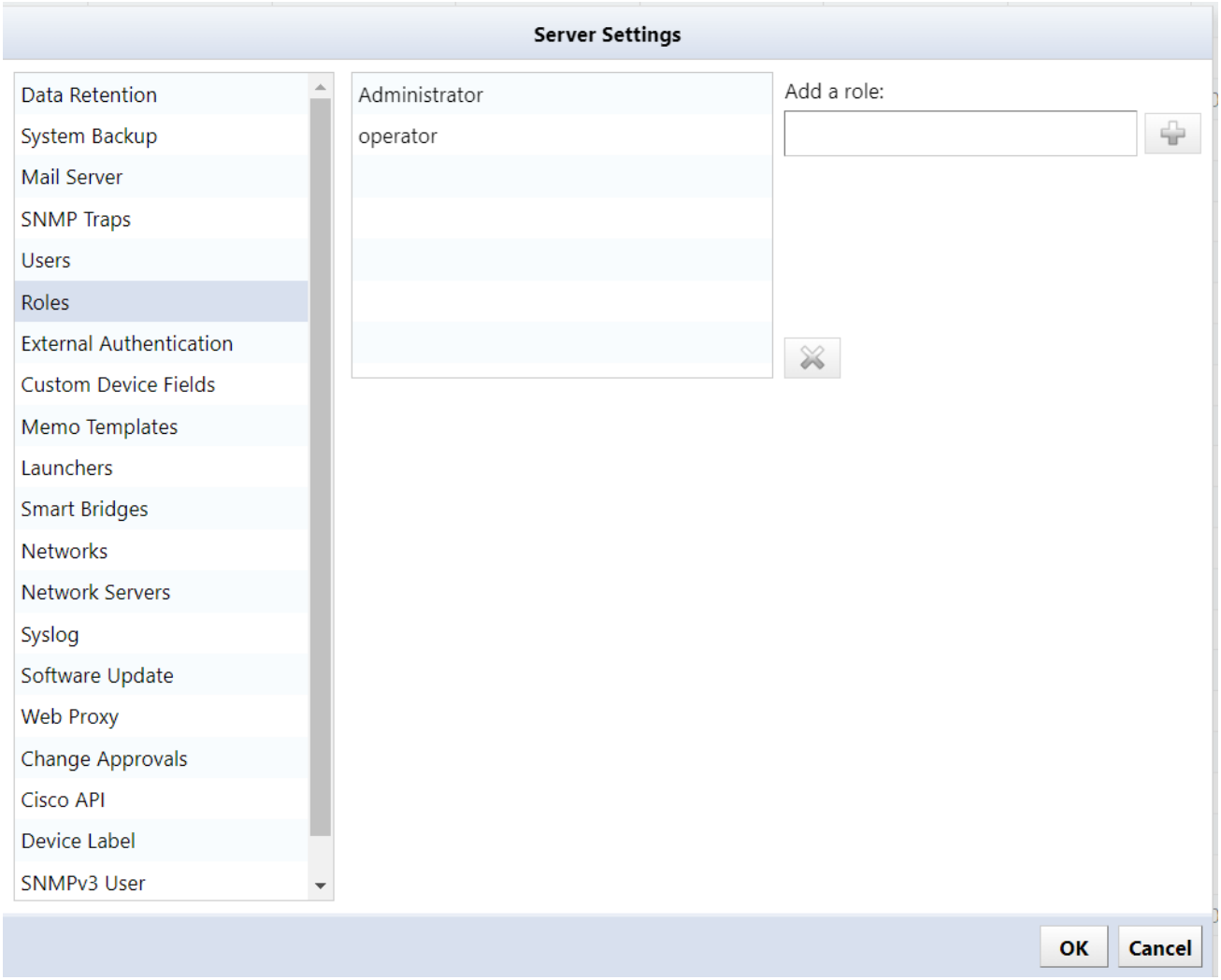
User and permission settings can be configured from Settings in the Global Menu.



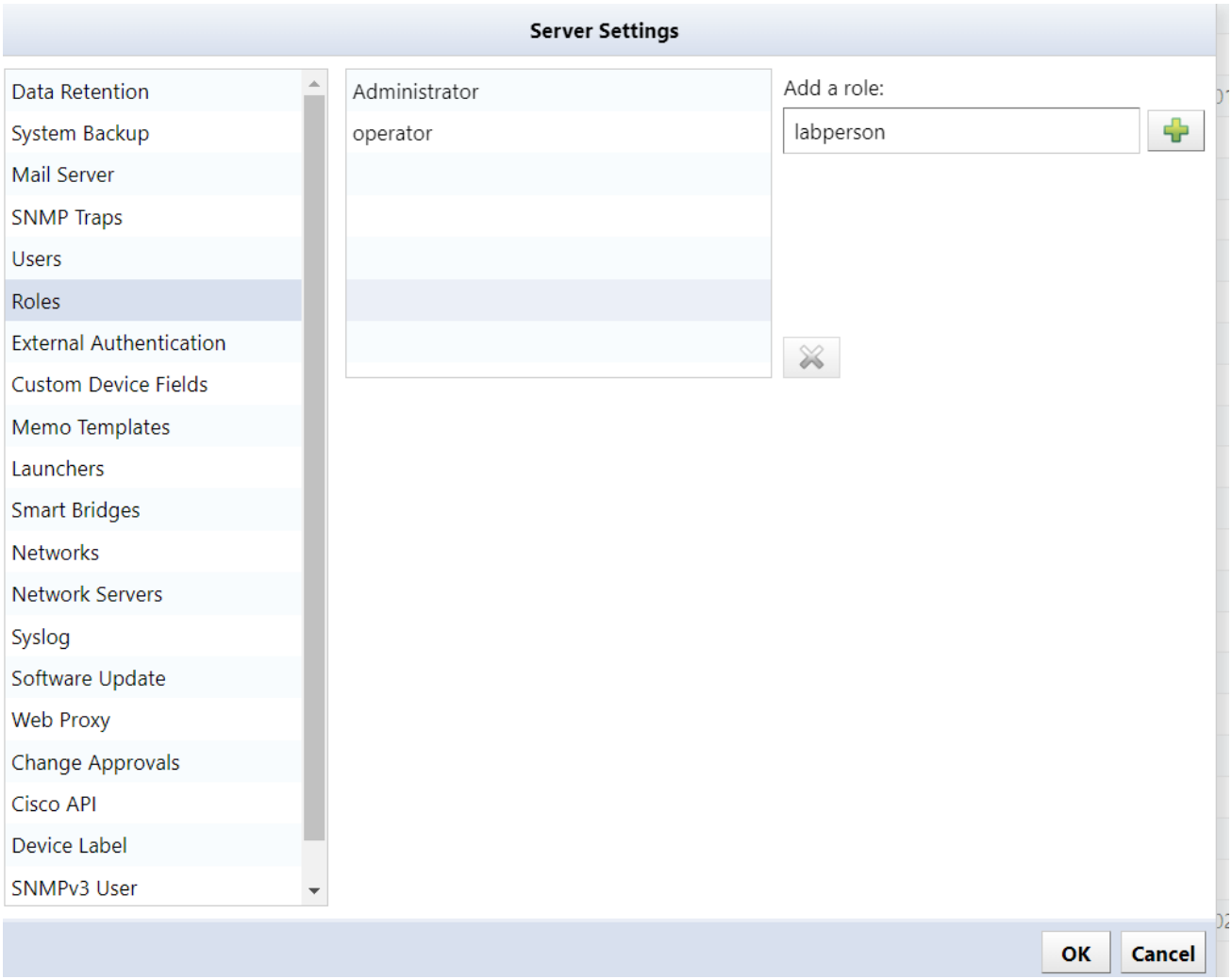
7.2 Add permissions

A user registered as “Administrator” has all execution privileges. Administrator privileges cannot be removed.

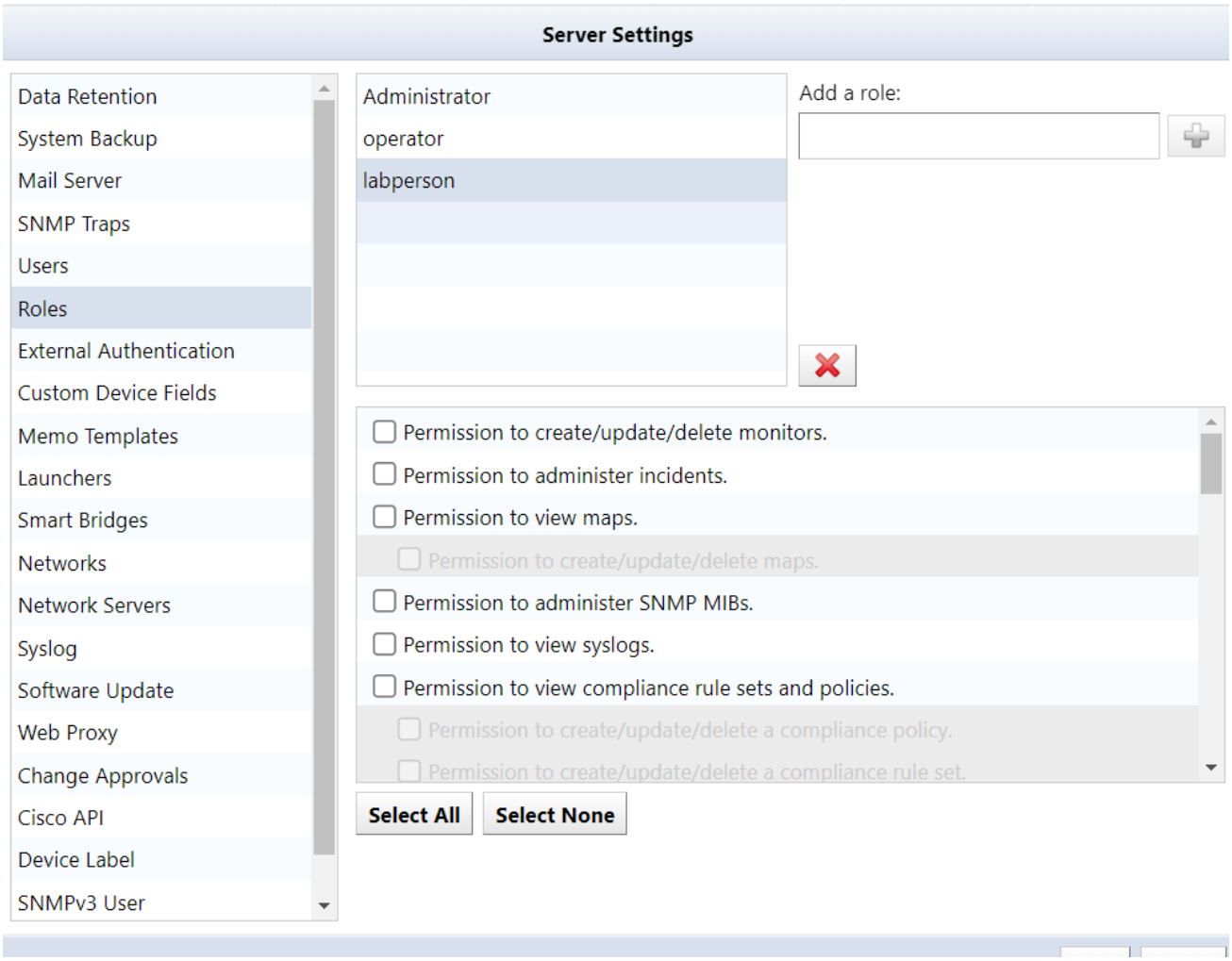
1. Click [Roles] in the left sidebar.



2. Enter the permission name in the [Add a Role] field and click the button.



3. The permission name is added to the list and becomes selected. Check the required items from the authority items at the bottom right of the screen.



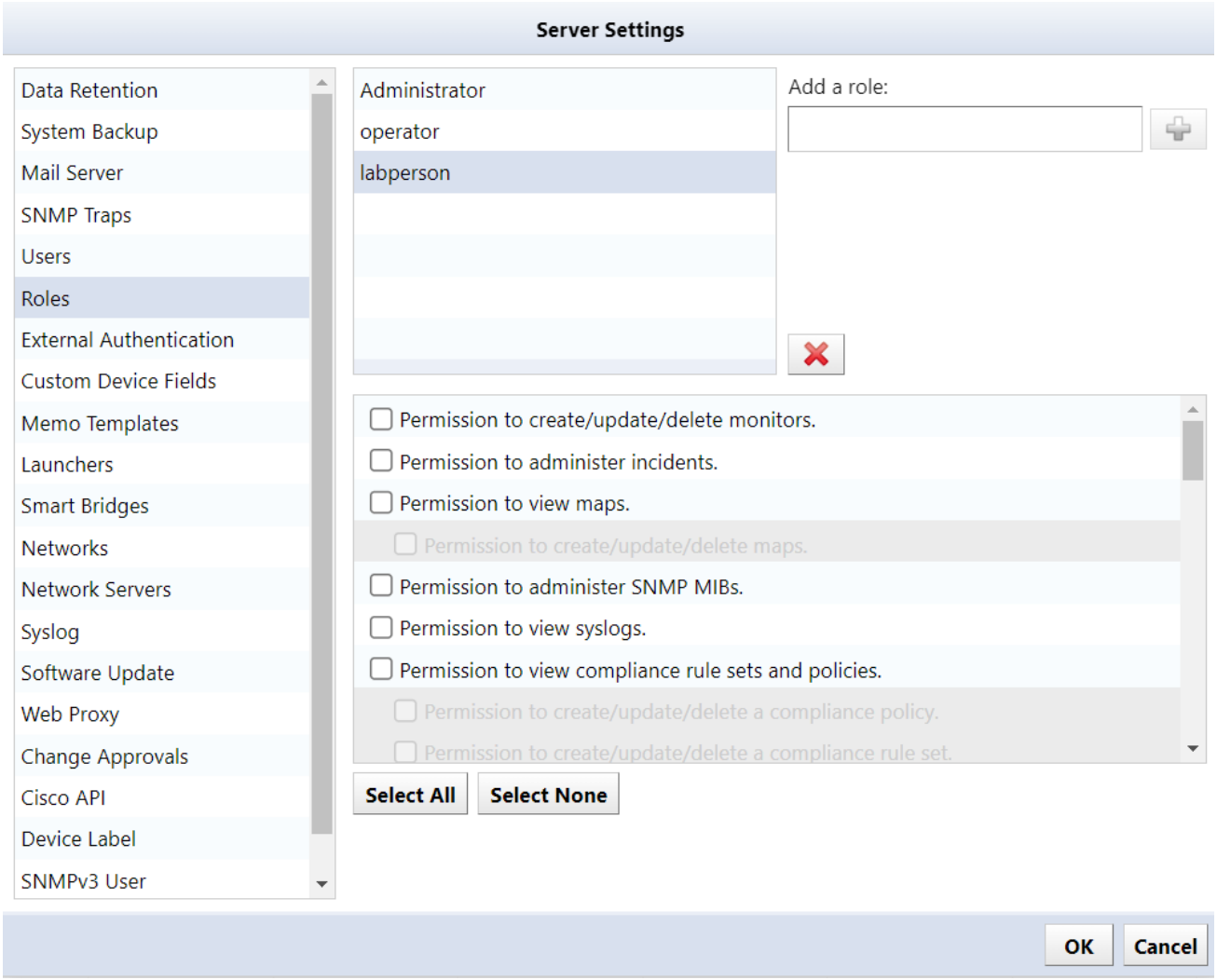
Permission Item	Edition	Explanation
Permission to create/update/delete monitors		You can create/update/delete monitors.
Permission to administer incidents		You can update incidents.
Permission to view maps		You can view the map.
Permission to create/update/delete maps		You can create/update/delete maps. (Permission associated with "Allow map viewing.")
Permission to administer SNMP MIBs		You can add/delete MIBs.
Permission to view syslogs		You can view Syslogs sent from devices.

Permission Item	Edition	Explanation
Permission to view compliance Rule Sets and policies	Suite	You can view the Compliance tab.
Permission to create/update/delete a compliance policy	Suite	You can create/update/delete compliance policies. (Permission associated with “Permission to view compliance Rule Sets and policies.”)
Permission to create/update/delete a compliance Rule Set	Suite	You can create/update/delete compliance rules. (Permission associated with “Permission to view compliance Rule Sets and policies.”)
Permission to view device configurations	Suite	You can view the configuration retrieved from the device.
Permission to administer credentials and protocols		You can configure credentials and protocols.
Permission to view secure credentials		You can view the secure credential.
Permission to create/update/delete device information in the inventory		You can create/update/delete device information in inventory.
Permission to assign names to custom fields		You can rename custom device fields.
Permission to tag/untag devices in the inventory		You can apply and remove tags to devices in your inventory.
Permission to view configuration drafts		You can view draft configurations.
Permission to create/update/delete configuration drafts		You can create/update/delete configuration draft jobs. (Permission associated with “Permission to view configuration drafts.”)
Permission to administer scheduler filters		You can set schedule filter.
Permission to run a backup job		You can run backup job.
Permission to create/update/delete a backup job		You can create/update/delete backup jobs. (Permission associated with “Permission to run a backup jobs.”)
Permission to run a device discovery job		You can run discovery.

Permission Item	Edition	Explanation
Permission to create/update/delete a device discovery job		You can create/update/delete discovery jobs. (Permission associated with “Permission to run a device discovery job.”)
Permission to run a Populate End Of Sale job	Suite	You can run Populate End Of Sale job.
Permission to run a tool	Suite	You can run the tool.
Permission to create/update/delete a tool job	Suite	You can create/update/delete tools. (Permission associated with “Permission to run a tool.”)
Permission to approve a tool job execution	Suite	You can approve jobs that require approval. (Permission associated with “Permission to run a tool.”)
Permission to run a tool job without approval	Suite	You can create and run jobs that do not require approval. (Permission associated with “Permission to run a tool.”)
Permission to run a Smart Change job (Permission associated with “Permission to run a tool.”)	Suite	You can run smart change jobs.
Permission to create/update/delete a Smart Change job	Suite	You can create/update/delete smart change jobs. (Permission associated with “Permission to run a Smart Change job.”)
Permission to run a tool which changes a device configuration	Suite	You can run the change tool. (Permission associated with “Permission to run a tool.”)
Permission to run a report		You can run the report.
Permission to create/update/delete a report job		You can create/update/delete reports. (Permission associated with “Permission to run a report.”)
Permission to run a restore job		You can run configuration restore jobs.
Permission to run Agent-D installer		You can run the Agent-D installer.
Permission to run a neighbor collection job		You can run neighbor information collection jobs.
Permission to create/update/delete a neighbor collection job		You can create/update/delete neighbor information collection jobs. (Permission associated with “Permission to run a neighbor collection job.”)

Permission Item	Edition	Explanation
Permission to create/update/delete URL launchers		You can create/update/delete URL launchers.
Permission to create/update/delete memos		You can create/update/delete notes.
Permission to create/update/delete managed networks		You can create/update/delete management networks.
Permission to administer security settings		You can set security.
Permission to create/update/delete inventory tags		You can create/update/delete inventory tags.
Permission to login using the terminal server proxy		You can log in via a terminal server proxy.
Permission to automatically log in to devices from the terminal server proxy		You can automatically login via terminal server proxy is possible. (Permission associated with “Permission to login using the terminal server proxy.”)
Permission to automatically log in directly into enable mode		You can automatically log in directly to enable mode. (Permission associated with “Permission to automatically log in to devices from the terminal server proxy.”)
Permission to view other users’ terminal proxy logs		You can view other users’ terminal access logs.
Permission to delete terminal proxy logs		You can delete terminal access logs. (Permissions associated with “Permission to view other users’ terminal proxy logs.”)

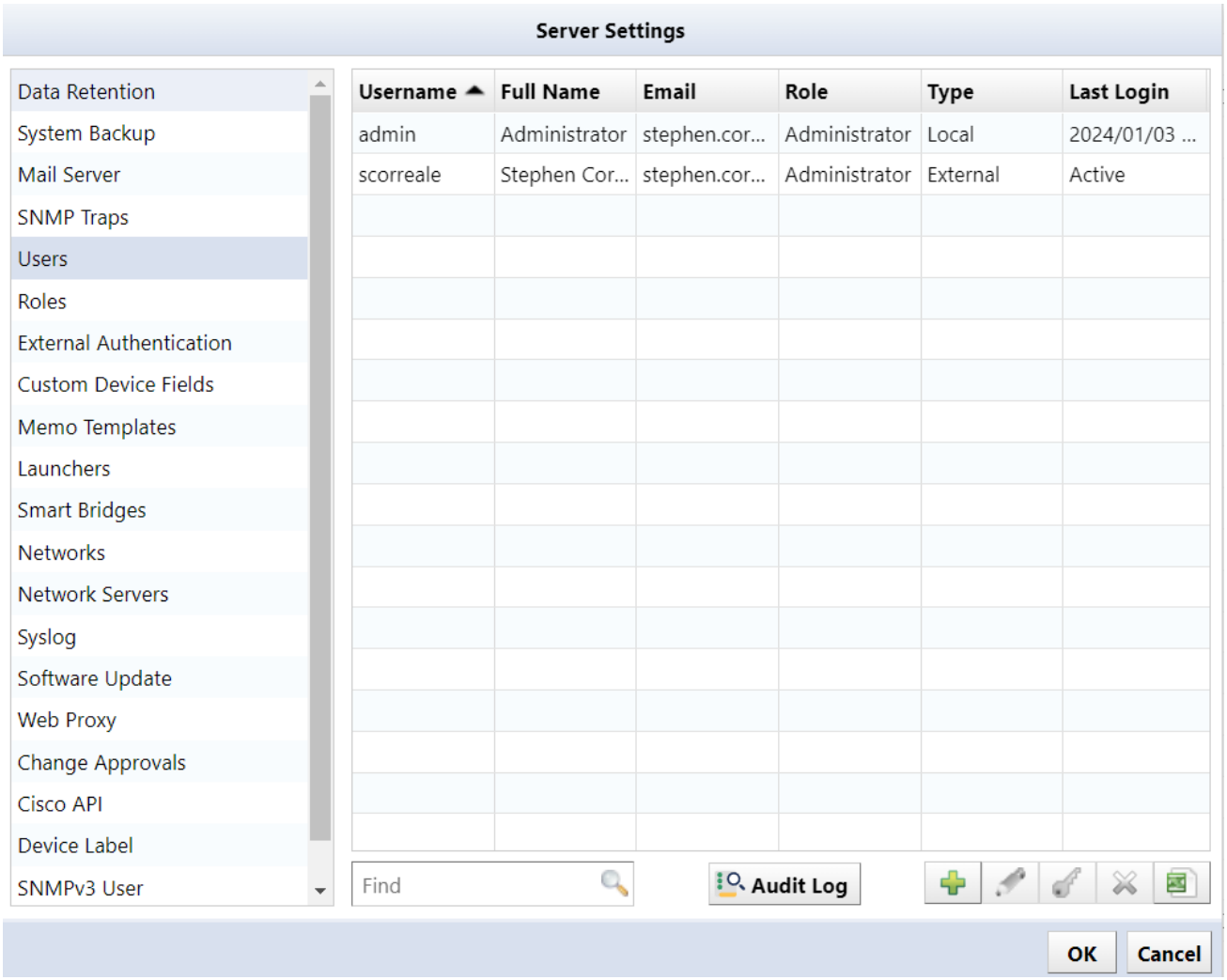
4. Click [OK].



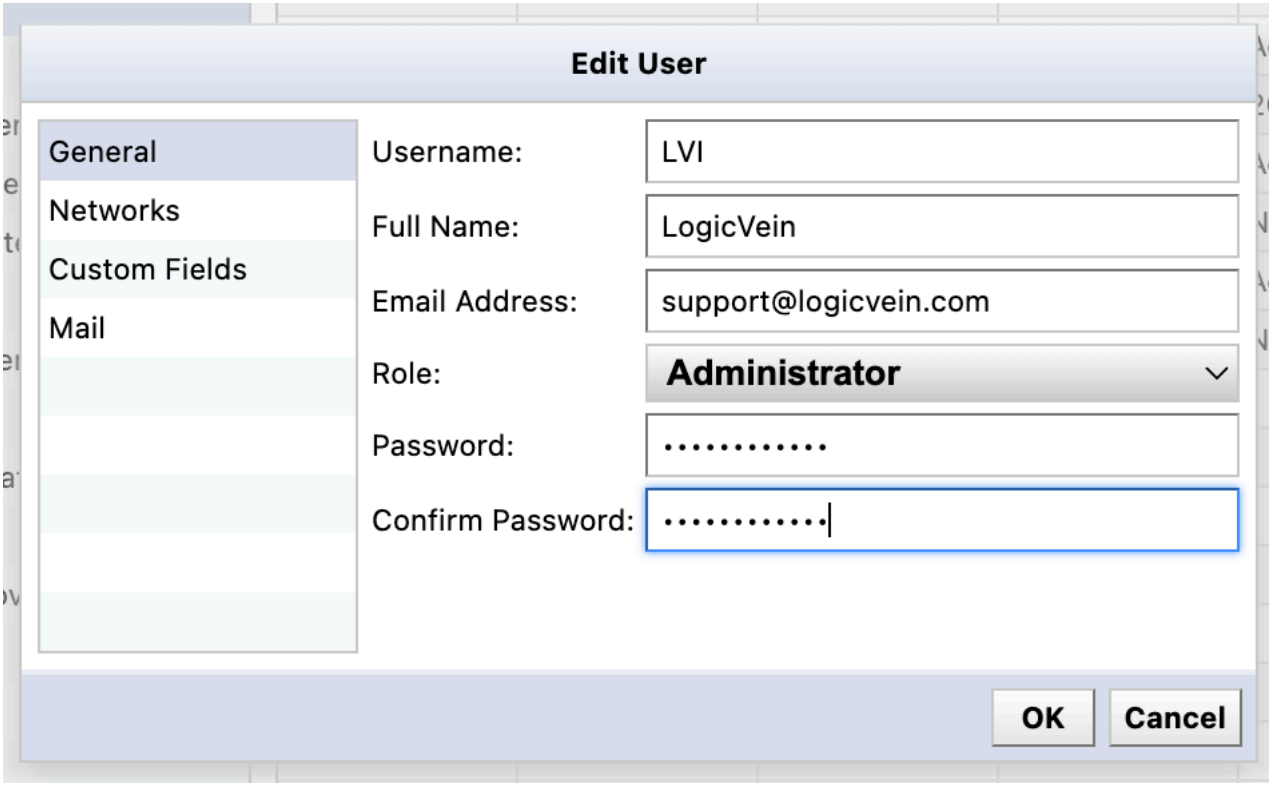
7.3 Add user

The “admin” user is pre-registered, and cannot be deleted.

1. Click the buton.



2. The user addition screen will be displayed. Enter the items and click [OK].

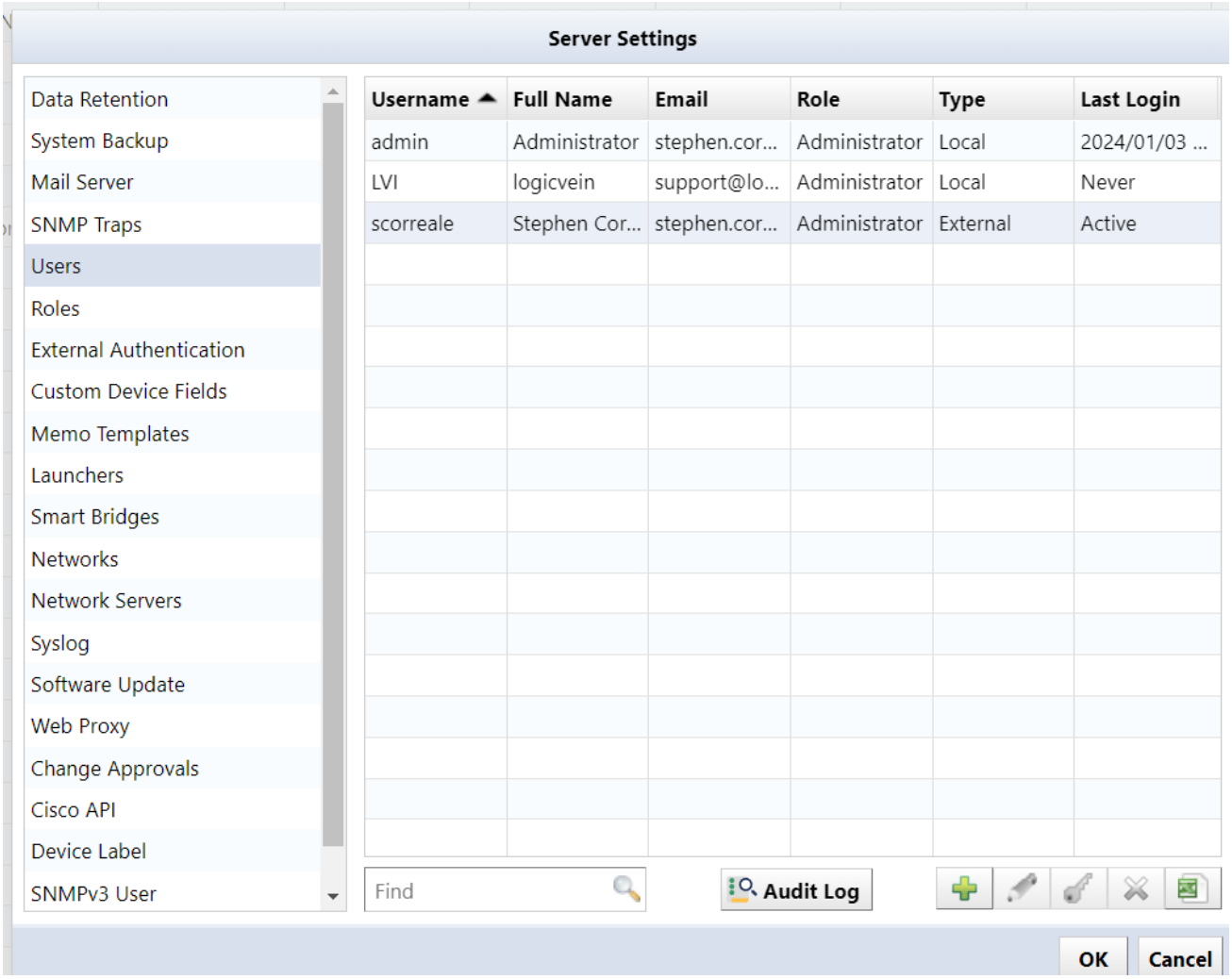


Item	Subitem	Explanation	Requirement
General	**Username**	Enter your username.	required
	Full Name	Enter the user's full name.	—
	Email	Enter the user's email address.	—
	Address		
	Role	Select the user's permissions. You can select the permissions set in "7.11.1 Add permissions" from the pull-down menu.	required
	Password	Set the user's password. To set a password, the following conditions must be met. - Must be at least 8 characters - Must not be a character string that is easy to guess	required

Item	Subitem	Explanation	Requirement
		(person’s name, proper noun, dictionary word, commonly used password) - Character strings that do not repeat the same characters or are arranged in an easy-to-understand manner	
Custom Fields	**Custom 1-5**	Select the custom device fields that users can view. *Displayed item names will change based on the settings in “7.15 Adding columns/changing column names for custom device fields”.	—
Networks	**Restrict user’s access Networks**	Determines whether this user has permission to see all managed networks configured within the system.	—
		A list of networks the user has been given access to. - When the “Restrict user” checkbox is unchecked, this table will be disabled, and no restriction is applied. The user will have permission to see all Managed Networks within the system. - When the “Restrict user” checkbox is checked, this	—

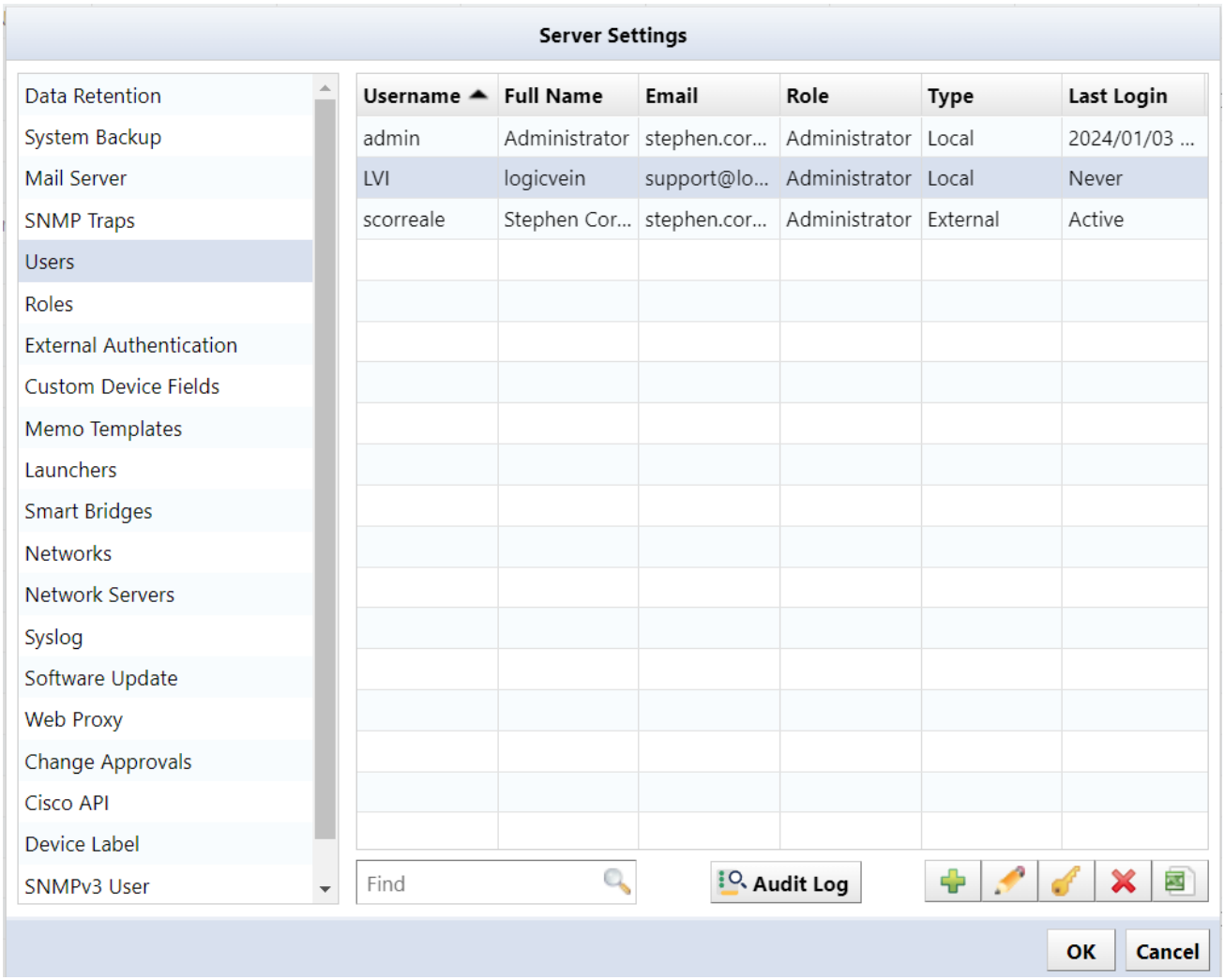
Item	Subitem	Explanation	Requirement
		table will be enabled, and the user will be configured to only have permission to the Managed Networks that are checked within this list.	
Mail	**Incident email**	Set this if you want to restrict incident emails by day of the week/time.	—

3. Click [OK].

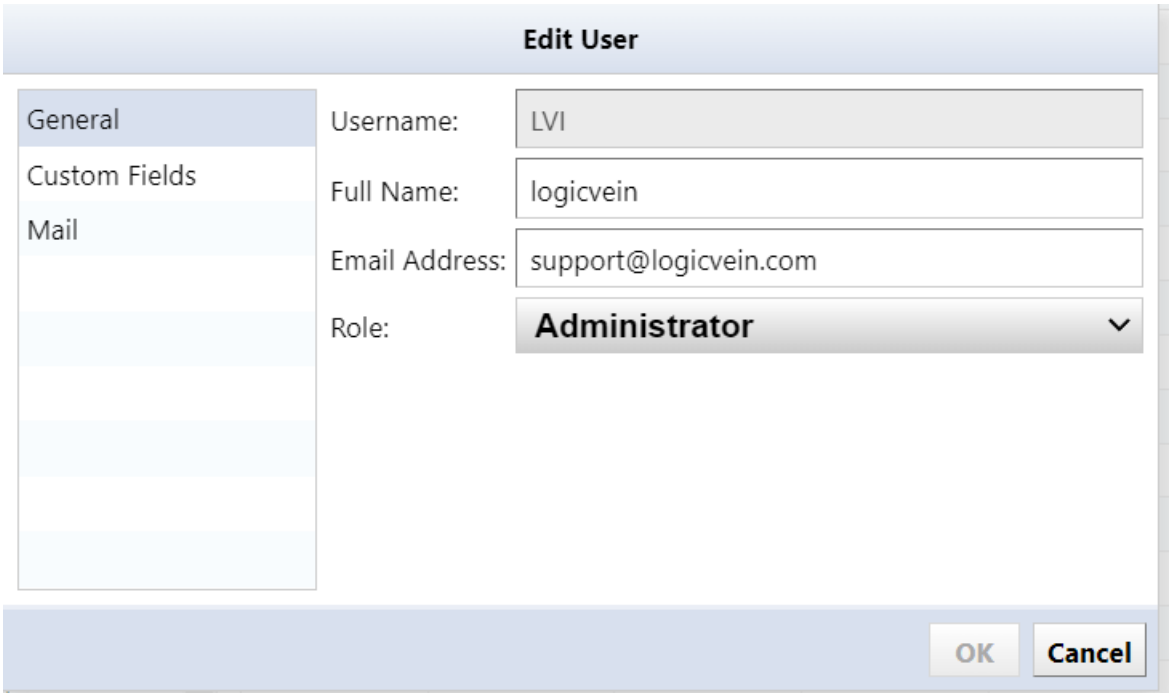


7.4 Change user information

1. Select the user you want to edit and click [Edit].



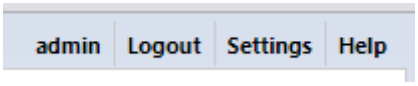
2. The user edit screen will be displayed. After editing, click [OK]. The Username cannot be changed. If you want to change your password, refer to the Change-password section below.



7.5 Change password

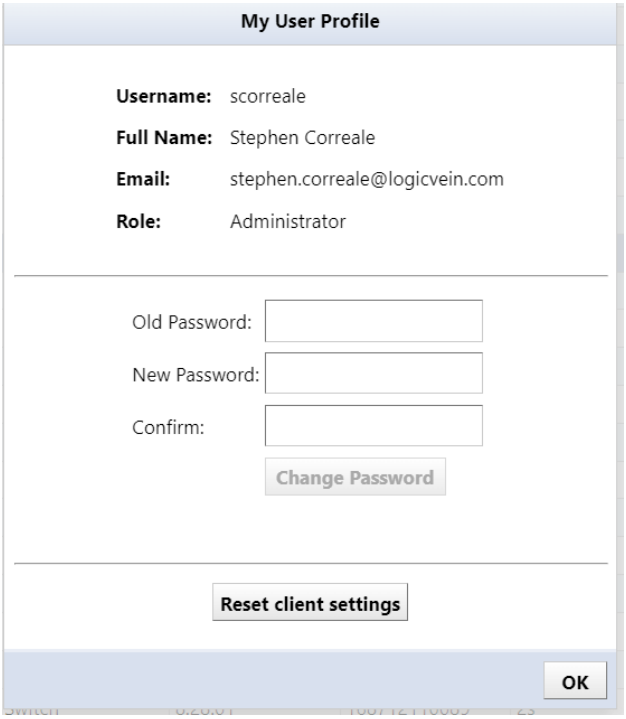
You can change your password from the login username in the Global Menu.

In this example, we are changing the password for the username “admin”.



1. Enter your new password in the [New Password] and [Retype Password] fields.
2. Click the Change password button to register the new password.

If the new password and the re-entered string are different, the Change password button will not be enabled.



Note

To set a password, the following conditions must be met:

- Must be at least 8 characters
- Must not be a character string that is easy to guess (person’s name, proper noun, dictionary word, commonly used password)
- Character strings that do not repeat the same characters or are arranged in an easy-to-understand manner

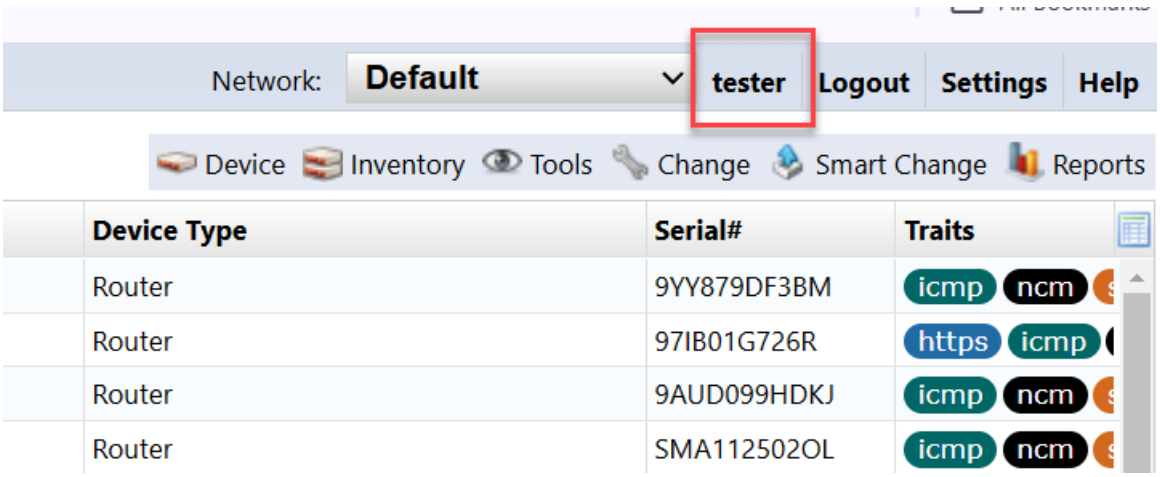
7.6 Setup two-factor authentication (2FA)

Two-factor authentication is a feature that enhances the security of user accounts by providing additional authentication with an authenticator app in addition to the password. Users can be optional, and administrators can set it to be mandatory for all users.

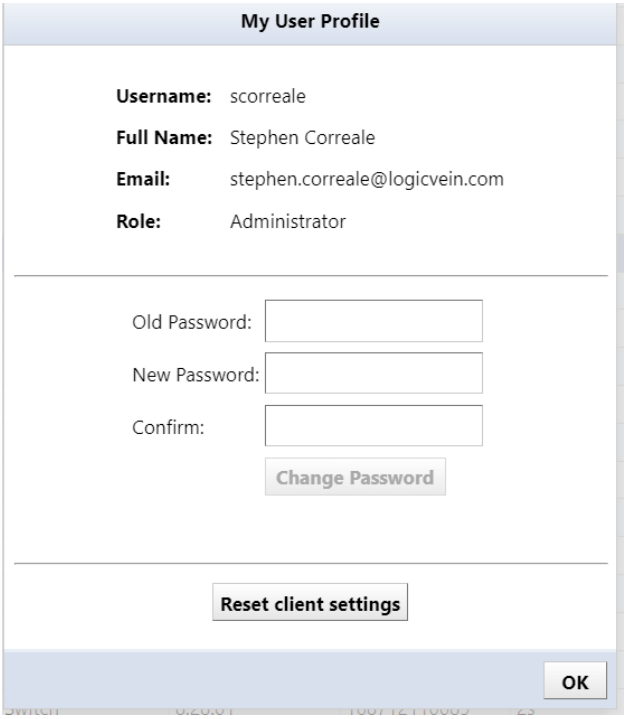
7.6.1 Enable two-factor authentication

If the user is logged in, you can setup two-factor authentication from the user profile dialog

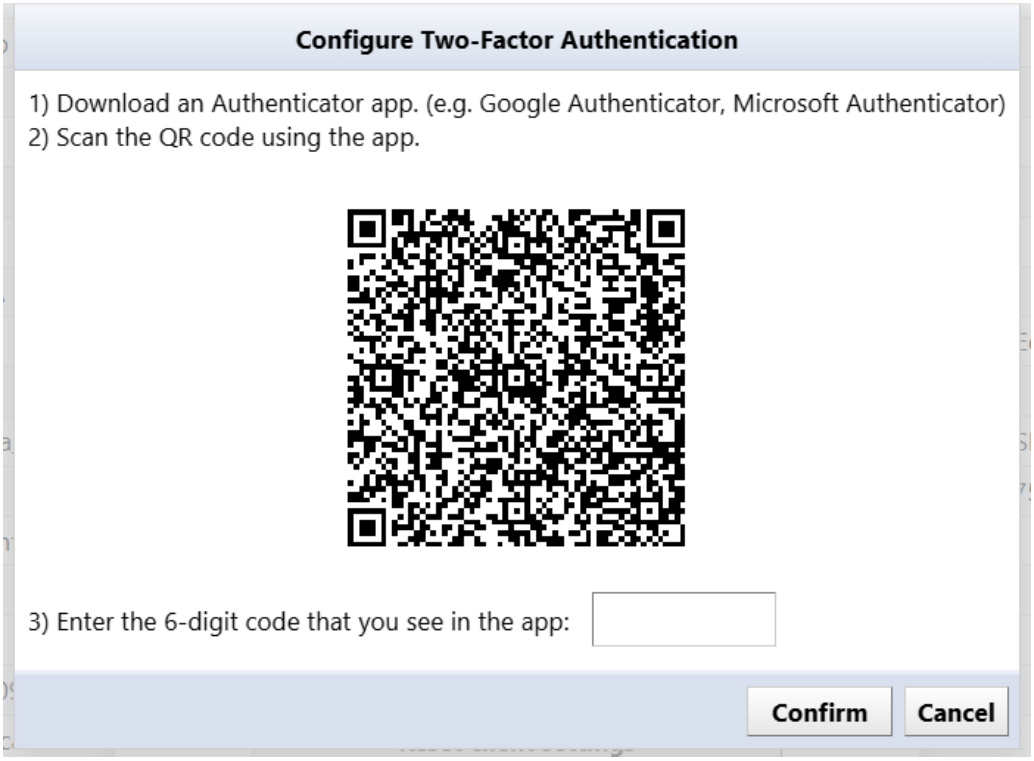
1. Click the username to open the User Profile dialog.



2. Click [Set up two-factor authentication]



3. Follow the onscreen instructions to set it up and enter the verification code.



4. Click [OK].

This completes the configuration. When you log out and log back in, you will be prompted to enter a verification code.

7.6.2 Remove two-factor authentication

If you want to cancel the two-factor authentication setting, you can do so while logged in.

If you are an admin user, you can unset two-factor authentication for all users

1. Open Settings > Users
2. Select the target user and click the [Key] button
3. Check “Remove two-factor authentication”, and click [OK]

> **Note**
>
> If two-factor authentication is not configured, “This user is not configured for two-factor authentication” is displayed, and this checkbox option is not displayed

5. In the Server Settings dialog, click [OK].

7.7 Configuring External Authentication

When you configure external authentication in {{ProductName}}, you can use an authentication server to log in to the product. This eliminates the need to create all user accounts in {{ProductName}} beforehand. Additionally, you can retrieve group information from the authentication server to automatically assign product rights and network browsing restrictions.

External Authentication can be configured by clicking [Server Settings] >[External Authentication]. On this page, you can configure protocol specific configuration settings and Group Mapping. You can tell {{ProductName}} which Role to assign to the user and which Managed Networks the user should be restricted to.

7.7.1 RADIUS

To integrate with a RADIUS server, {{ProductName}} sends an Access-Request for authentication. To configure this integration, set up {{ProductName}} to send Access-Accept with Filter-Id attached.

Below is a sample user configuration for FreeRADIUS:

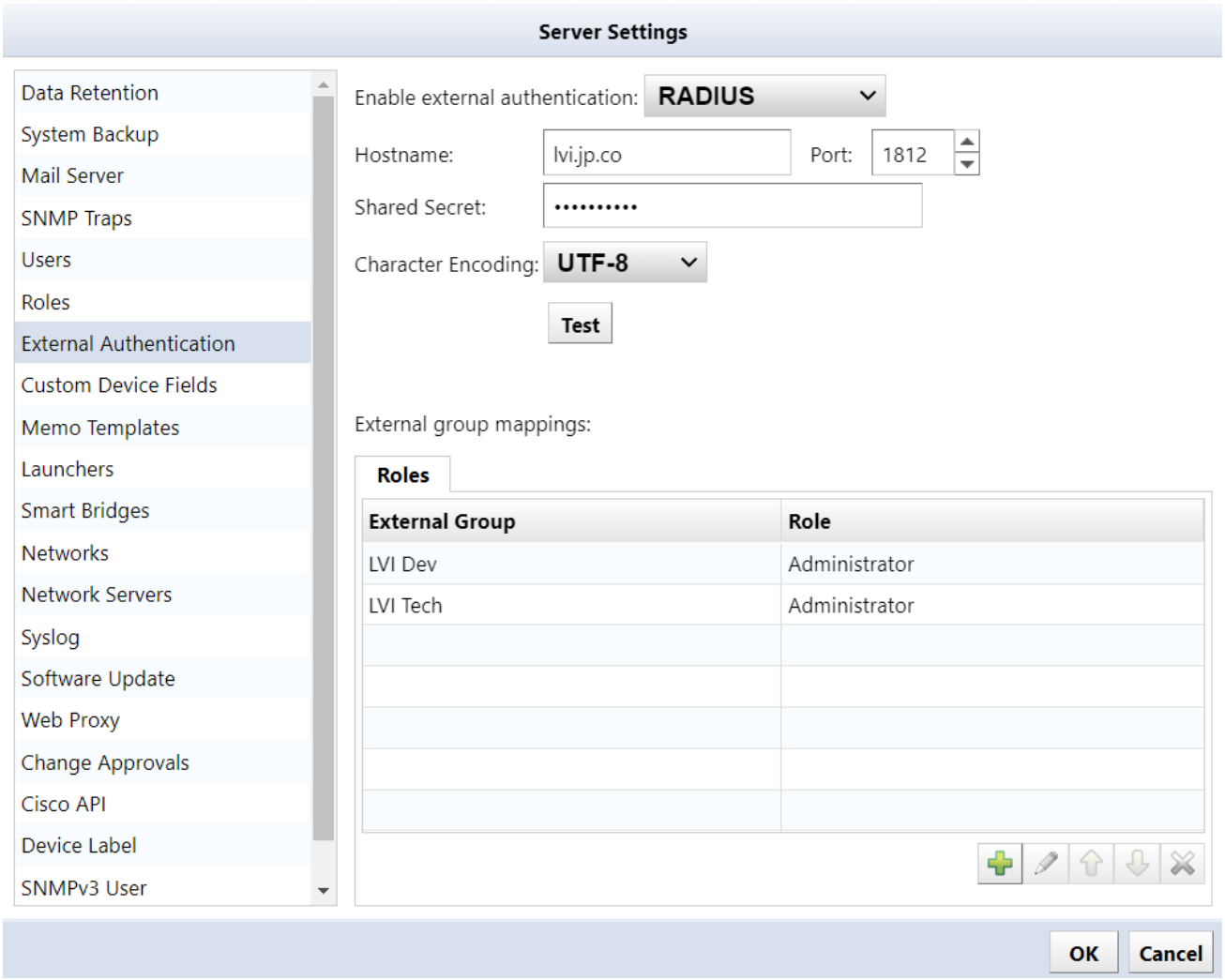
```
LogicVein Cleartext-Password: = "password"

Filter-Id += "GROUP"
```

With this configuration, when {{ProductName}} receives an Access-Request with the username "`LogicVein`" and the password "`password`", it sends Access-Accept with Filter-Id set. Filter-Id is used to designate the group to which the authenticated user belongs.

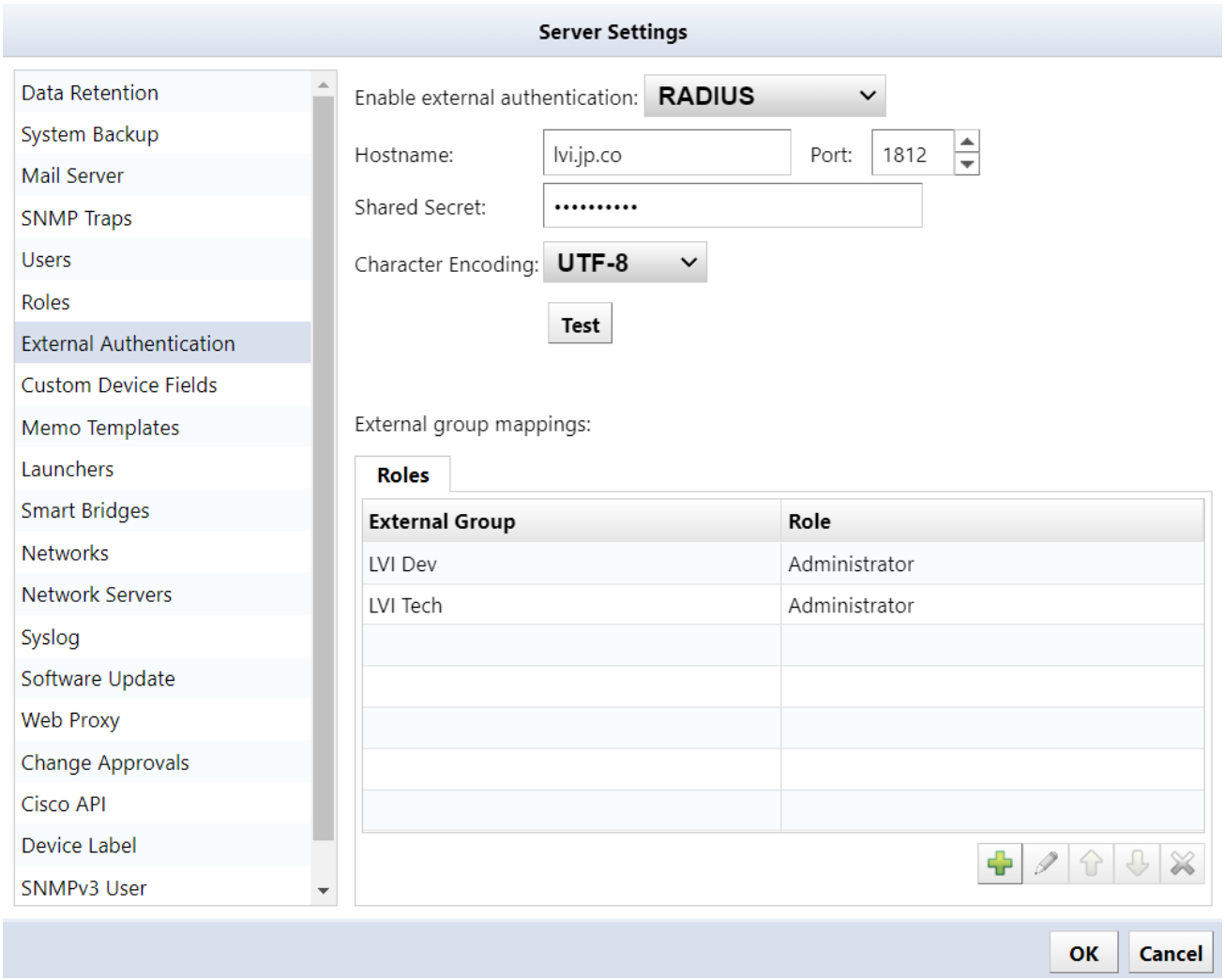
To configure external authentication:

1. Navigate to the Server Settings window in {{ProductName}}, and click [External Authentication].

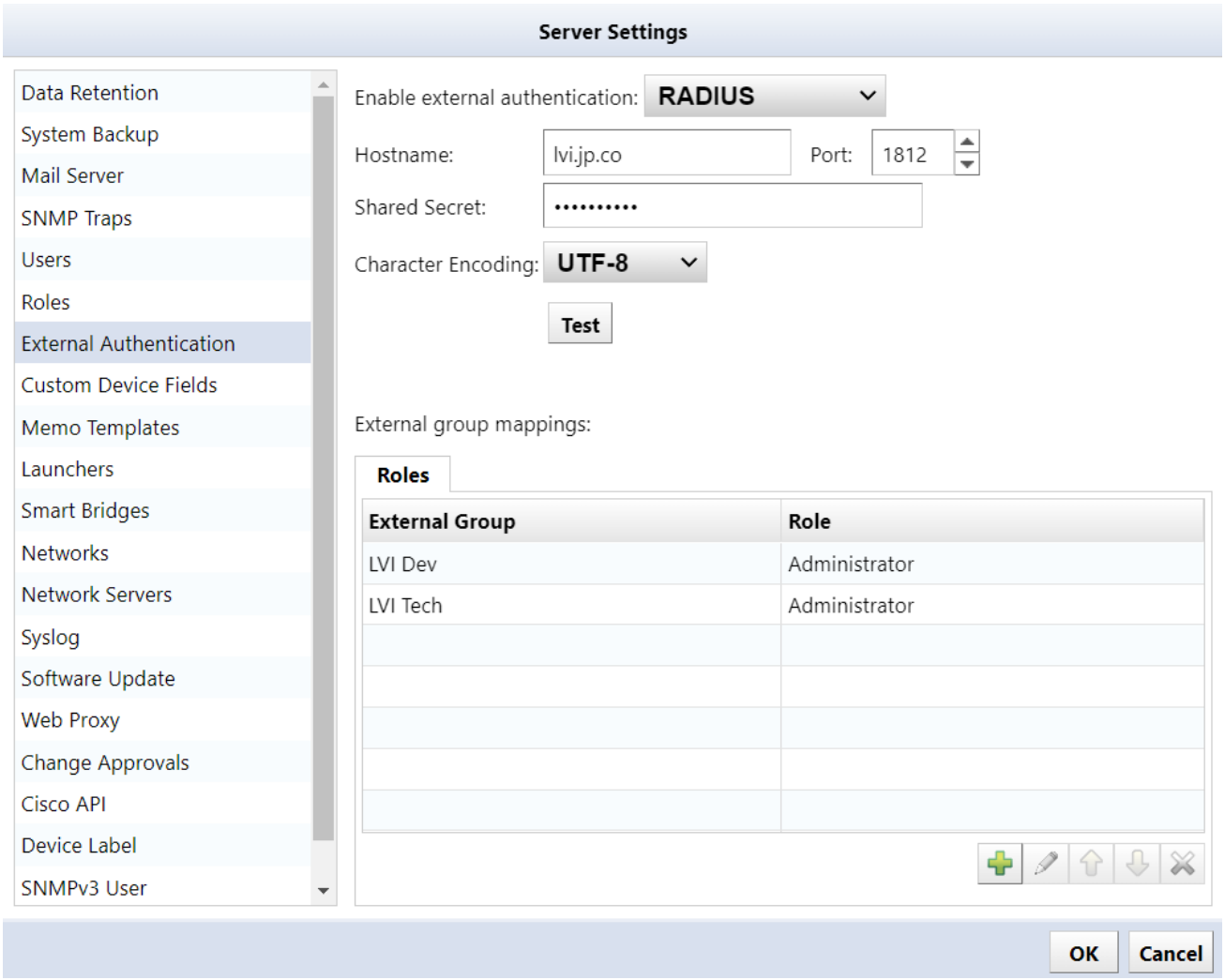
2. Change the [Enable external authentication] selection to “RADIUS”.



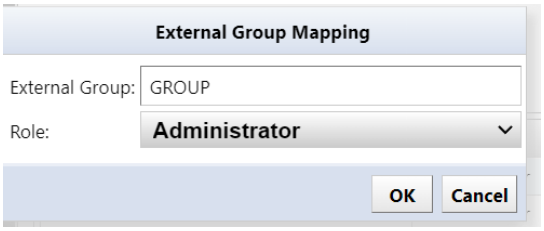
3. Set the RADIUS server's IP address (or hostname) and [Shared Secret].



4. Click the button to set permissions for external group mappings.



5. Input the RADIUS server's Filter-Id group settings into [External Group] and select "Role" for assignment.



The Active Directory RADIUS settings have now been successfully configured.

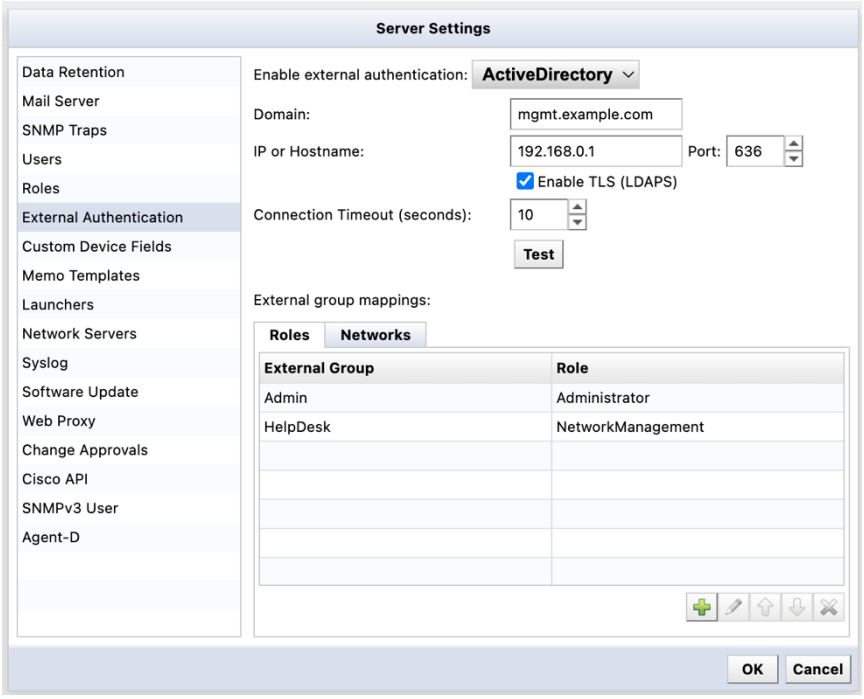
6. Click [OK] to save.
7. Click [Close] to exit the server settings.

After configuration, input a username and password in the Test Section, then click [Test] to confirm integration with the RADIUS server. If successful, "Authentication succeeded" will be displayed.

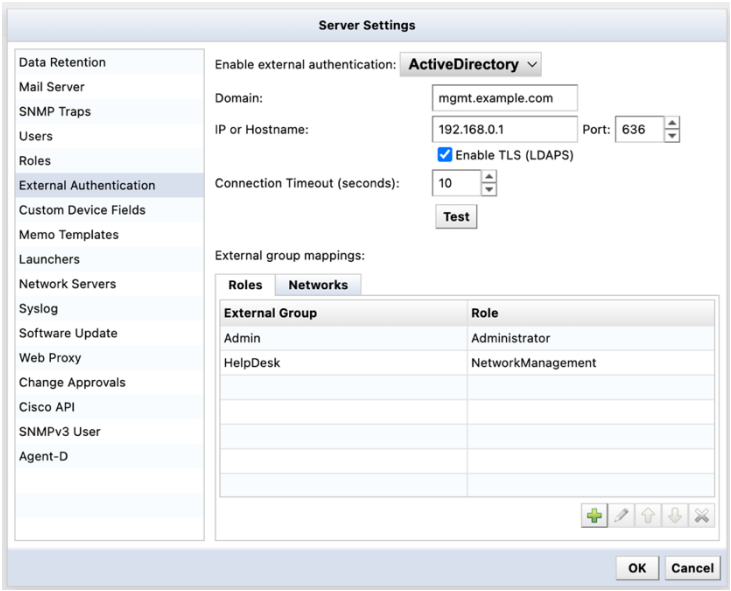
7.7.2 Active Directory

When integrating with an Active Directory server, the Roles and Managed Networks are determined using the groups to which registered users belong.

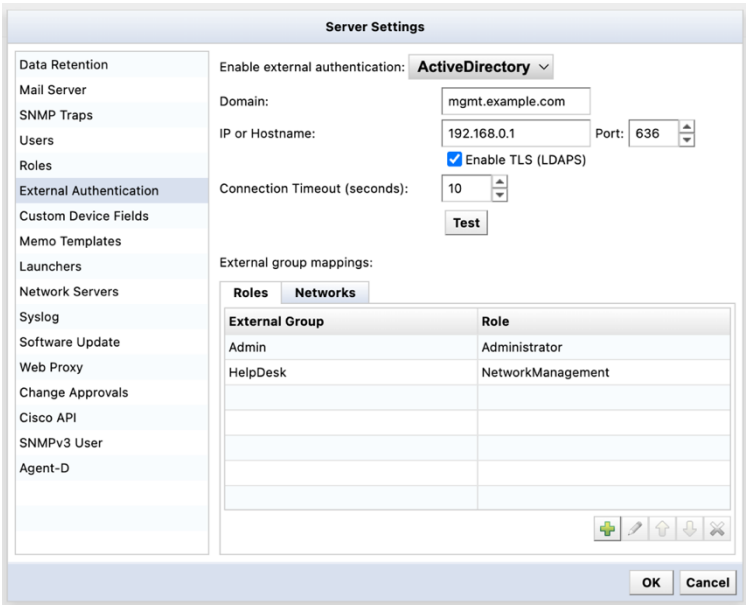
1. Navigate to the [Server Settings] window in {{ProductName}} and select [External Authentication].
2. Change [Enable external authentication] to Active Directory.



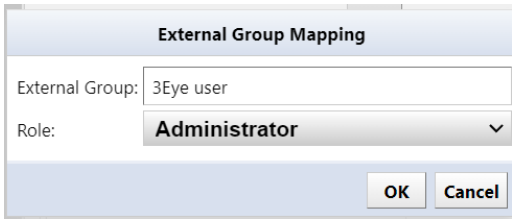
3. Set the domain name and the IP address (or host name) of the Active Directory server.



4. Add a new item using the button.



5. Enter the group to which the user belongs in [External group] and select the "Role" to be assigned.



The Active Directory settings have been successfully configured. Click [OK] to save the settings and log in using the user credentials configured on the Active Directory server.

7.7.3 SAML

By configuring SAML authentication with an external Identity Provider (IdP), you can enable Single Sign-On (SSO). This allows users to seamlessly log in to {{ProductName}} via the IdP.

7.7.3.1 Microsoft Entra ID Integration Prerequisites

Before configuring single sign-on, please make sure the following conditions are met:

- You can sign in to Microsoft Entra ID with administrator privileges.
- The users and groups to be linked exist in Microsoft Entra ID.
- You have the necessary permissions* to configure settings in {{ProductName}}.

*Administrator permissions or permissions to “allow security settings”.

Procedure

Configure SAML 1. Log in to {{ProductName}}.

2. Open Settings > [External Authentication].
3. Select “SAML” from [Enable external authentication] dropdown menu.
4. Verify that [Callback URL] is the correct URL for the {{ProductName}} server.

The format for the callback URL is: `https://[IP address or hostname]/auth`

By default, it refers to the value in [Network Servers] > [Hostname/IP Address].

5. Click the [Download LogicVein SAML Service Provider Metadata XML] link to download the Metadata XML file.

File name: `LogicVein-saml-sp-metadata.xml`

The downloaded file will be used in the next step.

Create a new application

1. Sign in to the Microsoft Entra Admin Center.
2. Click [Identity] > [Applications] > [Enterprise Applications].
3. Click [New Application].
4. Click [Create your own application].
5. Set a name for the app, select [Integrate any other application you don't find in the gallery (Non-gallery)], and click [Create].
6. Click [Manage] > [Single Sign-On].
7. On the [Select a Single Sign-On Method] page, click SAML.
8. On Set up Single Sign-On with SAML. Click [Upload metadata file], and upload the downloaded ed `logicVein-saml-sp-metadata.xml` file.
9. Click [Add].
10. Ensure that the fields for @Identifier","Reply URL", and "Logout URL" contain the callback URL configured in the {{ProductName}} server settings.
11. Click [Save].
12. Click the  button to exit the window.

(If the pop-up message "Test Single Sign-On" appears, click [No, I"ll test it later].)

13. In the [Attributes and Claims] section, click [Edit].
14. On the [Attributes and Claims] page, select [Add a group claim].
15. Select the [Security Group] option and select "Group ID" in [Source Attribute]. (If you prefer to use display names instead of Group IDs in the {{ProductName}} "External Group Mapping" configuration, select "Cloud-only group display names")
16. Click [Save].
17. Click the  button to close the [Attributes and Claims] page.

Obtain IdP Metadata

1. In the [SAML Certificates] section, click [Download] under [Federation Metadata XML].
2. Download the IdP metadata XML file.
3. On the [Set up Single Sign-On with SAML] page, locate [Federation Metadata XML] under the [SAML Signing Certificate] section and select [Download] to download and save the certificate to your computer.

Register the Application in {{ProductName}}

1. Open Settings > [External Authentication].
2. Click [Upload IdP metadata XML] and select the XML file created in the “Get IdP metadata” step.
3. Click [OK] to save.

Note the object ID

1. Return to the Microsoft Entra admin center and click [Manage] > [Users and Groups].
2. Click [Add user or group].
3. Click [None selected] in the [Users] section.
4. Select the users who need to be allowed to log in to {{ProductName}} from the list.
5. Click [Select].
6. Click [Assign] to complete the user assignment.
7. In the left sidebar, click [Identity] > [Groups] > [All groups].
8. Note the [Object ID] of the groups allowed to log in to {{ProductName}}.

Configure external group mapping

1. Open Settings > [External Authentication].
2. On the [External Group Mapping] screen, click  button.
3. In the [External Group] field, enter the “Object ID” noted in the previous steps.
4. Specify the permissions to be assigned in the [Permissions] field, and click [OK]. (If you chose “Cloud-only group display names” in Entra Application “Attributes & Claims” configuration, enter the name of the group instead of “Object ID”.)
5. Click [OK] and save the [Server Settings].
6. Click Log out. You will be redirected to the Microsoft login page.

7.7.3.2 Okta Integration Prerequisites

Before configuring single sign-on, make sure the following conditions are met.

- You can sign in to the Okta dashboard with administrator privileges
- The users and groups to be integrated exist in Okta
- You have the permission* to configure settings in {{ProductName}}.

  *Administrator privileges or the permission to “Allow security settings.

Configure SAML

1. Log in to {{ProductName}}.
2. Open Settings > [External Authentication].
3. Select “SAML” from [Enable external authentication].
4. Make sure that [Callback URL] is the correct URL for your server.

By default, it refers to the value of [Network Servers] > [Hostname/IP Address].

5. Click the [Download LogicVein SAML Service Provider Certificate] link to download the certificate file.

File name: `LogicVein-saml-sp-signing-certificate.crt`

The downloaded file will be used in the next step.

Create a new application

1. In the Okta Admin Console, open [Applications] > [Applications].
2. Click [Create App Integration].
3. Select “SAML 2.0” as the Sign-in method and click [Next].
4. Enter a name for your App name and click [Next].
5. In the General section of SAML Settings, configure the following:

Item	Explanation
Single sign-on URL	https://[IP address or Hostname]/auth?client_name=SAML2Client
Audience URI (SP Entity ID)	https://[IP address or Hostname]/auth
Application username	mail
Update application username on	create and update

6. Click [Show Advanced Settings].
7. In [Signature Certificate], click [Browse files…] and select the SP certificate the downloaded file.

File name: `LogicVein-saml-sp-signing-certificate.crt`.

8. Set the following items:

Item	Explanation
Enable Single Logout	Enable “Allow application to initiate Single Logout”
Single Logout URL	https://[IP address or Hostname]
SP Issuer	https://[IP address or Hostname]/auth

9. In the [Attribute Statements] (optional) section, add the following two items:

Item 1:

Item	Explanation
Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name format	Refer URI
Value	user.email

Item 2:

Item	Explanation
Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Name format	Refer URI
Value	user.lastName

10. In the [Group Attribute Statements] (optional) section, set the following:

Item	Explanation
Name	http://schemas.logicvein.com/ws/2024/05/identity/claims/groups
Name format	Refer URI
Filter	Matches with regex expression `.*`

11. Click [Next].
12. Select “I”m an Okta customer adding an internal app”.
13. Select “It”s required to contact the vendor to enable SAML”.
14. Click [Finish].

Assigning groups to use the application

1. Select the [Assignments] tab of your application.
2. Select [Assign] > [Assign to Groups].
3. Find the group you want to assign and click the [Assign].
4. Click [Done].

Get IdP metadata

1. Click the [Sign On] tab.
2. Copy the Metadata URL in Settings.
3. Open a new tab in your browser and paste the URL in the address bar to access it.
4. Right-click the metadata page and select [Save As…].
5. Save the metadata as an .xml file.
6. You will use the downloaded file in the next step.

Register application with {{ProductName}}

1. Open {{ProductName}} Settings > [External Authentication].
2. Click [Upload IdP Metadata XML] and select the XML file created in step “Get IdP Metadata”.

Configure external group mapping

1. Open Settings > [External Authentication].
2. In External Group Mapping, click  button.
3. Enter the Okta group in the External Group field, specify the permissions you want to assign in [Permissions] and click [OK.]
4. Click [OK].

Log in to {{ProuctName}}

Log in to {{ProuctName}} as an Okta user.

After completing the settings described in **Okta Integration**, the Okta sign-on screen will be displayed when you access {{ProuctName}}.

7.7.3.3 Keycloak Integration Prerequisites

Before configuring single sign-on, make sure the following conditions are met.

- You can sign in to the Keycloak dashboard with administrator privileges
- The users and groups to be integrated exist in Keycloak.
- You have the permission* to configure settings in {{ProdcutName}}.

  *Administrator privileges or the permission to “Allow security settings”.

Configuaring SAML with Keycloak

Keycloak can be run with docker:

```
docker run -d --name keycloak \
  -p 8080:8080 \
  -e KEYCLOAK_ADMIN=admin \
  -e KEYCLOAK_ADMIN_PASSWORD=admin \
  quay.io/keycloak/keycloak:25.0.6-0 start-dev
```

1. Enter username “`KEYCLOAK_ADMIN`” and password “`KEYCLOAK_ADMIN_PASSWORD`” when you login to Keycloak.

Use following command to follow Keycloak logs and debug any authentication issues:

```
docker logs -f keycloak
```

2. Go to `http://localhost:8080/` and log in with username “`admin`” and password “`admin`”.
3. Go to [Clients] > [Create Client].
4. Enter “Client ID” and “Name”.

Client ID is: https:///auth

You can select any name (e.g. “{{ProductName}}”).

5. Click [Next] and add a callback URL

The callback URL should be: https:///auth?client_name=SAML2Client

e.g. https://192.168.0.93/auth?client_name=SAML2Client>

6. Click [Save].
7. Click the [Client Scopes] tab.
8. Click [https:///auth-dedicated].
9. Click [Add Predefined Mapper].
10. Select [X500 email] and click [Add].
11. Click “X500 email”.

Set “`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`” as the [SAML Attribute Name].

Set [SAML Attribute NameFormat] to “`URI Reference`”.

12. Click [Save].
13. Click [Client Scopes] in the left sidebar and then click [Role List] in the “Name” column.
14. Click the [Mappers] tab then click [Role List] in the “Name” column.

Set [Role attribute name] to “`http://schemas.logicvein.com/ws/2024/05/identity/claims/groups`”.

Set [SAML Attribute NameFormat] to “`URI Reference`”.

15. Click [Save].
16. Click [Users] in the left sidebar.
17. Click [admin] in the [Username] column and set an email address.
18. Click [Save].
19. Click [Clients] in the left sidebar and click [`https://192.168.0.93/auth`] in the client list.
20. Click the [Advanced] tab.

Set Logout Service POST Binding URL to “https:///”

(e.g. https://192.168.0.93/>)

21. Click the [Keys] tab.
22. Turn “Client signature required” off and back on.
23. In the pop-up window, select [Import].
24. Set the “Archive format” to “Certificate PEM”
25. Download the “LogicVein SAML Service Provider Certificate” from the NetLD SAML External Authentication page, upload it here. (You can view the upload certificate in a text editor.)
26. Click [Confirm].

(You can view the upload certificate in a text editor.)

> **Note**
>
> Please make sure it is the new certificate shown in the textbox to ensure UI compatibility (Last tested version: keycloak:25.0.6-0)

27. Click [Realm Settings] in the left sidebar, and click [Save] to download the

SAML 2.0 Identity Provider Metadata file.

28. Upload the SAML 2.0 Identity Provider Metadata file to [NetLD SAML Upload IDP Metadata XML].
29. Log out of {{ProductName}} to be redirected to Keycloak for SSO Login.

7.7.4 Use Local Authentication After Setting Up SAML Authentication

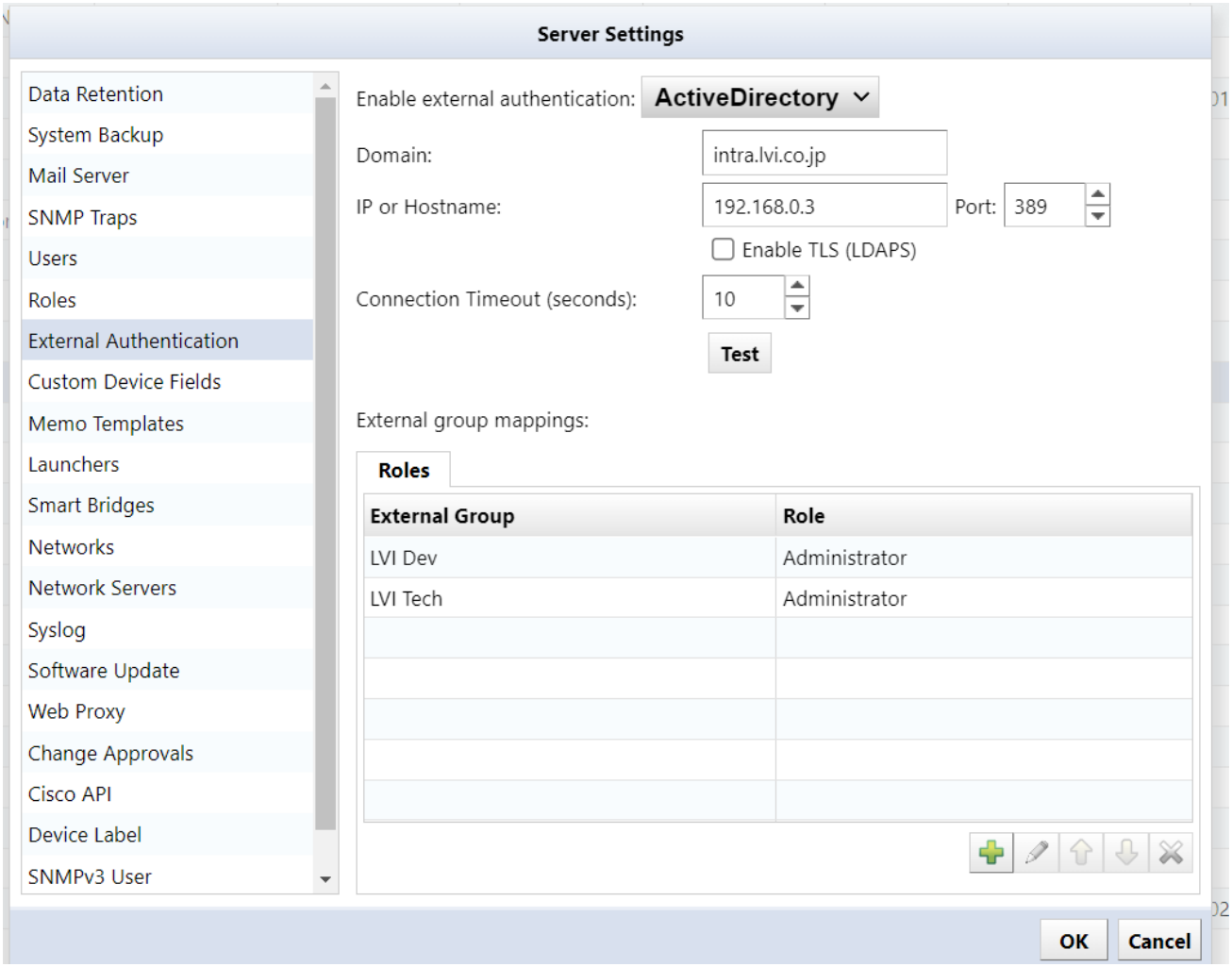
After completing the SAML authentication setup, when you access a NetLD product page, the linked sign-in page will be displayed. If you want to log in to the product using local authentication instead of SAML authentication, add the variable `"/?forceLoginPage=true"` to the end of the URL to access it:

`https://[IP address or Hostname]/?forceLoginPage=true`

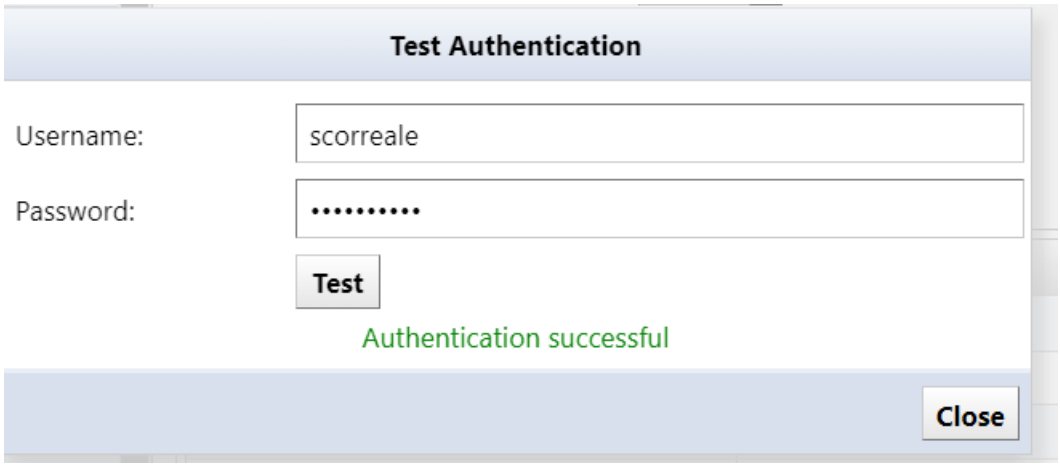
When you open the URL with the variable added, the product's login page will be displayed. You can log in with a local account such as admin.

7.7.5 Testing external authentication

After configuring external authentication, you can test external authentication from [Test].



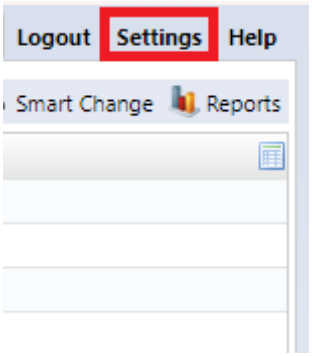
When the [Authentication Test] dialog appears, enter the [Username] and [Password] to test authentication, and click [Test]. If the authentication is successful, the message “Authentication was successful” will be displayed as shown below.



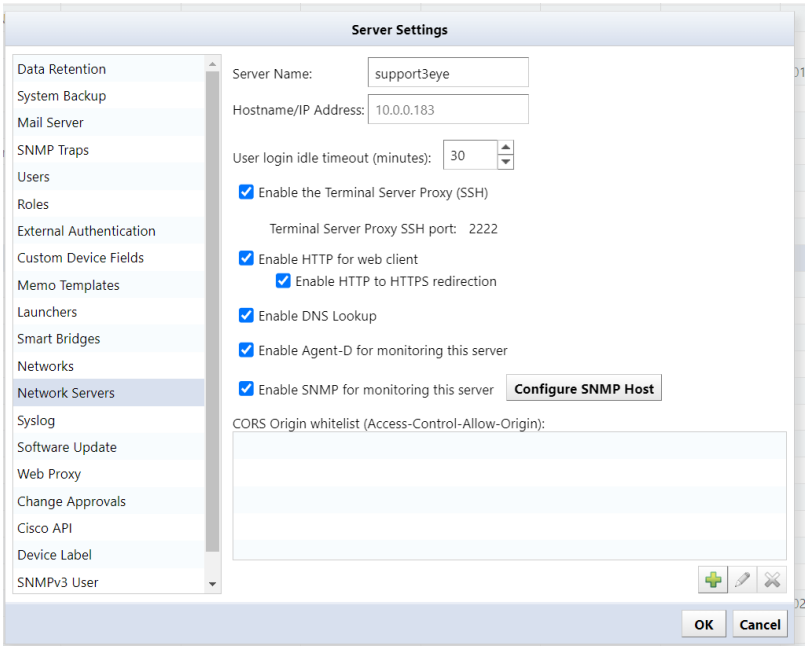
7.8 Set session timeout for users

{{ProductName}} requires users to re-authenticate after 30 minutes of inactivity. To change this time, follow the steps below:

1. Click Settings on the Global Menu.



2. Click [Network Server] and change the “User Login Idle Timeout” time. Settable range: `10` to `525600` (minutes)



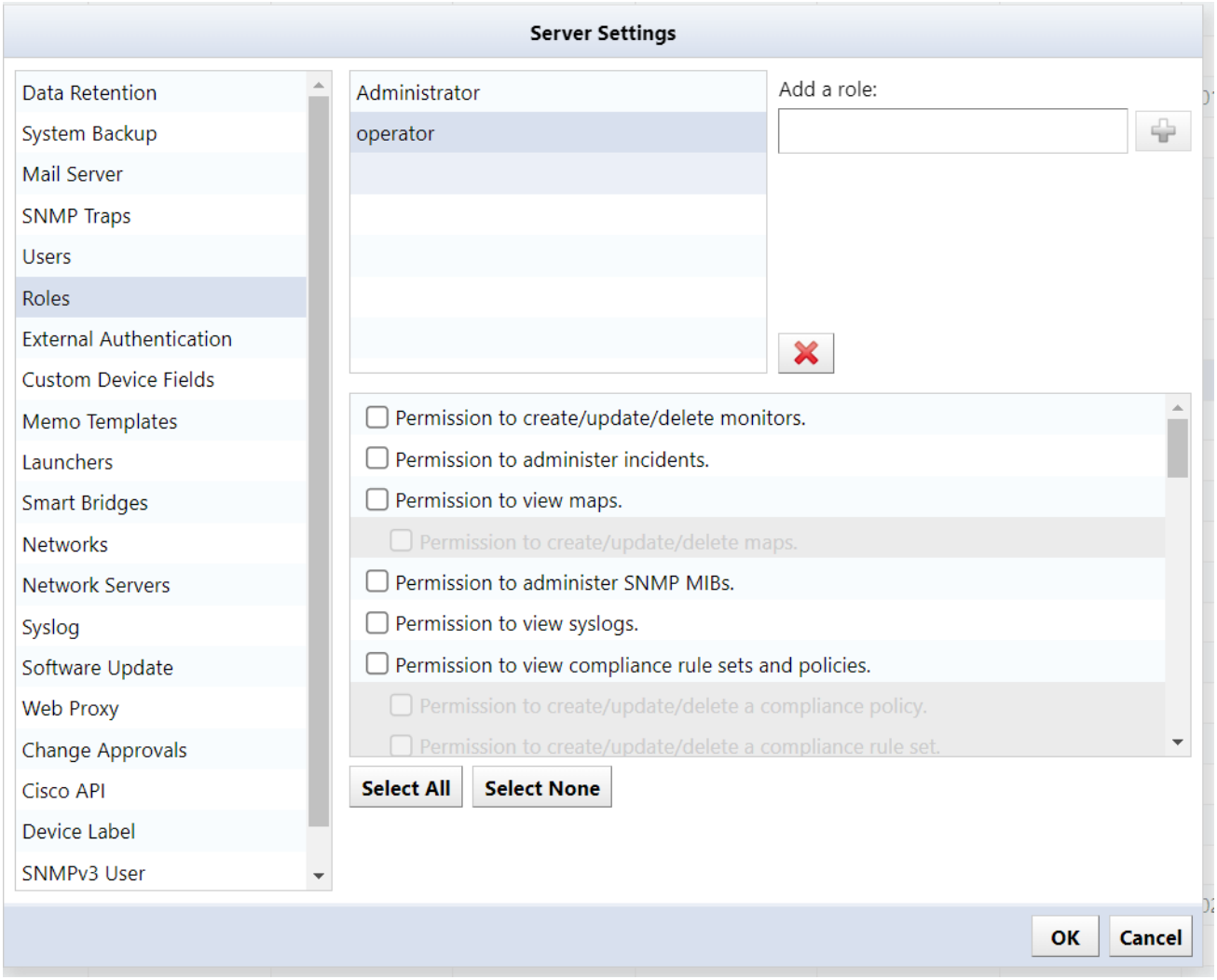
3. Click [OK].

For the settings to take effect, you must log out of ThirdEye and log in again.

4. Log out and log back in.

7.9 Remove permissions

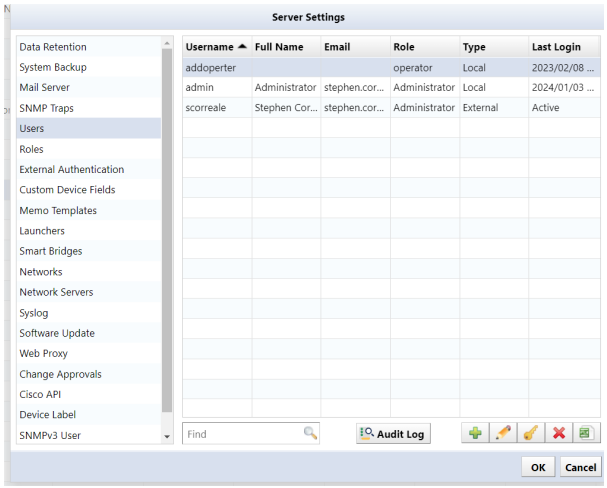
3. Select the authority name you want to delete and click  .



4. Click [OK] on the server settings.

7.10 Delete user

1. Select the user you want to delete and click the  button.



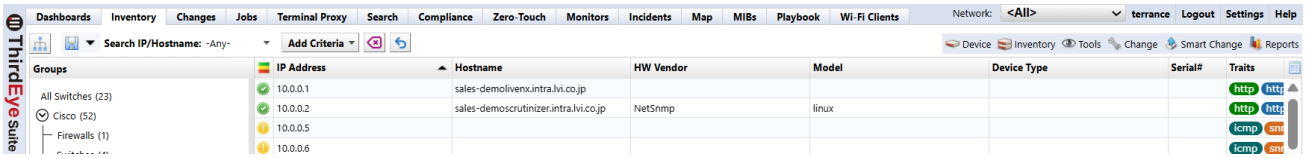
The user will be deleted.

]2. Click [OK] on the server settings.

If you delete a user by mistake, click [Cancel].

8 Main tabs

ThirdEye interface provides manages networks through 13 main tabs:



Tab	Edition	Explanation
Dashboard		View the dashboard
Inventory		Displays registered devices as an inventory (list).
Changes		View the configuration change history.
Jobs		Display a list of jobs.
Terminal Proxy		Displays a list of records when connecting to a device with a terminal.
Search		You can perform switch port searches, ARP searches, and interface searches.
Compliance	Suite	Configuring the device.
Zero-Touch	Suite	Display a list of incidents.
Monitors		Configure monitoring settings.
Incident		Display a list of incidents.
Map		Show map. Maps lets you create, edit, and delete maps.
MIBs		Search and view MIB.
Playbook		Configure automation workflow settings for network operations.
Wi-Fi Clients		Configure wireless client monitoring

8.1 Dashboards

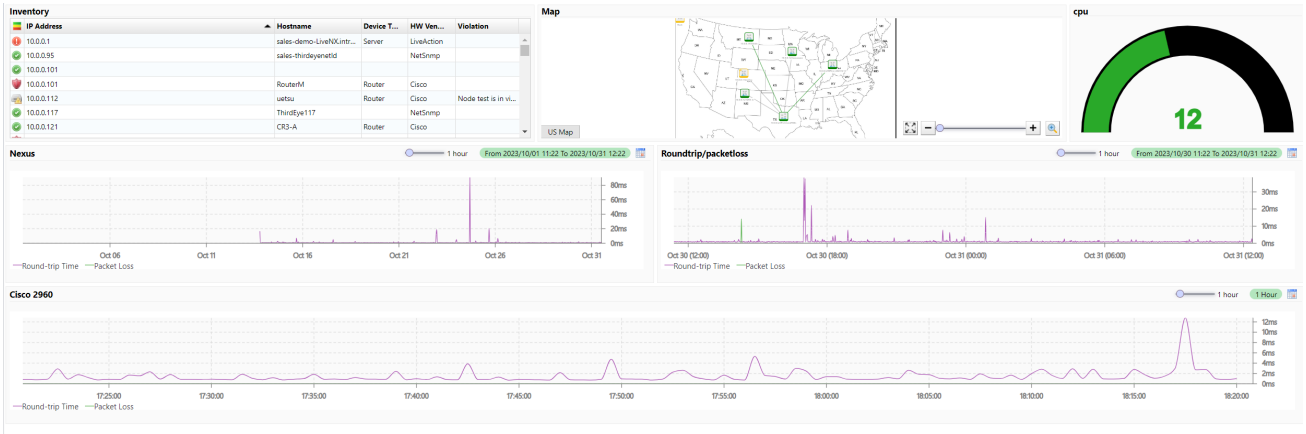
The Dashboards tab is an interface that allows you to configure a single monitoring screen by embedding various items. Each embedded item is called a Widget. By adding widgets to your dashboard, you can more quickly access information.

Users can create new dashboards and add and rearrange widgets.

On the Dashboard tab you can:

- Create new dashboards
- Add and rearrange widgets
- Combine multiple widgets (inventory lists, gauges, histograms, maps, violation tables)
- Display both real-time and historical data
- Arrange components through drag-and-drop
- Share dashboards across teams or keep them private

8.1.1 Dashboard screen components



Item	Explanation
Main screen	The entirety of the screen being displayed.
Main tab	This name of the current Dashboard is shown in the upper left (“Inventory” in the example above). The Dashboard can be changed by clicking the Dashboard [“Name”] to show the dropdown menu, and selecting a different Dashboard. At the bottom of the dropdown menu, Dashboards can be edited by clicking the [Manage Dashboards..] button.
Global Menu	This is the fixed menu that is always visible at the top right of the screen. (“schedule”, “date,”export” in the example above)

8.1.2 Dashboard edit menu

On the Dashboard screen, the [schedule], [date], [export], and [edit] buttons are displayed by default:

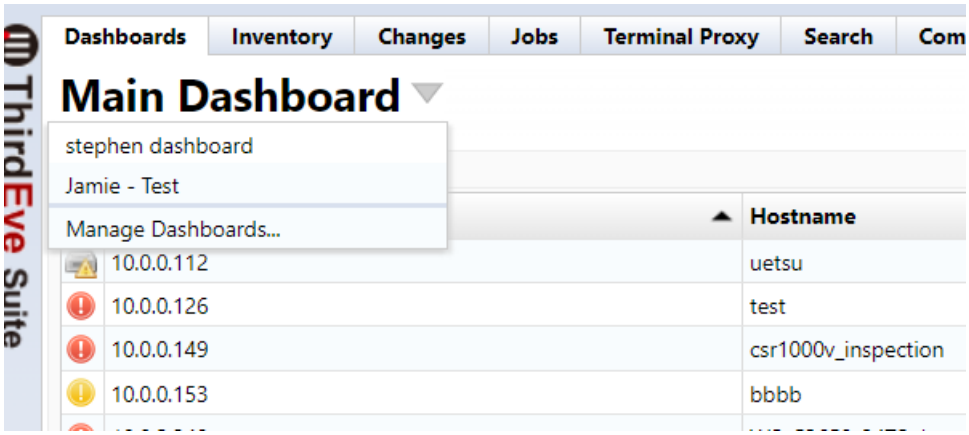
Button	Explanation
schedule	Schedule a PDF report of your dashboard to be emailed. Schedule applies to “Inventory” and “Line Graph” widgets.
date	You can change the display period of line graphs on the dashboard all at once. Date applies to the “line graph” widget.
export	Create a PDF report of the dashboard you are viewing. Export is for “Inventory” and “Line Graph” widgets.
edit	Go to edit mode for the dashboard.

Once you click [edit], additonal buttons are displayed:

Additional buttons	Explanation
keep	Save your dashboard changes and return from edit mode.
discard changes	Aborts dashboard edit mode.
⊕	Add widgets to your dashboard.

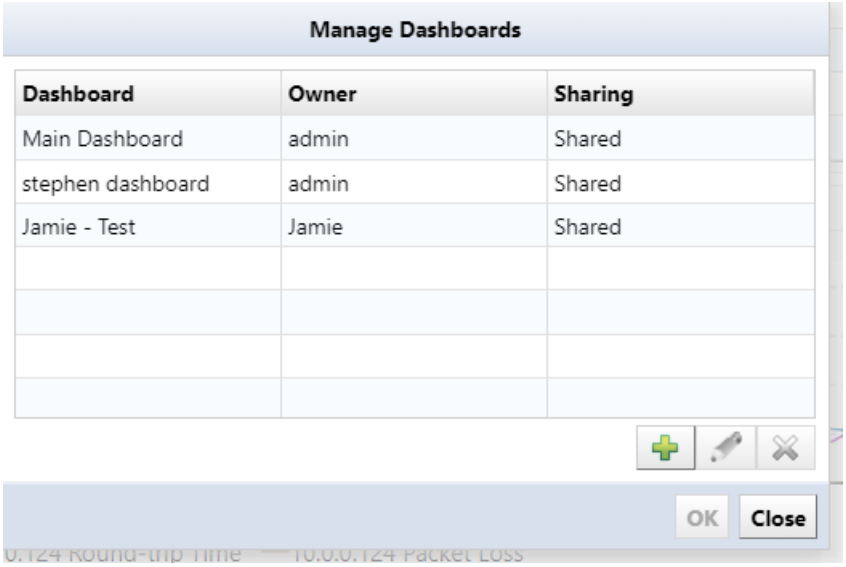
8.1.3 Add a Dashboard

1. Click the Dashboard name (“Main Dashboard” in the image below), and select [Manage Dashboard].

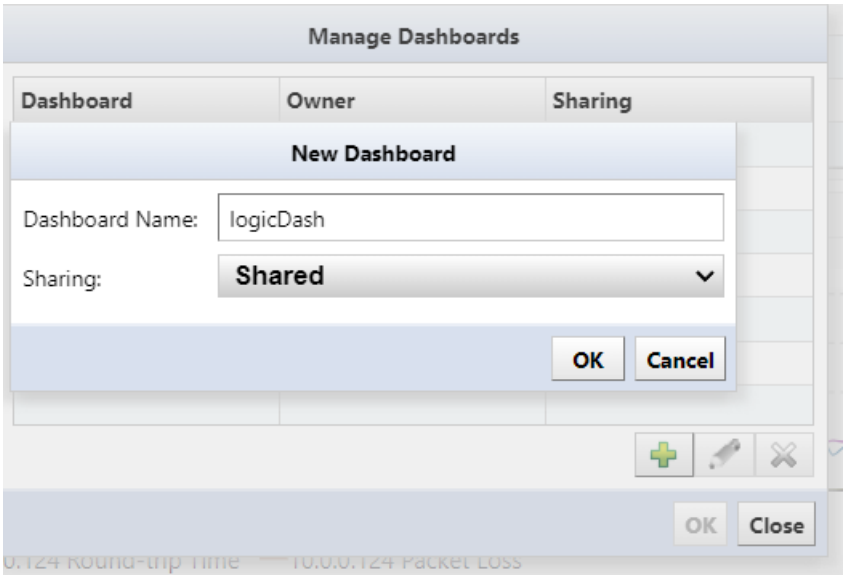


> **Note**
>
> If the current user can view more than one Managed Network, this screen will also include the option to explicitly select which Managed Networks the dashboard is associated with. The Managed Network will then impact which other users can view the dashboard. A user must have access to every Managed Networks associated with the dashboard to have access to it.

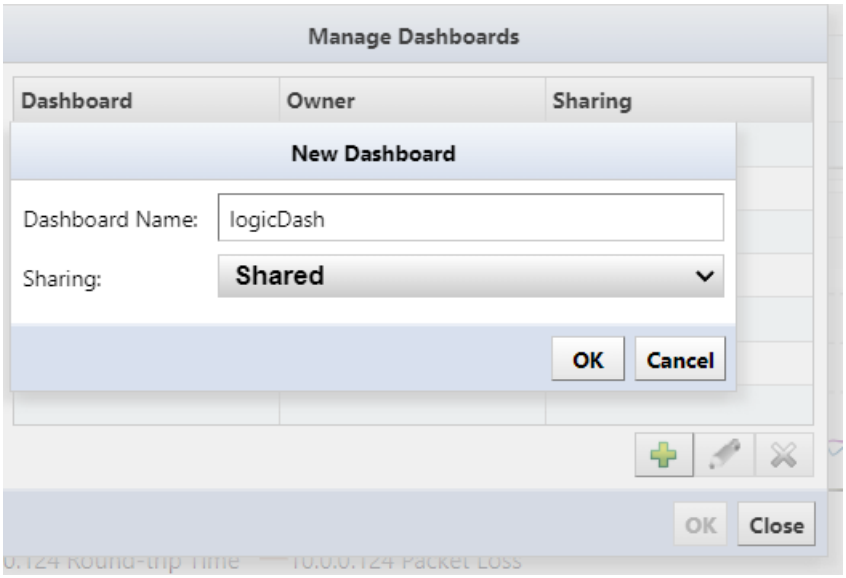
2. Click the  button.



3. Enter the dashboard name.



4. Select the type of dashboard you want to share from the dropdown menu and click [OK].



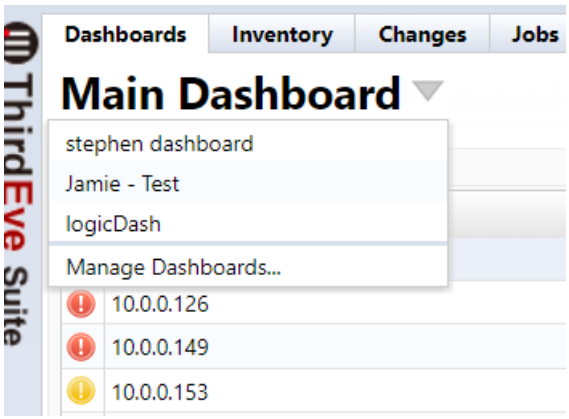
Dashboard type	Explanation
Shared	Add dashboards that other users can view.
Private	Add a dashboard that can only be viewed by the user who created it.

The dashboard will be added to the list.

5. Click [Close] to close the [Manage Dashboard] screen.

8.1.4 Switch Dashboards

1. In the [Dashboard] tab, click the Dashboard name (“Main Dashboard” in the image below), and select [Manage Dashboards].

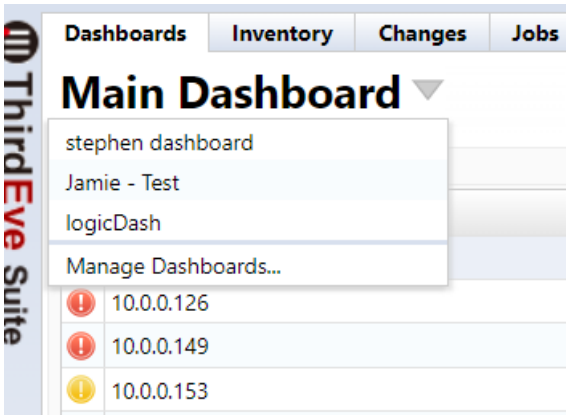


2. Select the dashboard you want to switch to, and click [OK].

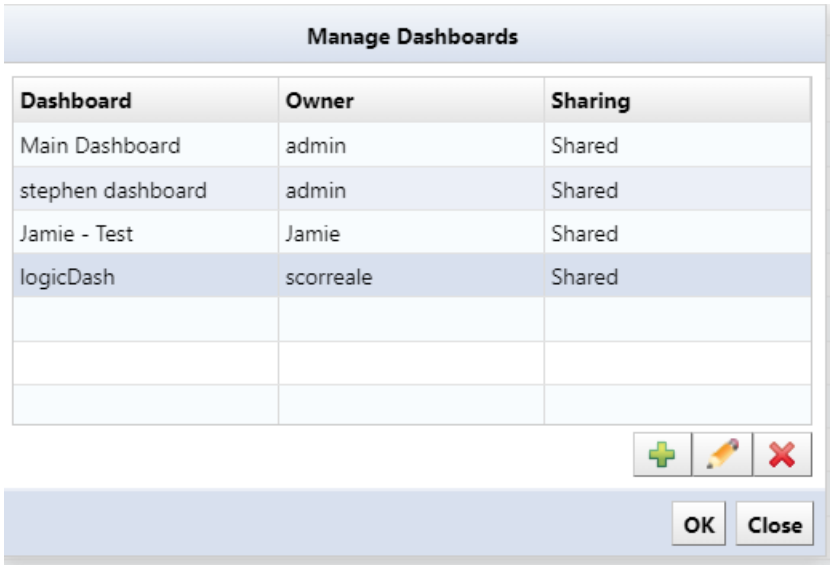
This switches to the selected Dashboard screen.

8.1.5 Delete a dashboard

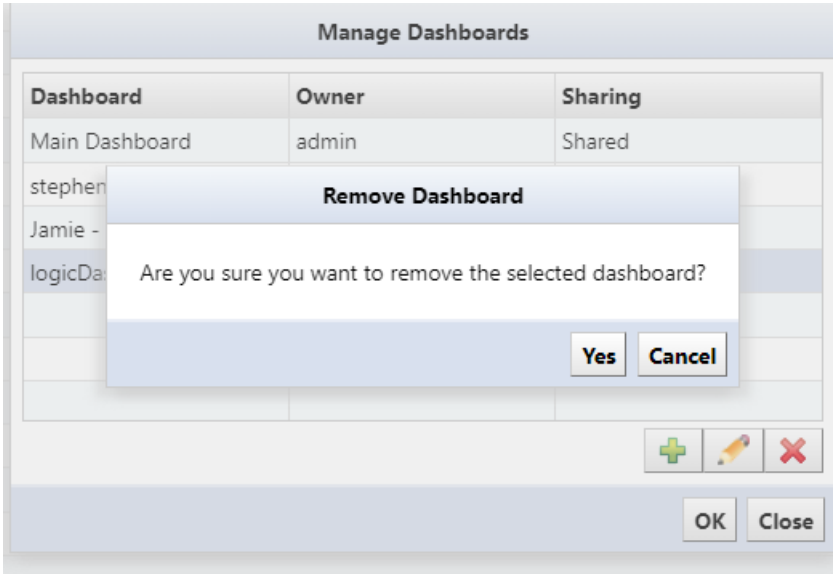
1. In the, click the dashboard name (“Main Dashboard” in the image below) and select [Manage Dashboards].



2. Select the dashboard you want to delete, and click the button.



3. A confirmation message will be displayed. Click [Yes].



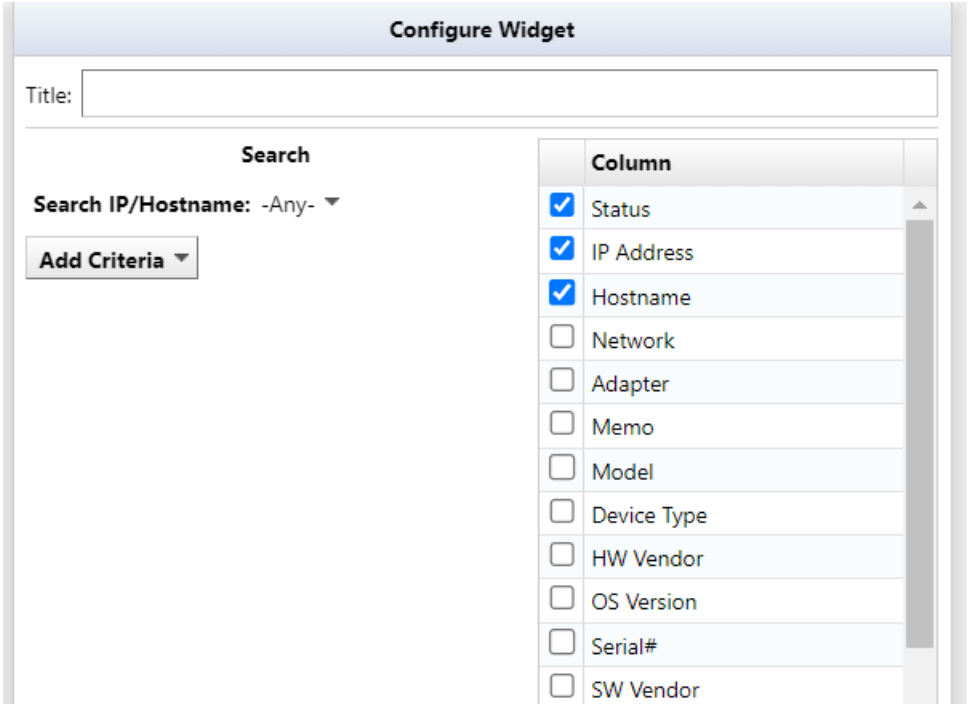
8.1.6 Widgets

8.1.7 Types of Widgets

The types of widgets that can be added are as follows:

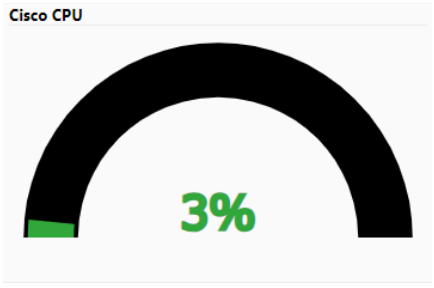
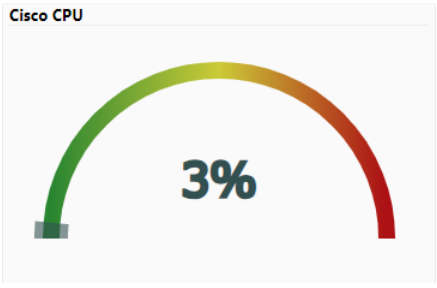
Inventory List

This inventory list widget is used to view the inventory. The maximum number of items displayed is 100. If there are more than 100 items, you can view them in the Inventory tab.



Gauge

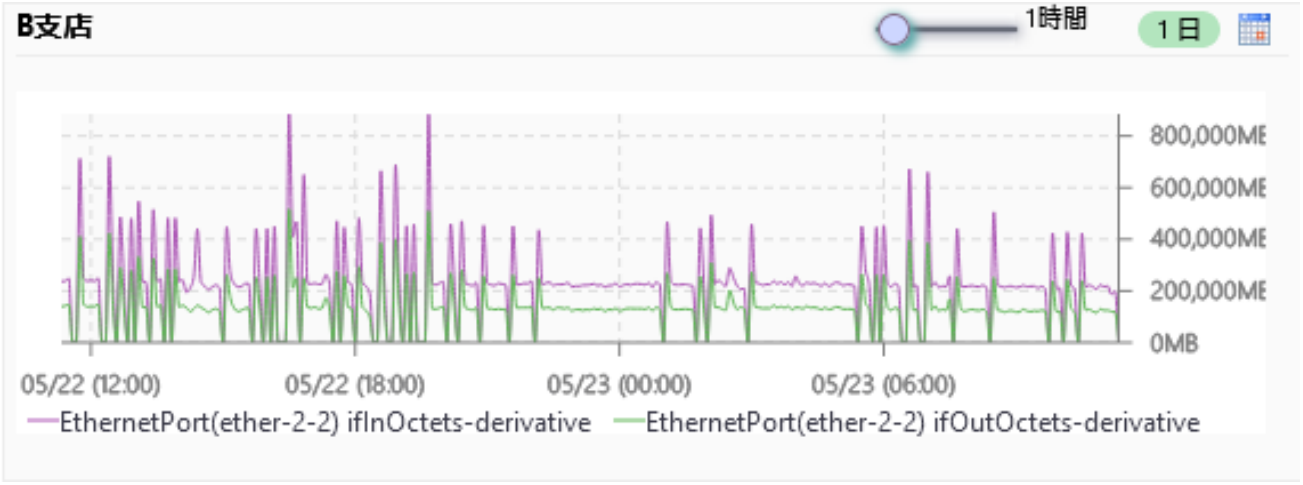
The gauge widget displays a meter graph. It can display two types of meter graphs: "Default" and "Thermal".

Default	Thermal
	

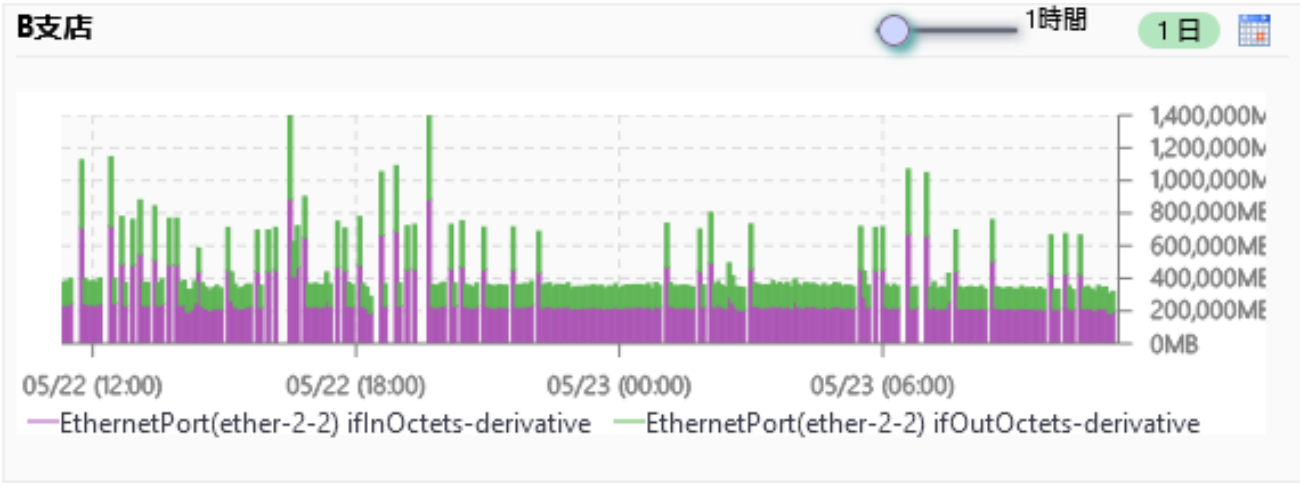
Histogram

The histogram widget displays a line chart or stacked bar chart:

Line chart:



Stacked bar chart:



Map

The map widget displays a map:

Violations

The violations displays violations:

Table

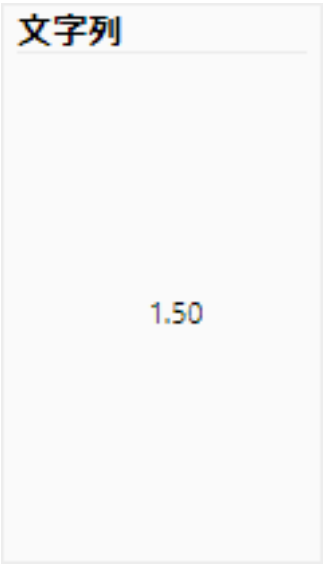
The tables widget displays a table:

テーブル

IPアドレス	ホスト名	indexName	ifInOctets-derivative	ifOutOctets-derivative
10.0.0.126	test123	GigabitEthernet1	183120	25314
10.0.0.126	test123	GigabitEthernet2	0	0
10.0.0.126	test123	GigabitEthernet3	170426	0
10.0.0.126	test123	VirtualPortGroup0	0	0
10.0.0.126	test123	Null0	0	0

Text

The text widget displays a string:



Image

The image widget displays an image:

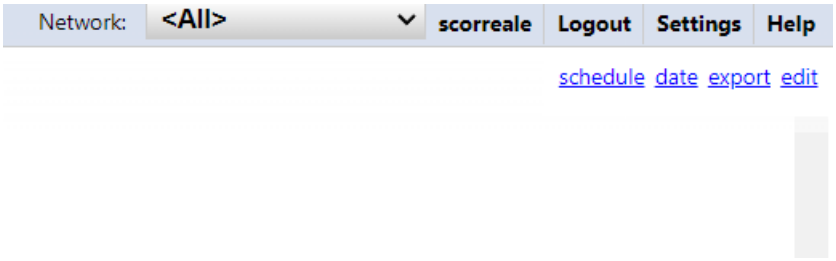
8.1.8 Widget edit menu

While in Dashboard edit mode, you can also add/edit/delete Widgets.

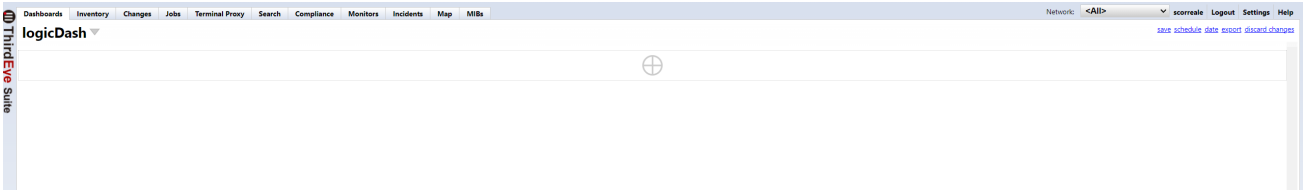
Button	Explanation
…	Click the three-dot button […] displayed to the right of the widget title to display the widget editing menu.
Edit	Edit the widget.
Remove	Delete a widget.

8.1.9 Add a Widget

You can add widgets by clicking [Edit] in the Global Menu.



, and then clicking the ⊕ at the top right of the Dashboard screen.



8.2 Inventory

The Inventory tab serves as the centralized registry for all devices managed by {{ProductName}}. It provides real-time information such as device status, configurations, and connectivity. It also displays details about as hardware/software versions, IP addresses, and operational health indicators. It is you can go for information about monitoring, compliance checks, and automation workflows.

The Inventory tab contains 6 subtabs:

- Device
- Inventory
- Tools
- Change
- Smart Change
- Reports

8.2.1 Set credentials

If you want to monitor using SNMP from the monitored device or obtain the configuration, you need to set the credentials (SNMP community, username, password) set on the monitored device in ThirdEye. Set the credentials on the device tab under Inventory > [Credentials].

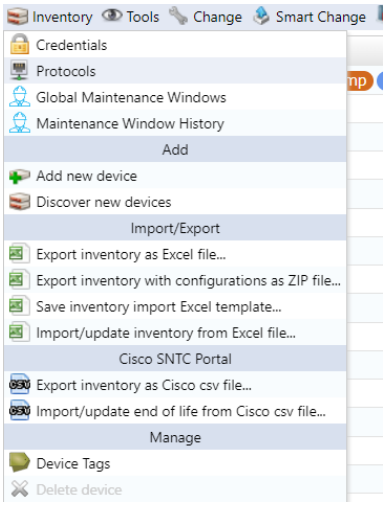
There are two ways to set credentials: **“dynamic”** and **“static”**.

Credential Setting	Explanation
dynamic	Set common credentials for address ranges. This is useful when common credentials are set for monitored devices. Up to three credentials can be registered in one network group.
static	Set credentials for each IP address. Use this when different credentials are set for each monitored device.

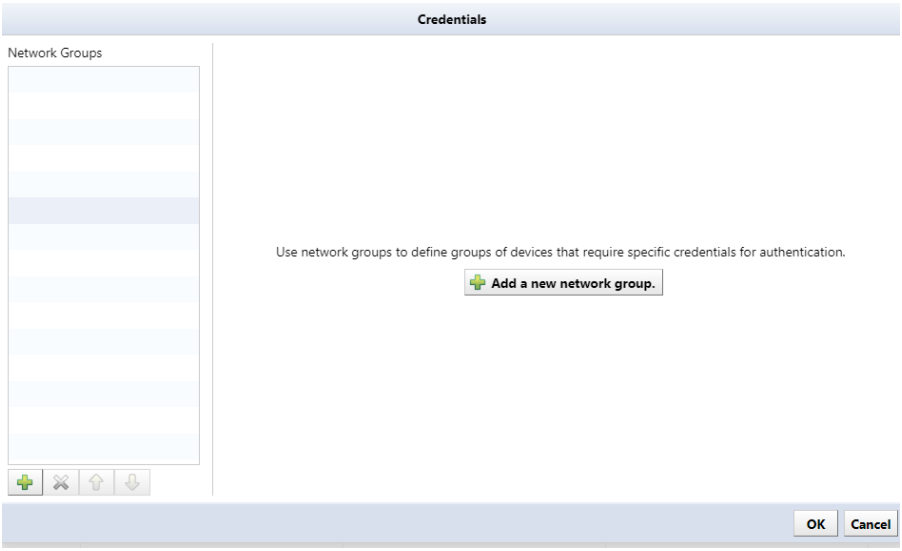
8.2.2 Set common credentials

If you have set common credentials for monitored devices, use **“Dynamic”** to set them.

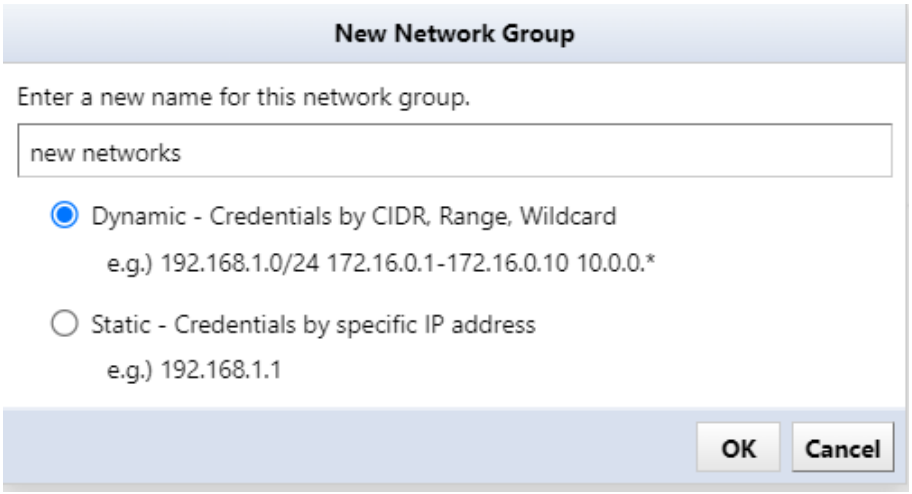
1. Select the [Devices] tab and click Inventory > [Credentials].



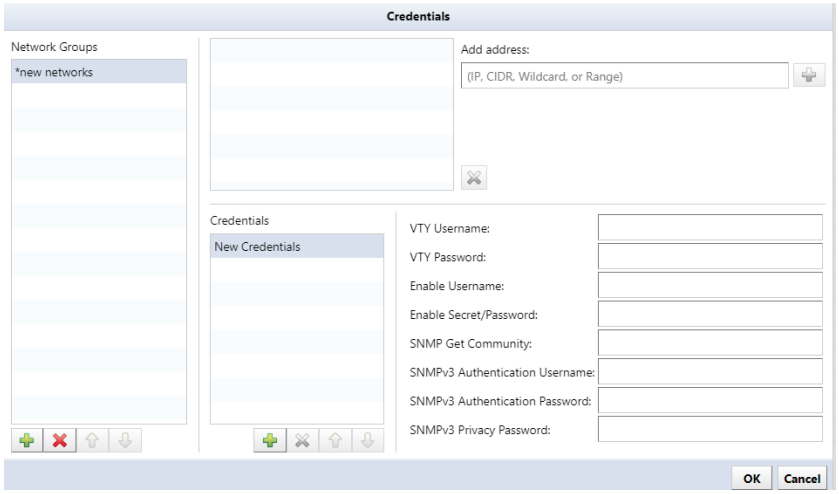
2. Click the button or [Add new network group].



