LogicVein

ThirdEye

User's Manual

November 4, 2025

Contents

SECTION 1

INTRODUCTION

This document is a manual for the network fault monitoring software “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.

ThirdEye’s capabilities include:

- 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: “ThirdEye” and “ThirdEye Suite”. Available features vary depending on the edition. For functional differences between editions, please refer to the **Main Feature**

Comparison Table by Edition below.

Features and functions in this manual are explained based on the “Suite” edition. Some “Suite” may not be available in the “ThirdEye” edition. 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”.

1.3 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	✗	✓

Function	ThirdEye	ThirdEye Suite
Restoration	✓	✓
Change Tools	✗	✓
Draft Configuration	✗	✓
Terminal Proxy		
Telnet/SSH Connection	✓	✓
Saving Operation History	✓	✓
Dashboard		
Addition	✓	✓
Share	✓	✓
Widget	✓	✓
Report	✓	✓
Incident	✓	✓
Job	✓	✓
Compliance	✗	✓
Report	✓	✓
MIB Compilation	✓	✓
Zero-Touch (Optional)	✗	✓
Playbooks	✗	✓

1.4 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

*Both thin and thick HDD provisioning types are supported.

Refer to the **Deployment** section for instructions on using ThirdEye with the above platforms.

ThirdEye requires the following environment:

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)

1.5 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)

Feature	**Port**	Protocol	UDP/TCP	Communication Direction
	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”.

SECTION 2

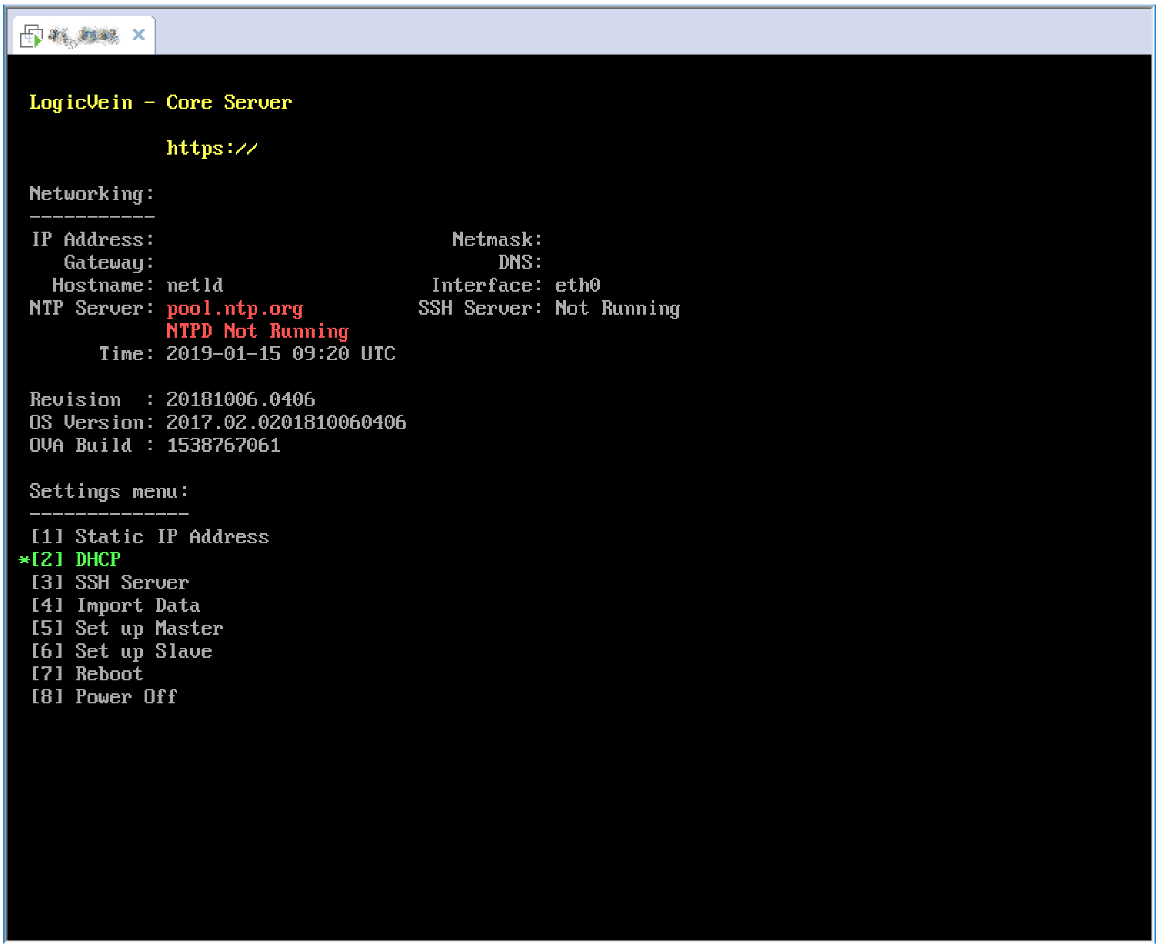
INSTALLATION

2.1 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.

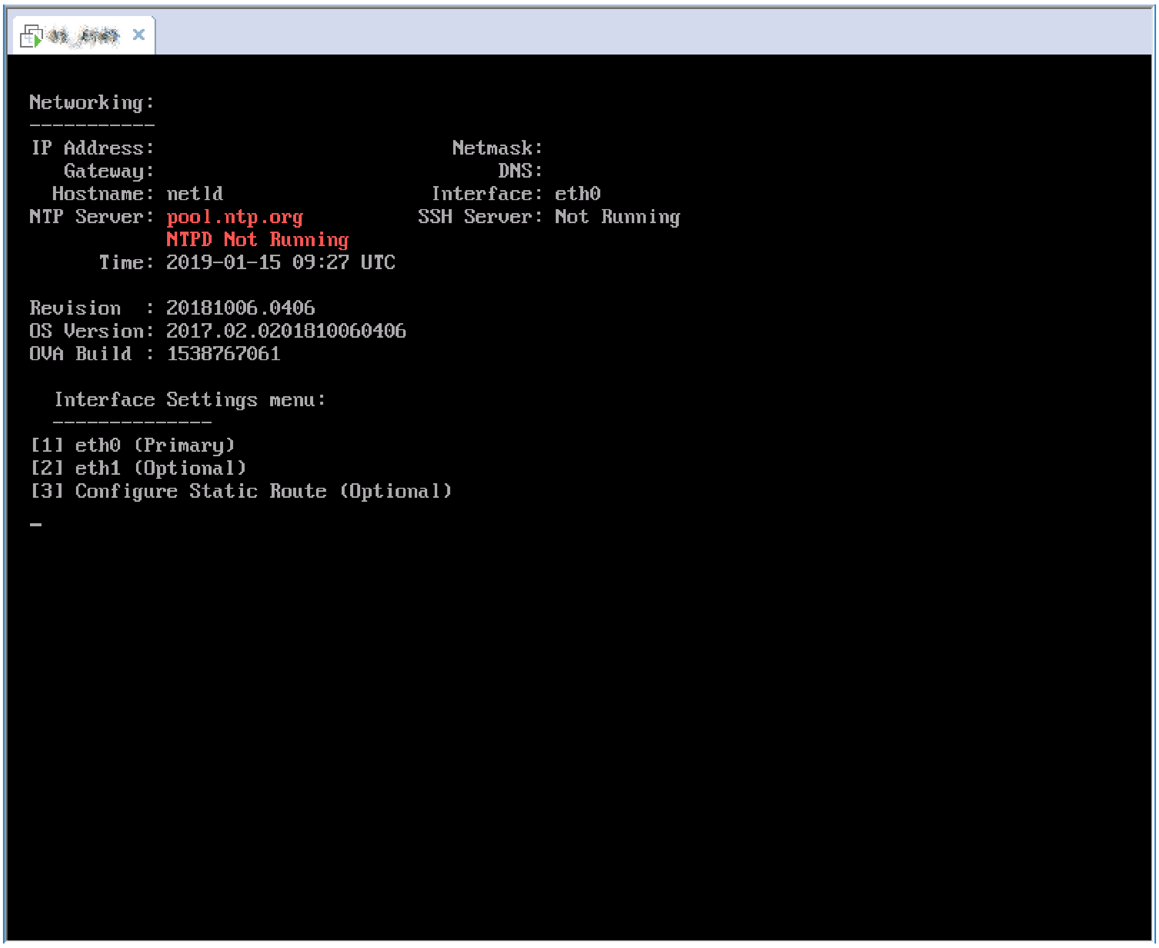
Network settings are operated using the keyboard on the virtual machine console.

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



```
LogicVein - Core Server

            https://

Networking:
-----------
IP Address:                          Netmask:
   Gateway:                              DNS:
  Hostname: netld                  Interface: eth0
NTP Server: pool.ntp.org          SSH Server: Not Running
            NTPD Not Running
      Time: 2019-01-15 09:20 UTC

Revision  : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

Settings menu:
--------------
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Set up Master
[6] Set up Slave
[7] Reboot
[8] Power Off
```

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

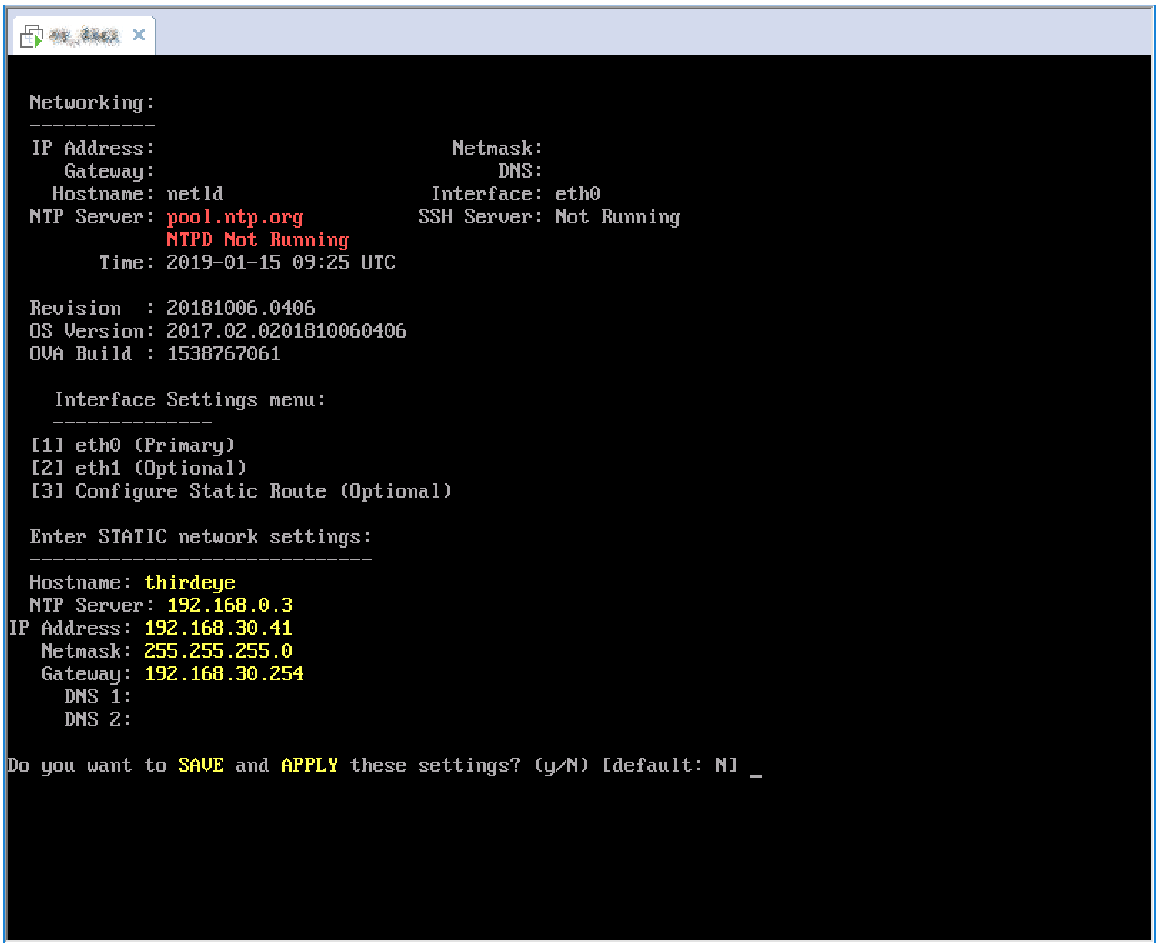


```
Networking:
-----------
IP Address:                      Netmask:
   Gateway:                          DNS:
  Hostname: netld              Interface: eth0
NTP Server: pool.ntp.org      SSH Server: Not Running
            NTPD Not Running
      Time: 2019-01-15 09:27 UTC

Revision  : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

  Interface Settings menu:
  --------------
[1] eth0 (Primary)
[2] eth1 (Optional)
[3] Configure Static Route (Optional)

_
```

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	DNS server IP address	—
DNS 2	DNS server IP address	—

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



```
 Networking:
 -----------
 IP Address:                          Netmask:
    Gateway:                              DNS:
   Hostname: netld                  Interface: eth0
 NTP Server: pool.ntp.org          SSH Server: Not Running
             NTPD Not Running
       Time: 2019-01-15 09:25 UTC

 Revision  : 20181006.0406
 OS Version: 2017.02.0201810060406
 OVA Build : 1538767061

   Interface Settings menu:
   --------------
 [1] eth0 (Primary)
 [2] eth1 (Optional)
 [3] Configure Static Route (Optional)

 Enter STATIC network settings:
 ------------------------------
 Hostname: thirdeye
 NTP Server: 192.168.0.3
IP Address: 192.168.30.41
  Netmask: 255.255.255.0
  Gateway: 192.168.30.254
    DNS 1:
    DNS 2:

Do you want to SAVE and APPLY these settings? (y/N) [default: N] _
```

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

2.2 Apply the License

Apply your license and activate your product.

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

```
https://<Address>/
```

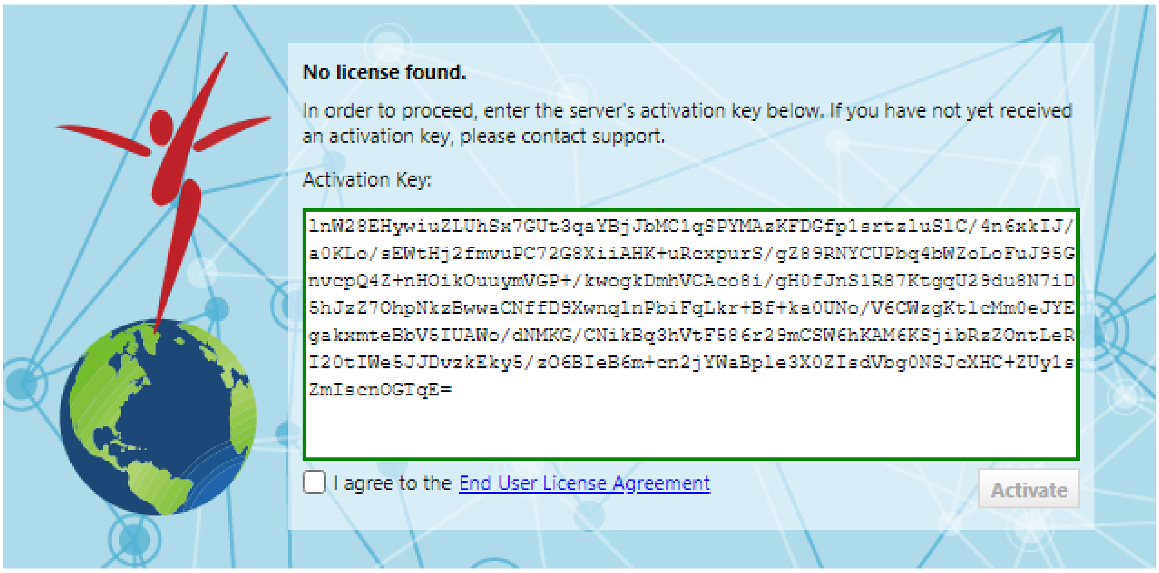
For `<Address>`, Specify the IP address or FQDN (Fully Qualified Domain Name).

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**.



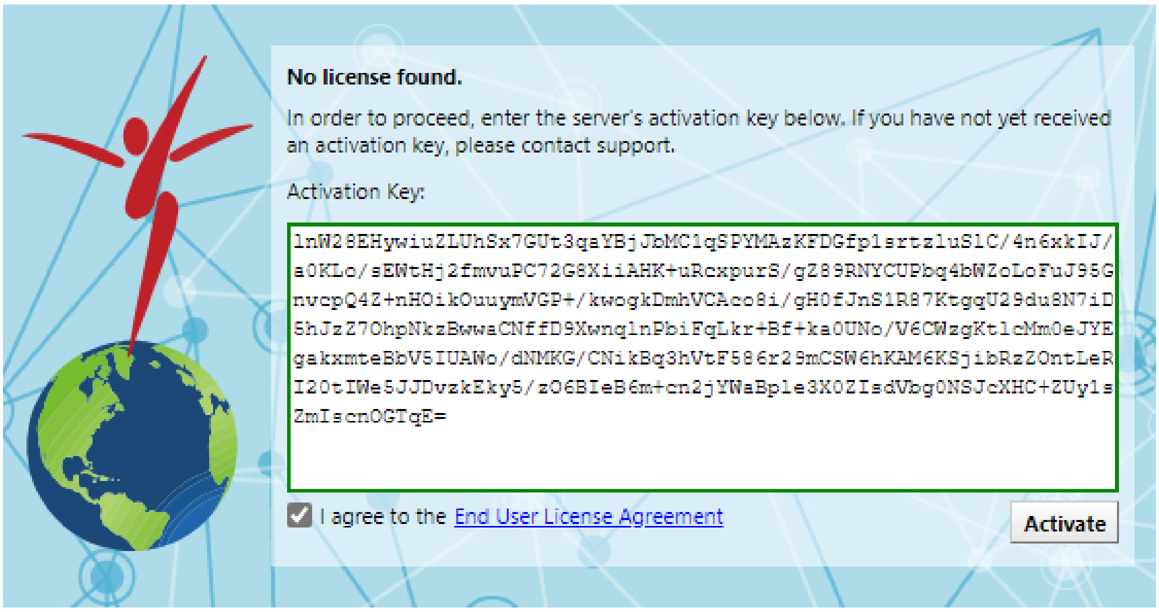
No license found.

In order to proceed, enter the server's activation key below. If you have not yet received an activation key, please contact support.

Activation Key:

```
lnW28EHywiuZLUhSx7GUt3qaYBjJbMC1qSPYMAzKFDGfplsrtzluS1C/4n6xkIJ/
a0KLo/sEWtHj2fmvuPC72G8XiiAHK+uRcxpurS/gZ89RNYCUPbq4bWZoLoFuJ95G
nvcpQ4Z+nHOikOuuymVGP+/kwogkDmhVCAco8i/gH0fJnS1R87KtgqU29du8N7iD
5hJzZ7OhpNkzBwwaCNffD9XwnqlnPbiFqLkr+Bf+ka0UNo/V6CWzgKtlcMm0eJYE
gakxmteBbV5IUAWo/dNMKG/CNikBq3hVtF586r29mCSW6hKAM6KSjibRzZOntLeR
I20tIWe5JJDvzkEky5/zO6BIeB6m+cn2jYWaBple3X0ZIsdVbg0NSJcXHC+ZUy1s
ZmIscnOGTqE=
```

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



No license found.

In order to proceed, enter the server's activation key below. If you have not yet received an activation key, please contact support.

Activation Key:

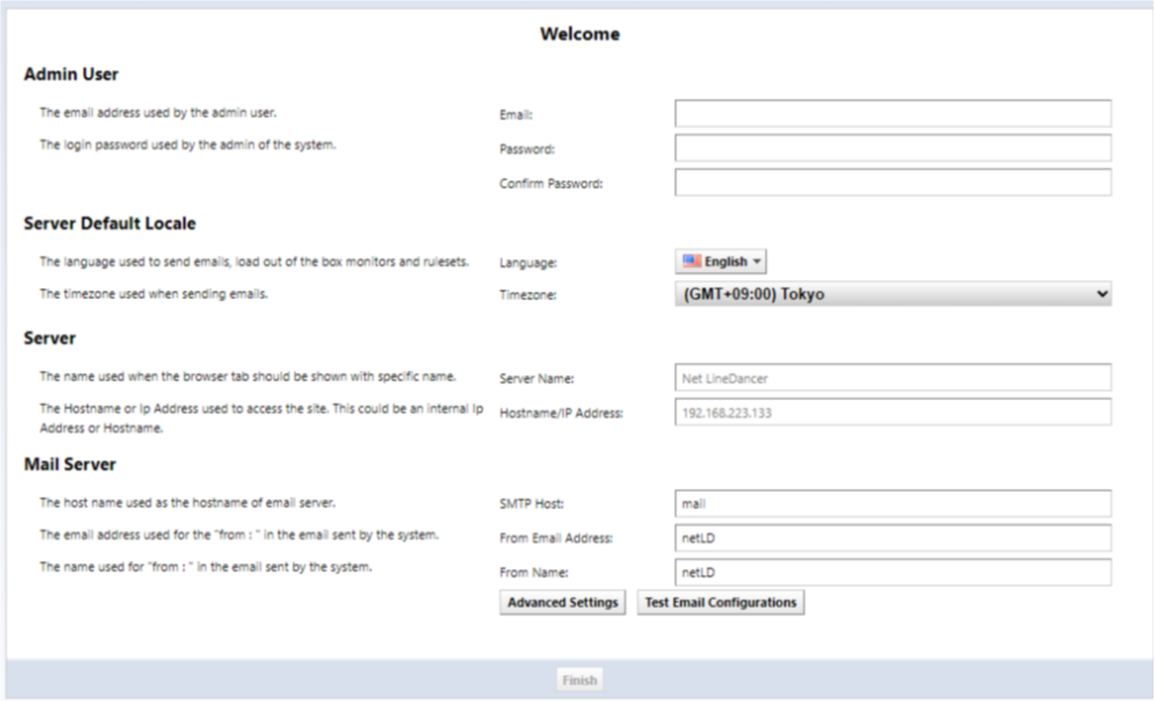
```
lnW28EHywiuZLUhSx7GUt3qaYBjJbMC1qSPYMAzKFDGfp1srtzluS1C/4n6xkIJ/
a0KLo/sEWtHj2fmvuPC72G8XiiAHK+uRcxpurS/gZ89RNYCUPbq4bWZoLoFuJ95G
nvcpQ4Z+nHOikOuuymVGP+/kwogkDmhVCAco8i/gH0fJnS1R87KtgqU29du8N7iD
5hJzZ7OhpNkzBwwaCNffD9XwnqlnPbiFqLkr+Bf+ka0UNo/V6CWzgKtlcMm0eJYE
gakxmteBbV5IUAWo/dNMKG/CNikBq3hVtF586r29mCSW6hKAM6KSjibRzZOntLeR
I20tIWe5JJDvzkEky5/zO6BIeB6m+cn2jYWaBple3X0ZIsdVbg0NSJcXHC+ZUy1s
ZmIscnOGTqE=
```

☑ I agree to the End User License Agreement

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

2.3 Initial 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.



Welcome

Admin User

The email address used by the admin user. — Email:

The login password used by the admin of the system. — Password:

Confirm Password:

Server Default Locale

The language used to send emails, load out of the box monitors and rulesets. — Language: English

The timezone used when sending emails. — Timezone: (GMT+09:00) Tokyo

Server

The name used when the browser tab should be shown with specific name. — Server Name: Net LineDancer

The Hostname or Ip Address used to access the site. This could be an internal Ip Address or Hostname. — Hostname/IP Address: 192.168.223.133

Mail Server

The host name used as the hostname of email server. — SMTP Host: mail

The email address used for the "from : " in the email sent by the system. — From Email Address: netLD

The name used for "from : " in the email sent by the system. — From Name: netLD

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.

SECTION 3

LOGIN/LOGOUT

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

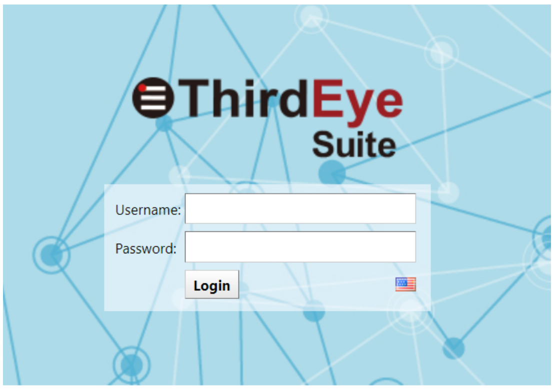
3.1 Log In

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.



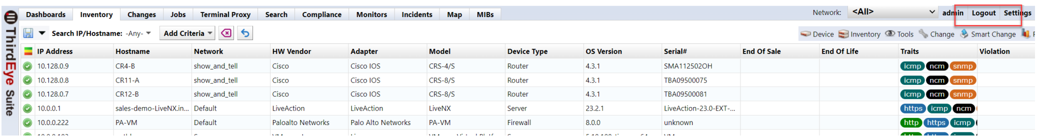
For new installation instructions, refer to the **Installation** section.

For instructions on setting the admin user password, refer to the **Initial Settings** section.

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

3.2 Log Out

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



IP Address	Hostname	Network	HW Vendor	Adapter	Model	Device Type	OS Version	Serial#	End Of Sale	End Of Life	Traits	Violation
10.128.0.9	CR4-B	show_and_tell	Cisco	Cisco IOS	CRS-4/S	Router	4.3.1	SMA112502OH			icmp ncm snmp	
10.128.0.8	CR11-A	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500075			icmp ncm snmp	
10.128.0.7	CR12-B	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500081			icmp ncm snmp	
10.0.0.1	sales-demo-LiveNX.in...	Default	LiveAction	LiveAction	LiveNX	Server	23.2.1	LiveAction-23.0-EXT-...			https icmp ncm	
10.0.0.222	PA-VM	Default	Paloalto Networks	Palo Alto Networks	PA-VM	Firewall	8.0.0	unknown			http https icmp	

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

SECTION 4

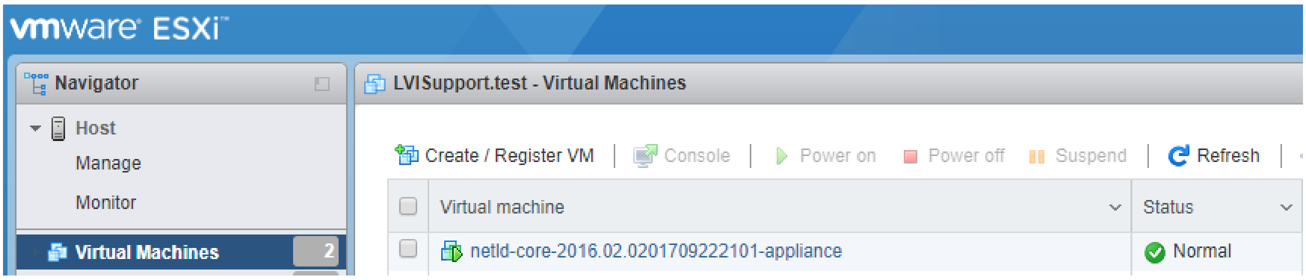
DEPLOYMENT

ThirdEye provides flexible deployment as a virtual appliance across major hypervisors and cloud platforms, maintaining consistent core requirements while adapting to platform-specific configurations.

4.1 VMware ESXi

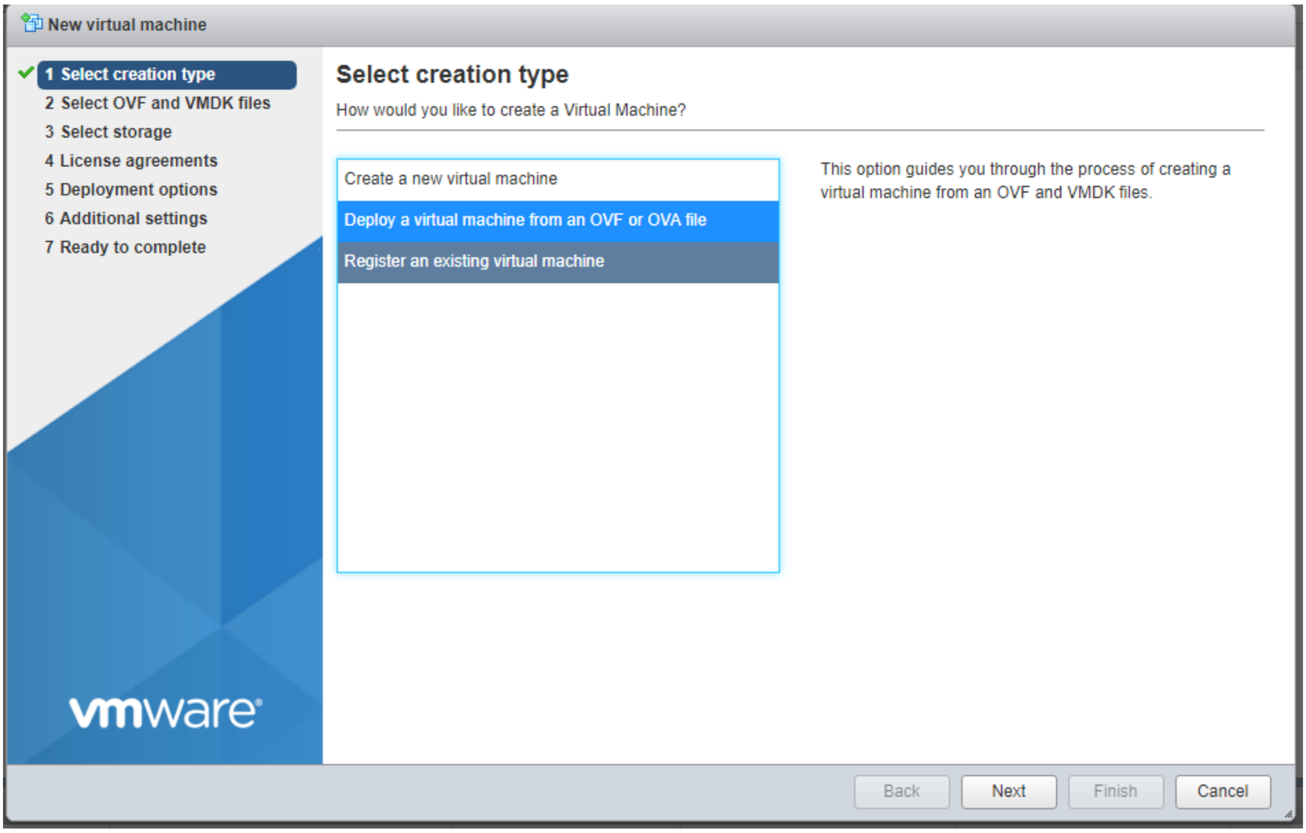
This section describes the deployment procedure to VMware ESXi. Here we will explain using ESXi 6.5 as an example.

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



□	Virtual machine	Status
□	netld-core-2016.02.0201709222101-appliance	Normal

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



New virtual machine

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

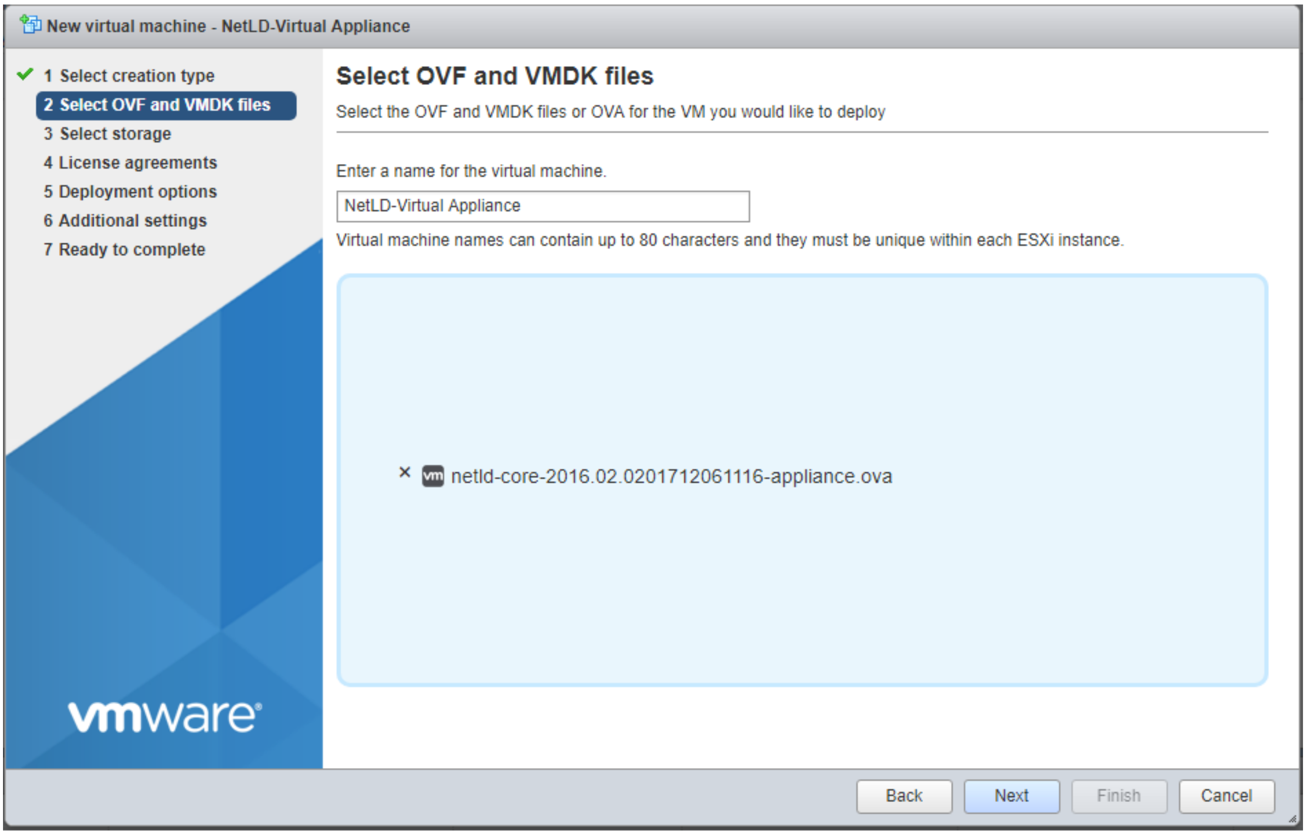
- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

3. After entering the desired virtual machine name, drag and drop the OVA file onto the virtual machine:

OVA file: `lvi-core-\*\*\*\*-appliance.ova`.

4. Click [Next].



New virtual machine - NetLD-Virtual Appliance

✓ 1 Select creation type

2 Select OVF and VMDK files

3 Select storage

4 License agreements

5 Deployment options

6 Additional settings

7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

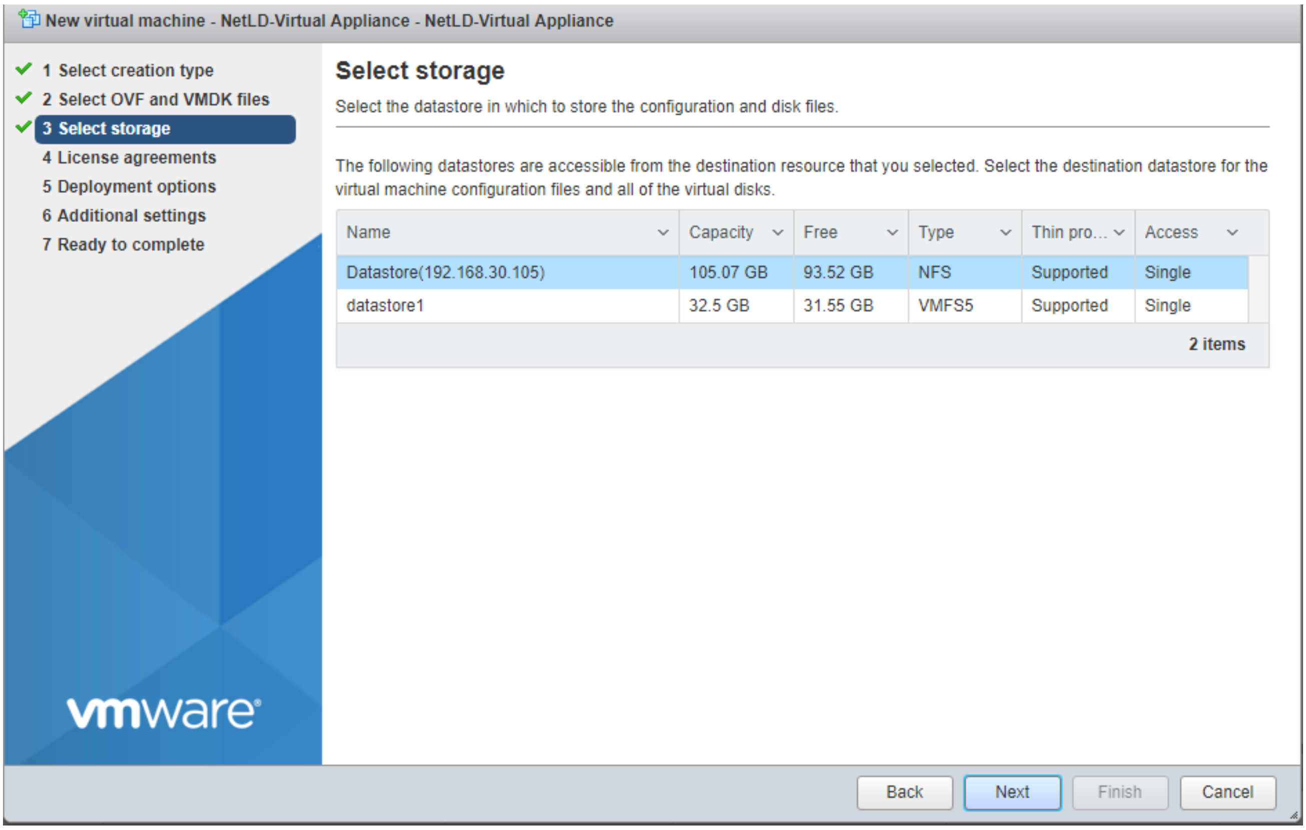
Enter a name for the virtual machine.

NetLD-Virtual Appliance

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× netld-core-2016.02.0201712061116-appliance.ova

5. Select your storage, and click [Next].



New virtual machine - NetLD-Virtual Appliance - NetLD-Virtual Appliance

Select storage

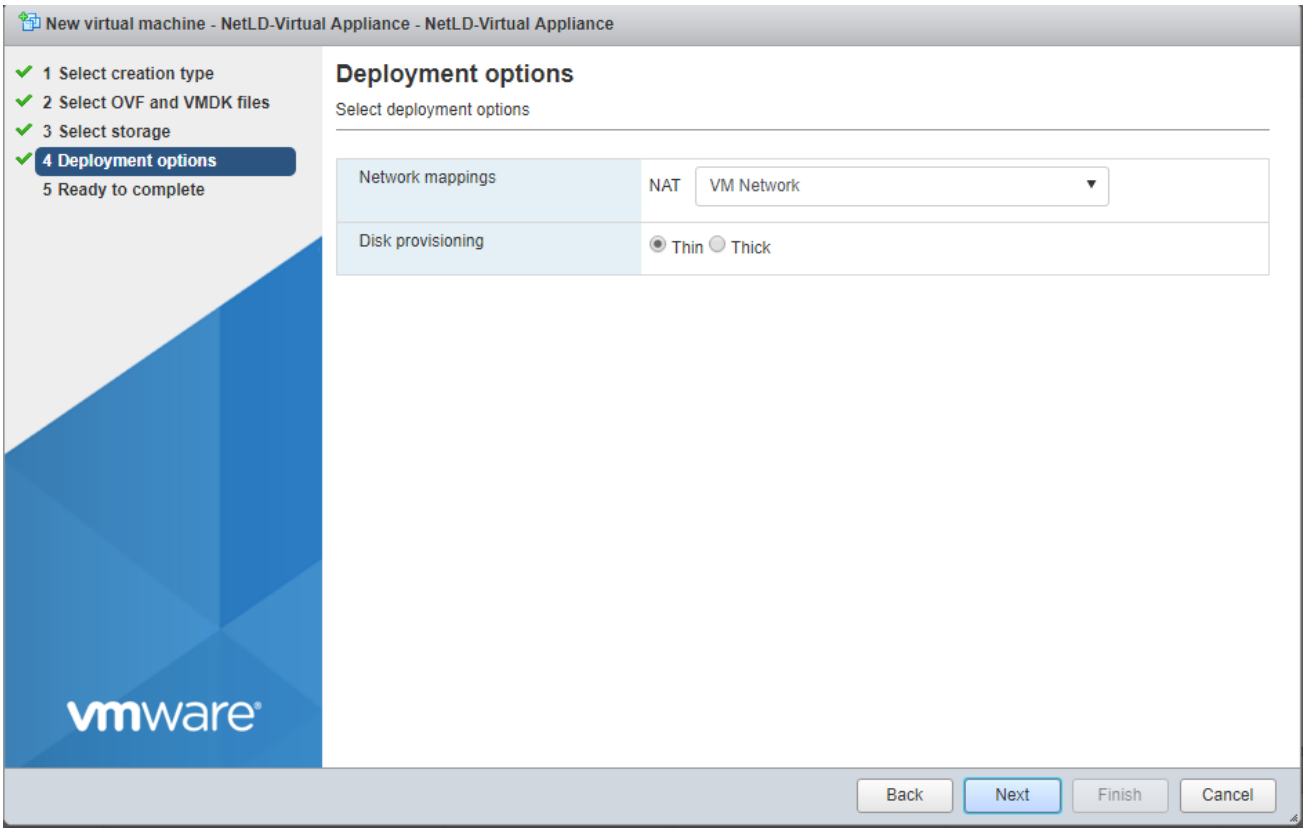
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
Datastore(192.168.30.105)	105.07 GB	93.52 GB	NFS	Supported	Single
datastore1	32.5 GB	31.55 GB	VMFS5	Supported	Single

2 items

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



New virtual machine - NetLD-Virtual Appliance - NetLD-Virtual Appliance

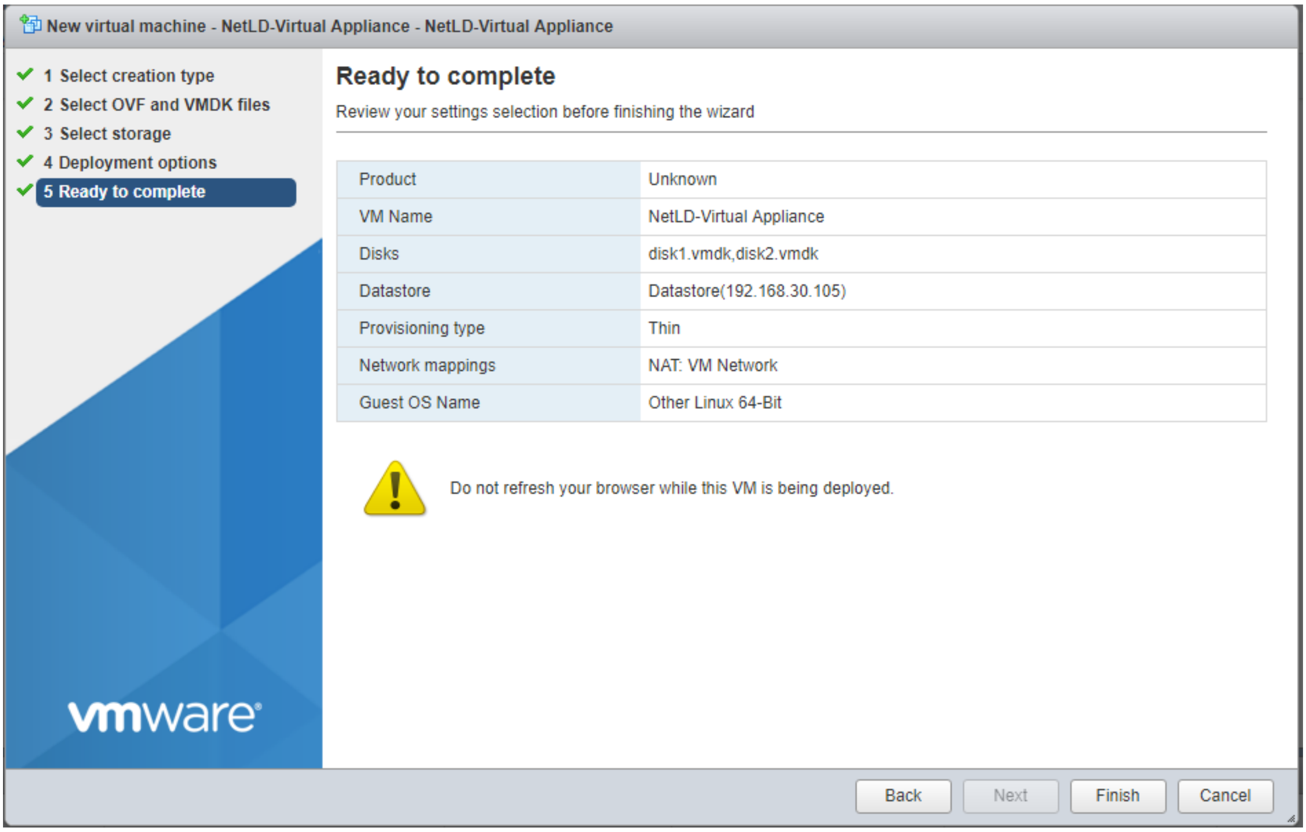
✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 Deployment options
5 Ready to complete

Deployment options

Select deployment options

Network mappings	NAT: VM Network
Disk provisioning	● Thin ○ Thick

7. Click [Finish].



New virtual machine - NetLD-Virtual Appliance - NetLD-Virtual Appliance

Ready to complete

Review your settings selection before finishing the wizard

Product	Unknown
VM Name	NetLD-Virtual Appliance
Disks	disk1.vmdk,disk2.vmdk
Datastore	Datastore(192.168.30.105)
Provisioning type	Thin
Network mappings	NAT: VM Network
Guest OS Name	Other Linux 64-Bit

Do not refresh your browser while this VM is being deployed.

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

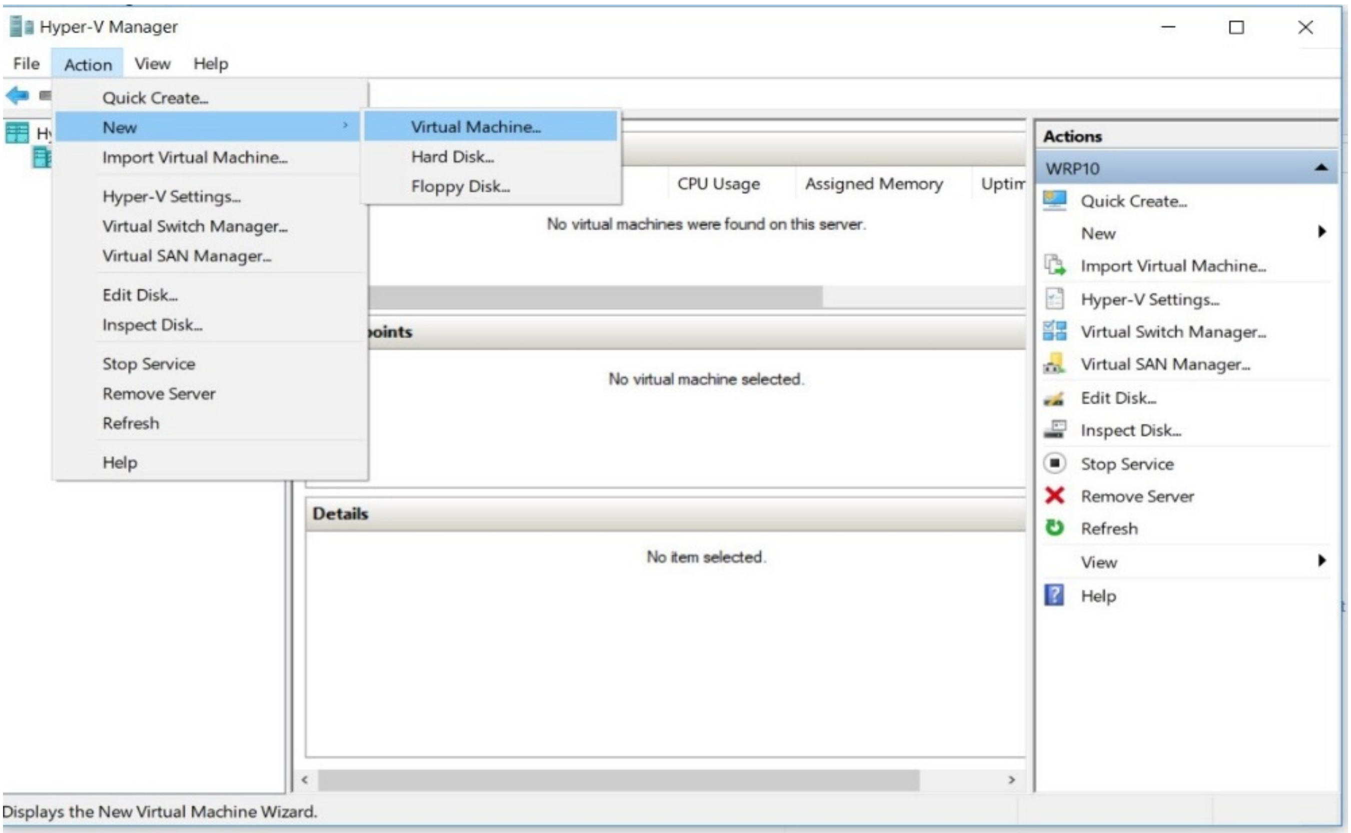
4.2 Windows Hyper-V

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].



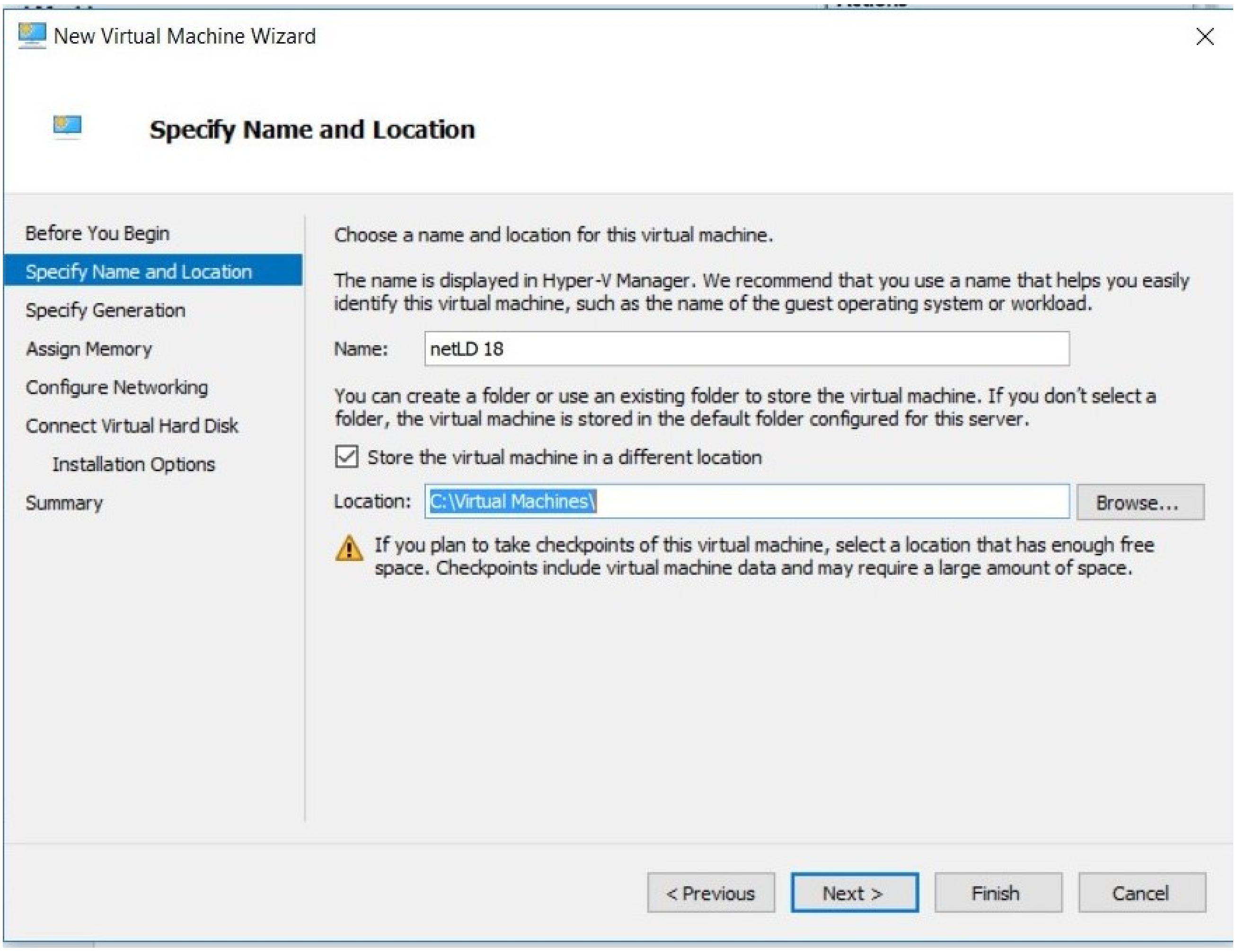
No virtual machines were found on this server.

No virtual machine selected.

No item selected.

Displays the New Virtual Machine Wizard.

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



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: netLD 18

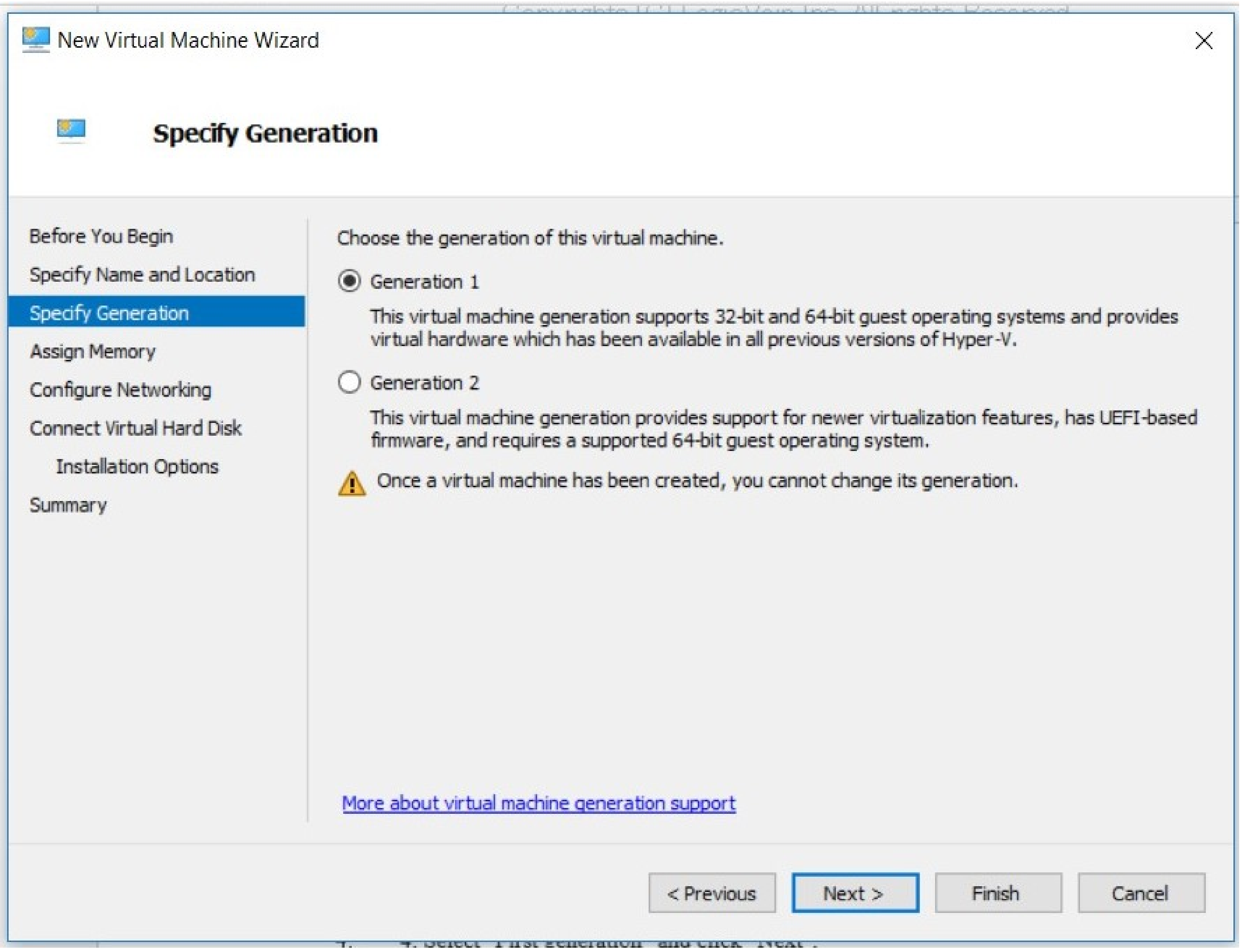
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: C:\Virtual Machines\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

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



Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

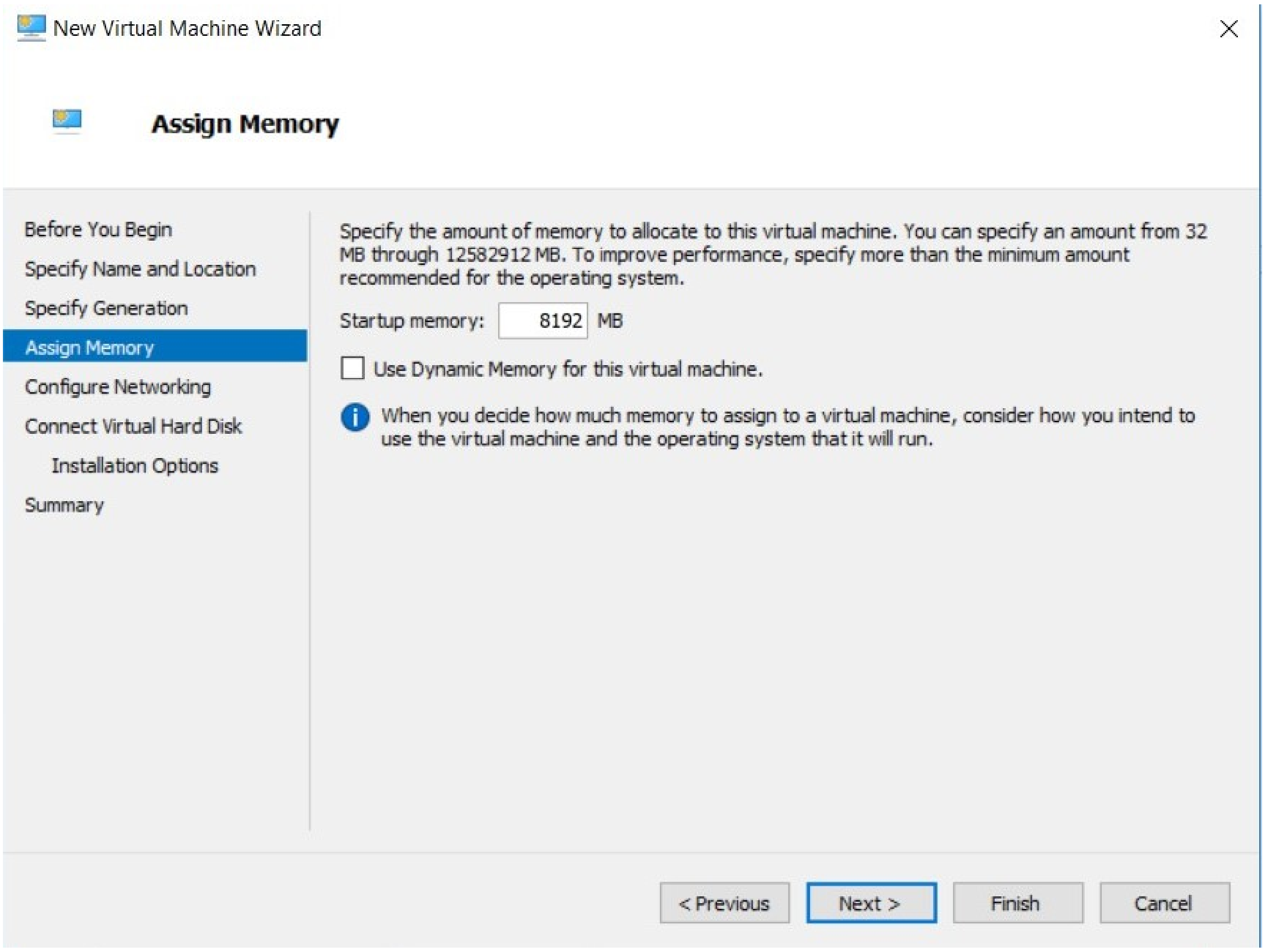
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

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



New Virtual Machine Wizard

Assign Memory

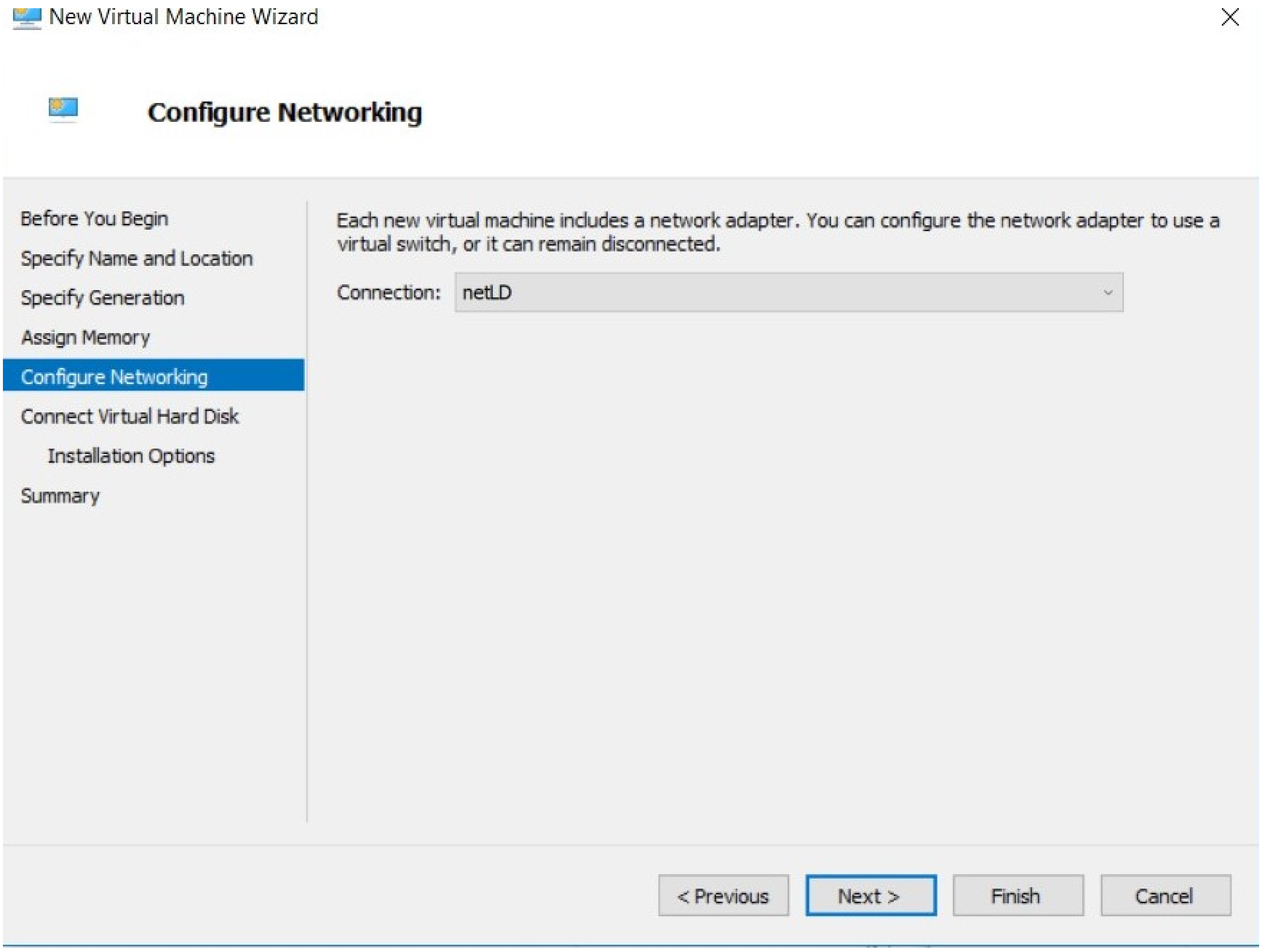
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 8192 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

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



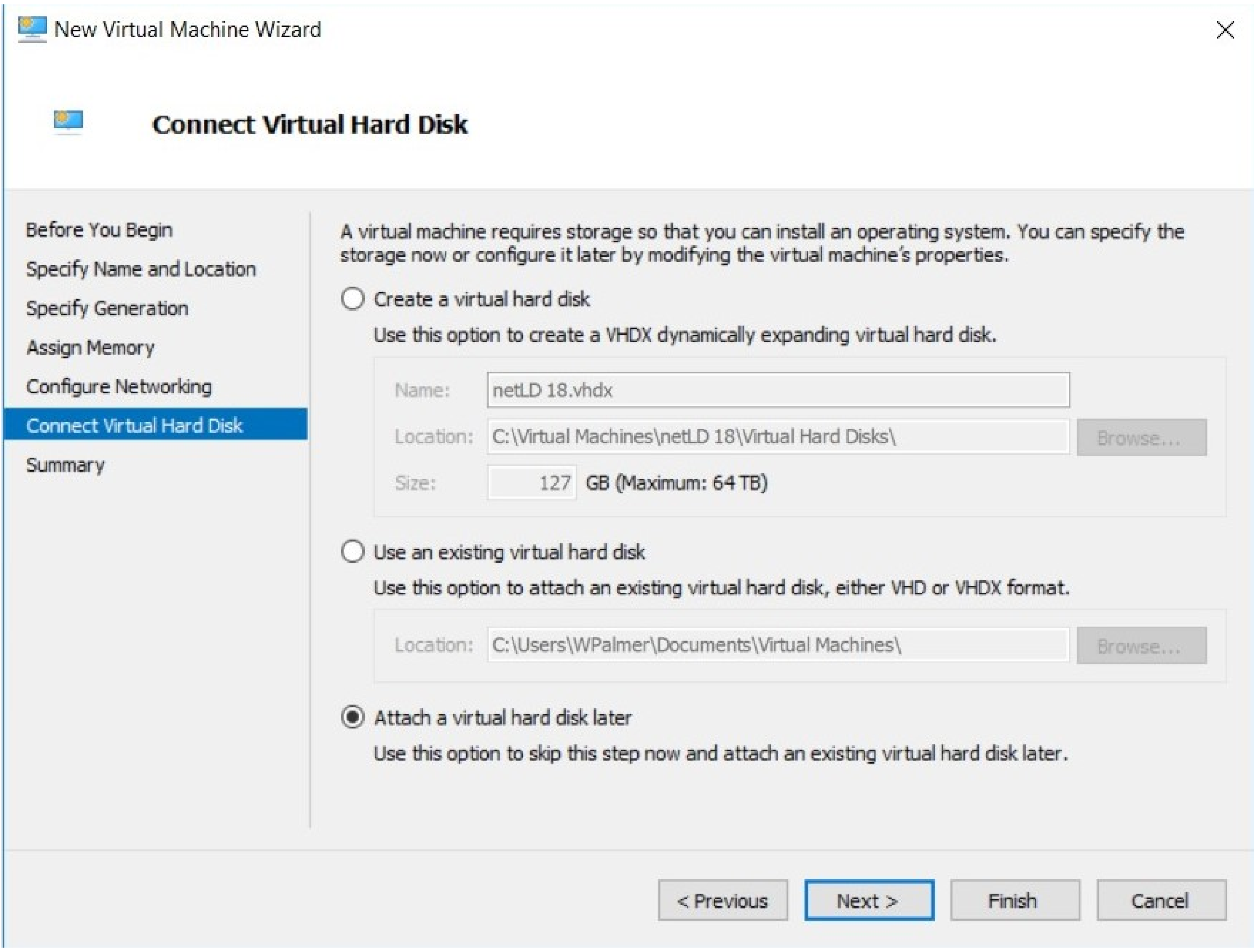
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: netLD

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



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine’s properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: netLD 18.vhdx

Location: C:\Virtual Machines\netLD 18\Virtual Hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

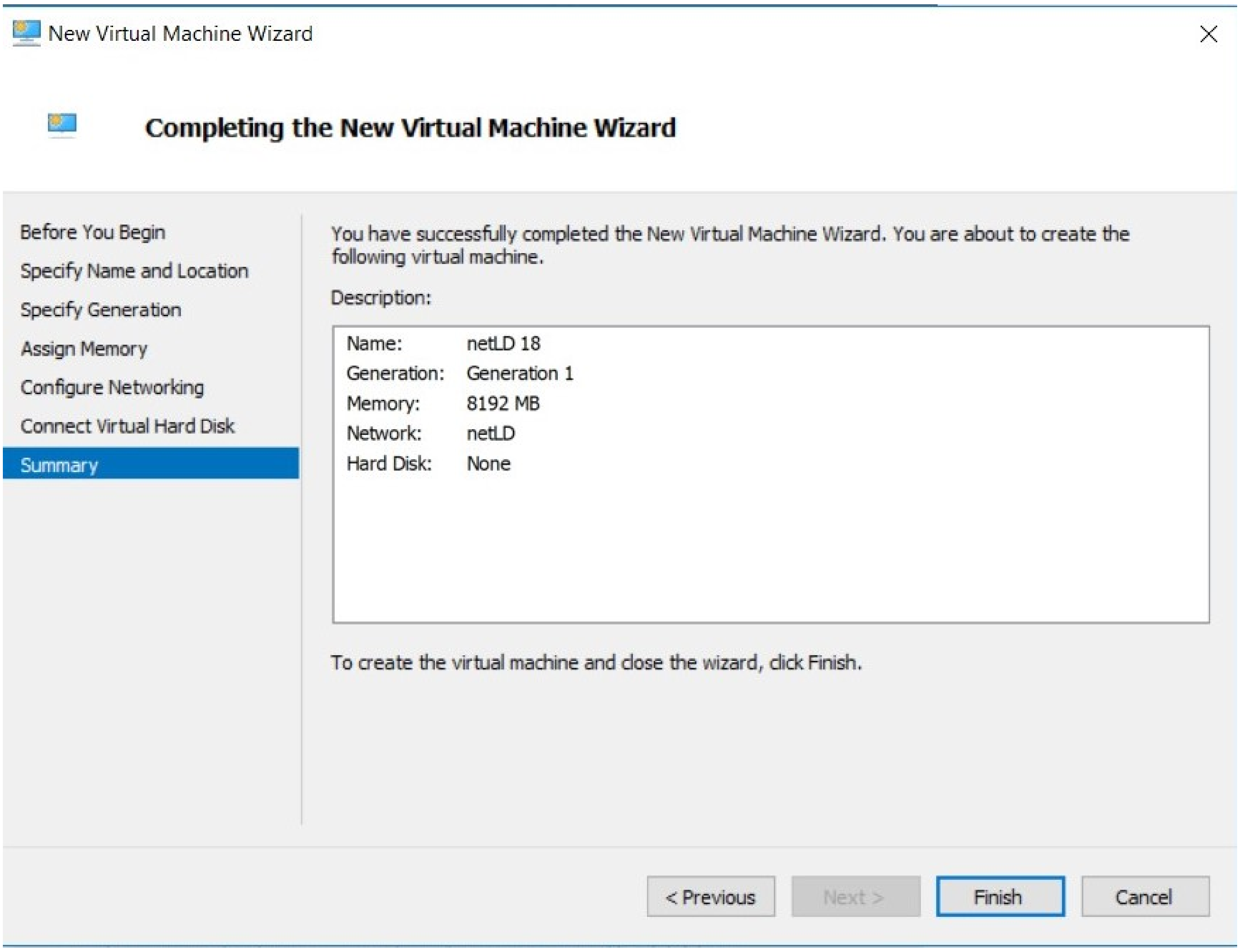
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\WPalmer\Documents\Virtual Machines\ Browse...

● Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

7. Click [Finish].



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

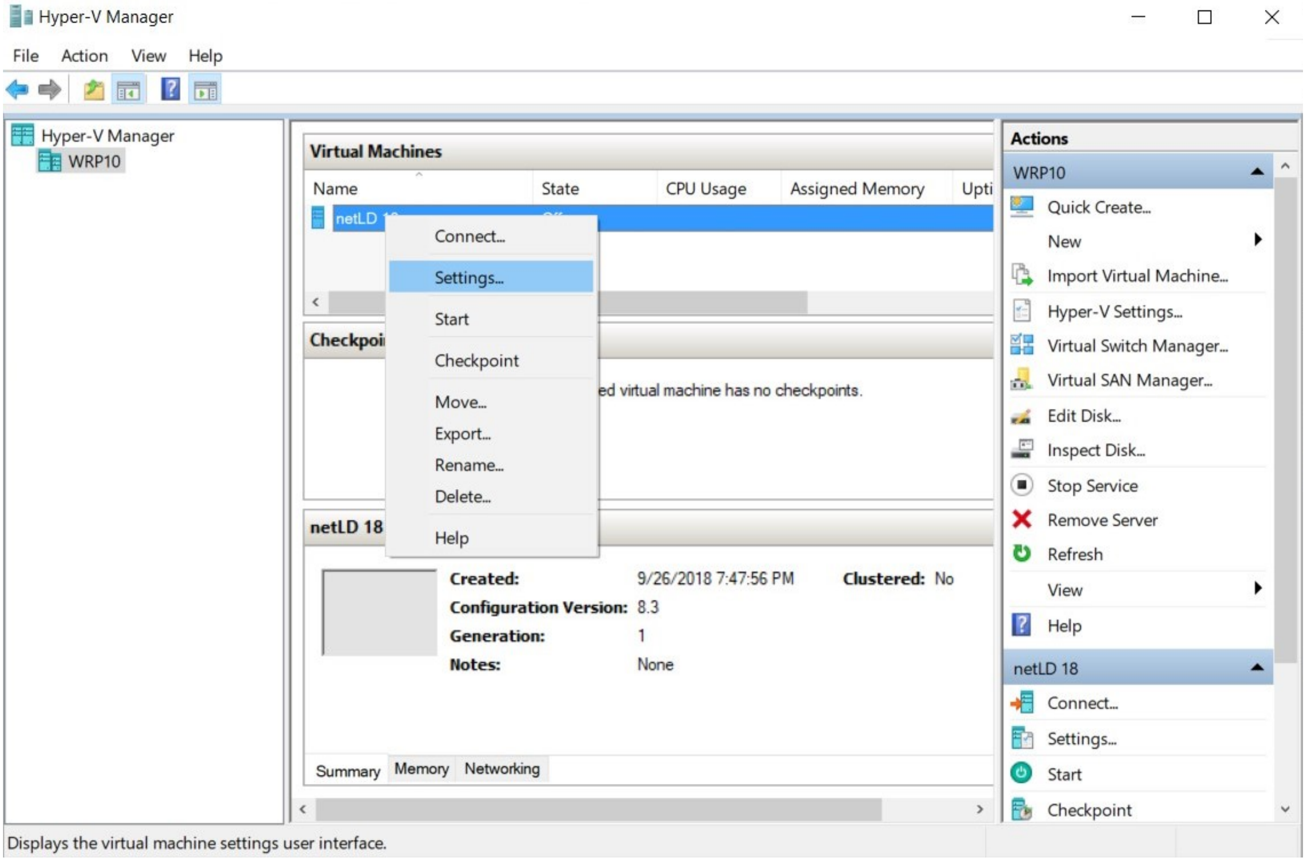
Name:	netLD 18
Generation:	Generation 1
Memory:	8192 MB
Network:	netLD
Hard Disk:	None

To create the virtual machine and close the wizard, click Finish.

The virtual machine will now be created.

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

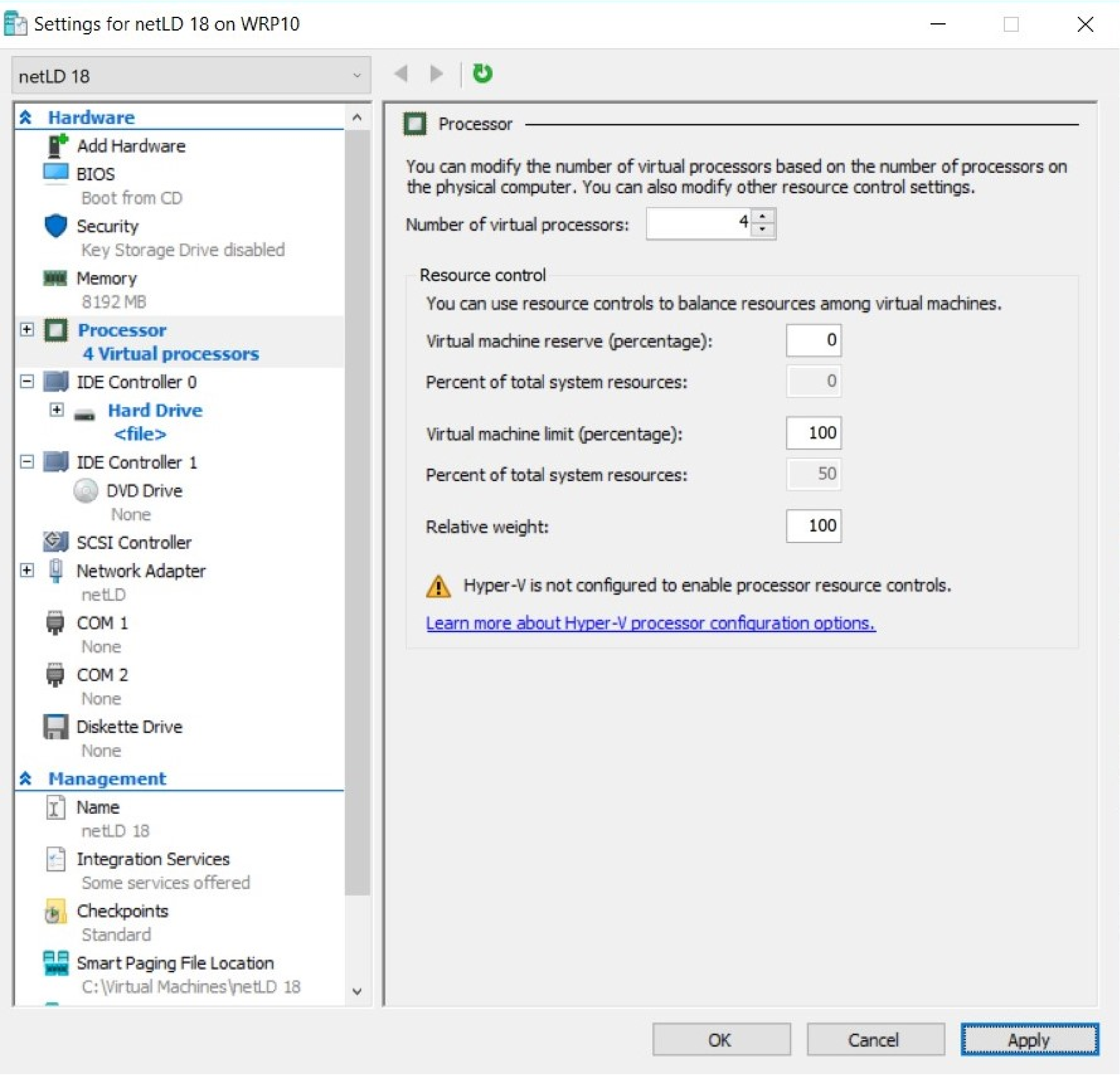
8. Right-click the virtual machine you created and click [Settings].



Created: 9/26/2018 7:47:56 PM **Clustered:** No
Configuration Version: 8.3
Generation: 1
Notes: None

Displays the virtual machine settings user interface.

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



Settings for netLD 18 on WRP10

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 4

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

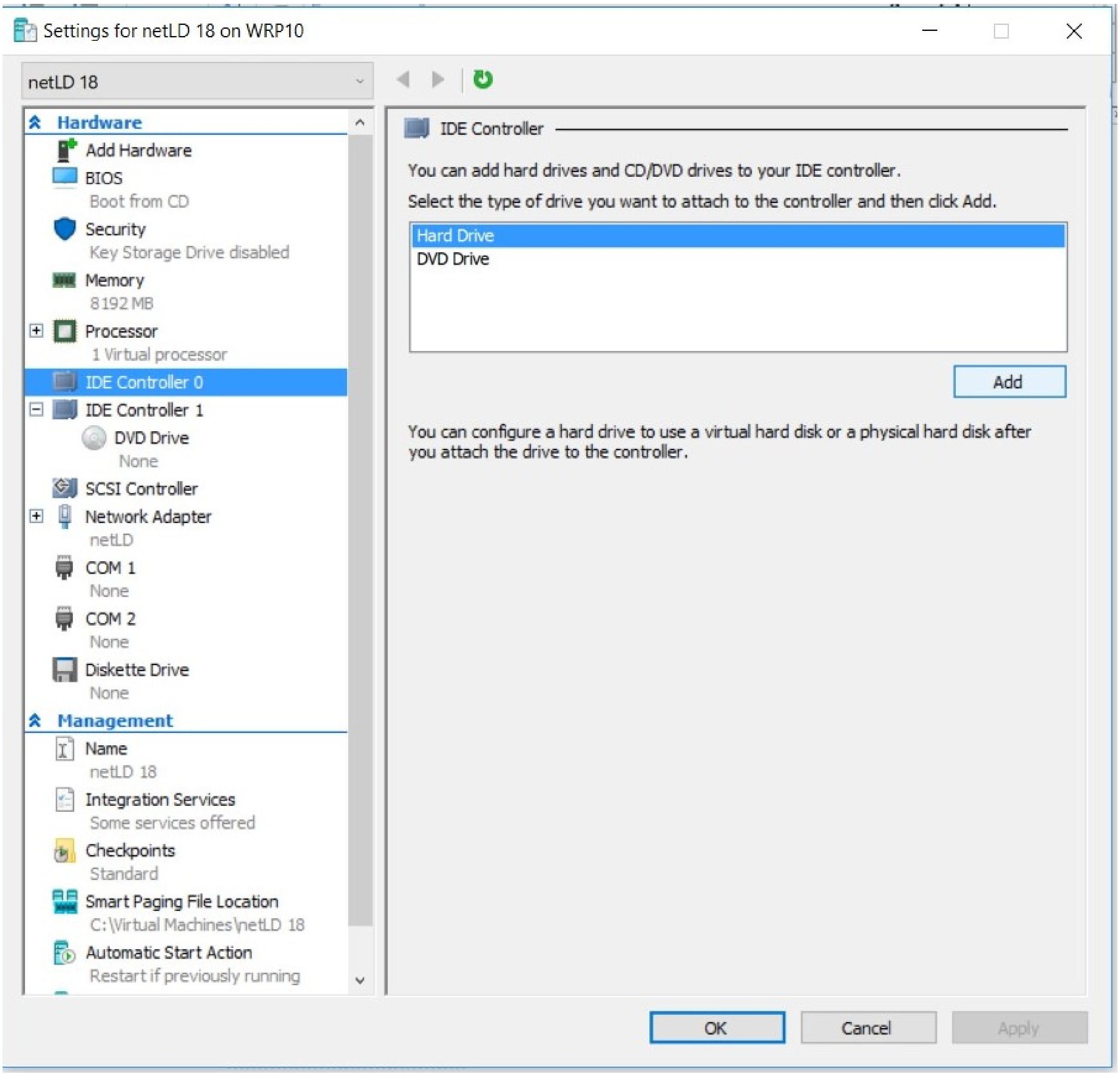
Percent of total system resources: 50

Relative weight: 100

Hyper-V is not configured to enable processor resource controls.

Learn more about Hyper-V processor configuration options.

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



Settings for netLD 18 on WRP10

netLD 18

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  8192 MB
- Processor
  1 Virtual processor
- IDE Controller 0
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  netLD
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  netLD 18
- Integration Services
  Some services offered
- Checkpoints
  Standard
- Smart Paging File Location
  C:\Virtual Machines\netLD 18
- Automatic Start Action
  Restart if previously running

IDE Controller

You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

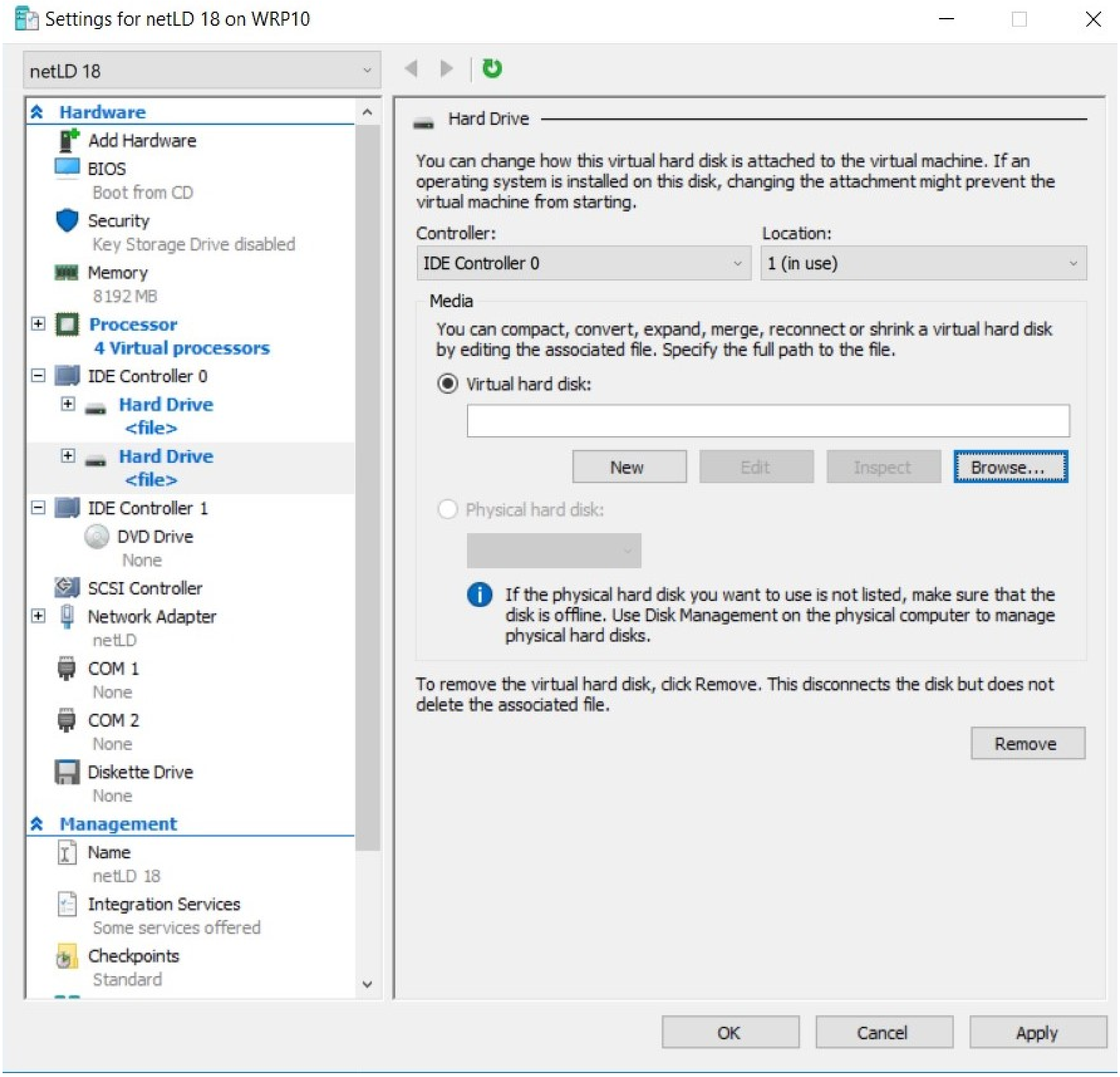
- Hard Drive
- DVD Drive

Add

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

OK Cancel Apply

11. Click [Browse].



Settings for netLD 18 on WRP10

netLD 18

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

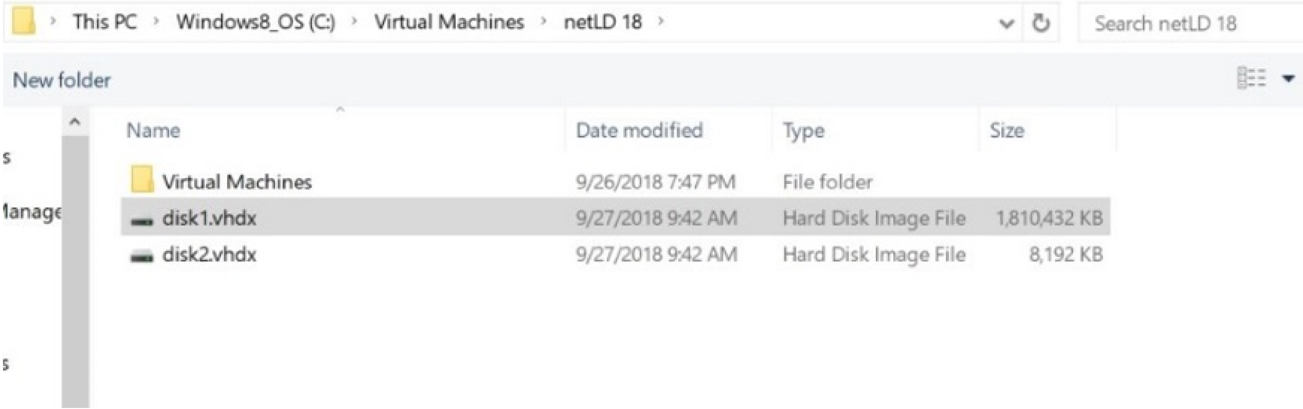
● Virtual hard disk:

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

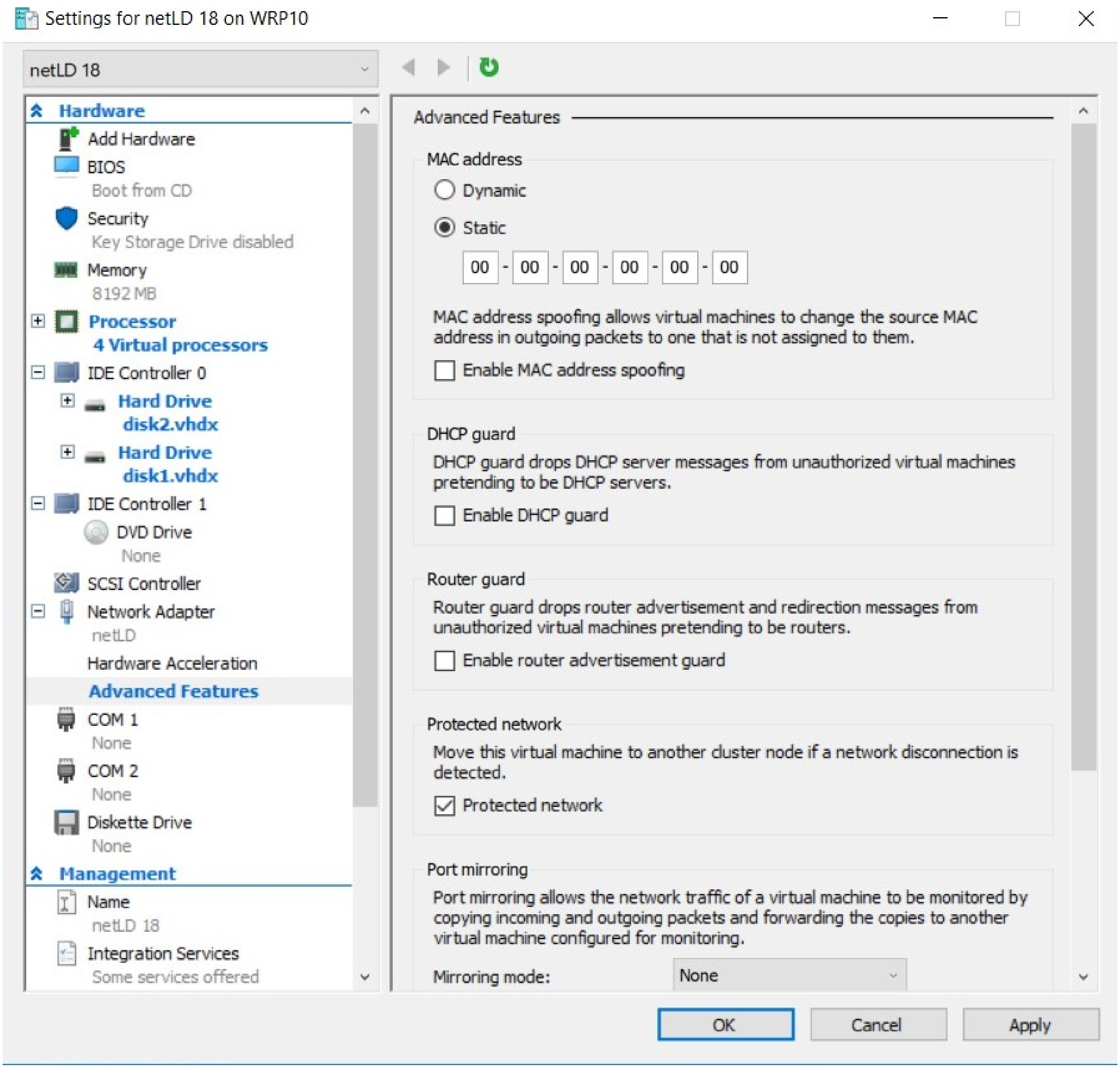
12. Add “disk1”, and click [OK].



Name	Date modified	Type	Size
Virtual Machines	9/26/2018 7:47 PM	File folder	
disk1.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	1,810,432 KB
disk2.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	8,192 KB

13. Repeat steps 8 to 12 to add `disk2.vhdx`.

14. Click [OK].



Advanced Features

MAC address

○ Dynamic

● Static

00 - 00 - 00 - 00 - 00 - 00

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

□ Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

□ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

□ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: None

This completes the Windows Hyper-V deployment.

4.3 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.

4.4 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.

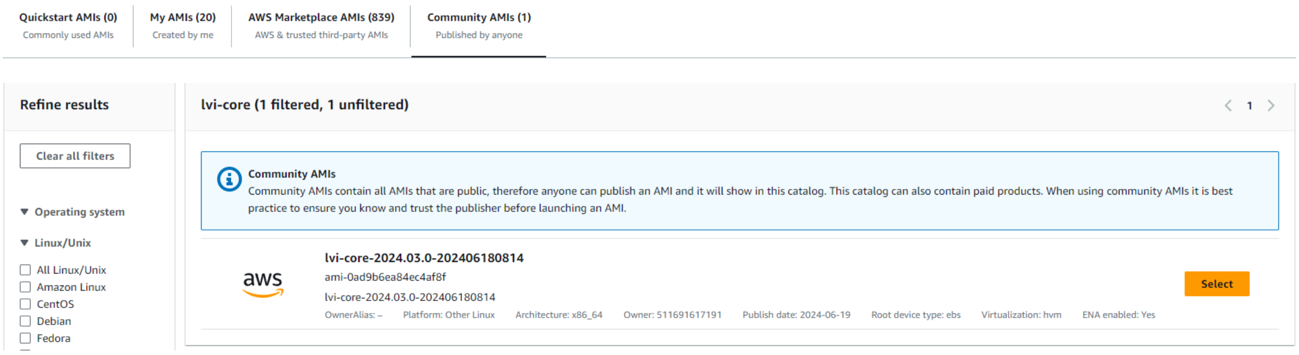
4.5 Microsoft Azure

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.

4.6 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.



Community AMIs

Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.

lvi-core-2024.03.0-202406180814
ami-0ad9b6ea84ec4af8f
lvi-core-2024.03.0-202406180814
OwnerAlias: – Platform: Other Linux Architecture: x86_64 Owner: 511691617191 Publish date: 2024-06-19 Root device type: ebs Virtualization: hvm ENA enabled: Yes

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].

4.7 Podman

Podman is a containerization tool designed for deploying and managing containerized applications, serving as a Docker alternative. ThirdEye can be deployed on the Podman container infrastructure.

Podman Features:

- **Security Focus:** Runs containers in isolated environments without requiring a daemon
- **Rootless Operation:** Supports running containers without root privileges (though some operations like low-port binding may require sudo)
- **Docker Compatibility:** Uses command structures similar to Docker, for example, `podman run` instead of `docker run`.

Example: Replace `docker` with `podman`:

```
docker pull harbor.logicvein.com/lvi/lvi-netld-core:2025.08.0-202509290840
```

4.7.1 Adapter Login

When deploying ThirdEye with Podman, `cap_net_admin` and `cap_net_raw` capabilities are not available by default. To use adapter login, `cap_net_admin` and `cap_net_raw` capabilities must be added.

4.7.2 Podman Deployment

Podman/Docker builds are published to LogicVein’s **Harbor** instance.