3. Enter the network group name, select “Dynamic”, and click [OK].

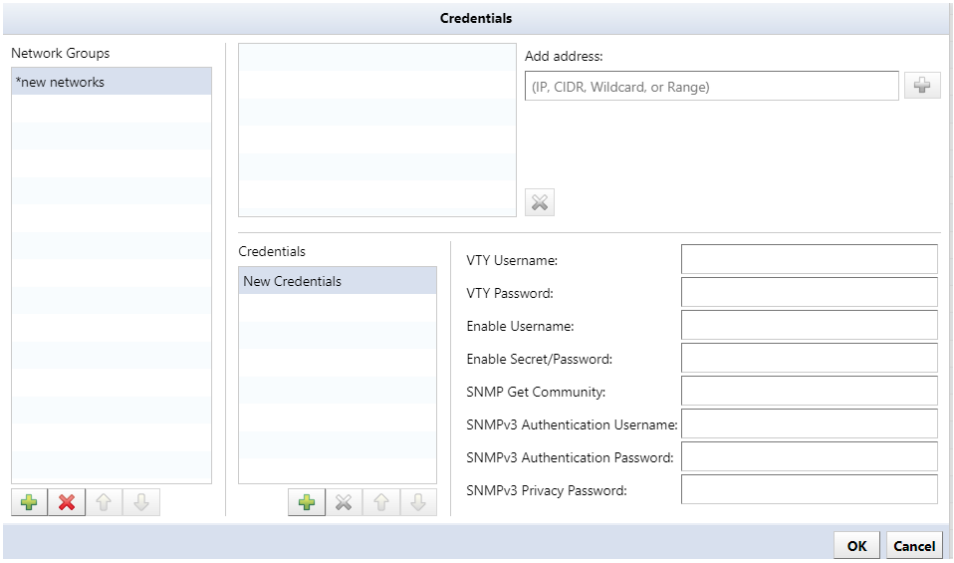


4. Enter the address range of the network group in the [Add Address] field, and click the button.



5. In the “Credential Set” window, enter the IP address and set each item.

It is possible to omit inputting items that are not required.



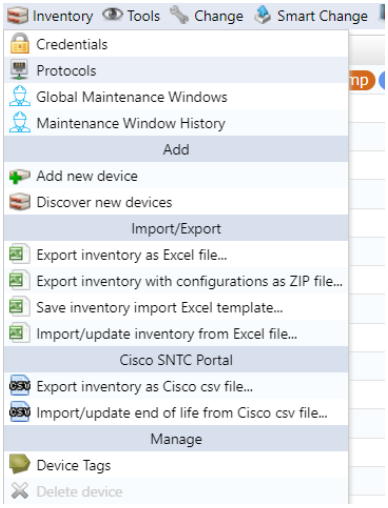
Item	Explanation
VTY Username /VTY Password	Enter the username/password required to log in to the network device.
Enable Username /Enable Secret/Password	Enter the username/password to enter enable mode.
SNMP Get Community	Enter the SNMP community to use when making an SNMP Get request.
SNMPv3 Authentication Username	Enter the authentication username defined in SNMPv3.
SNMPv3 Authentication Password	Enter the password for the community defined in SNMPv3.
SNMPv3 Privacy Password	Enter the password used for encryption when communicating via SNMP.

6. Click [OK] to save your settings.

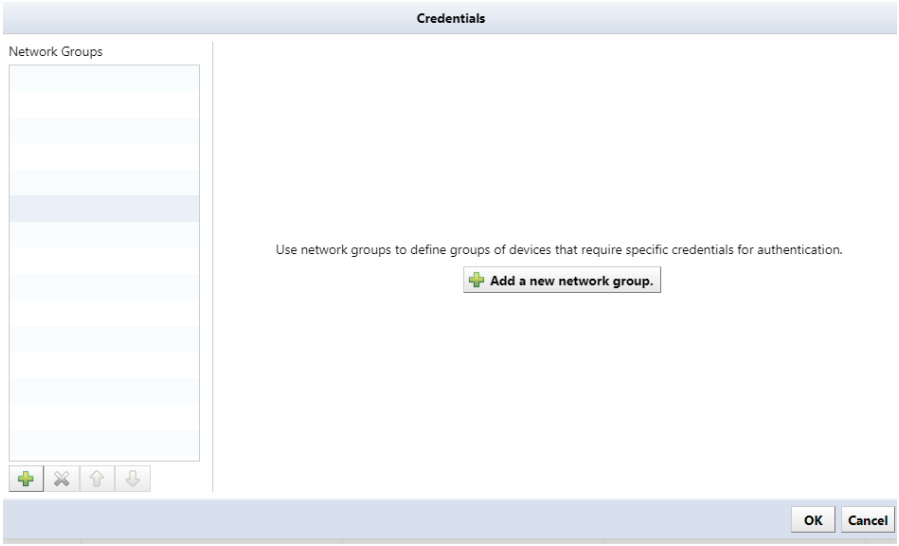
8.2.3 Set credentials for each device

If you are setting different credentials for each monitored device, use **“Static”** to set them.

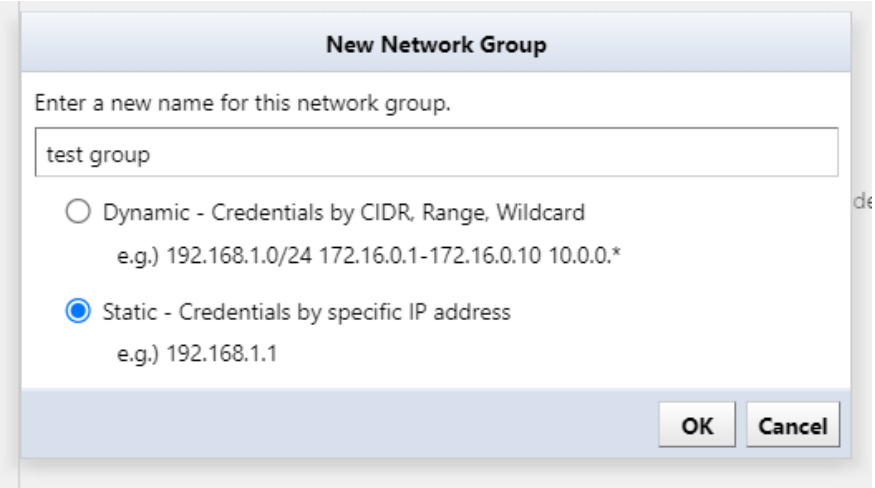
1. Select the [Devices] tab and click Inventory > [Credentials].



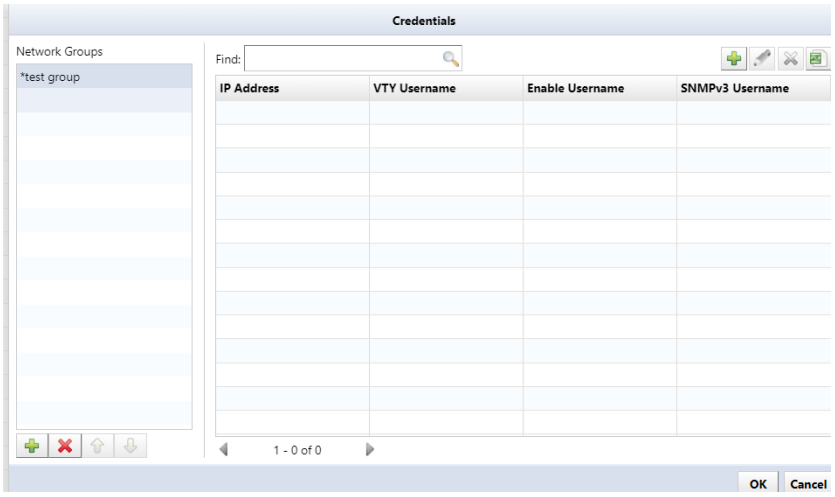
2. Click the button or the [Add new network group] buttons.



3. Enter the network group name, select “Static”, and click [OK].

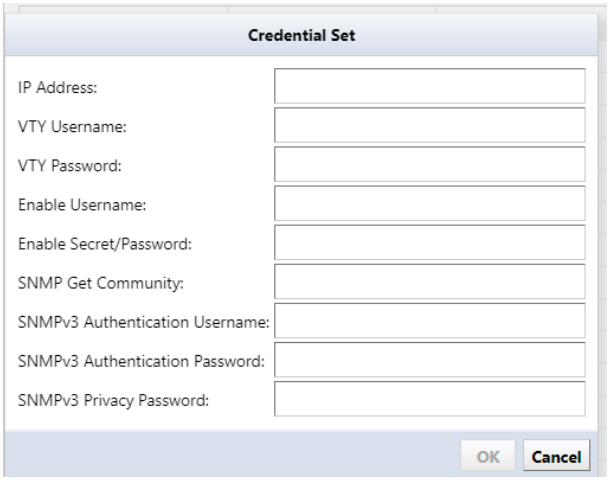


4. Click the  button.



5. In the “Credential Set” window, enter the IP address and set each item.

It is possible to omit items that are not required.



Item	Explanation
IP address	Enter the IP address of your network device.
VTY Username /VTY Password	Enter the username/password required to log in to the network device.
Enable Username /Enable Secret/Password	Enter the username/password to enter enable mode.
SNMP Get Community	Enter the SNMP community to use when making an SNMP Get request.
SNMPv3 Authentication Username	Enter the authentication username defined in SNMPv3.
SNMPv3 Authentication Password	Enter the password for the community defined in SNMPv3.
SNMPv3 Privacy Password	Enter the password used for encryption when communicating via SNMP.

6. Click [OK] to save your settings.

8.2.4 Add devices

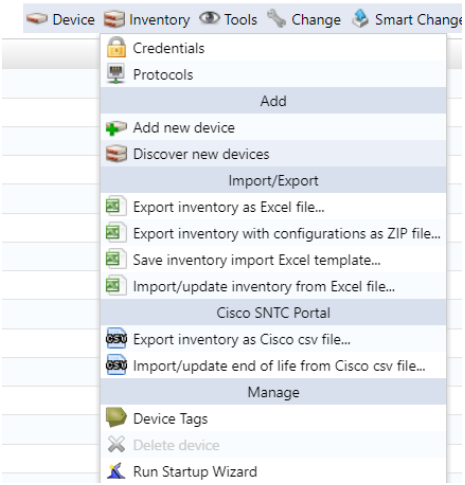
When adding devices to ThirdEye, use one of the following methods:

Method	Explanation
manual	Add a device by directly entering the device's IP address. Add one unit at a time.
discovery	Automatically discover and add devices within the specified IP address range.
import	This function reads device data from an XLSX file. Export the template file for import and enter information about the monitored devices in that file.

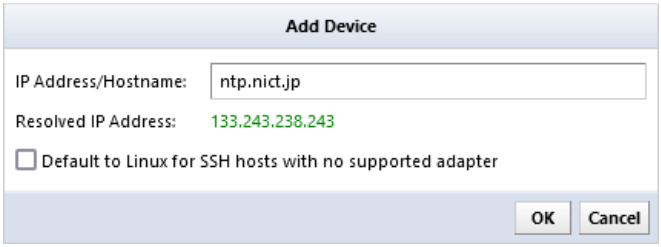
> **Note**
>
> When adding a device, the device does not appear on the map by default.
>
> If you want your device to appear as an object on the map, you must add it.

8.2.5 Register one device

1. Click the Inventory > [Add new device] buttons.

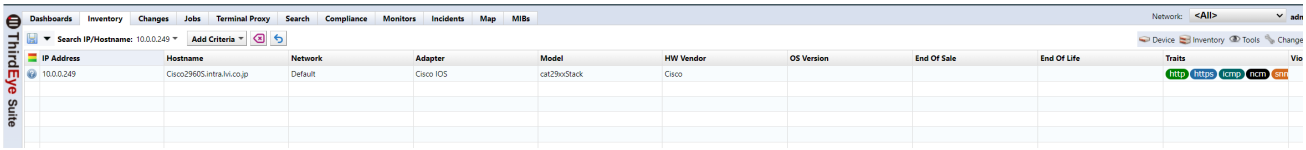


2. Enter the IP address or hostname of the device and click [OK].



Item	Explanation
Default to Linux for SSH hosts with no supported adapter	Assigns a Linux adapter when the adapter for configuration backup cannot be recognized.

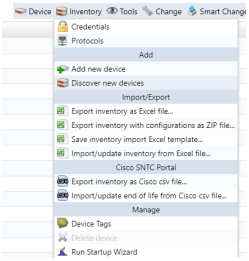
Once ThirdEye completes collecting information from the monitored devices, the added devices will be added to the device list in the Inventory tab.



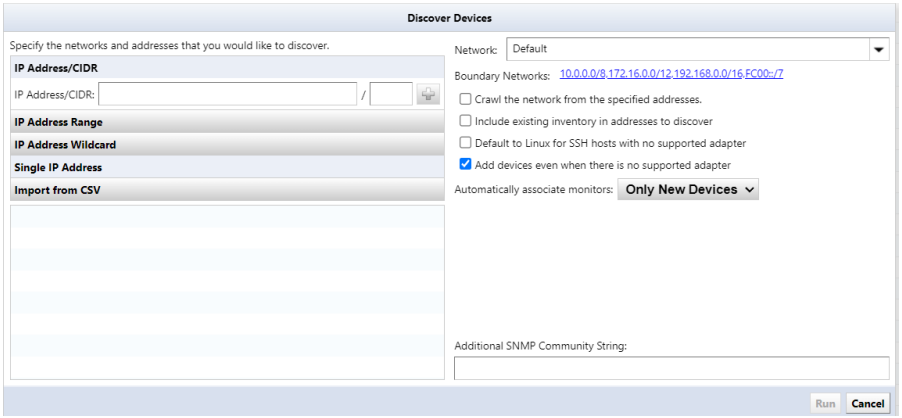
The device will be added even if it is not possible to communicate with the target IP address. However, the host name and interface information will not be obtained.

8.2.6 Discover devices on your network

1. Click the Inventory and click [Discover new device].



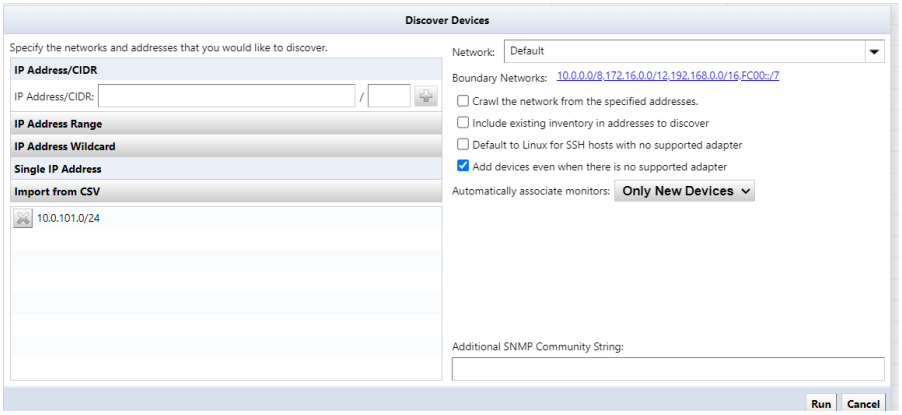
2. Specify the IP address range to discover, and click the button.



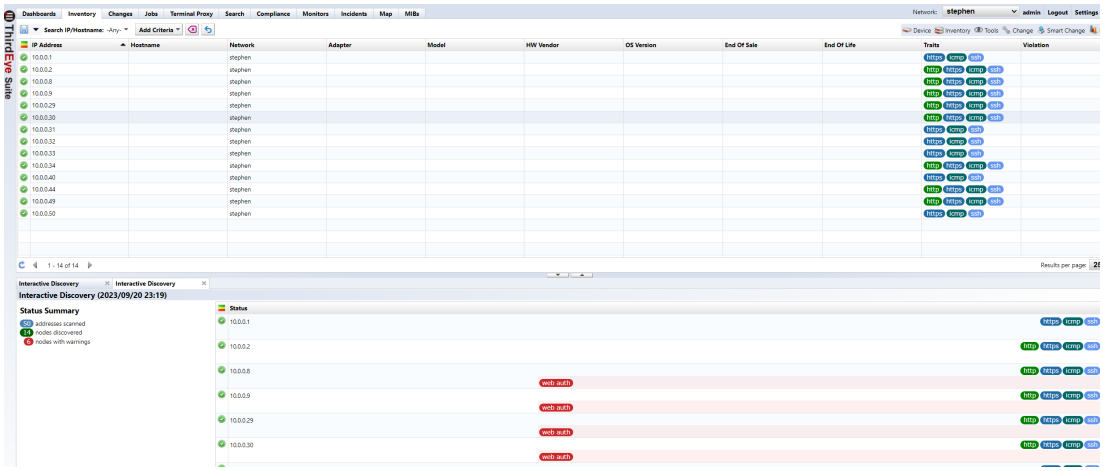
Item	Explanation
Crawl the network from the specified addresses	Add a discovery target network by referring to the discovered device's routing table.
Include existing inventory in addresses to discover	If there is already an added device, add a discovery target network by referring to the routing table of the registered device.
Default to Linux for SSH hosts with no supported adapter	Assigns a Linux adapter when the adapter for configuration backup cannot be recognized.
Add devices even when there is no supported adapter	Add the device even if the adapter is not recognized.
Automatically associate monitors	Assign the selected monitor set to the discovered devices.

The input information will be added to the bottom left of the screen.

3. Click [Run].



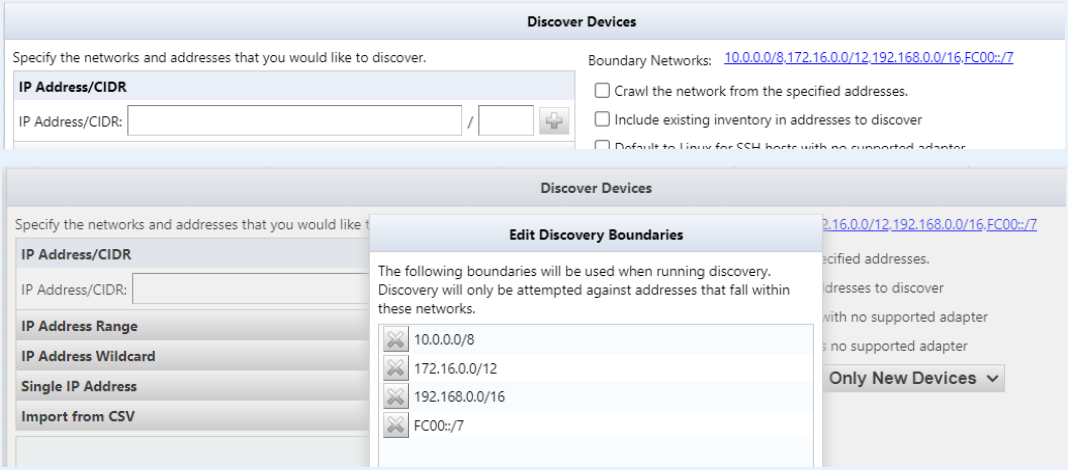
4. Discovery will start, and the discovery results will be displayed at the bottom of the screen.



Once discovery is complete, discovered devices are automatically added to ThirdEye.

Note

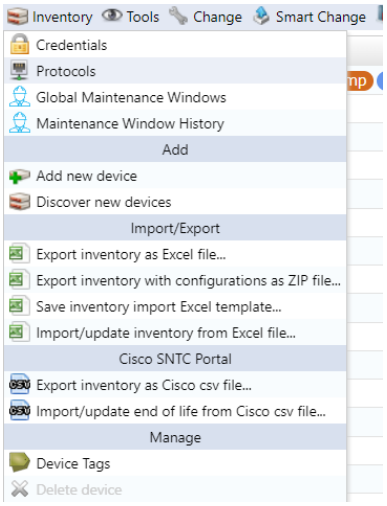
"Discovery Devices" several ranges are specified for "Boundary Networks" by default. "Discovery Devices" also has a setting called "Boundary Networks", which allows you to limit the scope of discovery to the range specified in "Boundary Networks". Clicking the Boundary Network value opens the "Edit Discovery Boundaries" window, which allows so edit "Boundary Network" as necessary.



8.2.7 Import devices from Excel file

Information on monitored devices can be imported from an Excel file. A template for import is provided. Input the monitored device information into the template in advance, then import it.

1. Click the Inventory > [Save inventory import Excel Template] buttons.



The file opening screen will be displayed.

2. Click [Save file] and [OK].

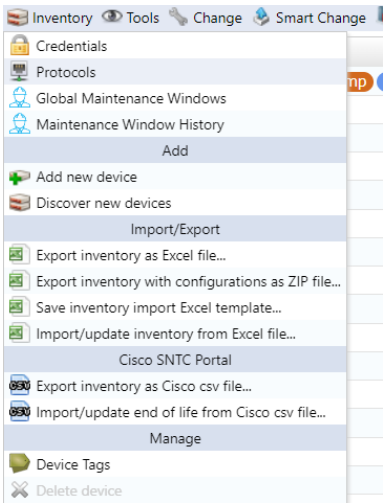
The file name will be “ThirdEye-inventory-template.xlsx” and will be saved in XLSX file format.

3. Edit the saved file, enter information in the following fields, and overwrite and save.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	IP Address	Network	Adapter ID	Hostname	Type	Vendor	Model	OS Version	Serial Number	Memo	End Of Sale	End Of Life	Custom 1	Custom 2	Custom 3	Custom 4	Custom 5
2	172.16.0.1	Default		Demo-01													
3	172.16.0.2	Default		Demo-02													
4	172.16.0.3	Default		Demo-03													
5	172.16.0.4	Default		Demo-04													
6	172.16.0.5	Default		Demo-05													
7	172.16.0.6	Default		Demo-06													
8	172.16.0.7	Default		Demo-07													
9	172.16.0.8	Default		Demo-08													
10	172.16.0.9	Default		Demo-09													
11	172.16.0.10	Default		Demo-10													
12																	

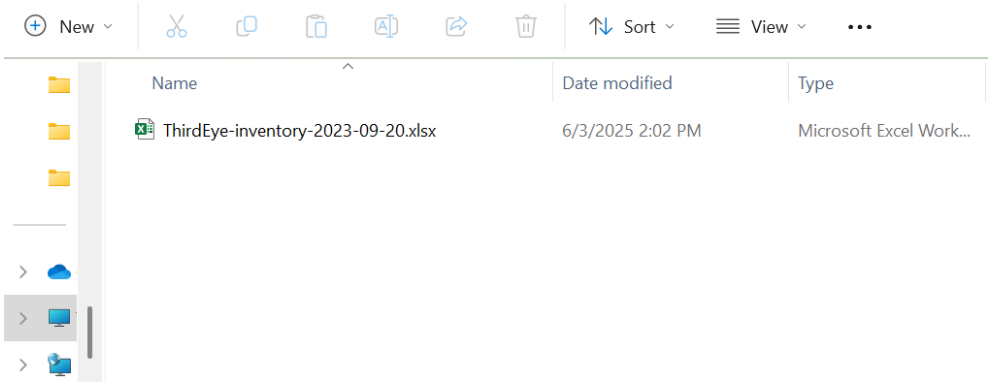
Item	Explanation	Requirements	Input example
IP Address	Enter the device's IP address.	required	192.168.1.10
Network	Select the network name to which you want to add the device.	required	Default
Adapter ID	Select your device's adapter. (In the current version, there is no need to specify this item.)	-	Cisco IOS
Hostname	Enter the device hostname.	-	
End Of Sale	Enter the sales end date in the format "yyyy/mm/dd".	-	2022/1/1
End Of Life	Enter the support end date in the format "yyyy/mm/dd".	-	2022/12/31
Custom 1-5	Enter the information for "Custom Device Field".	-	

4. Click Inventory > [Import/Update Inventory from Excel File].

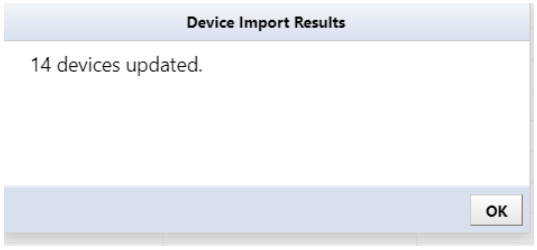


A file selection dialog will be displayed.

5. Select the edited file and click [Open].



6. A confirmation message will be displayed. Click [OK].



8.2.8 Get Device Configuration

ThirdEye allows you to use the functionality of Net LineDancer (config management tool). Obtaining the device configuration is called a "(config) backup." For configuration backup, ThirdEye connects to the device via SSH or Telnet and retrieves the configuration using show commands, TFTP commands, etc.

8.2.8.1 Prerequisites Before performing a configuration backup, ensure the following requirements are met:

- A login username and password for logging into the device have been set.

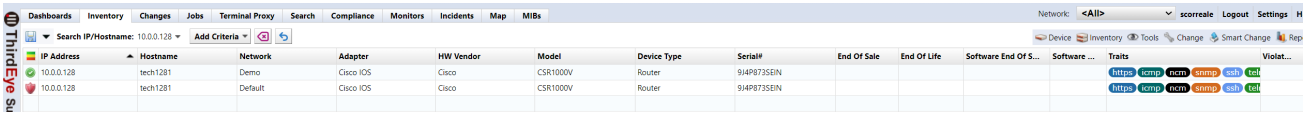
  Refer to the **Set Credentials** sections to make sure the credentials are set.

- The model supports configuration backup by ThirdEye.

  For a list of supported devices, see the following web page:

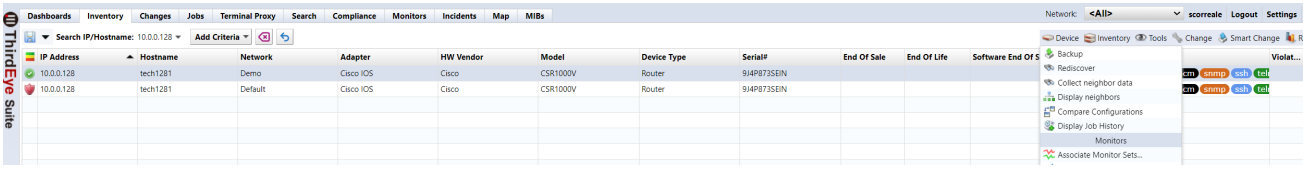
https://logicvein.com/supported-devices

- NCM function is enabled. The target of configuration backup is the device with "ncm" displayed in the trait column.

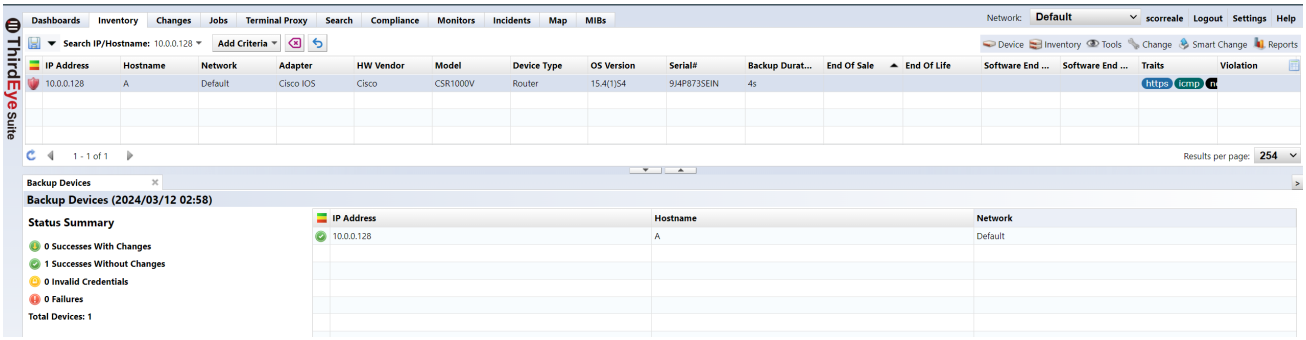


8.2.8.2 Run a backup To perform a backup, select the target device and click [Backup] from the device menu.

If no device is selected, execute for devices with NCM function is enabled.



When you run the backup, the execution results will be displayed at the bottom of the screen.



The status summary list for backup execution is as follows:

Icon	Explanation
	Backup successful, changes made. Displayed when a difference is detected between the last backup and the configuration on the device. It will also be displayed during the first backup.
	Backup successful, no changes. Displayed when the configuration data on the device is the same as the last backup.
	Backup failed due to credentials mismatch. The registered credentials are incorrect. Click on the result shown on the right to see the credentials used for the backup. Please check the Inventory > Credential Settings tab.
	Backup failed. Configuration could not be obtained. Doubleclick the icon to view details.

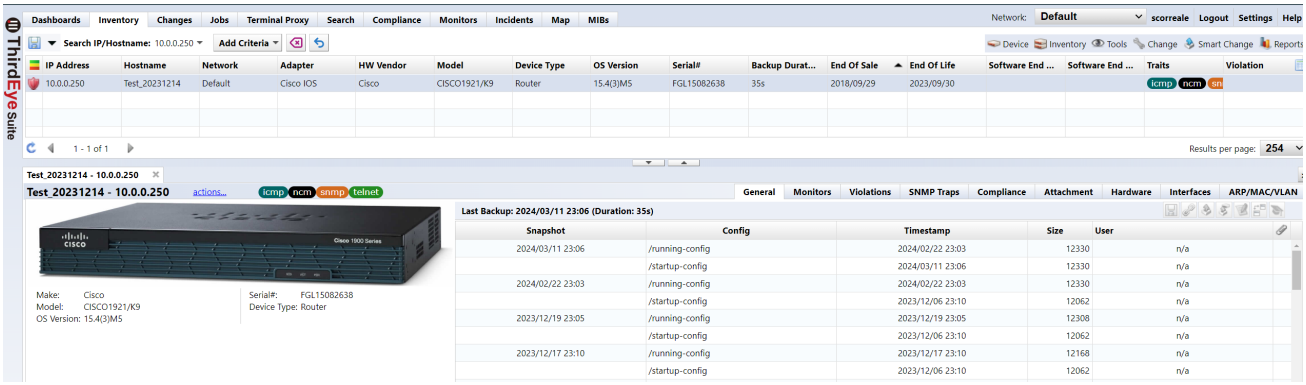
8.2.8.3 About the status after backup After the backup, the status icon displayed on the left side of the device view will change. The icons used for backup status are as follows.

Icon	Status	Condition Description
	**Backup complete**	Configuration acquisition has completed successfully.
	**Configuration mismatch**	There are differences between the device's running-config and startup-config. Doubleclick the icon to see the comparison results.
	**Credential mismatch**	You cannot log in with the registered credentials and the backup is failing. Please check your credential settings.
	**Backup failure**	Backup has failed for some reason.
	**Backup not executed**	No backups have been performed.
	**Warning**	This device violates a compliance policy with severity set to Warning.
	**Error**	This device violates a compliance policy with failure level set to Error.

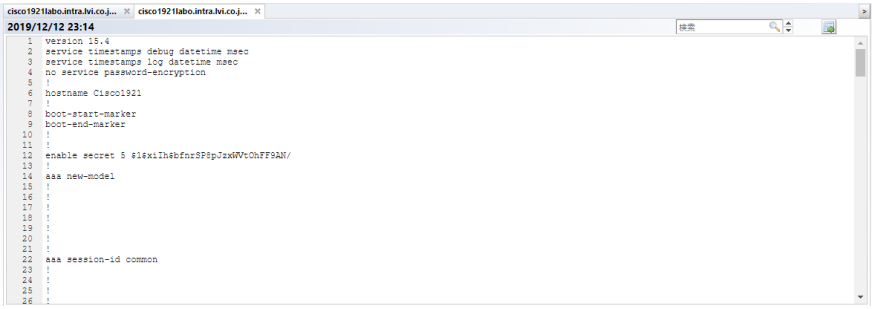
The icon displayed in the status column is the icon with the highest priority among the severity and backup status set in the trigger in the monitor settings.

Priority	Status	Severity Status Icon :	Backup Status Icon
High	**Emergency**		-
	Alert		-
	Backup failure	-	
	Critical		-
	Credential mismatch	-	
Priority	**Error**		-
	Config mismatch	-	
	Warning		-
	Notify		-
	Information		-
	Debug		-
Low	**Backup not executed**	-	

8.2.8.4 Check the obtained configuration You can check the acquired configuration from the device details screen.

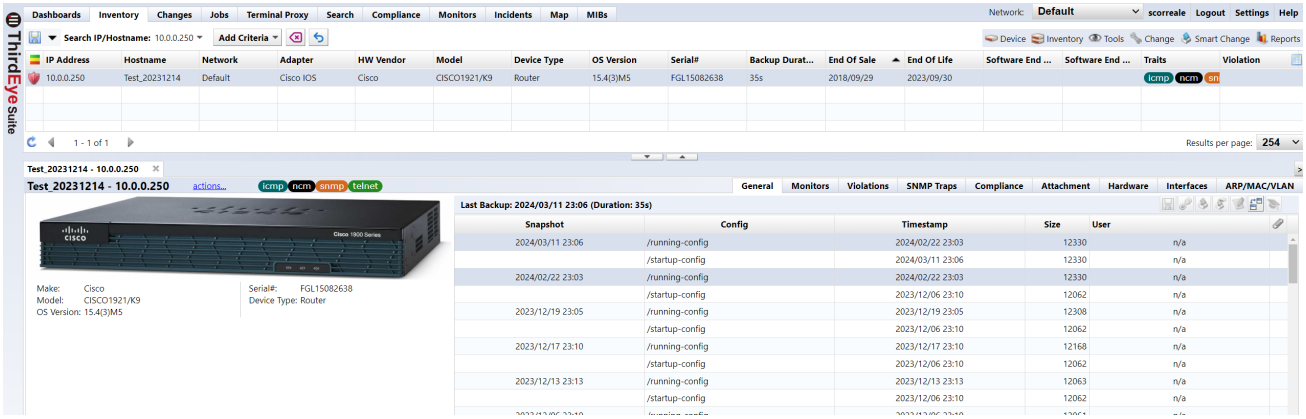


You can check the contents by doubleclicking on the [Config] button.

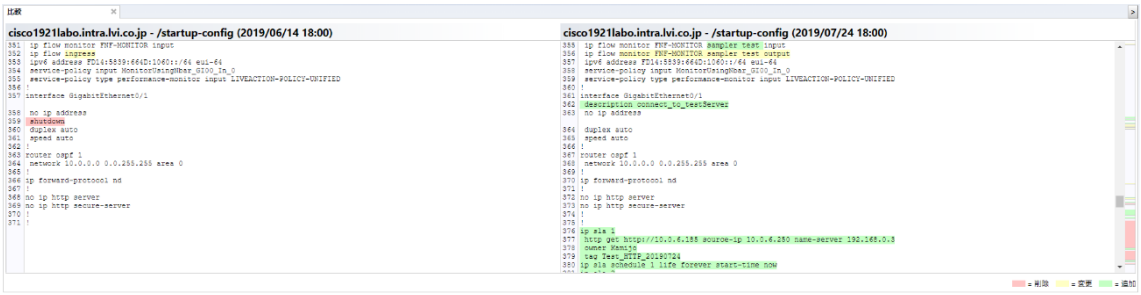


8.2.8.5 Configuration Comparison You can compare the configurations by selecting two configurations and clicking the [Compare] button.

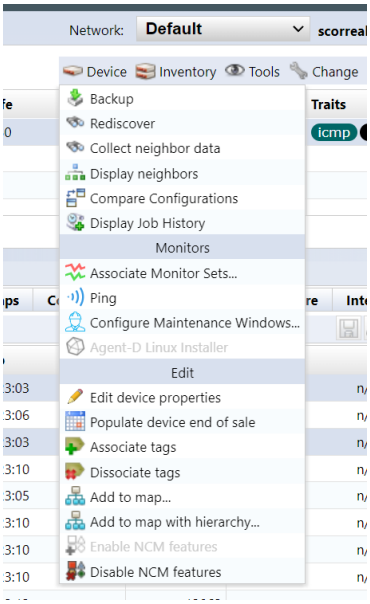
Multiple selections can be made by holding down the [Ctrl] key while selecting.



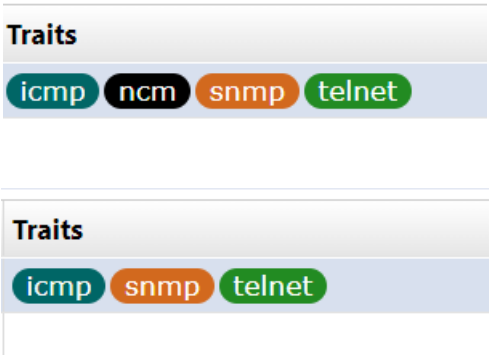
When you compare configurations, configuration differences are highlighted in color. Each type of difference is displayed in a different color, with red representing deleted parts, yellow representing changed parts, and green representing added parts.



8.2.8.6 Disable config backup Even if the model supports configuration backup, if you do not want to acquire the configuration, you can exclude it from the backup target by disabling the NCM function. To disable NCM functionality, select the target device in the Inventory and click [Disable NCM functionality] in the [Device] menu.



If you disable the NCM feature, “ncm” will no longer appear in the trait.



To enable the NCM function, select the target device and click [Enable NCM function] in the device menu.

8.2.9 Maintenance mode

Stopping monitoring is called “Non-Monitoring.” When a monitored device is placed in a Non-Monitored state, even if a monitored event occurs on that device, failure events will not be detected. This function is useful when you want to temporarily stop monitoring during maintenance, etc.

When a device is in Maintenance Mode, the map icon changes as follows:

TODO: replace green checkmark with bluearrowright.png!

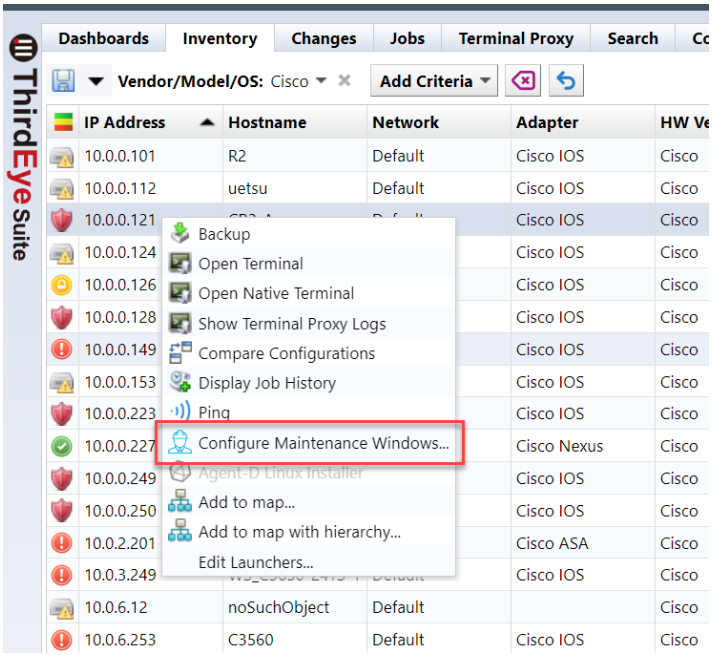
monitoring mode	maintenance mode
	

8.2.9.1 Configure maintenance mode manually

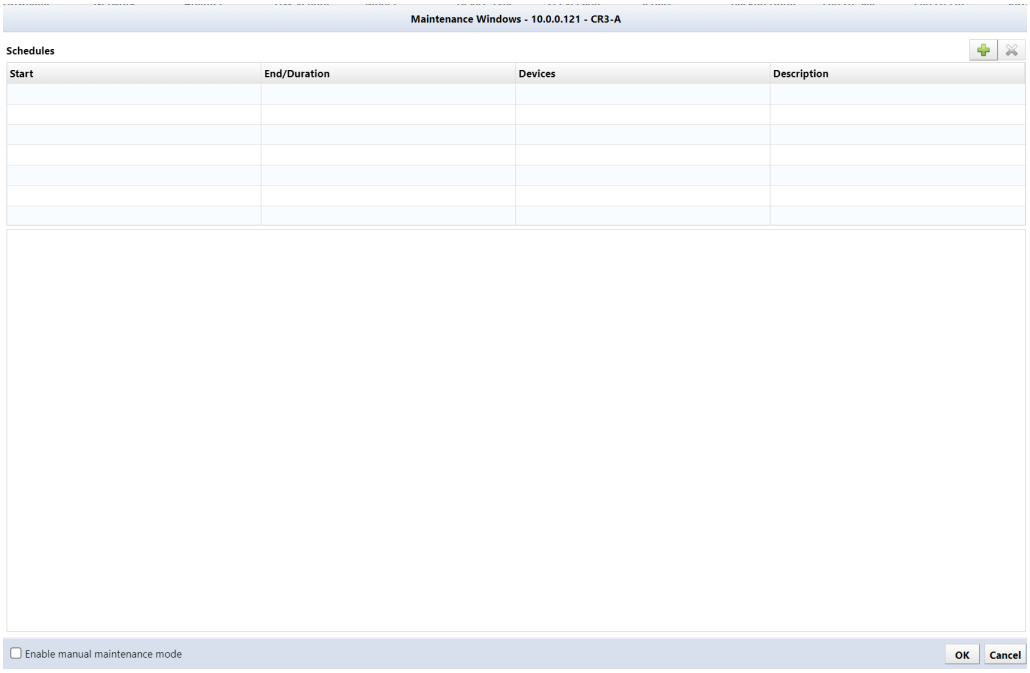
1. Open the Inventory tab, select the device you want to set maintenance mode, and right-click it.

Multiple selections can be made by holding down the [Ctrl] key while selecting.

2. Click [Configure Maintenance Windows…].

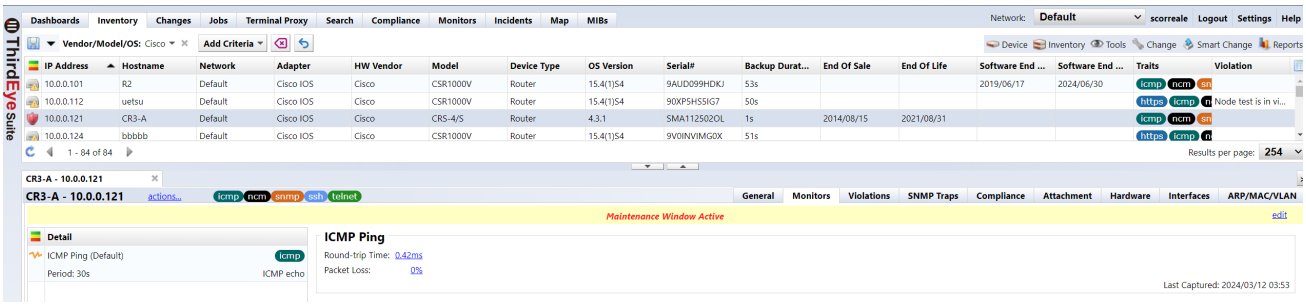


3. Check “Enable manual maintenance mode” and click [OK].



The operation is now complete.

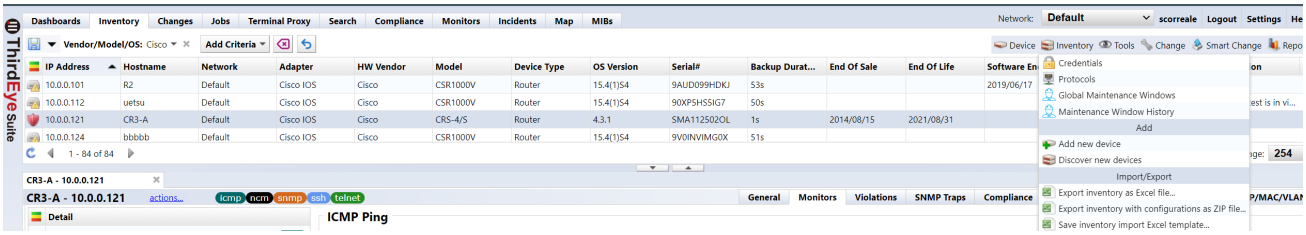
When you doubleclick a device to display the device view, the Monitors tab displays the **Maintenance Windows Active** You can confirm that it is displayed.



To cancel maintenance mode, uncheck “Enable manual maintenance mode” in Step 3 above and click [OK].

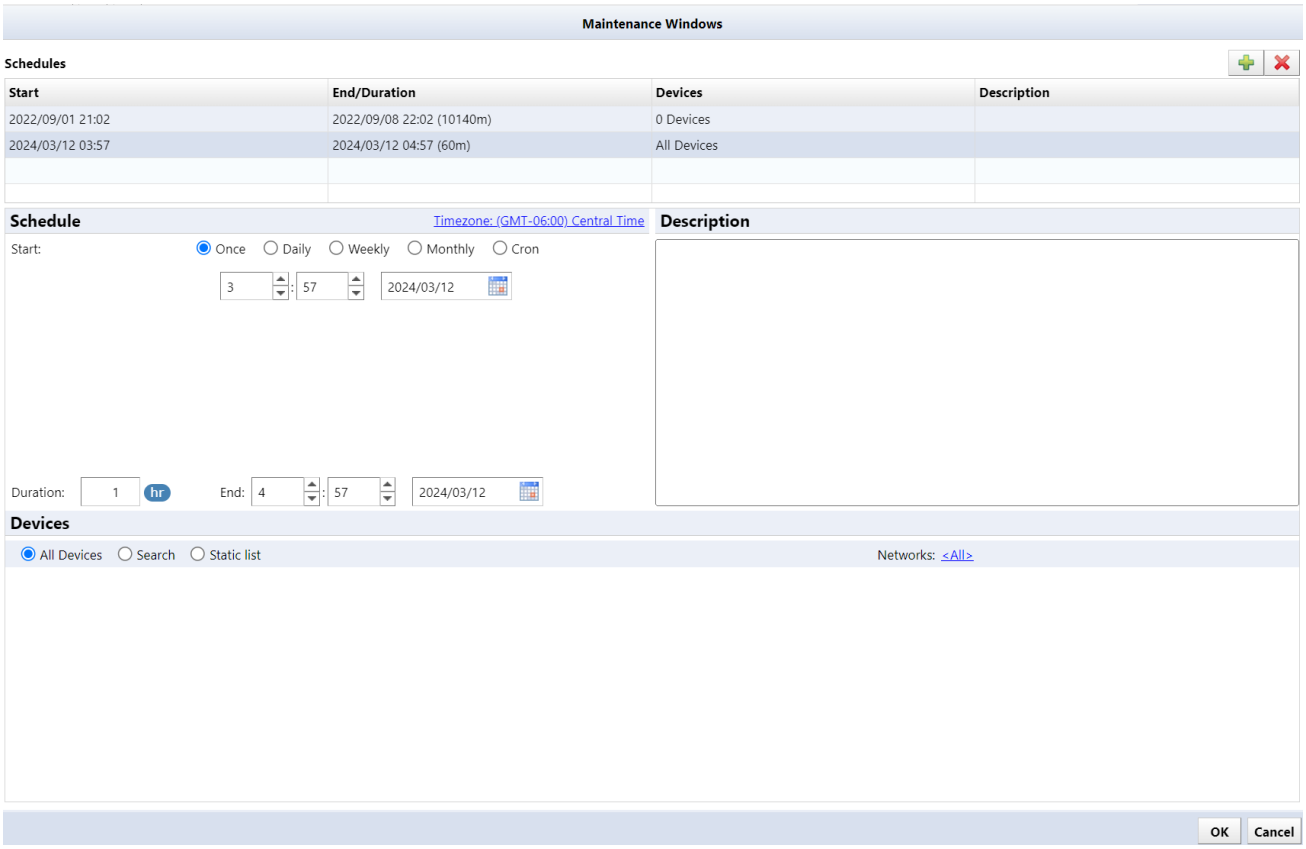
8.2.9.2 Maintenance mode by schedule

1. Open the Inventory tab and click Inventory > [Global Maintenance Windows].



2. Click the button.

3. Set the schedule and devices.



[Maintenance Windows Menu Items]

Menu Item	Submenu Item	Explanation
Schedule	**Start**	Select the schedule to start non-monitoring from the following five types of execution schedules: **Once**: Execute only once at the date and time set **Daily**: Execute every n days (starting point is the 1st of current month) **Weekly**: Execute on a specific day of the week **Monthly**: Execute every specified month **Cron**: Run at specified date/time in cron format
	Duration	Specify the non-monitoring period. The period unit can be changed from “min”, “hr”, and “day”. *The end date/time can only be specified when the execution schedule is “Once”.

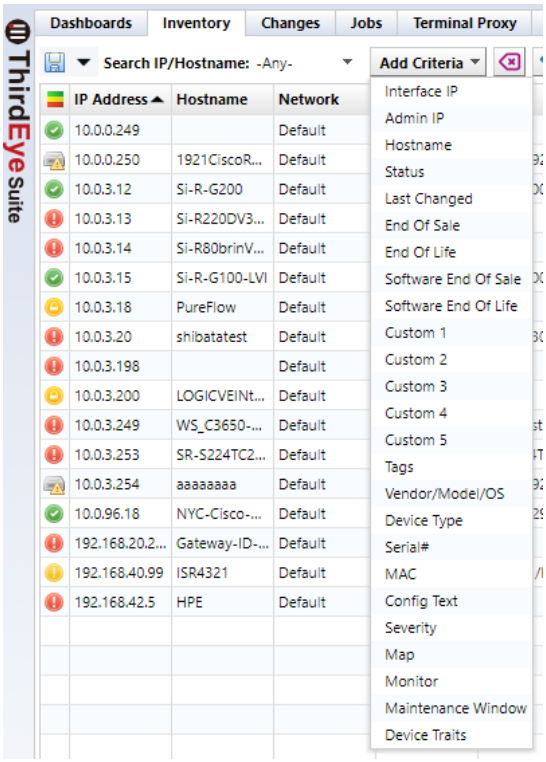
Menu Item	Submenu Item	Explanation
Description		Enter a description for the non-monitoring schedule.
Device		Specify the device for non-monitoring schedule: **All devices**: Target all devices **Search**: Target only devices matching specified search **Static list**: Target only specified devices

4. Click [OK].

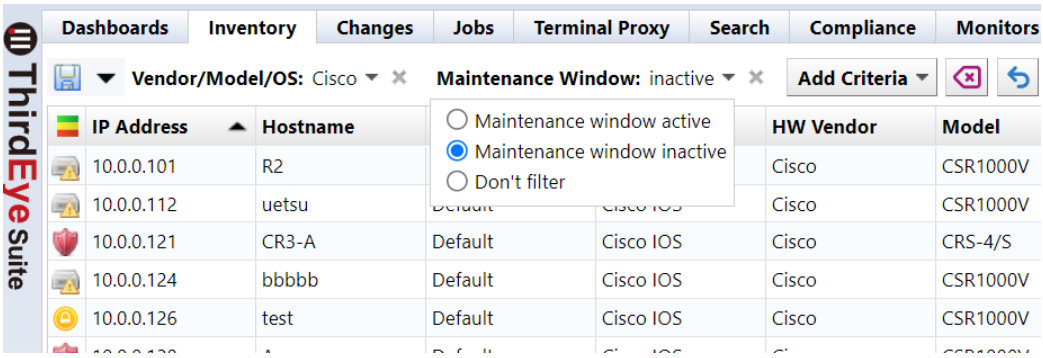
With the above operations, the device will be placed in a non-monitoring state according to the time set in the schedule.

8.2.9.3 Find devices that maintenance window is inactive You can search devices that maintenance using the search criteria on the Inventory tab.

1. Open the Inventory tab and click [Add criteria] > [Maintenance Window].



2. Select [Maintenance window inactive].

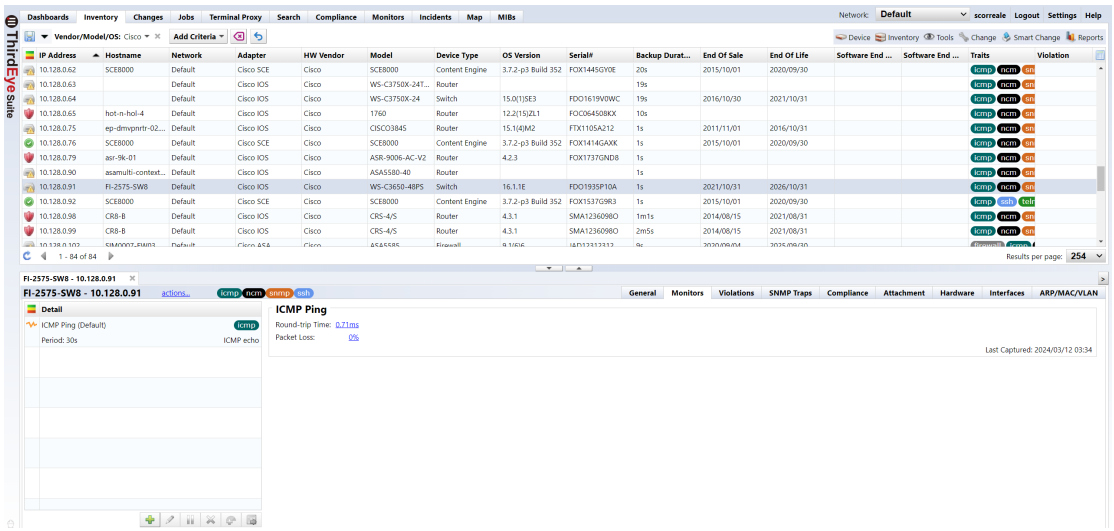


With the above operations, a list of unmonitored devices will be displayed.

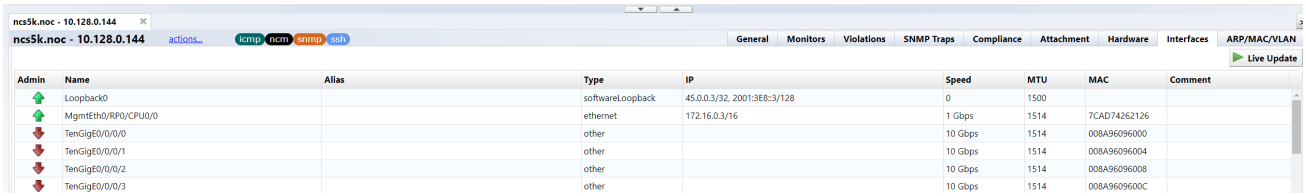
8.2.10 Check the Up/Down status of the device interface

On the [Device Details] screen, you can check the status of the device's interface. To use this function, SNMP communication with the monitored device must be possible.

1. From the list of monitored devices on the Inventory tab,doubleclick the device for which you want to check interfaces.



2. Click the [Interface] tab on the [Device Details] screen.
3. Click [Live Update].



35. Information on the interfaces of monitored devices can be obtained periodically and the current status can be checked.

To stop, close the [Device Details] screen or click [Pause Updates].

8.2.11 Device Groups

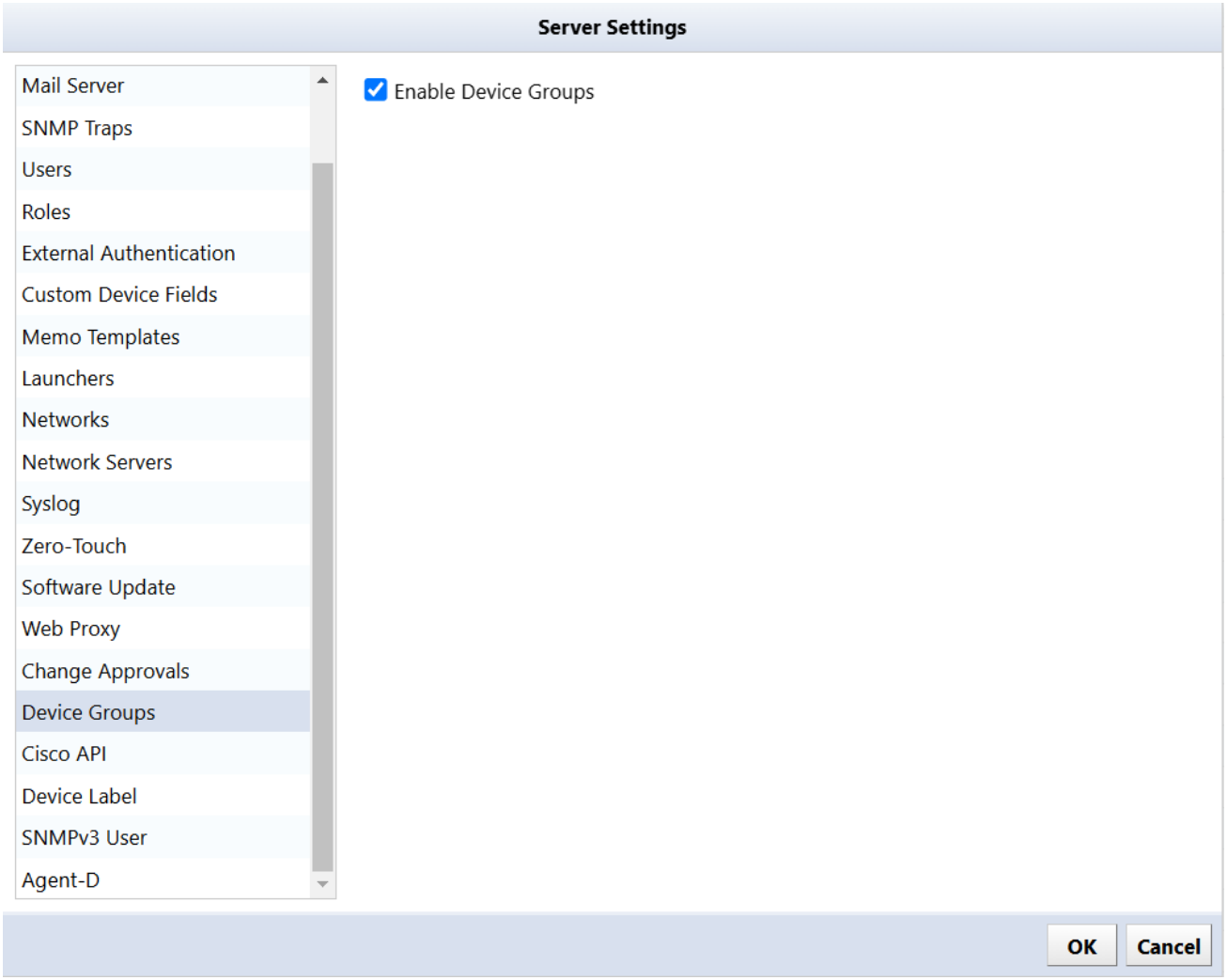
Device groups is a collection of devices grouprd together for easier administration and monitoring. Here are some key points:

- **Organization**: Grouping devices helps in managing them based on criteria such as location, function, or type. This is especially useful in large networks.
- **Simplified Management**: By managing devices in groups, administrators can apply settings, updates, and policies uniformly, saving time and reducing the potential for errors.
- **Monitoring**: Grouping allows for consolidated monitoring and reporting, making it easier to identify issues or trends across multiple devices.
- **Security**: Device groups can be used to enforce security policies. For instance, a group of devices may have specific firewall rules or access controls applied.
- **Scalability**: As networks grow, device groups make it easier to scale management efforts without getting overwhelmed by the number of individual devices.

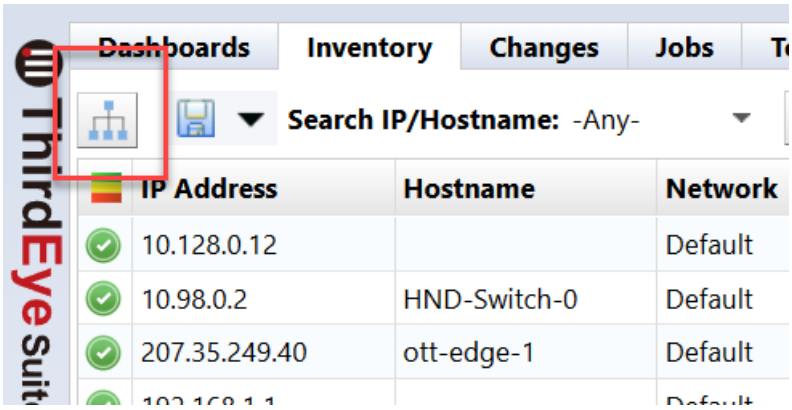
8.2.11.1 Setup and configuration

1. Go to Settings > Server Settings, and click Device Groups in the left sidepanel.

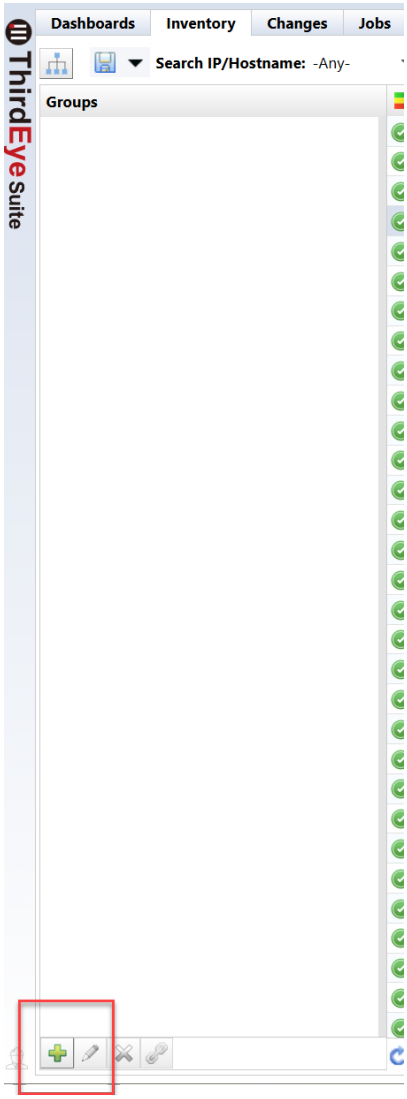
(Ensure “Enable Device Groups” is checked.)



2. Click the Inventory tab, then click the button in the top left corner.



4. Click the button in the bottom left corner.

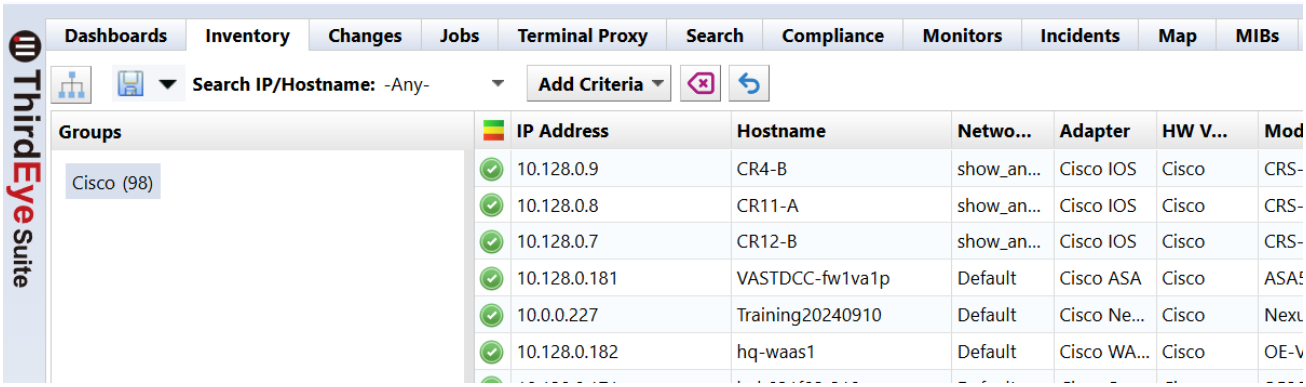


5. In the popup window, enter a name for the grouping (“Cisco” in the screenshot below).

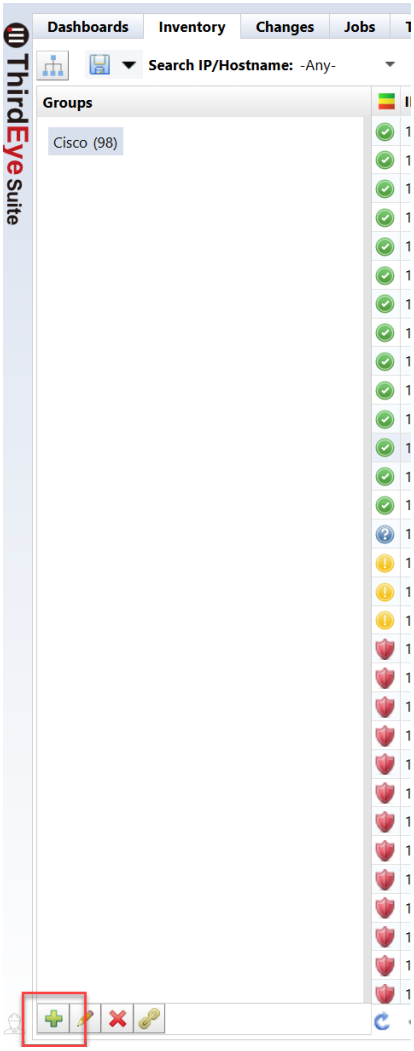
Sharing pulldown menu:

Item	Explanation
Shared	Visible to everyone
Private	Only viewable by creator
Criteria	Allows you to select the criteria for the grouping. For example, select “Vendor/Model/OS” and select the vendor.

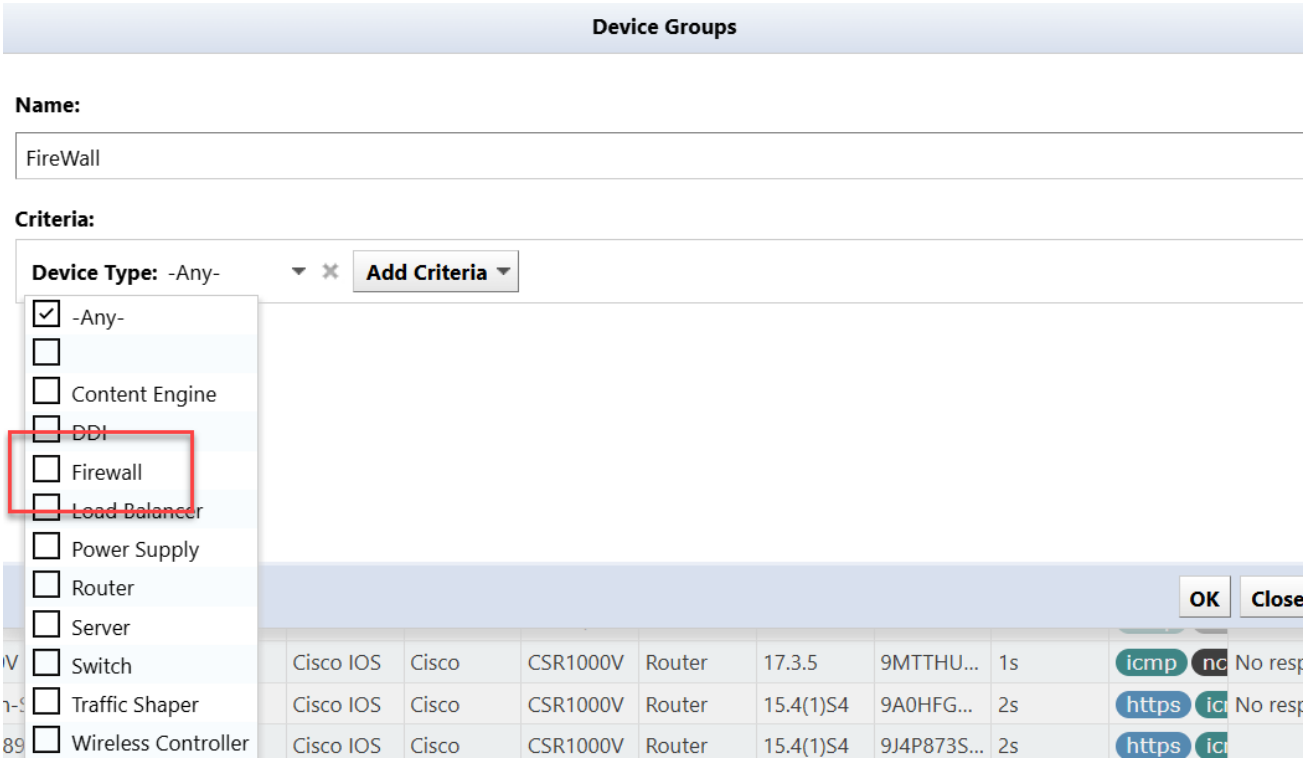
6. In the [Groups] sidebar, click on the vendor name, and those devices will appear in the Inventory tab.



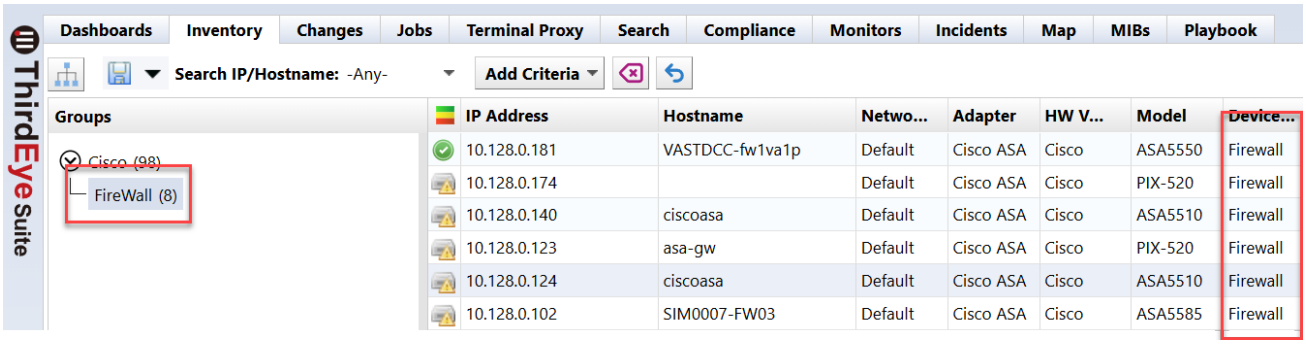
7. To make subgroups, click on the vendor name, and click on the  at the bottom of the page.



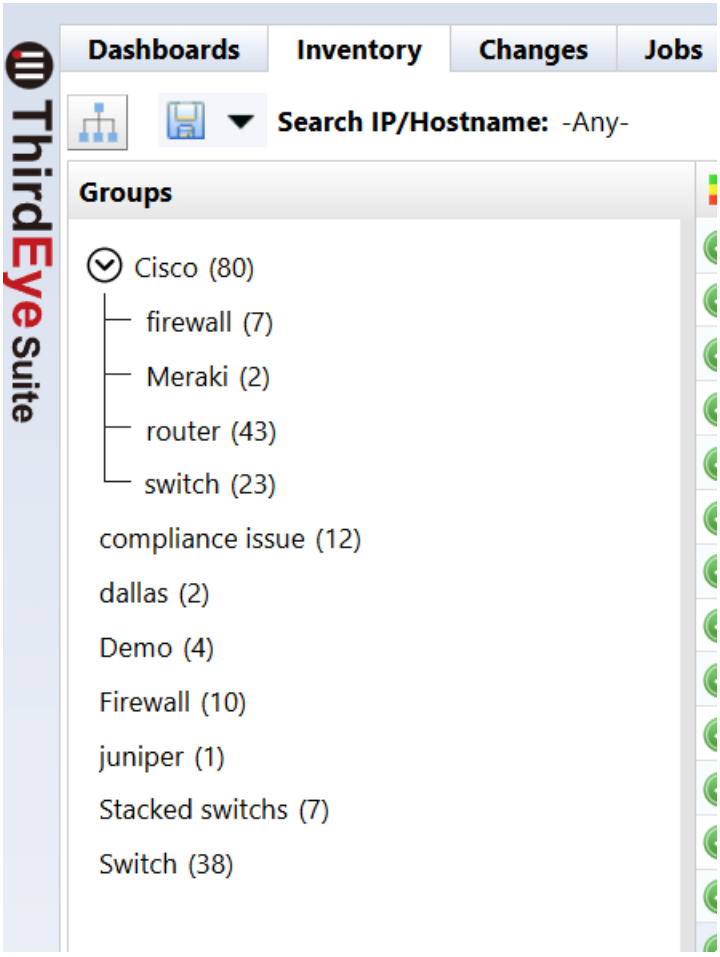
8. Enter a “Name” for the subgroup, (for example “FireWall” in the example below).
9. In the [Criteria] > [Device Type] left sidebar, select your new subgroup (“FireWall” in the example below).
10. Click [OK].



11. Click on the subgroup (“FireWall” in the example below) to display only devices in that subgroup.



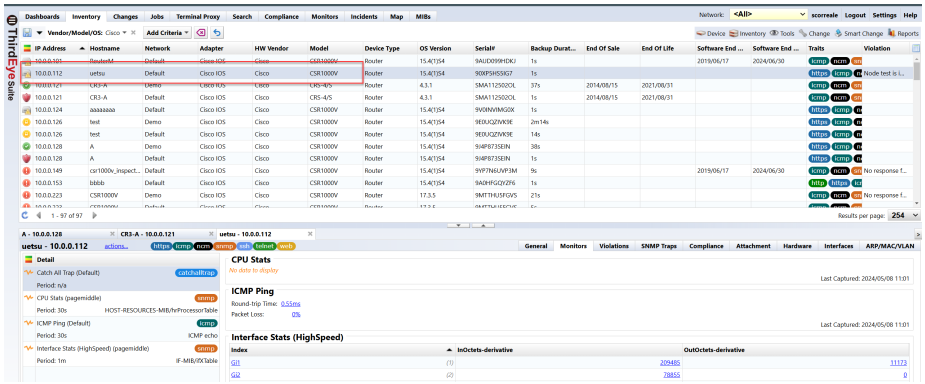
You can use Device Groups to isolate the devices you want to view, monitor, or run jobs against.



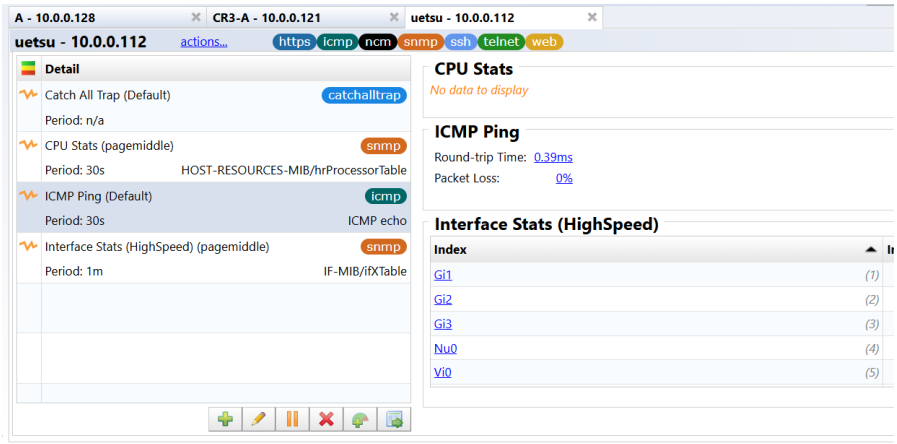
8.2.12 Cancel monitoring settings

8.2.12.1 Remove monitor

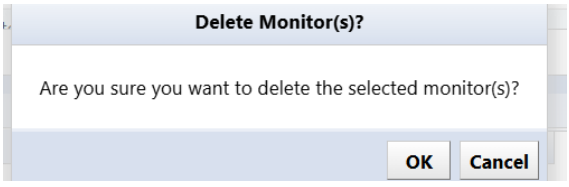
1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.



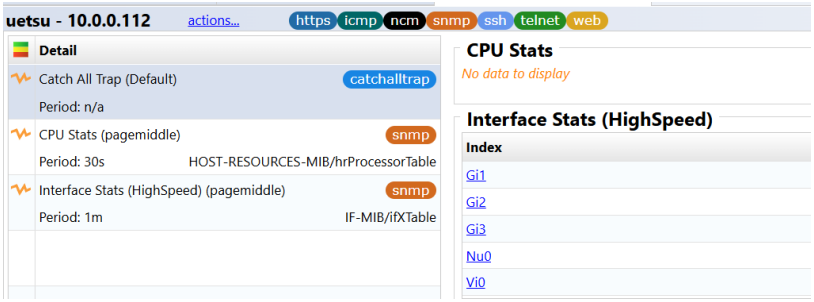
2. Select the monitor you want to delete from the monitor details and click [Delete].



3. Click [OK] on the confirmation screen.

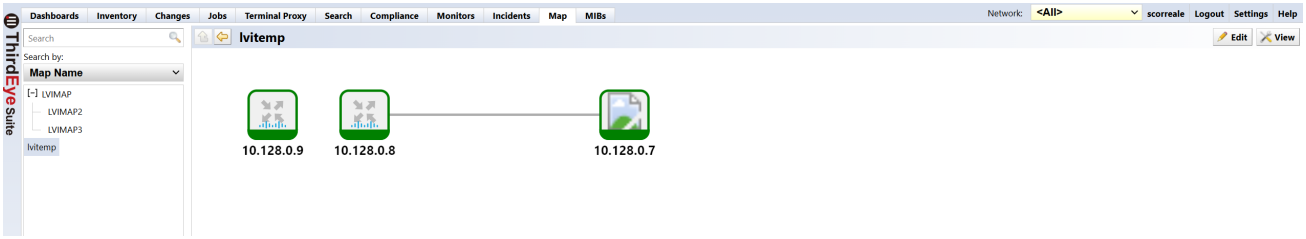


The monitor is removed from the monitor details and data collection is discontinued.

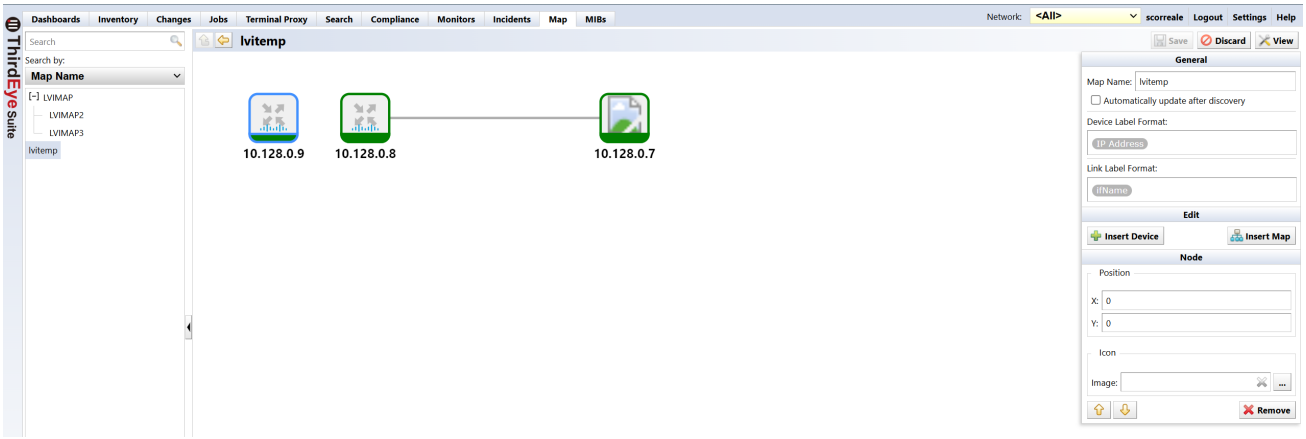


8.2.12.2 Remove an object (device/map) from the map

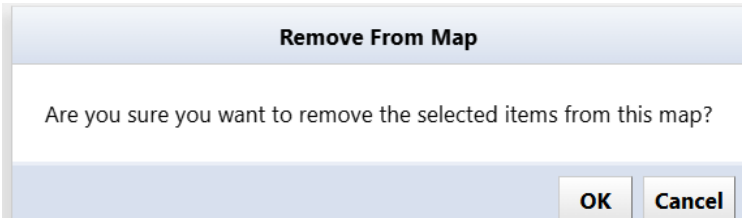
1. Doubleclick a map from the map list on the left side of the screen to open it, and click [Edit].



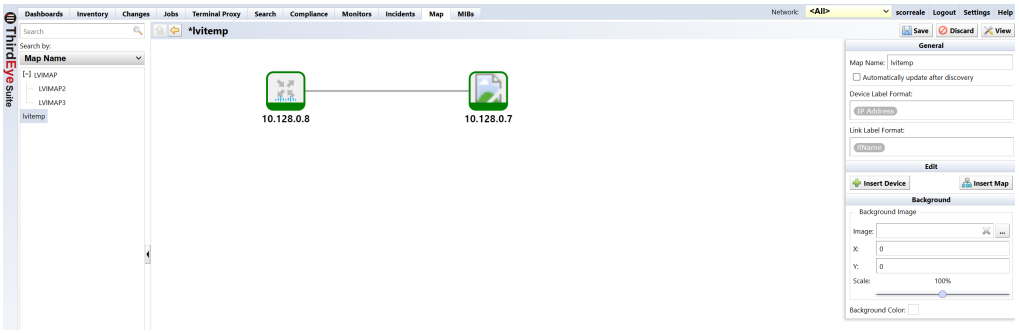
2. Select the object you want to delete and click [Remove].



A confirmation message will be displayed. Click [OK].

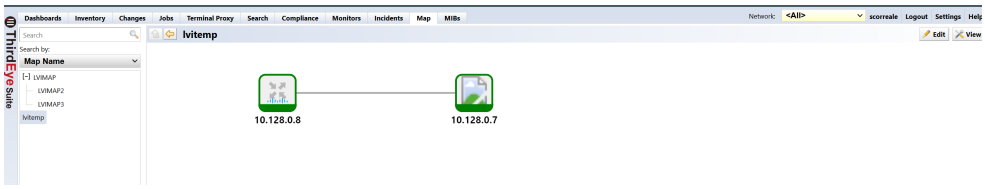


3. The device will be removed. Click [Save] to complete your edits.

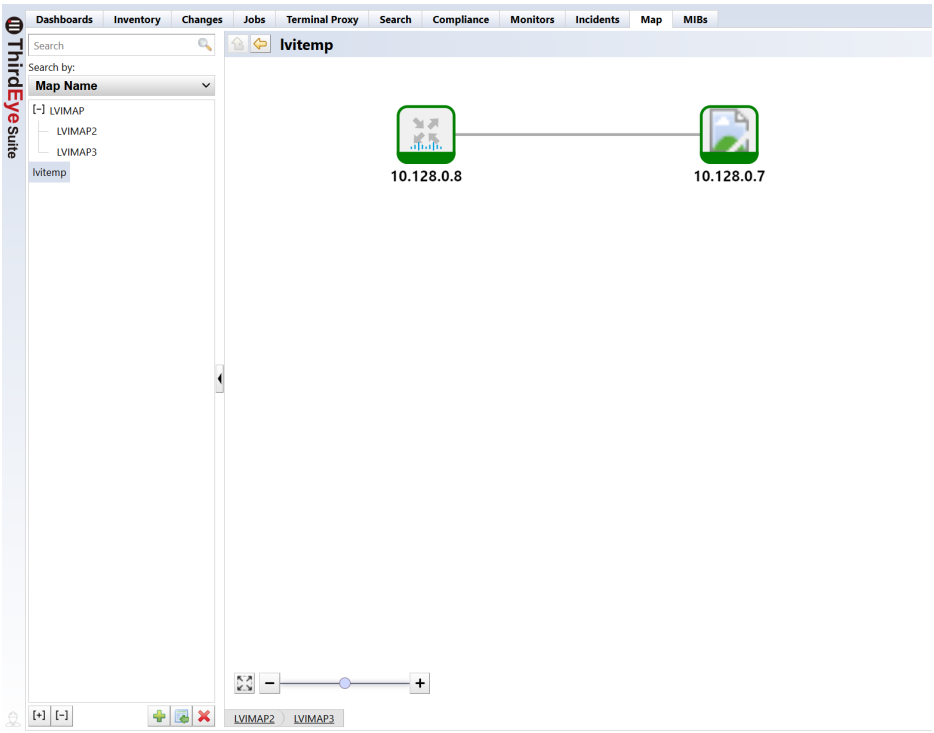


8.2.12.3 Delete map

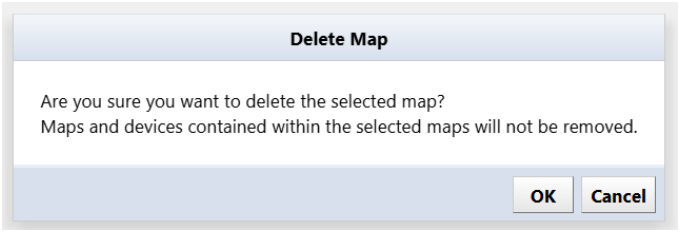
1. Select the map you want to delete from the Map Tree.



2. Click the  button in the bottom left of the window.

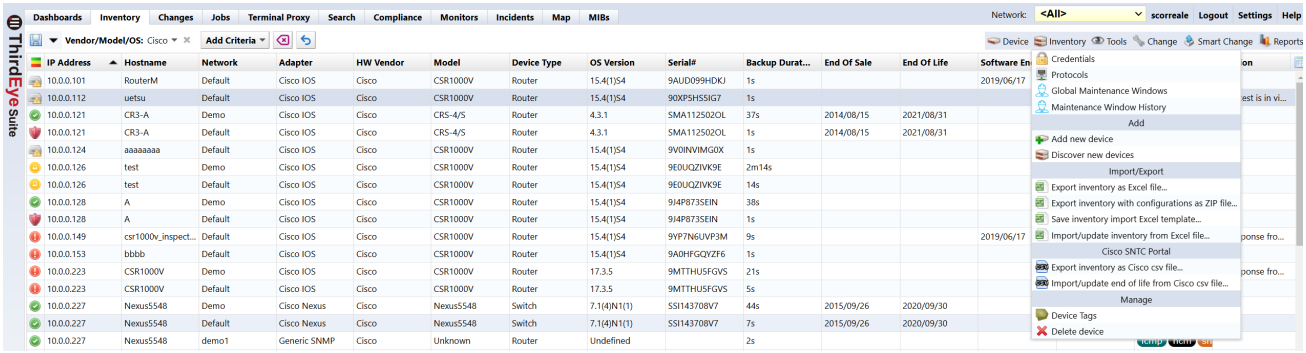


3. A confirmation message will be displayed. Click [OK].



8.2.12.4 Delete device

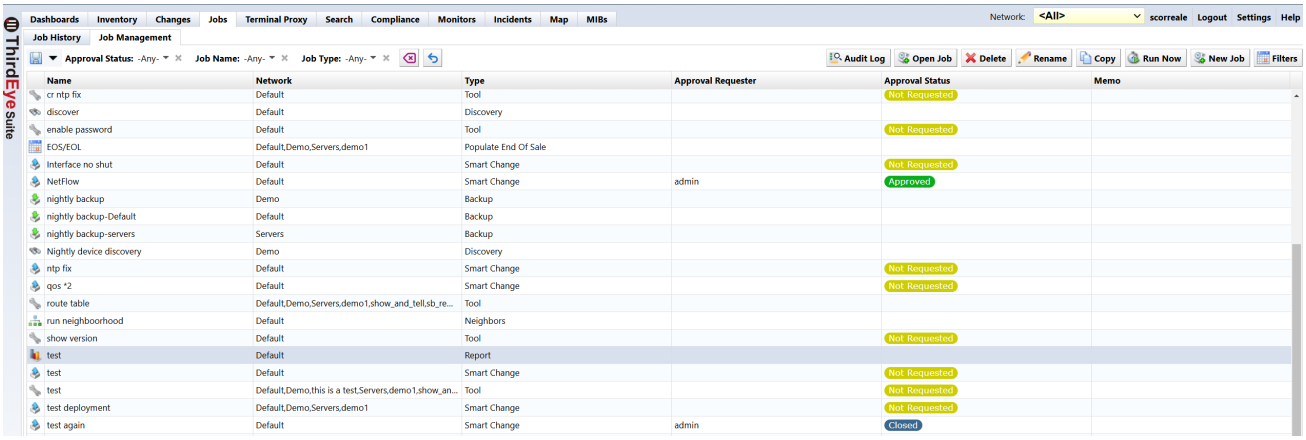
1. Select the device you want to delete on the Inventory tab. Multiple selections are possible.
2. With the device selected, click Inventory > Delete Device.



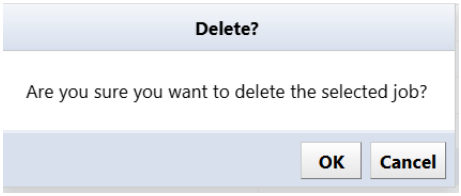
3. A confirmation message will be displayed. Click [Yes].

8.2.12.5 Delete job

1. Click the Jobs > [Job Management] tabs.



2. Select the job you want to delete and click [Delete].
3. Click [Yes] on the confirmation screen.

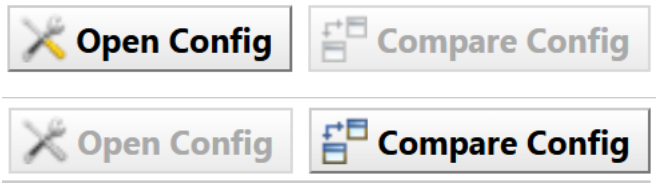


The selected job will be deleted from the job management list.

8.3 Changes

The Changes tab allows you to track and manage network device configurations across deployments. It provides administrators with a centralized view of historical configurations, and enables easy comparison.

The Changes tab contains two main buttons that facilitate this; the [Open Config] button, and the [Compare Config] button.



8.4 Jobs

The Jobs tab consists of a Job History tab and a [Job Management] tab. In the job history, you can view the results of past job executions. The [Job Management] tab allows you to create, edit, manage and run jobs. You can also set the created job to be automatically executed periodically.

The Job History subtab has the following buttons:

Button	Edition
Open Results	Opens the execution results of the selected job.
Compare Results	Compare the results of two selected jobs.
Cancel	Cancels the selected running job.
Job Approvals Log	View the job approval log.

The [Job Management] subtab has the following buttons:

Button	Explanation
Audit Log	View audit log for changing job settings
Open Job	Open the properties of the selected job.
Delete	Delete the selected job.
Rename	Renames the selected job.
Copy	Copy an existing job and create it as new job.
Run Now	Run the selected job immediately.
New Job	Create a new job.
Filters	Register a cron-style filter.

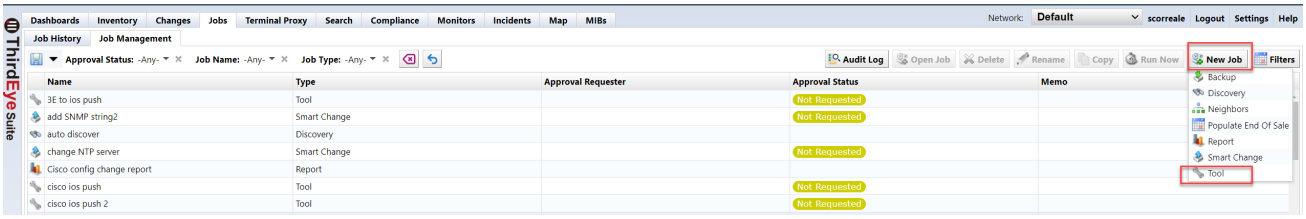
8.4.1 Create a job

Jobs can be created from the submenu under [Job Management] > [New Job]. Various types of jobs are registered in this submenu, but the general flow of creating the job remains the same regardless of the type of job.

Job creation procedure]

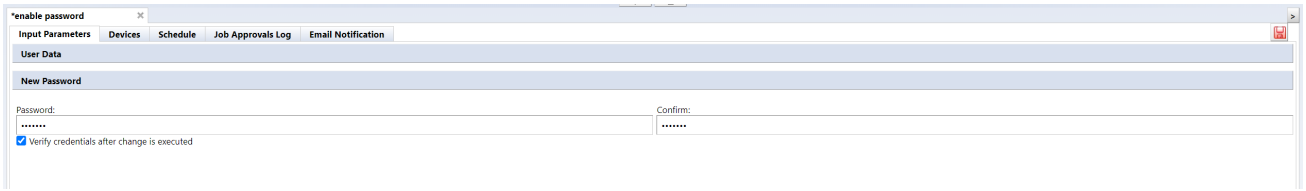
1. Decide on a job name and select the functions you want to use.
2. Enter the required parameters.
3. Select the target device.
4. Finally, enter the job trigger (execution frequency).

Below, we will create a job as a trial and explain how it works screen by screen. Click [New Job] > [Tools].



8.4.1.1 Choose a job name and function First, enter a job name of your choice. It would be a good idea to add comments in the comments section that will be easy for others to understand later. Next, choose your tool. You can select almost all the available tools from the [Tools] > [View tools], and [Change] menus on the Inventory tab. This time, we choose Change Enable Password.

8.4.1.2 Enter the required parameters Then, in the new tab that opens, enter the required parameters. To use Change Enable Password, enter the password string to be changed in the password field.

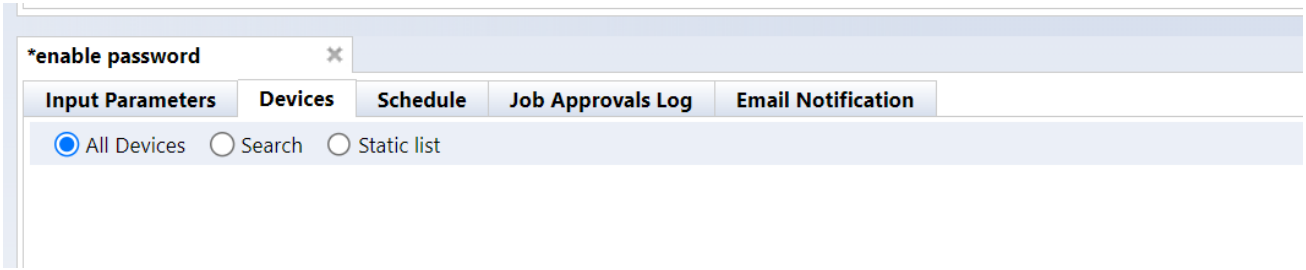


8.4.1.3 Select target device Select the device on which you want to run this job on the [Devices] subtab. There are three selection methods:

- All devices
- Search
- Static list

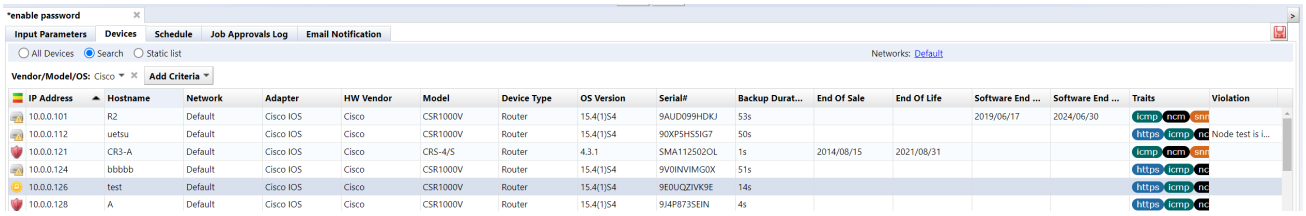
All devices

This applies to all registered devices.



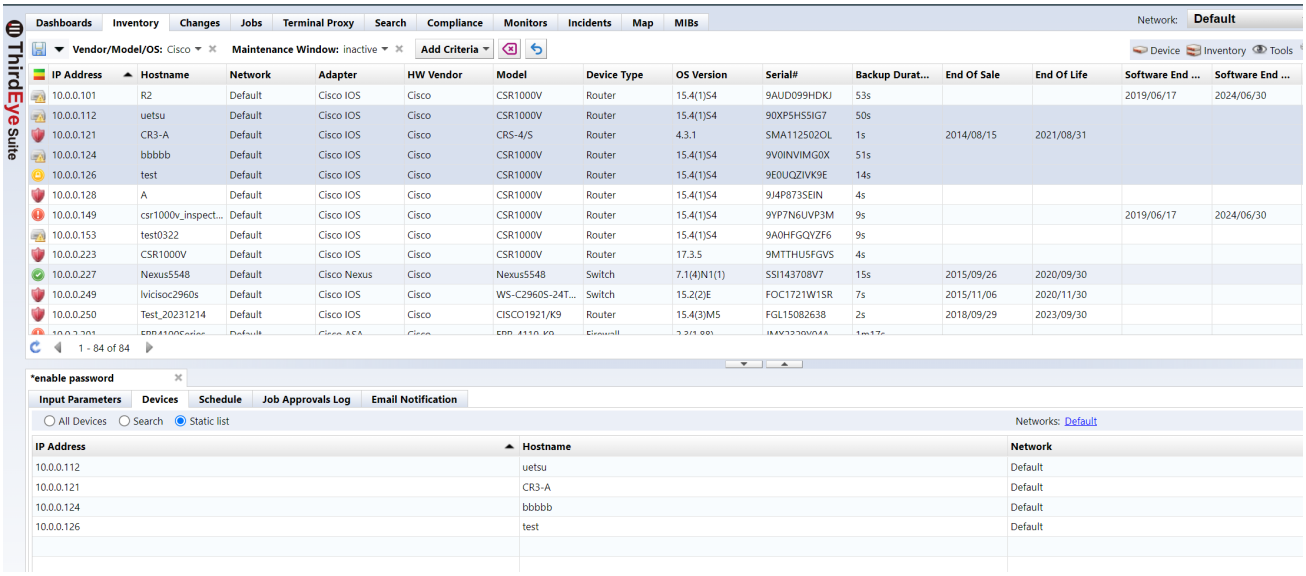
Search

Devices that match the search criteria will be targeted. However, since the search is performed when the job is executed, it does not only target devices that are displayed in the search results list when the job is created. If a device matching the search conditions is added after job creation, that device will also be targeted.

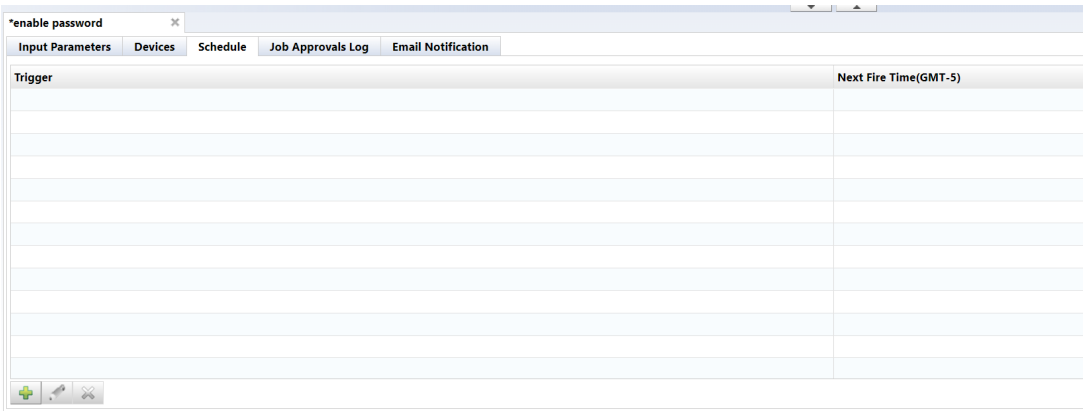


Static list

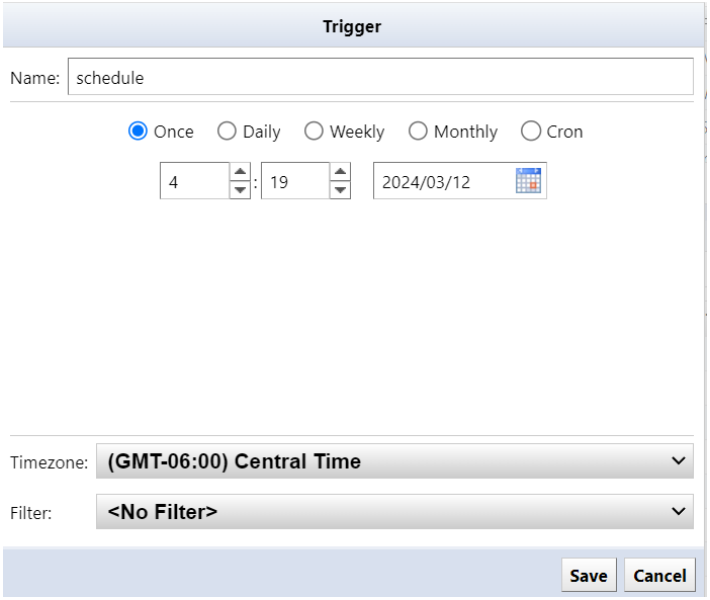
In the static list, you can add the devices selected in the [Devices] tab, and the added devices will be targeted.



8.4.1.4 Add a trigger Finally, add the trigger. Click the [Schedule] subtab. You can add new triggers using the button.



Create a trigger by setting the date and repeat frequency. When you have finished entering all information, click the [Save] button.



Item	Explanation
name	Trigger name
time	Time and date to run the job
Schedule	Select from the following 5 types of execution schedules: - **Once**: Execute only once at the date and time set in the time. - **Daily**: Execute every n days (starting from the 1st of the month) - **Weekly**: Execute on a specific day of the week - **Monthly**: Execute every specified month - **Cron**: Run at the specified date and time in cron format
time zone	Time zone
filter	Select the registered schedule filter in “Filter Settings”. Timings that match this filter will be removed from the trigger.

Finally, at the top right of the status panel, remember to press the  button to save your job settings. Unsaved changes will still exist.

8.4.2 Job history

The [Job] > Job History subtab displays a list of past job execution history. Past job execution status is recorded along with the status of whether the job was successful or failed. The status icon is displayed on the left side of the Job History list. The status icons and their meanings are as follows:

Icon	Explanation
	**Successfully connected to all devices**
	**Processing failed on some devices**
	**Processing failed on all devices**

8.4.3 Job approval function Suite

The approval function is a function that allows a job created or edited by an applicant to be executed when an approver such as a superior approves the job. Jobs that do not have approval will not be able to run. By using this function, you can achieve secure operations such as preventing erroneous operations and strengthening compliance.

This approval function is only valid for jobs that change the settings of network devices.

Approval process

1. The applicant creates/edits a job and makes an [approval request] (approval request)
2. The person in charge of approval checks the approval request from the [Job Approval Log] in the relevant job.
3. If there are no problems, perform [Approval]. If there is a problem, select [Reject] or [Comment] from the confirmation screen and contact the applicant.
4. After [approval] is performed, the applicant executes the corresponding job.

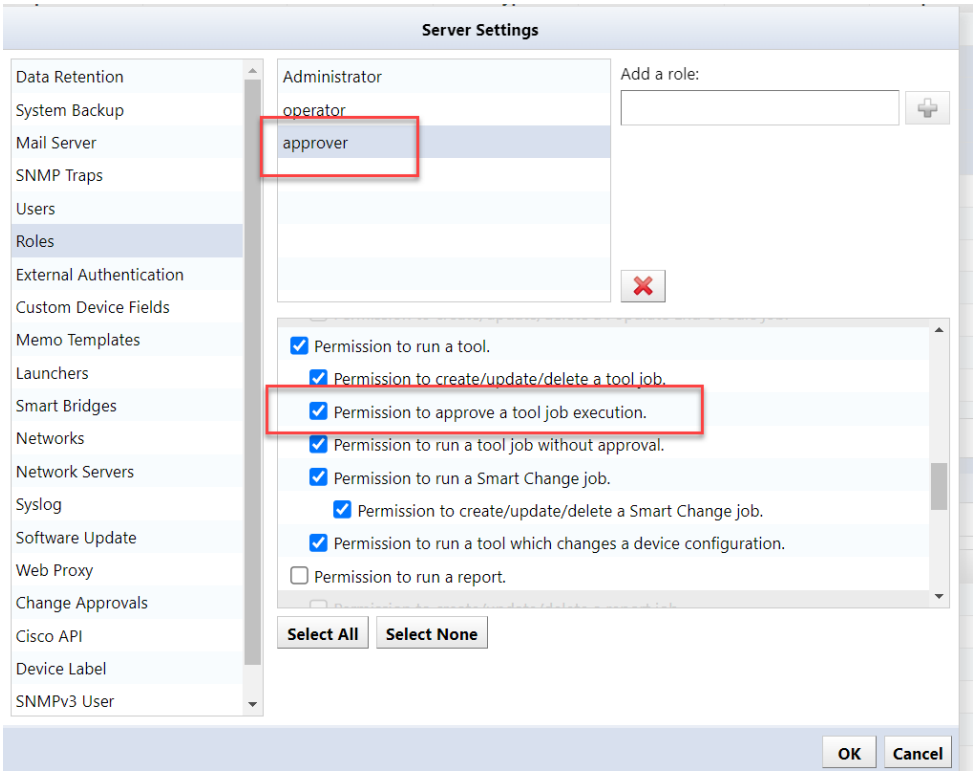
8.4.3.1 Set permissions for approval function Set approvers for registered permissions. Users assigned the configured permissions can approve jobs.

1. Click Settings.
2. Select [Permissions] and select the desired permissions.
3. Specify the permission details and click [OK].

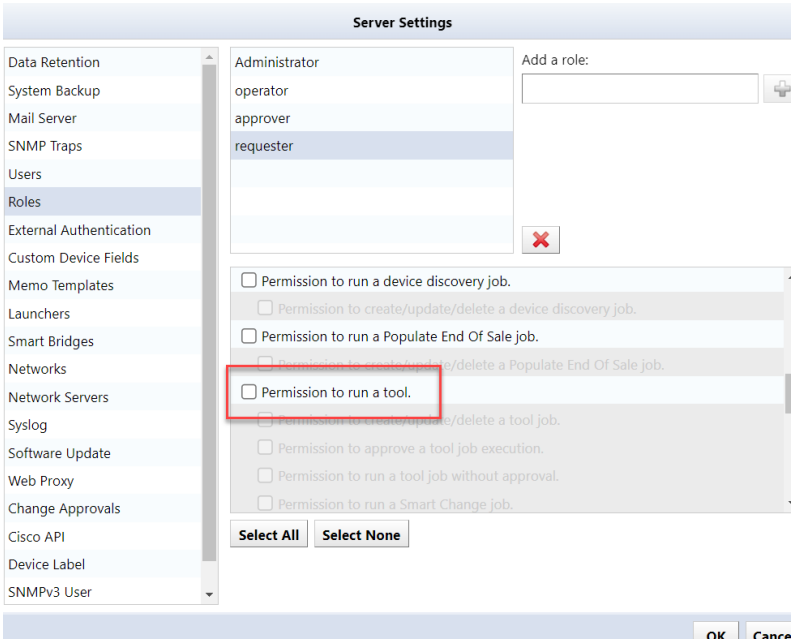
The authority related to the approval function consists of the following two authority contents.

Permission	Explanation
Permission to approve a tool job execution.	Authority to approve jobs that have been requested for approval (approval request).
Permission to run a tool job without approval.	Authority to execute a job without requesting approval.

*When setting the approver's authority, check "Permission to approve a tool job execution."



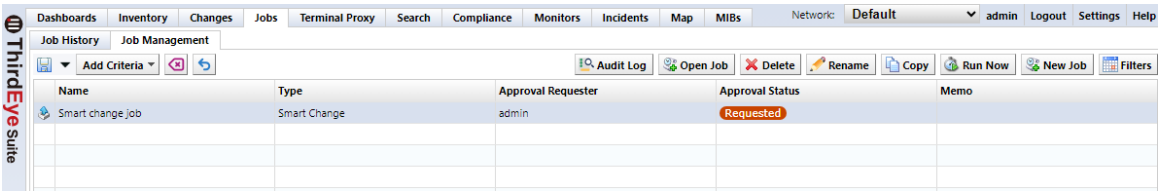
When setting the applicant’s authority, uncheck “Permission to run a tool”.



8.4.3.2 Submit an approval request (submit a job) Applicants can request approval when creating or editing a job.

8.4.3.2.1 Create/edit jobs. Open the [Job Approval Logs] tab, enter a message in the Comments field, and click [Request Approval]. When the application is completed, “Requested” is displayed in the [Approval Status] column.

Display example of the [Job approval status] column



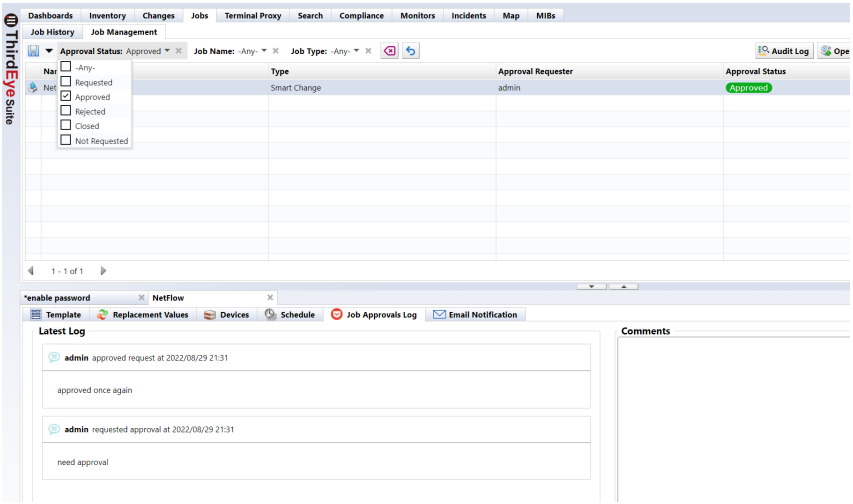
- List of display contents in the [Approval status] column

Job Approval Status	Explanation
Not Requested	Job approval request is not set.
Requested	Job execution approval is requested.
Approved	Job execution is approved.
Rejected	Job approval request has been rejected.
Closed	Job is closed. This status is set when: 1. Job is executed 2. Closed by administrator/job requester If you want to execute a closed job, you will need to request approval again.

8.4.3.3 Approve an approval request (approve the job) Approver can approve jobs (approval requests) applied by applicants.

1. Open the [Job Management] tab.
2. Open the job that has been requested for approval.

You can filter the jobs to be displayed from [Job Execution Approval Status] at the top of the [Job Management] screen.



3. Check the job details and open the [Job Approval Log] tab.
4. Enter your message in the message field and click [Approve].

If you have a problem, enter your message in the message field and click [Reject] or [Comment].

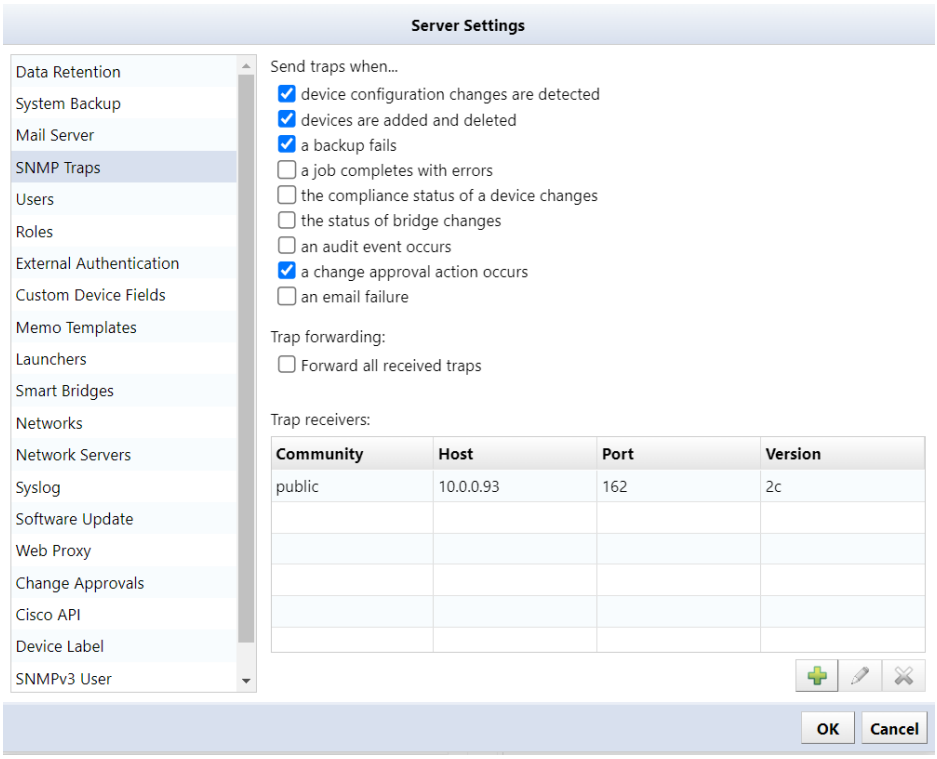
8.4.3.4 Check the record up to approval On the Job History screen, select the target job and click [Job Approval Log] to check the record (messages) up to approval.

The [Job Approval Log] button is enabled only for jobs executed after approval.

8.4.3.5 Notification of approval function When a job is applied for, executed, or completed, notifications can be sent via SNMP trap or email to the relevant job user.

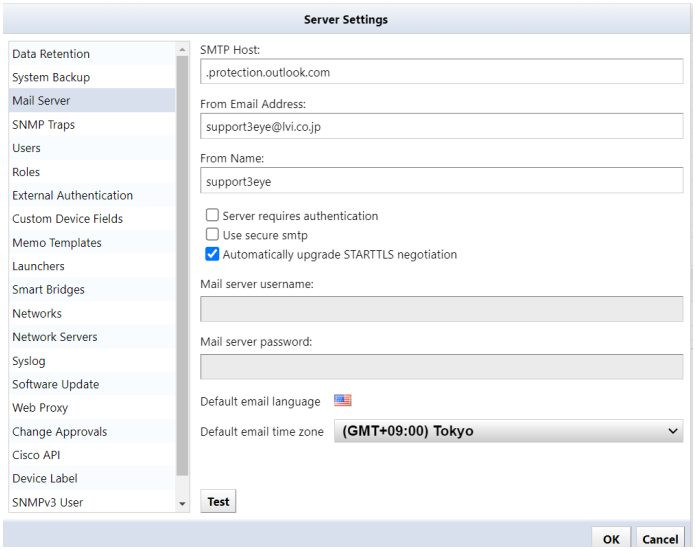
8.4.3.5.1 SNMP trap settings Send a trap when an approval event occurs from the SNMP trap settings on the server settings screen.

A trap is sent when a job is requested/executed/approved/rejected/closed.

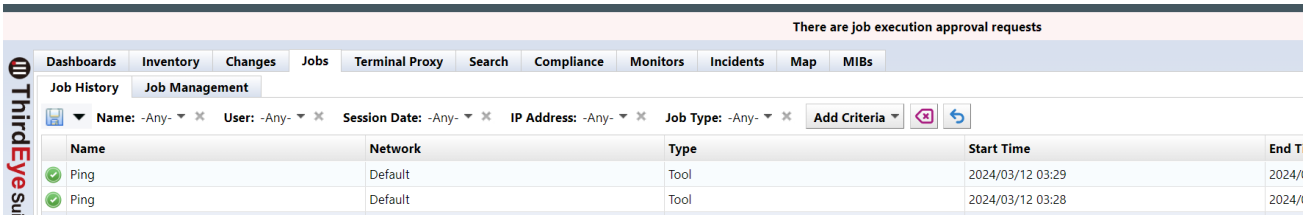


8.4.3.5.2 Send e-mail By setting the email address in the user edit on the server settings screen, you can send an email when an approval event occurs. An email will be sent when a job is requested/submitted/approved/rejected/closed.

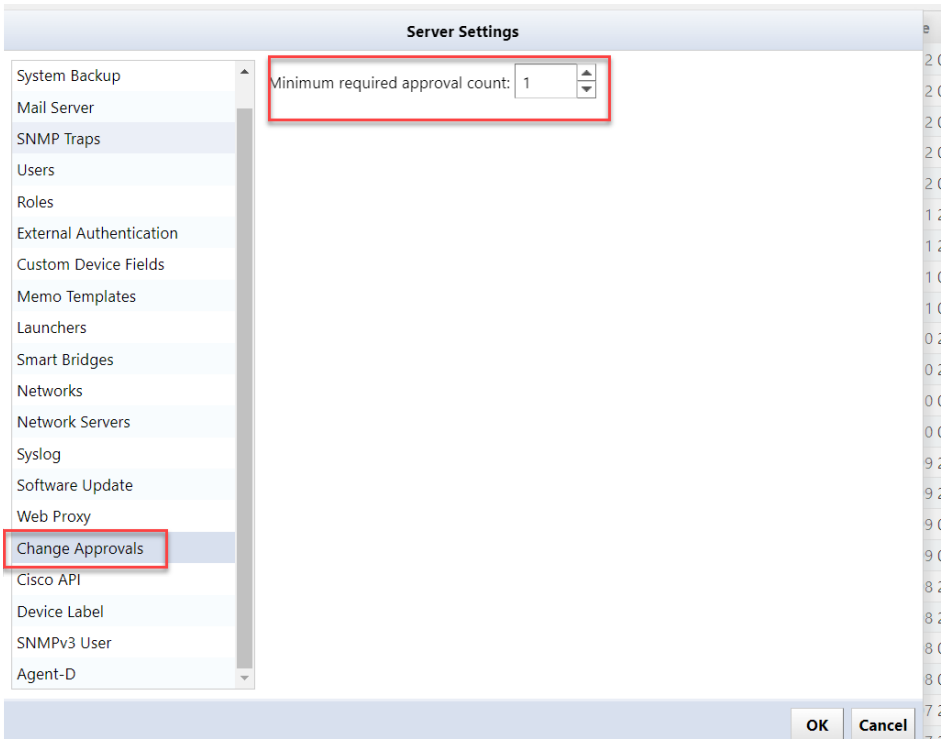
In order to send email, you need to configure the email server in advance.



Additionally, if there is a job approval request, a banner like the one below will be displayed at the top of the screen.



8.4.3.6 Change the number of required approvals You can specify the number of approvals required before a job created or edited by an applicant can be executed. The required number of approvals can be set from Settings > [Approval function]. The configurable range is 1 to 3.



8.4.4 Check past job history

You can check the job history from the Jobs > Job History tabs, and the jobs that have been executed so far are displayed. You can also view published reports by doubleclicking on the report job. Job types include the following:

- Report
- Discover
- Neighbor
- Backup
- Agent-D
- Tool
- information such as “when”, “who”, and “what was done” is recorded

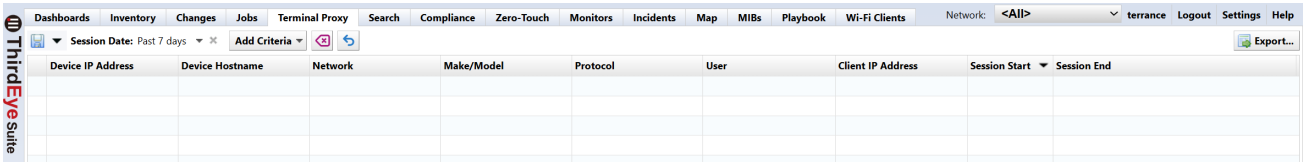
[Column list]

Item	Explanation
Name	Displays the name of the job.
Type	Displays the job type.
Start Time	Displays the start date and time when the job was executed.
End Time	Displays the completion date and time when the job was completed.
User	Displays the name of the user who executed the job.

8.5 Terminal Proxy

The Terminal Proxy tab allows you to securely connect to network devices (SSH/Telnet) On the Terminal Proxytab, you can:

- Establish SSH/Telnet connections through a centralized proxy
- Record sessions and log all commands
- Manage credentials securely
- Apply uniform security controls (timeouts, role restrictions)



The Terminal Proxy tab provides information about devices such as:

- Device IP Address
- Device Hostname
- Network
- Make/Model
- Protocaol
- User
- Client IP Address
- Session Start
- Session End

You can export information about selected devices, or search filter results by clicking the [Export] button in the upper right corner of the window.

8.5.1 Make an SSH/Telnet connection to the device

You can connect to monitored devices via SSH/Telnet from the device list. This feature is called “terminal proxy.” A terminal proxy automatically saves the commands and output you run on your terminal.

8.5.1.1 Terminal Proxy Setup There are two ways to use terminal proxy: using a web browser and using Tera Term. When using Tera Term, the following preparations are required.

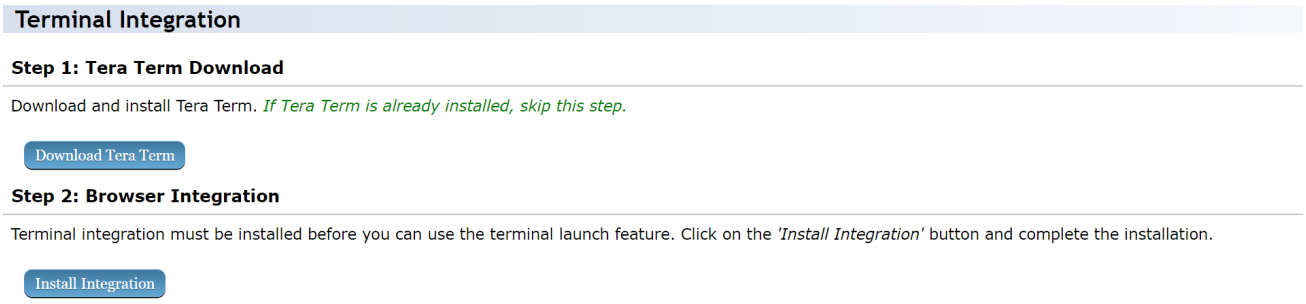
- Install Tera Term on the terminal to be operated (The terminal proxy calls Tera Term on the PC you are operating.)
- Install browser integration

It is necessary to link the browser connected to ThirdEye and Tera Term.

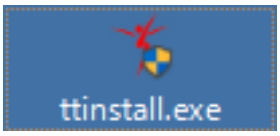
This preparation can be done from the screen that appears when you start the terminal proxy for the first time. The installation procedure for **Browser Integration**”** is described below.

For information on installing Tera Term, please skip to the **Tera Tera** section.

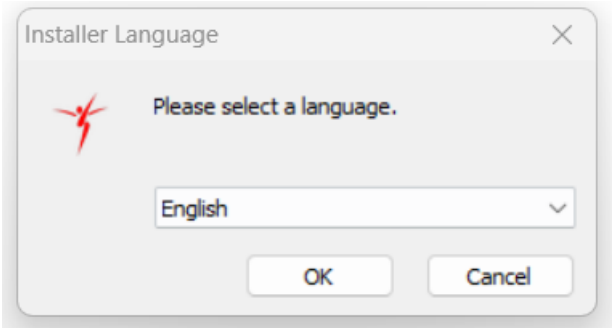
1. Click [Install Integration] and download the `ttinstall.exe` file.



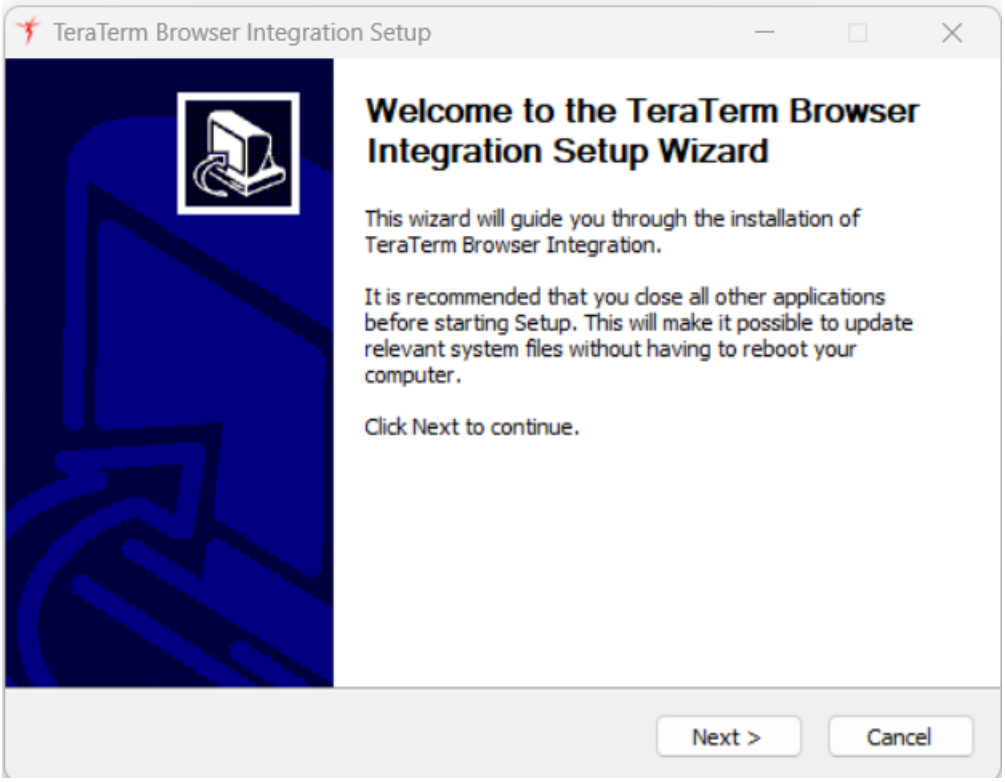
2. Run the downloaded `ttinstall.exe` file.



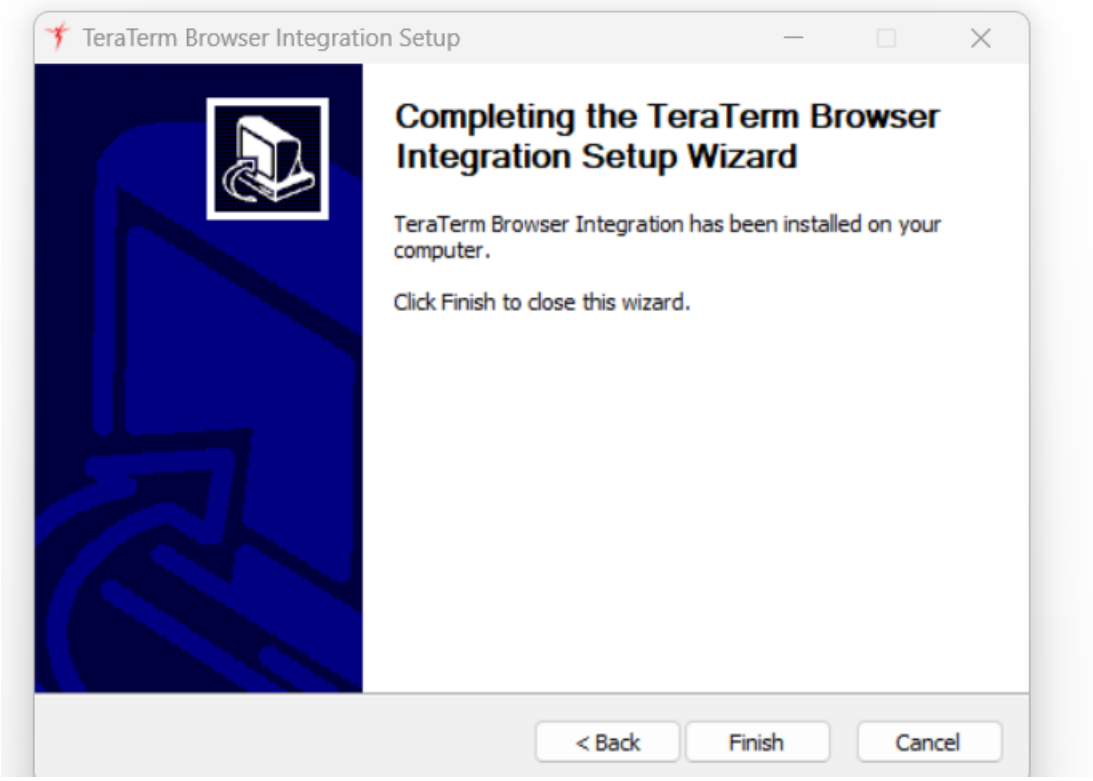
3. Select the display language and click [OK]



4. Click [Next].



5. Click [Finish].

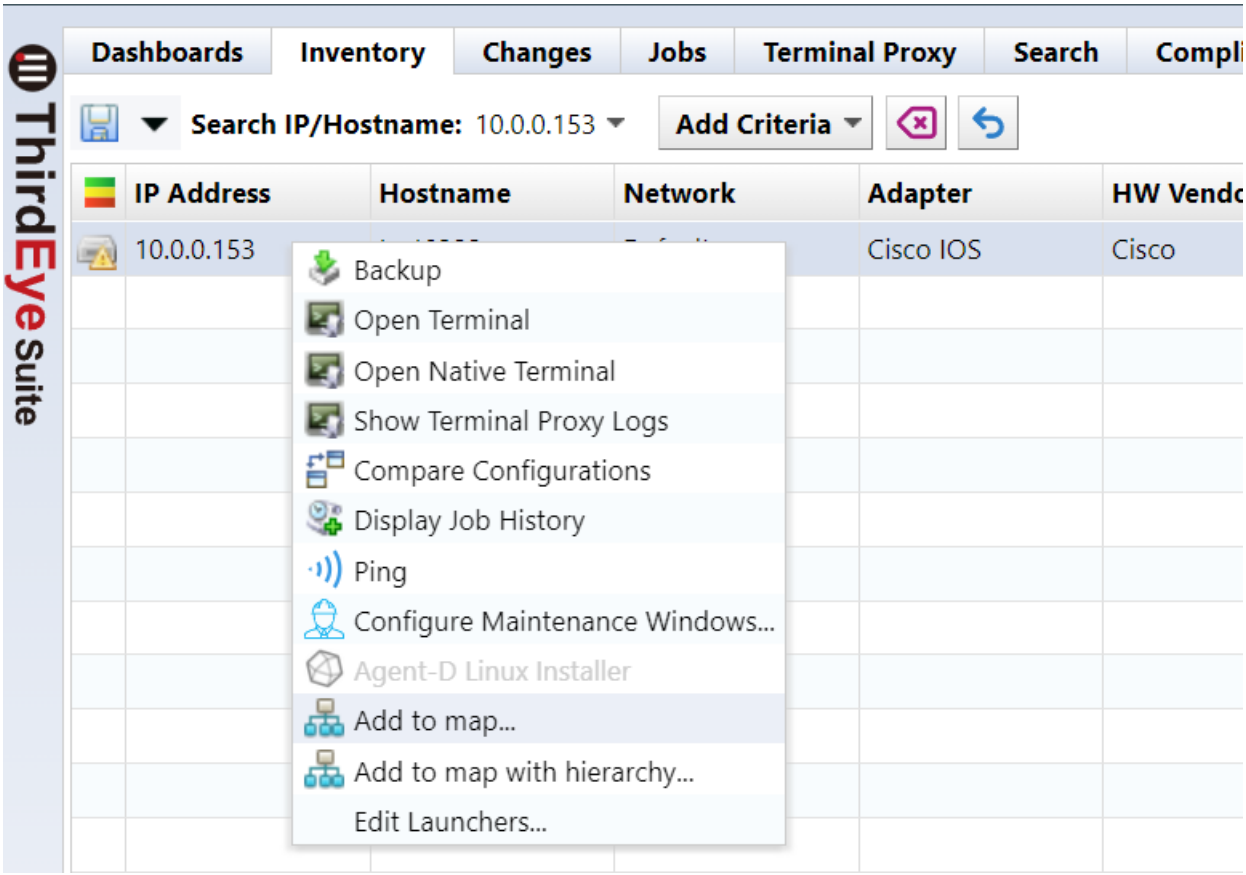


Preparation is now complete.

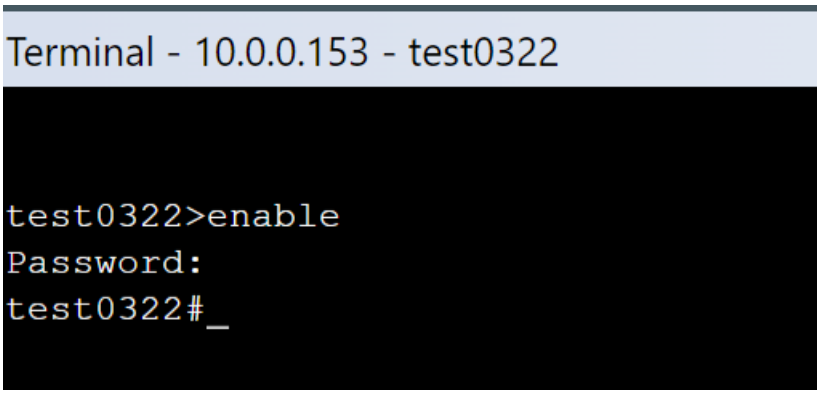
8.5.1.2 Start the terminal proxy If a device configuration backup has been obtained when you start the terminal proxy, you can skip selecting the protocol and entering the user name/password after starting the terminal proxy.

8.5.1.2.1 Use web browser

1. Select the Inventory tab.
2. Right-click the device to which you want to connect the terminal and select [Open Terminal].

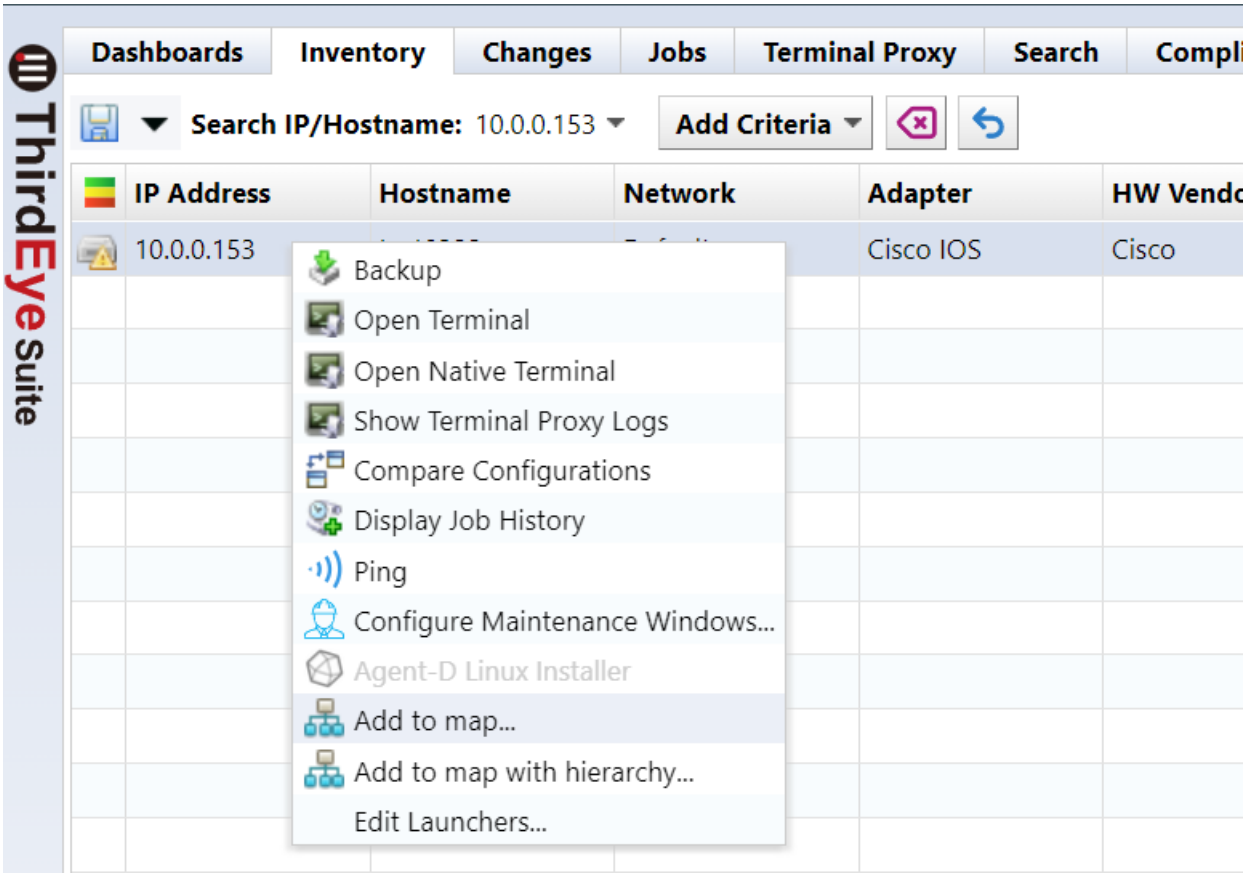


3. The terminal will open in a separate browser tab, and the device's login screen will be displayed. Enter your username and password to log into your device.

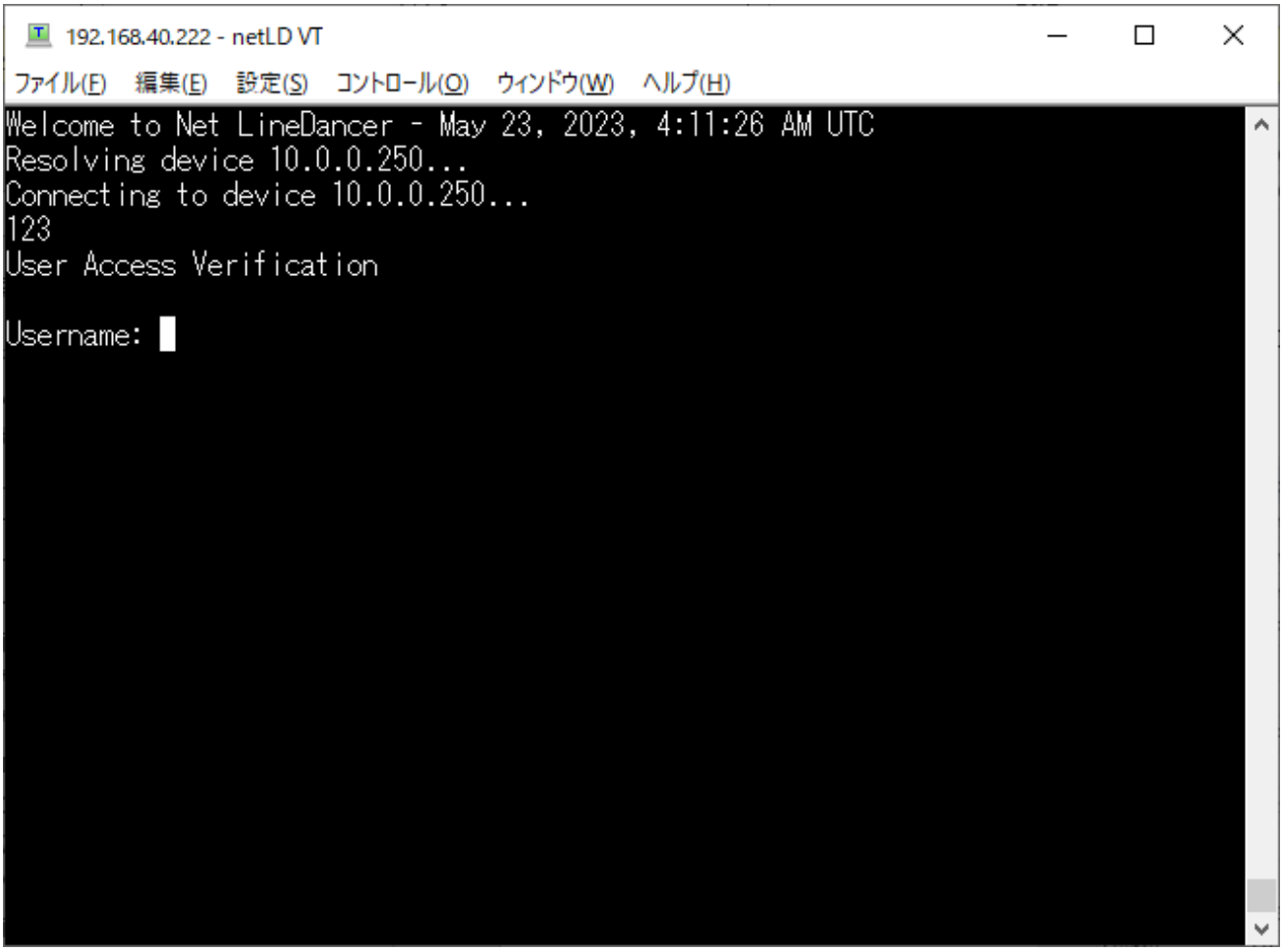


8.5.1.2.2 Use Tera Term

1. Select the Inventory tab.
2. Right-click the device to which you want to connect the terminal and select [Open Native Terminal].
3. The [Select Protocol] screen is displayed. Select the connection protocol and click [OK].

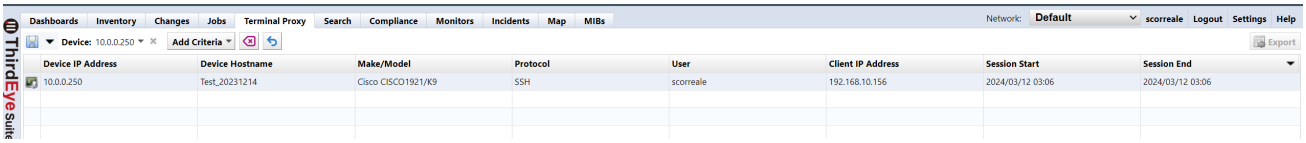


Tera Tera will start and the device login screen will be displayed. Enter your username and password to log into your device.



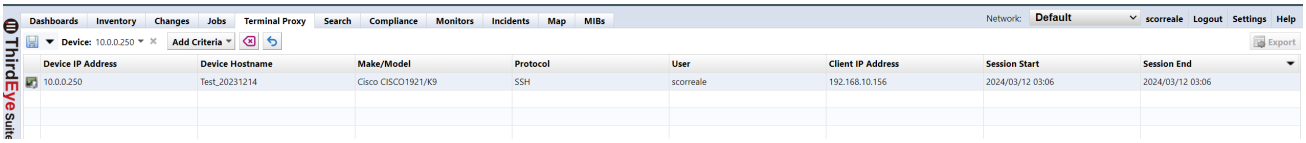
8.5.1.3 Check the operation log

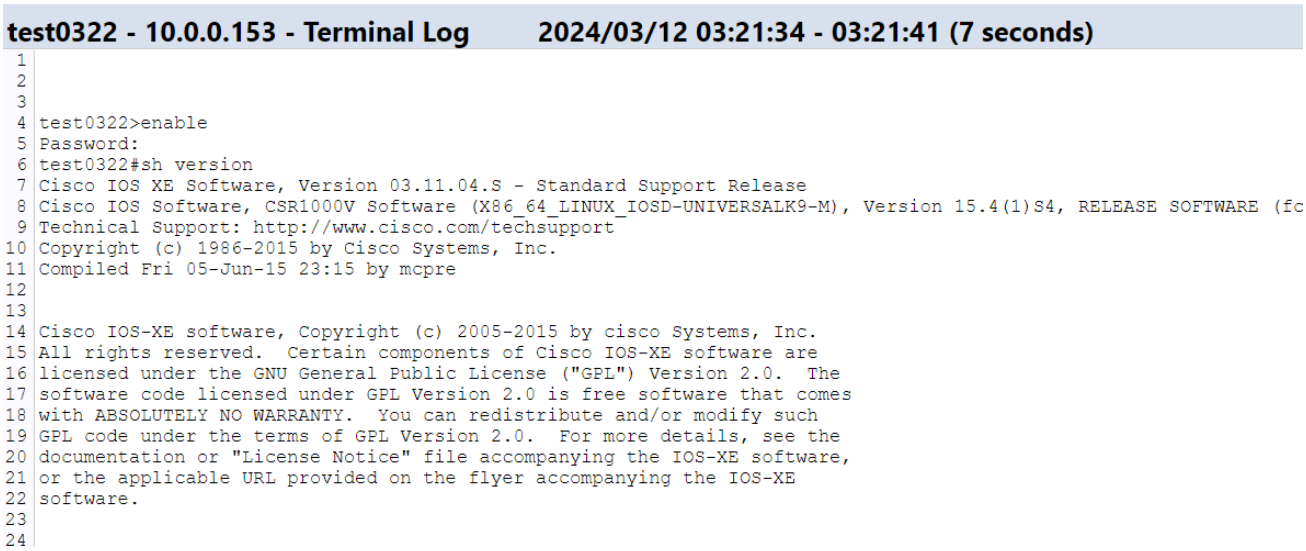
1. Select the Terminal Proxy tab.



2. Doubleclick the log you want to view from the list.

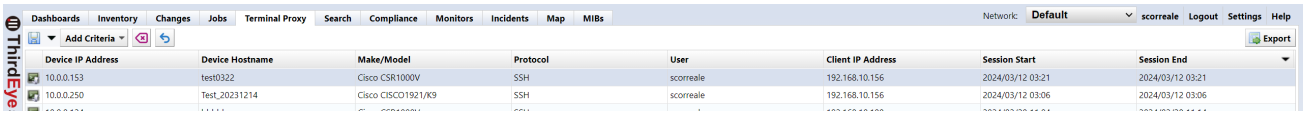
(You cannot check the session log while connected.)





3. Click [Export] at the top right of the log screen to save session data as a text file.

The file name is “`termlogs".*YYYY-MM-DD*.zip`” and is compiled in ZIP file format. “`*YYYY-MM-DD*`” indicates the date of saving.



8.6 Search

The Search main tab serves as a centralized investigation interface. In ThirdEye, it enables network-focused searches including switch port tracing, ARP record lookups, and interface configuration queries.

8.6.1 Search subtabs

The Search main tab contains three subtabs:

- [Interfaces]subtab
- [Switch Port Search] subtab
- [ARP Search] subtab (Results are based on ARP entries)

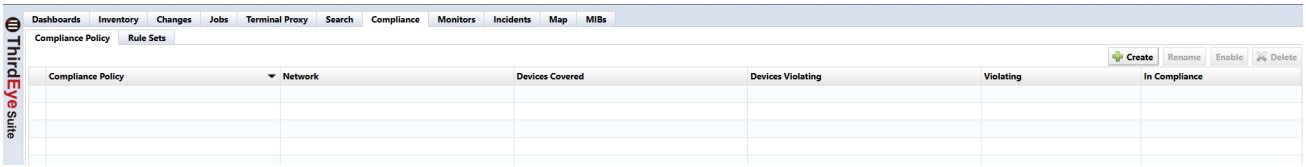
Doubleclicking a device in the [Inteface] subtab list will display more information about that device at the bottom of the screen:

Device Information	Explanation
General	General information about the device (device name, make, model, OS version, serial number, device type, last backup/snapshot, config, timestamp, size, user).
Compliance	Information about compliance policies and associated messages, violations for Rule Sets.
Attachment	Information about any attachments associated with the device (name, size, MD5 hash)
Hardware	Description of device, and information about device type (chasis, card, memory, power, CPU, slots, model, serial number, version, port number, EOS, EOL)
Interfaces	Device name, alias, type, IP, Speed, MTU, MAC, and any related comments
ARP/MAC/VLAN	Information about device VLAN Member Port names and numbers, and option to collect a snapshot of MAC forwarding tables and ARP tables from the device by clicking the [Run Neighbor Collection Now] button.
Memo	Extra information about the device.

8.7 Compliance

The Compliance tab consists of the following subtabs:

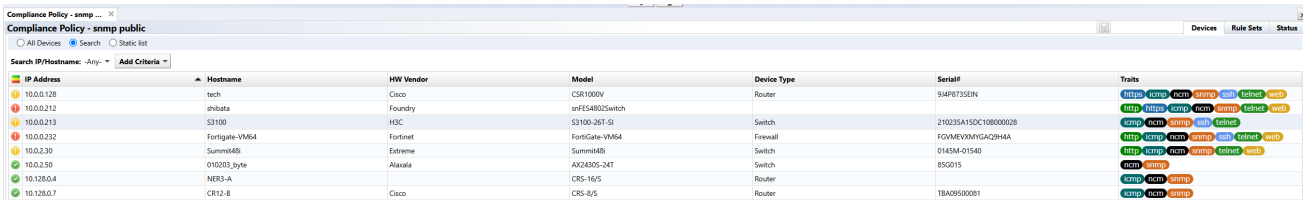
- **Compliance Policy** subtab
- **Rule Sets** subtab



8.7.1 Compliance Policy subtab Suite

This subtab selects which devices the policy applies to. The input interface is the same as that of [Job Management]. You can select devices using three criteria:

- **All devices**
- **Search**
- **Static list**



Item	Explanation
All devices	Apply policies to all devices.
Search	Applies the policy to devices that match your search criteria.
Static list	Apply the policy to the selected and added devices on the Devices tab.

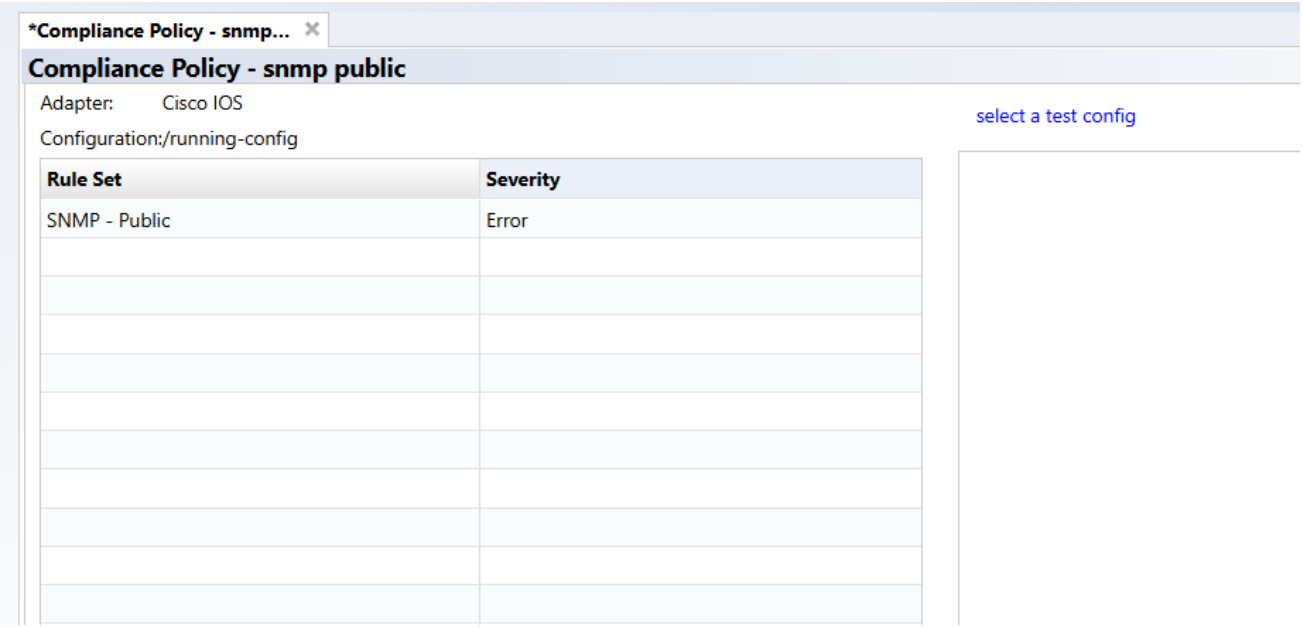
By setting a compliance policy, you can automatically ensure device configuration settings. For this automatic detection, you need to create a device compliance rule. A rule is constructed using the following four matching conditions.

- If matched, it is excluded.
- If it does not match, it is not applicable.
- If matched, it is a violation.
- If it does not match, it is a violation.

Each condition has a single search string, and checks if the given configuration matches that string. A collection of compliance rules is called a Rule Set. Rule Sets can customized.

In addition, policies can be used to manage compliance on a larger scale. A policy is created by combining multiple Rule Sets. It also contains information such as the list of devices to which it applies, the severity of violations (errors, warnings, or notifications), and the violation history.

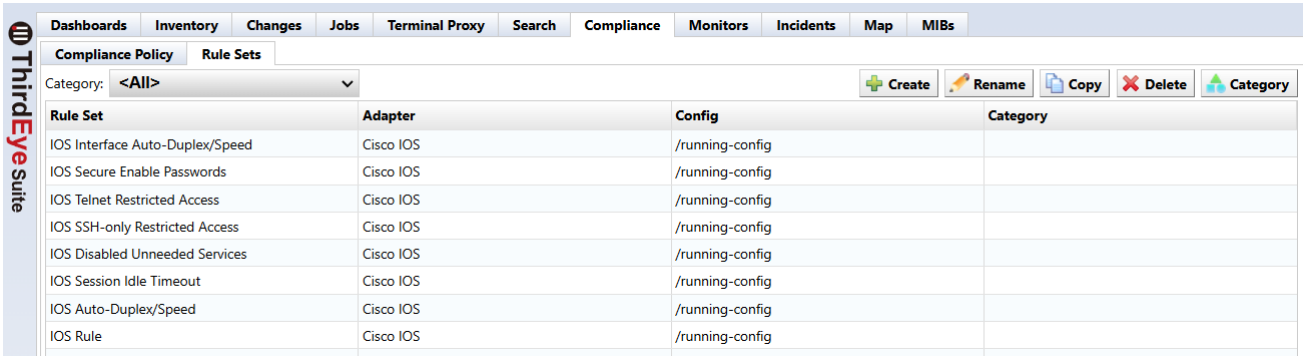
Doubleclick a [Compliance Policy] to open the Compliance Policy window.



Item	Explanation
Adapter	Displaying adapters to which the policy applies.
Configuration	Displaying the configuration to which the policy is applied.
Rule Set	A rule added to a policy.
Severity	You can select the failure level from error or warning. The icon displayed when a policy is violated is different.

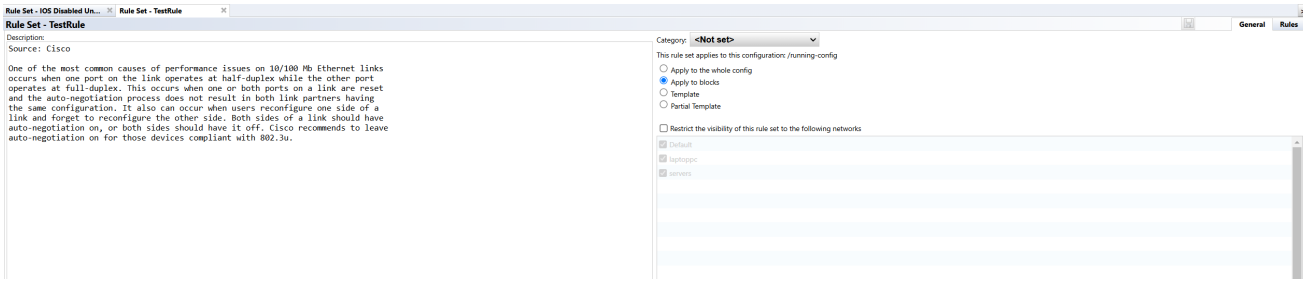
8.7.2 Rule Sets subtab

The [Rule Sets] subtab manages Rule Sets. On this subtab, you can register the created Rule Set to the policy.



Doubleclicking a Rule Set displays its contents in a new tab on the righthand side of the screen. The new tab has two further subtabs, the [General] subtab and the [Rules] subtab.

- **General tab**: You can set rule descriptions and scopes for applications. Writing explanations for rules becomes important during maintenance. Even a minimumal explanation of the rules is helpful, but it is best to also add an easy-to-understand explanation.



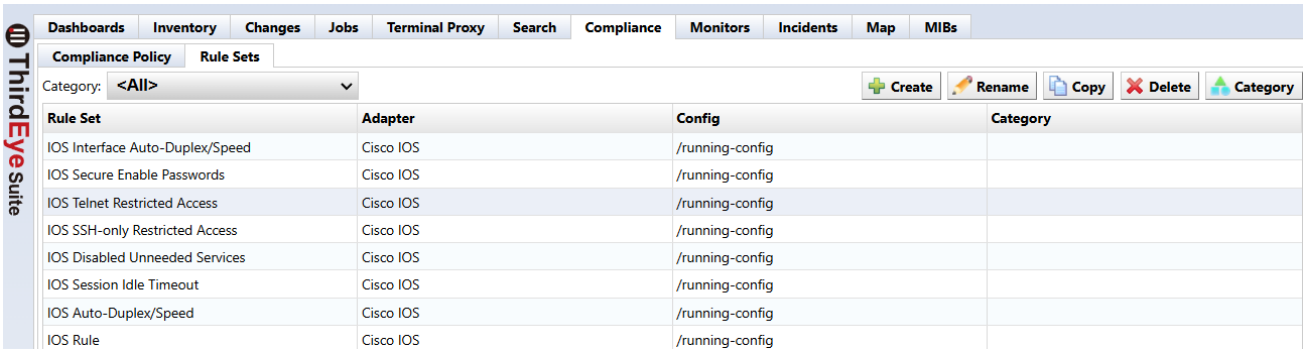
General Items	Explanation
Category	Select a category for the rule.
Description	Enter a description for the rule.
Apply to the whole config	Applies the rule to the entire configuration.
Apply to block	Divide the configuration into blocks and apply rules to each blog.
Template	The configuration is compared line by line from the template, and if there is a difference, it will be a violation.
Partial Template	The configuration is compared line by line against the template, but the comparison can be started from anywhere in the config text, not just from the first line.
Restrict the visibility of this Rule Set to the following networks	Enabling the check limits the networks to which the rule applies.

- **Rule subtab**: You can configure the rule itself.

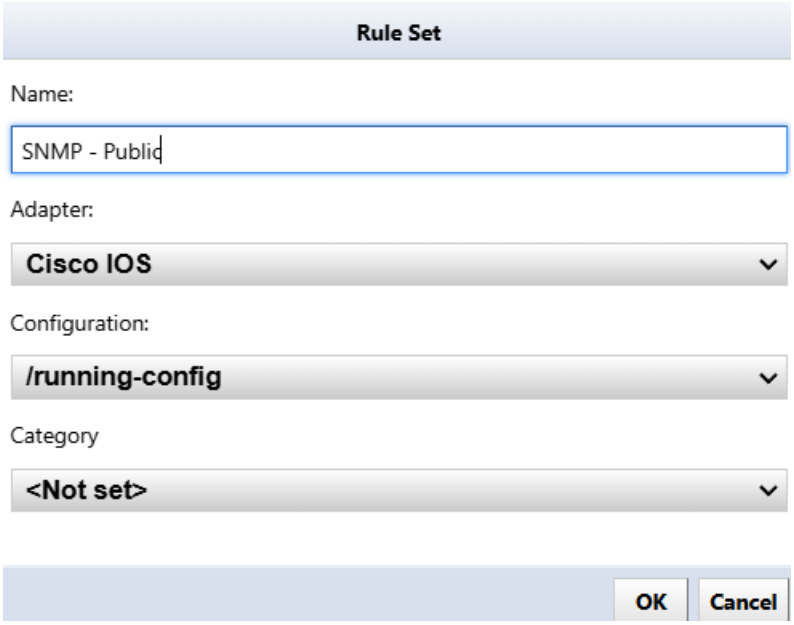
Rule Sets Item	Explanation
Violation message	Enter the message that will be displayed if the rule is violated.
Start/End	Specify the range to search for the string specified in the “Match” item. This field appears when Apply to Blocks is selected on the [General] subtab.
Match Expression	Specifies the string to be searched for. You can convert a string into a variable by enclosing it between ~ (tilde). Example: `interface gigabitEthernet ~INT_NUM~`
Action	Select matching conditions: - If it doesn’t match, it’s not applicable - If matched, excluded - If it doesn’t match, it’s a violation - If matched, violation
Variable	Displays the value when a variable is used in the string specified in the “Match” item.
Type	Specify possible types of matches. If it does not match the type, it will be excluded from the search conditions: - Text: Matches all text - IP address: Matches only strings representing IP addresses - Hostname: Matches hostname - Word: Matches words - Regular expression: Search using regular expressions
Restriction	Enter the string or value to search for. If ： is entered, it means “any value is fine”.
Ignore Case	Allows configuring case sensitivity through an explicit “Ignore Case”
Remediation job or playbook . . .	Select a remediation job or playbook for incidents and compliance issues. Define variable Names to be used as Replacement Names in the Job.

8.7.2.1 Creating a new rule In this section we will explain how to create a new rule with screen-shots. The examples below will generate a violation when the SNMP community setting is “public” in the Cisco IOS device configuration.

1. Click the [Create] button on the Compliance > [Rule Sets] tab.

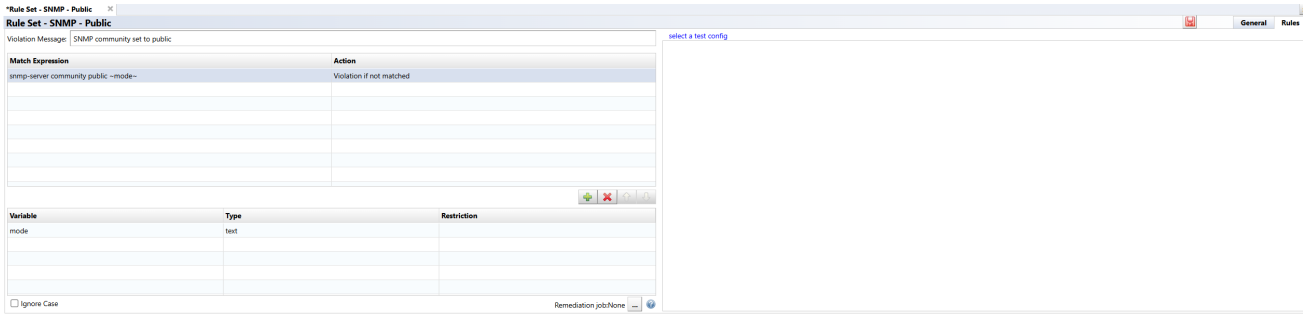


2. The name of the rule, the target adapter (model classification), and which configuration the rule applies to (running-config startup-config) and click the [OK] button.

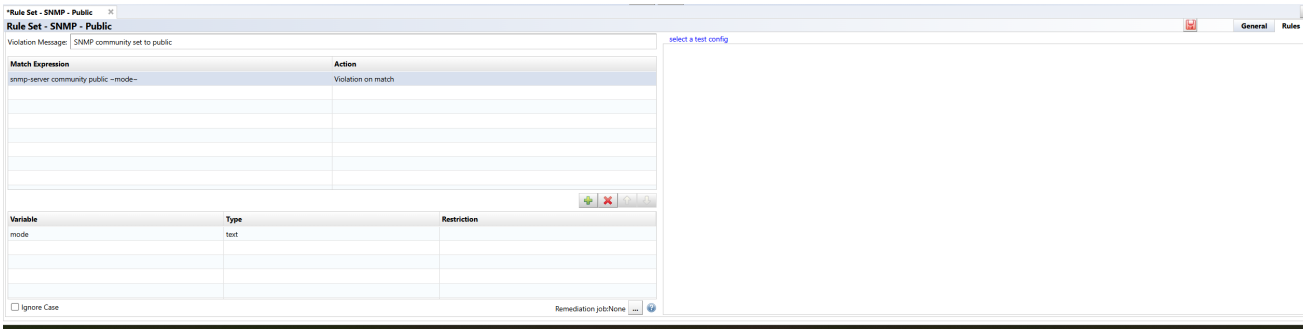


3. In the [Violation Message] field, enter the message that will be displayed when a violation is detected, and click the  button.

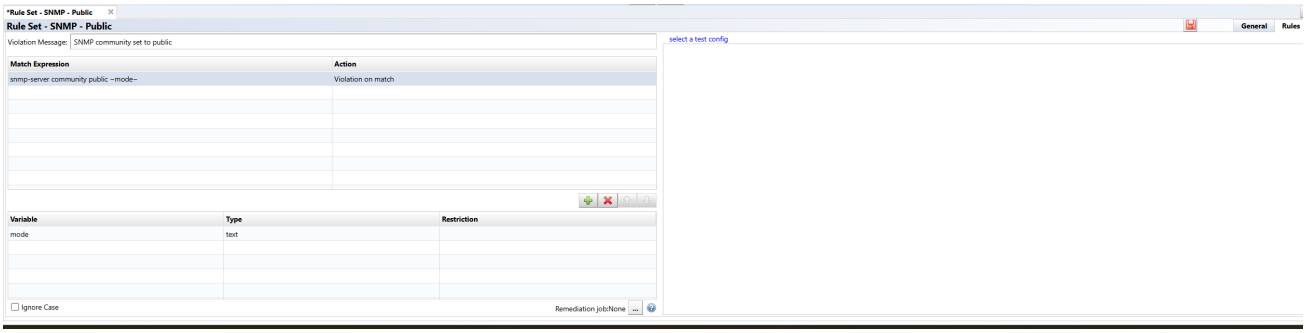
In the example below, the message is “SNMP community set to”public”:



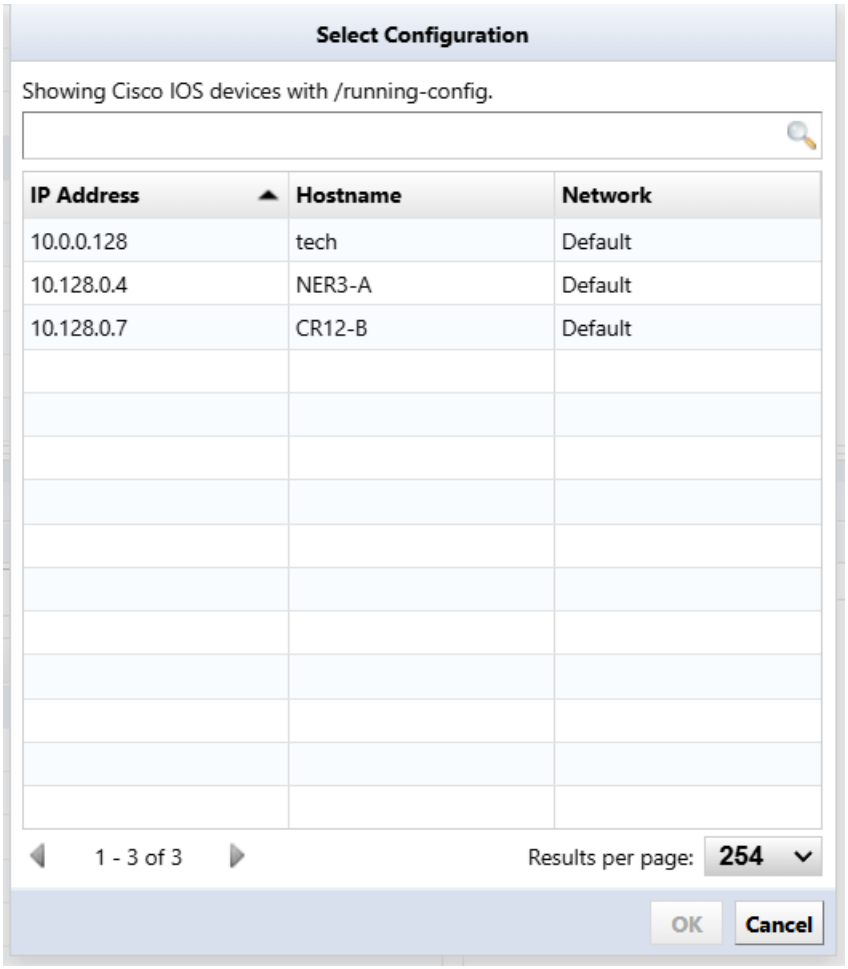
4. In the [Match Expression] column, enter the text that is a violation, and in [Action] column select [Violate on match].



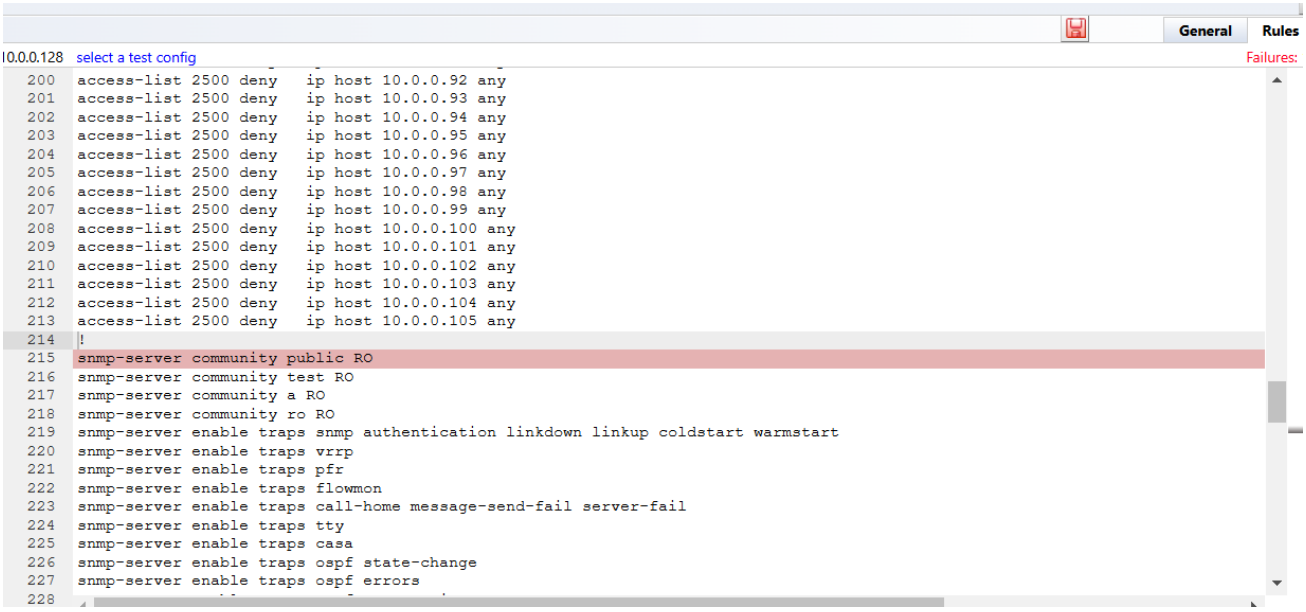
5. If you want to test the rule you created, click [Select a configuration] in the upper right to test and select a configuration from your inventory.



6. The configuration selection window displays a list of devices that apply to the adapter you selected when creating the rule. This column only displays devices that match the IOS adapter you originally selected.

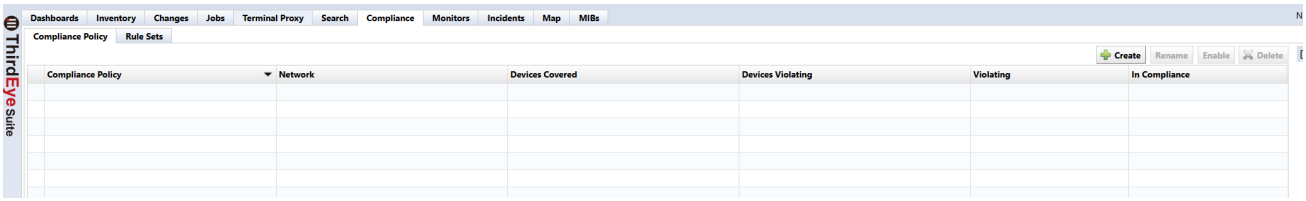


Violations will be searched for against this text rule, and if violations are found, they will be displayed in red. The following section will cover creating policies from this Rule Set.

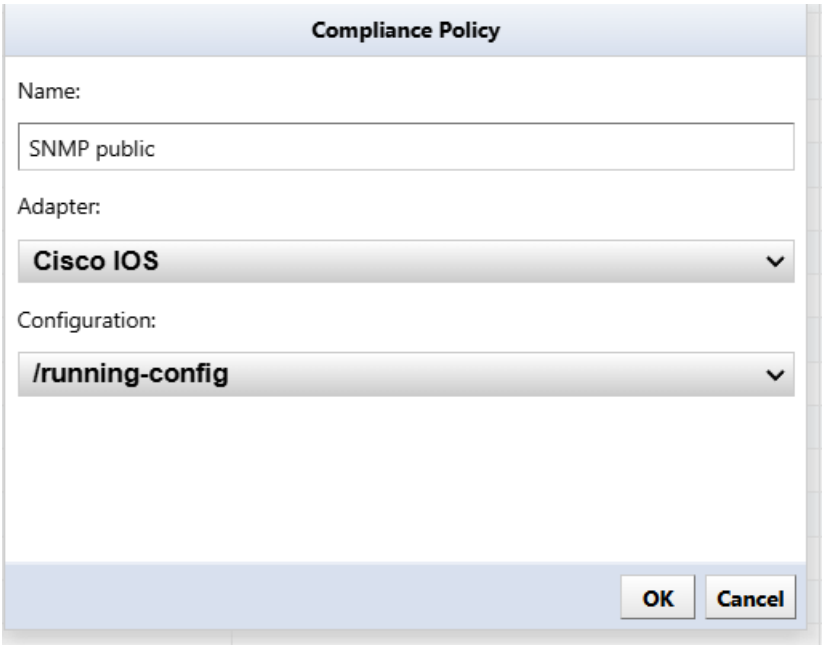


8.7.2.2 Creating a new policy This section will create a policy for a Cisco IOS device configuration using the Rule Set created in the previous section.

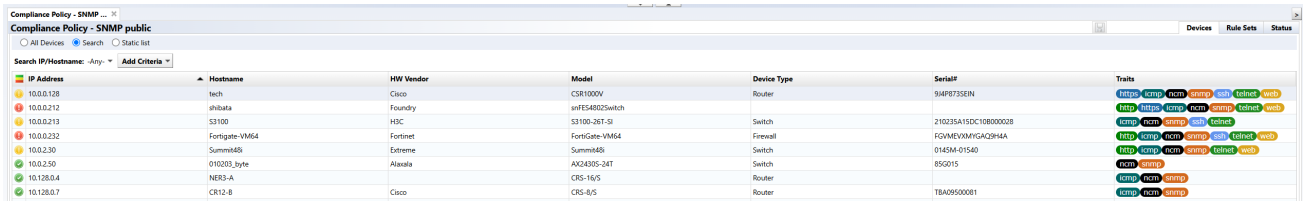
1. Click the Compliance > [Compliance Policy] tabs, then click the [Create] button.



2. Enter the policy “Name”, “Adapter” target , and “Configuration” type, then click [OK].



3. In this example, Search is selected in the [Devices] subtab.



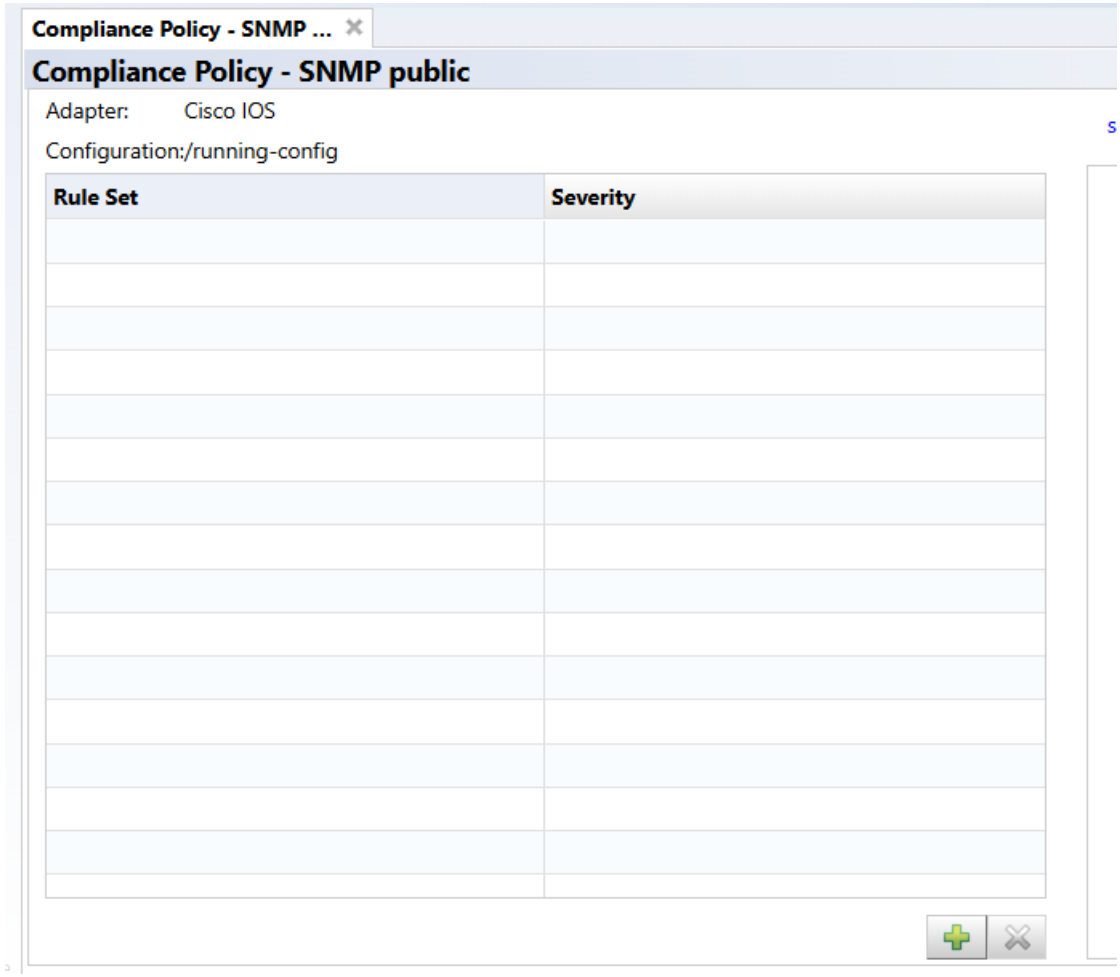
The setting behavior for Search and [Static list] in the [Device] subtab is same as the behavior setting behavior in [Job Management].

Devices will be searched every time a violation check is activated when using search rules, and violation checks will be performed on these devices.

Note

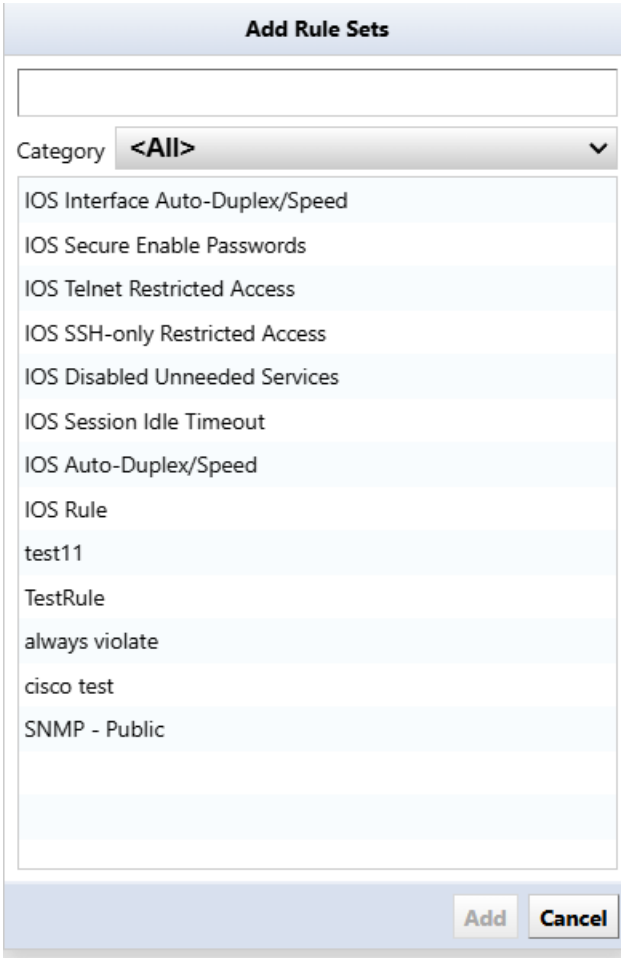
Search result is not saved when creating policy.

4. Click the button on the [Rule Set] subtab of the status panel.



5. Select a Rule Set and click the button.

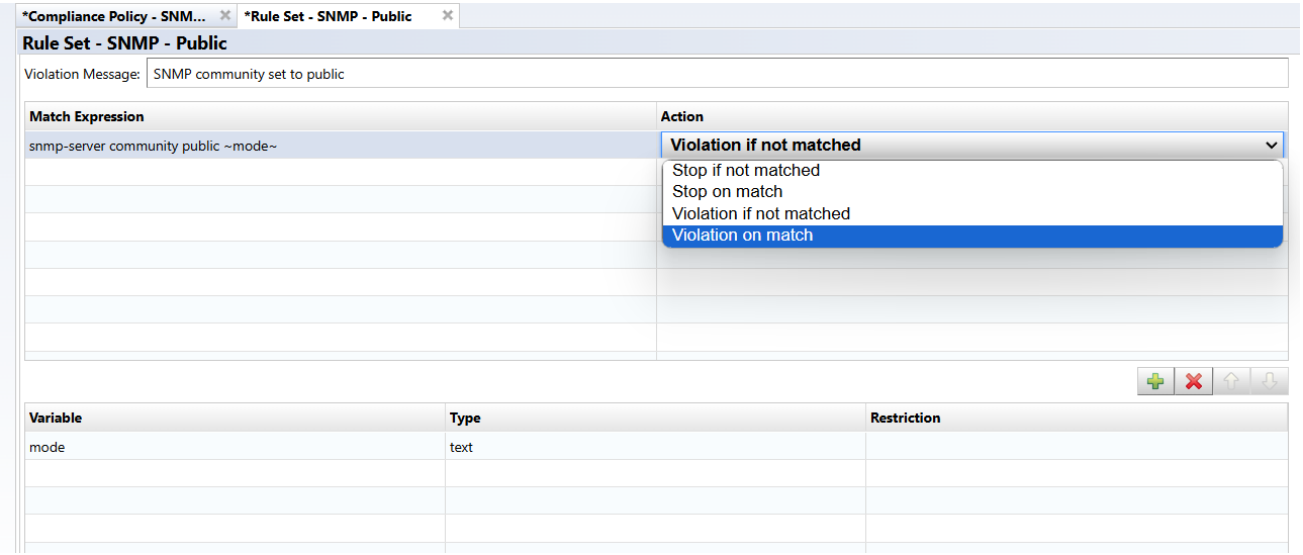
In this example, “IOS Secure Enable Password” Rule Set is selected.



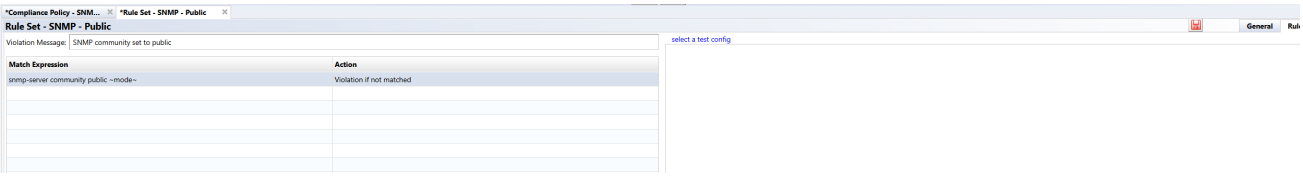
6. Select an Action for the rule. Different Actions can be set for each Rule Set.

In this example, the Action is set to “Violation on match”.

If no Actions are displayed, please review the policy or the adapter type of the Rule Set.



7. Save the policy.



Note

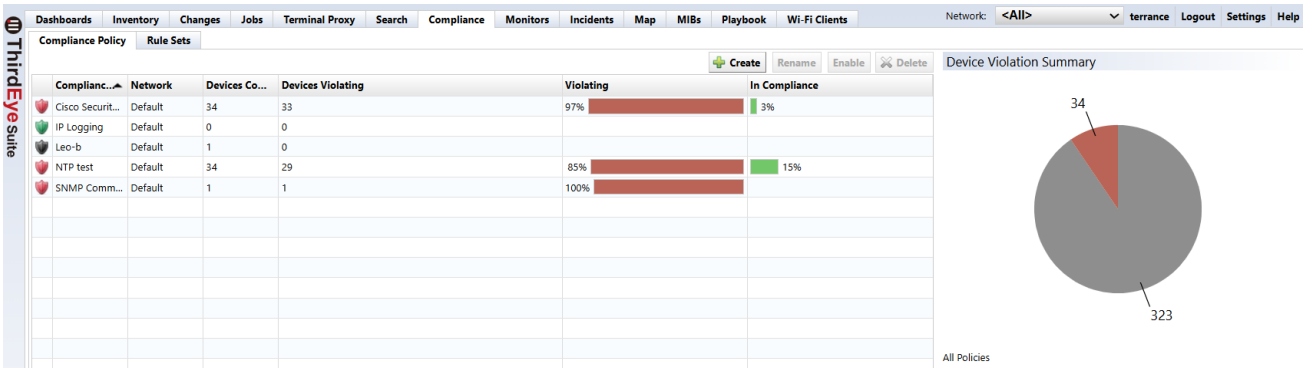
Activate the policy after saving. Simply creating a policy does not check for violations.

8.7.2.3 Applying the created policy

After you create a policy, you need to enable it.

1. Click Compliance > [Compliance Policy].
2. Click the [Enable] button with policy selected.

A pie chart is displayed, it allows you to check the violation status.



If a device violates the policy, the policy icon changes. Depending on the severity of the problem, an orange warning or red error icon will be displayed.

(Refer to the **Set up monitoring** section for more information about severity icons.)

Doubleclick the changed icon. A subtab opens in the status panel. This subtab contains details of the violation.

The violation icon also appears in the device view. Doubleclick the icon to learn more about the violation.

8.7.3 Automatic remediation function

By combining the compliance function and the smart change function, it is possible to automatically execute a pre-specified smart change job when a compliance violation is detected. This allows you to immediately resolve compliance violations.

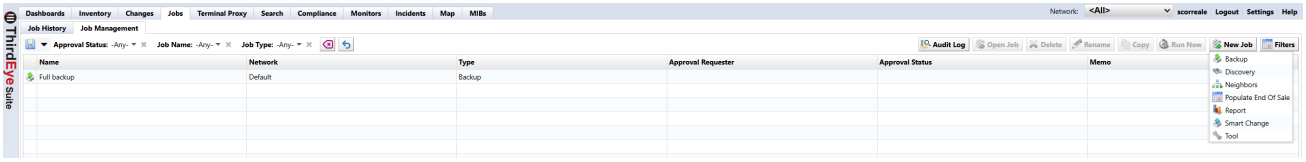
Setting Process

1. **Create smart change job** (Create a smart change job to be executed when a compliance violation occurs.)
2. **Create rules for compliance violations** (Create a violation rule and link the rule to the smart change job.)
3. **Creating a compliance policy** (Associate compliance rules with devices and configure detection settings.)

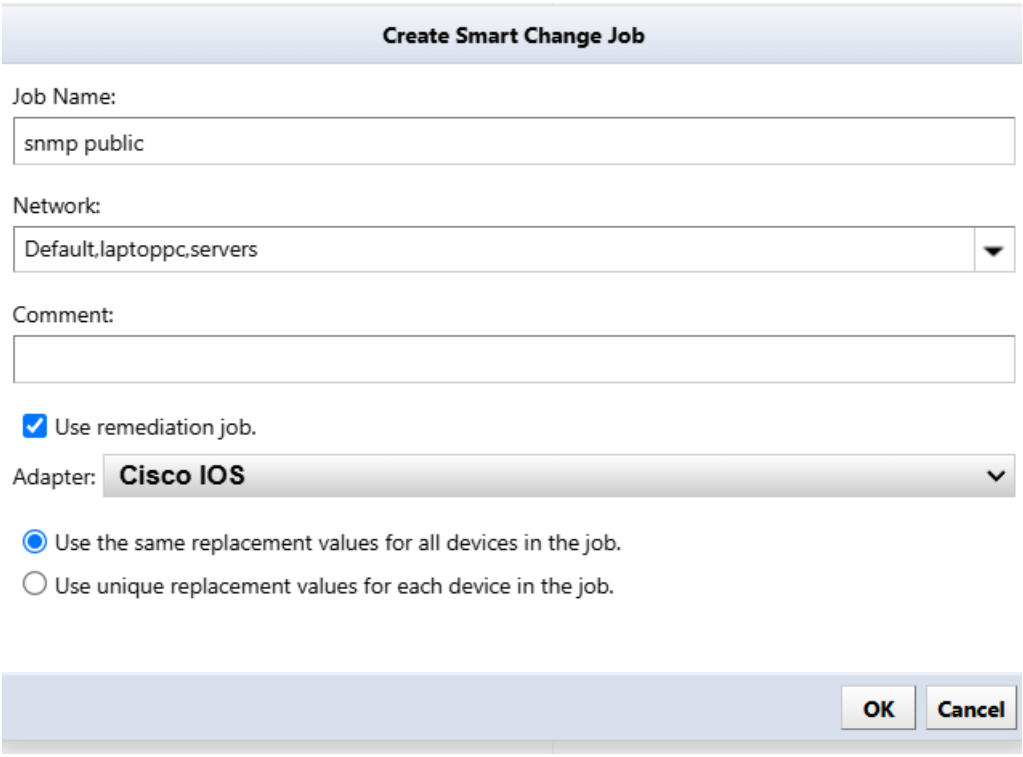
The following explains how to set it up using a setting example.

8.7.3.1 Case 1: When the use of Read-Write authority is prohibited in the SNMP community settings

1. Go to Jobs > [Job Management] and select [New Job] > [Smart Change].

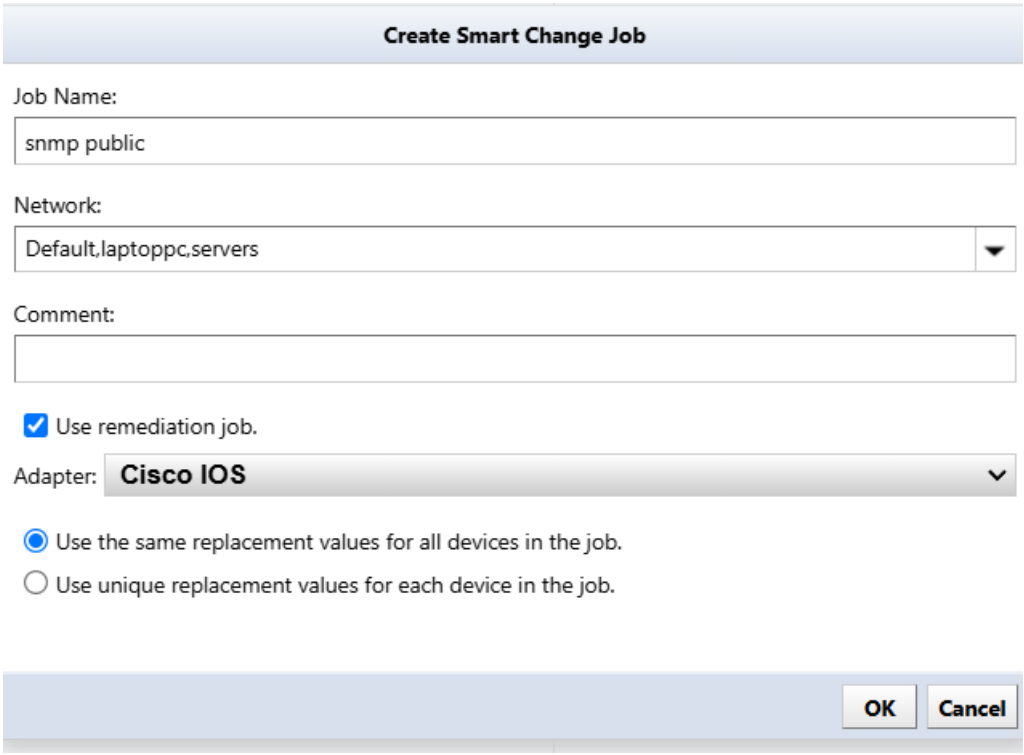


2. Enter the job name and comment (optional).



3. Check “Use remediation job”, select the device adapter, and click [OK].

This is used for linking with Rule Sets.

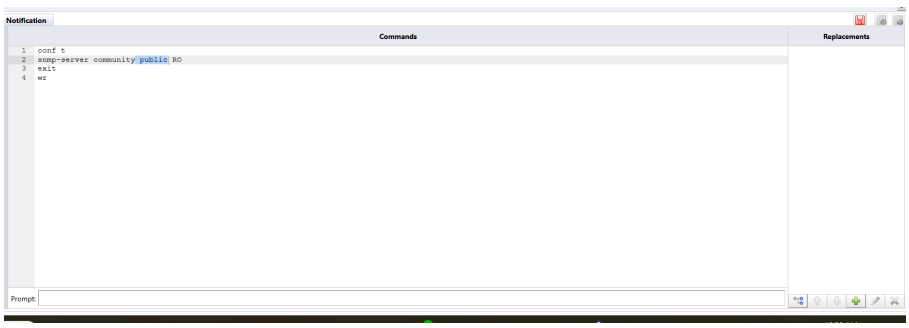


4. Enter the command you want the template to run.

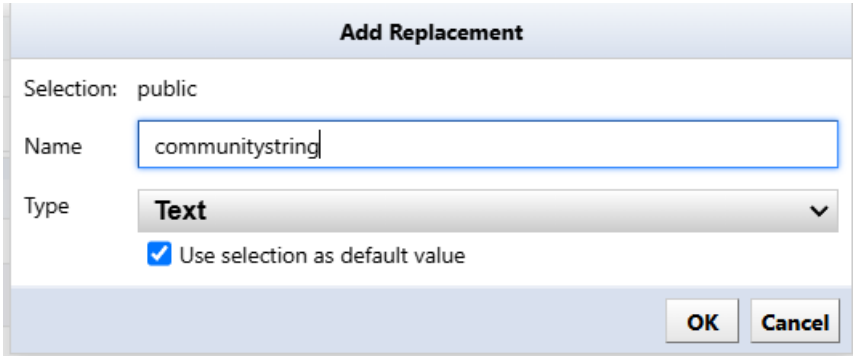
5. Select the part you want to convert into a variable and click the the button.

Skip this step if you want to execute the command as is without converting it to a variable.

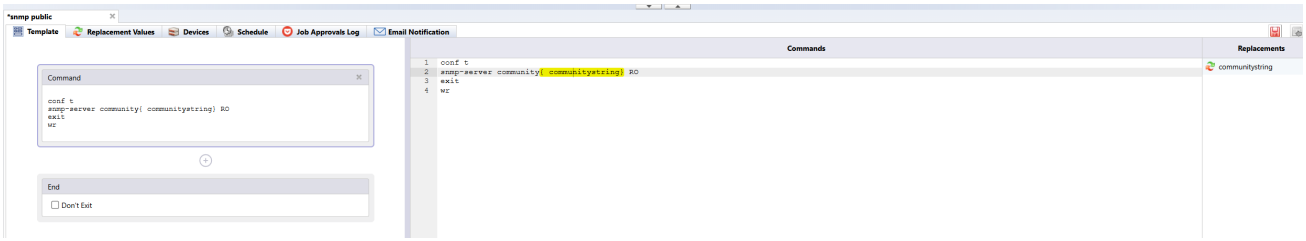
In this case, the community name will be obtained from the config, so we will convert the community name part into a variable.



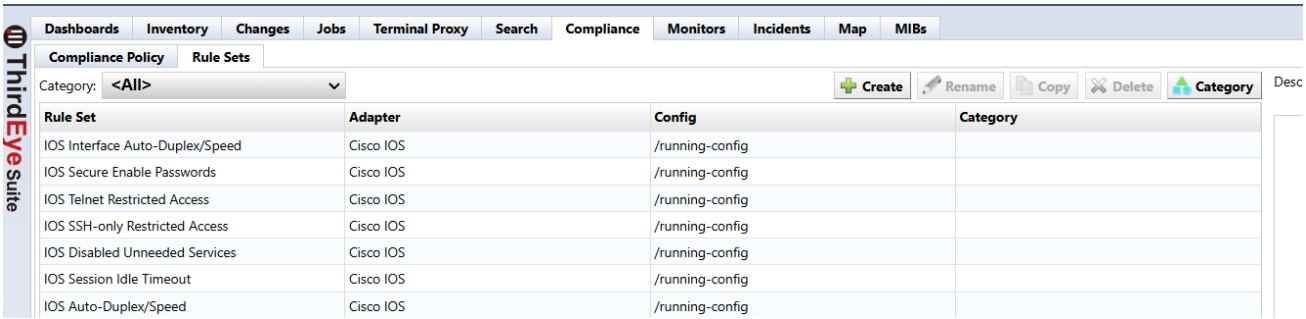
6. Enter the variable “Name” and click [OK].



7. Save the settings.



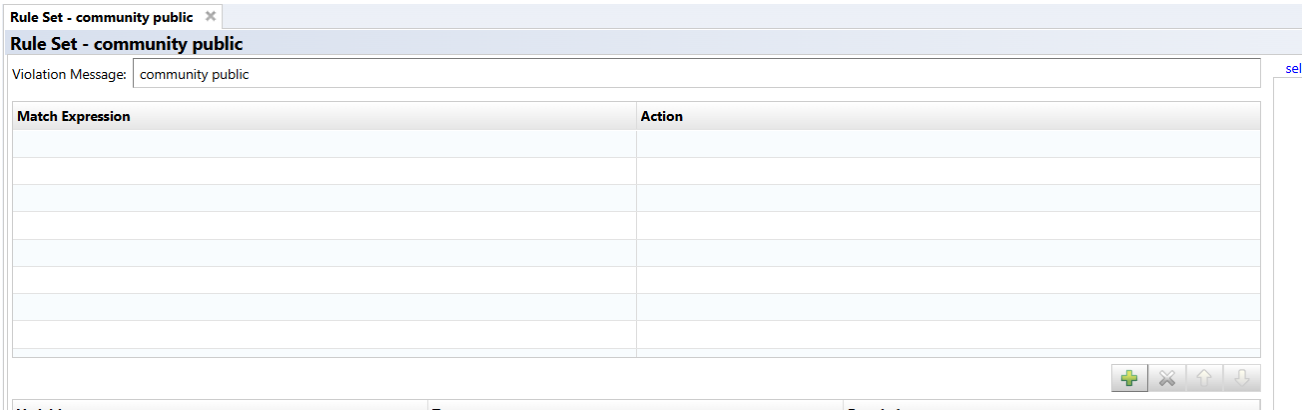
8. Go to Compliance > [Rule Sets] and click [Create].



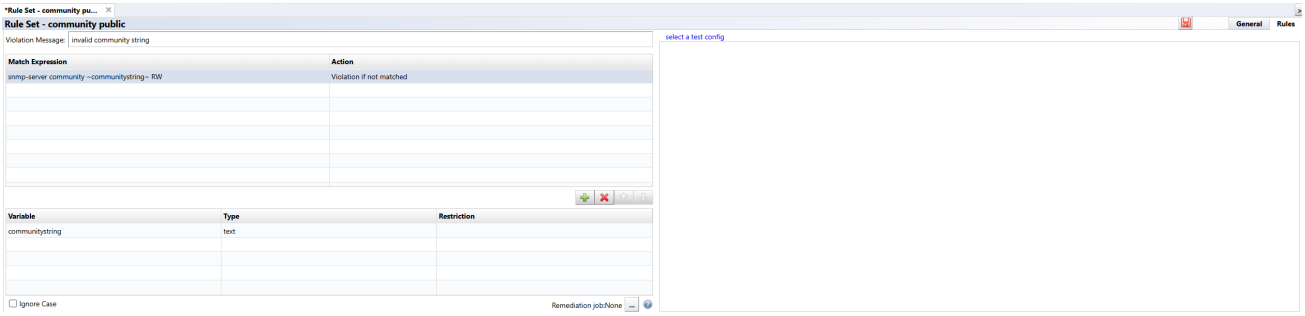
9. Enter the rule name, select the adapter, and click [OK].

Please select the adapter you selected when creating the smart change.

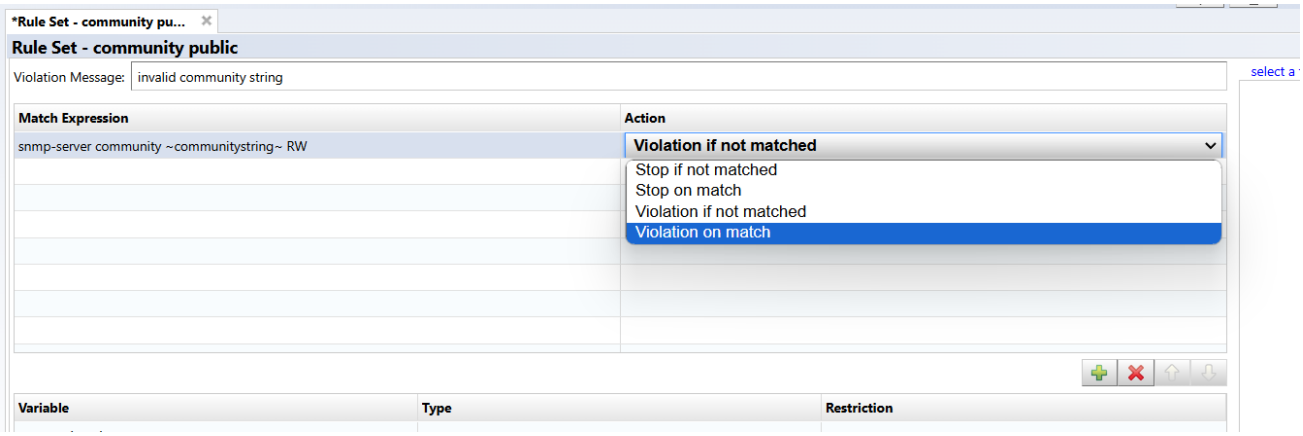
10. Click the button to add “Match Expression”.



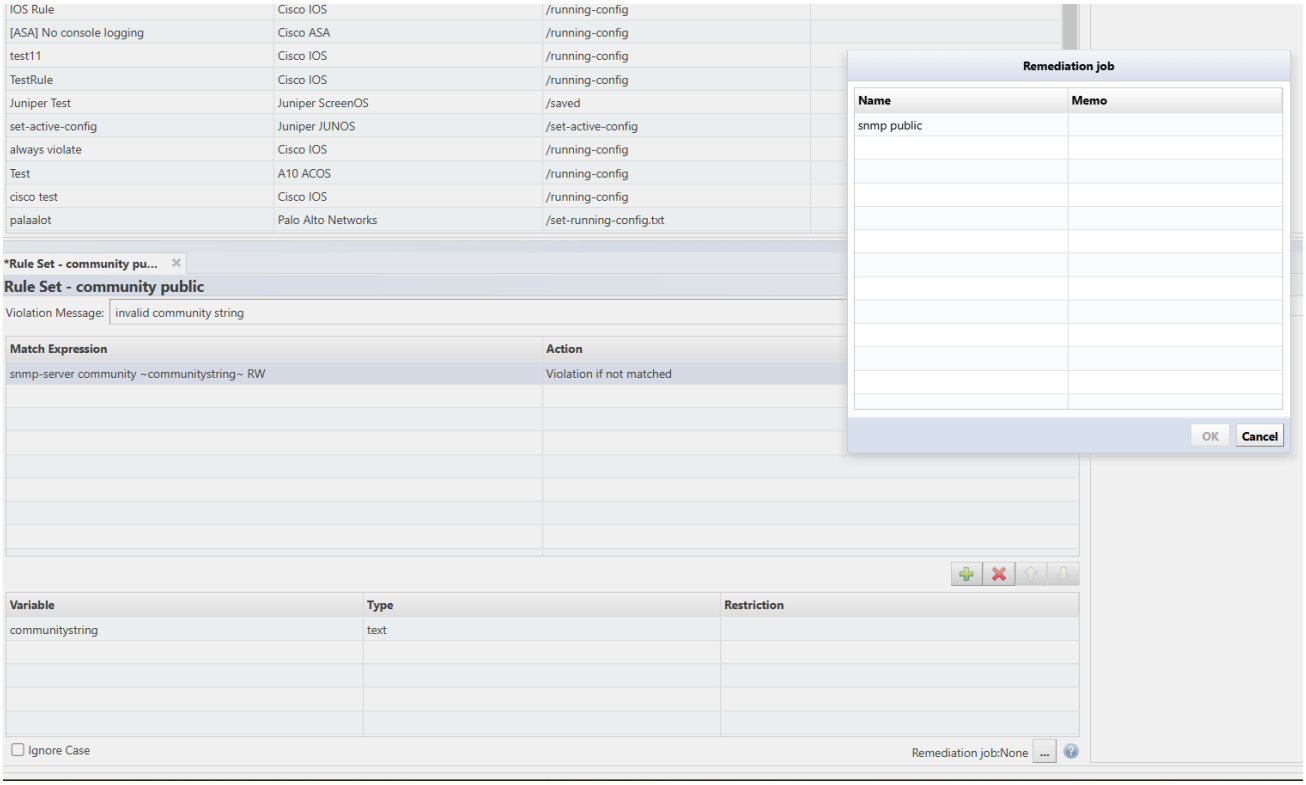
11. In the “Variable” section in the bottom half of the page, specify the community name as the smart change Variable.
12. In the “Match Expression” section in the top half of the page, add “~” before and after the variable name.



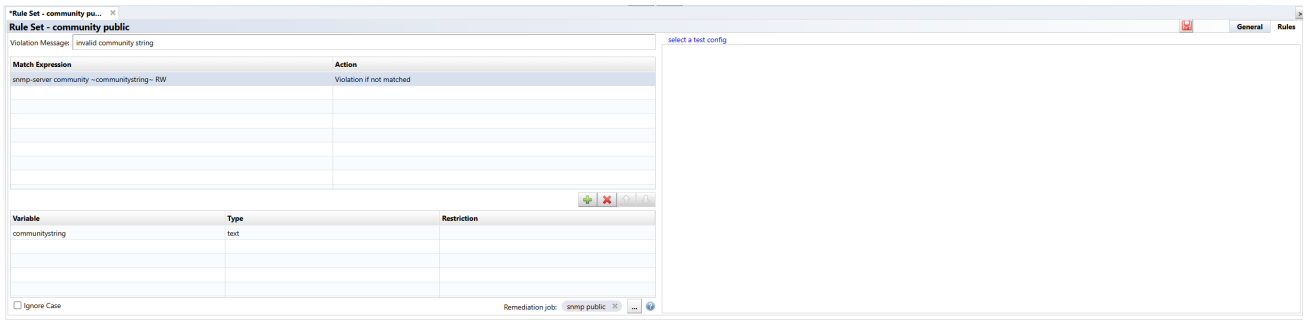
13. Set the Action to “Violation on match.”



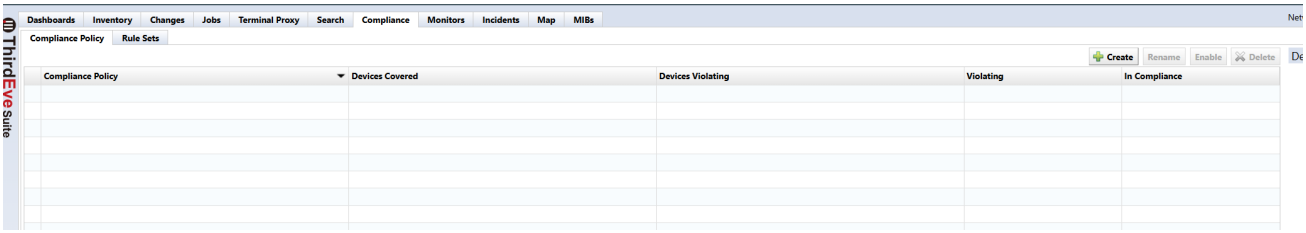
14. In the bottom right of the panel, click the […] button next to “Remediation job” to specify the smart change job to be executed in the event of a violation. Only one job can be specified.



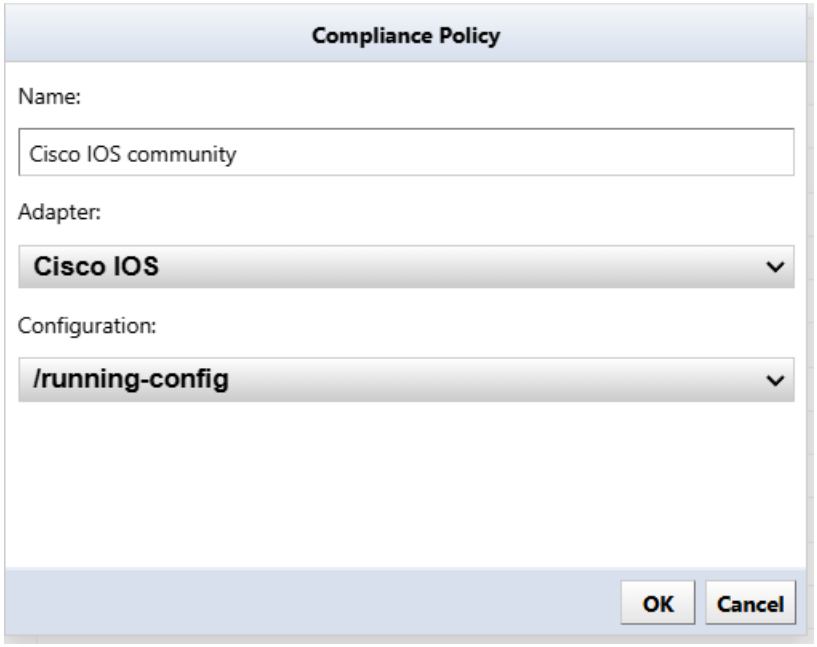
15. Save your settings.



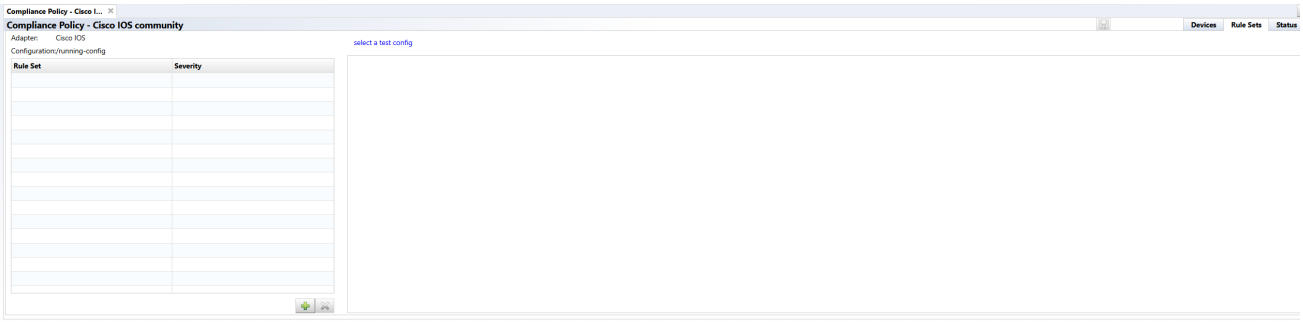
16. Go to Compliance > [Compliance Policy] and click [Create].



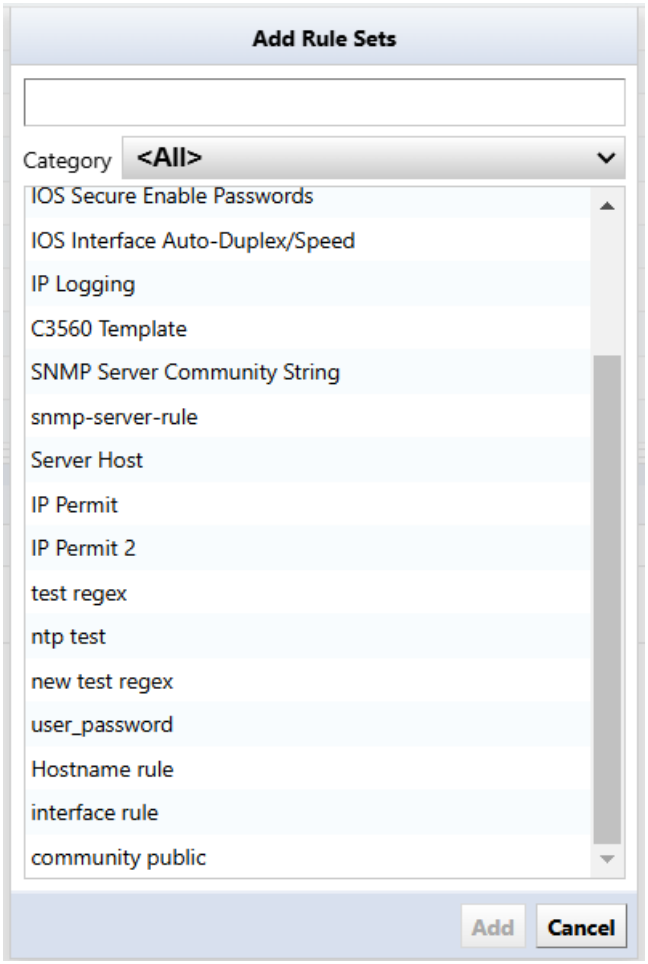
17. After entering the “Name”, select the adapter and target configuration file, and click [OK].



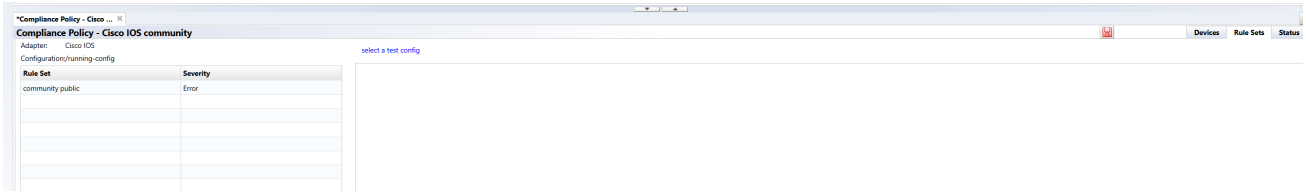
18. Click the  button.



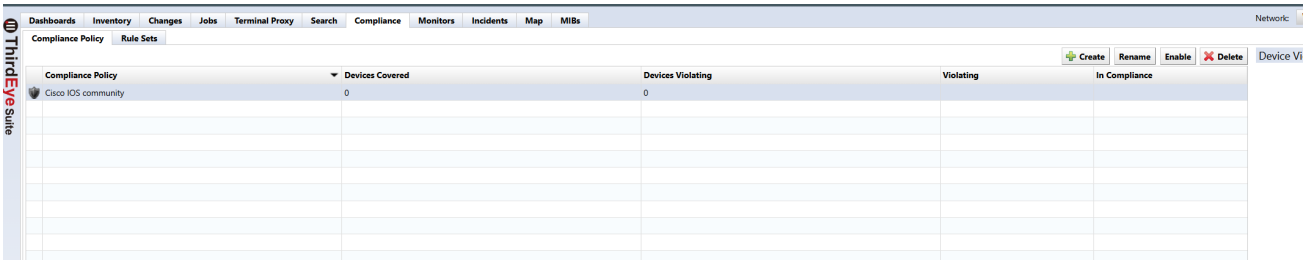
19. Select [Rule Sets] and click [Add].



20. Click [Save].

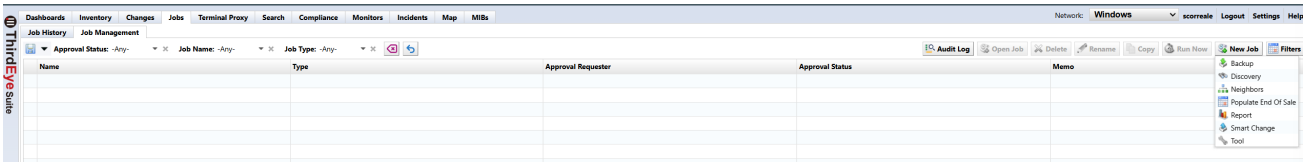


21. Select the compliance policy you created and click [Enable].

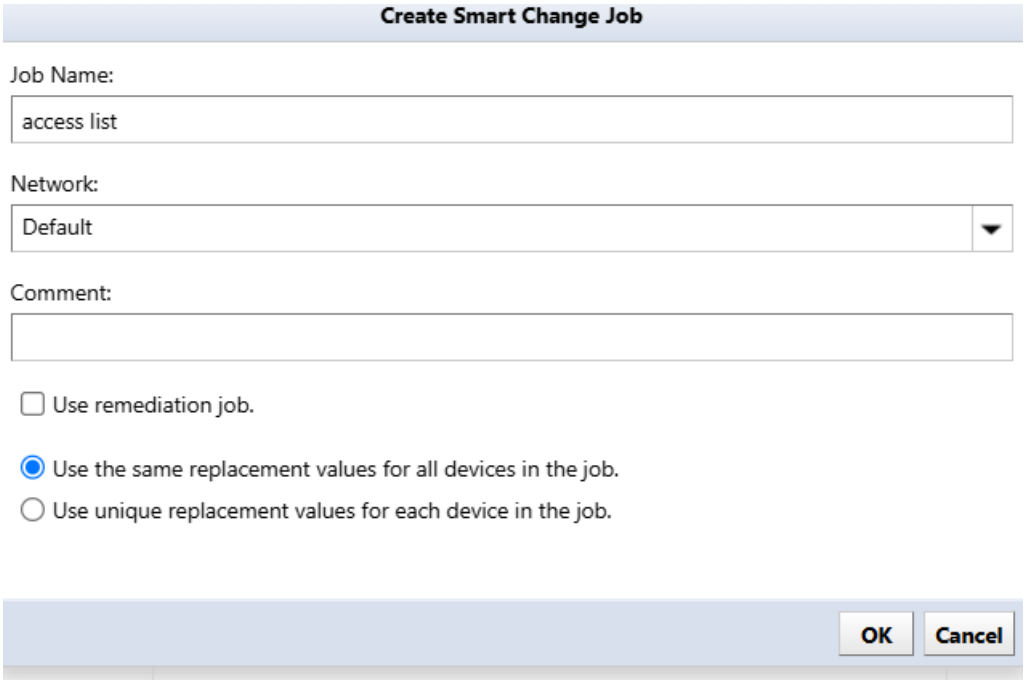


8.7.3.2 Case 2: No access list added to the interface

1. Go to Jobs > [Job Management] and select [New Job] > [Smart Change].



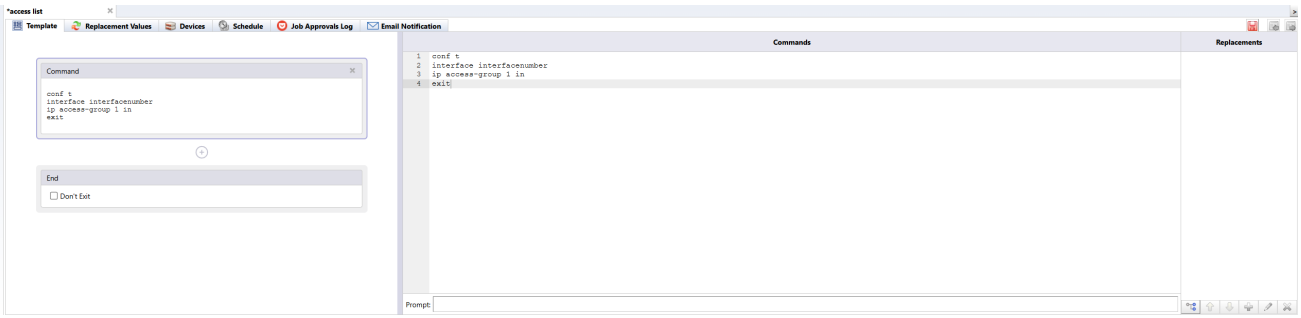
2. Enter the job name and comment (optional).



3. Check “Use remediation jobs”, select the device adapter, and click [OK].

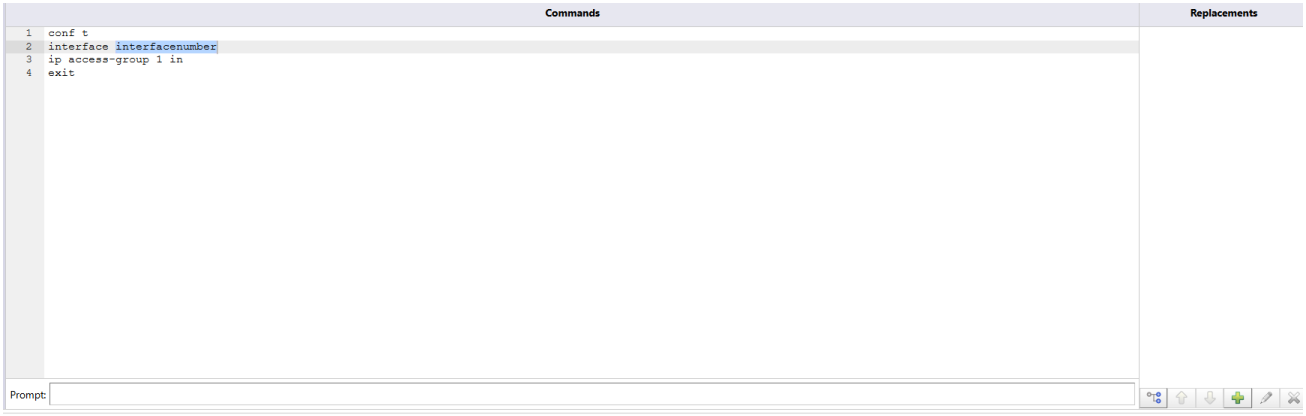
This is used for linking with Rule Sets.

4. Enter the command you want the template to run.

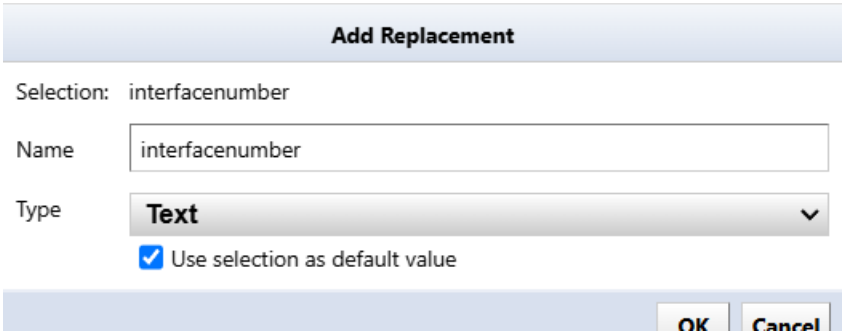


5. Select the part you want to convert into a variable and click the button.

Skip this step if you want to execute the command as is without converting it to a variable.



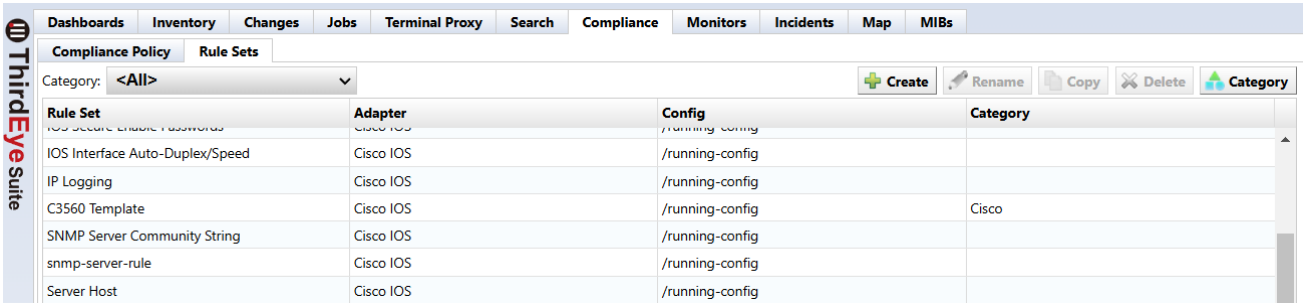
6. Enter the variable name and click [OK].



{n .center}

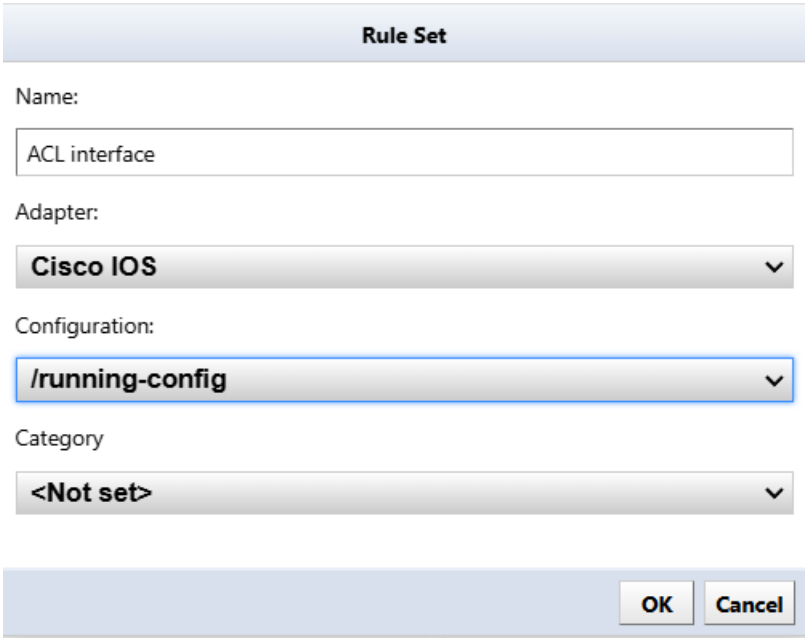
7. Click [Save].

8. Go to Compliance > [Rule Sets] and click [Create].

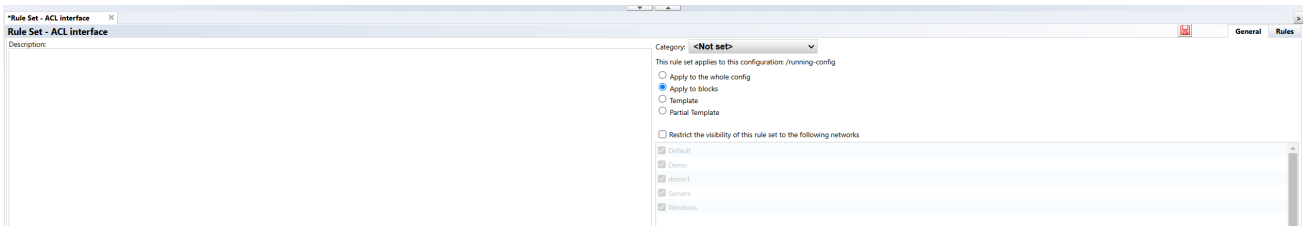


9. After entering the rule name, select the adapter and click [OK].

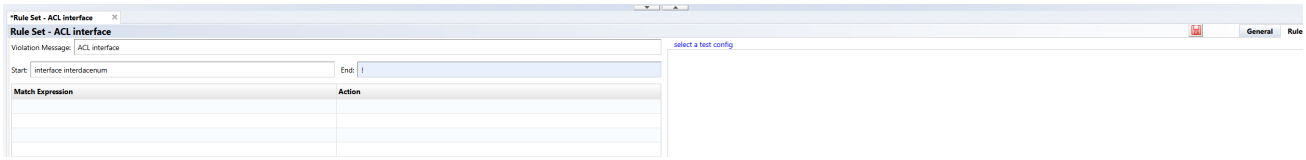
Please select the adapter you selected when creating the smart change.



10. Go to the General tab and select [Apply to Blocks].

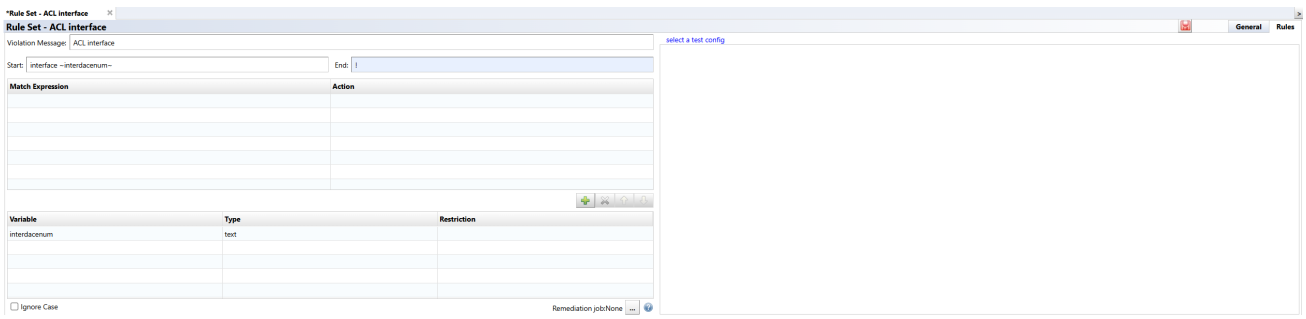


11. Specify the block to which the rule applies using “Start” and “End”.



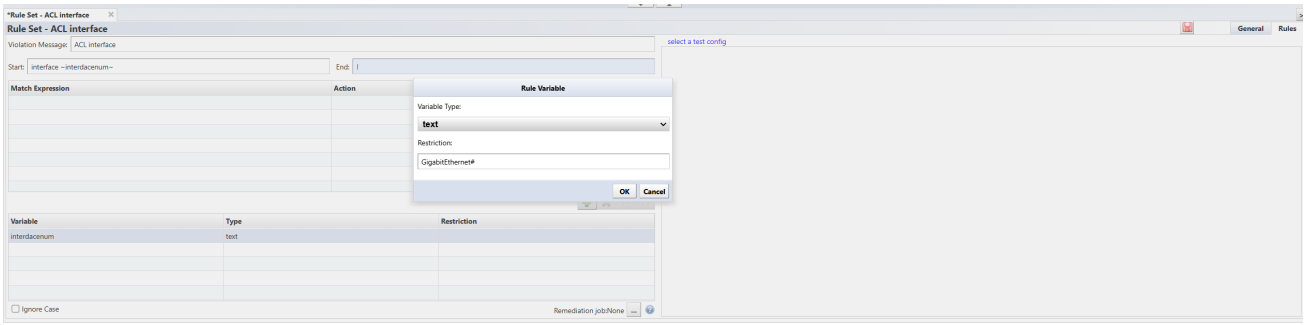
12. In the “Variable” section in the bottom half of the page, specify the interface number as the smart change Variable.

In the “Start” field at the top of the page, add “~” before and after the variable name.

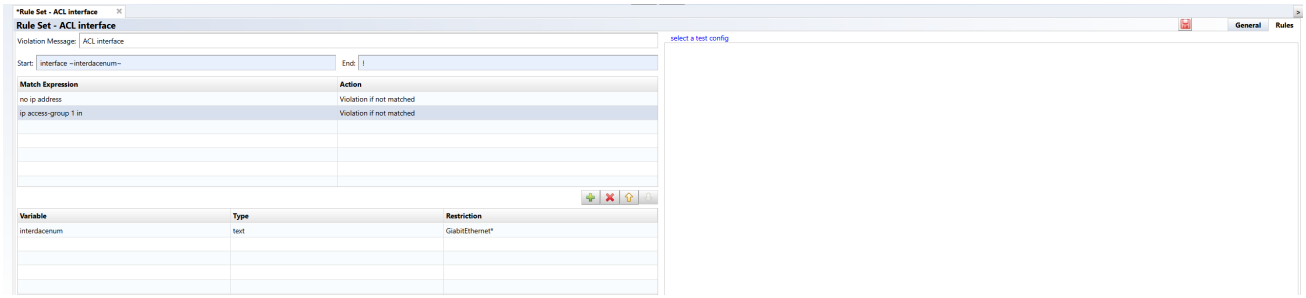


13. Doubleclick the added variable and add a text filter.

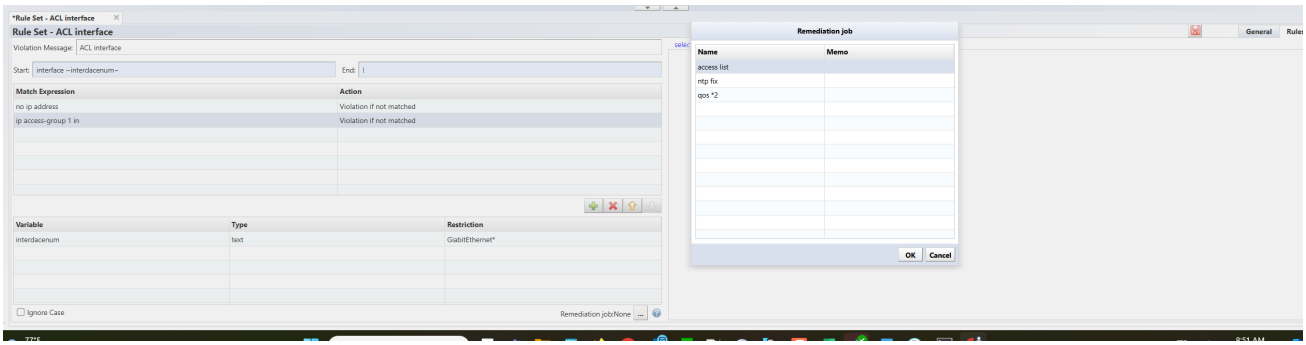
In this example, the GigabitEthernet interface is targeted, so “Gigabit Ethernet” is specified.



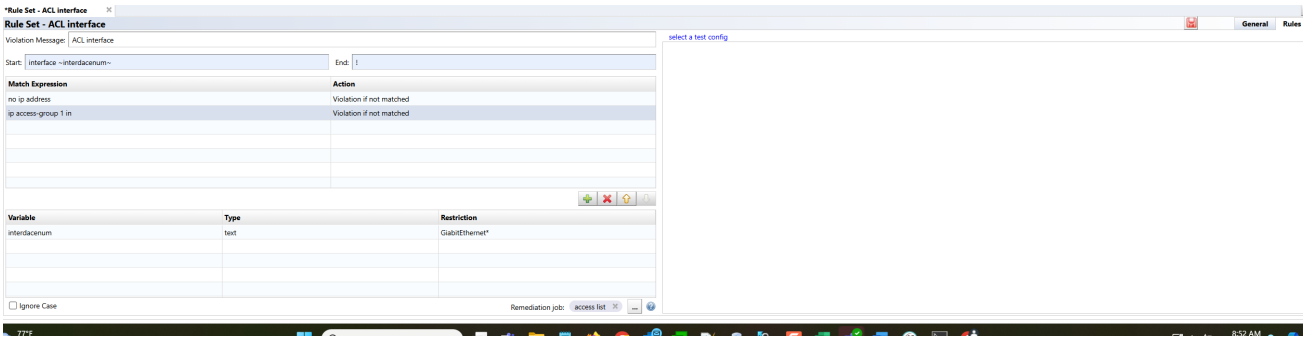
14. Click the button to add matching conditions.



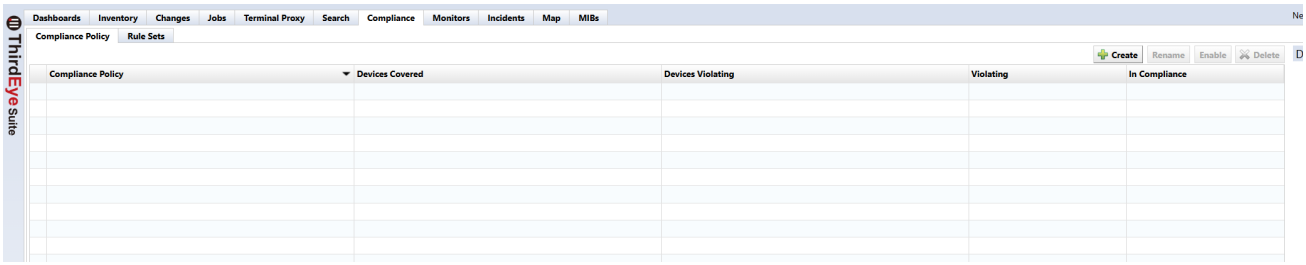
15. In the bottom right of the panel, click the […] button next to the “Remediation job”, and specify the smart change job to be executed in the event of a violation. Only one job can be specified.



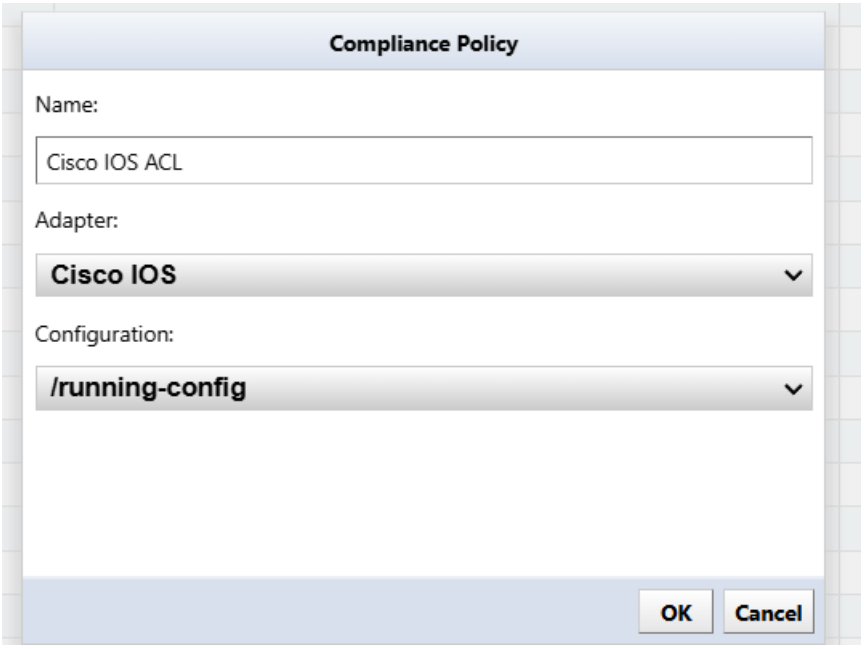
16. Save your settings.



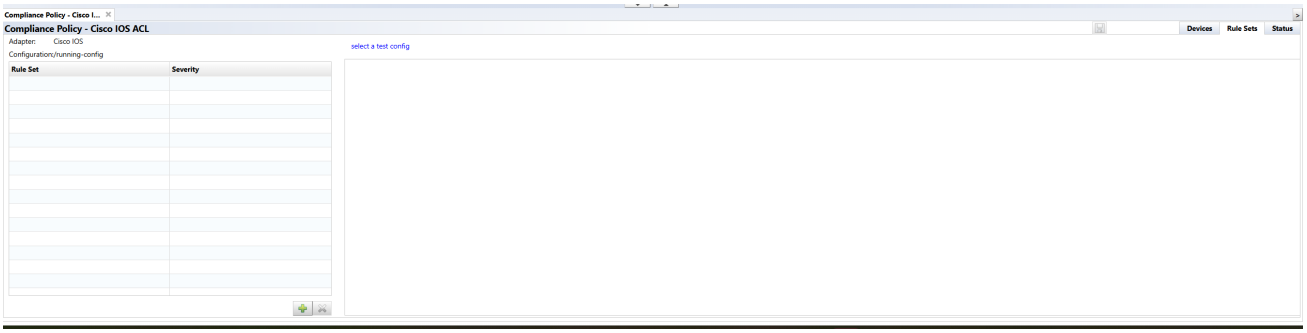
17. Go to Compliance > [Compliance Policy] and click [Create].



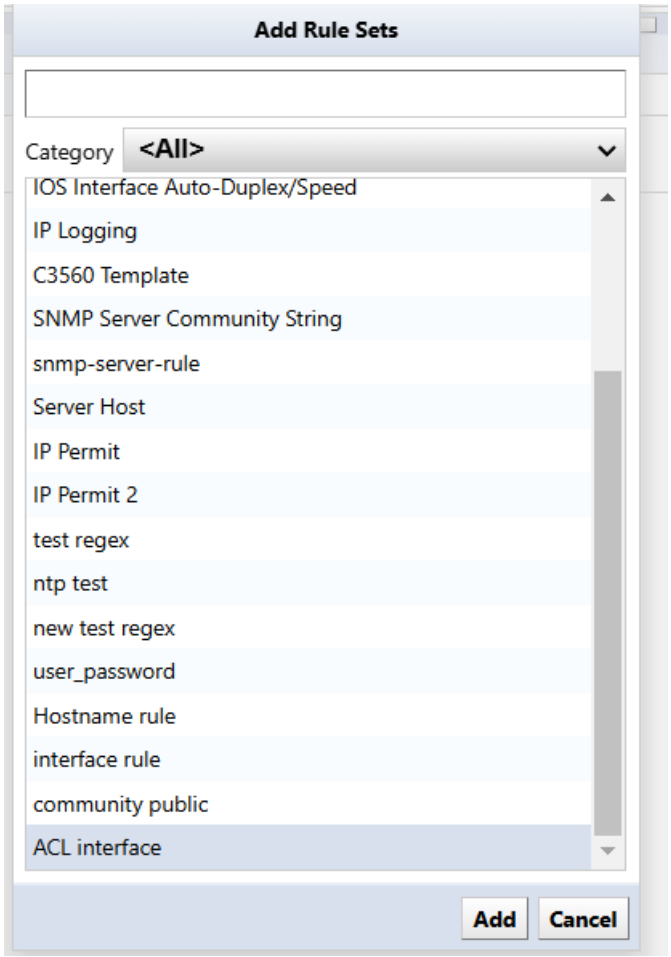
18. After entering the “Name”, select the “Adapter” and “Configuration” target file, and click [OK].



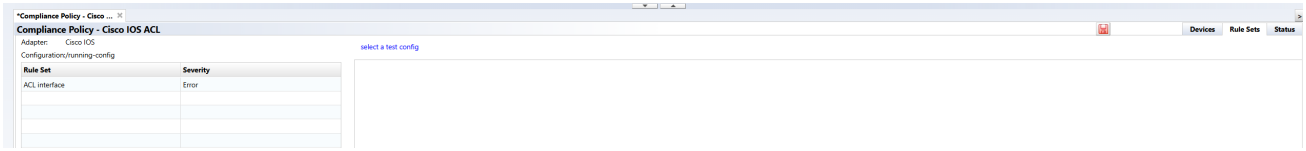
19. Click the button.



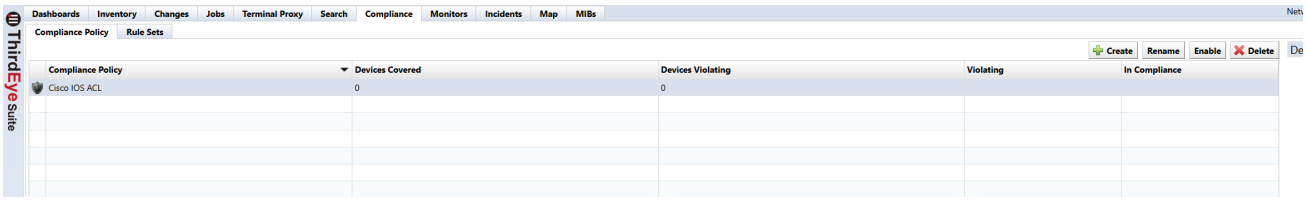
20. Add a Rule Set.



21. Click [Save].



22. Select the compliance policy you created and click [Enable].



8.8 Zero-Touch (optional) Suite

The [Zero-Touch] tab streamlines automated network device deployment, and allows you to use templates to distribute configurations. It allows you to restore devices to operational states when configurations become corrupted, while serial number tracking facilitates seamless hardware replacement without manual reconfiguration. Deployments can also be completed via bulkspreadsheet import/export.

Zero-Touch is a useful tool for distributing configurations to devices on a physically separated network. Because the tool is based on the capabilities of Cisco Plug and Play, Zero-Touch can only be used with devices that support those capabilities.

8.8.1 Zero-Touch formats

There are three main formats in which Zero-Touch distributes configurations:

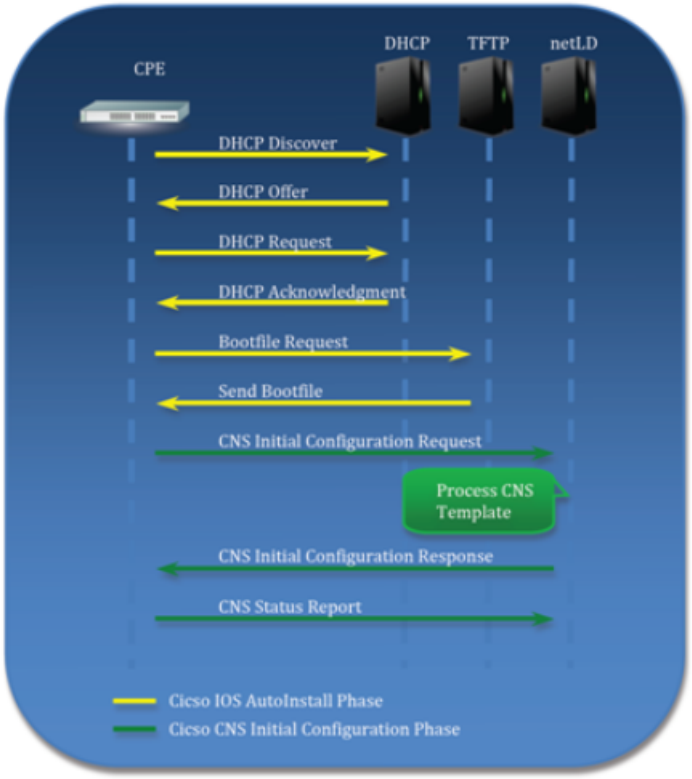
-**Template**: Distribute configurations based on templates. Used when introducing a new device to the network at a remote office.

-**Self-recovery**: Convenient for resetting a device that has been overwritten with an abnormal configuration and no longer works properly.

-**Restore specific device**: Useful for updating device equipment. For example, if the device you were previously using breaks down and you want to replace it with another device of the same model, you can write the settings that were used until then to the new device.

{{ProductName}} Zero-Touch distributes configurations using these protocols. Therefore, it is necessary to properly configure a firewall when using it.

The figure below shows the flow of processing performed by Plug and Play using PnP. To make the diagram easier to read, the DHCP and {{ProductName}} servers are shown divided, but this does not mean that three computers are used. All three server programs run on the same computer running the {{ProductName}} server.

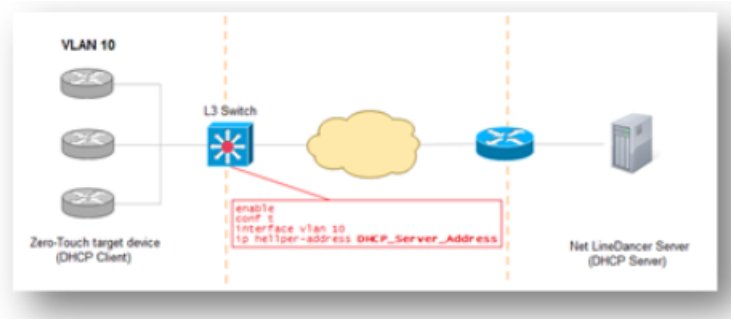


8.8.2 Zero-Touch requirements

To use Zero-Touch, the following conditions must be met. Please check before use.