Example execution:

```
podman run \
  --name <CONTAINER-NAME> \
  --detach \
  --env LICENSE_SERIAL=<SERIALNUM> \
  --env JAVA_OPTIONS="-DNAT_RETURN_ADDRESS=<HOST-IP>" \
  --ulimit nofile=8192:8192 \
  --ulimit nproc=128294:128294 \
  --pids-limit=-1 \
  --memory=8g \
  --cpus=4.0 \
  --sysctl net.ipv4.ping_group_range="0 9999" \
  --volume <DATA-DIR>:/data \
  --publish 20:20 \
  --publish 21:21 \
  --publish 67:67/udp \
  --publish 69:69/udp \
  --publish 162:162/udp \
  --publish 162:162/tcp \
  --publish 443:443 \
  --publish 512:512/udp \
  --publish 2222:2222 \
  --publish 50000-50031:50000-50031 \
  --cap-add=NET_RAW \
  --cap-add=NET_ADMIN \
  harbor.logicvein.com/lvi/lvi-netld-core:2025.08.0-202509290840
```

In a SE Linux enabled system (e.g. RedHat), Docker / Podman can be run using following command. This will set the SE Linux context for the directory for just this container:

```
sudo podman run \
  --name <CONTAINER-NAME> \
  --env LICENSE_SERIAL=<SERIALNUM> \
  --env JAVA_OPTIONS="-DNAT_RETURN_ADDRESS=<HOST-IP>" \
  --ulimit nofile=8192:8192 \
  --ulimit nproc=128294:128294 \
  --pids-limit=-1 \
  --memory=8g \
  --cpus=4.0 \
  --sysctl net.ipv4.ping_group_range="0 9999" \
  --volume <DATA-DIR>:/data:Z \
  --publish 20:20 \
  --publish 21:21 \
  --publish 67:67/udp \
  --publish 69:69/udp \
  --publish 162:162/udp \
  --publish 162:162/tcp \
  --publish 443:443 \
  --publish 512:512/udp \
  --publish 2222:2222 \
  --publish 50000-50031:50000-50031 \
  --cap-add=NET_RAW \
  --cap-add=NET_ADMIN \
  harbor.logicvein.com/lvi/lvi-netld-core:2025.08.0-202509290840
```

Or you can manually set SE Linux context using following command:

```
sudo semanage fcontext -a -t container_file_t "/home/lvi/data2(/.*)?"
sudo restorecon -Rv /home/lvi/data2/
```

This will set SE Linux context for this directory to allow any container to access this folder.

Example:

```
drwxr-xr-x. 2 lvi lvi unconfined_u:object_r:container_file_t:s0 6 Mar 26 19:37 /home/lvi/data2/
```

Note

In the command above there are three components that need user-supplied values:

- `<SERIALNUM>` : This is the license serial number that ***must*** match the serial number of the applied license. See License Creation below.
- `<DATA-DIR>` : This is the ***local directory*** in which data will be stored. This is the equivalent of the "data" disk that is normally attached to an OVA-style appliance instance.
- `<HOST-IP>` : This is the ***ip address*** to be used for both FTP and TFTP NAT reflection.

This directory must exist, it is not created automatically.

4.7.3 Ubuntu Linux

1. Install Ubuntu Linux from `ubuntu-24.04.1-live-server-amd64.iso`.

> **Note**
>
> - Do *not* select the "docker" package during installation (we will install it next).
> - Instead, select the OpenSSH install option during install for remote access.

2. Login and update:

   ```
   sudo apt upgrade
   ```

3. Reboot:

   ```
   sudo shutdown -r now
   ```

4. Install Docker using the following steps 1 and 2 in the following install guide:

   https://docs.docker.com/engine/install/ubuntu/#install-using-the-repository.

5. Add your user to the "docker" group:

   ```
   sudo usermod -aG docker $USER
   ```

6. Configure Docker to start at boot time:

   ```
   sudo systemctl enable docker
   ```

7. Reboot again:

   ```
   sudo shutdown -r now
   ```

8. Login as non-root user to verify that you can run Docker commands *without* using the `sudo` command.

   (This should execute without error):

   ```
   docker ps
   ```

9. Create a data directory as a non-root user. For example, login as user "lvi", and execute the following command:

   ```
   mkdir data
   ```

   (This should create the directory `/home/lvi/data`.)

> **Note**
>
> There is no need to change permissions with `chmod` at this time.

10. Start Docker using the previous command syntax as a non-root user, *without* using the `sudo` command.

Example:

```
sudo podman run \
  --name <CONTAINER-NAME> \
  --ulimit nofile=8192:8192 \
  --ulimit nproc=128294:128294 \
  --pids-limit=-1 \
  --env LICENSE_SERIAL=<SERIAL-NUMBER> \
  --memory=4g \
  --cpus=4.0 \
  --sysctl net.ipv4.ping_group_range="0 9999" \
  --volume <DATA-DIRECTORY>:/data:Z \
  --publish 20:20 \
  --publish 21:21 \
  --publish 67:67/udp \
  --publish 69:69/udp \
  --publish 162:162/udp \
  --publish 443:443 \
  --publish 512:512/udp \
  --publish 2222:2222 \
  --publish 512:512/udp \
  --publish 50000-50031:50000-50031 \
  --cap-add=NET_RAW \
  --cap-add=NET_ADMIN \
harbor.logicvein.com/lvi_dev/lvi-netld-core:<REVISION>
```

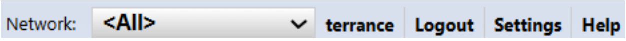
Note

To execute the docker container in the background add the option `--detach` .

SECTION 5

GLOBAL MENU

The Global Menu is the fixed menu that is always visible in the upper right of the ThirdEye window:

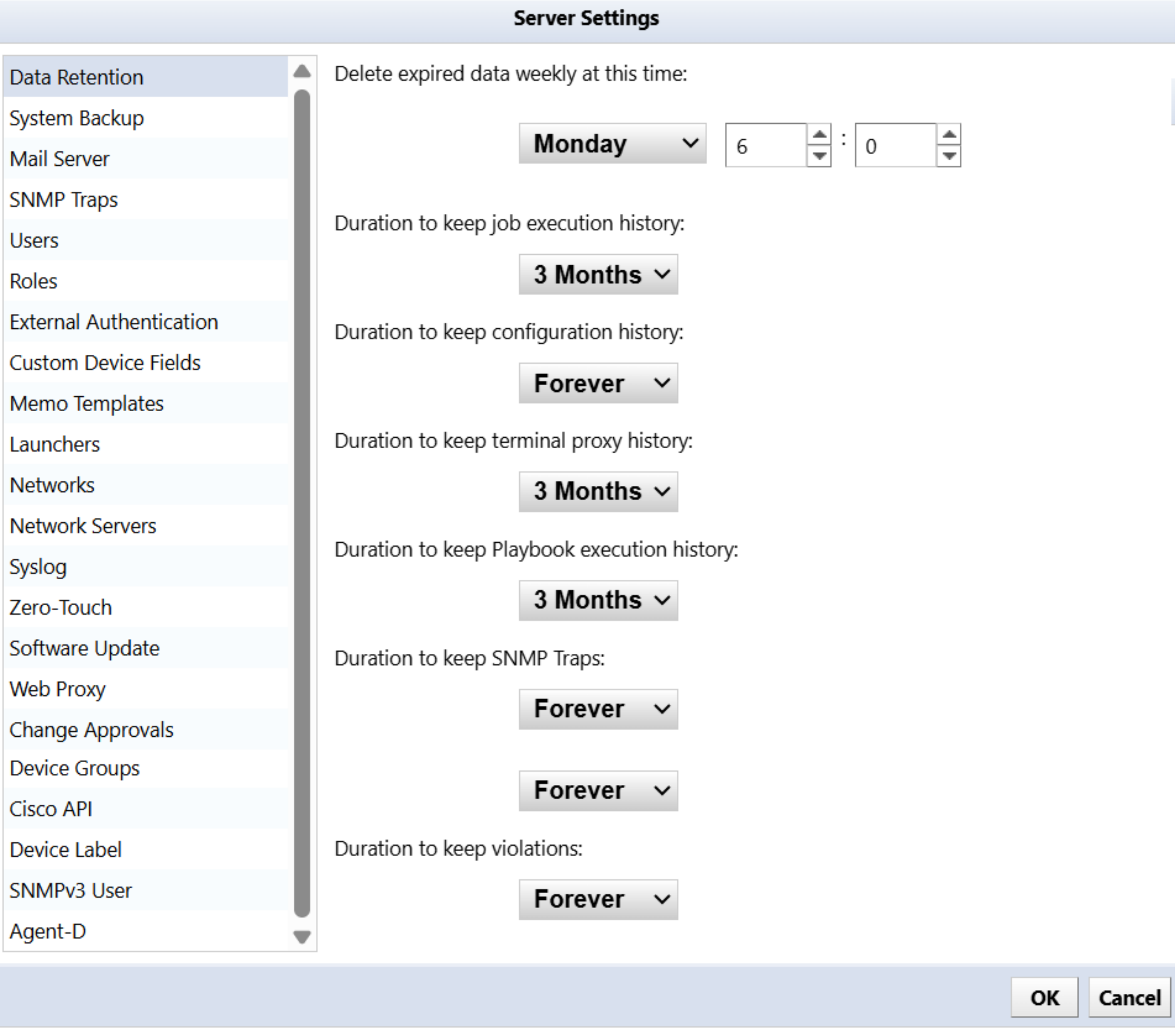


Global Menu Item	Explanation
Network	The currently selected Managed Network. (This option is not visible when the logged in user only has access to a single Managed Network, or if no Managed Networks are configured.)
User name	The current login user name is displayed.
Logout	Log out of ThirdEye.
Setting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

5.1 Settings

The Global Menu [Settings] link provides centralized access to server configuration and system-wide preferences.

Click [Settings] to open the [Server Settings] window.



Server Settings

Delete expired data weekly at this time: Monday 6 : 0

Duration to keep job execution history: 3 Months

Duration to keep configuration history: Forever

Duration to keep terminal proxy history: 3 Months

Duration to keep Playbook execution history: 3 Months

Duration to keep SNMP Traps: Forever

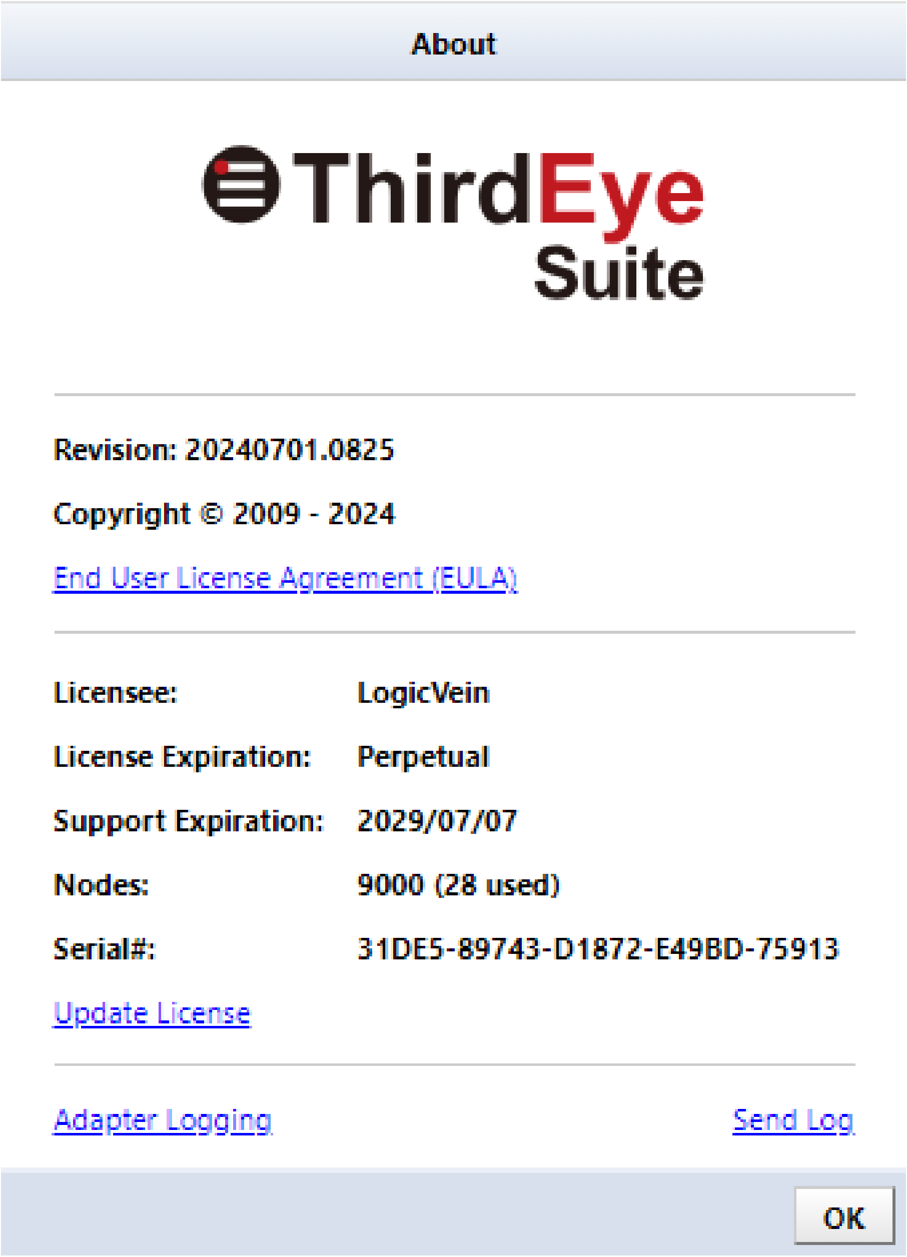
Forever

Duration to keep violations: Forever

5.2 About

Click [About] for the following information about ThirdEye:

- Product revision number
- Copyright information
- License and support expiration dates
- Nodes (and number used)
- Product serial number



About

ThirdEye Suite

Revision: 20240701.0825

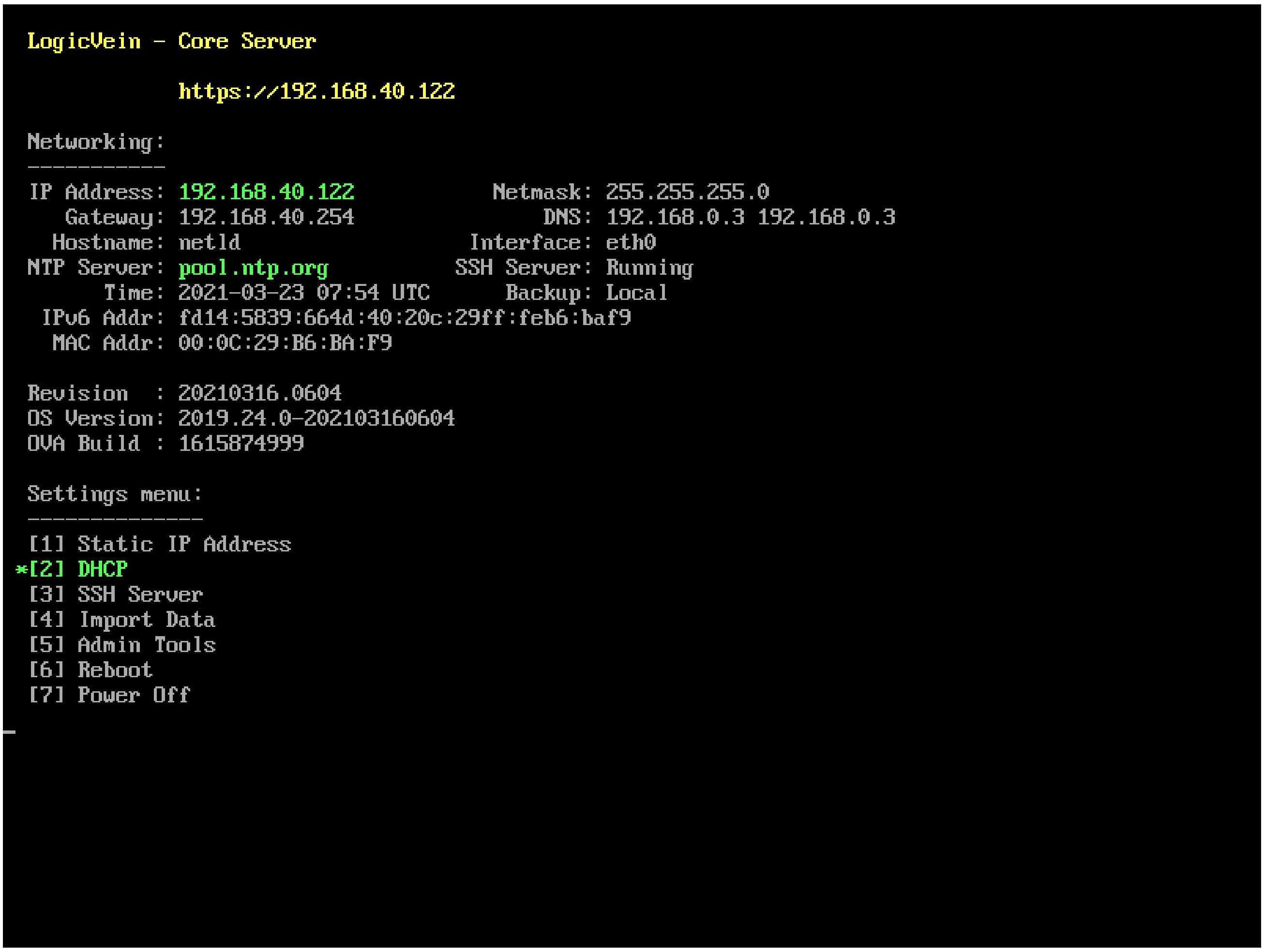
Copyright © 2009 - 2024

End User License Agreement (EULA)

Licensee:	LogicVein
License Expiration:	Perpetual
Support Expiration:	2029/07/07
Nodes:	9000 (28 used)
Serial#:	31DE5-89743-D1872-E49BD-75913

Update License

You can also check the Product revision number from the virtual machine console.



```
 LogicVein - Core Server

            https://192.168.40.122

 Networking:
 -----------
 IP Address: 192.168.40.122          Netmask: 255.255.255.0
    Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                 Interface: eth0
 NTP Server: pool.ntp.org         SSH Server: Running
       Time: 2021-03-23 07:54 UTC     Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

 Settings menu:
 --------------
 [1] Static IP Address
*[2] DHCP
 [3] SSH Server
 [4] Import Data
 [5] Admin Tools
 [6] Reboot
 [7] Power Off
_
```

You can configure adapter diagnostic settings, send information to support via email, and update the product license.

Note

Your SMTP (mail) server must be configured in Server Settings in order to send information to support using this feature.

5.3 Update License

If you update support, or increase the number of license nodes, you will need to update the applied license.

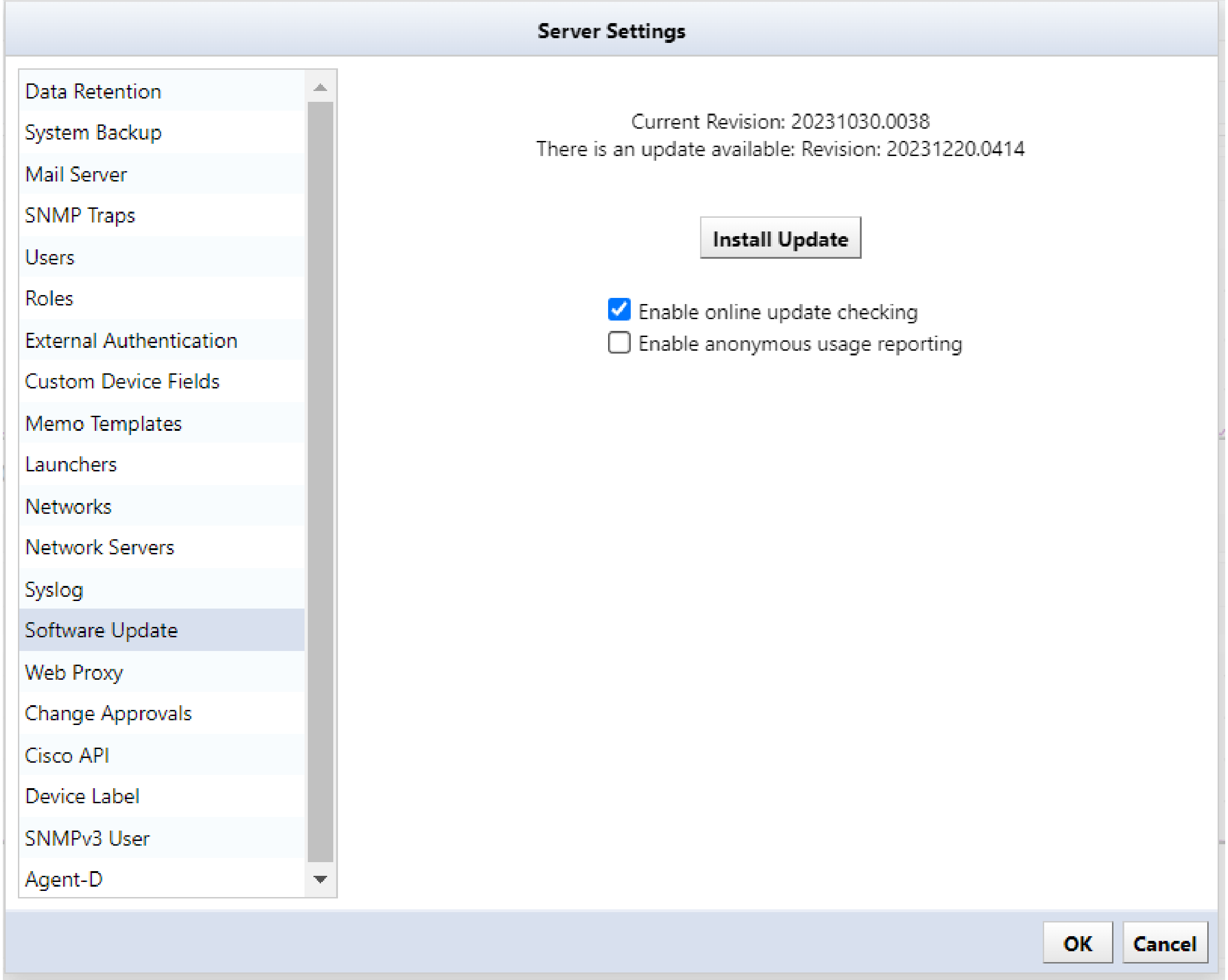
This task can only be performed by a user with administrator privileges.

1. Click [Help] > [About] on the Global Menu.
2. Click [Update License].

5.4 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. In the online environment, the license will be updated automatically.

1. Click [Settings] In the Global Menu to open the [Server Settings] window.
2. Click [Software Update] in the left sidepanel.



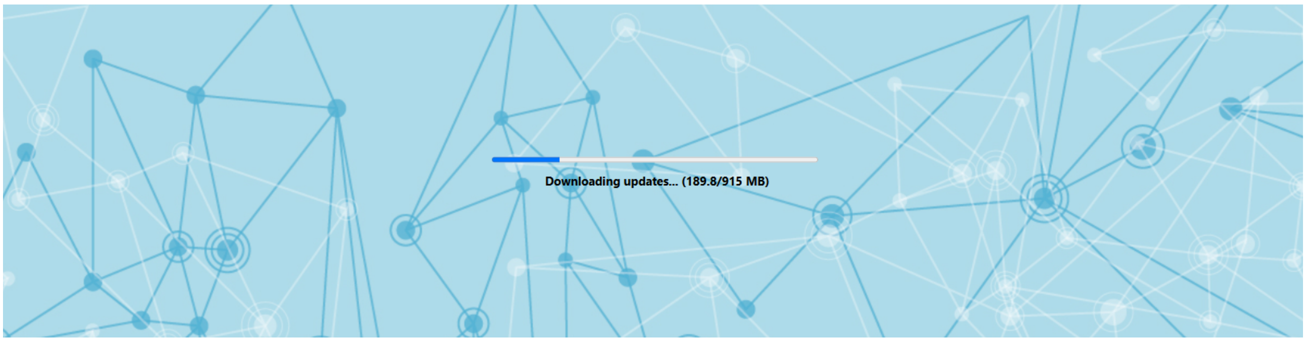
Current Revision: 20231030.0038
There is an update available: Revision: 20231220.0414

☑ Enable online update checking
□ Enable anonymous usage reporting

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)

Setting	Explanation
Enable anonymous usage reporting	If Enable Anonymous Usage Reporting is checked, usage data will be sent anonymously.

The update will then begin, and ThirdEye will restart.



Downloading updates... (189.8/915 MB)

5.5 Update Offline

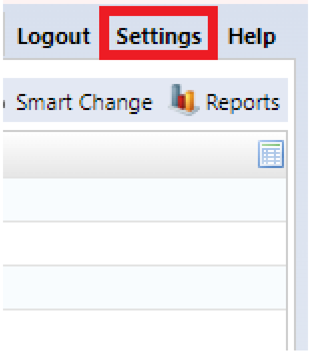
If you are in an offline environment, a screen to enter the activation key will be displayed. Please prepare the activation key in advance and update.

Refer to the **Apply the License** section for instructions on using the activation key.

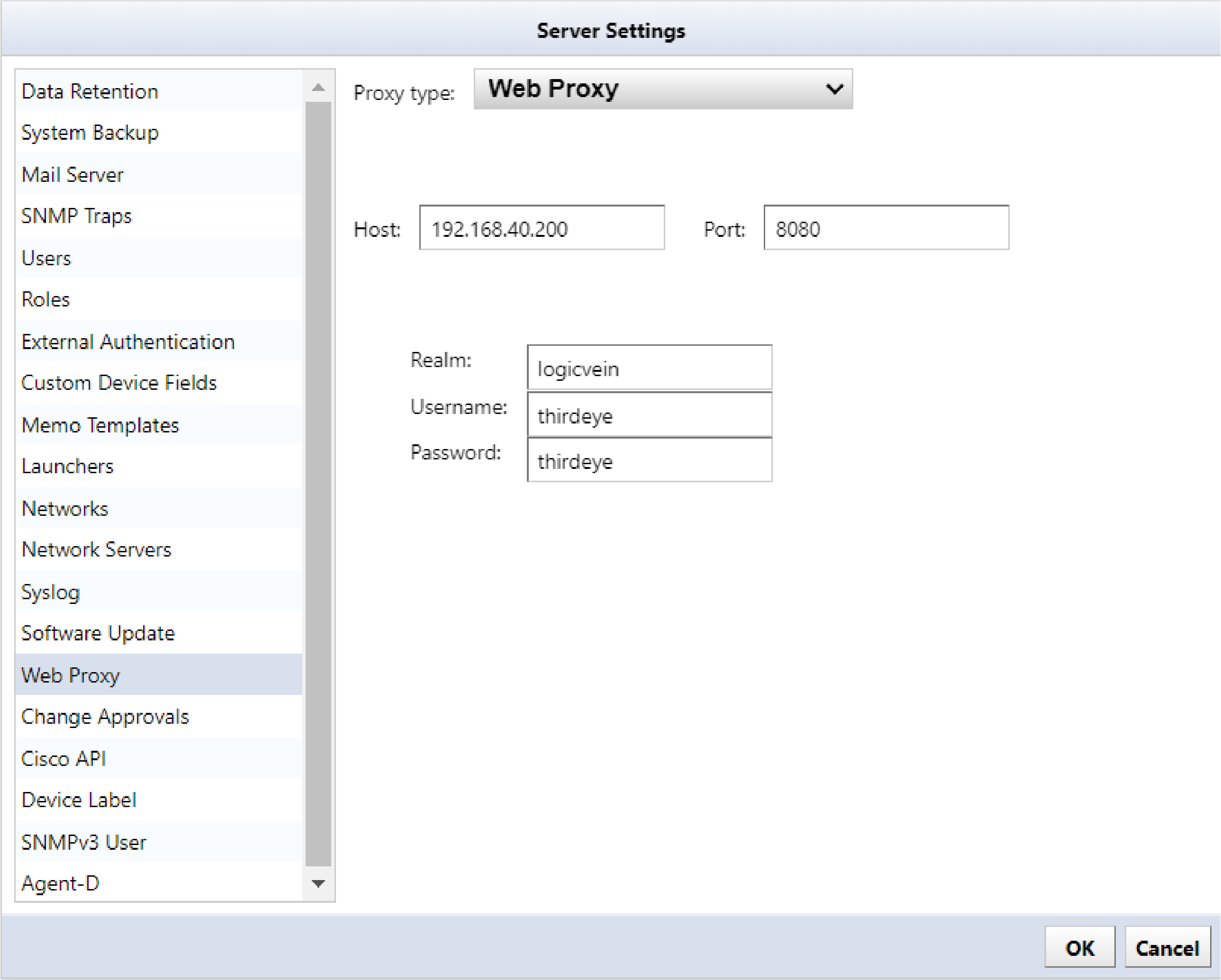
5.6 Proxy Server Updates

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.



Proxy type: Web Proxy

Host: 192.168.40.200 Port: 8080

Realm: logicvein

Username: thirdeye

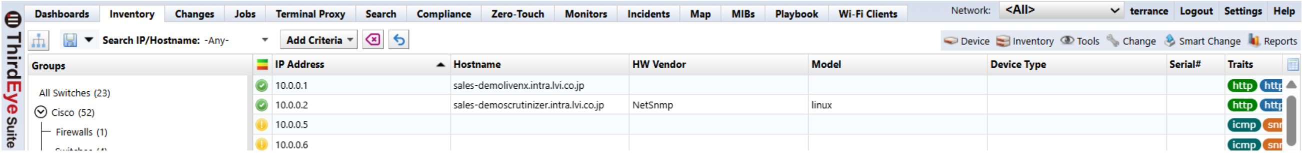
Password: thirdeye

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.

SECTION 6

TABS

The ThirdEye interface provides manages networks through 13 main tabs:



IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.0.0.1	sales-demolivenx.intra.lvi.co.jp					http http
10.0.0.2	sales-demoscrutinizer.intra.lvi.co.jp	NetSnmp	linux			http http
10.0.0.5						icmp snı
10.0.0.6						icmp snı

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

6.1 Dashboards Tab

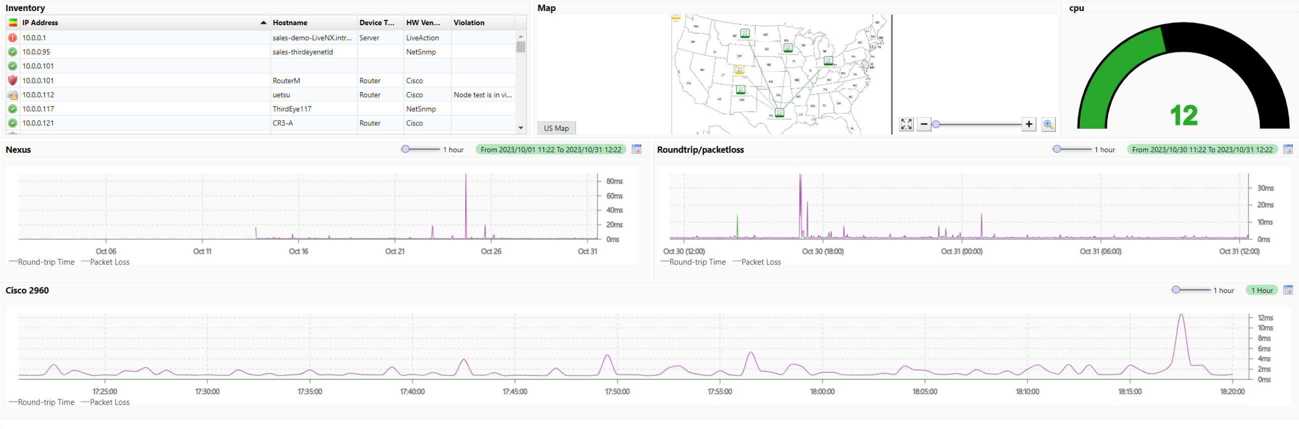
The [Dashboards] main tab is an interface that allows you to configure a single monitoring screen by embedding various items. Each embedded item is called a Widget. By adding widgets to your dashboard, you can more quickly access information.

Users can create new dashboards and add and rearrange widgets.

On the [Dashboards] 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

6.1.1 Dashboard Screen Components



Inventory

	IP Address	Hostname	Device T...	HW Ven...	Violation
●	10.0.0.1	sales-demo-LiveNX.intr...	Server	LiveAction	
✓	10.0.0.95	sales-thirdeyenetId		NetSnmp	
✓	10.0.0.101				
●	10.0.0.101	RouterM	Router	Cisco	
⚠	10.0.0.112	uetsu	Router	Cisco	Node test is in vi...
✓	10.0.0.117	ThirdEye117		NetSnmp	
✓	10.0.0.121	CR3-A	Router	Cisco	

Nexus — 1 hour — From 2023/10/01 11:22 To 2023/10/31 12:22

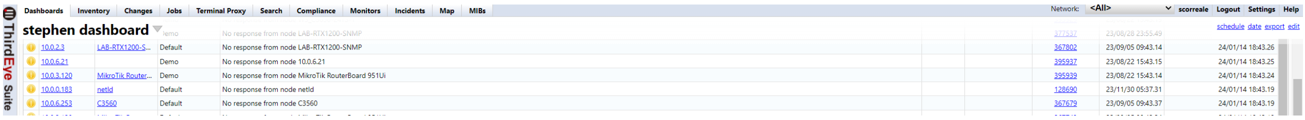
Roundtrip/packetloss — 1 hour — From 2023/10/30 11:22 To 2023/10/31 12:22

Cisco 2960 — 1 hour — 1 Hour

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)

6.1.2 Dashboard Edit Menu

In the [Dashboards] screen, the [schedule], [date], [export], and [edit] links are displayed by default in the upper right of the window:



		Demo	No response from node LAB-RTX1200-SNMP	377537	23/08/28 23:55.49	
10.0.2.3	LAB-RTX1200-S...	Default	No response from node LAB-RTX1200-SNMP	367802	23/09/05 09:43.14	24/01/14 18:43.26
10.0.6.21		Demo	No response from node 10.0.6.21	395937	23/08/22 15:43.15	24/01/14 18:43.25
10.0.3.120	MikroTik Router...	Demo	No response from node MikroTik RouterBoard 951Ui	395939	23/08/22 15:43.14	24/01/14 18:43.24
10.0.0.183	netld	Default	No response from node netld	128690	23/11/30 05:37.31	24/01/14 18:43.19
10.0.6.253	C3560	Default	No response from node C3560	367679	23/09/05 09:43.37	24/01/14 18:43.19

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.

Click [edit] to display additional buttons:

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

More details regarding the [Dashboards] main tab are available in the **Dashboard Management** section and throughout this manual.

6.2 Inventory Tab

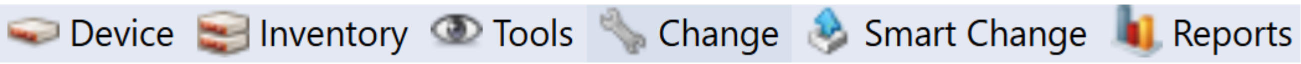
The [Inventory] main tab serves as the centralized registry for all devices managed by ThirdEye. It provides real-time information such as device status, configurations, and connectivity. It also displays details about as hardware/software versions, IP addresses, and operational health indicators. It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

More details regarding the [Inventory] main tab are available in the **Device Management** section and throughout this manual.

6.3 Inventory Tab Menu Bar

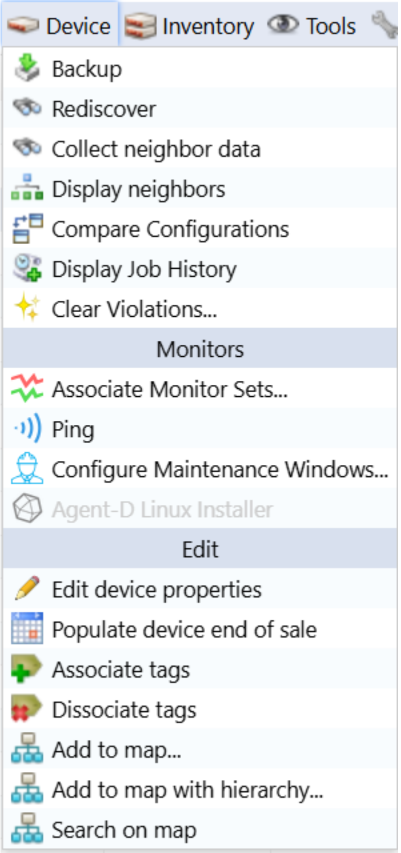
The [Inventory] tab contains a Menu Bar with 6 items:

- [Device]
- [Inventory]
- [Tools]
- [Change]
- [Smart Change]
- [Reports]



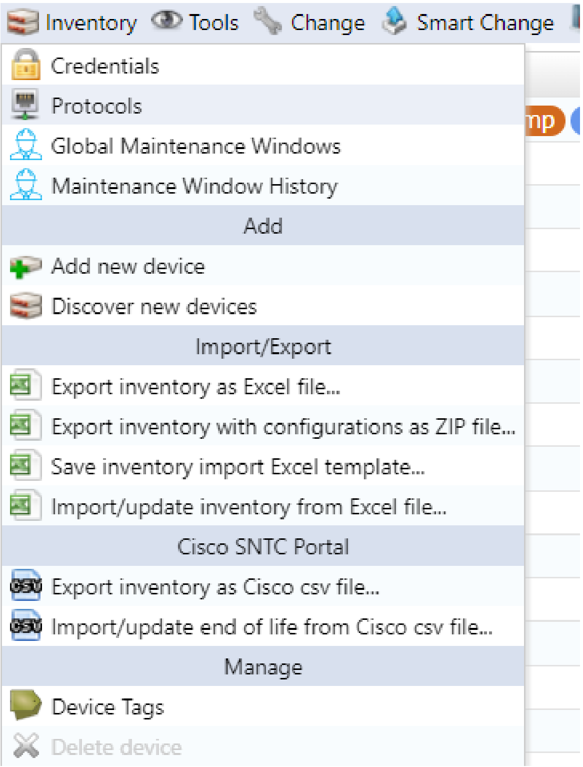
6.3.1 Device Menu

The [Device] Menu is the core interface for adding/editing individual devices (manual entry, network discovery, Excel imports) with detailed attribute management.



6.3.2 Inventory Menu

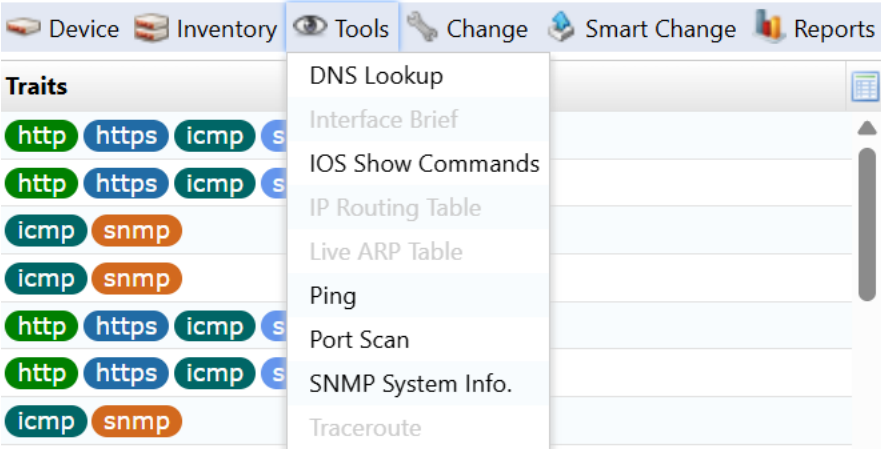
The [Inventory] Menu provides a unified view of all managed devices, with bulk operations and advanced filtering capabilities.


Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device
mp

6.3.3 Tools Menu

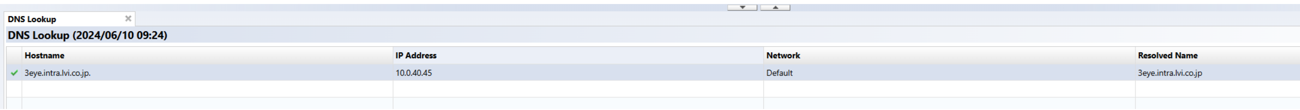
The [Tools] Menu allows you to determine the real-time status of the selected device. It is also possible to export all detected results as a CSV file.

Using items in the [Tools] menu opens a dedicated window. Exporting can be done using the ▤ button located in the top right corner of this window.



6.3.3.1 DNS Lookup

The [DNS Lookup] window displays the device's DNS information.



DNS Lookup (2024/06/10 09:24)

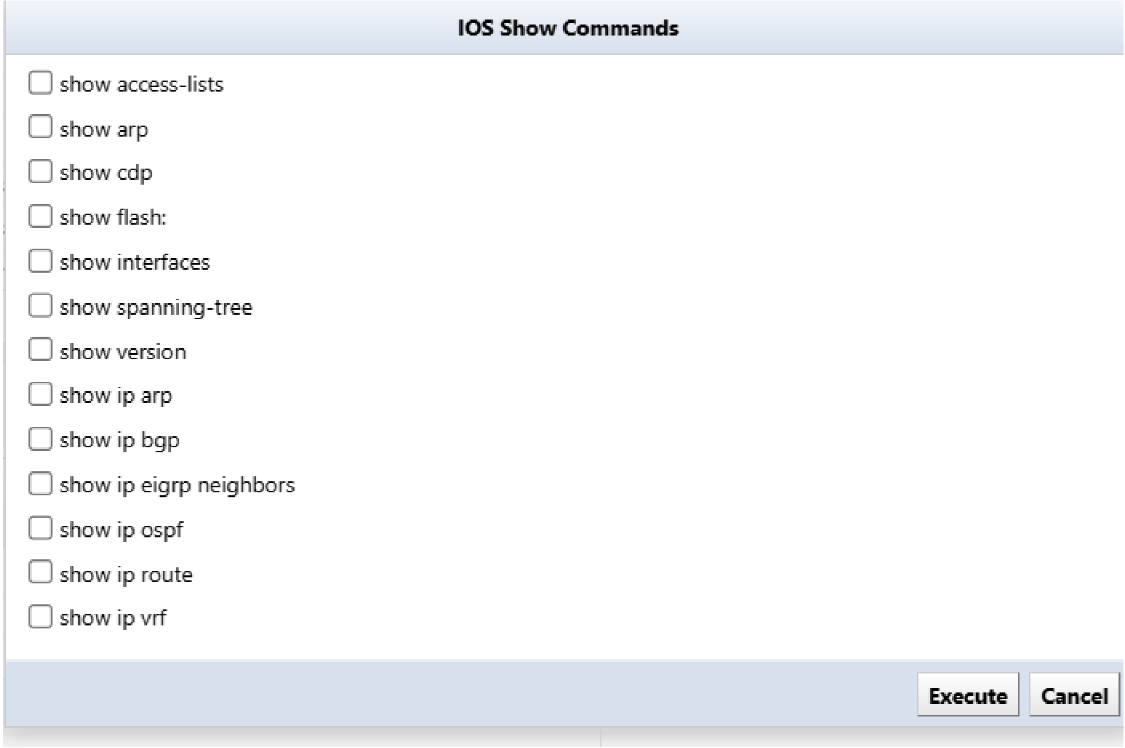
	Hostname	IP Address	Network	Resolved Name
✓	3eye.intra.lvi.co.jp.	10.0.40.45	Default	3eye.intra.lvi.co.jp

6.3.3.2 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 **Execute** to issue the command.

Note

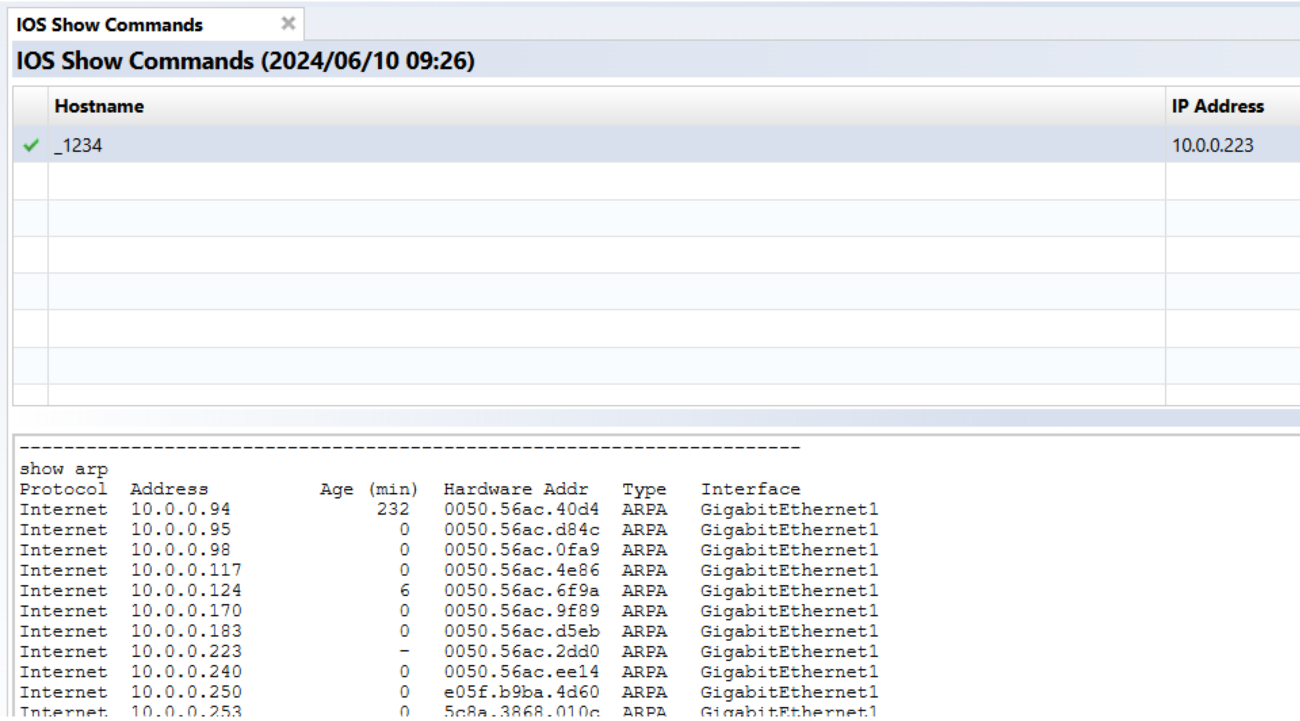
This command can only be run on devices that are compatible with Cisco IOS.



IOS Show Commands

□ show access-lists
□ show arp
□ show cdp
□ show flash:
□ show interfaces
□ show spanning-tree
□ show version
□ show ip arp
□ show ip bgp
□ show ip eigrp neighbors
□ show ip ospf
□ show ip route
□ show ip vrf

An ARP screen showing the results of executing the command will be displayed.



IOS Show Commands

IOS Show Commands (2024/06/10 09:26)

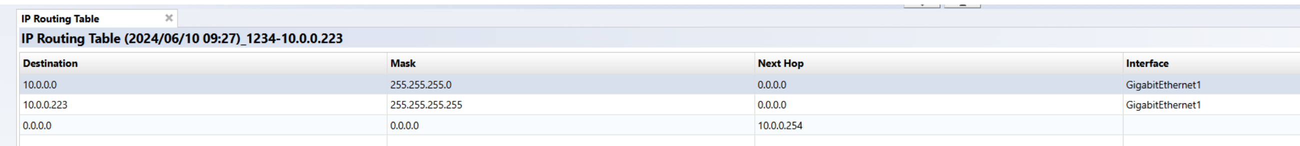
	Hostname	IP Address
✓	_1234	10.0.0.223

```
---------------------------------------------------------------------
show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.94             232   0050.56ac.40d4  ARPA   GigabitEthernet1
Internet  10.0.0.95               0   0050.56ac.d84c  ARPA   GigabitEthernet1
Internet  10.0.0.98               0   0050.56ac.0fa9  ARPA   GigabitEthernet1
Internet  10.0.0.117              0   0050.56ac.4e86  ARPA   GigabitEthernet1
Internet  10.0.0.124              6   0050.56ac.6f9a  ARPA   GigabitEthernet1
Internet  10.0.0.170              0   0050.56ac.9f89  ARPA   GigabitEthernet1
Internet  10.0.0.183              0   0050.56ac.d5eb  ARPA   GigabitEthernet1
Internet  10.0.0.223              -   0050.56ac.2dd0  ARPA   GigabitEthernet1
Internet  10.0.0.240              0   0050.56ac.ee14  ARPA   GigabitEthernet1
Internet  10.0.0.250              0   e05f.b9ba.4d60  ARPA   GigabitEthernet1
Internet  10.0.0.253              0   5c8a.3868.010c  ARPA   GigabitEthernet1
```

6.3.3.3 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.



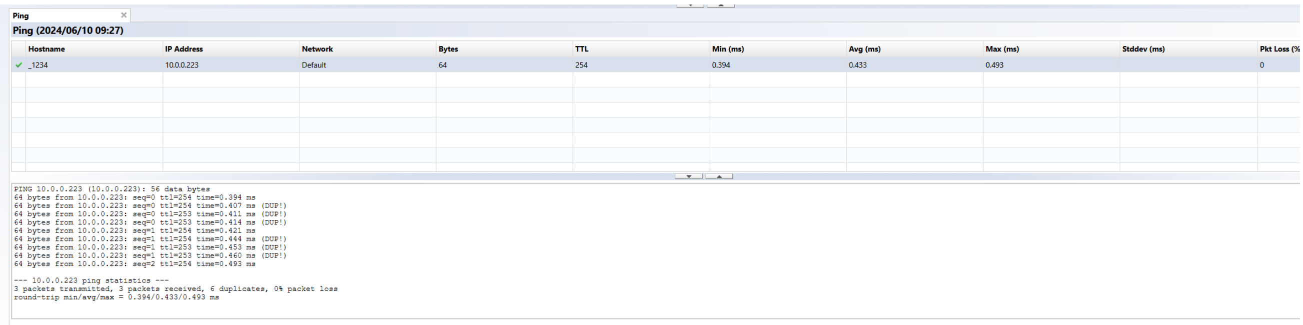
IP Routing Table

IP Routing Table (2024/06/10 09:27)_1234-10.0.0.223

Destination	Mask	Next Hop	Interface
10.0.0.0	255.255.255.0	0.0.0.0	GigabitEthernet1
10.0.0.223	255.255.255.255	0.0.0.0	GigabitEthernet1
0.0.0.0	0.0.0.0	10.0.0.254	

6.3.3.4 Ping

From the [Ping] window, you can ping a device and check the response.



Ping

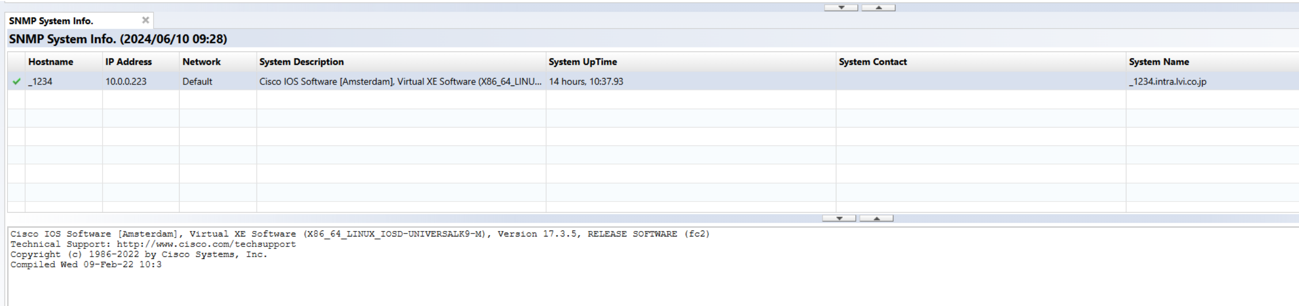
Ping (2024/06/10 09:27)

	Hostname	IP Address	Network	Bytes	TTL	Min (ms)	Avg (ms)	Max (ms)	Stddev (ms)	Pkt Loss (%
✓	_1234	10.0.0.223	Default	64	254	0.394	0.433	0.493		0

```
PING 10.0.0.223 (10.0.0.223): 56 data bytes
64 bytes from 10.0.0.223: seq=0 ttl=254 time=0.394 ms
64 bytes from 10.0.0.223: seq=0 ttl=254 time=0.407 ms (DUP!)
64 bytes from 10.0.0.223: seq=0 ttl=253 time=0.411 ms (DUP!)
64 bytes from 10.0.0.223: seq=0 ttl=253 time=0.414 ms (DUP!)
64 bytes from 10.0.0.223: seq=1 ttl=254 time=0.421 ms
64 bytes from 10.0.0.223: seq=1 ttl=254 time=0.444 ms (DUP!)
64 bytes from 10.0.0.223: seq=1 ttl=253 time=0.453 ms (DUP!)
64 bytes from 10.0.0.223: seq=1 ttl=253 time=0.460 ms (DUP!)
64 bytes from 10.0.0.223: seq=2 ttl=254 time=0.493 ms

--- 10.0.0.223 ping statistics ---
3 packets transmitted, 3 packets received, 6 duplicates, 0% packet loss
round-trip min/avg/max = 0.394/0.433/0.493 ms
```

6.3.3.5 SNMP System Info

The [SNMP System Info] window displays the device’s SNMP system information.



SNMP System Info. (2024/06/10 09:28)

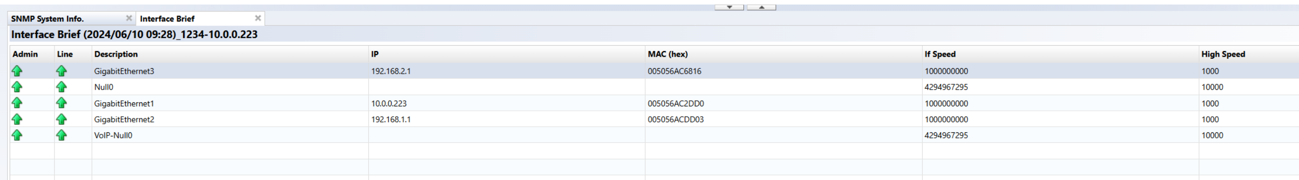
	Hostname	IP Address	Network	System Description	System UpTime	System Contact	System Name
✓	_1234	10.0.0.223	Default	Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINU...	14 hours, 10:37.93		_1234.intra.lvi.co.jp

```
Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed 09-Feb-22 10:3
```

6.3.3.6 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.



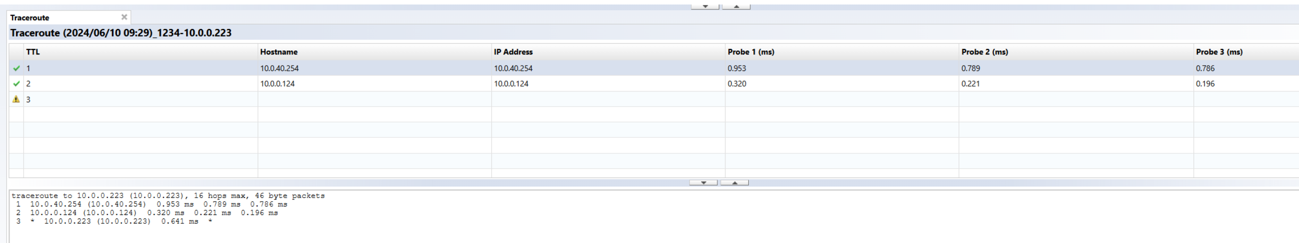
Interface Brief (2024/06/10 09:28)_1234-10.0.0.223

Admin	Line	Description	IP	MAC (hex)	If Speed	High Speed
⇧	⇧	GigabitEthernet3	192.168.2.1	005056AC6816	1000000000	1000
⇧	⇧	Null0			4294967295	10000
⇧	⇧	GigabitEthernet1	10.0.0.223	005056AC2DD0	1000000000	1000
⇧	⇧	GigabitEthernet2	192.168.1.1	005056ACDD03	1000000000	1000
⇧	⇧	VoIP-Null0			4294967295	10000

6.3.3.7 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.



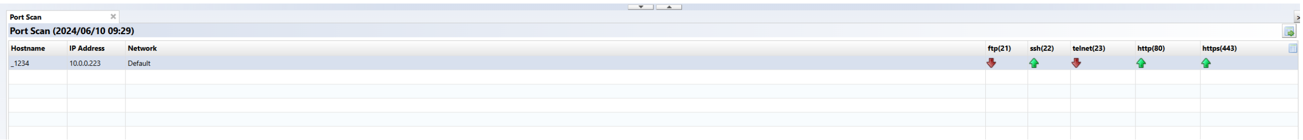
Traceroute (2024/06/10 09:29)_1234-10.0.0.223

	TTL	Hostname	IP Address	Probe 1 (ms)	Probe 2 (ms)	Probe 3 (ms)
✓	1	10.0.40.254	10.0.40.254	0.953	0.789	0.786
✓	2	10.0.0.124	10.0.0.124	0.320	0.221	0.196
⚠	3					

```
traceroute to 10.0.0.223 (10.0.0.223), 16 hops max, 46 byte packets
 1  10.0.40.254 (10.0.40.254)  0.953 ms  0.789 ms  0.786 ms
 2  10.0.0.124 (10.0.0.124)  0.320 ms  0.221 ms  0.196 ms
 3  *  10.0.0.223 (10.0.0.223)  0.641 ms  *
```

6.3.3.8 Port Scan

The [Port Scan] window displays device port opening/closing information.



Port Scan

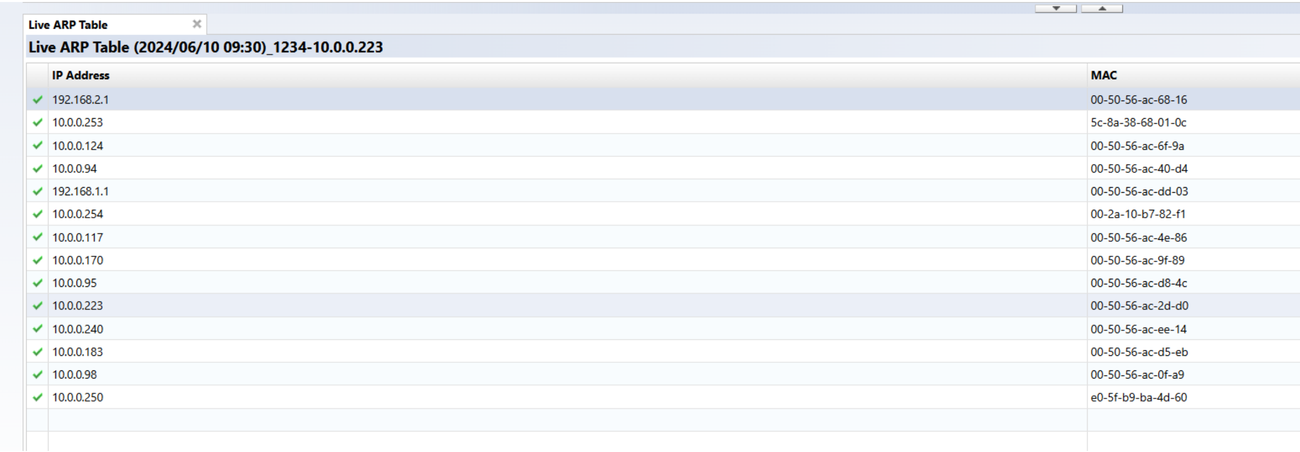
Port Scan (2024/06/10 09:29)

Hostname	IP Address	Network	ftp(21)	ssh(22)	telnet(23)	http(80)	https(443)
_1234	10.0.0.223	Default	⬇	⬆	⬇	⬆	⬆

6.3.3.9 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.



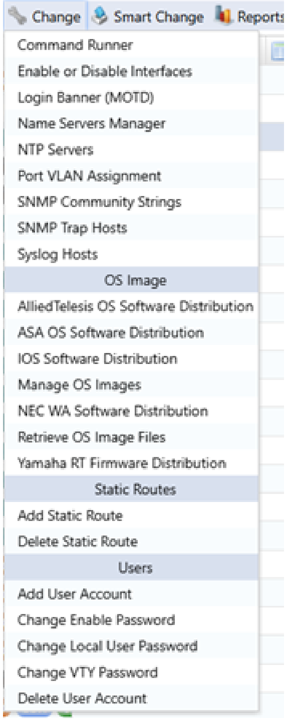
Live ARP Table

Live ARP Table (2024/06/10 09:30)_1234-10.0.0.223

	IP Address	MAC
✓	192.168.2.1	00-50-56-ac-68-16
✓	10.0.0.253	5c-8a-38-68-01-0c
✓	10.0.0.124	00-50-56-ac-6f-9a
✓	10.0.0.94	00-50-56-ac-40-d4
✓	192.168.1.1	00-50-56-ac-dd-03
✓	10.0.0.254	00-2a-10-b7-82-f1
✓	10.0.0.117	00-50-56-ac-4e-86
✓	10.0.0.170	00-50-56-ac-9f-89
✓	10.0.0.95	00-50-56-ac-d8-4c
✓	10.0.0.223	00-50-56-ac-2d-d0
✓	10.0.0.240	00-50-56-ac-ee-14
✓	10.0.0.183	00-50-56-ac-d5-eb
✓	10.0.0.98	00-50-56-ac-0f-a9
✓	10.0.0.250	e0-5f-b9-ba-4d-60

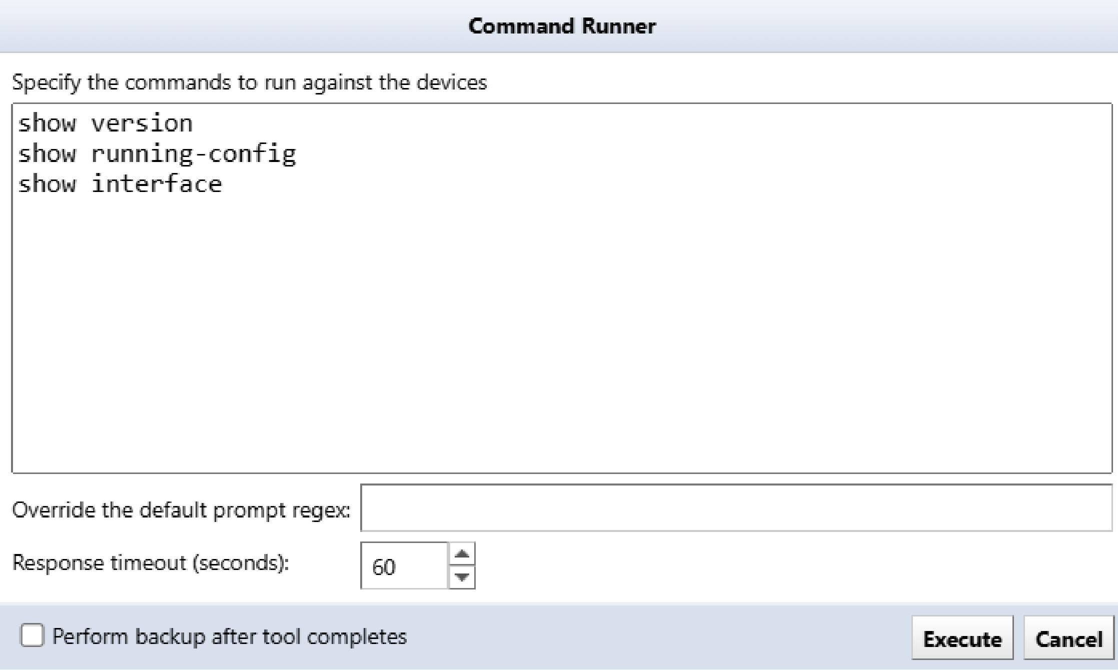
6.3.4 Change Menu Suite

The [Change] Menu collects operations related to modifying the configuration of the selected device.



6.3.4.1 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.



Command Runner

Specify the commands to run against the devices

```
show version
show running-config
show interface
```

Override the default prompt regex:

Response timeout (seconds): 60

☐ Perform backup after tool completes

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.

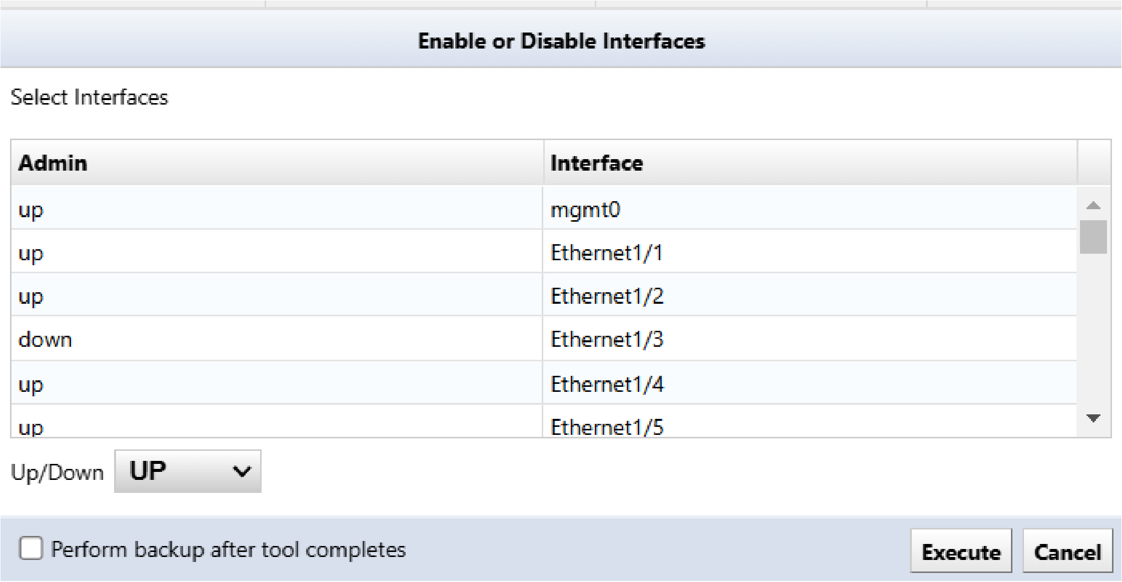
For example, some interactive commands may prompt for the next input with a simpler `<` instead of the usual `<username>#` prompt. In these cases, you must specify using the regular expression `^<` (at the beginning of the line). Otherwise, it will be impossible to distinguish between the output result of the command and the prompt.

6.3.4.2 Enable or Disable Interfaces

Here you can change the Admin Status of the device interface.

> **Note**
>
> This function cannot be executed when multiple devices are selected.

In 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.



Enable or Disable Interfaces

Select Interfaces

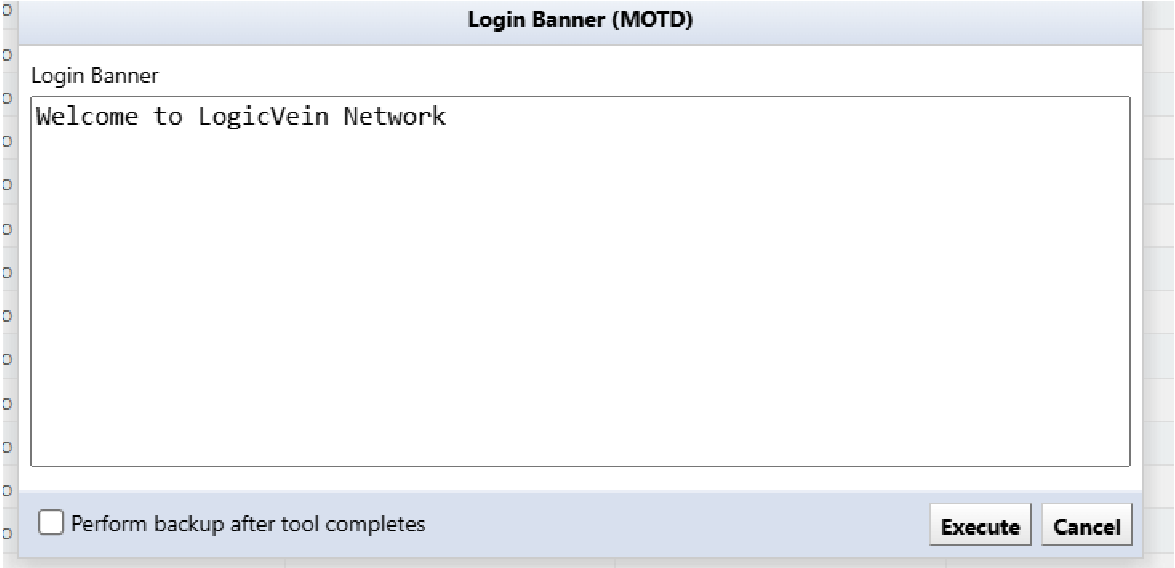
Admin	Interface
up	mgmt0
up	Ethernet1/1
up	Ethernet1/2
down	Ethernet1/3
up	Ethernet1/4
up	Ethernet1/5

Up/Down: UP

☐ Perform backup after tool completes

6.3.4.3 Login Banner (MOTD)

Here you can set the device login banner.



Login Banner (MOTD)

Login Banner

```
Welcome to LogicVein Network
```

☐ Perform backup after tool completes

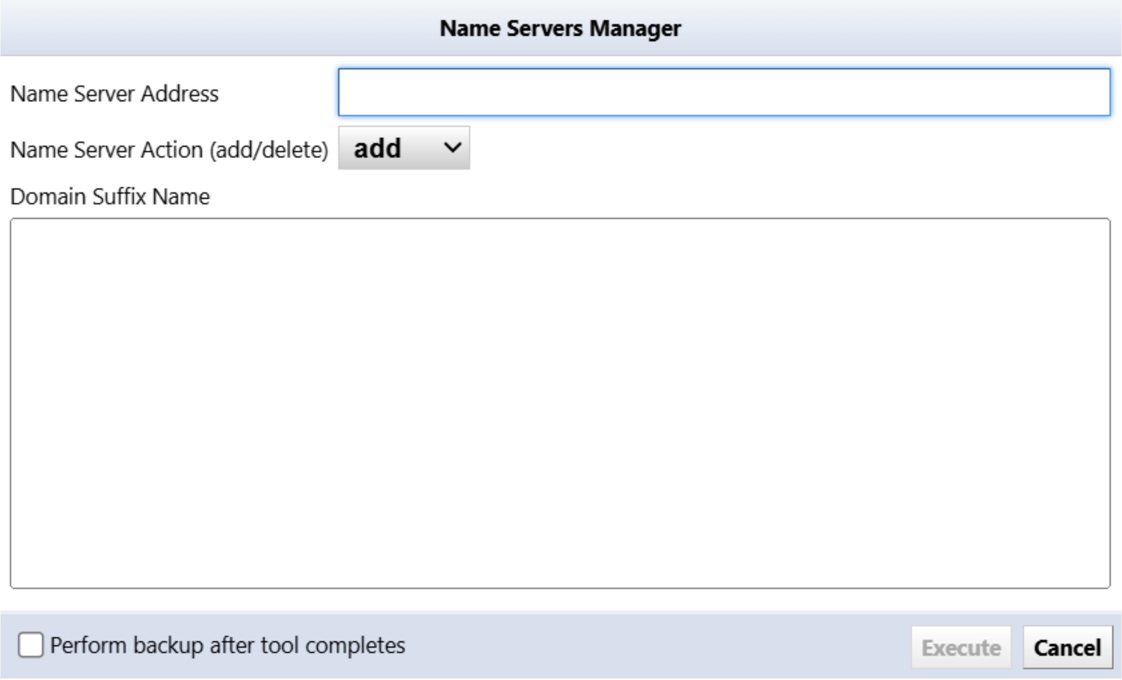
6.3.4.4 Name Servers Manager

In this window, you can 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.



Name Servers Manager

Name Server Address

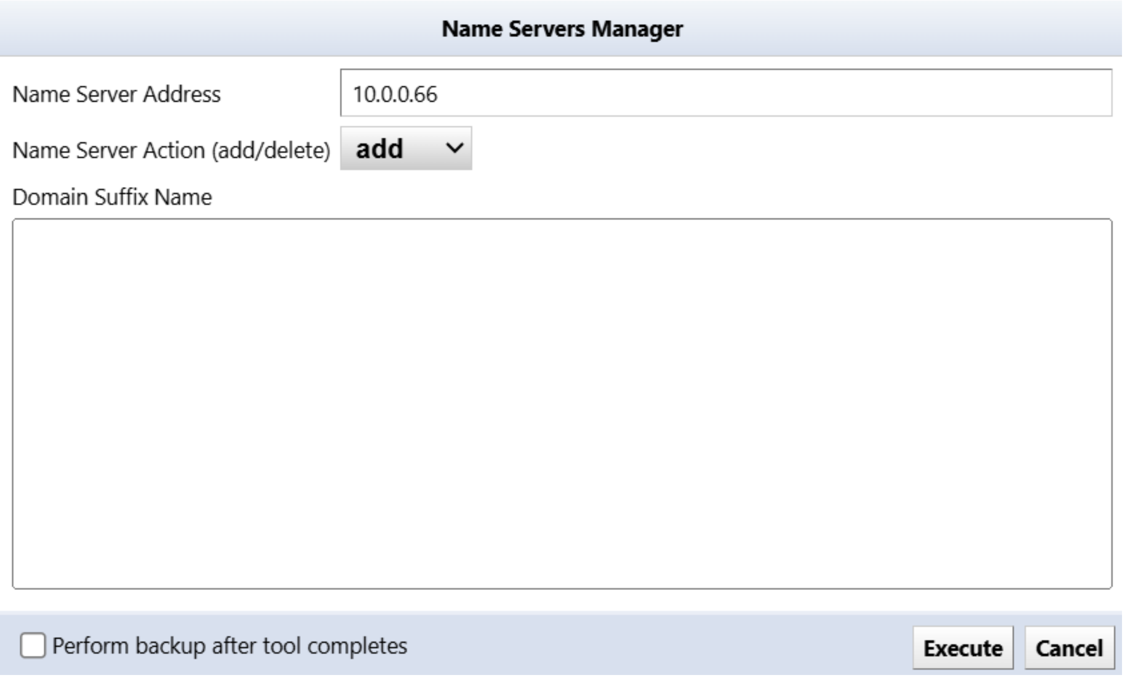
Name Server Action (add/delete) add

Domain Suffix Name

□ Perform backup after tool completes

The **Execute** button, will become clickable.

3. Click **Execute**.



Name Servers Manager

Name Server Address 10.0.0.66

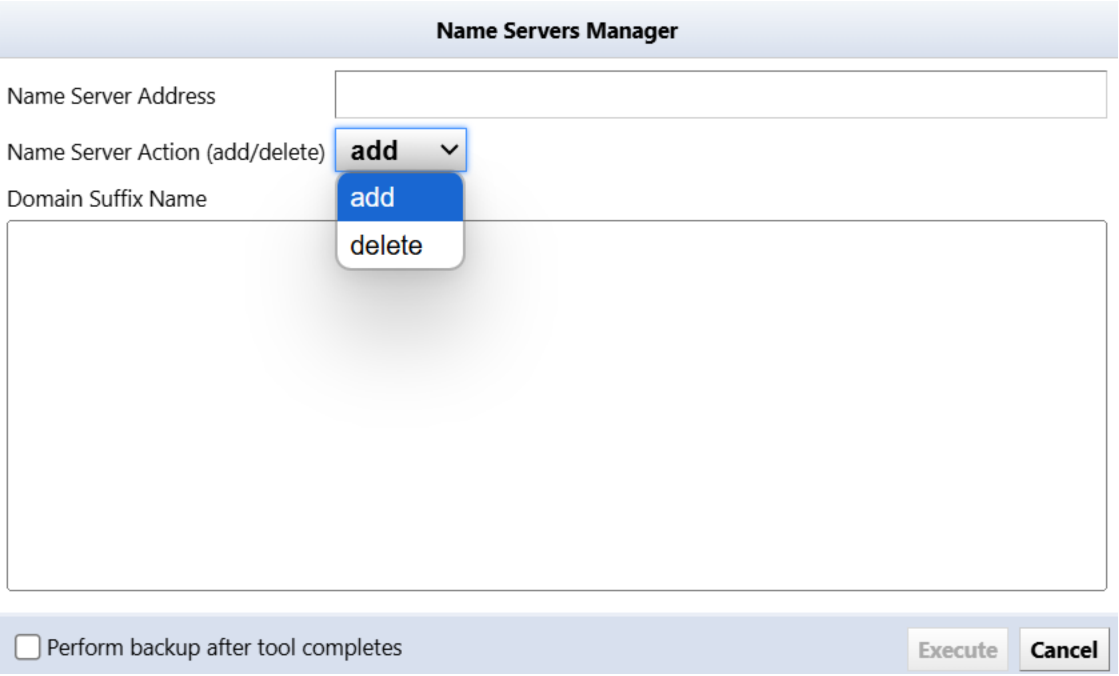
Name Server Action (add/delete) add

Domain Suffix Name

□ Perform backup after tool completes

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".



Name Servers Manager

Name Server Address

Name Server Action (add/delete) add

add
delete

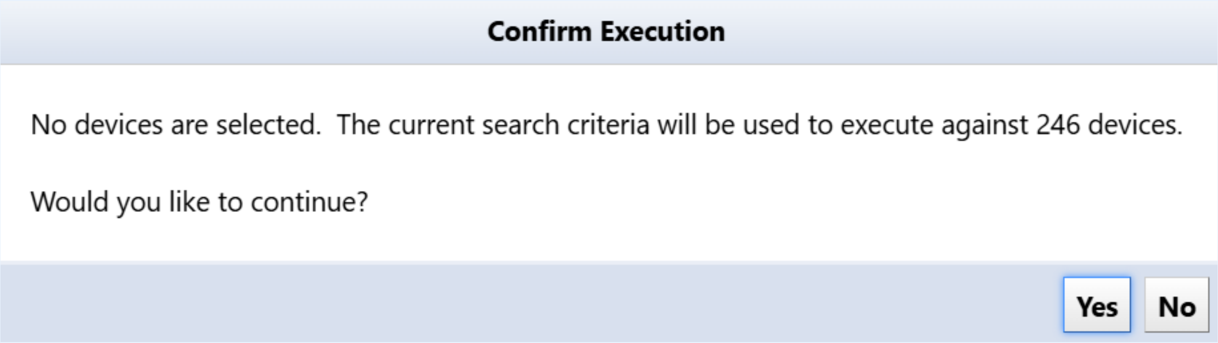
Domain Suffix Name

□ Perform backup after tool completes

Execute Cancel

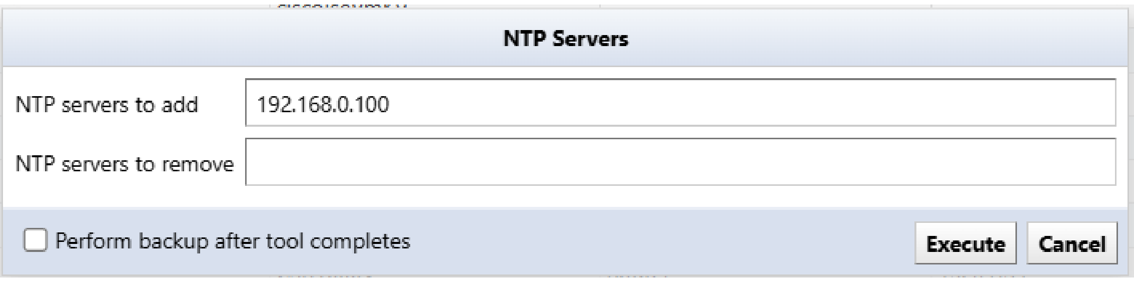
The **Execute** button, will become clickable.

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.
>
> 
>
> **Confirm Execution**
>
> No devices are selected. The current search criteria will be used to execute against 246 devices.
>
> Would you like to continue?
>
> Yes No

6.3.4.5 NTP Servers

In this window, you can add/remove NTP servers.



NTP Servers

NTP servers to add: 192.168.0.100

NTP servers to remove:

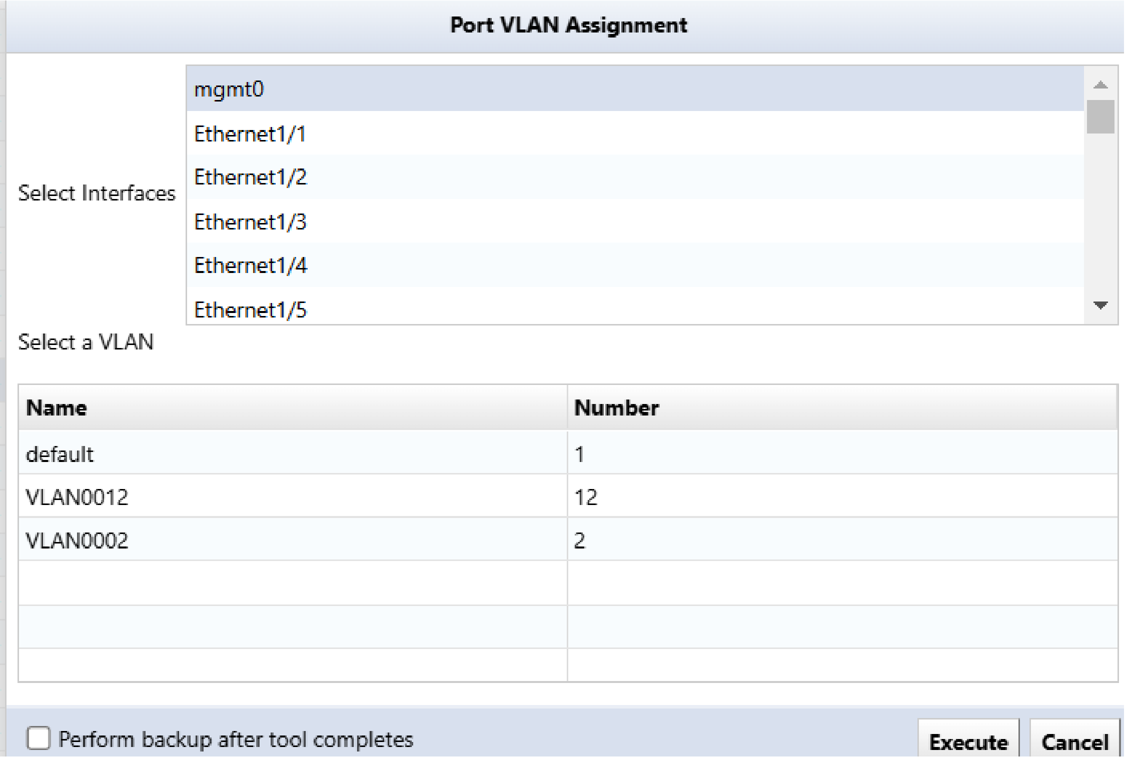
□ Perform backup after tool completes

6.3.4.6 Port VLAN Assignment

This feature allows you to perform VLAN port settings for the device's access port.

> **Note**
>
> This function cannot be executed when multiple devices are selected.

1. Select the interface on the screen.
2. Select the interface for VLAN settings (multiple selections are possible).
3. Select the VLAN.
4. Select the VLAN to be assigned from the field.
5. Click the **Execute** button.



Port VLAN Assignment

Select Interfaces

- mgmt0
- Ethernet1/1
- Ethernet1/2
- Ethernet1/3
- Ethernet1/4
- Ethernet1/5

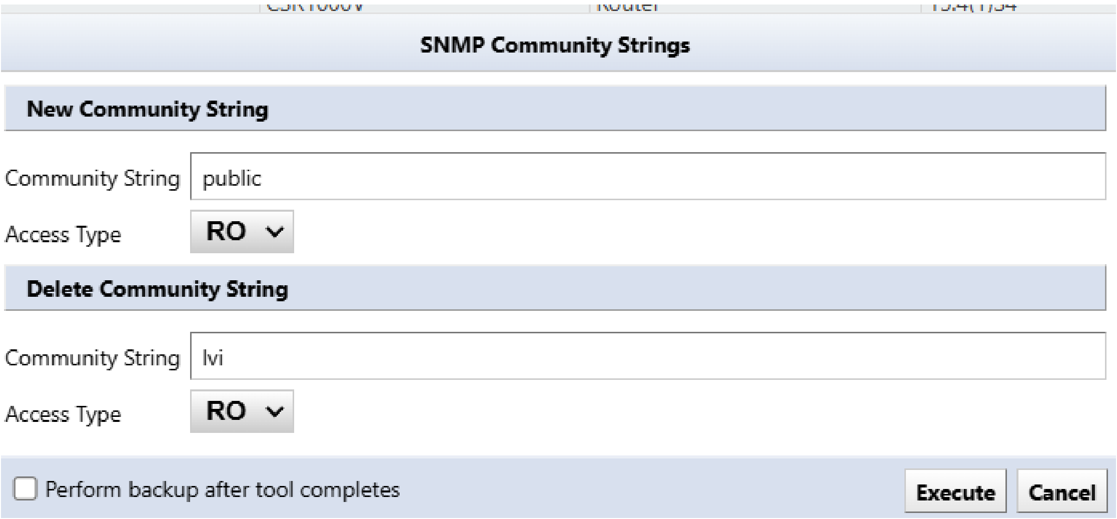
Select a VLAN

Name	Number
default	1
VLAN0012	12
VLAN0002	2

□ Perform backup after tool completes

6.3.4.7 SNMP Community Strings

Add/delete SNMP communities to/from devices.



SNMP Community Strings

New Community String

Community String: public

Access Type: RO

Delete Community String

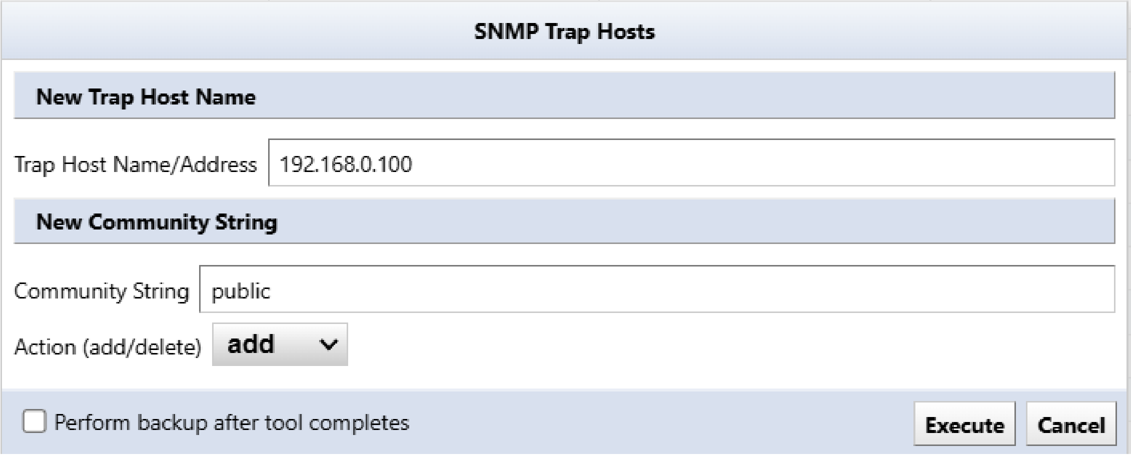
Community String: lvi

Access Type: RO

□ Perform backup after tool completes

6.3.4.8 SNMP Trap Hosts

Add/delete SNMP trap host settings for devices. (Effective for batch setting of new NMS installations.)



SNMP Trap Hosts

New Trap Host Name

Trap Host Name/Address: 192.168.0.100

New Community String

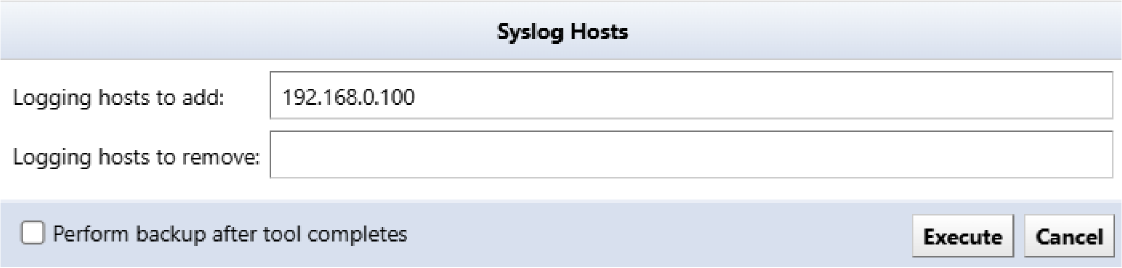
Community String: public

Action (add/delete): add

□ Perform backup after tool completes

6.3.4.9 Syslog Hosts

Add/delete Syslog hosts to/from the device.



Syslog Hosts

Logging hosts to add: 192.168.0.100

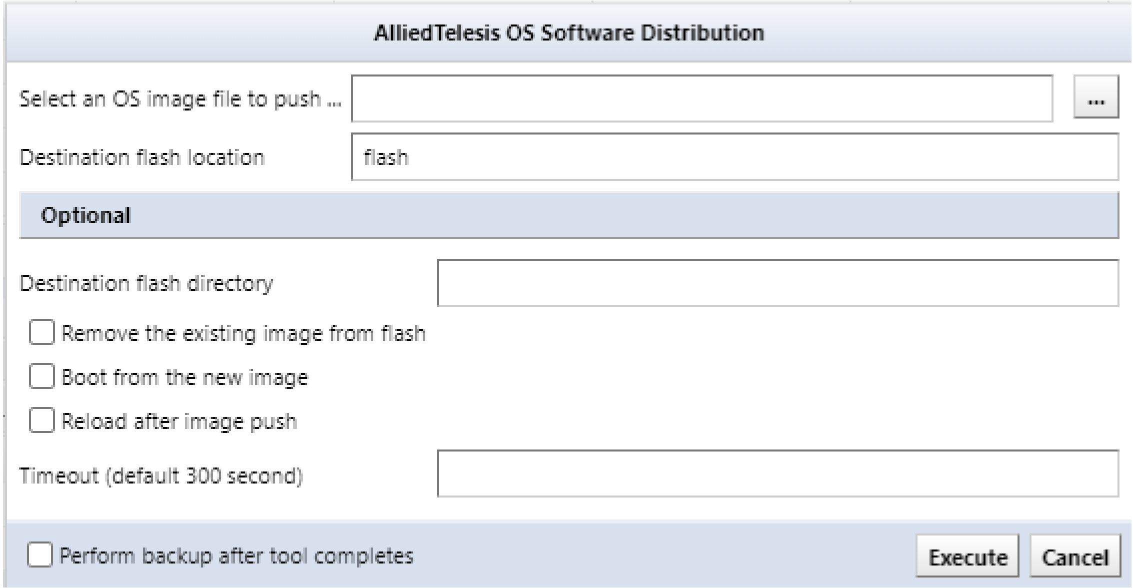
Logging hosts to remove:

□ Perform backup after tool completes

6.3.4.10 OS Image

6.3.4.10.1 AlliedTelesis OS software distribution

You can remotely distribute the OS to AlliedTelesis devices. To use this function, you must save the OS in advance.



AlliedTelesis OS Software Distribution

Select an OS image file to push ...

Destination flash location: flash

Optional

Destination flash directory

□ Remove the existing image from flash

□ Boot from the new image

□ Reload after image push

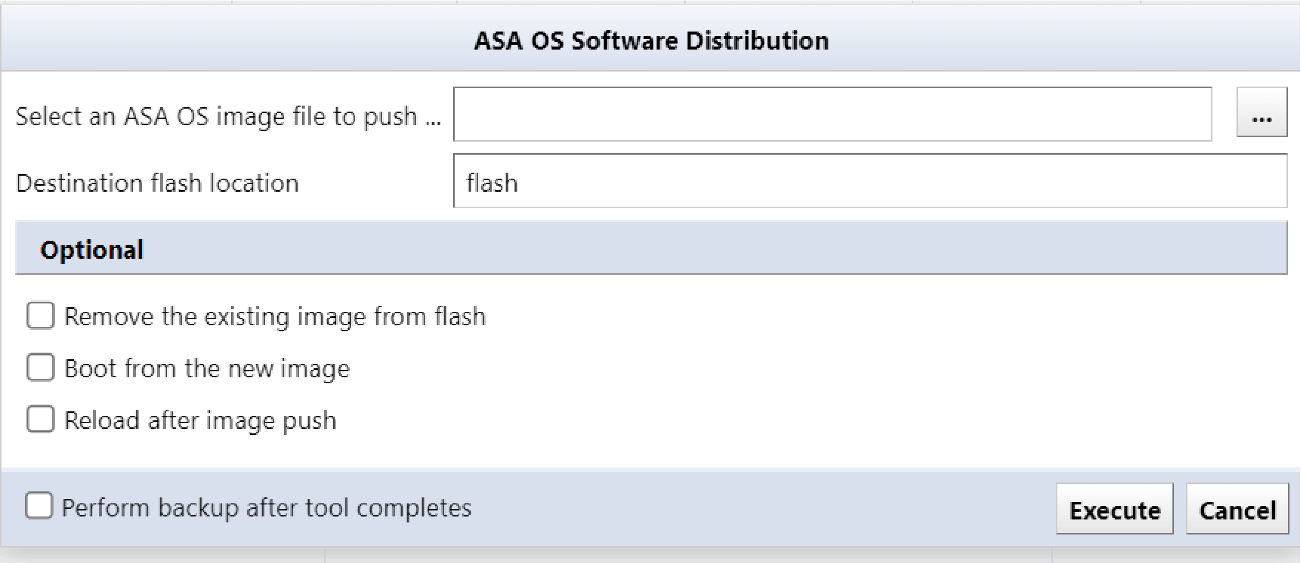
Timeout (default 300 second)

□ Perform backup after tool completes

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

6.3.4.10.2 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.



ASA OS Software Distribution

Select an ASA OS image file to push ...

Destination flash location: flash

Optional

□ Remove the existing image from flash

□ Boot from the new image

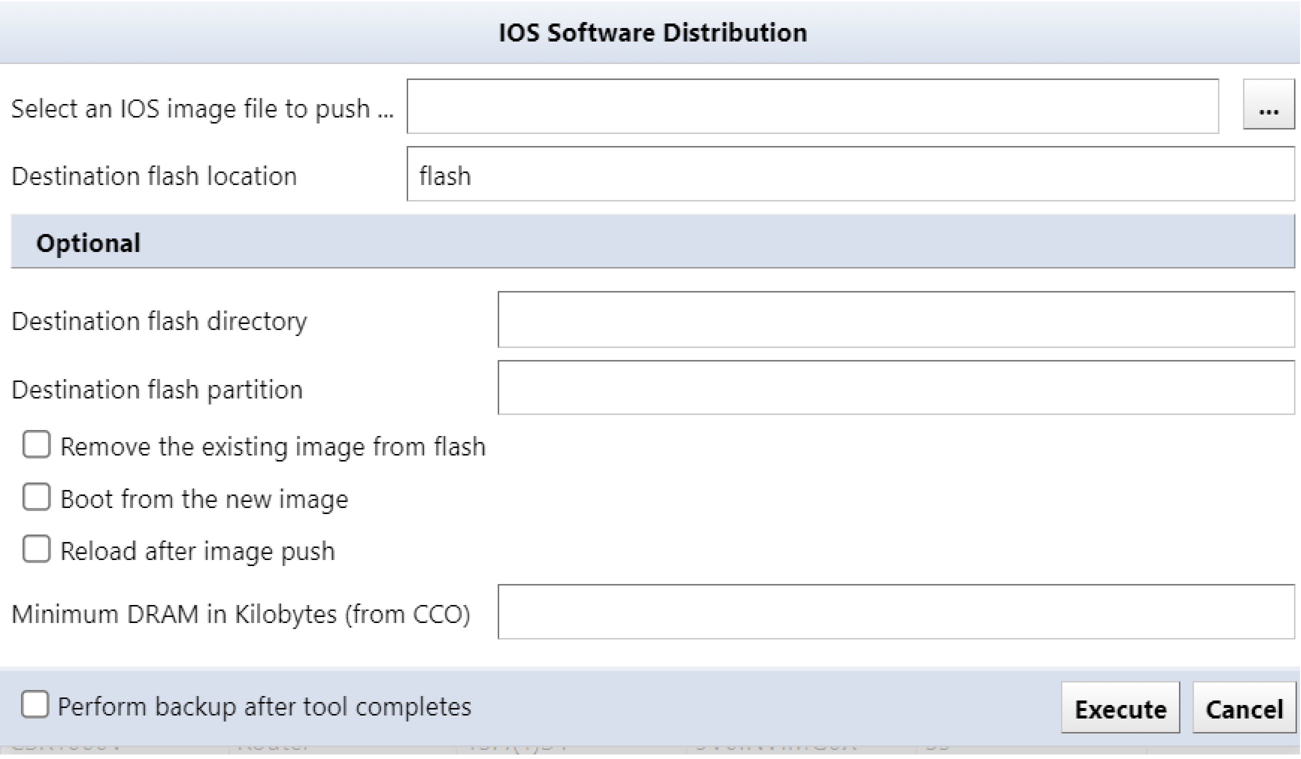
□ Reload after image push

□ Perform backup after tool completes

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

6.3.4.10.3 IOS software distribution

You can remotely distribute IOS to Cisco IOS devices. To use this feature, you must save the IOS in advance.



IOS Software Distribution

Select an IOS image file to push ... [ ] ...

Destination flash location: flash

Optional

Destination flash directory

Destination flash partition

☐ Remove the existing image from flash

☐ Boot from the new image

☐ Reload after image push

Minimum DRAM in Kilobytes (from CCO)

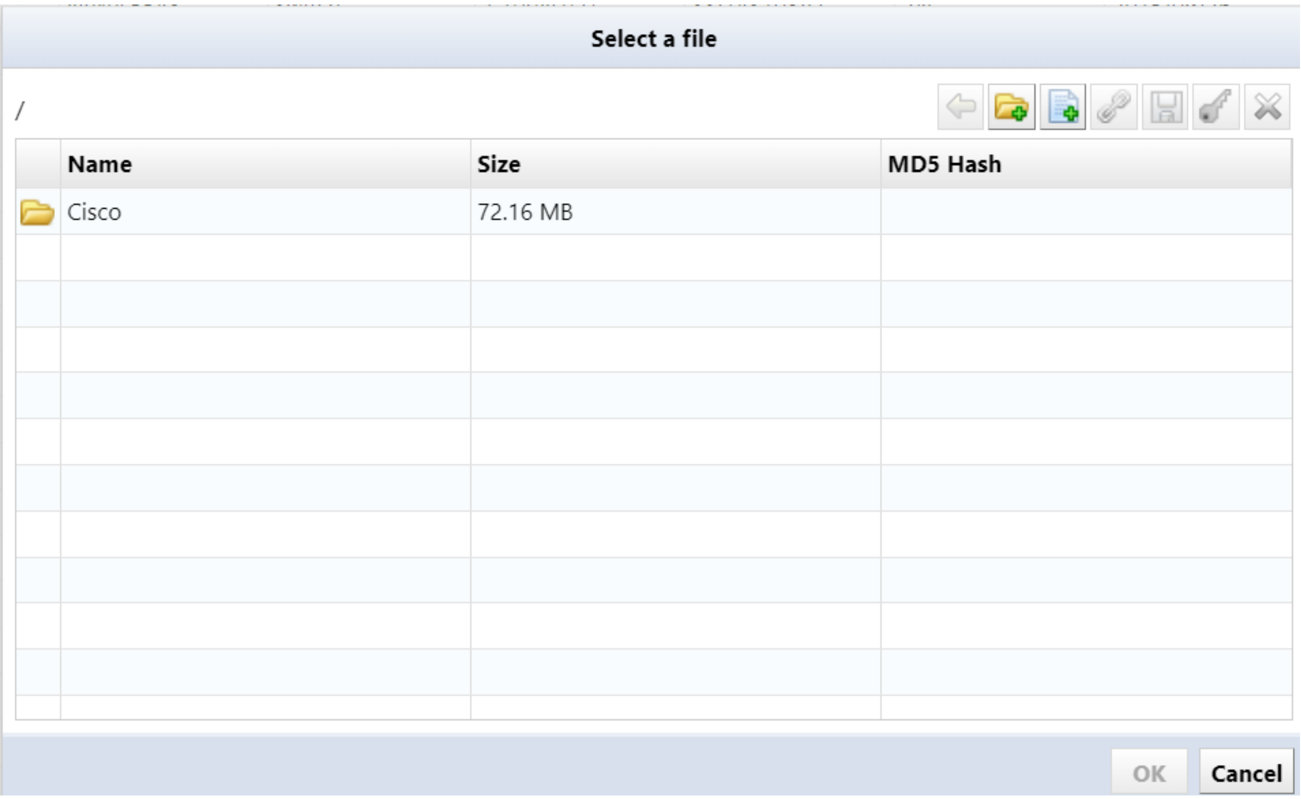
☐ Perform backup after tool completes

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

Setting	Explanation
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

6.3.4.10.4 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.