- The IOS version of the target device must be IOS 15.2(2) or later for PnP.
- Devices must not have a startup-config.
- DHCP Server - If you want {{ProductName}} to perform the DHCP server itself, the target device must be in a network where DHCP IP address distribution is possible. Additionally, if the target device exists outside the network where {{ProductName}} can be distributed, by setting DHCP relay on the device on the route, the {{ProductName}} server will be able to receive DHCP requests from the target device.

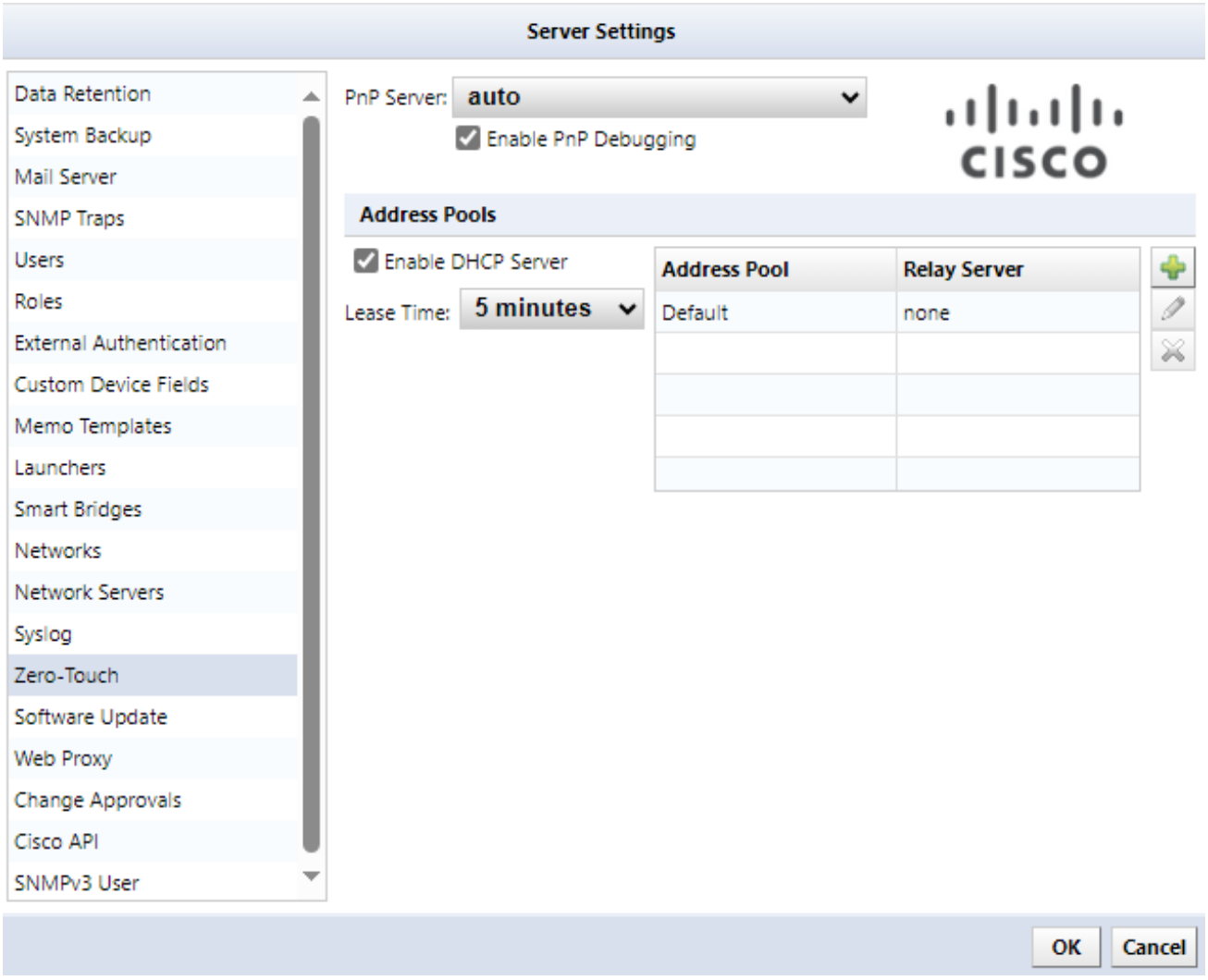
DHCP relay example:



8.8.3 DHCP server

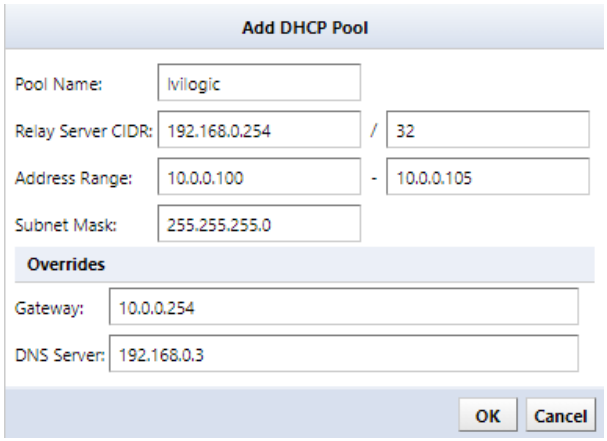
To set up a DHCP server:

1. Open the Server Settings window.
2. Click [Zero-Touch] in the left sidepanel.
3. Click the button to set up a new DHCP pool.



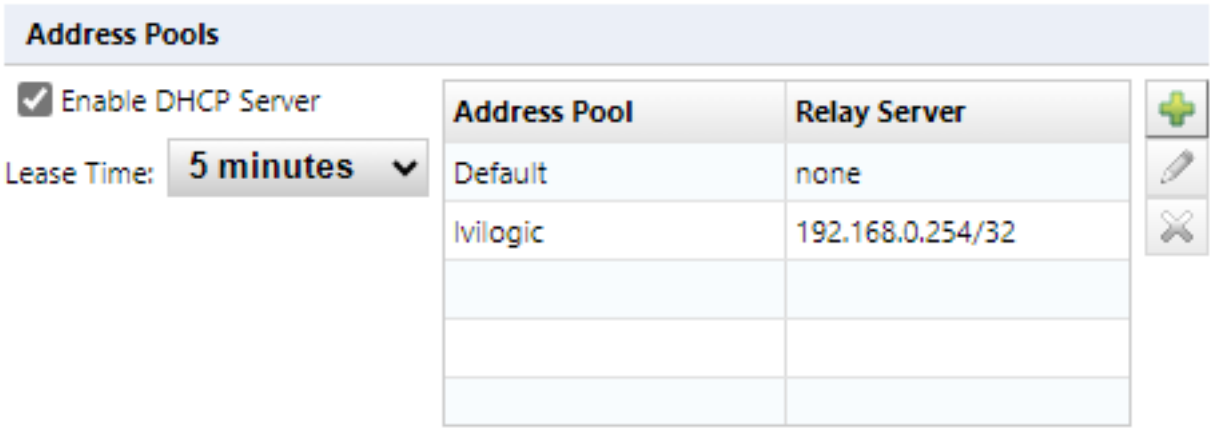
Item	Explanation
Enable DHCP server	Check this box if you want to use {{ProductName}}'s DHCP server.
lease time	Set the DHCP lease time.

4. Enter the necessary information, and click the [OK] button.



Item	Explanation
Pool name	Enter the name of the DHCP pool to create
Relay server CIDR	Enter the IP range where the DHCP relay server exists
Address range	Enter the IP address range to distribute (required)
Sub-net mask	Enter subnet mask (required)
Default gateway	Specify the device’s default gateway
DNS server (optional)	Specify the DNS server for server name resolution from the device

If done correctly, a new item should be added to the table below.

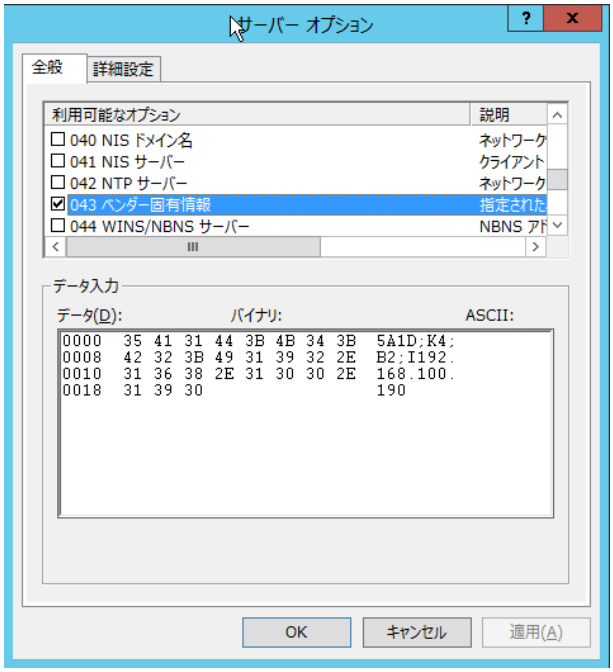


8.8.4 Use an external DHCP server

If you use a DHCP server other than {{ProductName}}, you will need to enter information in addition to the basic information necessary for {{ProductName}} communication. The options you need to add depend on the type of PnP. “`Option 43`” allows you to add vendor-specific information.

The figure below is an example of a Windows DHCP server setting.

Enter the information in the ASCII field, using “;” to separate.

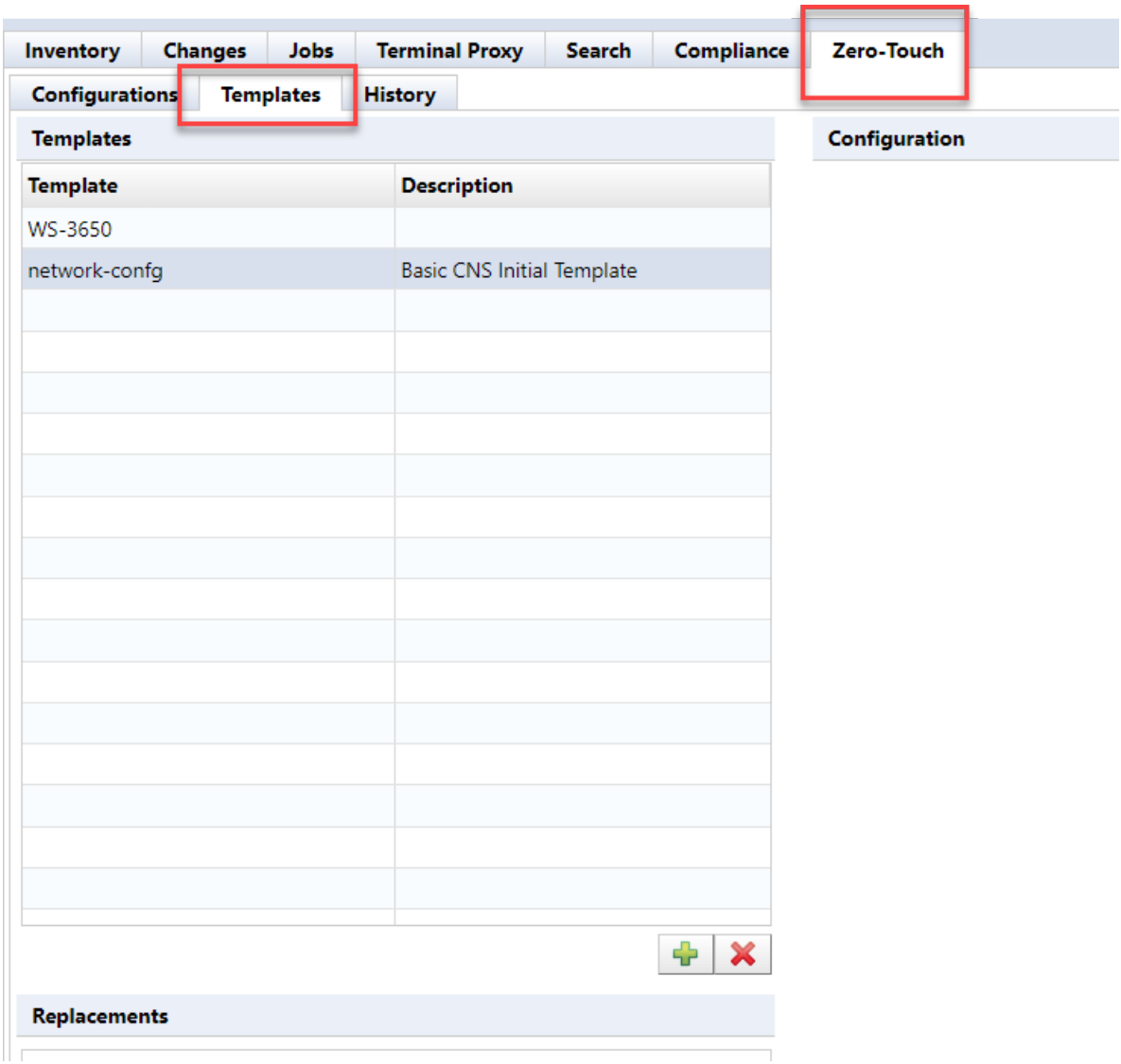


8.8.5 Creating a template

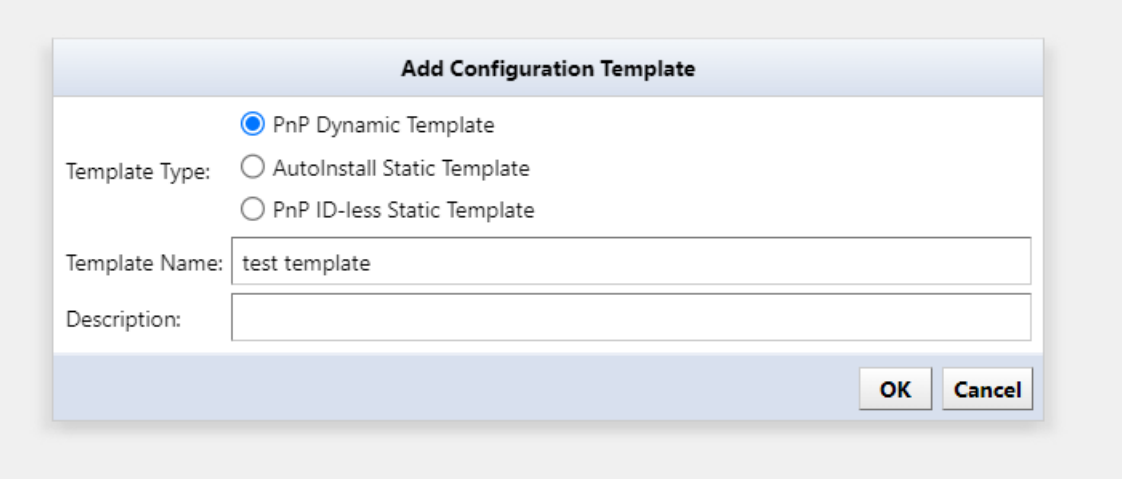
In large networks, there may be multiple devices with similar configurations, but differeng IP addresses, hostnames, DNSs, and syslog server addresses, Smart Change utilizes templates to send similar commands tailored for each device. Zero-Touch can utilize the same template for commands *and* device configurations.

Follow the steps below to create a template:

1. Click the [Zero-Touch] > [Templates] tabs.
2. Click the button to create a template.



4. Select [Dynamic Configuration] as the template type .
5. Enter a name for the new template in the “Template Name” field. (The “Description” is optional.)
6. When finished, click the [OK] button.



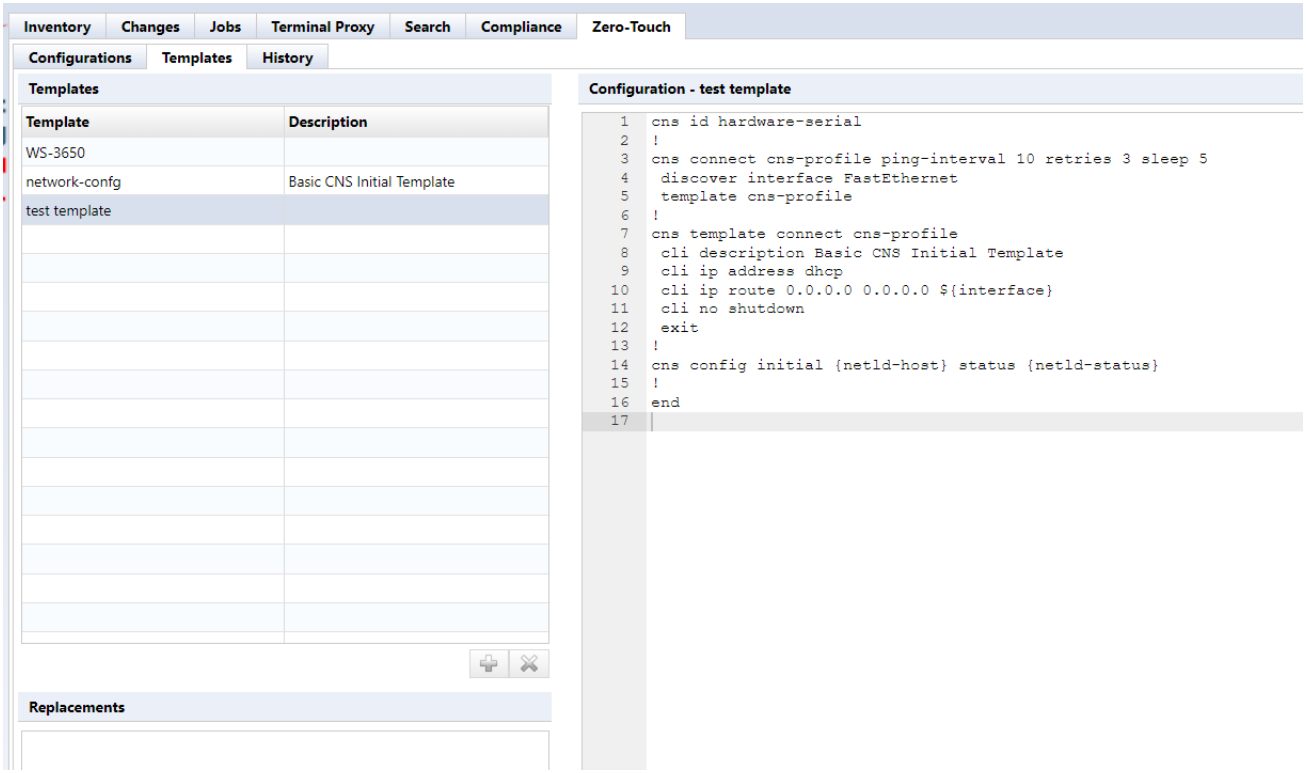
A large “Configuration” text area called the will open on the right side of the screen.

7. Enter the original configuration in this area.

(If you already have a device of the same model in your inventory as the one you plan to use with Zero-Touch, you can change that device”s configuration (e.g.start-up config) and paste it here.)

Once you have added all the required variables, you need to save your template

8. Click the [Save] button at the top right of the text area to save your created template.

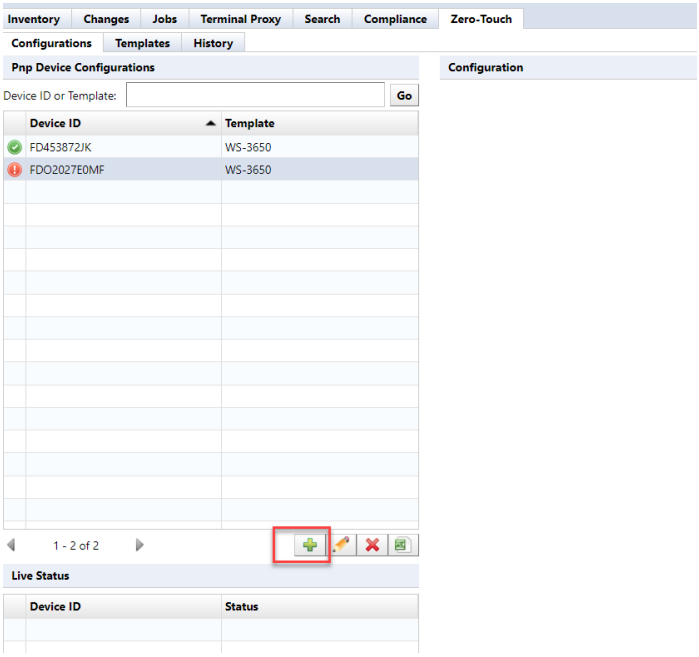


If you do not want to save the deployed configuration on the device, add a no-persist option at the end of cns "`config initial...`" when deploying the configuration.

Device registration

Now we have the necessary templates ready for Zero-Touch. The next step is to register the devices to which you want to distribute the settings. You also need to set values for template variables for each target device.

1. Click the [Zero Touch] > [Configuration] tabs.
2. Click the button to configure Zero-Touch on the device.



Importing values from outside into template variables

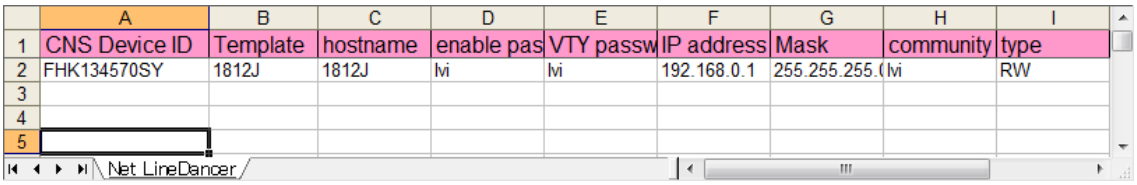
Tables written externally in can be used as template values.

Follow the steps below to import Excel files:

1. In the [Zero-Touch] tab, click the [Close] button if editing device data.
2. Click the [Import] button to display the submenu.
3. Select [Export import file] or [Export template] from the menu that appears.

Item	Explanation
Import template	Load and register the Excel file containing variable values.
Export file for import	Outputs a blank Excel sheet where you can add values.
Export template	Outputs an Excel sheet that reflects the current variable values.

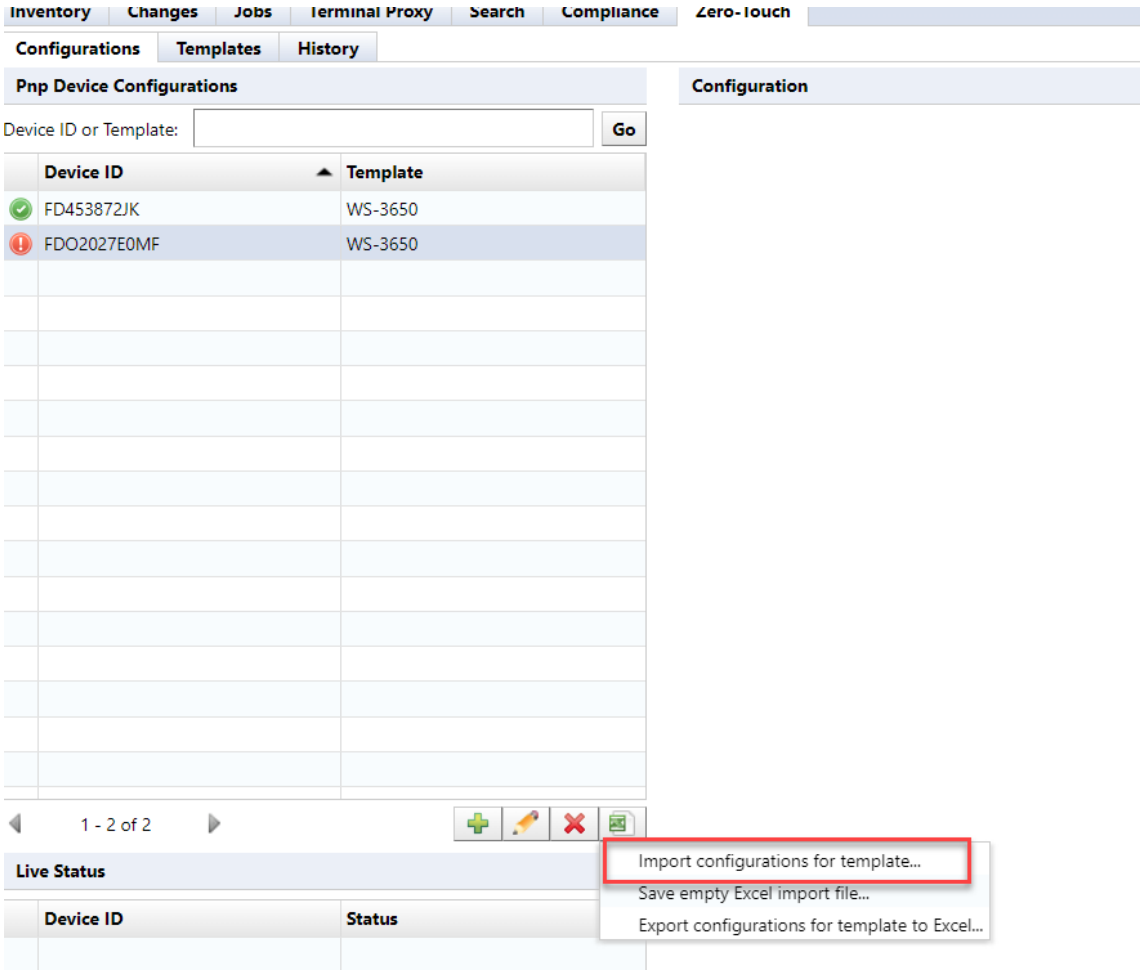
4. Edit the output file and input the values of the template variables in order.
5. Save after entering.



	A	B	C	D	E	F	G	H	I
1	CNS Device ID	Template	hostname	enable pas	VTY passw	IP address	Mask	community	type
2	FHK134570SY	1812J	1812J	lvi	lvi	192.168.0.1	255.255.255.(	lvi	RW
3									
4									
5									

Net LineDancer

6. Return to {{ProductName}}, and click [Zero Touch] > [Configuration] again.
7. Select [Import Template] from the menu that appears.

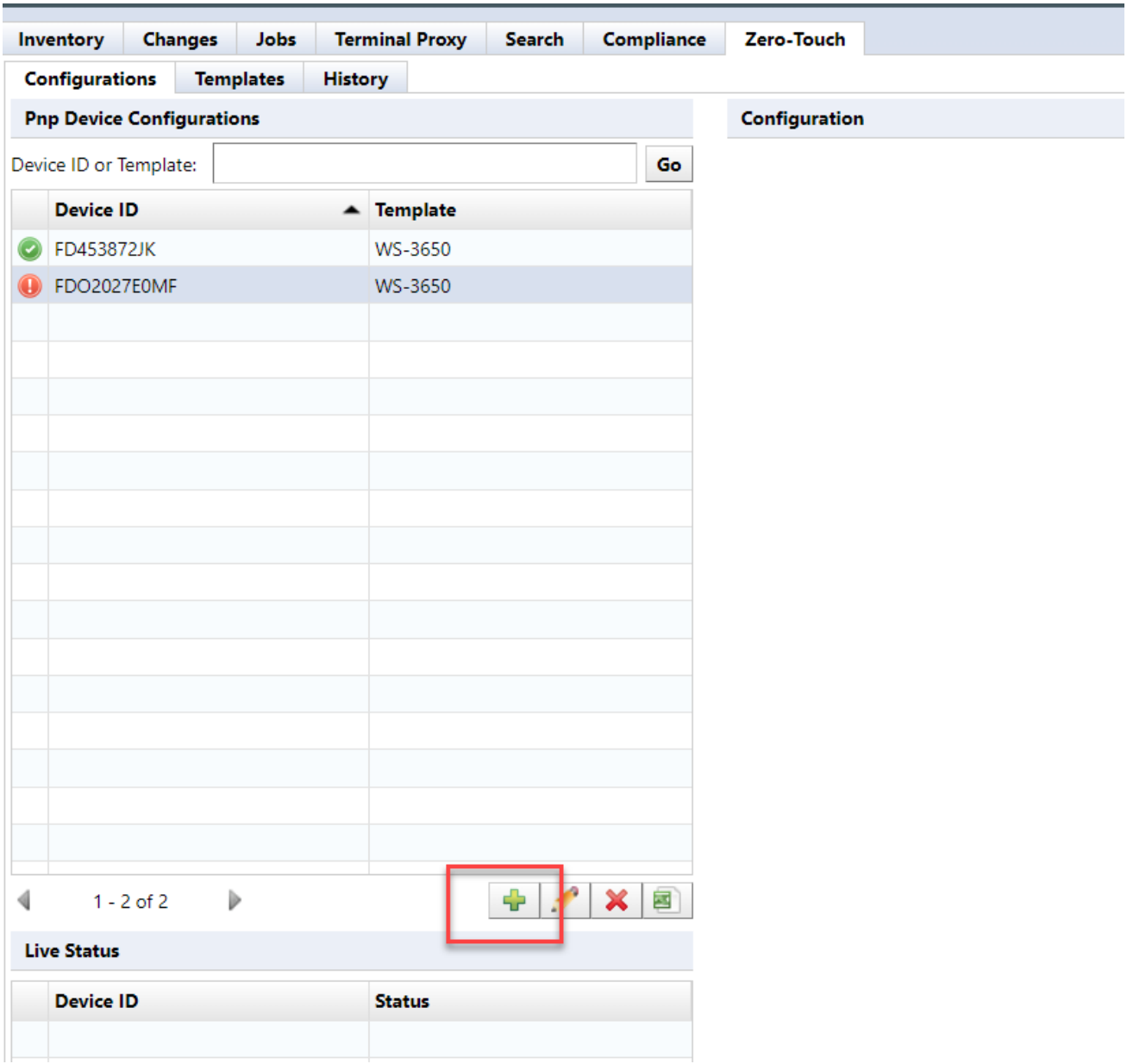


8.8.6 Zero-Touch self-recovery

Instead of sending a new configuration, Zero-Touch can send other configurations previously stored inside {{ProductName}}. This function is useful, for example, if the currently running device configuration is accidentally deleted. A device that loses its configuration will become unresponsive and cannot be recovered without the use of special features such as Zero-Touch.

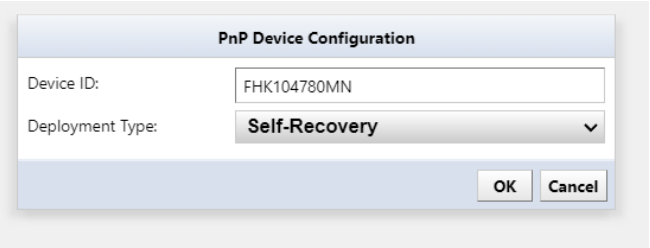
The steps are similar to other Zero-Touch template steps:

1. Click the [Zero-Touch] > [Configuration] tabs.
2. Click the button on the [Configuration] tabs.



3. Enter the necessary information in the device configuration dialog.
4. In the [PnP Device Configuration] window, select the [Self-Recovery] option in the [Distribution type] dropdown menu.

5. Click the [OK] button to save.



The configuration data stored within {{ProductName}} is then written back to the device. There are no other differences from template delivery mode.

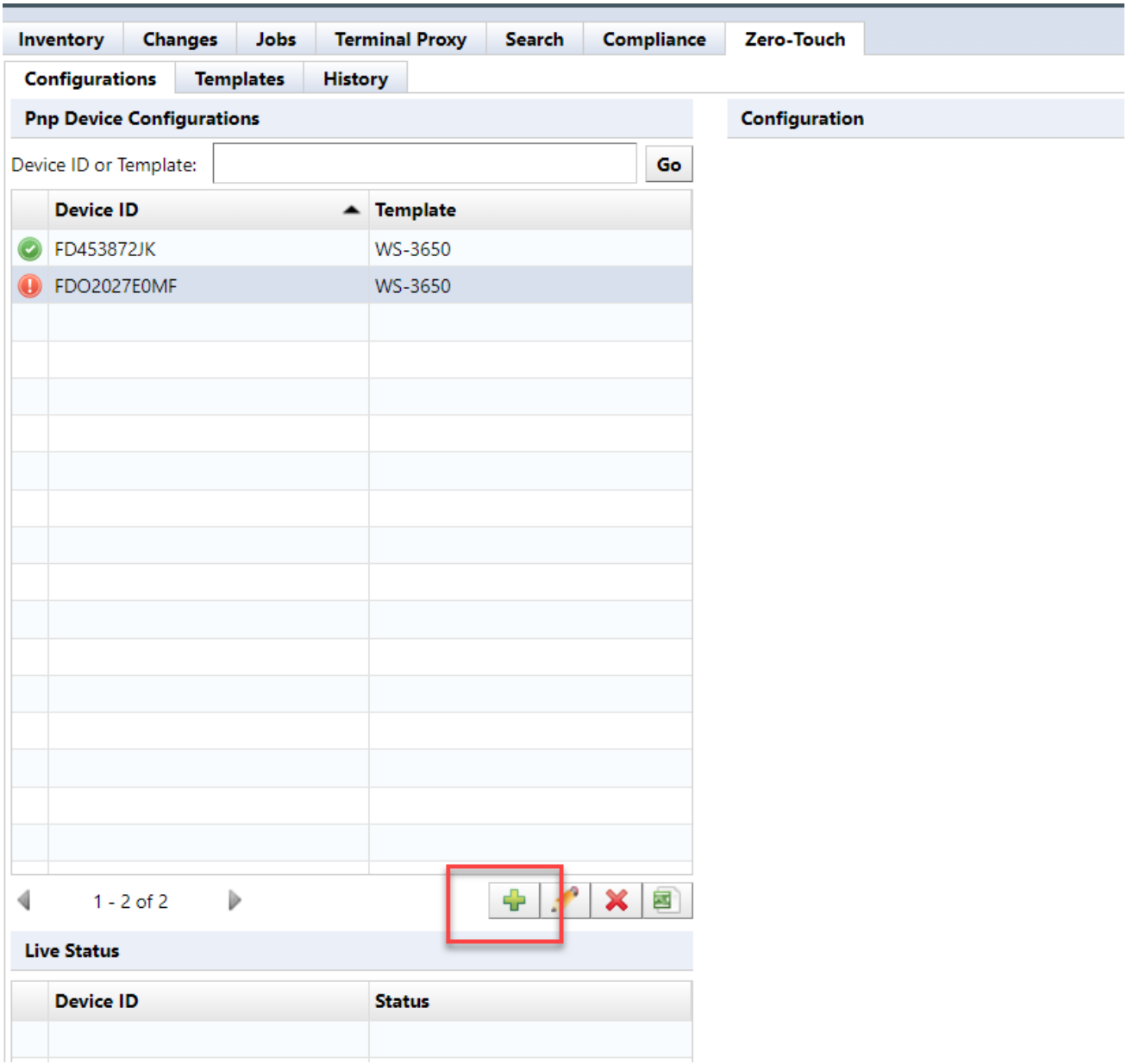
8.8.7 Zero-Touch Specific Device Restore

This feature is used when replacing an old device with a new device. This feature is extremely useful when the device is located far away (e.g. in another data center) and there is no one on site to operate it directly.

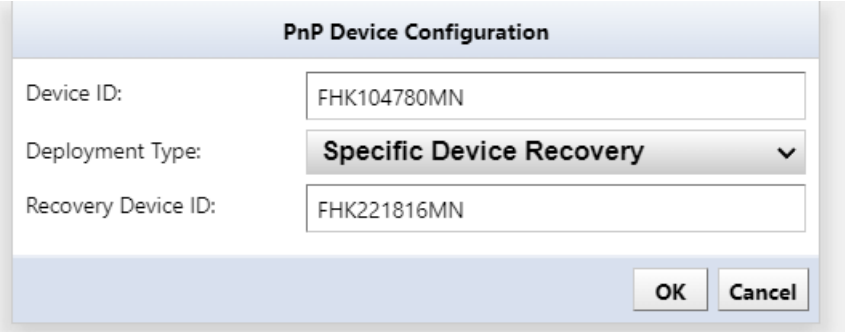
When you run Zero-Touch in this mode, you can connect a new device to the same location as the old device, write configuration from your old device to your new device, and restore your old device.

The device restore function is similar to the Zero-Touch template function:

1. Click the [Configuration] tab, and click the button.



2. Enter the required information in the Zero-Touch [PnP Device Configuration] window.
3. Select the [Specific Device Recovery].
4. Click the [OK] button to save.



There is an additional field here called Recovery Device ID. For the recovery device ID, specify the device ID as in the first field, but enter the ID of the old device before replacement in this field.

The configuration information for the old device in {{ProductName}} is then uploaded to the new device over the network. Other operations are the same as those for Zero-Touch templates.

8.8.8 Precautions when handling newly introduced devices

When uploading a configuration using {{ProductName}} Zero-Touch, if this is the first time the device has been powered on, the device will startup-config must not exist. To do so, specify the appropriate ordering option when ordering the device from the vendor (e.g., CCP-CD-NOCF, CCP-EXPRESS-NOCF option, etc.)

8.9 Monitors

The [Monitors] tab provides centralized management for monitoring network devices, services, wireless controllers, and supporting protocols (including SNMP, ICMP, VMware, MySQL, PostgreSQL, WinRM). You can configure monitoring templates, apply monitor sets to device groups, validate credentials, and track performance metrics like resource utilization and response times. The interface allows navigation through template-based configuration and real-time status monitoring.

The [Monitors] tab contains five subtabs:

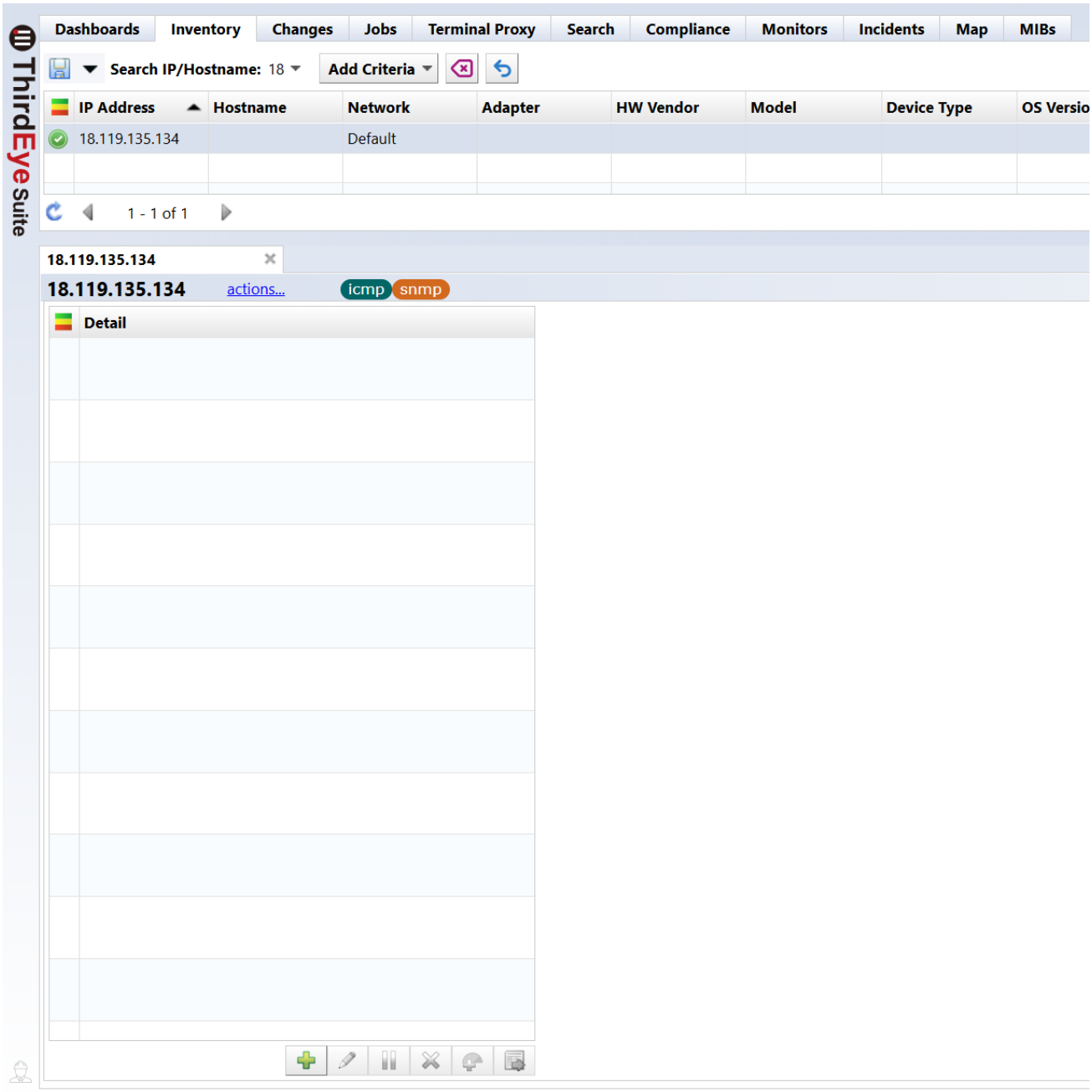
- [Sets]
- [Templates]
- [Alert Policies]
- [Violations]
- [SNMP Traps]
- [Syslog]

Subtab	Explanation
Sets	Manage groups of monitors (Monitor Sets) for bulk application to multiple devices
Templates	Store preconfigured monitoring templates with collection methods and threshold definitions
Alert Policies	Configure automated responses to detected issues (notifications/incidents/commands)
Violations	Track and display policy breaches with severity levels and affected devices
SNMP Traps	Configure real-time trap monitoring with OID-specific conditions and auto-clear rules
Syslog	Manage syslog message monitoring through Agent-D with pattern matching capabilities

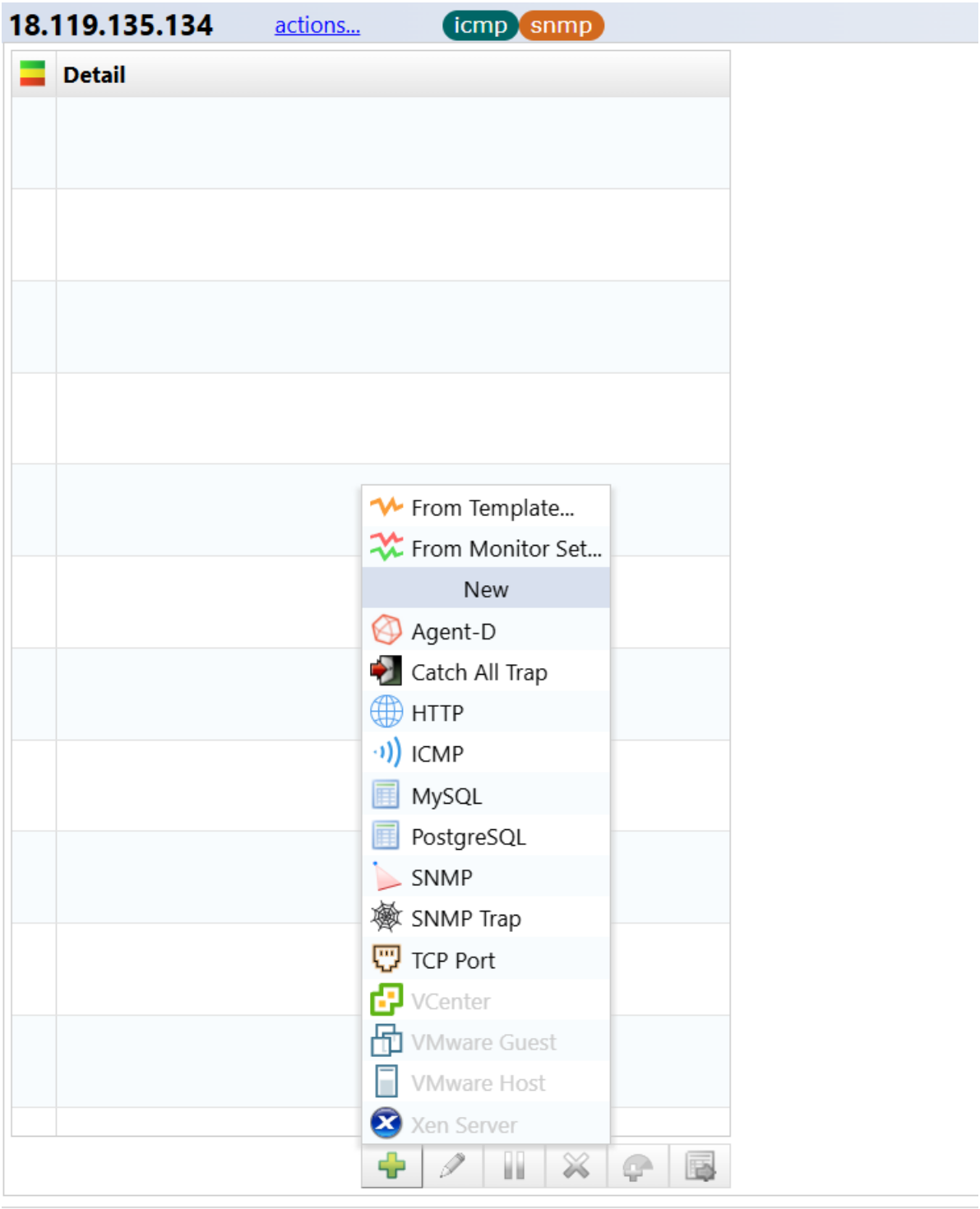
8.9.1 Configure various monitoring settings

8.9.1.1 Monitor your website You can send HTTP requests, monitor web ports, and monitor specific sites.

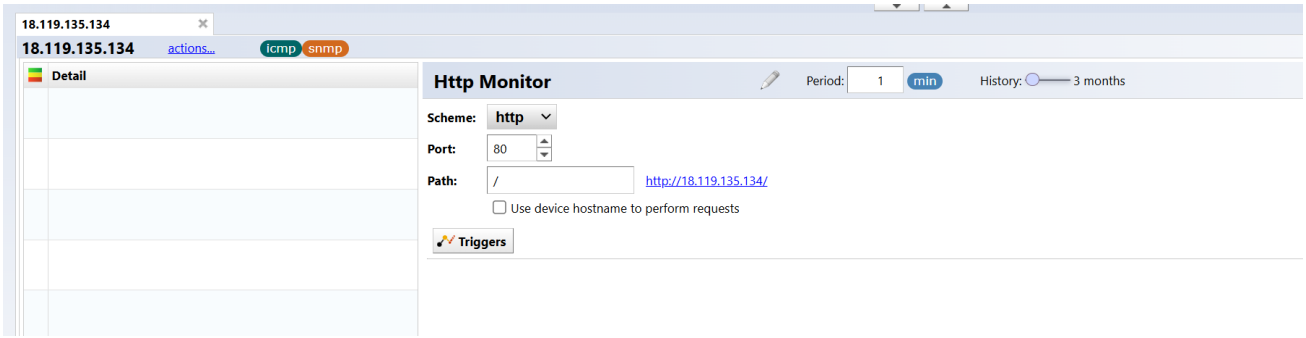
1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.



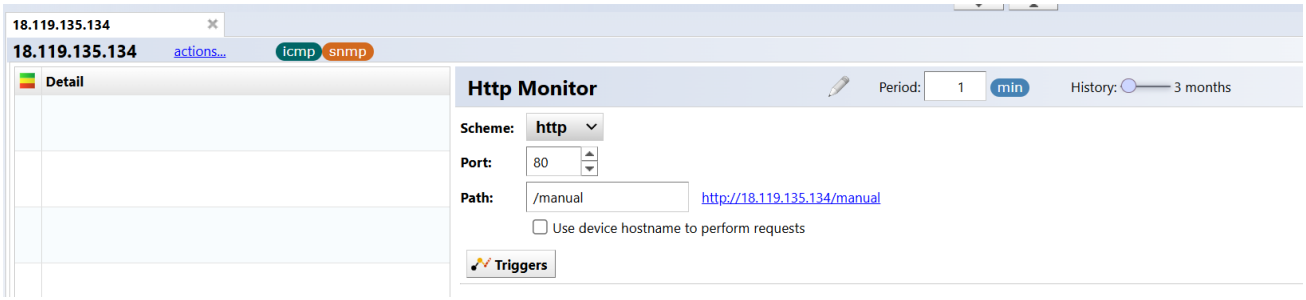
2. Click the button at the bottom left, and then click [HTTP].



3. Set any monitor name and interval.

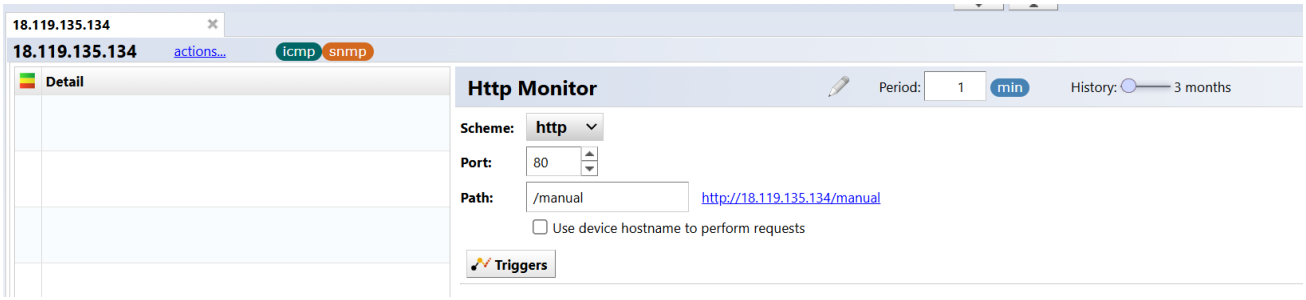


4. Enter the following items.



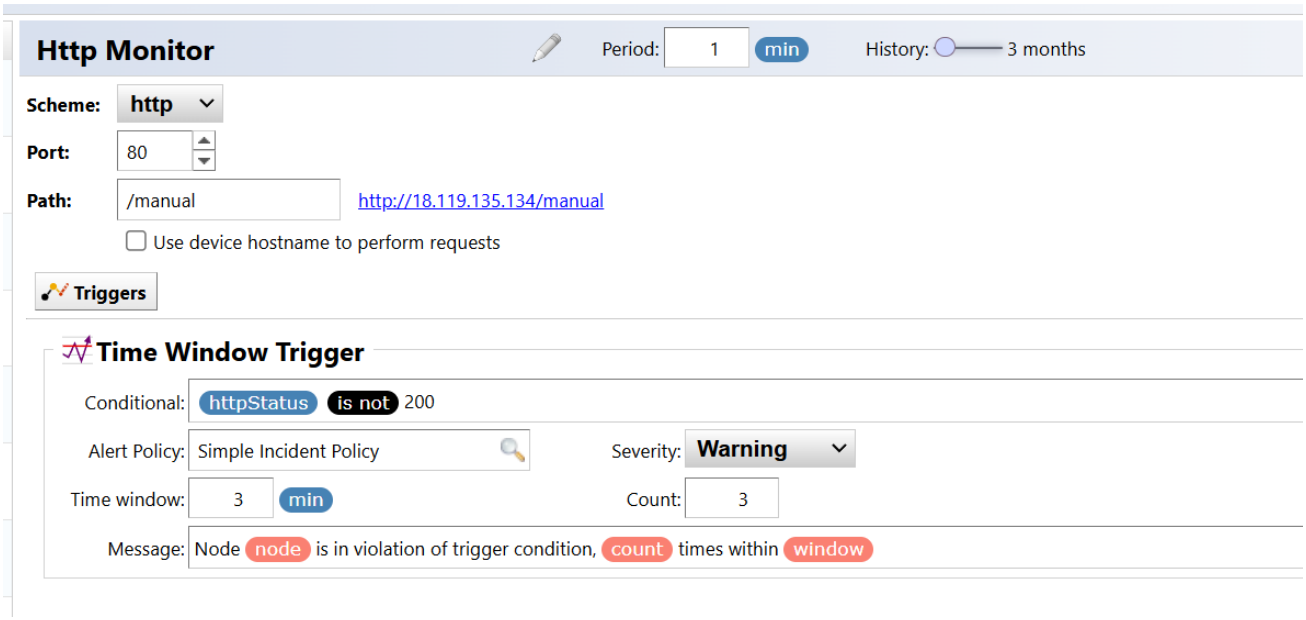
Item	Explanation
scheme	Select HTTP or HTTPS.
port	Specify the web port.
path	Enter the path of the site you want to monitor.

5. Click [Trigger], then click [Time window].



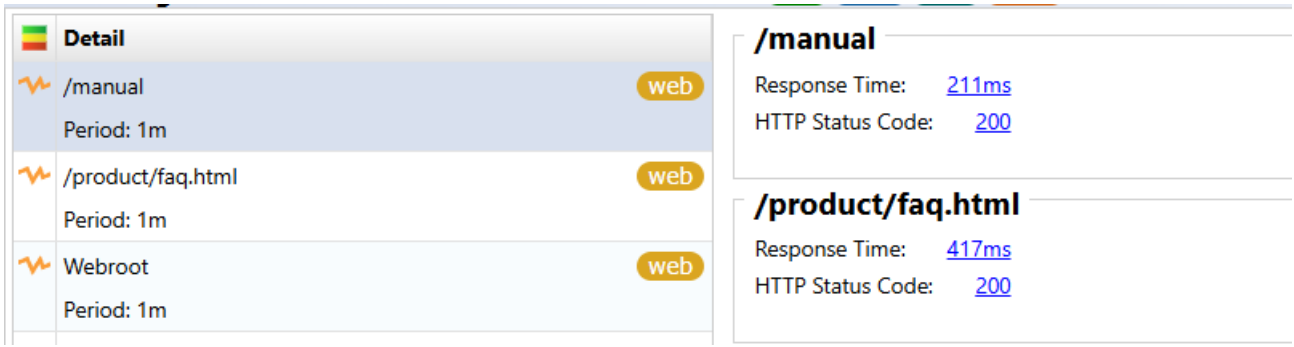
6. Set each item.

In the conditions on the screen below, any status code other than “200” will be alerted.



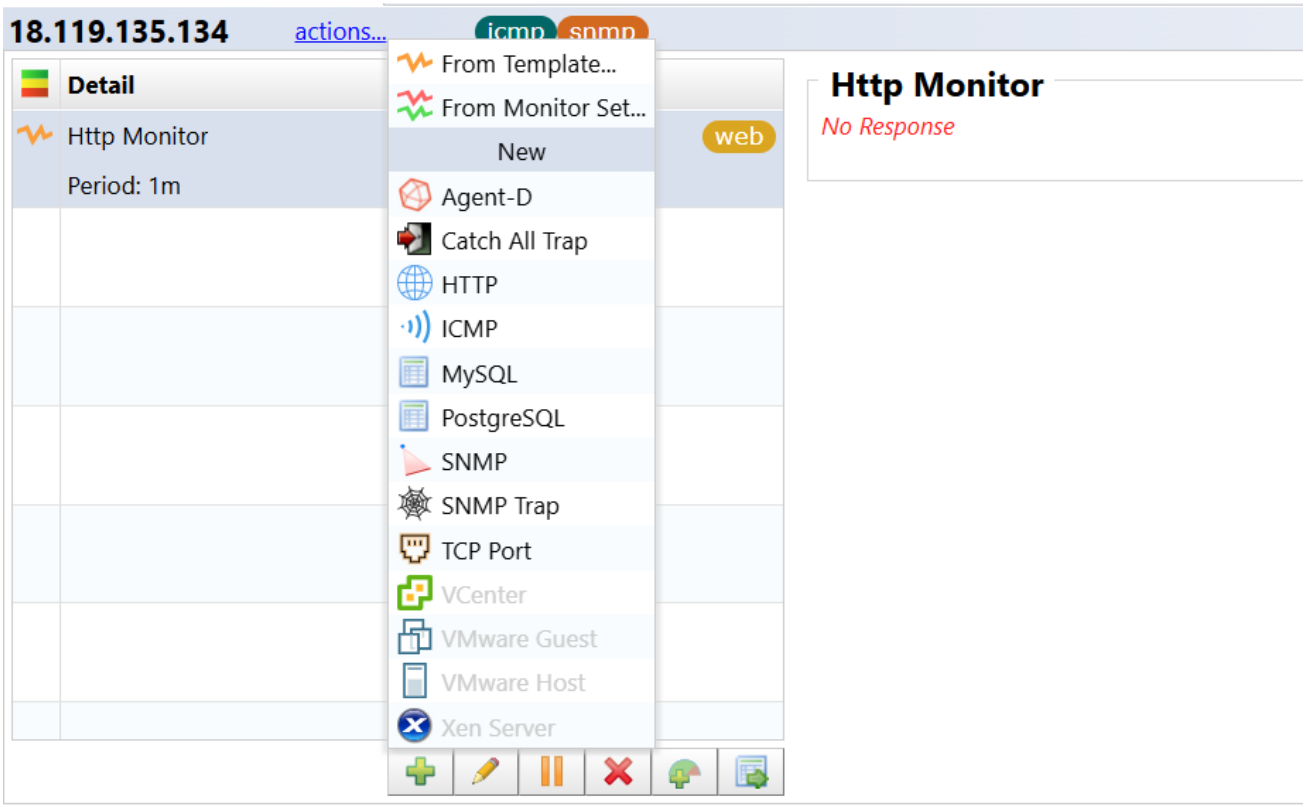
7. Click [Save].

After saving, the request will start and if successfully retrieved, the data will be displayed on the device details screen.



8.9.1.2 Monitor TCP ports You can send a syn message to a TCP port and check if there is a response.

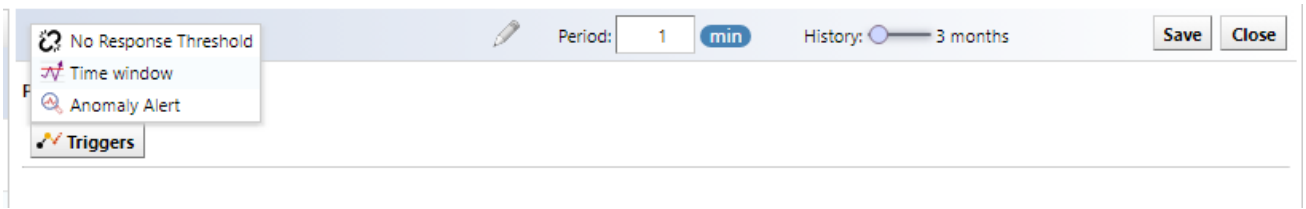
1. Click the button at the bottom left, and then click [TCP Port].



2. Set any monitor name and interval.

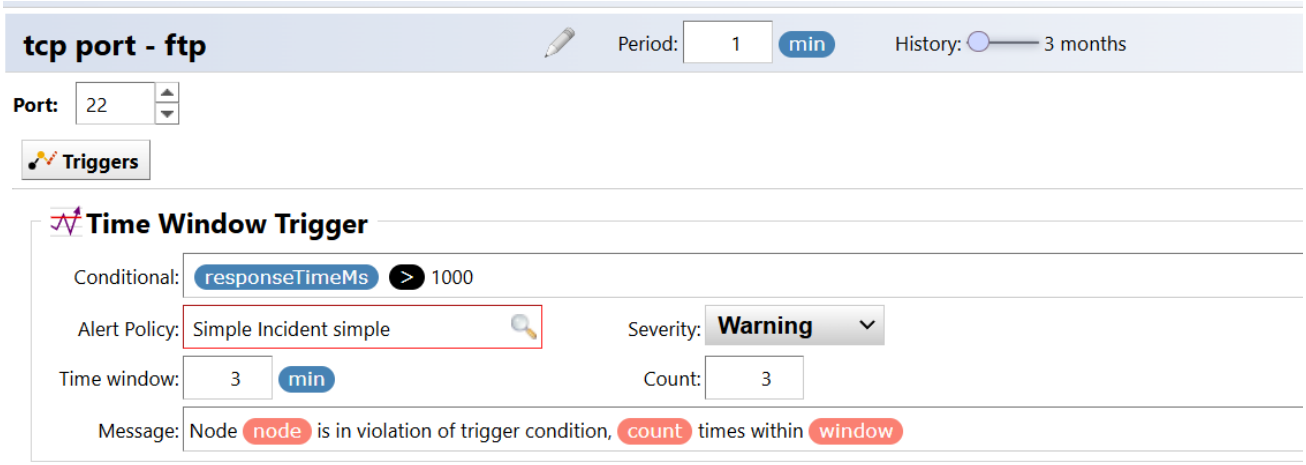
3. Set the port number to monitor.

4. Click [Triggers], then click [Time window].



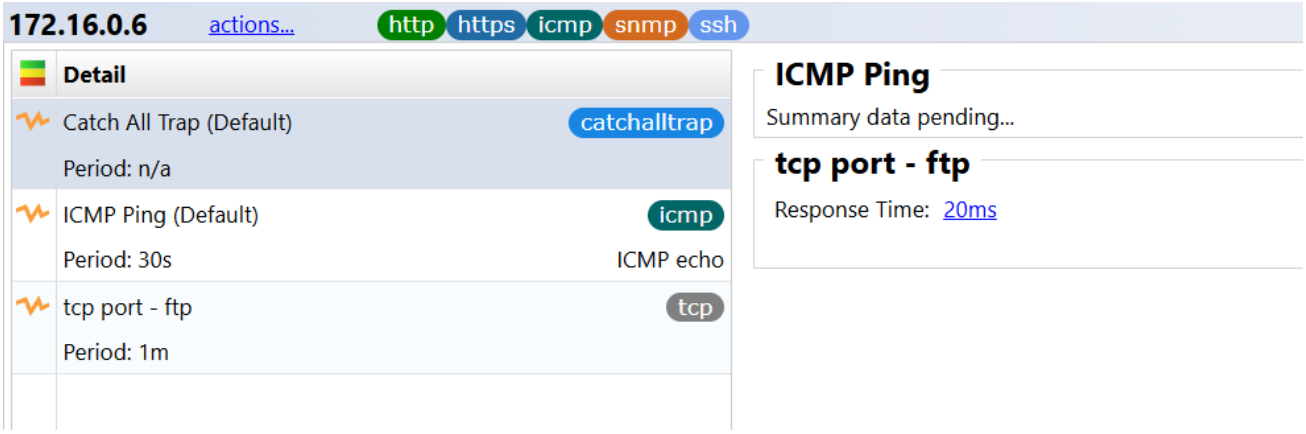
5. Set each item.

In the conditions shown on the screen below, if the response is longer than 1000 milliseconds, it will be alerted.



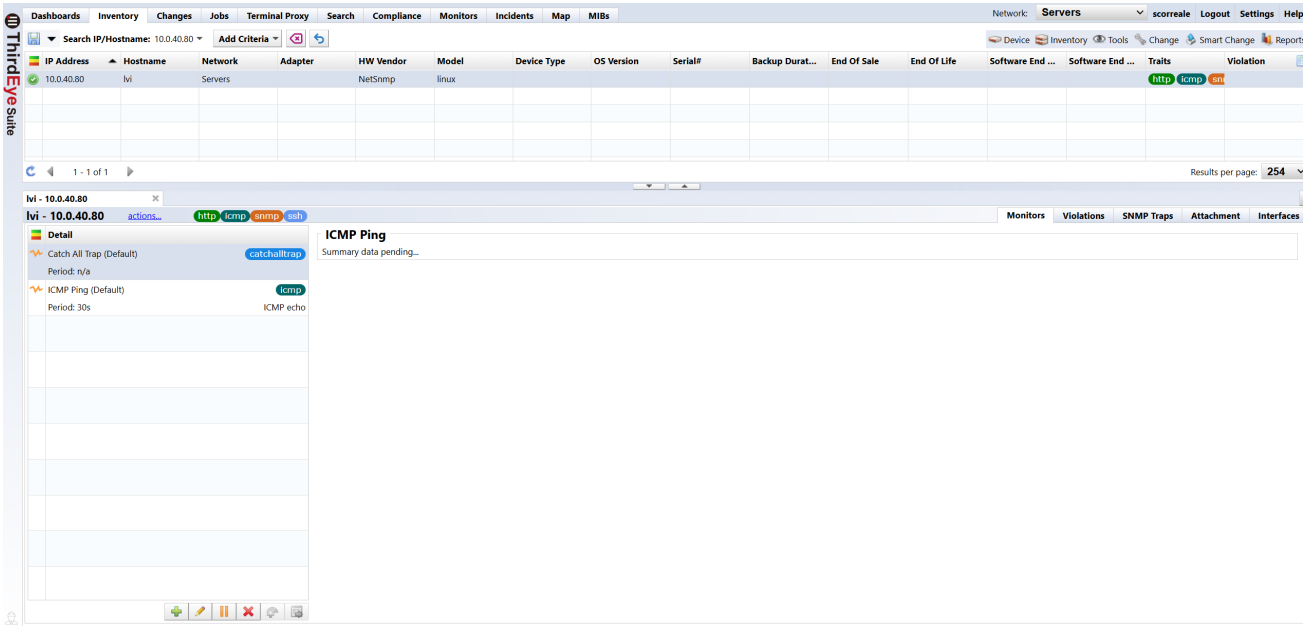
6. Click [Save].

After saving, the request will start and if successfully retrieved, the data will be displayed on the device details screen.



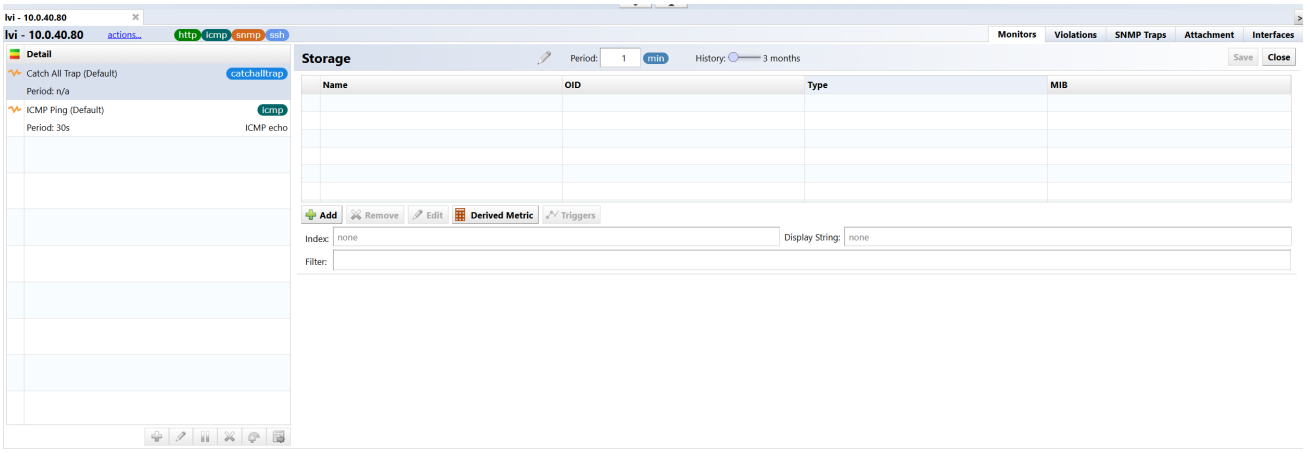
8.9.1.3 Monitor using calculation formulas ThirdEye allows you to automatically calculate acquired data using custom formulas. For example, the standard MIB HOST-RESOURCE-MIB includes MIBs for server disk size and usage, but does not include MIBs for usage rate (%). By using a custom formula, you can calculate disk size and usage to give a usage percentage. Here, we will describe the procedure using HOST-RESOURCE-MIB as an example.

1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.

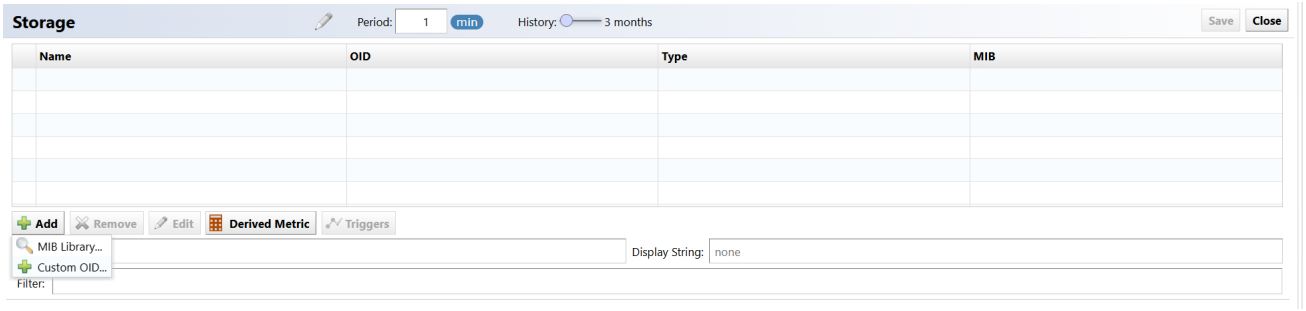


2. Click the  button at the bottom left, and then click [SNMP].

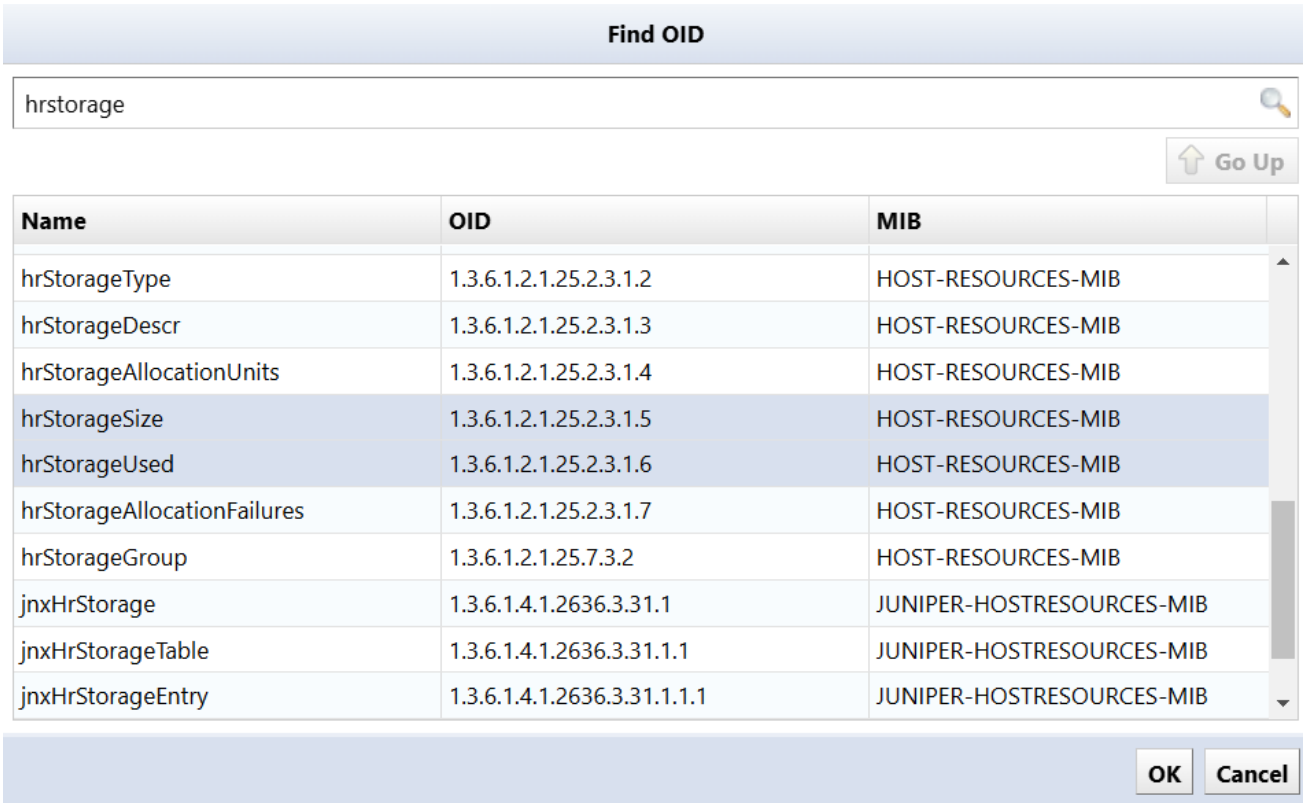
3. Set any monitor name and interval.



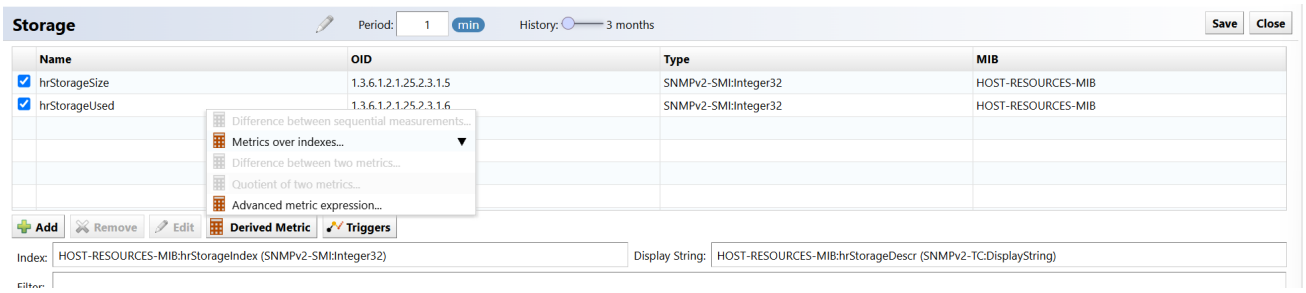
4. Click [Add] > [MIB Library].



5. Enter "`hrstorage`" in the OID search, select "`hrStorageSize`" and "`hrStorageUsed`" from the search results, and click [OK].

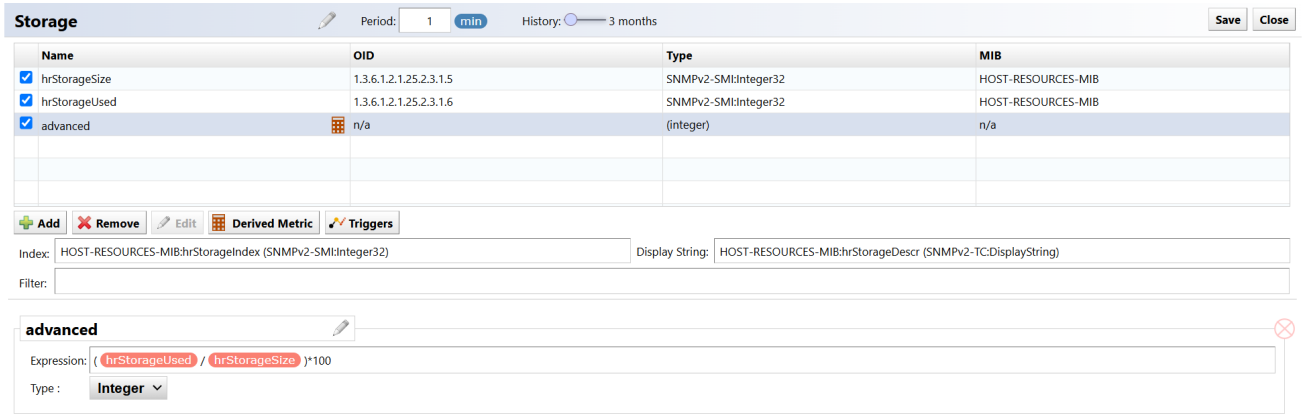


6. Click [Derived Metric] > [Advanced metric expression].

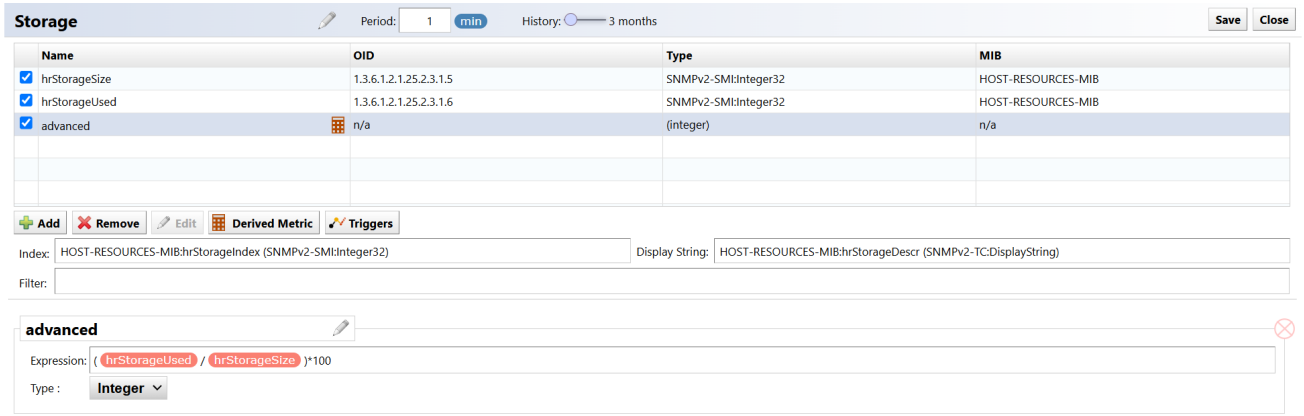


7. Enter the name and formula, and select the type.

The type can be Integer or Float. Integer uses whole numbers, Float uses up to two decimal places.

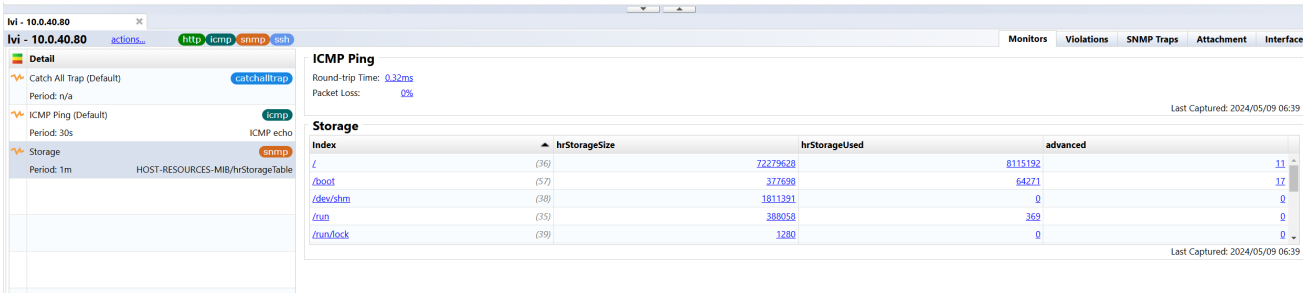


8. Click [Save].



After saving, data collection will begin and results will be displayed.

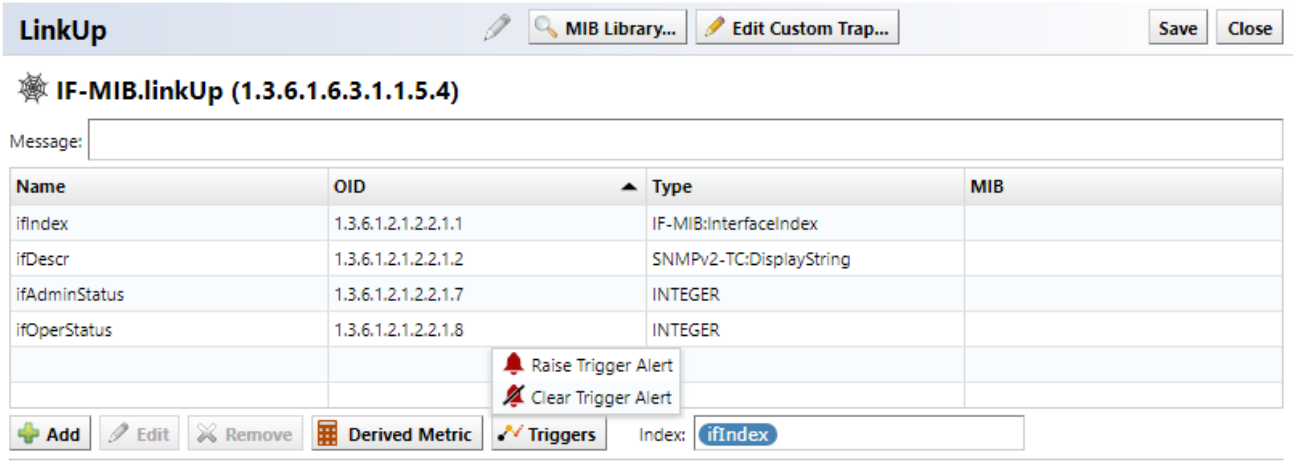
You can also set thresholds for calculated values using custom formulas.



8.9.2 Automatically clear specific trap incidents when traps are received

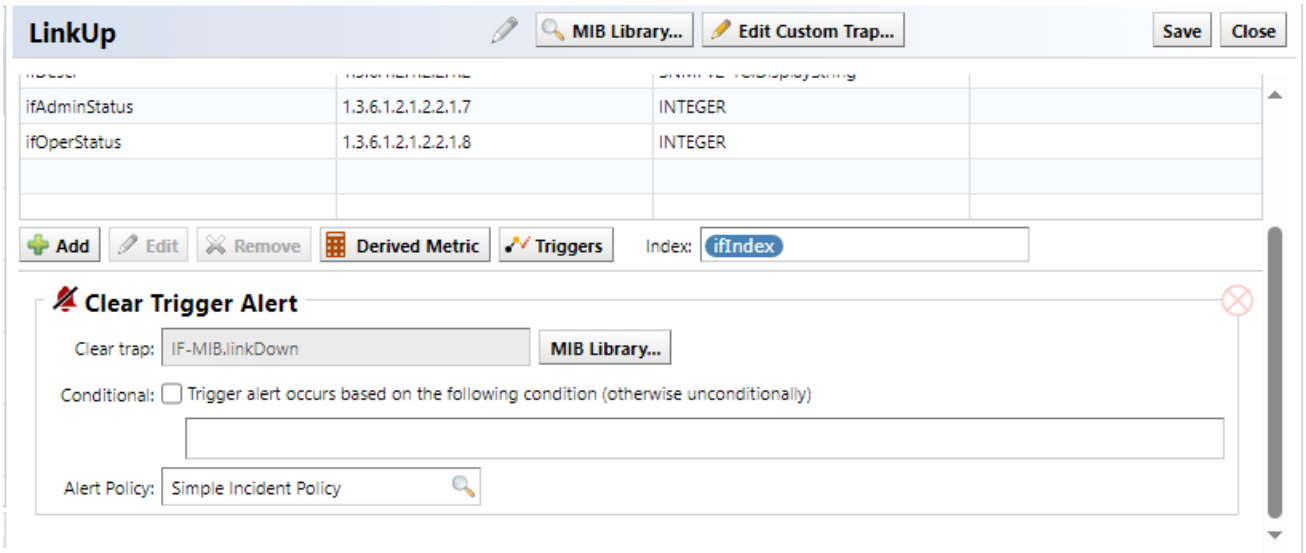
When you receive a correlated trap, you can automatically clear the fault and return the icon color and status icon on the map to their normal state. For example, LinkDown trap and LinkUp trap. After a LinkDown trap is received and an incident occurs as a failure, the LinkDown trap is cleared when a LinkUp trap is received.

1. Create a monitor for LinkDown traps.
2. Create an SNMP trap monitor for LinkUp.
3. Click [Trigger], then click [Clear Trigger Alert].



4. Click [MIB Library] for the trap you want to release and add the LinkDown trap.

5. Click [Save].

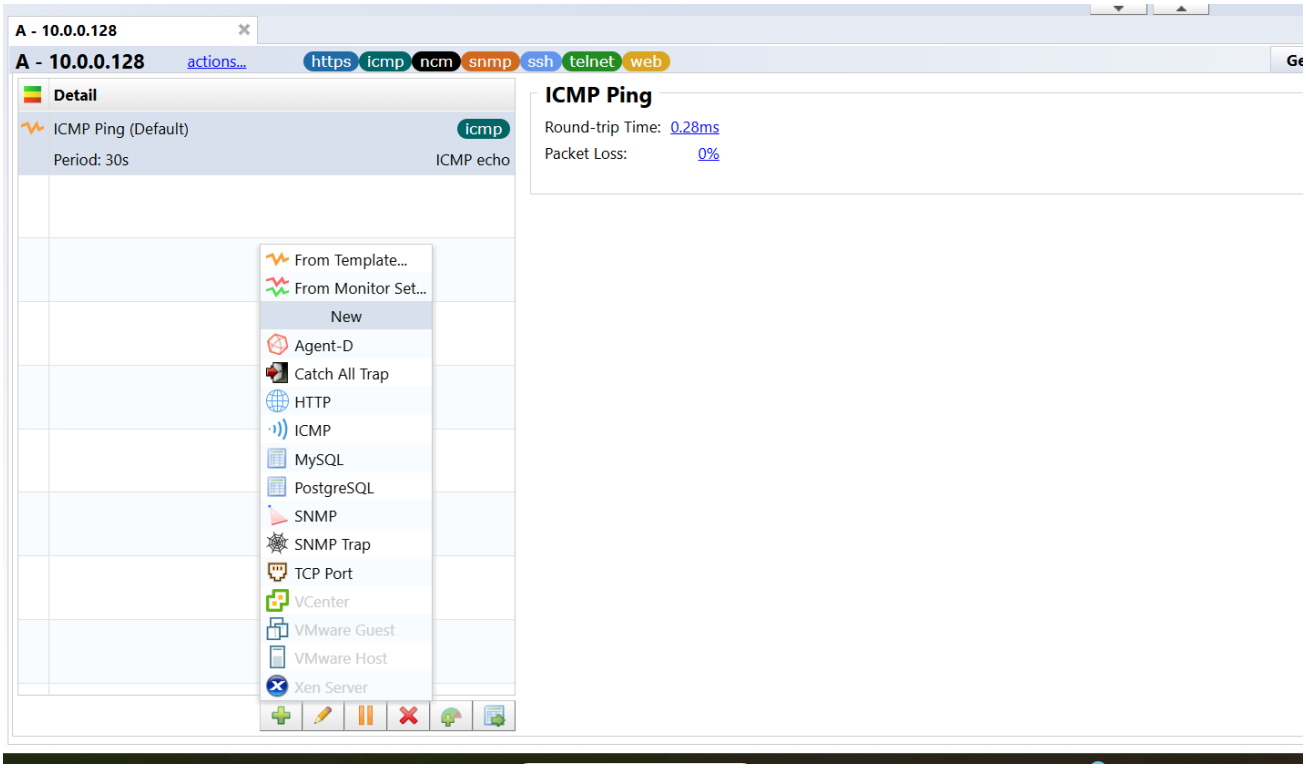


8.9.3 Change the action based on the value contained in the trap

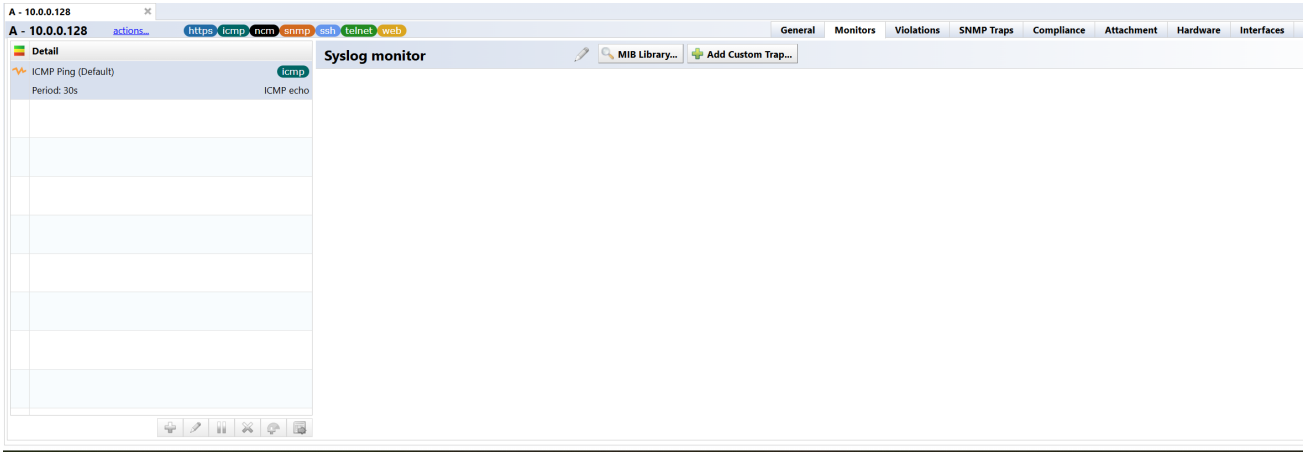
When the monitored device sends a trap, it puts various information into the trap and sends it. Depending on the content, you may not want to detect it as a failure. ThirdEye allows you to filter by specifying conditions.

The example below uses Syslog traps from Cisco equipment to filter traps.

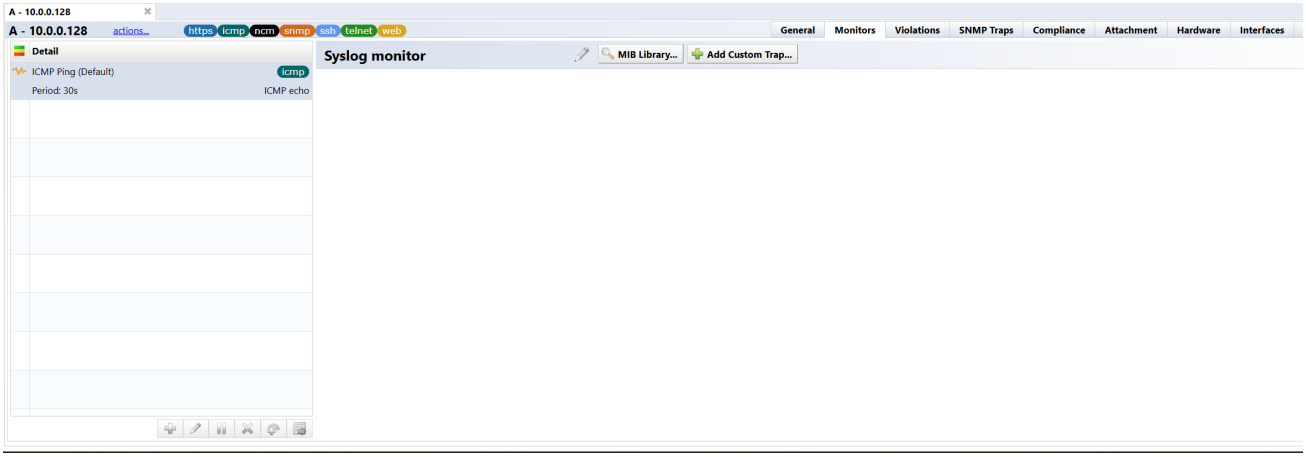
1. Add an SNMP trap monitor.



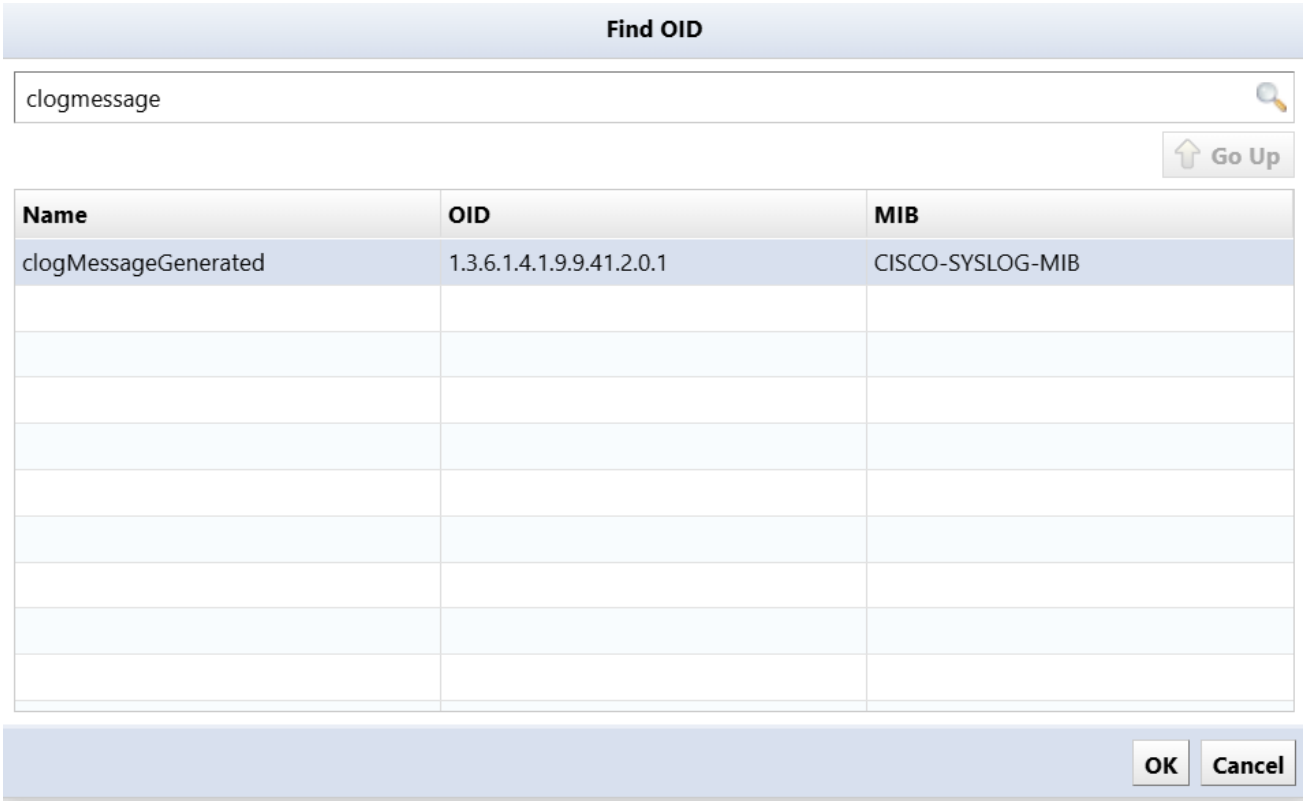
2. Displays any monitor name.



3. Click [MIB Library].

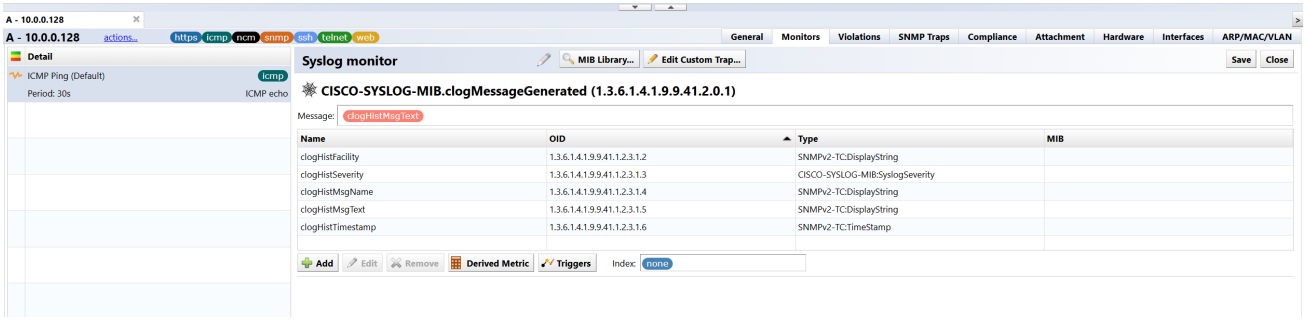


Enter "`clogmessage`" in the OID search, select "`clogMessageGenerated`" from the search results, and click [OK].

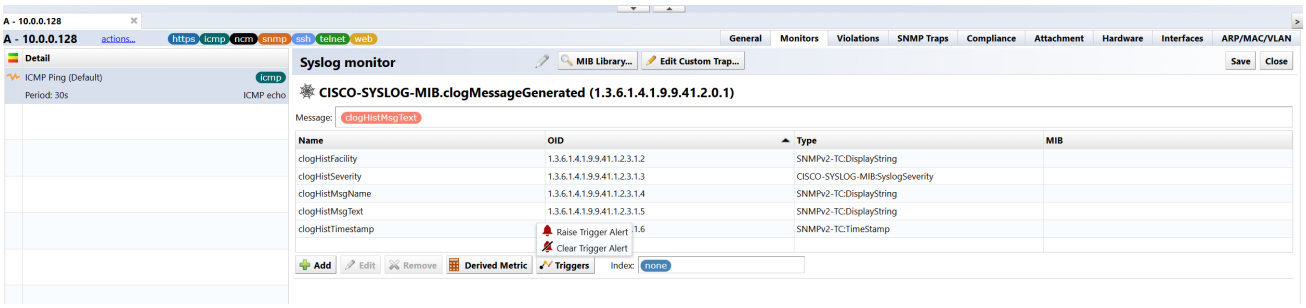


4. Enter a message when a failure occurs.

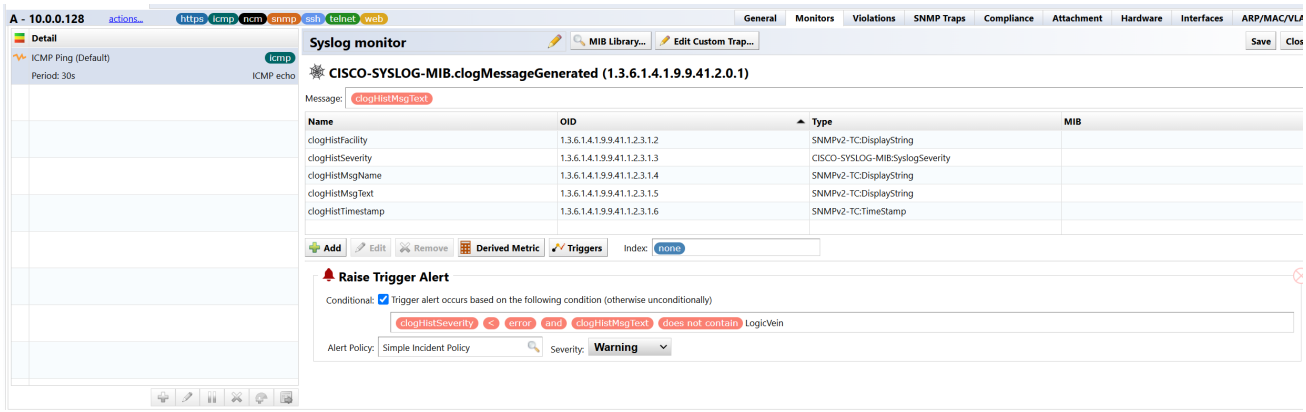
The following shows "clogHistMsgText" (message content) included in the trap.



5. Click [Trigger] and then click [Raise Trigger Alert].

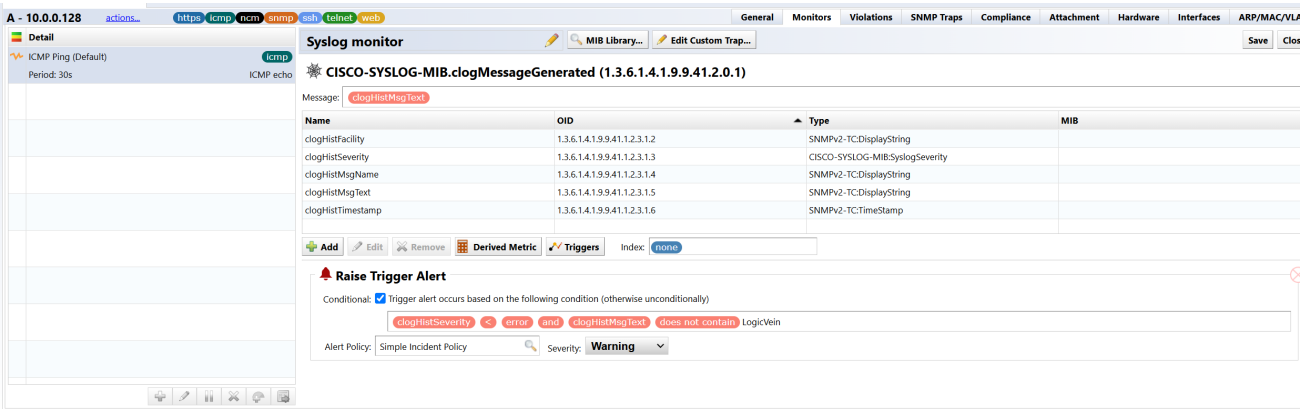


6. Check the box next to "Conditional" and enter your Trigger Alert conditions.



In the above example, if "clogHistSeverity" is severity "error" or higher ("emergency", "alert", "critical"), and the value of "clogHistMsgText" does not include "LogicVein", the alert will be targeted.

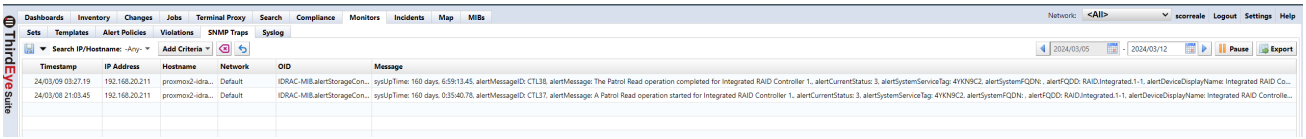
7. Set the policy and severity.



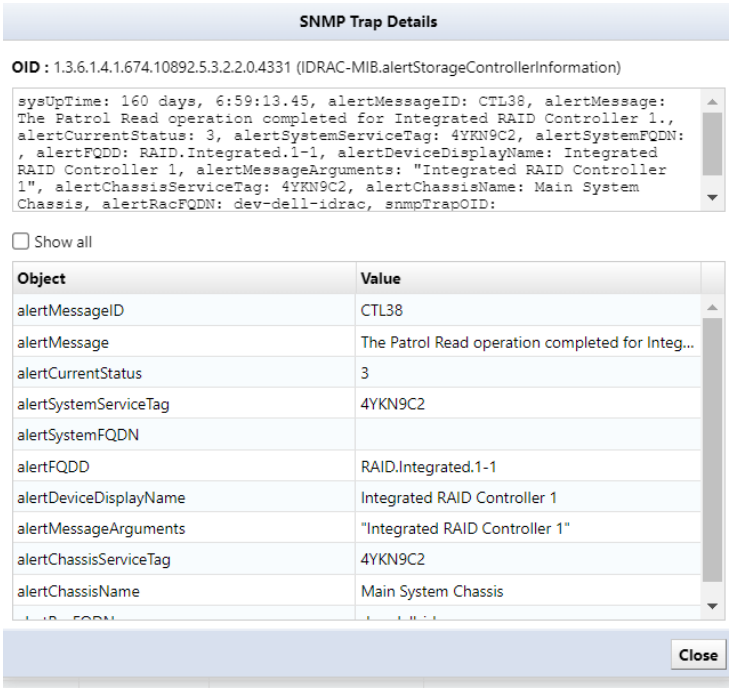
8. Click [Save].

8.9.4 Check SNMP traps from registered devices

SNMP traps sent from monitored devices registered as devices in ThirdEye can be checked from the [Monitors] > [SNMP Trap] tabs. You can also use the search function to display only SNMP traps sent from a specific device.



You can view trap details by doubleclicking on a trap. Additionally, the displayed traps can be exported to a CSV file by clicking the [Export] button.



8.9.5 Set up monitoring

There are several ways to monitor devices, such as information collection using SNMP and monitoring using ICMP Ping. This section describes the flow of basic monitoring settings.

The flow to start monitoring is as follows:

1. Setting actions (alert policy function)
2. Setting monitoring items (monitor function)
3. Trigger settings such as threshold value (trigger function)

8.9.5.1 Set actions when a failure is detected There are several ways to take action when a failure is detected:

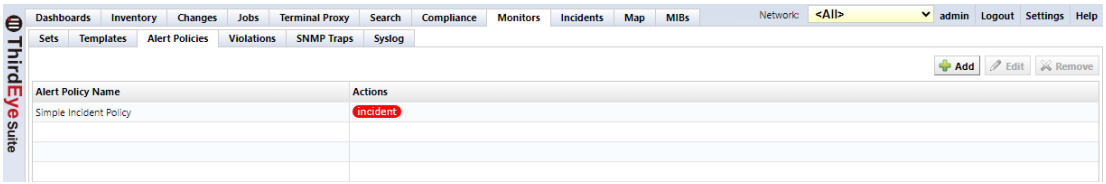
- Incident registration/sending emails
- Program execution
- SNMP trap

Configure these actions on the [Monitors] > [Alert Policy] tabs.

> **Note**
>
> If you change the alert policy after detecting a failure, the changed alert policy will be applied once you clear the violation caused by the failure.

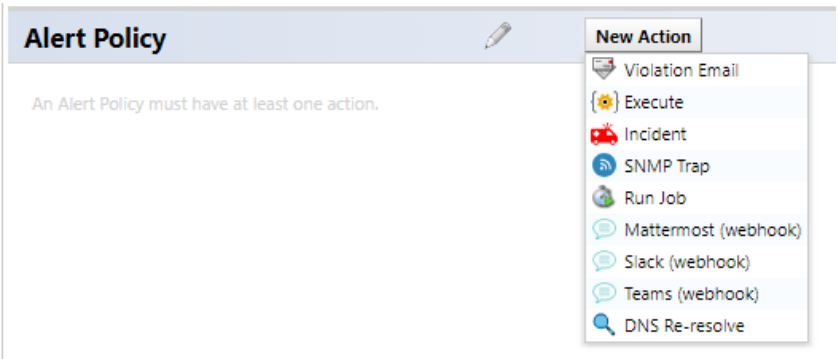
Below are the steps to create a new alert policy.

1. Click [Monitors] > [Alert Policy] tabs, then click the [Add] button.



2. Enter the alert policy name, click [New Action], and select an action.

Multiple actions can be added. These actions are explained in the table below:



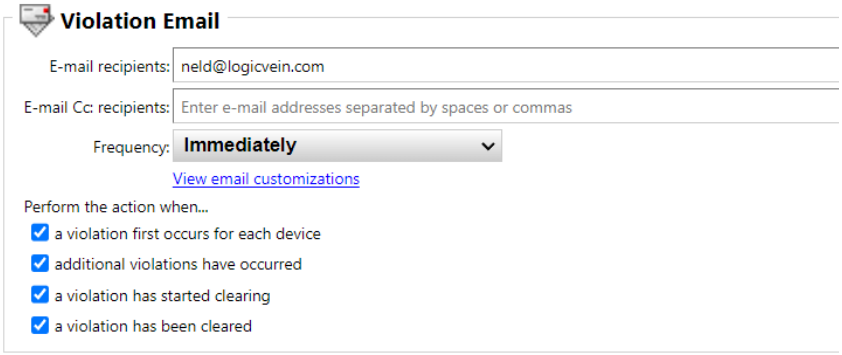
Action details

Action	Explanation
Execution	Executes a command on a remote host when a failure is detected.
Incident	Registers an incident and sends an email when a failure is detected.
SNMP Trap	Sends an SNMP trap when a failure is detected.
Run job	Execute the registered job.
Violation mail	Sends an email when a failure is detected.
Mattermost	Notify Mattermost when a failure is detected.
Slack	Notify Slack when a failure is detected.
Teams	Notify Teams when a failure is detected.
Line	Notify Line when a failure is detected.
DNS Re-resolve	When monitoring based on host name, if ICMP monitoring fails, a reverse lookup will be performed on the DNS server again.

3. Click [Save], then click [Close].

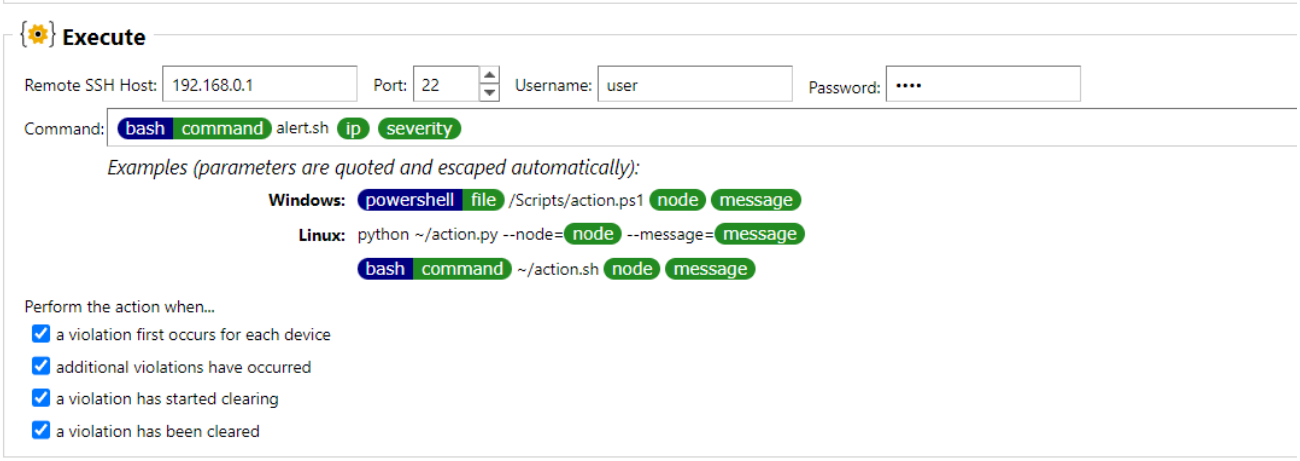
The alert policy settings are now complete. Each action is explained in detail below.

8.9.5.1.1 Violation Email Violation Email sends an email when an error occurs. To send e-mail, you must set up an e-mail server in advance.



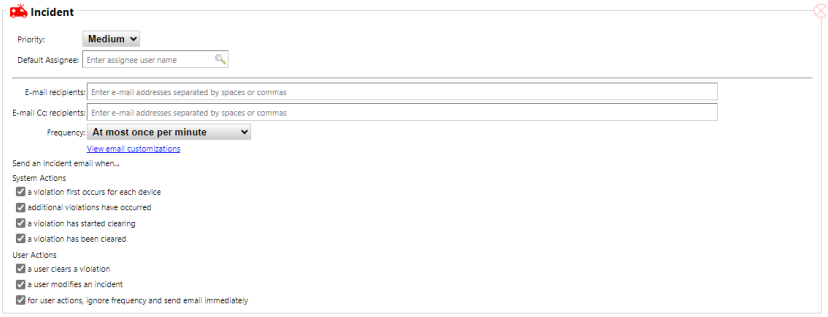
Violation Email Setting	Explanation
Email destination	Set the incident email destination.
Email destination Cc	Set the CC email destination.
limit	Specify when to notify by email. (Initial value: Do not notify more than once per minute)
View email customizations	You can customize the subject, preamble, and concluding sentence.
a violation first occurs for each device	Sends an email on first violation on a device-by-device basis.
additional violations have occurred	Sends an email when the number of violations increases.
a violation has started clearing	Sends an email when the status automatically transitions to “Clearing”.
a violation has been cleared	Sends an email when the status automatically transitions to “Cleared”.

8.9.5.1.2 Execute You can run programs from remote hosts. Logs in to the specified remote host via SSH and executes the specified command from the remote host.



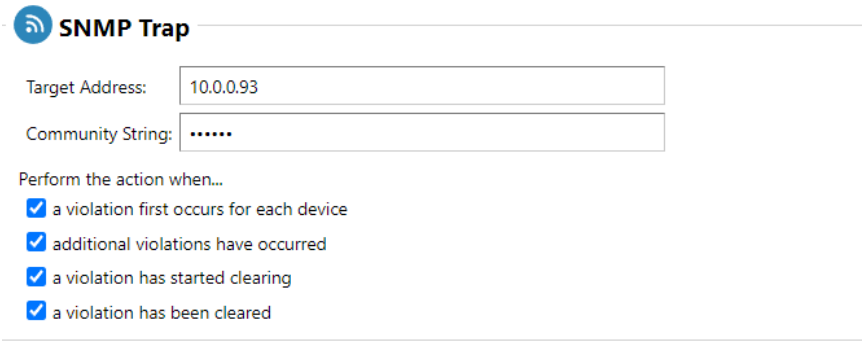
Execute Setting	Explanation
Remote SSH Host	Specifies the remote host (external server) on which to execute the command.
Port	Port number used for SSH connections.
Username	User used to log in to the remote host.
Password	The user's password used to log in to the remote host.
Command	Command to run on remote host.
a violation first occurs for each device	Execute the command on the first violation on a device-by-device basis.
additional violations have occurred	Executes a command when the number of violations increases.
a violation has started clearing	Execute the command when the status automatically transitions to "Clearing".
a violation has been cleared	Execute the command when the status automatically transitions to "Cleared".

8.9.5.1.3 Incident This action creates an incident when a failure occurs. You can also send an email by entering the email address in the email recipient/Cc field. To send e-mail, you must set up an e-mail server in advance.



Incident Setting	Explanation
Priority	Specify the priority when registering an incident.
Default Assignee	Specify the person responsible for the incident. If the user account that registered the email address is designated as the person in charge, when an incident is updated, the update will be notified to the email address of that user account.
E-mail recipients	Set the incident email destination. If not entered, the email will not be sent.
E-mail Cc recipients	Set the CC email destination. If not entered, the email will not be sent.
Frequency	Specify when to notify by email. Initial value: Do not notify more than once per minute.
View email customizations	You can customize the subject, preamble, and concluding sentence.
a violation first occurs for each device	Sends an email on first violation on a device-by-device basis.
additional violations have occurred	Sends an email when the number of violations increases.
a violation has started clearing	Sends an email when the status automatically transitions to “Clearing”.
a violation has been cleared	Sends an email when the status automatically transitions to “Cleared”.
a user clears a violation	Send an email when a violation is manually updated.
a user modifies an incident	Send an email when an incident is manually updated.
for user actions, ignore frequency and send email immediately	Regardless of the violation/incident, if it is manually updated, email will be sent immediately regardless of the “Frequency” setting above.

8.9.5.1.4 Send SNMP trap to devices When a failure occurs, a trap can be sent to other NMSs, alarm devices, etc.



Setting	Explanation
Target Address	Specify the destination of the SNMP trap sent when a failure occurs.
Community String	Specify the community string for SNMP traps to be sent.
a violation first occurs for each device	Sends an SNMP trap on a device-by-device basis at the first violation.
additional violations have occurred	Sends an SNMP trap when the number of violations increases.
a violation has started clearing	Sends an SNMP trap when the status automatically transitions to “Clearing”.
a violation has been cleared	Sends an SNMP trap when the status automatically transitions to “Cleared”.

The traps sent by ThirdEye are as follows:

trap name: triggerViolation

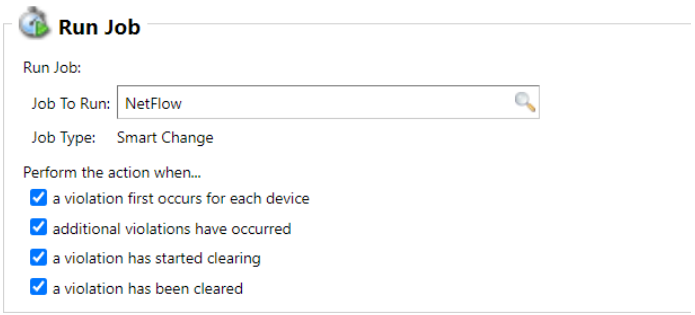
trap OID: 1.3.6.1.4.1.45654.2.1.1

Trap Variables	Variable Name	Explanation
	thirdEyeDeviceUuid	UUID of the failed device (used internally by ThirdEye)
	thirdEyeDeviceIpAddress	IP address of the device where the failure occurred
	thirdEyeManagedNetwork	Management network to which the failed device belongs (used by ThirdEye)
	thirdEyeDeviceHostname	Host name of the device where the failure occurred
	thirdEyeMessage	Incident message
	thirdEyeMeasurement	Monitor content
	thirdEyeSeverity	Incident severity

Trap Variables	Variable Name	Explanation
	thirdEyeDeviceCustom1	Custom 1 contents of the device where the failure occurred
	thirdEyeDeviceCustom2	Custom 2 contents of the failed device
	thirdEyeDeviceCustom3	Custom 3 contents of the failed device
	thirdEyeDeviceCustom4	Custom 4 contents of the device where the failure occurred
	thirdEyeDeviceCustom5	Custom 5 contents of the failed device
	thirdEyeClearStatus	Violation status (not cleared/clearing/cleared)
	thirdEyeOccurrenceCount	violation count
	thirdEyeFirstViolation	First violation (True/False)
	thirdEyeSeverityEnum	Incident severity number

8.9.5.2 Run Job Suite

You can run programs from remote hosts. Log in to the specified remote host via SSH and execute the specified command from the remote host.

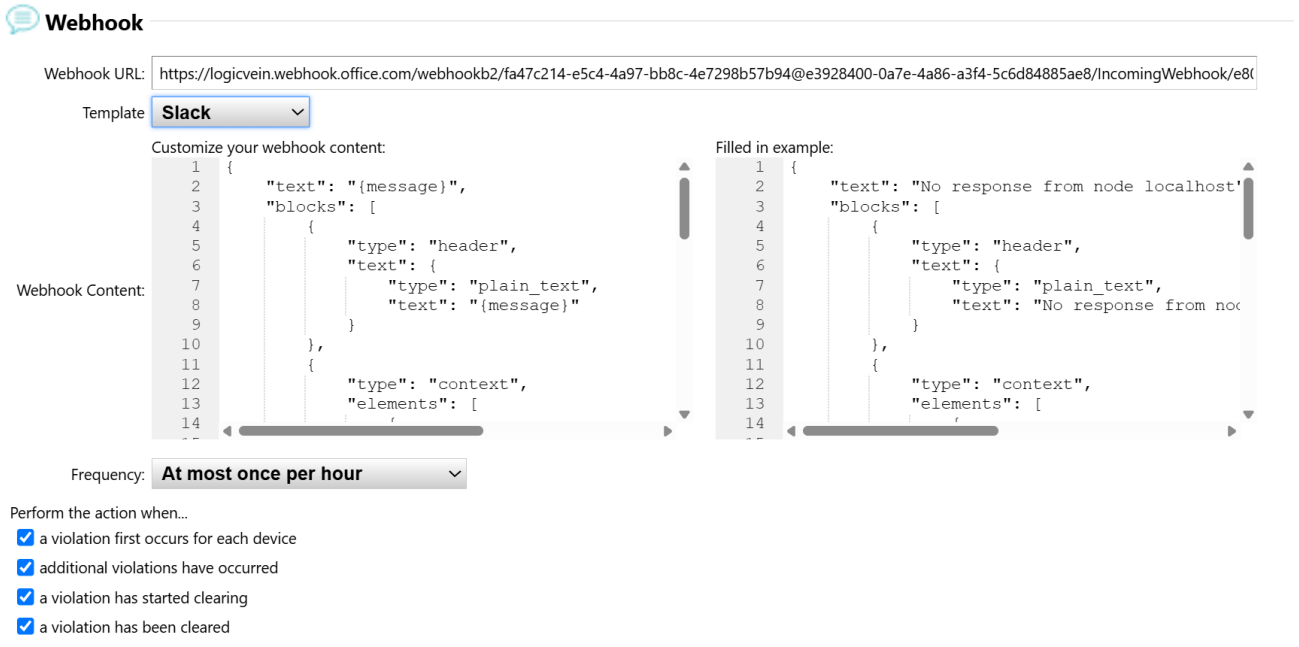


Run Job Setting	Explanation
Job To Run	Enter the job name of the job you want to run.
a violation first occurs for each device	Execute the command on the first violation on a device-by-device basis.
additional violations have occurred	Executes a command when the number of violations increases.
a violation has started clearing	Execute the command when the status automatically transitions to “Clearing”.
a violation has been cleared	Execute the command when the status automatically transitions to “Cleared”.

8.9.5.2.1 Webhooks Webhooks can be used to notify via Mattermost, Slack, Teams. and Lins when an abnormality occurs. To use this feature, you need to set up webhooks and add apps on each tool in advance.

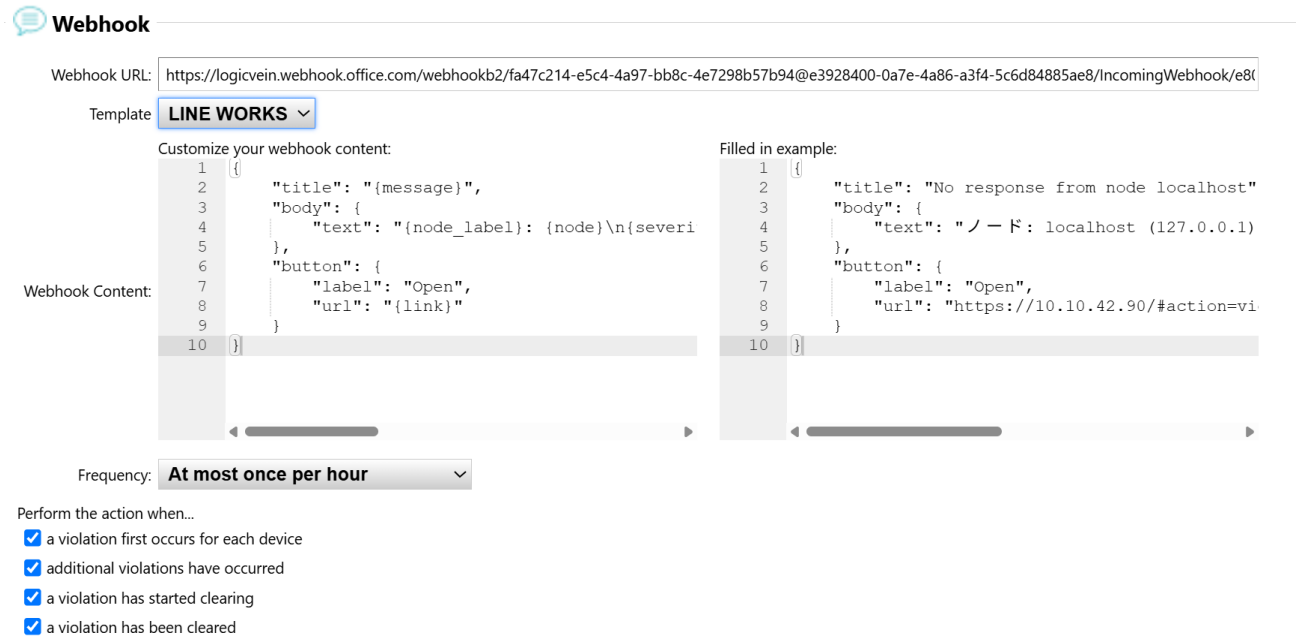
Mattermost:

Slack:



Teams:

Line:



Webhook Setting	Explanation
webhook url	Enter the URL generated on Mattermost/Slack/Teams/Line.
Channel	Enter the channel to post the notification to. (Mattermost only)
A user	Enter the user who will post the notification. (Mattermost only)
a violation first occurs for each device	Notifications will be sent on a device-by-device basis at the first violation.
additional violations have occurred	We will notify you if the number of violations increases.
a violation has started clearing	Notifies you when the status automatically transitions to “Clearing”.
a violation has been cleared	Notifies you when the status automatically transitions to “Cleared”.

8.9.5.3 Set up Ping monitoring You can add an ICMP monitor for ping monitoring. The "Default" ThirdEye monitor settings are automatically applied. A monitor called "ICMP Ping (Default)" is automatically assigned to monitored devices added manually or through discovery. Ping monitoring starts immediately after addition.

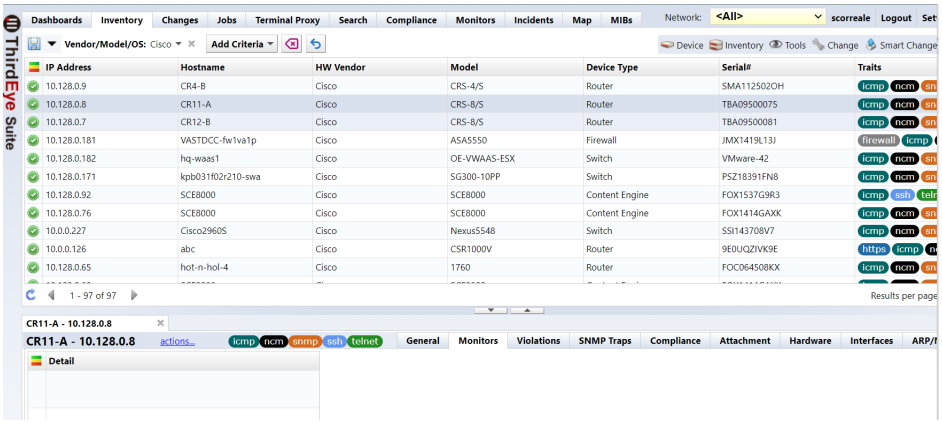
This section describes the steps to add a monitor with specific conditions to monitored devices.

Conditions:

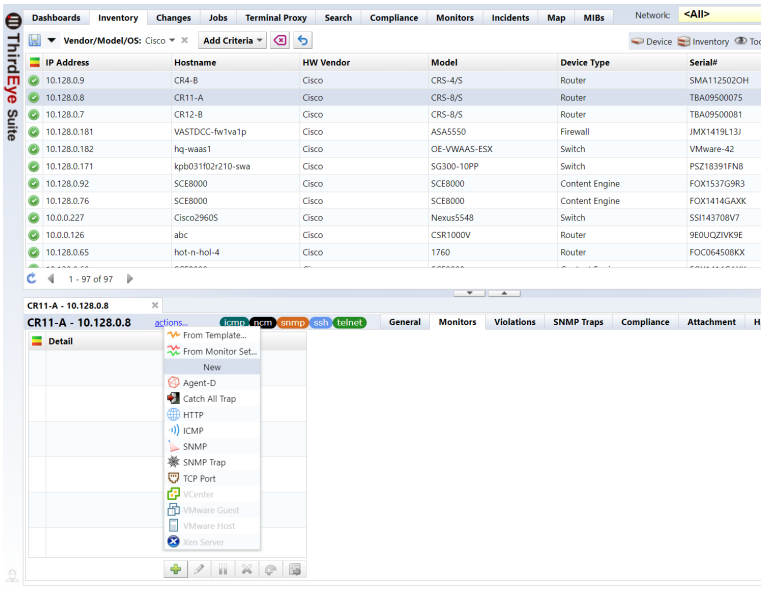
Monitoring interval: 5 minutes

Alert condition: Twice in 10 minutes if there is no response.

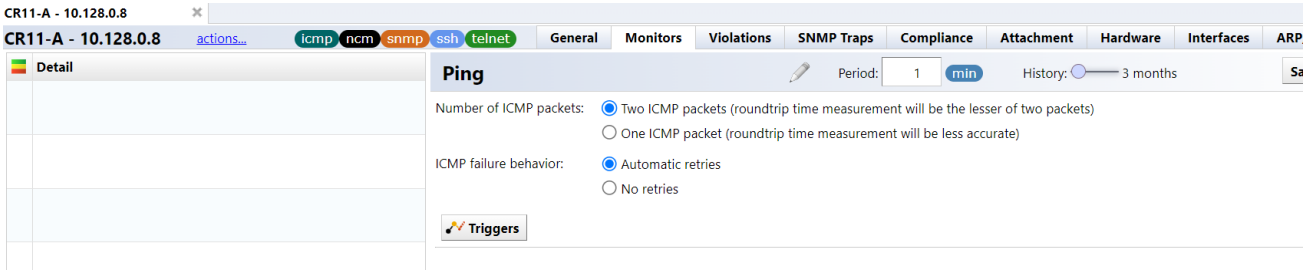
1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.



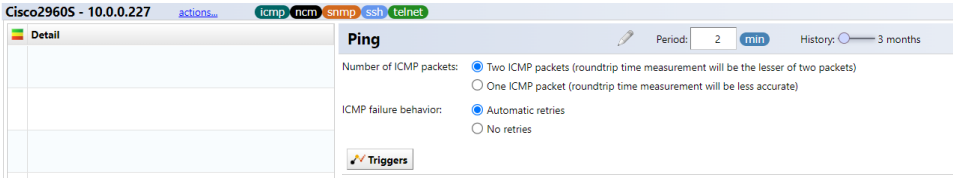
2. Click the button. in the bottom left of the window, and then click [ICMP] in the pop up menu.



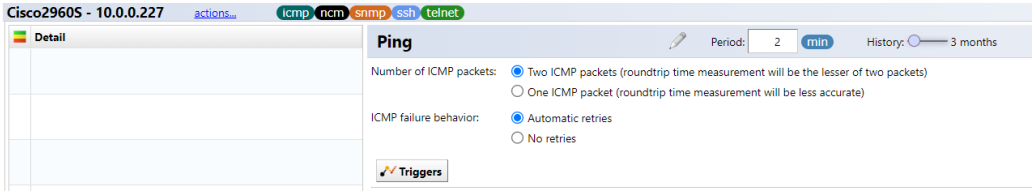
3. Enter any monitor name (“Ping” in the example below).



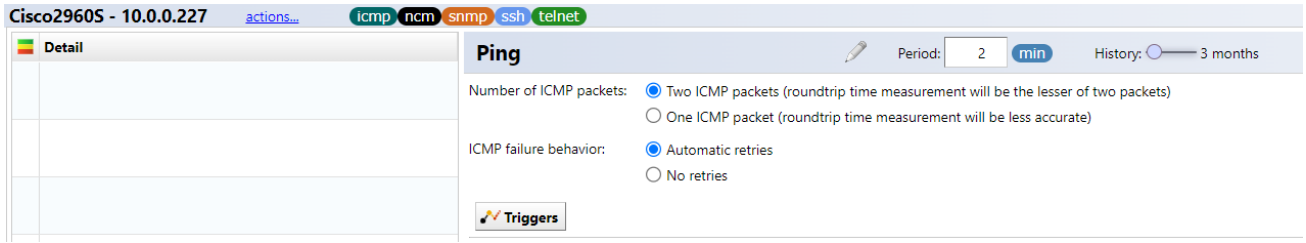
4. In the [Period] field, specify the interval (“2” in the example below).



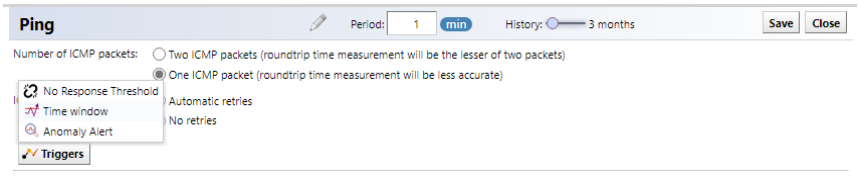
5. Use the [History] slider to specify a data retention period of 3, 6, or 12 months.



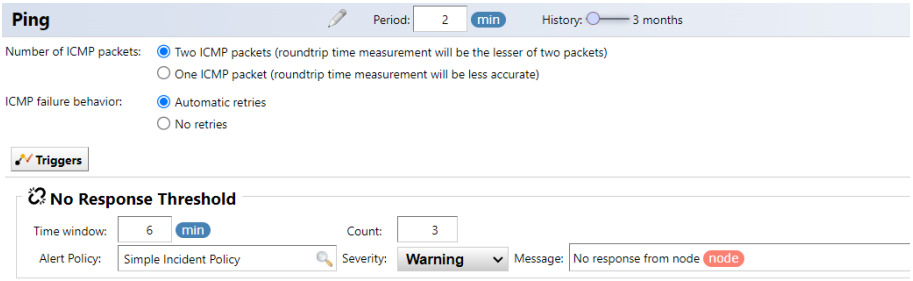
6. Use the “Number of ICMP packets” and “ICMP failure” options to select the ICMP transmission and retry counts.



7. Click [Trigger] and then select [No Response Threshold] from the pop up menu.



8. Enter the following items.

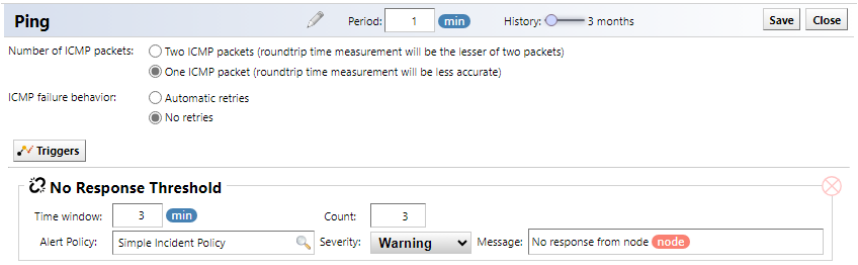


Monitor Setting	Explanation
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (Minimum value: 1)
Alert Policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning) “Emergency”, “Alert”, “Critical”, “Error”, “Warning”, “Notification”, “Information”, “Debug”
Message	Set the message displayed when a failure is detected. *In order to display the message, the “Incident Registration” action must be defined in the alert policy.

The different alert severity icons are shown in the correspondence table below:

Security level	Status	Severity status icon
High	**emergency**	
	alert	
	critical	
Priority	**error**	
	warning	
	notification	
	information	
Low	**debug**	

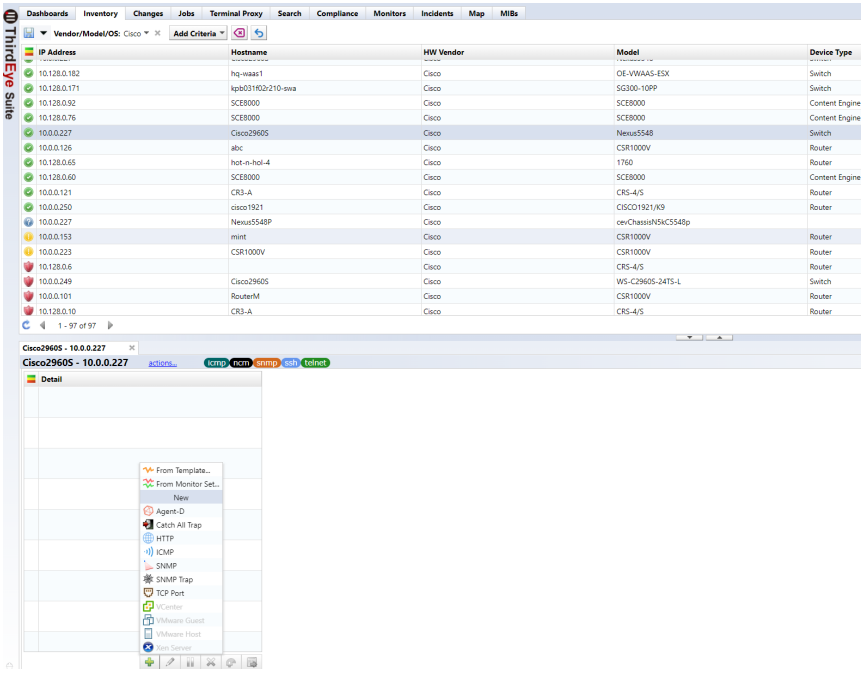
9. Click [Save].



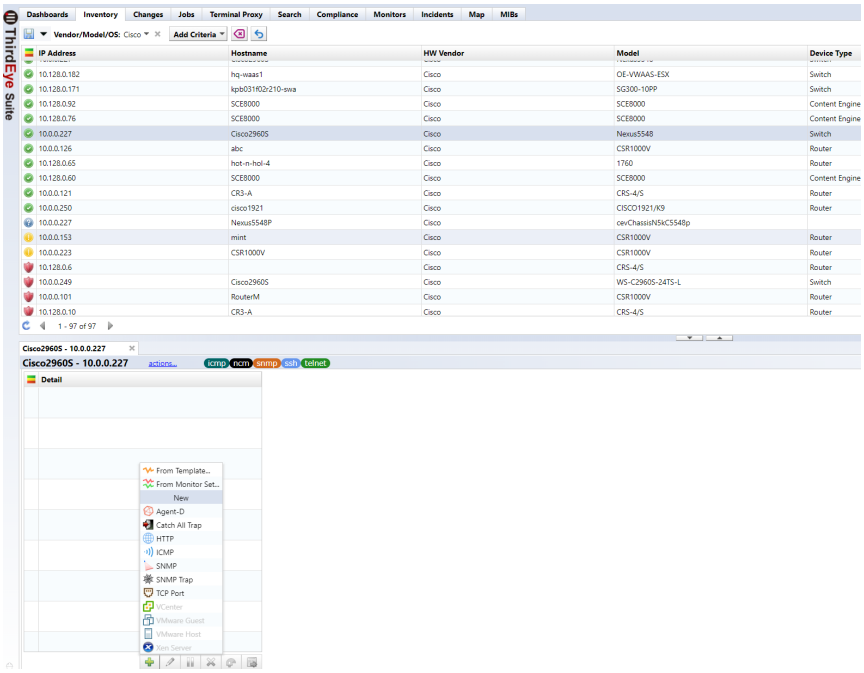
8.9.5.4 Collect SNMP information You can add an SNMP monitor to obtain MIB information such as CPU usage rate and traffic volume from monitored devices.

This steps to obtain the CPU usage rate (cpmCPUTotal1minRev) of a monitored Cisco device are explained below:

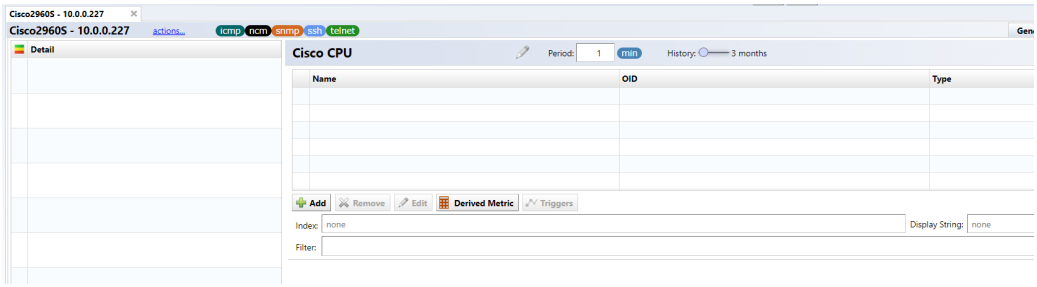
1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.



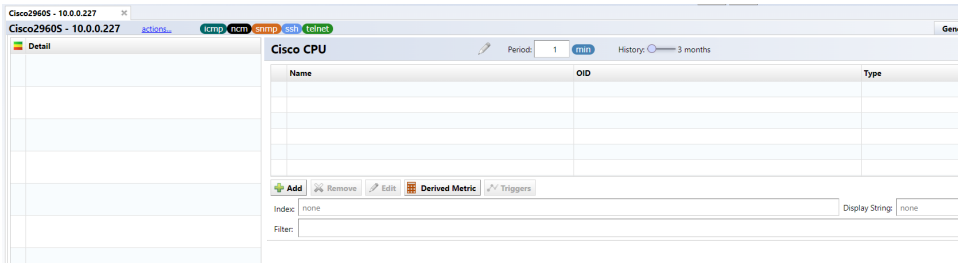
2. Click the button in the bottom left of the window, and then click [SNMP] in the pop up menu.



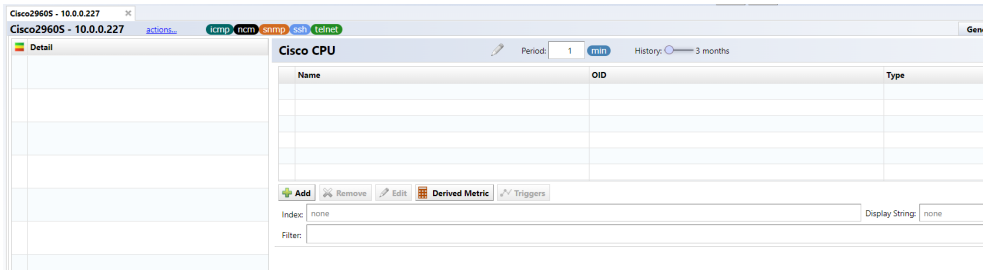
3. Enter any monitor name (“Cisco CPU” in the below example).



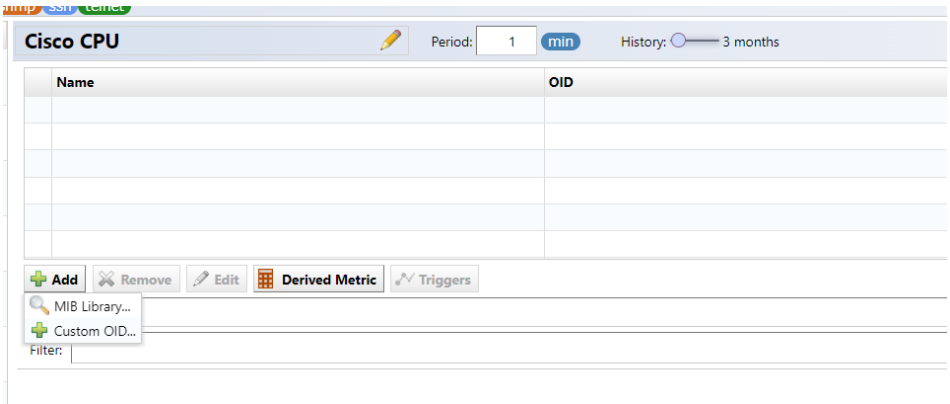
4. In the [Period] field, specify the interval (“1” in the example below).



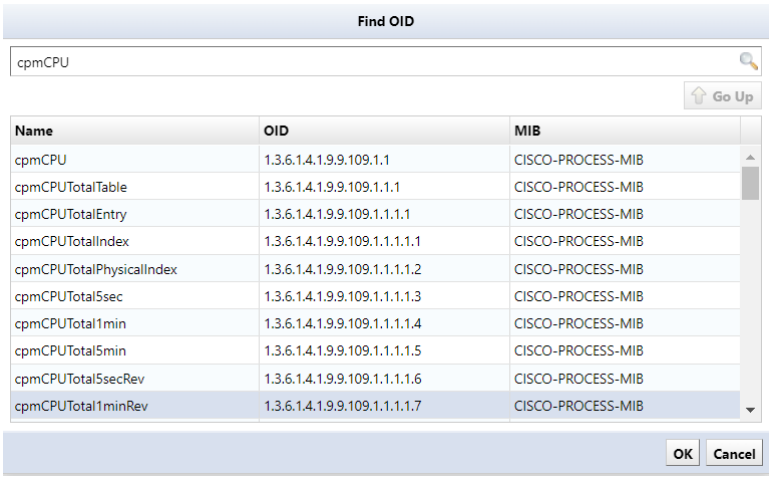
5. Use the [History] slider to specify a data retention period of 3, 6, or 12 months.



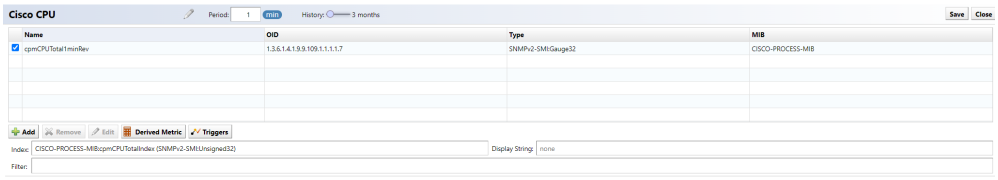
6. Click the  button and then click [MIB Library].



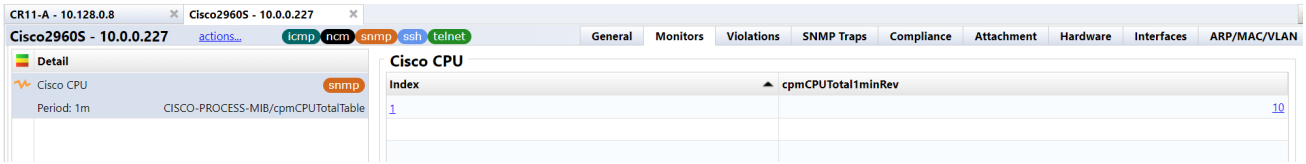
7. In the “Find OID” window, enter the MIB OID or name (“cpmCPU” in the example below) in the OID search field, select the MIB you want to add, and click [OK].



8. Click [Save] in the upper right-hand corner of the window.



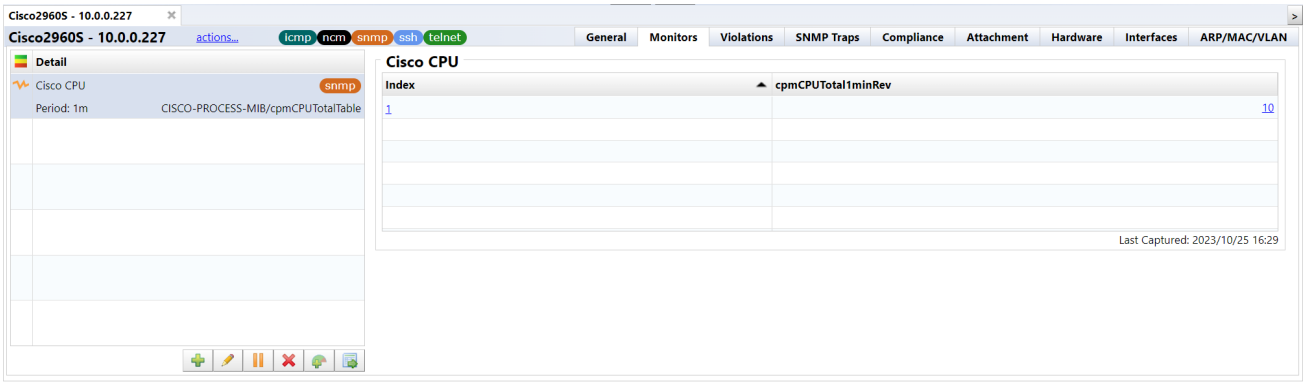
After saving, data collection will begin. If successfully acquired, the data will be displayed on the device details screen.



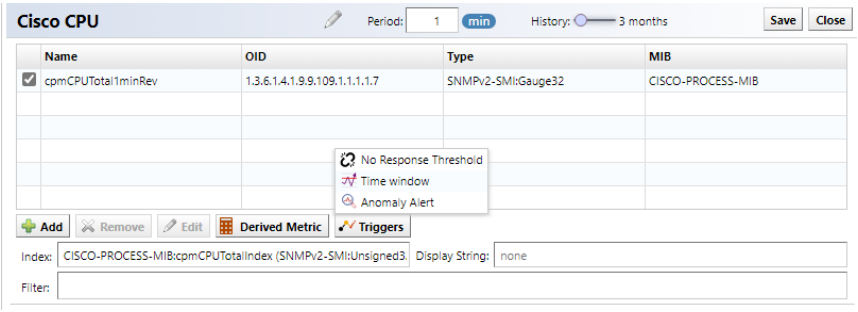
8.9.5.5 Set and monitor thresholds You can set thresholds for the data you retrieve and raise alerts when violations occur.

The following steps will create a threshold for the previously created SNMP monitor.

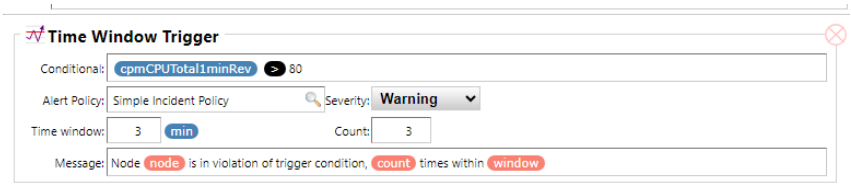
1. From the details screen, doubleclick the monitor for which you want to set thresholds or click [Edit].



2. Click [Trigger], then click [Time Window] in the pop up menu.



The image below is an example of setting an alert to be issued when the CPU usage rate exceeds 80%.



3. Enter the following items:

Setting	Explanation

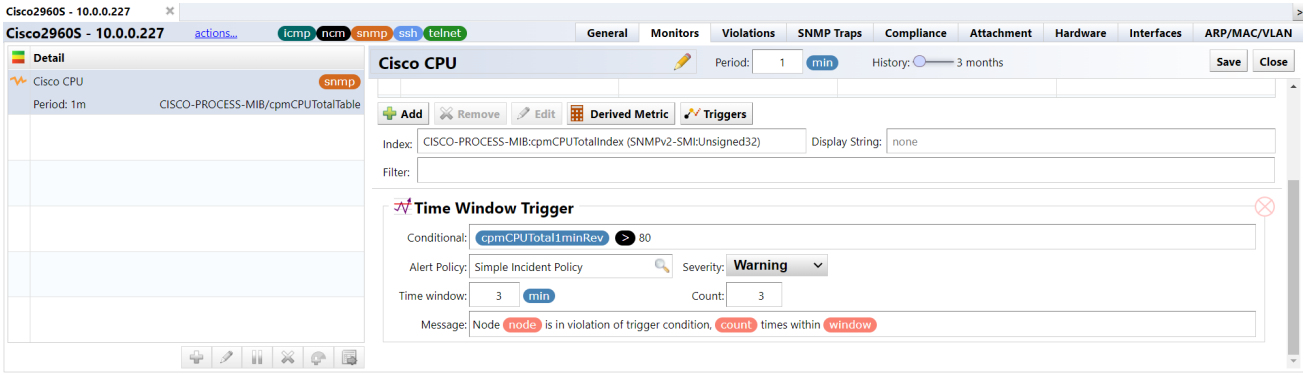
Conditional	You can specify conditions using the following items
	`is` (equal)
	`is not` (not equal)
	> (less than, the value on the right is smaller)
	< (greater than, the value on the right is greater)
	`contains`
	`does not contain`

Alert Policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning): “Emergency”, “Alert”, “Critical”, “Error”, “Warning”, “Notification”, “Information”, “Debug”
Time window	Set the period for executing the process. (Minimum value: 30 seconds) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (*Minimum value: 1)
Message	Set the message when executing the process.

The different alert severity icons are shown in the correspondence table below:

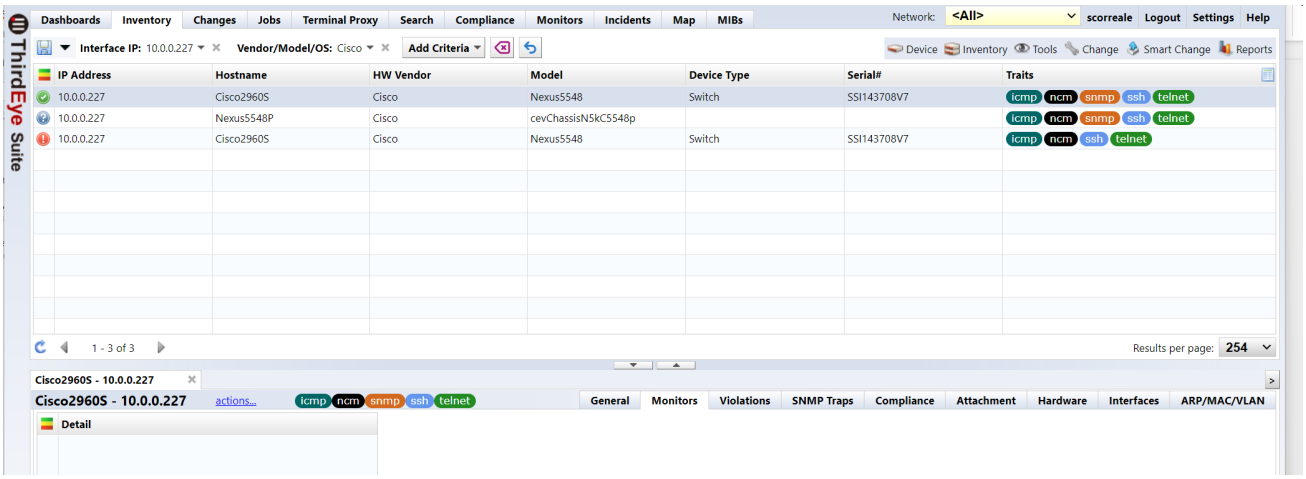
Security level	Status	Severity status icon
High	**emergency**	
	alert	
	critical	
Priority	**error**	
	warning	
	notification	
	information	
Low	**debug**	

4. Click [Save].



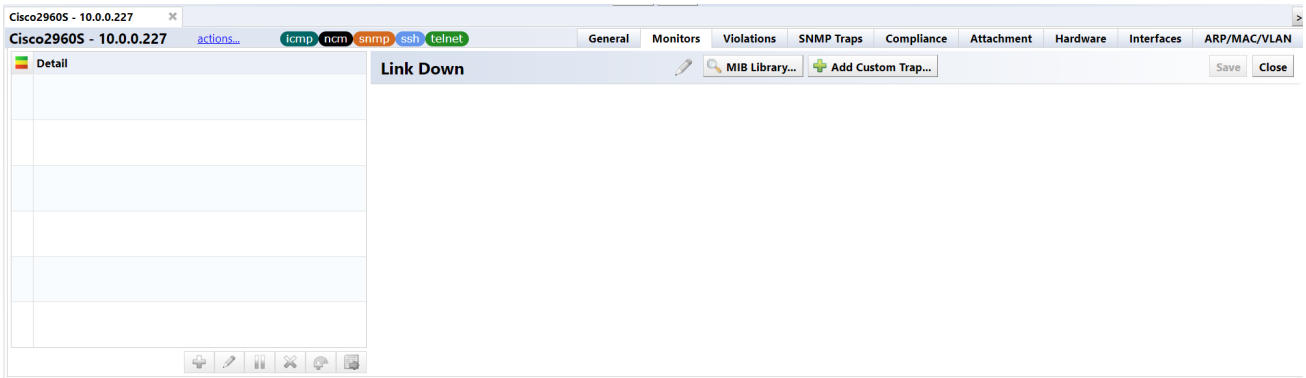
8.9.5.6 Monitor SNMP traps (OID specification) You can monitor specified SNMP traps and configure different actions for each. By setting the OID of an SNMP trap in advance, you can execute actions based on those settings when the corresponding SNMP trap is received. There is also a setting to monitor all SNMP traps.

1. From the list of monitored devices on the Inventory tab, doubleclick the device for which you want to set up a monitor.

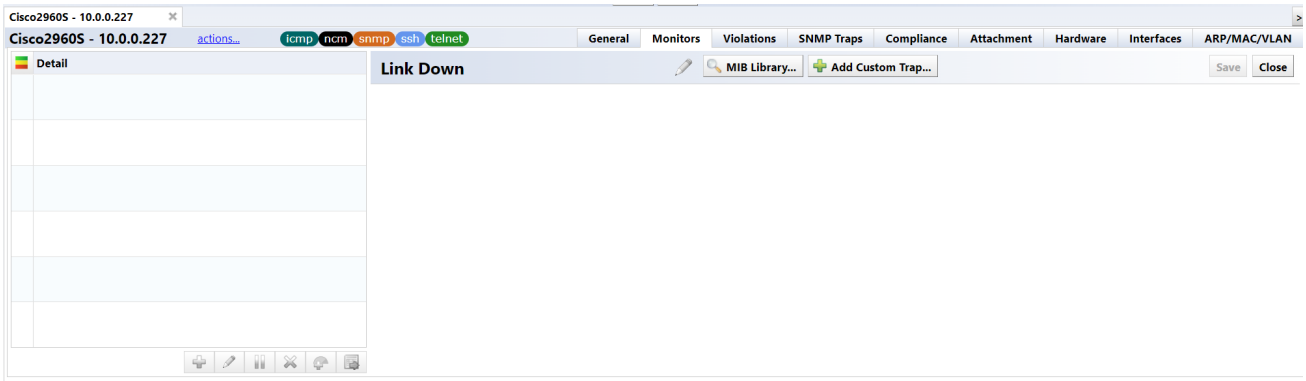


2. Click the button at the bottom left, and then click “SNMP Trap”.

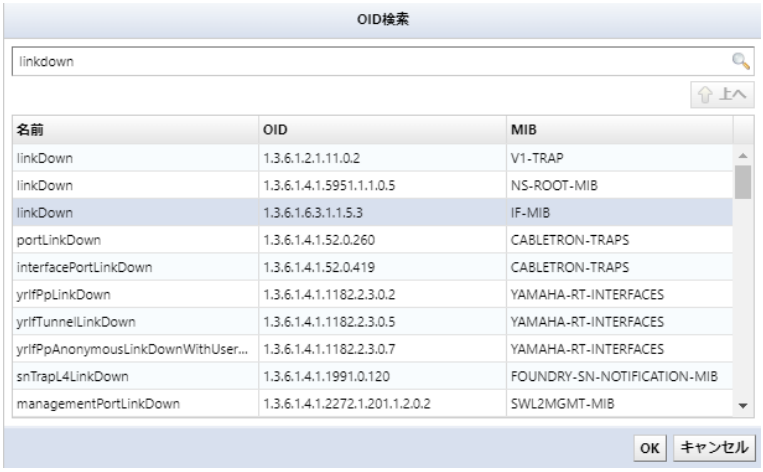
3. Enter any monitor name (“Link Down” in the example below).



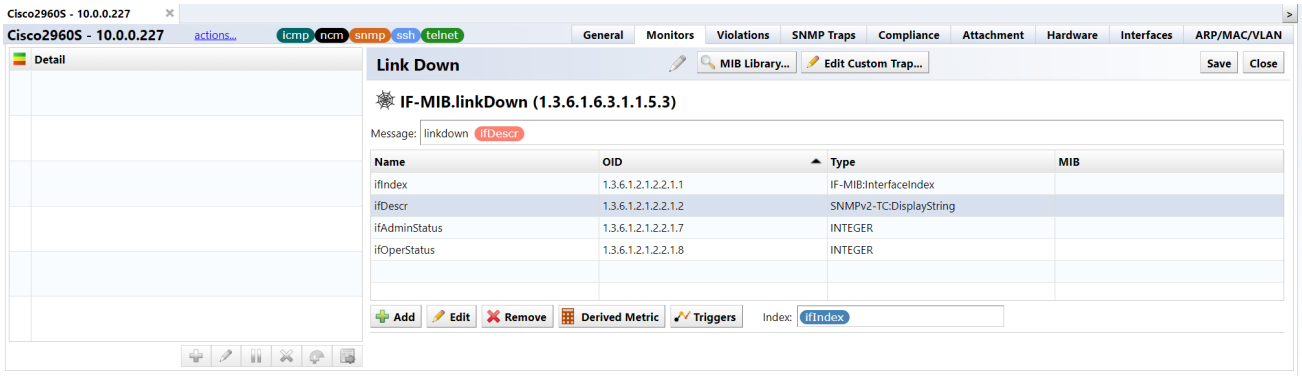
4. Click the [MIB Library] button near the top of the window.



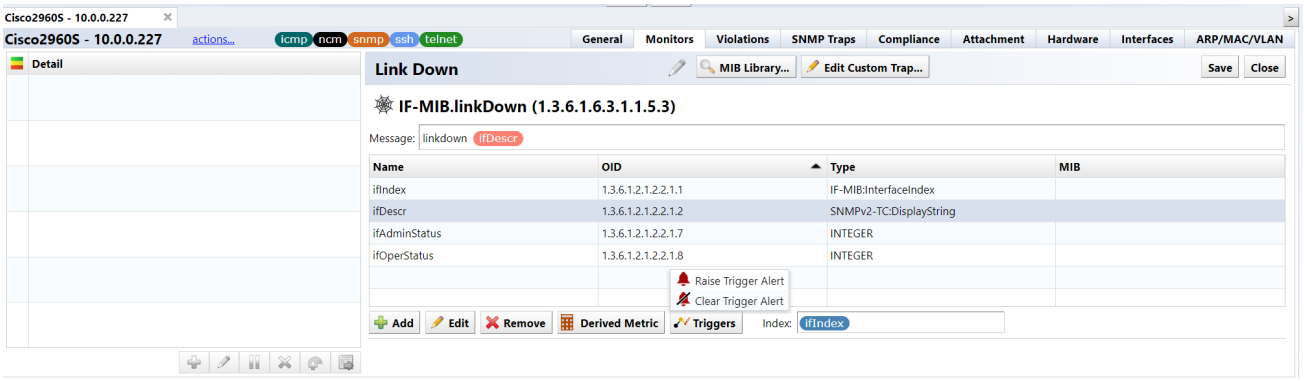
5. Enter the trap OID or name (“linkdown” in the example below) in the OID search, select the trap to monitor, and click [OK].



6. Enter a message for when a failure occurs.

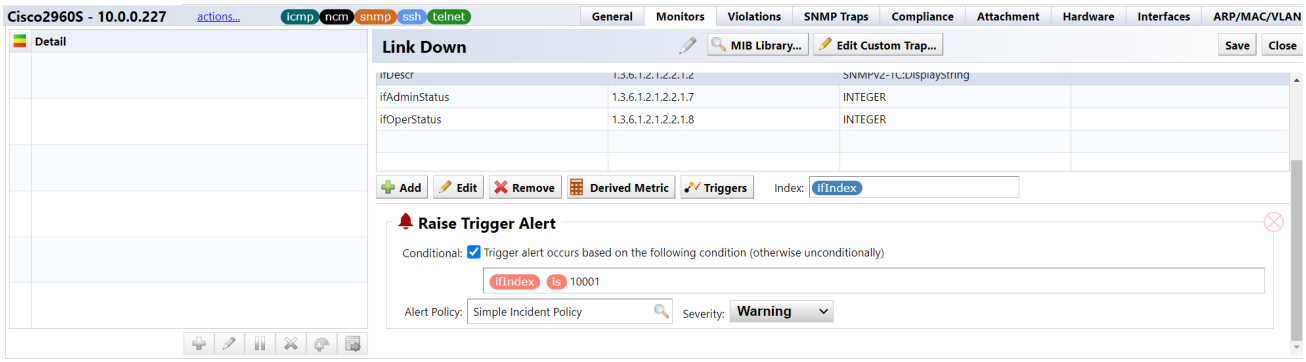


7. Click [Trigger] and then click [Raise Trigger Alert].



8. Select the “Conditional”, “Alert Policy”, and “Severity” settings.

(The image below is an example of setting an alert for the “Link Down” monitor.)



Alert Setting	Explanation

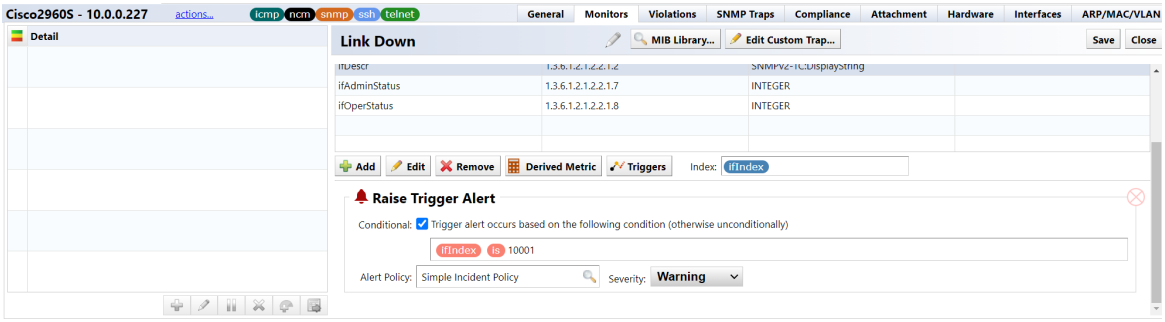
Conditional	If you check [Trigger alert occurs based on the following condition (otherwise unconditionally)], you can specify the conditions using the following items.
	`is` (equal)
	`is not` (not equal)
	> (less than, the value on the right is smaller)
	< (greater than, the value on the right is greater)
	`contains`
	`does not contain`

Alert Policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning): “Emergency”, “Alert”, “Critical”, “Error”, “Warning”, “Notification”, “Information”, “Debug” (*chart of the correspondence between severity and icon border/status icons is shown in the table below.)

The different alert severity icons are shown in the correspondence table below:

Security level	Status	Severity status icon
High	**emergency**	
	alert	
	critical	
Priority	**error**	
	warning	
	notification	
	information	
Low	**debug**	

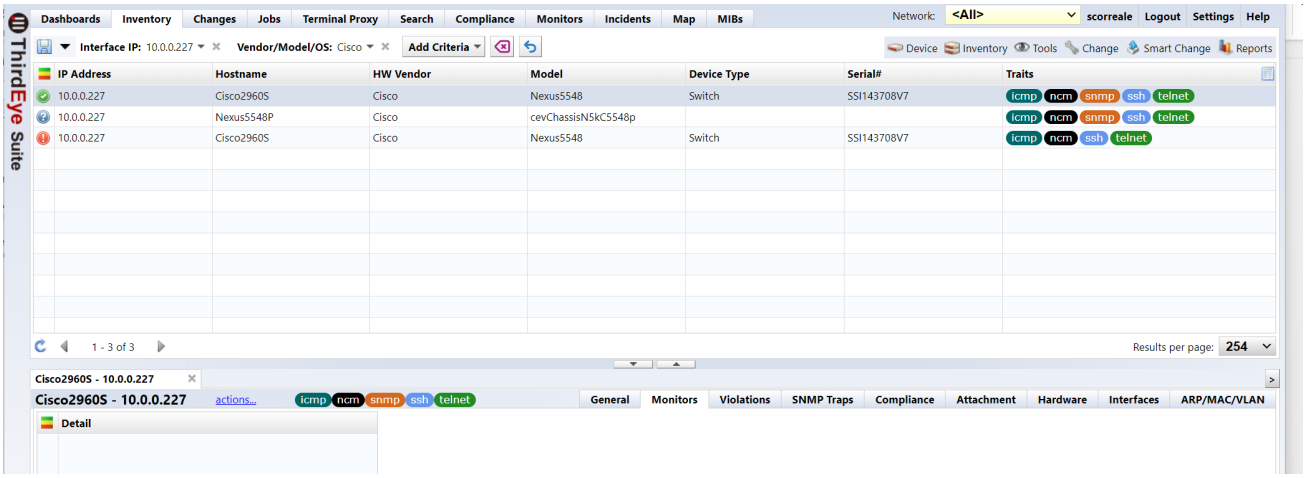
9. Click [Save].



8.9.5.7 Monitor SNMP traps (all) You can monitor all SNMP traps. By setting "SNMP Trap (All)" in advance, you can perform common actions based on those settings when receiving an SNMP trap. This is useful when you have not clearly decided which traps to monitor, or when you want to monitor all SNMP traps and register incidents.

> **Note**
>
> The "SNMP Trap (All)" and "SNMP Trap (Optional)" settings can be used together. If used together, the "SNMP Trap (optional)" setting takes precedence.

1. Click the Inventory tab, and doubleclick the device for which you want to set up a monitor.

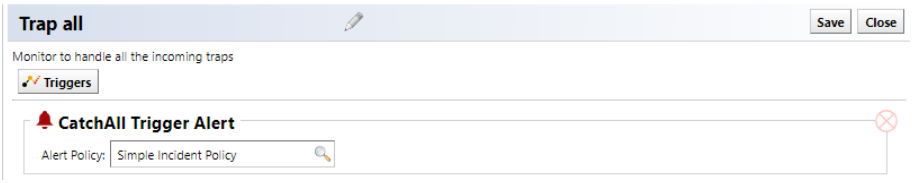


2. Click the button. at the bottom left, and then click "Catch All Trap (All)."

3. Enter any monitor name.

4. Click [Triggers], then click [Catch All Trigger Alert].

5. Specify the alert policy.

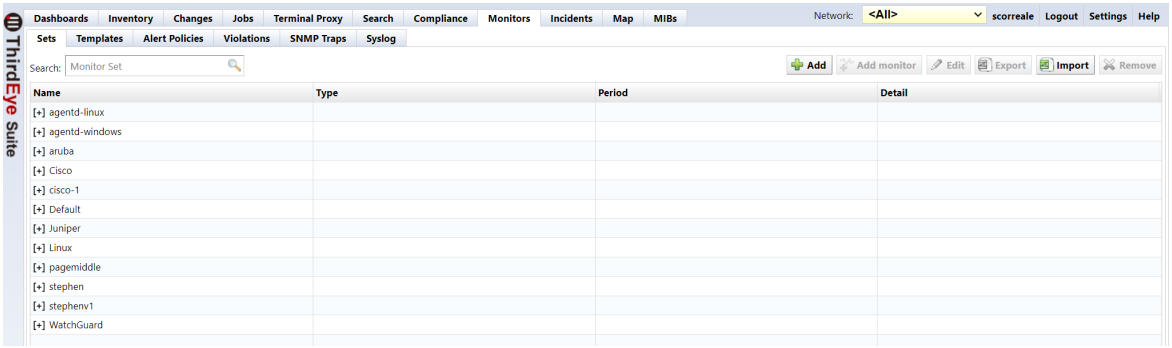


6. Click [Save].

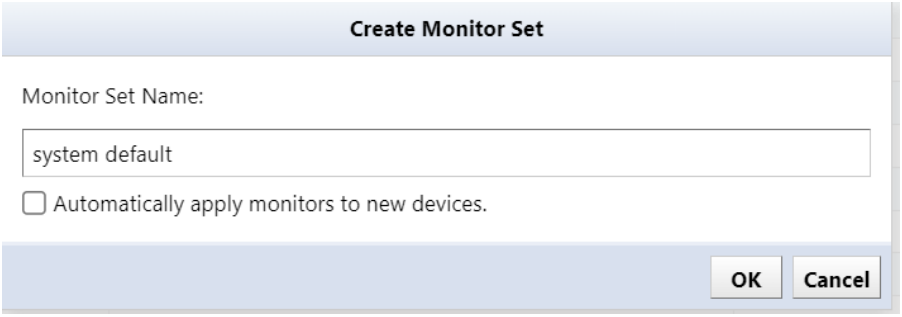
With the above settings, alerts will be issued for all SNMP traps received from monitored devices.

8.9.5.8 Configure monitoring settings for multiple devices using monitor sets ThirdEye's monitor settings include a function called "Monitor Set" that combines multiple monitors into one. Monitor Sllets allow you to apply configured monitors to many devices at once.

1. Click [Monitors] > [Set] > [Add].

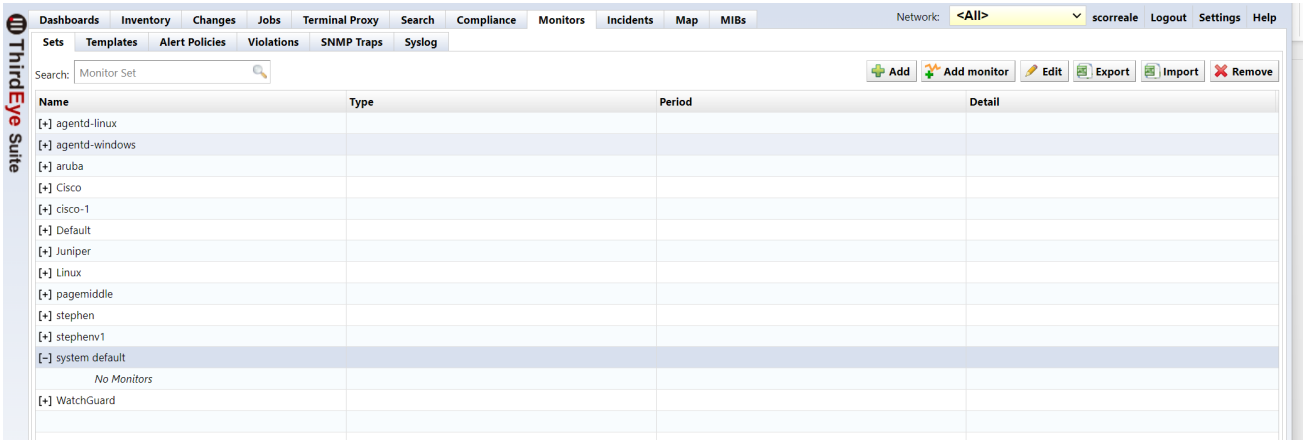


2. Enter the monitor set name and click [OK].



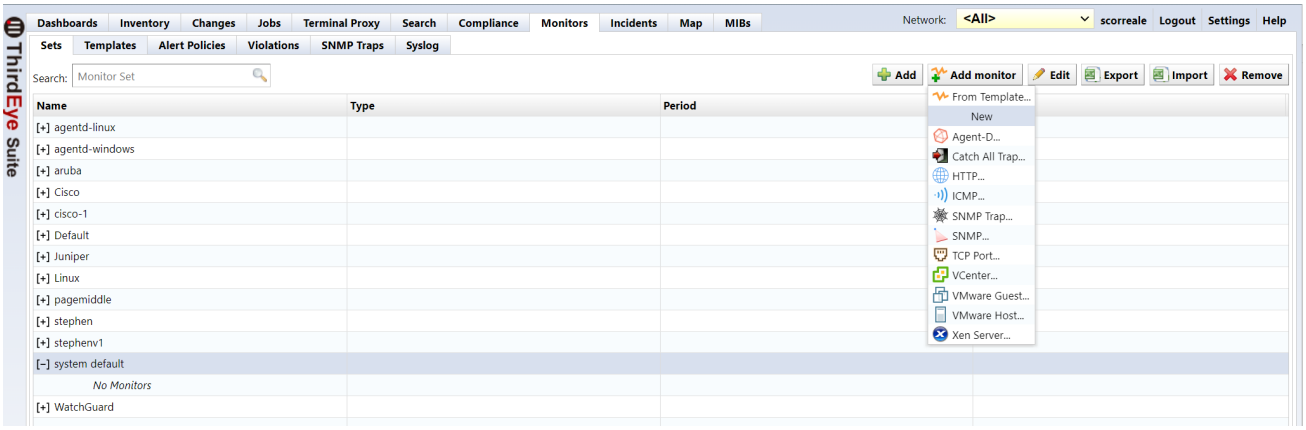
Setting	Explanation
Automatically apply monitor to new devices	When a device is added to a monitor included in this monitor set, it will be automatically assigned if it is able to communicate with the device.

3. Select the monitor set you created.



Monitors can be added with the [Add Monitor] button using the same method as when setting individual monitors.

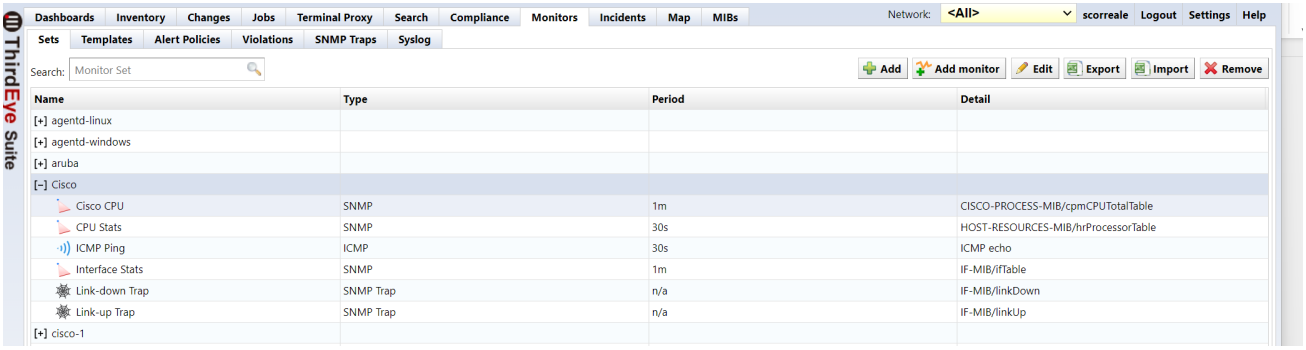
4. Click [Add Monitor] and set the monitoring items.



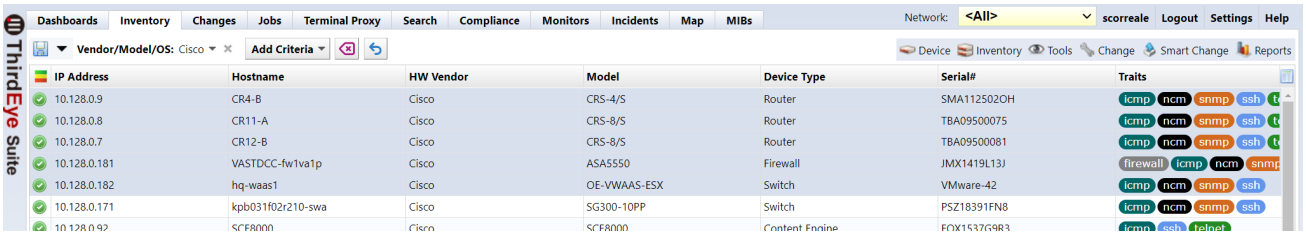
[Add Monitor] dropdown menu options:

Menu option	Explanation
Add from template	Add a monitor from the created monitor templates to Template.
Agent-D	Add a monitor for Agent-D.
HTTP	Add a monitor for http or https.
ICMP	Add monitoring by ICMP Ping.
SNMP	Add a monitor to specify the MIB object to be monitored from the MIB table.
SNMP traps (all)	Add a monitor to watch all SNMP traps.
SNMP trap (optional)	Adds a monitor to watch the specified SNMP trap.
TCP port	Adds a monitor for the specified TCP port.
VCenter	Add a monitor to obtain vCenter resource information.
VMware Guest	Add a monitor to obtain VMware guest resource information via vCenter.
VMware Host	Add a monitor to obtain VMware host resource information via vCenter.
Xen Server	Add a monitor to check memory usage of Citrix Xen Server.

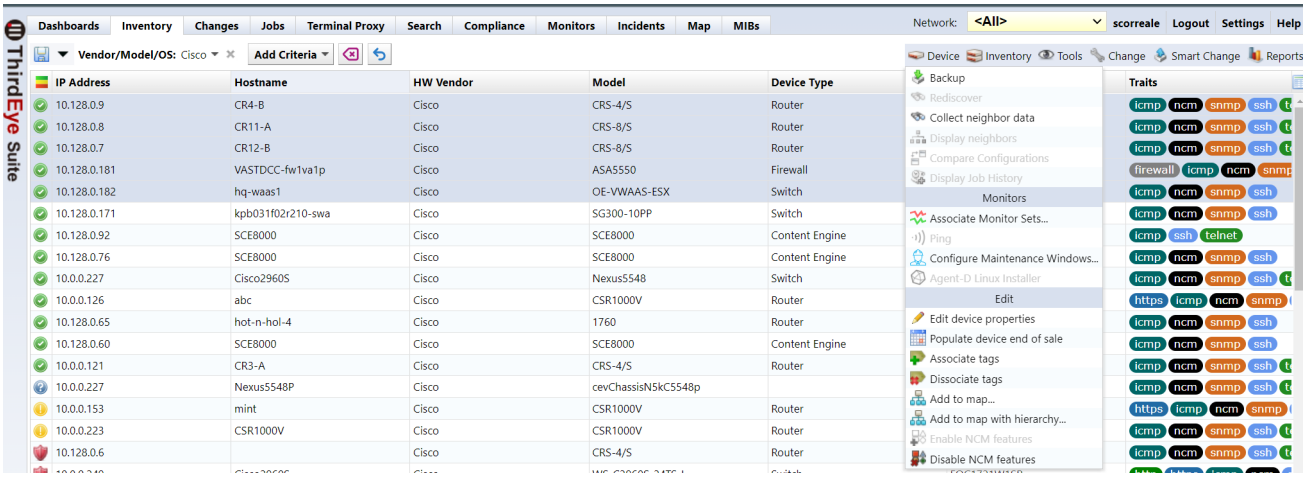
Example of screen after adding monitor (Cisco example from above)



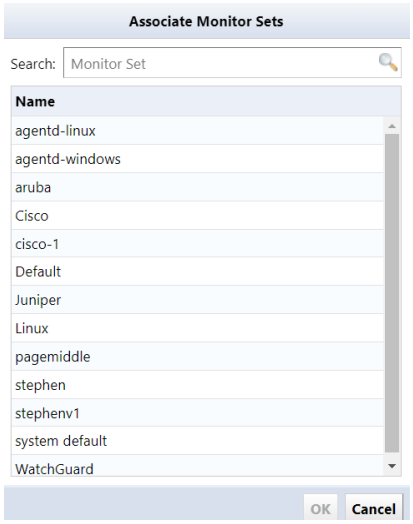
5. Select the [Devices] tab and select the device to which you want to assign the monitor set.



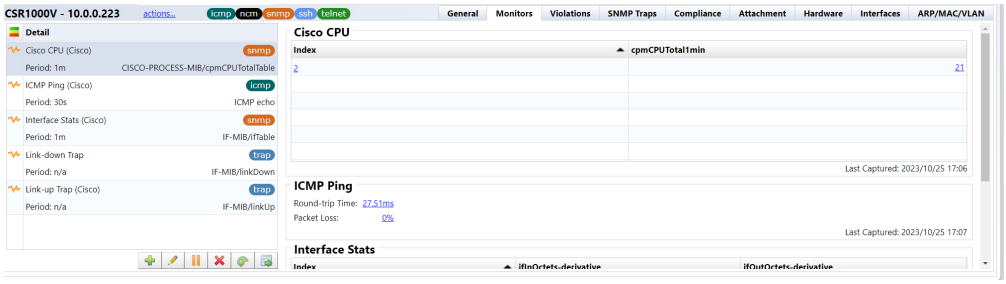
6. Click [Device] > [Monitor Set].



7. Select the monitor set you want to apply and click [OK].

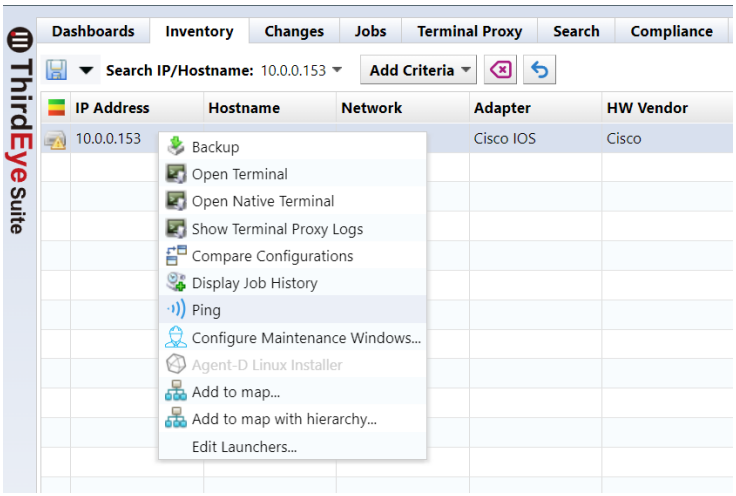


With the above operations, the application of the monitor set is completed. The [Details] column in nthe left panel displays a list of monitors being monitored. You can doubleclick the device to expand it and see if the monitor is reflected in the [Details] column.

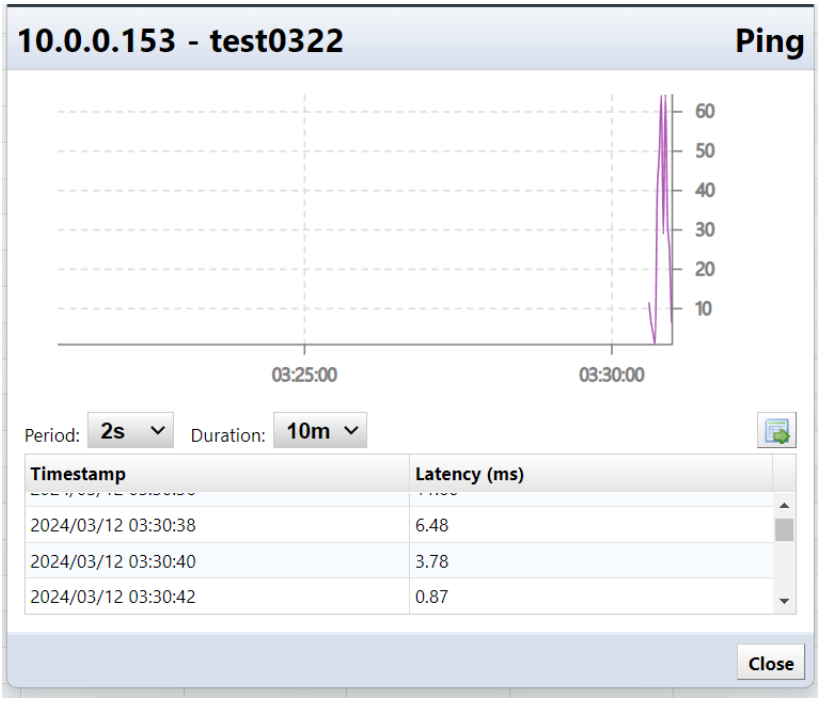


8.9.6 Ping in real time

You can ping a monitored device from the device list or map from the right-click menu. The transmission interval is 2 seconds at startup, but you can change it from the screen that appears after executing Ping.



When you click Ping, the following screen will be displayed and the ping result will be displayed.



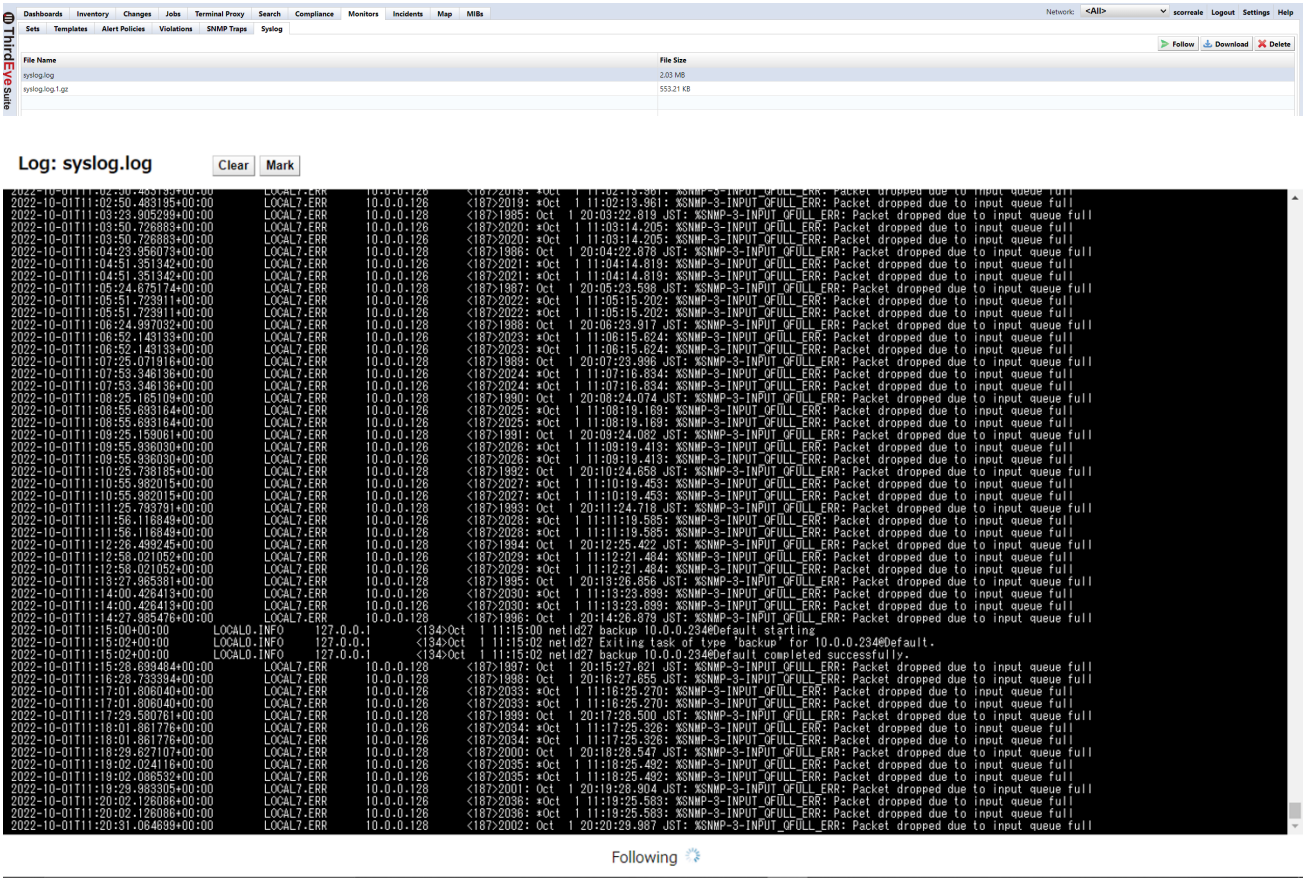
Click [Export] on the right side of the screen to export the ping results to a CSV file.

8.9.7 Check the received Syslog

From Rev. 20221026.0600, you can now check syslog on the [Syslog] tab.

Click the [Download] button to download the syslog file.

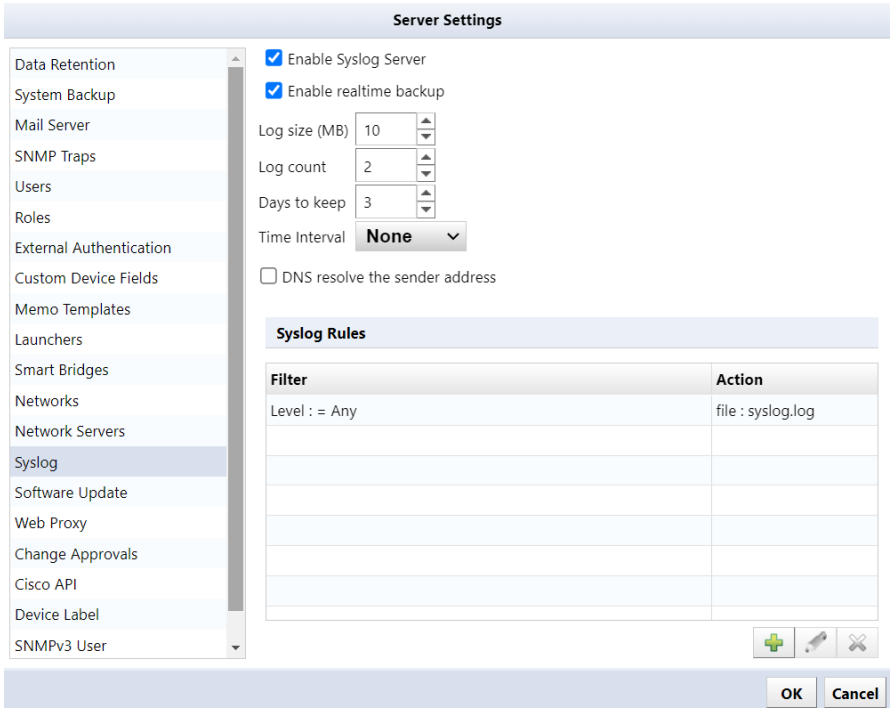
Click the [View] button to view the syslog on your browser.



8.9.8 Advanced Syslog file settings

8.9.8.1 Set Syslog file retention period/size Set the retention period for Syslog files.

1. Click Settings on the Global Menu.
2. Click [Syslog] and set each item.



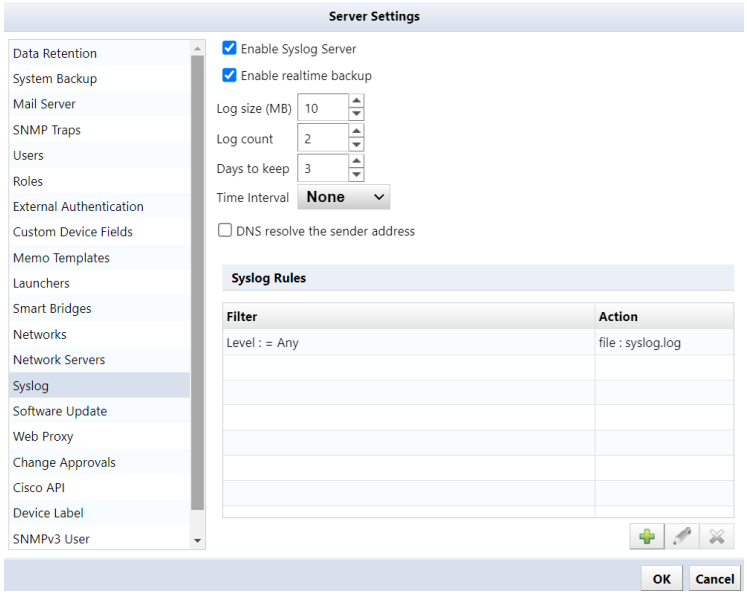
Items	Explanation
Enable Syslog server	Set enable (start)/disable (stop) the Syslog server.
Enable realtime backup	Enable/disable realtime backup while leaving the syslog server on.
Log size (MB)	Specify the size of the syslog file.
Log count	Specifies the number of rotated files to keep.
Days to keep	Specifies the number of days to retain rotated files.
Time interval	Rotates syslog files at specified time intervals.
DNS resolve the sender address	Performs a reverse DNS lookup for the Syslog source IP address and records the host name in the Syslog file.

3. Click [OK].

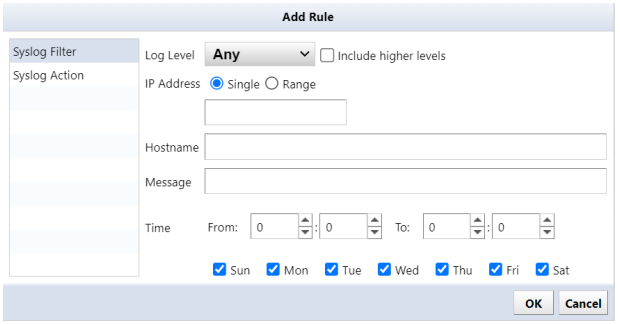
8.9.8.2 Set up Syslog rules According to set conditions, you can sort Syslog output destinations, forward Syslogs to other hosts, and exclude unnecessary messages.

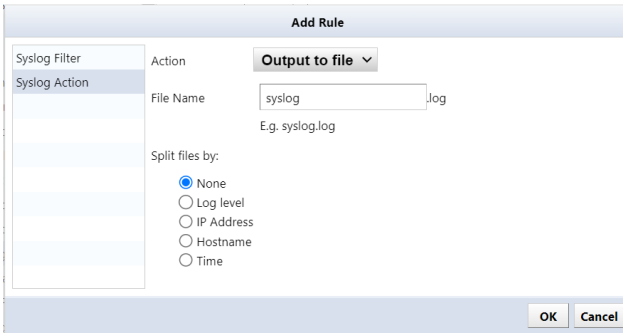
To add a Syslog rule:

1. Click Settings on the Global Menu.
2. Click Syslog, then the button under [Syslog rules].



3. In the left sidepanel, click on [Syslog Filter] and [Syslog Action] to configure settings.





Syslog filter Items

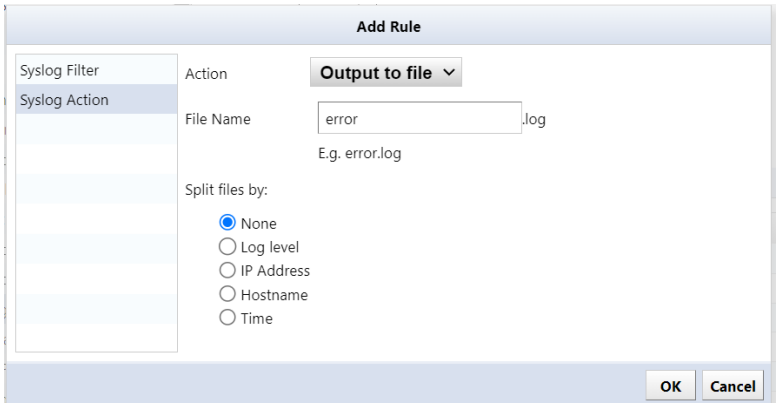
Filter	Explanation
Log level	Filter by Syslog level. If you enable the “Include higher levels” option, filtering will be performed at the selected level and above.
IP Address	Filter by IP address. [Single] filters by a single IP address [Range] filters by IP range If not entered, filtering by IP address will not be performed.
Hostname	Filter by hostname. If not entered, filtering by host name will not be performed.
Message	Filters syslogs containing the specified string. In the “Message” field, you can filter by partial match. Uppercase/lowercase letters are case sensitive. Filtering based on regular expressions (Regex) is not supported. If not entered, message filtering will not be performed.
Time	Filter by time. Syslogs received within the time specified by the start time and end time are subject to filtering.
Day of week	Filter by day of the week.

Syslog action

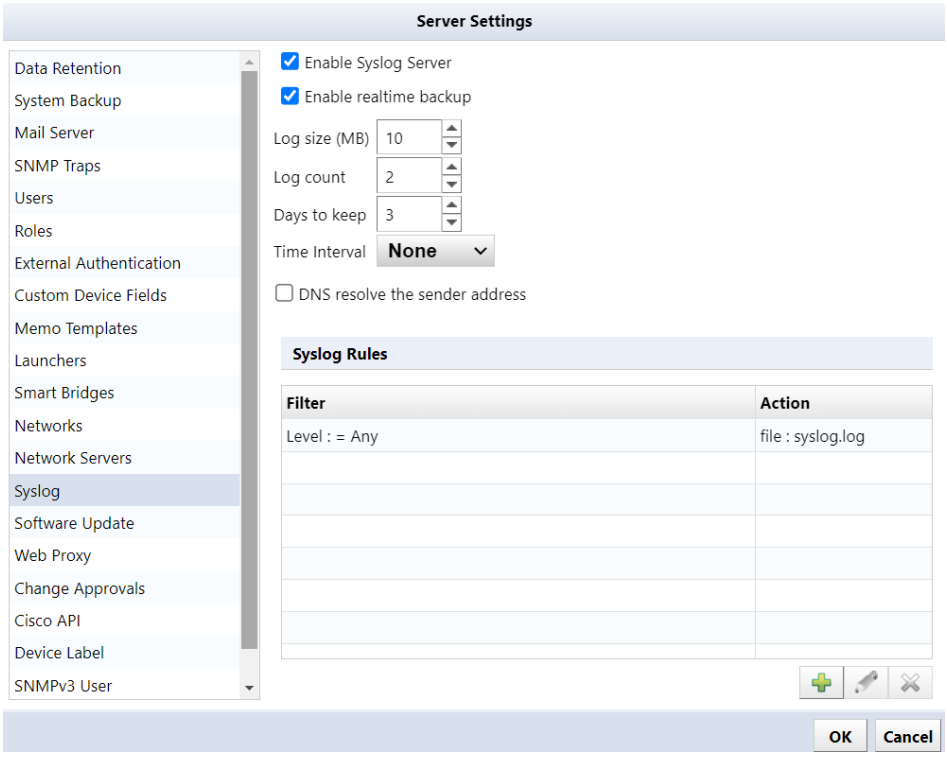
Action	Item	Explanation
Output to file	File name	Specify the Syslog file name to output.
	Split files by	Divide the output Syslog file into specified units. `None`: Do not split `Log Level`: Divide by log level `IP address`: Divide by IP address or octet (1st, 2nd, 3rd) `Hostname`: Split by host name `Time`: Divide into selected time units
Forward	Transfer format	Select the transfer format from Syslog and SNMP.
	Target IP/Host name	Specify the forwarding destination.
	Port	Set the forwarding destination port number.

Action	Item	Explanation
	Protocol	Select the transfer protocol from UDP or TCP. *Displayed when the transfer format is Syslog*
	Spoofed source IP	*Displayed when the transfer format is Syslog*
	Community	Specify the SNMP trap community. *Displayed when the transfer format is SNMP*
Discard	—	Excludes the Syslog specified by the Syslog filter and will no longer log it to the Syslog file.

4. After setting, click [OK].



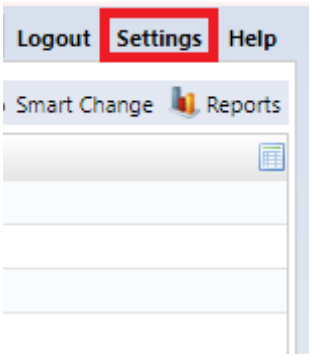
5. Click [OK] on the server settings screen.



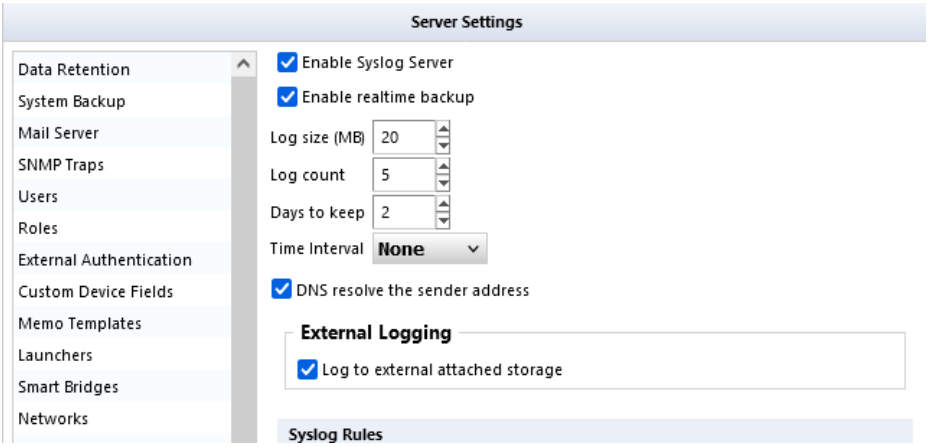
8.9.8.3 Save syslog files to external storage Normally, received Syslogs are saved to a local syslog.log file, but by linking with an NFS/SMB server, they can be saved to external storage.

You must restart the ThirdEye appliance for this setting to take effect.

1. Click Settings on the Global Menu.



2. Click [Syslog] and check “Logging to external storage”.



This “External logging” option is displayed when linked with an NFS/SMB server.

3. click [OK].
4. Click [OK] on the reboot confirmation screen.

ThirdEye must be restarted for the settings to take effect. Click OK and ThirdEye will automatically restart.

> **Note**
>
> Changing the `syslog.log` file location from local to external storage copies the local file to external storage. However, changing the `syslog.log` file location from external to local storage does not copy the files to external storage locally. This is not supported for security reasons.

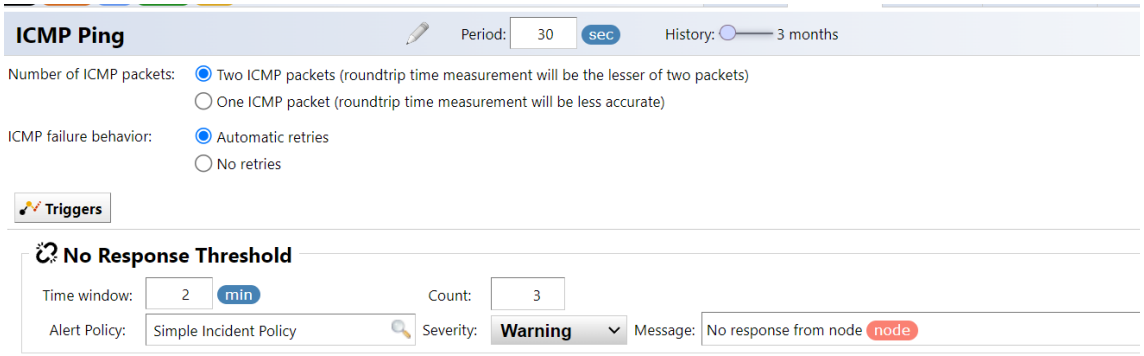
8.9.9 ICMP polling

ThirdEye's ICMP monitor consists of the following settings:

- Interval
- ICMP Send Count
- Retry

ICMP timeout is always 2 seconds and cannot be changed.

A description of each item is shown below:



Item	Explanation
interval	ICMP monitor polling interval
ICMP transmission count	Select the number of ICMP packet transmissions from the following. **sent twice** For "roundTripTime"* (response time) that can be monitored with the ICMP monitor, the smaller value of the two times is saved. **send once**
retry	Separately from the number of ICMP transmissions, select whether to perform retries. **automatic retry** If there is no response to the first poll and automatic retry, automatic retry will not be performed in the second and subsequent polls. **none**

8.10 Operation image 1

Setting details

Item	Setting value
interval	30 seconds
ICMP transmission count	Send once
retry	automatic retry

Explanation

If you set the interval to 30 seconds, a ping (in this case 1 time) and 5 retries will be executed within 30 seconds. The retry interval is dynamically averaged based on the monitor's polling interval, here 5.2 seconds.

8.11 Operation image 2

Setting details

Item	Setting value
interval	5 minutes (300 seconds)
ICMP transmission count	sent twice
retry	automatic retry

Explanation

If the ICMP transmission count is "send 2 times", pings will be sent 2 times and then retries will be performed 5 times.

The retry interval is dynamically averaged based on the monitor's polling interval, but is up to 25 seconds, so a long interval will perform as shown above.

Time required until alert occurs:

Theoretical value: 30 seconds (2+5.2*5+2) if the interval is set to 30 seconds.

Additionally, ThirdEye has "response confirmation" and "period" as triggers for generating alerts.

In the response confirmation trigger, you can use "count" and "period" to generate an alert if "there is no response N times within a certain period of time."

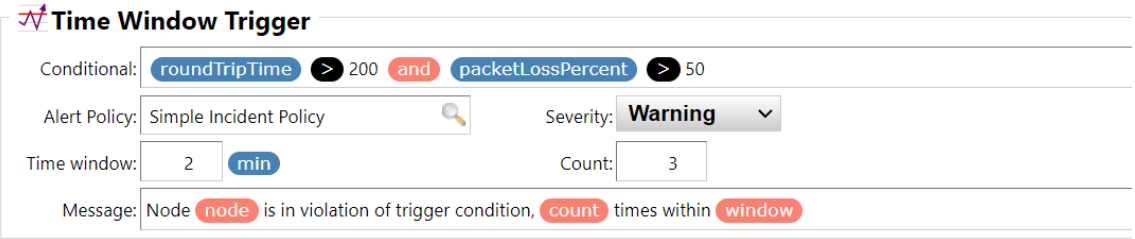
In the below case, an alert will be generated if there is no response twice within 3 minutes.

Sample image

In period triggers, you can use “conditions” in addition to “count” and “period” of response confirmation triggers. The “condition” can be the round trip time (RTT) of the ping response packet and the packet loss percentage.

By using these conditions together, it is possible to perform monitoring. For example, even if a ping response is returned from the monitoring target, the RTT does not reach the level expected by the user, so it is judged as NG and an alert is generated.

Sample image



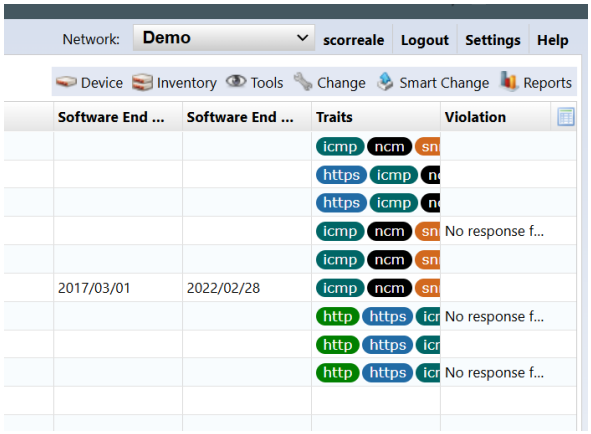
8.11.1 Monitoring using Agent-D

Monitoring using an SNMP agent requires installing the agent on the monitored device, and if there are many targets to be monitored, installation alone can take a lot of time.

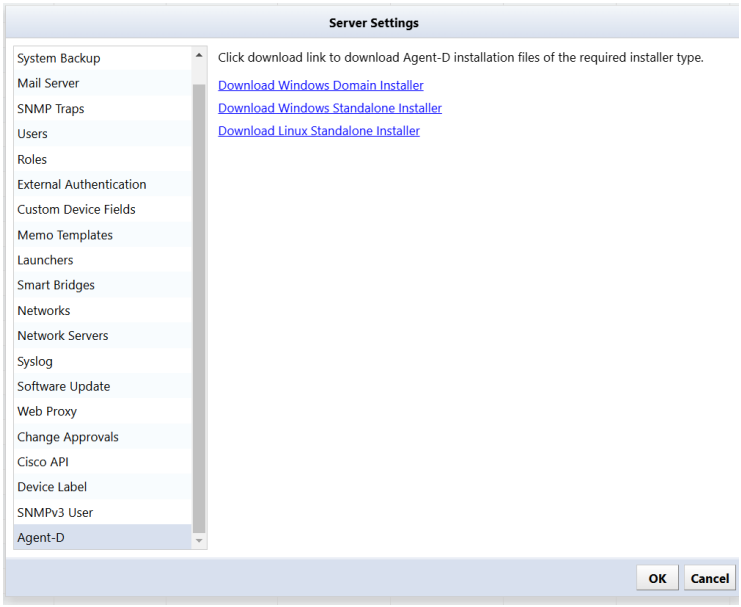
Agent-D is an SNMP agent for server monitoring. By installing Agent-D on a Windows or Linux-based OS, you can monitor the server's CPU, memory, logs, etc. It allows you to bulk distribute (install) on monitored devices, and reduce installation time.

8.11.1.1 Install on Linux Download the installer from ThirdEye and install it on any Linux. Supported OS are RedHat Linux 7/8, CentOS 7/8, and Ubuntu.

1. Click Settings on the Global Menu.



2. Click [Agent-D] and the ledt sidepanel, then click [Download Linux Standalone Installer].



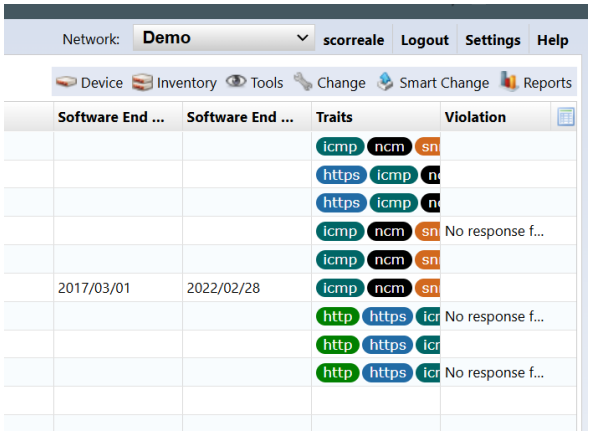
3. Copy the downloaded file to the installation destination Linux server.
4. Unzip the downloaded file using the unzip command.

5. Run `install.sh`.

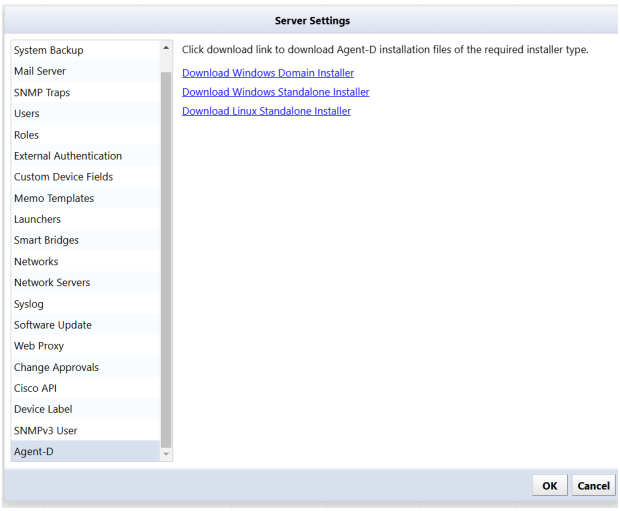
6. Enter ThirdEye's IP address and press the [Enter] key.

8.11.1.2 Install on Windows Download the installer from ThirdEye and install it on any Windows server. Windows OS Server versions 2016, 2019, and 2022 are supported.

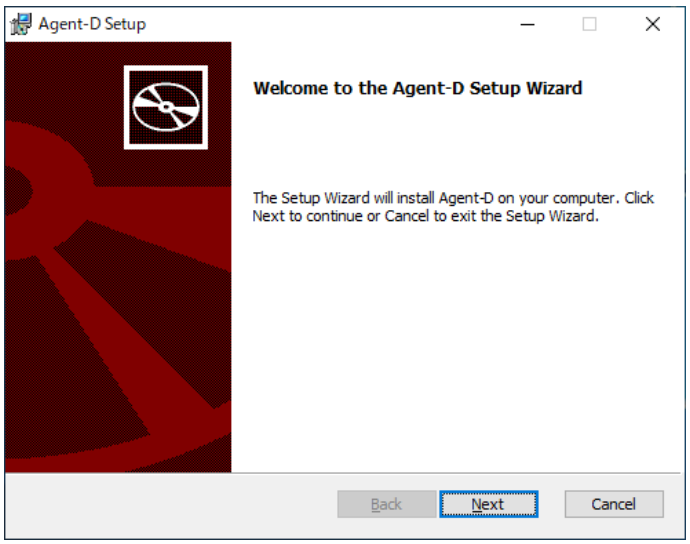
1. Click Settings on the Global Menu.



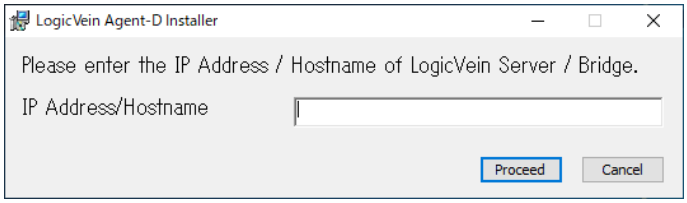
2. Click [Agent-D] in the left sidebar, then click [Download Windows Standalone Installer].



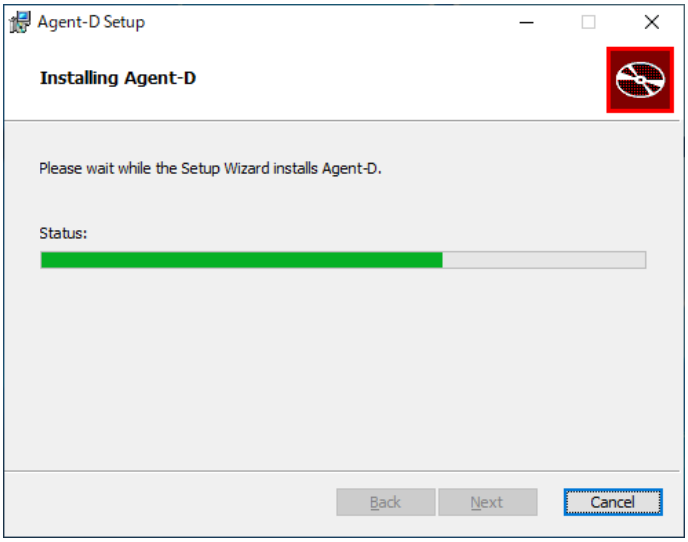
3. Copy the downloaded file to the Windows server where you will install it.
4. Unzip the downloaded file and doubleclick the file "`agent-d-standalone.msi`" to run it.
5. Click [Next].



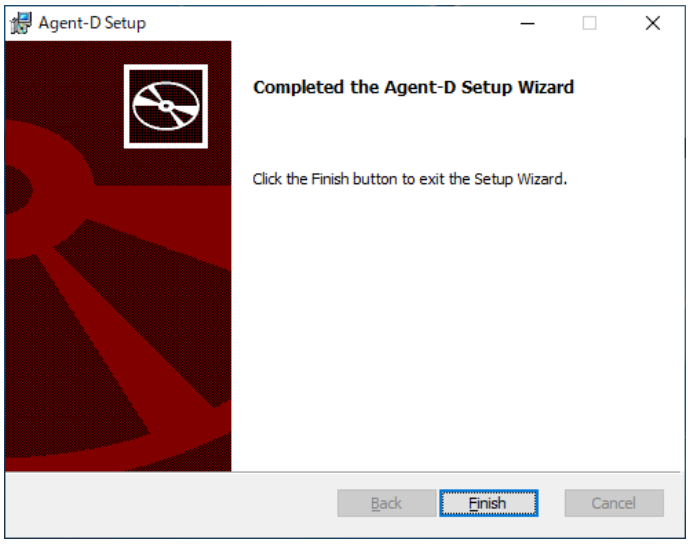
6. Enter ThirdEye's IP address or hostname and click [Proceed].



Installation will begin.



7. Click [Finish].



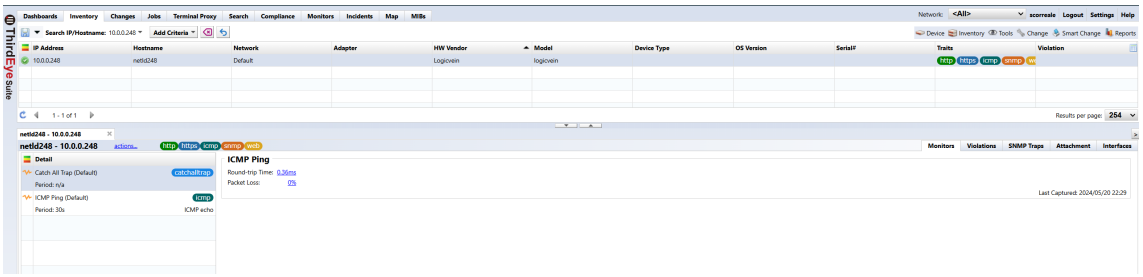
8.11.1.3 Windows service monitoring Use Agent-D to obtain information about Windows services on the installed Windows server. By setting thresholds for service status, you can issue an alert when the threshold is exceeded.

The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

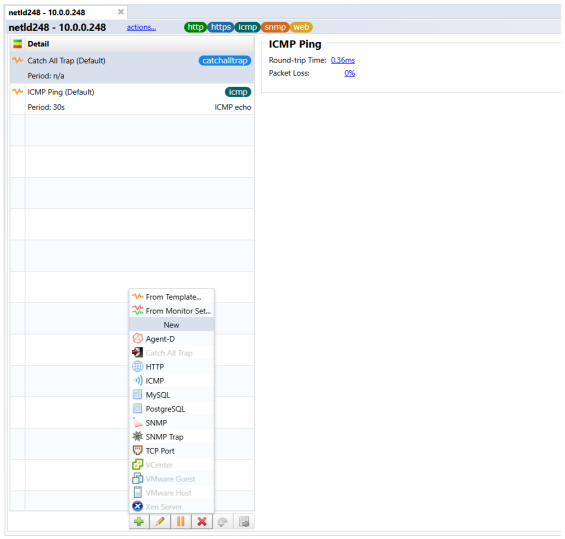
- Windows Service Status

The [Agent-D] > [Agent-D] > [Windows Services] plug-in can be set up as as a monitor for a Windows server device:

1. Doubleclick the device for which you want to configure a monitor to open the device details.



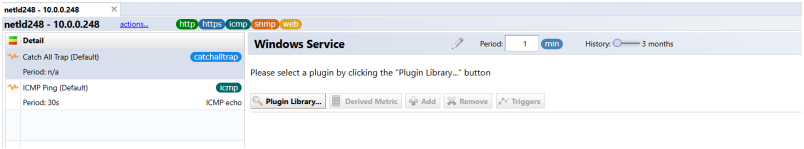
2. Click the button, then click [Agent-D].



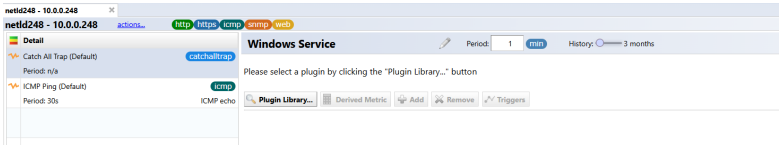
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

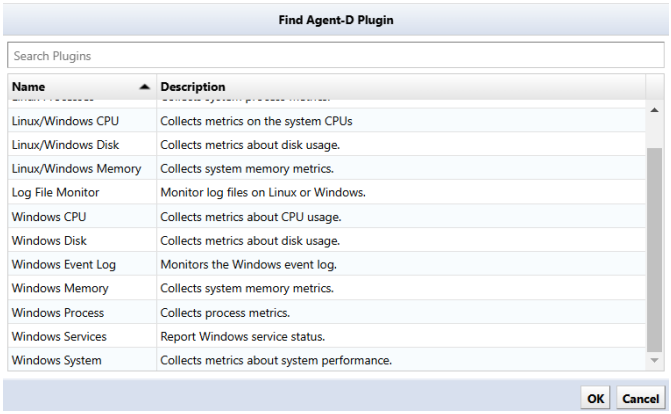
The [History] slider specifies a data retention period of 3, 6, or 12 months.



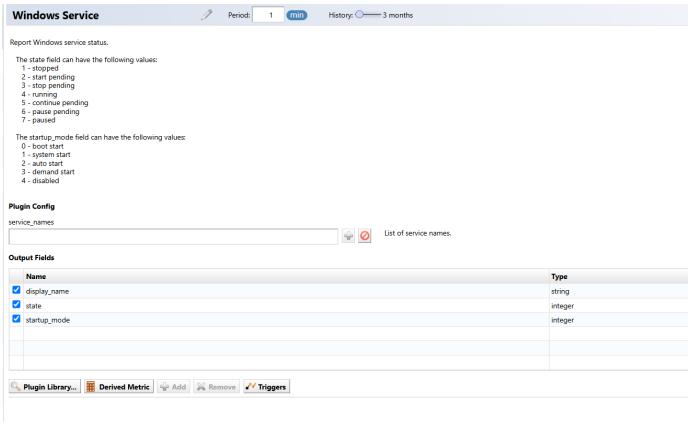
4. Click [Plugin Library…].



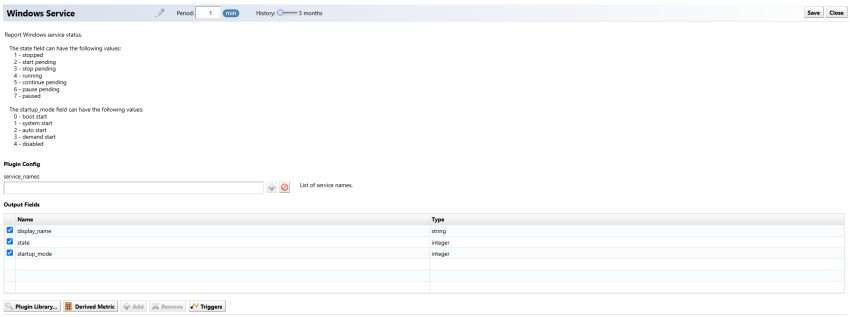
5. Select [Windows Services] and click [OK].



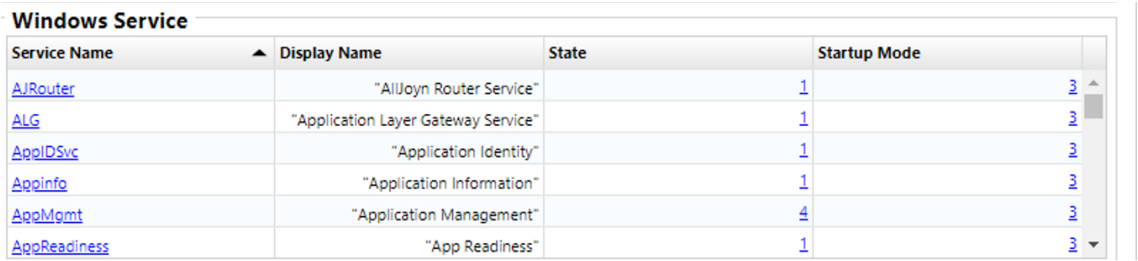
6. Add the service name to be monitored by entering it in the [service_names] field Service name is an exact match. (uppercase and lowercase letters are not sensitive)



6. Check the items you want to obtain in [Output Fields] and click [Save].



Now, Agent-D will send the service information and you can check it in the device details.



Windows Service

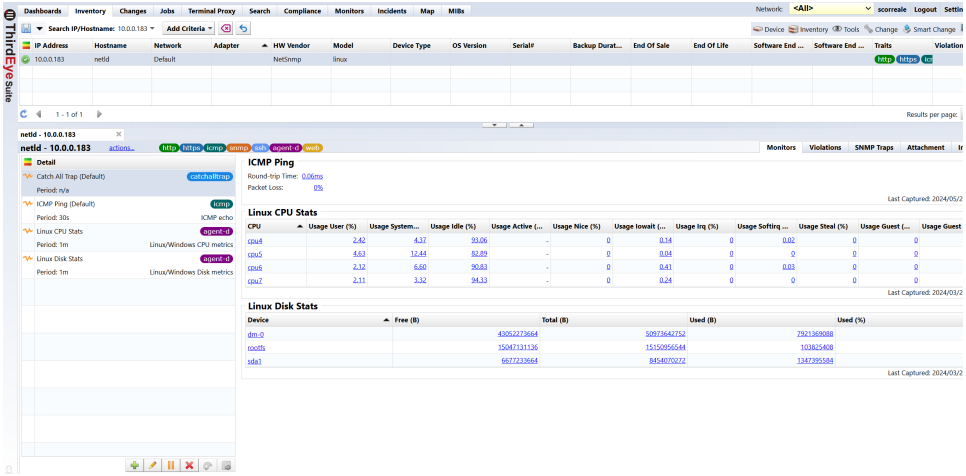
Service Name	Display Name	State	Startup Mode
AJRouter	"AllJoyn Router Service"	1	3
ALG	"Application Layer Gateway Service"	1	3
AppIDSvc	"Application Identity"	1	3
Appinfo	"Application Information"	1	3
AppMgmt	"Application Management"	4	3
AppReadiness	"App Readiness"	1	3

8.11.1.4 Windows event log monitoring Use Agent-D to obtain Windows event log information for the installed Windows server. An alert can be issued when an event log containing a specific string is detected.

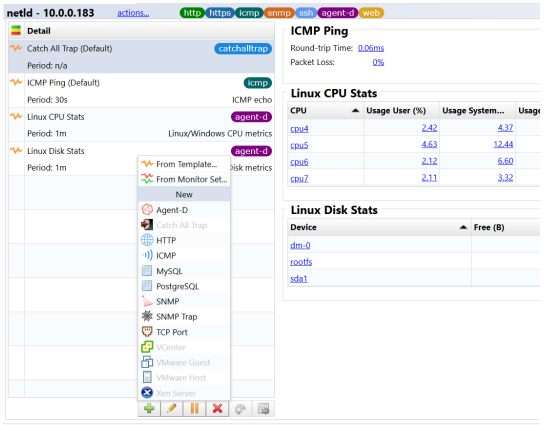
The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

- Windows Event Log Monitor

1. Doubleclick the device for which you want to configure a monitor to open the device details.



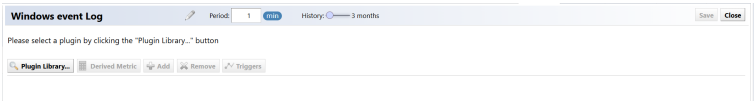
2. Click the button, then click [Agent-D].



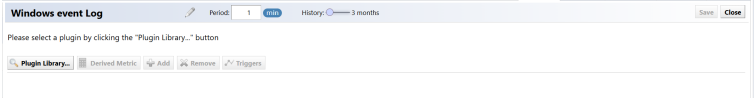
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

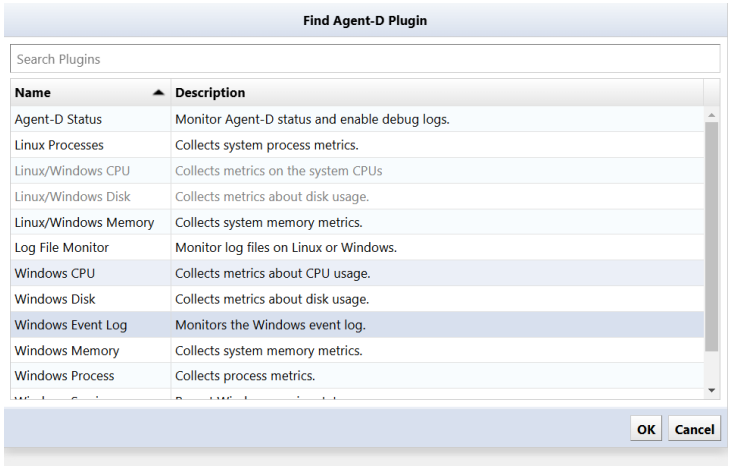
The [History] slider specifies a data retention period of 3, 6, or 12 months.



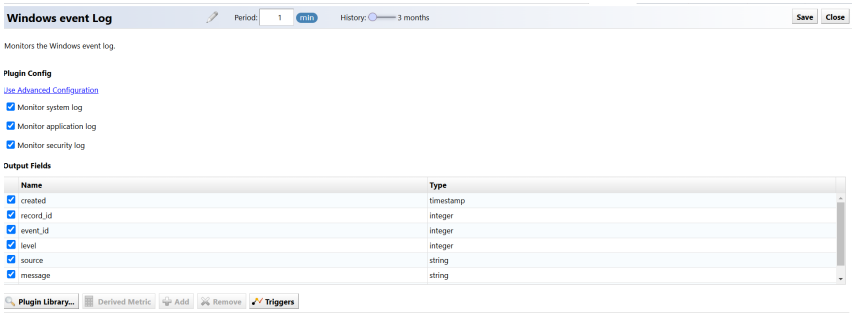
4. Click [Plugin Library …].



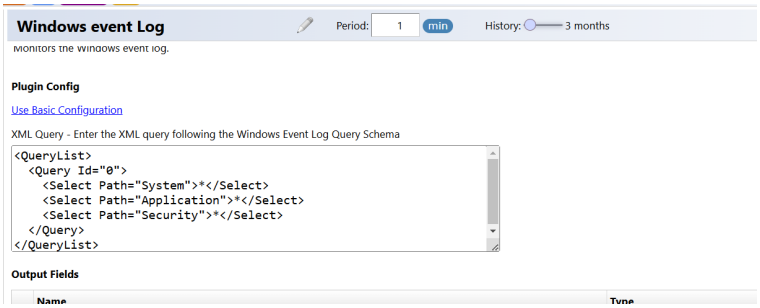
5. Click Windows Eventlog, then click [OK].



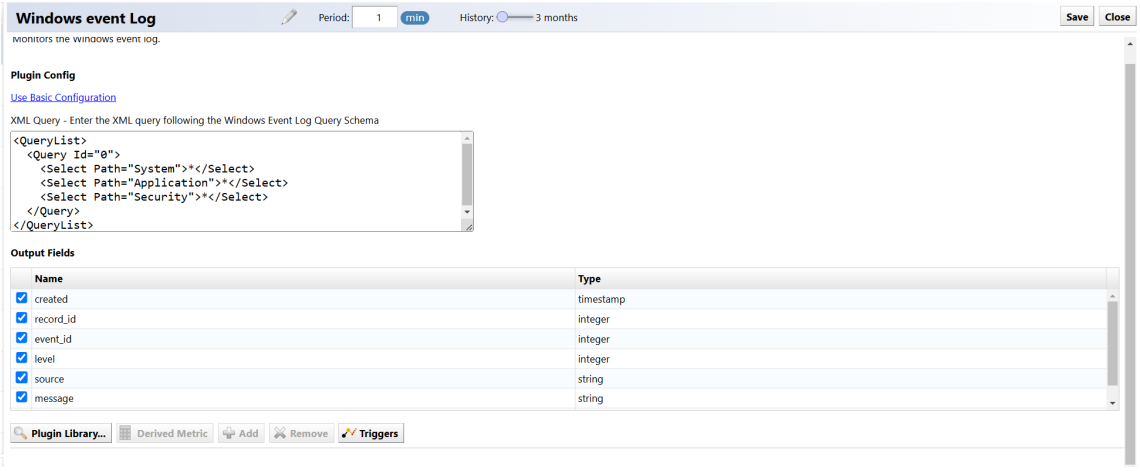
6. Check the event logs you want to monitor.



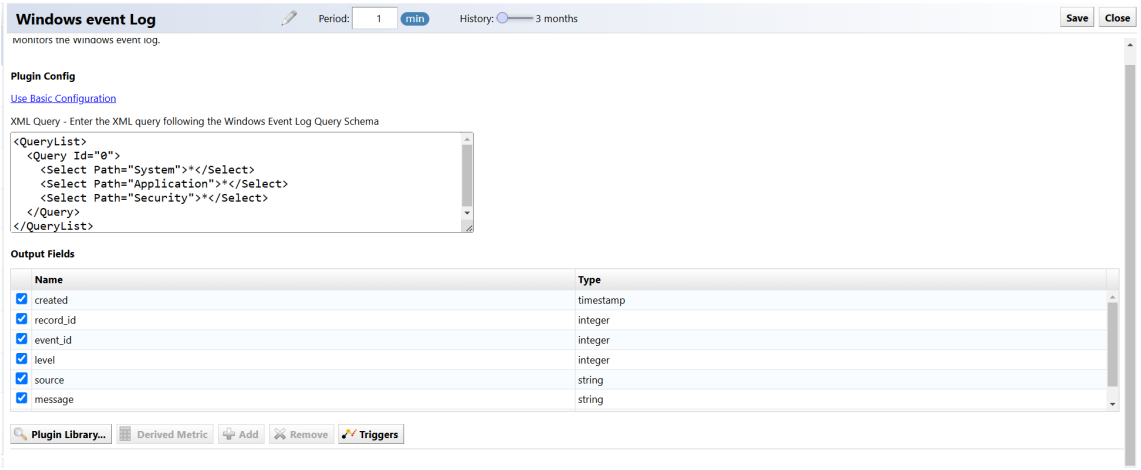
7. Click [Use advanced settings] to specify in XML format.



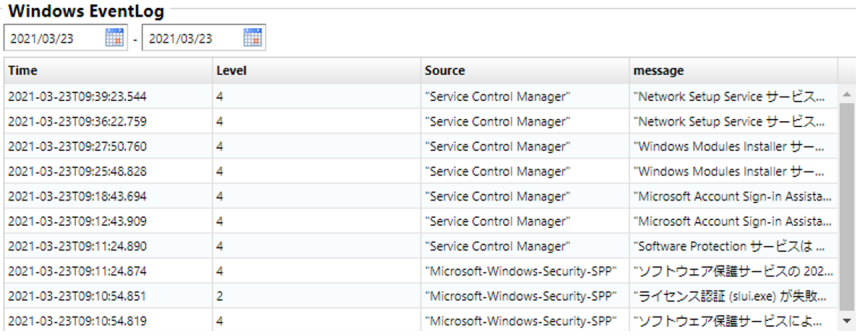
8. Check the items to be retrieved in [Output Fields].



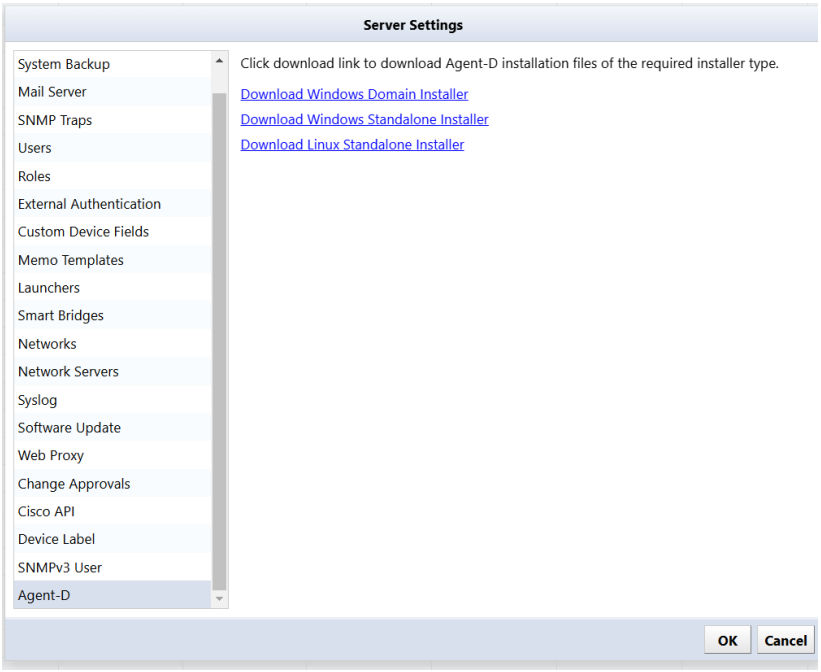
9. Click [Save].



Now, the event log information will be sent from Agent-D and can be checked in the device details.



8.11.1.4.1 Distribute and install Agent-D using Group Policy on domain controllers You can install Agent-D on multiple servers in bulk using new or existing Active Directory group policies. You can download the MSI file by clicking Settings > [Agent-D] > [Download Windows Domain Installer] in the Global Menu.



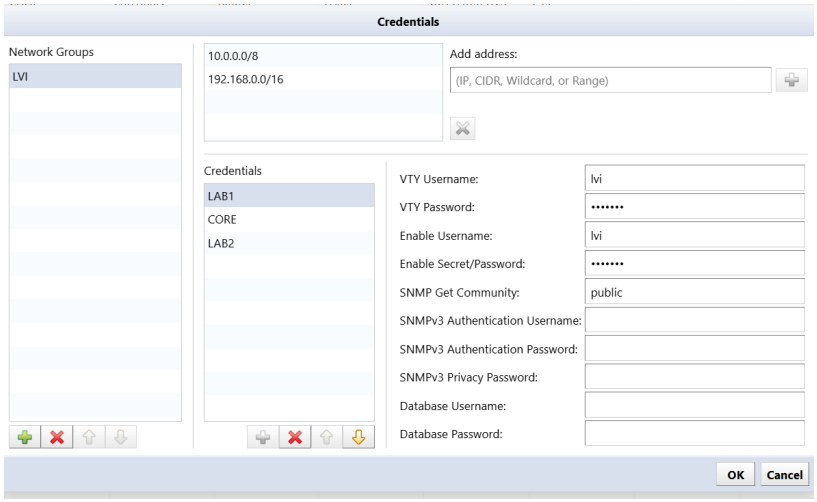
Please check the Microsoft Docs guide “Install software remotely using Group Policy” for details:

https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

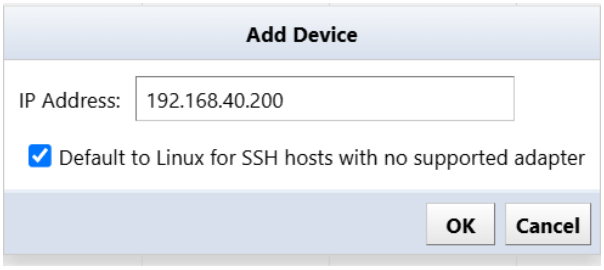
8.11.1.5 Install on Linux

8.11.1.5.1 Distribute and install Agent-D from ThirdEye For Linux, if you are in an environment where you can SSH into Linux from ThirdEye, you can install Agent-D from the ThirdEye menu. By selecting devices at once, similar to configuration backup, you can distribute to many devices at once.

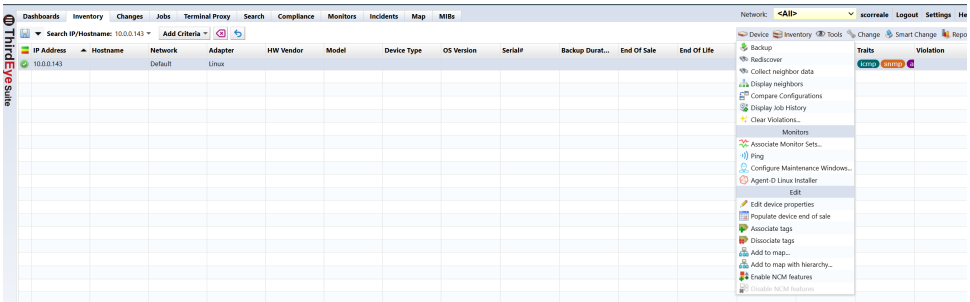
1. Set the authentication information (username/password) for SSH connection.



2. Add a Linux device to monitor.

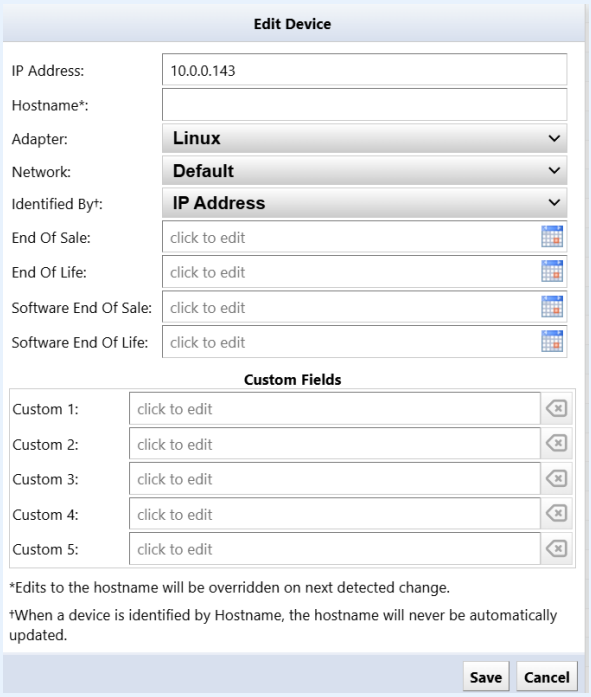


3. With the Linux device to be monitored selected, click [Agent-D Linux Installer] on the Inventory menu.

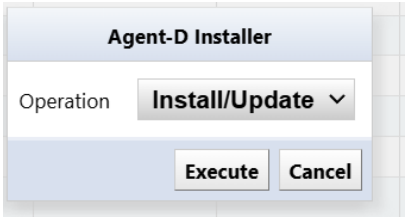


Note

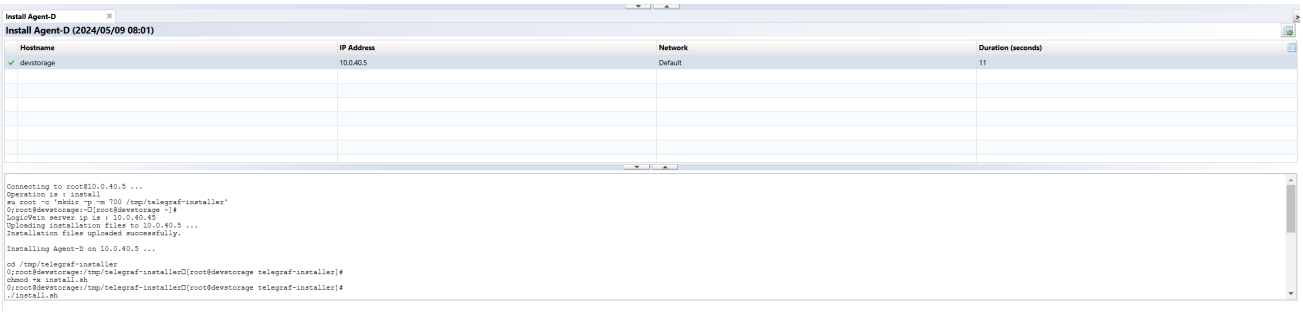
If [Agent-D Linux Installer] is grayed out and cannot be selected, there may be no Linux adapter assigned to the selected device. Make sure that a Linux adapter is assigned to the target device. You can check from [Edit device properties] in the device menu:



4. Click [Install/Update] > Execute.



5. The installation will execute and the results will be displayed in the bottom half of the screen.



8.11.1.6 CPU monitoring Use Agent-D to obtain CPU information for the installed server. By setting thresholds for CPU usage, etc., you can issue an alert when the threshold is exceeded.

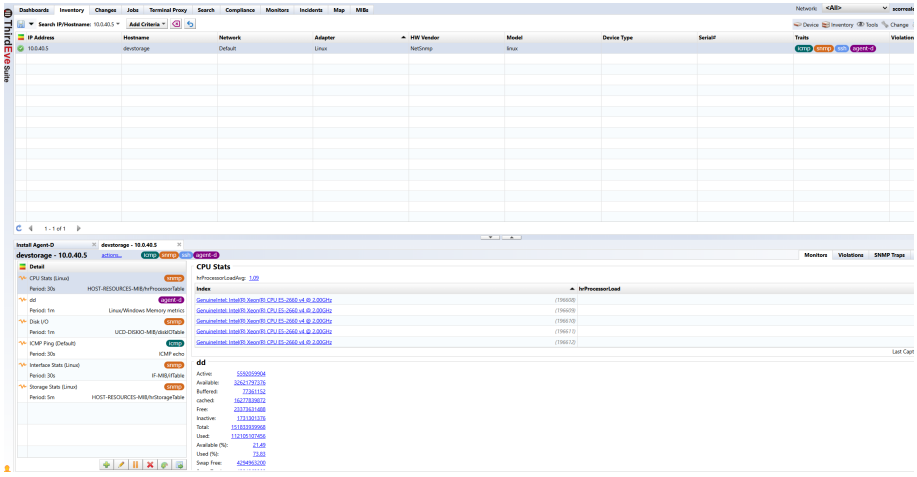
The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

- Linux CPU Stats
- Windows CPU Stats

The plugin in the [Agent-D] > [Linux CPU] window can set up as a monitor for a CentOS device.

(Refer to the **5.3.7 Monitor SNMP traps (all)** section for instructions.)