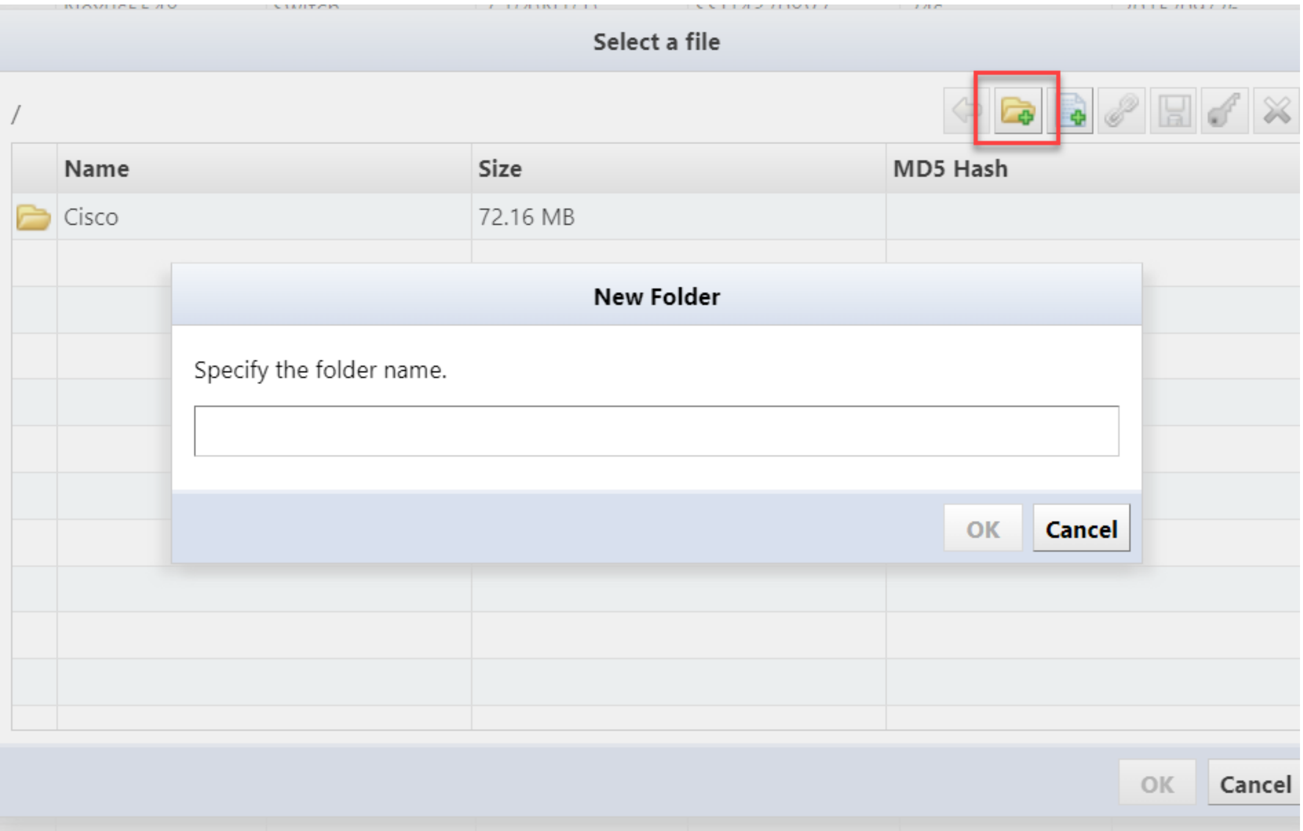


Select a file

/

Name	Size	MD5 Hash
Cisco	72.16 MB	

You can add a directory on the server's file system by clicking the 🗀 button.

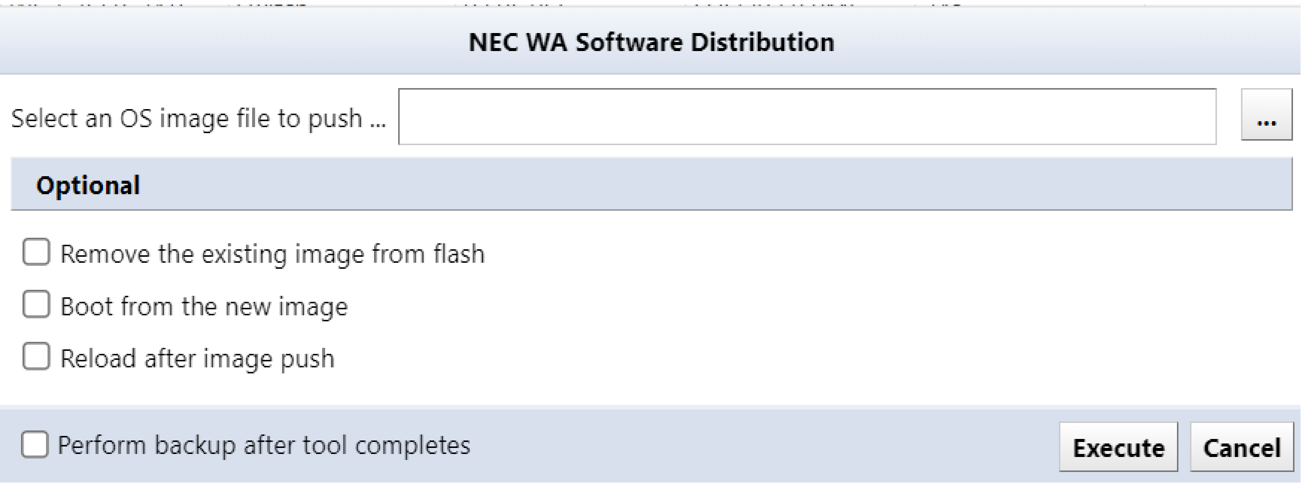


Once the OS image is added to the list, click the [OK] button.

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.

6.3.4.10.5 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.



NEC WA Software Distribution

Select an OS image file to push ...

Optional

□ Remove the existing image from flash

□ Boot from the new image

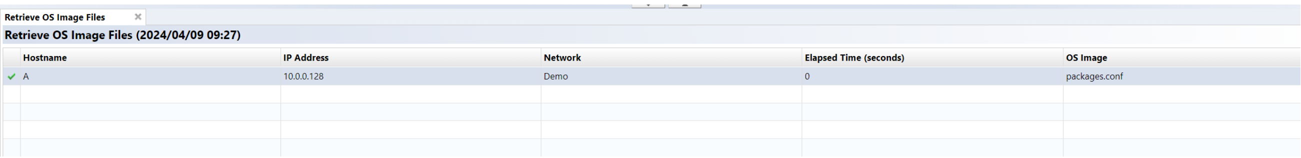
□ Reload after image push

□ Perform backup after tool completes

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

6.3.4.10.6 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.

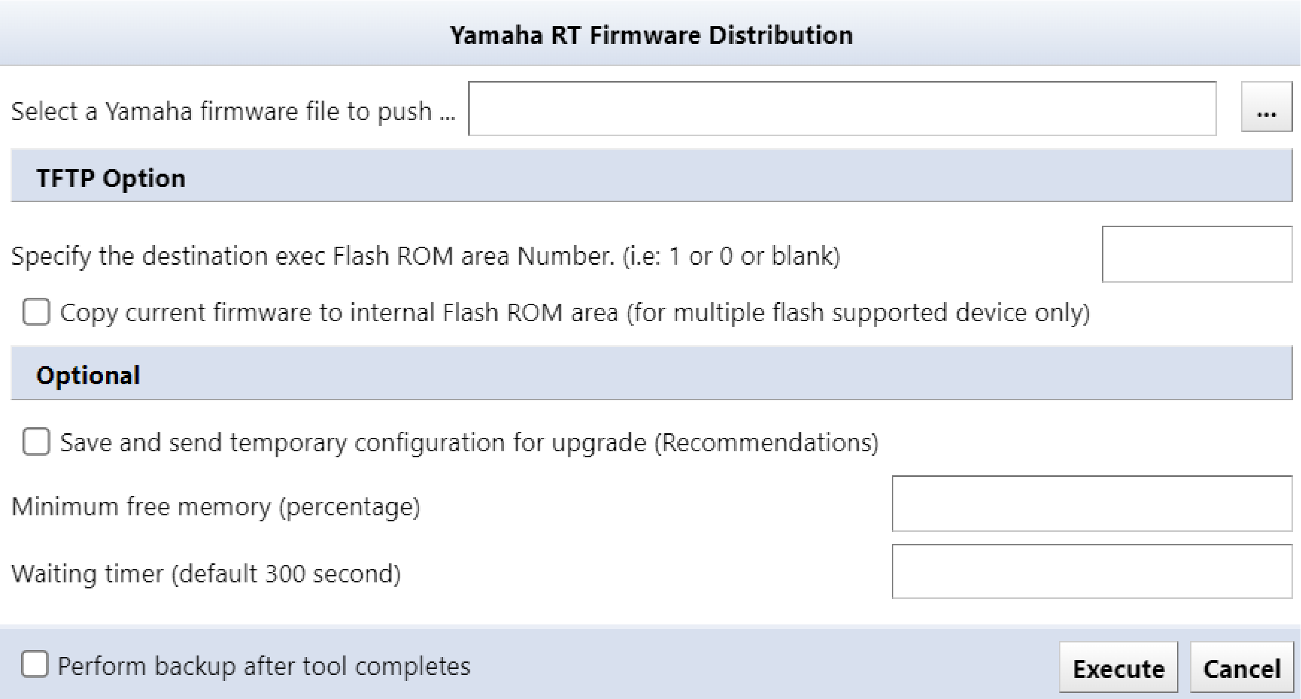


Retrieve OS Image Files (2024/04/09 09:27)

	Hostname	IP Address	Network	Elapsed Time (seconds)	OS Image
✓	A	10.0.0.128	Demo	0	packages.conf

6.3.4.10.7 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.



Yamaha RT Firmware Distribution

Select a Yamaha firmware file to push ... [ ] ...

TFTP Option

Specify the destination exec Flash ROM area Number. (i.e: 1 or 0 or blank) [ ]

□ Copy current firmware to internal Flash ROM area (for multiple flash supported device only)

Optional

□ Save and send temporary configuration for upgrade (Recommendations)

Minimum free memory (percentage) [ ]

Waiting timer (default 300 second) [ ]

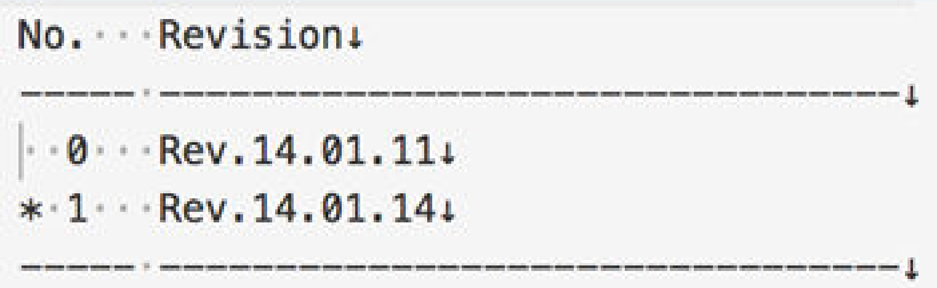
□ Perform backup after tool completes

Execute Cancel

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.



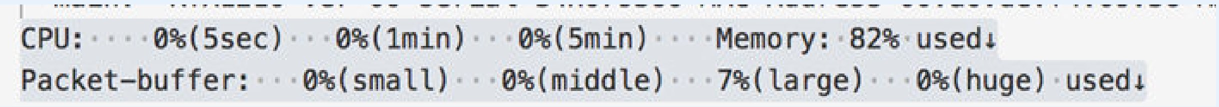
```
No.   Revision↓
----- -------------------------------↓
  0   Rev.14.01.11↓
* 1   Rev.14.01.14↓
----- -------------------------------↓
```

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.

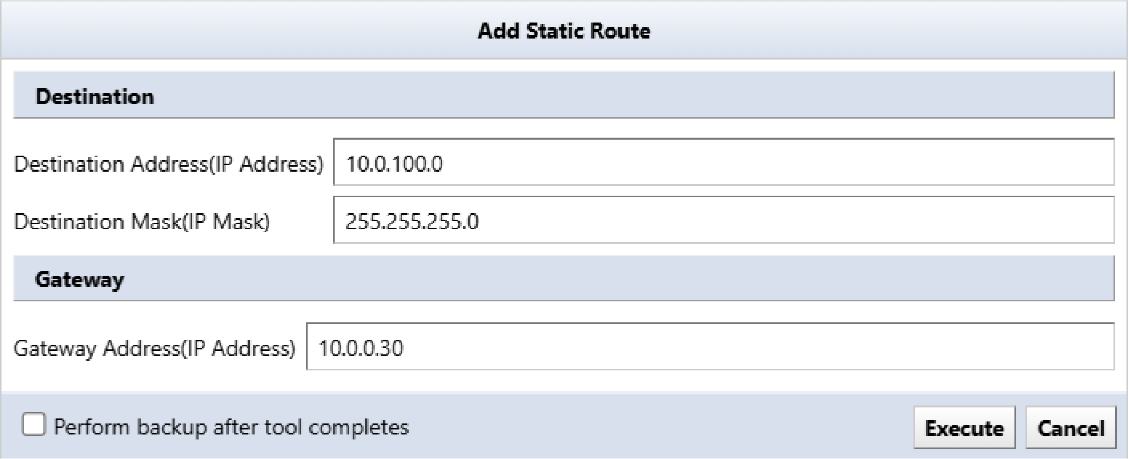


```
CPU:    0%(5sec)   0%(1min)   0%(5min)    Memory: 82% used↓
Packet-buffer:   0%(small)   0%(middle)   7%(large)   0%(huge) used↓
```

6.3.4.11 Static Routes

6.3.4.11.1 Add Static Route

Enter the required information, click **Execute** to add the route.



Add Static Route

Destination

Destination Address(IP Address)	10.0.100.0
Destination Mask(IP Mask)	255.255.255.0

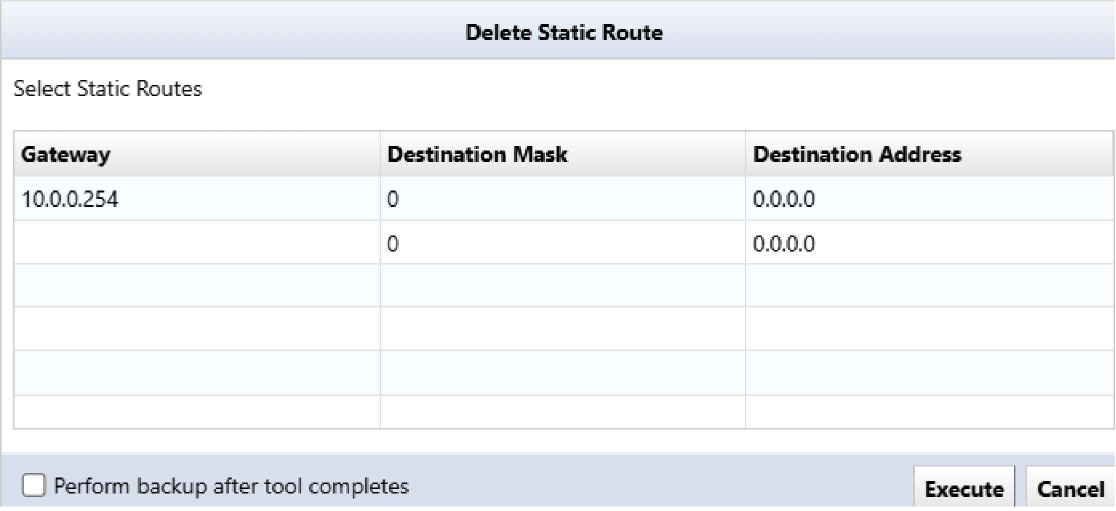
Gateway

Gateway Address(IP Address)	10.0.0.30

□ Perform backup after tool completes

6.3.4.11.2 Delete Static Route

Select and delete an existing static route configuration.



Select Static Routes

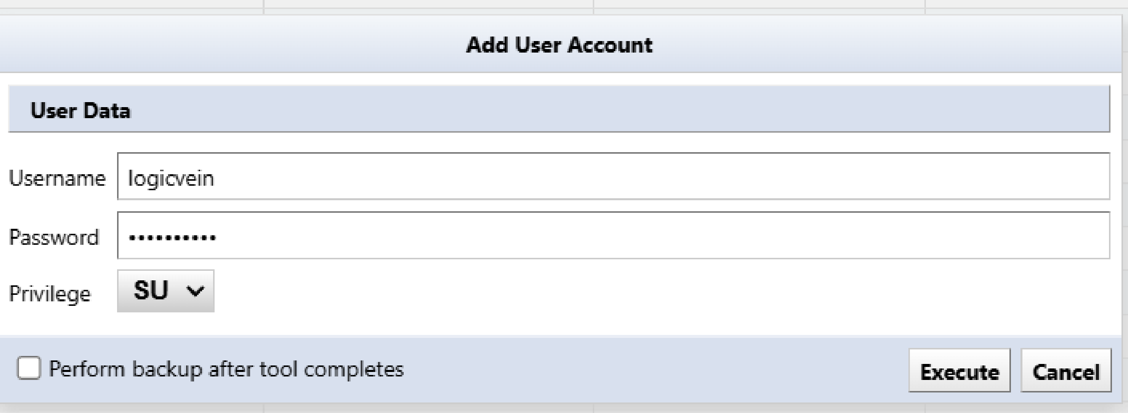
Gateway	Destination Mask	Destination Address
10.0.0.254	0	0.0.0.0
	0	0.0.0.0

□ Perform backup after tool completes

6.3.4.12 Users

6.3.4.12.1 Add User Account

Add a new user account to your device. Please note that this function cannot be executed when multiple devices are selected.



Add User Account

User Data

Username: logicvein

Password: ••••••••••

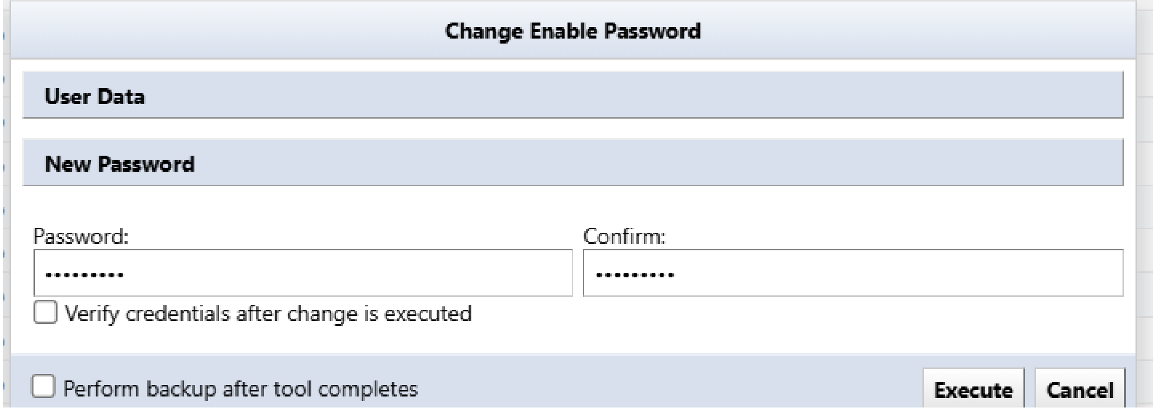
Privilege: SU

□ Perform backup after tool completes

6.3.4.12.2 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.



Change Enable Password

User Data

New Password

Password: •••••••••

Confirm: •••••••••

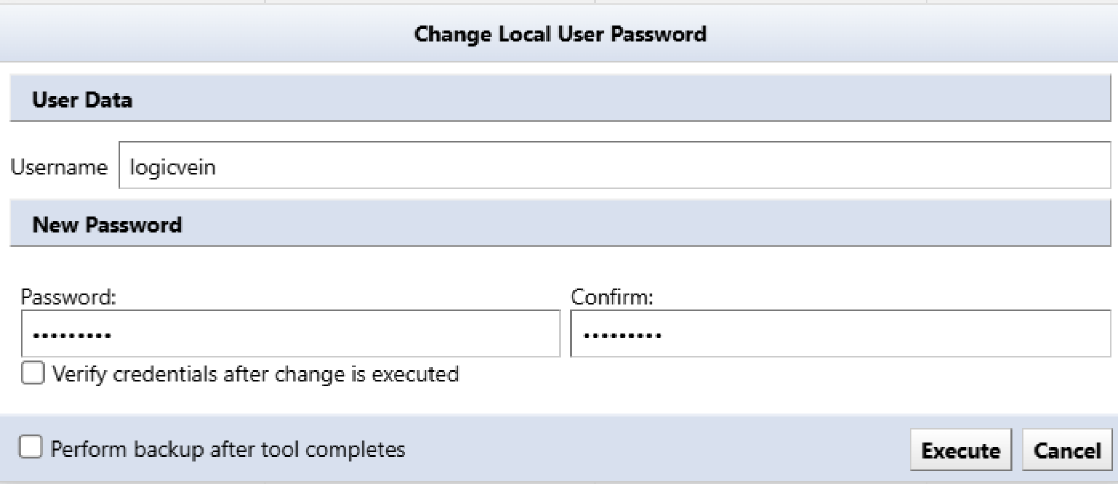
□ Verify credentials after change is executed

□ Perform backup after tool completes

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 the password you set.

6.3.4.12.3 Changing Local User Password

Change the password for the user account set on the device.



Change Local User Password

User Data

Username: logicvein

New Password

Password: •••••••••

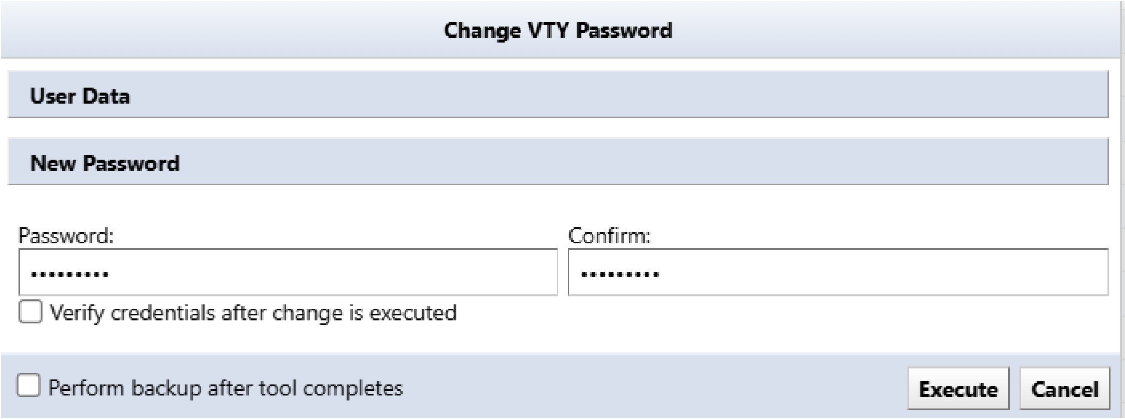
Confirm: •••••••••

☐ Verify credentials after change is executed

☐ Perform backup after tool completes

6.3.4.12.4 Change VTY Password

Change the device's VTY Password settings.



Password: ••••••••• Confirm: •••••••••

□ Verify credentials after change is executed

□ Perform backup after tool completes

Just as with changing Enable Password by checking "Confirm credentials after change", the credentials will be automatically changed.

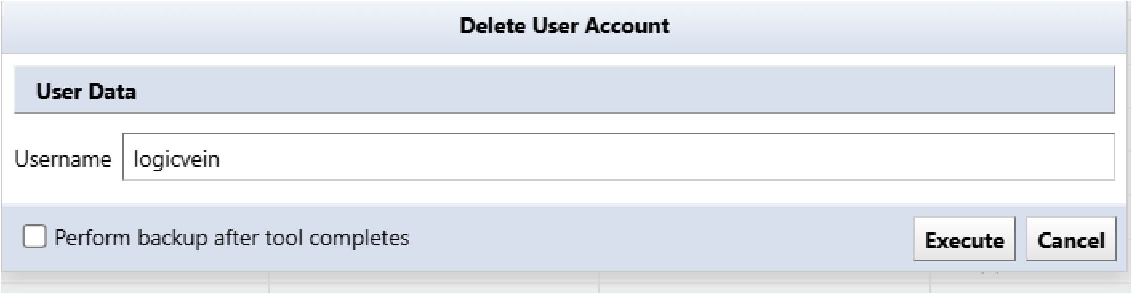
Test your new password after changing.

6.3.4.12.5 Delete User Account

Delete an existing user account configured on the device.

Note

This function cannot be executed when multiple devices are selected.



Delete User Account

User Data

Username: logicvein

☐ Perform backup after tool completes

6.3.5 Smart Change Menu Suite

The [Smart Change] Menu contains similar actions 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.

Smart Change jobs can be created from the [Jobs] main tab > [Job Management] tab.

For more information on Jobs, please refer to the **Jobs** section.

6.3.6 Reports Menu

The [Reports] Menu serves as a centralized hub for generating detailed summaries of network device data.

You can create customizable reports that include inventory details such as device models, serial numbers, firmware versions, hardware specifications, and operational statuses. Integration with dashboard widgets allows visual representation of metrics like device uptime or compliance rates, while job management configurations enable batch report generation across device groups.

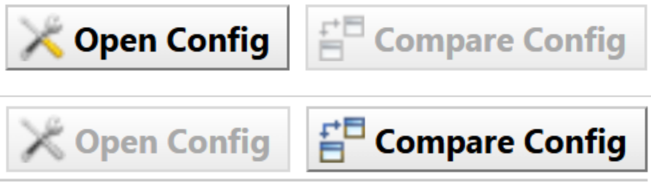
For more information on Reports, please refer to the **Reports** section.

6.4 Changes Tab

The [Changes] main tab offers an interface for tracking configuration modifications across network devices. It provides you with a centralized view of historical configurations, and enables easy comparison.

More details regarding Configuration Changes are available in the **Monitoring** section and throughout this manual.

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



6.5 Jobs Tab

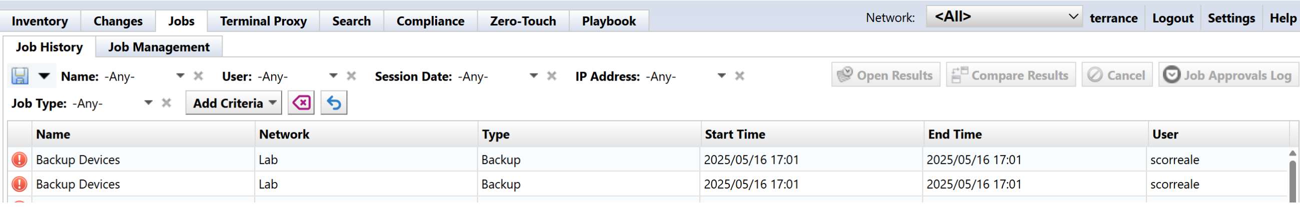
The [Jobs] main tab provides a centralized interface for managing automated network operations. It enables administrators to create, monitor, and audit recurring workflows. You can schedule jobs, set execution parameters, and review historical run logs. The tab features real-time status tracking with color-coded progress indicators and error reporting. You can also filter devices by groups, job types, and completion states.

More details regarding the [Jobs] main tab are available in the **Jobs** section and throughout this manual.

The [Jobs] main tab also contains two subtabs; the [Job History] tab, and the [Job Management] tab.

6.5.1 Job History Subtab

The [Job History] subtab provides a chronological record of all executed jobs. It displays key details like execution status (success/failure), timestamps, and visual indicators for quick status assessment.



Network: <All>

Name: -Any-
User: -Any-
Session Date: -Any-
IP Address: -Any-
Job Type: -Any-

	Name	Network	Type	Start Time	End Time	User
❗	Backup Devices	Lab	Backup	2025/05/16 17:01	2025/05/16 17:01	scorreale
❗	Backup Devices	Lab	Backup	2025/05/16 17:01	2025/05/16 17:01	scorreale

Button	Explanation
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.

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.

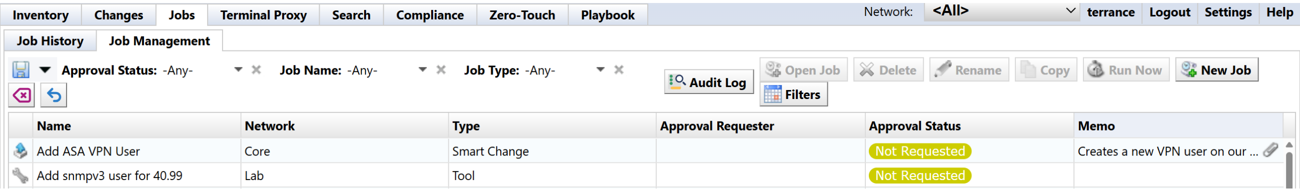
The status icons and their meanings are as follows:

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

6.5.2 Job Management Subtab

The [Job Management] subtab allows you to manage the full lifecycle of jobs. You can:

- Create new jobs
- Configure parameters
- Schedule executions (immediate/periodic)
- Clone/rename existing jobs
- Access audit logs



Network: <All>

Approval Status: -Any-   Job Name: -Any-   Job Type: -Any-

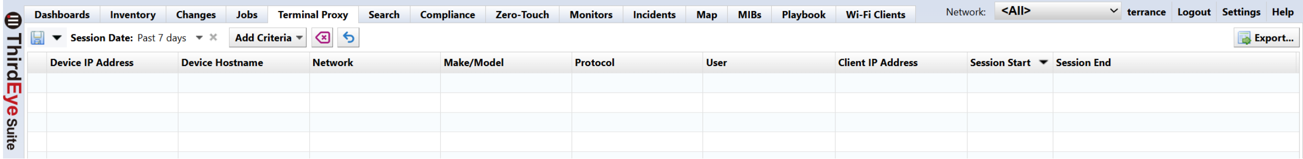
Name	Network	Type	Approval Requester	Approval Status	Memo
Add ASA VPN User	Core	Smart Change		Not Requested	Creates a new VPN user on our ...
Add snmpv3 user for 40.99	Lab	Tool		Not Requested	

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.

6.6 Terminal Proxy Tab

The [Terminal Proxy] main tab allows you to securely connect to network devices (SSH/Telnet). On the [Terminal Proxy] tab, 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)



Network: <All>

Session Date: Past 7 days

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

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.

More details regarding the [Terminal Proxy] main tab are available in the **Check Operation Log** and **Change Data Retention Period** sections of this manual.

6.7 Search Tab

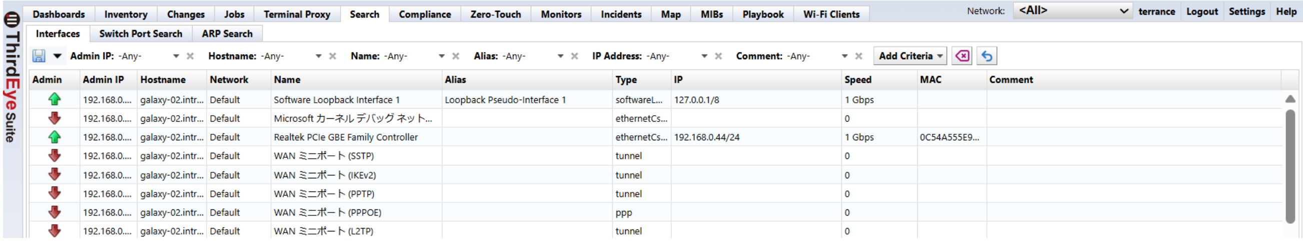
The [Search] main tab serves as a centralized investigation interface. In ThirdEye, it enables network-focused searches including switch port tracing, ARP record lookups, and interface configuration queries.

The [Search] main tab contains three subtabs:

- [Interfaces] subtab
- [Switch Port Search] subtab
- [ARP Search] subtab

6.7.1 Interfaces Subtab

The [Interfaces] subtab allows you to quickly locate device interfaces with status, VLAN associations, and configuration details across your network infrastructure.



Admin IP: -Any- Hostname: -Any- Name: -Any- Alias: -Any- IP Address: -Any- Comment: -Any-

Admin	Admin IP	Hostname	Network	Name	Alias	Type	IP	Speed	MAC	Comment
⬆	192.168.0....	galaxy-02.intr...	Default	Software Loopback Interface 1	Loopback Pseudo-Interface 1	softwareL...	127.0.0.1/8	1 Gbps		
⬇	192.168.0....	galaxy-02.intr...	Default	Microsoft カーネル デバッグ ネット...		ethernetCs...		0		
⬆	192.168.0....	galaxy-02.intr...	Default	Realtek PCIe GBE Family Controller		ethernetCs...	192.168.0.44/24	1 Gbps	0C54A555E9...	
⬇	192.168.0....	galaxy-02.intr...	Default	WAN ミニポート (SSTP)		tunnel		0		
⬇	192.168.0....	galaxy-02.intr...	Default	WAN ミニポート (IKEv2)		tunnel		0		
⬇	192.168.0....	galaxy-02.intr...	Default	WAN ミニポート (PPTP)		tunnel		0		
⬇	192.168.0....	galaxy-02.intr...	Default	WAN ミニポート (PPPOE)		ppp		0		
⬇	192.168.0....	galaxy-02.intr...	Default	WAN ミニポート (L2TP)		tunnel		0		

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

- Monitors
- Violations
- SNMP Traps
- Attachment
- Interfaces
- Memo

6.7.2 Switch Port Search Subtab

The [Switch Port Search] subtab pinpoints switch ports by MAC/IP addresses or hostnames to identify connected devices and trace network connections.

6.7.3 ARP Search Subtab

The [ARP Search] subtab resolves IP-MAC address mappings, and analyze ARP table relationships for troubleshooting connectivity issues. Results are based on ARP entries.

6.8 Compliance Tab

The [Compliance] main tab provides unified configuration control for features such as Policy Management, Rule Sets, Compliance Checks, and Violations.

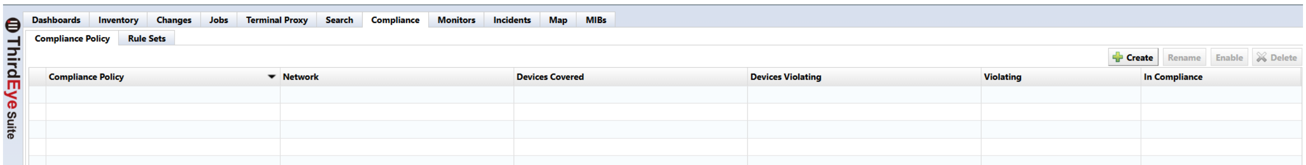
More details regarding the [Compliance] main tab are available in the **Compliance Policies** section and throughout this manual.

The [Compliance] main tab consists of the following subtabs:

- [Compliance Policy] subtab
- [Rule Sets] subtab

6.8.1 Compliance Policy Subtab

In the [Compliance Policy] subtab, you can view information about Compliance Policies, and select which devices the policy applies to.



Compliance Policy	Network	Devices Covered	Devices Violating	Violating	In Compliance

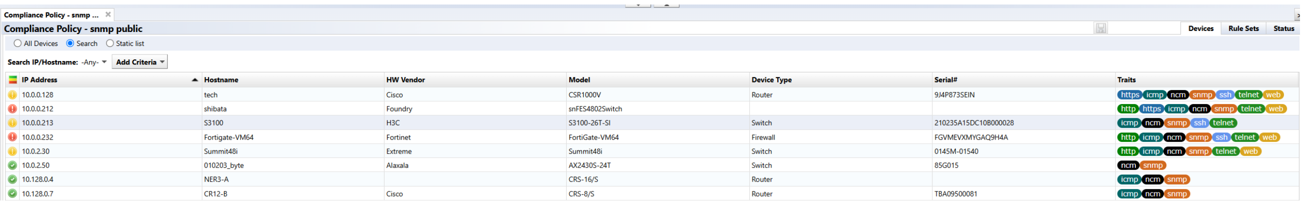
Doubleclicking a Compliance Policy opens the Editor at the bottom of the window. The Editor contains three tabs:

- [Devices]
- [Rulesets]
- [Status]

6.8.1.1 Devices

In the Editor's [Devices] tab, you can select devices using three criteria:

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



Compliance Policy - snmp public

○ All Devices ● Search ○ Static list

Search IP/Hostname: -Any- Add Criteria

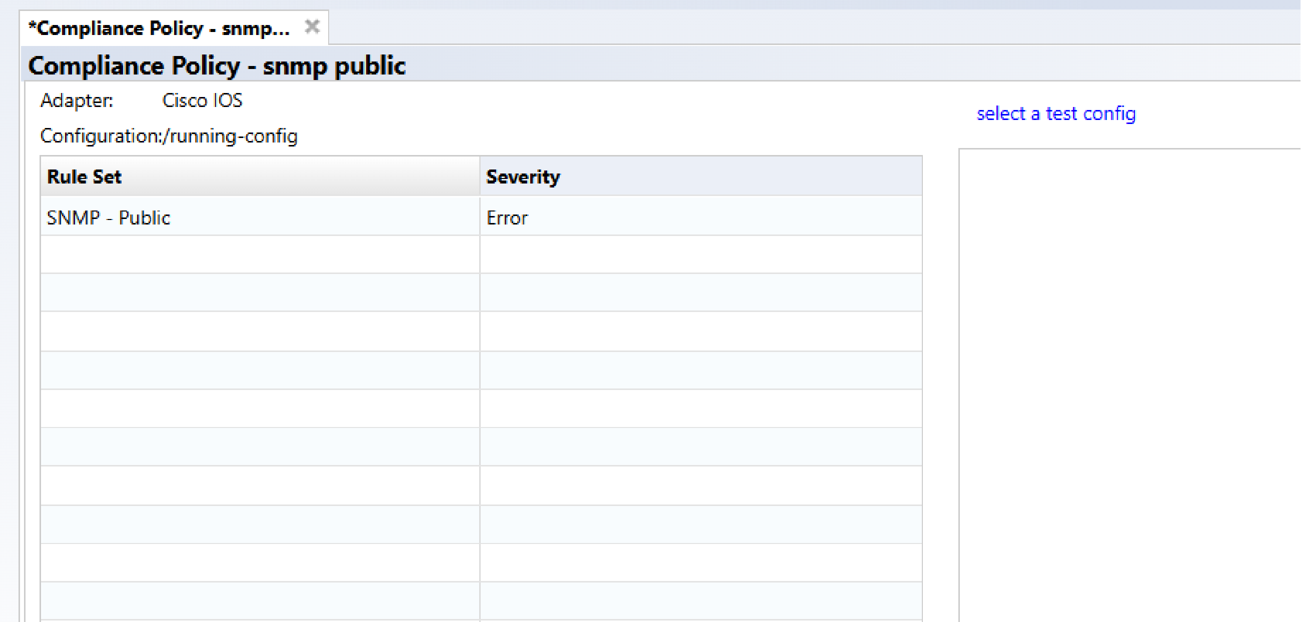
	IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
!	10.0.0.128	tech	Cisco	CSR1000V	Router	9J4P873SEIN	https icmp ncm snmp ssh telnet web
!	10.0.0.212	shibata	Foundry	snFES4802Switch			http https icmp ncm snmp telnet web
!	10.0.0.213	S3100	H3C	S3100-26T-SI	Switch	210235A15DC10B000028	icmp ncm snmp ssh telnet
!	10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGVMEVXMYGAQ9H4A	http icmp ncm snmp ssh telnet web
!	10.0.2.30	Summit48i	Extreme	Summit48i	Switch	0145M-01540	http icmp ncm snmp telnet web
✓	10.0.2.50	010203_byte	Alaxala	AX2430S-24T	Switch	85G015	ncm snmp
✓	10.128.0.4	NER3-A		CRS-16/S	Router		icmp ncm snmp
✓	10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	TBA09500081	icmp ncm snmp

Item	Explanation
All devices	Apply policies to all devices.

Item	Explanation
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.

6.8.1.2 Rulesets

In the Editor’s [Rulesets] tab, you can manage compliance rule collections. It provides information about the Compliance Policy’s Ruleset, Adapter, Configuration, and failure Severity level.



Compliance Policy - snmp public

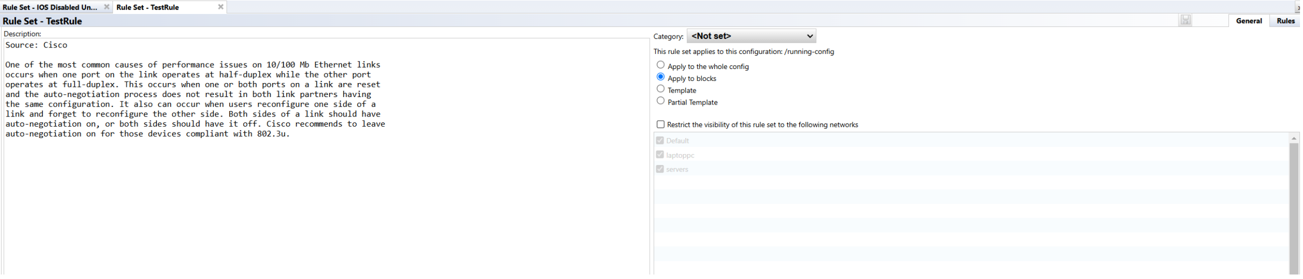
Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity
SNMP - Public	Error

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.

You can register the created Rule Set to the policy.



Rule Set - TestRule

Description:

```
Source: Cisco

One of the most common causes of performance issues on 10/100 Mb Ethernet links
occurs when one port on the link operates at half-duplex while the other port
operates at full-duplex. This occurs when one or both ports on a link are reset
and the auto-negotiation process does not result in both link partners having
the same configuration. It also can occur when users reconfigure one side of a
link and forget to reconfigure the other side. Both sides of a link should have
auto-negotiation on, or both sides should have it off. Cisco recommends to leave
auto-negotiation on for those devices compliant with 802.3u.
```

Category: <Not set>

This rule set applies to this configuration: /running-config

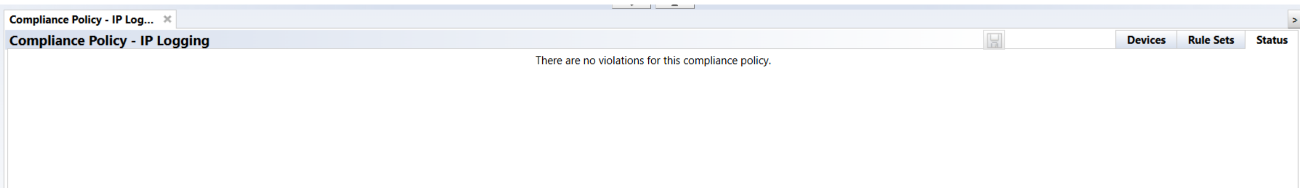
○ Apply to the whole config
● Apply to blocks
○ Template
○ Partial Template

□ Restrict the visibility of this rule set to the following networks

☑ Default
☑ laptoppc
☑ servers

6.8.1.3 Status

In the Editor’s [Status] tab, you can view violations for a selected compliance policy.

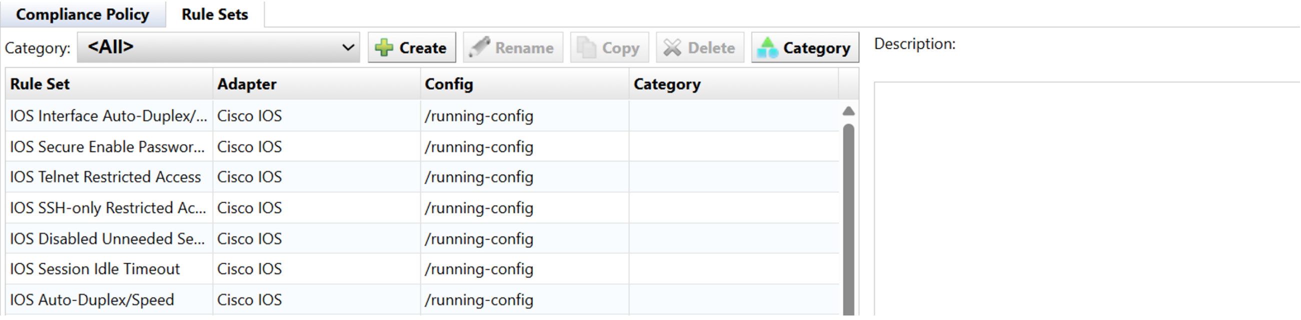


There are no violations for this compliance policy.

6.8.2 Rule Sets Subtab

Doubleclicking a Rule Set in the [Rule Sets] subtab opens the Editor at the bottom of the window. The Editor contains two tabs:

- [General] information
- [Rules] information

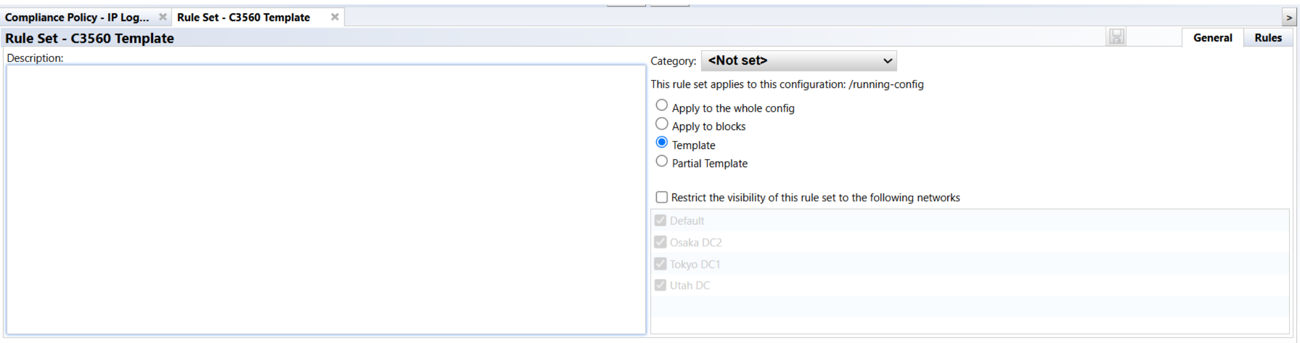


Category: <All>

Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/...	Cisco IOS	/running-config	
IOS Secure Enable Passwor...	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Ac...	Cisco IOS	/running-config	
IOS Disabled Unneeded Se...	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	

6.8.2.1 Editor General Tab

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



Rule Set - C3560 Template

Category: <Not set>

This rule set applies to this configuration: /running-config

○ Apply to the whole config
○ Apply to blocks
● Template
○ Partial Template

□ Restrict the visibility of this rule set to the following networks

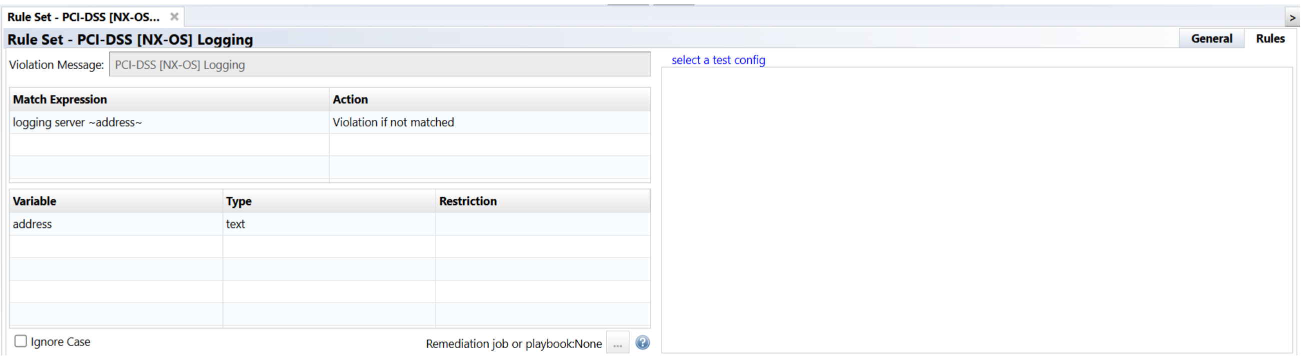
☑ Default
☑ Osaka DC2
☑ Tokyo DC1
☑ Utah DC

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 block.
Template	The configuration is compared line by line from the template, and if there is a difference, it will be a violation.

General Items	Explanation
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.

6.8.2.2 Editor Rules Tab

In the Editor's [Rules] tab, you can configure the rule itself:


Rule Set - PCI-DSS [NX-OS...
Rule Set - PCI-DSS [NX-OS] Logging
General
Rules
select a test config

Violation Message: PCI-DSS [NX-OS] Logging

Match Expression	Action
logging server ~address~	Violation if not matched

Variable	Type	Restriction
address	text	

☐ Ignore Case

Remediation job or playbook:None

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 Editor's [General] tab.
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.

6.9 Zero-Touch Tab (optional) Suite

The [Zero-Touch] main 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.

More details regarding the [Zero-Touch] main tab are available in the **Zero-Touch** section and throughout this manual.

6.10 Monitors Tab

The [Monitors] main 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.

More details regarding the [Monitors] main tab are available in the **Configuration Backup** and **Monitoring** sections, and throughout this manual.

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

6.11 Incidents Tab

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.

More details regarding the [Incidents] main tab are available in the **Maps** section and throughout this manual.

6.12 Map Tab

The [Map] main 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.

More details regarding the [Map] main tab are available in the **Maps** section of this manual.

6.13 MIBs Tab

The [MIBs] (Management Information Base files) main 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.

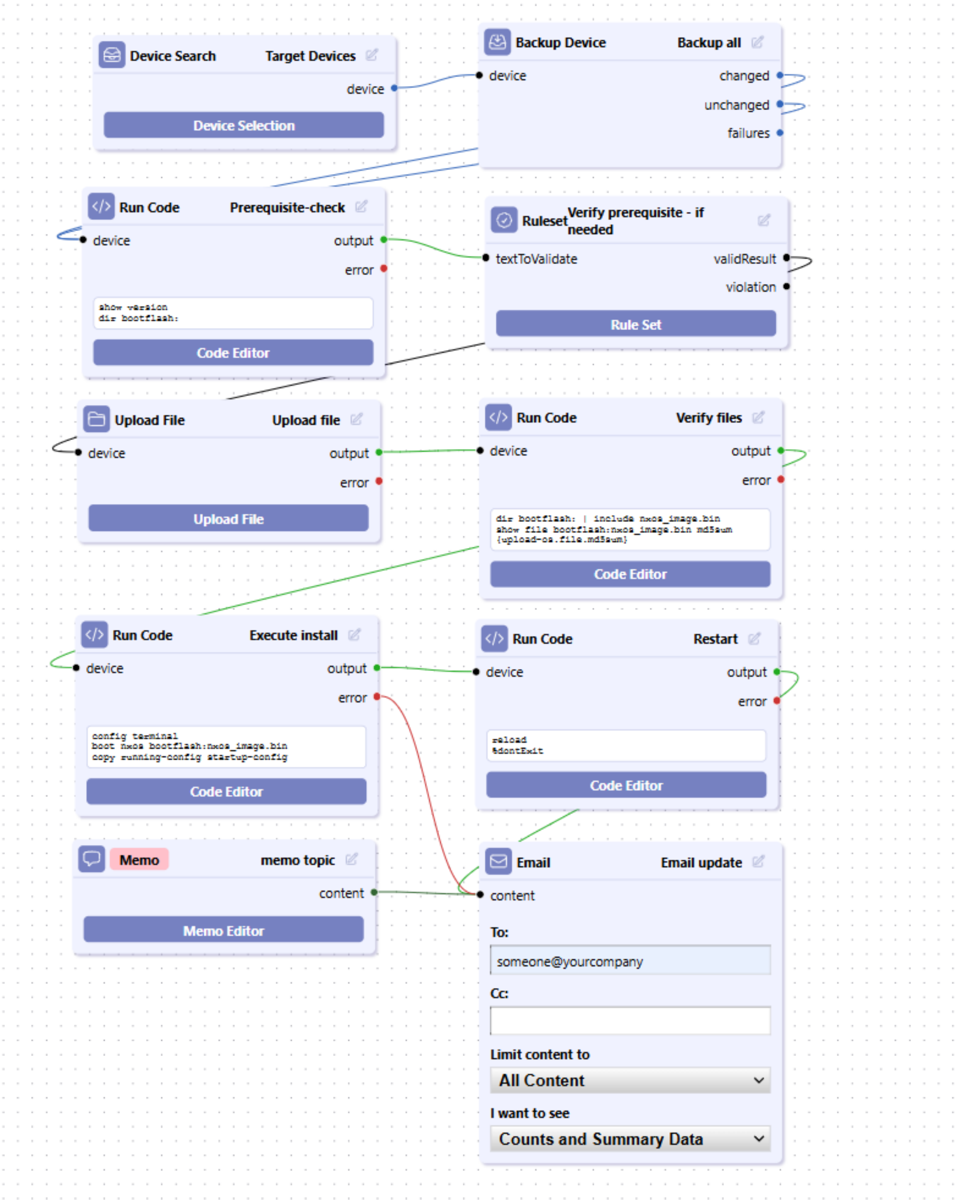
More details regarding MIBs are available in the **Monitoring** section and throughout this manual.

6.14 Playbooks Tab

The [Playbook] main tab is a workflow automation interface designed to simplify and automate network management tasks using your custom scripts. Playbook features include:

- **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:



```
show version
dir bootflash:
```

```
dir bootflash: | include nxos_image.bin
show file bootflash:nxos_image.bin md5sum
{upload-os.file.md5sum}
```

```
config terminal
boot nxos bootflash:nxos_image.bin
copy running-config startup-config
```

```
reload
&dontExit
```

To: someone@yourcompany

Cc:

Limit content to: All Content

I want to see: Counts and Summary Data

6.15 Wi-Fi Clients Tab

The [Wi-Fi Clients] main 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.

SECTION 7

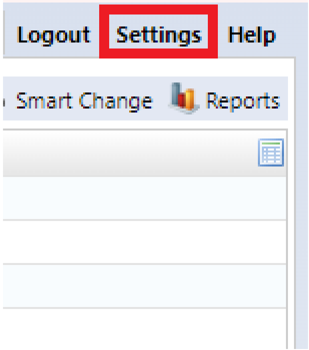
USER MANAGEMENT

7.1 Create User Account

Create a user to log in to ThirdEye.

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

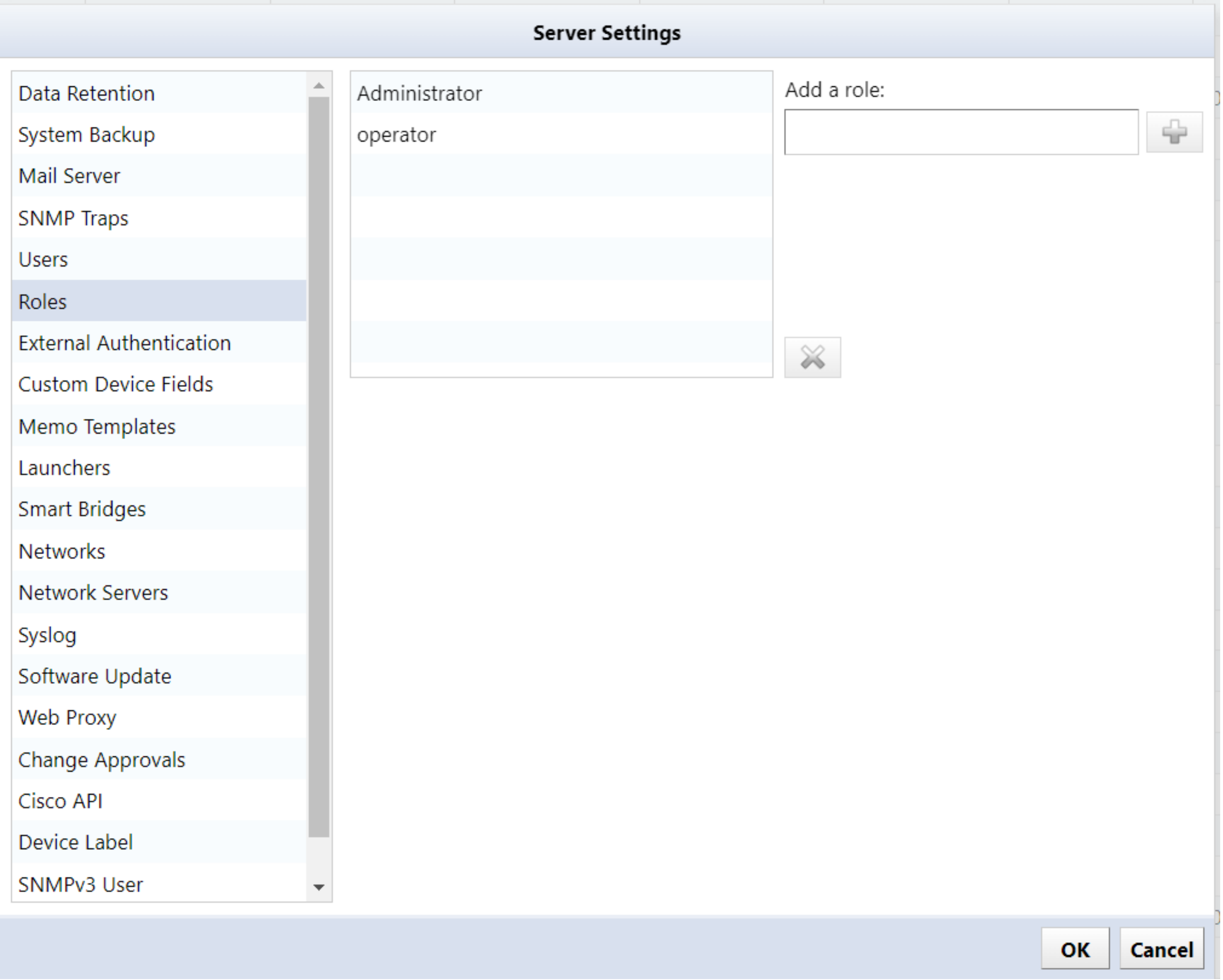
User and permission settings can be configured from [Settings] in the Global Menu.



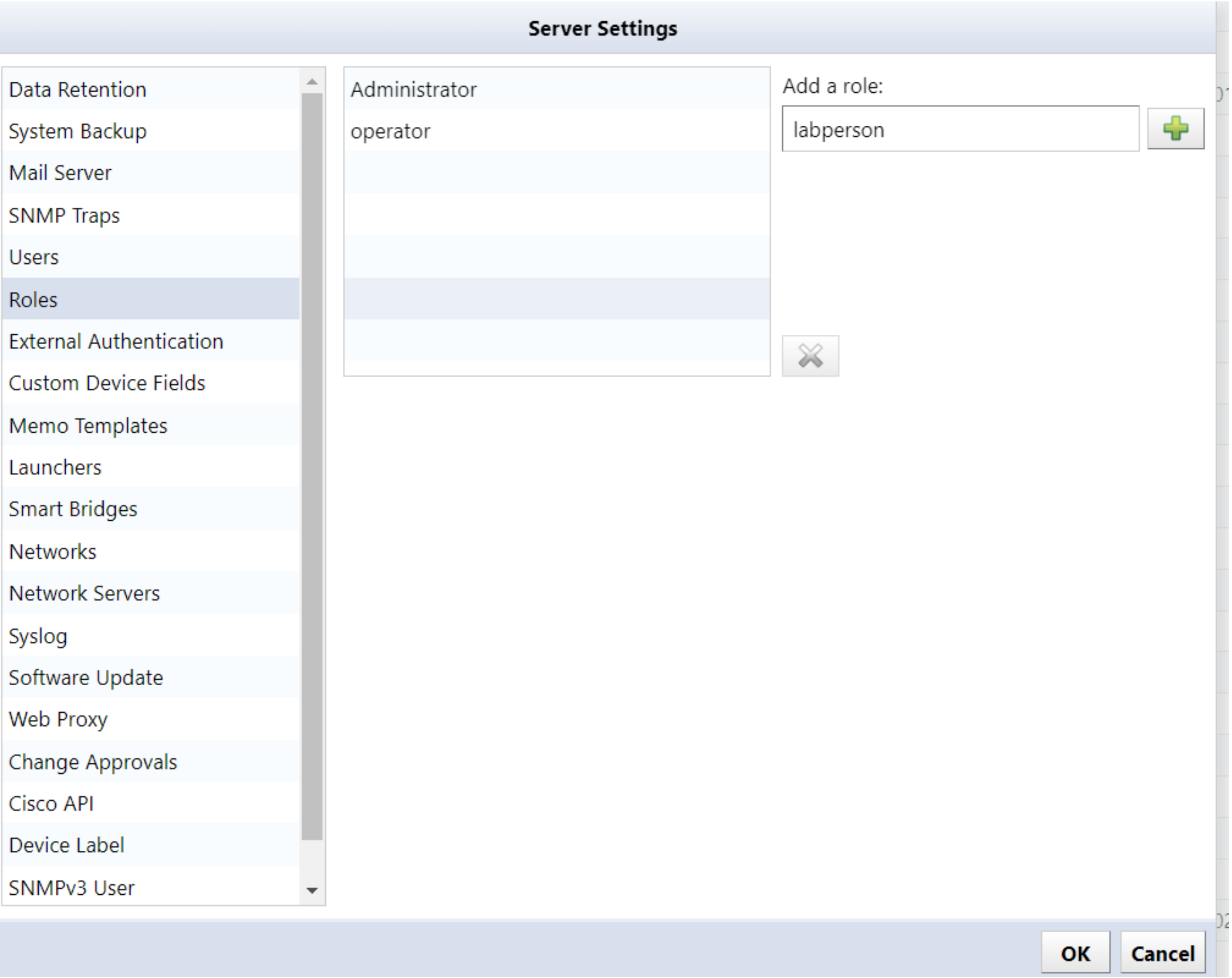
7.2 Add Permissions

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

1. Click [Roles] in the left sidebar.



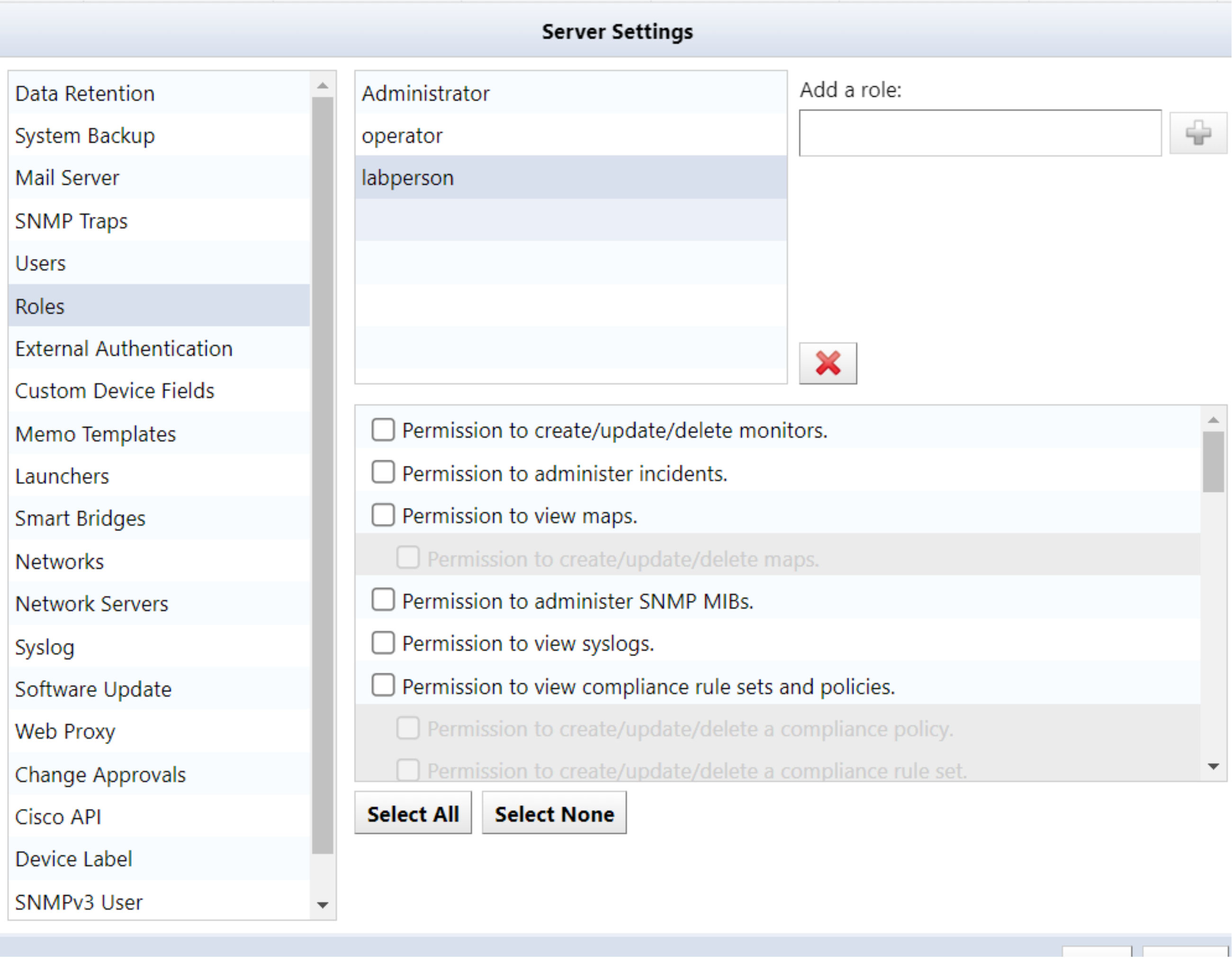
2. Enter the permission name in the [Add a Role] field and click the + button.



Administrator
operator

Add a role: labperson

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.



Server Settings

Data Retention
System Backup
Mail Server
SNMP Traps
Users
Roles
External Authentication
Custom Device Fields
Memo Templates
Launchers
Smart Bridges
Networks
Network Servers
Syslog
Software Update
Web Proxy
Change Approvals
Cisco API
Device Label
SNMPv3 User

Administrator
operator
labperson

Add a role:

□ Permission to create/update/delete monitors.
□ Permission to administer incidents.
□ Permission to view maps.
□ Permission to create/update/delete maps.
□ Permission to administer SNMP MIBs.
□ Permission to view syslogs.
□ Permission to view compliance rule sets and policies.
□ Permission to create/update/delete a compliance policy.
□ Permission to create/update/delete a compliance rule set.

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.”)

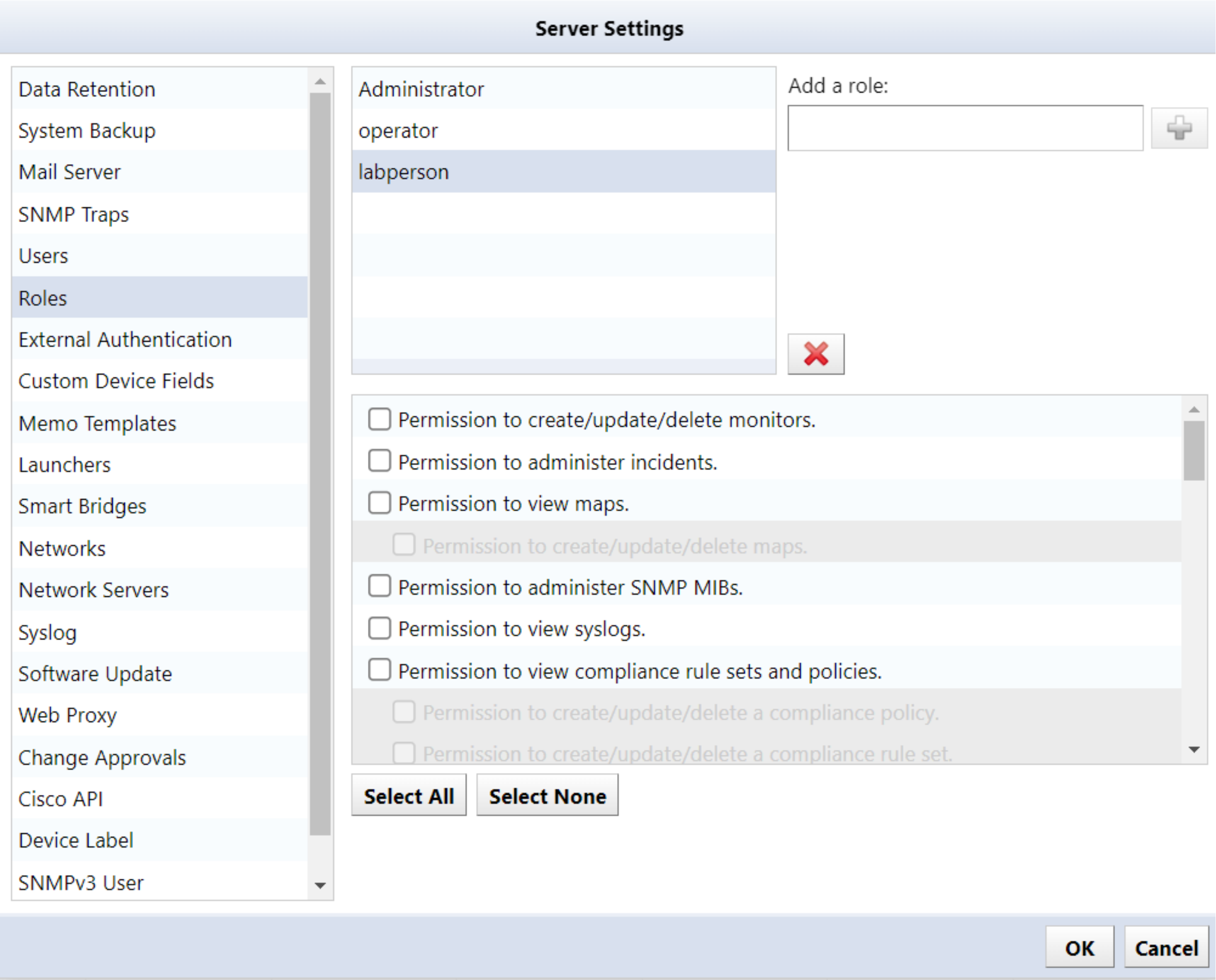
Permission Item	Edition	Explanation
Permission to administer SNMP MIBs		You can add/delete MIBs.
Permission to view syslogs		You can view Syslogs sent from devices.
Permission to view compliance Rule Sets and policies	Suite	You can view the [Compliance] tab.
Permission to create/update/delete a compliance 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 Item	Edition	Explanation
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 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 Item	Edition	Explanation
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 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 Item	Edition	Explanation
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].



Administrator
operator
labperson

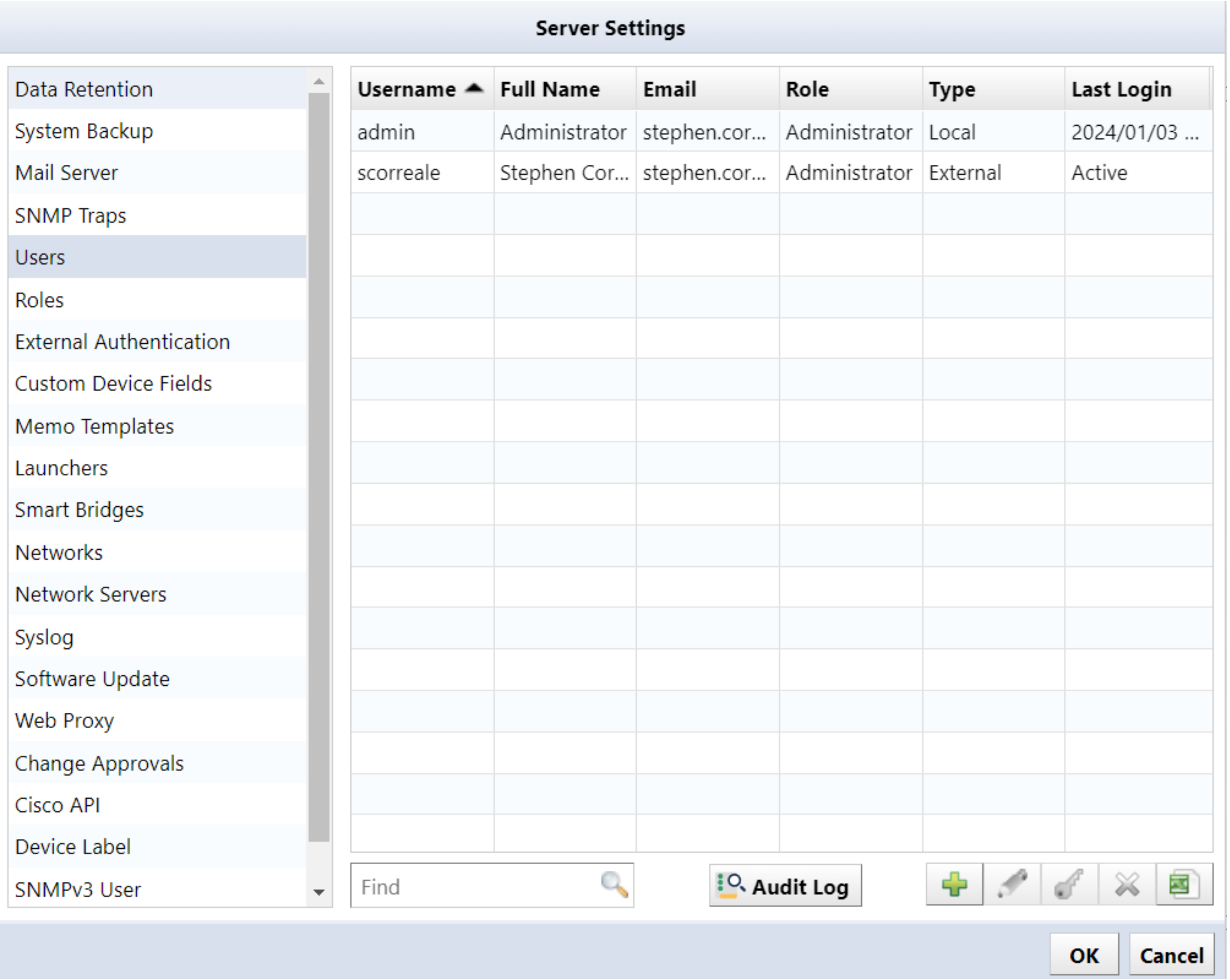
Add a role:

- □ Permission to create/update/delete monitors.
- □ Permission to administer incidents.
- □ Permission to view maps.
  - □ Permission to create/update/delete maps.
- □ Permission to administer SNMP MIBs.
- □ Permission to view syslogs.
- □ Permission to view compliance rule sets and policies.
  - □ Permission to create/update/delete a compliance policy.
  - □ Permission to create/update/delete a compliance rule set.

7.3 Add User

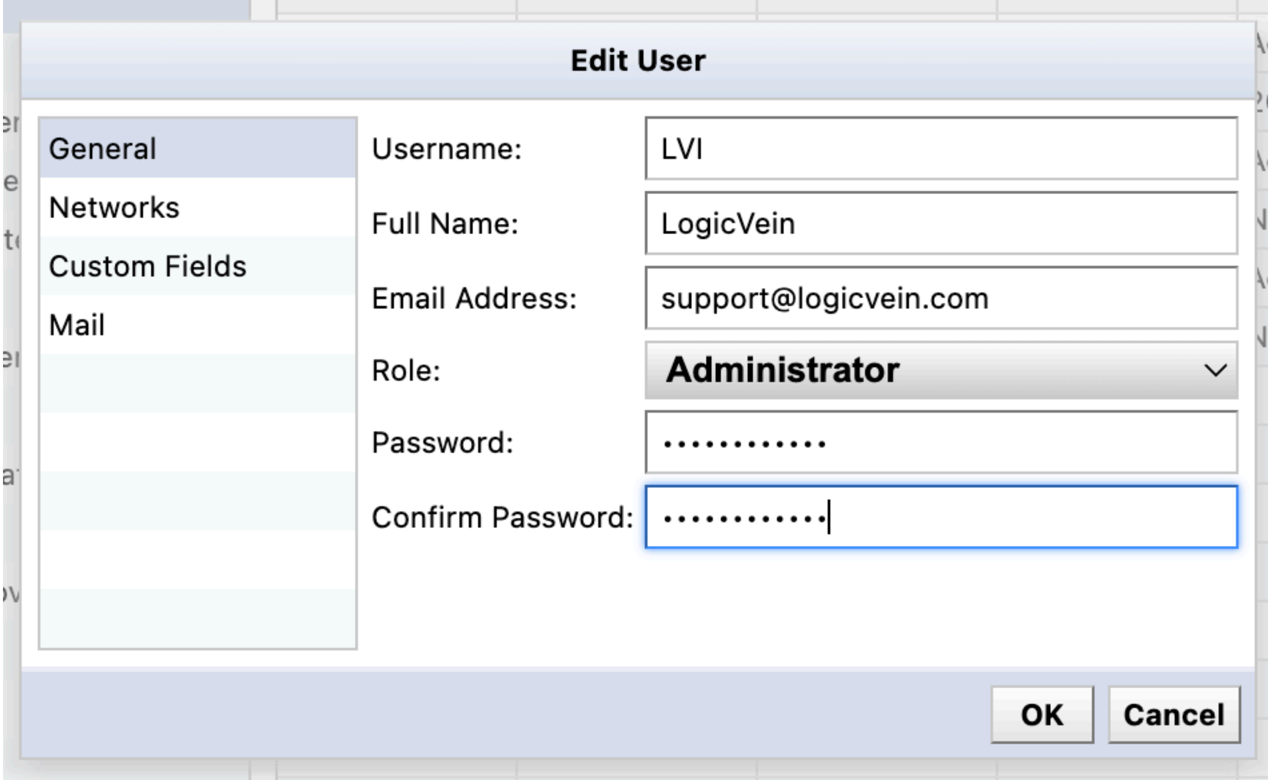
The `admin` user is pre-registered, and cannot be deleted.

1. Click the + button.



Username ▲	Full Name	Email	Role	Type	Last Login
admin	Administrator	stephen.cor...	Administrator	Local	2024/01/03 ...
scorreale	Stephen Cor...	stephen.cor...	Administrator	External	Active

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



Username: LVI

Full Name: LogicVein

Email Address: support@logicvein.com

Role: Administrator

Password: ••••••••••••

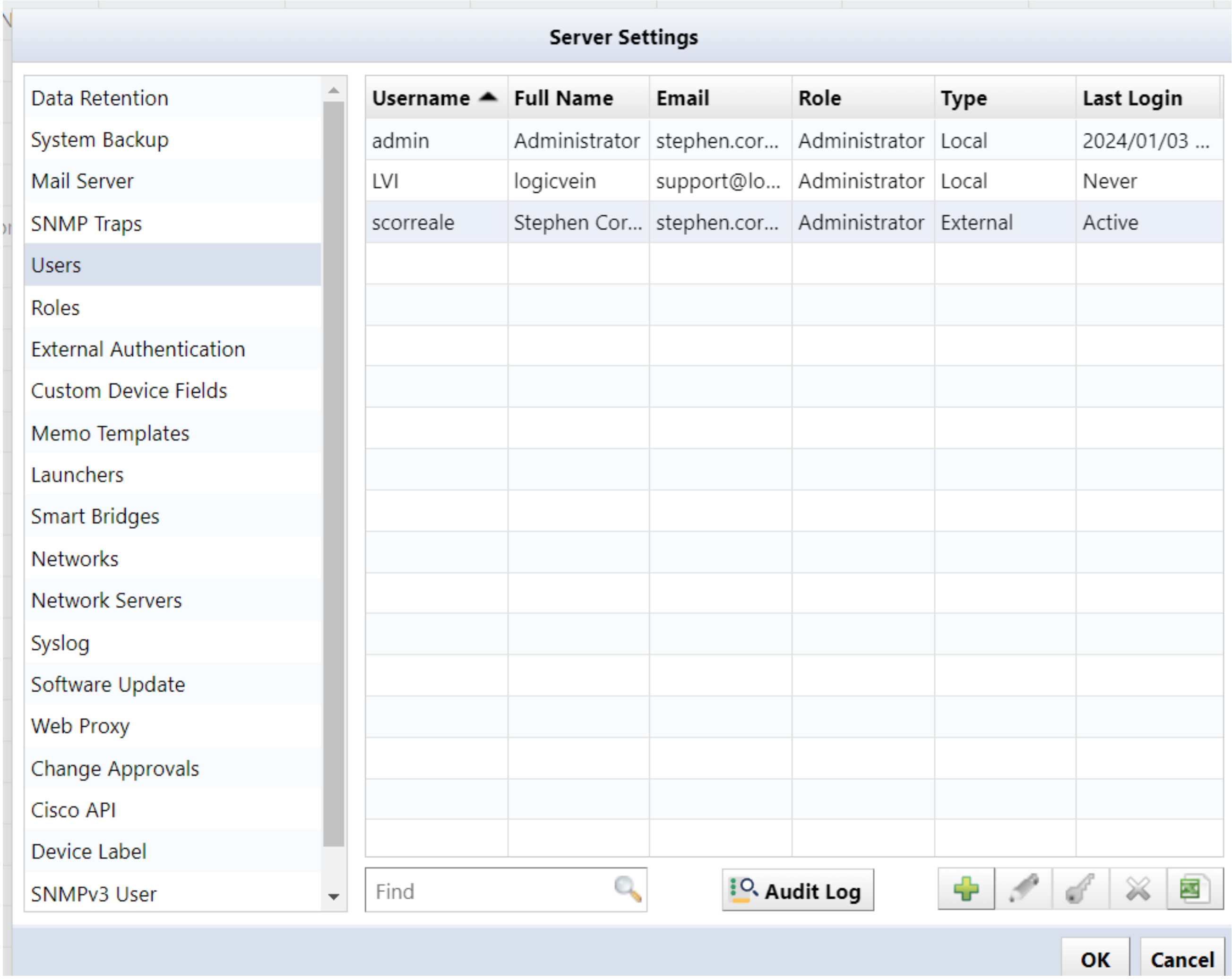
Confirm Password: ••••••••••••

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.	required

Item	Subitem	Explanation	Requirement
General		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	
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.	—

Item	Subitem	Explanation	Requirement
General		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 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].



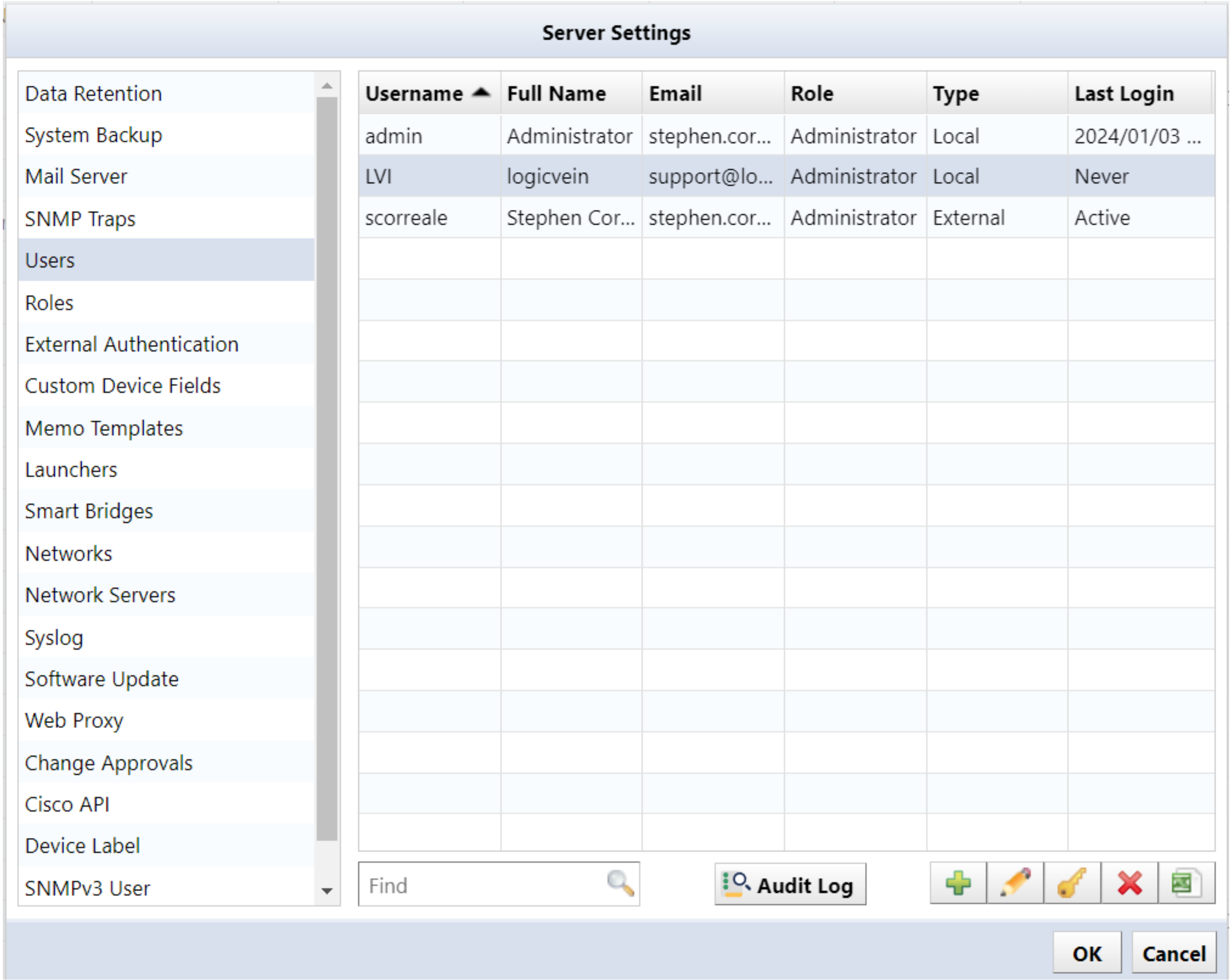
Server Settings

- Data Retention
- System Backup
- Mail Server
- SNMP Traps
- Users
- Roles
- External Authentication
- Custom Device Fields
- Memo Templates
- Launchers
- Smart Bridges
- Networks
- Network Servers
- Syslog
- Software Update
- Web Proxy
- Change Approvals
- Cisco API
- Device Label
- SNMPv3 User

Username ▲	Full Name	Email	Role	Type	Last Login
admin	Administrator	stephen.cor...	Administrator	Local	2024/01/03 ...
LVI	logicvein	support@lo...	Administrator	Local	Never
scorreale	Stephen Cor...	stephen.cor...	Administrator	External	Active

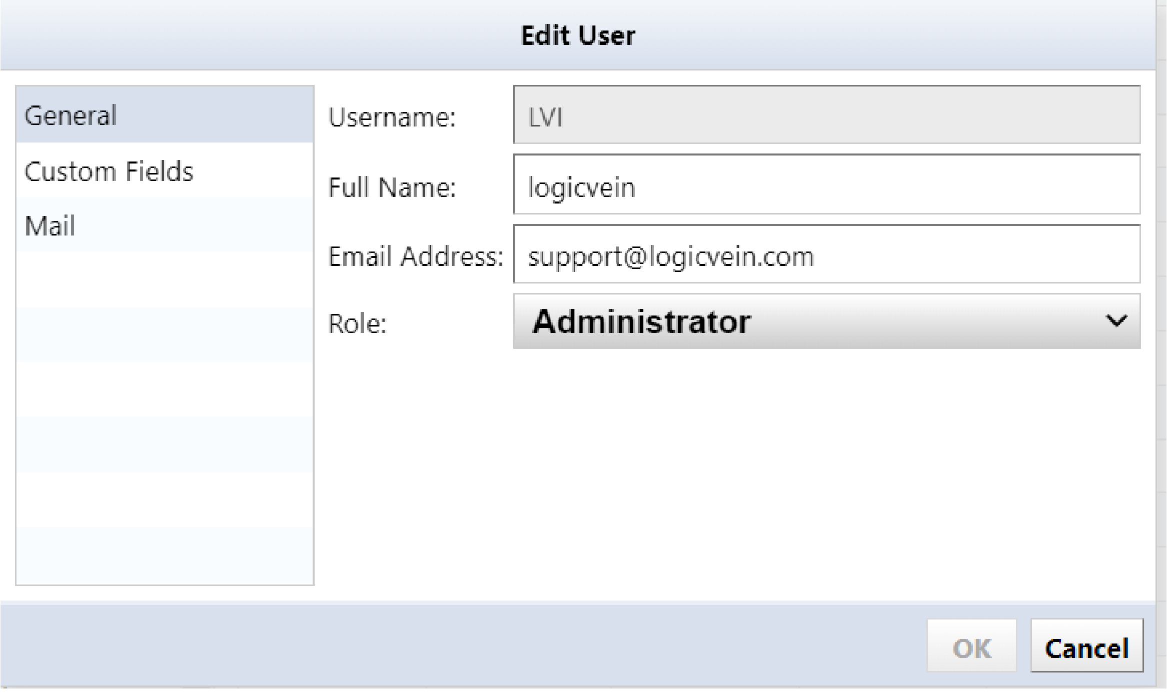
7.4 Change User Information

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



Username ▲	Full Name	Email	Role	Type	Last Login
admin	Administrator	stephen.cor...	Administrator	Local	2024/01/03 ...
LVI	logicvein	support@lo...	Administrator	Local	Never
scorreale	Stephen Cor...	stephen.cor...	Administrator	External	Active

2. . After editing, click [OK]. The Username cannot be changed. If you want to change your password, refer to the **Change Password** section below.



Edit User

Username: LVI

Full Name: logicvein

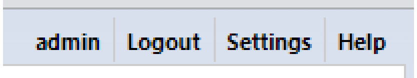
Email Address: support@logicvein.com

Role: Administrator

7.5 Change Password

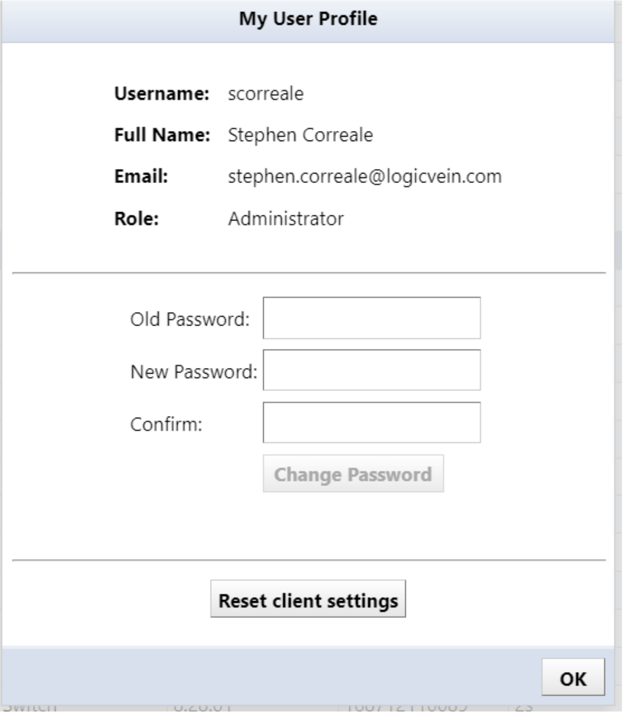
You can change your password from the login username in the Global Menu.

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.


My User Profile

Username: scorreale

Full Name: Stephen Correale

Email: stephen.correale@logicvein.com

Role: Administrator

Old Password:

New Password:

Confirm:

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

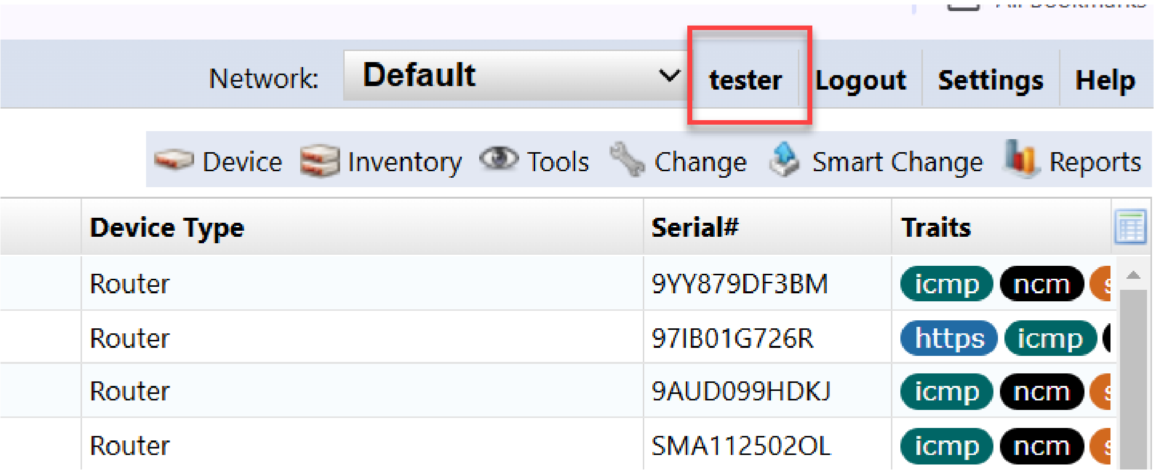
7.6 Setup Two-Factor Authentication (2FA)

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

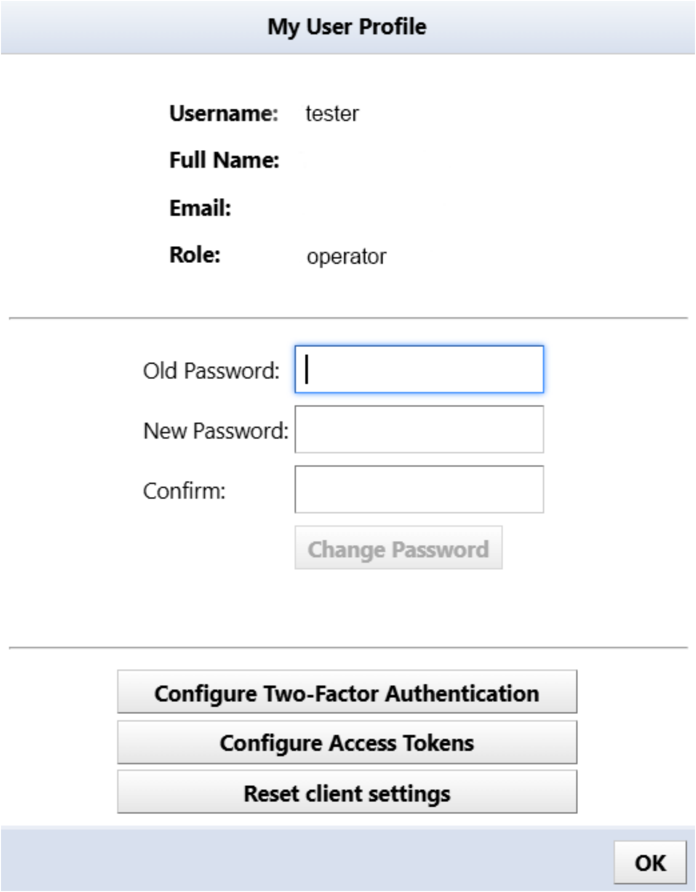
If the user is logged in, you can setup two-factor authentication from the user profile dialog

1. Click the username ("tester" in the example below) in the Global Menu to open the My User Profile window.



Device Type	Serial#	Traits
Router	9YY879DF3BM	icmp ncm
Router	97IB01G726R	https icmp
Router	9AUD099HDKJ	icmp ncm
Router	SMA112502OL	icmp ncm

2. Click [Set up two-factor authentication]



Username: tester

Full Name:

Email:

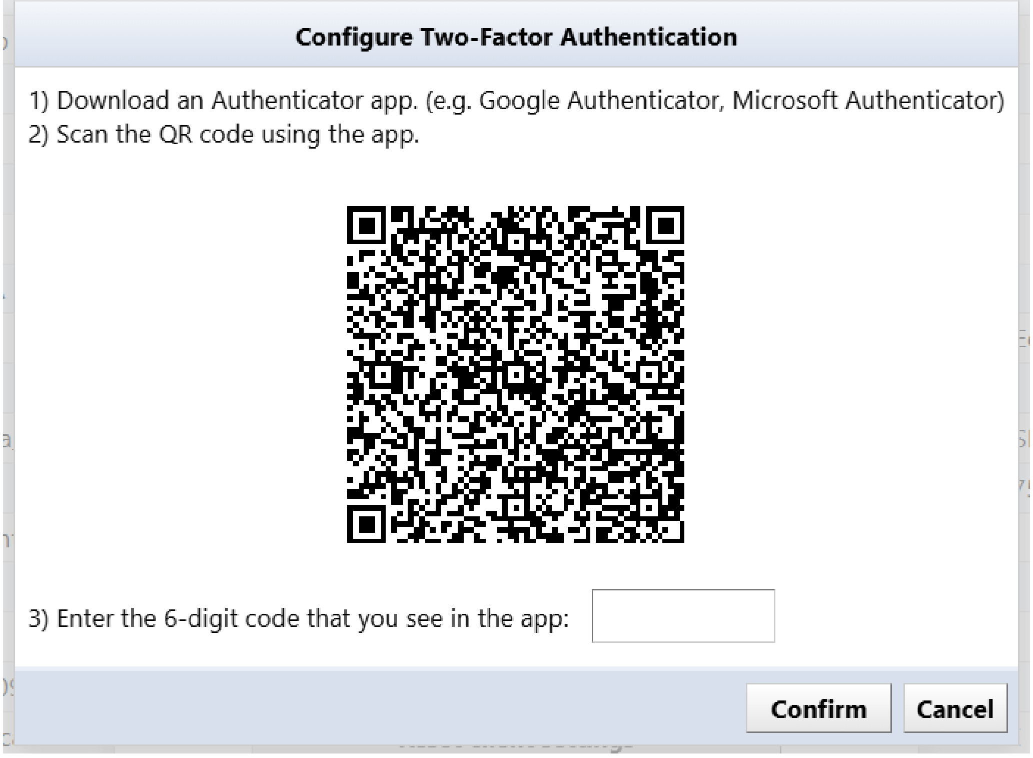
Role: operator

Old Password:

New Password:

Confirm:

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



Configure Two-Factor Authentication

1) Download an Authenticator app. (e.g. Google Authenticator, Microsoft Authenticator)
2) Scan the QR code using the app.