1. Doubleclick the device for which you want to configure a monitor to open the device details.

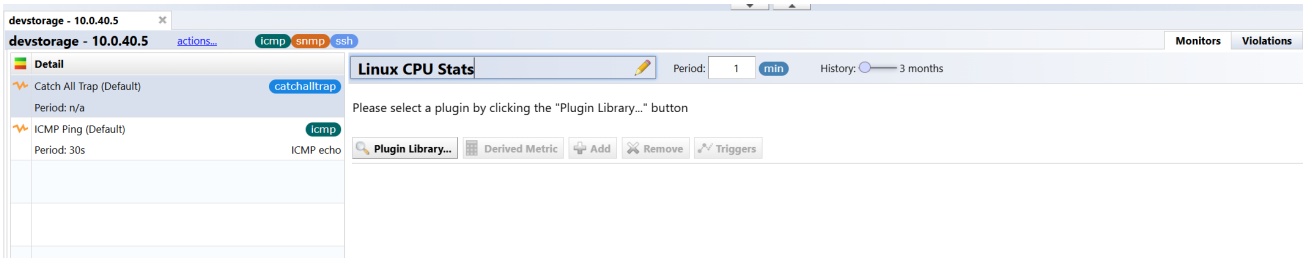


2. Click the button, then click [Agent-D].

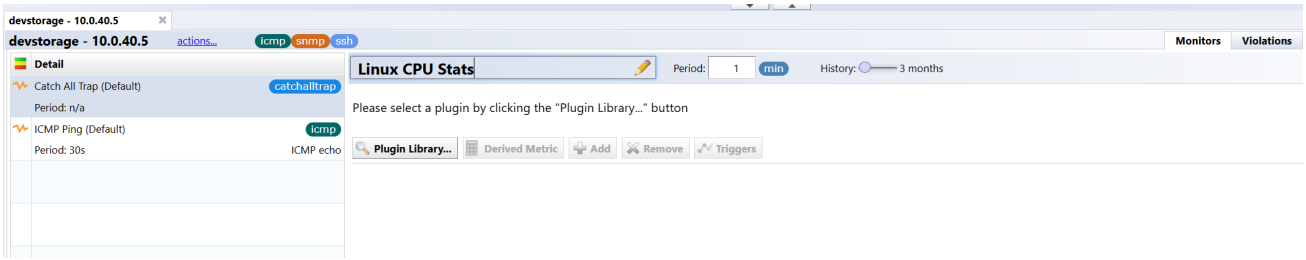
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

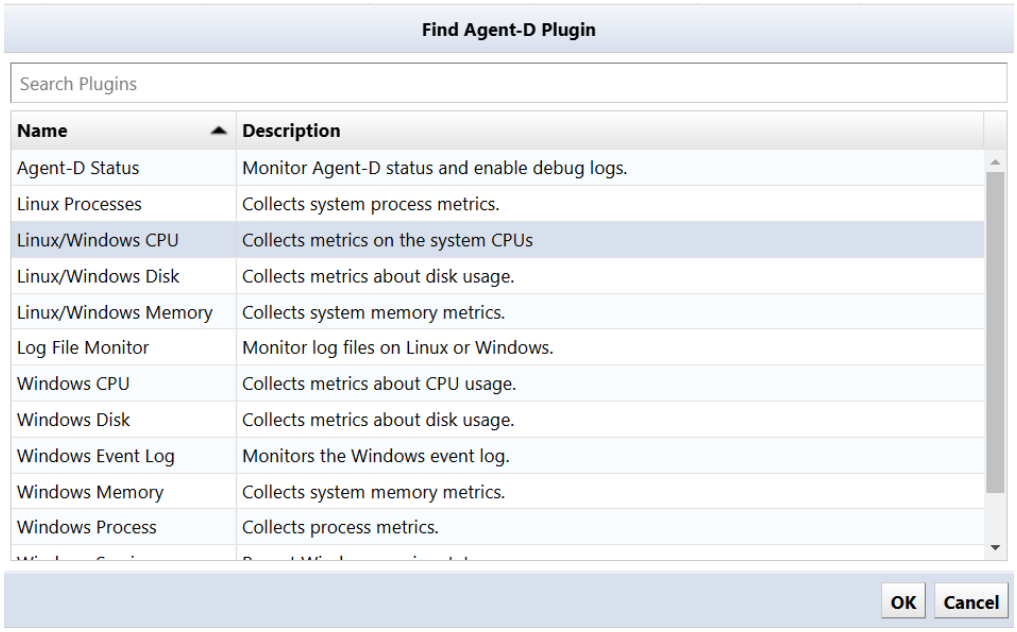
The [History] slider specifies a data retention period of 3, 6, or 12 months.



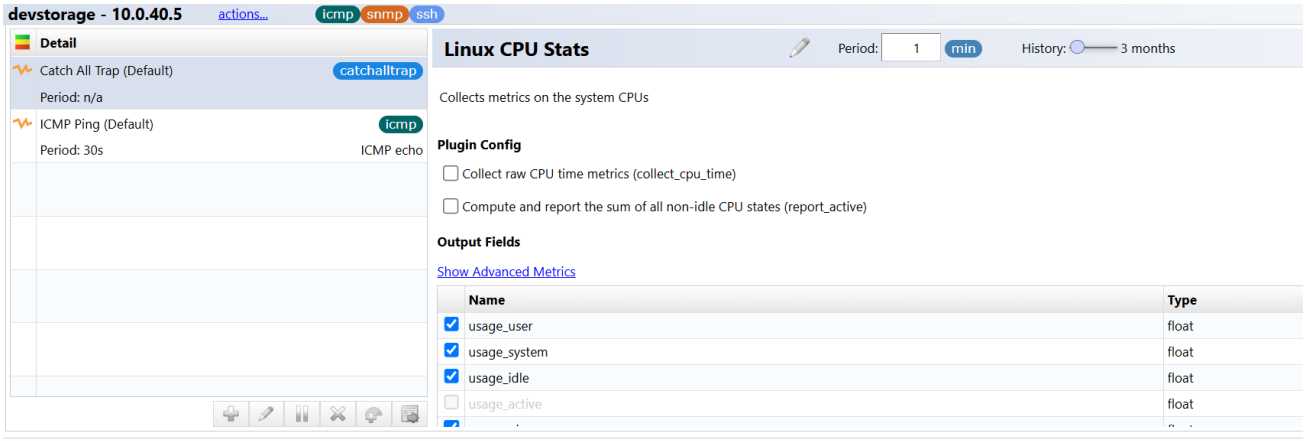
4. Click [Plugin Library…].



5. Select [Linux CPU] and click [OK].

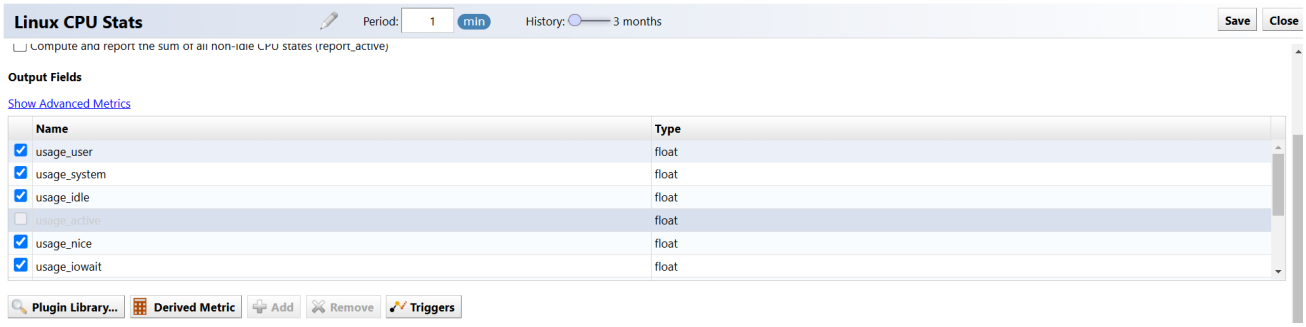


6. Check the items to be acquired in Plugin Config.



Item	Description
Collect raw CPU time metrics (collect_cpu_time)	Collects the time the CPU was used. If it is not checked, no value will be displayed even if you check the field starting from `time_` in Output fields.
Compute and report the sum of all non-idle CPU states (report_active)	Calculate the total value of values other than idle/guest/guest_nice. If there is no check, no value will be displayed even if time_active/usage_active is checked in the Output fields.

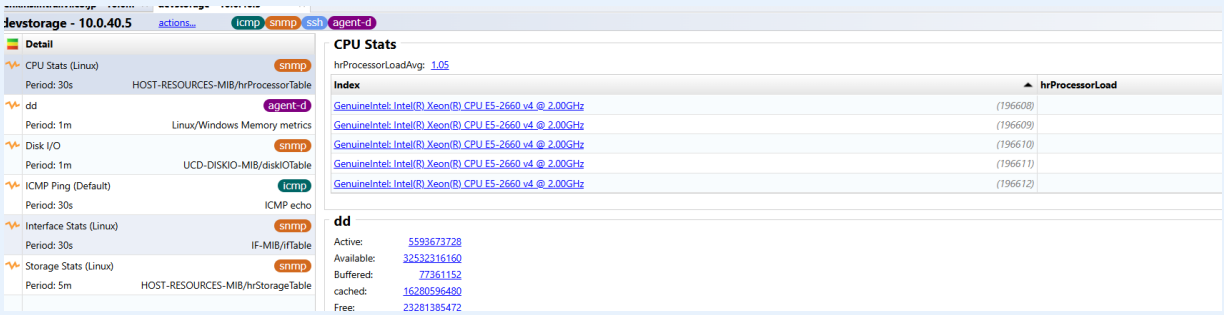
7. Check the items to be retrieved in Output Fields and click [Save].



Note

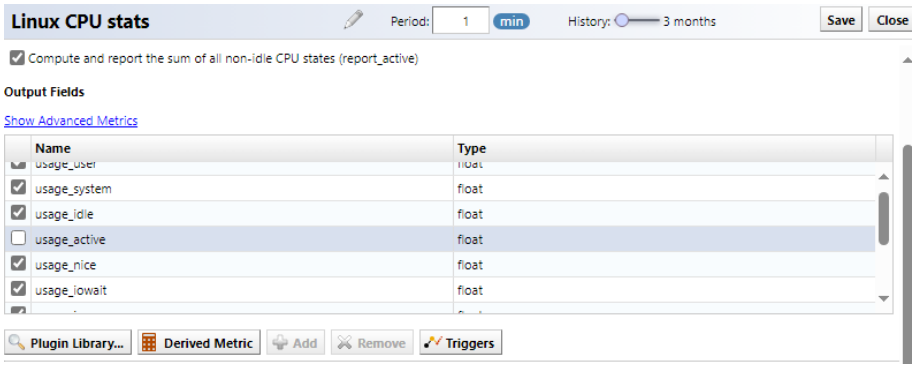
In Agent-D's Output Fields, common monitoring items are checked by default. To view other monitoring items, click "View details".

Now, Agent-D will send the CPU information and you can check it in the device details.

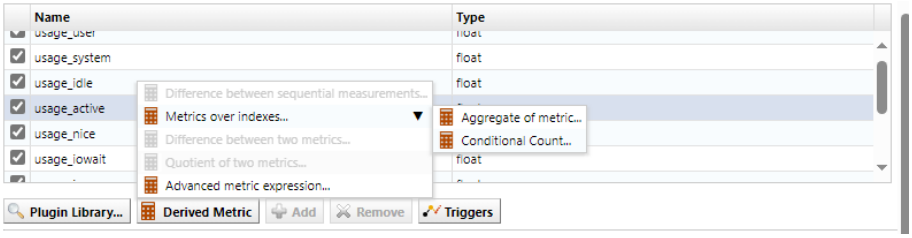


8.11.1.7 Get the overall CPU usage Agent-D's CPU monitor obtains information on a per-core basis. Click [Calculated Metrics] to get the overall CPU usage.

1. Doubleclick the CPU monitor to open it.
2. Click [usage_active] from [Output Fields] menu.



3. Click [Derived Metrics] > [Metrics over indexes] > [Aggregation of Multiple Indexes].



4. Change the metric name (The `usage_active` aggregate in the example above) to something meaningful and choose the aggregation type.
5. Click [Save].

With the above steps, you can display the aggregated value of usage_acticve for each index (each core). By setting a threshold for this, it is possible to monitor the overall CPU usage rate.

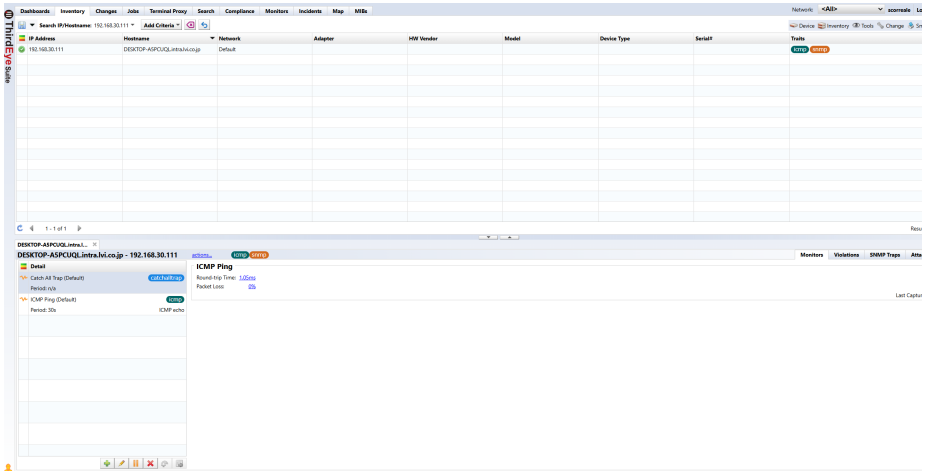
8.11.1.8 Memory monitoring Use Agent-D to obtain memory information for installed servers. By setting thresholds for things like memory usage, you can issue an alert when the threshold is exceeded.

The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

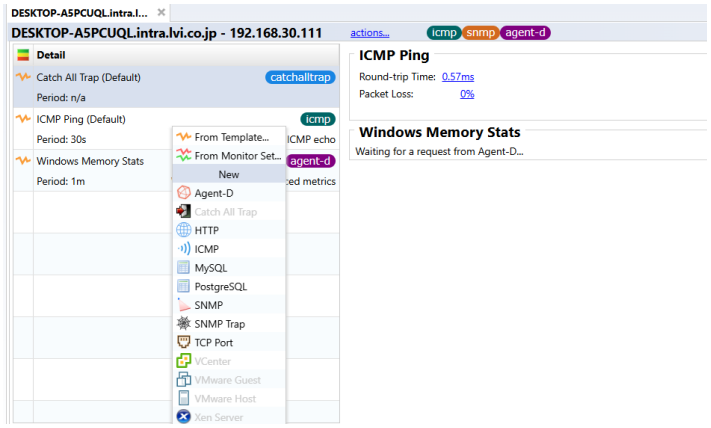
- Linux Memory Stats
- Windows Memory Stats

The [Agent-D] > [Windows Memory] plug-in can be set up as as a monitor for a Windows server device:

1. Doubleclick the device for which you want to configure a monitor to open the device details.



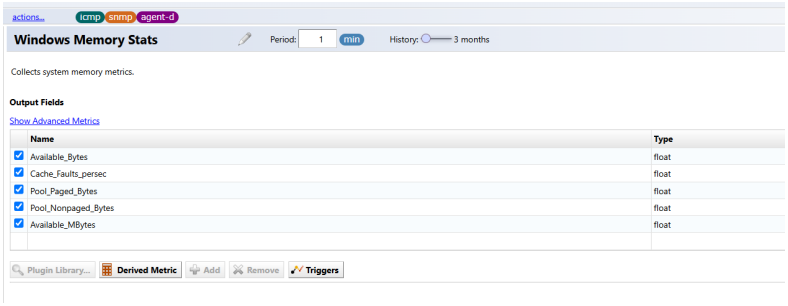
2. Click the button, then click [Agent-D].



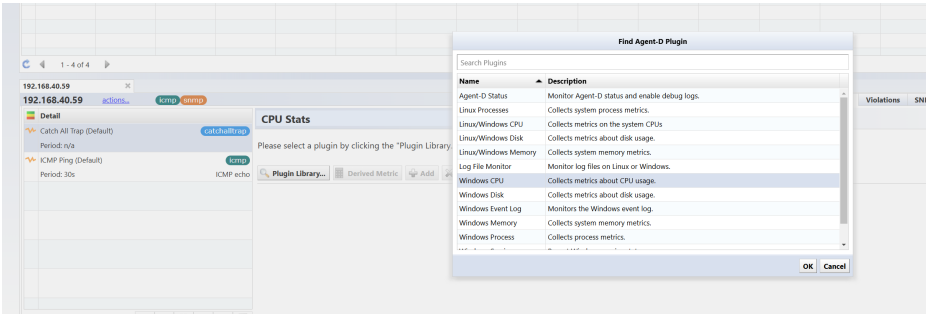
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

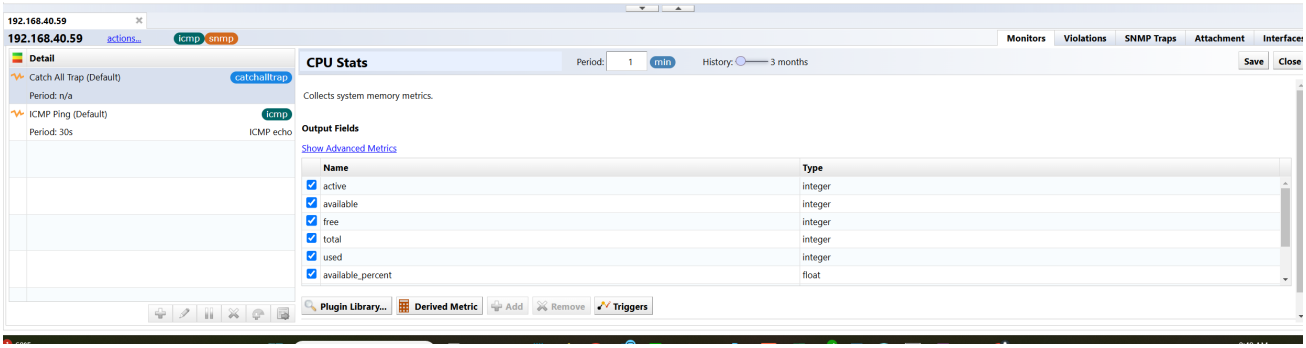
The [History] slider specifies a data retention period of 3, 6, or 12 months.



4. Click [Plugin Library…] and select [Windows Memory] and click [OK]



5. Check the items for which you want to obtain data in [Output Fields], and click [Save].



Note

In Agent-D's Output Fields, common monitoring items are checked by default. To view other monitoring items, click [View details].

Now, Agent-D will send the memory information and you can check it in the device details.

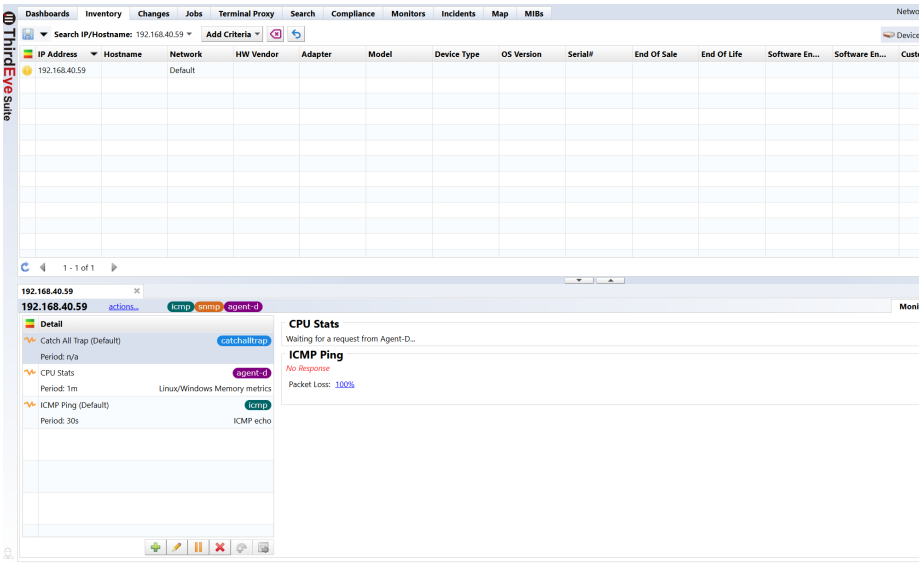
8.11.1.9 HDD monitoring Use Agent-D to obtain the HDD information of the installed server. By setting thresholds for HDD free space, usage rate, etc., you can issue an alert when the thresholds are exceeded.

The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

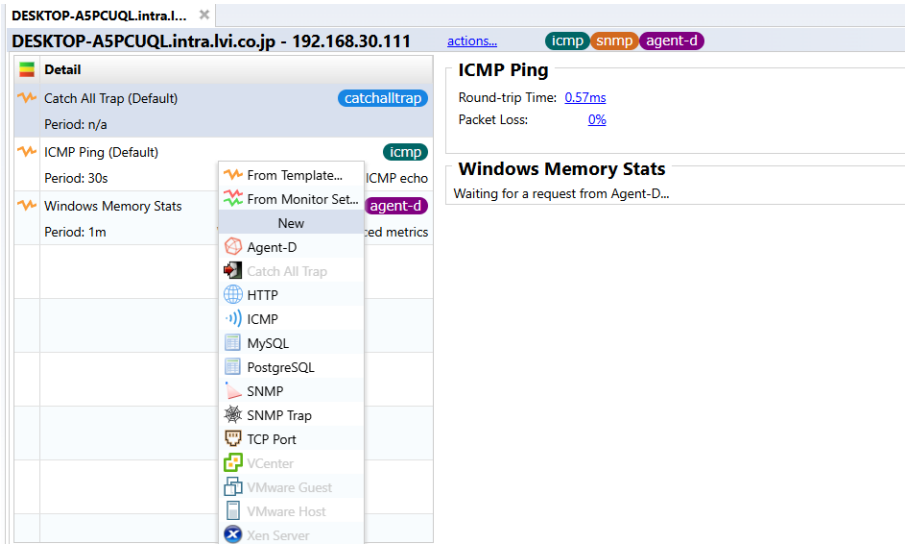
- Linux Disk Stats
- Windows Disk Stats

The [Agent-D] > [Linux Disk] plug-in can be set up as a monitor for a CentOS device:

1. Doubleclick the device for which you want to configure a monitor to open the device details window in the bottom half nof the screen.



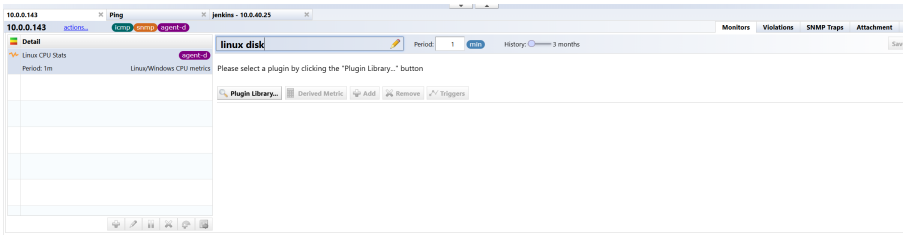
2. Click the button, then click [Agent-D].



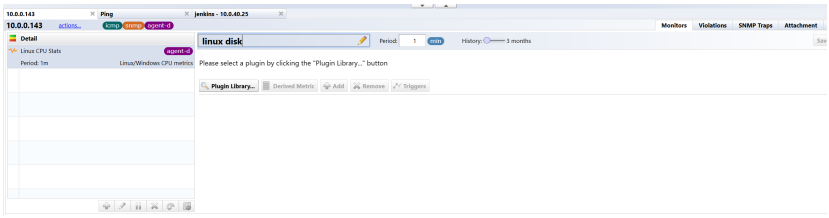
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

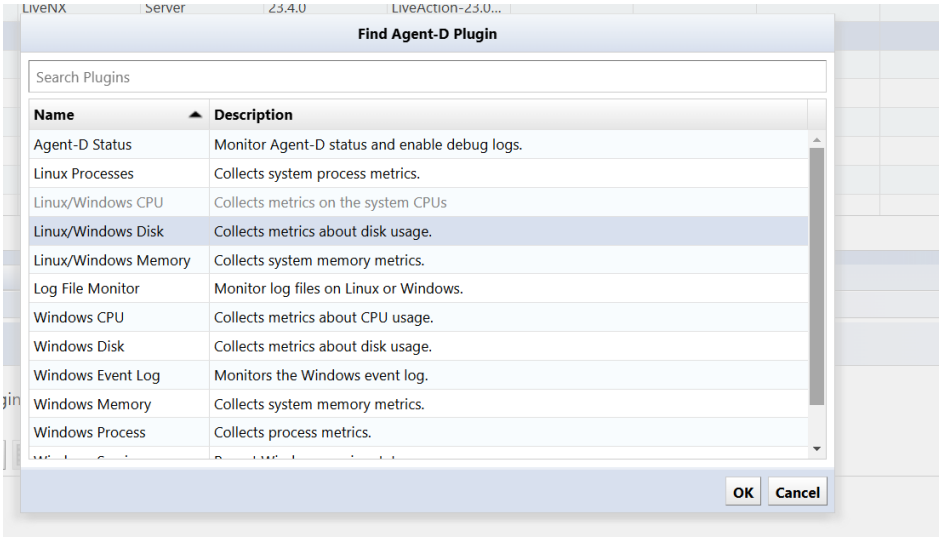
The [History] slider specifies a data retention period of 3, 6, or 12 months.



4. Click [Plugin Library…].

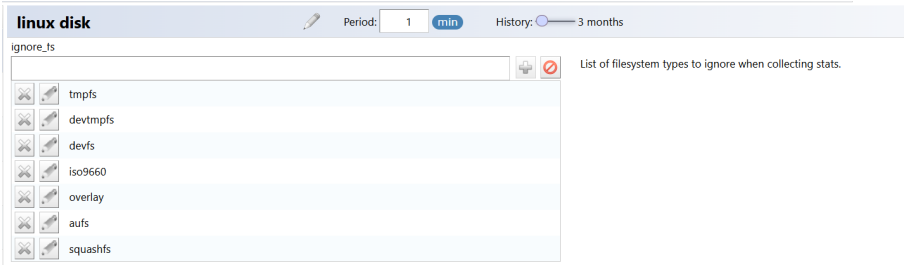


5. Select [Linux/Windows Disk] and click [OK].

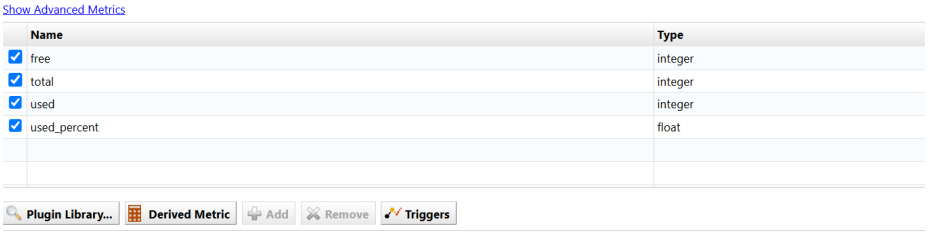


6. In the "`ignore_fs`" field, specify file systems to exclude from data collection.

Several file systems are preset in the exclusion list. Edit as necessary using the (Add), (Delete), or (Edit) buttons.



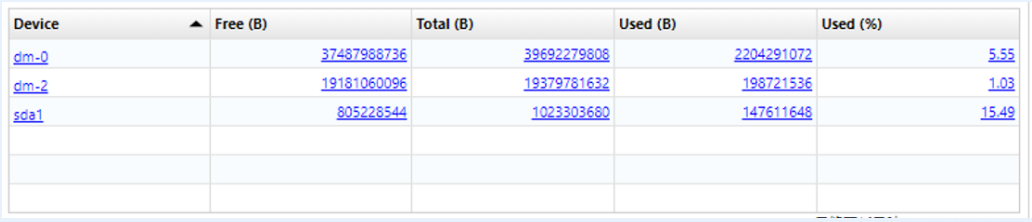
7. Check the items you want to obtain in [Output Fields] and click [Save].



Note

In Agent-D's Output Fields, common monitoring items are checked by default. To view other monitoring items, click "View details".

Now, Agent-D will send the HDD information and you can check it in the device details.



Device	Free (B)	Total (B)	Used (B)	Used (%)
dm-0	37487988736	39692279808	2204291072	5.55
dm-2	19181060096	19379781632	198721536	1.03
sda1	805228544	1023303680	147611648	15.49

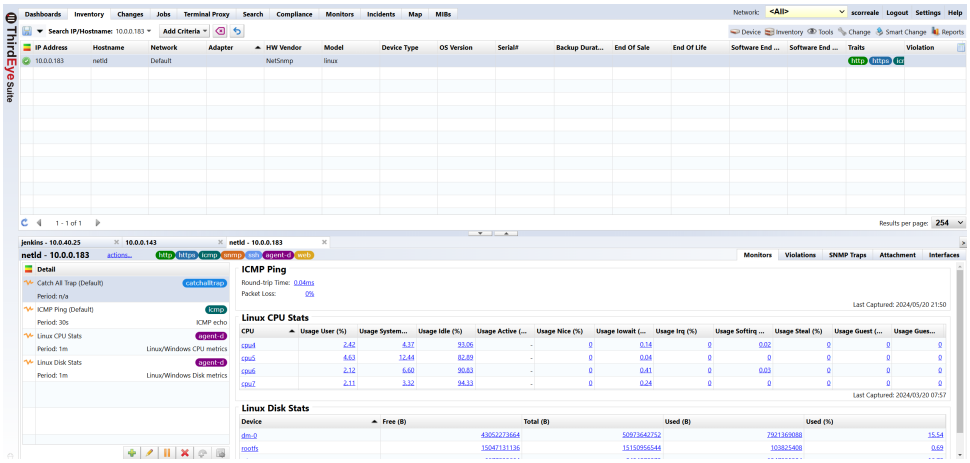
8.11.1.10 Process monitoring Use Agent-D to obtain information about installed server processes. By setting thresholds for process status, memory usage, etc., you can issue alerts when thresholds are exceeded.

The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

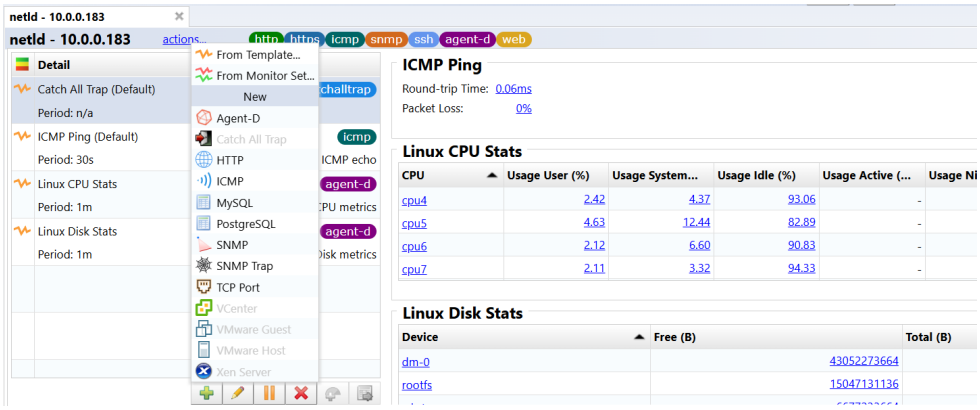
- Linux Process Stats
- Windows Process Stats

The [Agent-D] > [Windows Process] plug-in can be set up as a monitor for a Windows server device:

1. Doubleclick the device for which you want to configure a monitor to open the device details.



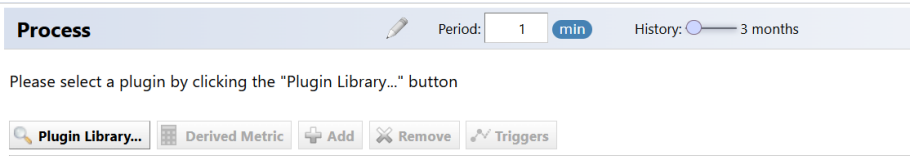
2. Click the button, then click [Agent-D].



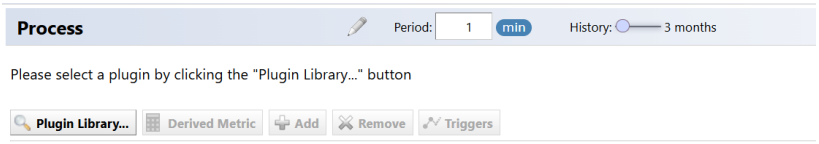
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

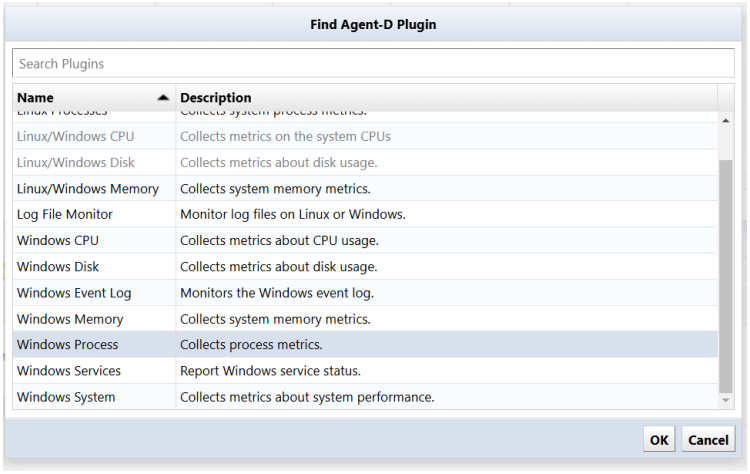
The [History] slider specifies a data retention period of 3, 6, or 12 months.



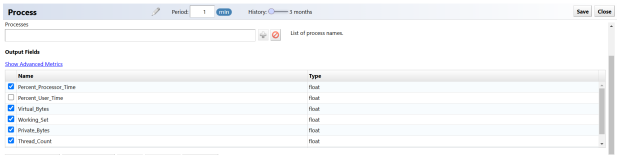
4. Click [Plugin Library…].



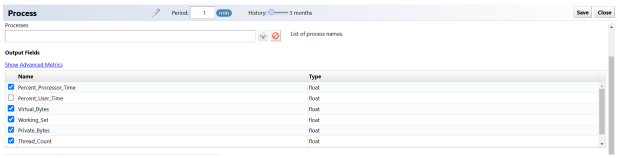
5. Select Window Process and click [OK].



6. Add the process name to be monitored by entering it in the [Processes] field.



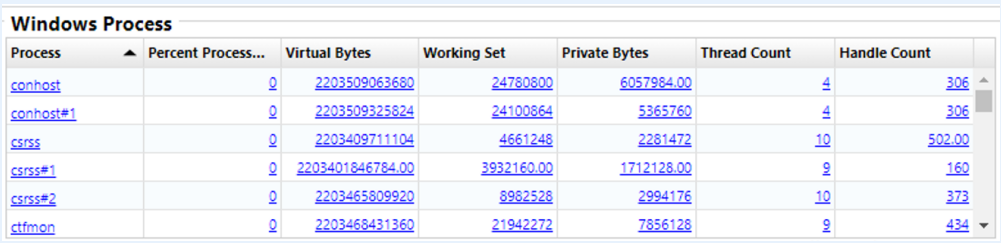
7. Check the items you want to obtain in [Output Fields] and click [Save].



Note

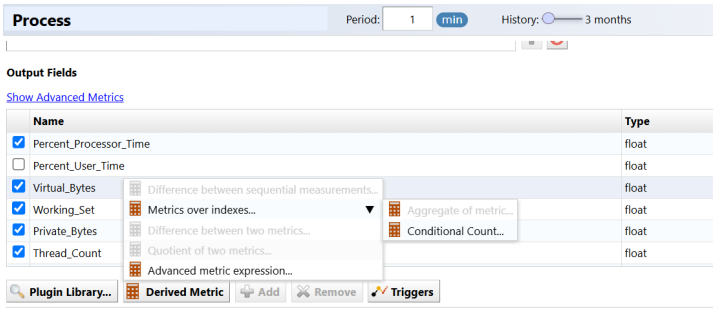
In Agent-D's Output Fields, common monitoring items are checked by default. To view other monitoring items, click "View details".

Now Agent-D will send the process information and you can check it in the device details.



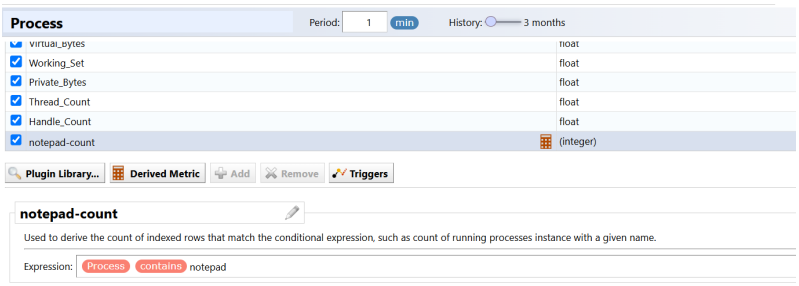
8.11.1.11 Monitor the number of processes If you want to monitor the number of running processes, you need to add a metric to count the number of processes.

1. Open the process monitor by doubleclicking it.
2. Click [Calculated Metrics] > [Metrics over indexes] > [Total Condition Passed].



3. Change the count metric name to something meaningful, and set the calculation formula.

(In the figure below, the metric name has been changed from the initial value "`count-metric`" to "`notepad-count`")

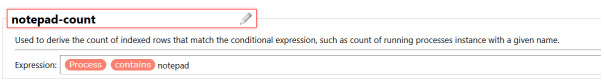


- **For Windows**, set the process name to "Process".

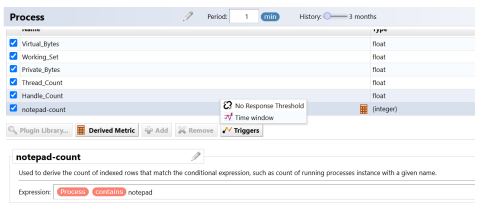
Setting calculation formula example: `process contains {Process name}`

- **For Linux**, set the process name to "process_name".

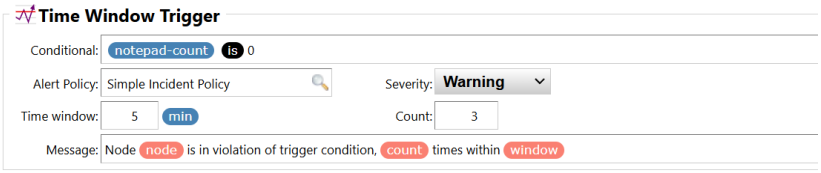
Setting calculation formula example: `process_name contains {Process name}`



4. Click [Trigger] > [Time Window].

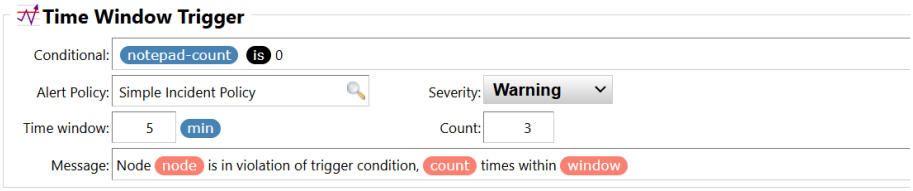


5. Once the Count has been set, set conditions using metrics.



Menu item	Explanation
Conditional	You can specify conditions using the following items: `is` (equal) `"is not"` (not equal) `">"` (less than, the value on the right is smaller) `"<"` (greater than, the value on the right is greater)

6. Set other items (“alert policy”/“severity”/“Time window”/“count/message”).



Item	Explanation
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (Minimum value: 1)
Alert Policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning) `"Emergency"`, `"Alert"`, `"Critical"`, `"Error"`, `"Warning"`, `"Notification"`, `"Information"`, `"Debug"`
Message	Set the message displayed when a failure is detected. *In order to display the message, the “Incident Registration” action must be defined in the alert policy.

7. Click [Save].

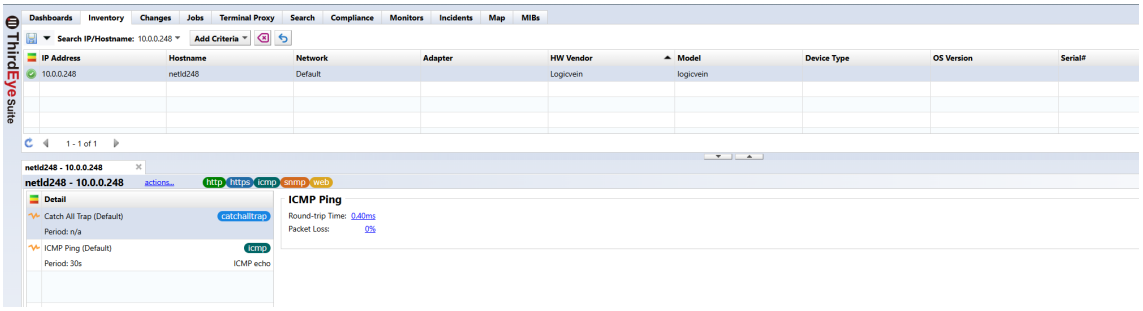
8.11.1.12 Text log monitoring Use Agent-D to obtain log information for the installed server. You can issue an alert when a log containing a specific string is detected.

The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

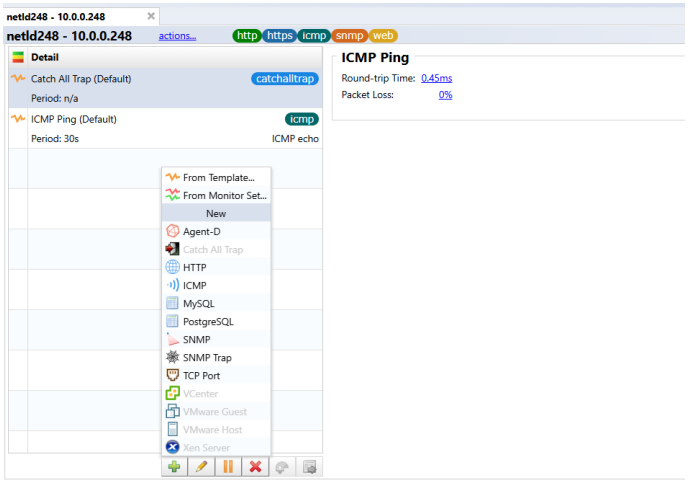
- Linux Syslog Monitor
- Windows Log File Monitor

Here, we will explain how to set up the [Agent-D] > [Log Fie Monitor] plug-in as a monitor for a Linux device.

1. Doubleclick the device for which you want to configure a monitor to open the device details.



2. click the button, then click [Agent-D].



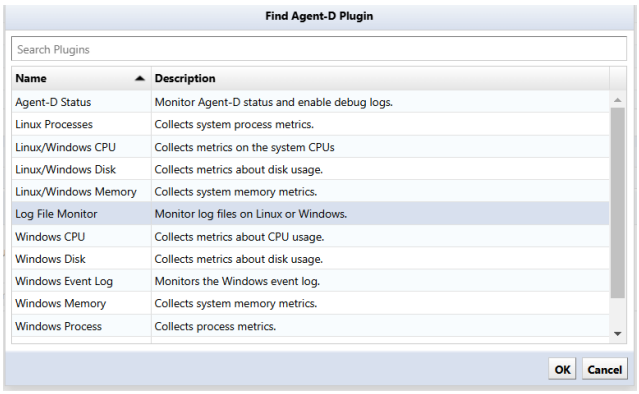
3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifes the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.

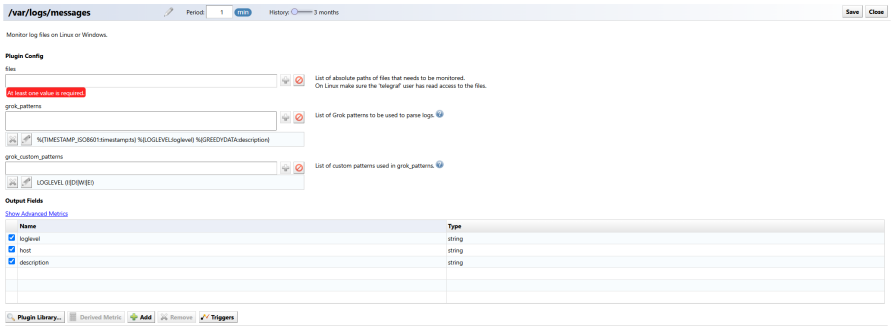
4. Click [Plugin Library …].

5. Select [Log Fie Monitor] and click [OK].

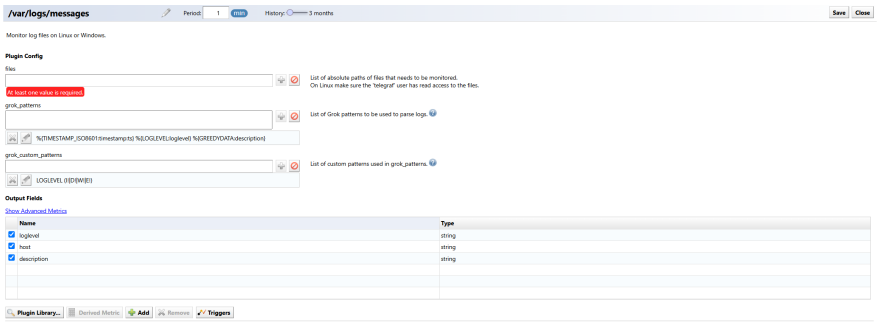


6. Add the absolute path of the log file to be monitored in the [files] field.

Security settings must be configured in advance so that the Agent-D program can read the target log file. It runs as the “SYSTEM” user on Windows and as the “telegraf” user on Linux.



7. Enter grok_patterns and grok_cusom_patterns.



8.11.1.13 Syslog monitoring Use Agent-D to capture syslog information that is forwarded to ThirdEye. An alert can be issued when an event log containing a specific string is detected.

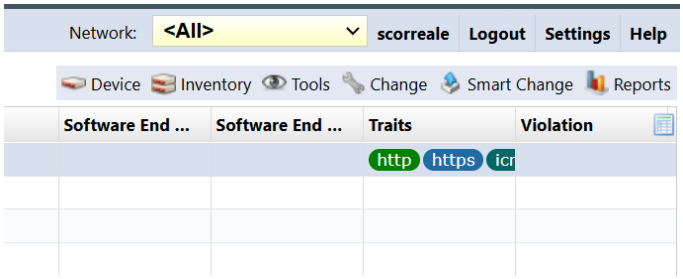
The following templates are registered in advance as monitors for HDD monitoring on the Monitors > [Templates] tab.

- ThirdEye Syslog Monitor

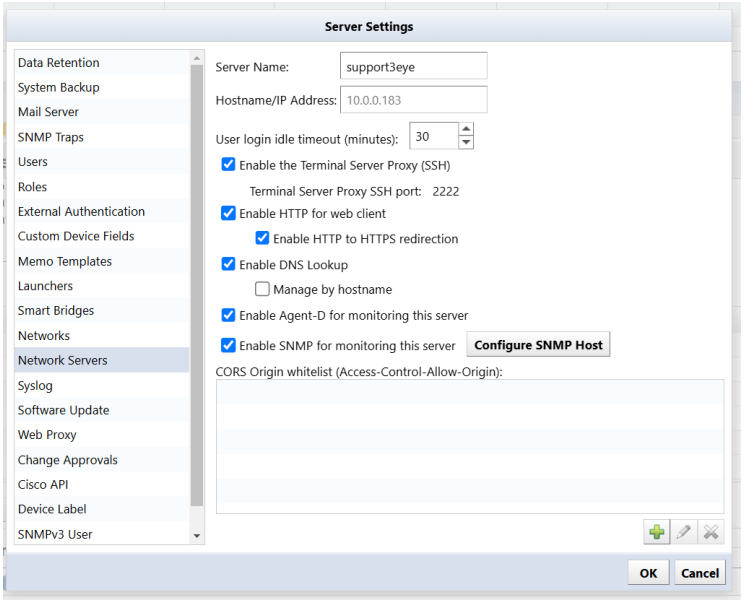
Agent-D is pre-installed on ThirdEye, but is disabled by default. If you want to enable/disable Agent-D, you must restart ThirdEye.

This section will explain how to enable ThirdEye'sAgent-D and set the ThirdEye Syslog Monitor as a monitoer on the [Templates] tab.

1. Click Settings.

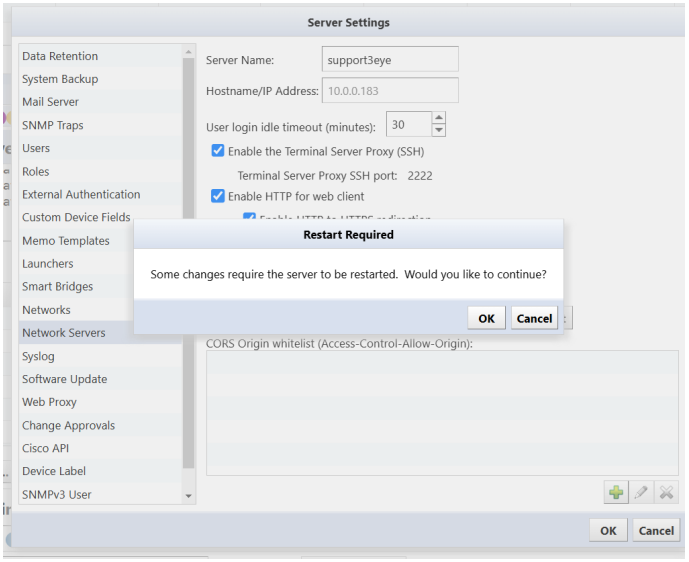


2. Select [Network Servers], check [Enable Agent-D for monitoring this server], and click [OK].

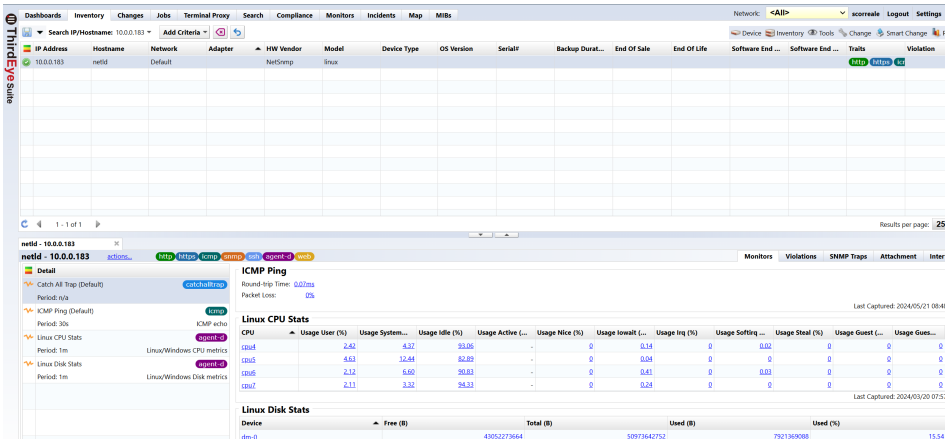


3. Click [OK] on the reboot confirmation screen.

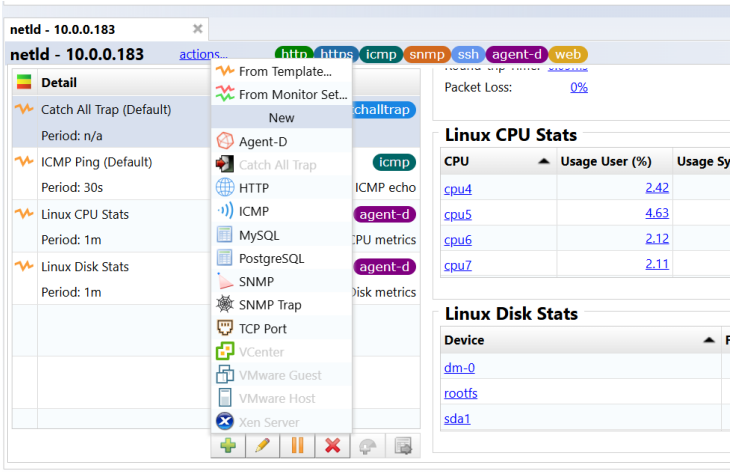
ThirdEye must be restarted for the settings to take effect. Click [OK] and ThirdEye will automatically restart.



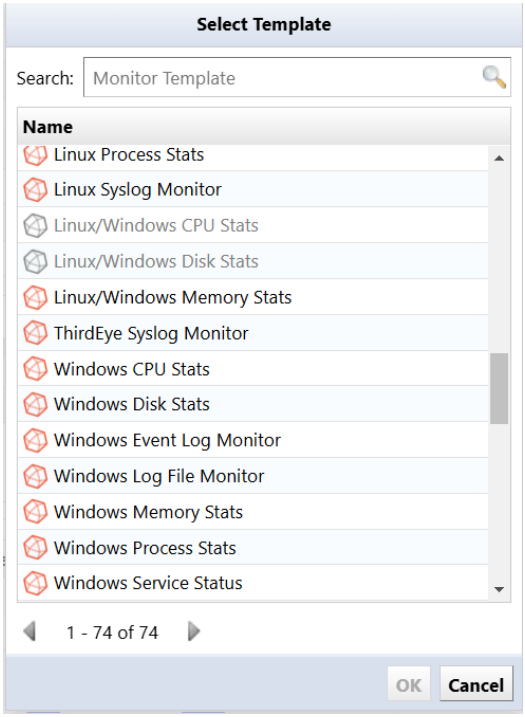
4. Check for the message “Restarting services …” and wait a few minutes.
5. A login screen will be displayed. After logging in, click the [Devices] tab.
6. Register ThirdEye’s own IP address as a monitored device from Inventory > [Add Device].
7. Doubleclick to open device details.



8. click the button, and then click [Add from Template].

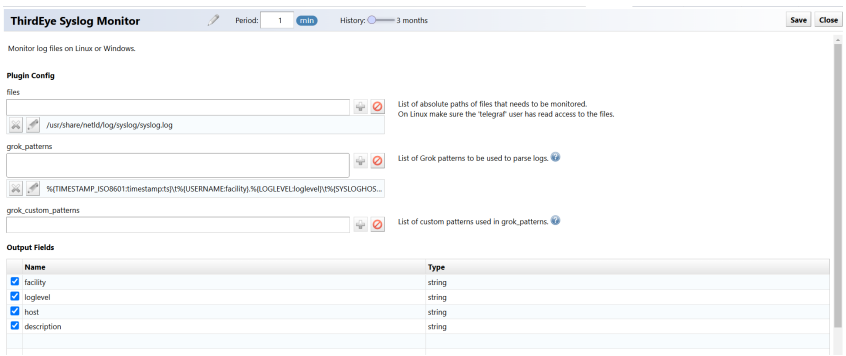


9. Select ThirdEye Syslog Monitor and click [OK].



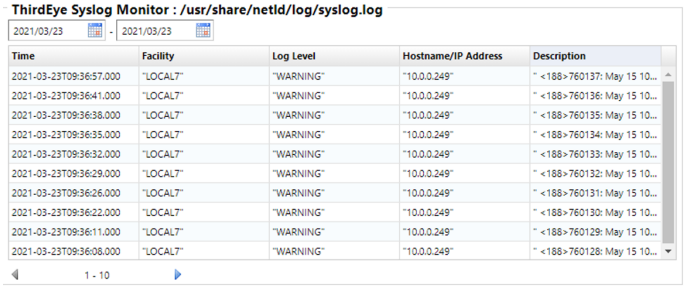
10. Check the items you want to obtain in [Output Fields] and click [Save].

There is no need to change the [files] or [grok_patterns] settings that are already set in the template.



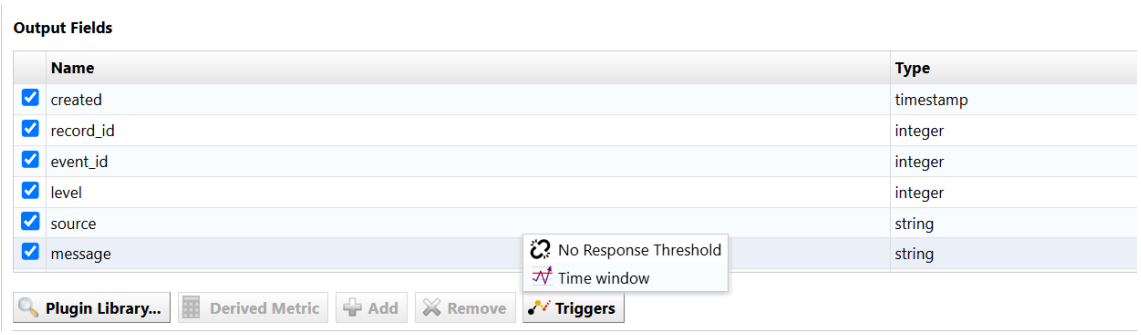
With the above steps, you can obtain the Syslog information sent to ThirdEye.

Syslog messages are displayed in the “Conditional” field.

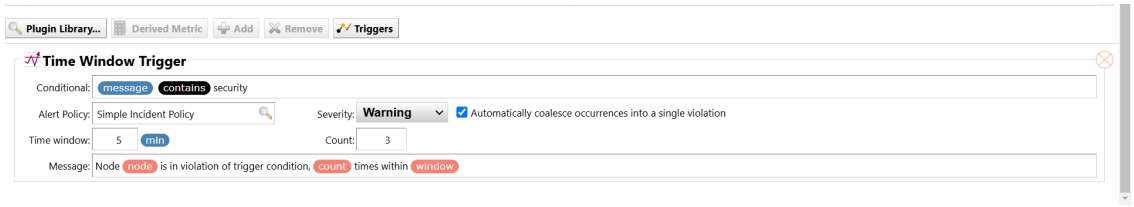


8.11.1.14 Trigger an alert if any string is included The contents of the [Windows Event Log General] tab are displayed in the message field of the Agent-D Windows Eventlog plugin. By setting a filter condition that this "message" field contains a specific string, you can trigger an alert if the Windows event log contains any string.

1. Doubleclick the event log monitor to open it.
2. Click [Trigger] > [Time window].

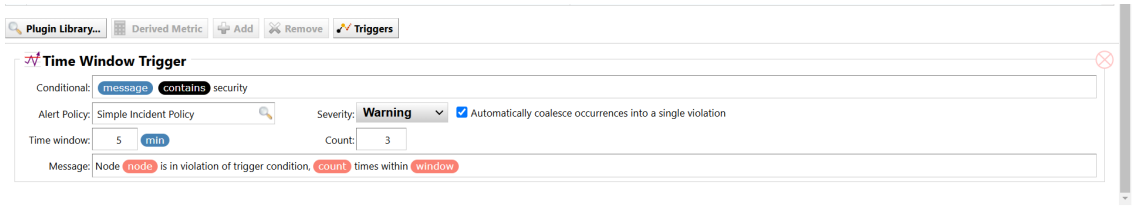


3. Set conditions in the "Conditional" field.



Setting Item	Explanation
Conditional	You can specify conditions using the following items: `contains` You can select other conditional expressions (`is`, `is not`, `>`, `<`, `not contains`), but if you want to set a condition that includes a specific string, use `contains`.

4. Set other items (“alert policy”/“severity”/“period”/“count/message”).

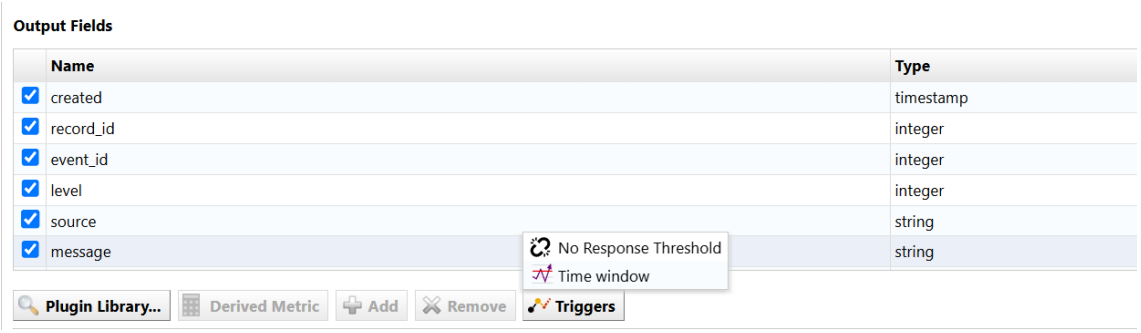


Item	Description
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (Minimum value: 1)
Alert policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning) `"Emergency"`, `"Alert"`, `"Critical"`, `"Error"`, `"Warning"`, `"Notification"`, `"Information"`, `"Debug"`
Message	Set the message displayed when a failure is detected. *In order to display the message, the “Incident Registration” action must be defined in the alert policy.

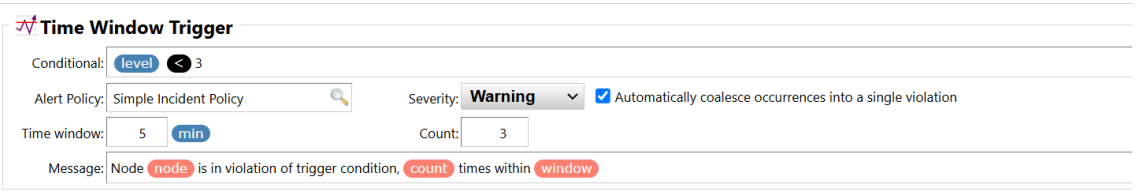
5. Click [Save].

8.11.1.15 Alert when logs above a certain level occur An alert can be triggered when an event with a specific log level such as “Critical” or “Error” occurs in the Windows event log. Here, we will use an example of setting up an alert to be issued when an event with a log level of “error” or higher occurs.

1. Doubleclick the event log monitor to open it.
2. Click [Trigger] > [Time window].

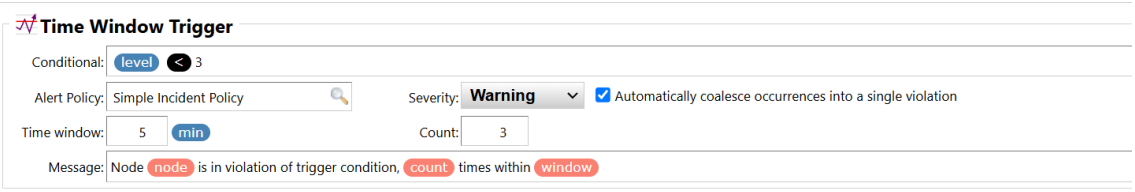


3. Set the condition using Agent-D’s “level”.



Item	Explanation
Conditional	You can specify conditions using the following items: `is` (equal) `is not`(not equal) > (less than, the value on the right is smaller) < (greater than, the value on the right is greater)

4. Set other items (“alert policy”/“severity”/“period”/“count/message”).

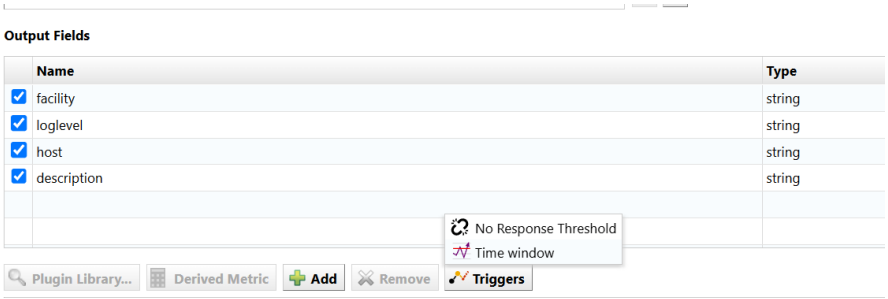


Item	Description
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (Minimum value: 1)
Alert policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning) `"Emergency"`, `"Alert"`, `"Critical"`, `"Error"`, `"Warning"`, `"Notification"`, `"Information"`, `"Debug"`
Message	Set the message displayed when a failure is detected. *In order to display the message, the “Incident Registration” action must be defined in the alert policy.

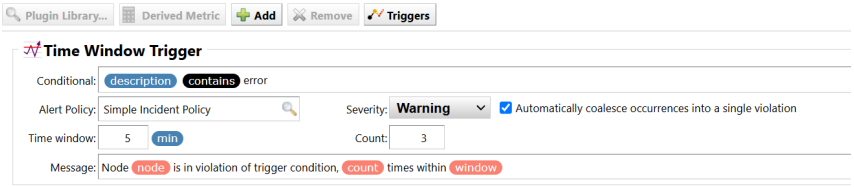
5. Click [Save].

8.11.1.16 Trigger an alert if any string is included The content of the Syslog message is displayed in the "description" field of the Agent-D "Log File Monitor" plugin. By setting a filter condition where the "description" contains a specific string, you can trigger an alert if the Syslog message contains the specific string.

1. Doubleclick the [ThirdEye Syslog Monitor] monitor to open it.
2. Click [Trigger] > [Time window].

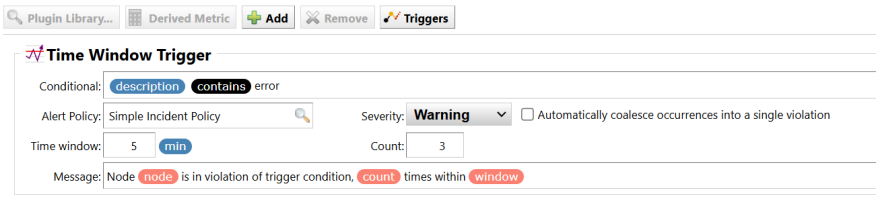


3. Set the "Conditionnal" using "`description`".



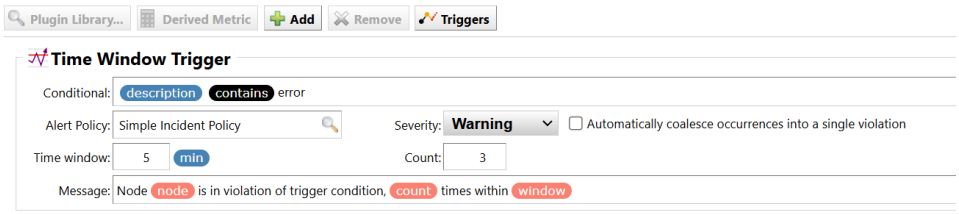
Item	Explanation
Conditional	You can specify conditions using the following items: `contains` (include) You can select other conditional expressions (`is`, `is not`, `>`, `<`, `not contains`), but if you want to set a condition that includes a specific string, use `contains`.

4. Uncheck “Automatically coalesce occurrences into a single violation”.



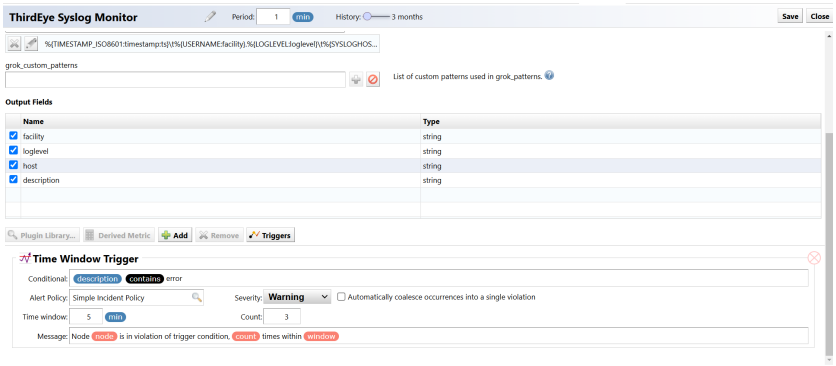
> **Note**
>
> In ThirdEye, violations that share the same trigger and index are aggregated into one monitored log file with the name “`Index`”. Unchecking “Automatically coalesce occurrences into a single violation” allows violations to occur for *each* log that matches the conditions.
>
> However, violations and emails will occur more frequently than when grouped. And a message with the same trigger and index will still be aggregated if the first violation has not been cleared. In such cases, only the most recently detected message will be displayed.

5. Set other items (“alert policy”/“severity”/“period”/“count/message”).



Item	Description
Period	Set the period for executing the process. (Minimum value: 1 minute). The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail within the set period before executing the process. (Minimum value: 1)
Alert Policy	Specify alert policy.
Significance	Select the severity from the following: (Initial value: warning) `"Emergency"`, `"Alert"`, `"Critical"`, `"Error"`, `"Warning"`, `"Notification"`, `"Information"`, `"Debug"`
Message	Set the message displayed when a failure is detected. *In order to display the message, the “Incident Registration” action must be defined in the alert policy.

6. Click [Save].



8.11.1.17 Grok Patterns

A grok_pattern is composed of:

`%{PATTERN_NAME:FIELD_NAME:MODIFIER(optinon)}`

and the content that matches the `PATTERN NAME` defined by the regular expression put into `FIELD_NAME`.

Use grok_pattern to enter a formula to split a single line of log and include the characters that match the specified field.

Example:

Log message `"Aug 20 11:15:40 192.168.0.1 ERROR systemd: Started Hostname Service."`

Equation:

`%{SYSLOGTIMESTAMP:timestamp}\s%{IPORHOST:iporhost}\s %{ LOGLEVEL:level}\s%{GREEDYDATA:me`

Save the value `"Aug 20 11:15:40"` in the field called “times” using the pattern `SYSLOGTIMESTAMP`.

grok_pattern: `%{SYSLOGTIMESTAMP:timestamp}`

Save the value `192.168.0.1` in the field called “iporhost” using the pattern `IPORHOST`.

grok_pattern: `%{IPORHOST:iporhost}`

Save the value in the field called “level” using the pattern `ERROR` called “LOGLEVEL”.

grok_pattern: `%{LOGLEVEL:level}`

Save the value of `"systemd: Started Hostname Service."` in the field called “message” using the pattern `GREEDYDATA`.

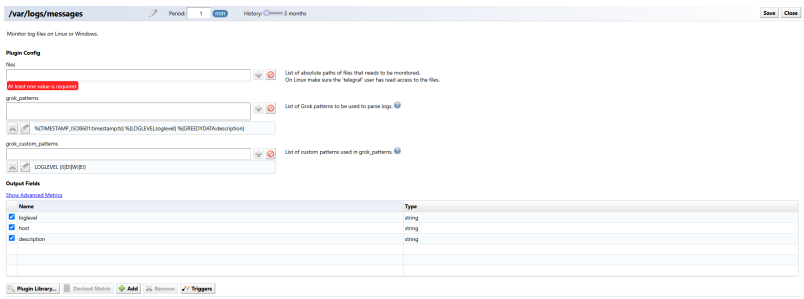
grok_pattern: `%{GREEDYDATA:message}`

8.11.2 Grok custom patterns

You can define a new `PATTERN_NAME` to be used with grok_pattern.

Create it using the following syntax: `PATTERN_NAME`(regular expression)

Check the items you want to obtain in [Output Fields] and click [Save].



Now, Agent-D will send log information and you can check it in the device details.

8.12 Incidents

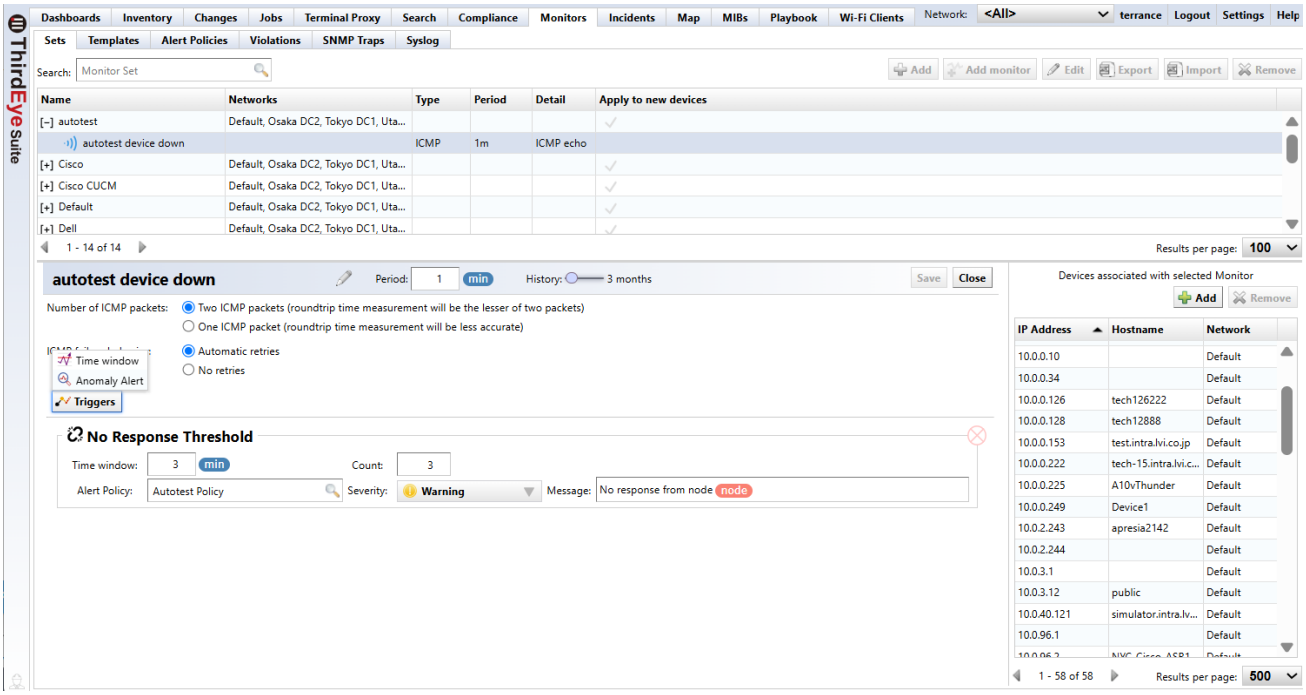
The Incidents main tab in centralizes network issue management by aggregating monitoring system violations into trackable incidents. It automatically groups related events under unique IDs to avoid duplication, provides status updates (e.g., resolution marking), and retains historical data until manual closure. Key features include filtering/sorting tools, email notifications, and audit trails for investigating network health events.

8.13 Anomaly Alert

This feature is utilized to determine the parameters for an alert. It will run for a 14-day period to define the parameters.

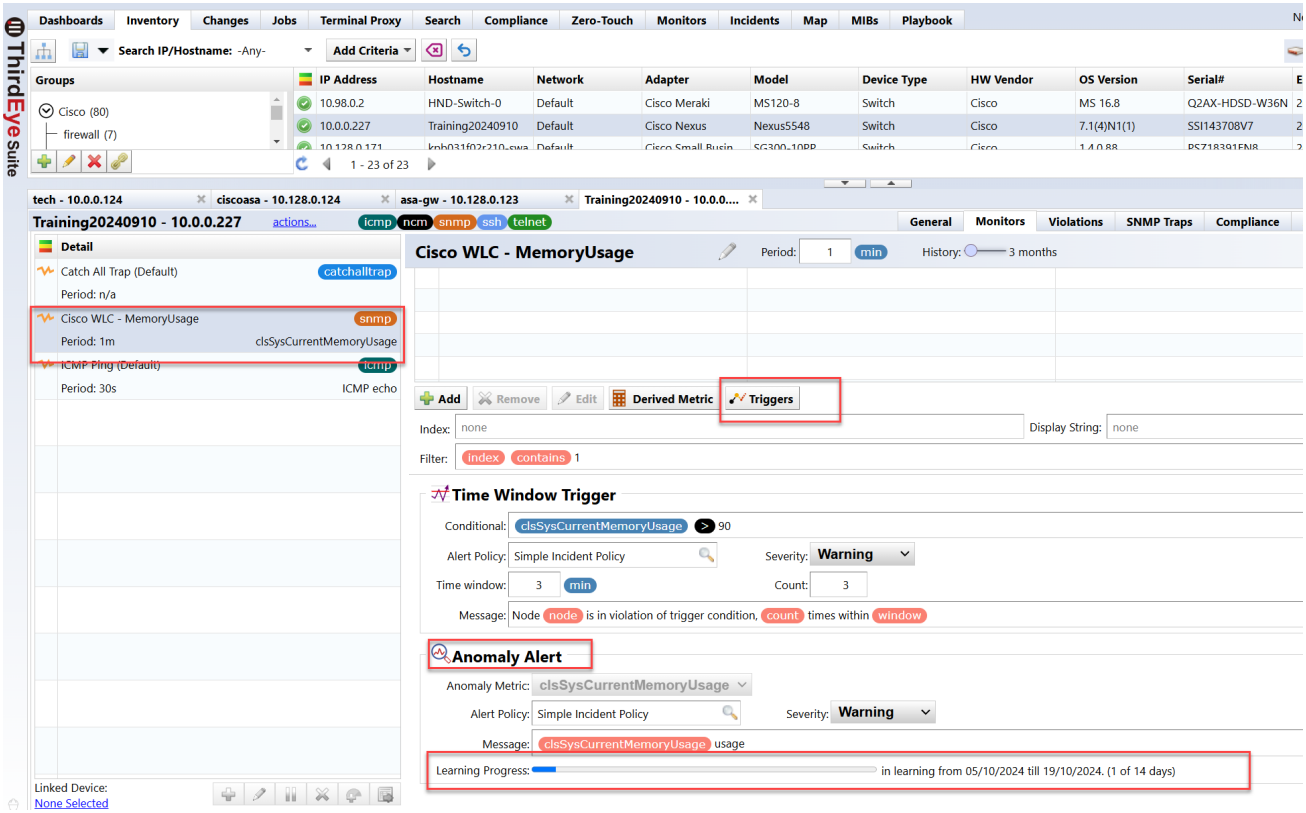
8.14 Enabling a device

1. Select ther device in the Inventory tab.
2. In the [Monitor Tab], double click to select the incident detail to apply the anomaly alert.
3. Click the [Triggers] button, and select [Anomaly Alert].



4. Add in your message, click [Save] then [Close].

This will cause the anomaly alert to run for 14 days, during which time it will learn the parameters to alert on.



8.15 Map

The Map tab provides network visualization and spatial infrastructure management capabilities. It allows hierarchical mapping (country > city > building) with automatic device synchronization from inventory updates, and integrates seamlessly with monitoring systems.

In the Map tab, you can:

- Monitor in real-time using color-coded alerts.
- Perform wireless client tracking.
- Customize icons/backgrounds customization.

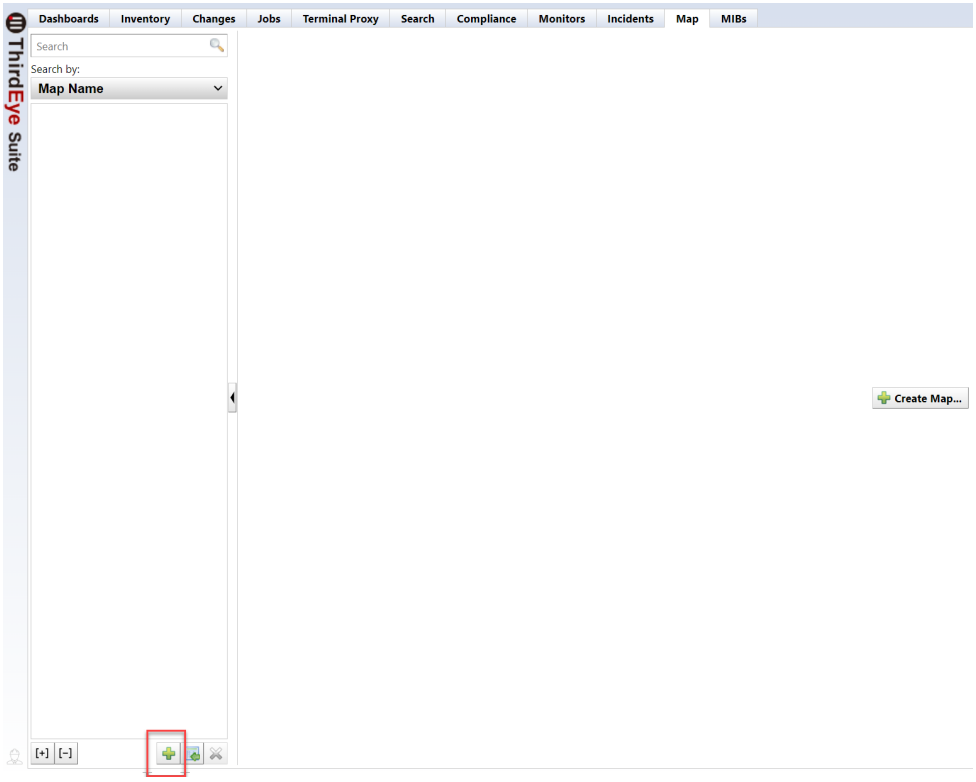
8.15.1 Set up the map

Maps are display features that allow you to visually manage your network configuration. By adding monitored equipment to the map as objects, you can visually display device failure conditions.

8.15.2 Create a map

You can create a map object and create multiple map objects to create a hierarchical monitoring map.

1. Click the button at the bottom left of the screen.



2. On the [New Map] screen, enter the map name and click [OK].

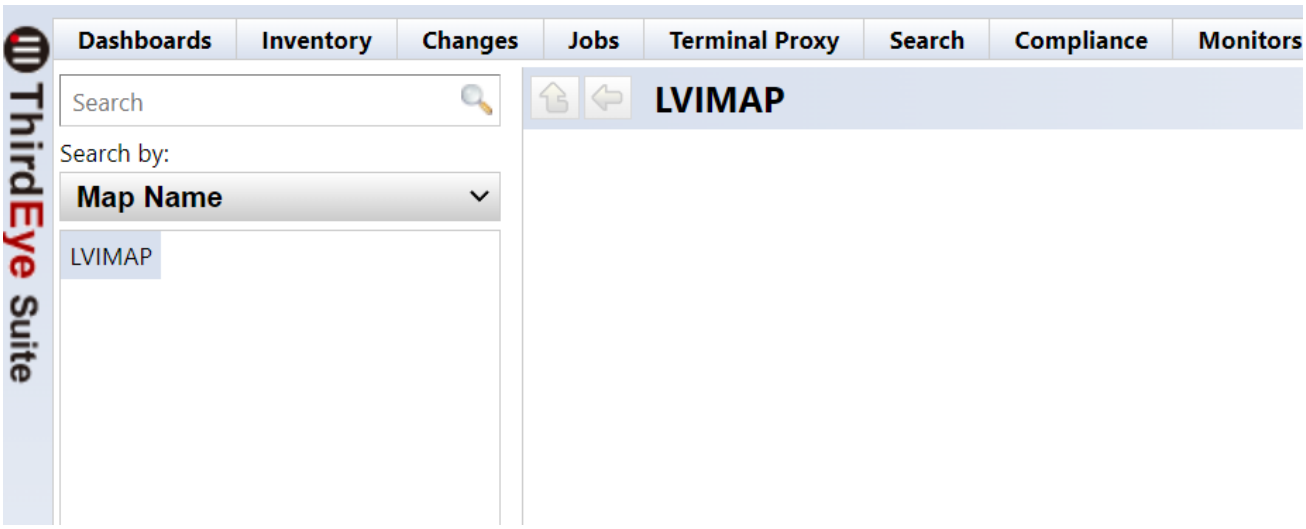
Note

If more than one Managed Network is visible, this screen will also include the option to explicitly select which Managed Networks the map is associated with.

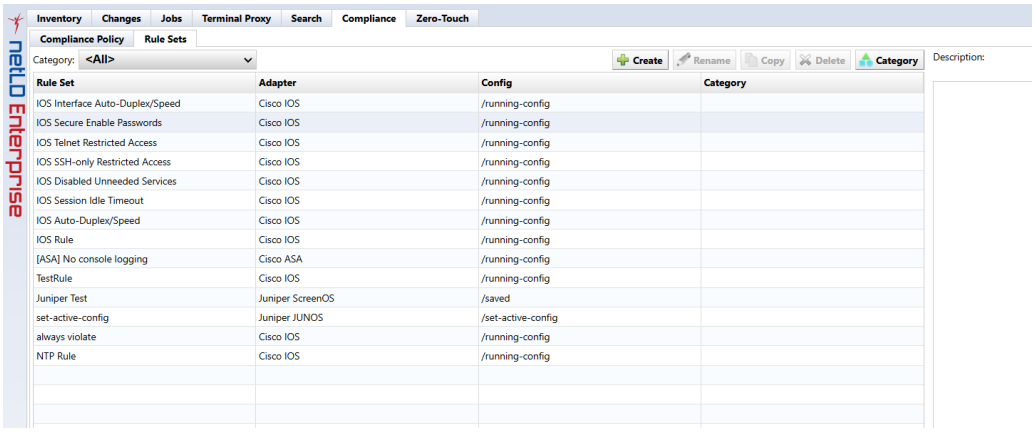
The selected Managed Network will impact which maps are visible to other users. For a user to have access to a map, they must have access to every Managed Network associated with the map.

When a map is created as a "child" of another map, the "child" map will not be associated with Managed Networks beyond that of the parent. If new Managed Networks are added, their parent map will be automatically updated to include them.

3. The saved map will be displayed in the "Map Name" list in the left sidebar.



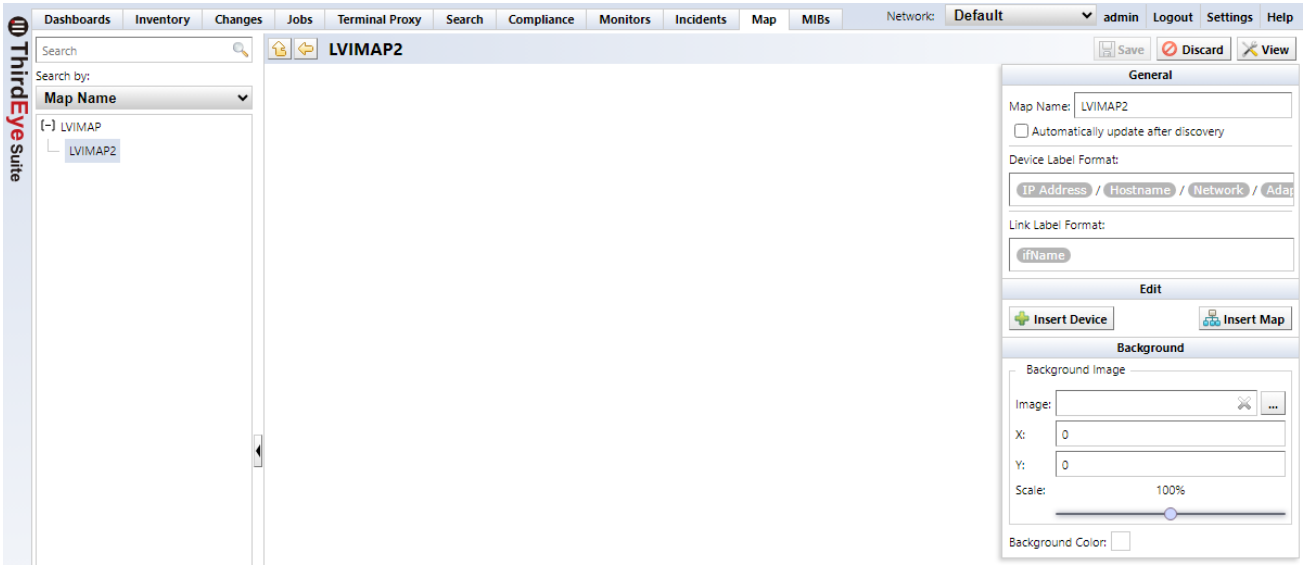
Clicking on a map in the map list in the “Map Name” left sidebar will create a new map below the selected map:



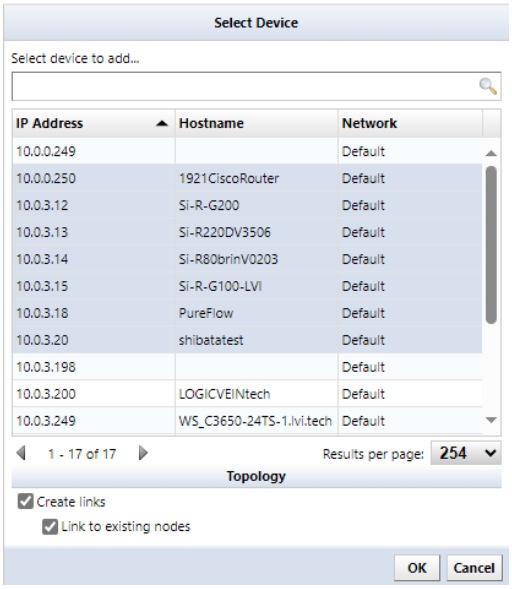
8.15.3 Insert a device into the map

1. To add a device to a map, doubleclick the map in the “Map Name” list in the left sidebar, and click [Edit].

2. Click [Insert Device] in the right sidebar.



3. Select the device you want to insert into the map and click [OK].

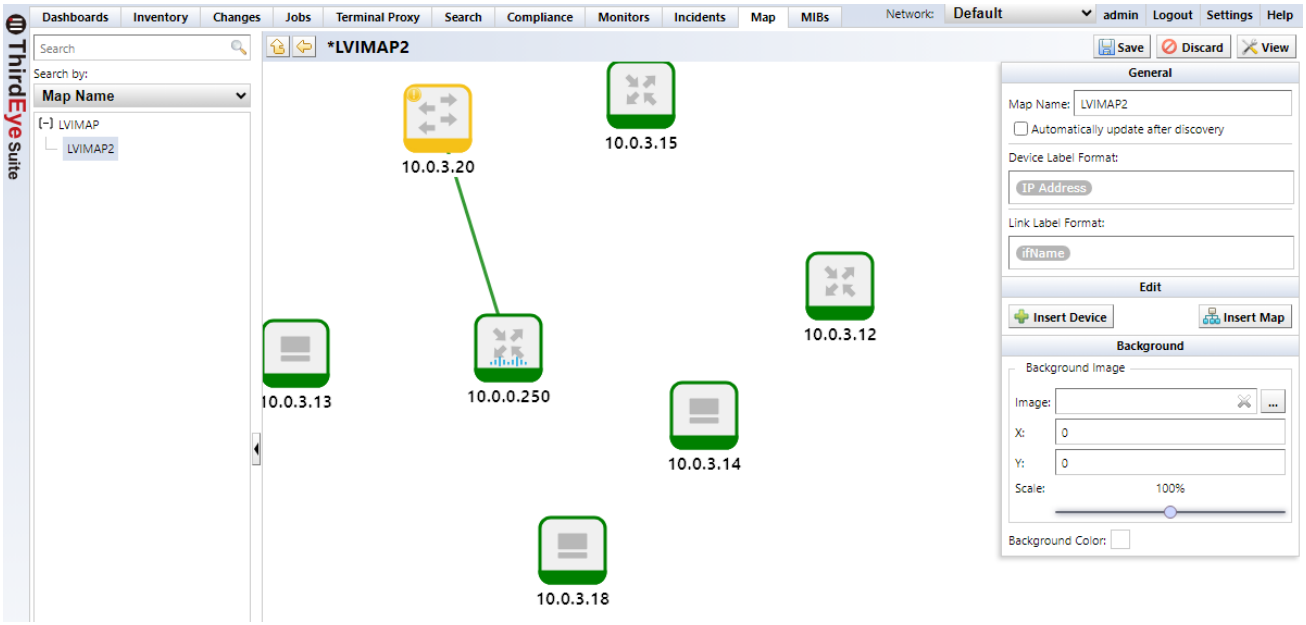


Note

When multiple Managed Networks are visible, the “Insert Device” dialog will only show selected devices visible in the Global Menu drop-down menu. This is regardless of the Networks setting for the current map.

When inserting a device into the Map from a Managed Network that is not already associated with the Map, the Map (and any parent maps) will need to be updated to include the additional Managed Networks.

4. After a device object is inserted, Click the  button.



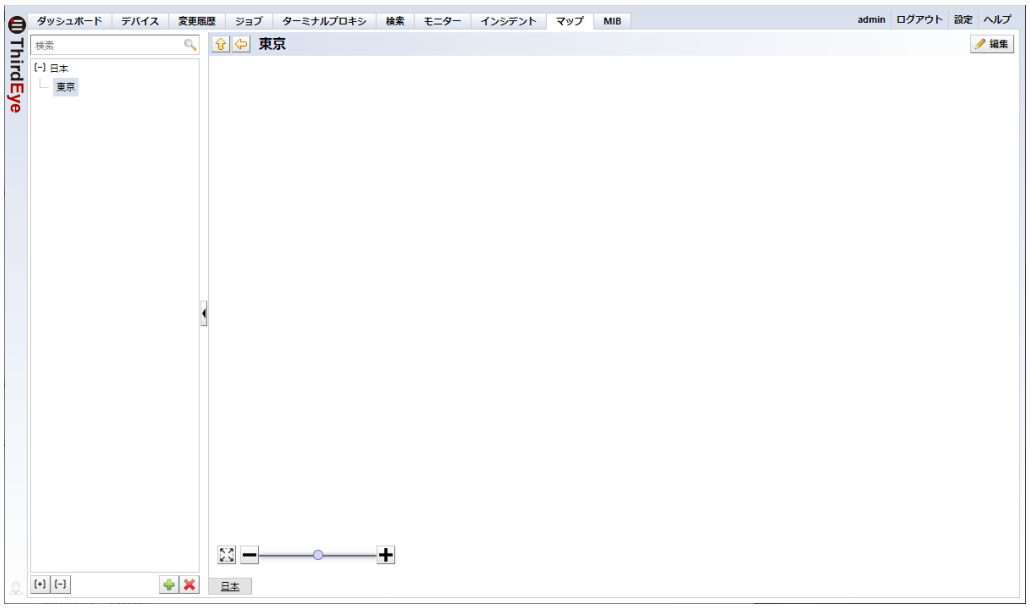
8.15.4 Create a topology map

From revision 20210730.0146, a function to automatically create L2 maps based on ARP/MAC address tableS, CDP, and LLDP information has been implemented. This information is obtained using SNMP when adding a device or updating device information.

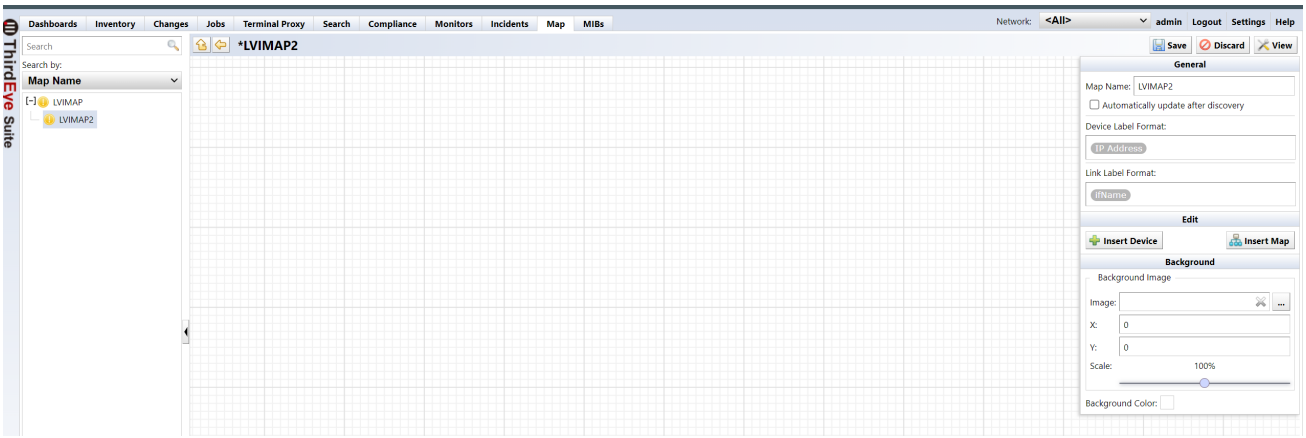
When using the topology function:

- It must be possible to retrieve information from the device using SNMP polling.
- Maps using the topology feature are created based on information at the time of information acquisition. The configuration information in the topology map is not always up-to-date.

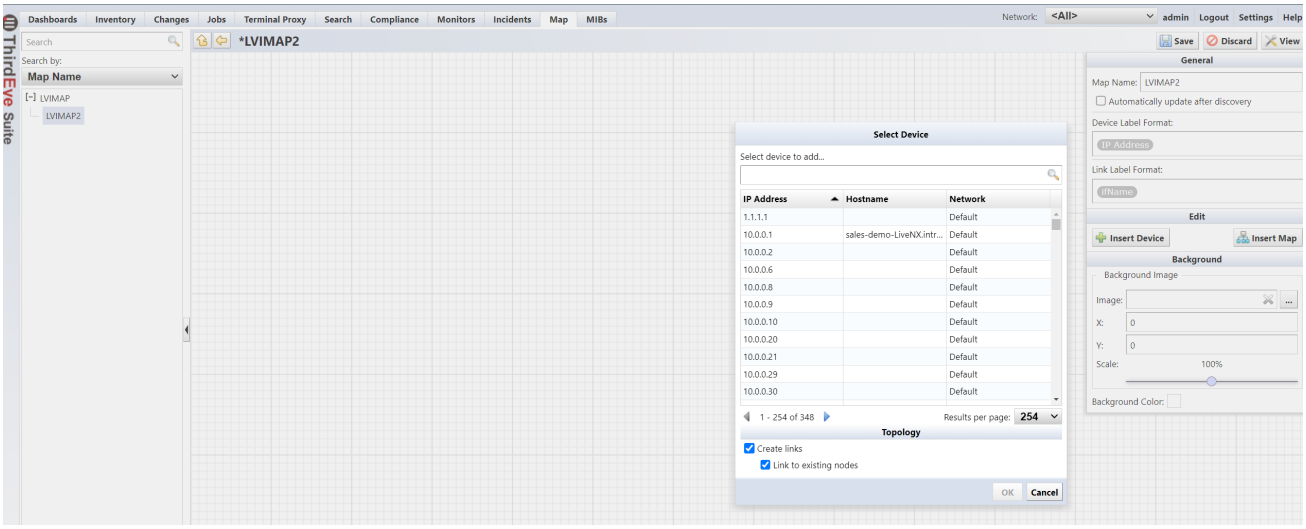
1. From the map list in the left panel, doubleclick the map to which you want to add a device, and click [Edit].



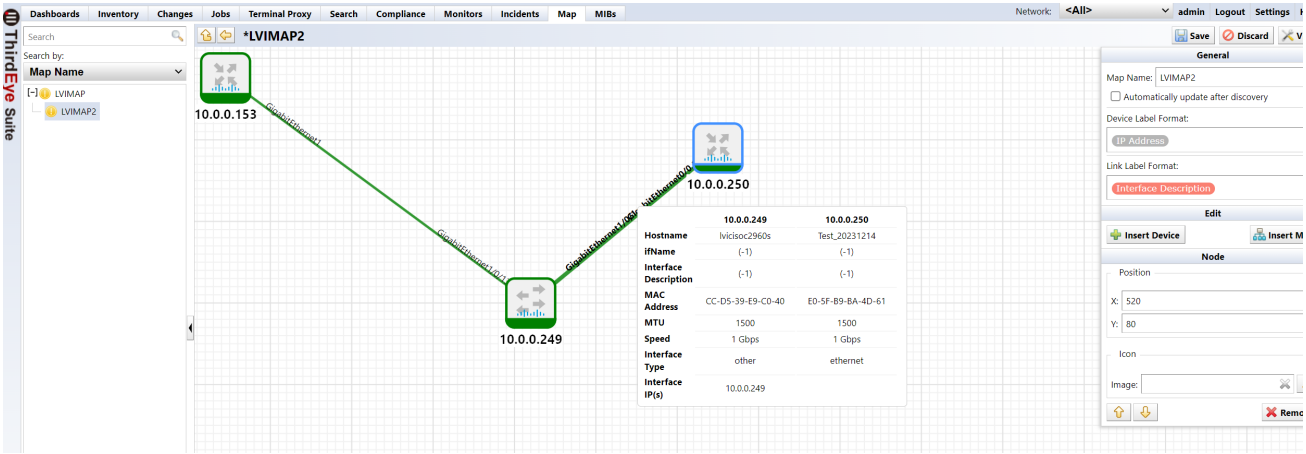
2. Click [Insert Device].



3. Select the device you want to insert into the map, check “Create link”, and click [OK].

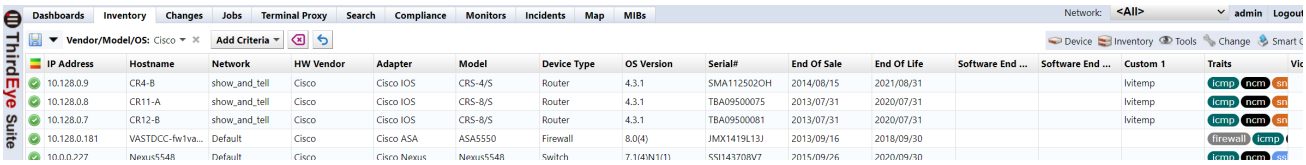


4. After the device object is inserted, click [Save] to complete your edits.

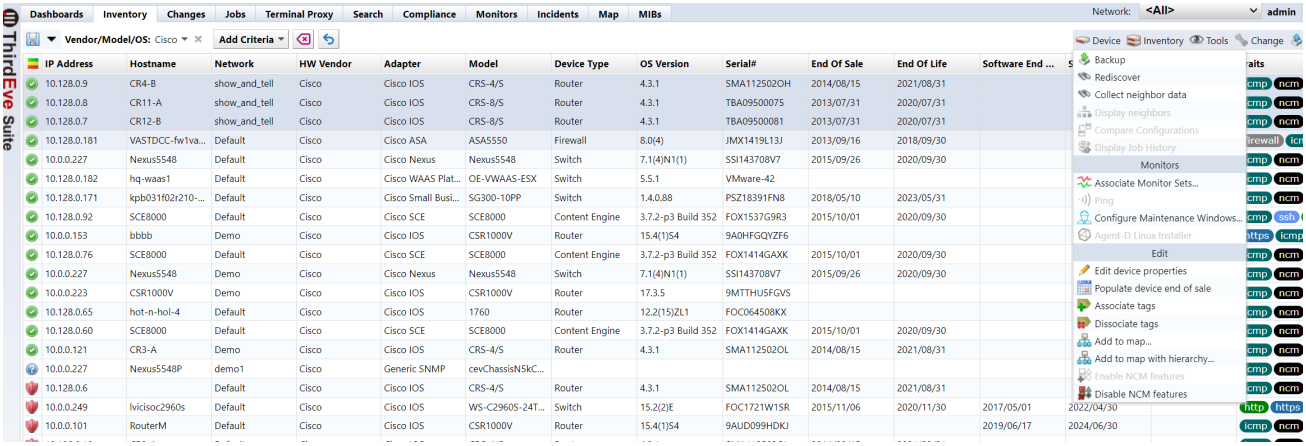


8.15.5 Create a location map with custom fields

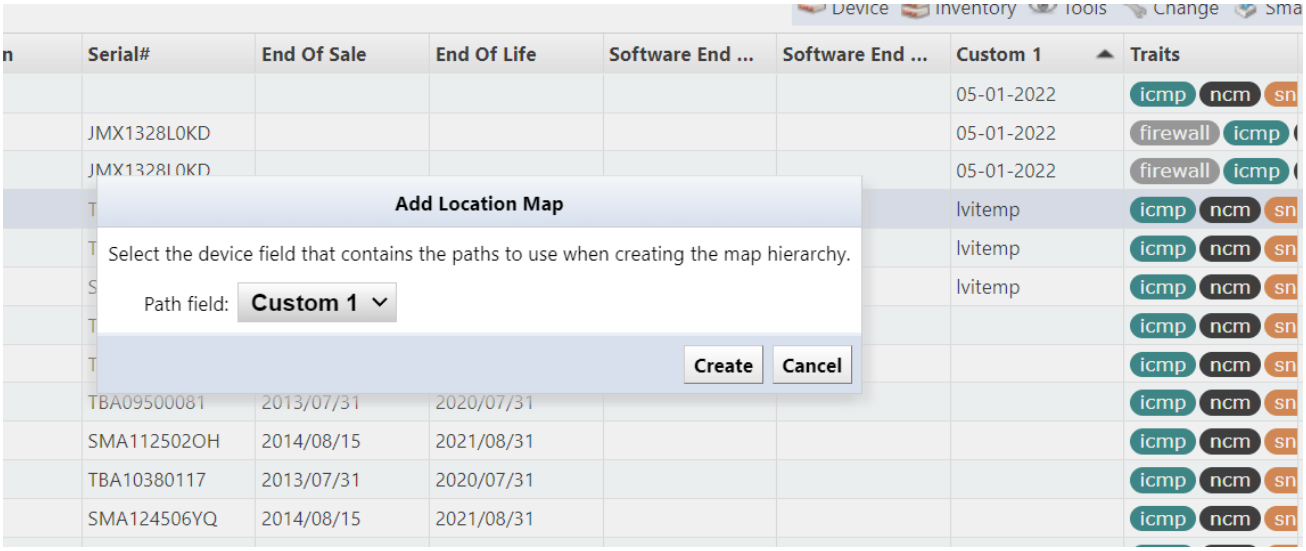
You can use information from custom fields to create maps. By selecting a device, you can create a location map for the selected device.



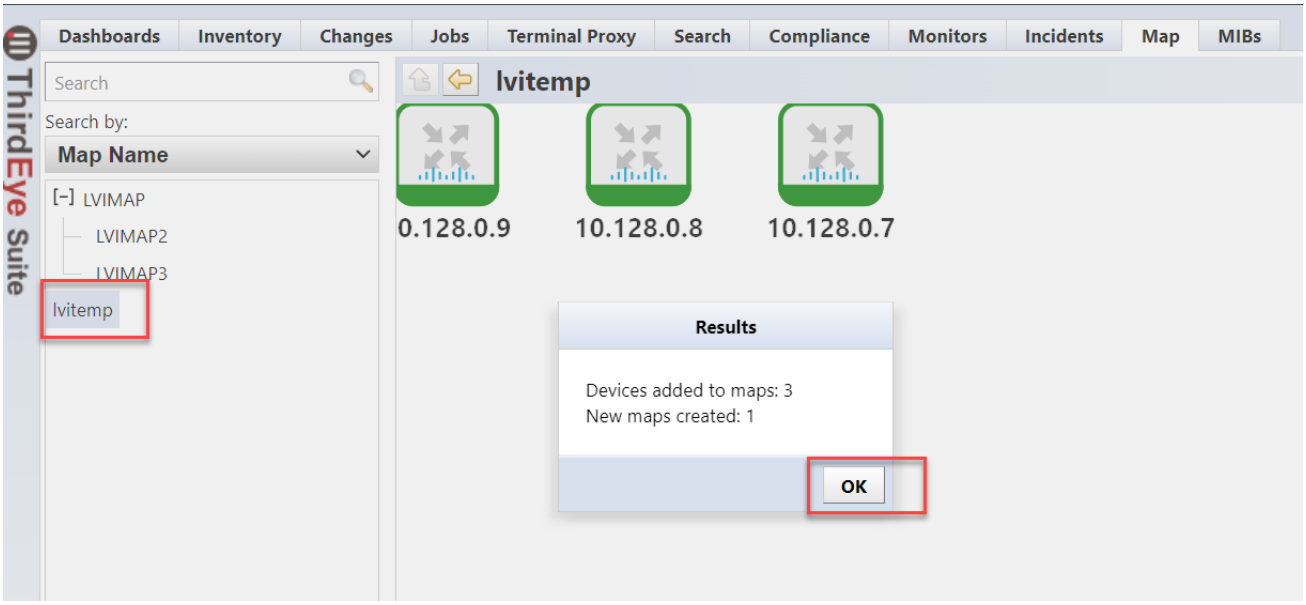
1. In the Inventory tab, click [Devices] in the right panel, then click [Add to map].



2. Select a custom field and click [Create].



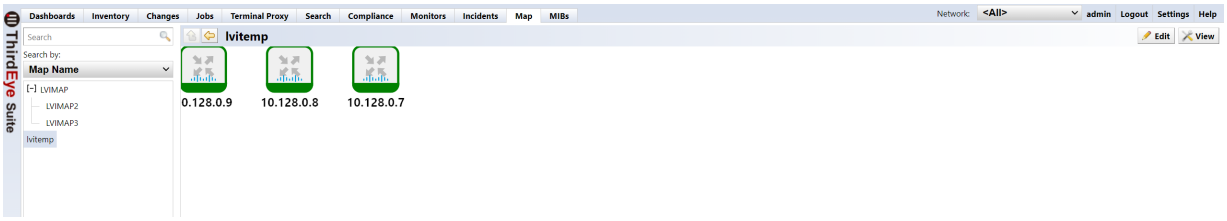
3. Click [OK].



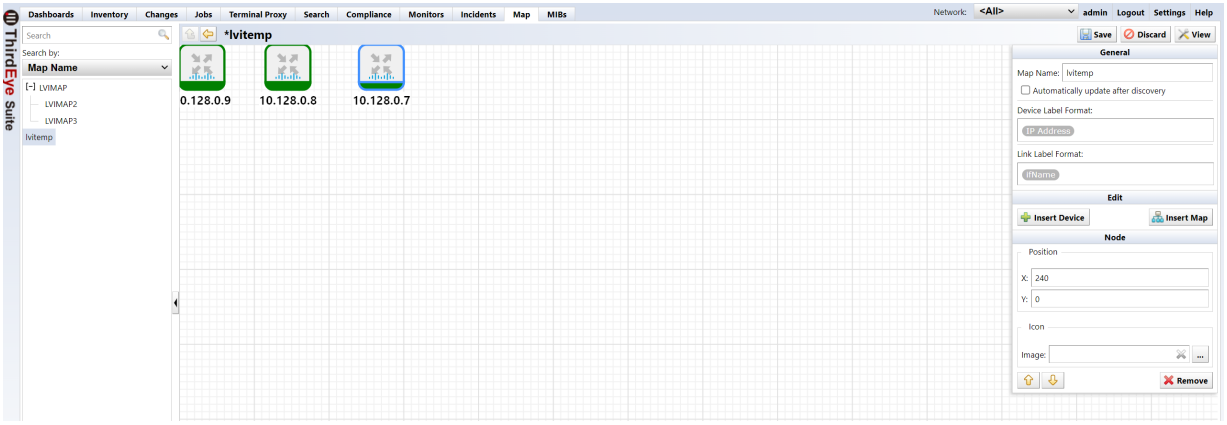
8.15.6 Set object icon

You can change the icon of an object.

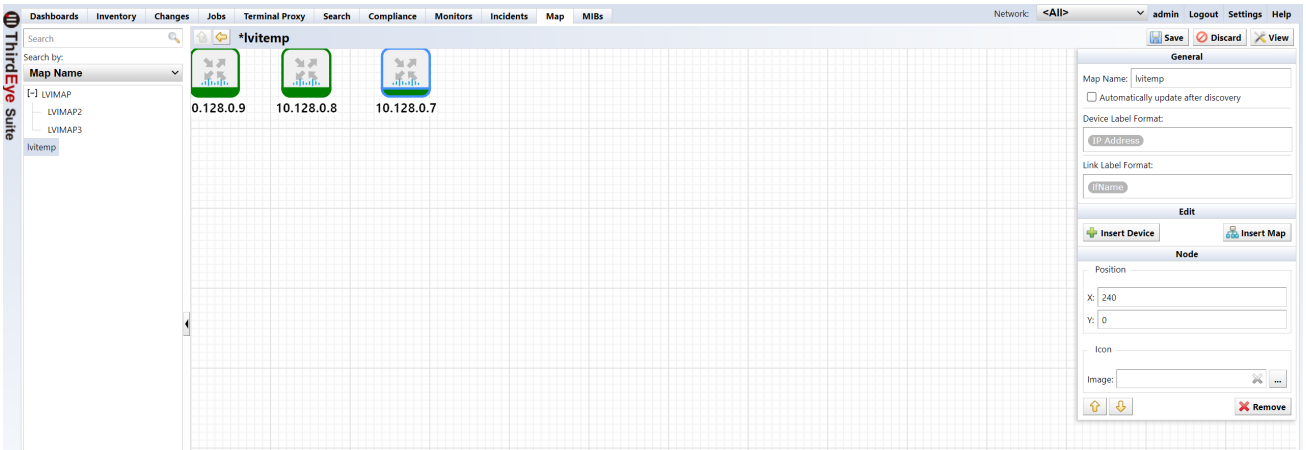
1. Doubleclick the map to open it, and click [Edit].



2. Select the object for which you want to set an icon.

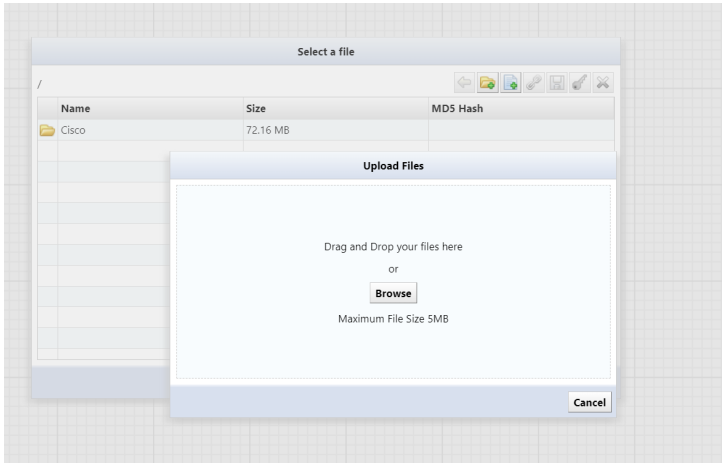


3. In the Map tab, the “General” window is located in right sidebar. From the edit menu, click the […] button in bottom of the [Image].

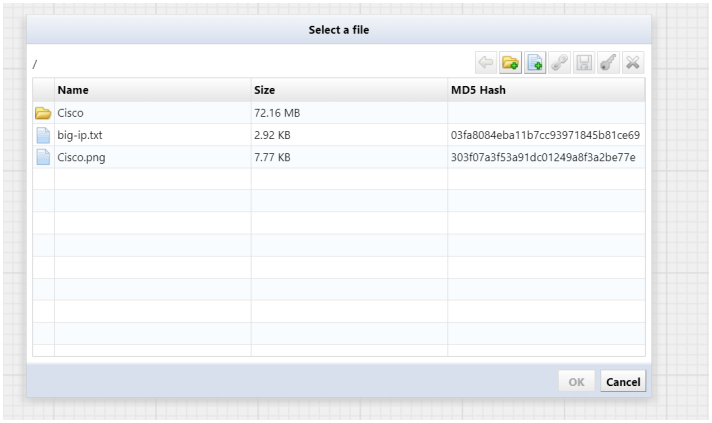


4. A file selection screen will be displayed.

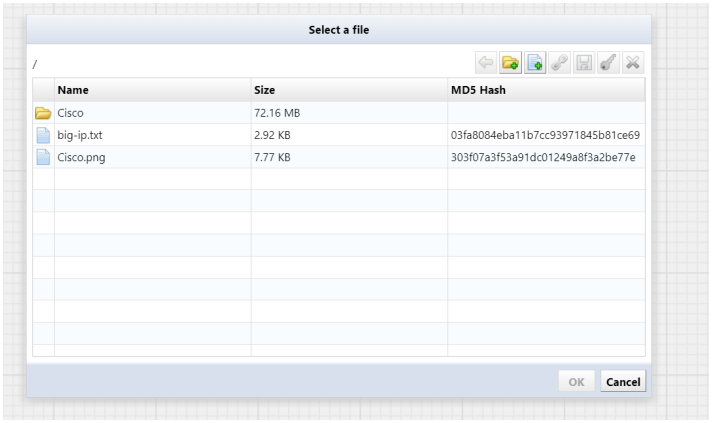
Click the  button, and upload the file.



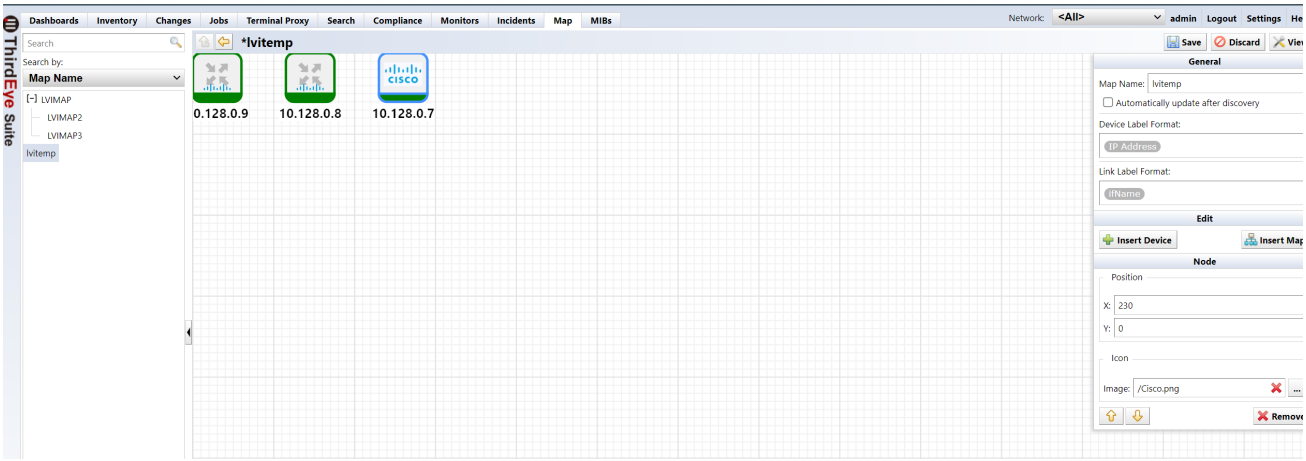
5. Select the icon you want to upload.



6. Select the file you want to set as the icon image and click [OK].



The object’s icon will change to the selected image.

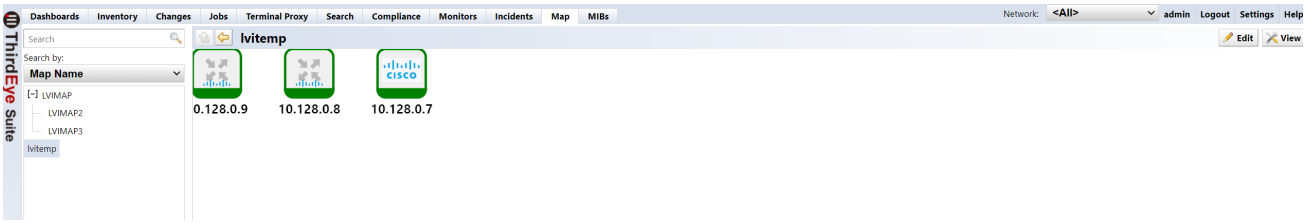


8.15.7 Connect two objects with a line

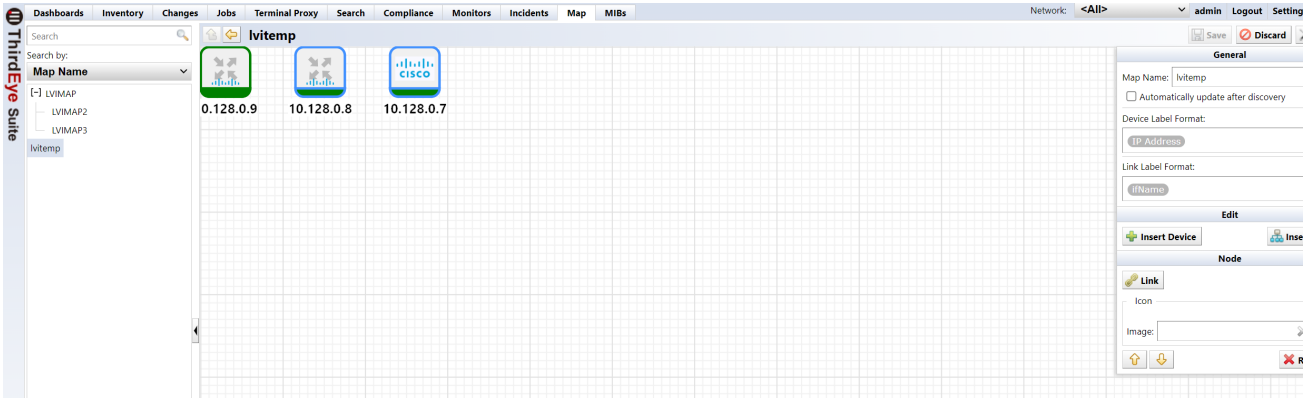
You can connect objects such as maps and devices with Link Lines.

The thickness of the Link Line cannot be changed.

1. Doubleclick the map to open it, and click [Edit].

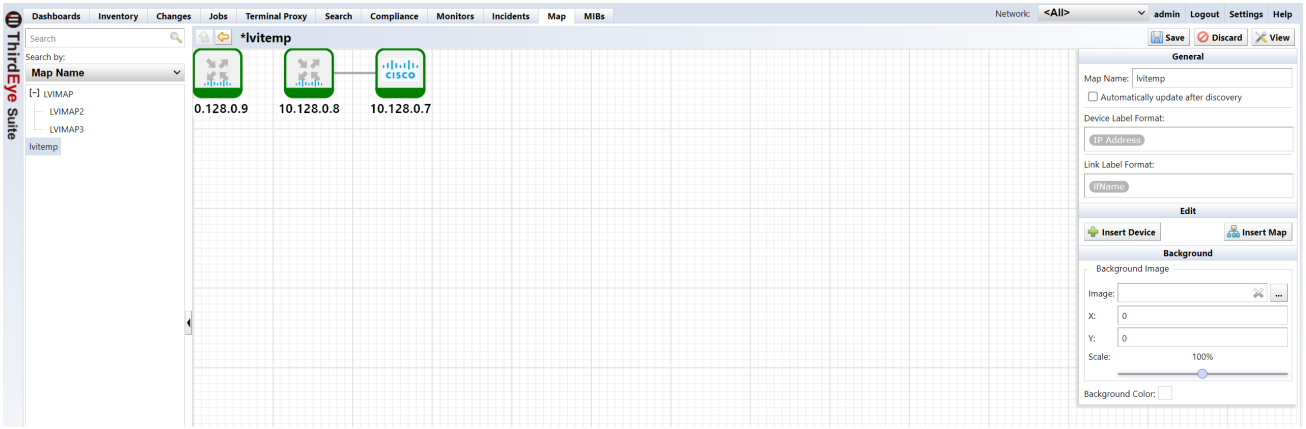


2. To select the devices, hold the [Ctrl] key on your keyboard, and click the two devices you want to connect with the Link Line. With the devices selected, click [Insert Link Line].



3. Once the Link Line is inserted, click [Save].

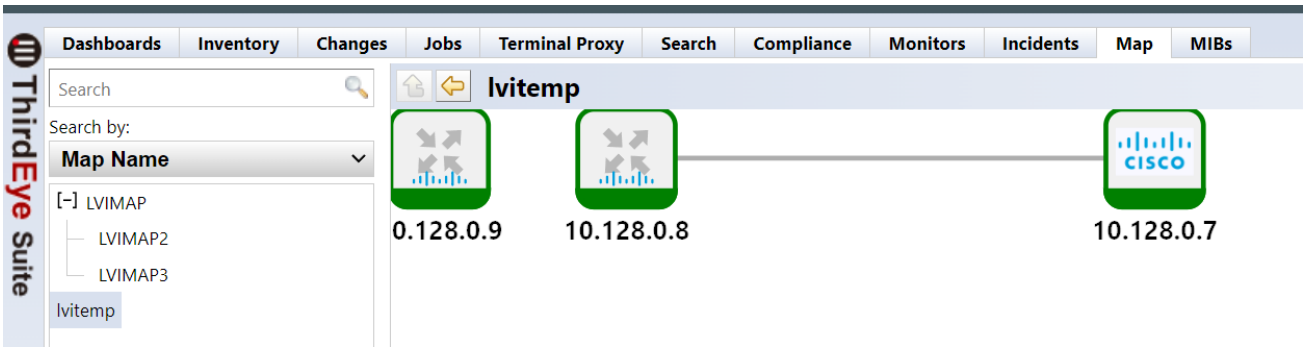
If you want to delete the Link Line, select the two devices and click [Delete link line]



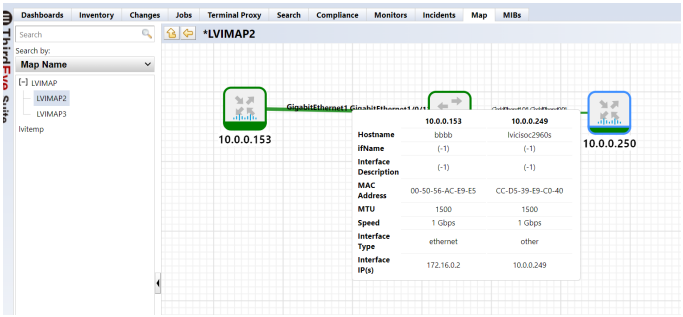
8.15.8 Attach an interface to a link line

From revision 20210730.0146, you can attach a device interface to a Link Line. By associating a device interface with a Link Line, when a failure (such as a LinkDown trap or a traffic threshold exceeded) occurs on that device interface, an item is added to the device object depending on the severity of the failure event. The color of the Link Line will change.