3) Enter the 6-digit code that you see in the app:

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. Click [Settings] > [Users]
2. Select the target user and click the 🔑 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 ThirdEye, you can use an authentication server to log in to the product. This eliminates the need to create all user accounts in ThirdEye 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 ThirdEye 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, ThirdEye sends an Access-Request for authentication. To configure this integration, set up ThirdEye to send Access-Accept with Filter-Id attached.

Below is a sample user configuration for FreeRADIUS:

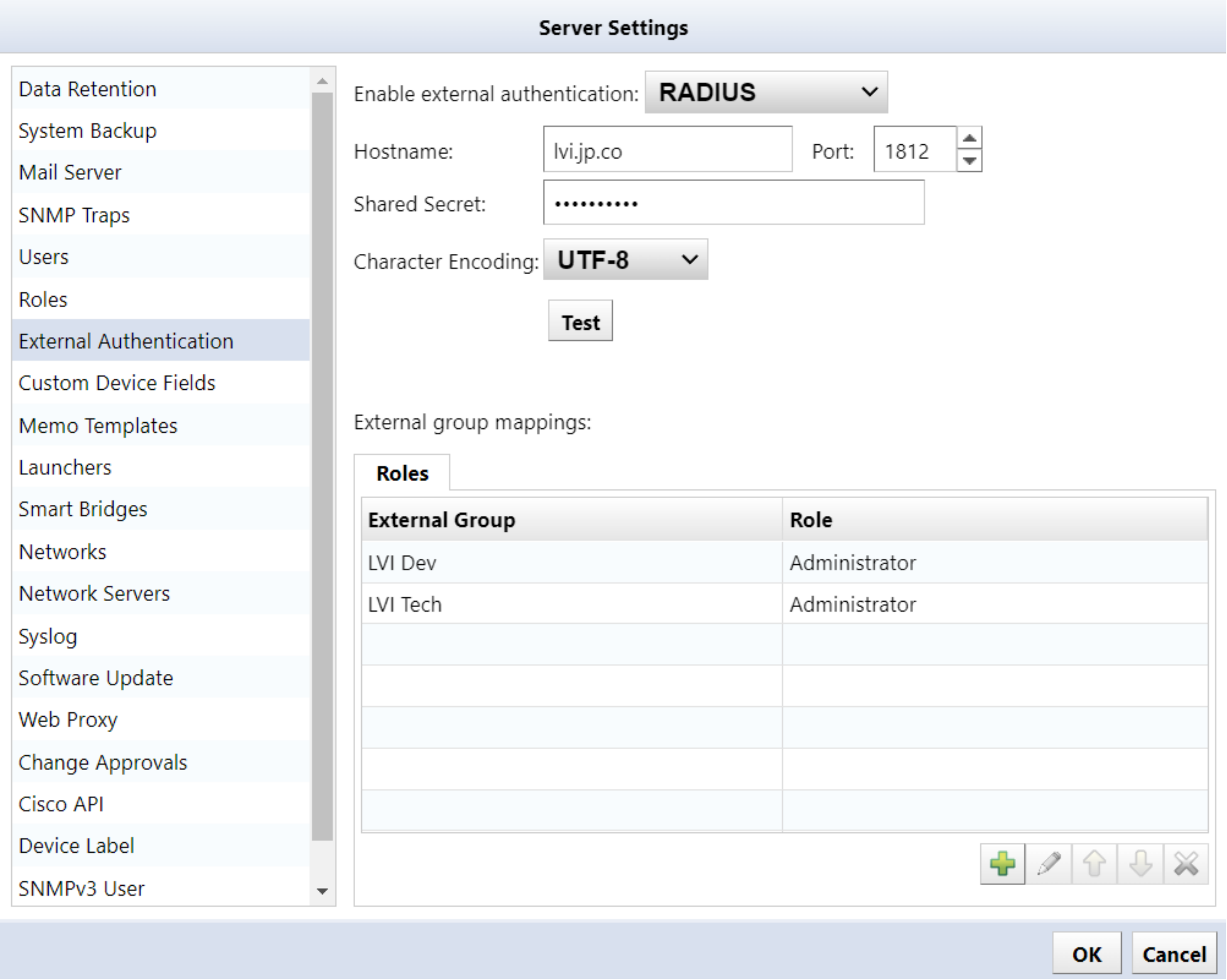
```
LogicVein Cleartext-Password: = "password"
```

```
Filter-Id += "GROUP"
```

With this configuration, when ThirdEye 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. Click [Settings] in the Global Menu to open the [Server Settings] window in ThirdEye, and click [External Authentication].
2. Change the [Enable external authentication] selection to `RADIUS`.



Server Settings

Enable external authentication: RADIUS

Hostname: lvi.jp.co

Port: 1812

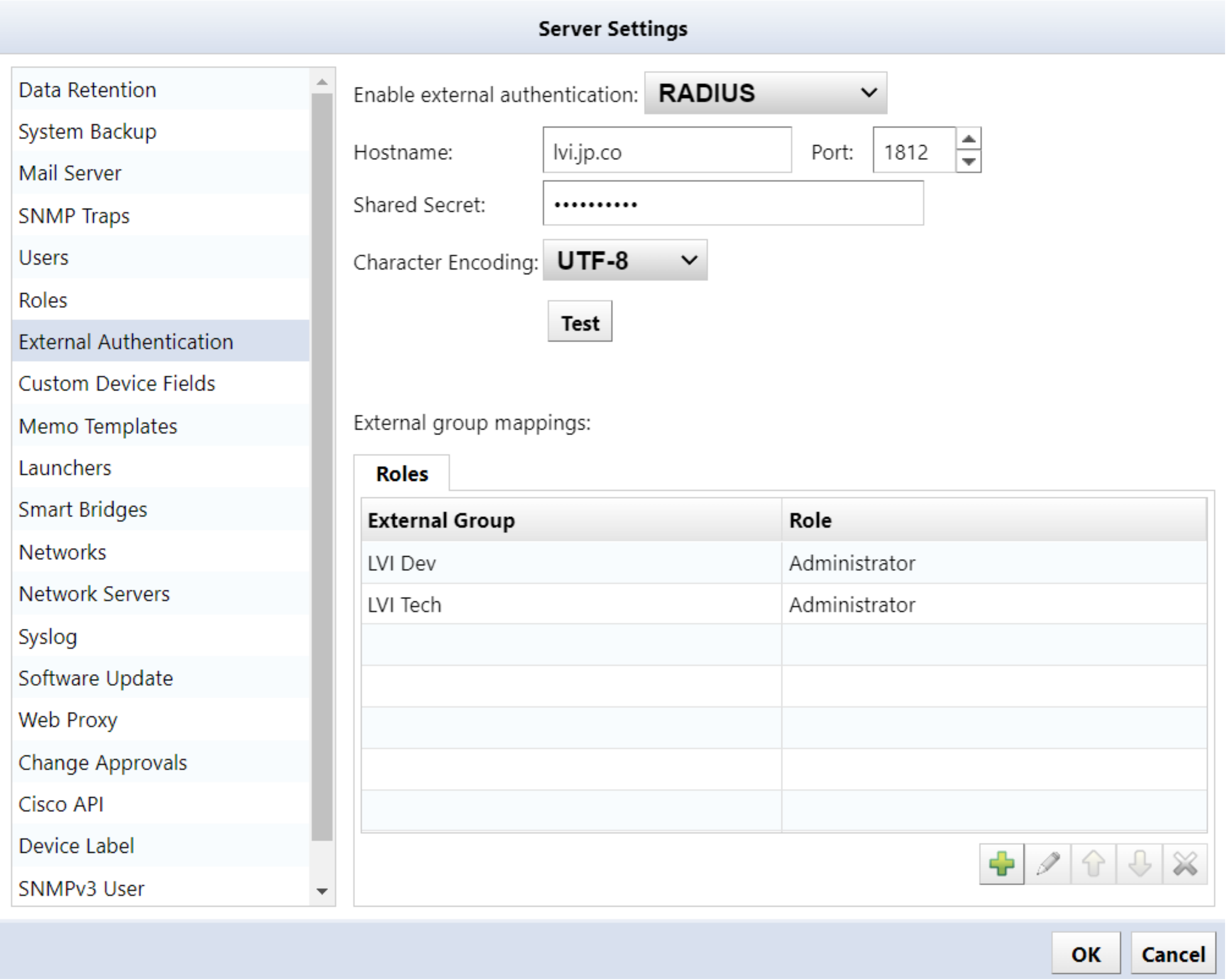
Shared Secret: ••••••••••

Character Encoding: UTF-8

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

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



Enable external authentication: RADIUS

Hostname: lvi.jp.co   Port: 1812

Shared Secret: ••••••••••

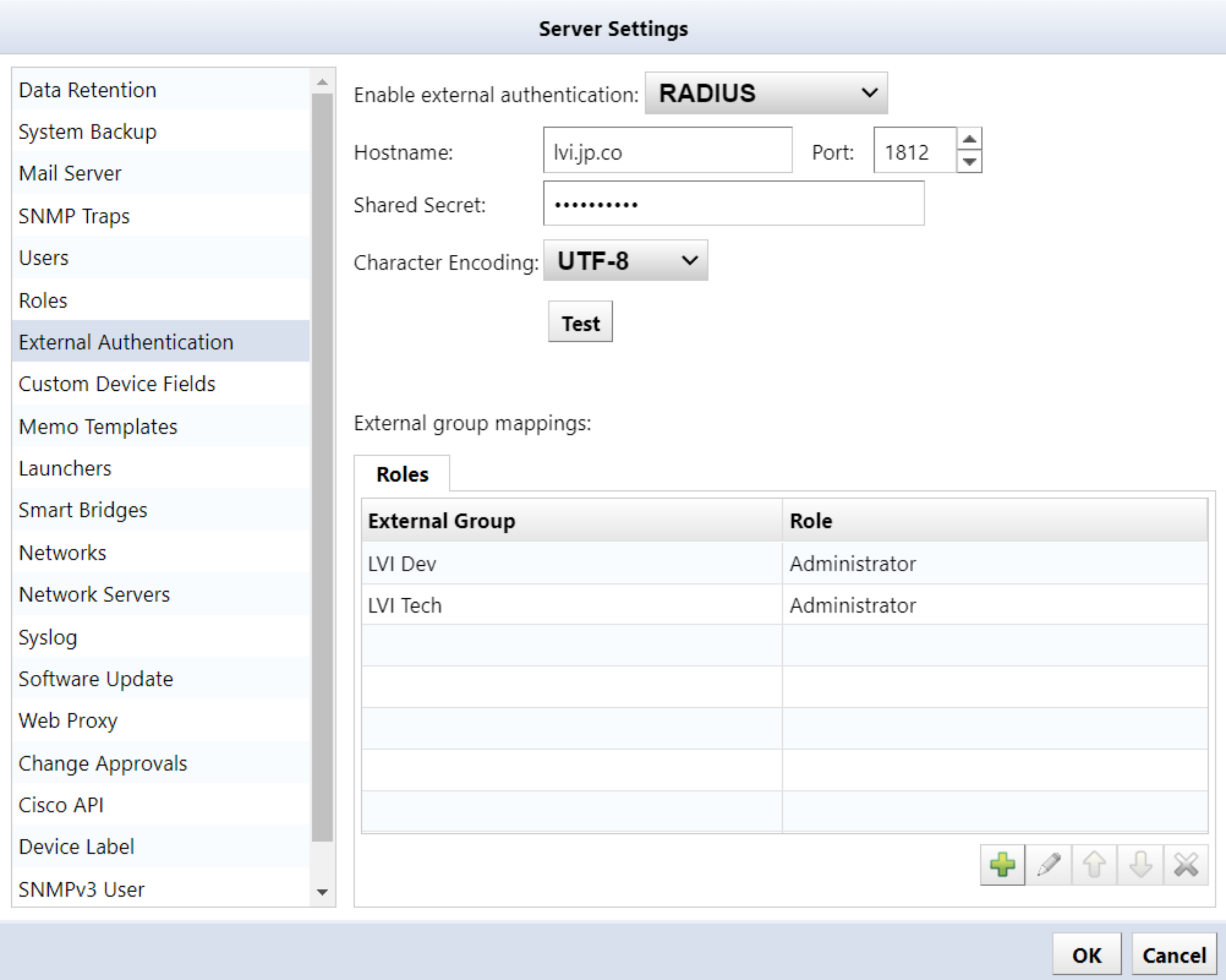
Character Encoding: UTF-8

External group mappings:

Roles

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

4. Click the ➕ button to set permissions for "External Group mappings".



Server Settings

Enable external authentication: RADIUS

Hostname: lvi.jp.co Port: 1812

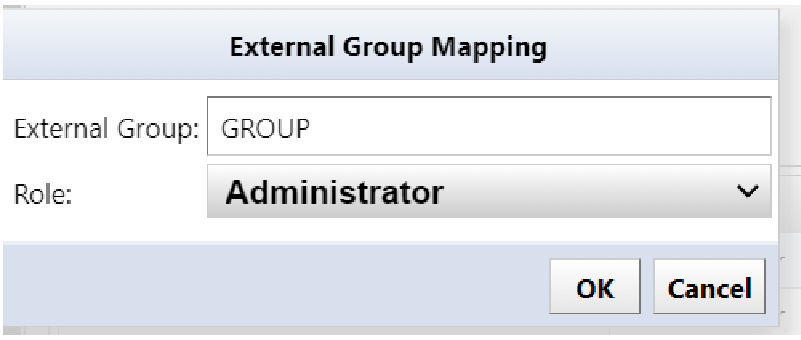
Shared Secret: ••••••••••

Character Encoding: UTF-8

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

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


External Group Mapping

External Group: GROUP

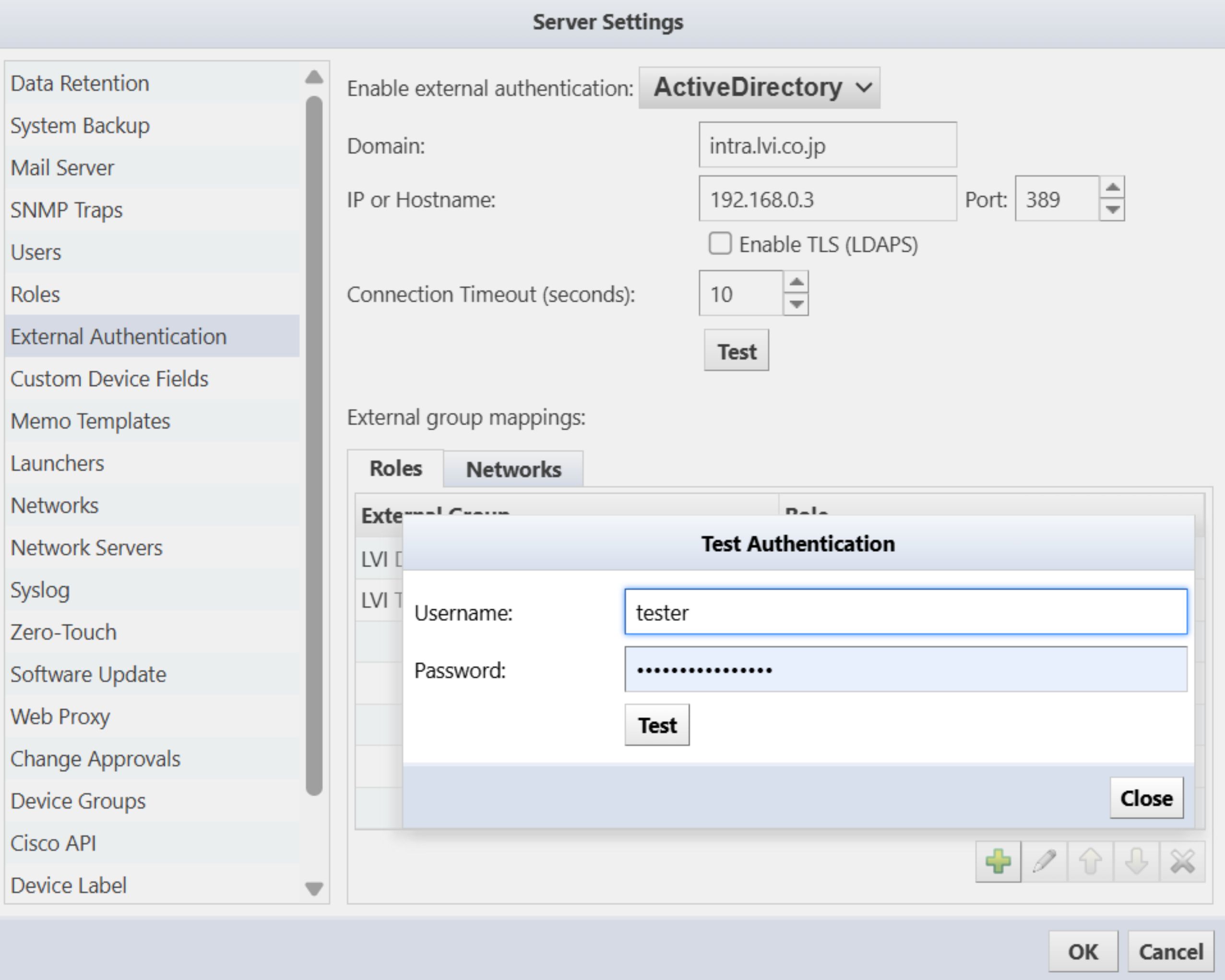
Role: Administrator

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.


Server Settings

Enable external authentication: ActiveDirectory

Domain: intra.lvi.co.jp

IP or Hostname: 192.168.0.3 Port: 389

□ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

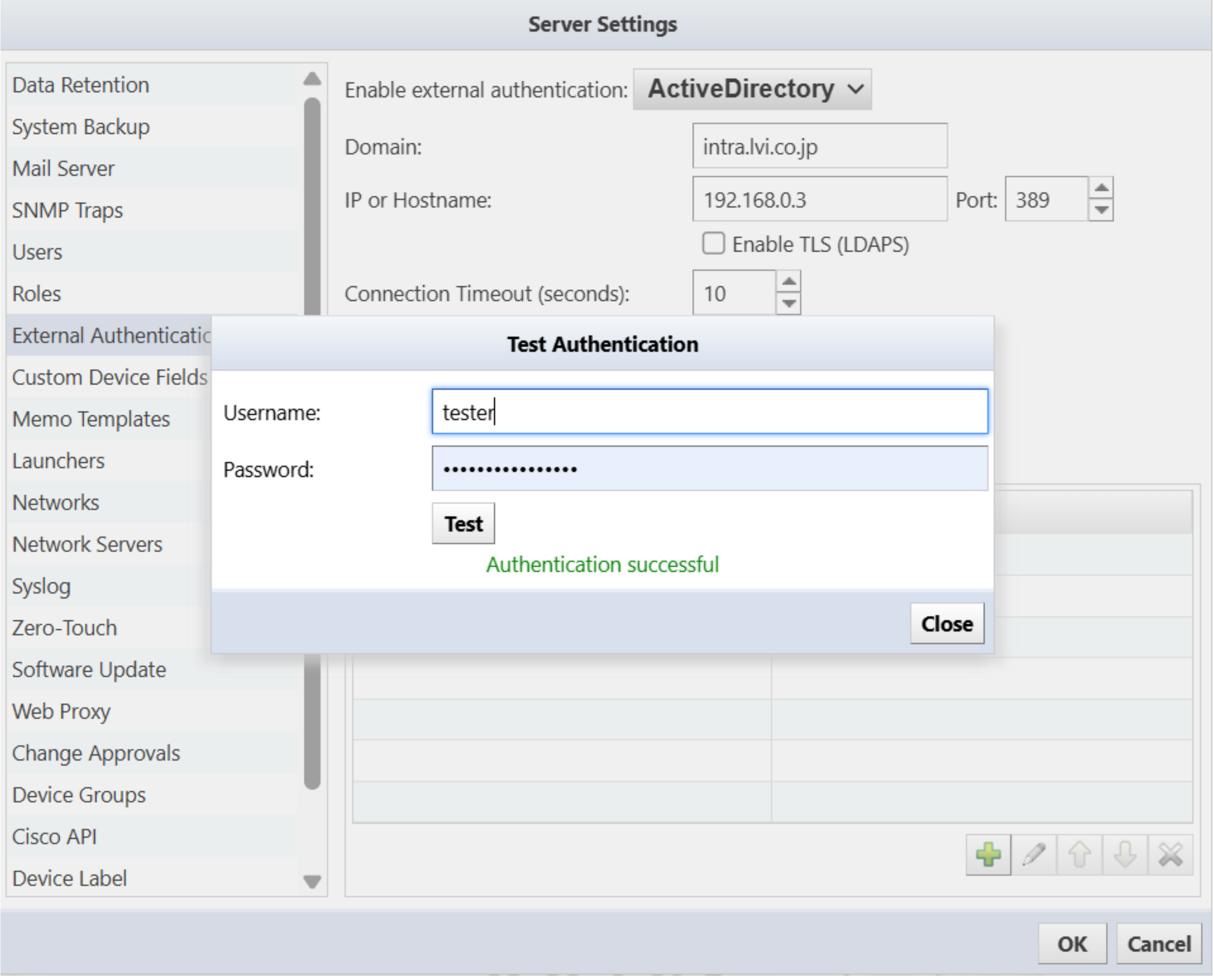
External group mappings:

Test Authentication

Username: tester

Password: ••••••••••••••••

If successful, the message “Authentication successful” will be displayed.



Server Settings

Enable external authentication: ActiveDirectory

Domain: intra.lvi.co.jp

IP or Hostname: 192.168.0.3 Port: 389

□ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

Test Authentication

Username: tester

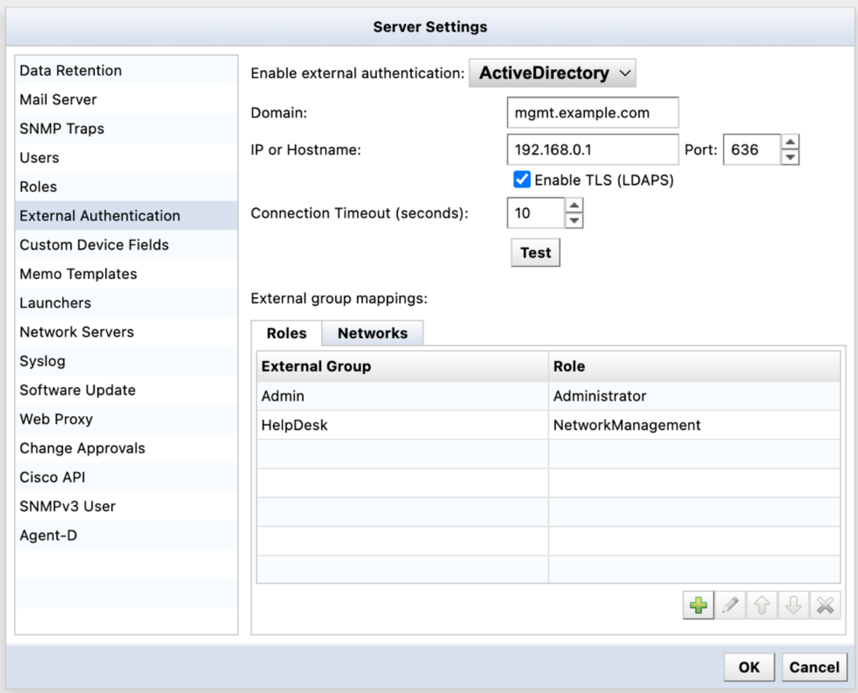
Password: ••••••••••••••••

Authentication successful

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. Click [Settings] in the Global Menu to open the [Server Settings] window in ThirdEye, and click [External Authentication].
2. Change “Enable external authentication” to [Active Directory].



Enable external authentication: ActiveDirectory

Domain: mgmt.example.com

IP or Hostname: 192.168.0.1 Port: 636

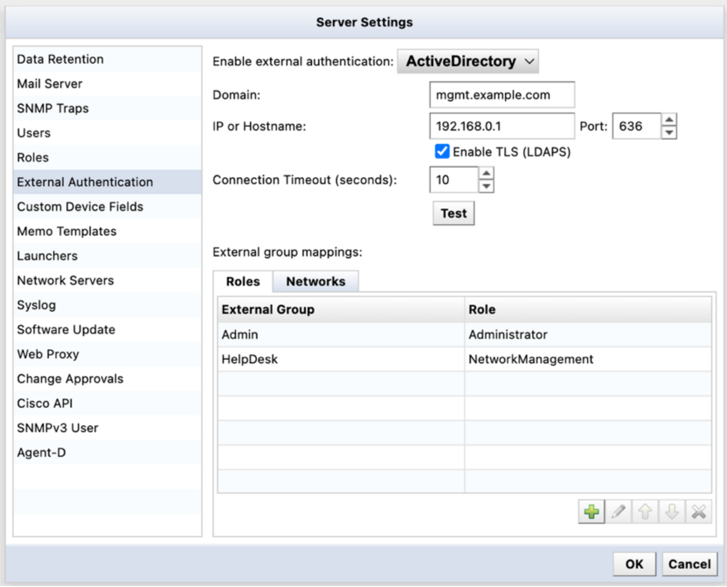
☑ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

External group mappings:

External Group	Role
Admin	Administrator
HelpDesk	NetworkManagement

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



Enable external authentication: ActiveDirectory

Domain: mgmt.example.com

IP or Hostname: 192.168.0.1 Port: 636

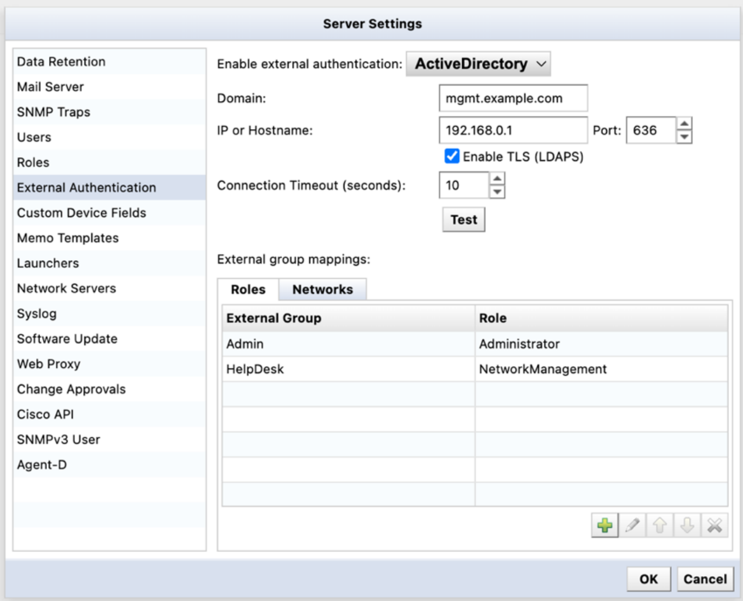
☑ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

External group mappings:

External Group	Role
Admin	Administrator
HelpDesk	NetworkManagement

4. Click the + button to set permissions for External Group Mapping.



Enable external authentication: ActiveDirectory

Domain: mgmt.example.com

IP or Hostname: 192.168.0.1 Port: 636

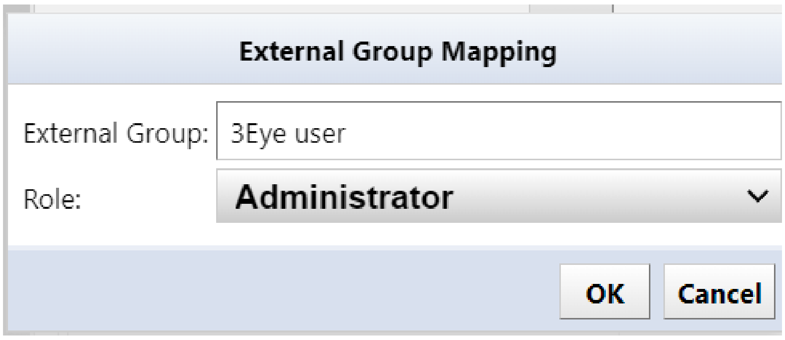
☑ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

External group mappings:

External Group	Role
Admin	Administrator
HelpDesk	NetworkManagement

5. Enter the group to which the user belongs in “External Group” field, and select the “Role” to be assigned.



External Group Mapping

External Group: 3Eye user

Role: Administrator

The Active Directory settings have now 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 ThirdEye via the IdP.

7.7.4 Local Authentication After SAML Configuration

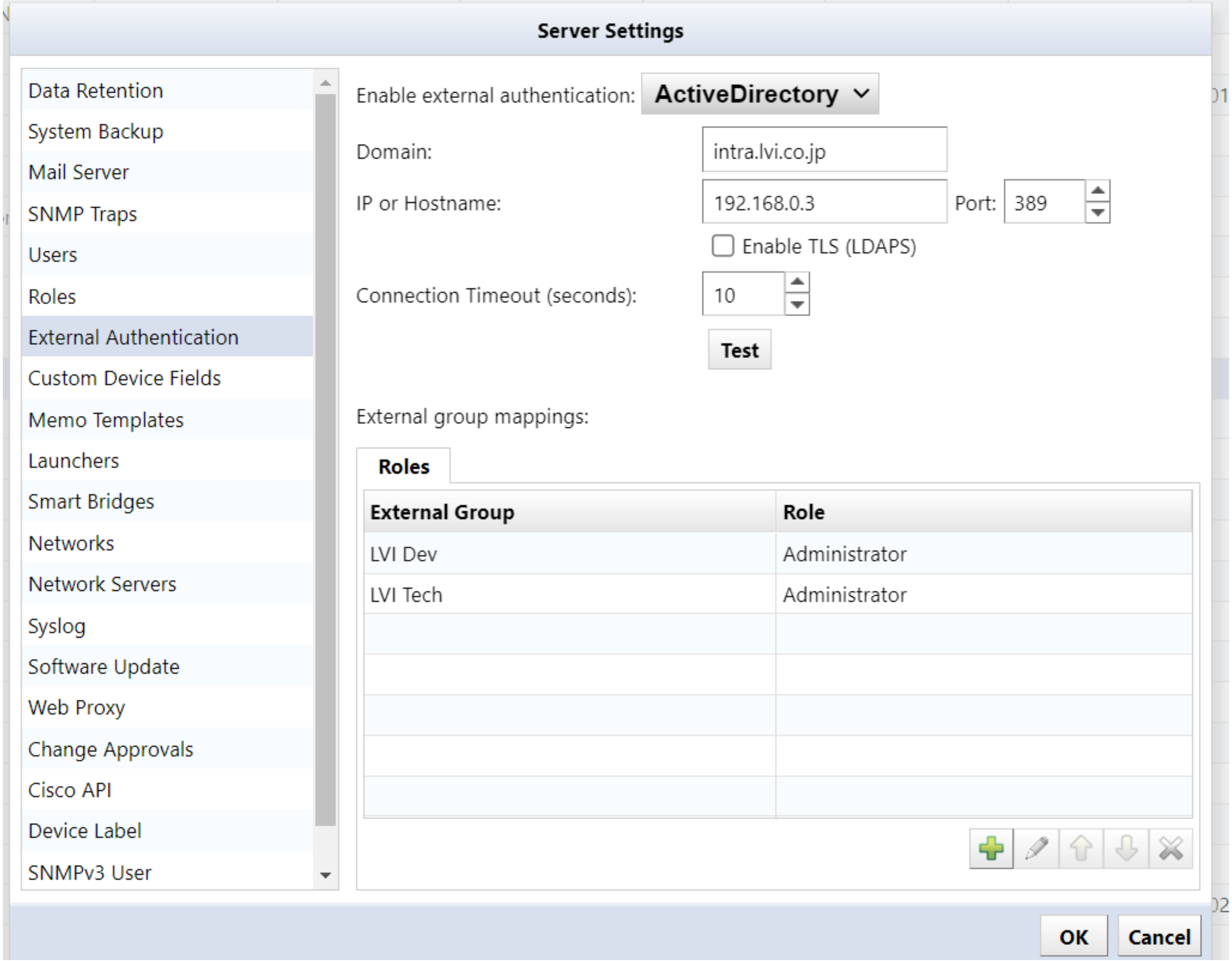
After completing the SAML authentication setup, when you access a ThirdEye product page, the linked sign-in page will be displayed. If you want to log in to the product using local authentication instead of SAML authentication, add the variable `/?forceLoginPage=true` to the end of the URL to access 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 by clicking the [Test] button in the [Server Settings] > [External Authentication] window.



Enable external authentication: ActiveDirectory

Domain: intra.lvi.co.jp

IP or Hostname: 192.168.0.3 Port: 389

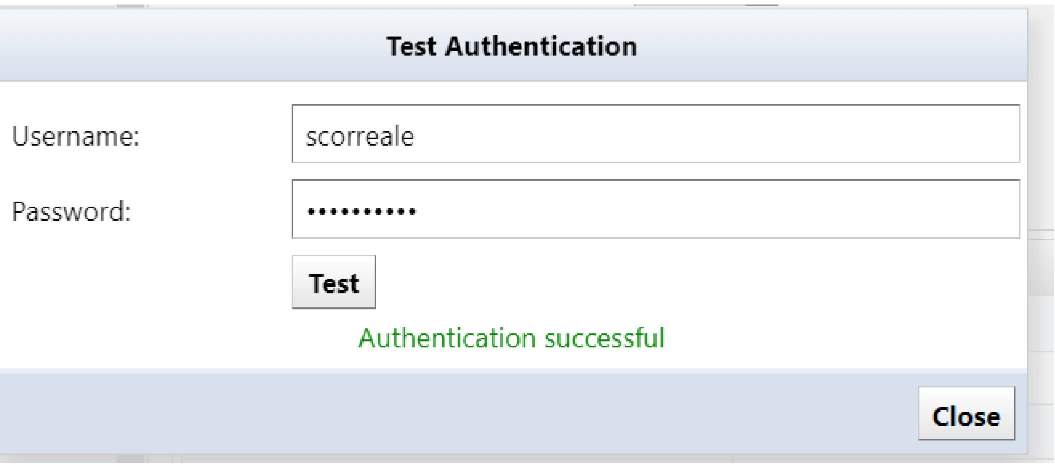
□ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

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.



Test Authentication

Username: scorreale

Password: ••••••••••

Authentication successful

7.7.6 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 ThirdEye.

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

Procedure

Configure SAML 1. Log in to ThirdEye.

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 ThirdEye 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. In the [Set up Single Sign-On with SAML] window, 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 ThirdEye 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 ThirdEye “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 ThirdEye

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 ThirdEye 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 ThirdEye.

Configure External Group mapping

1. Open [Settings] > [External Authentication].
2. On the [External Group Mapping] screen, click the + 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.

7.7.7 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 administrator privileges or permission to “Allow security settings in ThirdEye.

Configure SAML

1. Log in to ThirdEye.
2. Click [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, click [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=SAML2Clien`
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 the [Signature Certificate] window, click [Browse files…] and select the SP certificate certificate downloaded from ThirdEye.

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

8. Configure 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:

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

Item 2:

- **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, configure the following:

- **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 ThirdEye

1. In ThirdEye, click [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 the [External Group Mappings] window, click the ➕ 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 ThirdEye

Log in to ThirdEye as an Okta user.

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

7.7.8 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 administrator privileges or permission to “Allow security settings in ThirdEye.

Configuring 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 the 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. Click [Clients] > [Create Client].

4. Enter “Client ID” and “Name”

- Client ID:

`https://<LOGIC_VEIN_SERVER_IP_OR_HOSTNAME>/auth`

- Name: Selected by user (e.g. “ThirdEye”).

5. Click [Next] and add a callback URL

The callback URL should be:

`https://<LOGIC_VEIN_SERVER_IP_OR_HOSTNAME>/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://<LOGIC_VEIN_SERVER_IP_OR_HOSTNAME>/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://<LOGIC_VEIN_SERVER_IP_OR_HOSTNAME>/`

(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 ThirdEye 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.

27. Click [Realm Settings] in the left sidebar, and click [Save] to download the “SAML 2.0 Identity Provider Metadata file”.

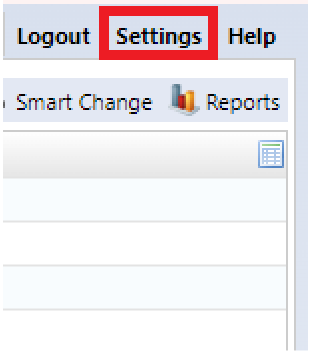
28. Upload the SAML 2.0 Identity Provider Metadata file to “ThirdEye SAML Upload IDP Metadata XML”.

29. Log out of ThirdEye to be redirected to Keycloak for SSO Login.

7.8 Set Session Timeout For Users

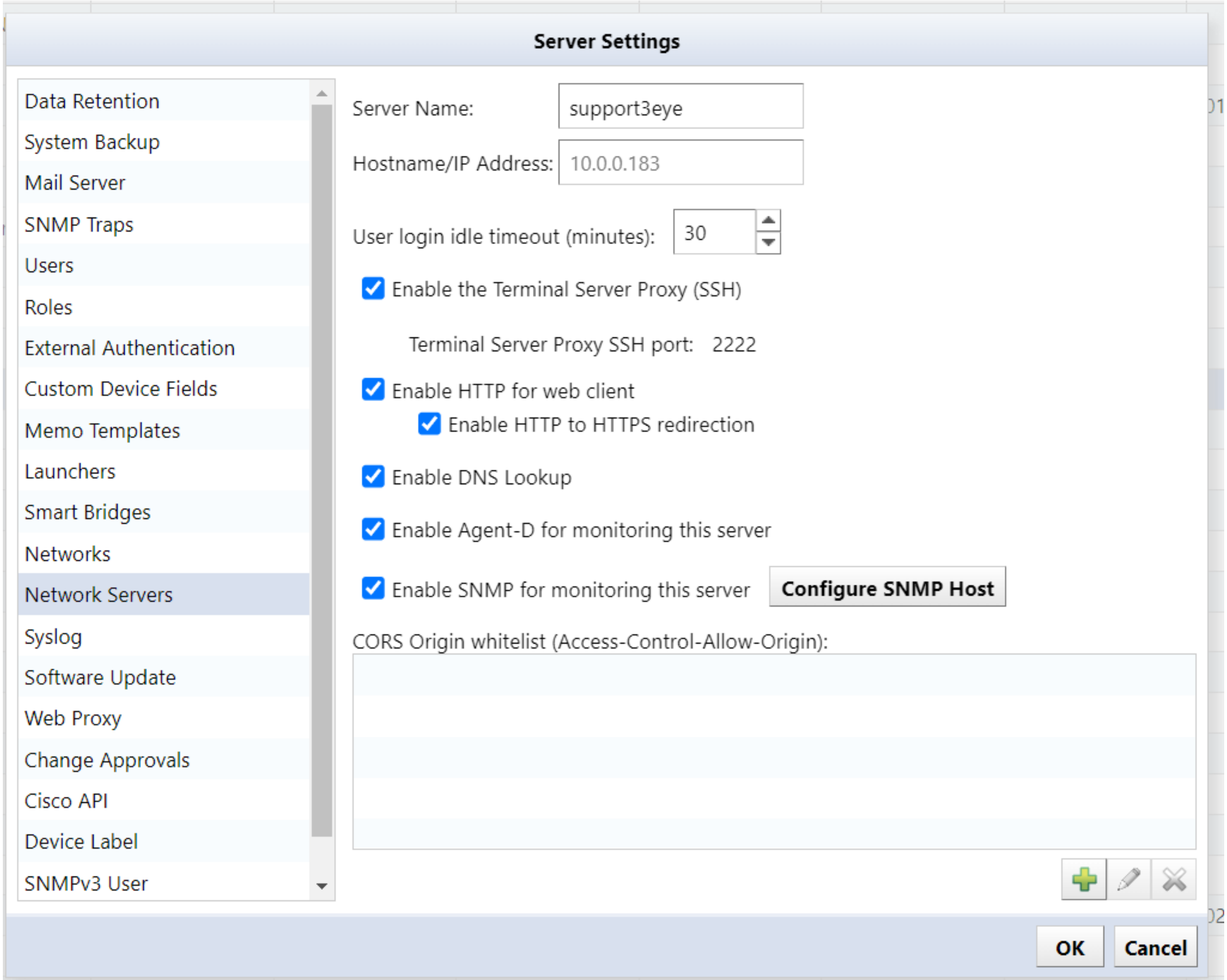
ThirdEye requires users to re-authenticate after 30 minutes of inactivity. To change this time, follow the steps below:

1. Click [Settings] on the Global Menu.



2. Click [Network Servers], and change the "User Login Idle Timeout" time.

Settable range: `10` to `525600` (minutes)


Server Settings

Server Name: support3eye

Hostname/IP Address: 10.0.0.183

User login idle timeout (minutes): 30

☑ Enable the Terminal Server Proxy (SSH)

Terminal Server Proxy SSH port: 2222

☑ Enable HTTP for web client

☑ Enable HTTP to HTTPS redirection

☑ Enable DNS Lookup

☑ Enable Agent-D for monitoring this server

☑ Enable SNMP for monitoring this server

CORS Origin whitelist (Access-Control-Allow-Origin):

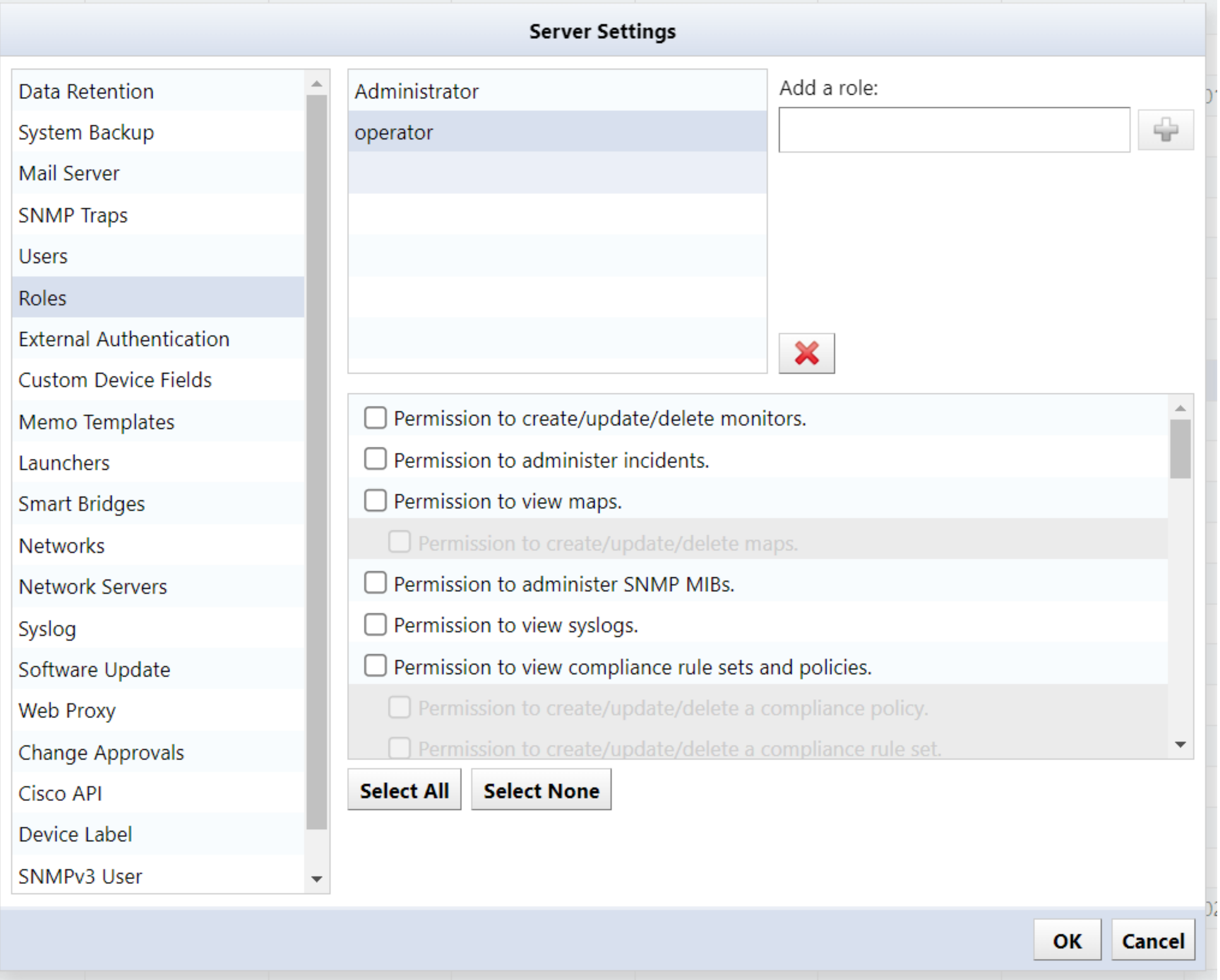
3. Click [OK].

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

1. Select the authority name you want to delete.
2. Click ✖.



Server Settings

- Data Retention
- System Backup
- Mail Server
- SNMP Traps
- Users
- Roles
- External Authentication
- Custom Device Fields
- Memo Templates
- Launchers
- Smart Bridges
- Networks
- Network Servers
- Syslog
- Software Update
- Web Proxy
- Change Approvals
- Cisco API
- Device Label
- SNMPv3 User

Administrator
operator

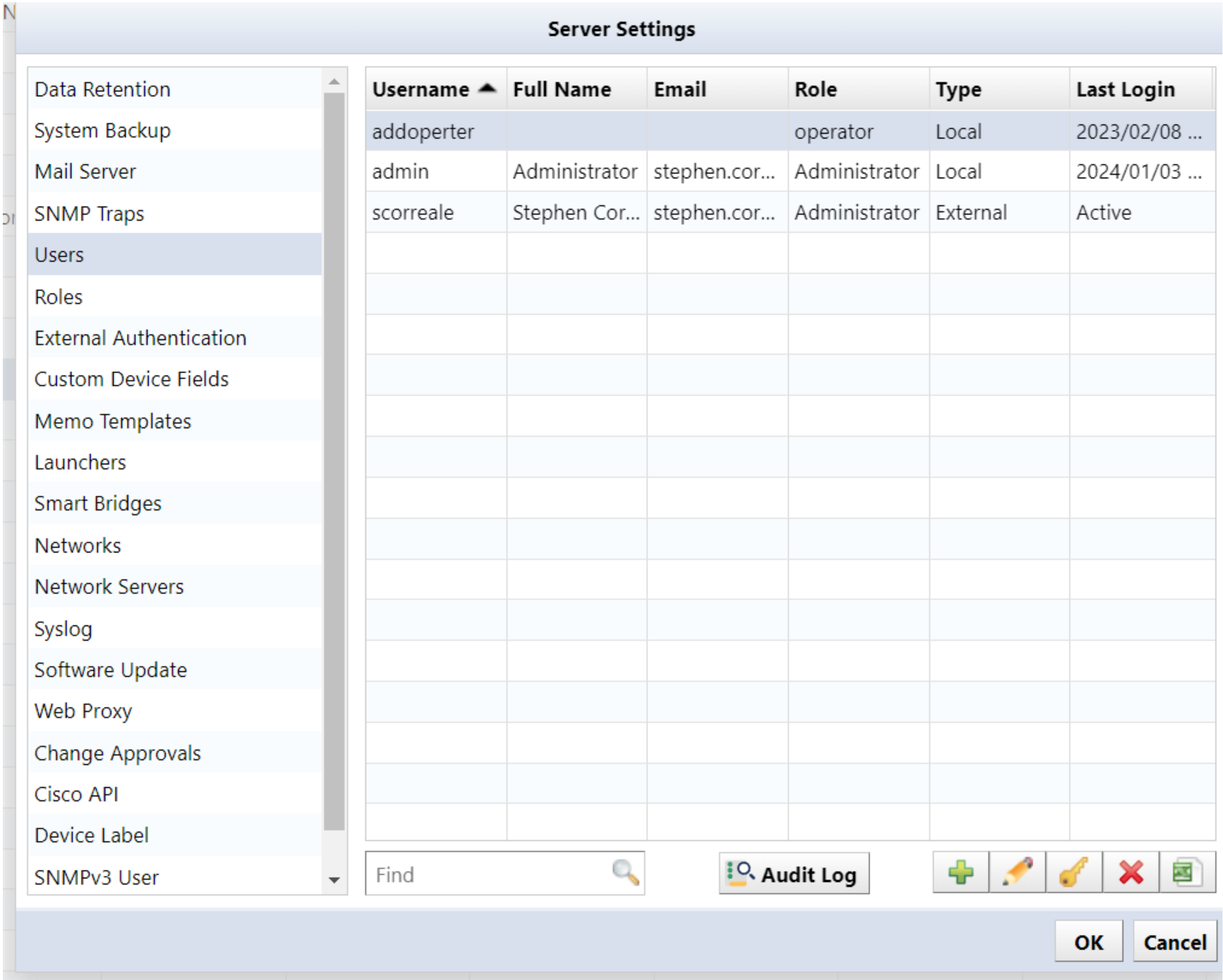
Add a role:

□ Permission to create/update/delete monitors.
□ Permission to administer incidents.
□ Permission to view maps.
□ Permission to create/update/delete maps.
□ Permission to administer SNMP MIBs.
□ Permission to view syslogs.
□ Permission to view compliance rule sets and policies.
□ Permission to create/update/delete a compliance policy.
□ Permission to create/update/delete a compliance rule set.

3. Click [OK] in the Server Settings window.

7.10 Delete User

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



Username	Full Name	Email	Role	Type	Last Login
addoperter			operator	Local	2023/02/08 ...
admin	Administrator	stephen.cor...	Administrator	Local	2024/01/03 ...
scorreale	Stephen Cor...	stephen.cor...	Administrator	External	Active

The user will be deleted.

2. Click [OK] on the server settings.

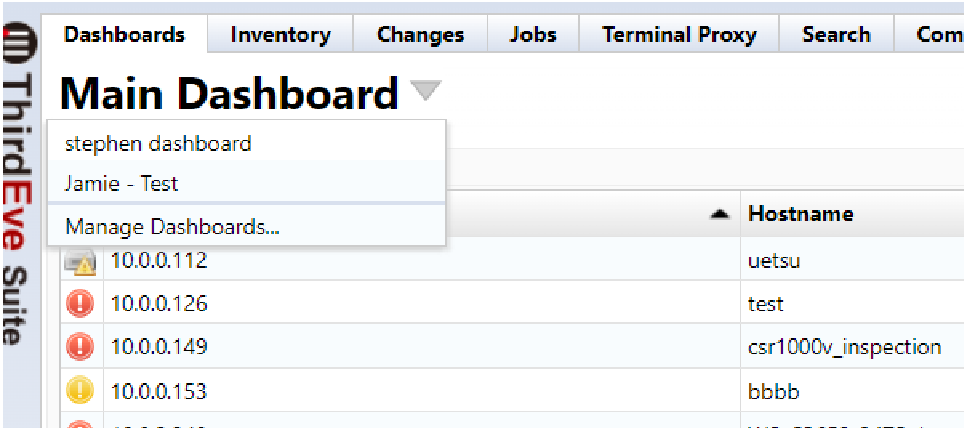
If you delete a user by mistake, click [Cancel].

SECTION 8

DASHBOARD MANAGEMENT

8.1 Add a Dashboard

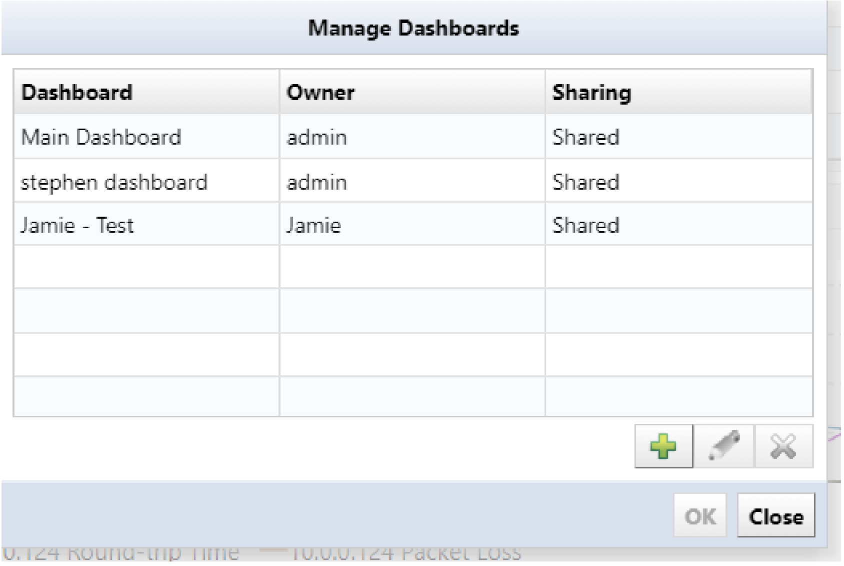
1. Click the Dashboard [Name] (“Main Dashboard” in the image below), and select [Manage Dashboard].



	Hostname
10.0.0.112	uetsu
10.0.0.126	test
10.0.0.149	csr1000v_inspection
10.0.0.153	bbbb

> 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.

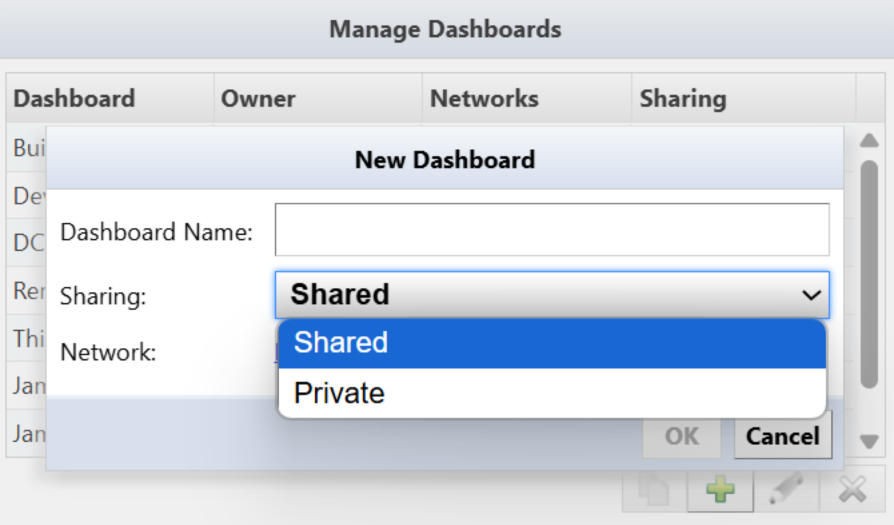
2. In the [Manage Dashboards] window, click the + button.



Dashboard	Owner	Sharing
Main Dashboard	admin	Shared
stephen dashboard	admin	Shared
Jamie - Test	Jamie	Shared

3. In the [New Dashboard] window, enter the Dashboard Name.

4. Select the type of sharing for the Dashboard from the dropdown menu, and click [OK].



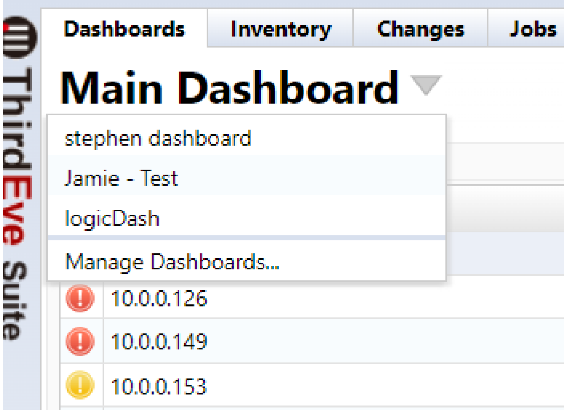
Dashboard type	Explanation
Shared	Add Dashboards that other users can view.
Private	Add a Dashboard that can only be viewed by the user who created it.

The Dashboard will be added to the list.

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

8.2 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.

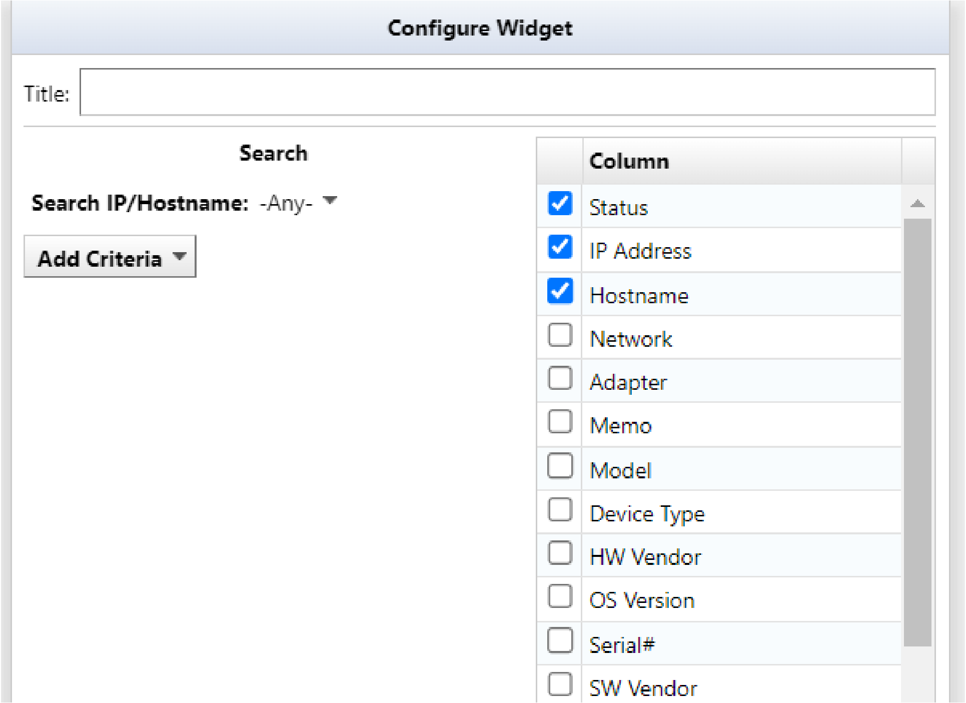
8.3 Widgets

8.3.1 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.



Configure Widget

Title:

Search

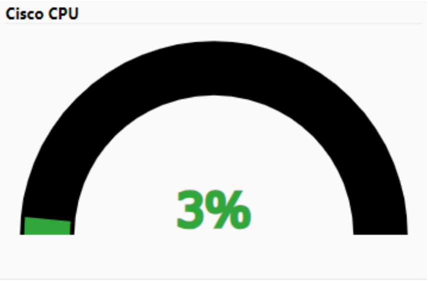
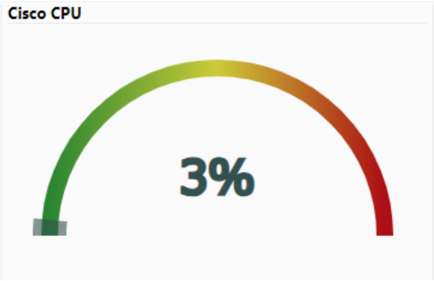
Search IP/Hostname: -Any-

Add Criteria

Column
☑ Status
☑ IP Address
☑ Hostname
□ Network
□ Adapter
□ Memo
□ Model
□ Device Type
□ HW Vendor
□ OS Version
□ Serial#
□ SW Vendor

Gauge

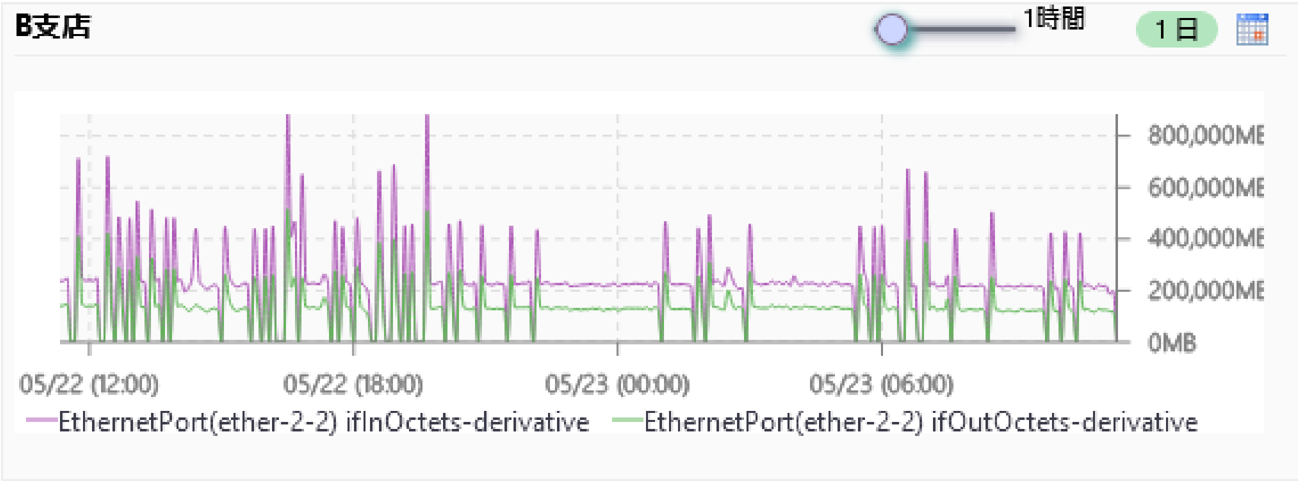
The gauge widget displays a meter graph. It can display two types of meter graphs: “Default” and “Thermal”.

Default	Thermal
	

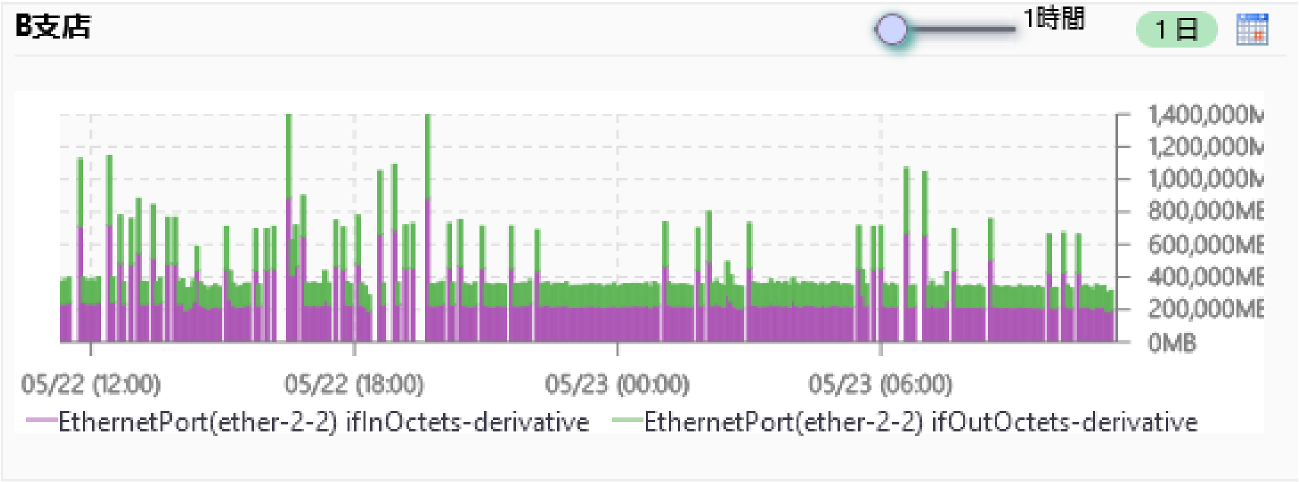
Histogram

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

Line chart:

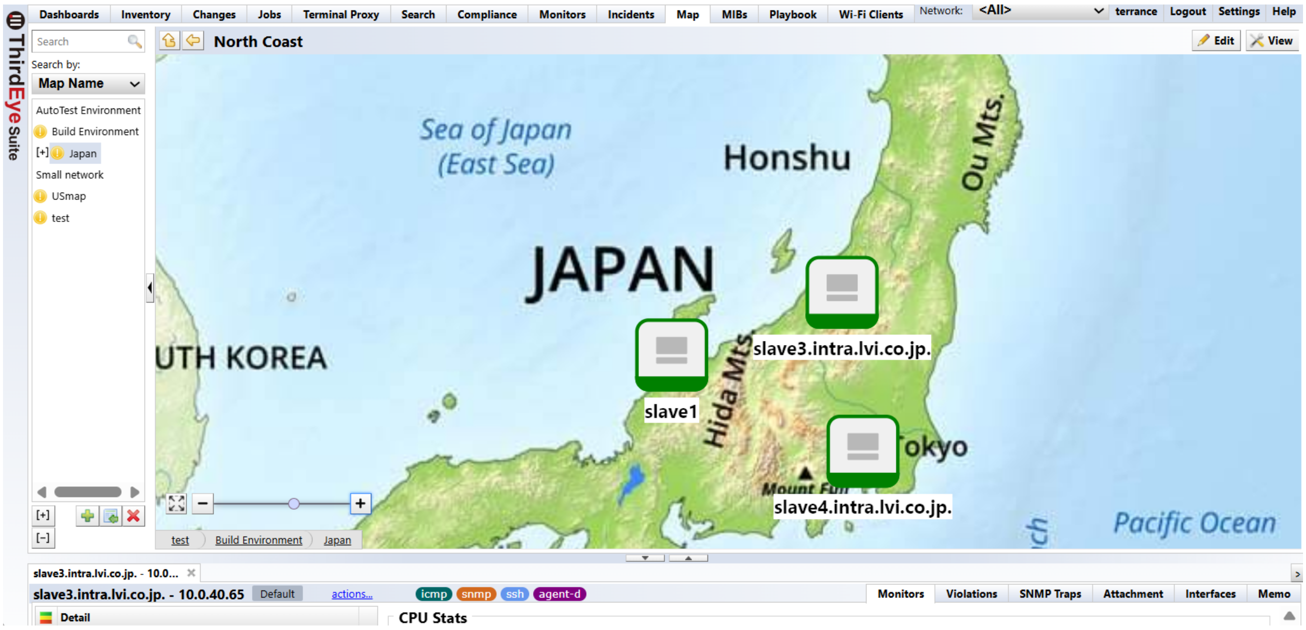


Stacked bar chart:



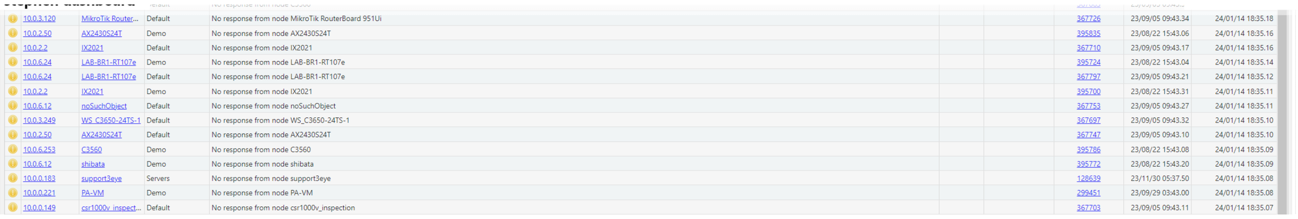
Map

The map widget displays a map:



Violations

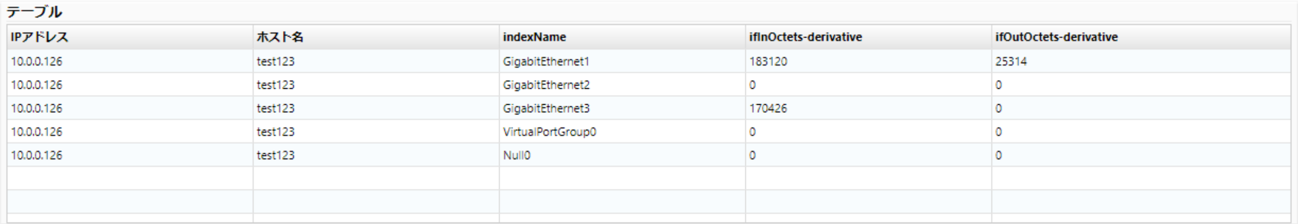
The violations displays violations:



!	10.0.3.120	MikroTik Router...	Default	No response from node MikroTik RouterBoard 951Ui			367726	23/09/05 09:43.34	24/01/14 18:35.18
!	10.0.2.50	AX2430S24T	Demo	No response from node AX2430S24T			395835	23/08/22 15:43.06	24/01/14 18:35.16
!	10.0.2.2	IX2021	Default	No response from node IX2021			367710	23/09/05 09:43.17	24/01/14 18:35.16
!	10.0.6.24	LAB-BR1-RT107e	Demo	No response from node LAB-BR1-RT107e			395724	23/08/22 15:43.04	24/01/14 18:35.14
!	10.0.6.24	LAB-BR1-RT107e	Default	No response from node LAB-BR1-RT107e			367797	23/09/05 09:43.21	24/01/14 18:35.12
!	10.0.2.2	IX2021	Demo	No response from node IX2021			395700	23/08/22 15:43.31	24/01/14 18:35.11
!	10.0.6.12	noSuchObject	Default	No response from node noSuchObject			367753	23/09/05 09:43.27	24/01/14 18:35.11
!	10.0.3.249	WS_C3650-24TS-1	Default	No response from node WS_C3650-24TS-1			367697	23/09/05 09:43.32	24/01/14 18:35.10
!	10.0.2.50	AX2430S24T	Default	No response from node AX2430S24T			367747	23/09/05 09:43.10	24/01/14 18:35.10
!	10.0.6.253	C3560	Demo	No response from node C3560			395786	23/08/22 15:43.08	24/01/14 18:35.09
!	10.0.6.12	shibata	Demo	No response from node shibata			395772	23/08/22 15:43.20	24/01/14 18:35.09
!	10.0.0.183	support3eye	Servers	No response from node support3eye			128639	23/11/30 05:37.50	24/01/14 18:35.08
!	10.0.0.221	PA-VM	Demo	No response from node PA-VM			299451	23/09/29 03:43.00	24/01/14 18:35.08
!	10.0.0.149	csr1000v_inspect...	Default	No response from node csr1000v_inspection			367703	23/09/05 09:43.11	24/01/14 18:35.07

Table

The tables widget displays a table:

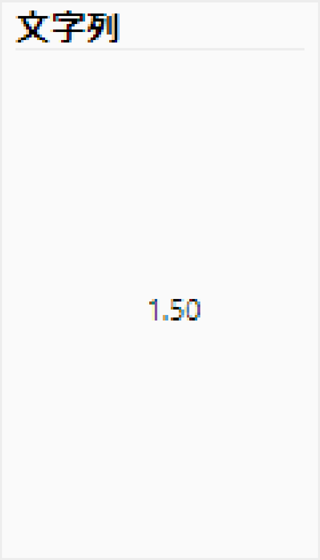


テーブル

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:

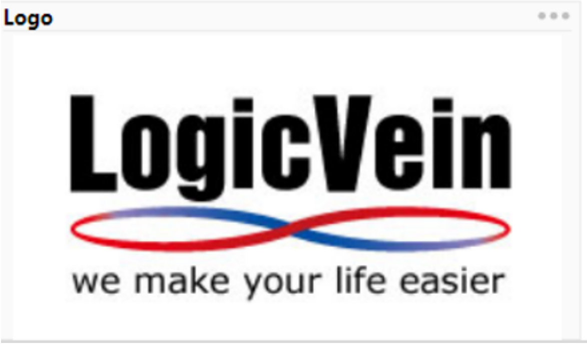


文字列

1.50

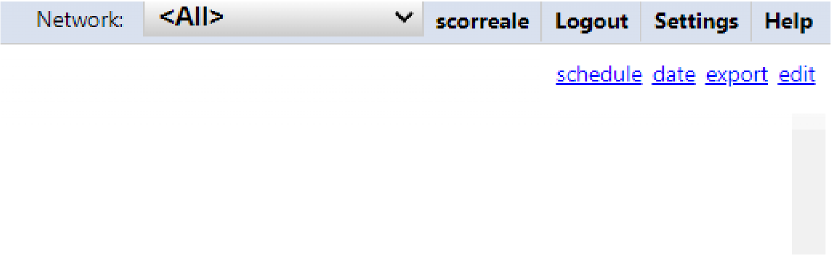
Image

The image widget displays an image:

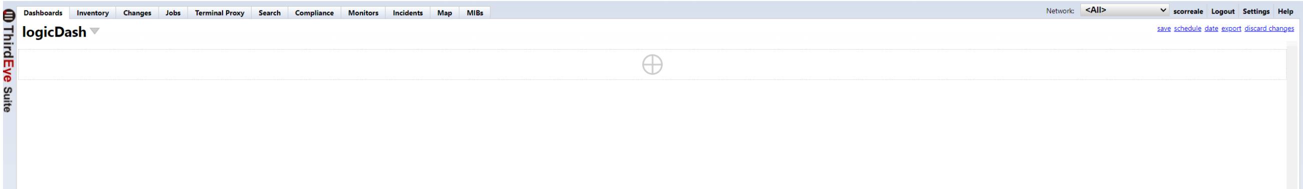


8.3.2 Add a Widget

1. Click [Edit] in the Global Menu.

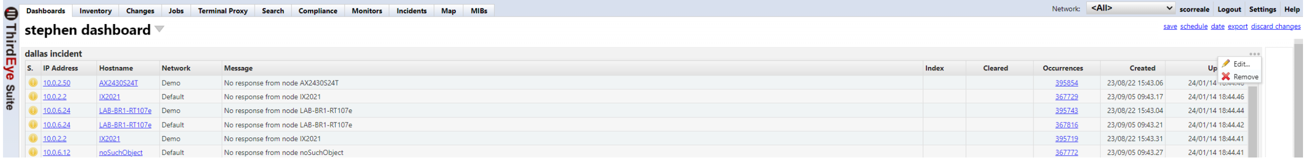


2. Click the ⊕ button at the top of the Dashboard screen.



8.3.3 Widget Edit Menu

While in Dashboard edit mode, you can also Add/Edit/Delete Widgets.



stephen dashboard

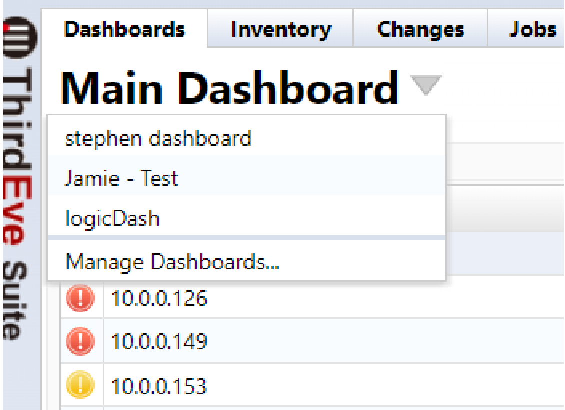
dallas incident

S.	IP Address	Hostname	Network	Message	Index	Cleared	Occurrences	Created	Up
●	10.0.2.50	AX2430S24T	Demo	No response from node AX2430S24T			395854	23/08/22 15:43.06	24/01/14
●	10.0.2.2	IX2021	Default	No response from node IX2021			367729	23/09/05 09:43.17	24/01/14 18:44.46
●	10.0.6.24	LAB-BR1-RT107e	Demo	No response from node LAB-BR1-RT107e			395743	23/08/22 15:43.04	24/01/14 18:44.44
●	10.0.6.24	LAB-BR1-RT107e	Default	No response from node LAB-BR1-RT107e			367816	23/09/05 09:43.21	24/01/14 18:44.42
●	10.0.2.2	IX2021	Demo	No response from node IX2021			395719	23/08/22 15:43.31	24/01/14 18:44.41
●	10.0.6.12	noSuchObject	Default	No response from node noSuchObject			367772	23/09/05 09:43.27	24/01/14 18:44.41

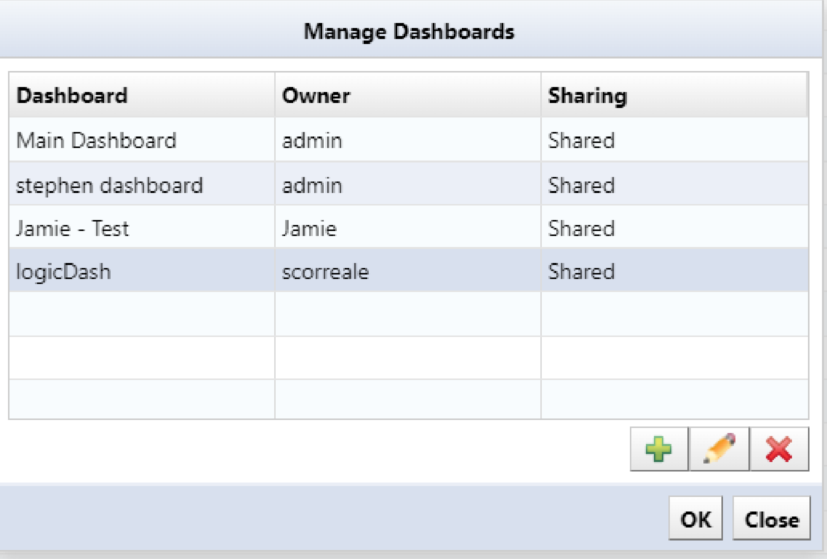
Button	Explanation
…	Click the three-dot button […] displayed to the right of the widget title to display the widget editing menu.
Edit	Edit the widget.
Remove	Delete a widget.

8.4 Delete Dashboard

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 delete, and click the ✖ button.

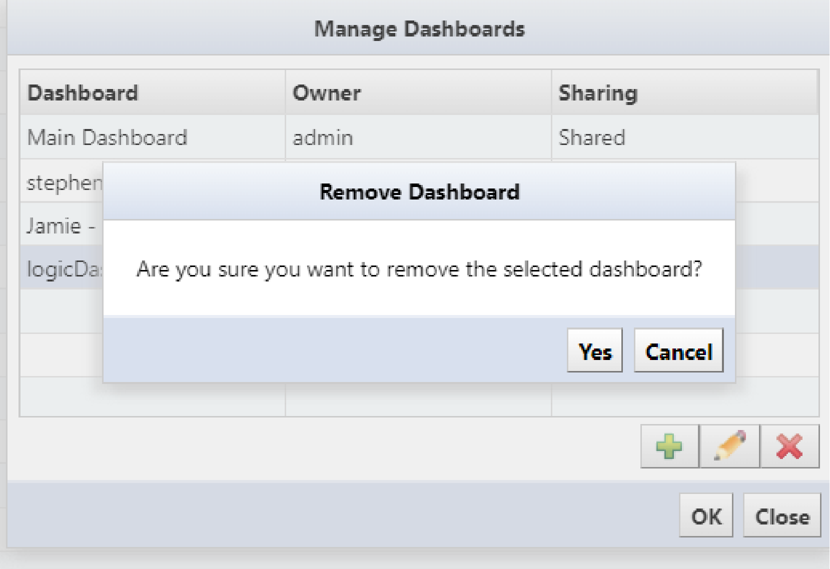


Manage Dashboards

Dashboard	Owner	Sharing
Main Dashboard	admin	Shared
stephen dashboard	admin	Shared
Jamie - Test	Jamie	Shared
logicDash	scorreale	Shared

A confirmation message will be displayed.

3. Click [Yes].



Dashboard	Owner	Sharing
Main Dashboard	admin	Shared
stephen		
Jamie -		
logicDa		

Are you sure you want to remove the selected dashboard?

SECTION 9

ZERO-TOUCH

Zero-Touch automates network device deployment and configuration, eliminating manual setup. Devices boot with no pre-existing configuration and automatically retrieve settings via protocols like DHCP/TFTP.

With Zero-Touch you can:

- Rapidly configure new devices remotely during initial deployments
- Automatically restore corrupted configurations during self-recovery
- Transfer settings seamlessly to replacement devices during hardware replacement

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

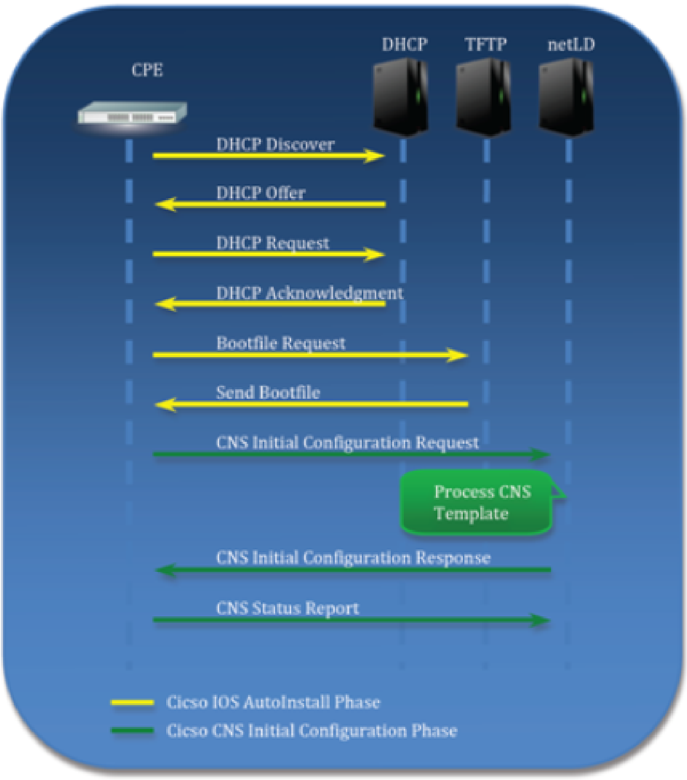
-**Template**: Distribute configurations based on templates. Used when introducing a new device to the network at a remote office.

-**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.

ThirdEye 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 ThirdEye 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 ThirdEye server.

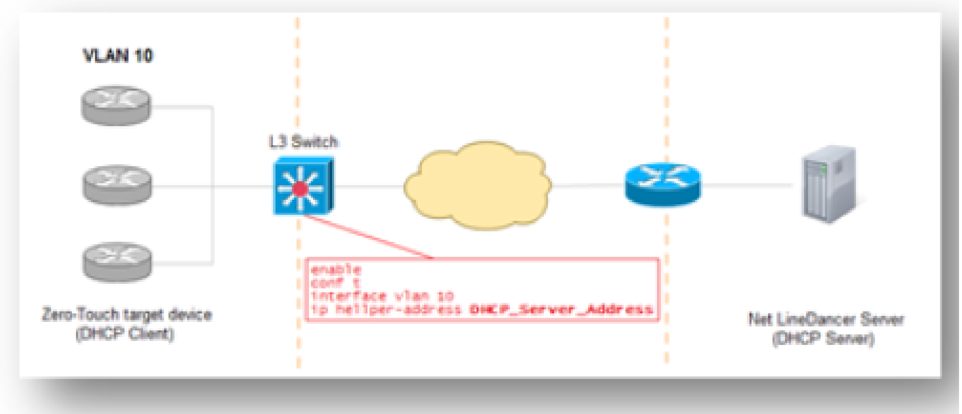


9.1 Zero-Touch Requirements

To use Zero-Touch, the following conditions must be met:

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

DHCP relay example:



```
enable
conf t
interface vlan 10
ip helper-address DHCP_Server_Address
```

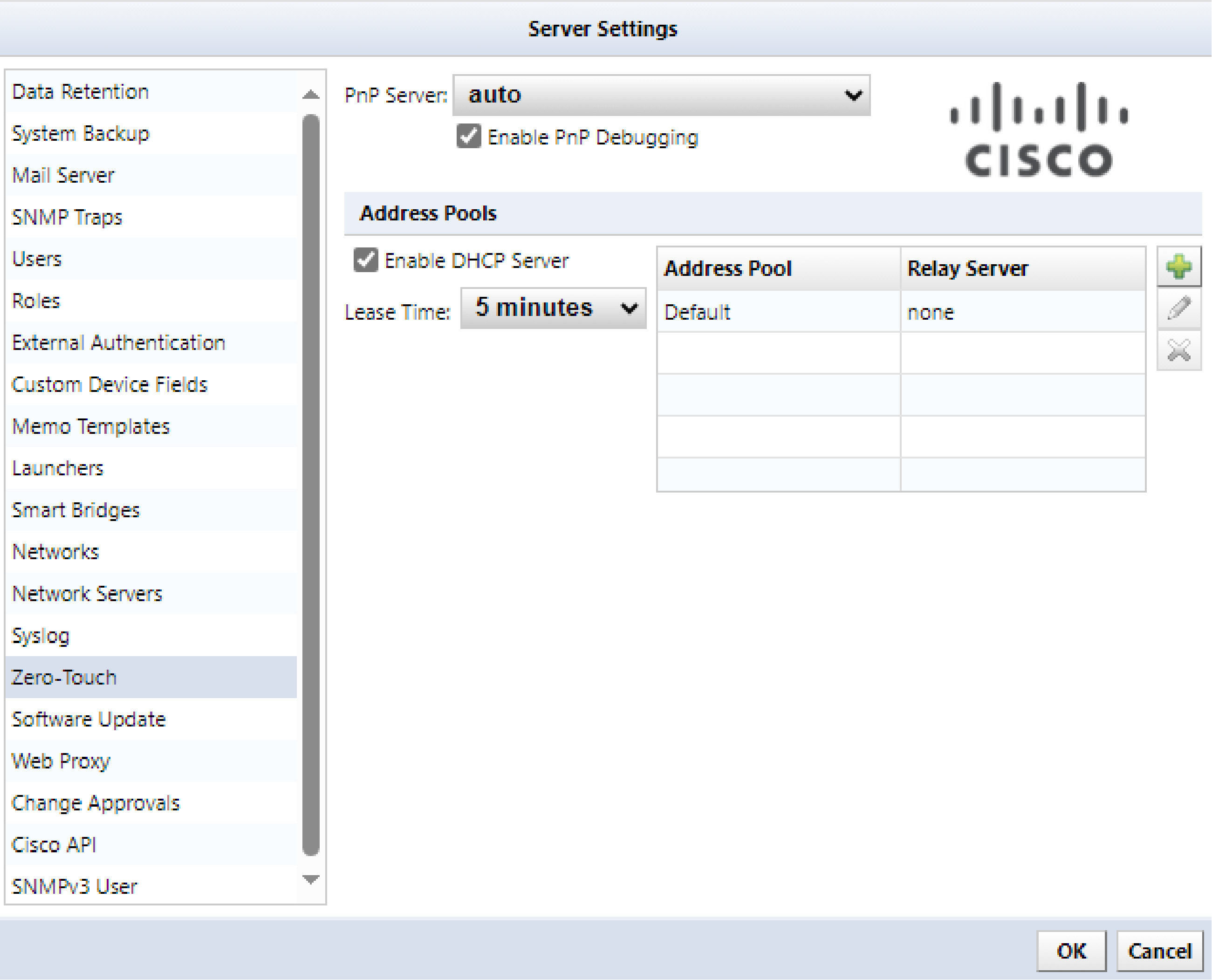
9.2 Managing New Devices

When deploying new devices via ThirdEye Zero-Touch, ensure the device has no pre-existing startup configuration during initial provisioning. To achieve this, select vendor-specific No Configuration ordering options (e.g., CCP-CD-NOCF or CCP-EXPRESS-NOCF) when procuring hardware. This ensures the device boots into a clean state for automated template deployment.

9.3 DHCP Server

To set up a DHCP server:

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



PnP Server: auto

☑ Enable PnP Debugging

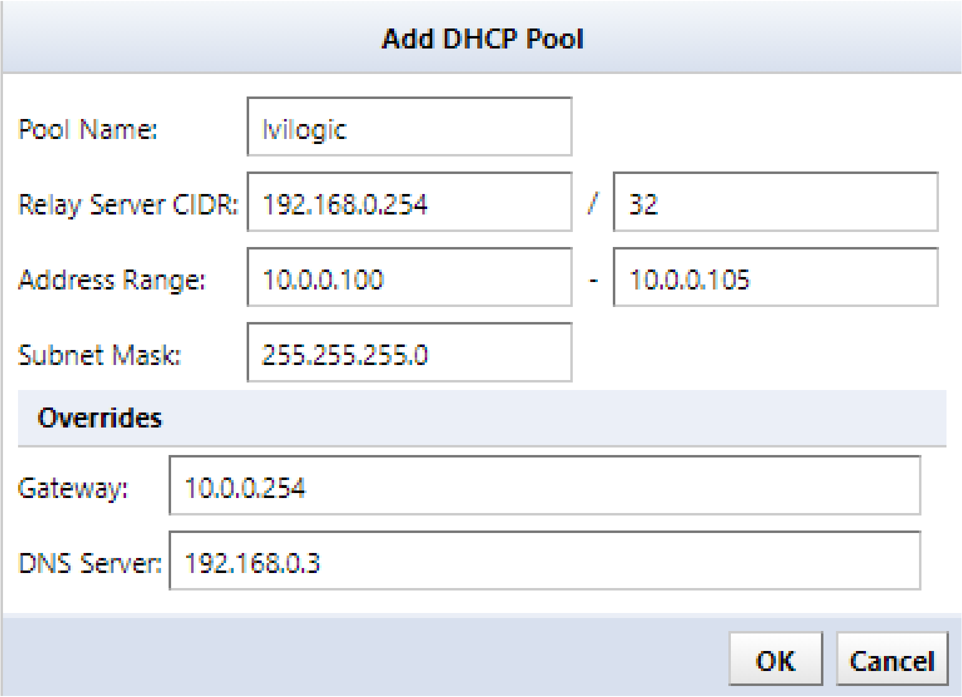
☑ Enable DHCP Server

Lease Time: 5 minutes

Address Pool	Relay Server
Default	none

Item	Explanation
Enable DHCP server	Check this box if you want to use ThirdEye’s DHCP server.
lease time	Set the DHCP lease time.

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



Add DHCP Pool

Pool Name: lvilogic

Relay Server CIDR: 192.168.0.254 / 32

Address Range: 10.0.0.100 - 10.0.0.105

Subnet Mask: 255.255.255.0

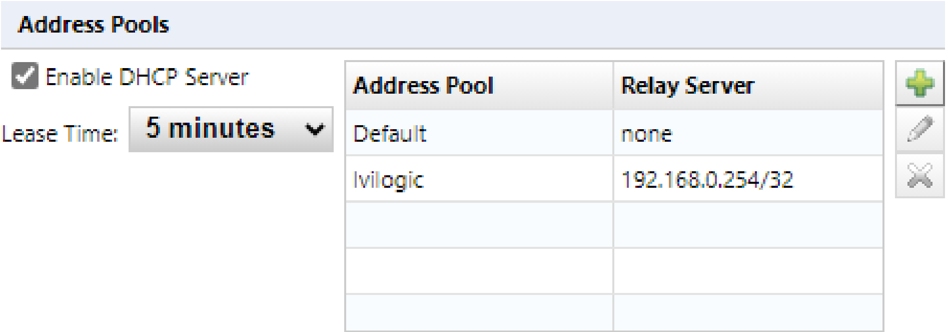
Overrides

Gateway: 10.0.0.254

DNS Server: 192.168.0.3

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.



Address Pools

☑ Enable DHCP Server

Lease Time: 5 minutes

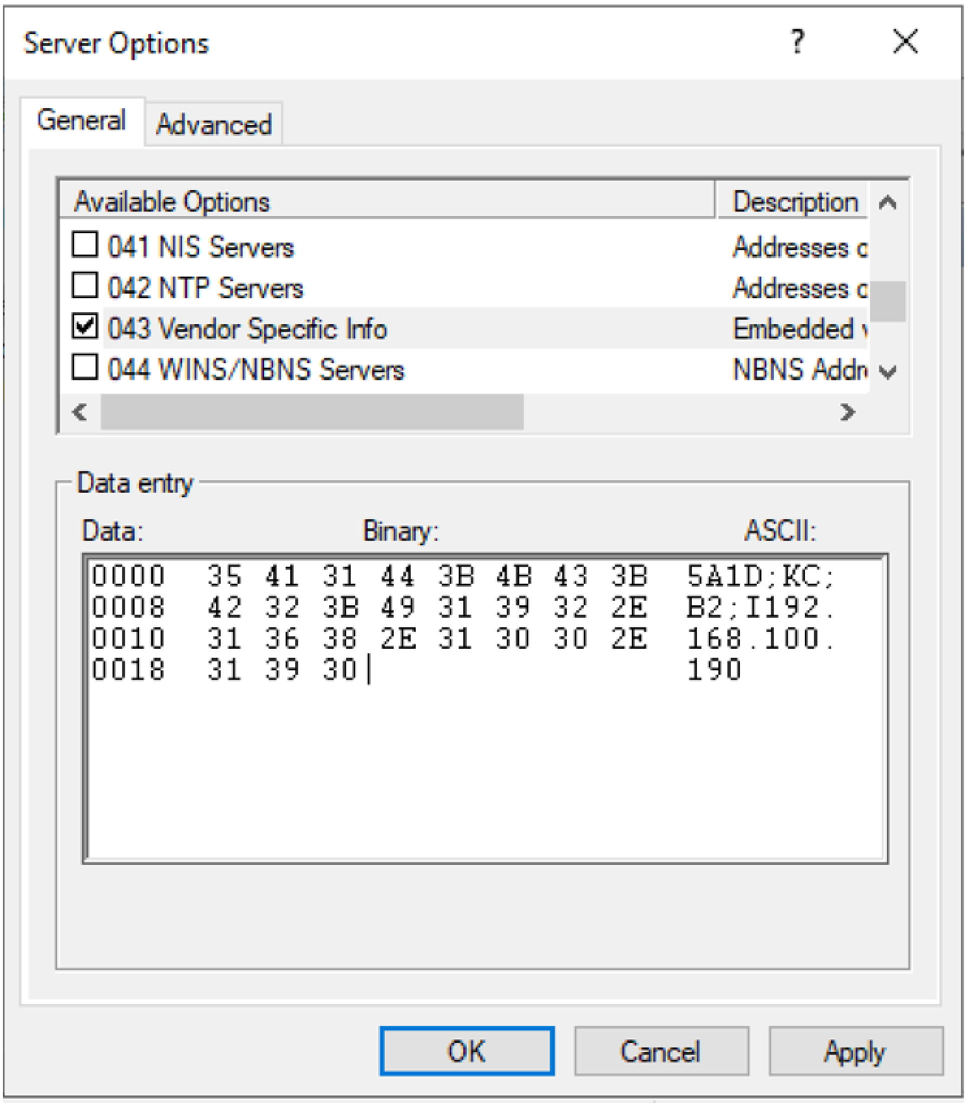
Address Pool	Relay Server
Default	none
lvilogic	192.168.0.254/32

9.4 Use an External DHCP Server

When using a non-ThirdEye DHCP server for device provisioning, you must configure additional DHCP options beyond basic network settings. Required configurations vary by Plug-and-Play (PnP) type. `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.



Available Options	Description
□ 041 NIS Servers	Addresses c
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr

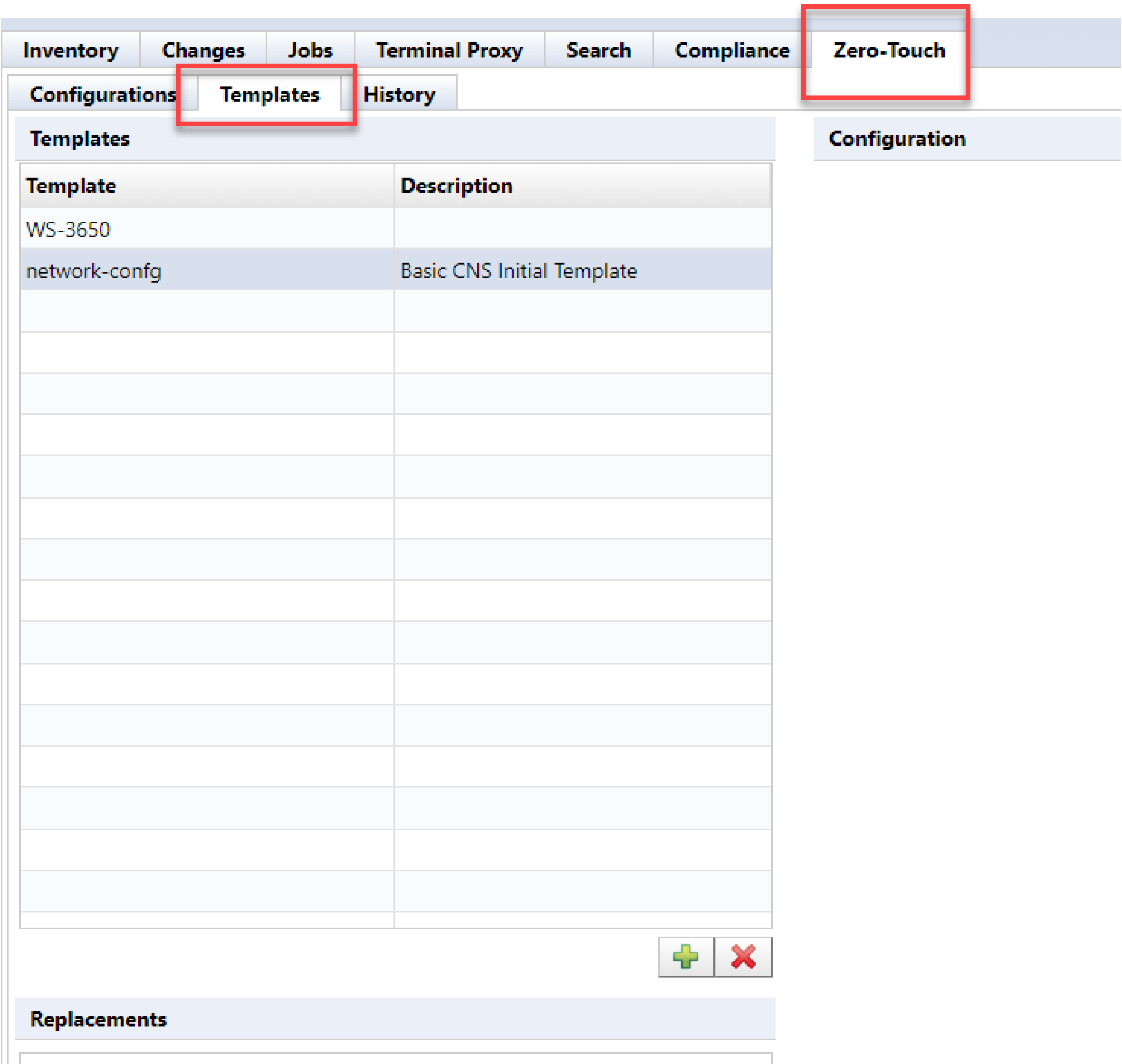
```
0000   35 41 31 44 3B 4B 43 3B   5A1D;KC;
0008   42 32 3B 49 31 39 32 2E   B2;I192.
0010   31 36 38 2E 31 30 30 2E   168.100.
0018   31 39 30                  190
```

9.5 Create a Template

In large networks, there may be multiple devices with similar configurations, but differing 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.

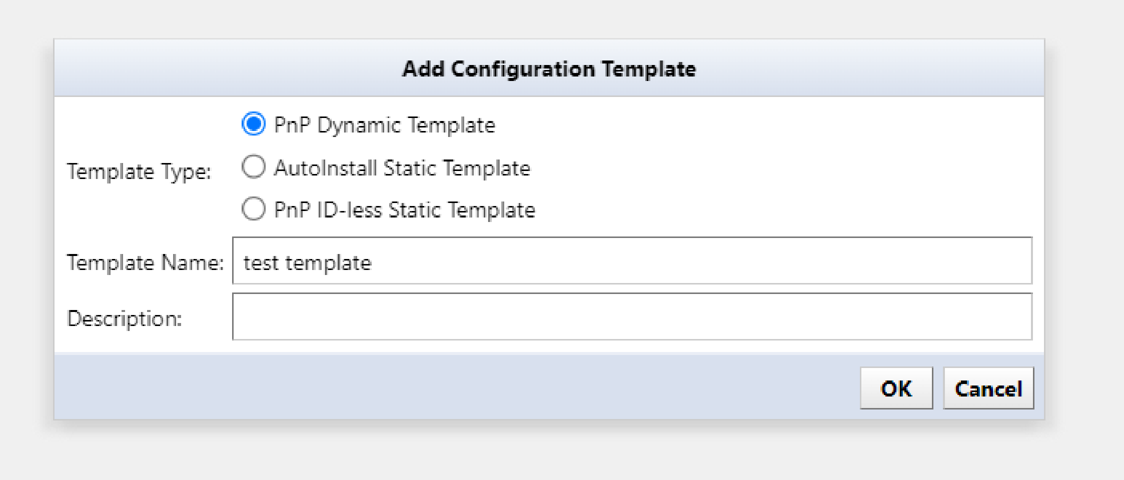
To create a template:

1. Click the [Zero-Touch] main tab > [Templates] subtab.
2. Click the + button to open the [Add Configuration Template] window.



Template	Description
WS-3650	
network-confg	Basic CNS Initial 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. Click the [OK] button.



Add Configuration Template

Template Type: ● PnP Dynamic Template ○ AutoInstall Static Template ○ PnP ID-less Static Template

Template Name: test template

Description:

The “Configuration” text area will open on the right side of the screen.

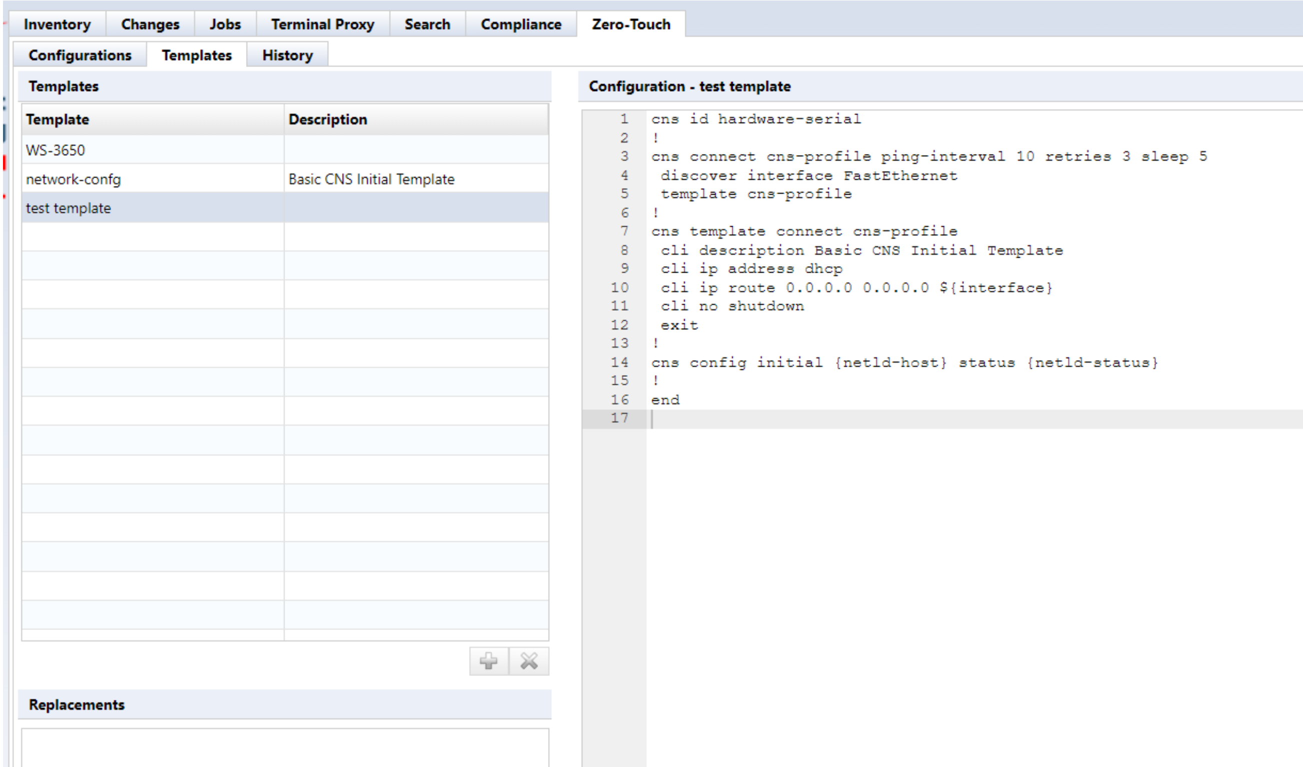
7. Enter the original configuration in this area.

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.



Template	Description
WS-3650	
network-confg	Basic CNS Initial Template
test template	

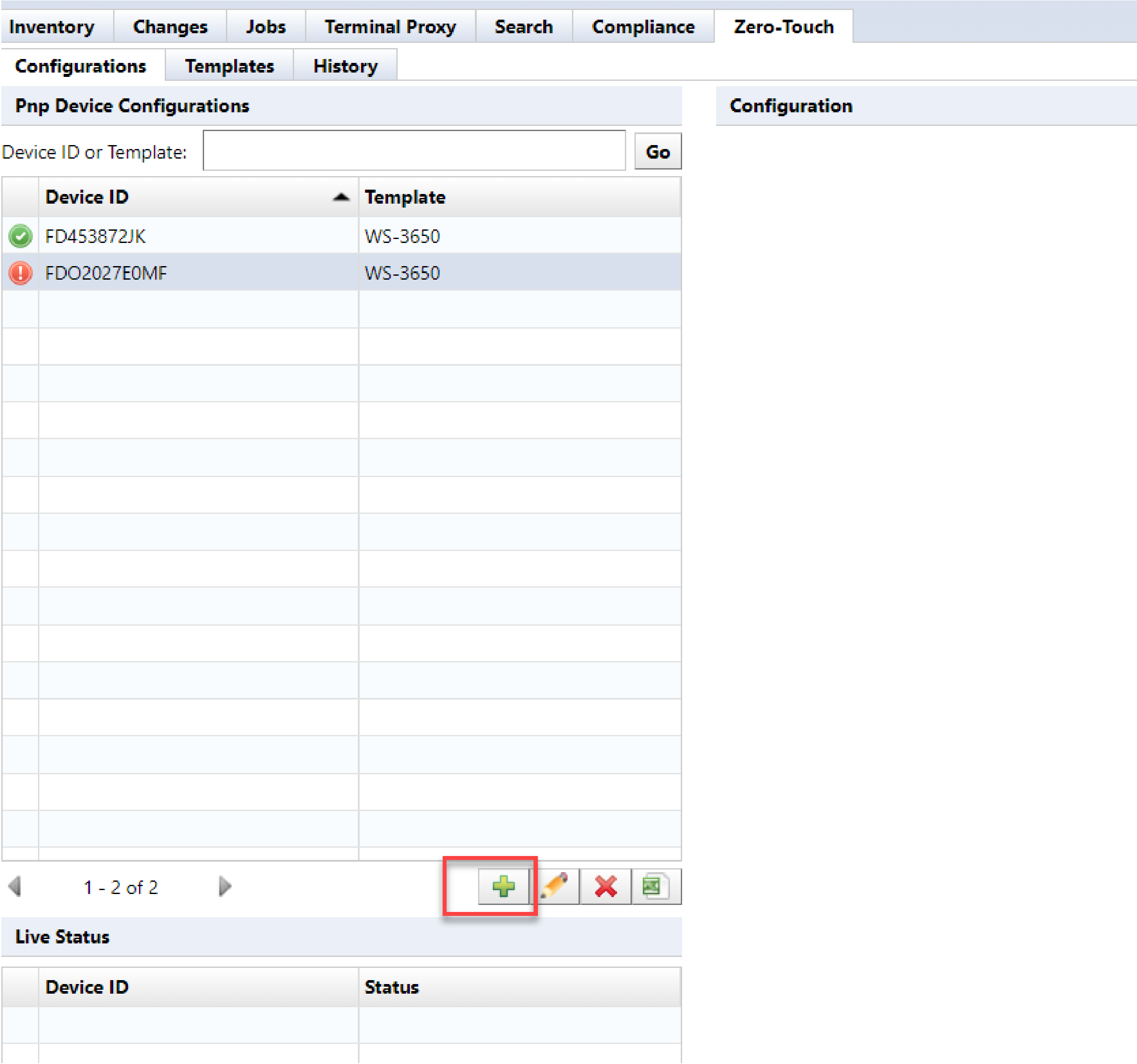
```
cns id hardware-serial
!
cns connect cns-profile ping-interval 10 retries 3 sleep 5
 discover interface FastEthernet
 template cns-profile
!
cns template connect cns-profile
 cli description Basic CNS Initial Template
 cli ip address dhcp
 cli ip route 0.0.0.0 0.0.0.0 ${interface}
 cli no shutdown
 exit
!
cns config initial {netld-host} status {netld-status}
!
end

```

9.6 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 template variable values for each target device.

1. Click the [Zero-Touch] main tab > [Configurations] subtab.

2. Click the + button to configure Zero-Touch on the device.



	Device ID	Template
✓	FD453872JK	WS-3650
!	FDO2027E0MF	WS-3650

	Device ID	Status

9.7 Import External Template Values

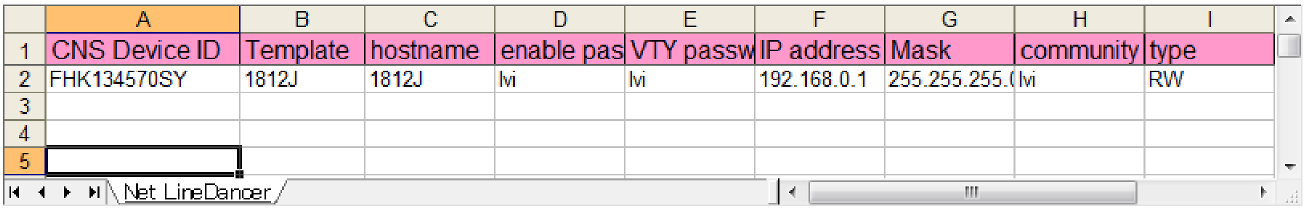
Tables written externally can be used as template values.

Follow the steps below to import Excel files:

1. Click the [Zero-Touch] main tab (Click the [Close] button if you are currently editing device data.)
2. Click the [Import] button to display the submenu.
3. Select [Export import file] or [Export template] from the submenu.

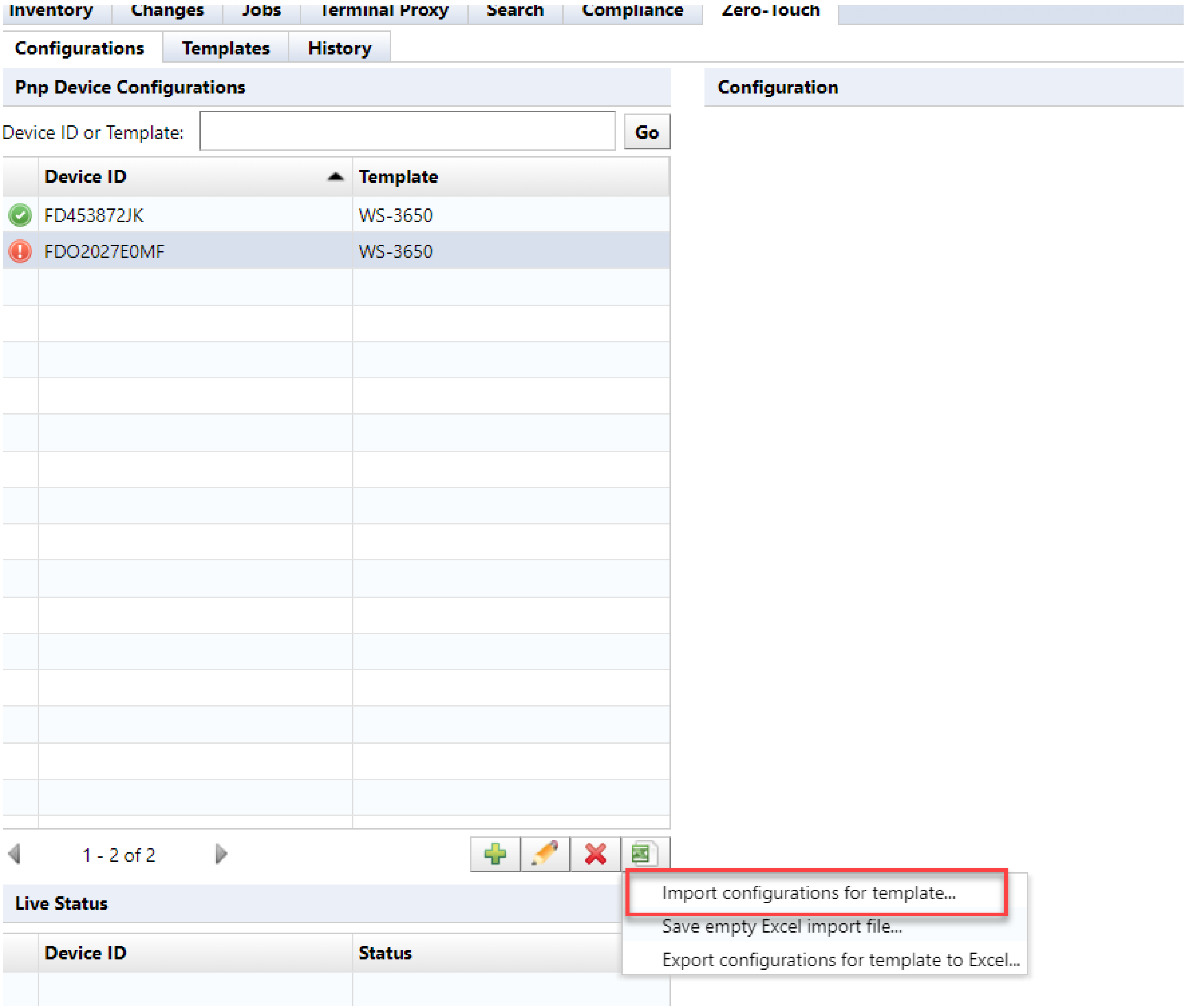
Item	Explanation
Import template	Load and register the Excel file containing variable values.
Export file for import	Outputs a blank Excel sheet where you can add values.
Export template	Outputs an Excel sheet that reflects the current variable values.

4. Edit the output file values, and enter 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									

6. Return to ThirdEye, and click the [Zero-Touch] main tab > [Configurations] subtab again.
7. Select [Import Template] from the menu that appears.



	Device ID	Template
✓	FD453872JK	WS-3650
!	FDO2027E0MF	WS-3650

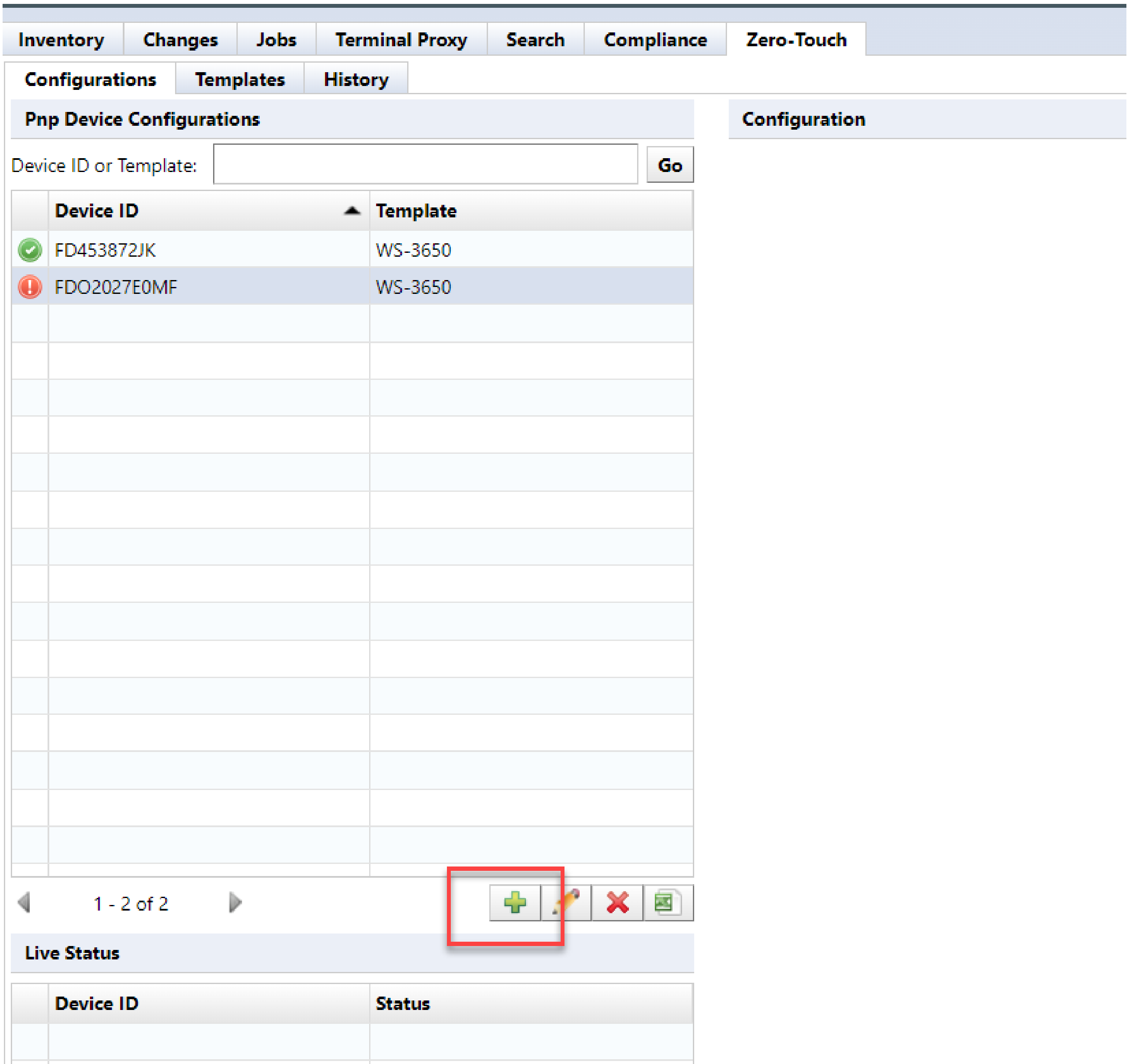
1 - 2 of 2
Import configurations for template...
Save empty Excel import file...
Export configurations for template to Excel...
Live Status
Device ID
Status

9.8 Zero-Touch Self-Recovery

Instead of sending a new configuration, Zero-Touch can send other configurations previously stored inside ThirdEye. 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] main tab > [Configurations] subtabs.
2. Click the + button on the [Configurations] subtab to open the “PnP Device Configuration” window.



Device ID or Template:

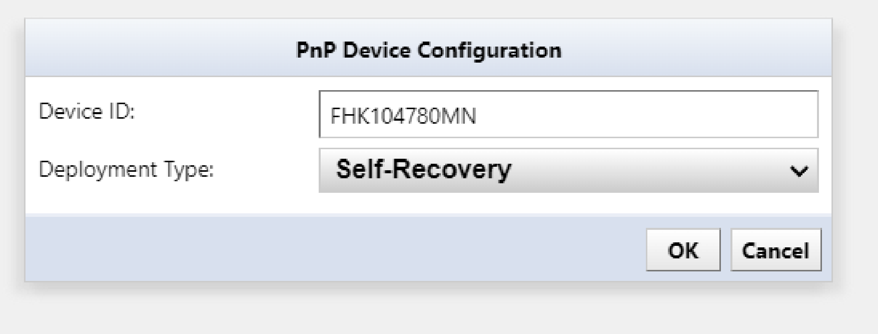
	Device ID	Template
✓	FD453872JK	WS-3650
!	FDO2027E0MF	WS-3650

1 - 2 of 2

Device ID	Status

3. Enter the necessary information in the device configuration dialog.

4. In the “PnP Device Configuration” window, select the [Self-Recovery] option in the dropdown menu as the “Deployment Type” .



PnP Device Configuration

Device ID: FHK104780MN

Deployment Type: Self-Recovery

5. Click the [OK] button to save.

The configuration data stored within ThirdEye will be rewritten to the device. There are no other differences from template delivery mode.

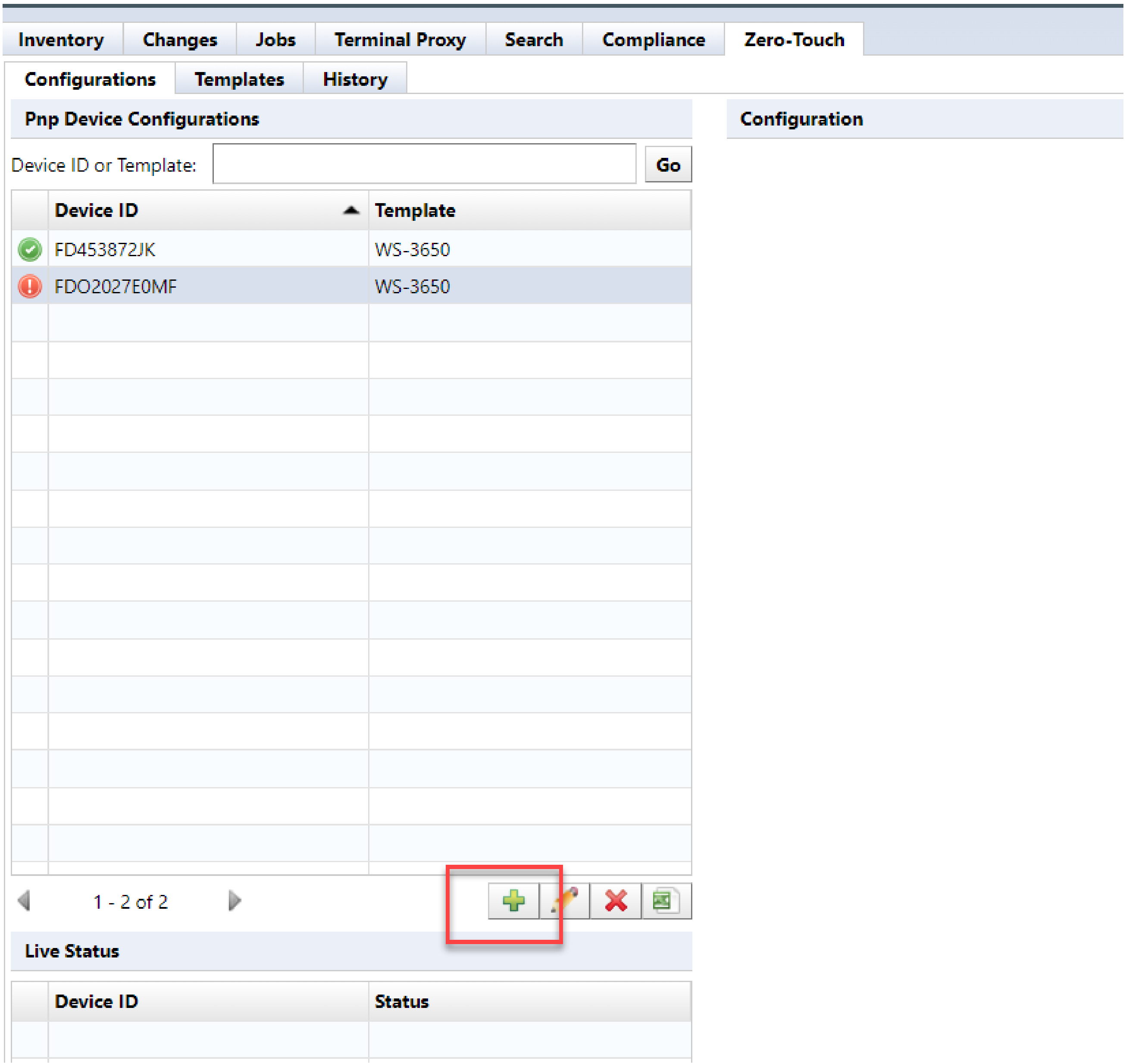
9.9 Zero-Touch Device Restore

Zero-Touch Device Restore 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 steps for Zero-Touch Device Restore are similar those for Zero-Touch Self-Recovery:

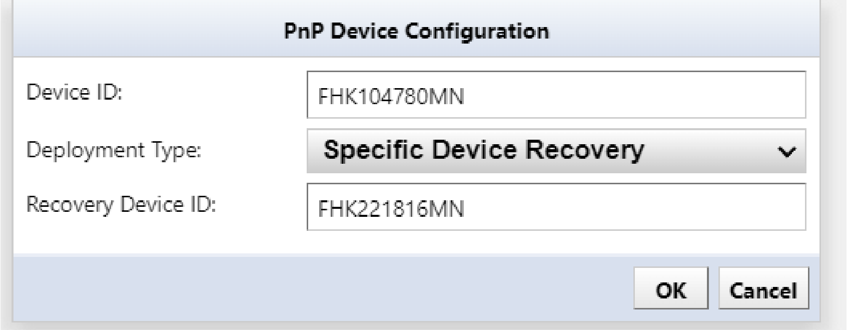
1. Click the [Configurations] subtab, and click the + button.



	Device ID	Template
✓	FD453872JK	WS-3650
!	FDO2027E0MF	WS-3650

	Device ID	Status

2. Enter the required information in the Zero-Touch “PnP Device Configuration” window.
3. Select the [Specific Device Recovery] from the dropdown menu as the “Deployment Type”.



PnP Device Configuration

Device ID: FHK104780MN

Deployment Type: Specific Device Recovery

Recovery Device ID: FHK221816MN

4. In the “Recovery Device ID” field, specify the device ID as in the first field, but enter the ID of the old device before replacement.

The configuration information for the old device in ThirdEye is then uploaded to the new device over the network. Other operations are the same as those for create a template

4. Click the [OK] button to save.

SECTION 10

DEVICE MANAGEMENT

10.1 Add Device

When adding devices to ThirdEye, you can 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.

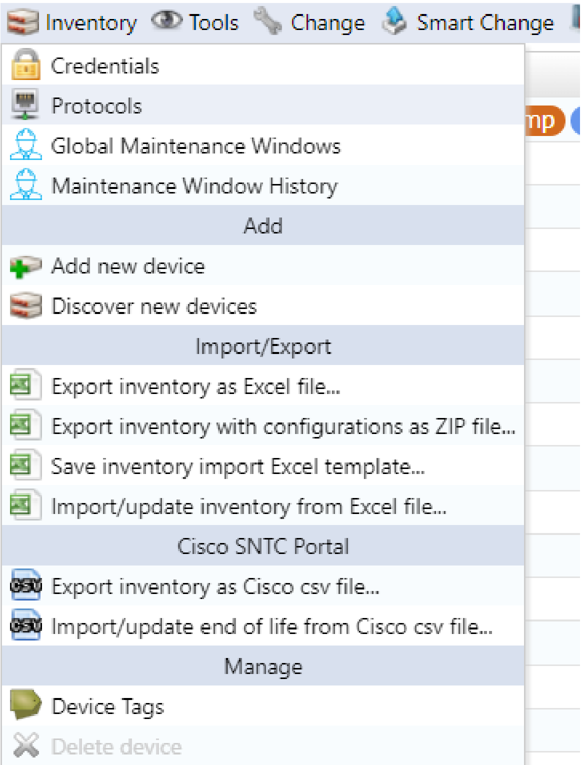
Note

When adding a device, the device does not appear on the map by default.

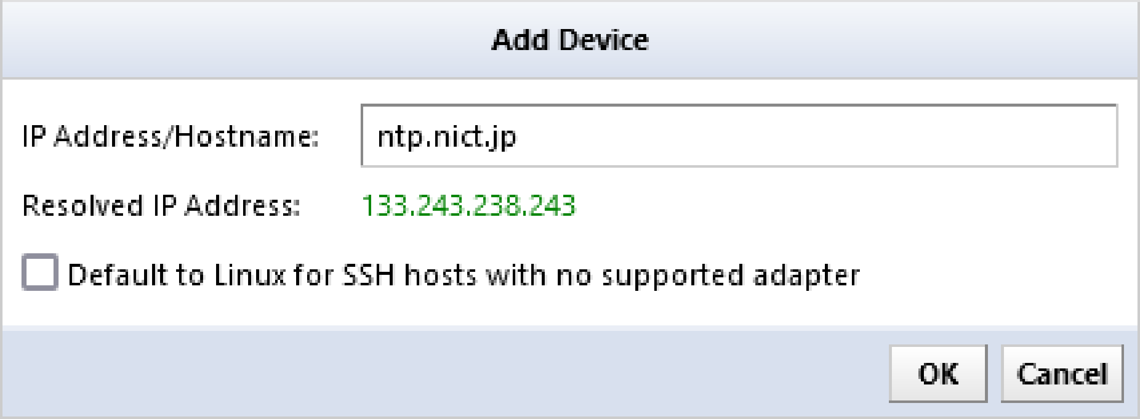
If you want your device to appear as an object on the map, you must add it.

10.2 Add New Device

1. Click the [Inventory] main tab.
2. Click the [Inventory] menu.
3. Click [Add new device] in the dropdown menu.


Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device

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



Add Device

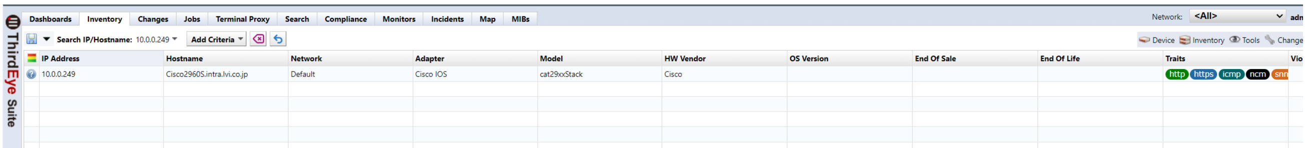
IP Address/Hostname: ntp.nict.jp

Resolved IP Address: 133.243.238.243

□ Default to Linux for SSH hosts with no supported adapter

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.



Network: <All>

Search IP/Hostname: 10.0.0.249

IP Address	Hostname	Network	Adapter	Model	HW Vendor	OS Version	End Of Sale	End Of Life	Traits	Vio
10.0.0.249	Cisco2960S.intra.lvi.co.jp	Default	Cisco IOS	cat29xxStack	Cisco				http https icmp ncm snn	

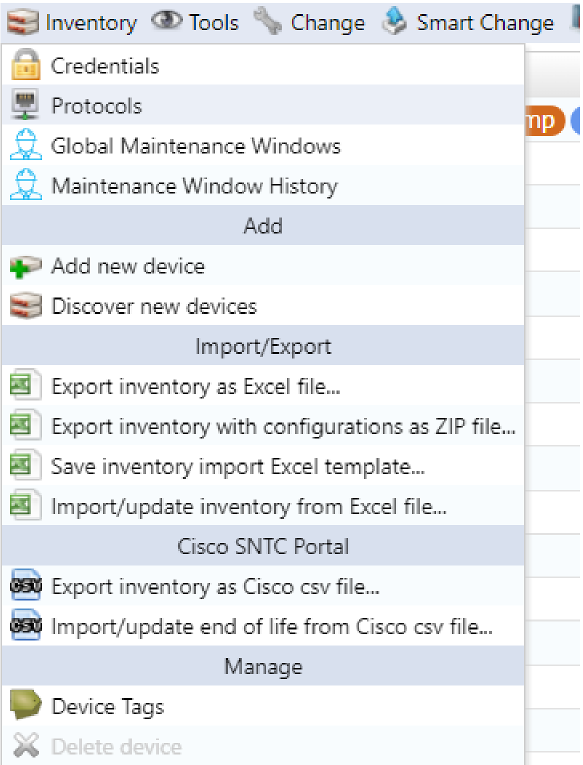
The device will be added even if it is not possible to communicate with the target IP address. However, the host name and interface information will not be obtained.

10.3 Discover Network Devices

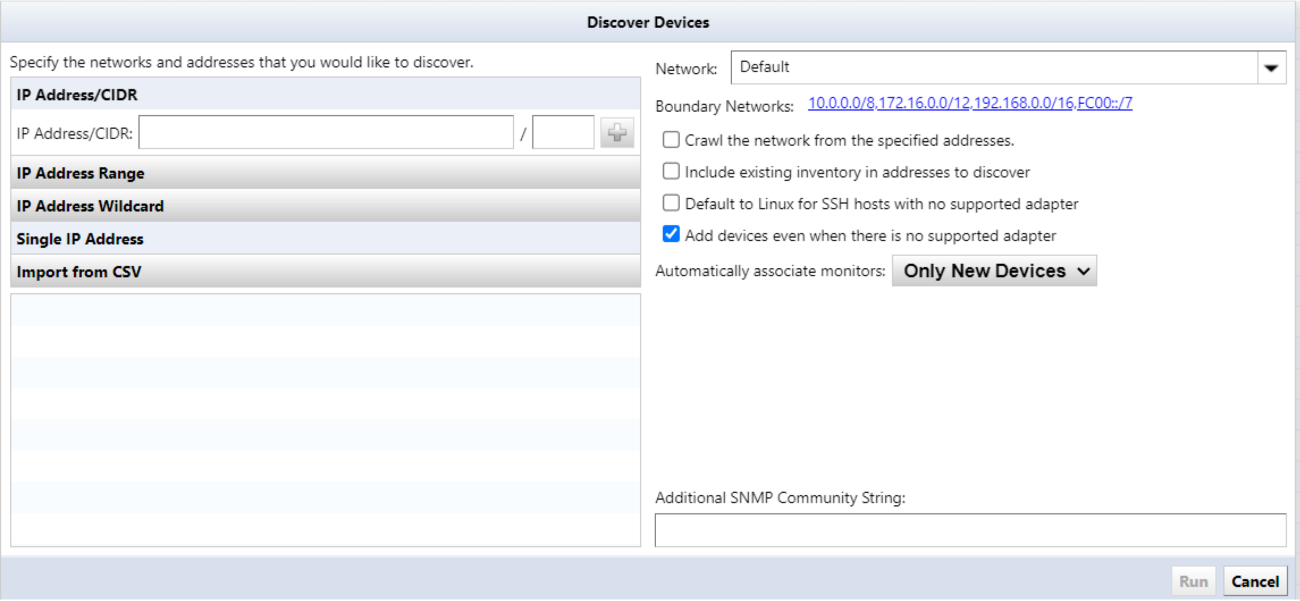
1. Click the [Inventory] main tab.

2. Click the [Inventory] menu.

3. Click [Discover new device] in the dropdown menu.


Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device

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



Discover Devices

Specify the networks and addresses that you would like to discover.

IP Address/CIDR

IP Address/CIDR: /

IP Address Range

IP Address Wildcard

Single IP Address

Import from CSV

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

☐ Crawl the network from the specified addresses.

☐ Include existing inventory in addresses to discover

☐ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

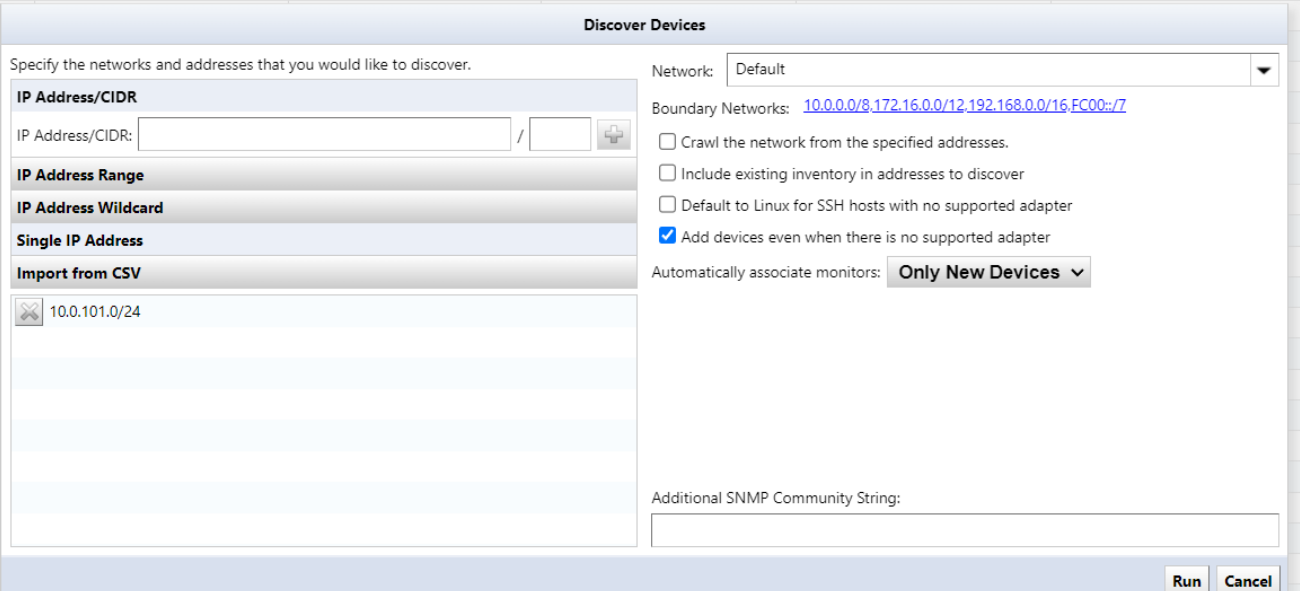
Automatically associate monitors: Only New Devices

Additional SNMP Community String:

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.

5. Click [Run].



Discover Devices

Specify the networks and addresses that you would like to discover.

IP Address/CIDR

IP Address/CIDR: [ ] / [ ]

IP Address Range

IP Address Wildcard

Single IP Address

Import from CSV

10.0.101.0/24

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

☐ Crawl the network from the specified addresses.

☐ Include existing inventory in addresses to discover

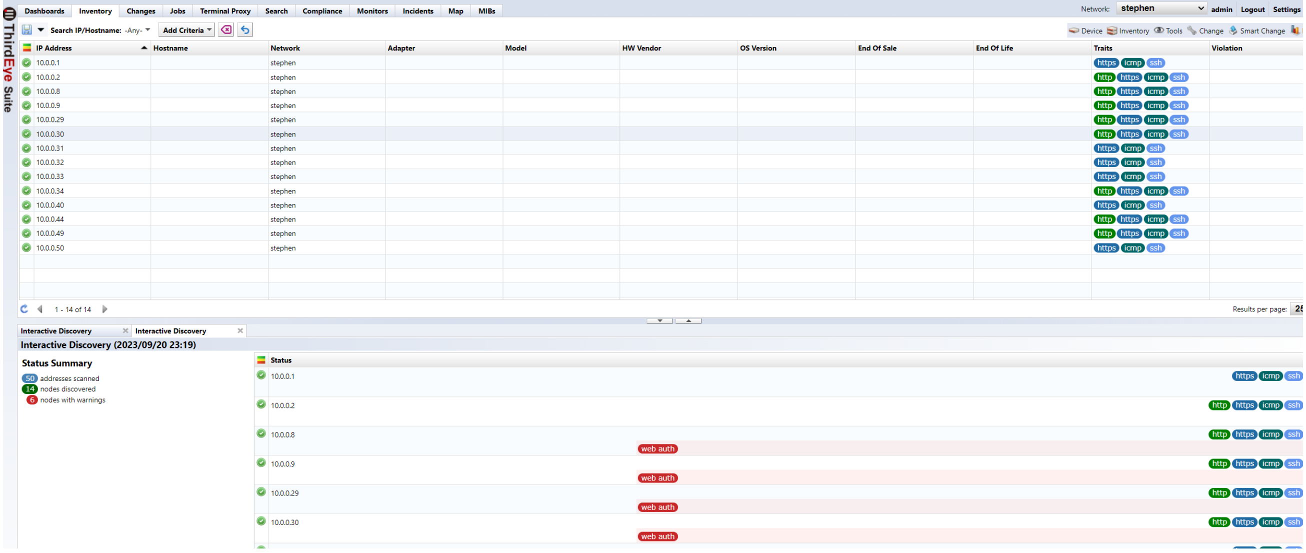
☐ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:

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



Network: stephen

Search IP/Hostname: -Any-

IP Address	Hostname	Network	Adapter	Model	HW Vendor	OS Version	End Of Sale	End Of Life	Traits	Violation
10.0.0.1		stephen							https icmp ssh	
10.0.0.2		stephen							http https icmp ssh	
10.0.0.8		stephen							http https icmp ssh	
10.0.0.9		stephen							http https icmp ssh	
10.0.0.29		stephen							http https icmp ssh	
10.0.0.30		stephen							http https icmp ssh	
10.0.0.31		stephen							https icmp ssh	
10.0.0.32		stephen							https icmp ssh	
10.0.0.33		stephen							https icmp ssh	
10.0.0.34		stephen							http https icmp ssh	
10.0.0.40		stephen							https icmp ssh	
10.0.0.44		stephen							http https icmp ssh	
10.0.0.49		stephen							http https icmp ssh	
10.0.0.50		stephen							https icmp ssh	

1 - 14 of 14

Results per page: 25

Interactive Discovery | Interactive Discovery

Interactive Discovery (2023/09/20 23:19)

Status Summary

50 addresses scanned

14 nodes discovered

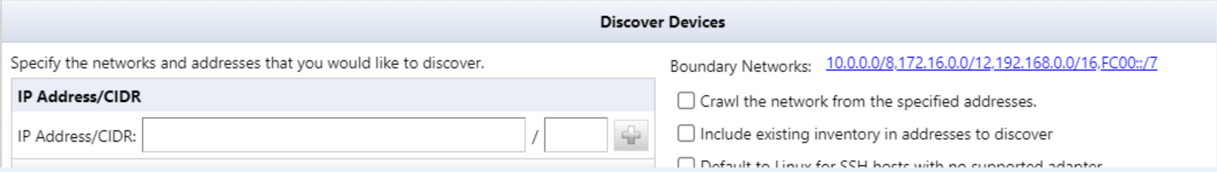
6 nodes with warnings

Status		
10.0.0.1		https icmp ssh
10.0.0.2		http https icmp ssh
10.0.0.8	web auth	http https icmp ssh
10.0.0.9	web auth	http https icmp ssh
10.0.0.29	web auth	http https icmp ssh
10.0.0.30	web auth	http https icmp ssh

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.



Discover Devices

Specify the networks and addresses that you would like to discover.

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

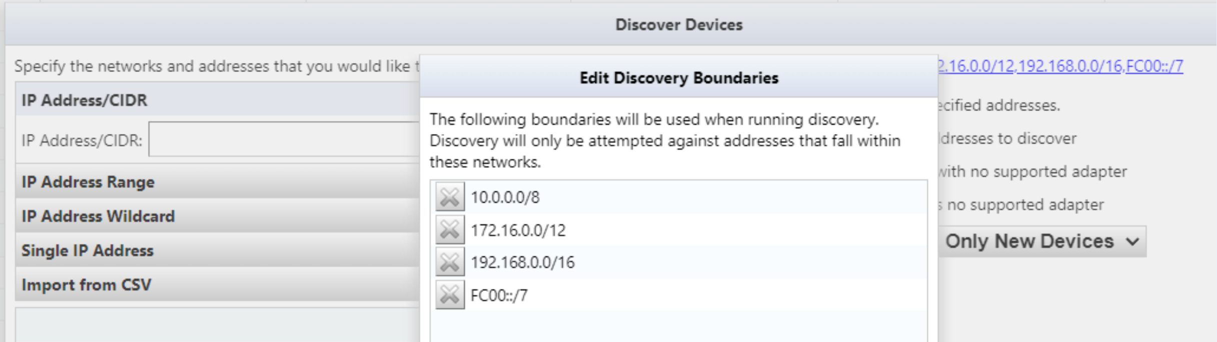
IP Address/CIDR

IP Address/CIDR: /

□ Crawl the network from the specified addresses.

□ Include existing inventory in addresses to discover

□ Default to Linux for SSH hosts with no supported adapter



Discover Devices

Specify the networks and addresses that you would like t

IP Address/CIDR

IP Address/CIDR:

IP Address Range

IP Address Wildcard

Single IP Address

Import from CSV

Edit Discovery Boundaries

The following boundaries will be used when running discovery. Discovery will only be attempted against addresses that fall within these networks.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- FC00::/7

2.16.0.0/12,192.168.0.0/16,FC00::/7

cified addresses.

dresses to discover

with no supported adapter

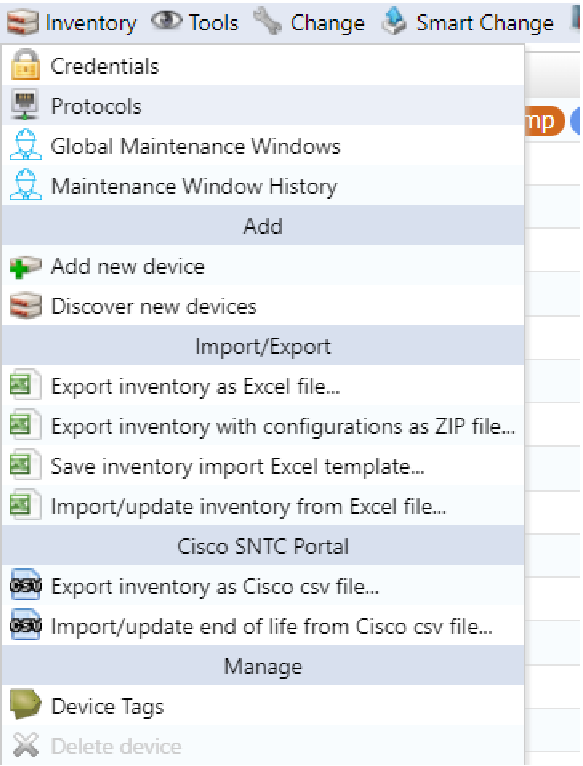
s no supported adapter

Only New Devices

10.4 Import Device Excel Template

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] main tab.
2. Click the [Inventory] menu.
3. Click [Save inventory import Excel Template] buttons.

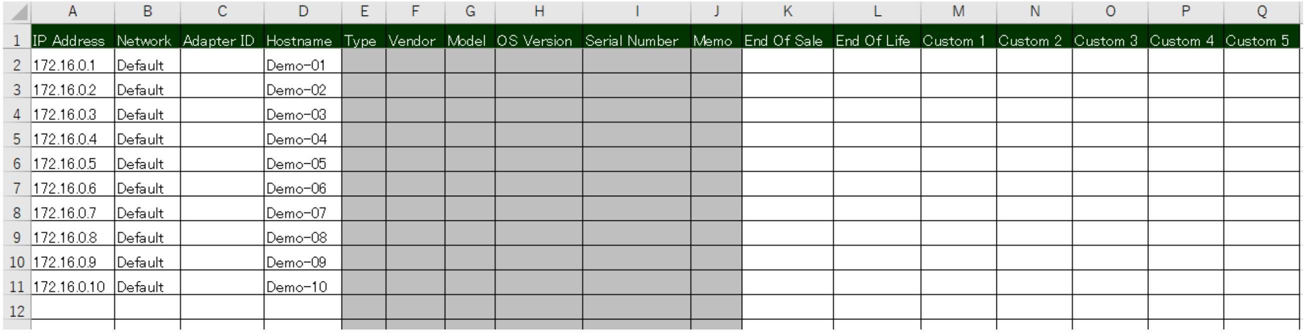

Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device

The file opening screen will be displayed.

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

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

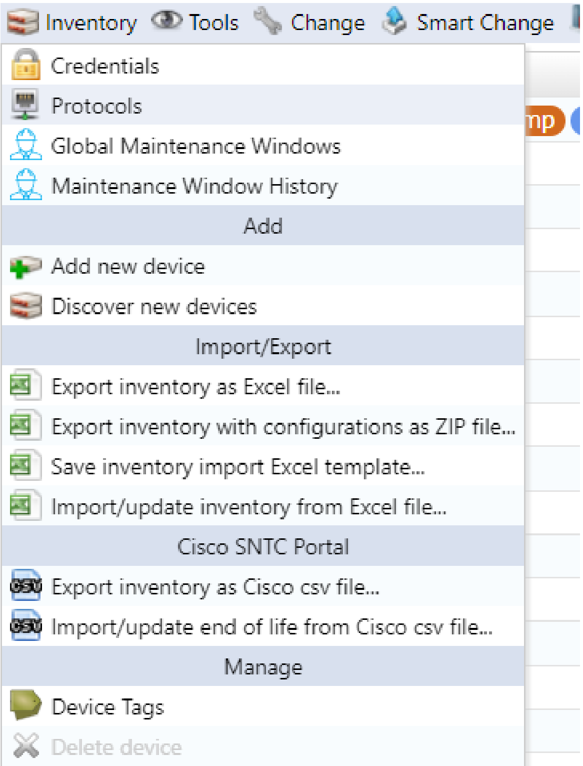
5. Edit the saved file, enter information in the following fields, and overwrite and save.



	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																	

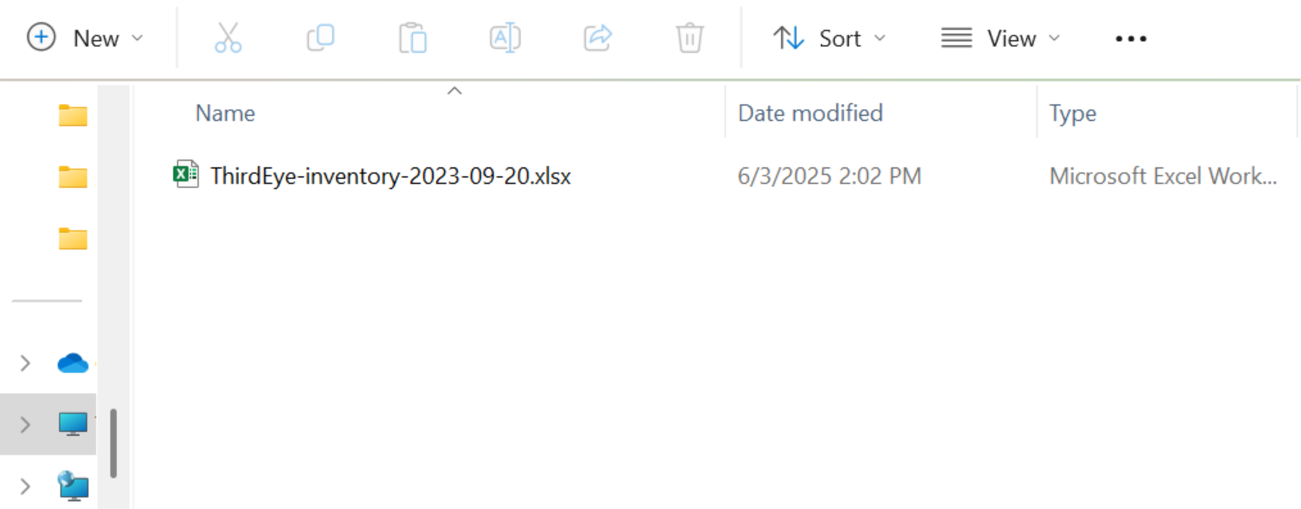
Item	Explanation	Requirements	Input example
IP Address	Enter the device's IP address.	required	192.168.1.10
Network	Select the network name to which you want to add the device.	required	Default
Adapter ID	Select your device's adapter. (In the current version, there is no need to specify this item.)	-	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".	-	

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


Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device

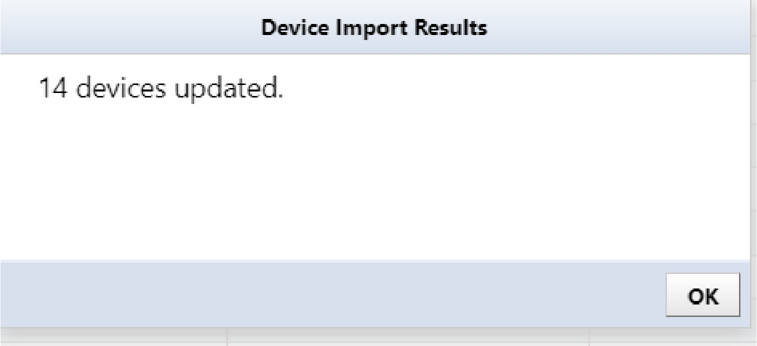
A file selection dialog will be displayed.

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



Name	Date modified	Type
ThirdEye-inventory-2023-09-20.xlsx	6/3/2025 2:02 PM	Microsoft Excel Work...

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



Device Import Results

14 devices updated.

10.5 Network Restriction

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. It allows organizations to host multiple customers on a single system while maintaining security and data separation.

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.

10.5.1 Device Groups

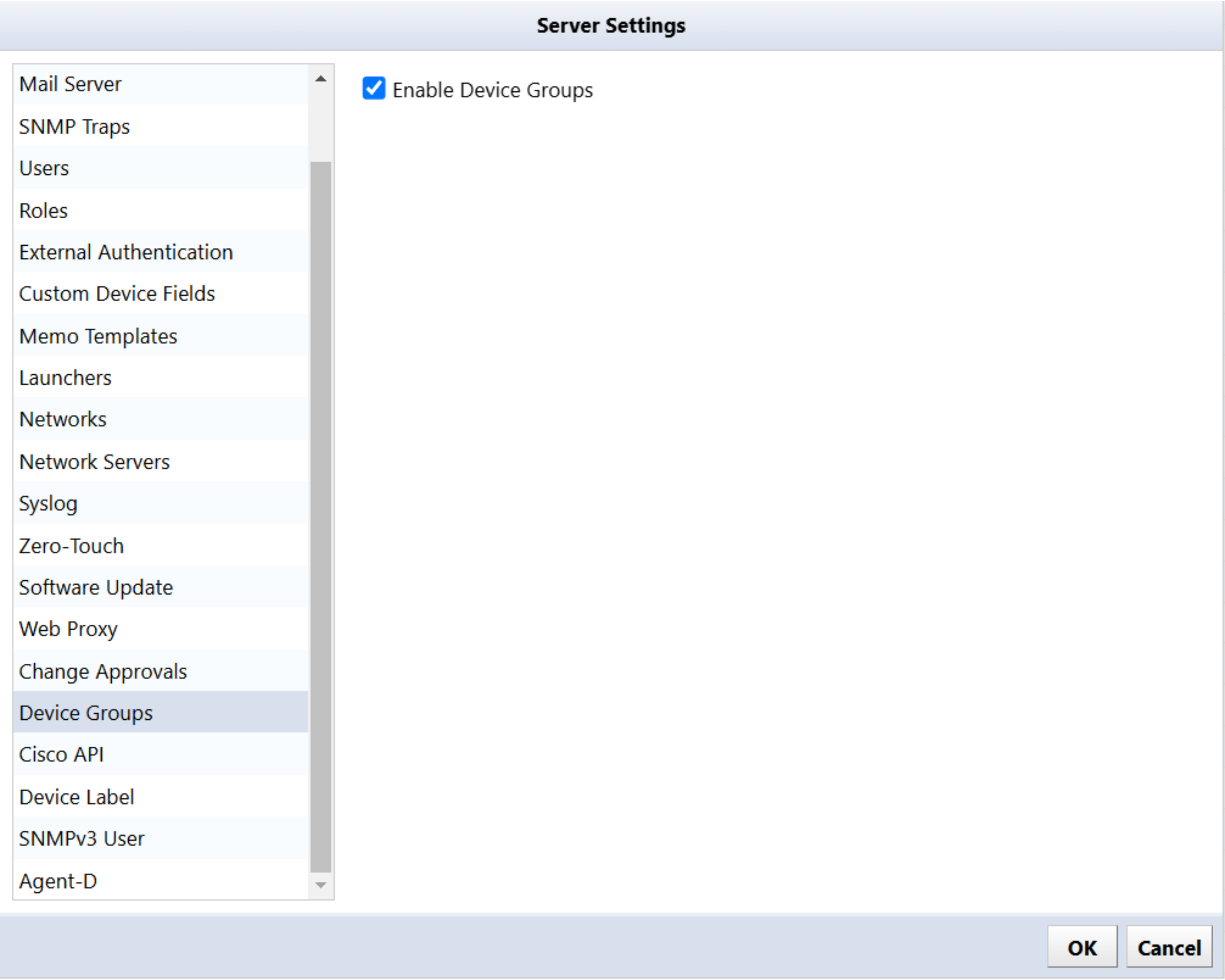
A Device Group is a collection of devices grouped together for easier administration and monitoring. Here are some key points:

- **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.

10.5.2 Configure Device Groups

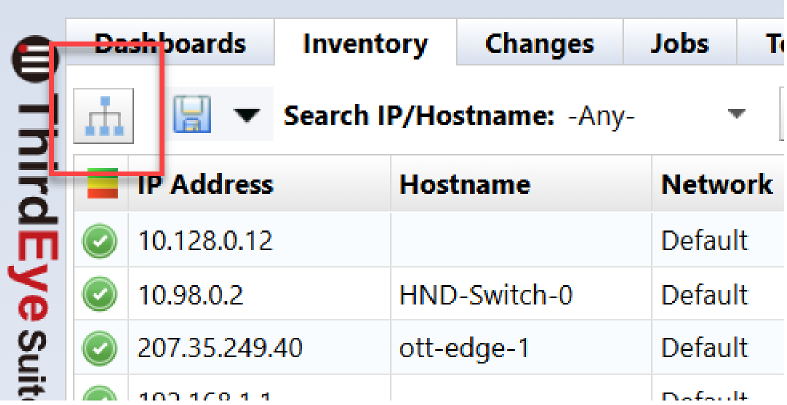
To setup and configure Device Groups:

1. Click [Settings] in the Global Menu.
2. Click [Server Settings]
3. Click [Device Groups] in the left sidepanel.
4. Check “Enable Device Groups”, and then [OK].



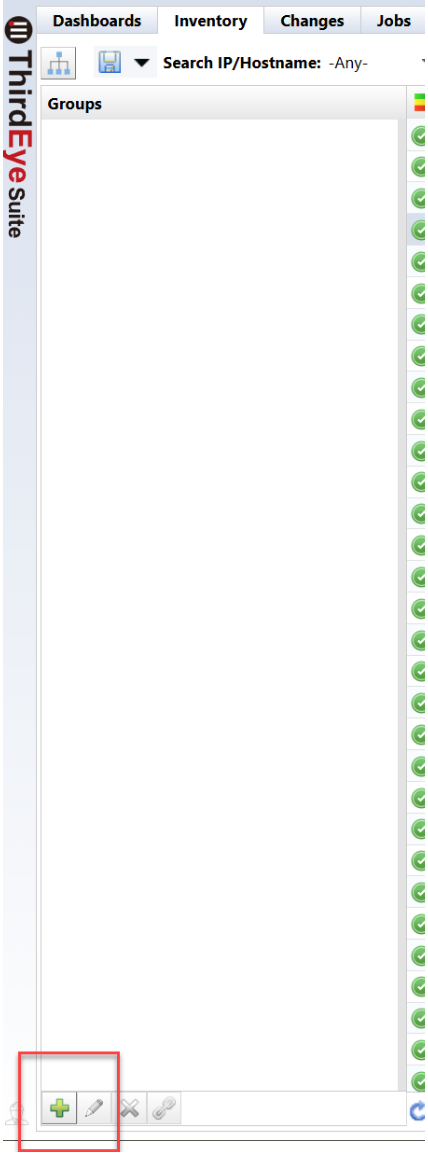
☑ Enable Device Groups

5. Click the [Inventory] main tab, then click the button in the top left corner.



	IP Address	Hostname	Network
✓	10.128.0.12		Default
✓	10.98.0.2	HND-Switch-0	Default
✓	207.35.249.40	ott-edge-1	Default
✓	192.168.1.1		Default

6. Click the + button in the bottom left corner.

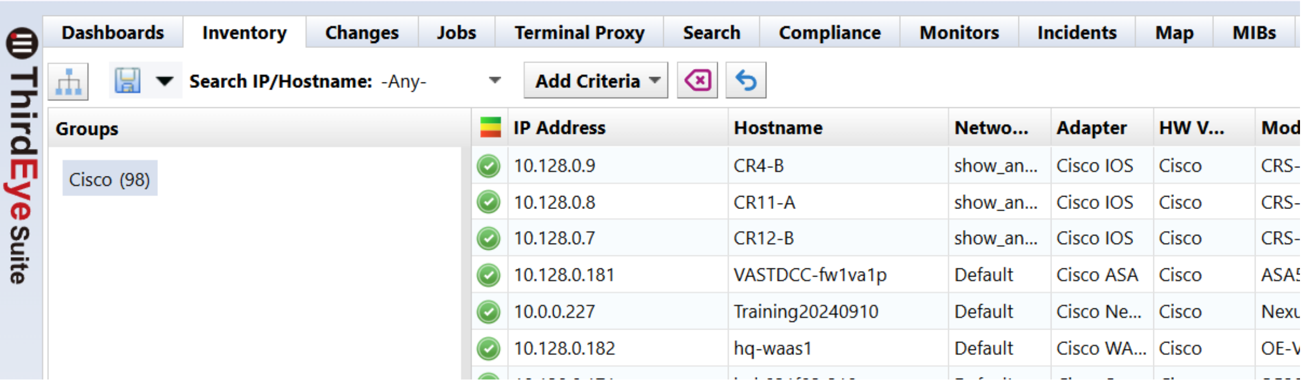


7. In the popup window, enter a name for the grouping (“Cisco” in the screenshot below).

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.

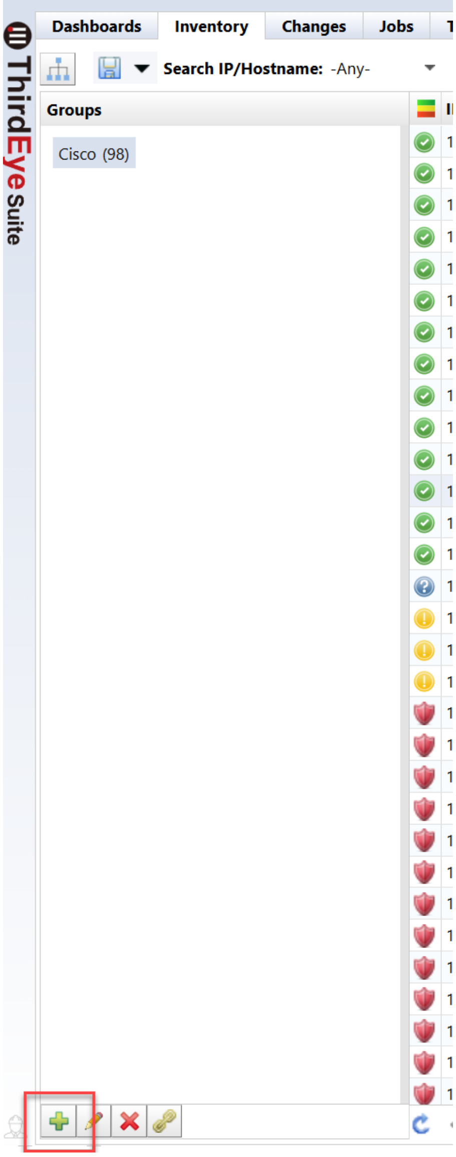
8. In the [Groups] sidebar, click on the vendor name, and those devices will appear in the [Inventory] tab.



Cisco (98)

	IP Address	Hostname	Netwo...	Adapter	HW V...	Mod
✓	10.128.0.9	CR4-B	show_an...	Cisco IOS	Cisco	CRS-
✓	10.128.0.8	CR11-A	show_an...	Cisco IOS	Cisco	CRS-
✓	10.128.0.7	CR12-B	show_an...	Cisco IOS	Cisco	CRS-
✓	10.128.0.181	VASTDCC-fw1va1p	Default	Cisco ASA	Cisco	ASA5
✓	10.0.0.227	Training20240910	Default	Cisco Ne...	Cisco	Nexu
✓	10.128.0.182	hq-waas1	Default	Cisco WA...	Cisco	OE-V

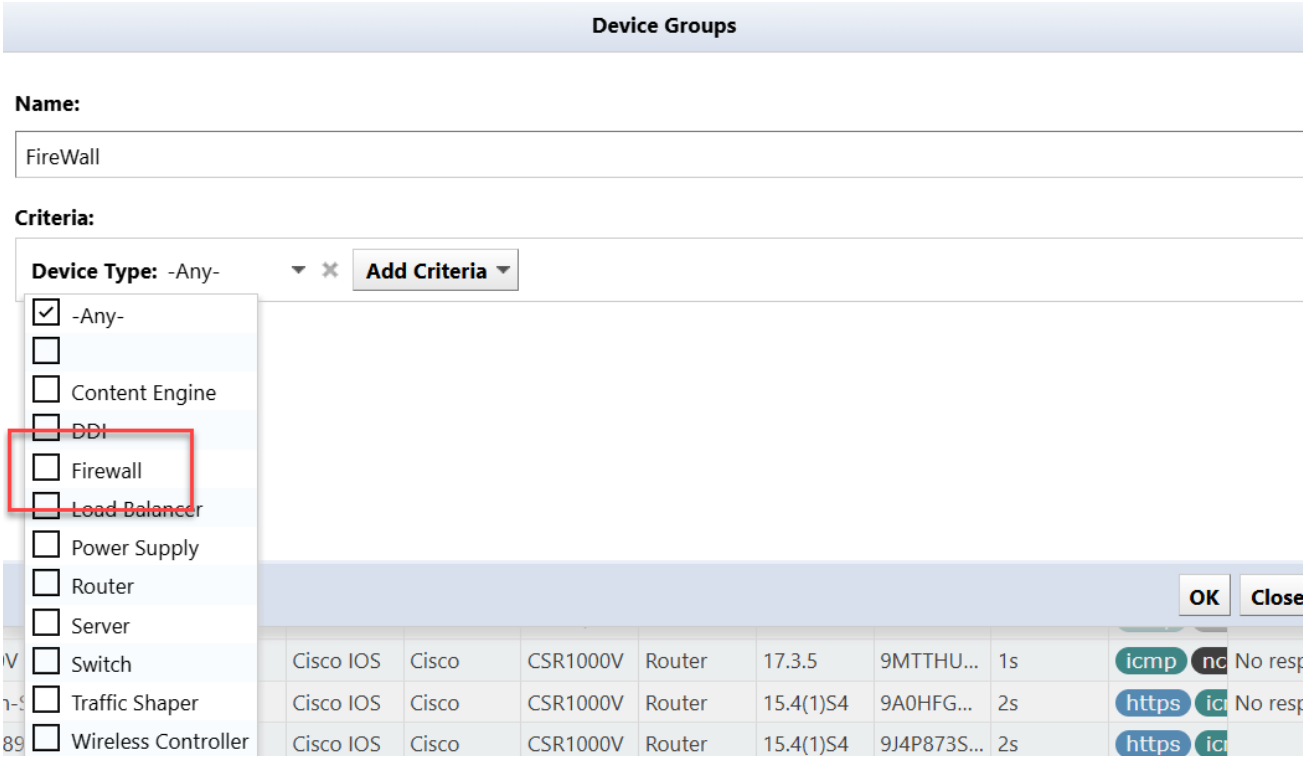
9. To make subgroups, click on the vendor name, and click on the ✚ at the bottom of the page.



10. Enter a “Name” for the subgroup, (for example “FireWall” in the example below).

11. In the [Criteria] > [Device Type] left sidebar, select your new subgroup (“FireWall” in the example below).

12. Click [OK].



Device Groups

Name:

FireWall

Criteria:

Device Type: -Any-

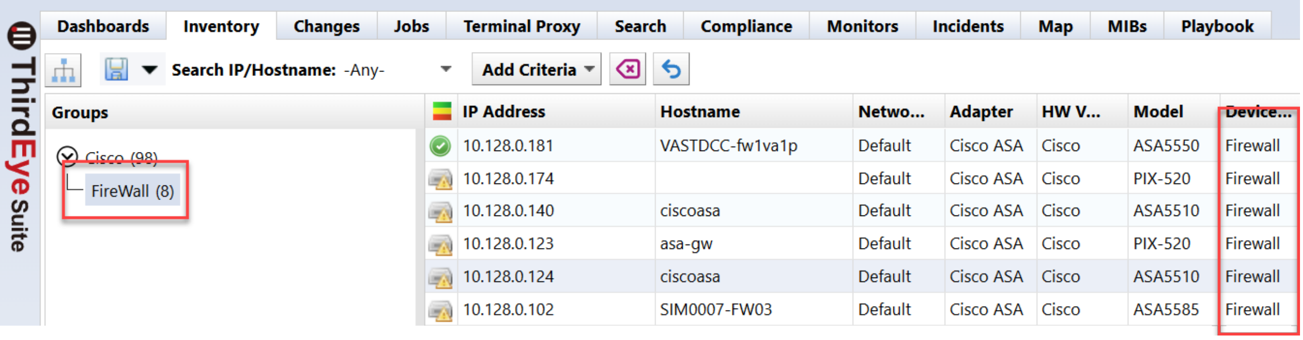
Add Criteria

- ☑ -Any-
- □
- □ Content Engine
- □ DDI
- □ Firewall
- □ Load Balancer
- □ Power Supply
- □ Router
- □ Server
- □ Switch
- □ Traffic Shaper
- □ Wireless Controller

OK | Close

V	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU...	1s	icmp nc	No resp
ı-ś	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFG...	2s	https ici	No resp
89	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873S...	2s	https ici	

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



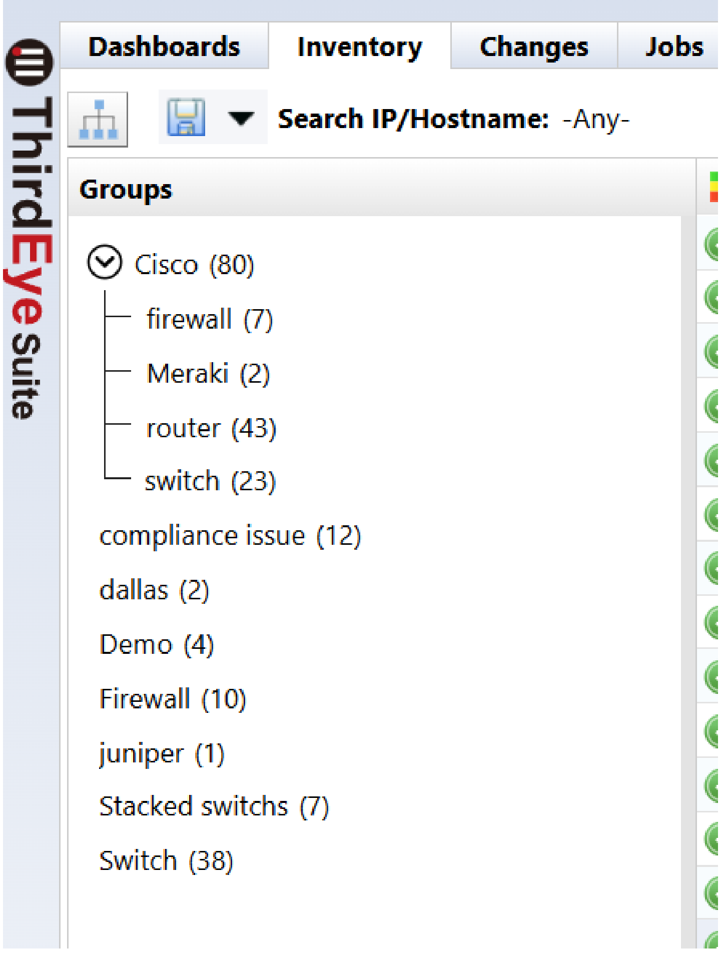
Search IP/Hostname: -Any-

Groups

- Cisco (98)
  - FireWall (8)

	IP Address	Hostname	Netwo...	Adapter	HW V...	Model	Device...
✓	10.128.0.181	VASTDCC-fw1va1p	Default	Cisco ASA	Cisco	ASA5550	Firewall
⚠	10.128.0.174		Default	Cisco ASA	Cisco	PIX-520	Firewall
⚠	10.128.0.140	ciscoasa	Default	Cisco ASA	Cisco	ASA5510	Firewall
⚠	10.128.0.123	asa-gw	Default	Cisco ASA	Cisco	PIX-520	Firewall
⚠	10.128.0.124	ciscoasa	Default	Cisco ASA	Cisco	ASA5510	Firewall
⚠	10.128.0.102	SIM0007-FW03	Default	Cisco ASA	Cisco	ASA5585	Firewall

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



Cisco (80)
- firewall (7)
- Meraki (2)
- router (43)
- switch (23)

compliance issue (12)

dallas (2)

Demo (4)

Firewall (10)

juniper (1)

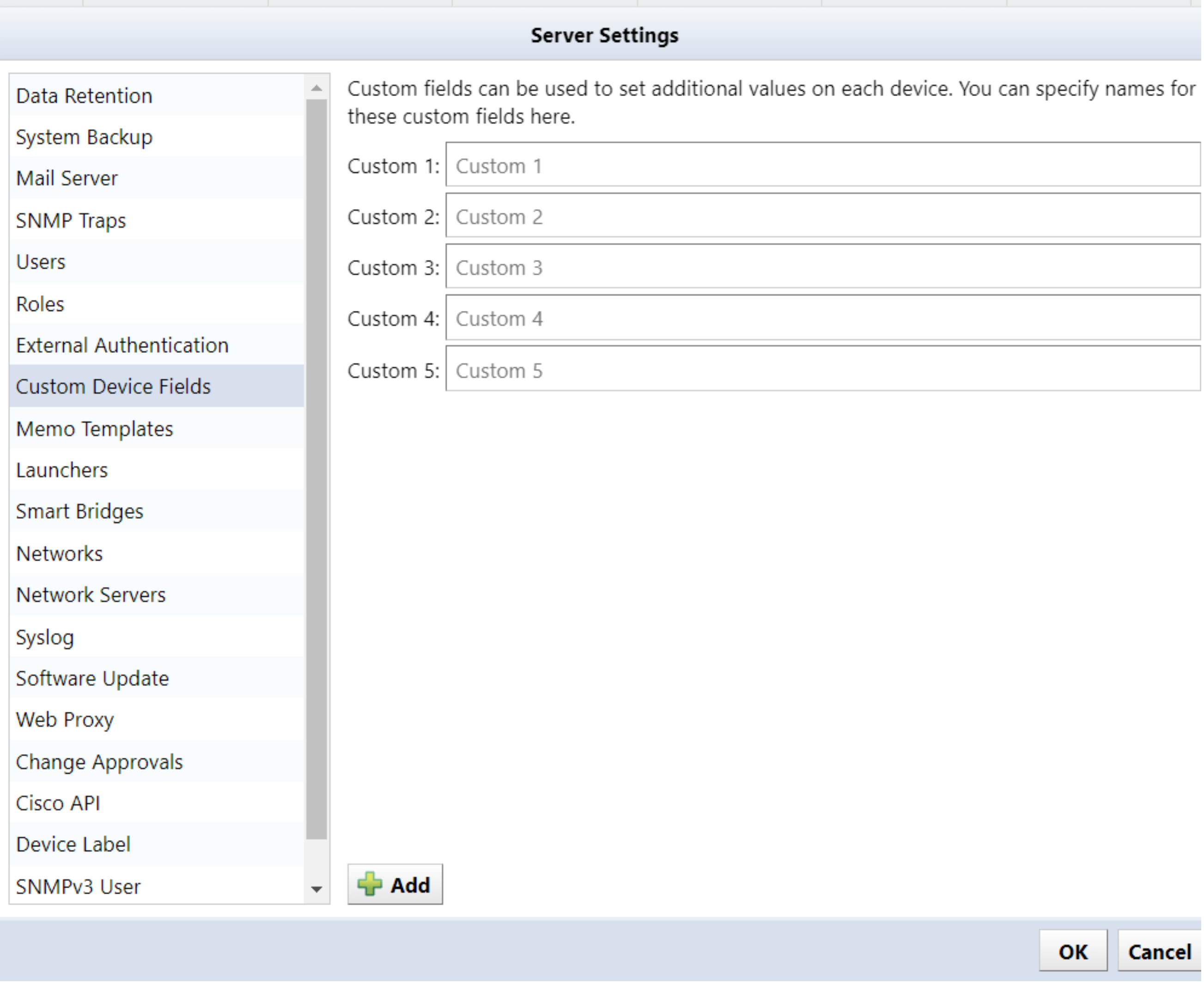
Stacked switchs (7)

Switch (38)

10.6 Custom Device Fields

The Custom Device field allows you to add/change column names in device tabs, and use them in searches.

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



Custom fields can be used to set additional values on each device. You can specify names for these custom fields here.

Custom 1: Custom 1

Custom 2: Custom 2

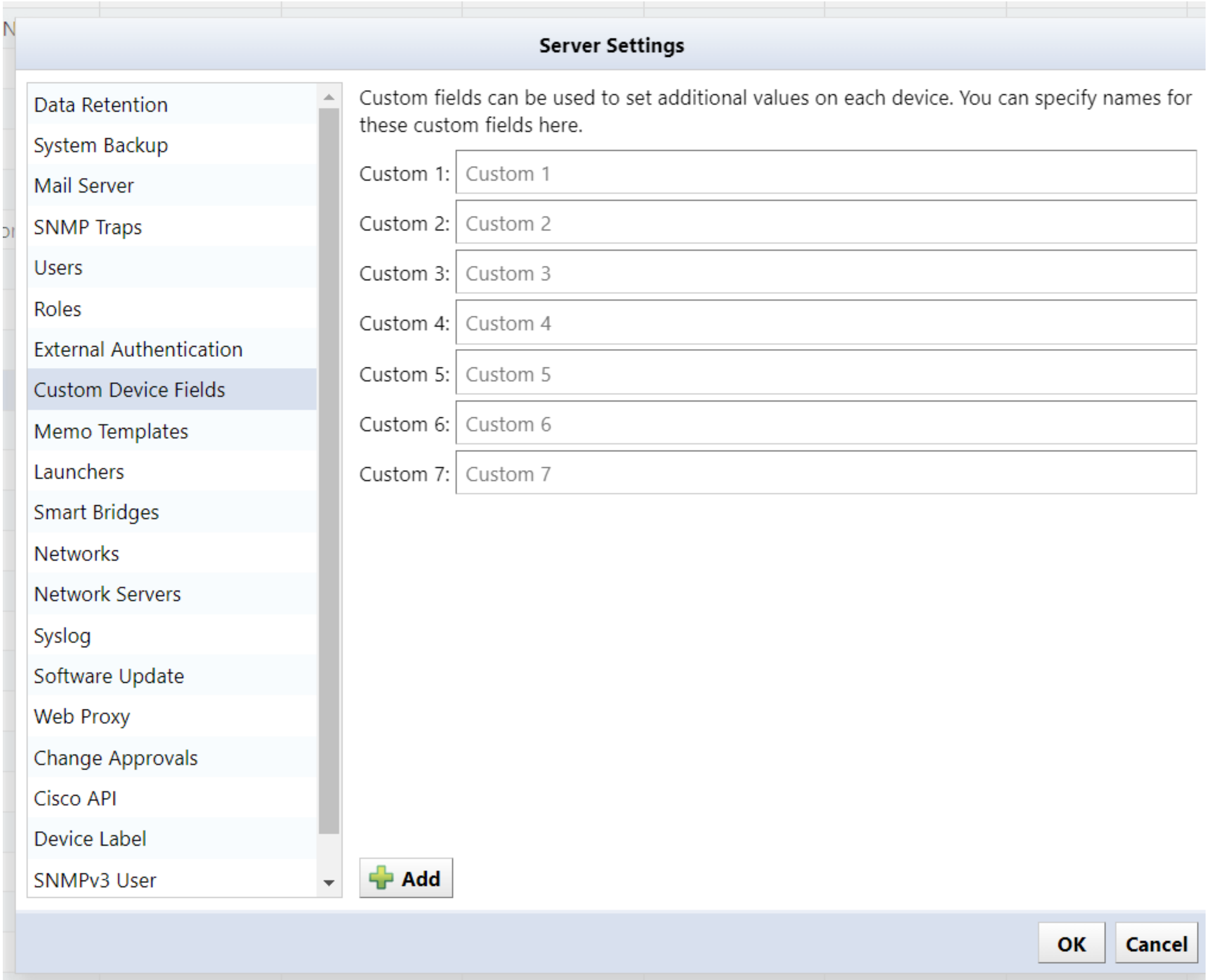
Custom 3: Custom 3

Custom 4: Custom 4

Custom 5: Custom 5

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.



Custom fields can be used to set additional values on each device. You can specify names for these custom fields here.

Custom 1: Custom 1

Custom 2: Custom 2

Custom 3: Custom 3

Custom 4: Custom 4

Custom 5: Custom 5

Custom 6: Custom 6

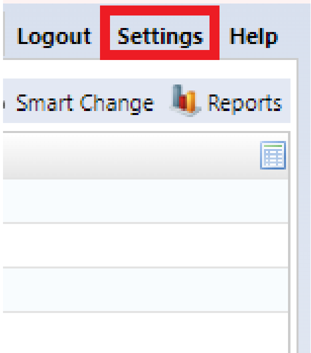
Custom 7: Custom 7

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

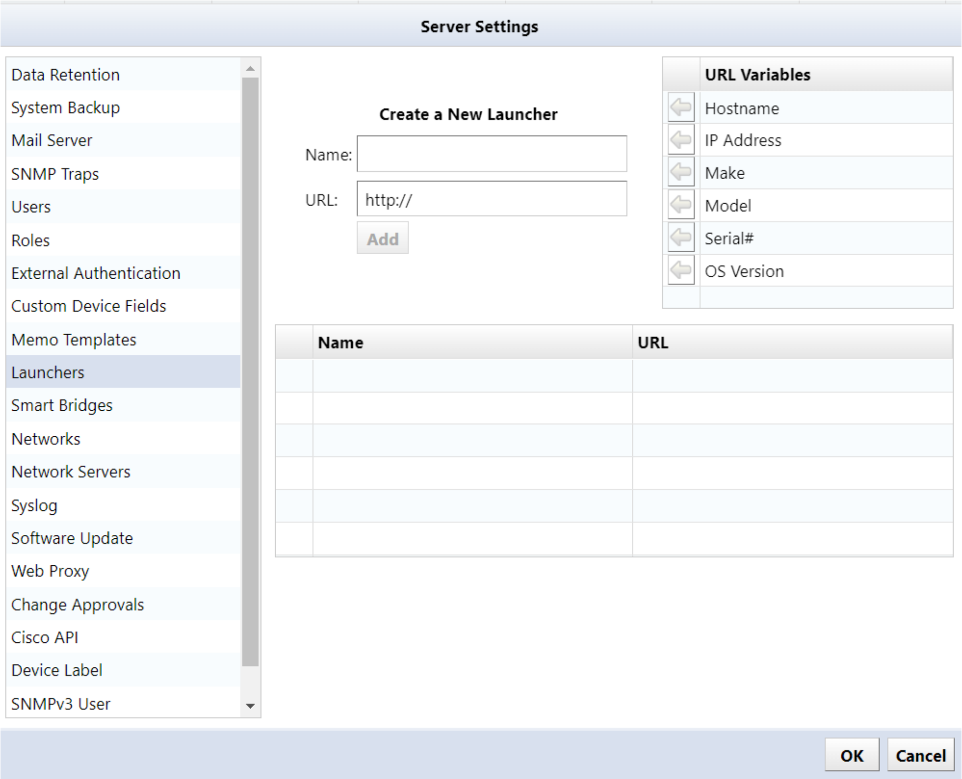
10.7 Add Specific URL to Right-Click menu

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 [Launchers] in the left side panel.



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: Hardware Vendor

Explanation: Quoting the hardware vendor 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.

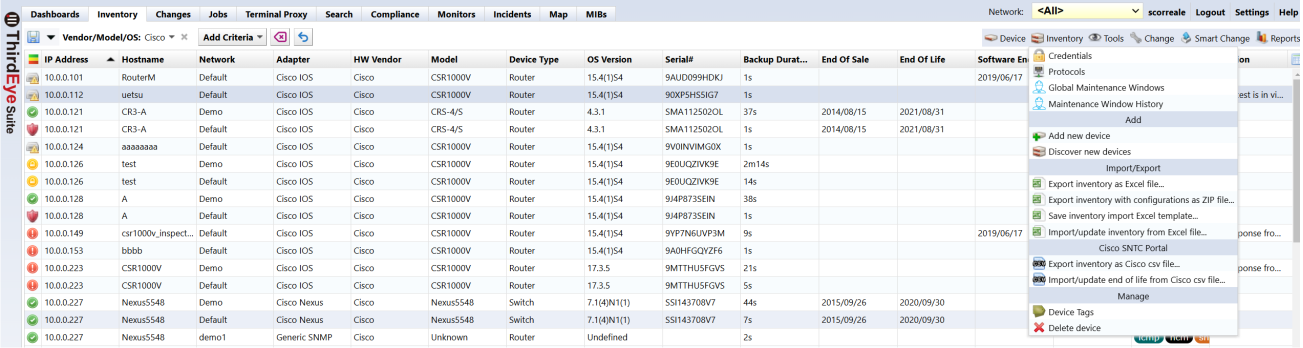
Example: `http://{device.osVersion}`

4. Click [OK].

10.8 Delete Device

1. Select the device you want to delete on the [Inventory] tab. Multiple selections are possible.

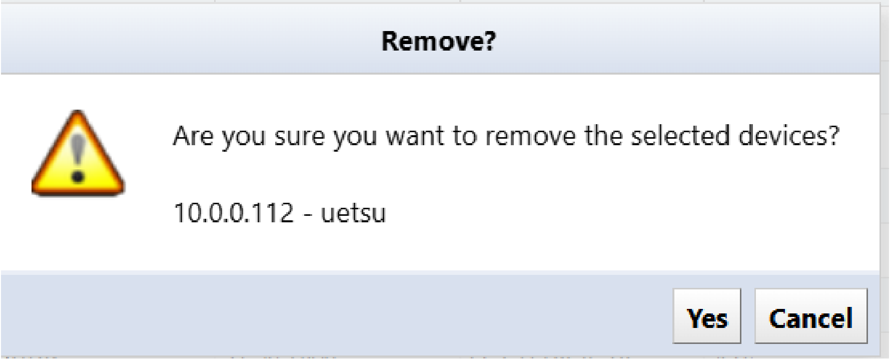
2. With the device selected, click [Inventory] in the Menu Bar > [Delete Device].



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software En	on
10.0.0.101	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	1s			2019/06/17	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	1s				est is in vi...
10.0.0.121	CR3-A	Demo	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	37s	2014/08/15	2021/08/31		
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31		
10.0.0.124	aaaaaaaa	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	1s				
10.0.0.126	test	Demo	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	2m14s				
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	14s				
10.0.0.128	A	Demo	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	38s				
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	1s				
10.0.0.149	csr1000v_inspect...	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9YP7N6UVP3M	9s			2019/06/17	ponse fro...
10.0.0.153	bbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFGQYZF6	1s				
10.0.0.223	CSR1000V	Demo	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	21s				ponse fro...
10.0.0.223	CSR1000V	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	5s				
10.0.0.227	Nexus5548	Demo	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	44s	2015/09/26	2020/09/30		
10.0.0.227	Nexus5548	Default	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	7s	2015/09/26	2020/09/30		
10.0.0.227	Nexus5548	demo1	Generic SNMP	Cisco	Unknown	Router	Undefined		2s				

A confirmation message will be displayed.

3. Click [Yes].



Are you sure you want to remove the selected devices?

10.0.0.112 - uetsu

SECTION 11

CLOUD DEVICES

ThirdEye supports cloud device management through dedicated credential management and discovery workflows. This section covers ThirdEye's cloud device support for features such as Credential Handling, Device Discovery, and Rediscovery.

11.1 Meraki

11.1.1 Cloud Credential Settings

As cloud devices mainly use cloud accounts to access devices, a new cloud credential type was introduced to already existing dynamic and static credentials. If you are a provider, you should configure the following items so that the credential/access token can access the cloud account:

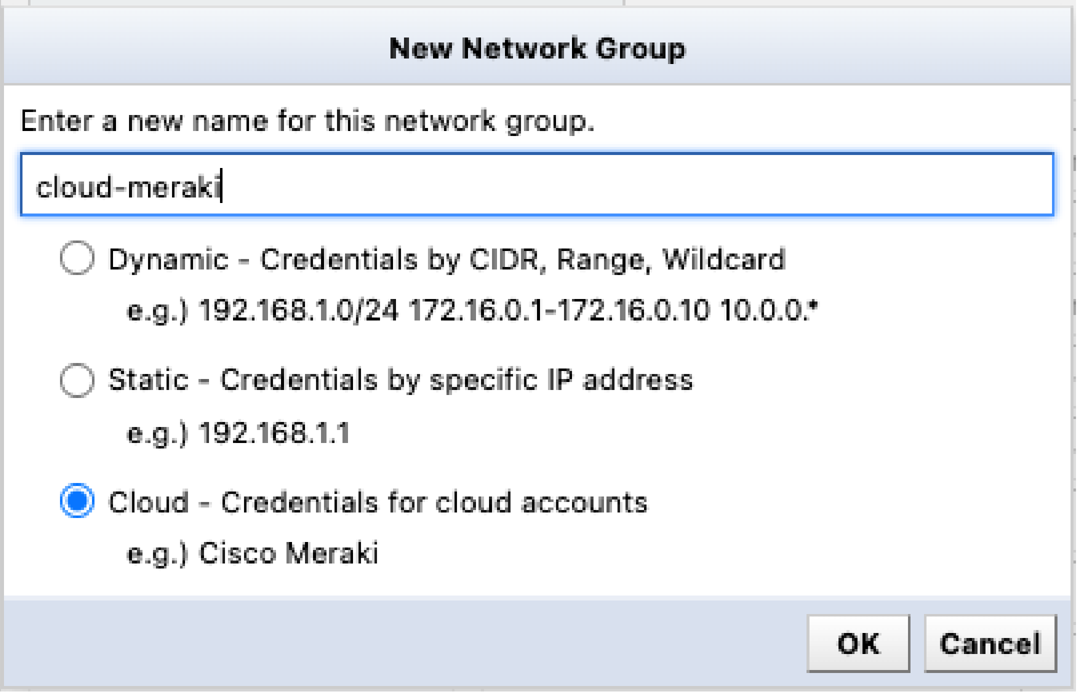
Item	Required	Description
Cloud Account Provider	Y	The service provider of the cloud account
Account User	Y	The username of the cloud credential
Api Key	Y	Password or the access token for the account
Address Set	N	The set of IPs or CIDR needed for the credential

Unlike with other credentials, there is no requirement to set an address. However, not setting an address limits the credential to the configured addresses.

To add a new credential set:

1. Click the [Inventory] main tab.
2. Click the [Inventory] sub-tab.
3. Click [Credentials].
4. Select a network.
5. Click the + button under the “Network Groups” left sidepanel, or click the [Add new network group] button.
6. In the “New Network Group” window, enter a name for the Network Group.

7. Select “Cloud - Credentials for cloud accounts” for the network type.



New Network Group

Enter a new name for this network group.

cloud-meraki

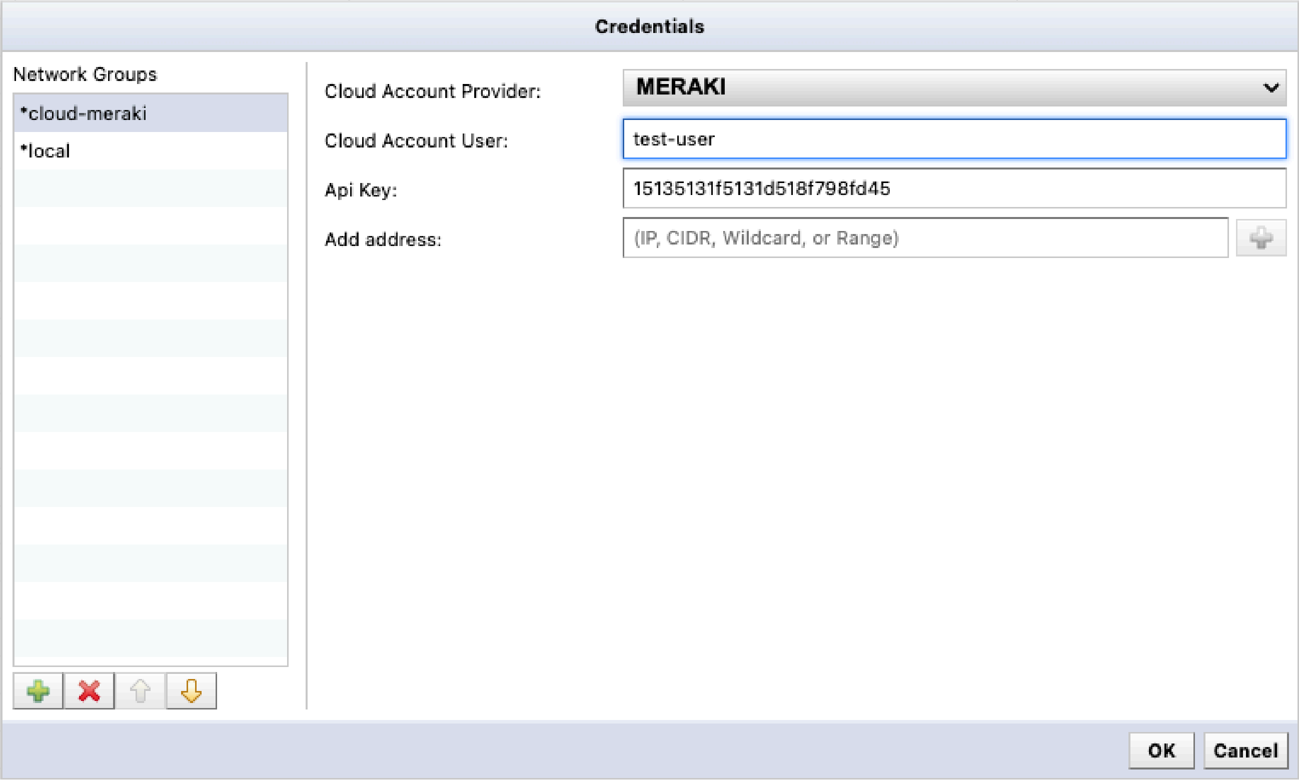
○ Dynamic - Credentials by CIDR, Range, Wildcard
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*

○ Static - Credentials by specific IP address
e.g.) 192.168.1.1

● Cloud - Credentials for cloud accounts
e.g.) Cisco Meraki

8. Click [OK].

The new credentials will be visible in the “Network Group” left sidepanel.



Credentials

Network Groups
- *cloud-meraki
- *local

Cloud Account Provider: MERAKI

Cloud Account User: test-user

Api Key: 15135131f5131d518f798fd45

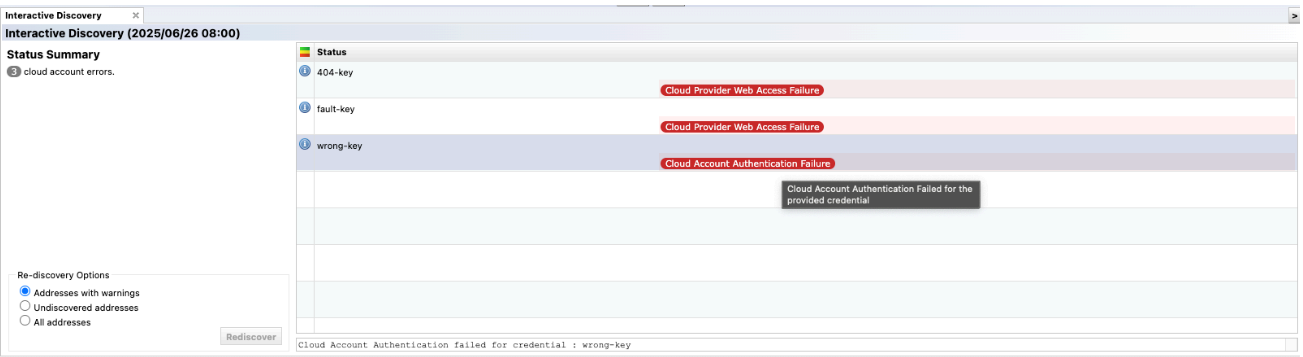
Add address: (IP, CIDR, Wildcard, or Range)

11.1.2 Device Discovery

Once you select the required cloud accounts, the system will use them in the discovery process to fetch the devices which are in the given discovery boundary. Any issues will be displayed to the user in same way as any other discovery errors.