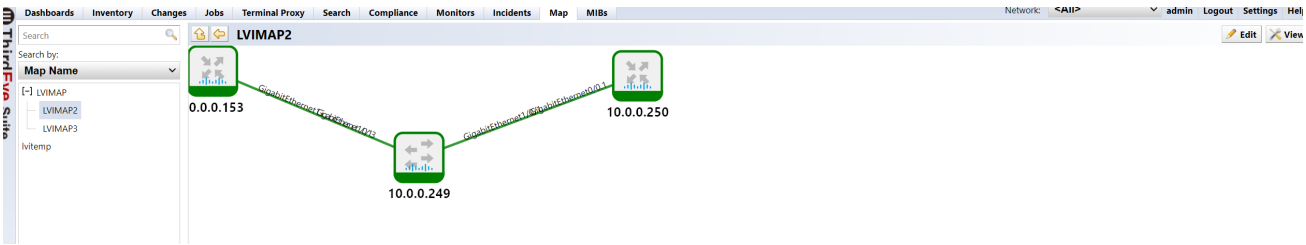
Example of status when device interface is not linked to the Link Line:



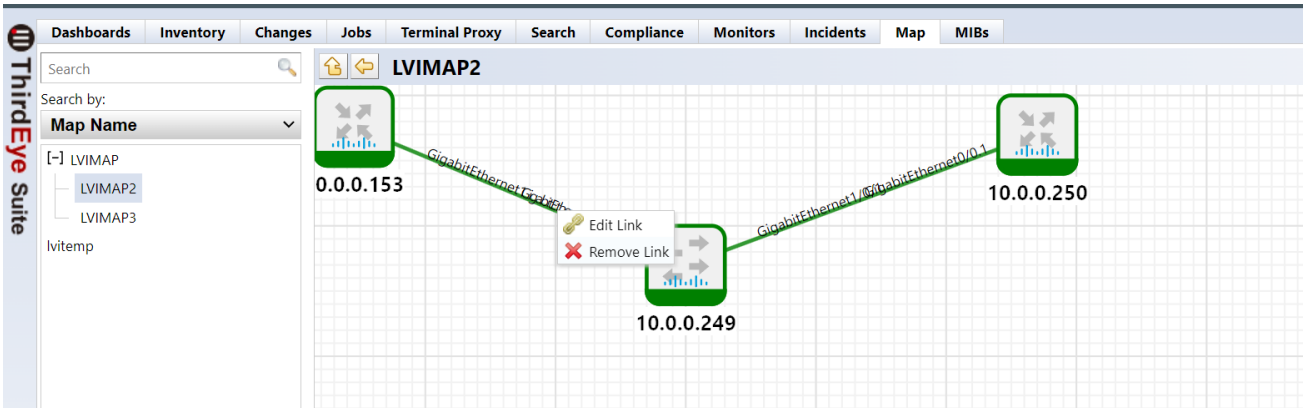
Example of status when device interface is linked to the link line:



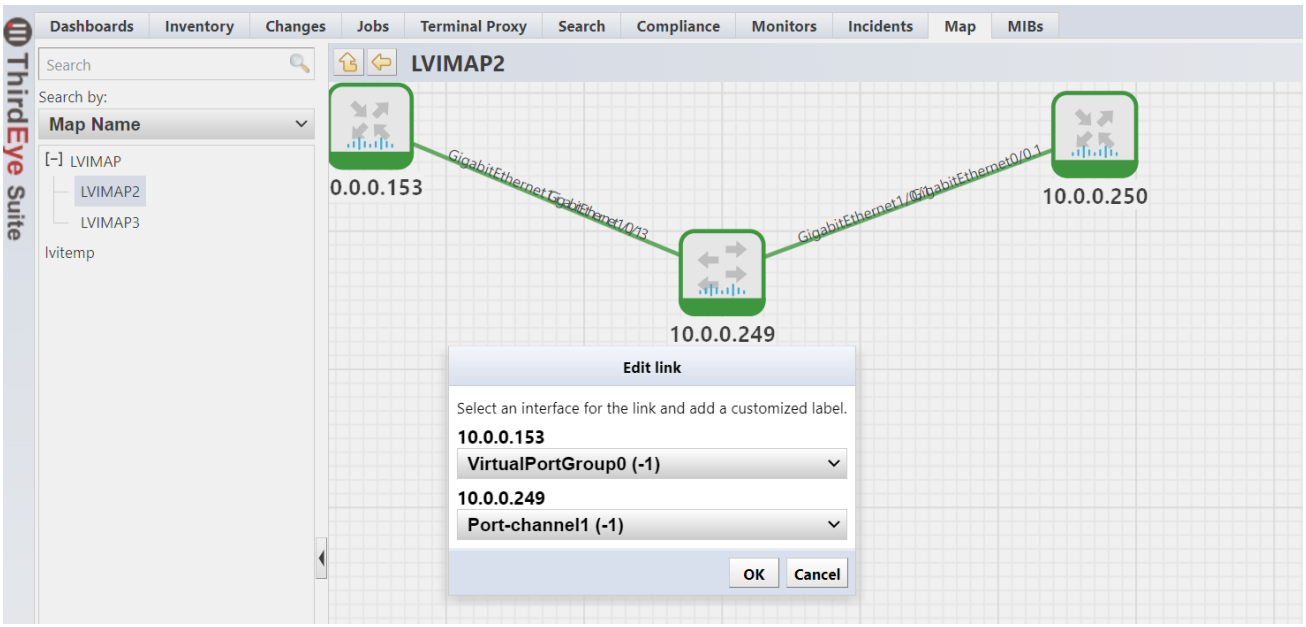
1. Doubleclick the Map to open it and click [Edit].



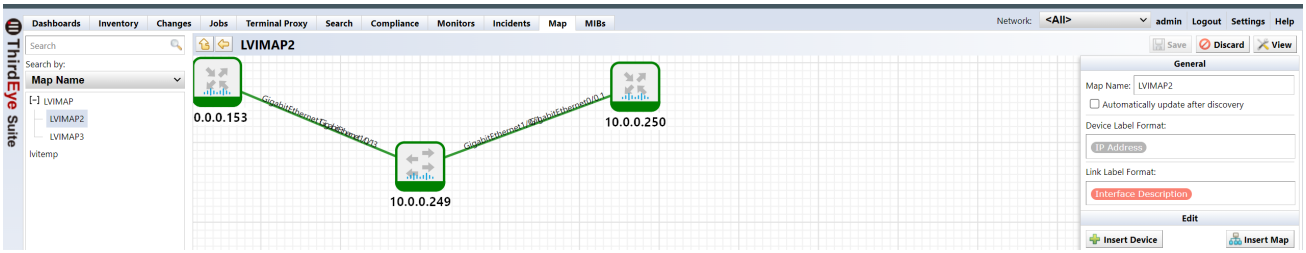
2. Right-click the Link Line, and click [Edit Link Line].



3. Select an interface from the [Edit Link] pull down menu for the device, and click [OK].

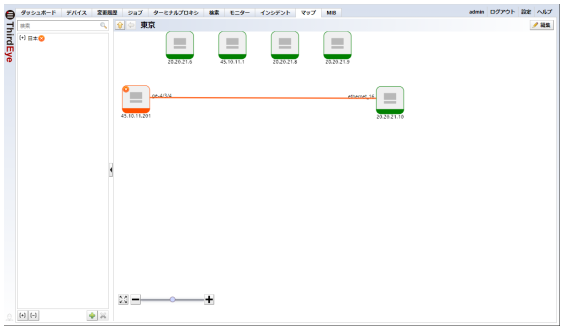


4. Click [Save].



This completes the linking between the Link Line and the interface.

When a violation occurs on the associated device's interface, the color of the Link Line and device object change.

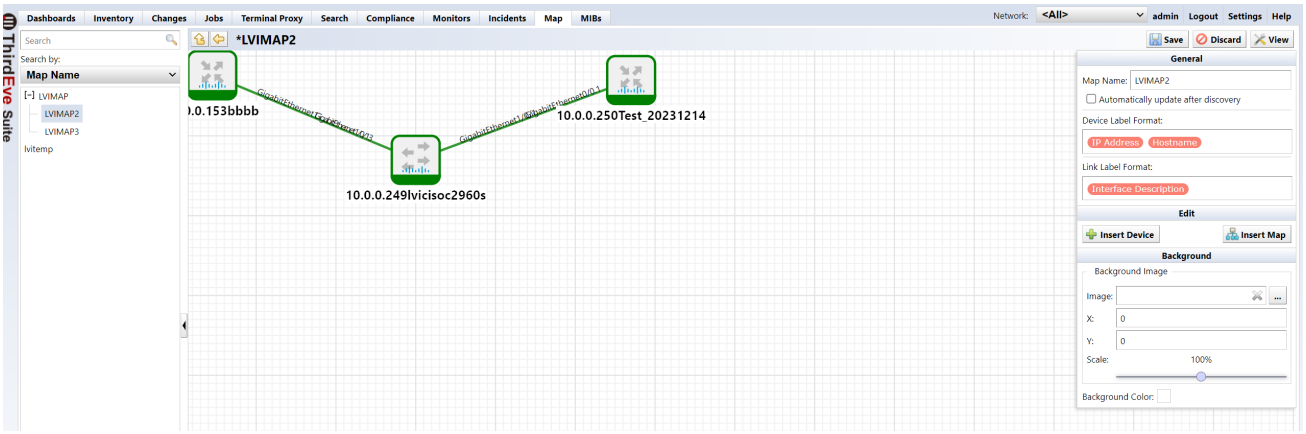


8.15.9 Setting the display format of icon labels and link lines

You can customize the display format of the strings (labels). You can also customize the evice objects Link Lines for each map.

1. Doubleclick the map, and click [Edit].
2. In the “General” right sidebar, change the settings for [Device label format] and [Link line label format].

You can specify any string.



The objects available for each label format are shown in the table below.

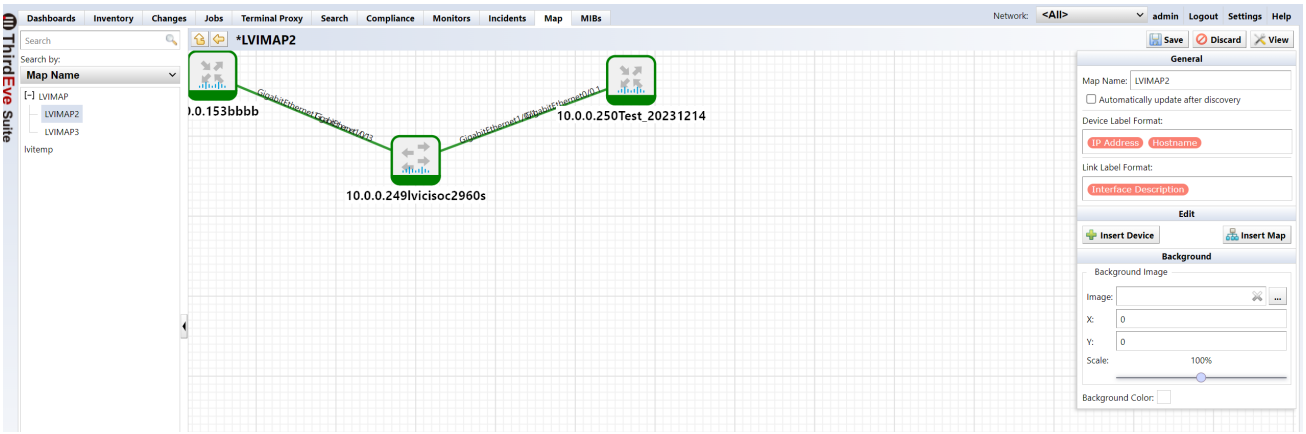
Device label format

Menu Item	Explanation
IP address	Display the device’s IP address. (initial value)
hostname	Display the device hostname.
network	View your device’s network.
adapter	Show device adapters.
device type	Display the device type of a device.
hard bender	Display the device’s hardware vendor.
software vendor	Display the device’s software vendor.
OS version	Display the device OS version.
Model	Display the device model.
Serial number	Display the device serial number.
custom 1	Display custom 1 information for the device.
custom 2	Display custom 2 information for the device.
custom 3	Display custom 3 information for a device.
custom 4	Display custom 4 information for a device.
custom 5	Display custom 5 information for a device.
new line	Insert line breaks in labels.

Link Line label format

Menu Item	Explanation
ifName	Display the value of ifName. (initial value)
Interface Index	Display ifIndex.
Interface Description	Display ifDescr.
MTU	Display ifMtu.
Speed	Display ifSpeed.
Mac Address	Display ifPhysAddress.
new line	Insert line breaks in labels.

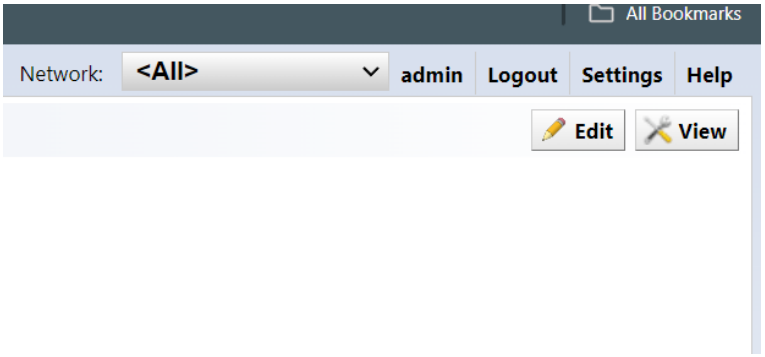
3. Click [Save].



8.15.10 Change the default device label format for maps

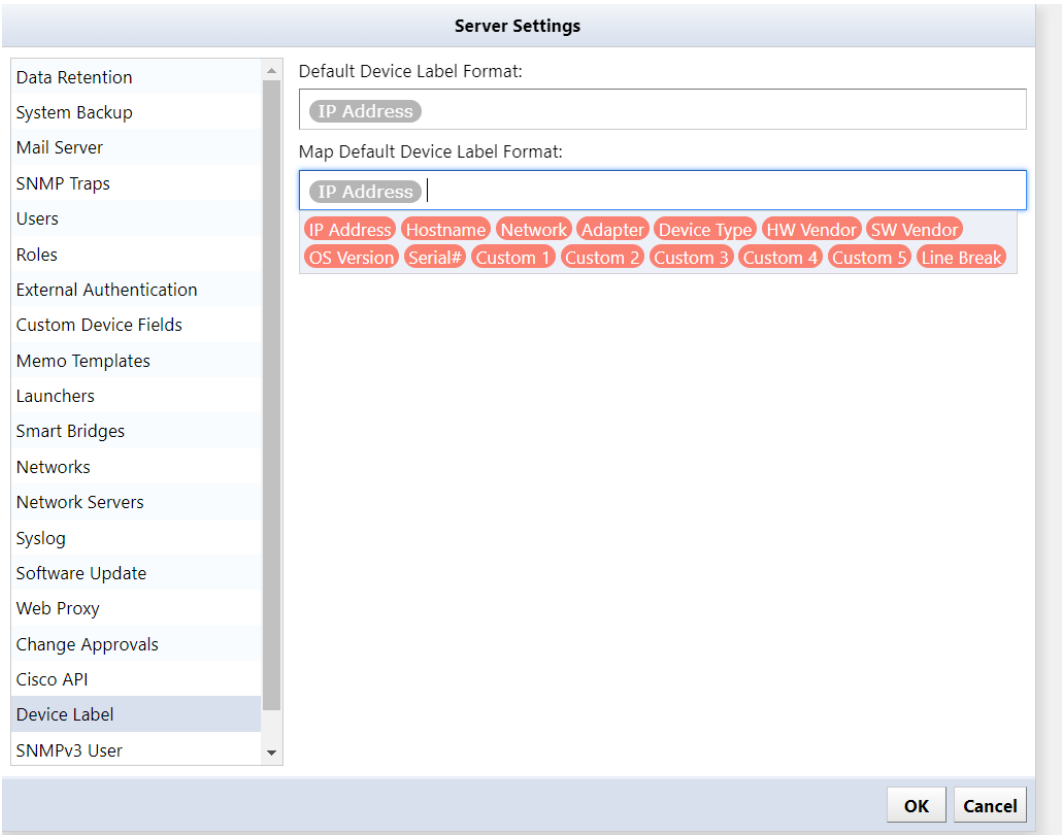
You can specify the default device label format when creating a new map. Maps will automatically reflect any changes in the settings. Changes will not be reflected in previously created maps.

1. Click Settings on the Global Menu.



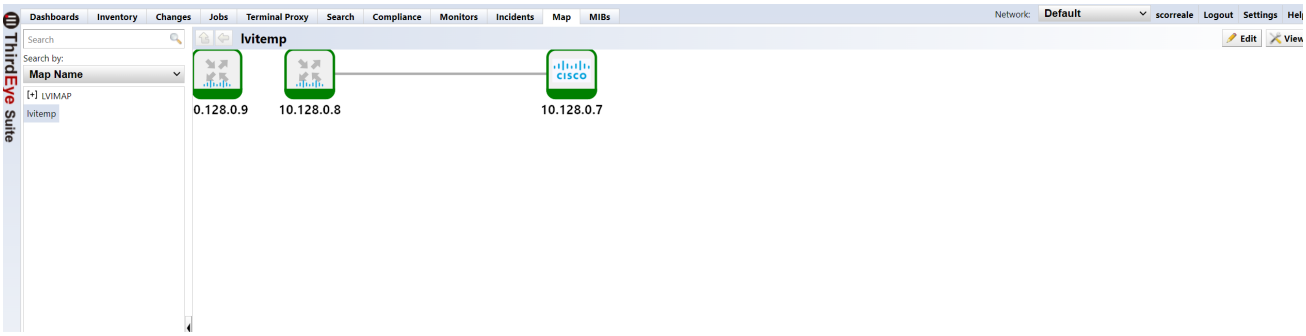
2. Click [Label Format] and set the label format to “Default Device Label Format for Maps”.

The gray default “IP address” is used for the “Default Device Label Format”. It is the default label format of the Live Ping feature and Maps.

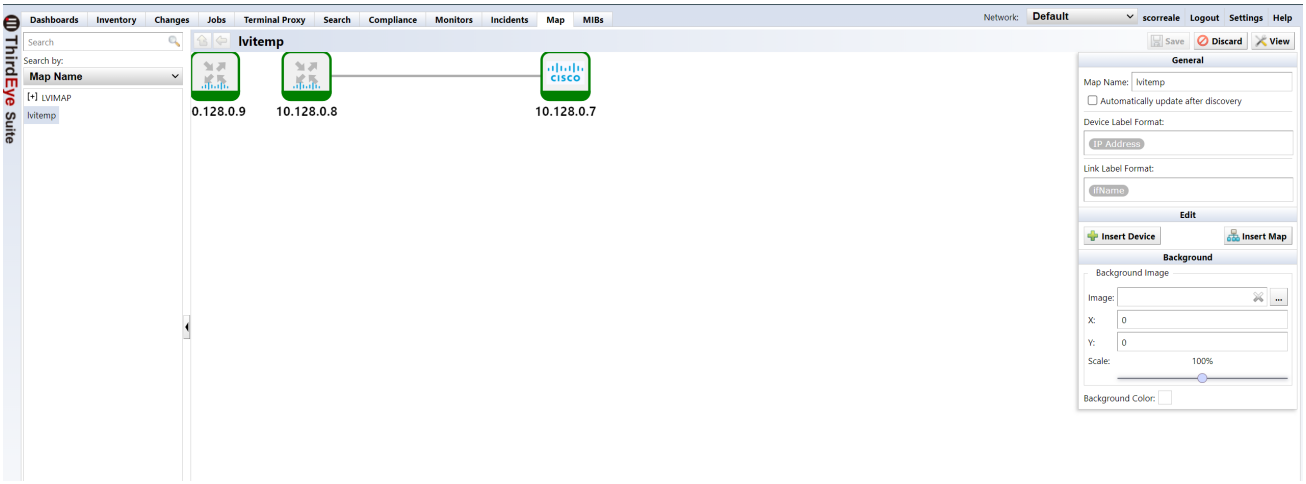


8.15.11 Set the map background image

1. Doubleclick the map to open it and click [Edit].

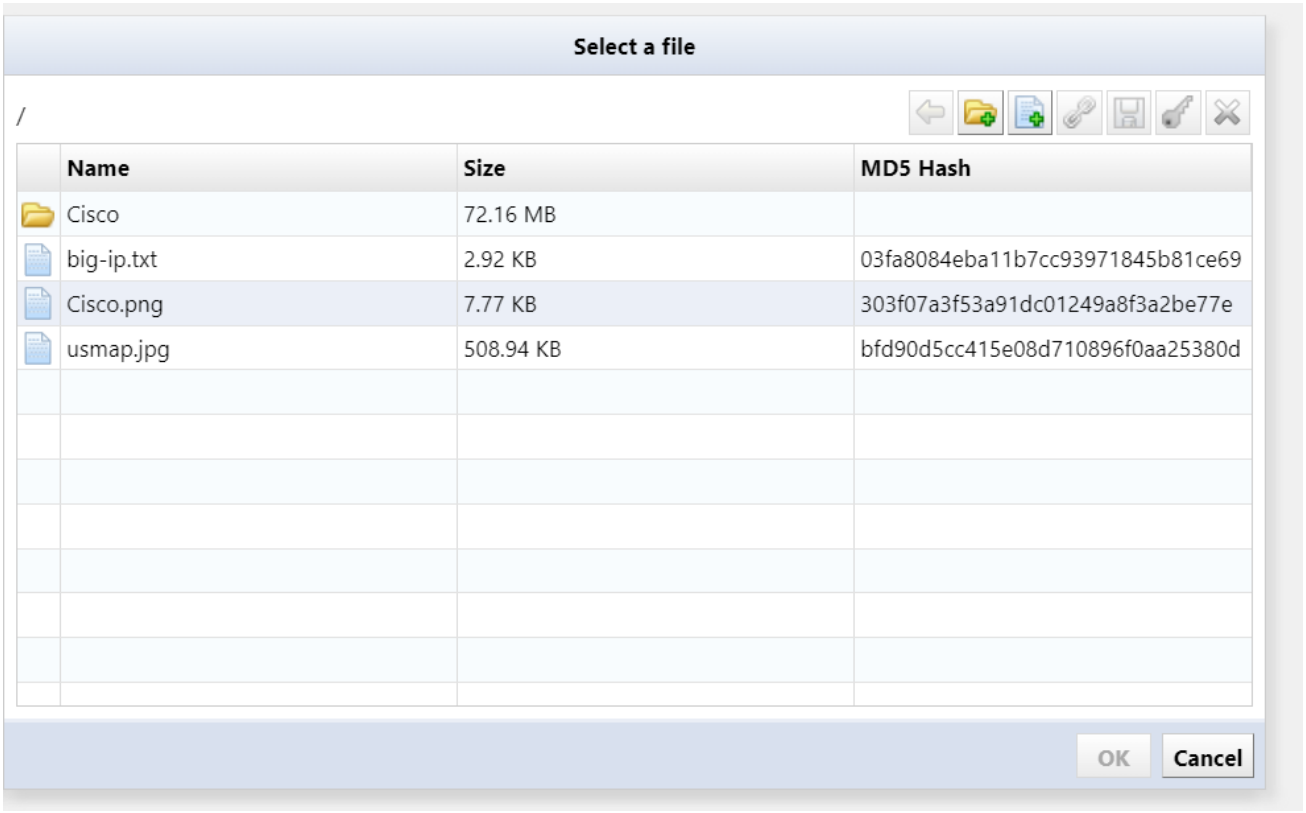


2. In the Map tab, the “Background” options are located in the bottom of the right sidebar. Click the […] button to the right of the [Image] field.



A file selection screen will be displayed.

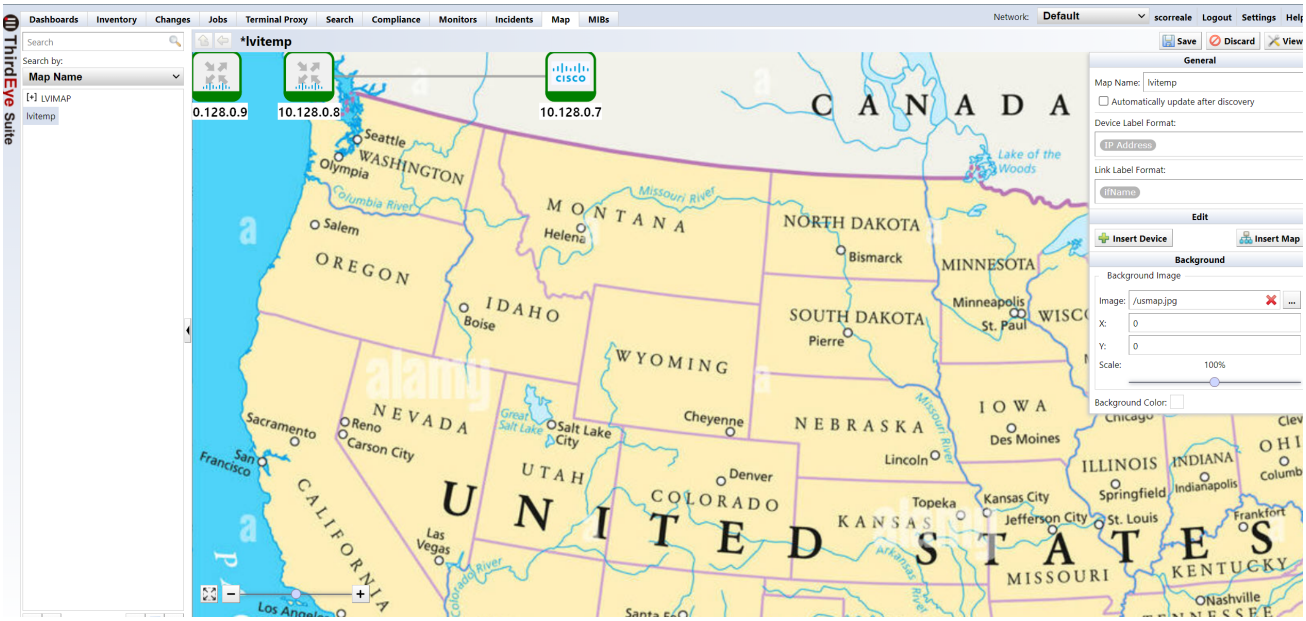
3. Select the file you want to set as the background image and click [OK].



Note

Client files can be uploaded to the ThirdEye server. Click the button to display the client-side file selection dialog. Then select the file to upload and click [Open].

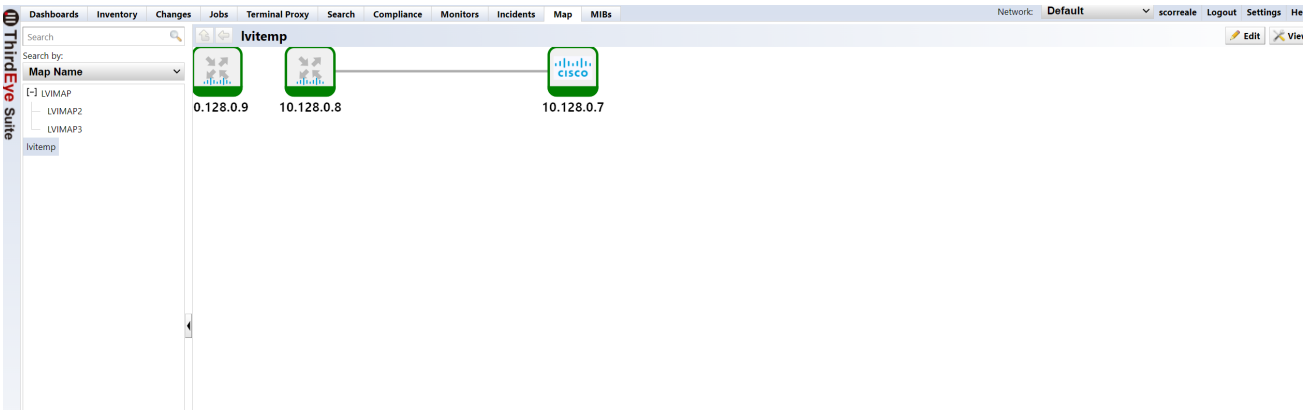
4. Click [Save] to complete your edits.



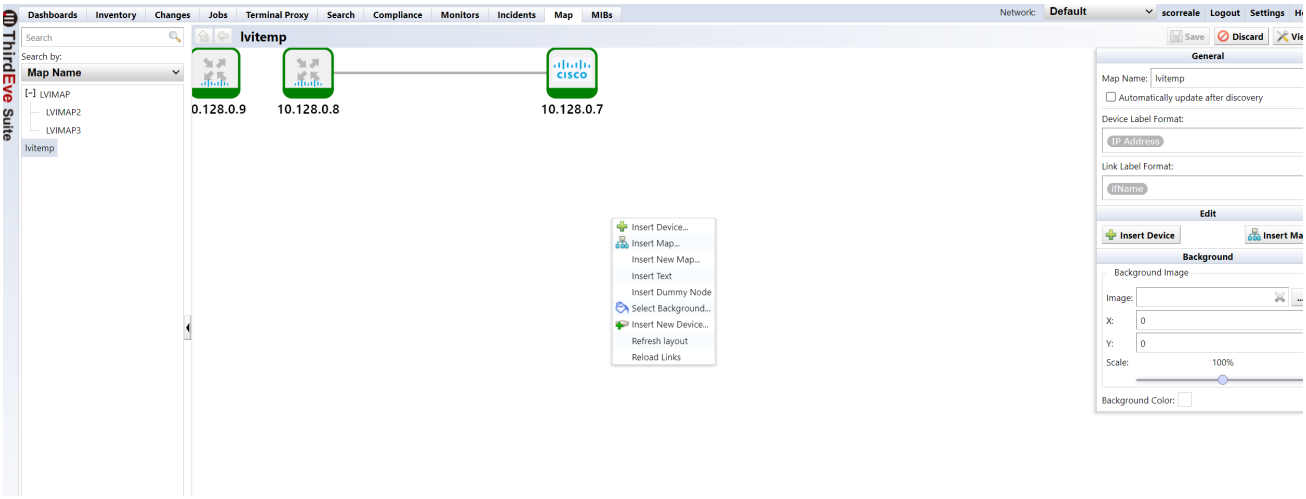
8.15.12 Set up the map tree

You can insert a Map as a child of another map, and display them in a tree structure,

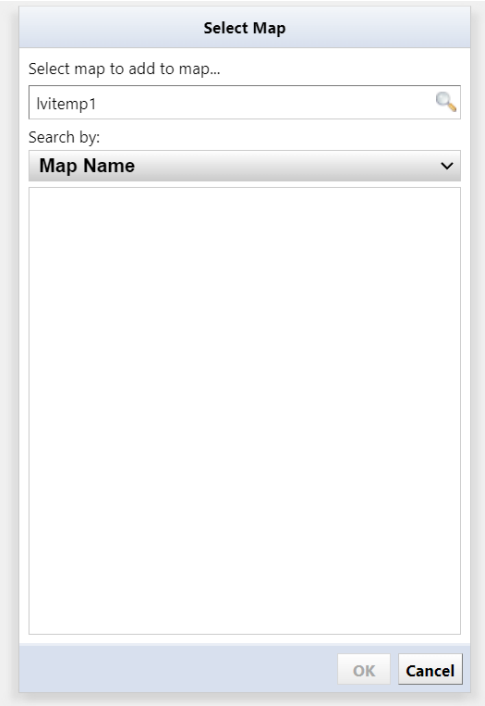
1. From the Map list on the left side of the screen, doubleclick the desired parent Map, and click [Edit].



2. Right click on the Map screen, and select [Insert Map] from the right-click menu.

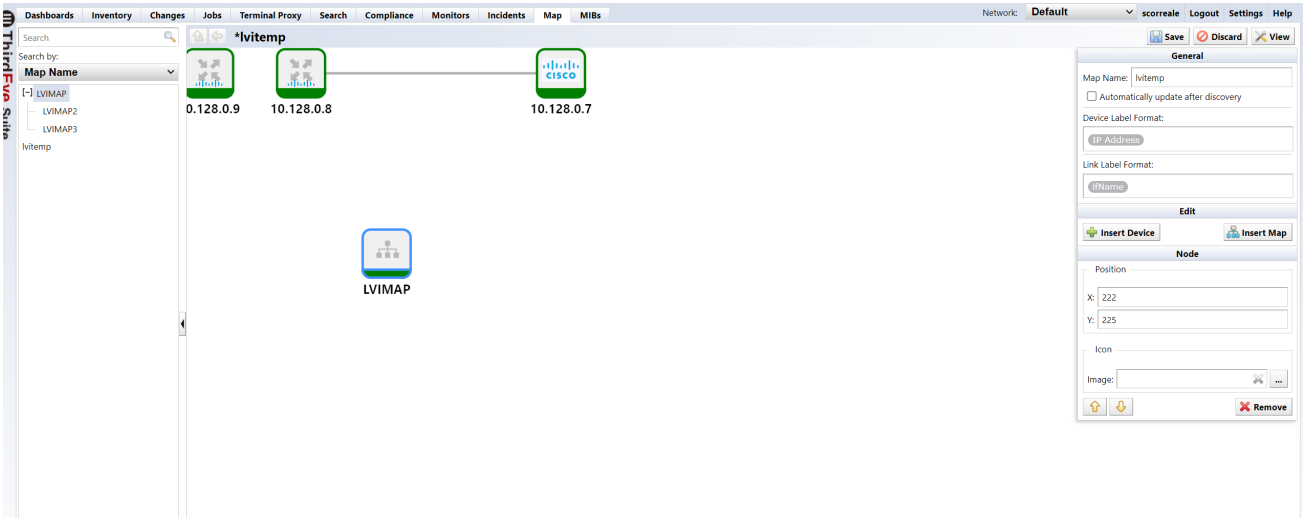


3. Select the map you want to insert as a child and click [OK].



If the selected Map is not associated with any other Maps in the Managed Networks, the Maps in Managed Networks will need to be updated.

4. After the child Map is inserted, click [Save].

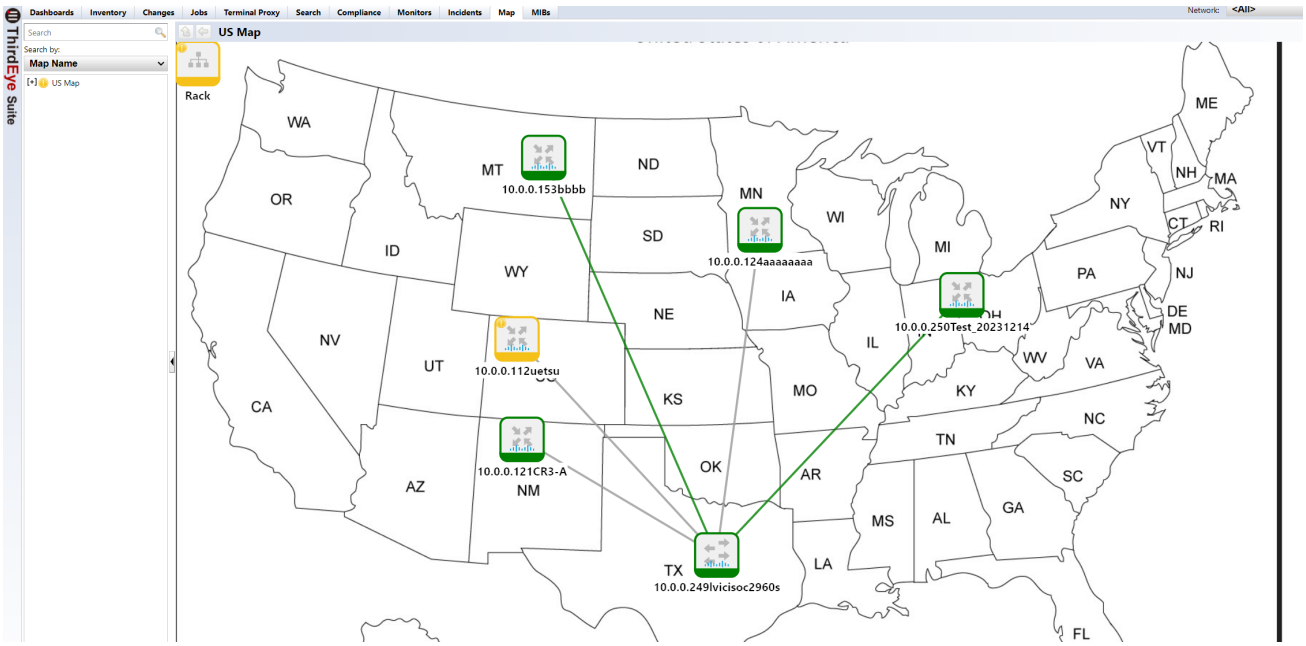


Once the child is added, it will be viewable in a tree view in the left sidebar. You can expand or collapse the tree by clicking the [+] or [-] symbols to the left of the map name.

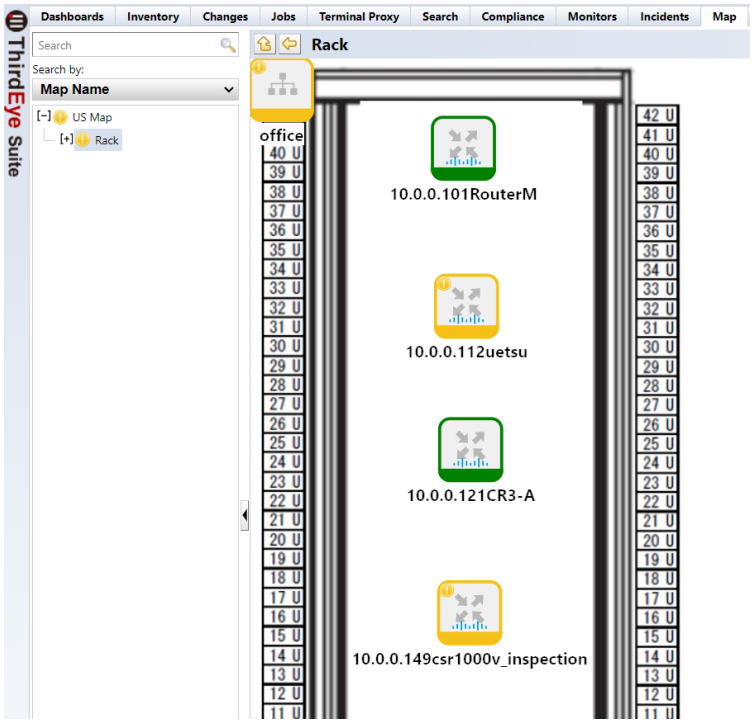
8.15.13 Troubleshooting using Maps

8.15.14 Checking failed devices

When a device failure is detected, the border color of the object on the map changes to match the severity level set on the monitor. A status icon indicating the severity level is then displayed in the upper left of the object. When the status of an object lower in the hierarchy changes, the change is reflected in Map Objects higher in the hierarchy. This behavior is the same for maps registered as widgets on the dashboard.

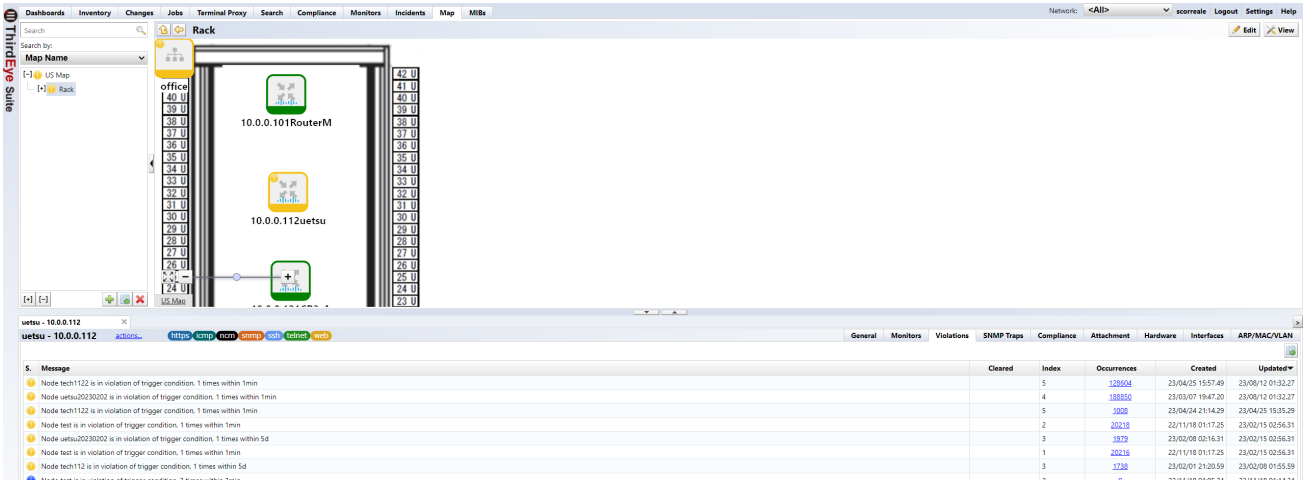


Doubleclick a Map Object to move to a lower level. You can also display the desired map by using the Map Tree.



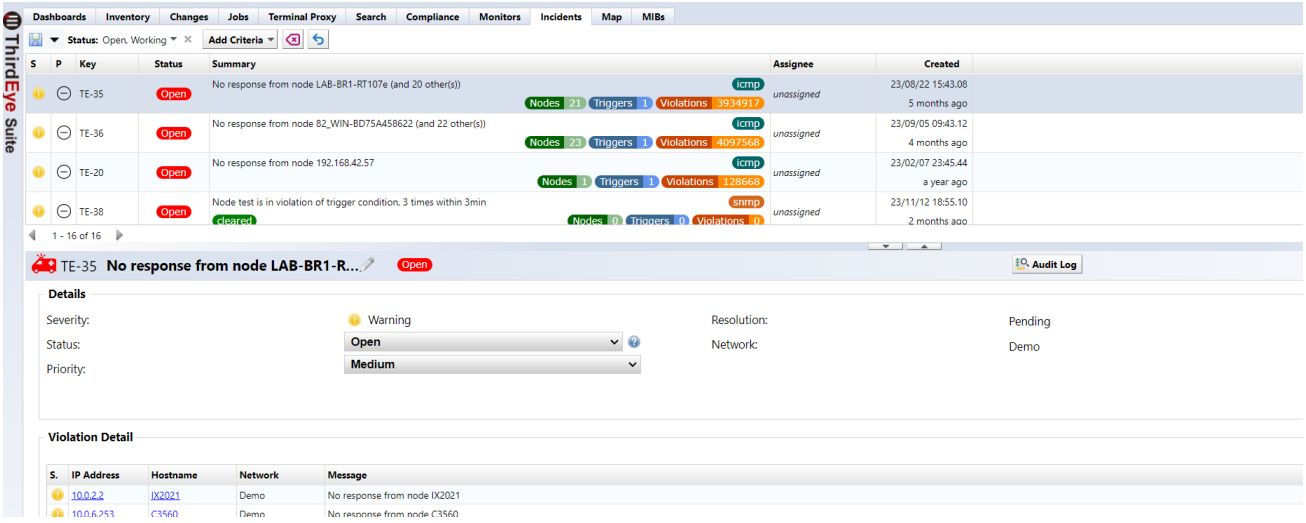
8.15.15 Check the details of the problem

Once you have identified the location of the problem, doubleclick the failed device to display the [Device Details] for more details about the problem. On the [Device Details] > [Violations] screen, you can check the failures that have occurred in the device.



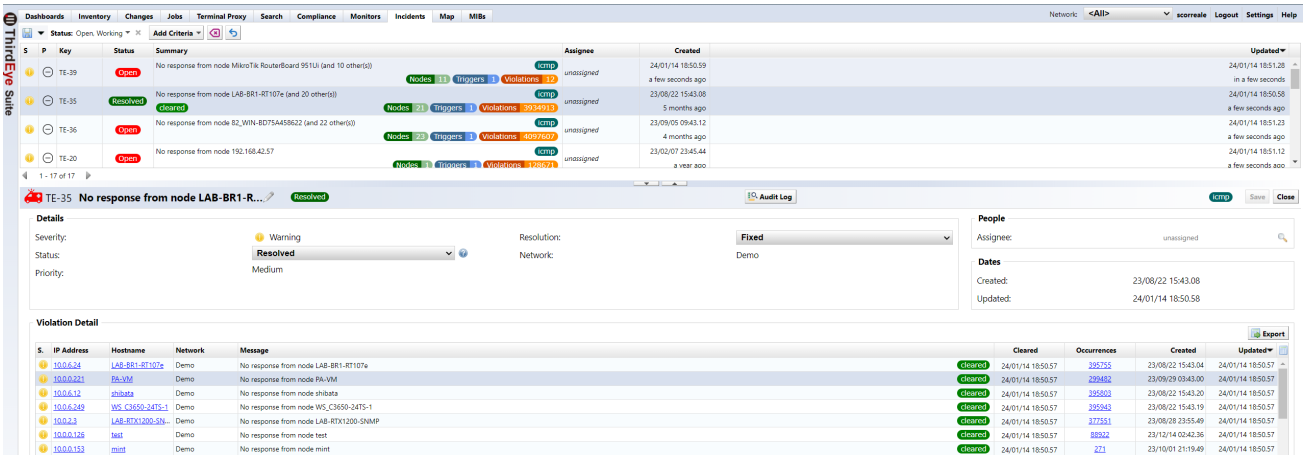
You can check the details of failures on the Incidents tab. The Incidents tab creates an incident for the first violation event detected based on the alert policy settings assigned to the monitor. Each incident is automatically assigned a unique incident number. Violation events detected by the same monitor, and configured with the same alert policy are aggregated into the same open incident to avoid duplicating incidents. Aggregation of the these types of incidents will continue until the incident status is saved as "Resolved". Note that users cannot delete incidents.

1. Doubleclick the incident row you want to check.
2. You can check the event details in the [Details] section at the bottom of the window.



8.15.16 Mark the incident as “resolved” after handling the problem

Close the incident when the problem has been resolved. Select [Resolved] from the [Status] pull-down menu and click [Save].



The status display will change to “Resolved” and the closing process will be completed.

Click [Close] to close the [Incident Details] screen.

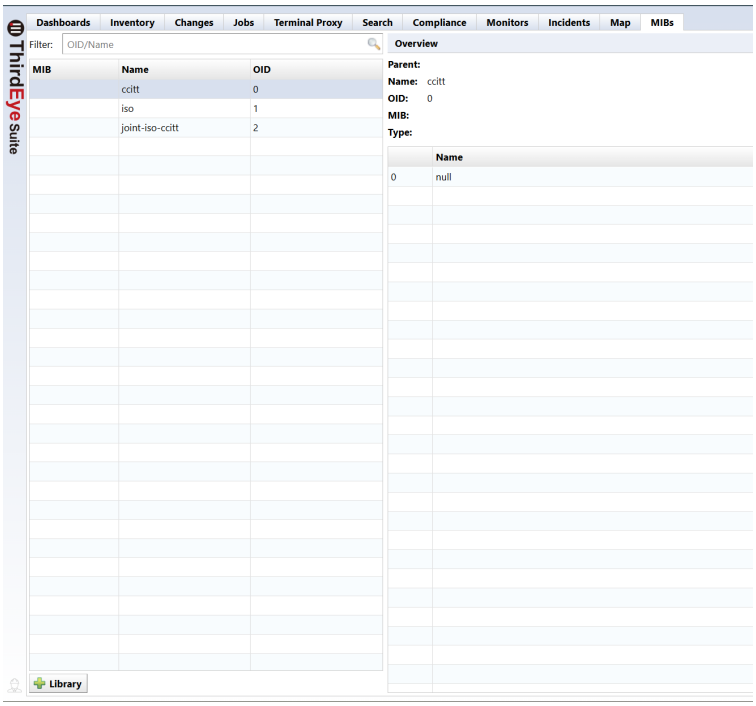
8.16 MIBs

The MIBs (Management Information Base files) tab provides centralized management of MIBs, which define standardized metrics for SNMP device monitoring. This interface allows you to search compiled MIB definitions, add/remove MIBs from the system library, and configure SNMP monitoring parameters. MIBs hierarchically organize network device attributes through Object Identifiers (OIDs). OIDs enable consistent interpretation of metrics like interface status, CPU utilization, and system uptime.

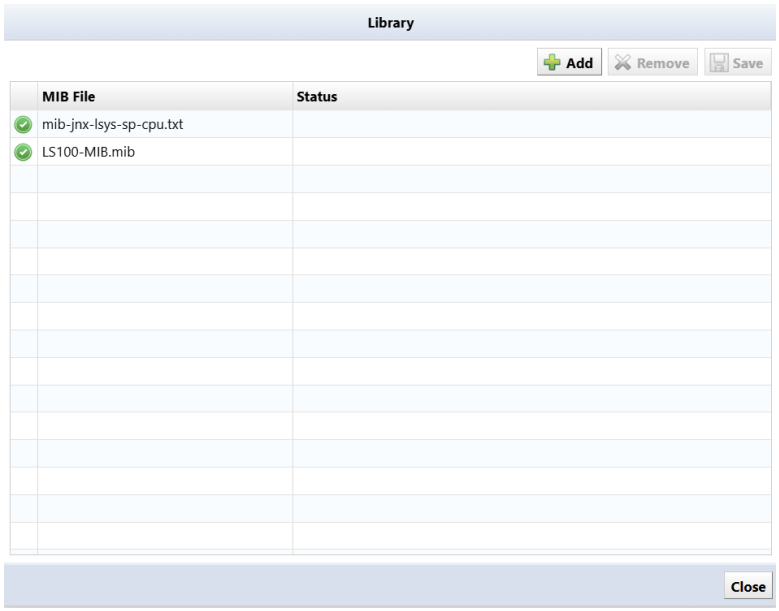
8.16.1 Compile the MIB

You can add uncompiled MIB files to ThirdEye.

1. Click [Library] at the bottom left of the MIB screen.



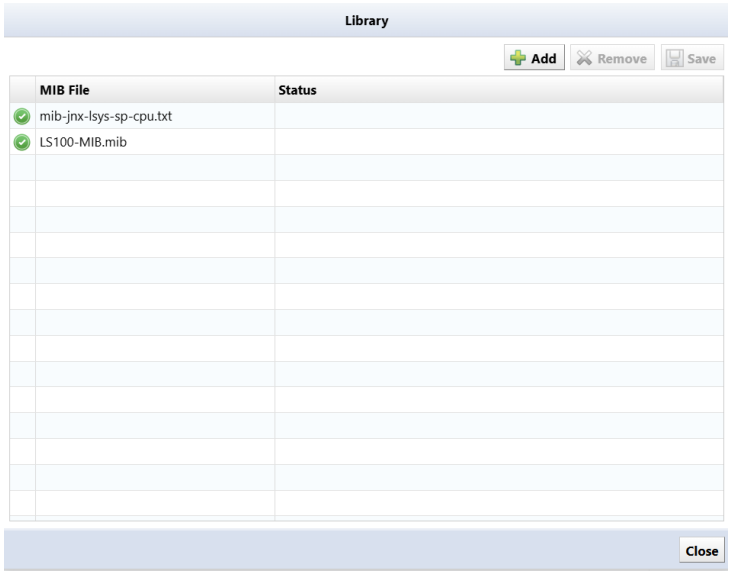
2. The library screen will be displayed. Click the (“Add”) button.



A file selection dialog will be displayed.

3. Select the MIB file to compile and click [Open].

Compilation is complete when the MIB file is displayed in the list, and the icon is displayed to the left of the MIB file.



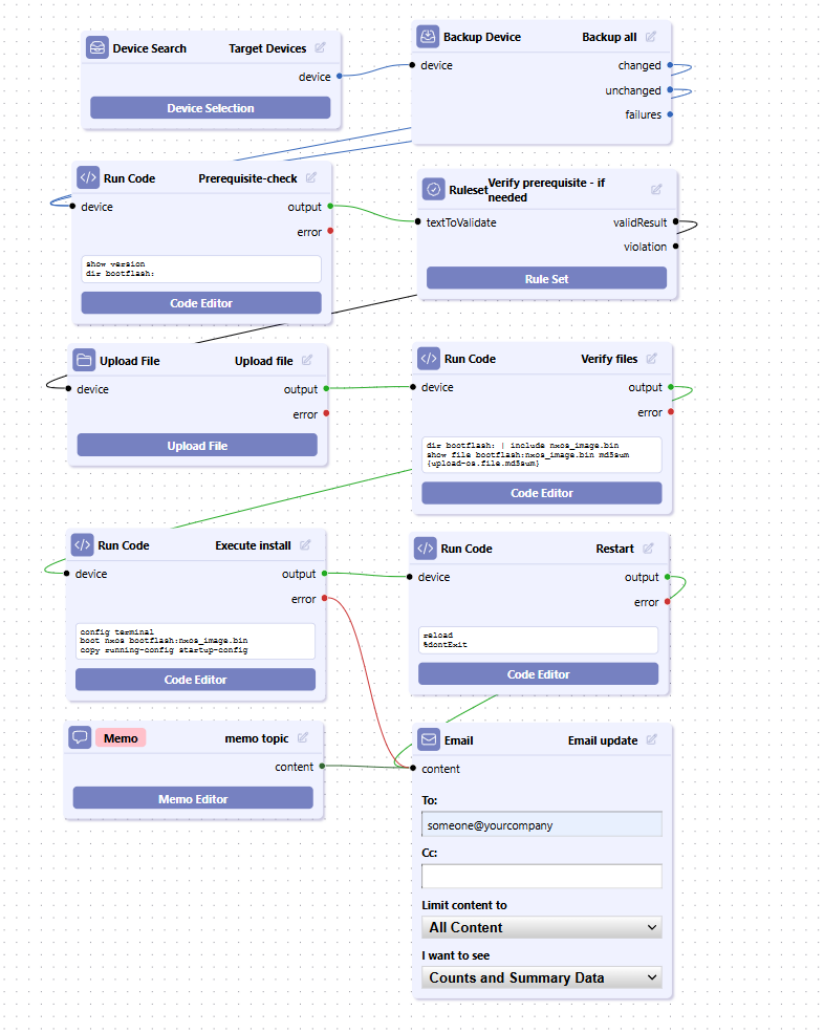
8.17 Playbook

The Playbook tab is a workflow automation interface designed to simplify and automate network management tasks using your custom scripts.

8.17.1 Playbook Features

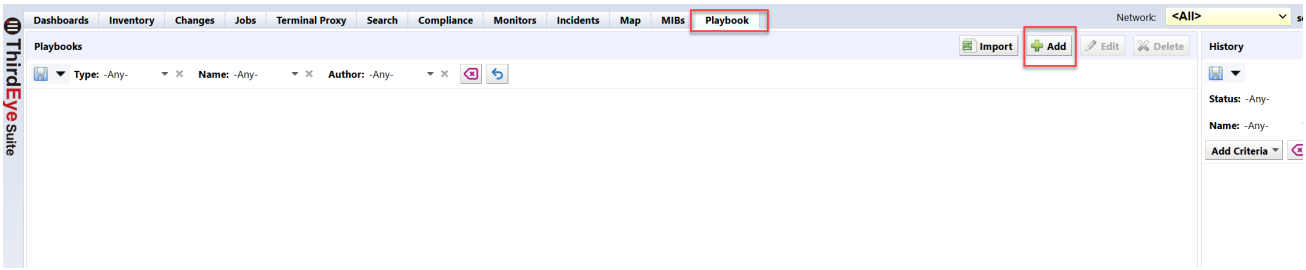
- **Drag-and-Drop Interface** allows design and implement complex automation workflows.
- **Customizable Plays** allows the creation of individual plays for specific tasks can then be combined into larger “Playbooks” for more comprehensive automation.
- **Push-Button Execution** allows push-button execution of complex tasks.
- **Streamlined Workflow** allows the facilitates the automation of repetitive tasks.

Playbook example:

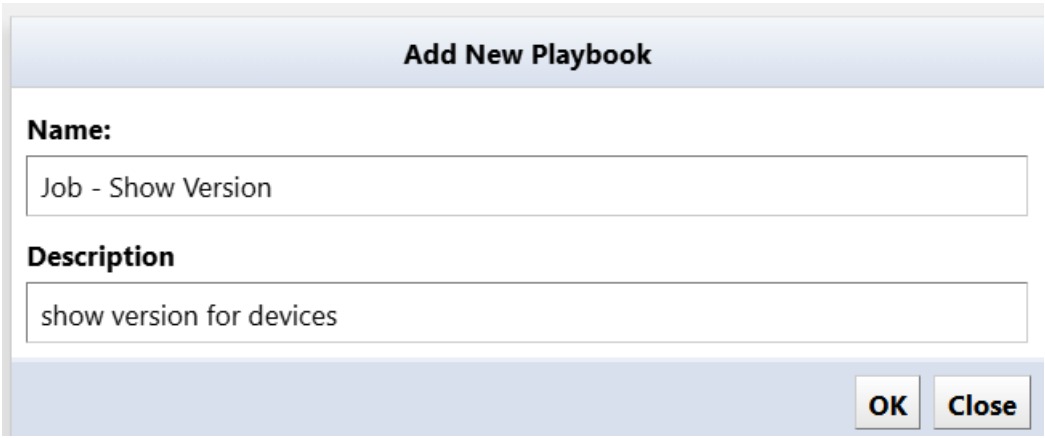


8.17.2 Setup and configuration

At the top of the page, click on the Playbook tab. Then click on the Add button.



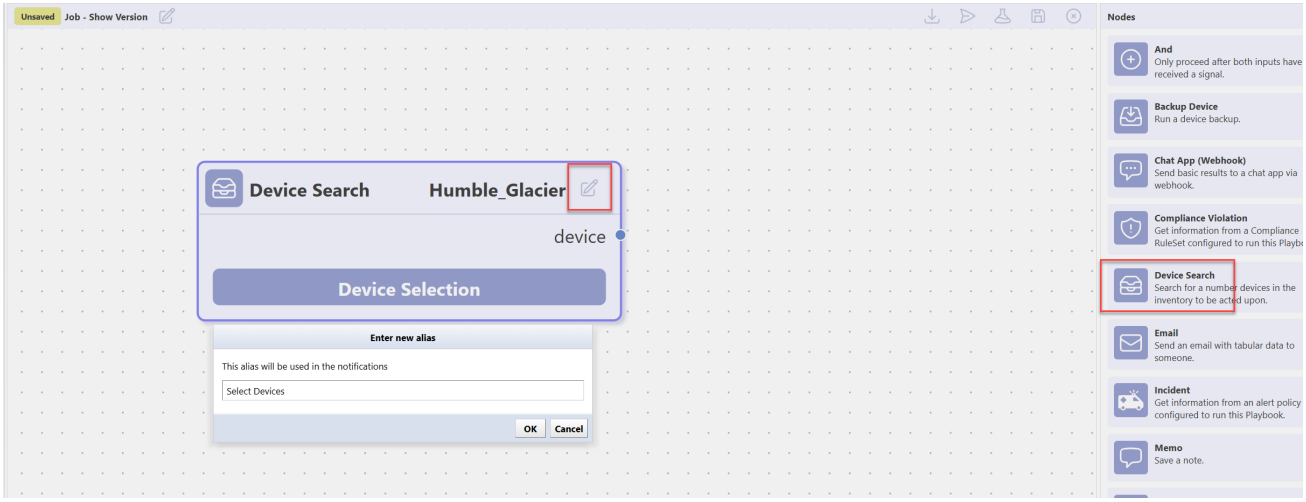
In the [Add New Playbook] popup window, enter the "Name" of the job, and a corresponding "Description", then click [OK].



On the right side of the screen, is the [Node] panel. These are the different options to configure a job to run. These are the current nodes, more will be added in future releases:

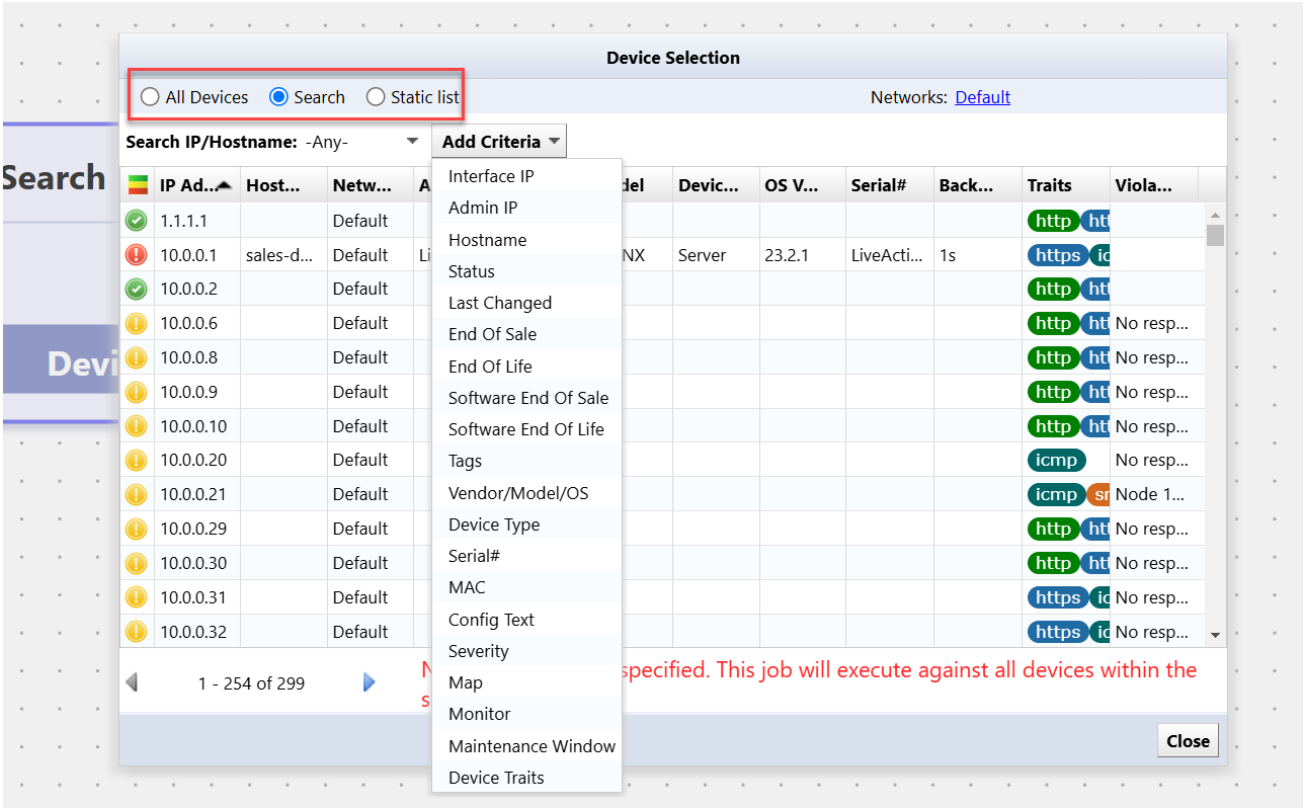
Node Option	Explanation
And	Only proceed after both inputs have received a signal
Backup Device	Run a device backup
Chat App	Webhook to send messages to either Teams/Slack/Mattermost/Webex
Compliance Violation	Get information from a Compliance Rule Set configured to run this playbook
Device Search	Search for devices in the inventory to be acted upon
Email	Send an email with tabular data
Incident	Get information from an alert policy configured to run this Playbook
Memo	Save a note
Regex Match	Execute a regular expression against the output of a node
Rule Set	Run a Rule Set against the output of a node
Run Code	Run a block of code on your devices
Run Code with Automatic Retry	Run a block of code on your devices a number of times or until it is successful
Schedule	Schedule this playbook to run automatically
Sleep	Delay for a number of milliseconds before forwarding input
Upload File	Send a file to your devices

8.17.2.1 Create a playbook From the node panel, click and hold a node, and drag it to the playbook field. Once the node is in the play field, click the button in the top right corner of the node to give the node a description.

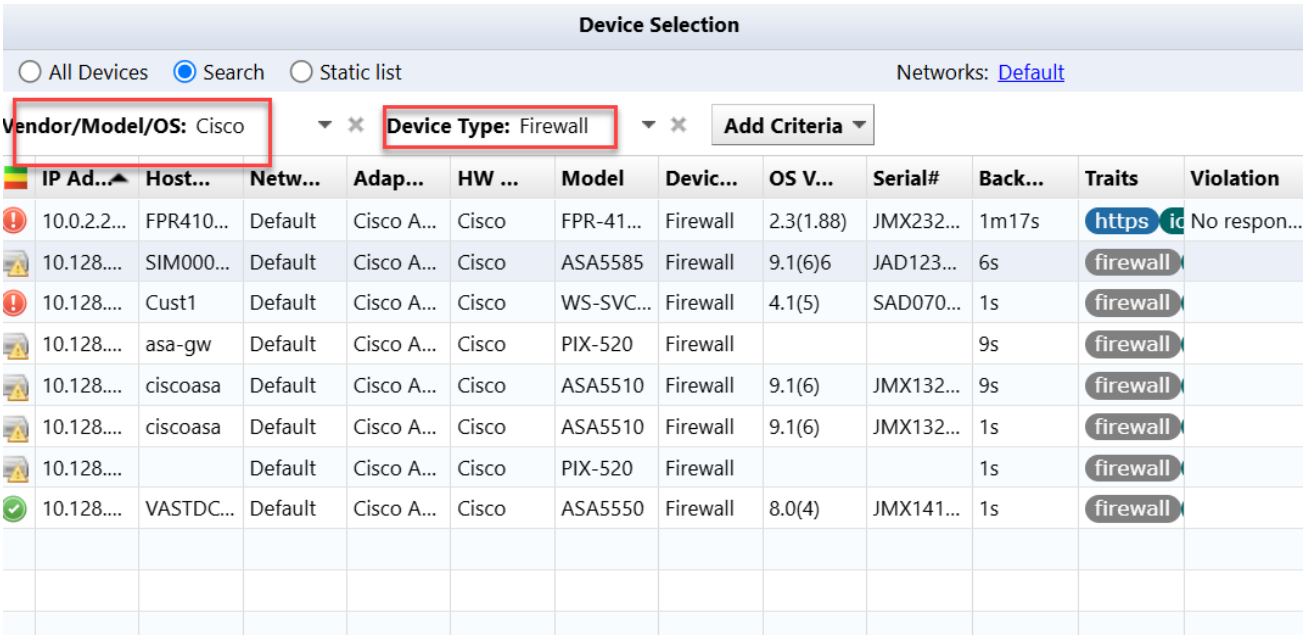


On the node, click on [Device Selection]. In this screen you have 3 options:

Option	Explanation
All Devices	Select all devices in the Inventory tab
Search	Select the [Add Criteria] and select options to select devices
Static List	Select devices from the Inventory tab and add to the selection



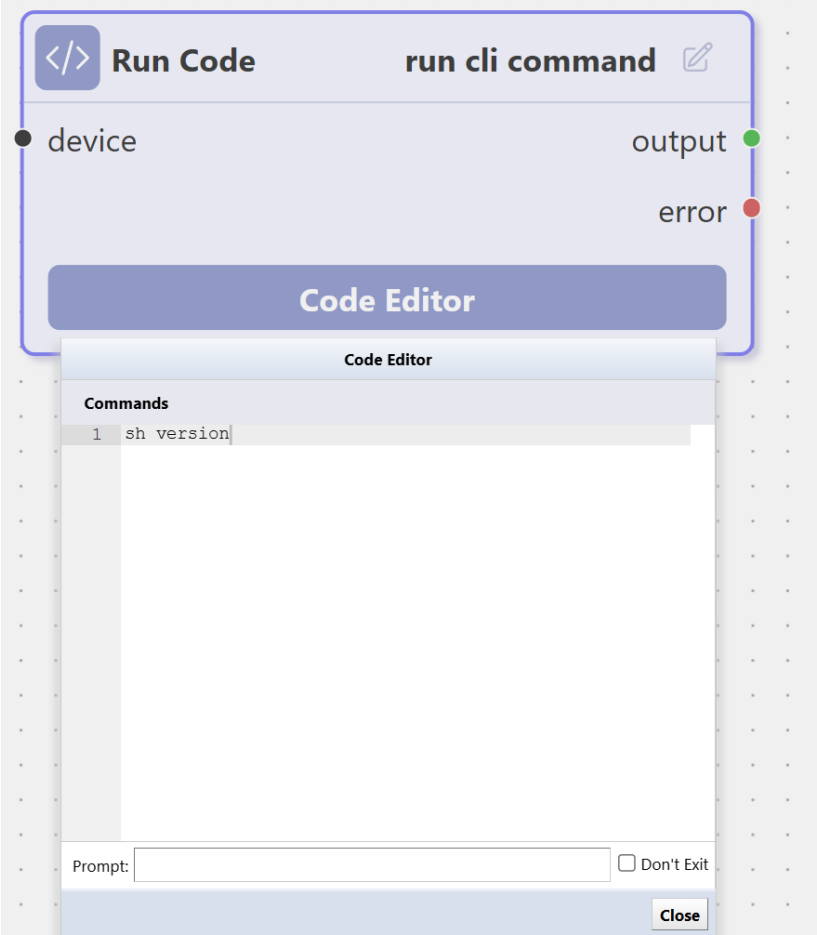
Enabling “Search” allows you to narrow your search using multiple criteria.



Add another node from the node table.

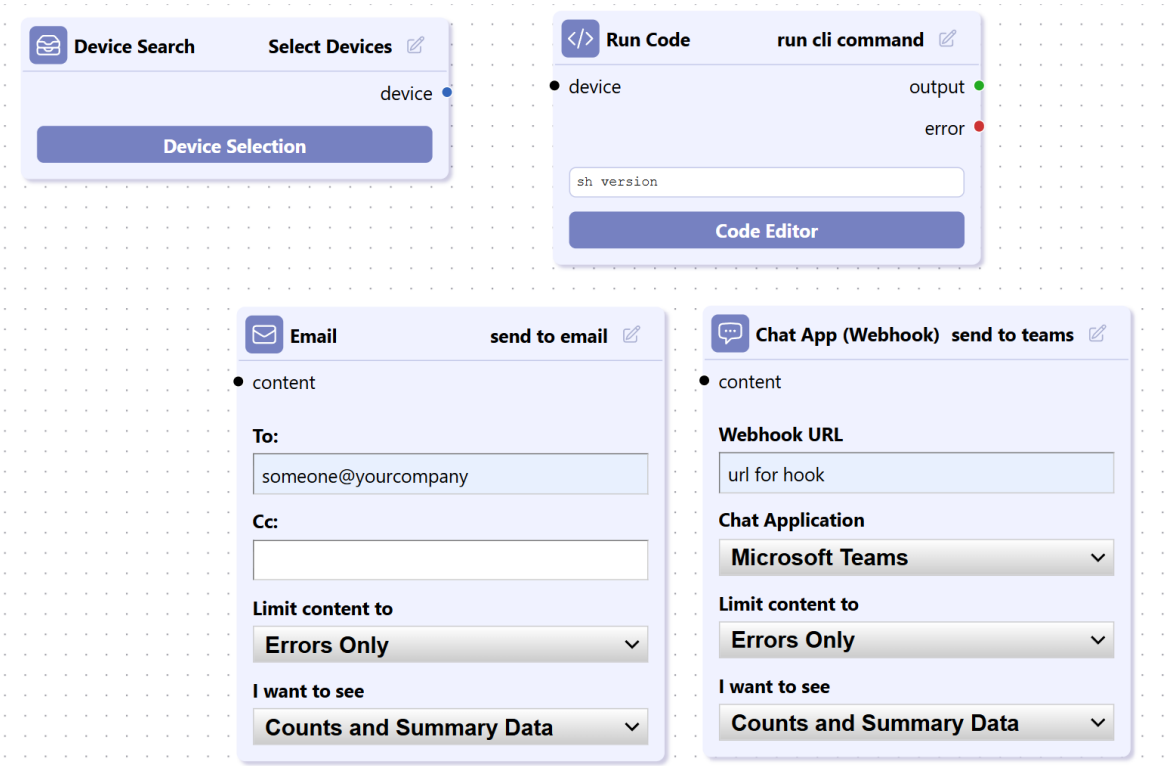
Select [Run Code] to change the description.

Click on [Code Editor] to enter any cli command for the devices you have selected.



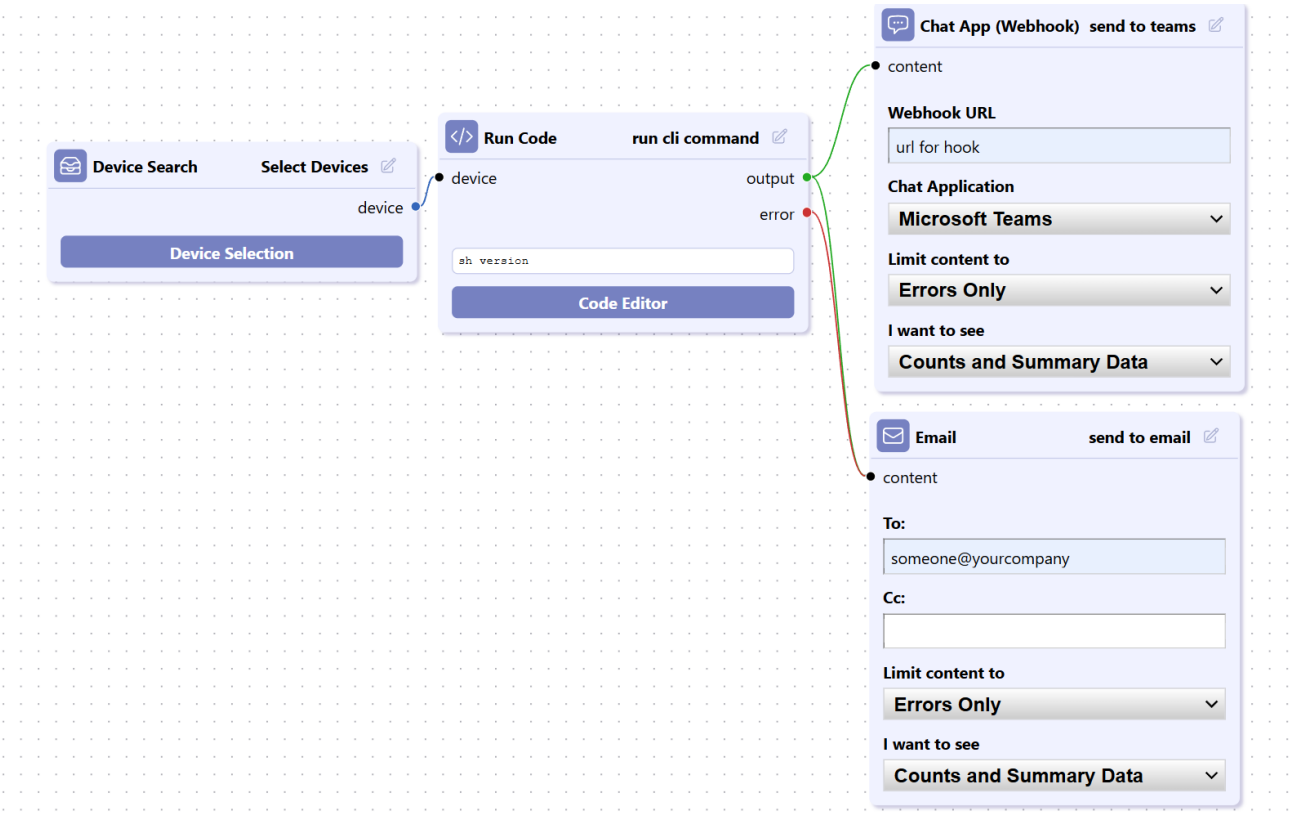
For Results you have three options:

Option	Explanation
Send email with results	Move email node to play field
Search	Send results with webhook to Teams/Slack/Mattermost/Webex/Line
Static List	Both email and webhook



In the “Email” and “Webhook” windows, you can click the pulldown menus to select reporting options.

Next, connect the nodes.

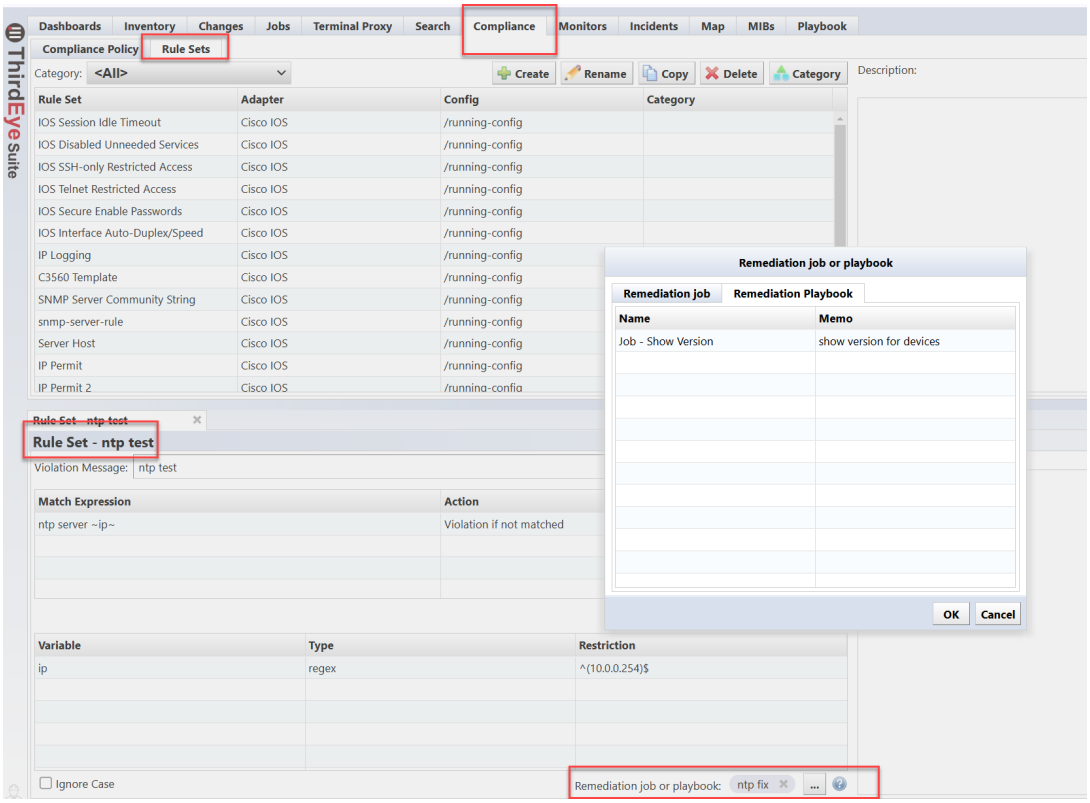


To remove a node, or a connection, select the desired item, and on your keyboard, click [Backspace].

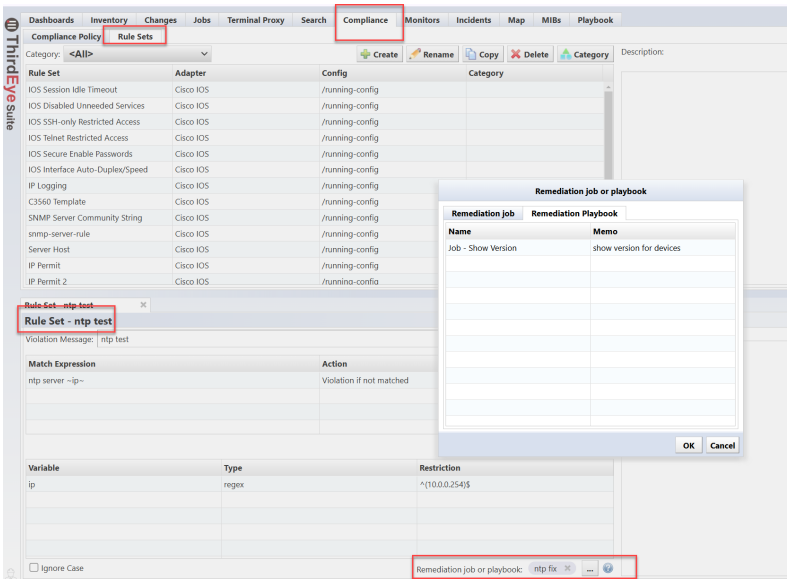
8.17.2.2 Compliance/Incident issues You can select a Playbook job to run remediation for both Incidents and Compliance issues.

Compliance Issues

1. Click the Compliance > [Rule Sets] tabs.
2. Select a Rule Set in the “Rule Set - ntp test”.
3. Click the [Remediation job or playbook] button in the lower right of the page.

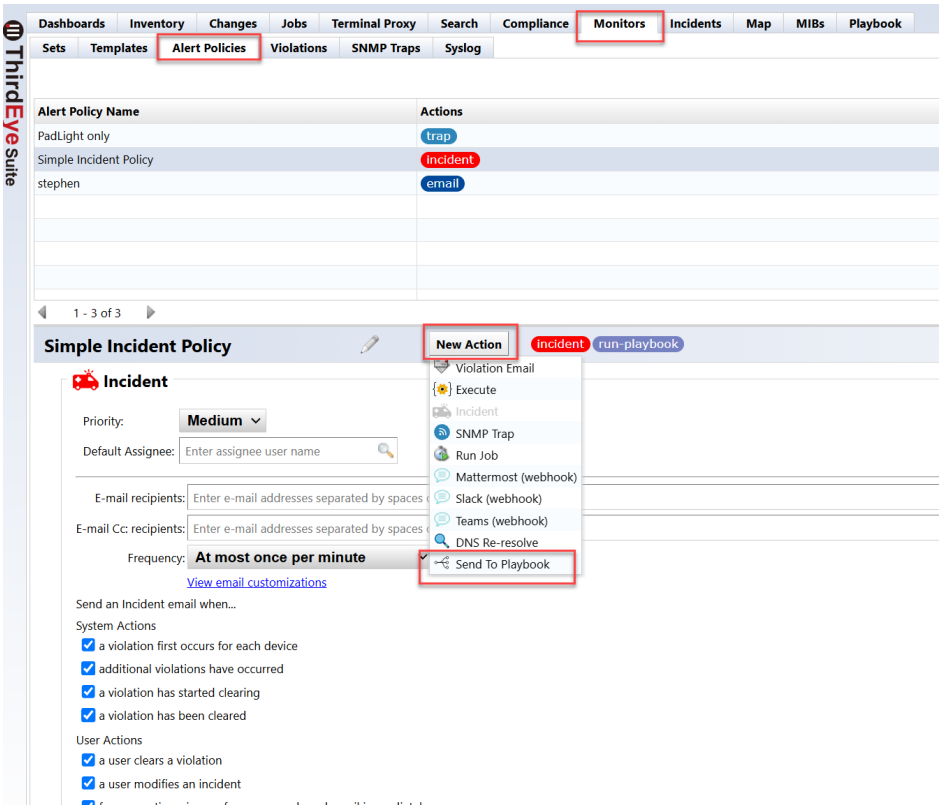


Compliance example:

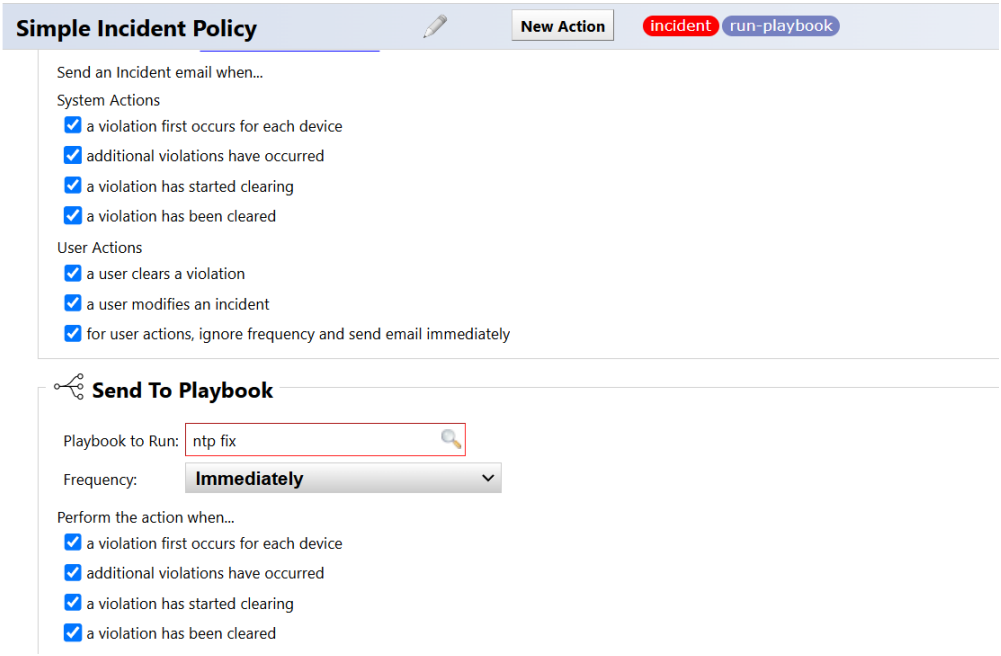


Incident Issues

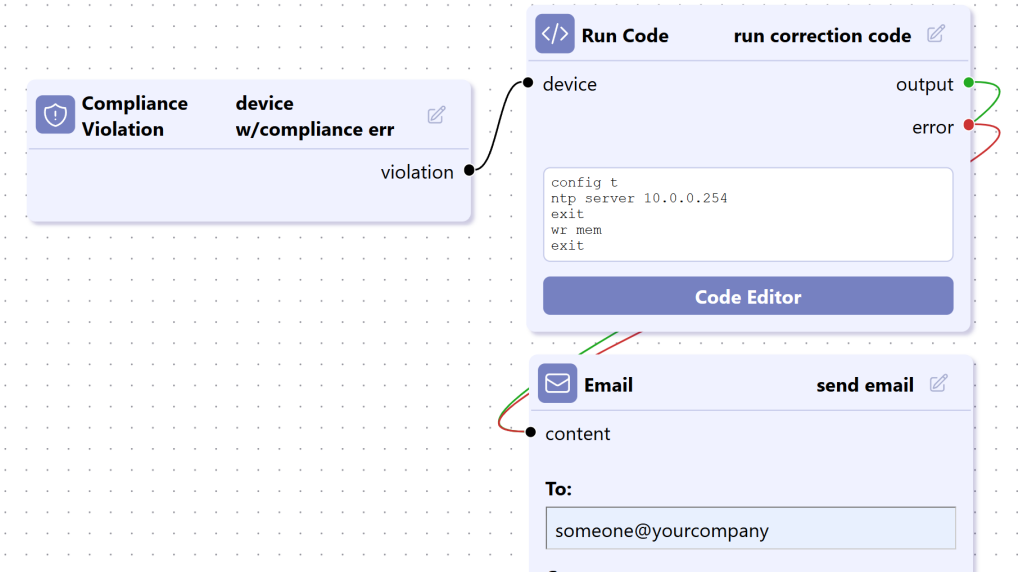
1. Click the Monitors > [Alert Policies] tabs.
2. Add a “Alert Policy Name”, or select an existing Alert Policy.
3. Click [New Action]. (You have the option to add [Send to Playbook]).



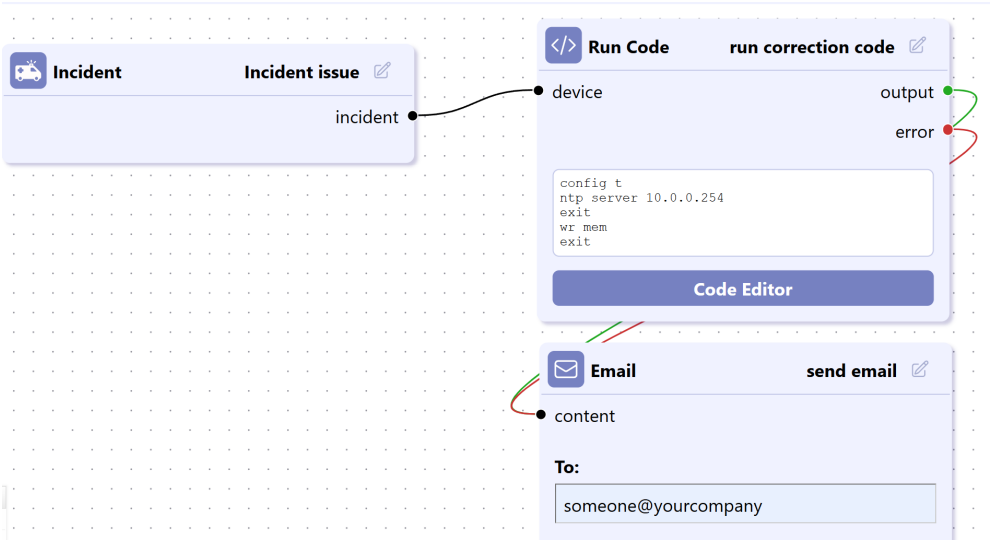
Once added, select the “Playbook to Run”, Frequency”, “Perform the action when…” options.



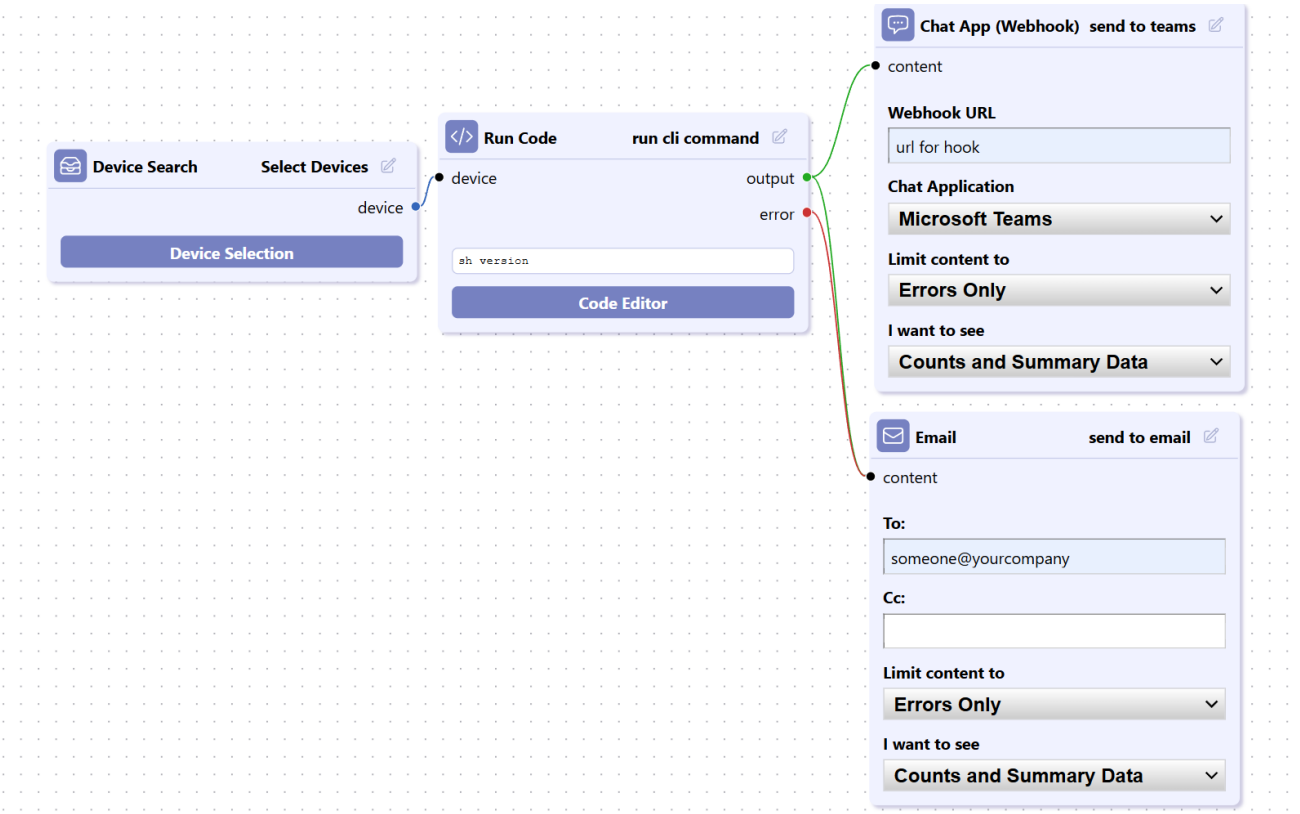
Compliance example:



Incident example:



Next, connect the nodes.



To remove a node, or a connection, select the desired item, and click on [Backspace] on your keyboard.

8.18 Wi-Fi Clients

The [Wi-Fi Clients] tab provides centralized monitoring of wireless client devices connected via Wireless LAN Controllers (WLCs). It displays real-time status, access point associations, and network details (MAC/IP addresses, SSID, connection duration). You can customize client labels/icons, and view historical data. Integrated mapping shows client locations relative to access points for troubleshooting.

8.18.1 Managed Network Restriction for Multi-Tenancy

Managed Networks allow administrators to logically group devices, either by IP space or other criteria. This functionality is particularly useful for Managed Service Providers (MSPs) that oversee multiple customers within a single platform.

In a multi-tenant environment, an MSP may require full visibility and control over all customer networks, while ensuring that individual customers can access only their own devices. To enforce these boundaries, Network Restriction settings can be applied to user accounts.

By configuring users with specific network restrictions, administrators can limit access to designated Managed Networks, preventing users from viewing or interacting with networks belonging to other customers. This ensures proper data isolation while maintaining centralized management capabilities.

This setup is ideal for organizations hosting multiple customers on a single system while maintaining security and data separation.

8.18.2 WMI Monitoring

ThirdEye uses the HTTP/SOAP based WS-Management protocol to retrieve WMI objects. The following objects can be obtained at the time:

```
Win32_PerfFormattedData_PerfOS_Processor (CPU Monitoring)
Win32_PerfFormattetedData_PerfDisk_LogicalDisk (Disk Monitor)
Win32_PerfFormattedData_PerfOS_Memory (Memory Monitoring)
```

8.18.3 Configuration on Windows

The Windows Remote Management (WinRM) service is required to remotely manage Windows systems. Currently, WinRM is already installed on systems supporte by Microsoft.

To get started, run the `winrm quickconfig` command from the command prompt or Powershell. This command sets the default configuration for WinRM. After executing the command, you can check the current configuration by executing `winrm get winrm/config/service`:

```
PS C:\\Users\\Administrator\> winrm get winrm/config/service
Service
  RootSDDL =
O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true

PS C:\\Users\\Administrator\>
```

You can also get the configuration of the current listener by running `winrm enumerate winrm/config/listener`:

```
PS C:\\Users\\Administrator\> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.40.66, ::1,
2001:0:348b:fb58:1077:394:3f57:d7bd, fd14:5839:664d:40:58c0:c882:310d:3
```

8.18.4 Non-secure HTTP connection settings

By default, only encrypted traffic si allowed. If you want to monitor using HTTP, execute `winrm set winrm/config/service '@{AllowUnencrypted="true"}` to allow unencrypted traffic:

```
PS C:\\Users\\Administrator\> winrm set winrm/config/service
\'@{AllowUnencrypted="true"}\'
Service
    RootSDDL =
O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
        IPv4Filter = *
        IPv6Filter = *
        EnableCompatibilityHttpListener = false
        EnableCompatibilityHttpsListener = false
        CertificateThumbprint
        AllowRemoteAccess = true
```

8.18.5 Authentication settings

If you want to use Basic authentication, run `winrm set winrm/config/service/auth '@{Basic="true}`. If the system is not joined to a domain (WORKGROUP), enable Basic authentication.

```
PS C:\\Users\\Administrator\> winrm set winrm/config/service/auth
\'@{Basic="true"}\'
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed `
```

8.18.6 Monitor Settings

8.18.6.1 Credential settings Register the username and password used for authentication in the credentials.

Set the Username to “VTY Username” and the password to “VTY Password”.

8.18.6.2 Monitoring Wireless LAN Controllers A WLC monitor can now be added to a wireless LAN controller running Cisco IOS XE. The WLC monitor periodically polls the monitored WLC devices via HTTPS to obtain a list of connected clients, the access points to which each client is connected, and other relevant information. It can then see which clients are associated with an access point based on data points such as MAC address, IP address, and date and time of last discovery. Additionally, it is possible to display the clients associated with each access point on a map.

8.18.6.2.1 WLC Monitor Settings

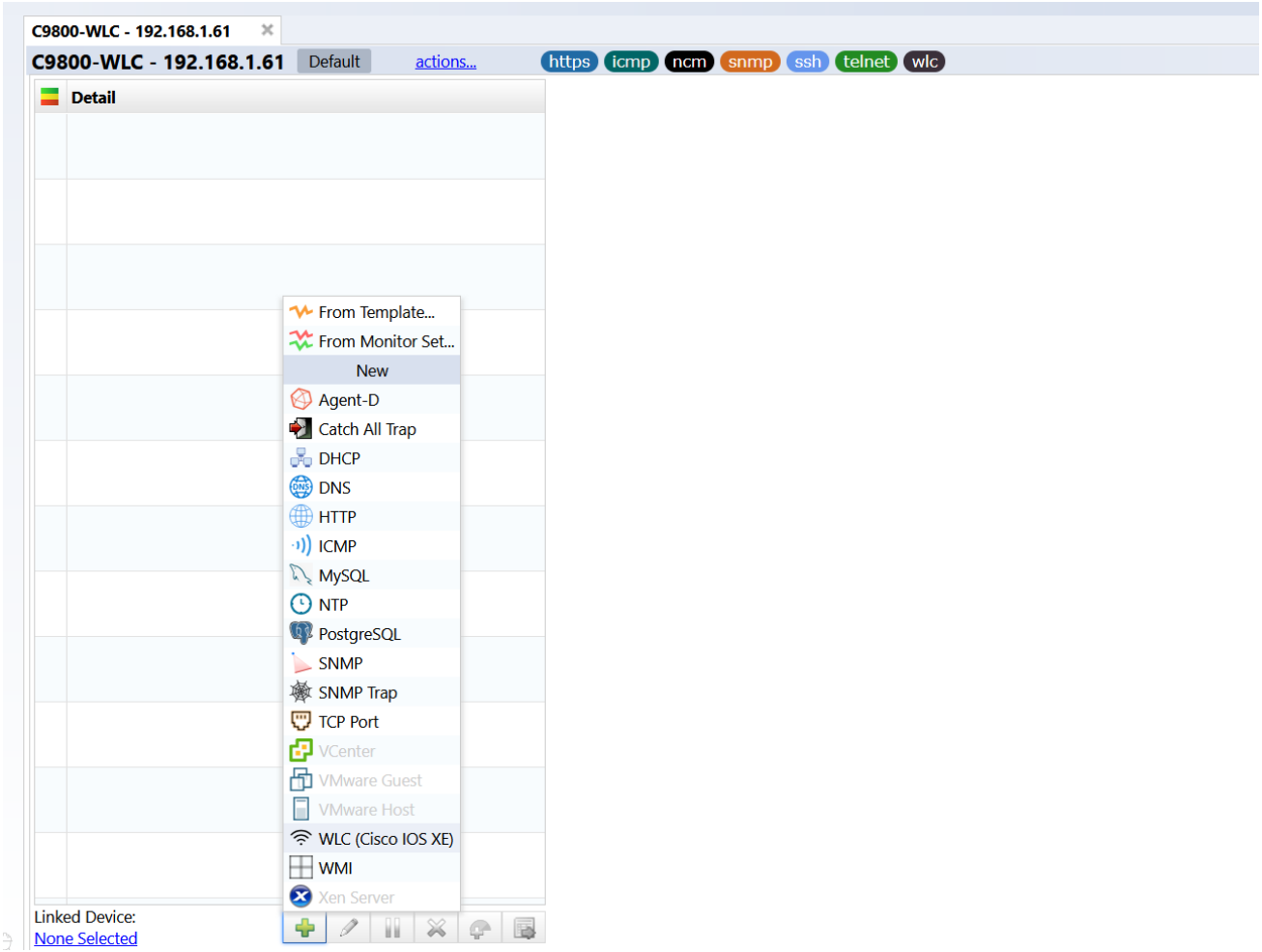
1. Add the wireless LAN controller to the inventory.

   The adapter of the wireless LAN controller must be “Cisco IOS”.

2. Set the credentials required to log in to the wireless LAN controller.

   “`VTY Username`” and “`VTY Password`” are used for authentication.

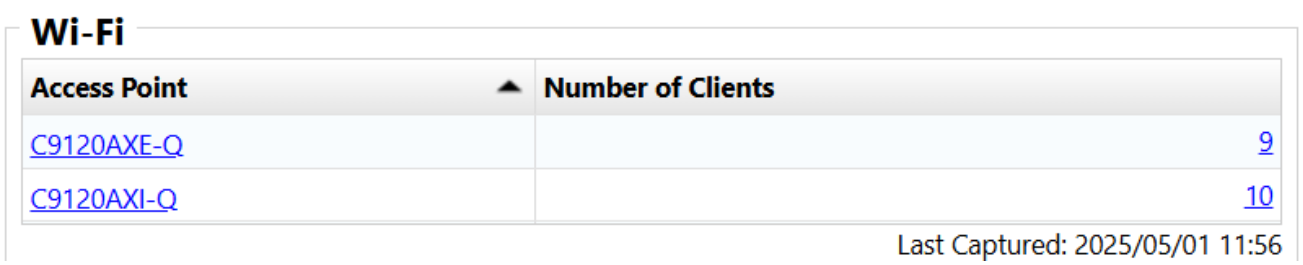
3. Add a “WLC (Cisco IOS XE)” monitor to the wireless LAN controller.



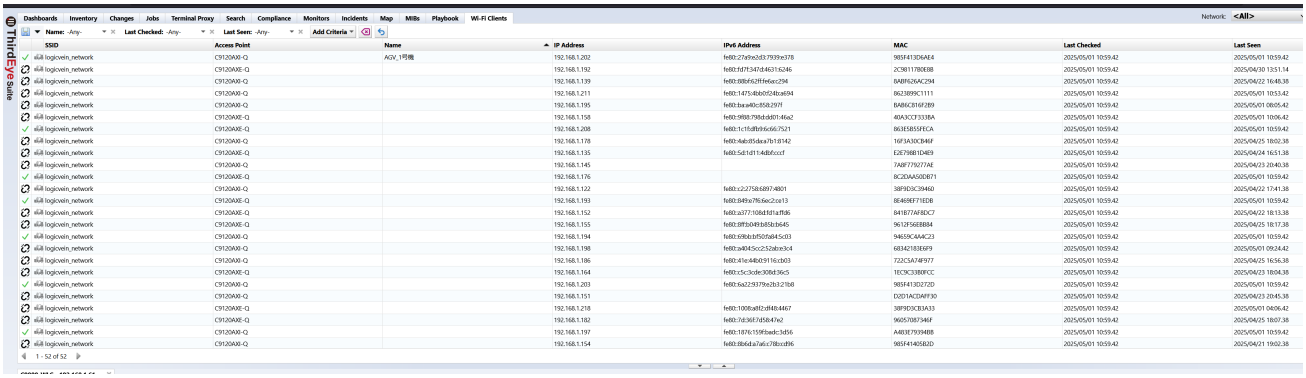
WLC monitors may now be added to Wireless Lan Controllers running the Cisco IOS XE Operating System. Monitored devices will be polled periodically via https for a set of connected clients as well as some associated information, such as which Access Point each client is connected to. This allows for the querying of clients based on data points such as MAC, IP Address, or when the client was last seen. It also allows for the display of clients on Maps under their associated Access Point.

4. Configure the monitor settings.

Set the monitor name, interval, data storage period, and optional triggers, then click [Save]. When data collection is complete, a table will appear showing the AP name and the number of clients currently connected.



8.18.6.2.2 WLC Monitor Settings The Wi-Fi Clients tab provides details on the clients acquired by the WLC monitor.



Item	Description
Status	The following two types of icons are displayed: Indicates that the client has been recognized as a client at least once in the past but is not currently connected. Indicates that the client is currently connected.
Icon	An image used as the icon for the node representing the client on the map. Any image can be uploaded and set.
SSID	The SSID name to which the client is connected is displayed.
Access Point	Displays the name of the access point to which the client is connected.
Name	A name may be associated with a client to make it easier to identify in this table and in maps.
IP Address	The IP address used by the client is displayed.
IPv6 Address	The IPv6 address used by the client is displayed.
MAC	The MAC address of the client is displayed.
Last Checked	Displays the date and time when ThirdEye last checked client information in the WLC.
Last Seen	The date and time the client was last connected is displayed.

The SSID, access point, IP address, IPv6 address, MAC information is the same as the information available in the [Monitoring] > [Wireless] > [Client] window of the WLC's Web Management Console.

The name and icon can be customized by clicking the Edit button in the upper right corner. Since this customization is associated with the client's MAC address, the customization will be applied even if the client gets a new IP address.

8.18.6.3 Displaying Clients on a Map

1. Add the access point to the same management network as the wireless LAN controller. Make sure the hostname of the access point is set correctly.
2. Verify that the access point has been given an “ap” trait.

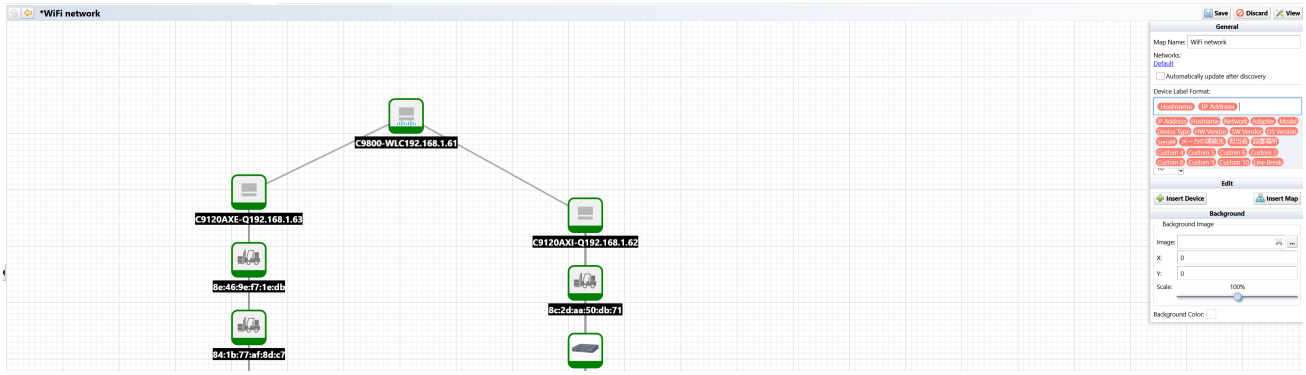
Hostname	Adapter	OS Version	Serial#	SW Vendor	Last Backup	Traits
C9800-WLC	Cisco IOS	16.12.4a	FCL245100KU	Cisco	2025/04/21 18:56	https icmp ncm snmp ssh telnet wlc

When the “WLC (Cisco IOS XE)” monitor on the wireless LAN controller completes data collection, the access point will automatically be assigned an “ap” trait.

3. Insert the access point with the “ap” trait into the map.

When an access point is selected while editing the map, a new option “Show Wi-Fi Clients” becomes available. When this option is enabled, all clients connected to the access point will be displayed in a vertical column under it. It is not possible to change the display direction of the clients or move the placement of the displayed clients.

4. Select the access point and activate the “Show Wi-Fi Clients” option.

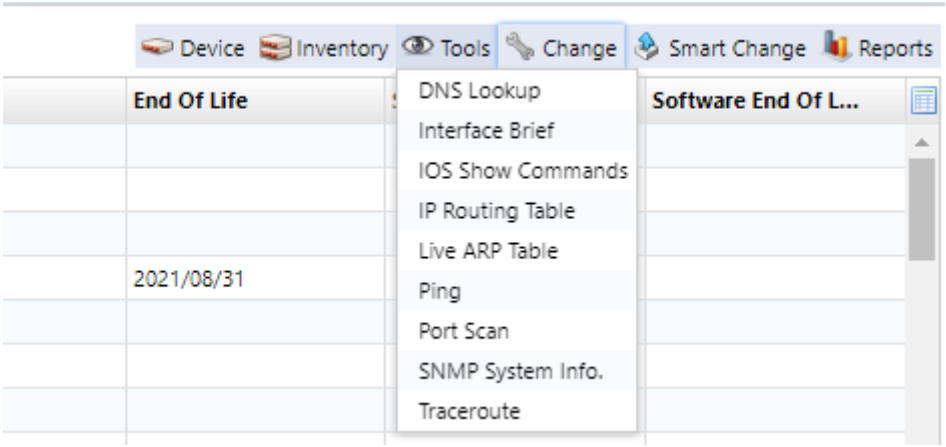


5. Save the map.

The name set in the Wi-Fi Clients tab will be used to label the clients that appear on the map. If no name is set, the client’s MAC address will be displayed. The name and icon can be edited in the Wi-Fi Client tab or by right-clicking on the client icon on the map. The client icon on the map will also be automatically updated when the client is disconnected or moved to another access point.

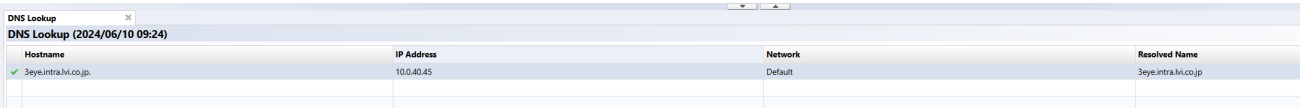
8.19 Viewing tools

The Viewing Tools menu allows you to determine the real-time status of the selected device. It is also possible to export all detected results as a CSV file. When using the viewing tool, a dedicated tab will be opened in the status panel, so exporting can be done using the button located in the top right corner.



8.19.1 DNS lookup

The DNS Lookup window displays the device's DNS information.

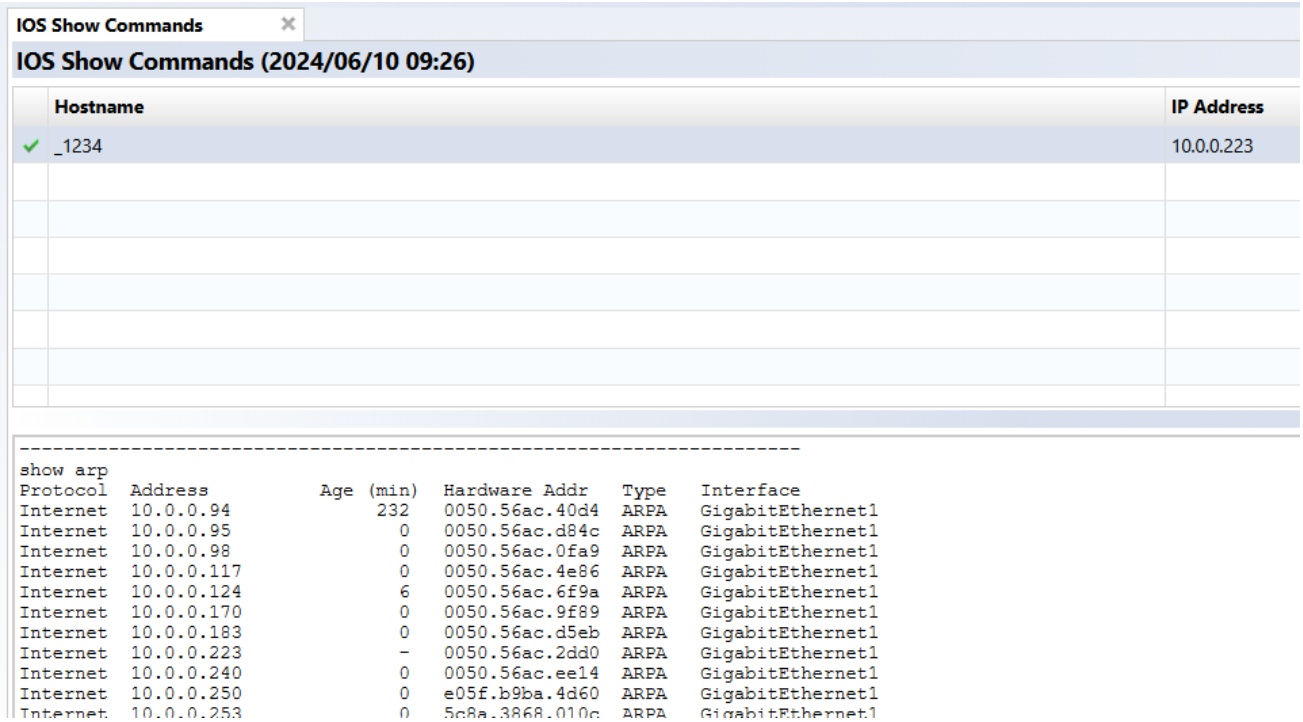


8.19.2 IOS Show commands

The IOS Show Commands window displays the results of the device's "IOS Show commands" request. Select the "show" command you want to run first from the list, and click [Execution] to issue the command.

> **Note**
>
> This command can only be run on devices that are compatible with Cisco IOS.

An ARP screen showing the results of executing the command will be displayed.



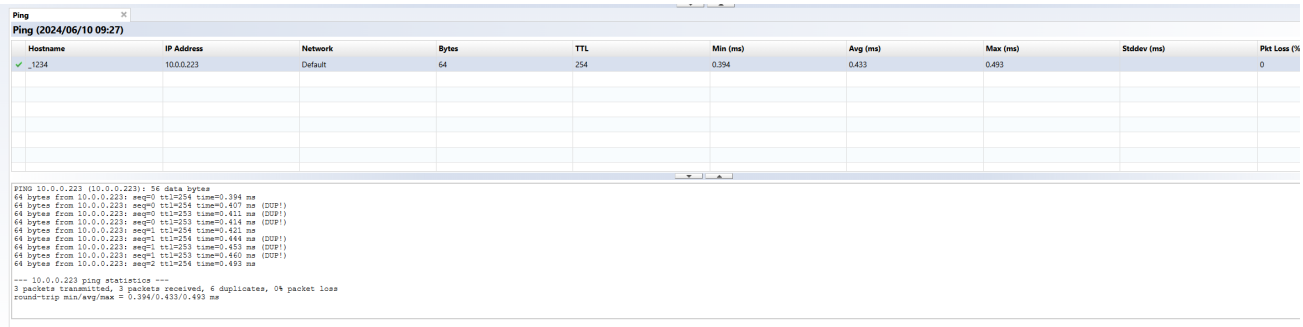
8.19.3 IP Routing table

The IP Routing table window displays the device's routing information.

> **Note**
>
> This function cannot be executed when multiple devices are selected.

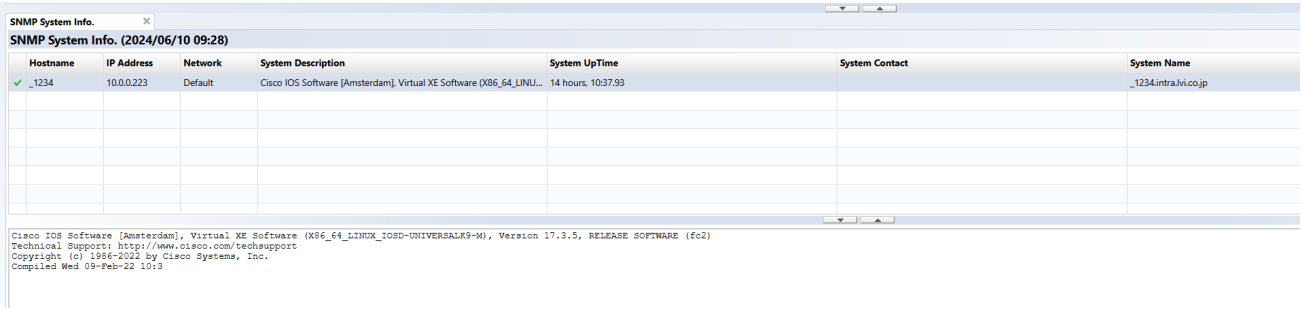
8.19.4 Ping

From the Ping window, you can ping a device and check the response.



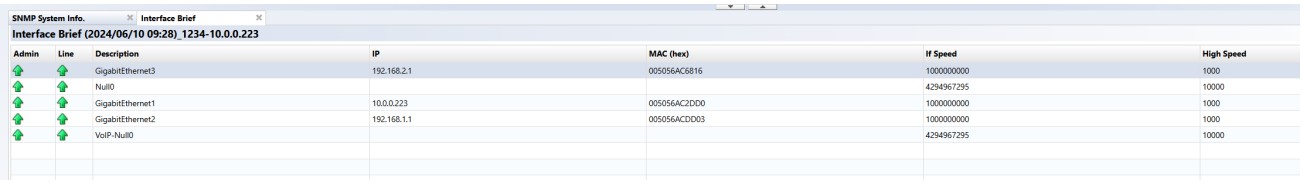
8.19.5 SNMP System Info

The SNMP System Info window displays the device's SNMP system information.



8.19.6 Interface Brief

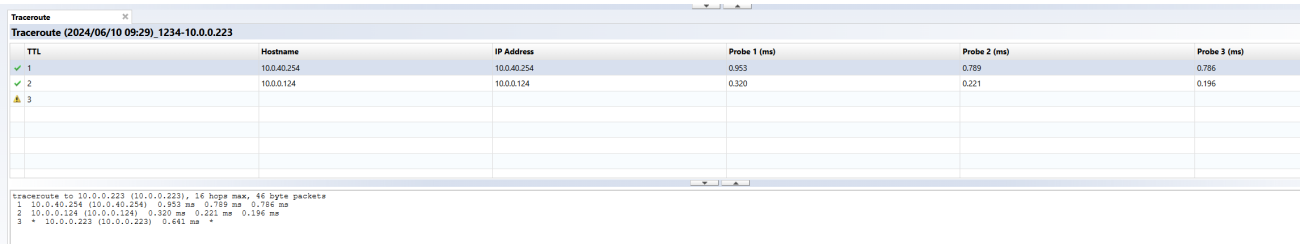
The Interface Brief window displays detailed information such as the open/close status of each interface of the device, device IP address, etc.



> **Note**
>
> This function cannot be executed when multiple devices are selected.

8.19.7 Traceroute

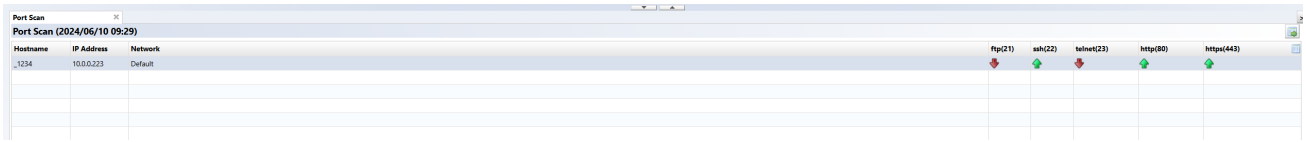
From the Traceroute window, you can perform a traceroute to the device and display the response.



> **Note**
>
> This function cannot be executed when multiple devices are selected.

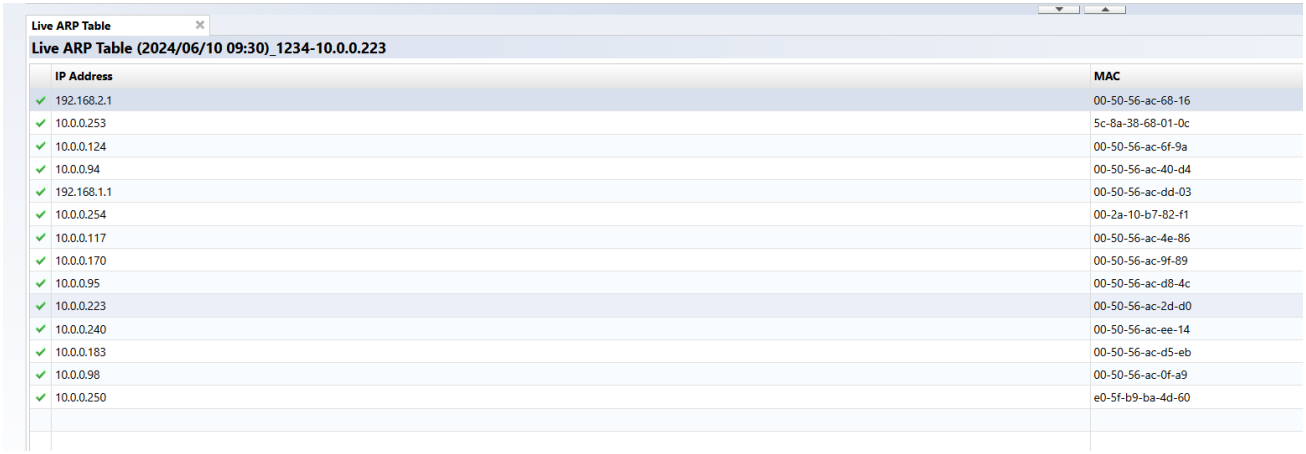
8.19.8 Port Scan

The Port Scan window displays device port opening/closing information.



8.19.9 Live ARP Table

The Live ARP Table window displays the live status of the ARP table.

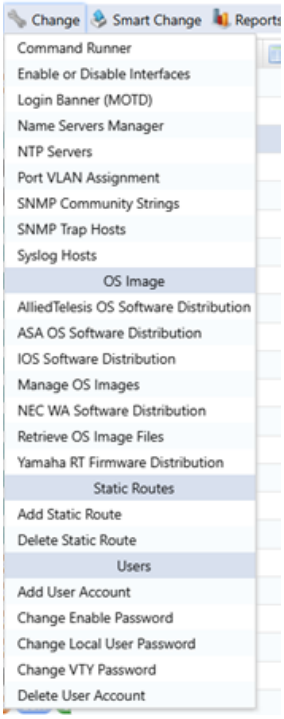


> **Note**
>
> This function cannot be executed when multiple devices are selected.

8.20 Change tools Suite

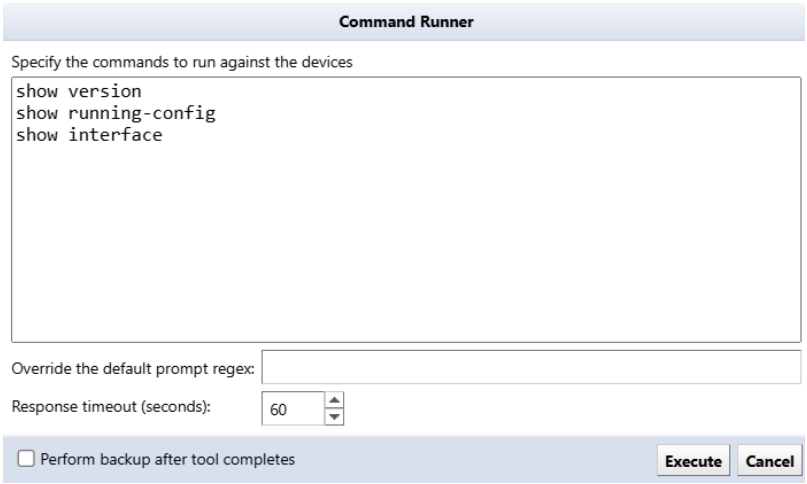
The [Change] submenu collects operations related to modifying the configuration of the selected device.

In this section, we will explain each function in the [Change] submenu.