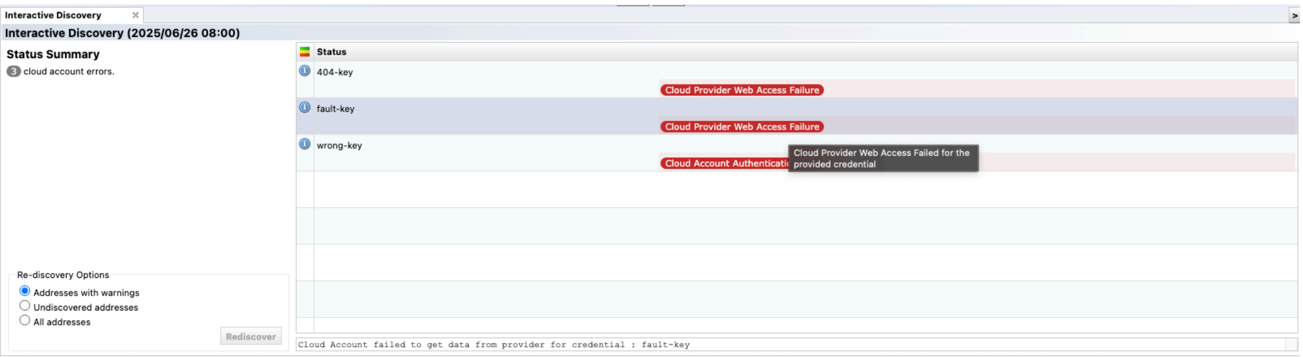
There are two main types of error which can occur:

- Usage of invalid credential (resulting in Cloud Account Authentication Failure).
- Communication and cloud provider-side errors (resulting in “Cloud Provider Web Access Failure”).


Interactive Discovery
Interactive Discovery (2025/06/26 08:00)
Status Summary
3 cloud account errors.
Status
404-key
Cloud Provider Web Access Failure
fault-key
Cloud Provider Web Access Failure
wrong-key
Cloud Account Authentication Failure
Re-discovery Options
● Addresses with warnings
○ Undiscovered addresses
○ All addresses
Rediscover

Cloud Account Authentication Failed for the provided credential

```
Cloud Account Authentication failed for credential : wrong-key
```



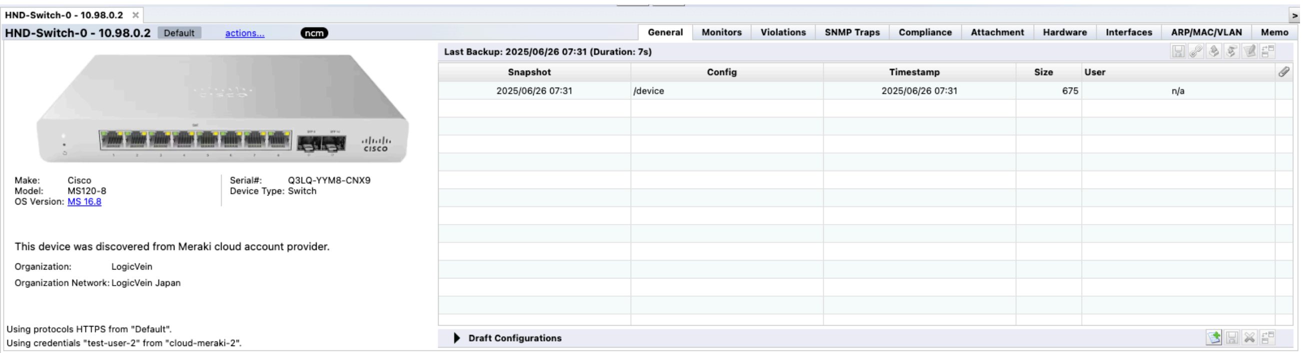
Cloud Provider Web Access Failed for the provided credential

```
Cloud Account failed to get data from provider for credential : fault-key
```

When finalizing the discovery system, enter the following information into the device’s `metaJson` using `cloudData` as the key:

Item	Description
cloudAccount	The name of the cloud account which was used.
cloudOrganizationName	The name of the cloud organization device
cloudNetworkName	The name of the organization’s device network

Discovered devices will appear in the Editor’s [General] tab as shown below:



Make: Cisco
Model: MS120-8
OS Version: MS 16.8

Serial#: Q3LQ-YYM8-CNX9
Device Type: Switch

This device was discovered from Meraki cloud account provider.

Organization: LogicVein
Organization Network: LogicVein Japan

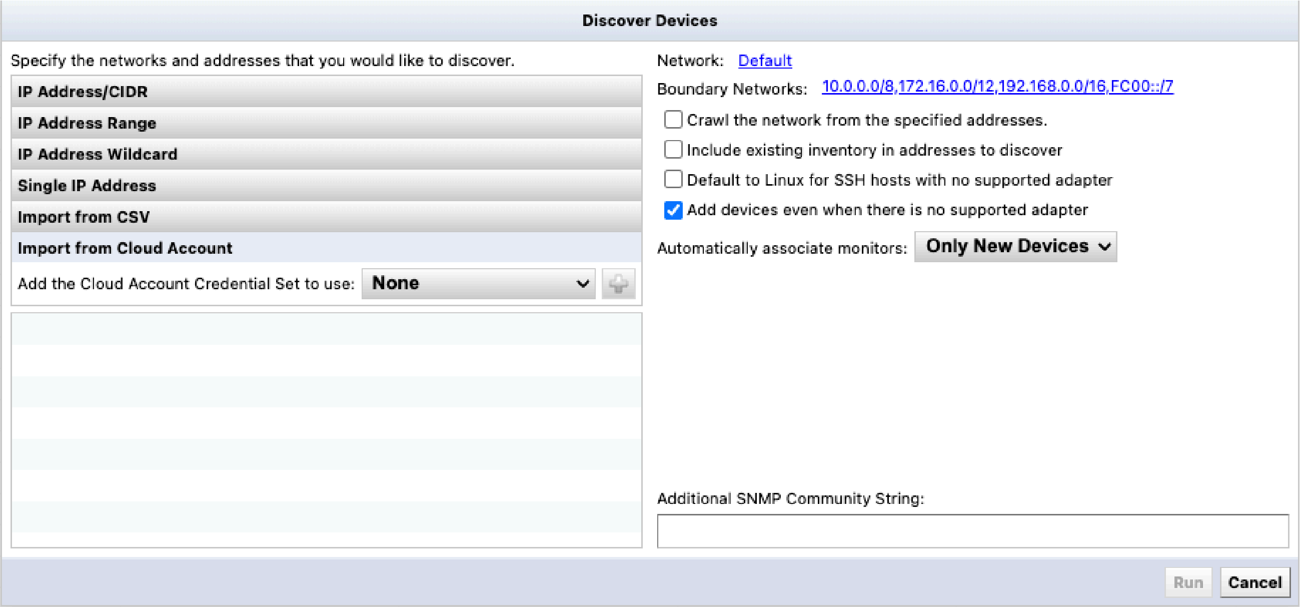
Using protocols HTTPS from "Default".
Using credentials "test-user-2" from "cloud-meraki-2".

Last Backup: 2025/06/26 07:31 (Duration: 7s)

Snapshot	Config	Timestamp	Size	User
2025/06/26 07:31	/device	2025/06/26 07:31	675	n/a

11.1.3 Multiple Cloud Account Discovery

Along with cloud credentials, ThirdEye also allows selecting multiple cloud accounts in device discovery.



Discover Devices

Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: None

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

□ Crawl the network from the specified addresses.

□ Include existing inventory in addresses to discover

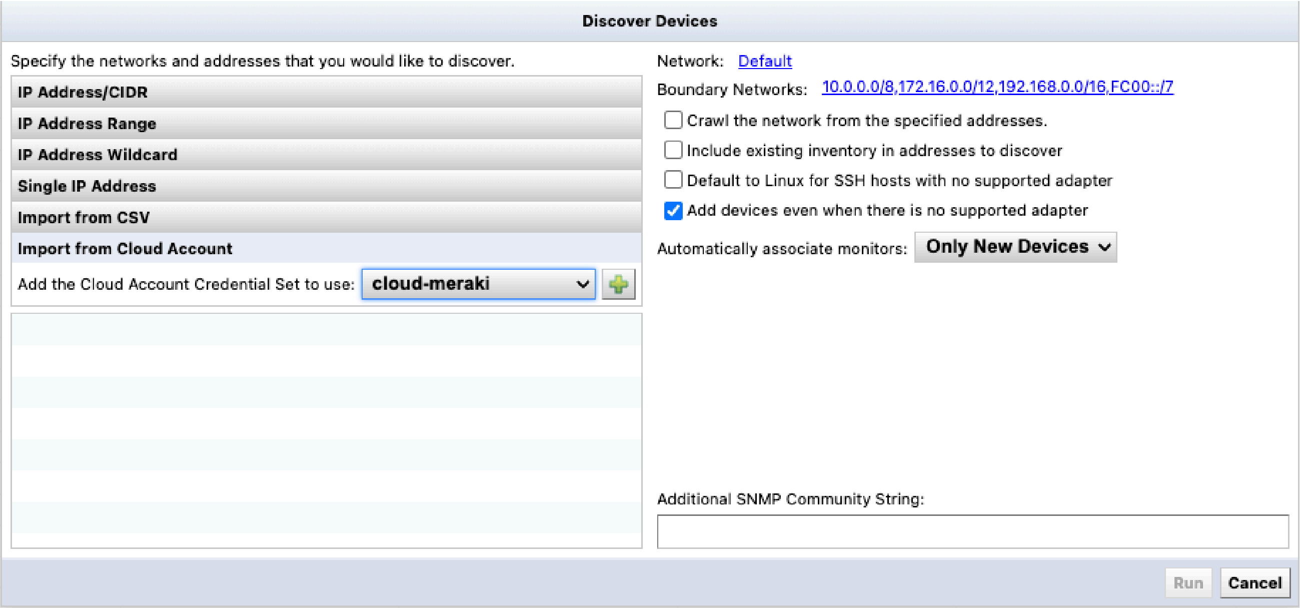
□ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:

You can choose one or more cloud accounts configured in the credentials, and manage them similarly to how IP addresses are managed.



Discover Devices

Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: cloud-meraki

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

□ Crawl the network from the specified addresses.

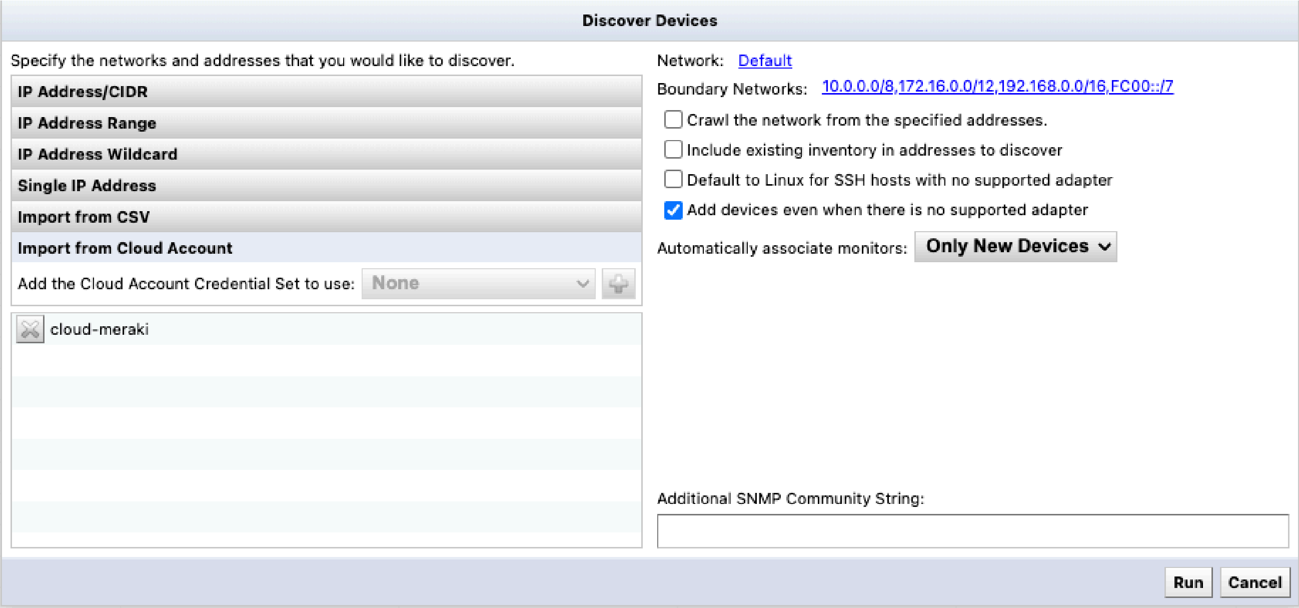
□ Include existing inventory in addresses to discover

□ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:



Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: None

cloud-meraki

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

□ Crawl the network from the specified addresses.

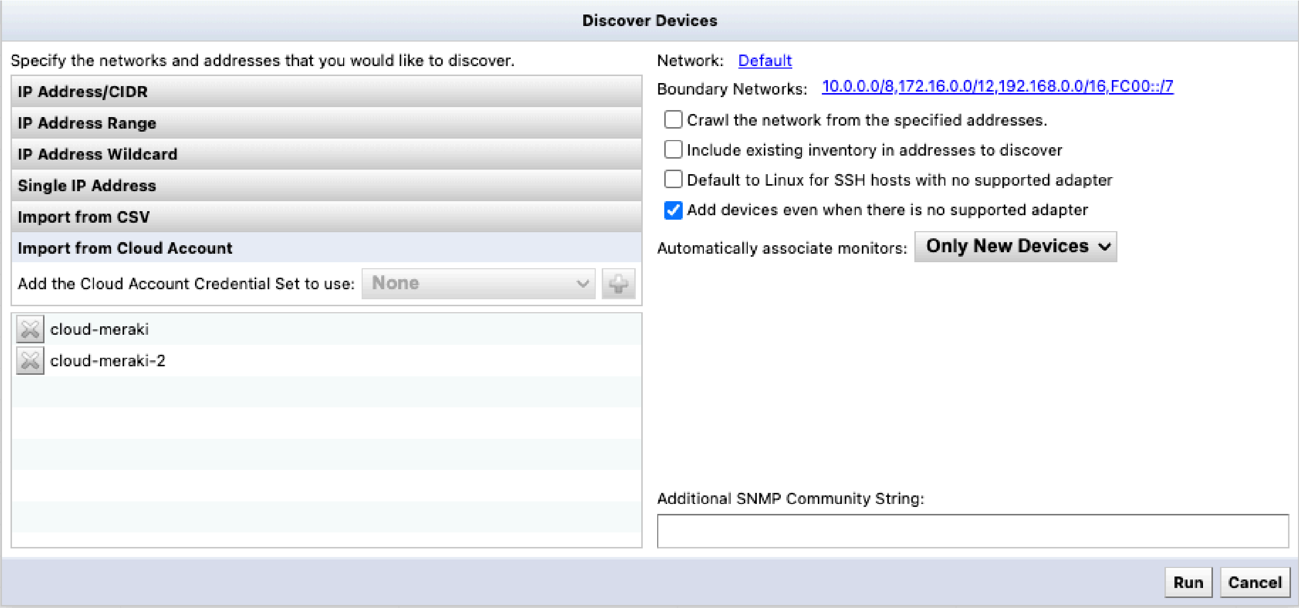
□ Include existing inventory in addresses to discover

□ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:



Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: None

cloud-meraki

cloud-meraki-2

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

□ Crawl the network from the specified addresses.

□ Include existing inventory in addresses to discover

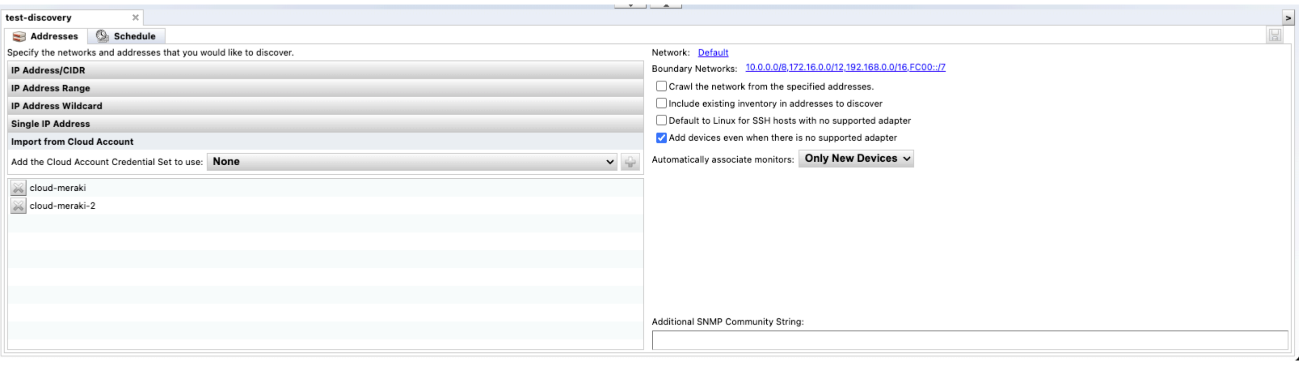
□ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:

You can configure cloud accounts in a discovery job in a similar way to executing device discovery via the inventory.



Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: None

cloud-meraki

cloud-meraki-2

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

□ Crawl the network from the specified addresses.

□ Include existing inventory in addresses to discover

□ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:

11.1.4 Rediscovery

With the cloud devices present in the Inventory, cloud devices Rediscovery Jobs will now accommodate cloud devices. The Rediscovery flow will not change from the user's perspective.

11.1.5 Support

At this time, support is focussed on Access Points. Meraki devices are primarily access points, but could also potentially be security cameras and other devices.These devices are deployed on-premises, but are managed via the Meraki Cloud.

11.2 Aruba EdgeConnect

ThirdEye's provides cloud device support for HPE Aruba EdgeConnect (EC) devices (formally known as SilverPeak). You can manage EdgeConnect devices locally via deployed Orchestrator or Aruba Central cloud portal.

11.2.1 Credential Handling

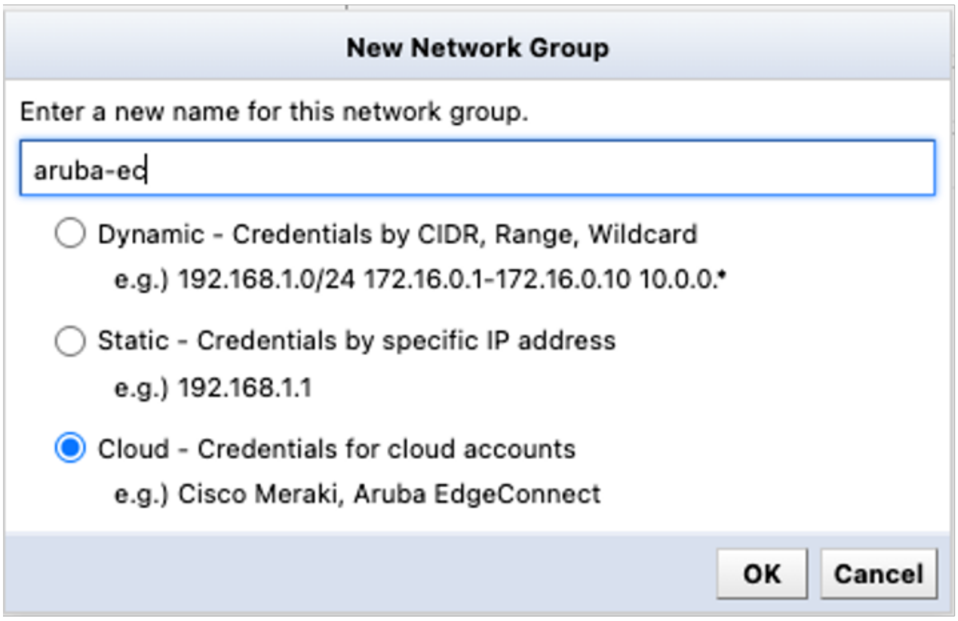
For EdgeConnect devices, you must configure the API key and API URL to access Orchestrator or the cloud portal.

Field	Required	Description
Cloud Account Provider	Y	The service provider of the cloud account (Aruba EdgeConnect)
Account User	Y	The username of the cloud credential
API URL	Y	The API provider url
API Key	Y	Password or the access token for the account
Address Set	N	The set of IPs or CIDR to use this credential

When configuring the API URL, only provide the IP (domain) and proxy mapping (if any).

ThirdEye will generate the base URL for the API.

When you set `https://10.0.99.8/` as the URL, the system will generate the base URL `https://10.0.99.8/gms/rest`.



New Network Group

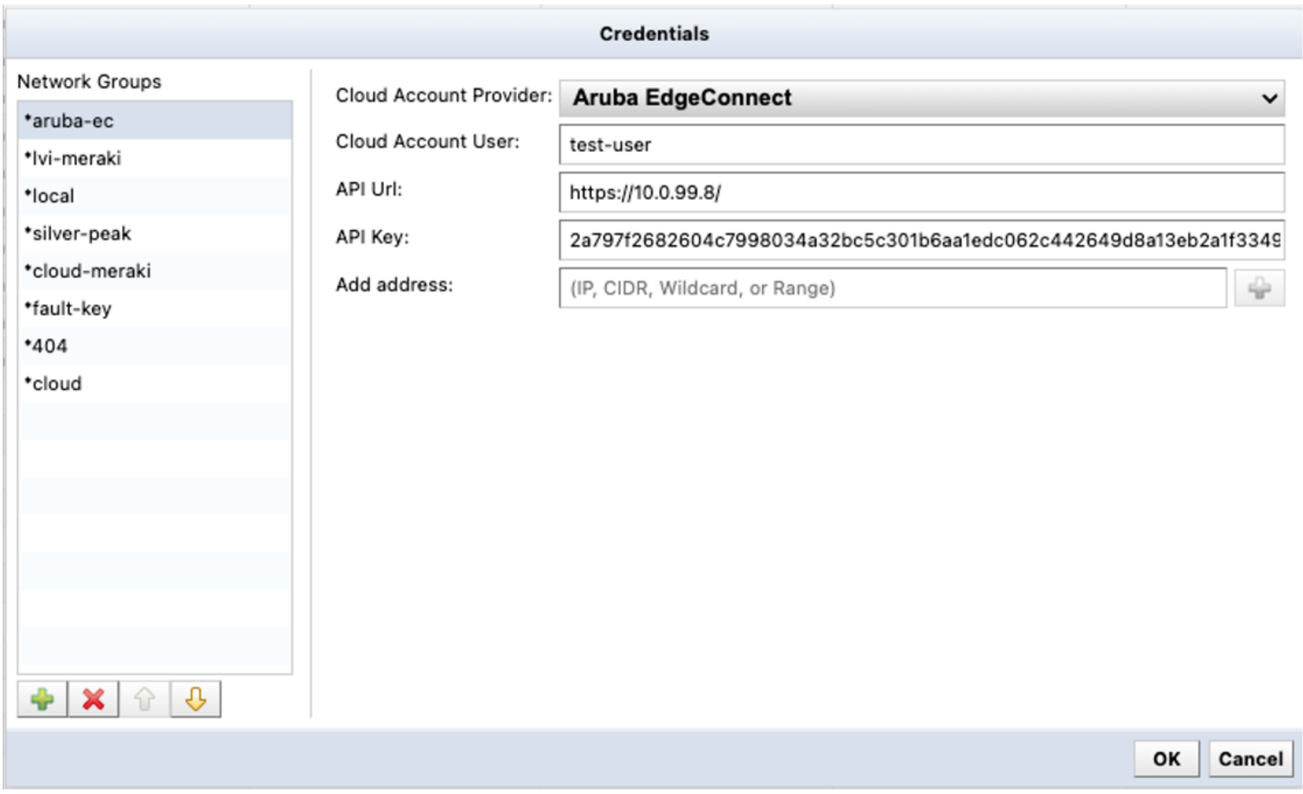
Enter a new name for this network group.

aruba-ec

○ Dynamic - Credentials by CIDR, Range, Wildcard
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*

○ Static - Credentials by specific IP address
e.g.) 192.168.1.1

● Cloud - Credentials for cloud accounts
e.g.) Cisco Meraki, Aruba EdgeConnect



Credentials

Network Groups
- *aruba-ec
- *lvi-meraki
- *local
- *silver-peak
- *cloud-meraki
- *fault-key
- *404
- *cloud

Cloud Account Provider: Aruba EdgeConnect

Cloud Account User: test-user

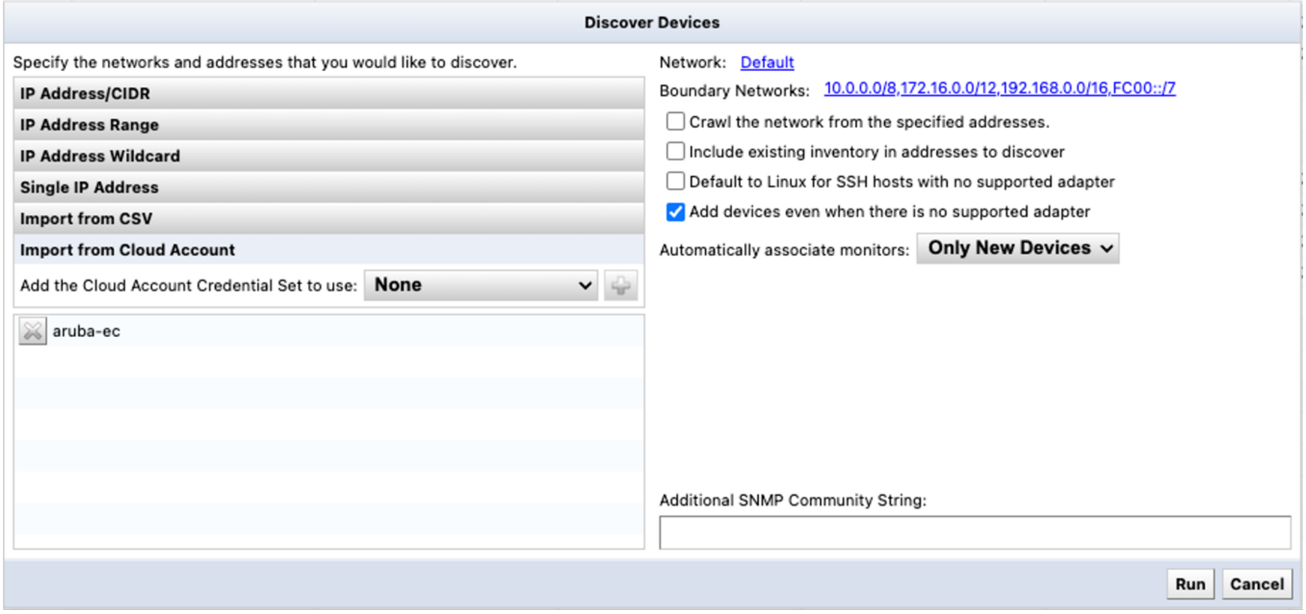
API Url: https://10.0.99.8/

API Key: 2a797f2682604c7998034a32bc5c301b6aa1edc062c442649d8a13eb2a1f3349

Add address: (IP, CIDR, Wildcard, or Range)

11.2.2 Discovery

Discovery for EdgeConnect devices is similar to that of other cloud devices. You can configure multiple cloud account credentials.



Specify the networks and addresses that you would like to discover.

Add the Cloud Account Credential Set to use: None

aruba-ec

Network: Default

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

☐ Crawl the network from the specified addresses.

☐ Include existing inventory in addresses to discover

☐ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

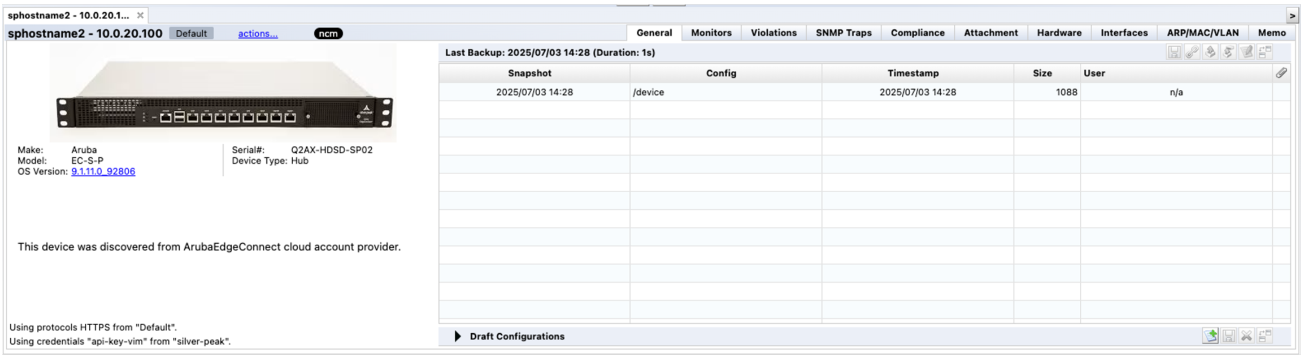
Automatically associate monitors: Only New Devices

Additional SNMP Community String:

Once you select the required cloud accounts, they will be used in the discovery process to fetch the devices within the discovery boundary from the Orchestrator API. Any issues will be displayed in same fashion as with any other discovery errors. Discovery will add the following information to the device's `metaJson` with the key `cloudData`.

Field	Description
cloudAccount	The name of the cloud account which was used
organizationalId	The Id used for the device in Orchestrator

Discovered devices will appear in the [General] tab as shown below:



Make: Aruba
Model: EC-S-P
OS Version: 9.1.11.0_92806

Serial#: Q2AX-HDSD-SP02
Device Type: Hub

This device was discovered from ArubaEdgeConnect cloud account provider.

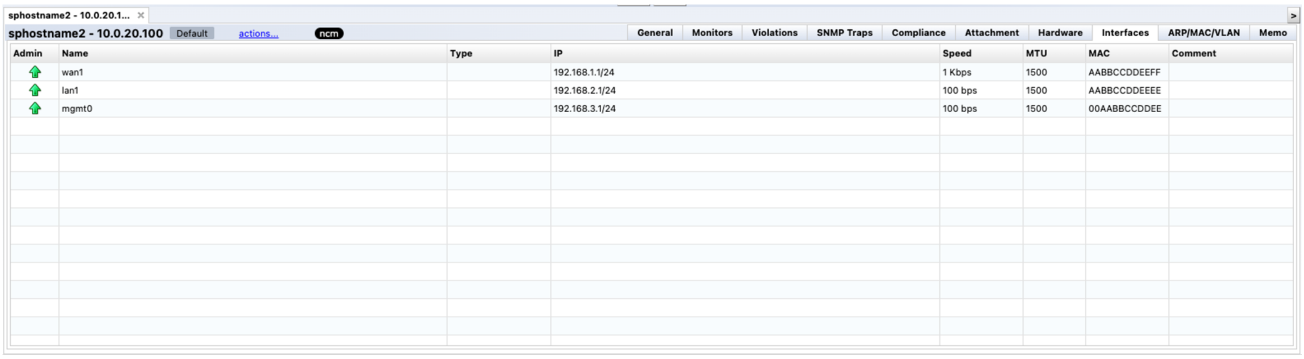
Using protocols HTTPS from "Default".
Using credentials "api-key-vim" from "silver-peak".

Last Backup: 2025/07/03 14:28 (Duration: 1s)

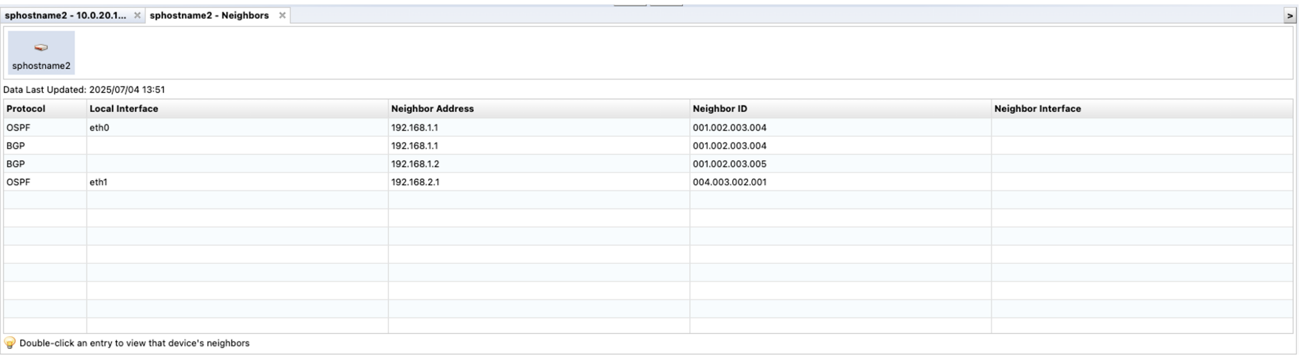
Snapshot	Config	Timestamp	Size	User
2025/07/03 14:28	/device	2025/07/03 14:28	1088	n/a

11.2.3 Telemetry (Neighbor Collection)

Any device discovered via an EdgeConnect provider will have support for Telemetry jobs, and can collect interface, OSPF and BGP neighbor data.



Admin	Name	Type	IP	Speed	MTU	MAC	Comment
⬆	wan1		192.168.1.1/24	1 Kbps	1500	AABBCCDDEEFF	
⬆	lan1		192.168.2.1/24	100 bps	1500	AABBCCDDEEEE	
⬆	mgmt0		192.168.3.1/24	100 bps	1500	00AABBCCDDEE	



Data Last Updated: 2025/07/04 13:51

Protocol	Local Interface	Neighbor Address	Neighbor ID	Neighbor Interface
OSPF	eth0	192.168.1.1	001.002.003.004	
BGP		192.168.1.1	001.002.003.004	
BGP		192.168.1.2	001.002.003.005	
OSPF	eth1	192.168.2.1	004.003.002.001	

Double-click an entry to view that device's neighbors

11.3 Aruba Access Points (via Aruba Central)

ThirdEye provides support for managing Aruba Access Points (AP) via Aruba Central as a Cloud Device. Before beginning, ensure that there is a valid Aruba Central account with the necessary permissions to access the API. To monitor Aruba Access Points, you will need to configure a Cloud Account Credential for Aruba Central, and then use that credential in a Discovery job to find the Access Points.

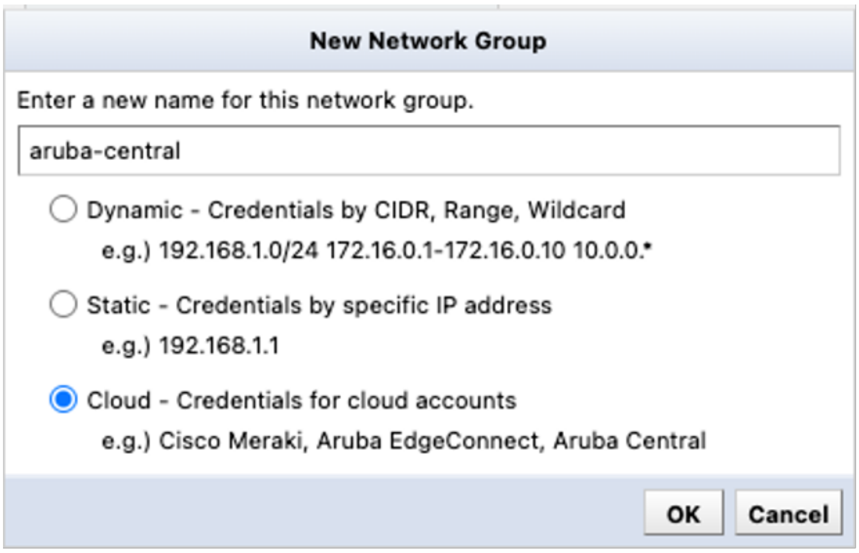
11.3.1 Credentials

When configuring a Cloud Account Credential for Aruba Central, first make sure to generate the access token from the Aruba Central portal. With the access token details available, navigate to the Credentials page and create a new Cloud Account Credential.

The Aruba Central api provider has token validity time for both access and refresh tokens, due to this ThirdEye will periodically refresh the tokens. Starting with initial configuration of the credential.

When configuring the credential, use the information from the access token generated in the Aruba Central portal.

Field	Required	Description
Credential Display Name	Y	The display name of this credential.
Cloud Account Provider	Y	The service provider of the cloud account (Aruba Central).
API Region	Y	The API Gateway region (According to the geographical cluster where the account is registered).
Client ID	Y	The client id to be used when requesting a new refresh token.
Client Secret	Y	The client secret to be used for token refresh.
Refresh Token	Y	The refresh token to be used.
Address Filter	N	The set of IPs or CIDR that will use this credential.



New Network Group

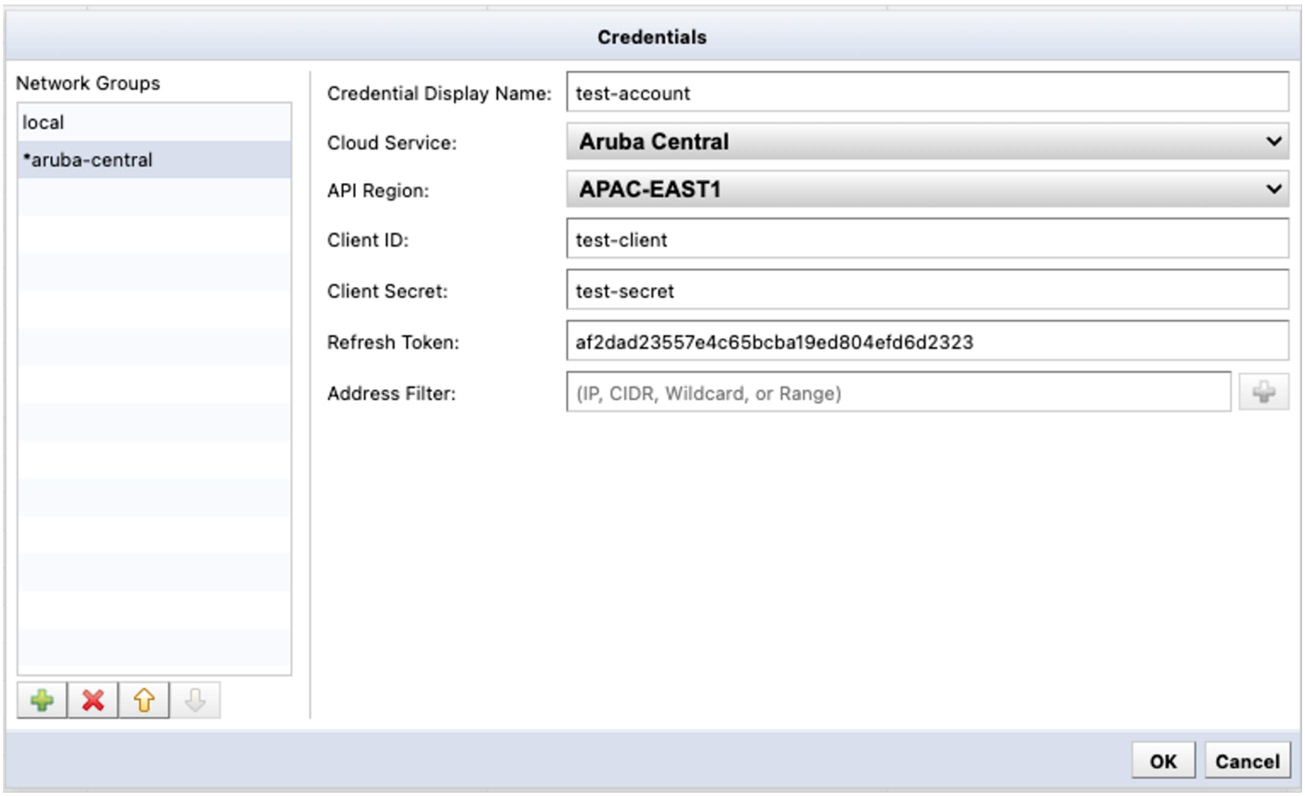
Enter a new name for this network group.

aruba-central

○ Dynamic - Credentials by CIDR, Range, Wildcard
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*

○ Static - Credentials by specific IP address
e.g.) 192.168.1.1

● Cloud - Credentials for cloud accounts
e.g.) Cisco Meraki, Aruba EdgeConnect, Aruba Central



Credentials

Network Groups: local, *aruba-central

Credential Display Name: test-account

Cloud Service: Aruba Central

API Region: APAC-EAST1

Client ID: test-client

Client Secret: test-secret

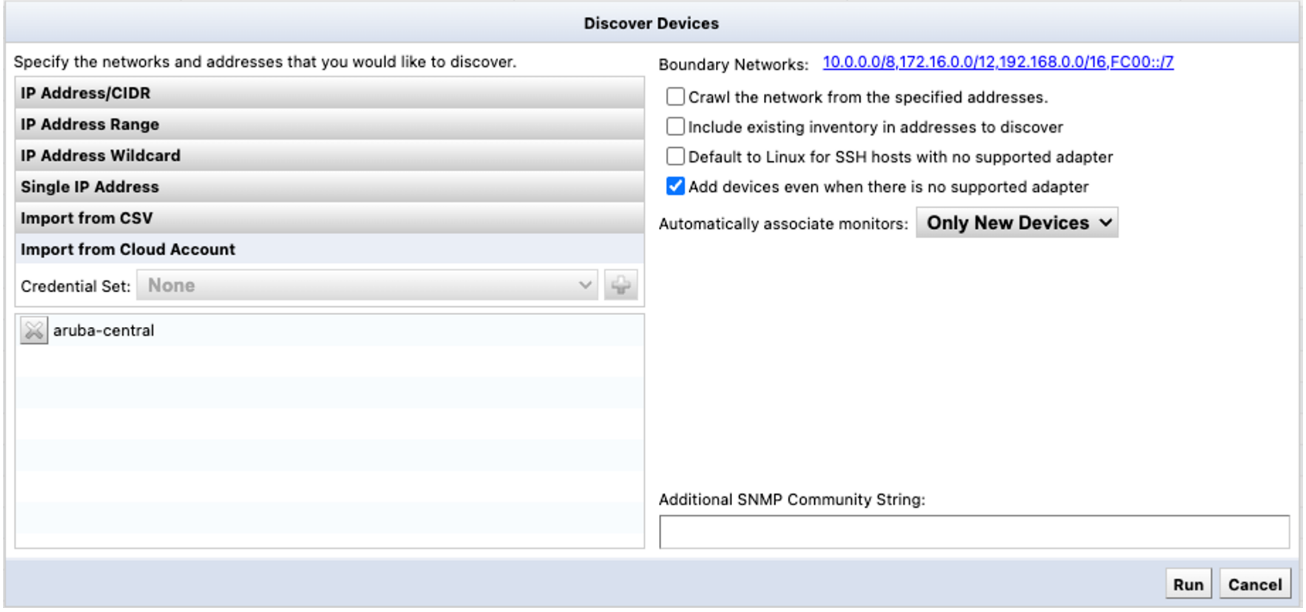
Refresh Token: af2dad23557e4c65bcba19ed804efd6d2323

Address Filter: (IP, CIDR, Wildcard, or Range)

Once the credential is configured, ThirdEye will do an initial token refresh to get the access token details. Thereafter, the tokens will be refreshed periodically, once 90% of the token's expiry time has elapsed.

11.3.2 Discovery

Discovery for Aruba Access Points are similar to that of other cloud devices. ThirdEye will use the configured cloud account credentials to fetch the access points from the Aruba Central API gateway for the region configured. If there are any Address Filters configured in the credential, the discovery boundary will be set according to that. You can configure multiple cloud account credentials as needed in a single discovery job.



Discover Devices

Specify the networks and addresses that you would like to discover.

Credential Set: None

aruba-central

Boundary Networks: 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

☐ Crawl the network from the specified addresses.

☐ Include existing inventory in addresses to discover

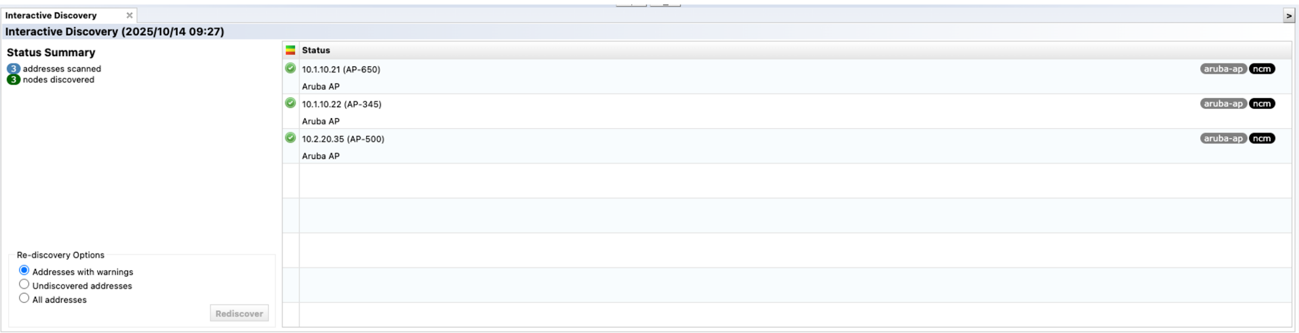
☐ Default to Linux for SSH hosts with no supported adapter

☑ Add devices even when there is no supported adapter

Automatically associate monitors: Only New Devices

Additional SNMP Community String:

Discovered devices will appear in the Interactive Discovery tab as shown below:



Interactive Discovery (2025/10/14 09:27)

Status Summary

3 addresses scanned

3 nodes discovered

Status
✓ 10.1.10.21 (AP-650) Aruba AP
✓ 10.1.10.22 (AP-345) Aruba AP
✓ 10.2.20.35 (AP-500) Aruba AP

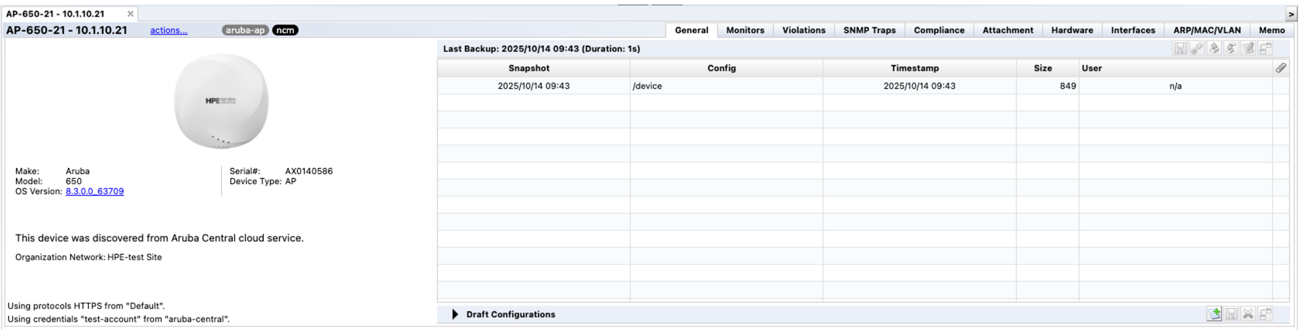
Re-discovery Options

● Addresses with warnings

○ Undiscovered addresses

○ All addresses

Discovered device data will appear in the [General] tab as shown below:



AP-650-21 - 10.1.10.21

Make: Aruba
Model: 650
OS Version: 8.3.0.0_63709

Serial#: AX0140586
Device Type: AP

This device was discovered from Aruba Central cloud service.

Organization Network: HPE-test Site

Using protocols HTTPS from "Default".
Using credentials "test-account" from "aruba-central".

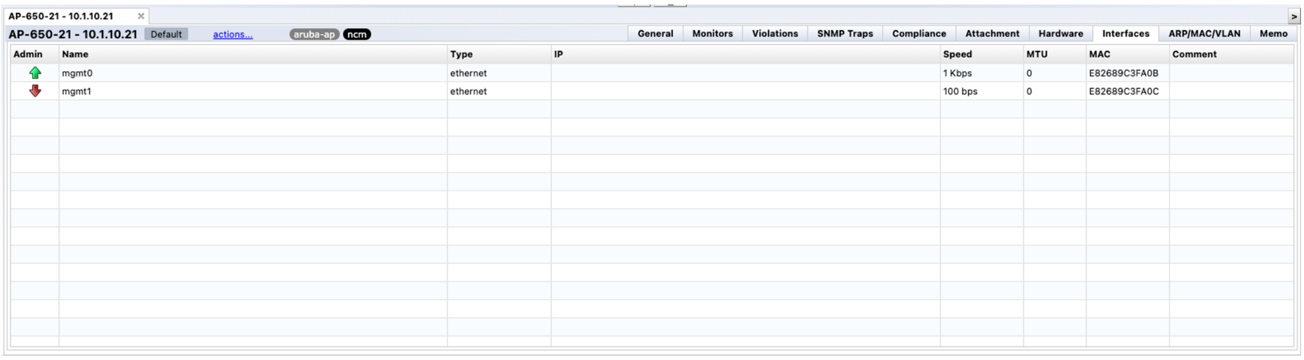
Last Backup: 2025/10/14 09:43 (Duration: 1s)

Snapshot	Config	Timestamp	Size	User
2025/10/14 09:43	/device	2025/10/14 09:43	849	n/a

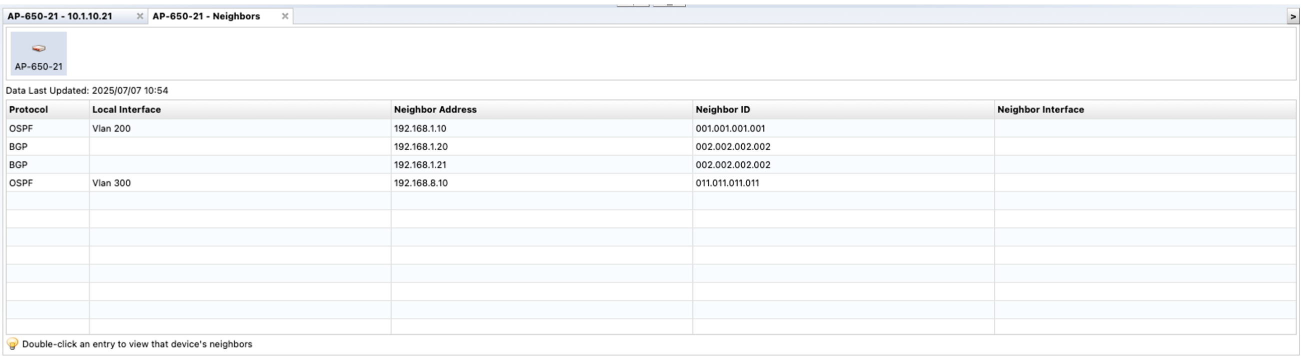
Draft Configurations

11.3.3 Telemetry (Neighbor Collection)

Any device discovered via Aruba Central will have support for Telemetry jobs, and can collect interface, OSPF and BGP neighbor data.



Admin	Name	Type	IP	Speed	MTU	MAC	Comment
⇧	mgmt0	ethernet		1 Kbps	0	E82689C3FA0B	
⇩	mgmt1	ethernet		100 bps	0	E82689C3FA0C	



Data Last Updated: 2025/07/07 10:54

Protocol	Local Interface	Neighbor Address	Neighbor ID	Neighbor Interface
OSPF	Vlan 200	192.168.1.10	001.001.001.001	
BGP		192.168.1.20	002.002.002.002	
BGP		192.168.1.21	002.002.002.002	
OSPF	Vlan 300	192.168.8.10	011.011.011.011	

Double-click an entry to view that device's neighbors

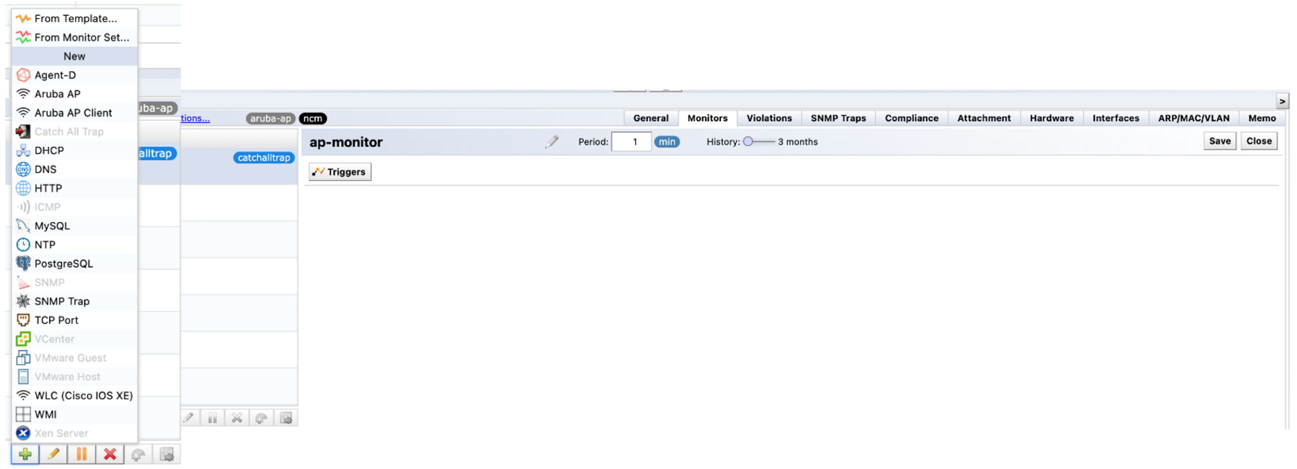
11.3.4 Monitoring

ThirdEye supports two monitor types for Aruba Access Points: `Aruba AP` and `Aruba AP Clients` . These monitors can be added only once to a device with `aruba-ap` trait. And they will monitor the access points via the Aruba Central APIs. Both of these monitors do not display any configuration settings other than the `Period` , but it will allow the user to configure any of the available triggers.

11.3.4.1 Aruba AP Monitor

An `Aruba AP` monitor can be used to monitor the access point using the following metric data,

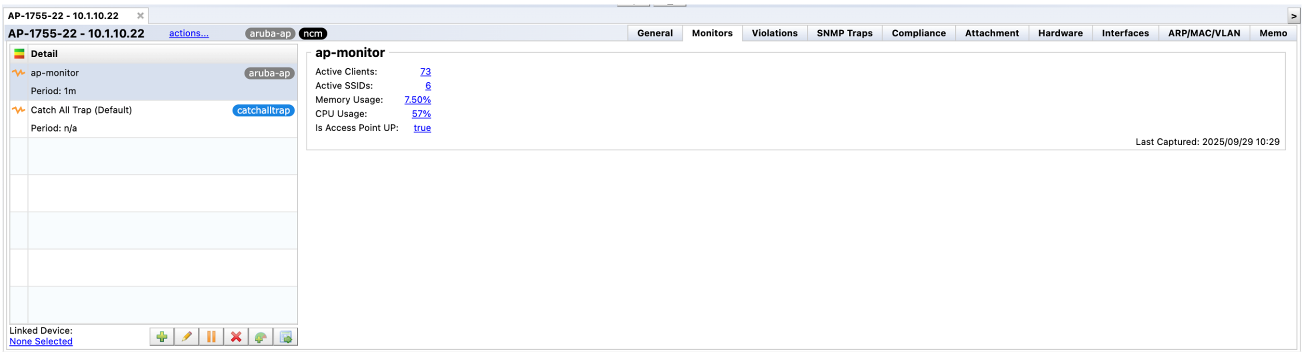
Metric	Data Type	Description
Active Clients	Numeric	Number of clients connected to AP.
Active SSIDs	Numeric	Number of SSIDs in AP.
Memory Usage	Numeric	Memory usage of the AP.
CPU Usage	Numeric	CPU Usage of the AP.
Access Point Operational Status	Boolean	If the AP is running.



ap-monitor

Period: 1 min

History: 3 months



AP-1755-22 - 10.1.10.22

ap-monitor
Period: 1m

Catch All Trap (Default)
Period: n/a

Linked Device:
None Selected

ap-monitor

Active Clients: 73
Active SSIDs: 6
Memory Usage: 7.50%
CPU Usage: 57%
Is Access Point UP: true

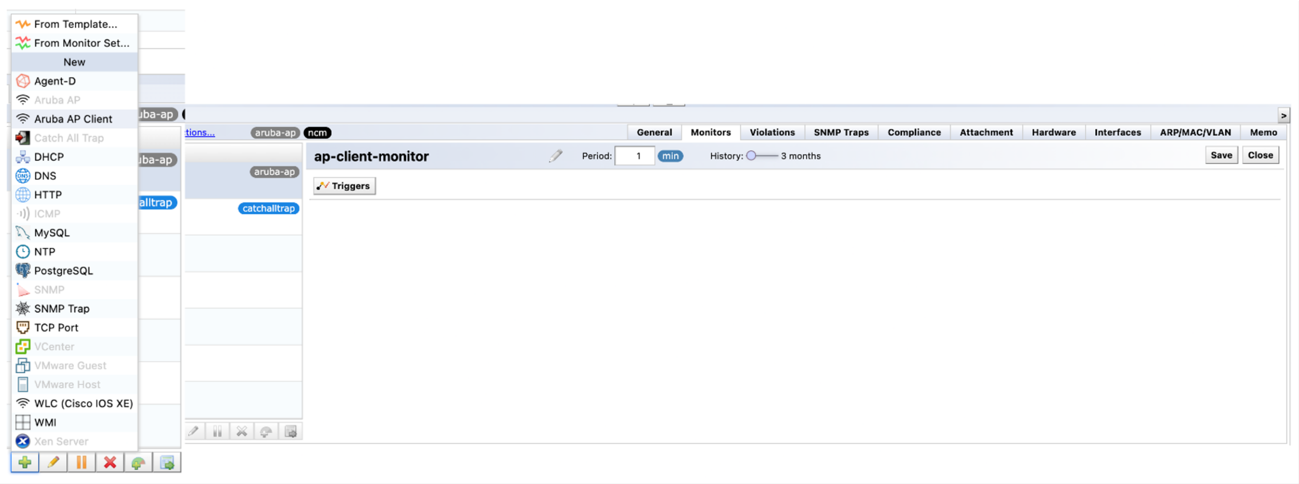
Last Captured: 2025/09/29 10:29

11.3.4.2 Aruba AP Client Monitor

An `Aruba AP Clients` monitor can be used to monitor the clients connected to the access point. Once this monitor is added to an Aruba Access Point, Wi-Fi clients will be viewable on the [Wi-Fi Clients] tab.

For `Aruba AP Clients` monitor following metric data is available:

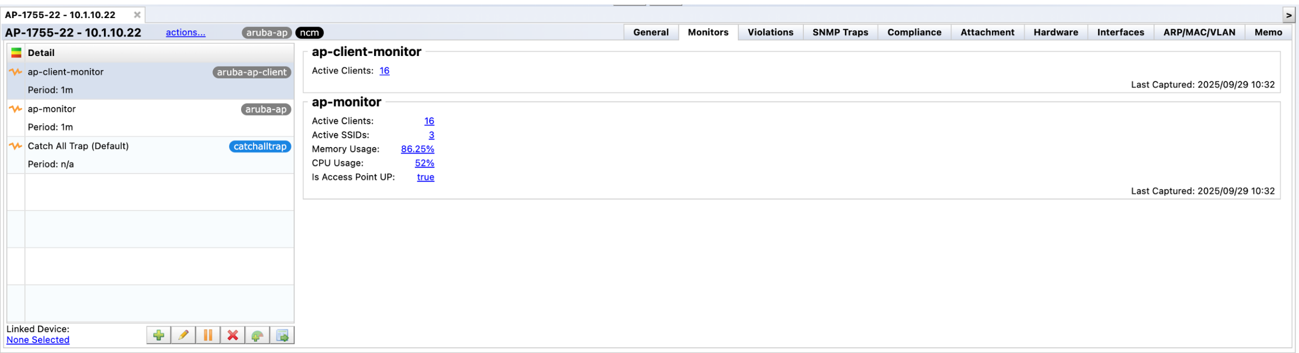
Metric	Data Type	Description
Active Clients	Numeric	Number of clients connected to AP.



ap-client-monitor

Period: 1 min

History: 3 months



ap-client-monitor
Period: 1m

ap-monitor
Period: 1m

Catch All Trap (Default)
Period: n/a

ap-client-monitor

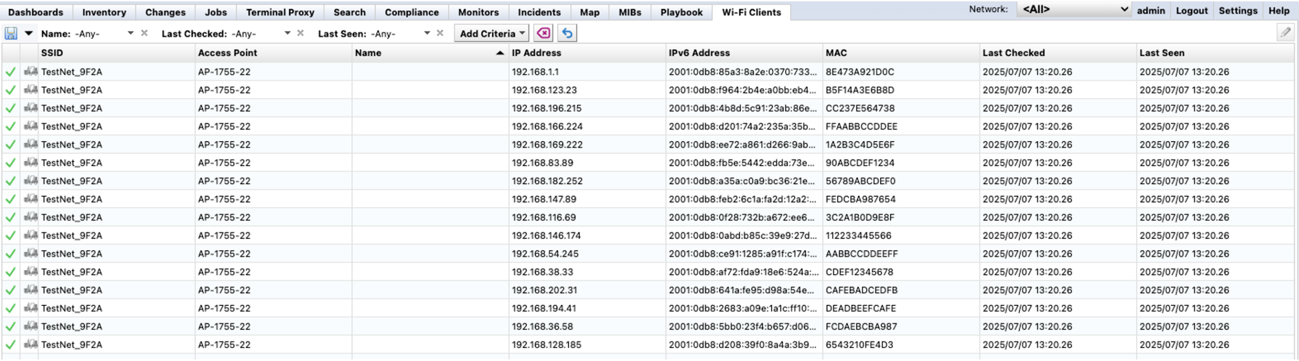
Active Clients: 16

Last Captured: 2025/09/29 10:32

ap-monitor

Active Clients: 16
Active SSIDs: 3
Memory Usage: 86.25%
CPU Usage: 52%
Is Access Point UP: true

Last Captured: 2025/09/29 10:32



Name: -Any- Last Checked: -Any- Last Seen: -Any-

		SSID	Access Point	Name	IP Address	IPv6 Address	MAC	Last Checked	Last Seen
✓		TestNet_9F2A	AP-1755-22		192.168.1.1	2001:0db8:85a3:8a2e:0370:733...	8E473A921D0C	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.123.23	2001:0db8:f964:2b4e:a0bb:eb4...	B5F14A3E6B8D	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.196.215	2001:0db8:4b8d:5c91:23ab:86e...	CC237E564738	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.166.224	2001:0db8:d201:74a2:235a:35b...	FFAABBCCDDEE	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.169.222	2001:0db8:ee72:a861:d266:9ab...	1A2B3C4D5E6F	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.83.89	2001:0db8:fb5e:5442:edda:73e...	90ABCDEF1234	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.182.252	2001:0db8:a35a:c0a9:bc36:21e...	56789ABCDEF0	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.147.89	2001:0db8:feb2:6c1a:fa2d:12a2:...	FEDCBA987654	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.116.69	2001:0db8:0f28:732b:a672:ee6...	3C2A1B0D9E8F	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.146.174	2001:0db8:0abd:b85c:39e9:27d...	112233445566	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.54.245	2001:0db8:ce91:1285:a91f:c174:...	AABBCCDDEEFF	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.38.33	2001:0db8:af72:fda9:18e6:524a:...	CDEF12345678	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.202.31	2001:0db8:641a:fe95:d98a:54e...	CAFEBADCEDFB	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.194.41	2001:0db8:2683:a09e:1a1c:ff10:...	DEADBEEFCAFE	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.36.58	2001:0db8:5bb0:23f4:b657:d06...	FCDAEBCBA987	2025/07/07 13:20.26	2025/07/07 13:20.26
✓		TestNet_9F2A	AP-1755-22		192.168.128.185	2001:0db8:d208:39f0:8a4a:3b9...	6543210FE4D3	2025/07/07 13:20.26	2025/07/07 13:20.26

SECTION 12

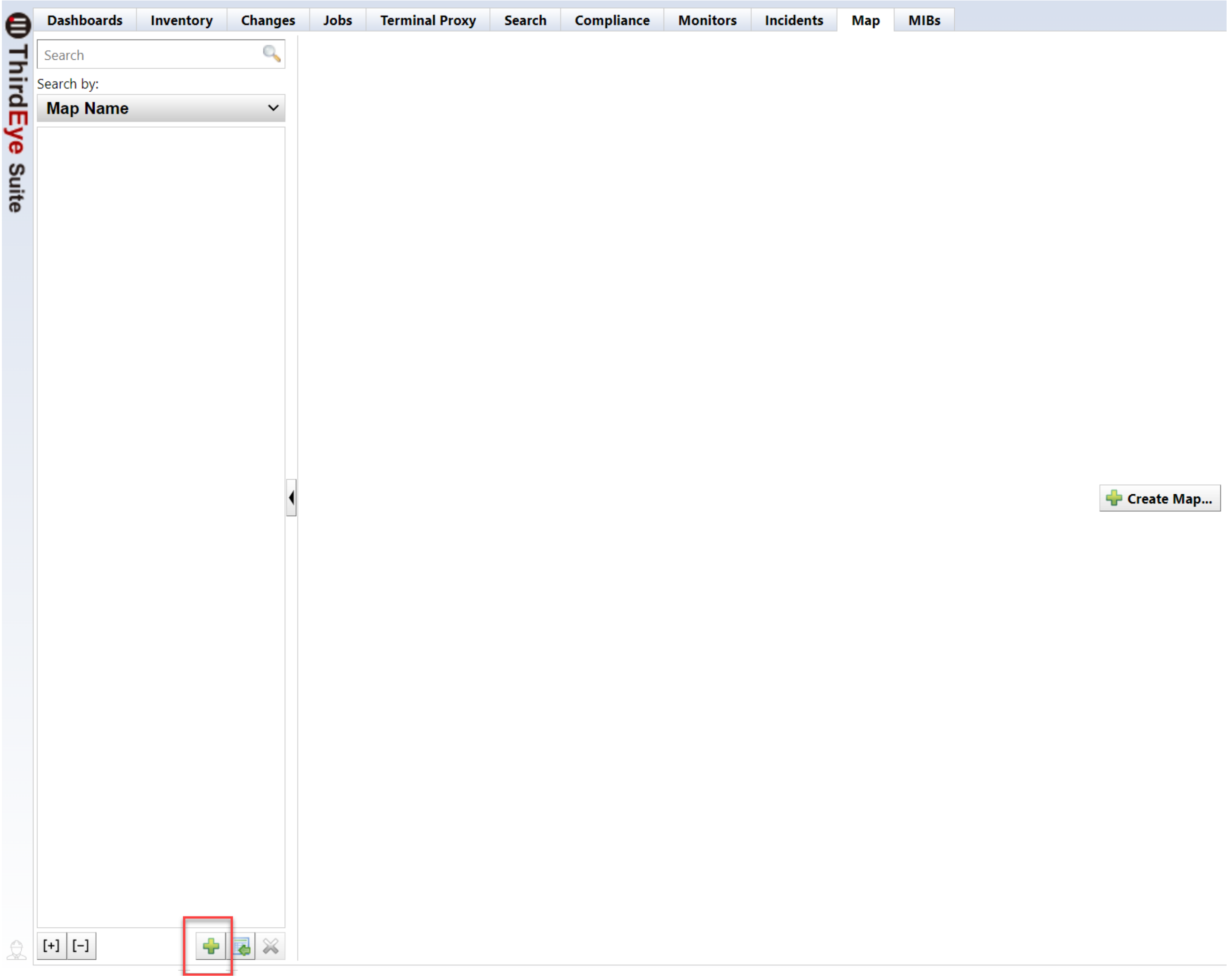
MAPS

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.

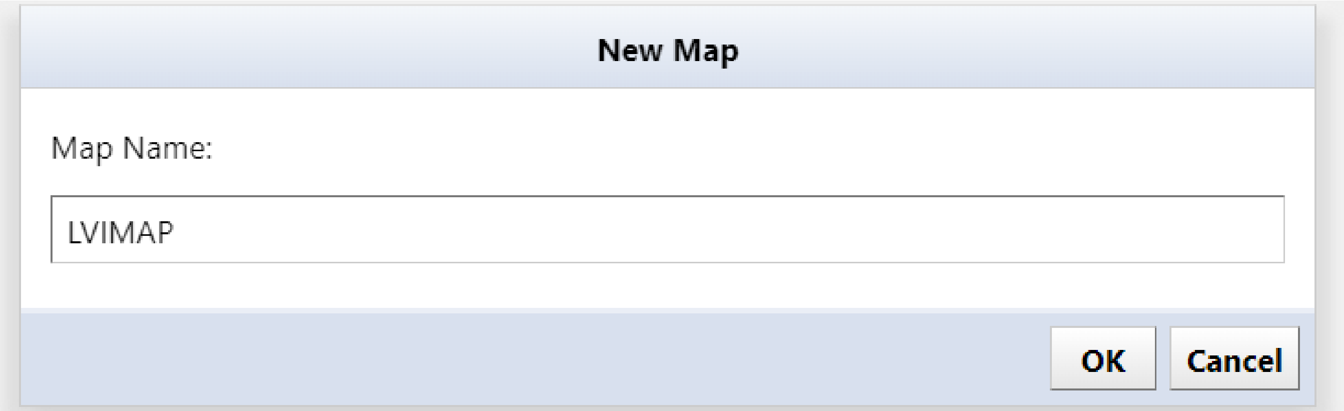
12.1 Create A Map

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.


Dashboards
Inventory
Changes
Jobs
Terminal Proxy
Search
Compliance
Monitors
Incidents
Map
MIBs
ThirdEye Suite
Search
Search by:
Map Name
Create Map...
[+]
[-]

2. On the [New Map] screen, enter the map name and click [OK].



Map Name: LVIMAP

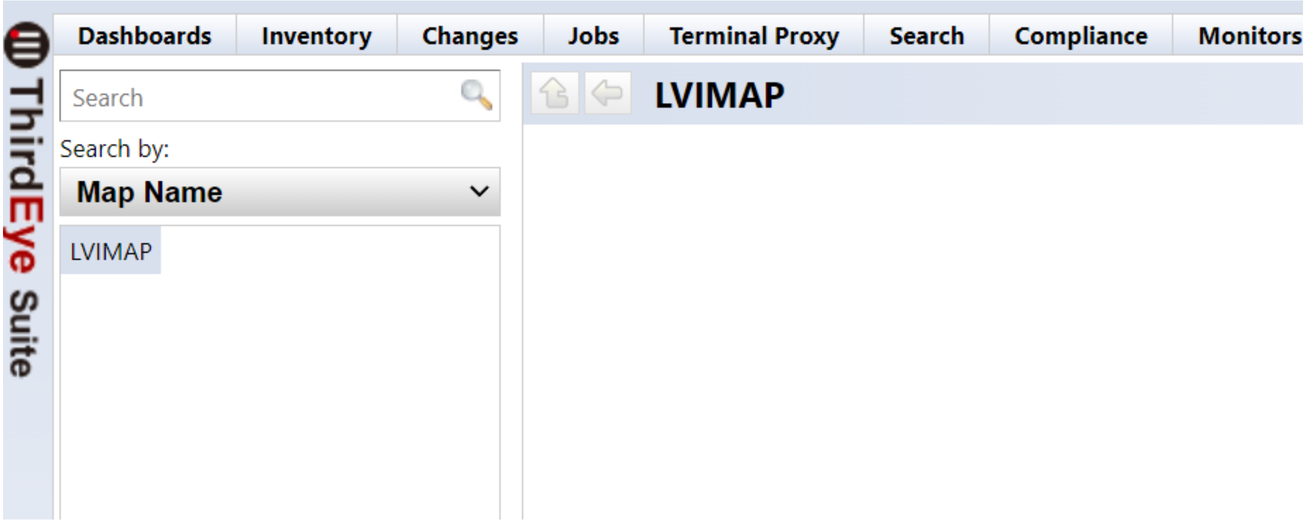
Note

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.

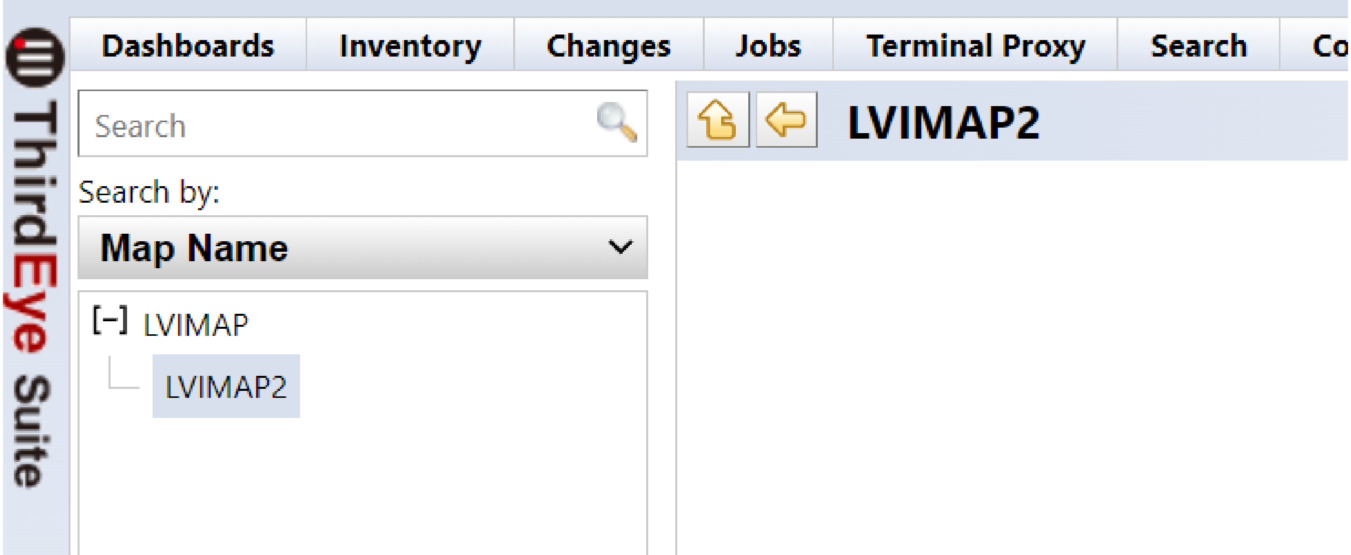
The selected Managed Network will impact which maps are visible to other users. For a user to have access to a map, they must have access to every Managed Network associated with the map.

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:



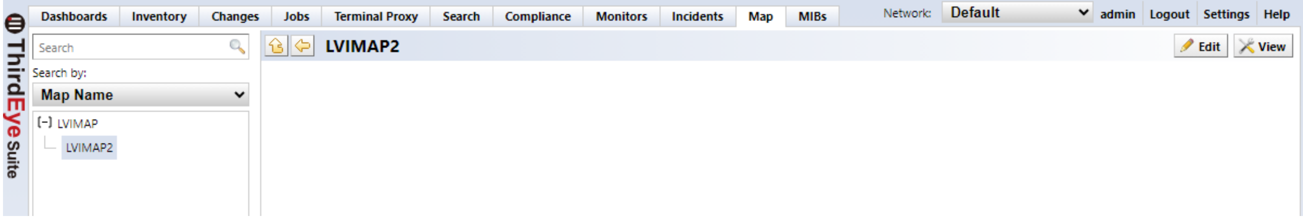
12.2 Insert Device

Note

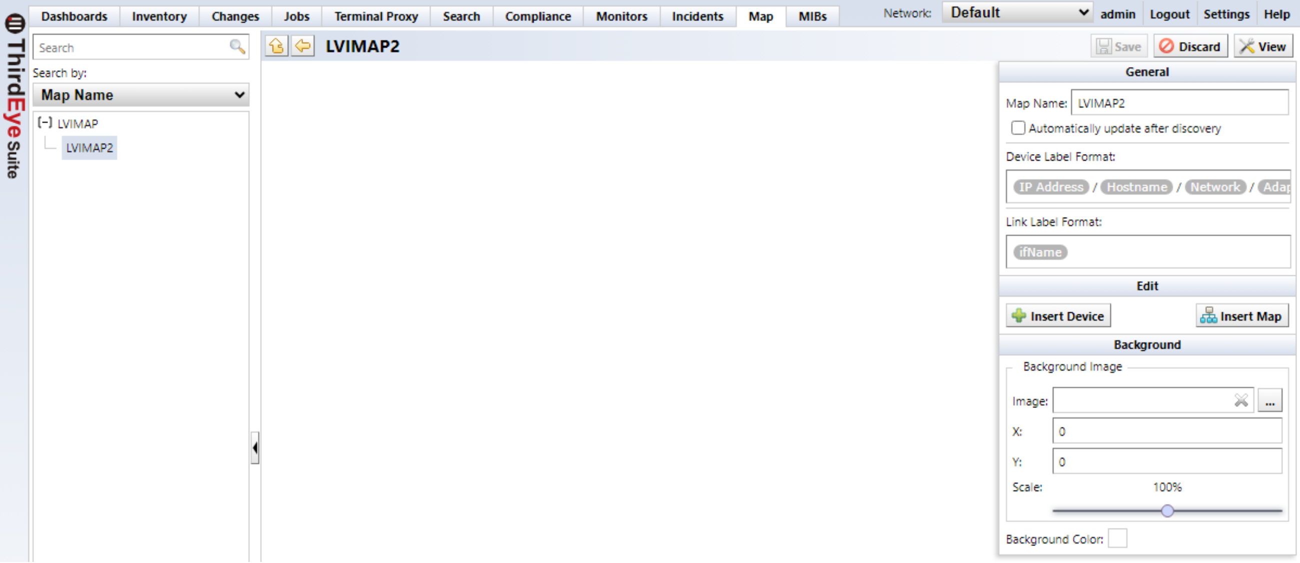
When adding a device, the device does not appear on the map by default.

If you want your device to appear as an object on the map, you must add it.

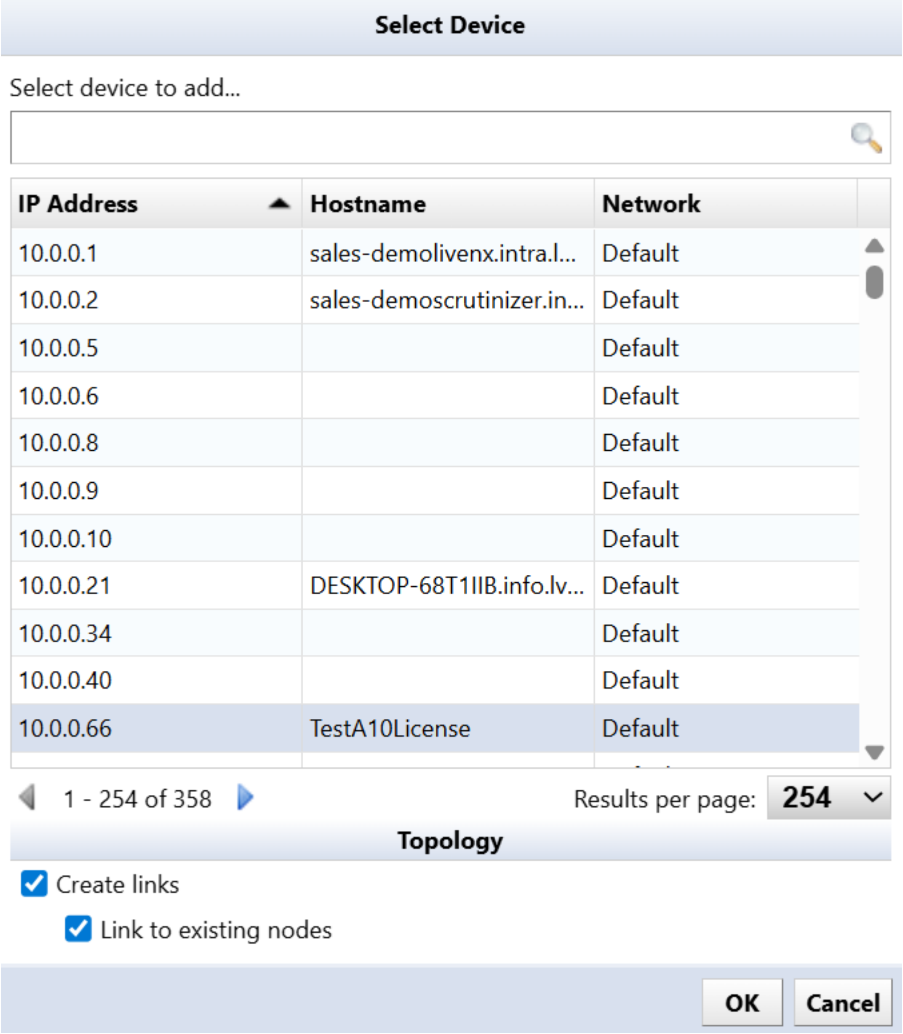
1. To add a device to a map, doubleclick the map in the "Map Name" list in the left sidebar, and click [Edit].



2. Click [Insert Device] in the right sidebar.



3. Select the device you want to insert into the map and click [OK].



Select Device

Select device to add...

IP Address	Hostname	Network
10.0.0.1	sales-demolivenx.intra.l...	Default
10.0.0.2	sales-demoscrutinizer.in...	Default
10.0.0.5		Default
10.0.0.6		Default
10.0.0.8		Default
10.0.0.9		Default
10.0.0.10		Default
10.0.0.21	DESKTOP-68T1IIB.info.lv...	Default
10.0.0.34		Default
10.0.0.40		Default
10.0.0.66	TestA10License	Default

1 - 254 of 358

Results per page: 254

Topology

☑ Create links

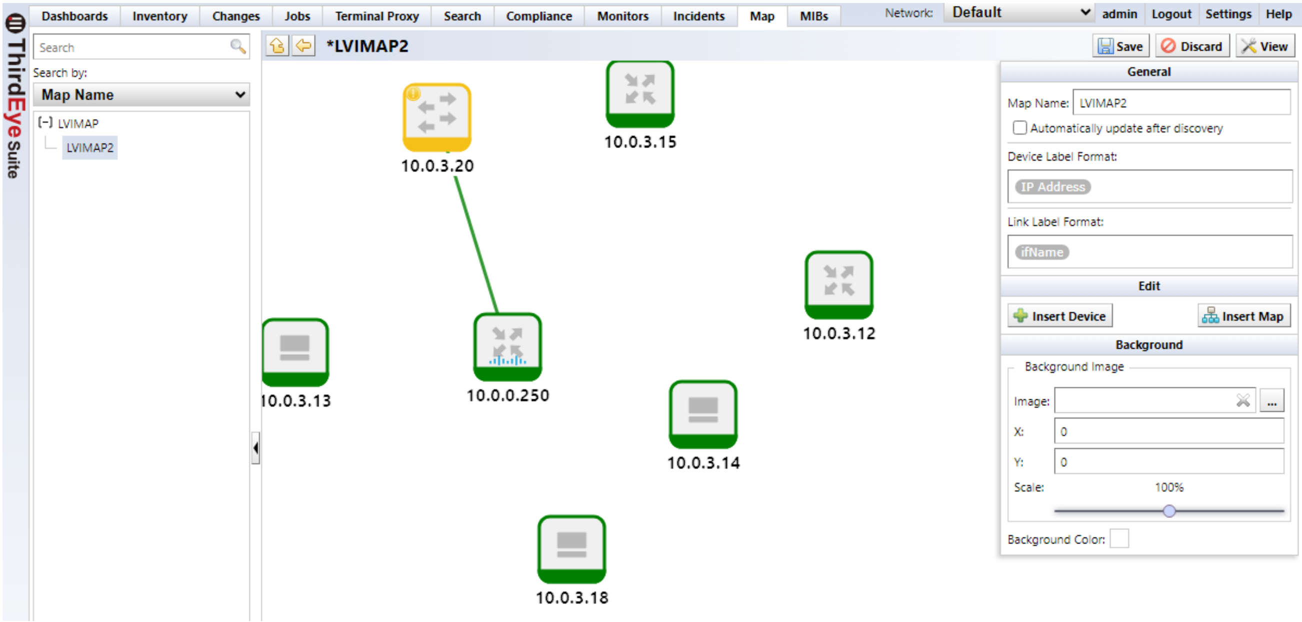
☑ Link to existing nodes

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.



Network: Default

Search by: Map Name

*LVIMAP2

General

Map Name: LVIMAP2

□ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Background Image

Image:

X: 0

Y: 0

Scale: 100%

Background Color:

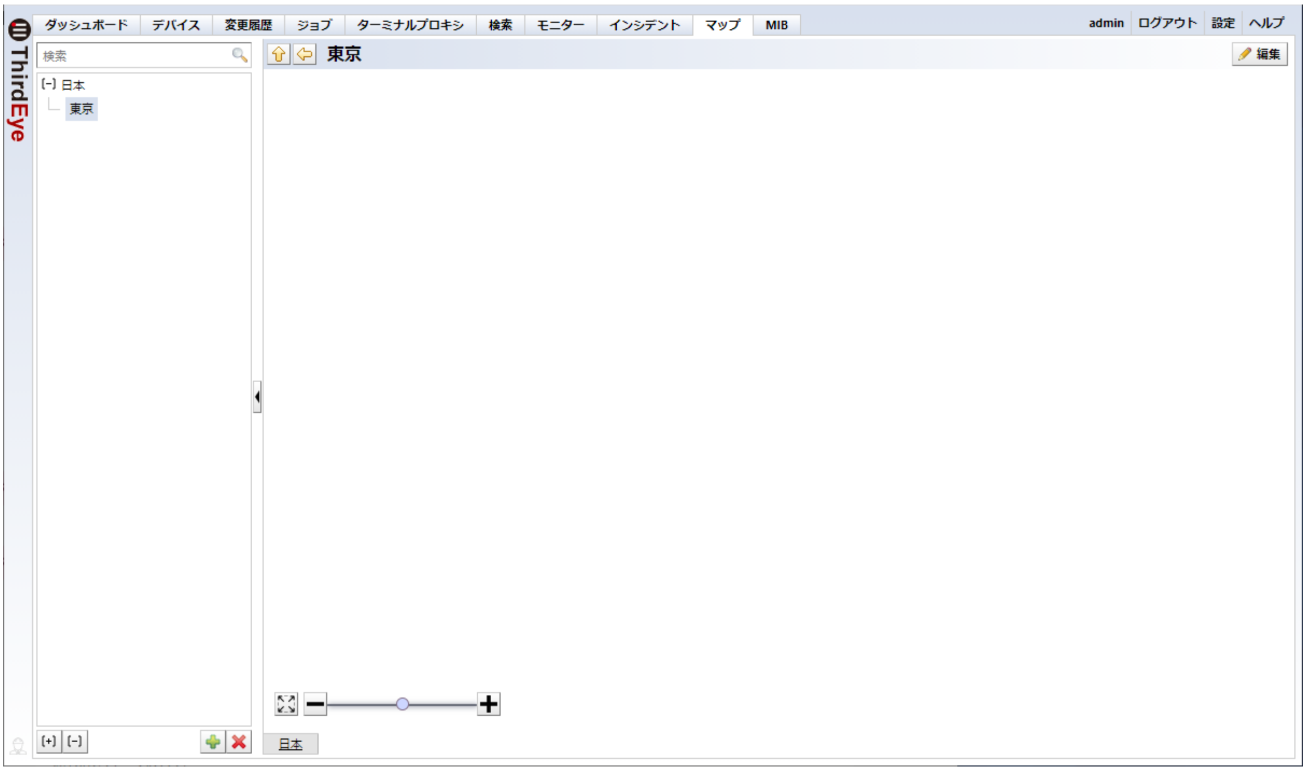
12.3 Create Topology Map

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.

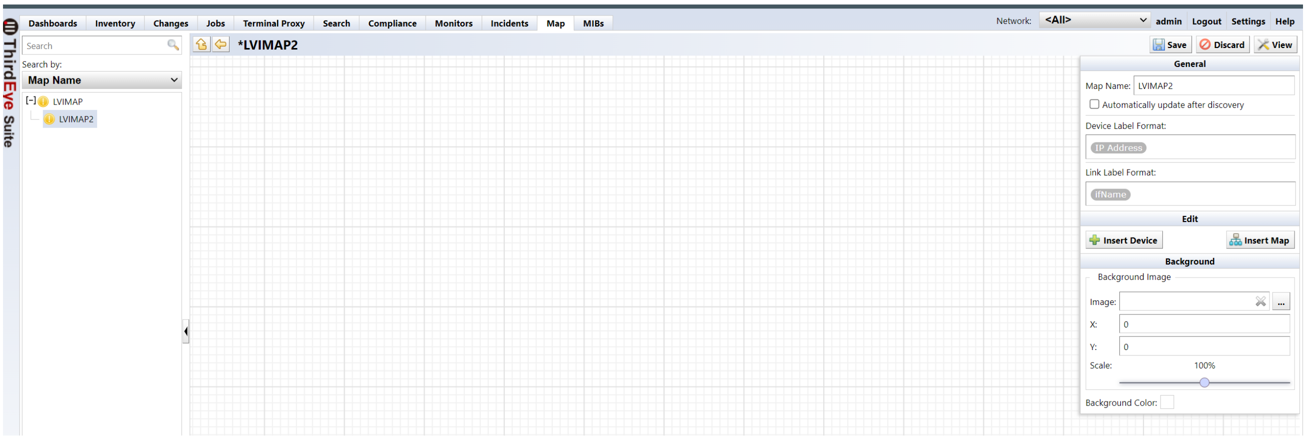
When using the topology function:

- 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].



Search by: Map Name

Map Name: LVIMAP2

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image:

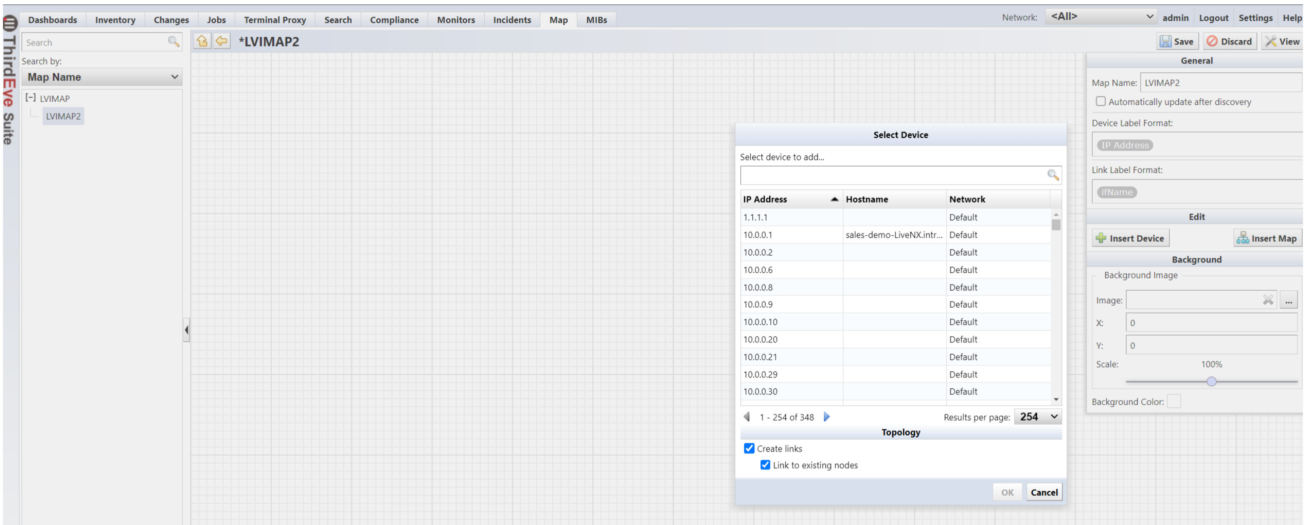
X: 0

Y: 0

Scale: 100%

Background Color:

3. Select the device you want to insert into the map, check “Create link”, and click [OK].



Select device to add...

IP Address	Hostname	Network
1.1.1.1		Default
10.0.0.1	sales-demo-LiveNX.intr...	Default
10.0.0.2		Default
10.0.0.6		Default
10.0.0.8		Default
10.0.0.9		Default
10.0.0.10		Default
10.0.0.20		Default
10.0.0.21		Default
10.0.0.29		Default
10.0.0.30		Default

1 - 254 of 348   Results per page: 254

☑ Create links

☑ Link to existing nodes

Search by: Map Name

Map Name: LVIMAP2

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image:

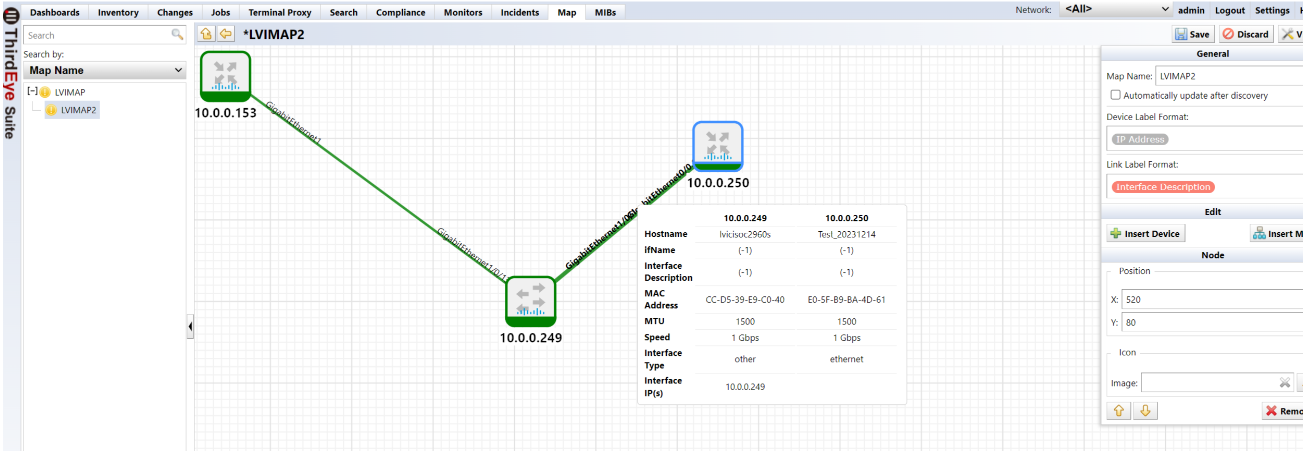
X: 0

Y: 0

Scale: 100%

Background Color:

4. After the device object is inserted, click [Save] to complete your edits.



	10.0.0.249	10.0.0.250
Hostname	lvicisoc2960s	Test_20231214
ifName	(-1)	(-1)
Interface Description	(-1)	(-1)
MAC Address	CC-D5-39-E9-C0-40	E0-5F-B9-BA-4D-61
MTU	1500	1500
Speed	1 Gbps	1 Gbps
Interface Type	other	ethernet
Interface IP(s)	10.0.0.249	

Search by: Map Name

Map Name: LVIMAP2

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: Interface Description

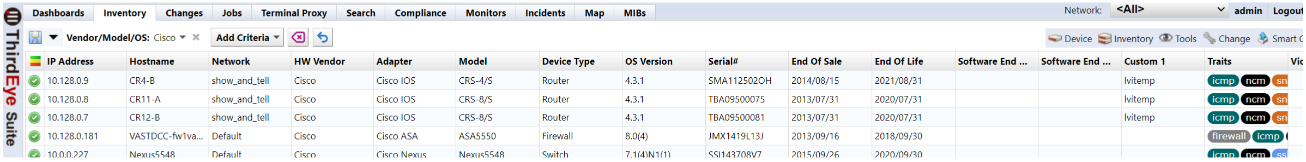
X: 520

Y: 80

Image:

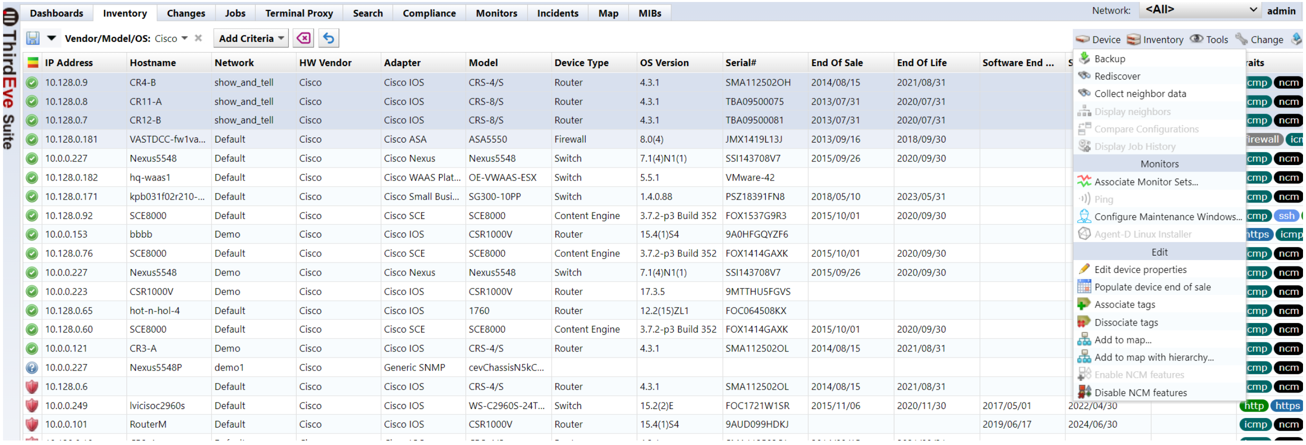
12.4 Create Custom Field Map

You can use information from custom fields to create maps. By selecting a device, you can create a location map for the selected device.



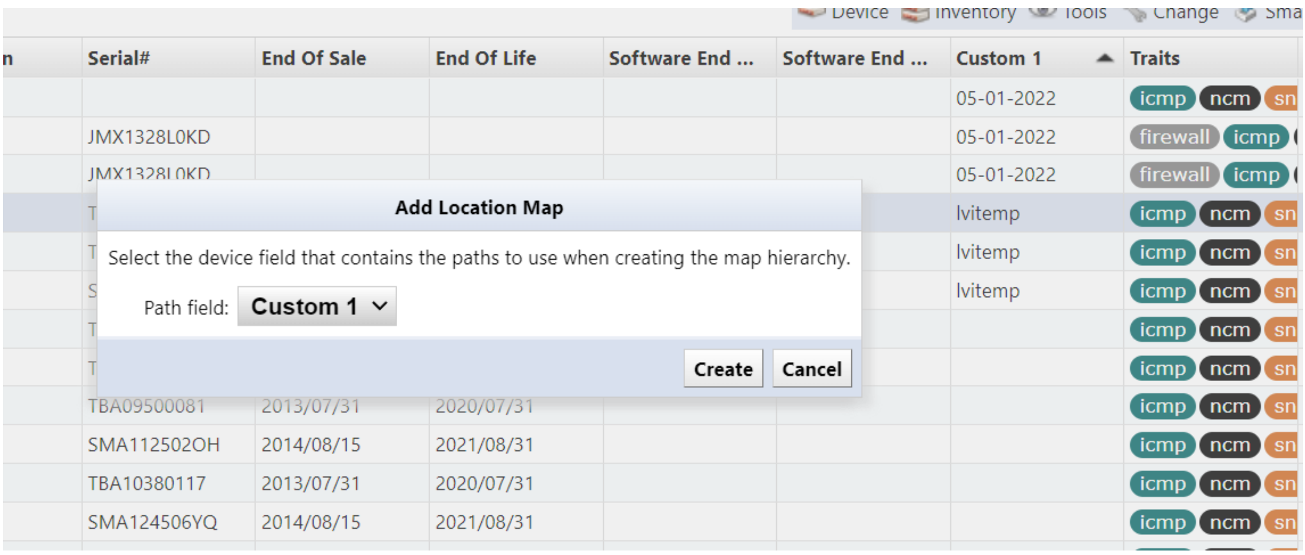
IP Address	Hostname	Network	HW Vendor	Adapter	Model	Device Type	OS Version	Serial#	End Of Sale	End Of Life	Software End ...	Software End ...	Custom 1	Traits
10.128.0.9	CR4-B	show_and_tell	Cisco	Cisco IOS	CRS-4/S	Router	4.3.1	SMA112502OH	2014/08/15	2021/08/31			lvitemp	icmp ncm sn
10.128.0.8	CR11-A	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500075	2013/07/31	2020/07/31			lvitemp	icmp ncm sn
10.128.0.7	CR12-B	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500081	2013/07/31	2020/07/31			lvitemp	icmp ncm sn
10.128.0.181	VASTDCC-fw1va...	Default	Cisco	Cisco ASA	ASA5550	Firewall	8.0(4)	JMX1419L13J	2013/09/16	2018/09/30				firewall icmp
10.0.0.227	Nexus5548	Default	Cisco	Cisco Nexus	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	2015/09/26	2020/09/30				icmp ncm ss

1. In the [Inventory] tab, click **Devices** in the right panel, then click [Add to map].



IP Address	Hostname	Network	HW Vendor	Adapter	Model	Device Type	OS Version	Serial#	End Of Sale	End Of Life	Software End ...	S	aits
10.128.0.9	CR4-B	show_and_tell	Cisco	Cisco IOS	CRS-4/S	Router	4.3.1	SMA112502OH	2014/08/15	2021/08/31			cmp ncm
10.128.0.8	CR11-A	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500075	2013/07/31	2020/07/31			cmp ncm
10.128.0.7	CR12-B	show_and_tell	Cisco	Cisco IOS	CRS-8/S	Router	4.3.1	TBA09500081	2013/07/31	2020/07/31			cmp ncm
10.128.0.181	VASTDCC-fw1va...	Default	Cisco	Cisco ASA	ASA5550	Firewall	8.0(4)	JMX1419L13J	2013/09/16	2018/09/30			irewall icn
10.0.0.227	Nexus5548	Default	Cisco	Cisco Nexus	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	2015/09/26	2020/09/30			cmp ncm
10.128.0.182	hq-waas1	Default	Cisco	Cisco WAAS Plat...	OE-VWAAS-ESX	Switch	5.5.1	VMware-42					cmp ncm
10.128.0.171	kpb031f02r210-...	Default	Cisco	Cisco Small Busi...	SG300-10PP	Switch	1.4.0.88	PSZ18391FN8	2018/05/10	2023/05/31			cmp ncm
10.128.0.92	SCE8000	Default	Cisco	Cisco SCE	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1537G9R3	2015/10/01	2020/09/30			cmp ssh
10.0.0.153	bbbb	Demo	Cisco	Cisco IOS	CSR1000V	Router	15.4(1)S4	9A0HFGQYZF6					ttps icmp
10.128.0.76	SCE8000	Default	Cisco	Cisco SCE	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1414GAXK	2015/10/01	2020/09/30			cmp ncm
10.0.0.227	Nexus5548	Demo	Cisco	Cisco Nexus	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	2015/09/26	2020/09/30			cmp ncm
10.0.0.223	CSR1000V	Demo	Cisco	Cisco IOS	CSR1000V	Router	17.3.5	9MTTHU5FGVS					cmp ncm
10.128.0.65	hot-n-hol-4	Default	Cisco	Cisco IOS	1760	Router	12.2(15)ZL1	FOC064508KX					cmp ncm
10.128.0.60	SCE8000	Default	Cisco	Cisco SCE	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1414GAXK	2015/10/01	2020/09/30			cmp ncm
10.0.0.121	CR3-A	Demo	Cisco	Cisco IOS	CRS-4/S	Router	4.3.1	SMA112502OL	2014/08/15	2021/08/31			cmp ncm
10.0.0.227	Nexus5548P	demo1	Cisco	Generic SNMP	cevChassisN5kC...								cmp ncm
10.128.0.6		Default	Cisco	Cisco IOS	CRS-4/S	Router	4.3.1	SMA112502OL	2014/08/15	2021/08/31			cmp ncm
10.0.0.249	lvicisoc2960s	Default	Cisco	Cisco IOS	WS-C2960S-24T...	Switch	15.2(2)E	FOC1721W1SR	2015/11/06	2020/11/30	2017/05/01	2022/04/30	http https
10.0.0.101	RouterM	Default	Cisco	Cisco IOS	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ			2019/06/17	2024/06/30	icmp ncm

2. Select a custom field and click [Create].

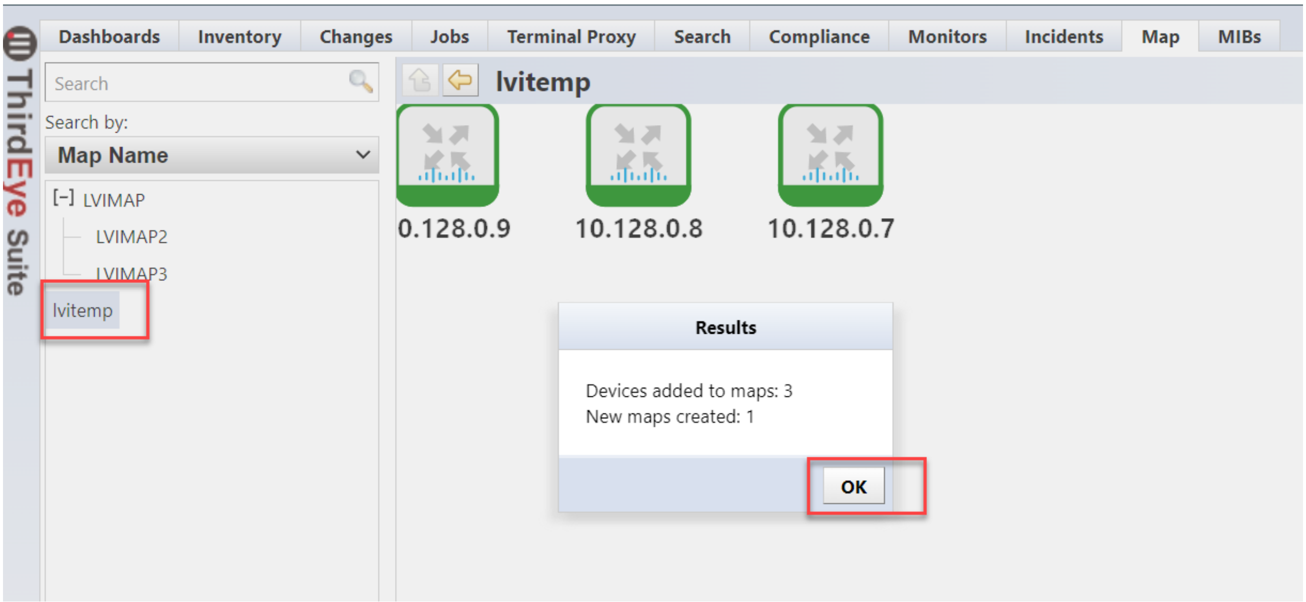


Select the device field that contains the paths to use when creating the map hierarchy.

Path field: Custom 1

Serial#	End Of Sale	End Of Life	Software End ...	Software End ...	Custom 1	Traits
					05-01-2022	icmp ncm sn
JMX1328L0KD					05-01-2022	firewall icmp
JMX1328L0KD					05-01-2022	firewall icmp
T					lvitemp	icmp ncm sn
T					lvitemp	icmp ncm sn
S					lvitemp	icmp ncm sn
T						icmp ncm sn
T						icmp ncm sn
TBA09500081	2013/07/31	2020/07/31				icmp ncm sn
SMA112502OH	2014/08/15	2021/08/31				icmp ncm sn
TBA10380117	2013/07/31	2020/07/31				icmp ncm sn
SMA124506YQ	2014/08/15	2021/08/31				icmp ncm sn

3. Click [OK].

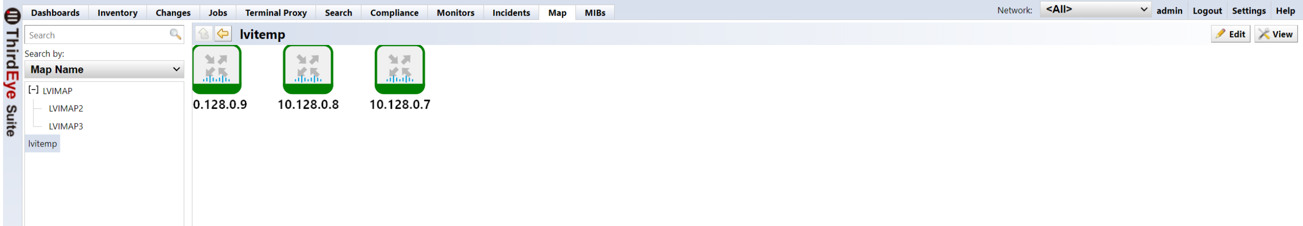


Devices added to maps: 3
New maps created: 1

12.5 Object Icons

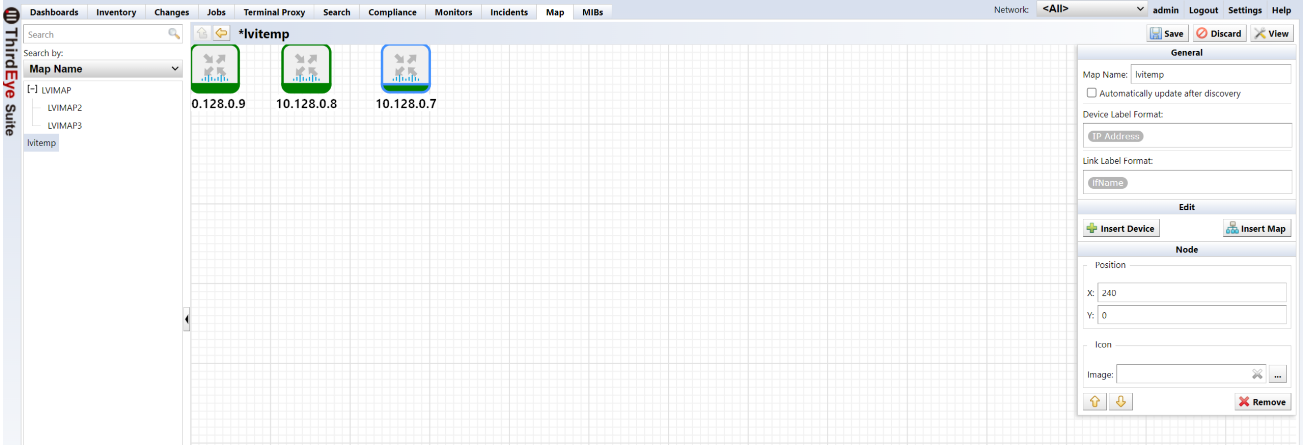
You can change the icon of an object.

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].



Map Name: lvitemp

□ Automatically update after discovery

Device Label Format: IP Address

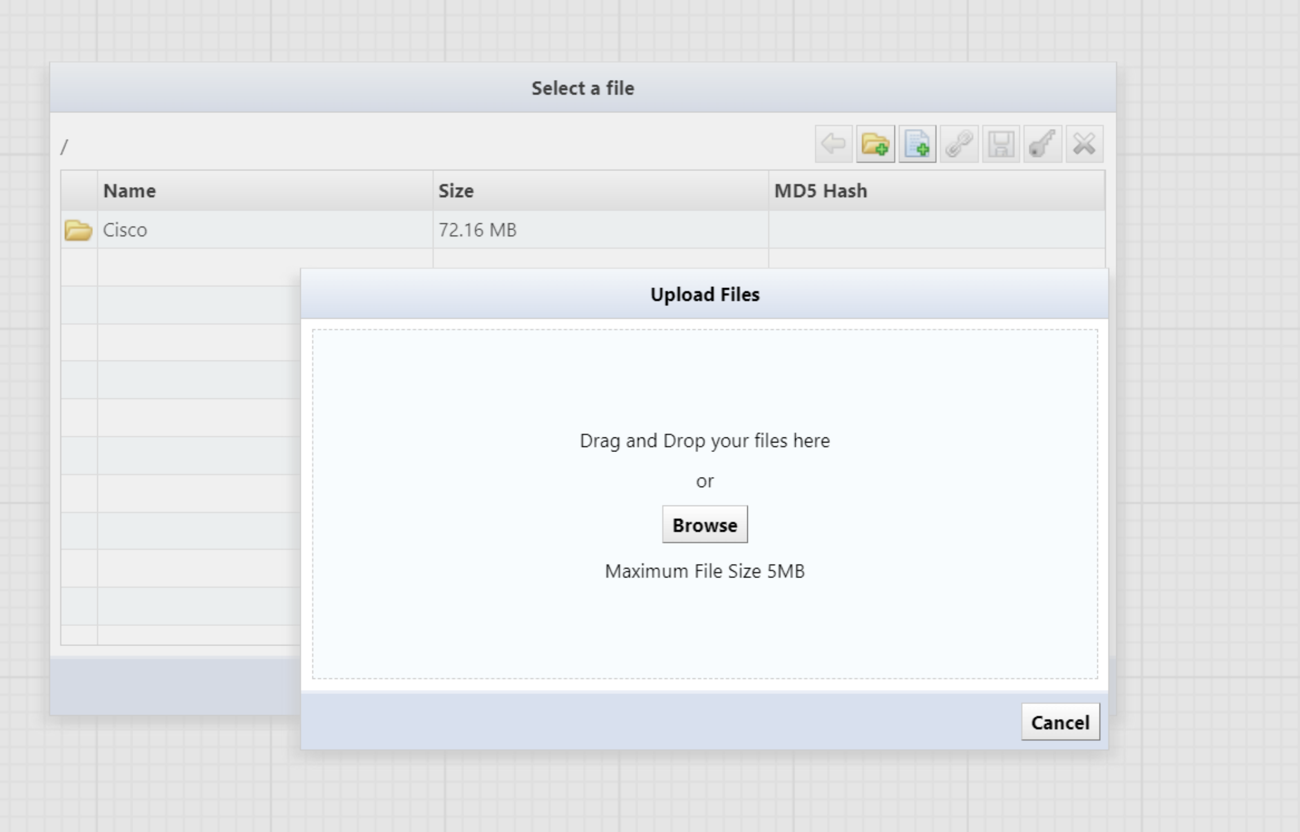
Link Label Format: ifName

X: 240

Y: 0

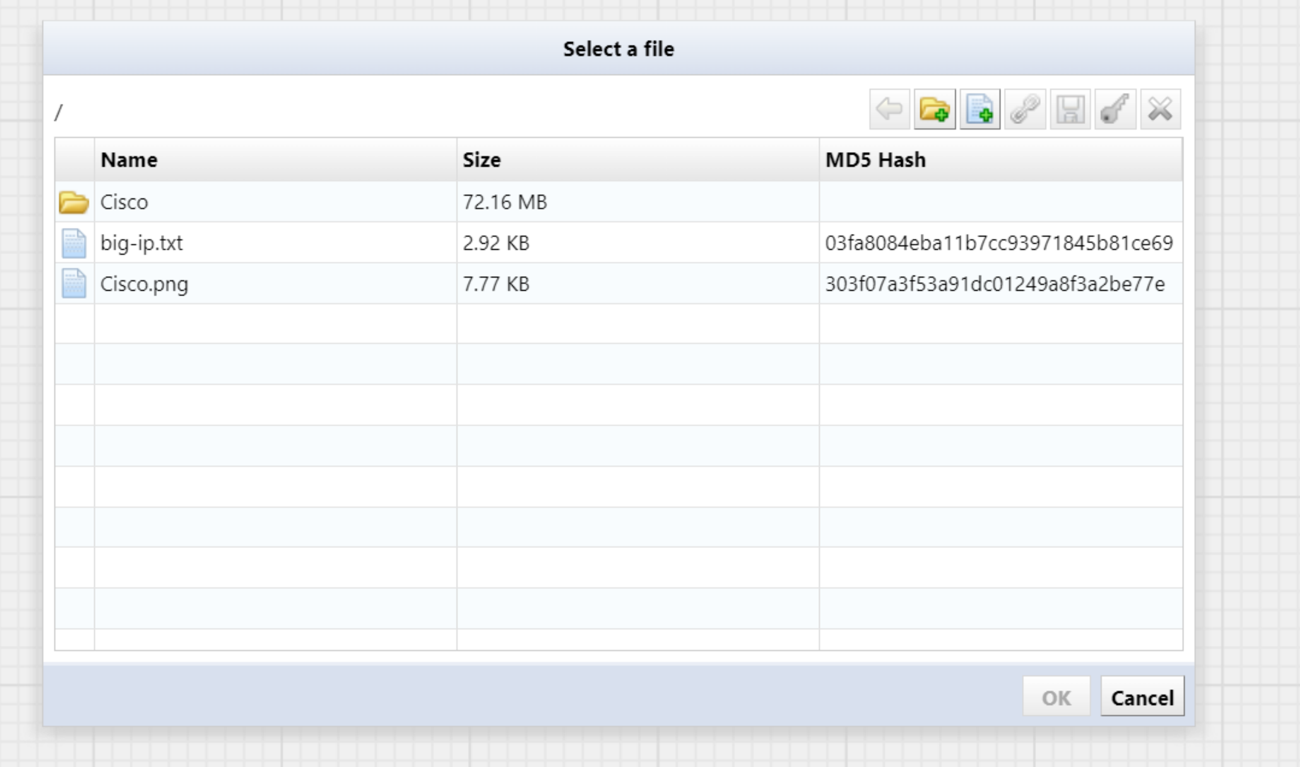
A file selection screen will be displayed.

4. Click the ⊞ button, and upload the file.



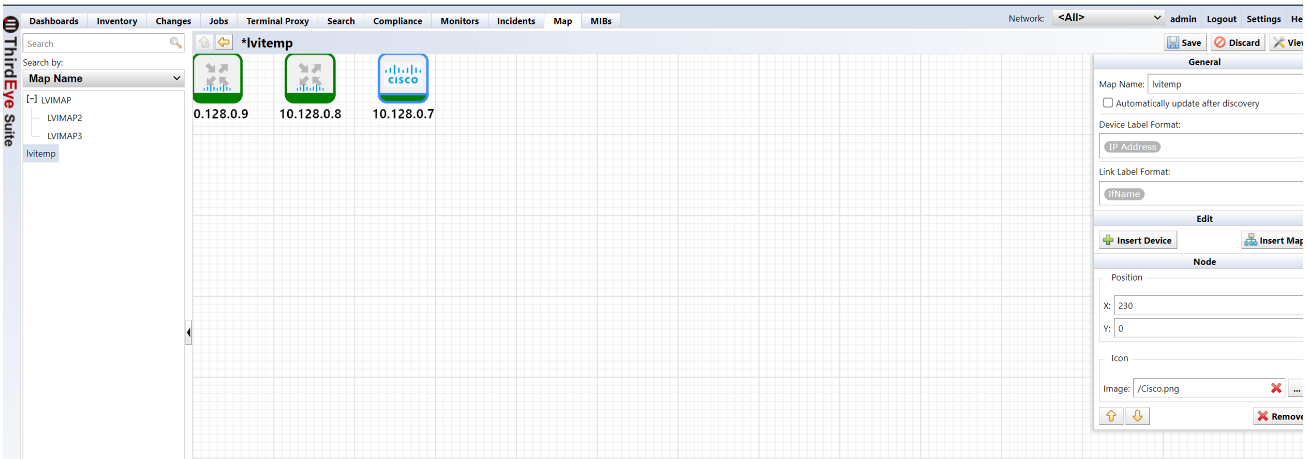
5. Select the icon you want to upload.

6. Select the file you want to set as the icon image and click [OK].



Name	Size	MD5 Hash
Cisco	72.16 MB	
big-ip.txt	2.92 KB	03fa8084eba11b7cc93971845b81ce69
Cisco.png	7.77 KB	303f07a3f53a91dc01249a8f3a2be77e

The object’s icon will change to the selected image.



Network: <All>

Search by: Map Name

Map Name: lvitemp

□ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

X: 230

Y: 0

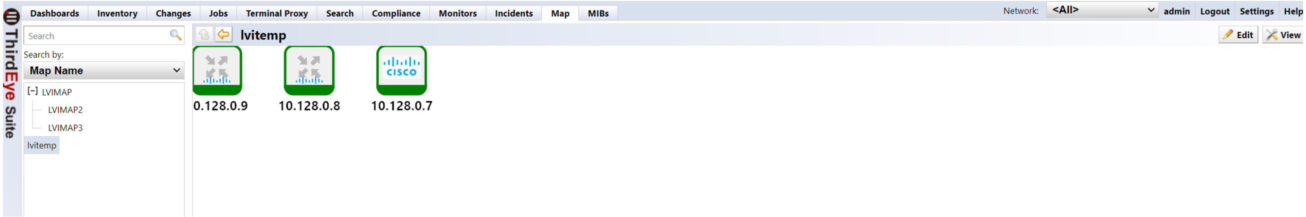
Image: /Cisco.png

12.6 Link Lines

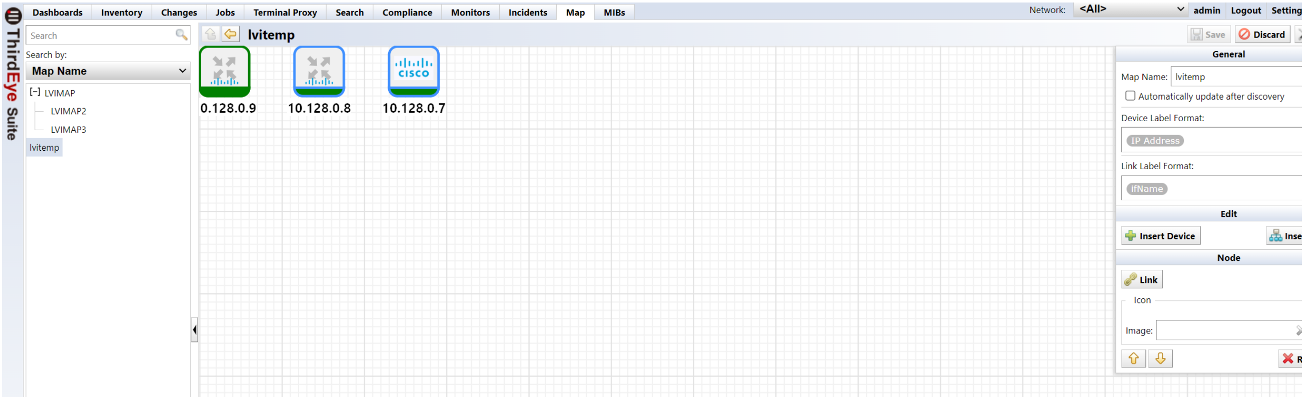
You can connect objects such as maps and devices with Link Lines.

The thickness of the Link Line cannot be changed.

1. Doubleclick the map to open it, and click [Edit].

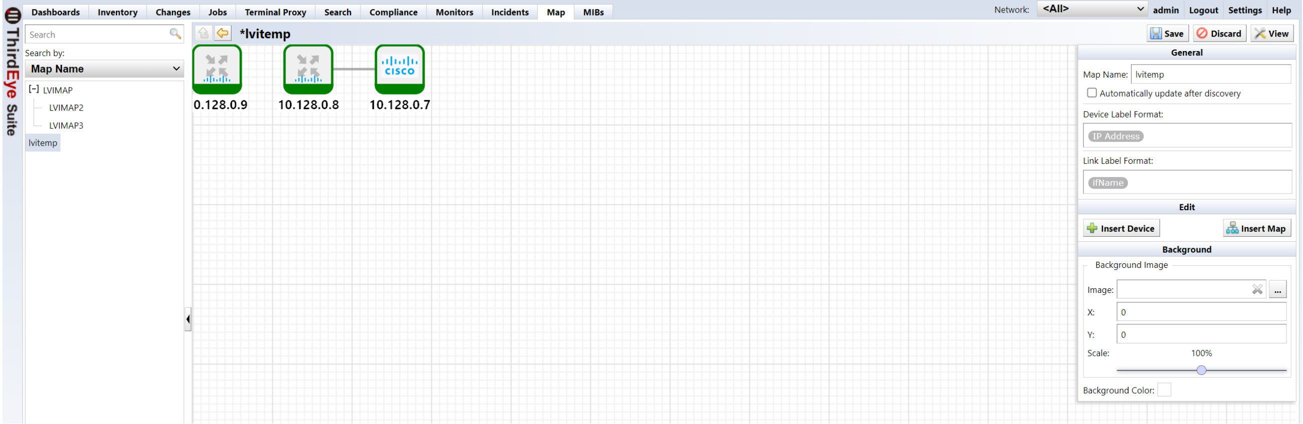


2. To select the devices, hold the [Ctrl] key on your keyboard, and click the two devices you want to connect with the Link Line. With the devices selected, click [Insert Link Line].



3. Once the Link Line is inserted, click [Save].

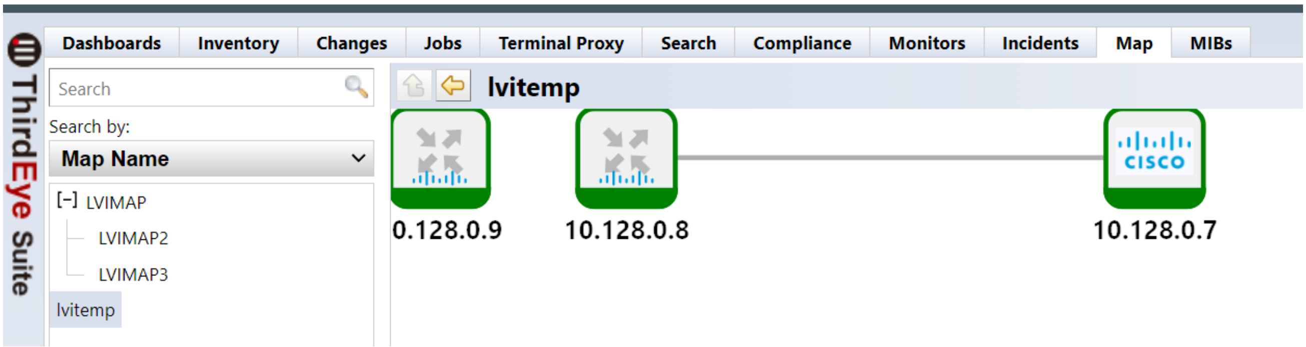
If you want to delete the Link Line, select the two devices and click [Delete link line]



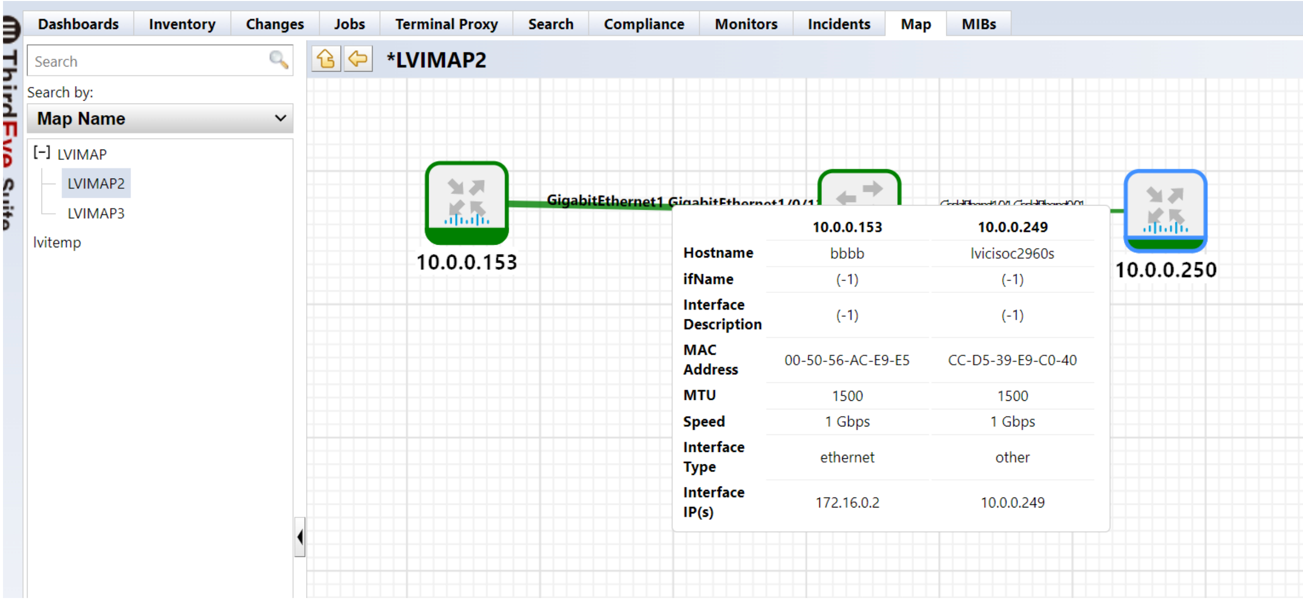
12.7 Attach Interface to Link Line

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:

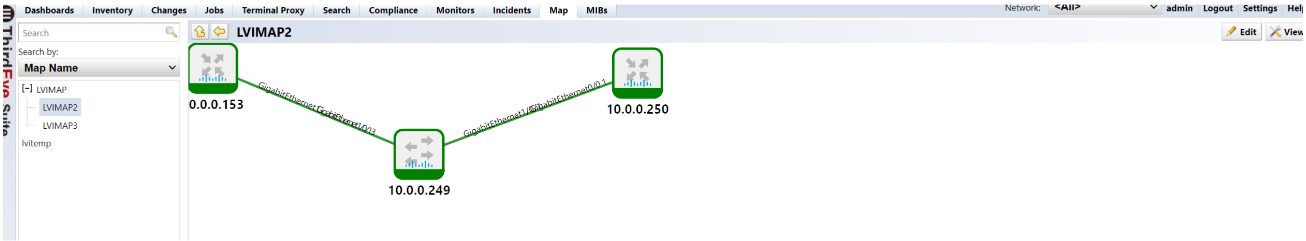


Example of status when device interface is linked to the link line:

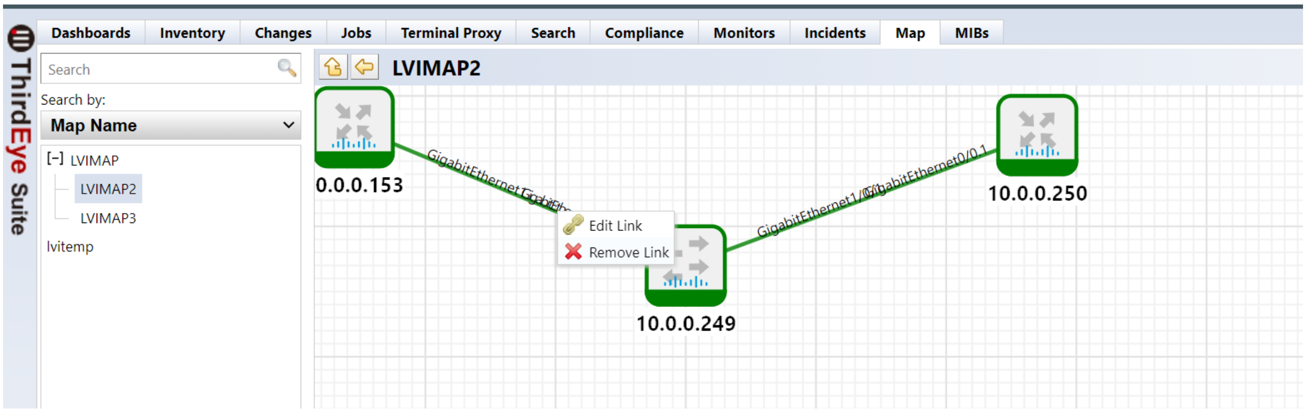


	10.0.0.153	10.0.0.249
Hostname	bbbb	lvicisoc2960s
ifName	(-1)	(-1)
Interface Description	(-1)	(-1)
MAC Address	00-50-56-AC-E9-E5	CC-D5-39-E9-C0-40
MTU	1500	1500
Speed	1 Gbps	1 Gbps
Interface Type	ethernet	other
Interface IP(s)	172.16.0.2	10.0.0.249

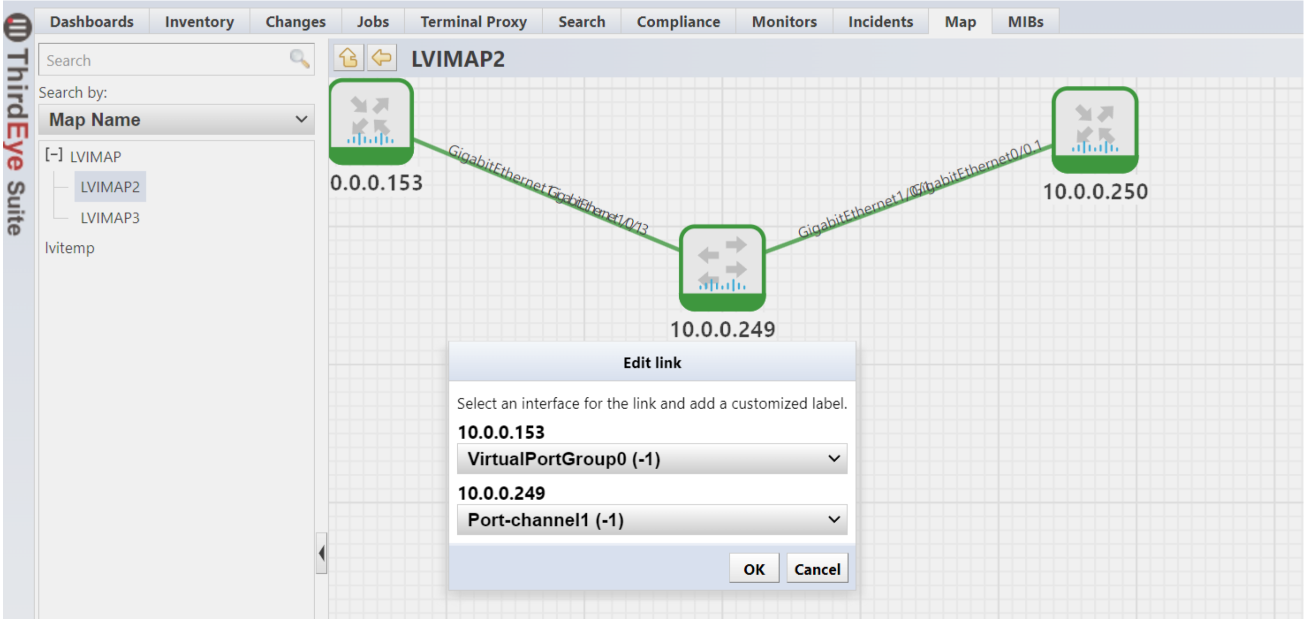
1. Doubleclick the Map to open it and click [Edit].



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].

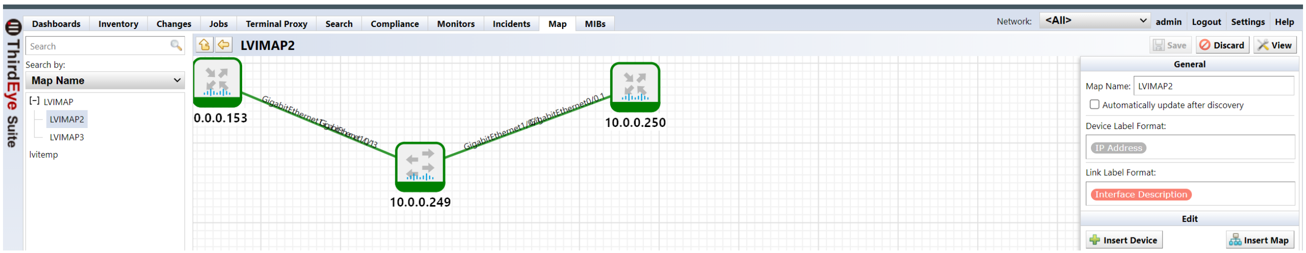


Select an interface for the link and add a customized label.

10.0.0.153: VirtualPortGroup0 (-1)

10.0.0.249: Port-channel1 (-1)

4. Click [Save].



Map Name: LVIMAP2

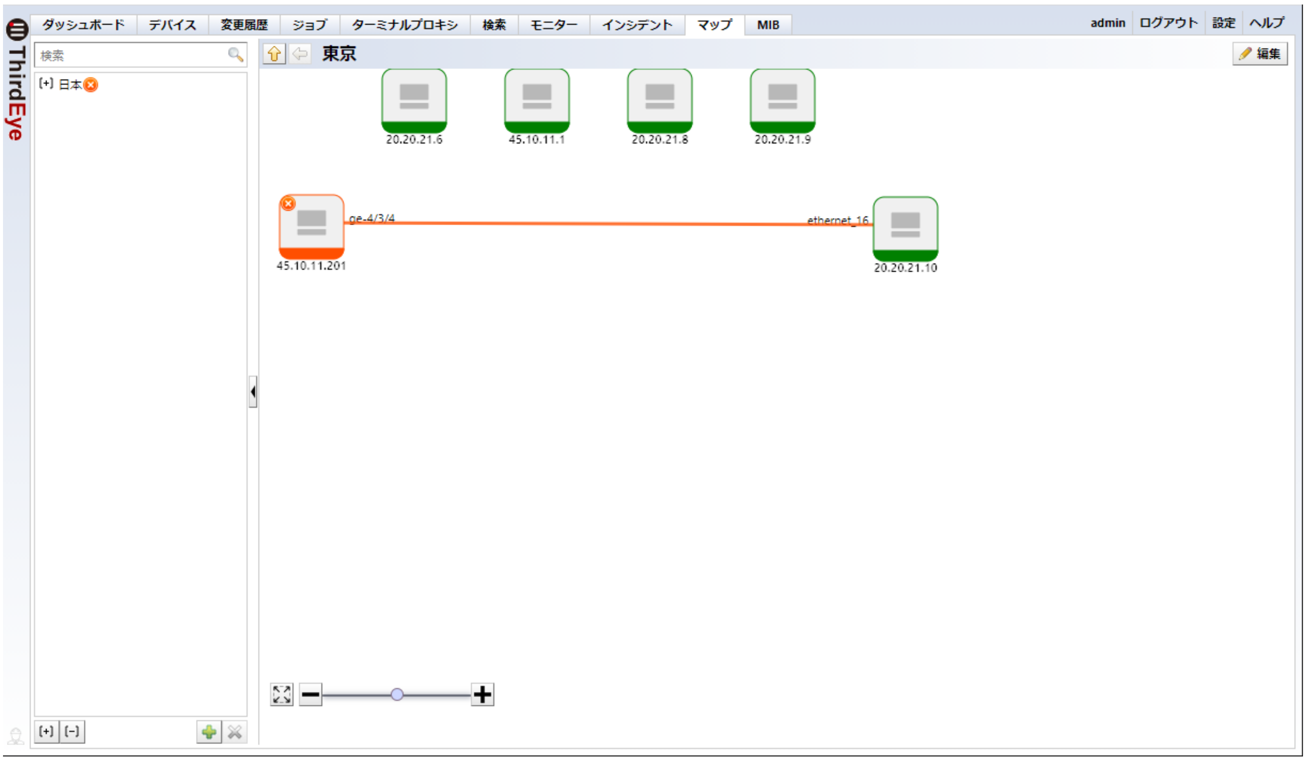
□ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: Interface Description

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.

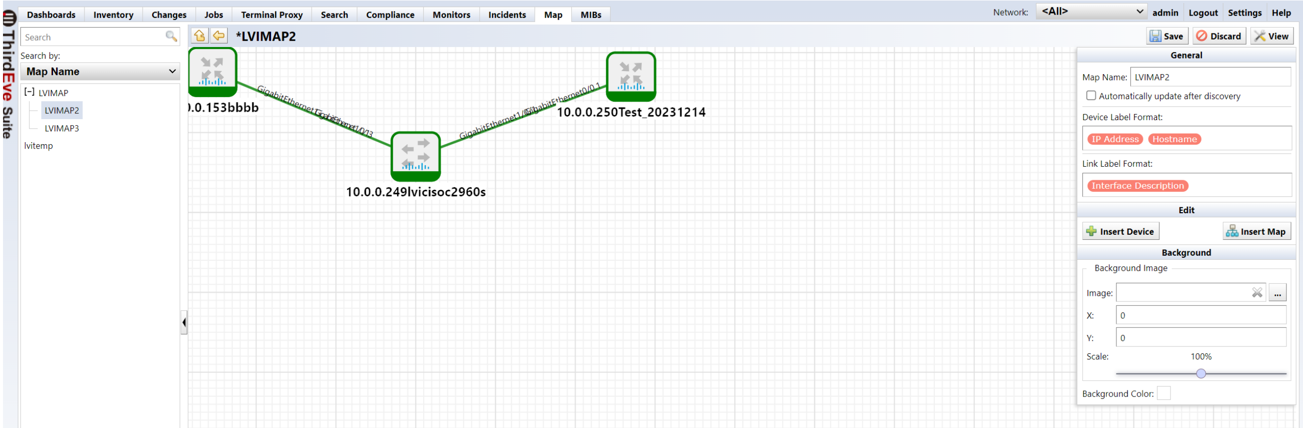


12.8 Changing Display Formats

You can customize the display format of the strings (labels). You can also customize the device 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.



Map Name: LVIMAP2

☐ Automatically update after discovery

Device Label Format: IP Address Hostname

Link Label Format: Interface Description

Image:

X: 0

Y: 0

Scale: 100%

Background Color:

The objects available for each label format are shown in the table below.

Device label format

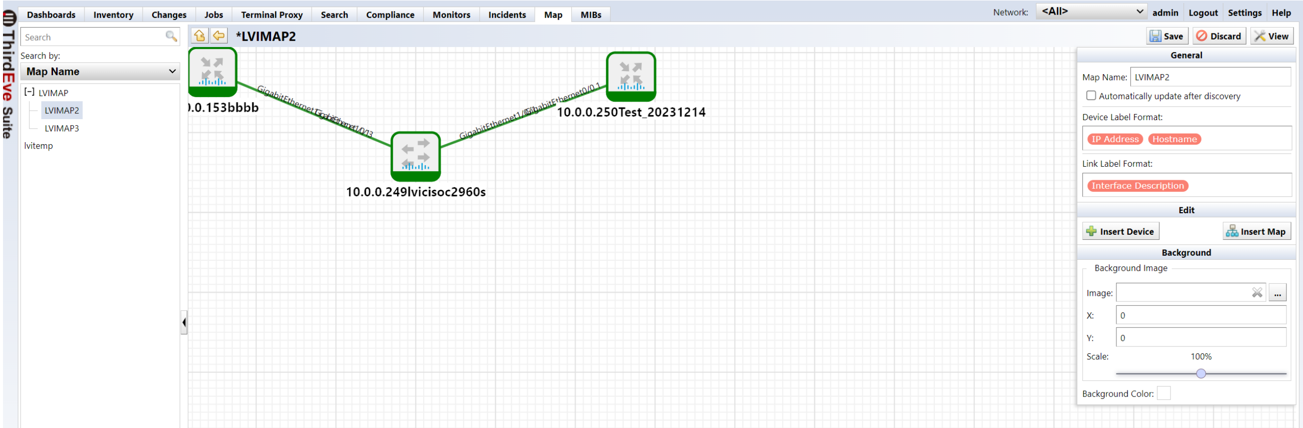
Menu Item	Explanation
IP address	Display the device’s IP address. (initial value)
hostname	Display the device hostname.
network	View your device’s network.
adapter	Show device adapters.
device type	Display the device type of a device.
hard bender	Display the device’s hardware vendor.
software vendor	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.

Menu Item	Explanation
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].



Map Name: LVIMAP2

☐ Automatically update after discovery

Device Label Format: IP Address Hostname

Link Label Format: Interface Description

Image:

X: 0

Y: 0

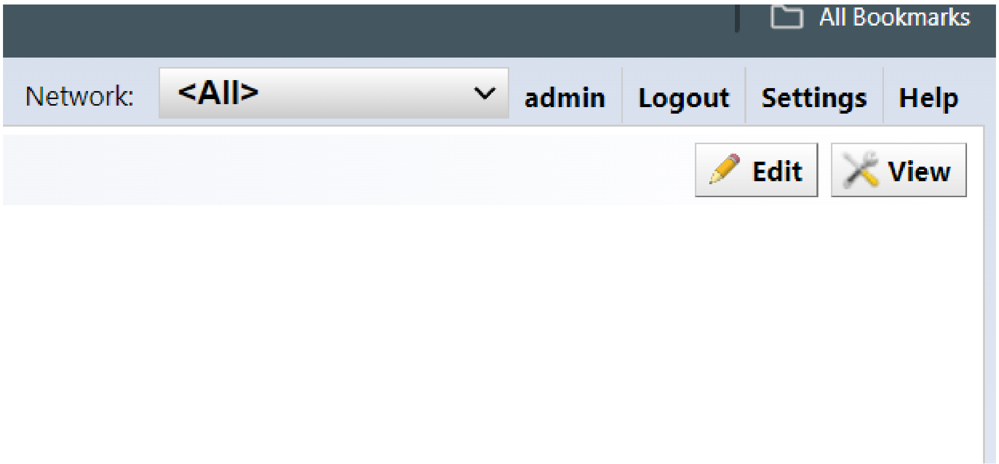
Scale: 100%

Background Color:

12.9 Changing Default Device Labels

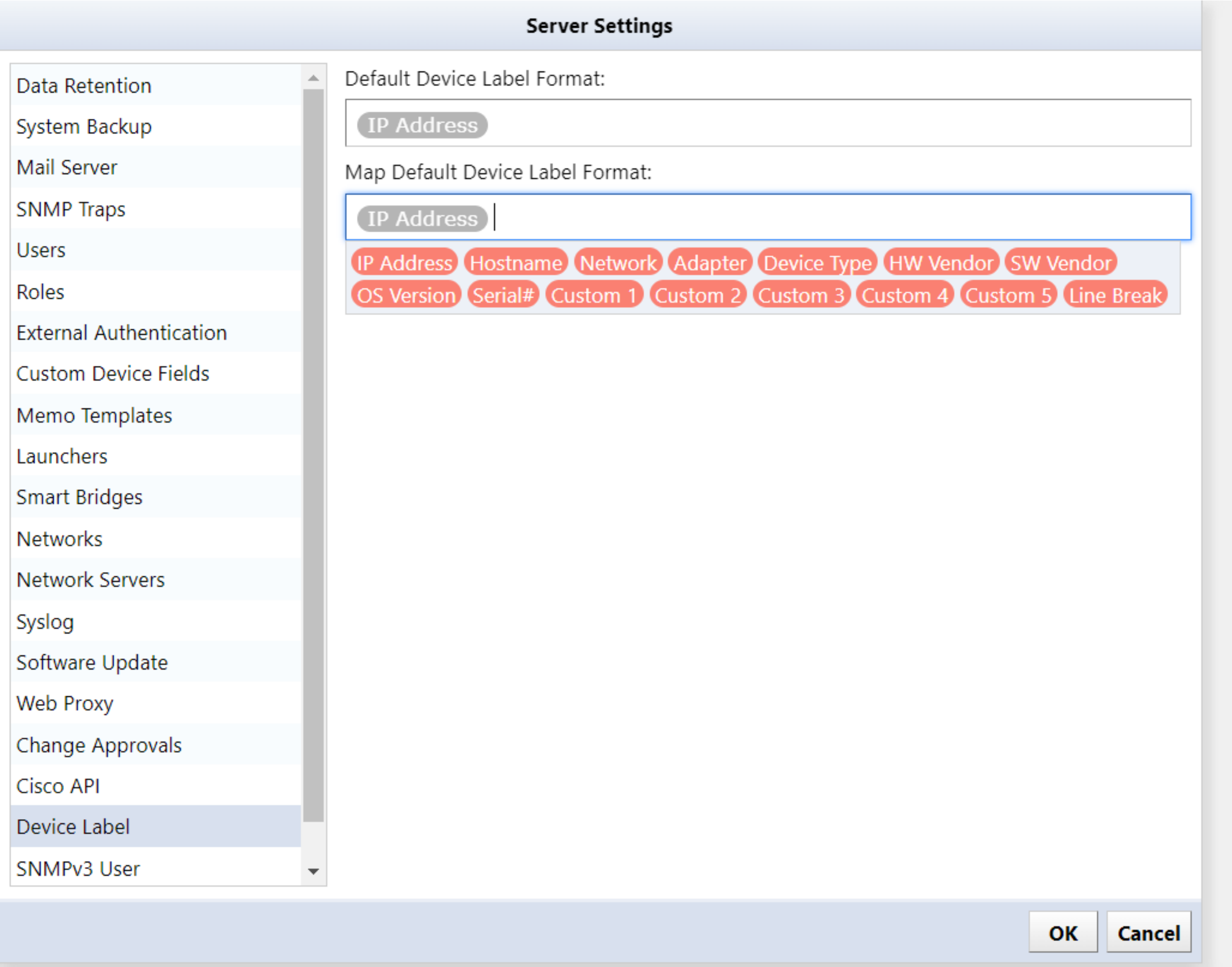
You can specify the default device label format when creating a new map. Maps will automatically reflect any changes in the settings. Changes will not be reflected in previously created maps.

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.



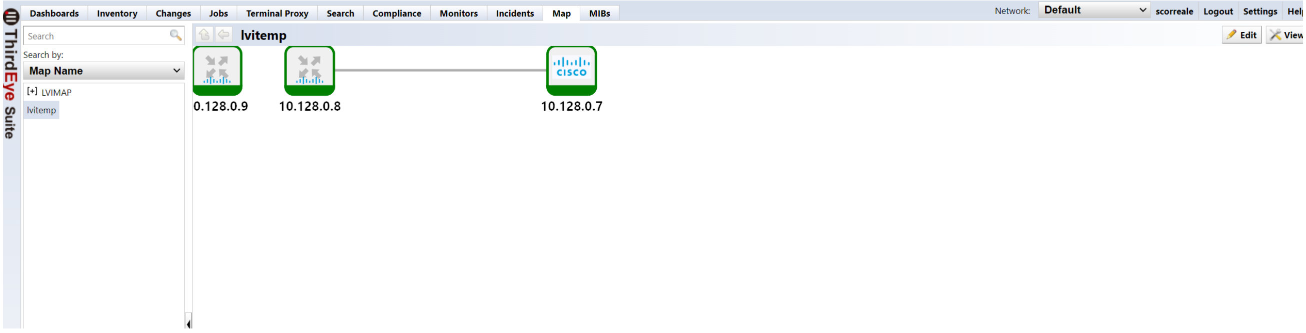
Server Settings

Default Device Label Format: IP Address

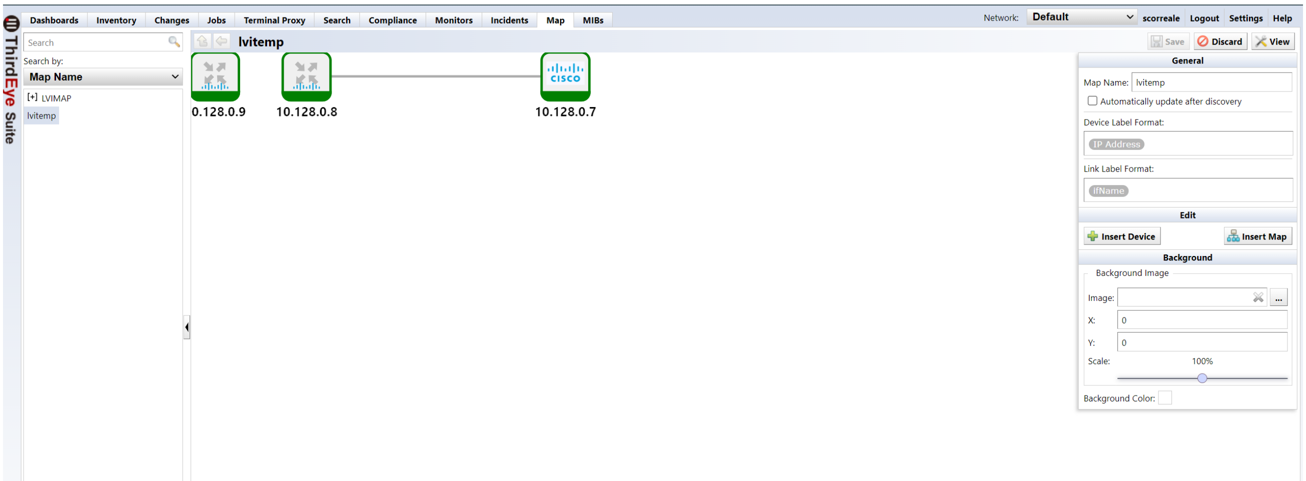
Map Default Device Label Format: IP Address

12.10 Changing 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.



Map Name: lvitemp

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image:

X: 0

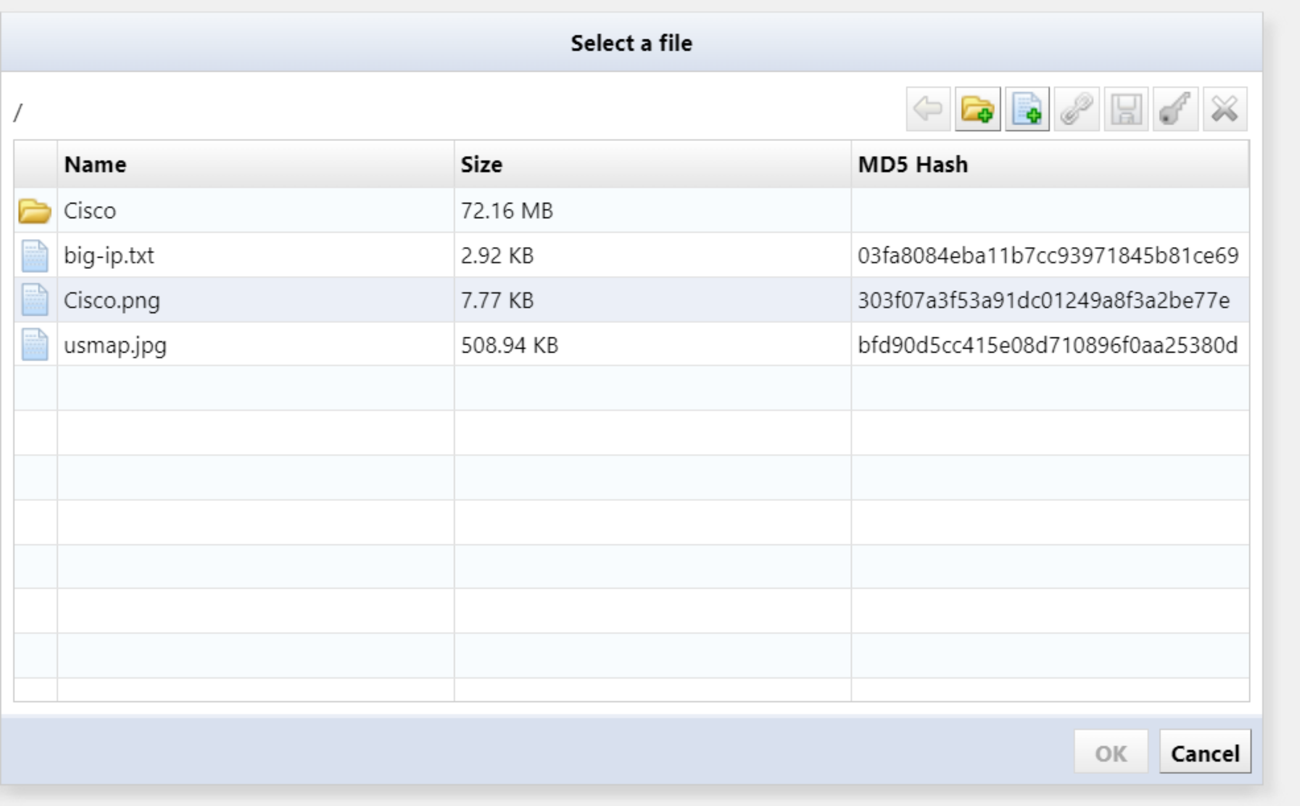
Y: 0

Scale: 100%

Background Color:

A file selection screen will be displayed.

3. Select the file you want to set as the background image and click [OK].



Select a file

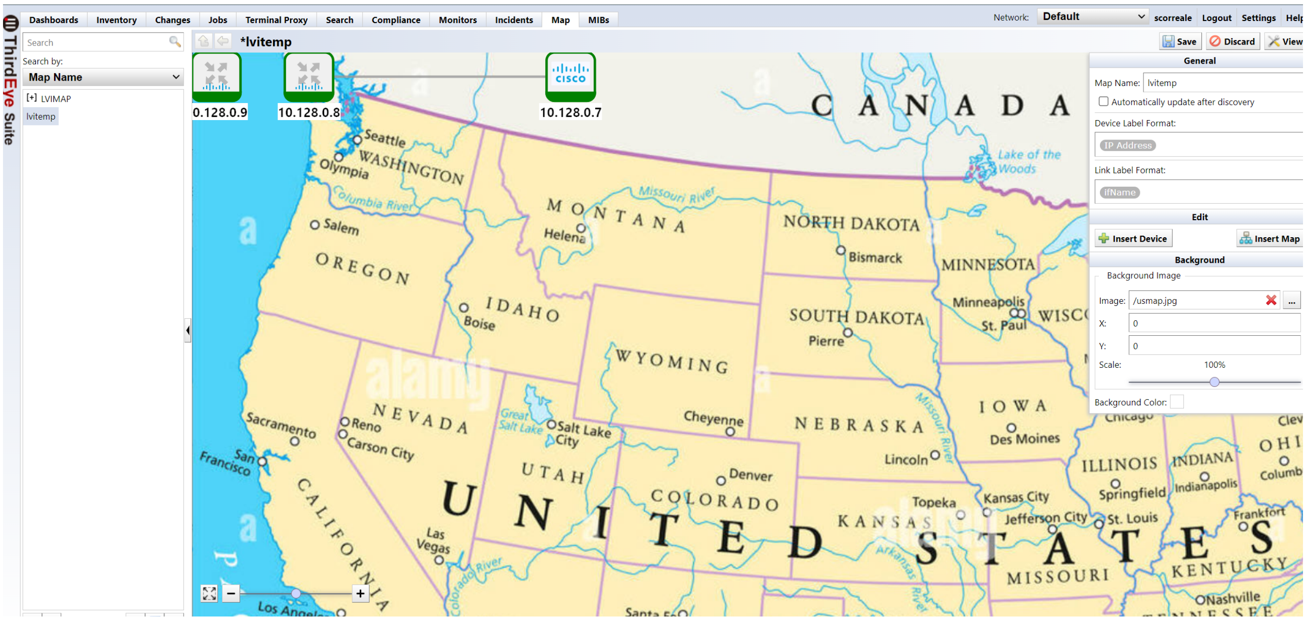
/

	Name	Size	MD5 Hash
	Cisco	72.16 MB	
	big-ip.txt	2.92 KB	03fa8084eba11b7cc93971845b81ce69
	Cisco.png	7.77 KB	303f07a3f53a91dc01249a8f3a2be77e
	usmap.jpg	508.94 KB	bfd90d5cc415e08d710896f0aa25380d

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.



Network: Default

Search by: Map Name

Map Name: lvitemp

□ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image: /usmap.jpg

X: 0

Y: 0

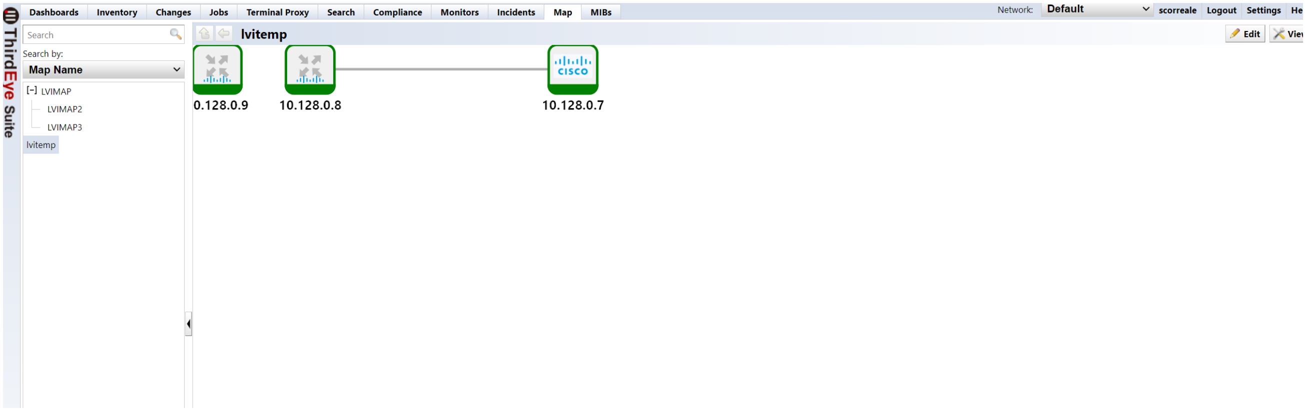
Scale: 100%

Background Color:

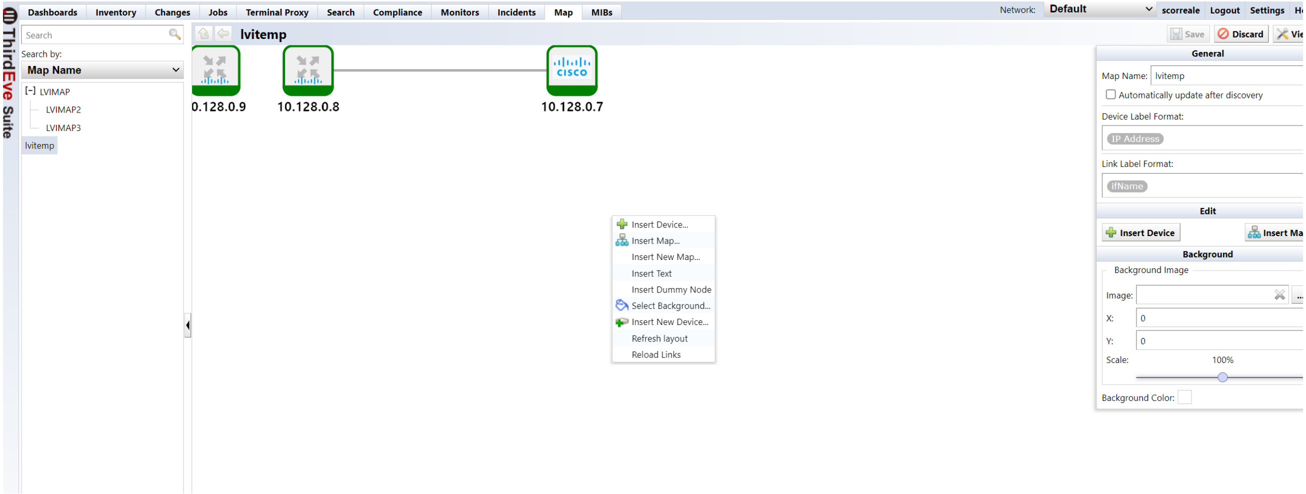
12.11 Map Tree

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.



Map Name: lvitemp

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image:

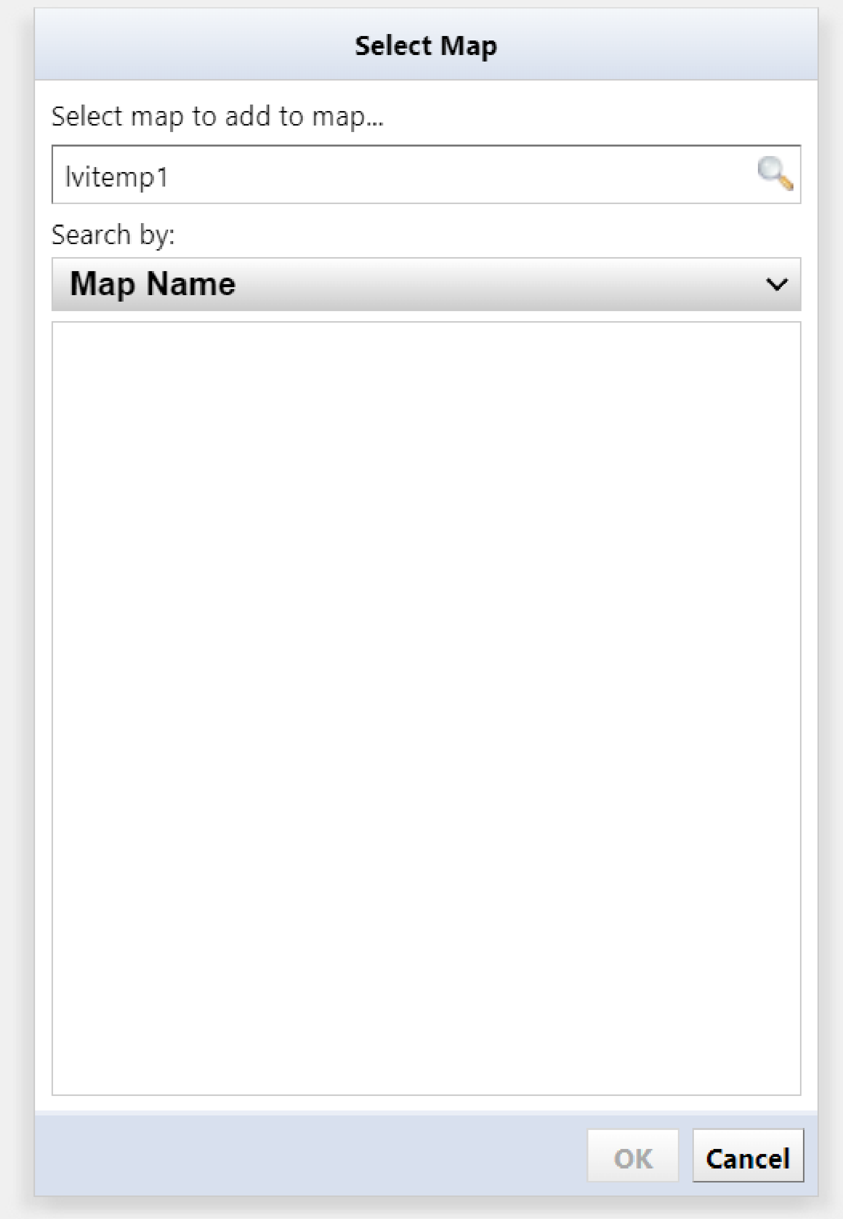
X: 0

Y: 0

Scale: 100%

Background Color:

3. Select the map you want to insert as a child and click [OK].



Select map to add to map...

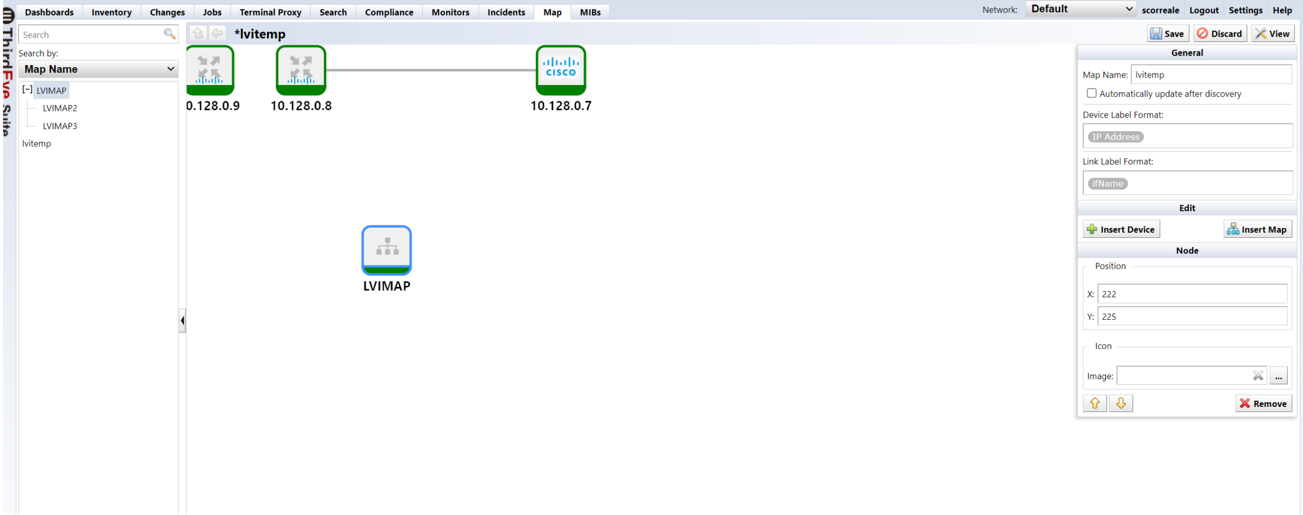
lvitemp1

Search by:

Map Name

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].



Map Name: lvitemp

☐ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

X: 222

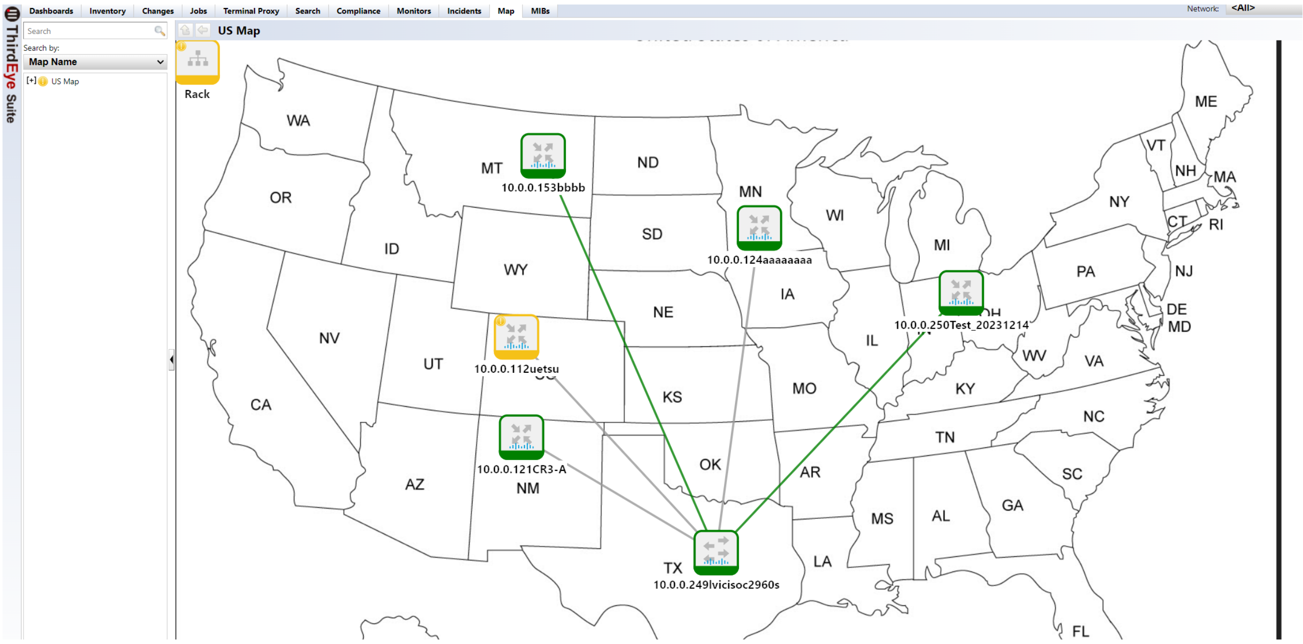
Y: 225

Image:

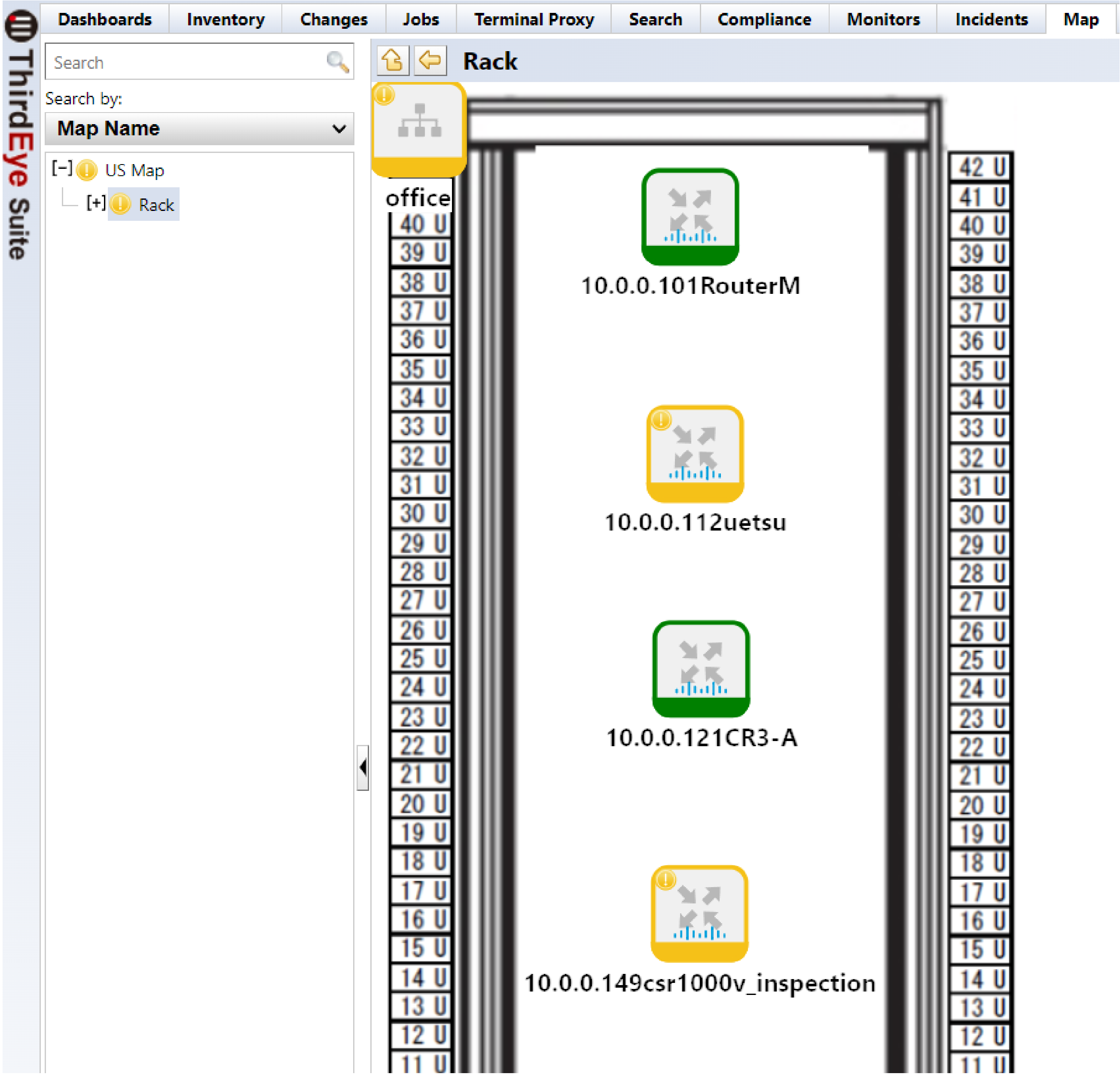
Once the child is added, it will be viewable in a tree view in the left sidebar. You can expand or collapse the tree by clicking the [+] or [-] symbols to the left of the map name.

12.12 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.

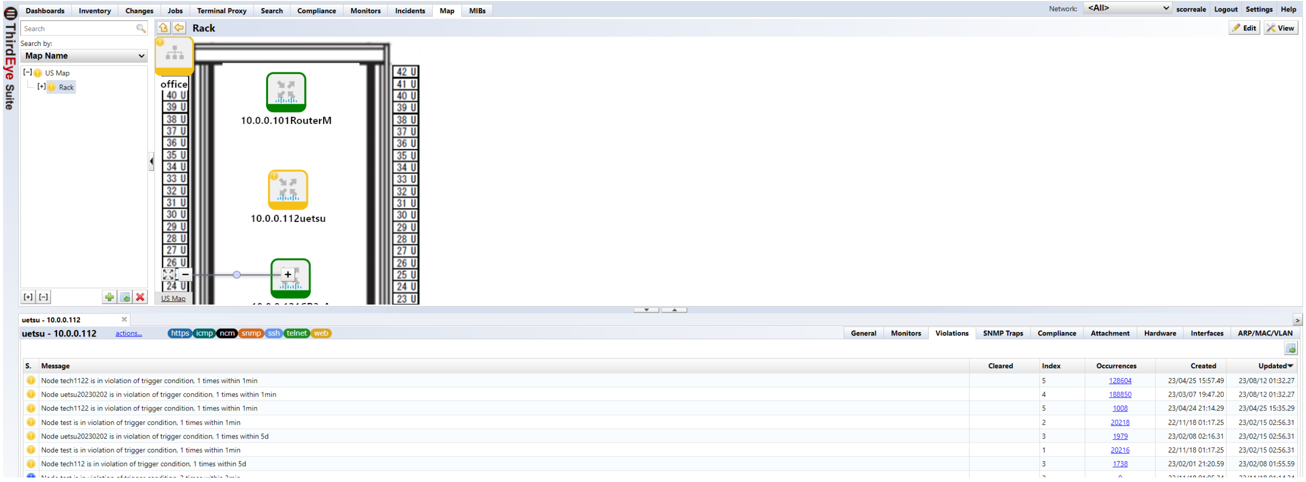


Doubleclick a Map Object to move to a lower level. You can also display the desired map by using the Map Tree.



12.12.1 Checking Issue Details

Once you have identified the location of the problem, doubleclick the failed device to display the device details in the [Editor] window for more details about the problem. On the [Editor] window > [Violations] screen, you can check the failures that have occurred in the device.



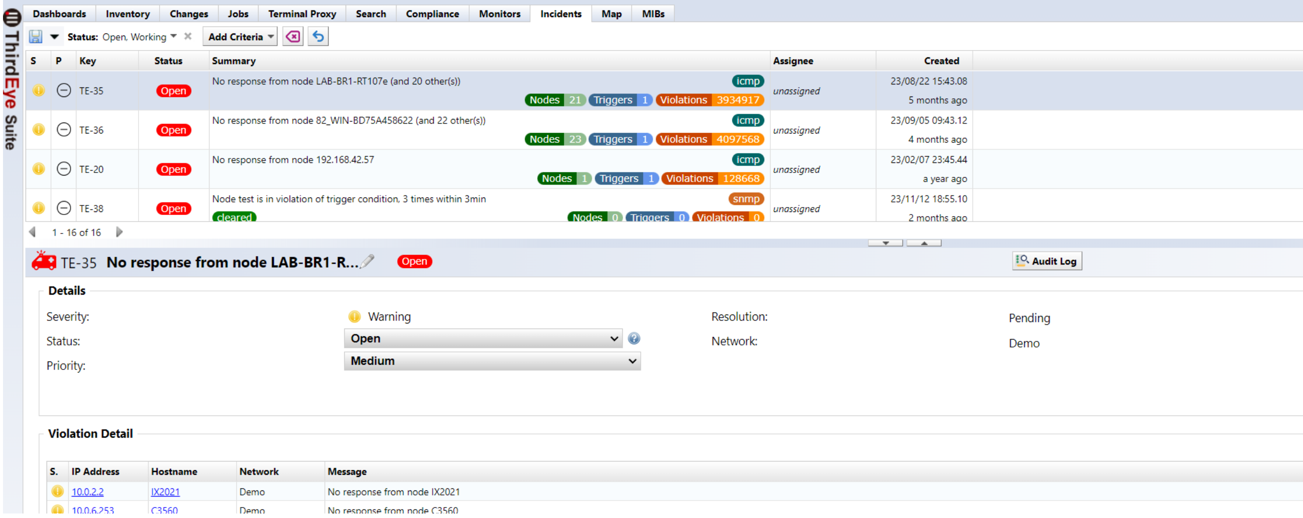
uetsu - 10.0.0.112

S.	Message	Cleared	Index	Occurrences	Created	Updated
●	Node tech1122 is in violation of trigger condition, 1 times within 1min		5	128604	23/04/25 15:57.49	23/08/12 01:32.27
●	Node uetsu20230202 is in violation of trigger condition, 1 times within 1min		4	188850	23/03/07 19:47.20	23/08/12 01:32.27
●	Node tech1122 is in violation of trigger condition, 1 times within 1min		5	1008	23/04/24 21:14.29	23/04/25 15:35.29
●	Node test is in violation of trigger condition, 1 times within 1min		2	20218	22/11/18 01:17.25	23/02/15 02:56.31
●	Node uetsu20230202 is in violation of trigger condition, 1 times within 5d		3	1979	23/02/08 02:16.31	23/02/15 02:56.31
●	Node test is in violation of trigger condition, 1 times within 1min		1	20216	22/11/18 01:17.25	23/02/15 02:56.31
●	Node tech112 is in violation of trigger condition, 1 times within 5d		3	1738	23/02/01 21:20.59	23/02/08 01:55.59

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 [Editor] at the bottom of the window.



Status: Open, Working

S	P	Key	Status	Summary	Assignee	Created
●	⊖	TE-35	Open	No response from node LAB-BR1-RT107e (and 20 other(s)) icmp Nodes 21 Triggers 1 Violations 3934917	unassigned	23/08/22 15:43.08 5 months ago
●	⊖	TE-36	Open	No response from node 82_WIN-BD75A458622 (and 22 other(s)) icmp Nodes 23 Triggers 1 Violations 4097568	unassigned	23/09/05 09:43.12 4 months ago
●	⊖	TE-20	Open	No response from node 192.168.42.57 icmp Nodes 1 Triggers 1 Violations 128668	unassigned	23/02/07 23:45.44 a year ago
●	⊖	TE-38	Open	Node test is in violation of trigger condition, 3 times within 3min snmp cleared Nodes 0 Triggers 0 Violations 0	unassigned	23/11/12 18:55.10 2 months ago

1 - 16 of 16

TE-35 No response from node LAB-BR1-R... Open

Details

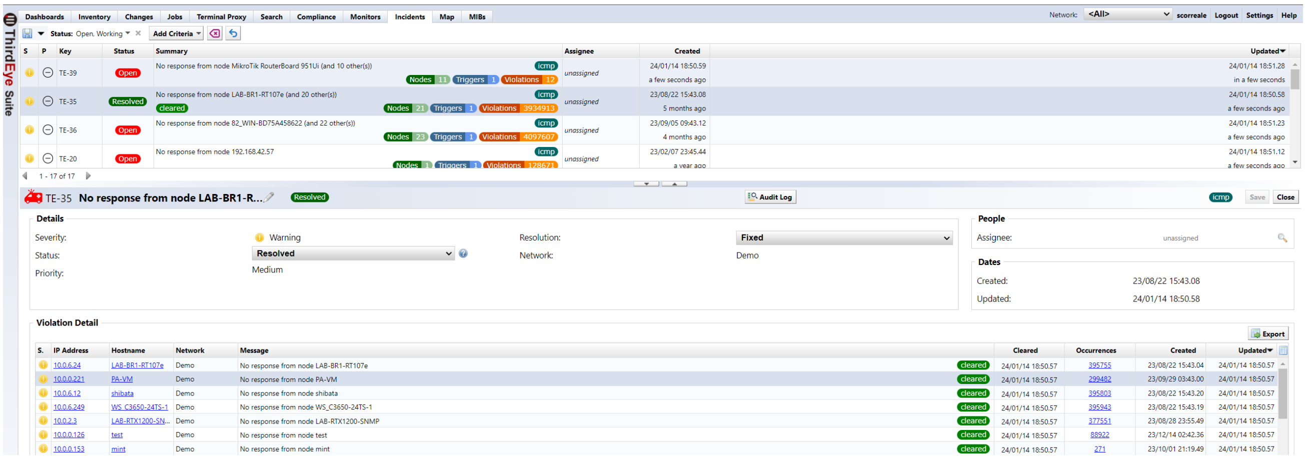
Severity:	● Warning	Resolution:	Pending
Status:	Open	Network:	Demo
Priority:	Medium		

Violation Detail

S.	IP Address	Hostname	Network	Message
●	10.0.2.2	IX2021	Demo	No response from node IX2021
●	10.0.6.253	C3560	Demo	No response from node C3560

12.12.2 Marking Incident as “Resolved”

Close the incident when the problem has been resolved. Select [Resolved] from the **Status** pull-down menu and click [Save].



Status: Open, Working

S	P	Key	Status	Summary	Assignee	Created	Updated
		TE-39	Open	No response from node MikroTik RouterBoard 951Ui (and 10 other(s)) icmp Nodes 11 Triggers 1 Violations 12	unassigned	24/01/14 18:50.59 a few seconds ago	24/01/14 18:51.28 in a few seconds
		TE-35	Resolved	No response from node LAB-BR1-RT107e (and 20 other(s)) icmp cleared Nodes 21 Triggers 1 Violations 3934913	unassigned	23/08/22 15:43.08 5 months ago	24/01/14 18:50.58 a few seconds ago
		TE-36	Open	No response from node 82_WIN-BD75A458622 (and 22 other(s)) icmp Nodes 23 Triggers 1 Violations 4097607	unassigned	23/09/05 09:43.12 4 months ago	24/01/14 18:51.23 a few seconds ago
		TE-20	Open	No response from node 192.168.42.57 icmp Nodes 1 Triggers 1 Violations 128671	unassigned	23/02/07 23:45.44 a year ago	24/01/14 18:51.12 a few seconds ago

1 - 17 of 17

TE-35 No response from node LAB-BR1-R... Resolved

Details

Severity: Warning

Status: Resolved

Priority: Medium

Resolution: Fixed

Network: Demo

People

Assignee: unassigned

Dates

Created: 23/08/22 15:43.08

Updated: 24/01/14 18:50.58

Violation Detail

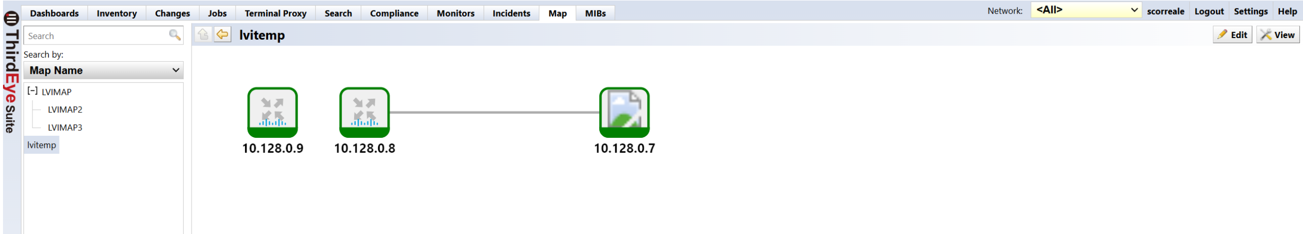
S.	IP Address	Hostname	Network	Message		Cleared	Occurrences	Created	Updated
	10.0.6.24	LAB-BR1-RT107e	Demo	No response from node LAB-BR1-RT107e	cleared	24/01/14 18:50.57	395755	23/08/22 15:43.04	24/01/14 18:50.57
	10.0.0.221	PA-VM	Demo	No response from node PA-VM	cleared	24/01/14 18:50.57	299482	23/09/29 03:43.00	24/01/14 18:50.57
	10.0.6.12	shibata	Demo	No response from node shibata	cleared	24/01/14 18:50.57	395803	23/08/22 15:43.20	24/01/14 18:50.57
	10.0.6.249	WS_C3650-24TS-1	Demo	No response from node WS_C3650-24TS-1	cleared	24/01/14 18:50.57	395943	23/08/22 15:43.19	24/01/14 18:50.57
	10.0.2.3	LAB-RTX1200-SN...	Demo	No response from node LAB-RTX1200-SNMP	cleared	24/01/14 18:50.57	377551	23/08/28 23:55.49	24/01/14 18:50.57
	10.0.0.126	test	Demo	No response from node test	cleared	24/01/14 18:50.57	88922	23/12/14 02:42.36	24/01/14 18:50.57
	10.0.0.153	mint	Demo	No response from node mint	cleared	24/01/14 18:50.57	271	23/10/01 21:19.49	24/01/14 18:50.57

The status display will change to “Resolved” and the closing process will be completed.

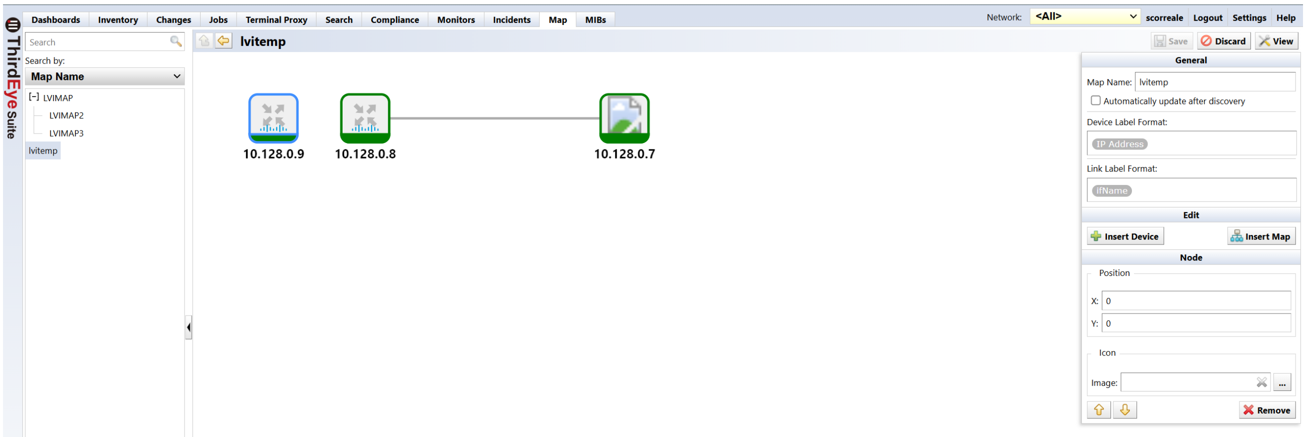
Click [Close] to close the [Incident Details] screen.

12.13 Remove Device

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].



Map Name: lvitemp

□ Automatically update after discovery

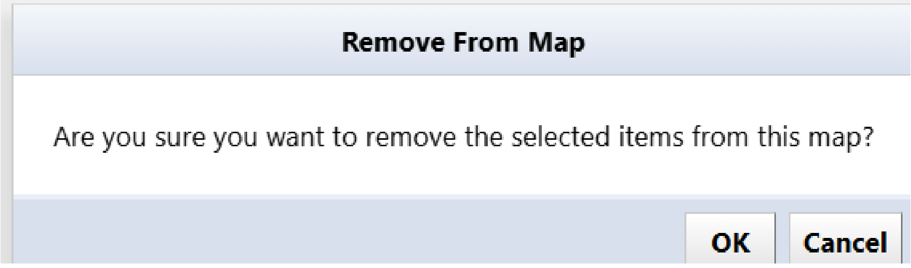
Device Label Format: IP Address

Link Label Format: ifName

X: 0

Y: 0

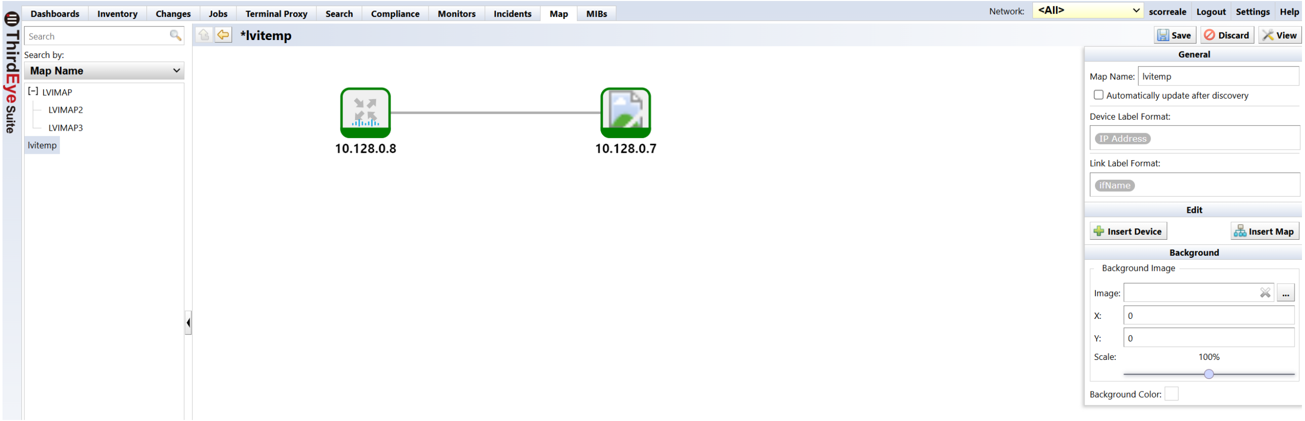
A confirmation message will be displayed. Click [OK].



Remove From Map

Are you sure you want to remove the selected items from this map?

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



Map Name: lvitemp

□ Automatically update after discovery

Device Label Format: IP Address

Link Label Format: ifName

Image:

X: 0

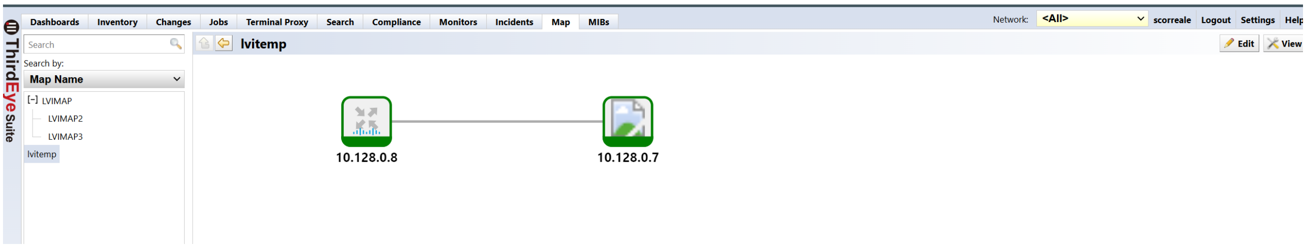
Y: 0

Scale: 100%

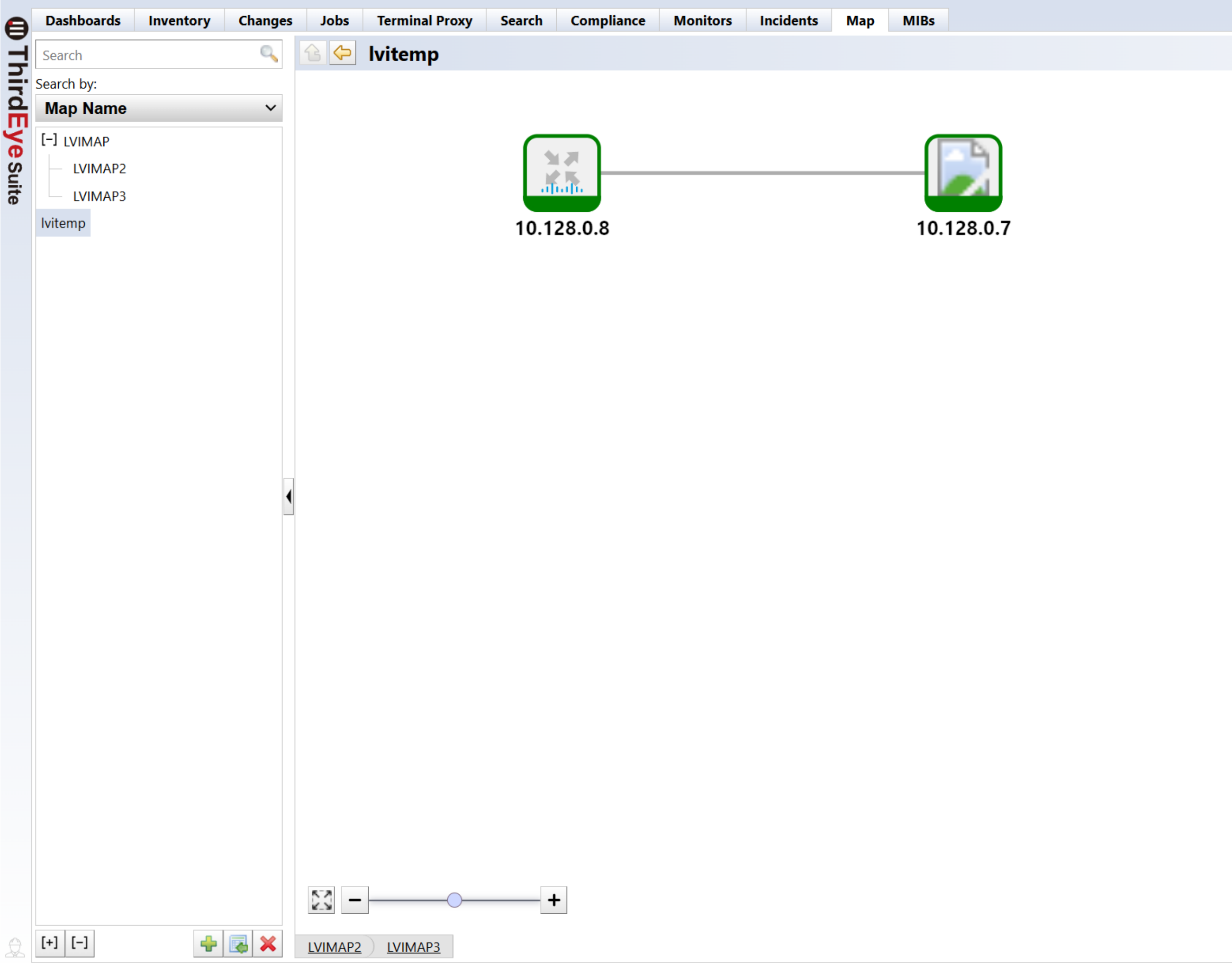
Background Color:

12.14 Delete Map

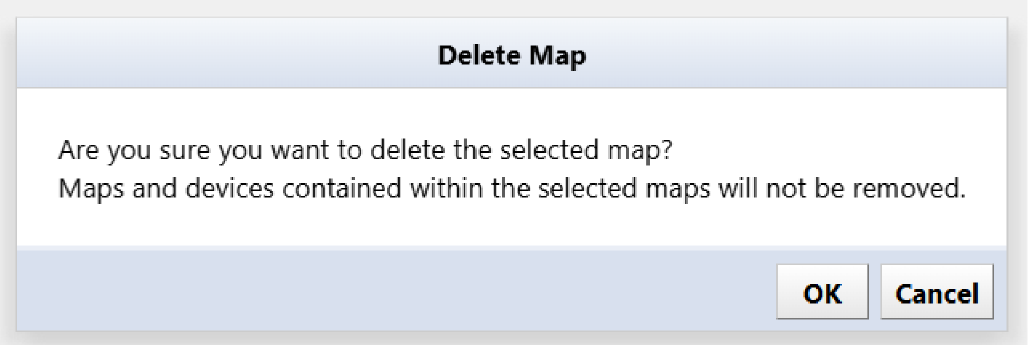
1. Select the map you want to delete from the Map Tree.