8.20.1 Command Runner

Command Runner is a useful tool when performing the same operation repeatedly on multiple devices. For example, you can run commands of over 100 lines to many devices at once. Commands that can be performed include downloading and uploading configurations. After entering the required items, click the Execute button.



The [Override the default prompt regex] field specifies a regular expression to match a particular type of prompt. The prompts to be matched are like PS1 variables in shell scripts. This field required if a command responds with an unusual prompt.

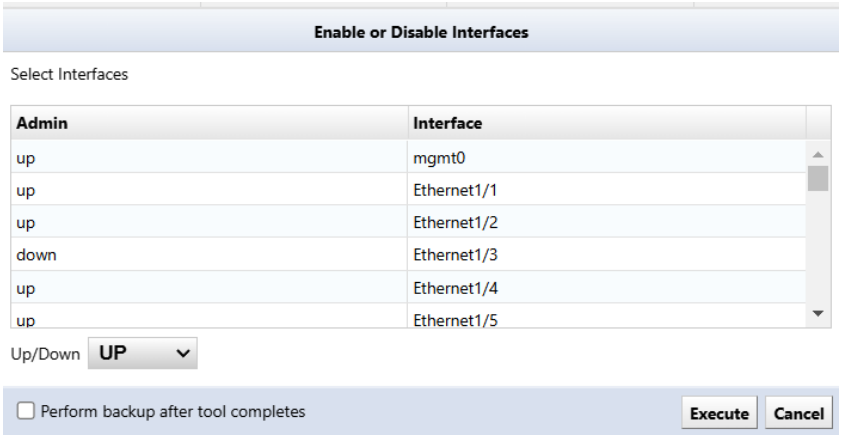
For example, some interactive commands may prompt for the next input with a simpler “<” instead of

the usual "`<username>#`" prompt. In these cases, you must specify using the regular expression "`^<`" (at the beginning of the line). Otherwise, it will be impossible to distinguish between the output result of the command and the prompt.

8.20.2 Enable or Disable Interfaces

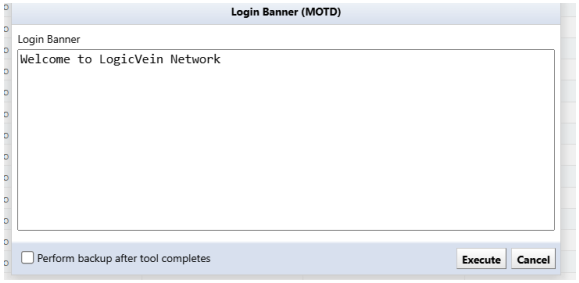
Change the Admin Status of the device interface. Please note that this function cannot be executed when multiple devices are selected.

From the [Select Interfaces] field, select the interface for which you want to change the Admin Status (multiple selections are possible), select [Up/Down] from the pull-down menu, and click the Execute button.



8.20.3 Login Banner (MOTD)

Set the device login banner.



8.20.4 Name Servers Manager

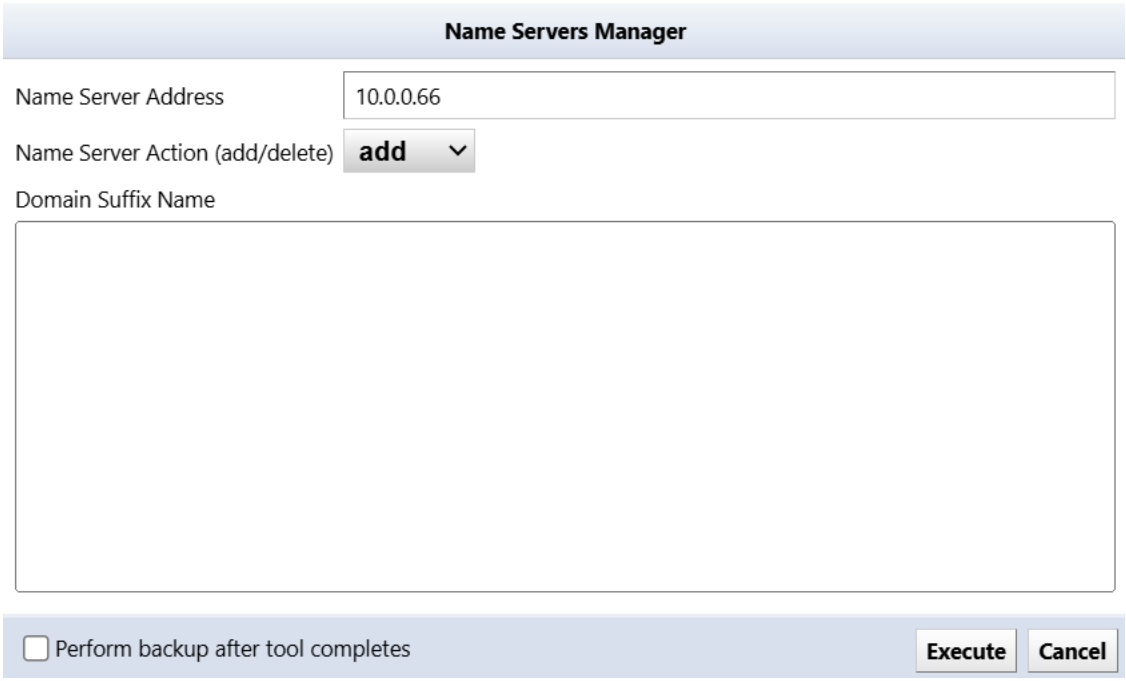
Add or delete a “Name Server Address”.

Add an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.

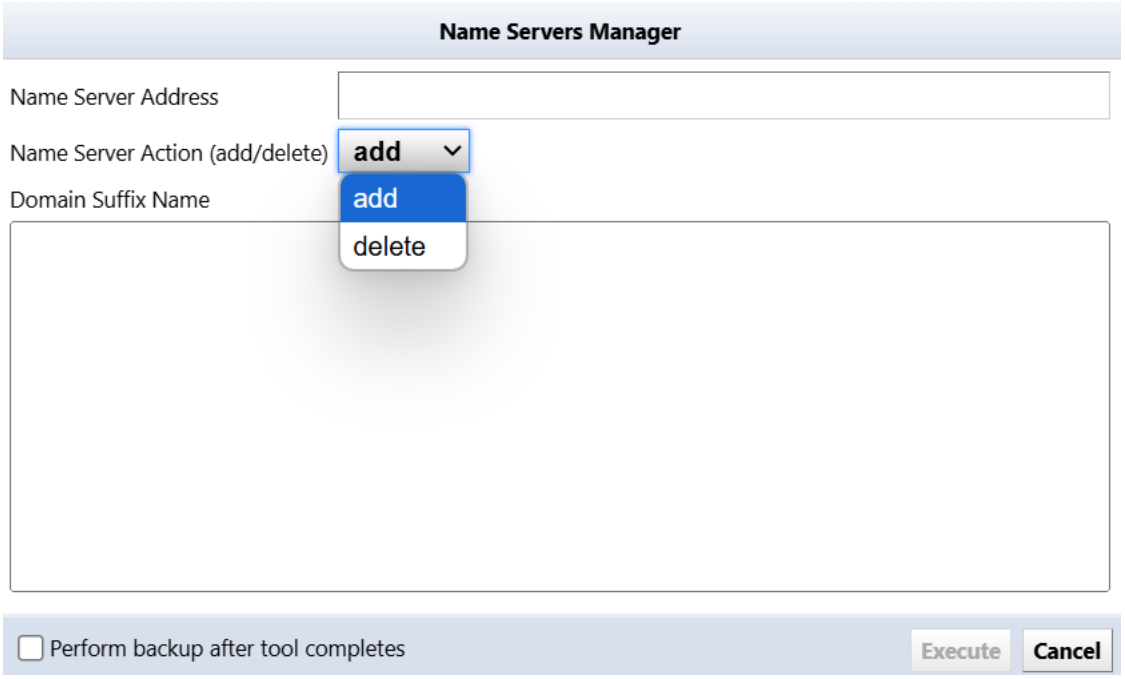
The Execute button, will become clickable.

3. Click Execute.



Delete an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.
3. Change the “Name Server Action” to “delete”.

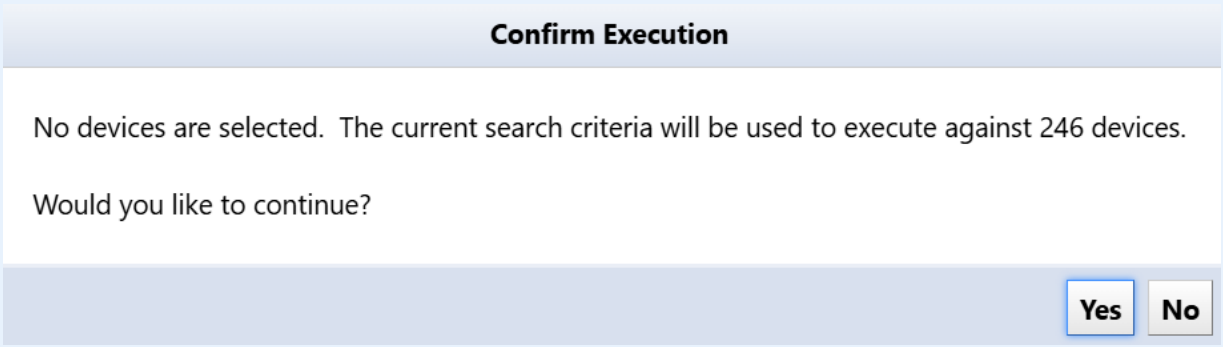


The Execute button, will become clickable.

4. Click Execute.

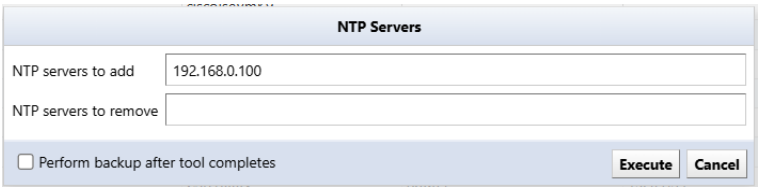
Note

If no IP Address is selected, clicking the [Name Server Manager] tool will act on all addresses in the Inventory window list.



8.20.5 NTP Servers

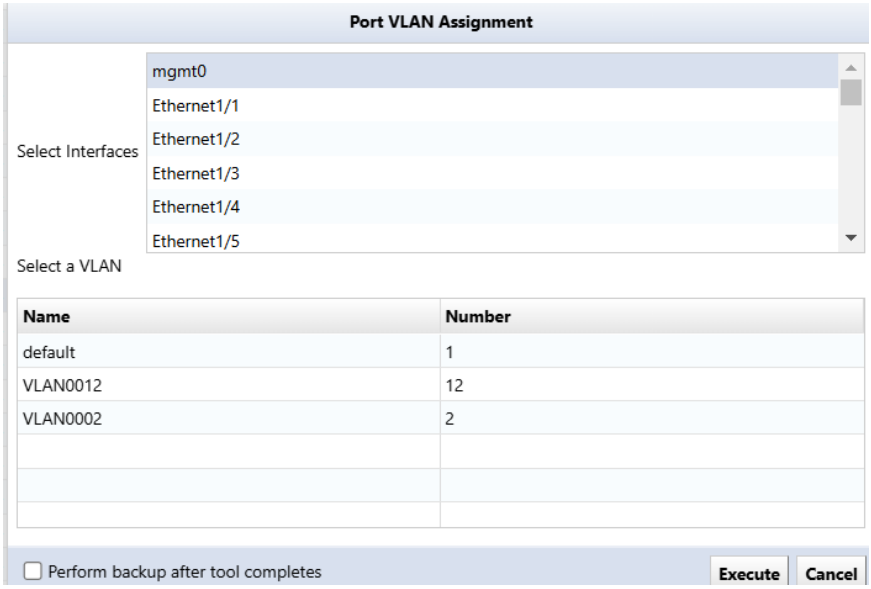
Add/remove NTP servers to your device.



8.20.6 Port VLAN Assignment

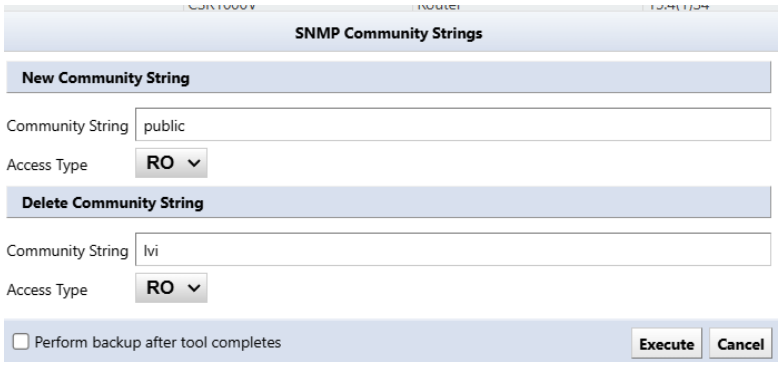
Perform VLAN port settings for the device's access port. Please note that this function cannot be executed when multiple devices are selected.

Select the interface on the screen. Select the interface for VLAN settings (multiple selections are possible), and select the VLAN. Select the VLAN to be assigned from the field and click the Execute button.



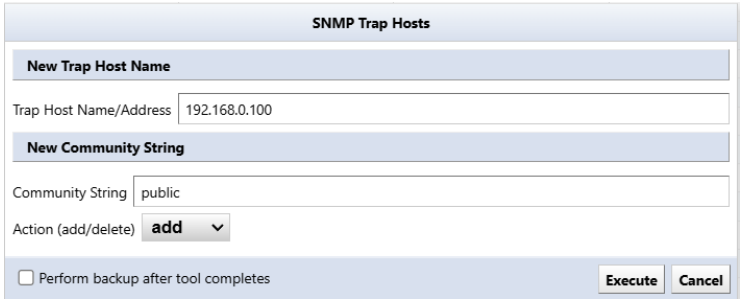
8.20.7 SNMP Community Strings

Add/delete SNMP communities to/from devices.



8.20.8 SNMP Trap Hosts

Add/delete SNMP trap host settings for devices. It is effective for batch setting of new NMS installations.

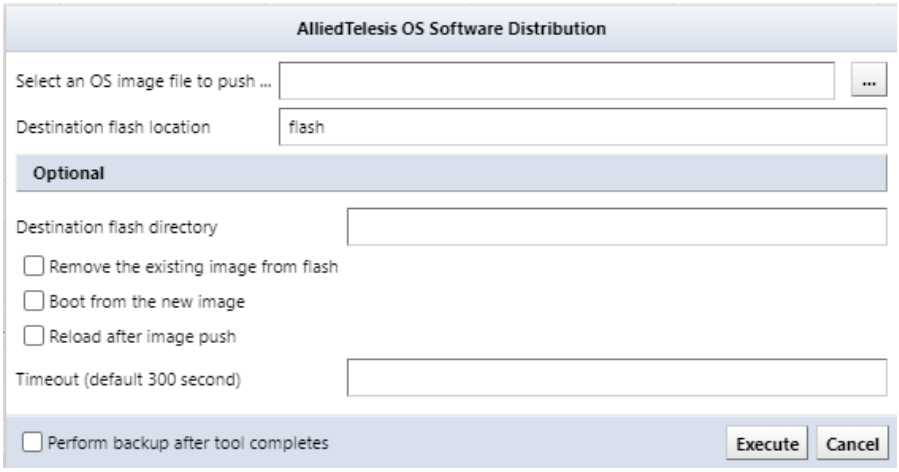


8.20.9 Syslog Hosts

Add/delete Syslog hosts to/from the device.

8.20.10 AlliedTelesis OS software distribution

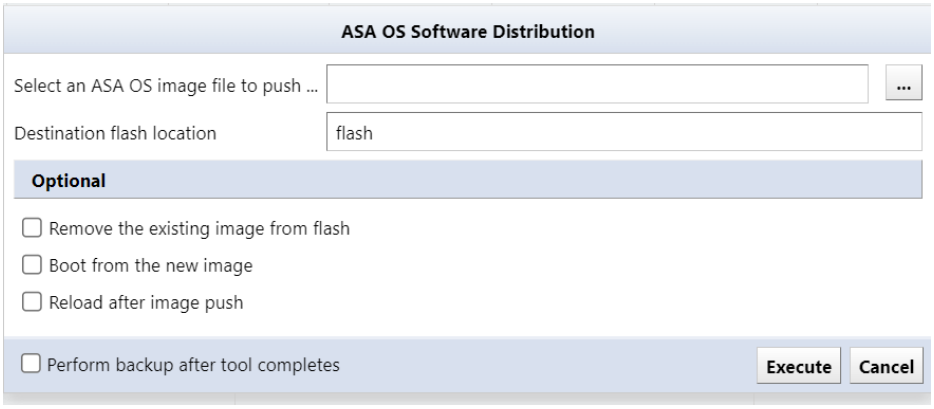
You can remotely distribute the OS to AlliedTelesis devices. To use this function, you must save the OS in advance.



Item	Explanation
Select an OS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, boot with new image
Reload after image push	After image transfer, reload the system.
Timeout (default 3000 seconds)	Timeout setting for setting transferring time

8.20.11 ASA OS software distribution

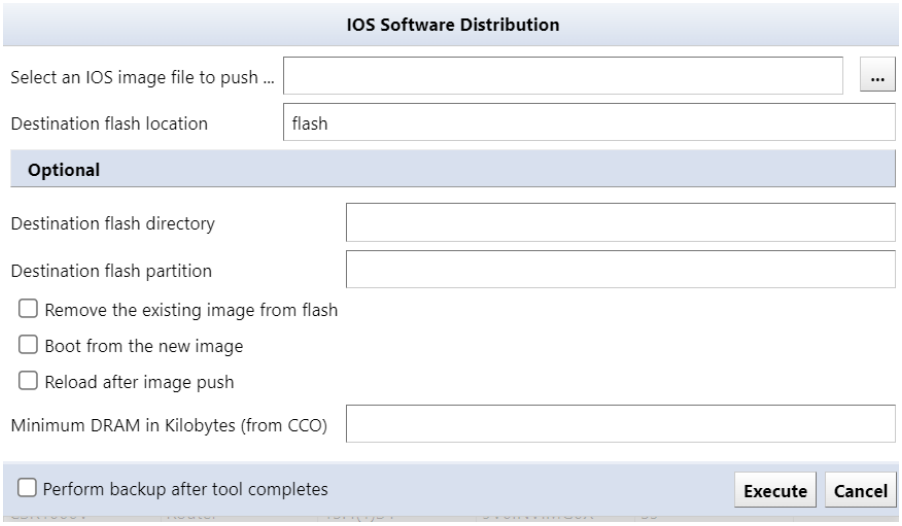
You can remotely distribute the OS to Cisco ASA devices. To use this function, you must save the OS in advance.



Item	Explanation
Select an ASA OS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time

8.20.12 IOS software distribution

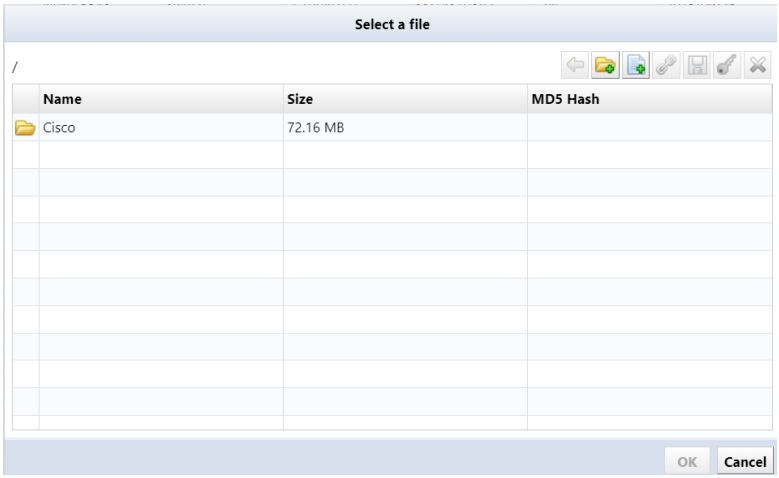
You can remotely distribute IOS to Cisco IOS devices. To use this feature, you must save the IOS in advance.



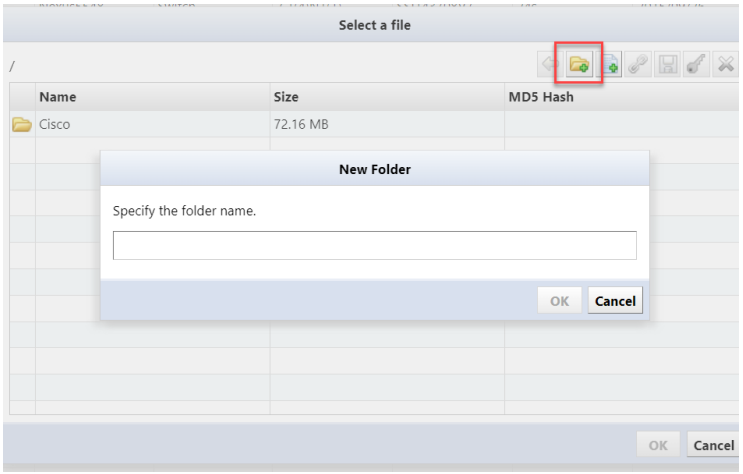
Setting	Explanation
Select an IOS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device. Depending on the model, flash/usbflash0/nvram - The content that can be specified differs.
Destination flash directory	A directory within the destination drive partition. If the directory does not exist, a directory with the specified name will be automatically created.
Destination flash partition	Partition of the destination drive. The command will fail if the specified partition does not exist.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time
Minimum DRAM in Kilobytes (from CCO)	Please check the DRAM capacity of the image to be submitted and enter it. Check if there is enough free space on the device before deploying the image

8.20.13 Manage OS Images

Save the OS image used for software distribution on the server's file system. Click the button and add the OS image file.



You can add a directory on the server's file system by clicking the button.

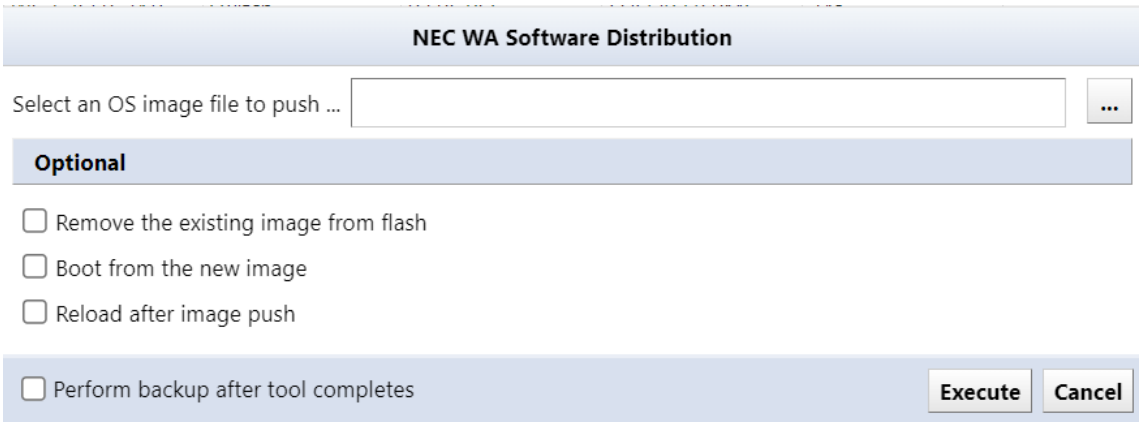


Once the OS image is added to the list, click the [OK] button.

Adding the OS image may take some time. If it takes too long or is not added, check the specified directory and try adding the file again.

8.20.14 NEC WA software distribution

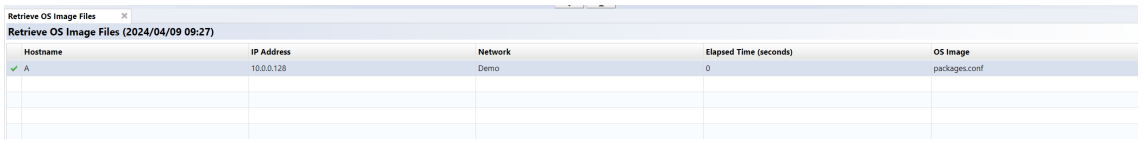
NEC WA software can be distributed remotely to the OS. To use this function, you must save the WA software in advance.



Item	Explanation
Select an OS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time

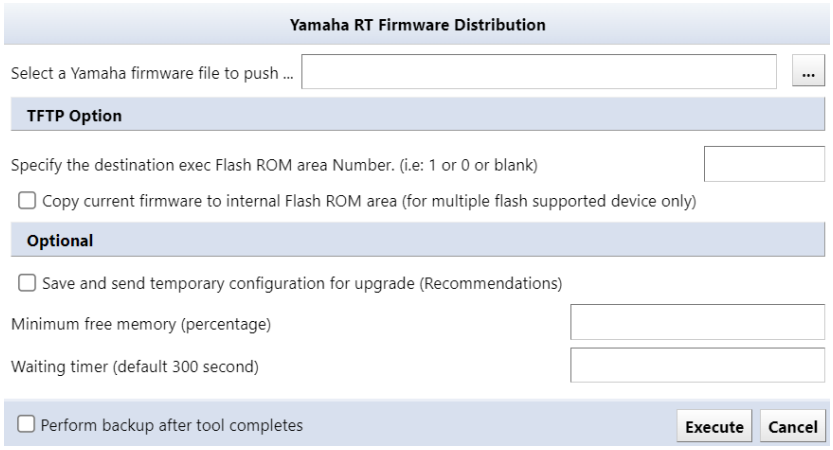
8.20.15 Retrieve OS image files

Downloads the OS image from the specified device and saves it to the database. Downloaded images can be uploaded again later.



8.20.16 Yamaha RT Firmware Distribution

Yamaha RT software can be distributed remotely to the OS. To use this function, you must save the Yamaha RT software in advance.



Item	Explanation
Select a Yamaha firmware file to push	Select target firmware file
Specify the destination exec Flash ROM area Number. (i.e: 1 or 0 or blank)	For models that support multiple firmware, you can select ROM area number (1,0). If not specified, the running firmware will be upgraded.
Copy current firmware to internal Flash ROM area (for multiple flash supported device only)	Back up the running firmware on models that support multiple firmware.*1
Save and send temporary configuration for upgrade (Recommendations)	Save the settings and execute the command before uploading the firmware.*2
Minimum free memory (percentage)	It is possible to cancel the firmware upgrade if the configured memory is exceeded*3
Waiting timer (default 300 seconds)	Specify standby time in environments with high network communication delays

Note

1. *Since Rev.14.01.14, firmware will be backed up in these cases.

```
No.   Revision
-----------------------------------
  0   Rev.14.01.11
* 1   Rev.14.01.14
-----------------------------------
```

If this check is performed on a model that does not support multiple firmware, the firmware upgrade will be aborted. The upgrade will also be canceled if the ROM number of the revision destination and the ROM number of the running firmware are the same.

2. *The following command will be executed:

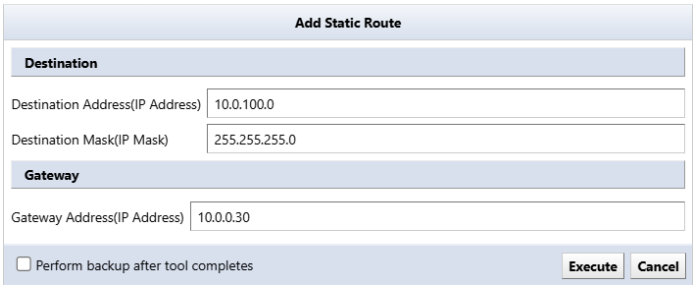
```
login timer [timer]
show config \| grep "tftp host"
tftp host [NetLD IP]
```

3. *If the memory usage is below, firmware upgrade will be canceled by setting 80.

```
CPU:    0%(5sec)   0%(1min)   0%(5min)    Memory: 82% used
Packet-buffer:   0%(small)   0%(middle)   7%(large)   0%(huge) used
```

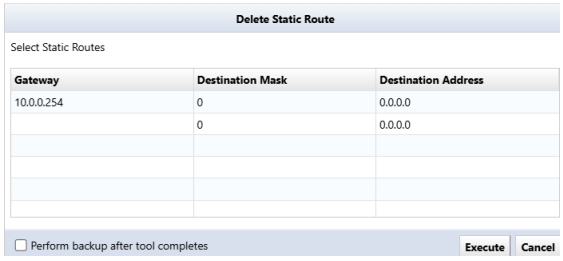
8.20.17 Add Static Route

Enter the required information, click Execute to add the route.



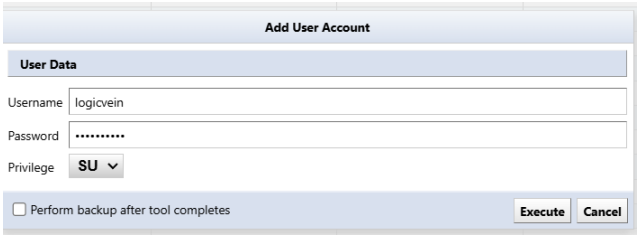
8.20.18 Delete Static Route

Select and delete an existing static route configuration.



8.20.19 Add User Account

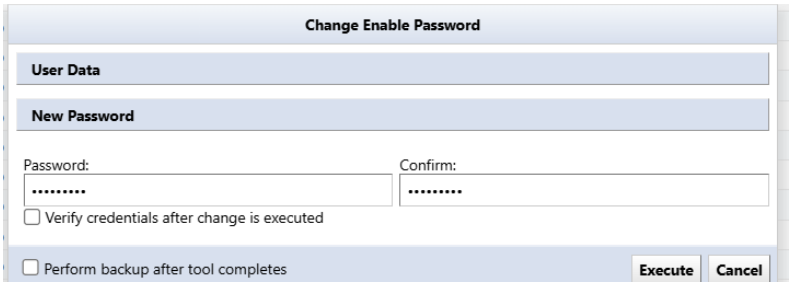
Add a new user account to your device. Please note that this function cannot be executed when multiple devices are selected.



8.20.20 Change Enable Password

Change the Enable Password or Enable Secret settings for your device:

- If Enable Password is set, Enable Password is changed.
- If Enable Secret is set, Enable Secret is changed.
- If both are set, Enable Secret will be changed.



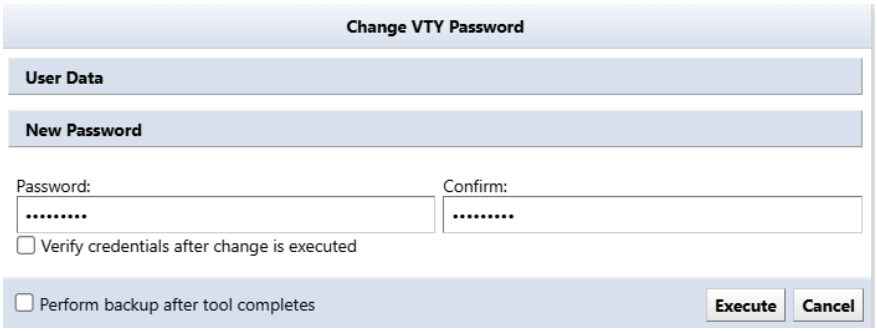
If static credentials are being used, by checking “Confirm credentials after change”, the credentials will be automatically changed, and you will be checked to see if you can log in with thempassword you set.

8.20.21 Changing Local User Password

Change the password for the user account set on the device.

8.20.22 Change VTY Password

Change the device's VTY Password settings.

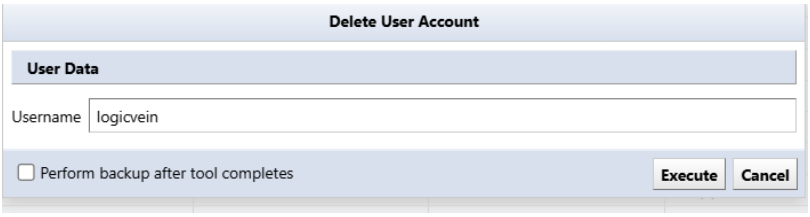


Just as with changing Enable Password by checking "Confirm credentials after change", the credentials will be automatically changed.

Test your new password after changing.

8.20.23 Delete User Account

Delete an existing user account configured on the device. Please note that this function cannot be executed when multiple devices are selected.



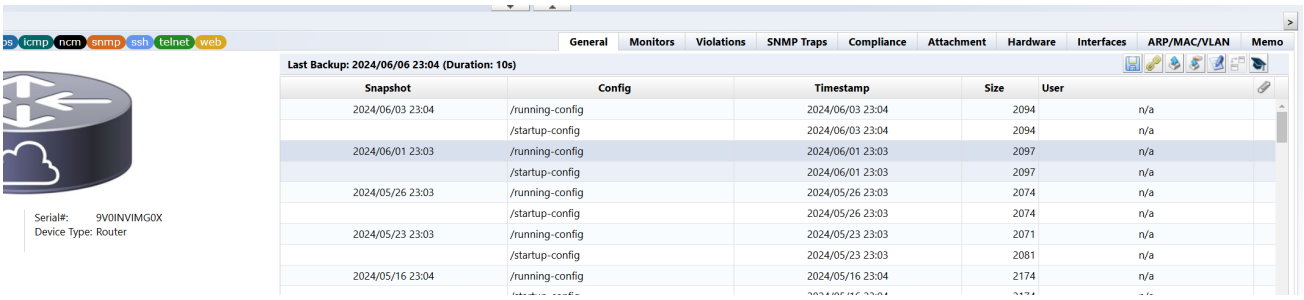
8.21 Change advisor Suite

Change Advisor analyzes current/specified configurations and outputs any changes in configuration. It generates necessary CLI commands for configuration changes, allows command review/editing before execution, and logs execution results in job history.

Change Advisor is not available on some devices.

8.21.1 Change advisor setup

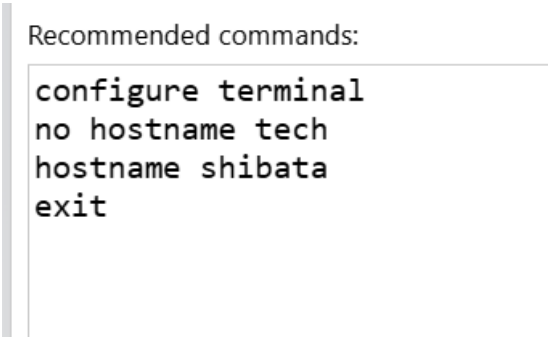
1. Doubleclick the device in the device view.
2. Select a configuration from configuration history or draft.
3. Click the  button.



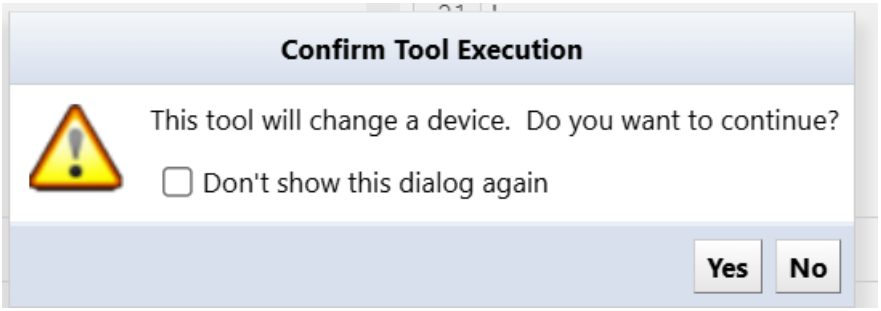
4. Change Advisor starts and presents commands in the lower panel.

8.21.2 Execute commands using change advisor

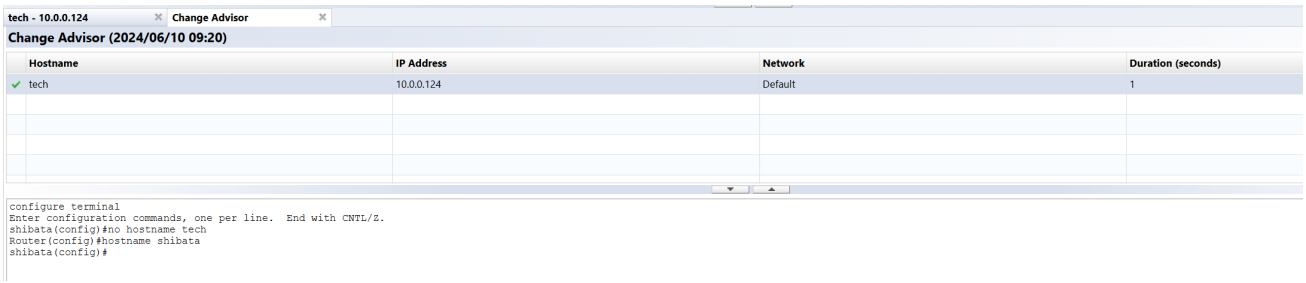
Commands output by Change Advisor can be executed on the device. Double check the command you want to run before executing the suggested command. If an incorrect command is antered, you can directly edit the output command.



To proceed, click [Run], then [Yes].



You can check the result after executing the command. Change Advisor execution results and history are also displayed in the job history.



Note

TFTP is the primary communication protocol for Configuration Restore and Draft Configuration upload. Therefore, restore and upload functionality is not available on devices that do not implement TFTP. However, the Change Advisor function can be used by most models as long as CLI login (telnet/SSH) is supported. Therefore, you can use the Change Advisor function as a substitute even in environments where uploading is not possible.

8.22 Smart change Suite

The smart change feature is similar to the command runner, but with more flexibility. Instead of issuing one fixed command, you can create a template of the command and set template variables to change the value of the variable for each device.

For example, if you want to change the password of a device, but you want to set a different password for each device, you will need to run a job for each device in the command runner.

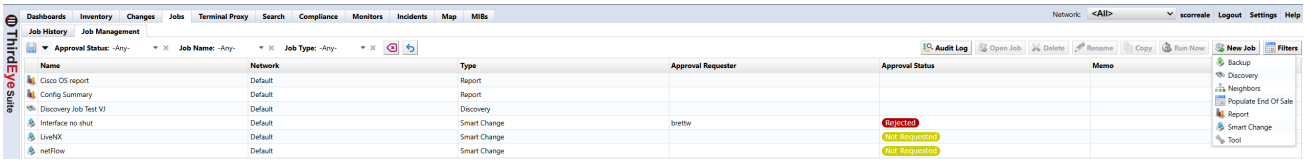
However, by using smart change, you can change passwords into variables and assign different values to each device, allowing you to set different passwords in one job.

8.22.1 Create a smart change job

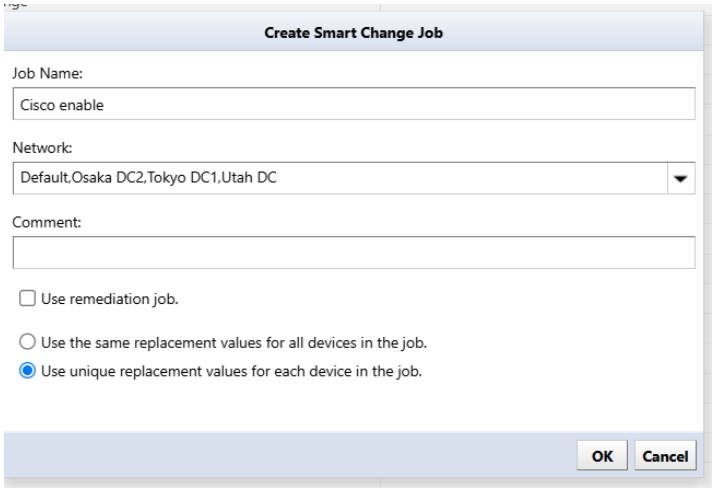
Smart change jobs can be created from the Jobs> [Job Management] tab. More information is available in the **Job management** section.

To create a job:

1. Click the [Job] > [Job Management] tabs, then click [New Job] > [Smart Change].



2. Enter the job name and comment, select the function, and click [OK].

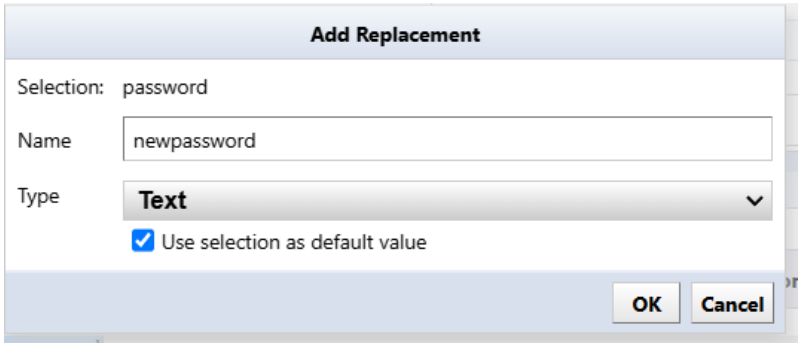


Item	Explanation
Job name	Enter the name of the smart change job.
Comment	Enter a comment (description) for the smart change job.
Use remediation job	Select whether to use smart change jobs as repair jobs. If selected, additionally select an adapter.
Use the same replacement values for all devices in the job / Use unique replacement values for each device in the job	Choose one. When executing a command, you can choose whether to execute it with the same value in the variable or with a different value.

3. In the template, enter the base command.

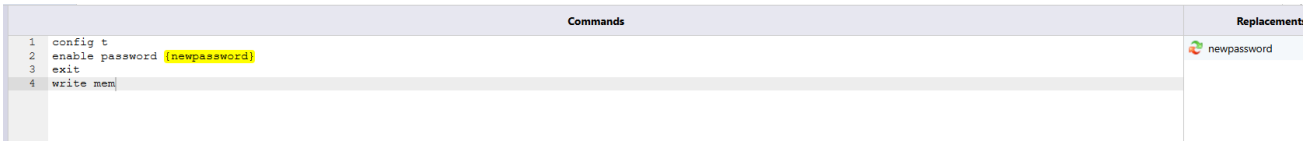
4. Select the part you want to change as an alternative value, click the  button.

5. Enter a name for the alternative value and select a type.

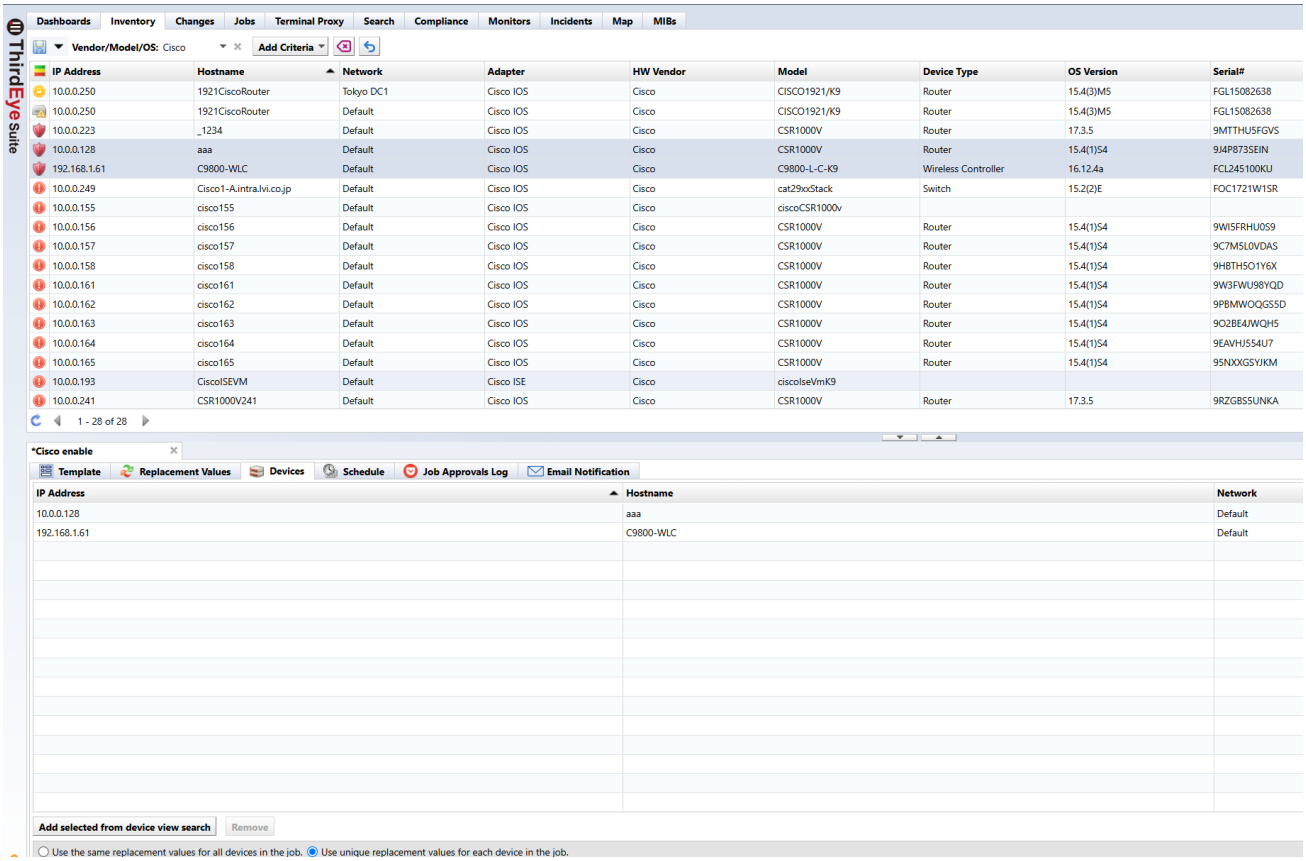


Item	Explanation
Text	Any text
IP address	IP address. If a value other than the correct IPv4 or IPv6 format is entered, an error will be reported.
Hostname	Hostname
IP address or hostname	IP address or host name
Choice	When entering an alternative value, you will be able to select it from a drop-down list. It is safe because only the preset values will be entered.
Condition selection	Provide a checkbox to enable or disable it. For devices marked as disabled, the alternative value is an empty string.

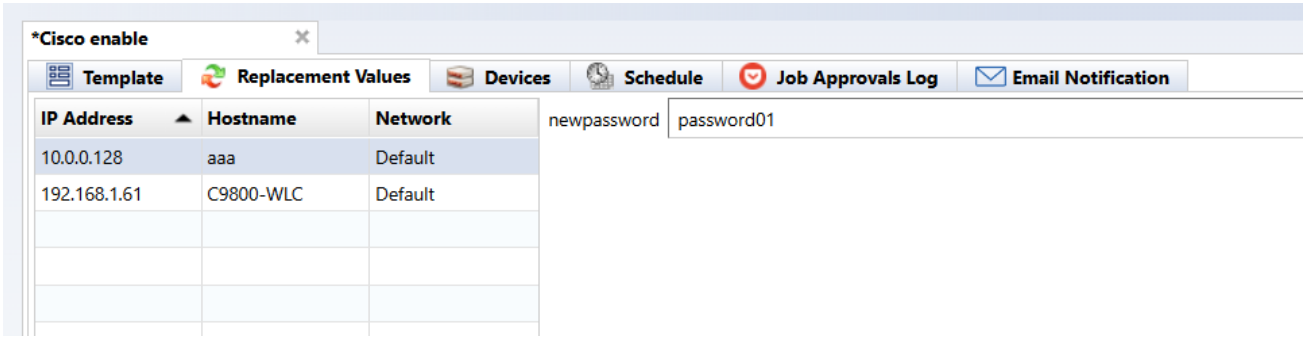
Variable parts are displayed in yellow.



6. Add the device you want to run on the Devices tab.

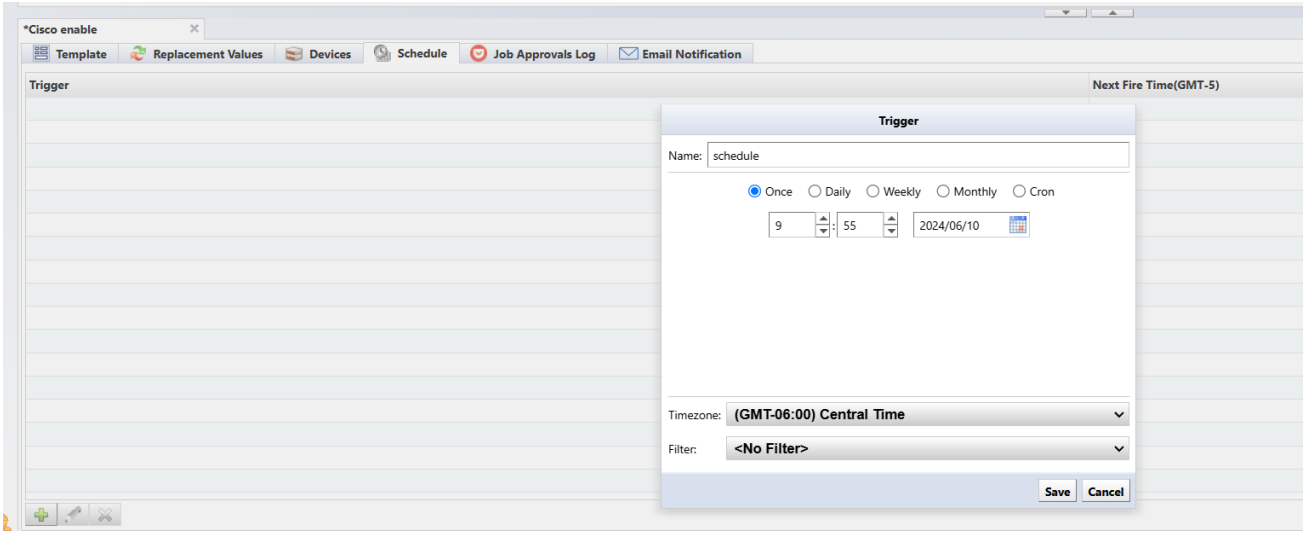


7. On the Replacement Values tab, enter the values.

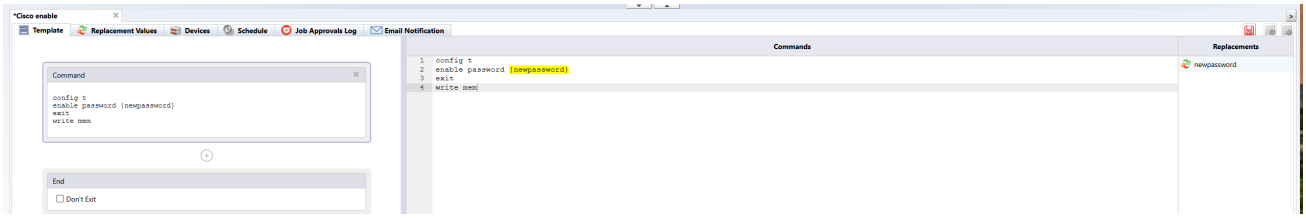


Alternative data can be can be imported/exported via Excel file using the (export) or (import) buttons.

8. Add triggers on the [Schedule] tab by clicking the the button in the lower lefthand corner of the window.

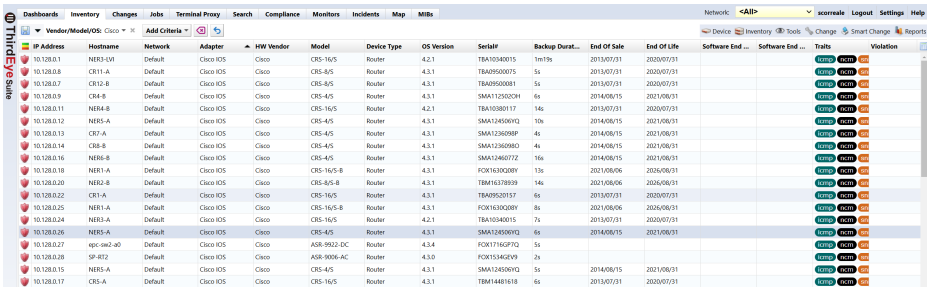


9. Click the button to save the job.



8.23 Device EOS/EOL management

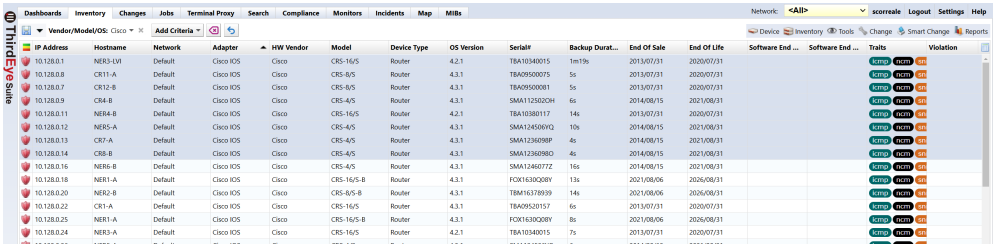
To manage EOS/EOL, “End of Product (EOS)”/“End of Support (EOL)” columns have been added to the inventory. EOS/EOL information can be configured manually or by importing from an Excel file, or automatically configured for Cisco devices using the Cisco Support API.



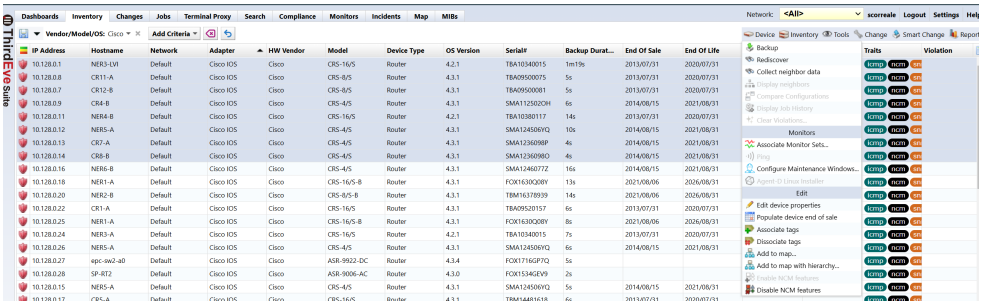
8.23.1 Manual setting

8.23.1.1 Procedure

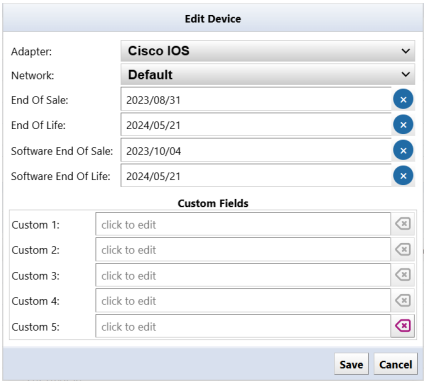
1. Select the device to set EOS/EOL.



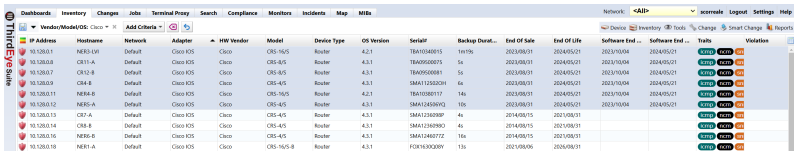
2. Click [Edit device properties] from the inventory menu.



3. Select the product end of life and end of support dates and click [Save].



By following the above steps, the date set in the column will be displayed.



8.23.2 Automatic configuration Suite

8.23.2.1 Prerequisites

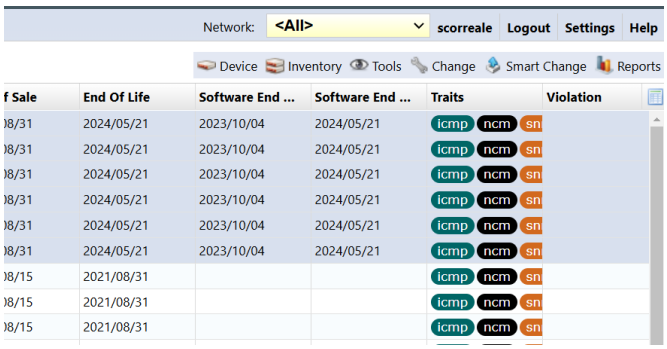
- The ThirdEye you are using must be able to connect to the Internet.
- You must log in with your Cisco account and obtain an API key and secret code before accessing Cisco Smart Net Total Care.
- Valid Cisco Smart Net Total Care (SNTC) required.

Please see below for information on obtaining API.

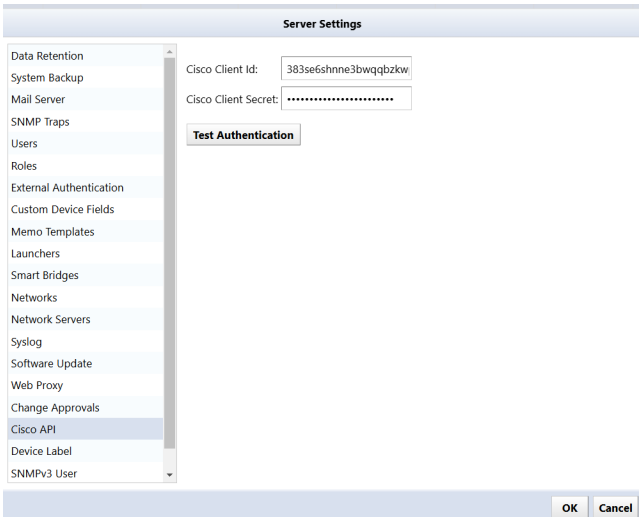
(https://developer.cisco.com/docs/support-apis/#!user-onboarding-process)

8.23.2.2 Procedure (online environment)

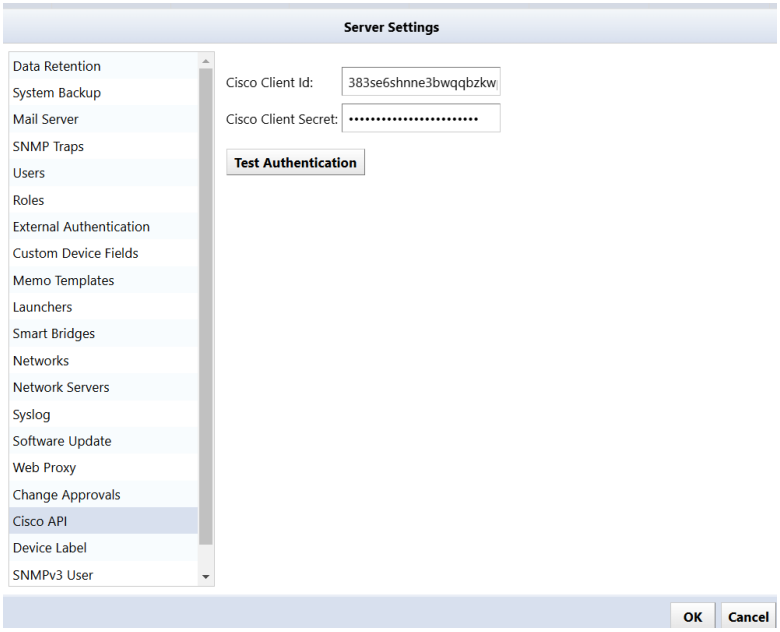
1. Click Settings.



2. Click on Cisco API.

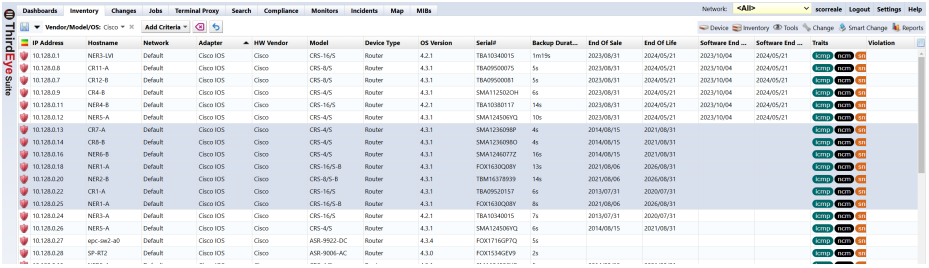


3. Enter your API key and secret code and click [OK].

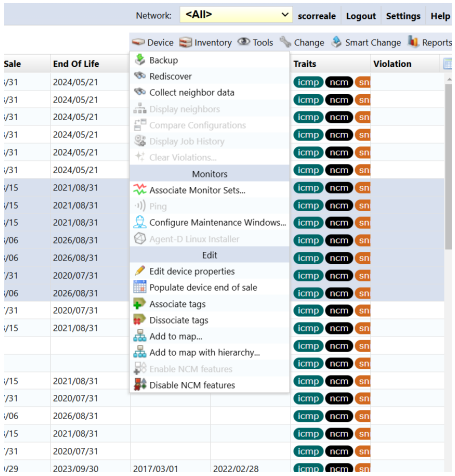


By clicking Authentication Test, you can check whether the ID and Secret code you entered can be used.

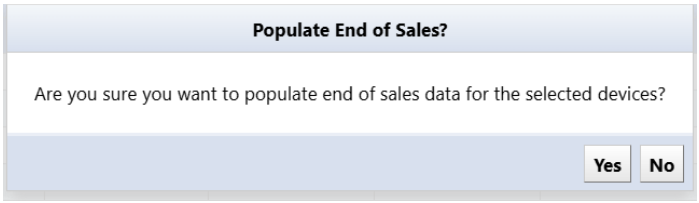
4. Select the device to obtain EOS/EOL.



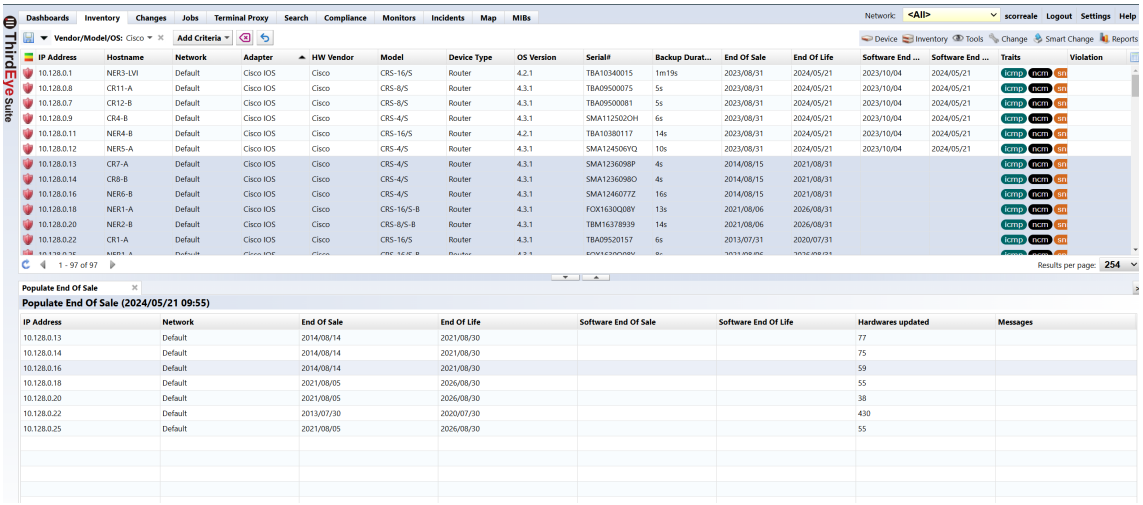
5. Click “Populate device end of sale” from the Device menu.



6. Click “Yes” on the screen below.

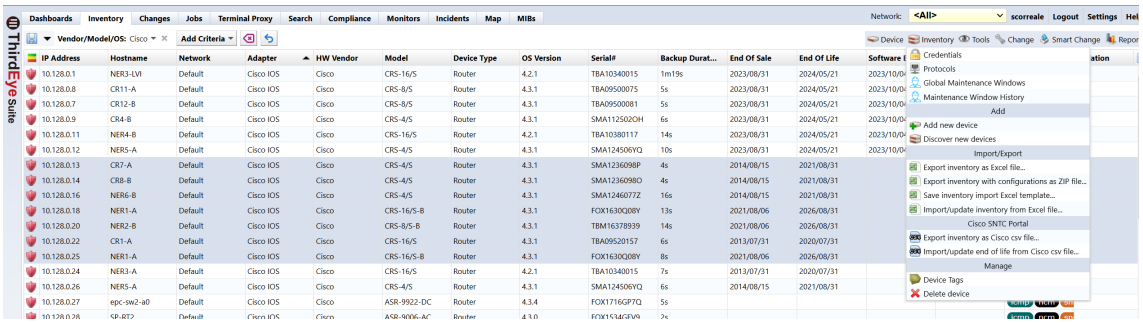


Using the above steps, EOS/EOL information will be automatically acquired and registered in the column.



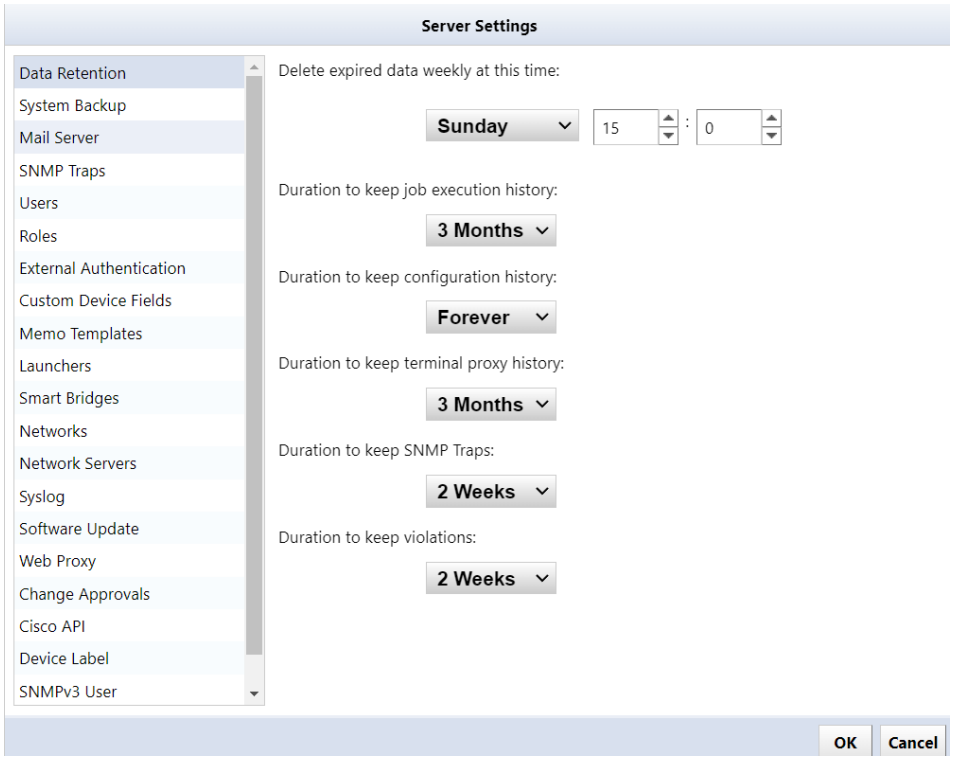
8.23.2.3 Procedure (offline environment) If ThirdEye cannot connect to the Internet, it will not be able to retrieve the end-of-sale date from the Cisco server. However, you can export your inventory as a csv file and use it for import into Cisco services. You can then export the csv file from your Cisco service and import it into ThirdEye to update the end of support date. Note that Cisco services do not include the end-of-sale date in the export file.

To export a csv file that can be used for import into Cisco services, select Export Inventory as CSV from the inventory menu.



8.24 Change data retention period

Data retention period sets the data retention period and automatic deletion timing.



Field	Explanation
Delete expired data weekly at this time	Data that has passed a certain period of time is automatically deleted every week on a specified day and time. (Initial value: Monday, 6:00) Specify the data retention period in the following items. (*However, if you specify “No expiration date”, the data will not be deleted)
Duration to keep job execution history	Specify the retention period for data on the [Job] > Job History tab from one of the following options. (Initial value: 3 months) `"Forever"`, `"3 months"`, `"6 months"`, `"9 months"`, `"1 year"`
Duration to keep configuration history	Specify the configuration retention period for each monitored device from the following: (Initial value: Forever) `"Forever"`, `"6 months"`, `"1 year"`, `"2 years"`, `"3 years"`, `"4 years"`, `"5 years"`, `"6 years"`, `"7 years"`

Field	Explanation
Duration to keep terminal proxy history	Specify the retention period for data on the Terminal Proxy tab from one of the following options. (Initial value: 3 months) `"Forever"`, `"3 months"`, `"6 months"`, `"9 months"`, `"1 year"`, `"3 years"`
Duration to keep SNMP trap	Specify the retention period for data on the Monitors > [SNMP Trap] tab from one of the following options. (Initial value: No deadline) `"No deadline"`, `"2 weeks"`, `"3 months"`, `"6 months"`, `"1 year"`
Duration to keep violations	Specify the retention period for data on the Monitors > [Violations] tab from one of the following options. (Initial value: No deadline) `"No deadline"`, `"2 weeks"`, `"3 months"`, `"6 months"`, `"1 year"`

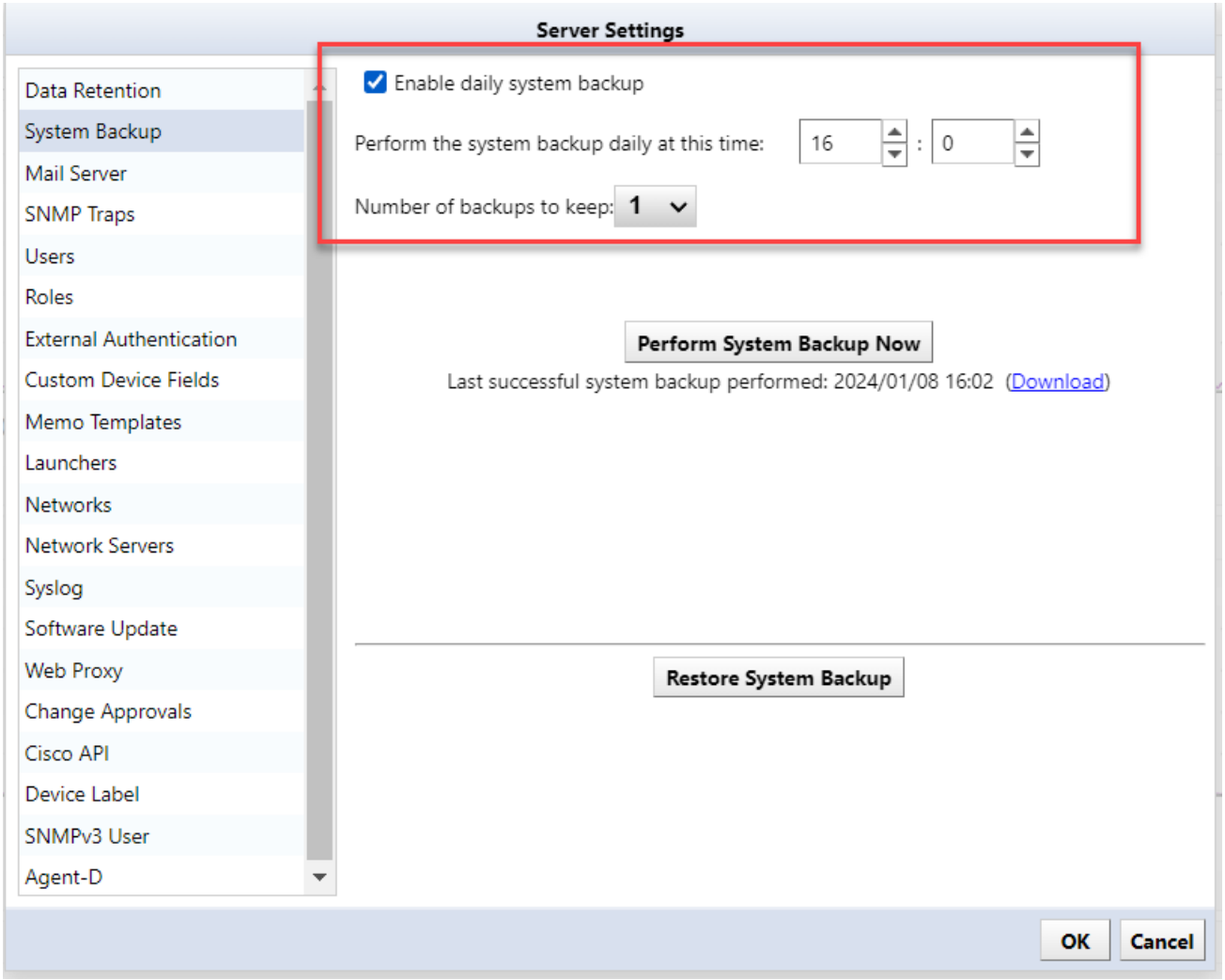
9 System backup/restore

A system backup is a backup of the entire {{ProductName}}. You can backup/restore various settings and monitor data (polling, SNMP traps, etc.).

To perform a system backup, click Settings > [System Backup] .

9.1 Perform system backup automatically

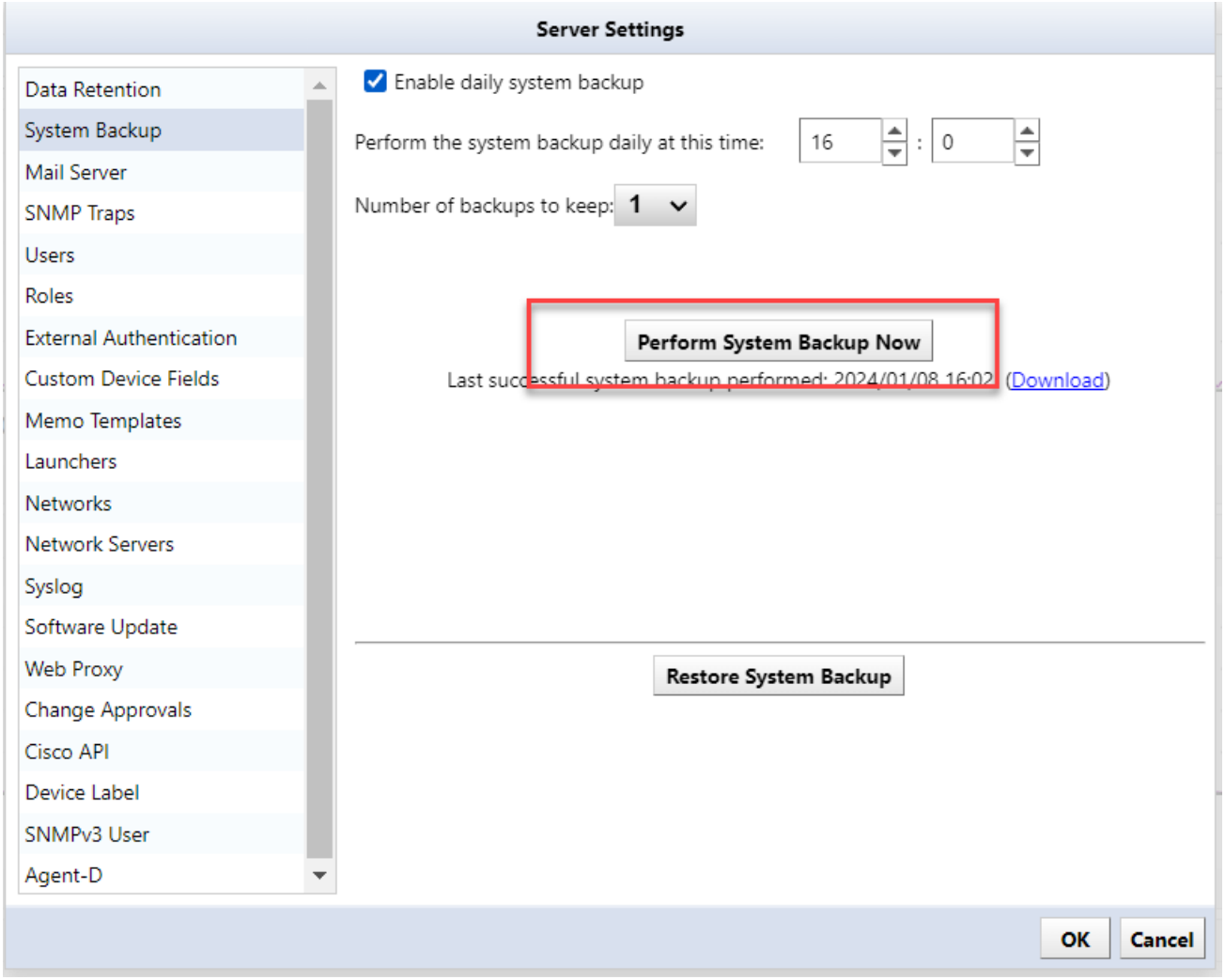
Automatica system backups are enabled by default. If you want to disable it or change the time for automatic nsystem backup, change the contents in the red frame below.



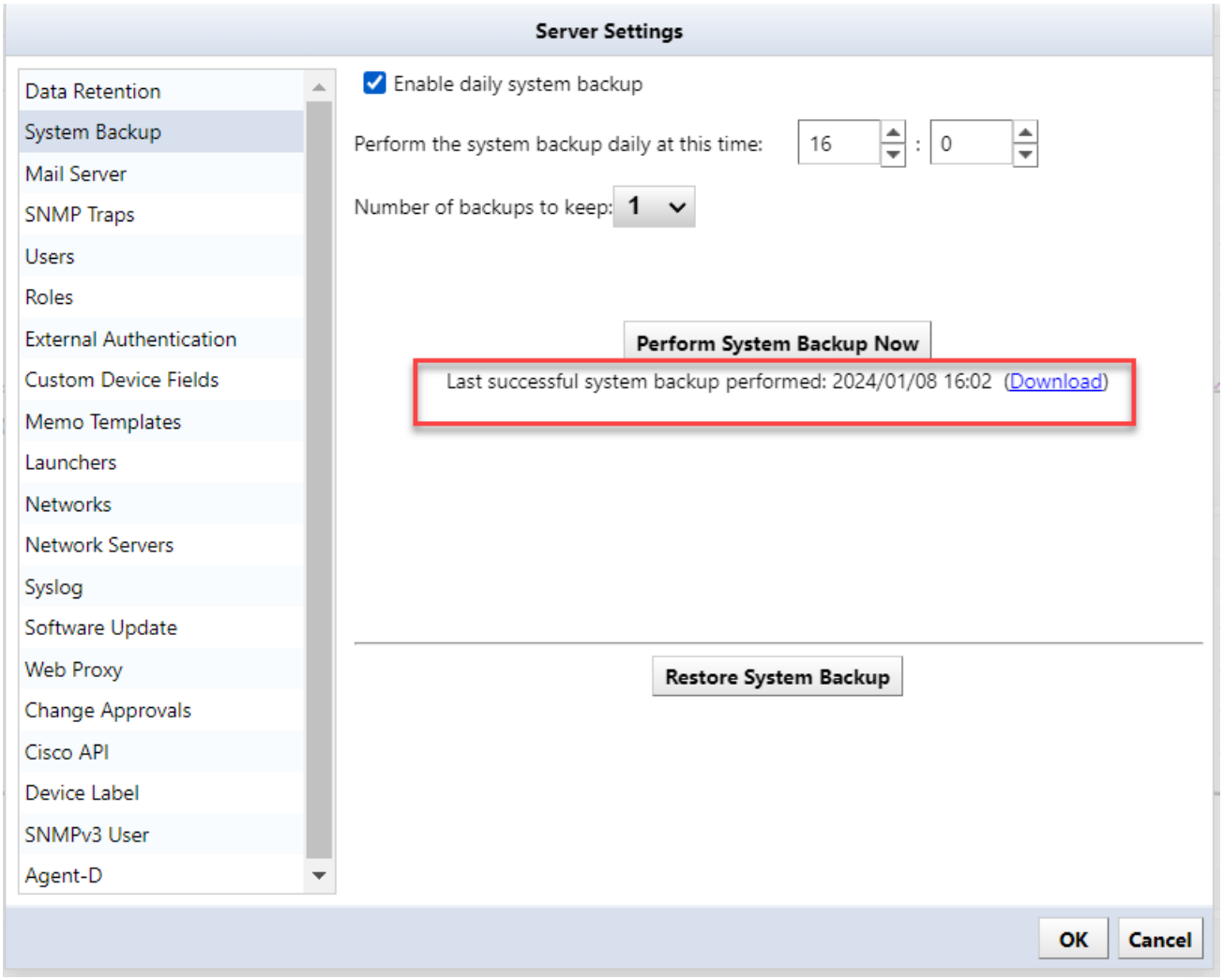
Item	Explanation
Enable daily system backups	Enable daily system backups. If this setting is enabled, a system backup will be performed at the specified time. (Initial value: `Enabled`)
Perform the system backup daily at this time	Specify the execution time for daily system backups. (Initial value: `7:00`)

9.2 Perform a manual system backup

To perform a manual system backum, click [Server Settings] in the Global Menu, then click [Perform System Backup].



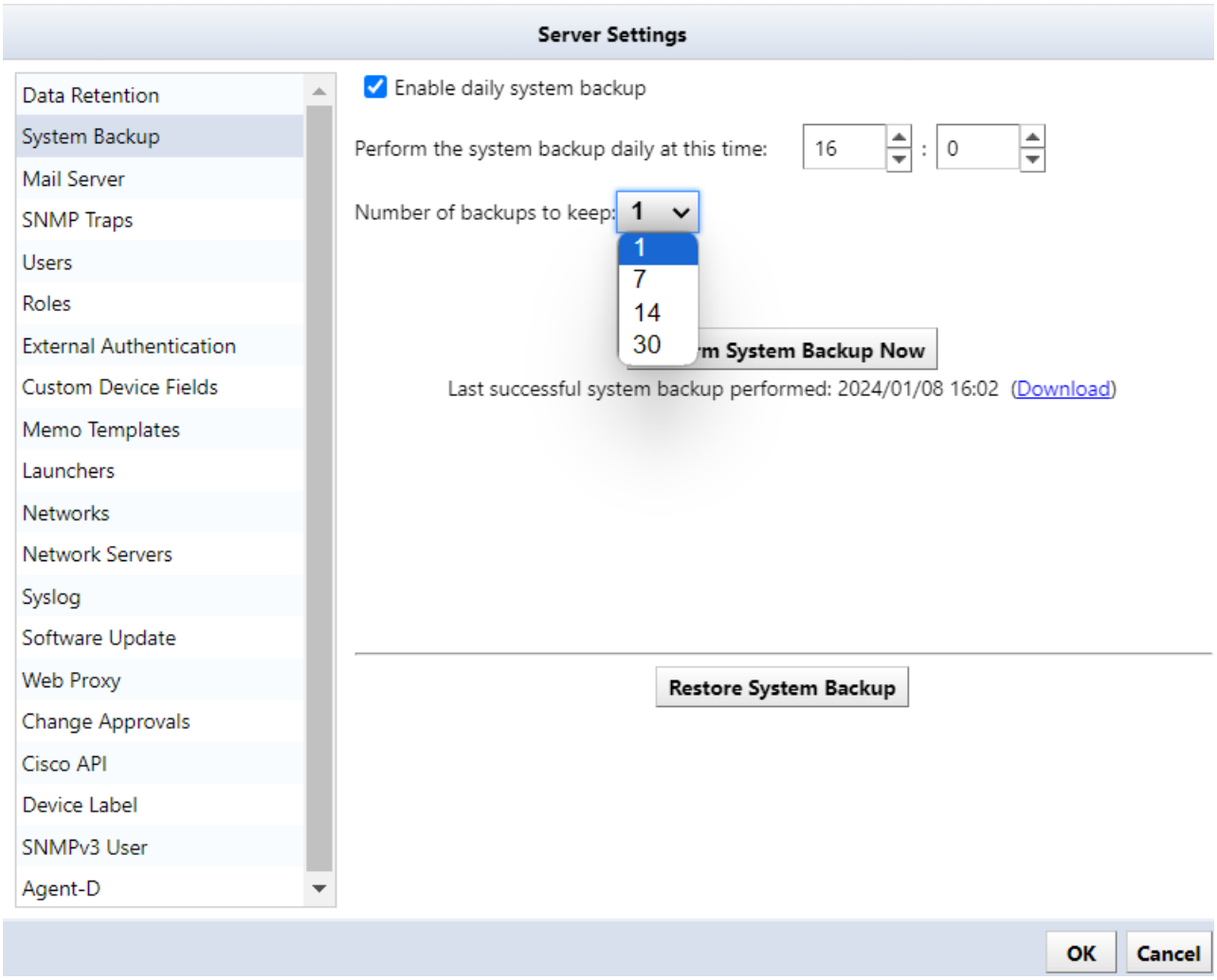
The button is grayed out while a backup is in progress. Once the button becomes clickable, the latest system backup date and time is updated, and the process is complete.



9.3 Change the number of system backups retained

You can select the number of system backups. The default value is 7. Any data that exceeds the selected number of backups is deleted.

Depending on the environment and length of operation period, the number of system backups can accumalate, and consume up disk space. Disk space usage can be reduced by reducing the number of system backups.

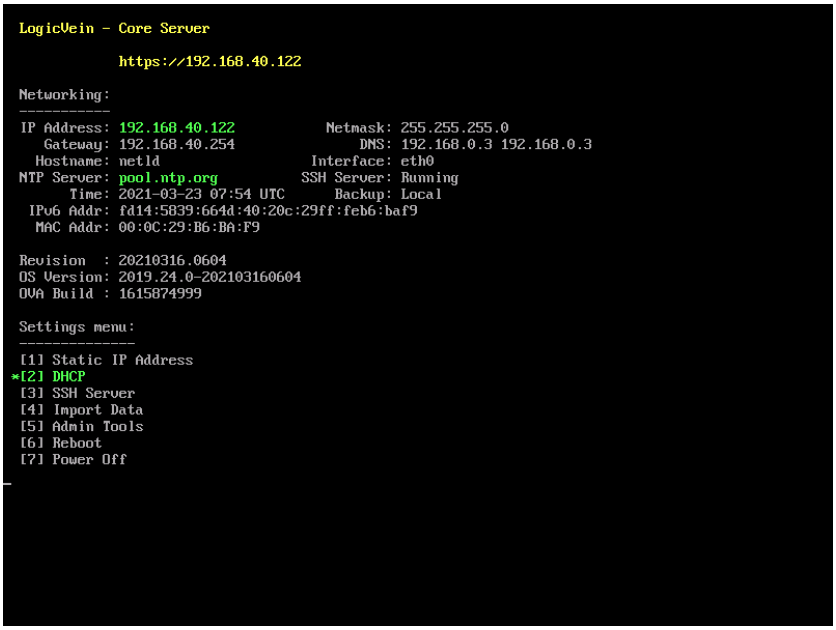


9.4 Save to external storage

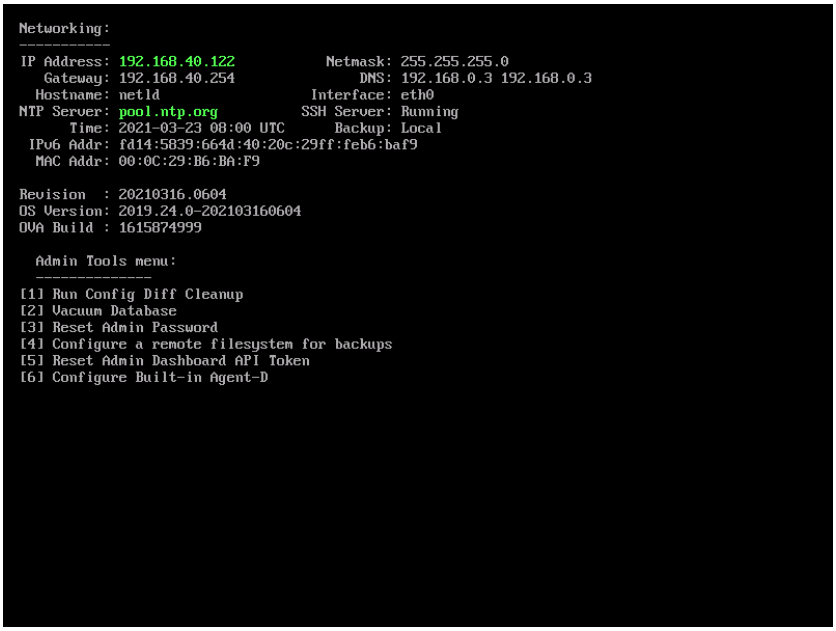
By default, system backup files are stored inside the virtual appliance. However, you can configure external storage to store them automatically outside the virtual appliance. Supported protocols are NFS/SMB.

To set up external storage:

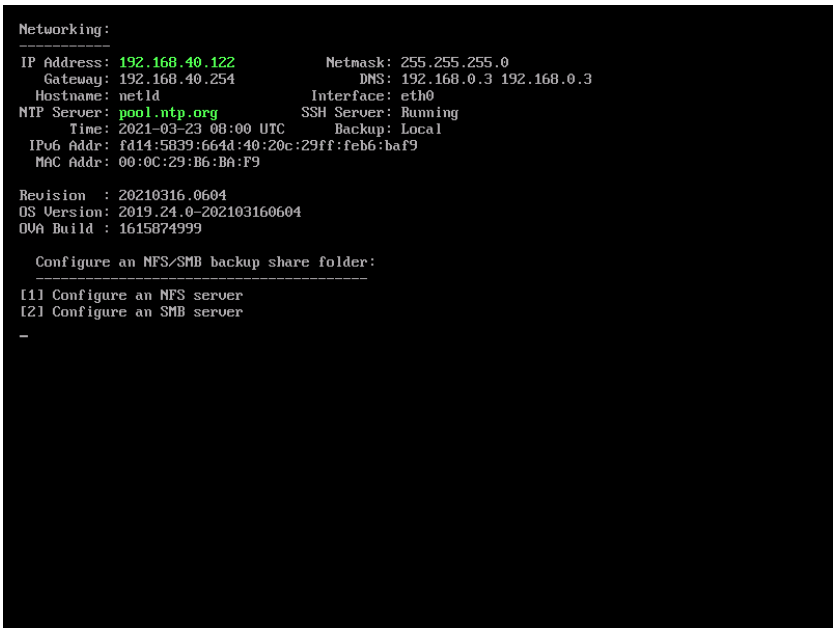
1. Click the [5] key on your keyboard, and select [Admin Tools].



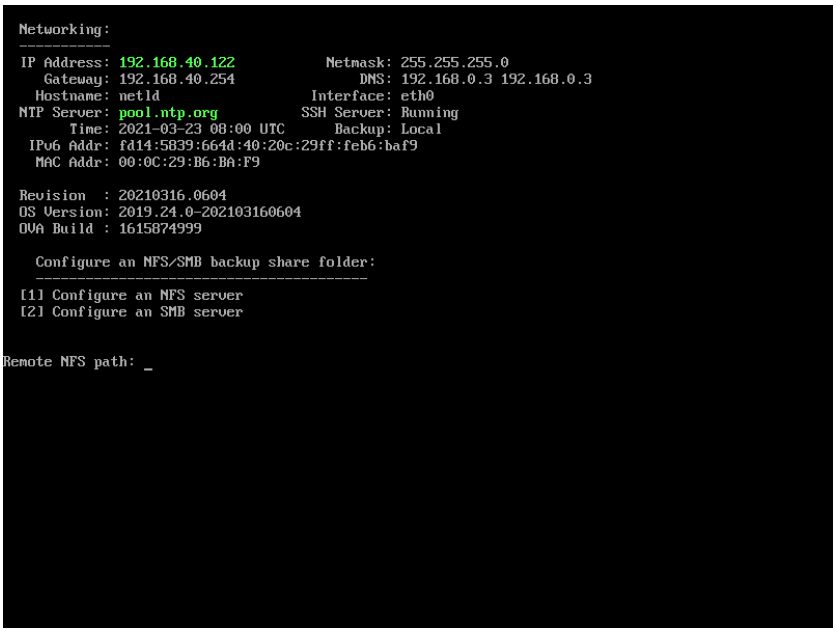
2. Click the [4] key on your keyboard, and select [Configure a remote filesystem for backups].



3. Select the server type.

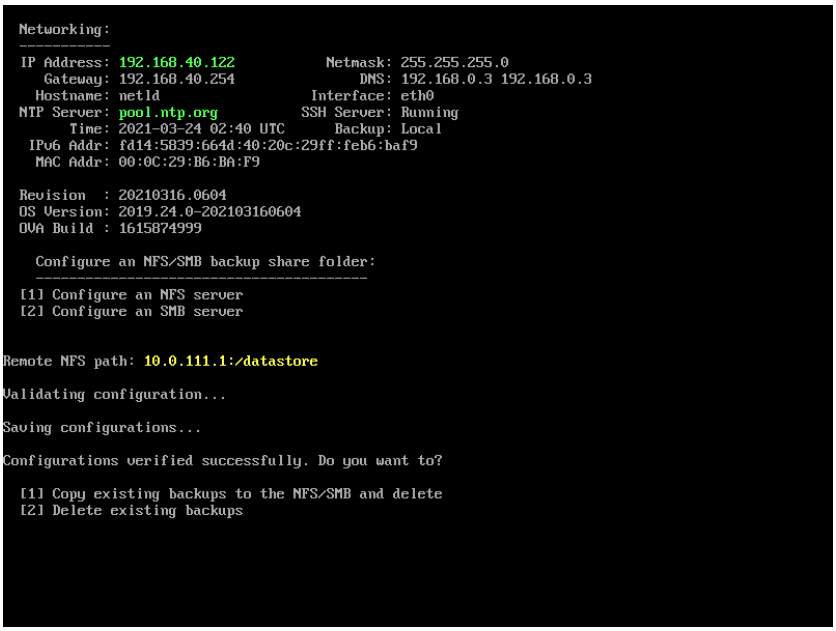


4. Enter the required information and press [Enter].



Item	Explanation
Remote NFS/SMB path	Network path/IP address
Username	Username set on the server. (For SMB only)
Password	Password set on the server. (For SMB only)

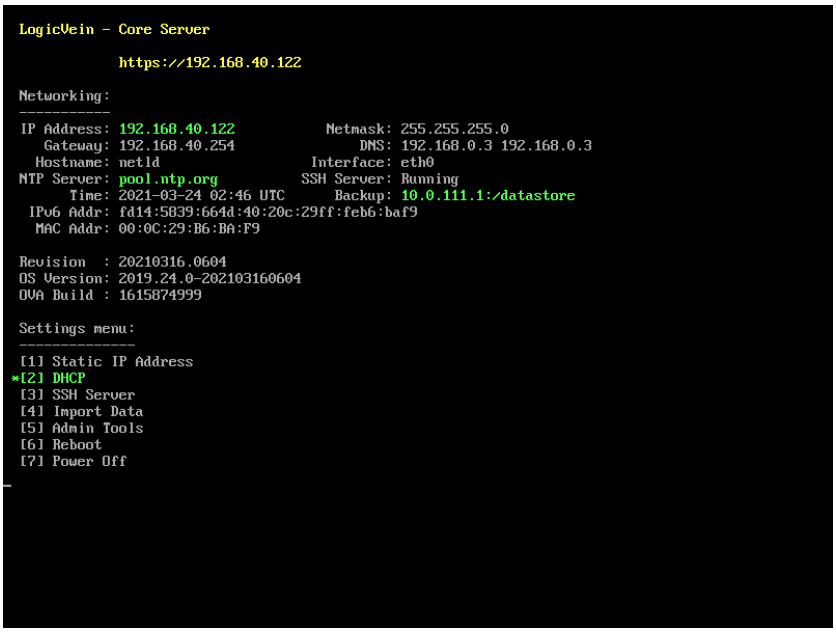
5. Select [1] or [2].



Selection	Explanation
[1] Copy existing backups to the NFS/SMB and delete	Copy existing backups to NFS/SMB and then delete them
[2] Delete existing backups	Delete existing backups

The console screen settings are now complete.

{{ProductName}} will restart automatically, and you can check the settings on the console screen.



9.5 Create system backup zip file

To create a backup zip file on external storage:

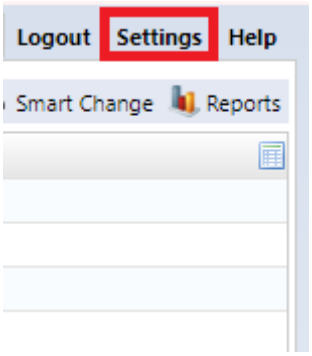
1. Open the backup folder. The folder name will be in the format "`(backup_YYYY\\MM\\DD)`".
2. Save the following three items to a zip file:
   - `pgsql` (folder)
   - `version.txt` (file)
   - `complete` (file)

9.6 Restore system backup from zip file

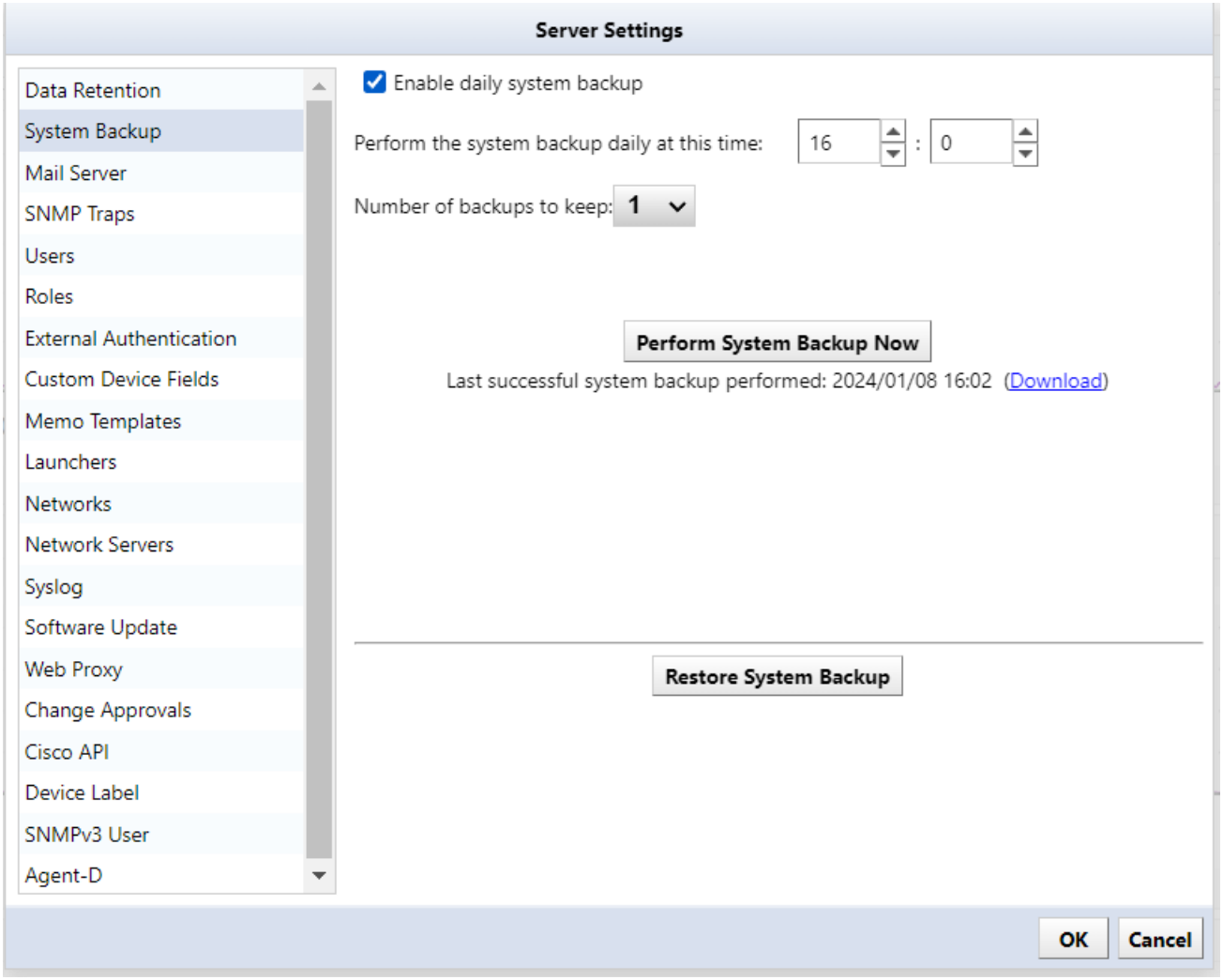
To restore system backup from a zip file, select the backup source and restore destination. It must be the same version (revision).

For information on how to check the version:

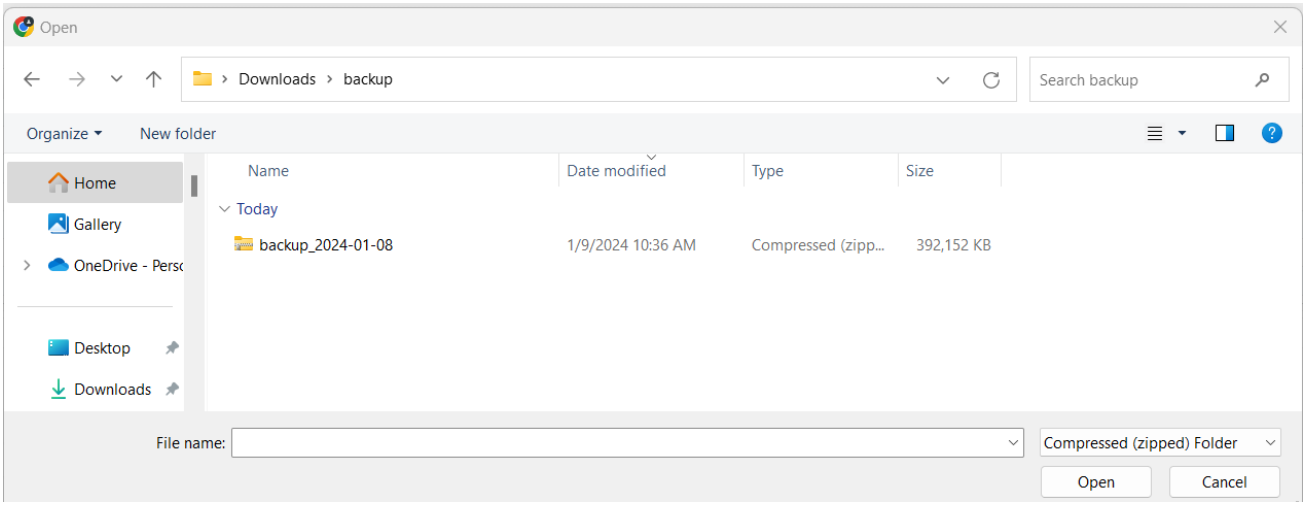
1. Log in as a user with administrator privileges.
2. Click Settings on the Global Menu.



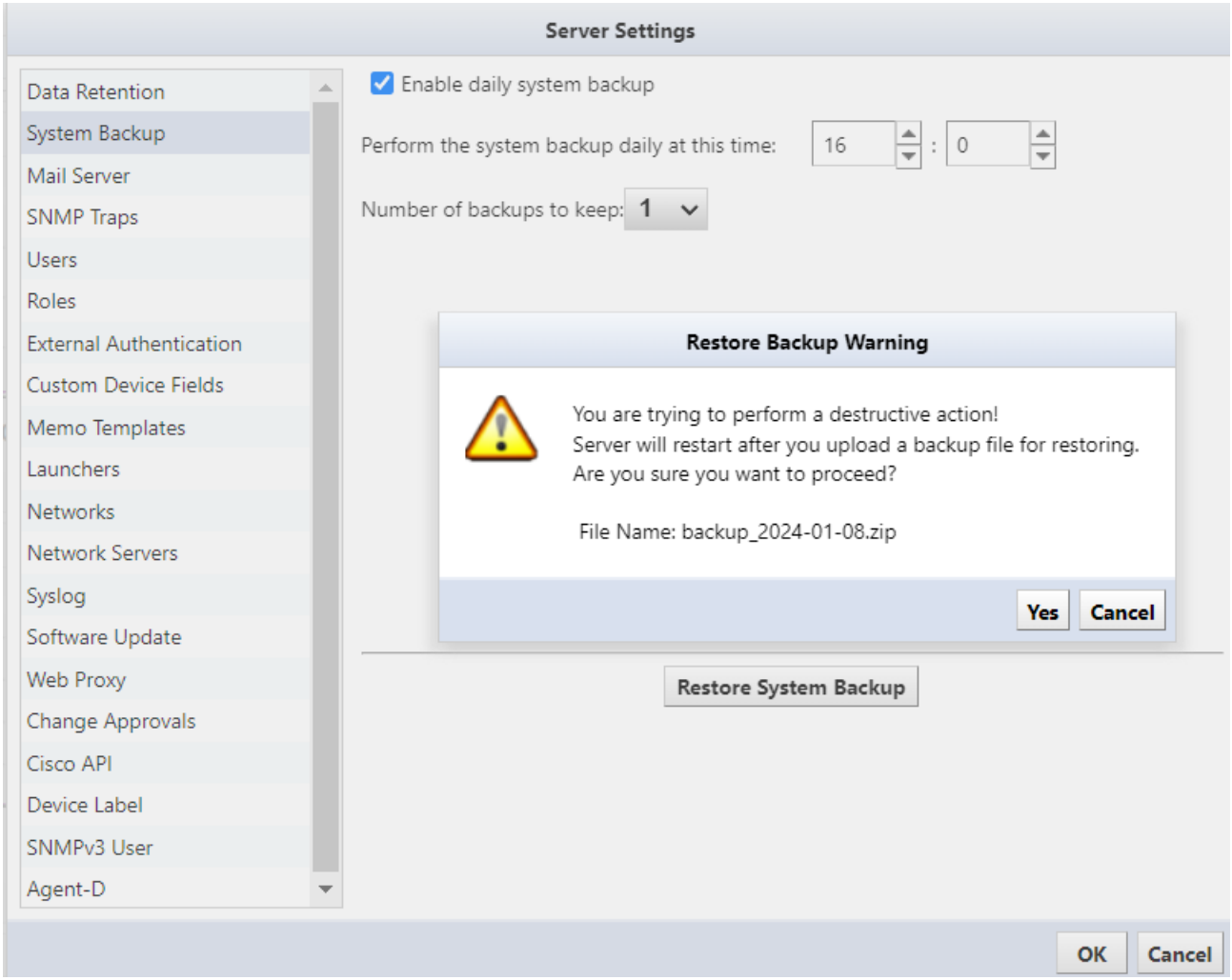
3. Click [System Backup] > [Restore System Backup].



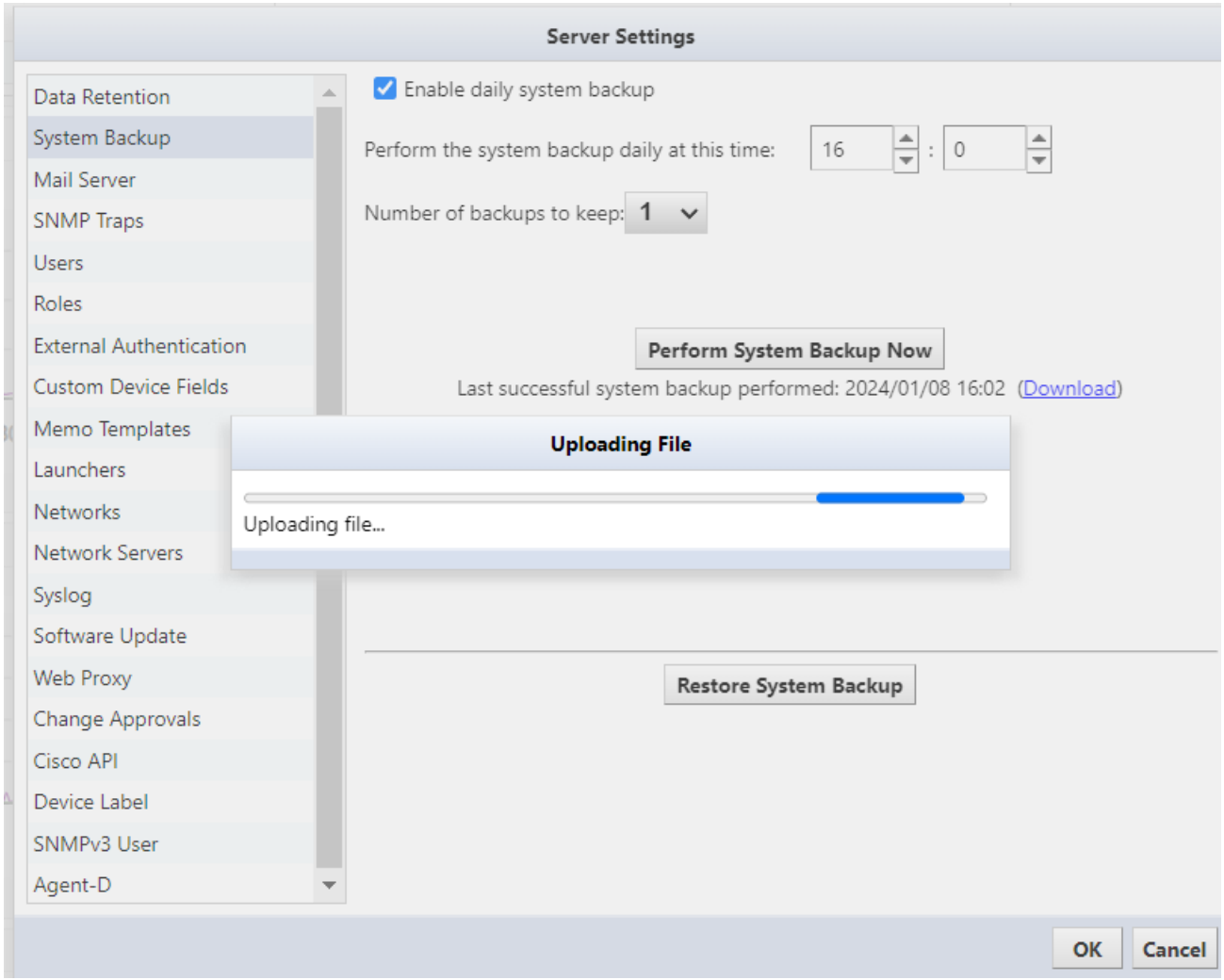
4. Select the file you want to restore, and click [Open].



5. Click [Yes] on the warning screen.



6. The file will be uploaded, and the restoration will begin.

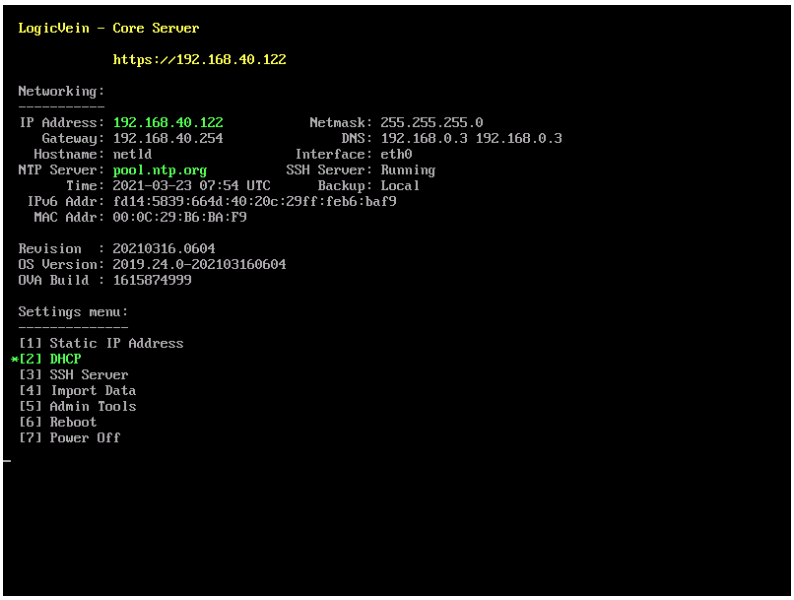


System backup/restore is now complete.

After uploading, the service will automatically restart and return to the login screen.

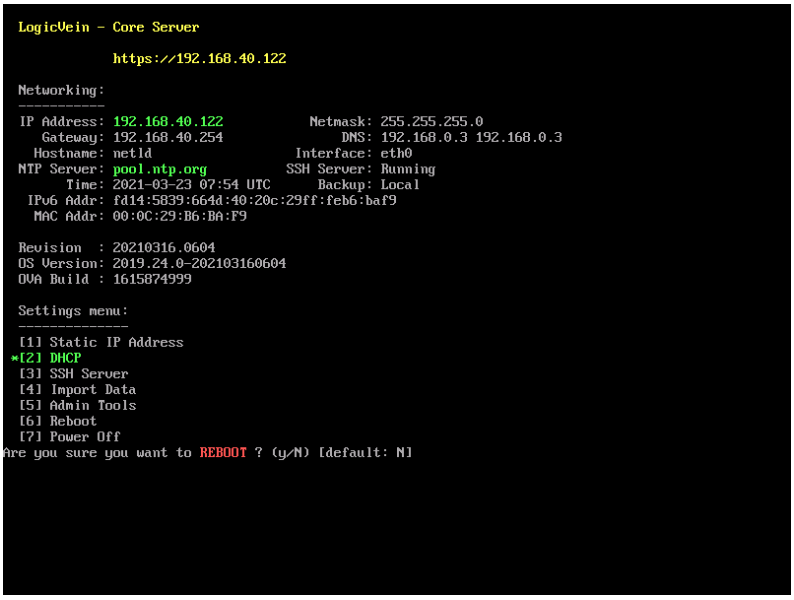
10 Reboot/Shutdown

Reboot and shutdown operations are performed using the keyboard on the virtual machine console.



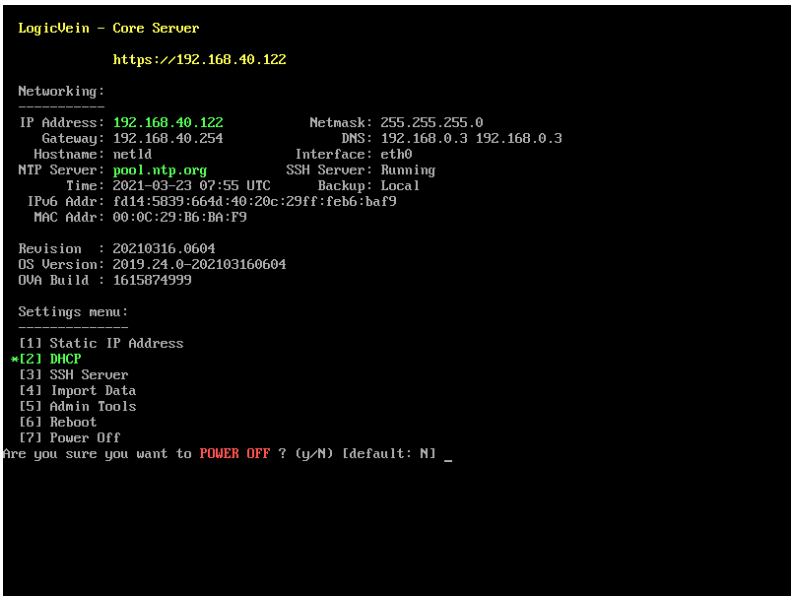
10.1 Restart procedure:

1. Click the [6] key on your keyboard.
2. Choose [Reboot].
3. Press the [Y] key on your keyboard to execute.



10.2 Shutdown procedure:

1. Click the [7] key on your keyboard.
2. Choose [Power Off].
3. Press the [Y] key on your keyboard to execute.

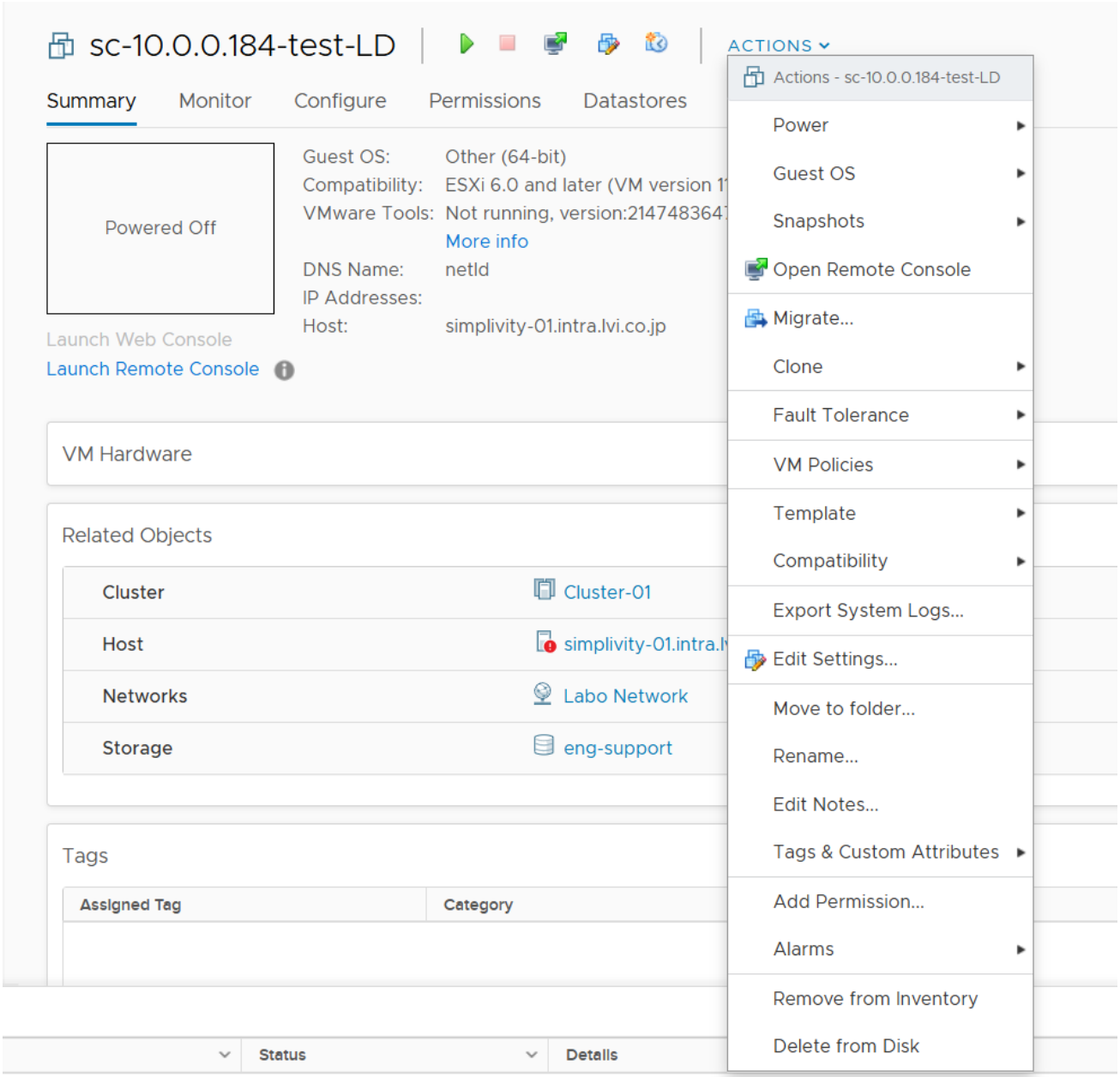


11 Uninstall

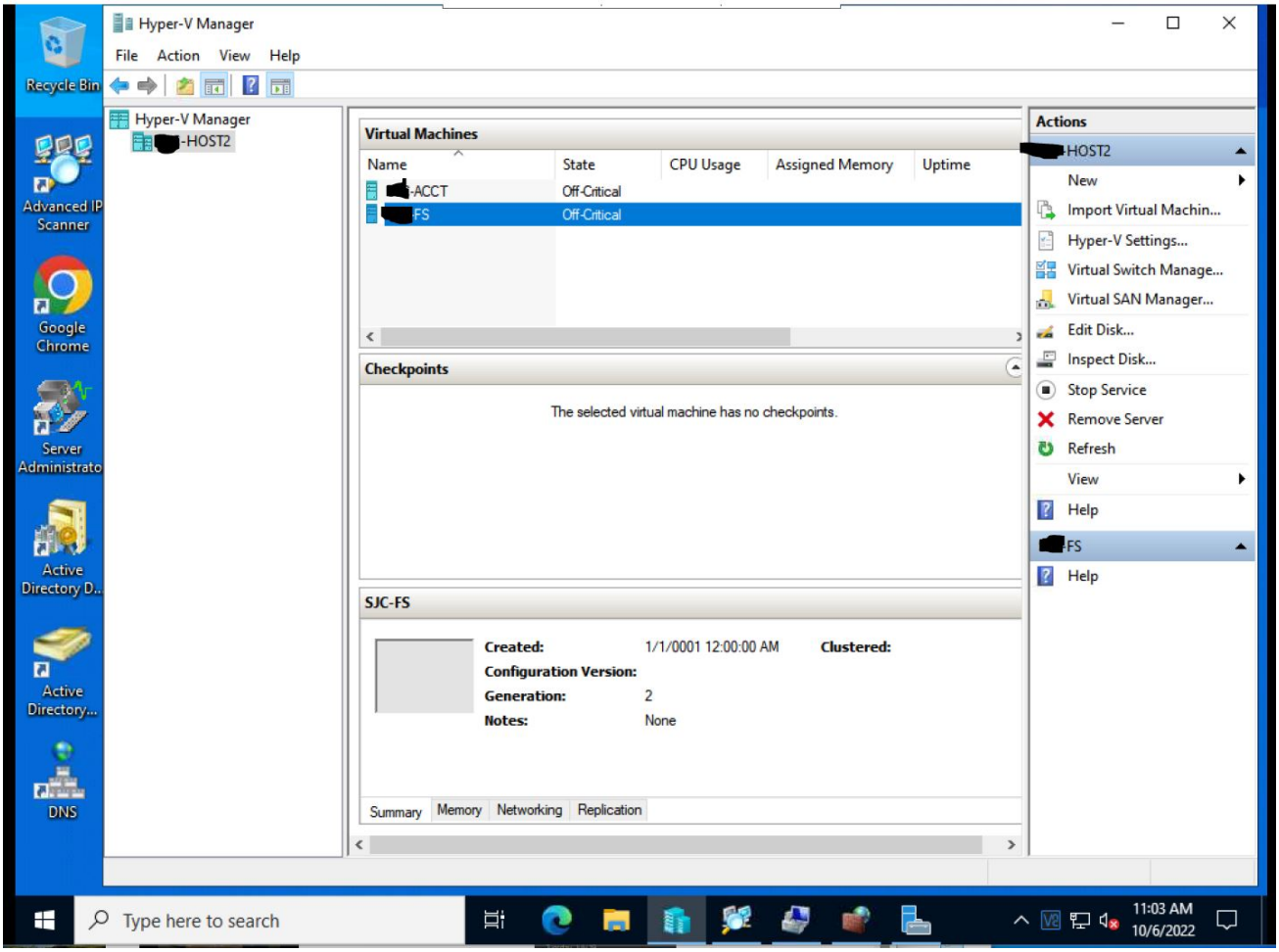
11.1 Uninstall

1. Shut down {{ProductName}}.
2. After the shutdown is complete, delete the {{ProductName}} virtual machine from the virtual host OS.

Example of deletion screen in VMware ESXi:



Example of deletion screen in Windows Hyper-V:



This completes the uninstallation of {{ProductName}}.

12 Inquiries

If you have any problems or questions while using {{ProductName}}, please contact our support team:

LogicVein Support Desk Contact information: Email: support@logicvein.com

Before have the following information ready:

1. Product name
2. Product version information (including revisions)
3. Product serial number ({{ProductName}} license information)
4. Specific issue(s) and questions.
5. A screenshot of the issue (if possible).