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



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



Delete Map

Are you sure you want to delete the selected map?
Maps and devices contained within the selected maps will not be removed.

SECTION 13

CREDENTIALS

Credentials are logins and other security information of your devices. ThirdEye uses this information to perform tasks on your behalf.

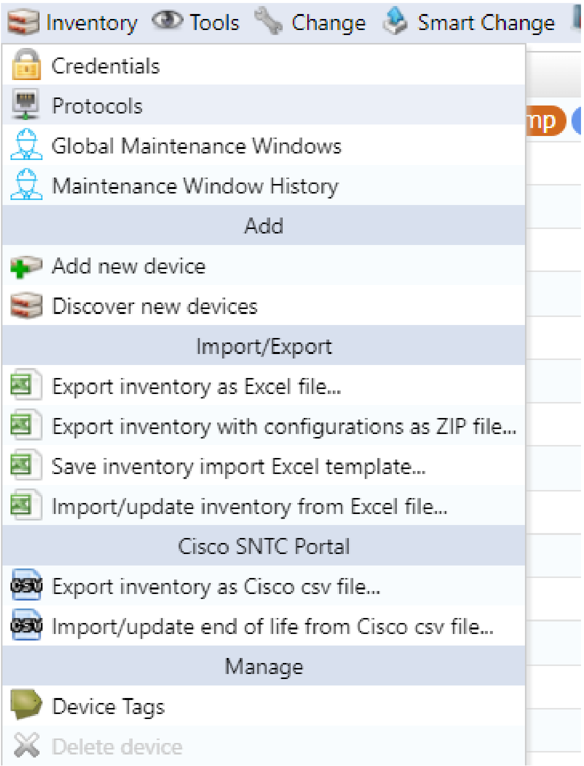
There are three ways to set credentials: **“dynamic”**, **“static”** and **“cloud”**.

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.
cloud	Set credentials for Cloud Accounts. Use this when the devices are managed by a Cloud Provider.

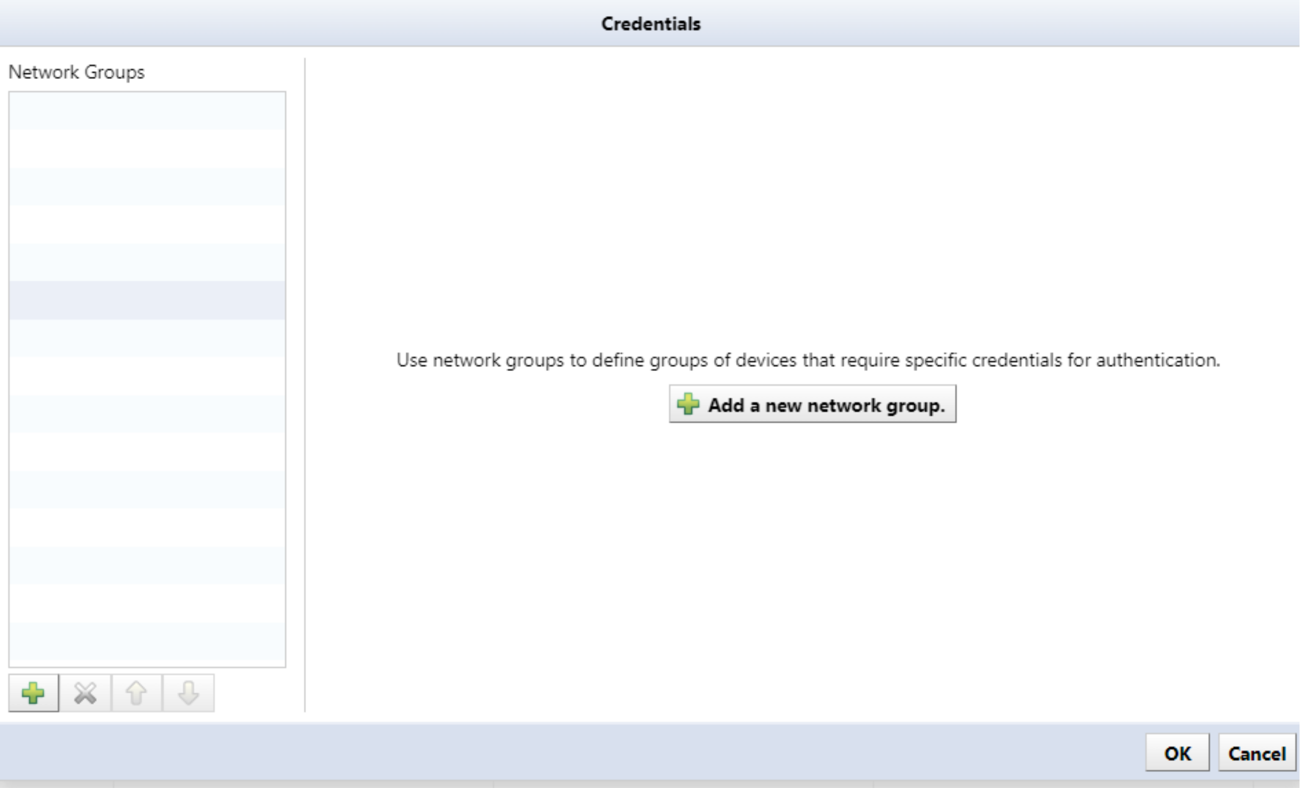
13.1 Set Common Credentials

If you have a set of common credentials for devices, use **“Dynamic”** to set them:

1. Click the [Inventory] main tab.
2. Click the [Inventory] menu.
3. Click [Credentials] in the dropdown menu.

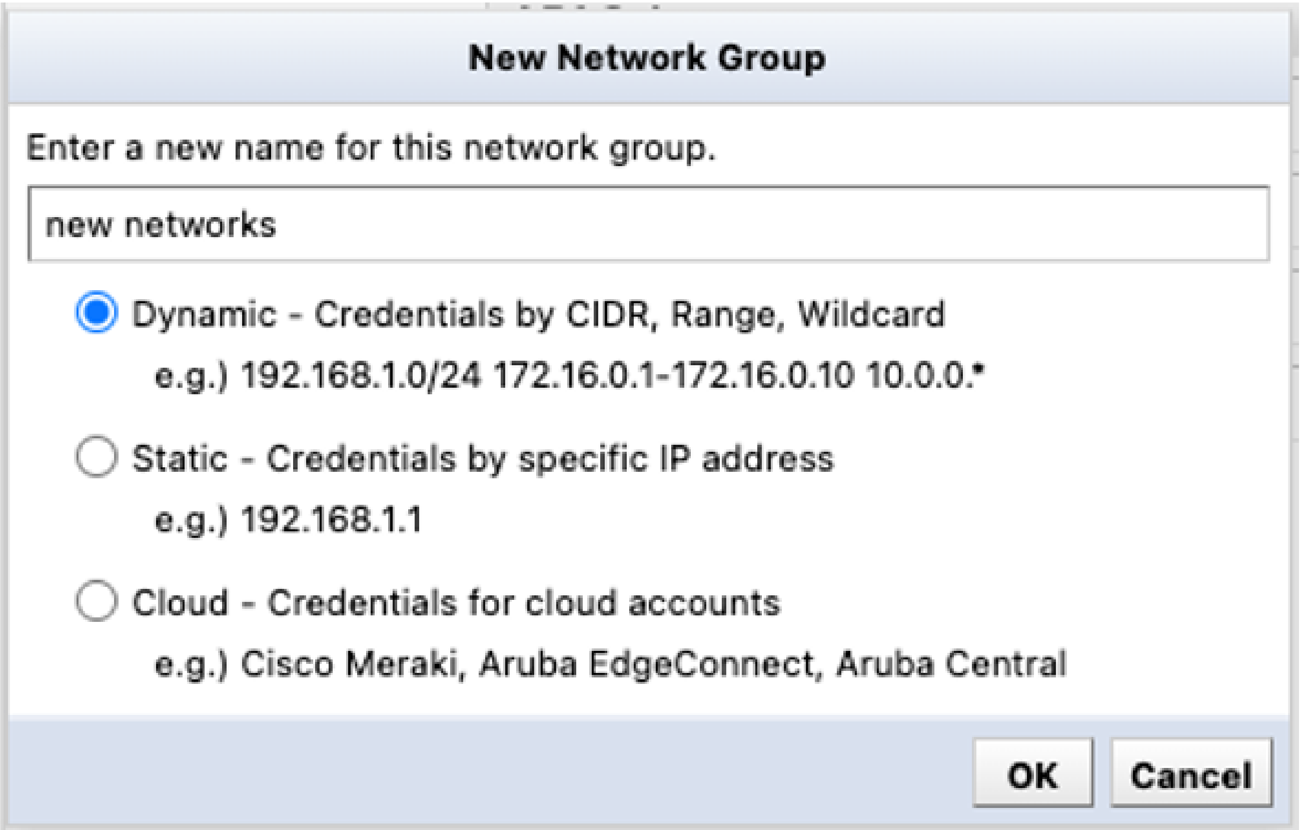

Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device
mp

4. Select a network, and click [OK].
5. Click the ✚ button under the “Network Groups” left sidepanel, or click the [Add new network group] button.



Credentials
Network Groups
Use network groups to define groups of devices that require specific credentials for authentication.
Add a new network group.
OK
Cancel

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



New Network Group

Enter a new name for this network group.

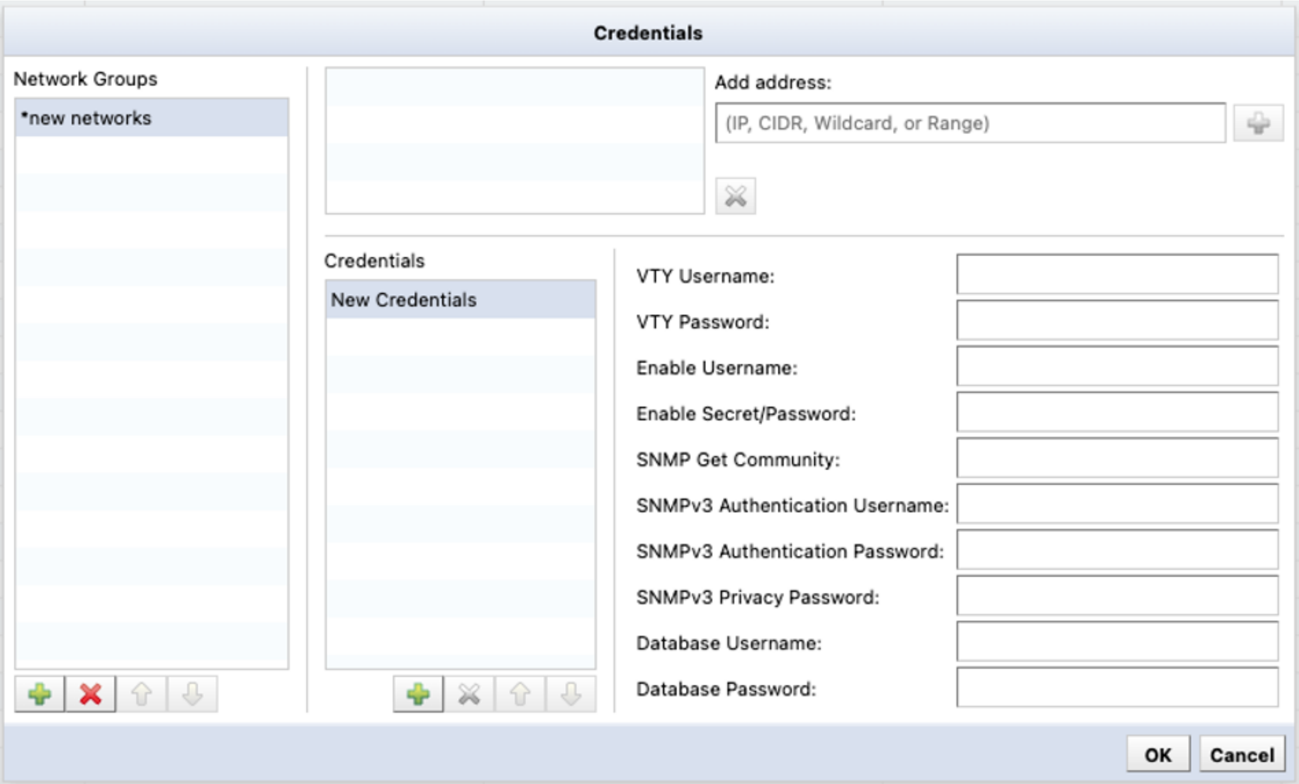
new networks

● Dynamic - Credentials by CIDR, Range, Wildcard
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*

○ Static - Credentials by specific IP address
e.g.) 192.168.1.1

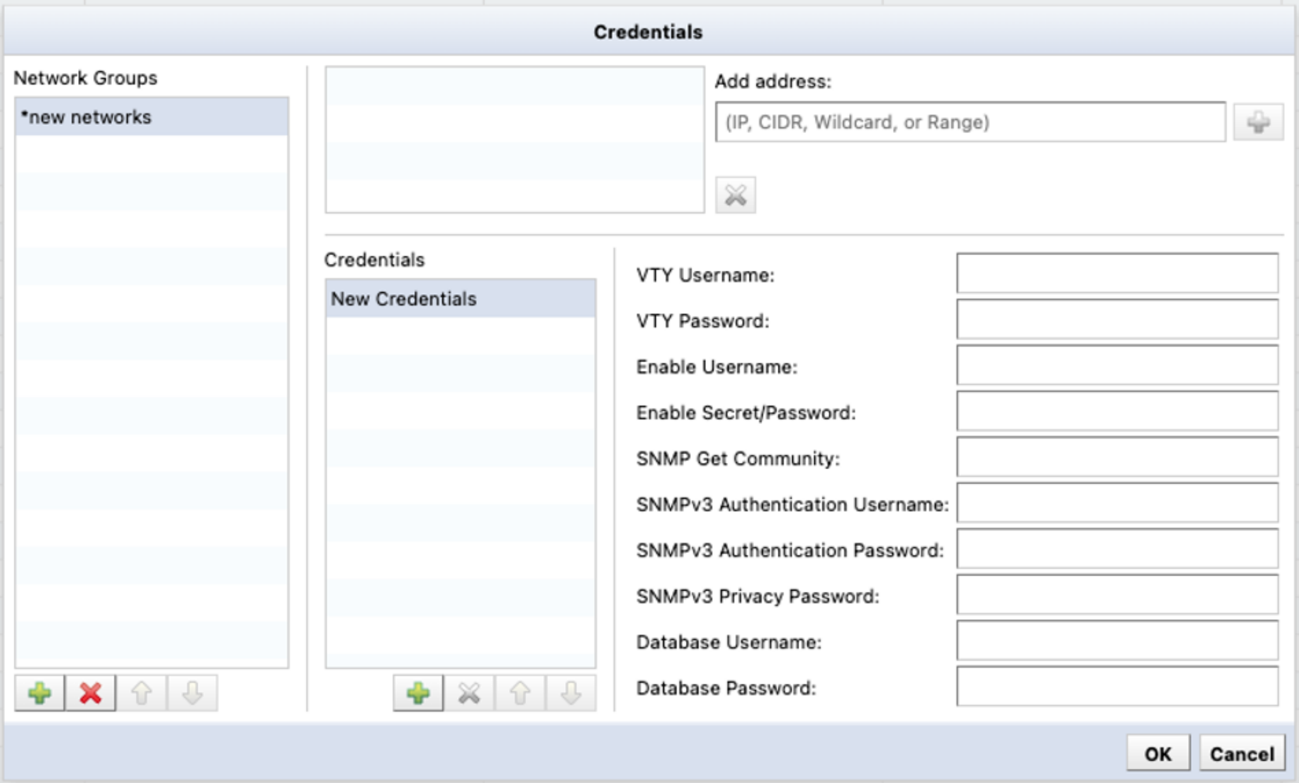
○ Cloud - Credentials for cloud accounts
e.g.) Cisco Meraki, Aruba EdgeConnect, Aruba Central

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



8. Fill in login information near the bottom right of the right panel.

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



Credentials

Network Groups

*new networks

Add address:

(IP, CIDR, Wildcard, or Range)

Credentials

New Credentials

VTY Username:

VTY Password:

Enable Username:

Enable Secret/Password:

SNMP Get Community:

SNMPv3 Authentication Username:

SNMPv3 Authentication Password:

SNMPv3 Privacy Password:

Database Username:

Database Password:

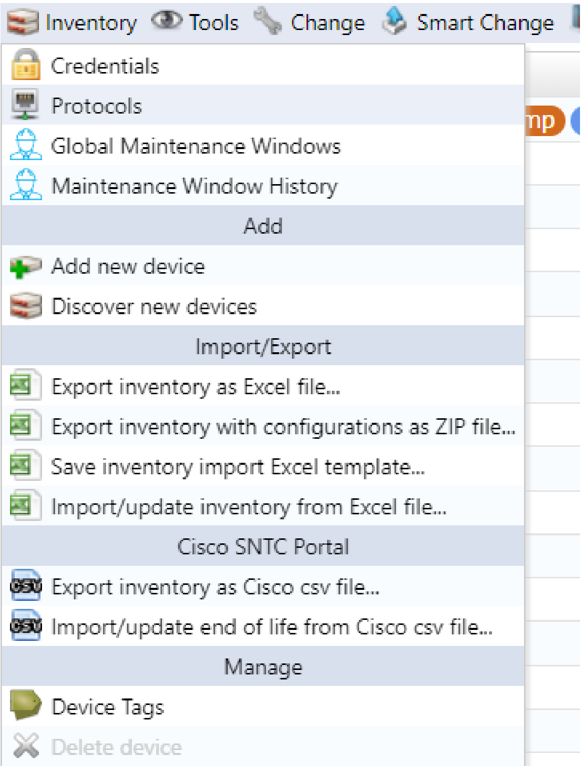
Item	Explanation
VTY Username /VTY Password	Enter the username/password required to log in to the network device.
Enable Username /Enable Secret/Password	Enter the username/password to enter enable mode.
SNMP Get Community	Enter the SNMP community to use when making an SNMP Get request.
SNMPv3 Authentication 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.
Database Username	Enter the database username.
Database Password	Enter the database password.

9. Click [OK] to save your settings.

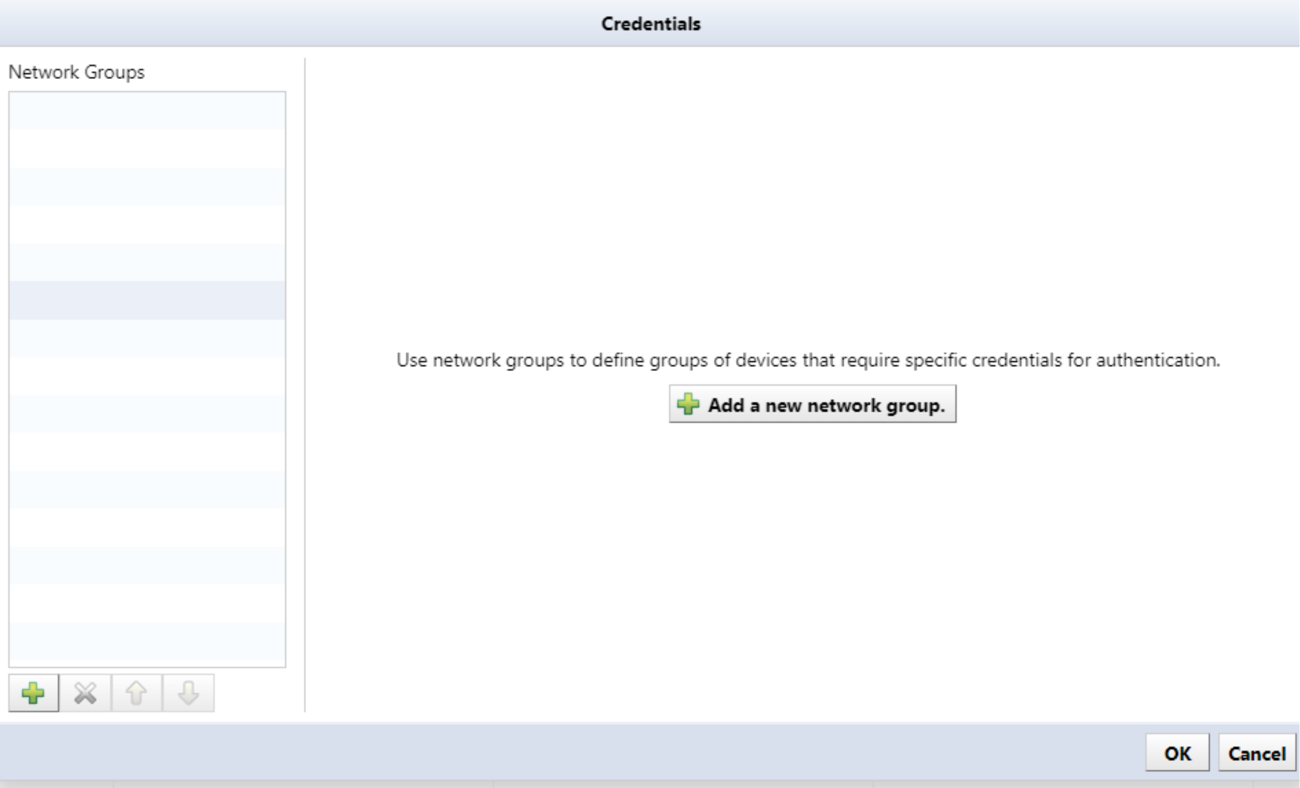
13.2 Set Credentials for Each Device

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

1. Click the [Inventory] main tab
2. Click the [Inventory] menu.
3. Click [Credentials].

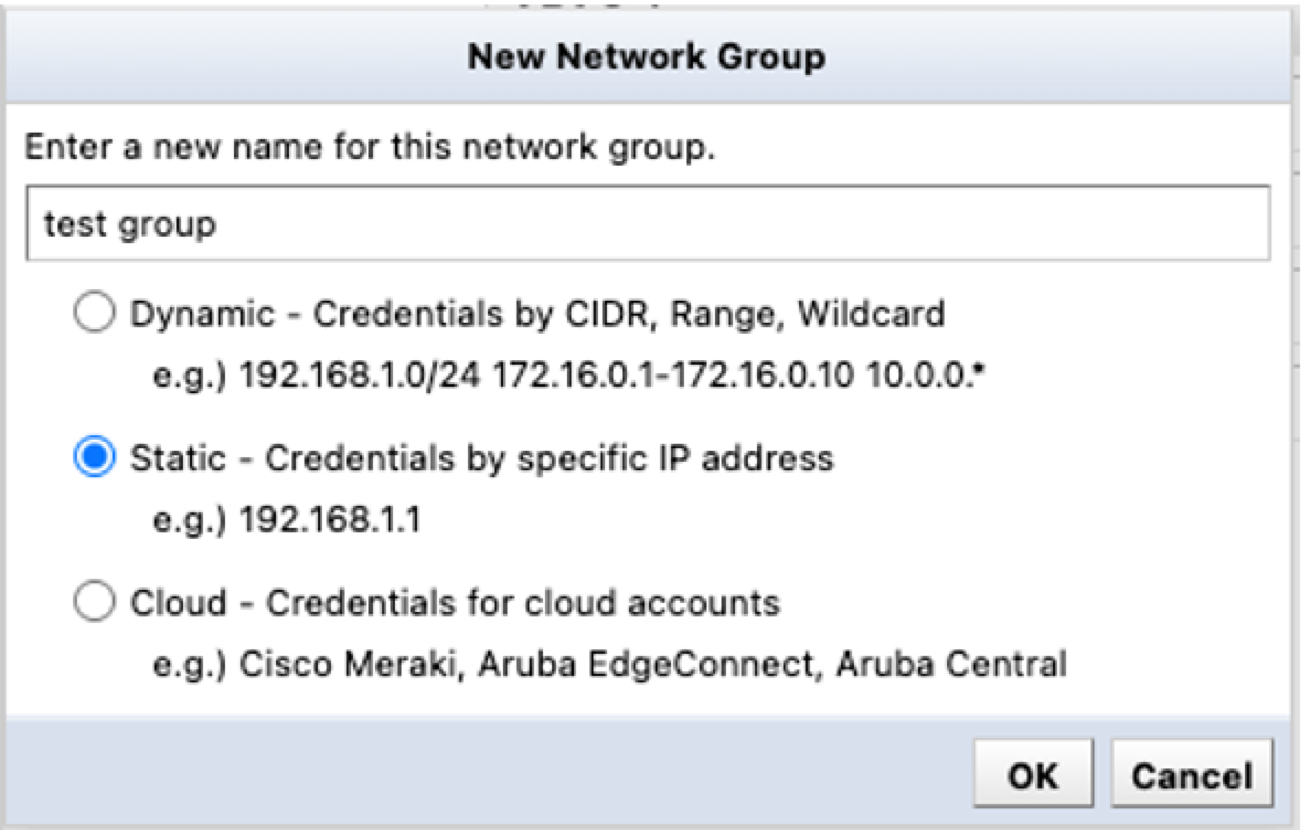

Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device
mp

4. Select a network, and click [OK].
5. Click the ✚ button under the “Network Groups” left sidepanel, or click the [Add new network group] button.



Use network groups to define groups of devices that require specific credentials for authentication.

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



New Network Group

Enter a new name for this network group.

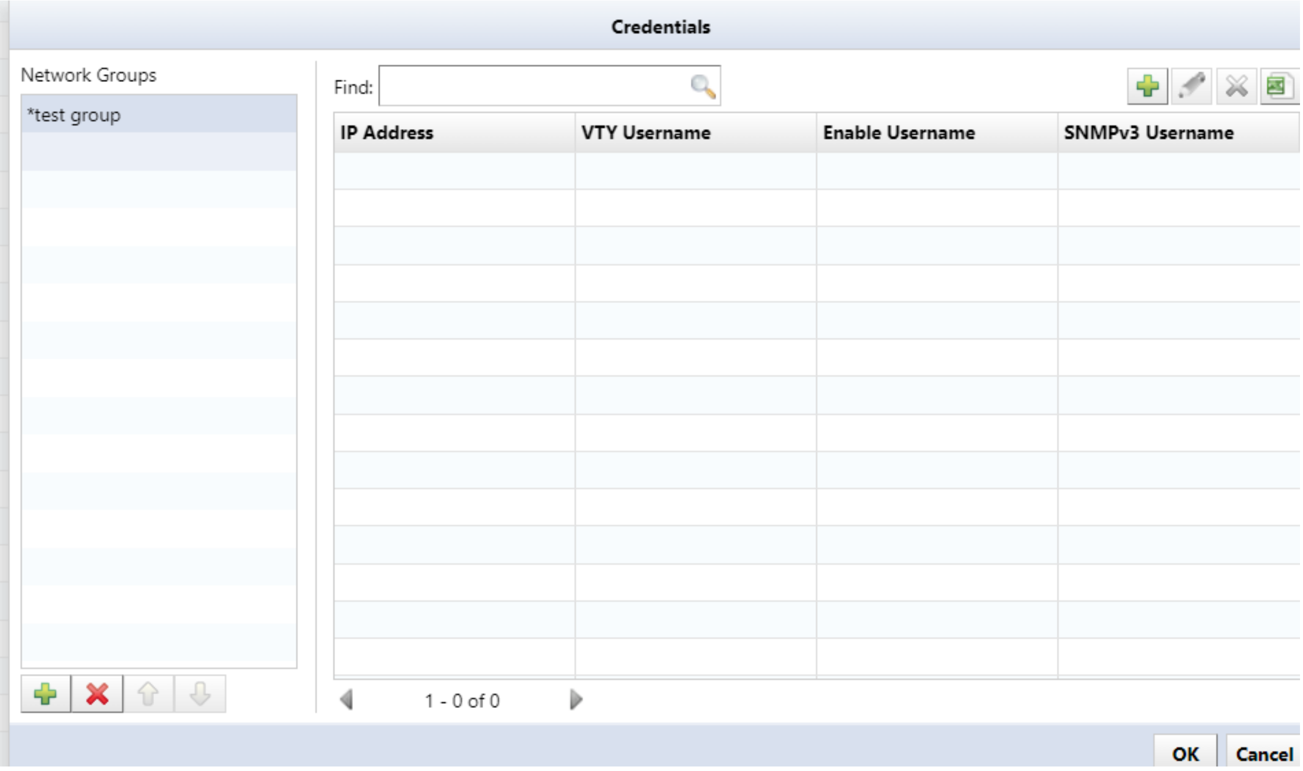
test group

○ Dynamic - Credentials by CIDR, Range, Wildcard
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*

● Static - Credentials by specific IP address
e.g.) 192.168.1.1

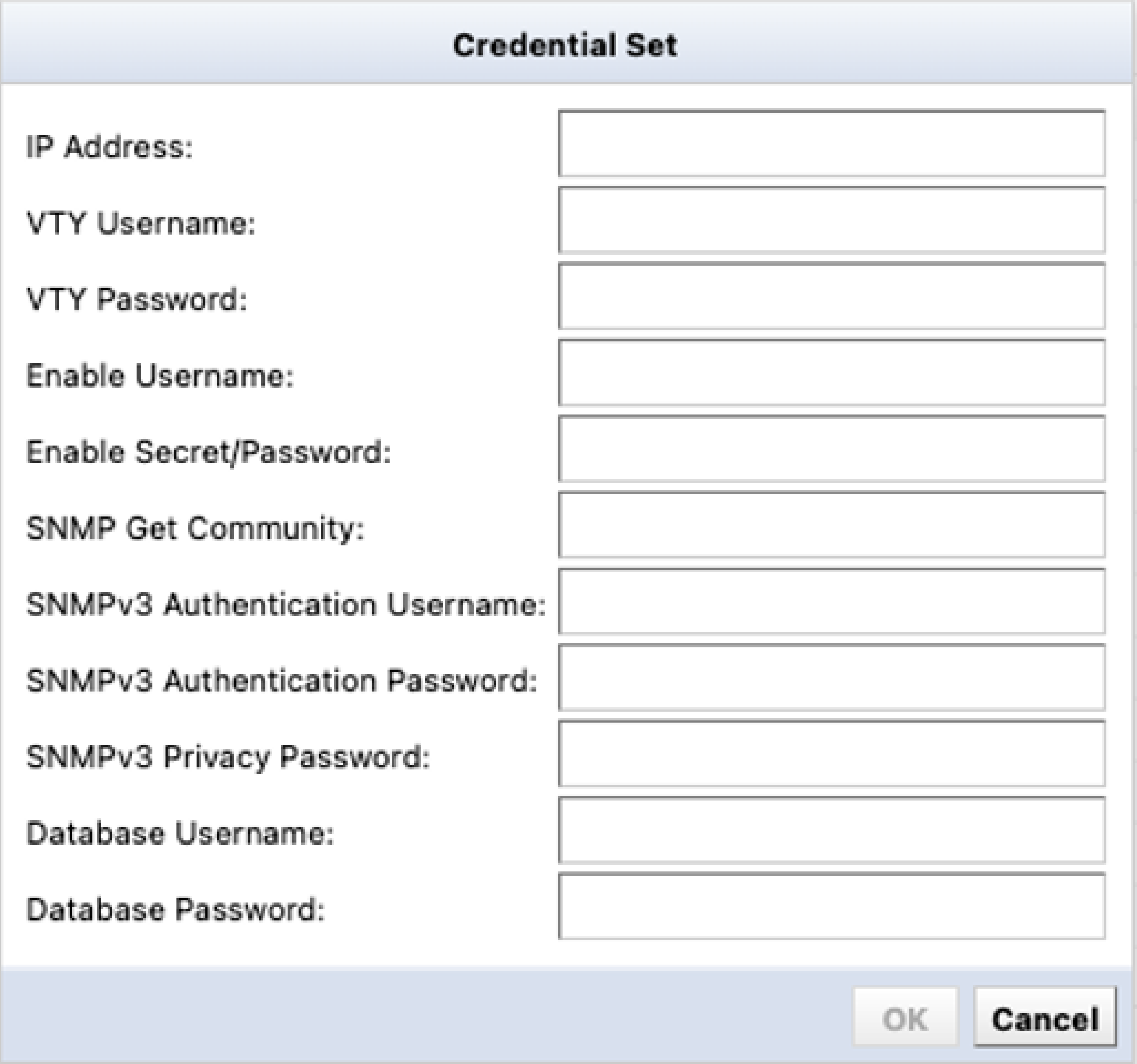
○ Cloud - Credentials for cloud accounts
e.g.) Cisco Meraki, Aruba EdgeConnect, Aruba Central

7. Click the ✚ button.



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

It is possible to omit items that are not required.



Credential Set

IP Address:

VTY Username:

VTY Password:

Enable Username:

Enable Secret/Password:

SNMP Get Community:

SNMPv3 Authentication Username:

SNMPv3 Authentication Password:

SNMPv3 Privacy Password:

Database Username:

Database Password:

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.

Item	Explanation
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.
Database Username	Enter the database username.
Database Password	Enter the database password.

9. Click [OK] to save your settings.

From revision 20240131.0729, database monitoring for Postgres/MySQL/MariaDB is supported.

SECTION 14

SYSLOGS

Syslogs are standardized event logging messages used across network devices and systems to record operational data.

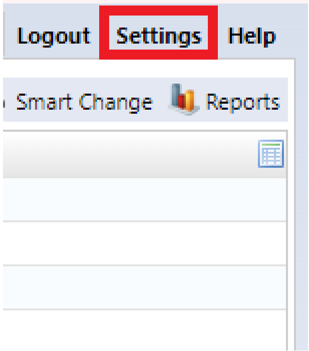
With syslogs you can:

- **Monitoring Devices**: Network equipment (routers, switches, etc.) automatically generates syslog messages for status changes, errors, and security events
- **Centralize Collection**: Aggregate logs from multiple devices into a unified repository
- **Monitor Integration**: You can trigger alerts based on log patterns (failed logins, interface errors), enable automated responses through Playbooks, and provide audit trails for compliance reporting

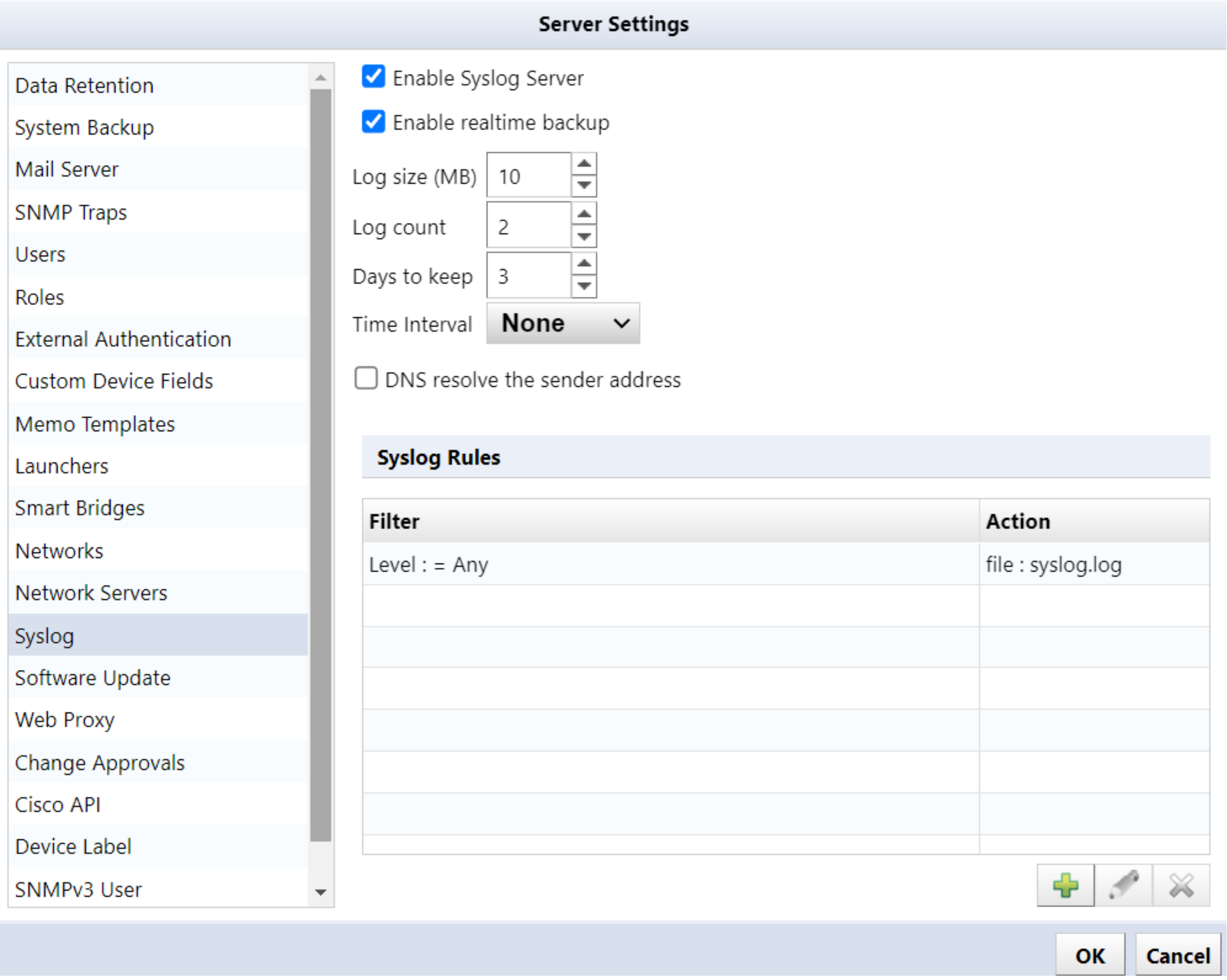
14.1 Syslog File Retention Period/Size

Set the retention period for Syslog files.

1. Click [Settings] on the Global Menu.



2. In the “Server Settings” window, click [Syslog] in the left sidepanel, and set each item.



Server Settings

☑ Enable Syslog Server

☑ Enable realtime backup

Log size (MB) 10

Log count 2

Days to keep 3

Time Interval None

□ DNS resolve the sender address

Syslog Rules

Filter	Action
Level : = Any	file : syslog.log

Item	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.

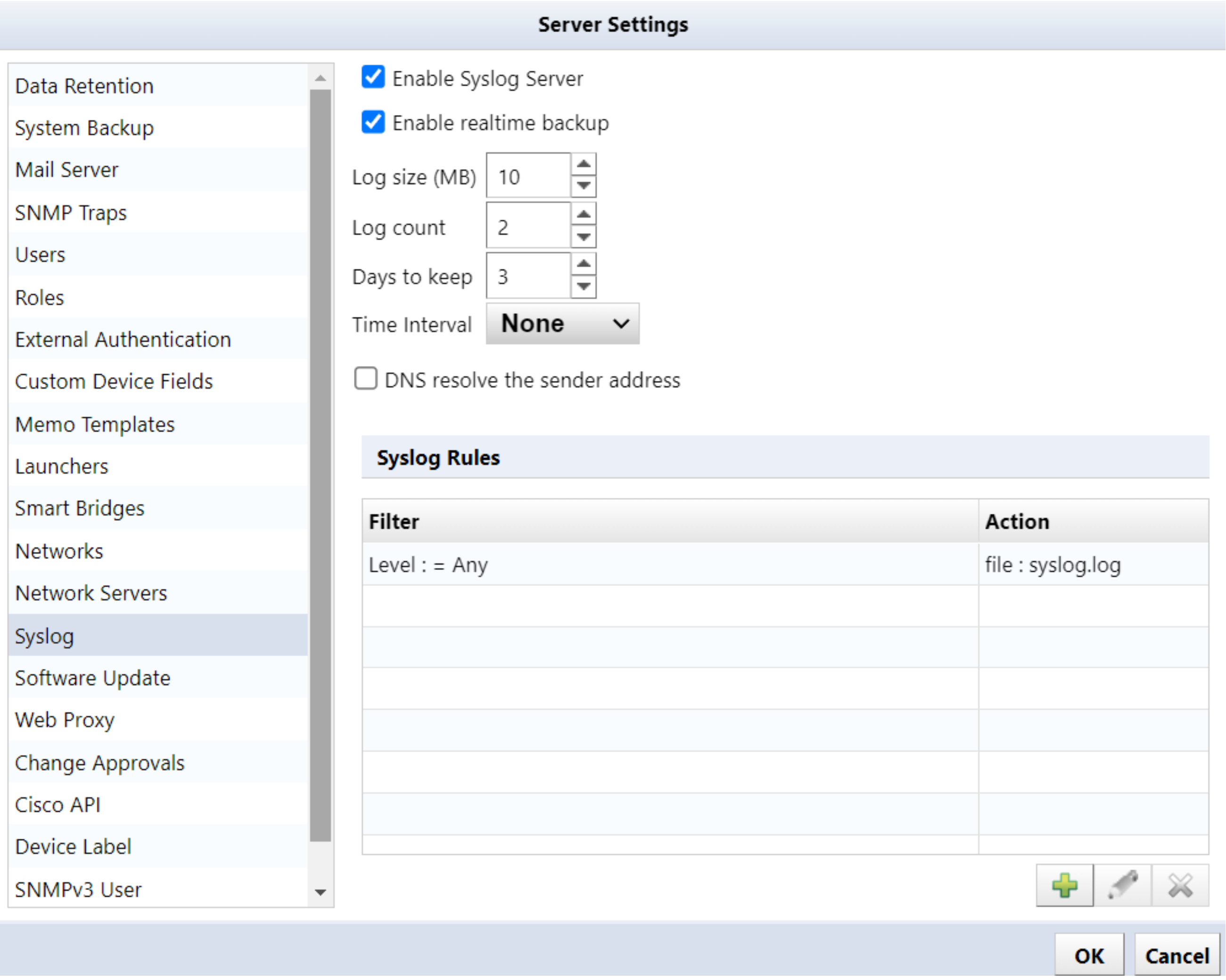
3. Click [OK].

14.2 Add Syslog Rule

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 click the ✚ button under “Syslog rules”.



Server Settings

☑ Enable Syslog Server

☑ Enable realtime backup

Log size (MB) 10

Log count 2

Days to keep 3

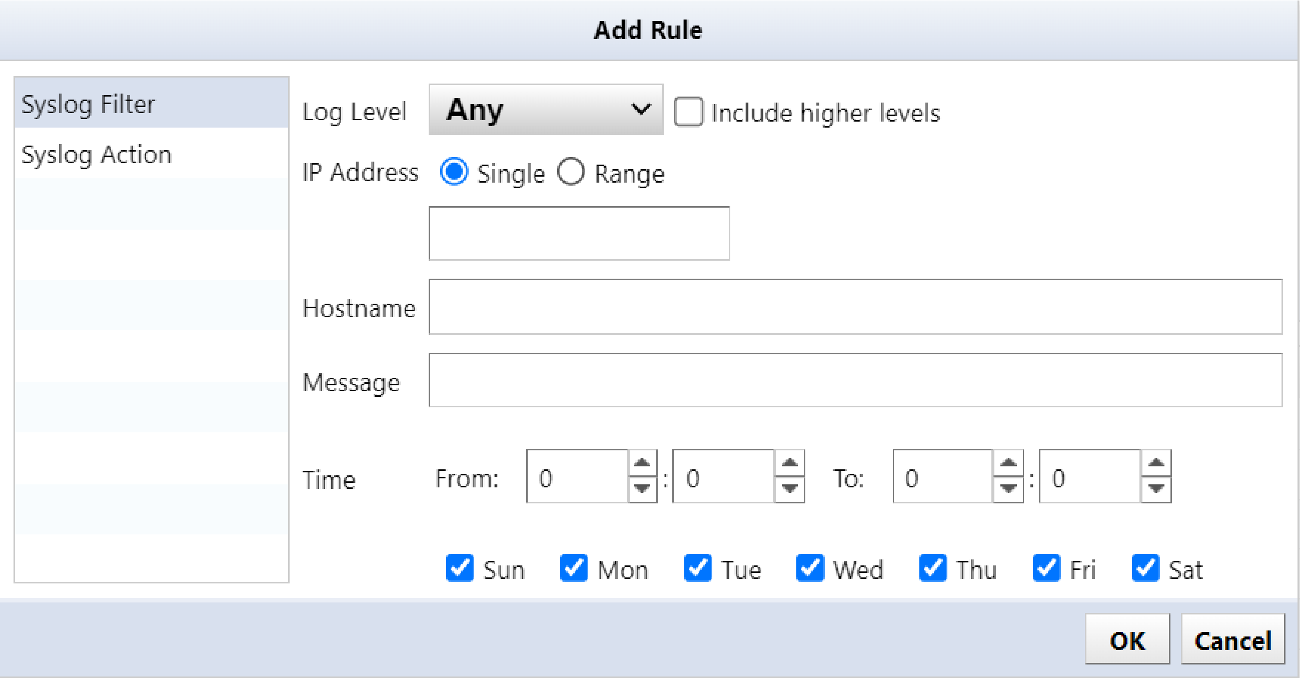
Time Interval None

☐ DNS resolve the sender address

Syslog Rules

Filter	Action
Level : = Any	file : syslog.log

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



Log Level: Any ▾ □ Include higher levels

IP Address: ● Single ○ Range

Hostname:

Message:

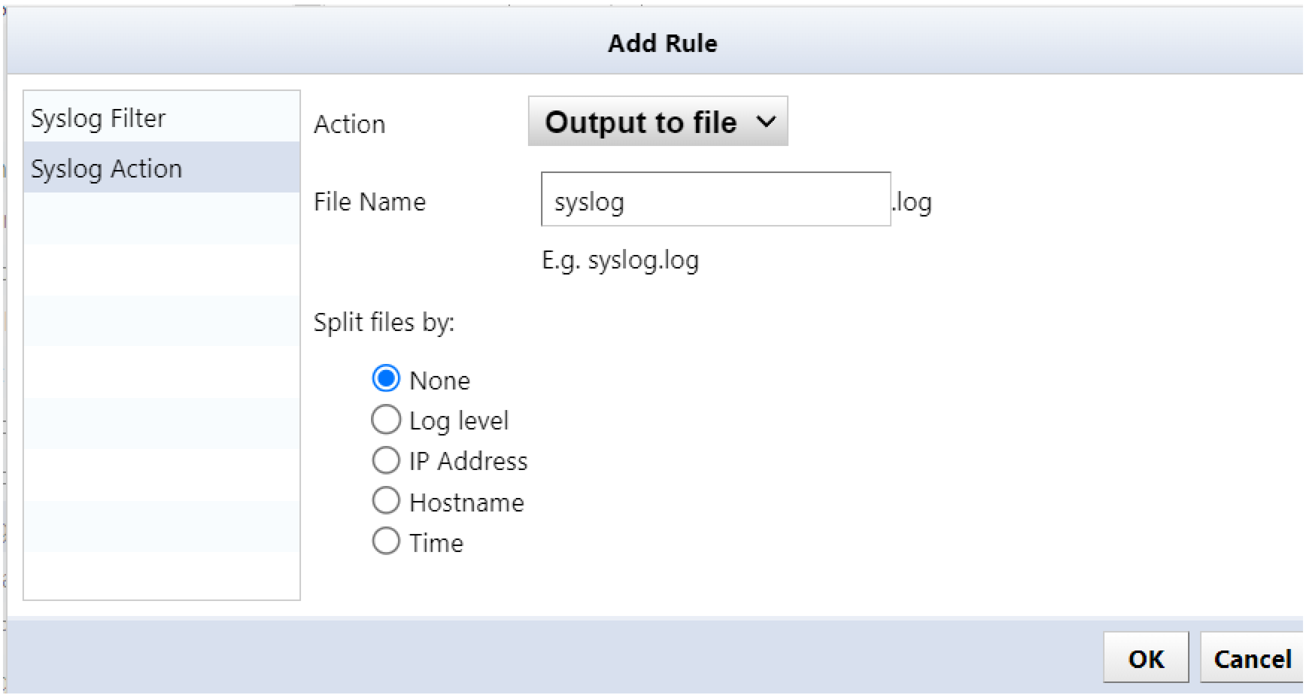
Time From: 0 : 0 To: 0 : 0

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

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.

Filter	Explanation
	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.



Action: Output to file

File Name: syslog .log

E.g. syslog.log

Split files by:

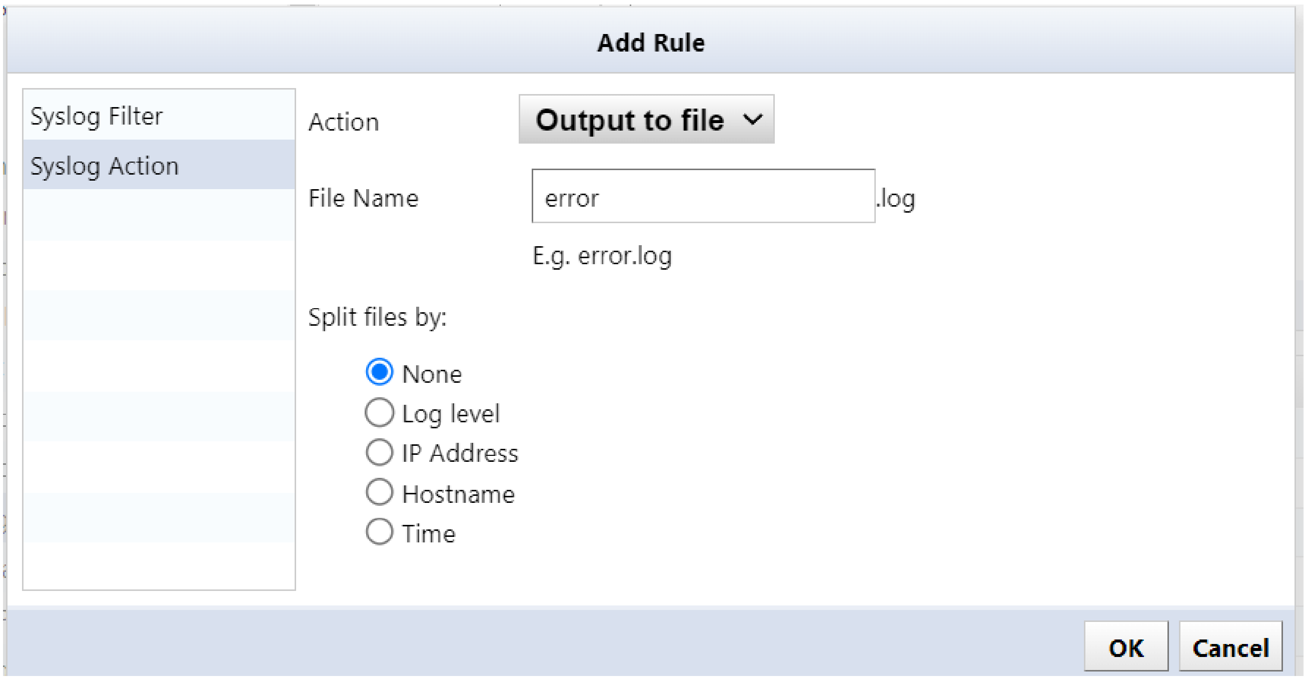
- ● None
- ○ Log level
- ○ IP Address
- ○ Hostname
- ○ Time

Syslog action items

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.
	Protocol	Select the transfer protocol from UDP or TCP.

Action	Item	Explanation
		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 configuration, click [OK].



Add Rule

Action: Output to file

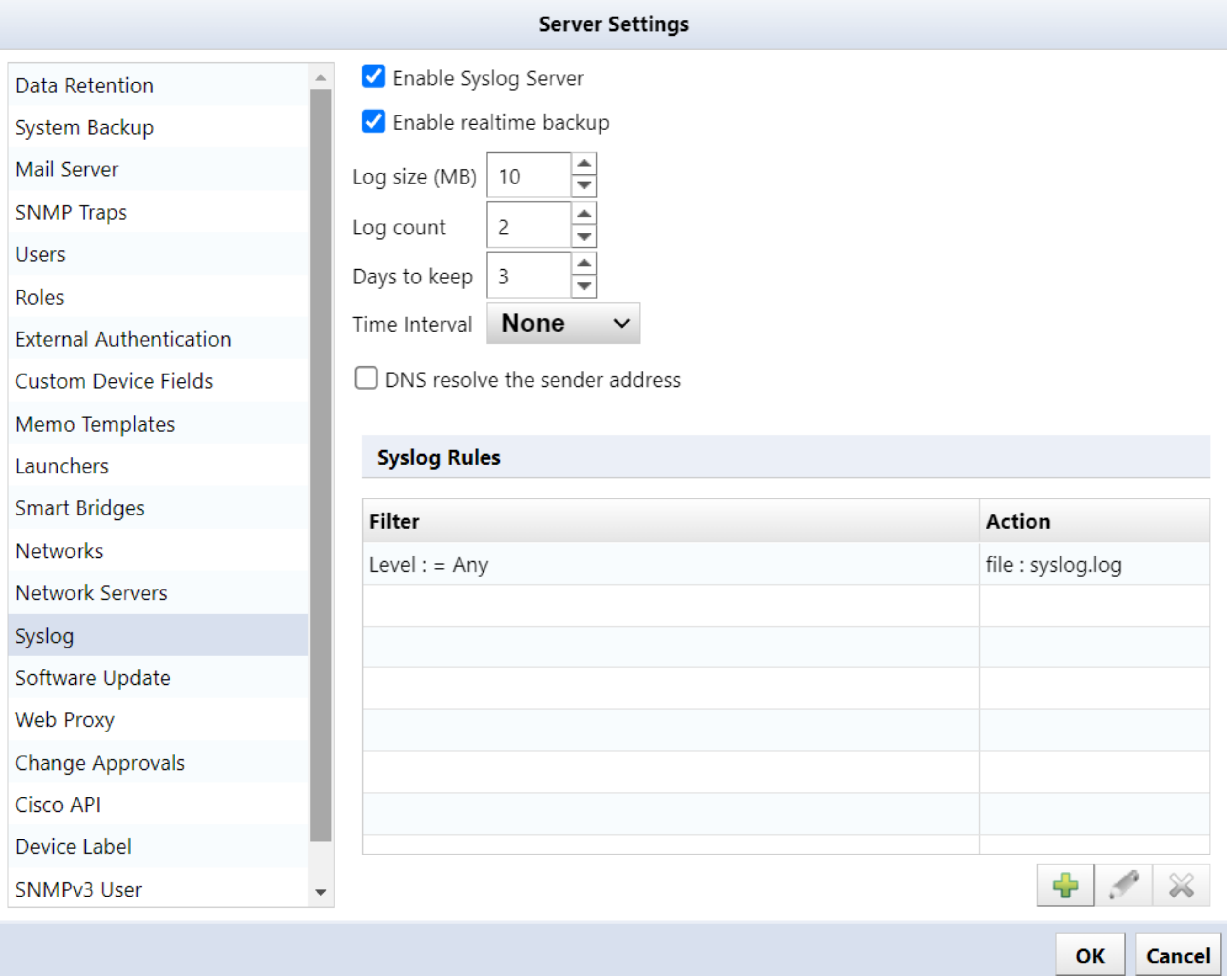
File Name: error .log

E.g. error.log

Split files by:

● None
○ Log level
○ IP Address
○ Hostname
○ Time

5. Click [OK] on the server settings screen.



Server Settings

☑ Enable Syslog Server

☑ Enable realtime backup

Log size (MB) 10

Log count 2

Days to keep 3

Time Interval None

□ DNS resolve the sender address

Syslog Rules

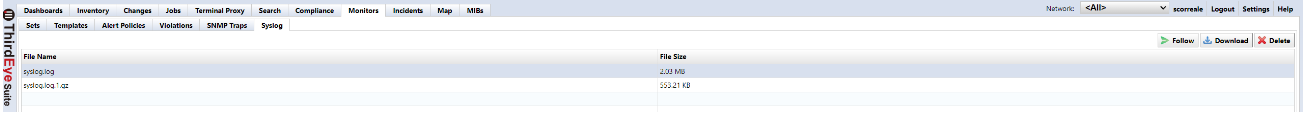
Filter	Action
Level : = Any	file : syslog.log

14.3 Check Received Syslog

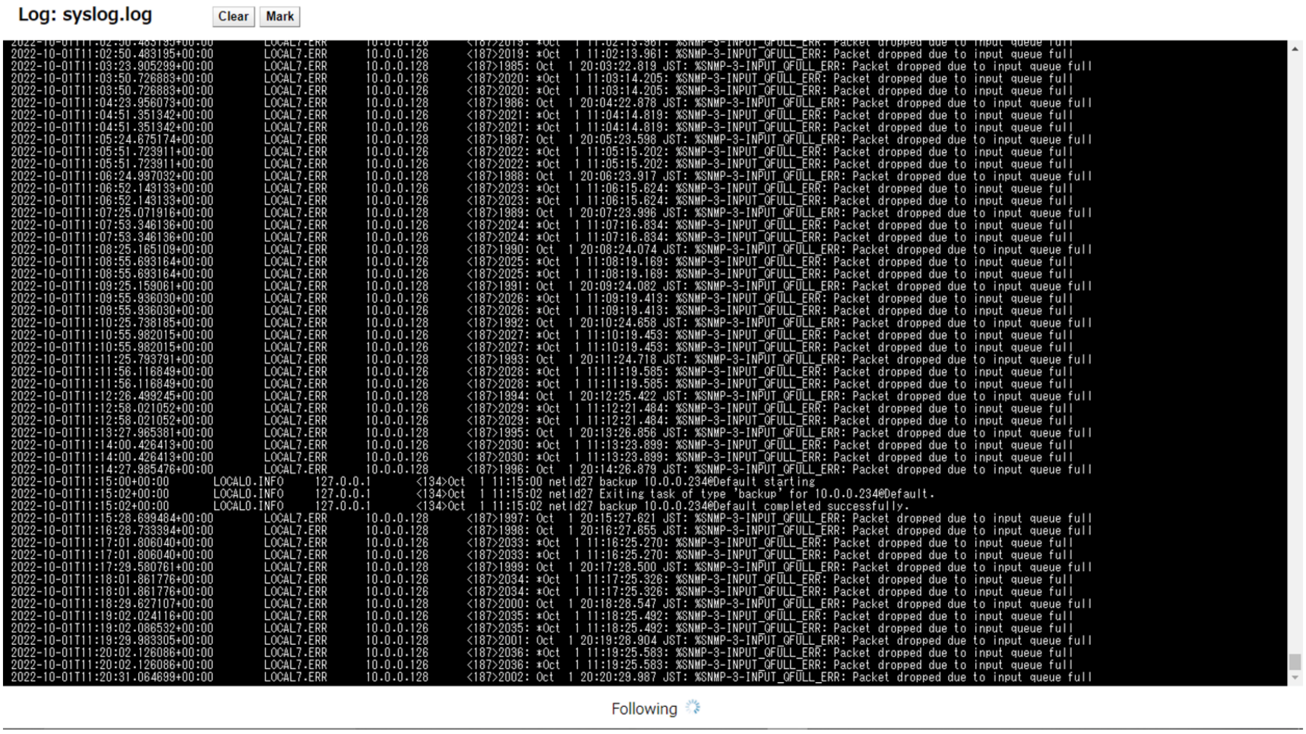
From Rev. 20221026.0600, you can check syslog on {{product_names}}'s [Syslog] tab.

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

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



File Name	File Size
syslog.log	2.03 MB
syslog.log.1.gz	553.21 KB



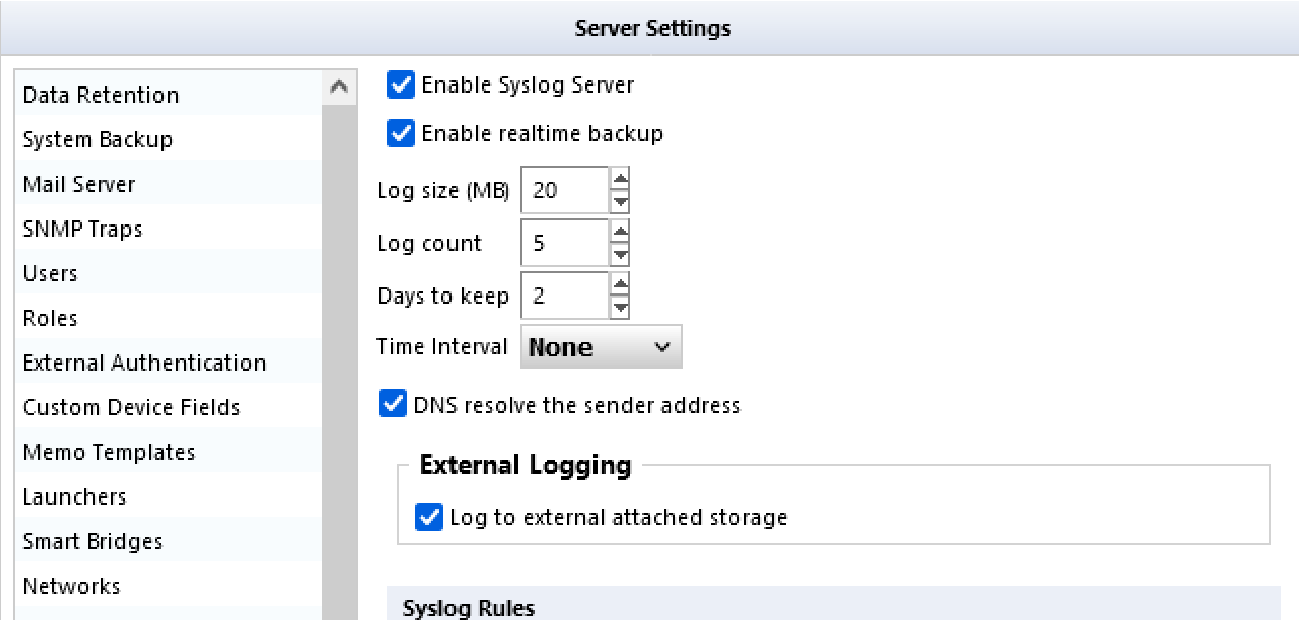
```
2022-10-01T11:02:50.483195+00:00        LOCAL7.ERR      10.0.0.126      <187>2019: *Oct  1 11:02:13.961: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:02:50.483195+00:00        LOCAL7.ERR      10.0.0.126      <187>2019: *Oct  1 11:02:13.961: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:03:23.905299+00:00        LOCAL7.ERR      10.0.0.128      <187>1985: Oct  1 20:03:22.819 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:03:50.726883+00:00        LOCAL7.ERR      10.0.0.126      <187>2020: *Oct  1 11:03:14.205: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:03:50.726883+00:00        LOCAL7.ERR      10.0.0.126      <187>2020: *Oct  1 11:03:14.205: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:04:23.956073+00:00        LOCAL7.ERR      10.0.0.128      <187>1986: Oct  1 20:04:22.878 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:04:51.351342+00:00        LOCAL7.ERR      10.0.0.126      <187>2021: *Oct  1 11:04:14.819: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:04:51.351342+00:00        LOCAL7.ERR      10.0.0.126      <187>2021: *Oct  1 11:04:14.819: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:05:24.675174+00:00        LOCAL7.ERR      10.0.0.128      <187>1987: Oct  1 20:05:23.598 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:05:51.723911+00:00        LOCAL7.ERR      10.0.0.126      <187>2022: *Oct  1 11:05:15.202: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:05:51.723911+00:00        LOCAL7.ERR      10.0.0.126      <187>2022: *Oct  1 11:05:15.202: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:06:24.997032+00:00        LOCAL7.ERR      10.0.0.128      <187>1988: Oct  1 20:06:23.917 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:06:52.143133+00:00        LOCAL7.ERR      10.0.0.126      <187>2023: *Oct  1 11:06:15.624: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:06:52.143133+00:00        LOCAL7.ERR      10.0.0.126      <187>2023: *Oct  1 11:06:15.624: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:07:25.071916+00:00        LOCAL7.ERR      10.0.0.128      <187>1989: Oct  1 20:07:23.996 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:07:53.346136+00:00        LOCAL7.ERR      10.0.0.126      <187>2024: *Oct  1 11:07:16.834: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:07:53.346136+00:00        LOCAL7.ERR      10.0.0.126      <187>2024: *Oct  1 11:07:16.834: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:08:25.165109+00:00        LOCAL7.ERR      10.0.0.128      <187>1990: Oct  1 20:08:24.074 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:08:55.693164+00:00        LOCAL7.ERR      10.0.0.126      <187>2025: *Oct  1 11:08:19.169: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:08:55.693164+00:00        LOCAL7.ERR      10.0.0.126      <187>2025: *Oct  1 11:08:19.169: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:09:25.159061+00:00        LOCAL7.ERR      10.0.0.128      <187>1991: Oct  1 20:09:24.082 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:09:55.936030+00:00        LOCAL7.ERR      10.0.0.126      <187>2026: *Oct  1 11:09:19.413: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:09:55.936030+00:00        LOCAL7.ERR      10.0.0.126      <187>2026: *Oct  1 11:09:19.413: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:10:25.738185+00:00        LOCAL7.ERR      10.0.0.128      <187>1992: Oct  1 20:10:24.658 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:10:55.982015+00:00        LOCAL7.ERR      10.0.0.126      <187>2027: *Oct  1 11:10:19.453: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:10:55.982015+00:00        LOCAL7.ERR      10.0.0.126      <187>2027: *Oct  1 11:10:19.453: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:11:25.793791+00:00        LOCAL7.ERR      10.0.0.128      <187>1993: Oct  1 20:11:24.718 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:11:56.116849+00:00        LOCAL7.ERR      10.0.0.126      <187>2028: *Oct  1 11:11:19.585: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:11:56.116849+00:00        LOCAL7.ERR      10.0.0.126      <187>2028: *Oct  1 11:11:19.585: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:12:26.499245+00:00        LOCAL7.ERR      10.0.0.128      <187>1994: Oct  1 20:12:25.422 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:12:58.021052+00:00        LOCAL7.ERR      10.0.0.126      <187>2029: *Oct  1 11:12:21.484: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:12:58.021052+00:00        LOCAL7.ERR      10.0.0.126      <187>2029: *Oct  1 11:12:21.484: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:13:27.965381+00:00        LOCAL7.ERR      10.0.0.128      <187>1995: Oct  1 20:13:26.856 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:14:00.426413+00:00        LOCAL7.ERR      10.0.0.126      <187>2030: *Oct  1 11:13:23.899: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:14:00.426413+00:00        LOCAL7.ERR      10.0.0.126      <187>2030: *Oct  1 11:13:23.899: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:14:27.985476+00:00        LOCAL7.ERR      10.0.0.128      <187>1996: Oct  1 20:14:26.879 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:15:00+00:00       LOCAL0.INFO     127.0.0.1       <134>Oct  1 11:15:00 netld27 backup 10.0.0.234@Default starting
2022-10-01T11:15:02+00:00       LOCAL0.INFO     127.0.0.1       <134>Oct  1 11:15:02 netld27 Exiting task of type 'backup' for 10.0.0.234@Default.
2022-10-01T11:15:02+00:00       LOCAL0.INFO     127.0.0.1       <134>Oct  1 11:15:02 netld27 backup 10.0.0.234@Default completed successfully.
2022-10-01T11:15:28.699484+00:00        LOCAL7.ERR      10.0.0.128      <187>1997: Oct  1 20:15:27.621 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:16:28.733394+00:00        LOCAL7.ERR      10.0.0.128      <187>1998: Oct  1 20:16:27.655 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:17:01.806040+00:00        LOCAL7.ERR      10.0.0.126      <187>2033: *Oct  1 11:16:25.270: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:17:01.806040+00:00        LOCAL7.ERR      10.0.0.126      <187>2033: *Oct  1 11:16:25.270: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:17:29.580761+00:00        LOCAL7.ERR      10.0.0.128      <187>1999: Oct  1 20:17:28.500 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:01.861776+00:00        LOCAL7.ERR      10.0.0.126      <187>2034: *Oct  1 11:17:25.326: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:01.861776+00:00        LOCAL7.ERR      10.0.0.126      <187>2034: *Oct  1 11:17:25.326: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:29.627107+00:00        LOCAL7.ERR      10.0.0.128      <187>2000: Oct  1 20:18:28.547 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:19:02.024116+00:00        LOCAL7.ERR      10.0.0.126      <187>2035: *Oct  1 11:18:25.492: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:19:02.086532+00:00        LOCAL7.ERR      10.0.0.126      <187>2035: *Oct  1 11:18:25.492: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:19:29.983305+00:00        LOCAL7.ERR      10.0.0.128      <187>2001: Oct  1 20:19:28.904 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:02.126086+00:00        LOCAL7.ERR      10.0.0.126      <187>2036: *Oct  1 11:19:25.583: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:02.126086+00:00        LOCAL7.ERR      10.0.0.126      <187>2036: *Oct  1 11:19:25.583: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:31.064699+00:00        LOCAL7.ERR      10.0.0.128      <187>2002: Oct  1 20:20:29.987 JST: %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
```

14.4 Save Syslogs 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".

The "External logging" option is displayed when linked with an NFS/SMB server.



Server Settings

- Data Retention
- System Backup
- Mail Server
- SNMP Traps
- Users
- Roles
- External Authentication
- Custom Device Fields
- Memo Templates
- Launchers
- Smart Bridges
- Networks

☑ Enable Syslog Server

☑ Enable realtime backup

Log size (MB): 20

Log count: 5

Days to keep: 2

Time Interval: None

☑ DNS resolve the sender address

External Logging

☑ Log to external attached storage

Syslog Rules

3. Click [OK].

ThirdEye must be restarted for the settings to take effect.

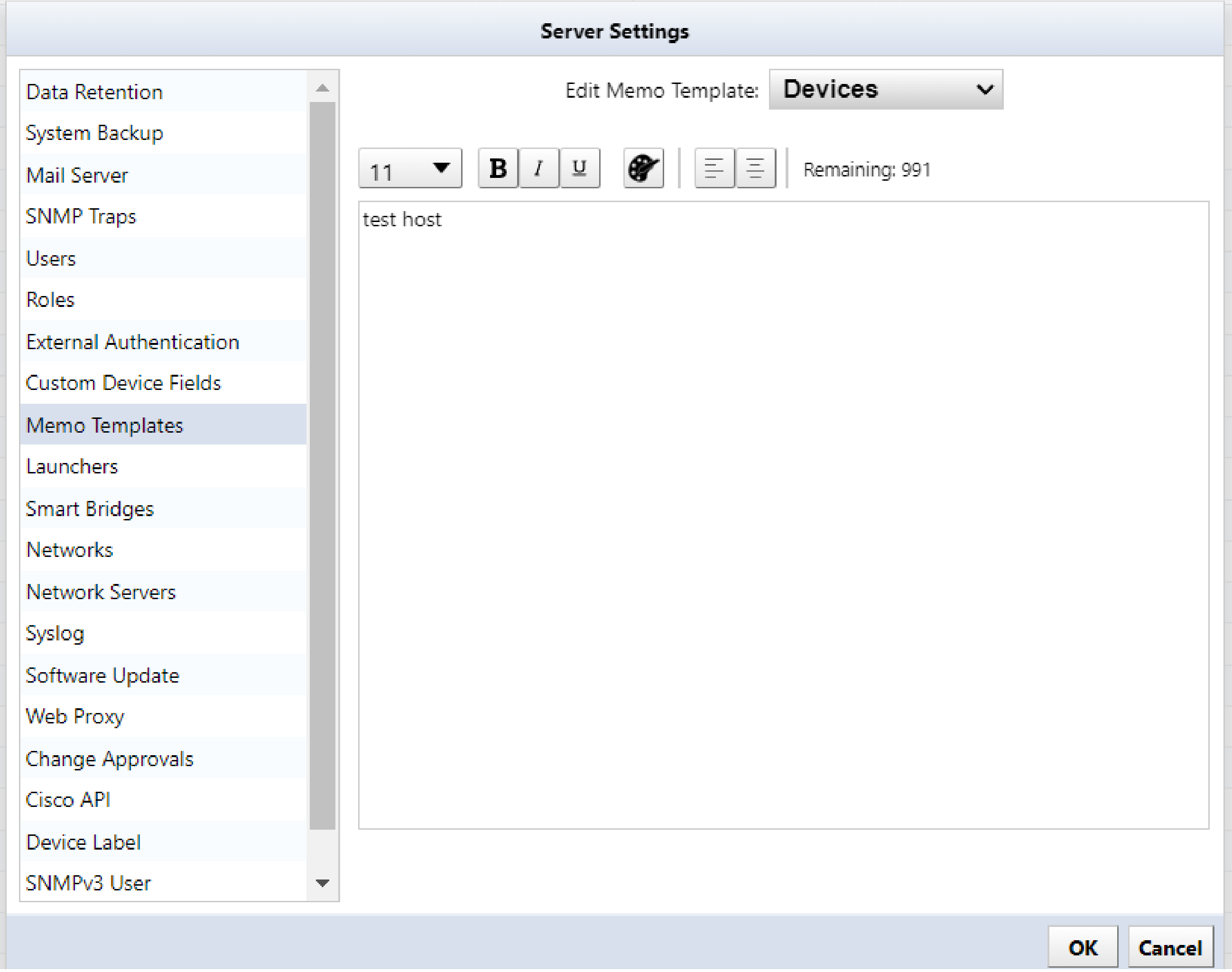
4. Click [OK] on the reboot confirmation screen, and ThirdEye will automatically restart.

> **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.

14.5 Edit 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]



Edit Memo Template: Devices

Remaining: 991

test host

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.

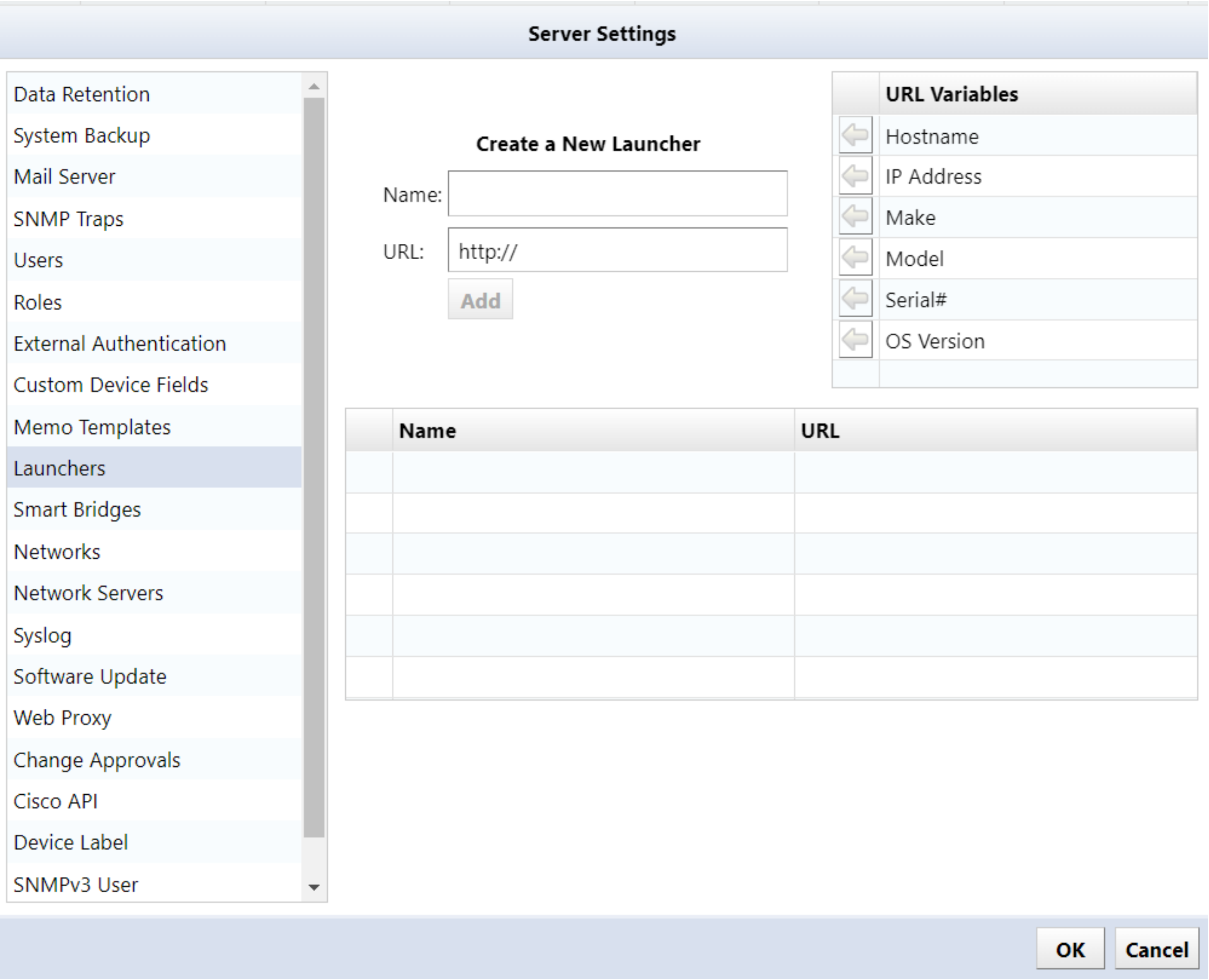
Item	Explanation
Centered	Set text alignment to center.
Number of input characters	Number of characters remaining that can be entered.All characters are counted as one character, regardless of whether they are full-width or half-width.

3. Click [OK].

14.6 Add 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 [Launchers]



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:

Item	Explanation	Example
Hostname	Quoting the device hostname.	If you select a device with host name=router1.example.com, the “{device.hostname}” part of the URL will be replaced with “router1.example.com” and executed. http://{device.hostname} → router1.example.com
IP address	Quote the device’s IP address.	If you select a device with IP address = 192.168.0.1, the `{device.ipAddress}` part of the URL will be replaced with `192.168.0.1` and executed. http://{device.ipAddress} → http://192.168.0.1
Manufacturer	Quoting the manufacturer name obtained during configuration backup	http://{device.hardwareVendor}
Model	Quoting the model name obtained from the configuration backup	http://{device.model}
Serial number	Quoting the serial number obtained during configuration backup	http://{device.assetIdentity}
OS version	Quoting the software version obtained by config backup	http://{device.osVersion}

4. Click [OK].

SECTION 15

MONITORING

There are several ways to monitor devices, such as information collection using SNMP and monitoring using ICMP Ping.

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)

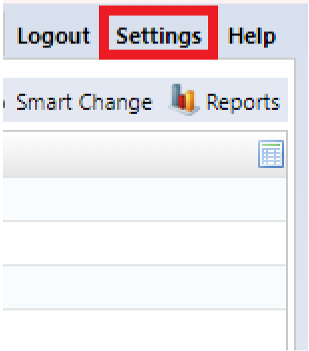
15.1 Set Up Mail Server

Enter the SMTP server information for Email Server notifications from ThirdEye.

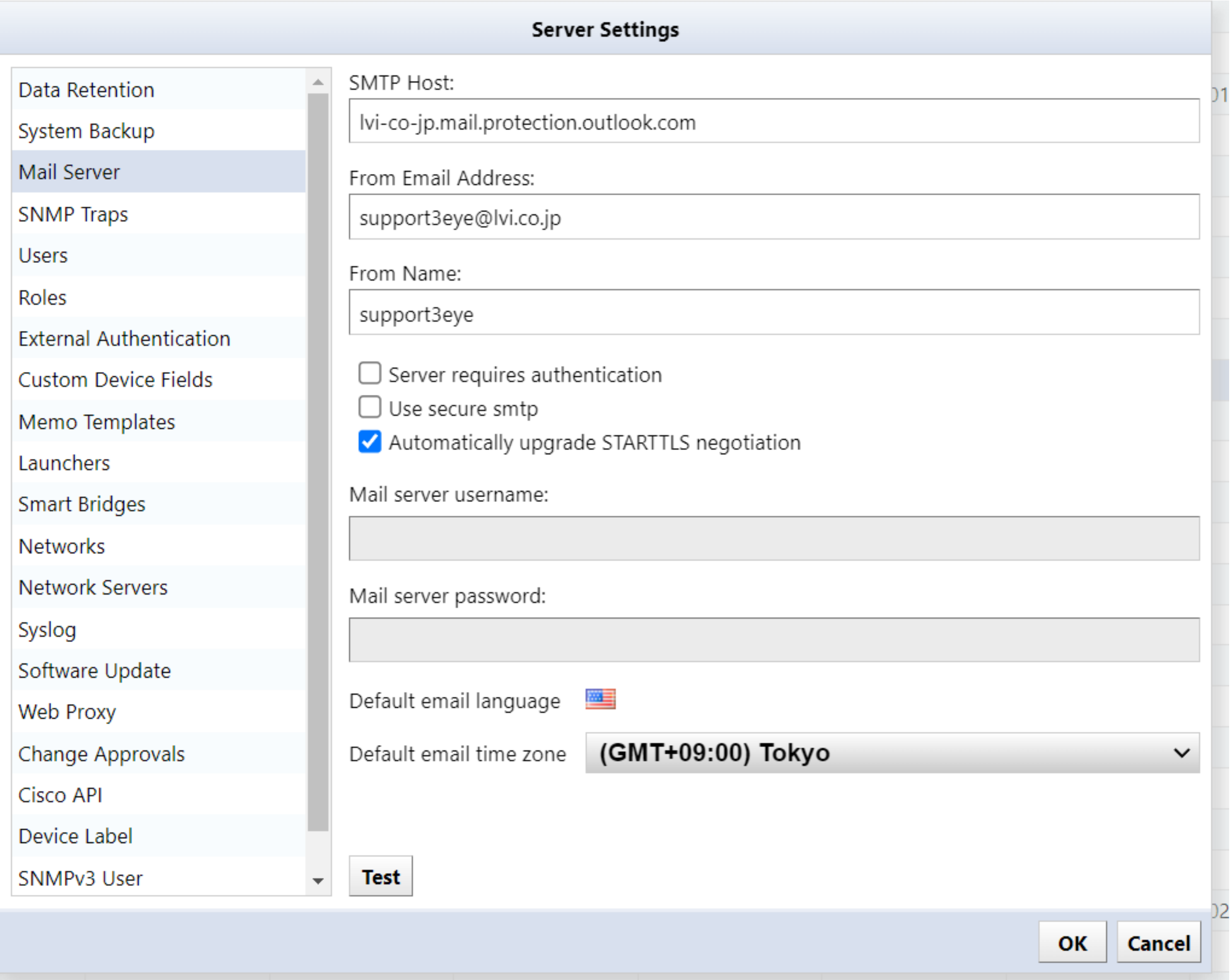
Note

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.



SMTP Host: lvi-co-jp.mail.protection.outlook.com

From Email Address: support3eye@lvi.co.jp

From Name: support3eye

□ Server requires authentication

□ Use secure smtp

☑ Automatically upgrade STARTTLS negotiation

Mail server username:

Mail server password:

Default email language 🇺🇸

Default email time zone (GMT+09:00) Tokyo

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

Field	Explanation
	Mail server password… Authentication password
Use secure SMTP	Enable TLS.
Automatically upgrade STARTTLS negotiation	Automatically upgrade to secure connections using TLS or SSL.
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].

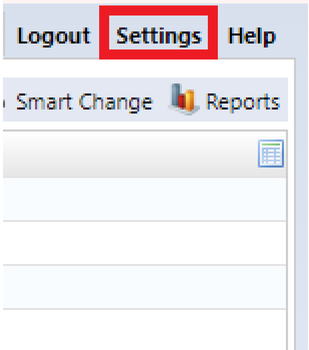
15.2 Use SysName for Hostname

ThirdEye retrieves the hostname from your DNS server and displays it in the Editor's [Devices] tab. `sysName` serves as the primary host identifier for syslog messages when DNS resolution is disabled. When configured to use SysName for hostname identification, syslog handling changes:

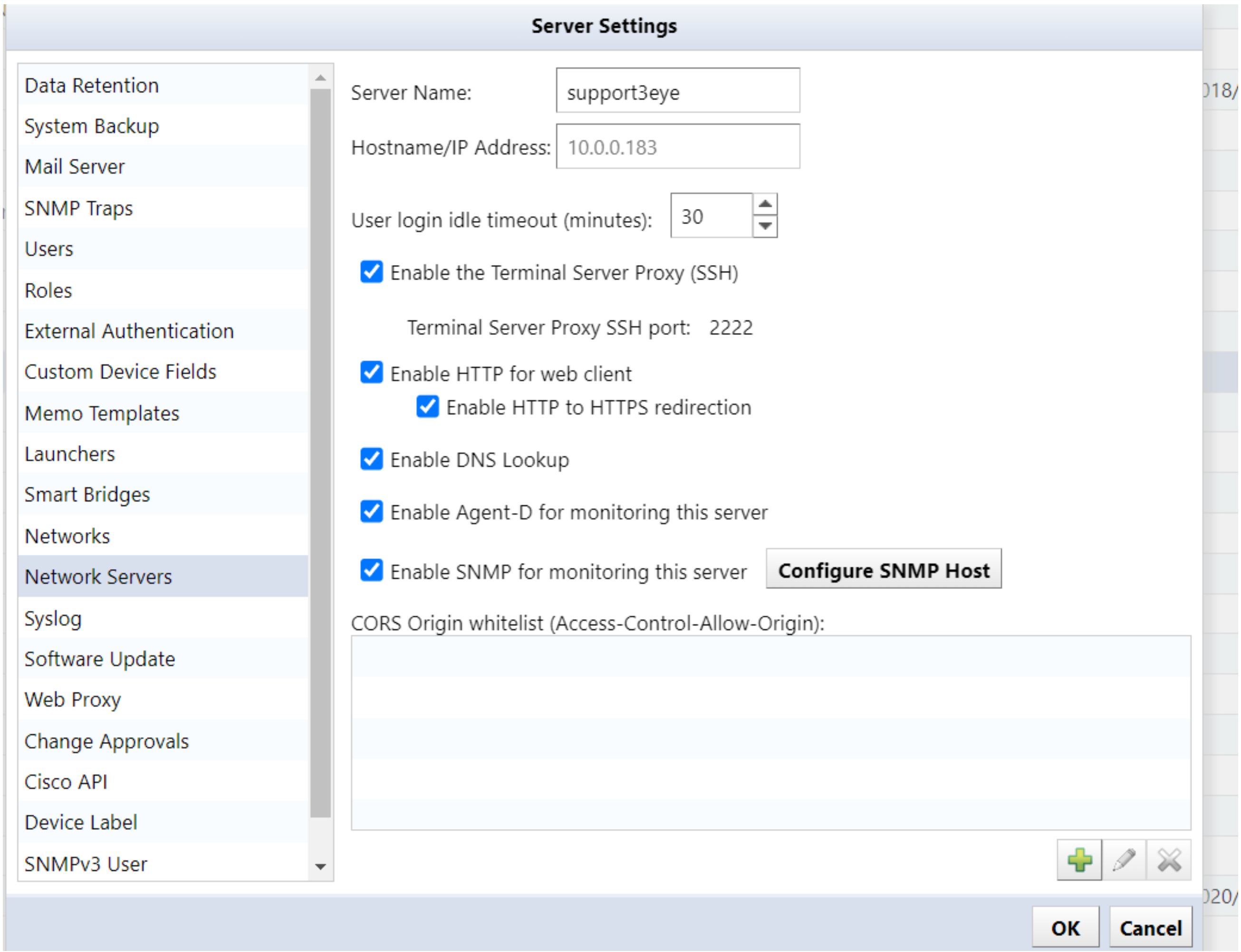
- **Host Identification**: SNMP sysName from device inventory are used instead of DNS reverse lookup. And valid SNMP credentials are required for accurate device correlation.
- **Syslog Rules**: Filtering rules based on hostname now reference `sysName` values.
- **Operations**: Consistent `sysName` values are required across devices. Audit logs show `sysName` instead of DNS-resolved names.

To use the host name `(sysName)` on 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”.



Server Settings

Server Name: support3eye

Hostname/IP Address: 10.0.0.183

User login idle timeout (minutes): 30

☑ Enable the Terminal Server Proxy (SSH)

Terminal Server Proxy SSH port: 2222

☑ Enable HTTP for web client

☑ Enable HTTP to HTTPS redirection

☑ Enable DNS Lookup

☑ Enable Agent-D for monitoring this server

☑ Enable SNMP for monitoring this server

CORS Origin whitelist (Access-Control-Allow-Origin):

3. Click [OK].

15.3 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.

15.3.1 Terminal Proxy Setup

There are two ways to use terminal proxy: using a **web browser** and using **Tera Term**.

15.3.1.1 Tera Term Setup

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.)

1. **Install Tera Term on the terminal to be operated.**

The terminal proxy calls Tera Term on the PC you are operating.

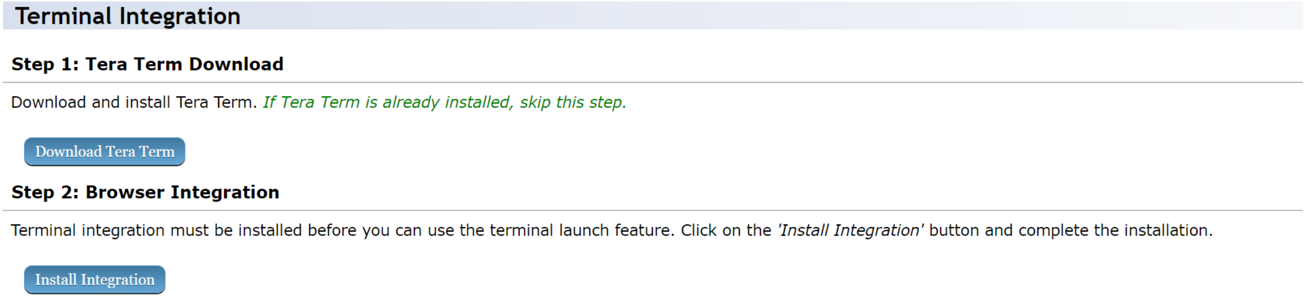
2. **Installing Browser Integration**

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 Term** section.

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



Terminal Integration

Step 1: Tera Term Download

Download and install Tera Term. *If Tera Term is already installed, skip this step.*

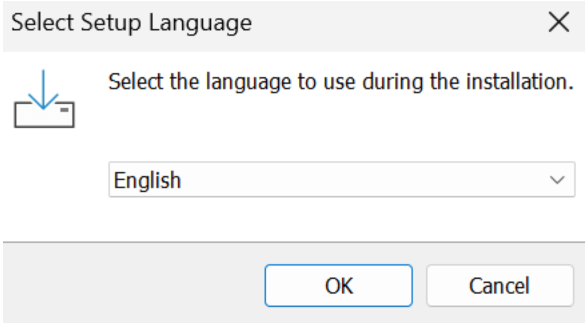
Step 2: Browser Integration

Terminal integration must be installed before you can use the terminal launch feature. Click on the *'Install Integration'* button and complete the installation.

> **Note**
>
> Regarding Browser Integration, you may need to reconfigure if you clear your browser's cache or update ThirdEye.

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

3. Select the display language and click [OK]

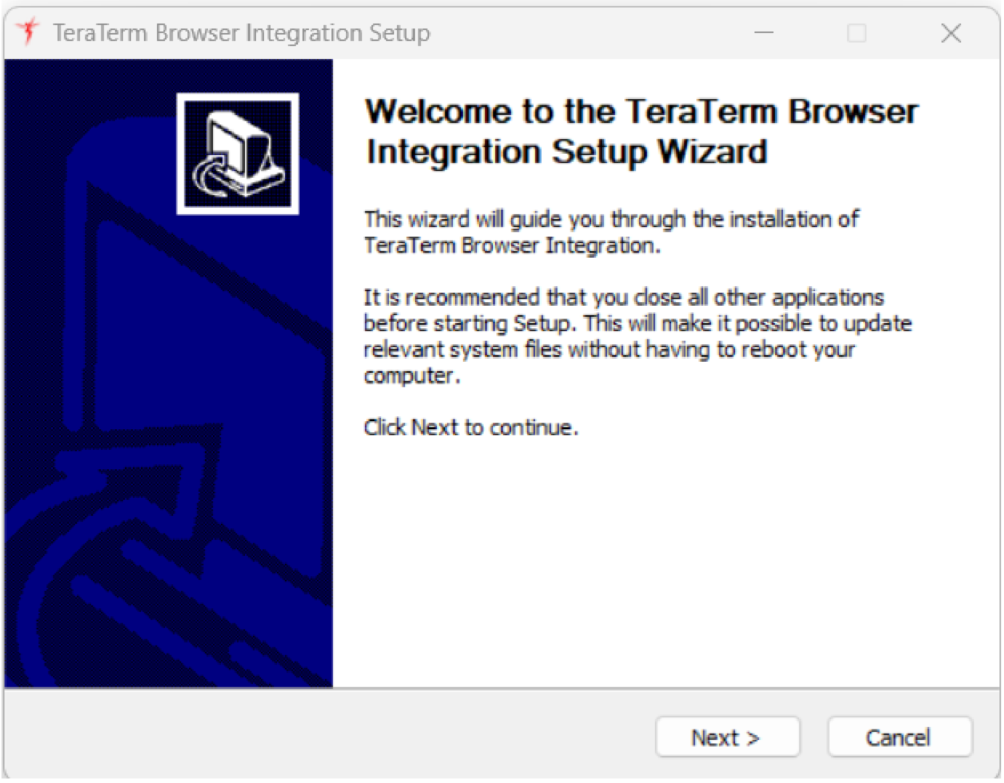


Select Setup Language

Select the language to use during the installation.

English

4. Click [Next].



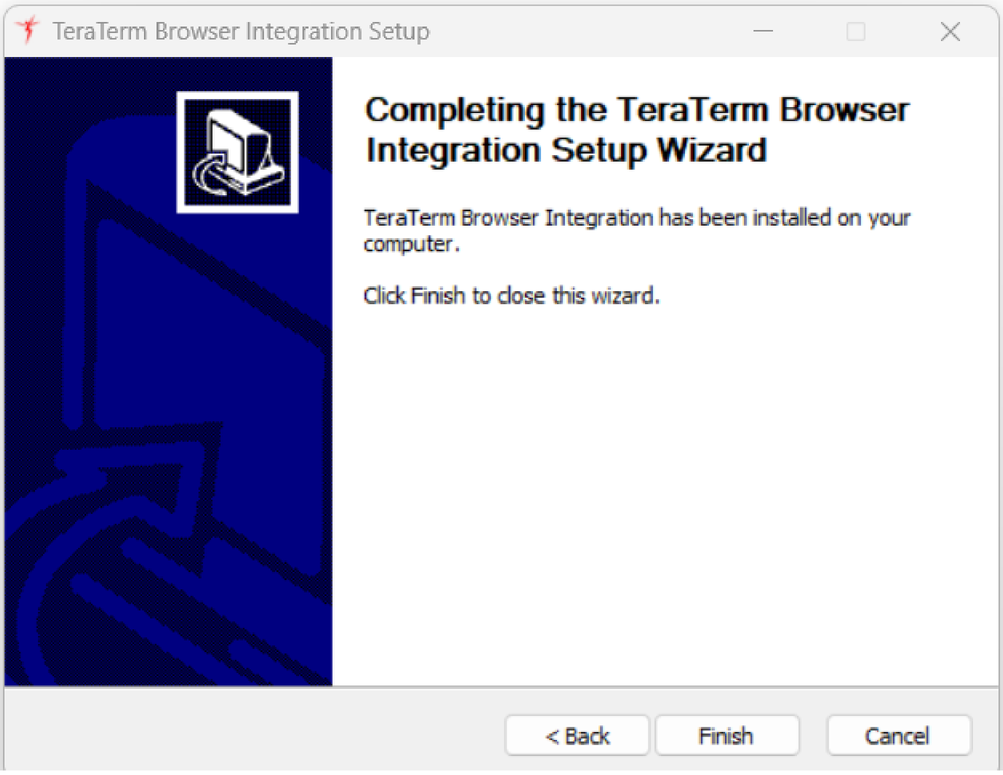
Welcome to the TeraTerm Browser Integration Setup Wizard

This wizard will guide you through the installation of TeraTerm Browser Integration.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

5. Click [Finish].



Completing the TeraTerm Browser Integration Setup Wizard

TeraTerm Browser Integration has been installed on your computer.

Click Finish to close this wizard.

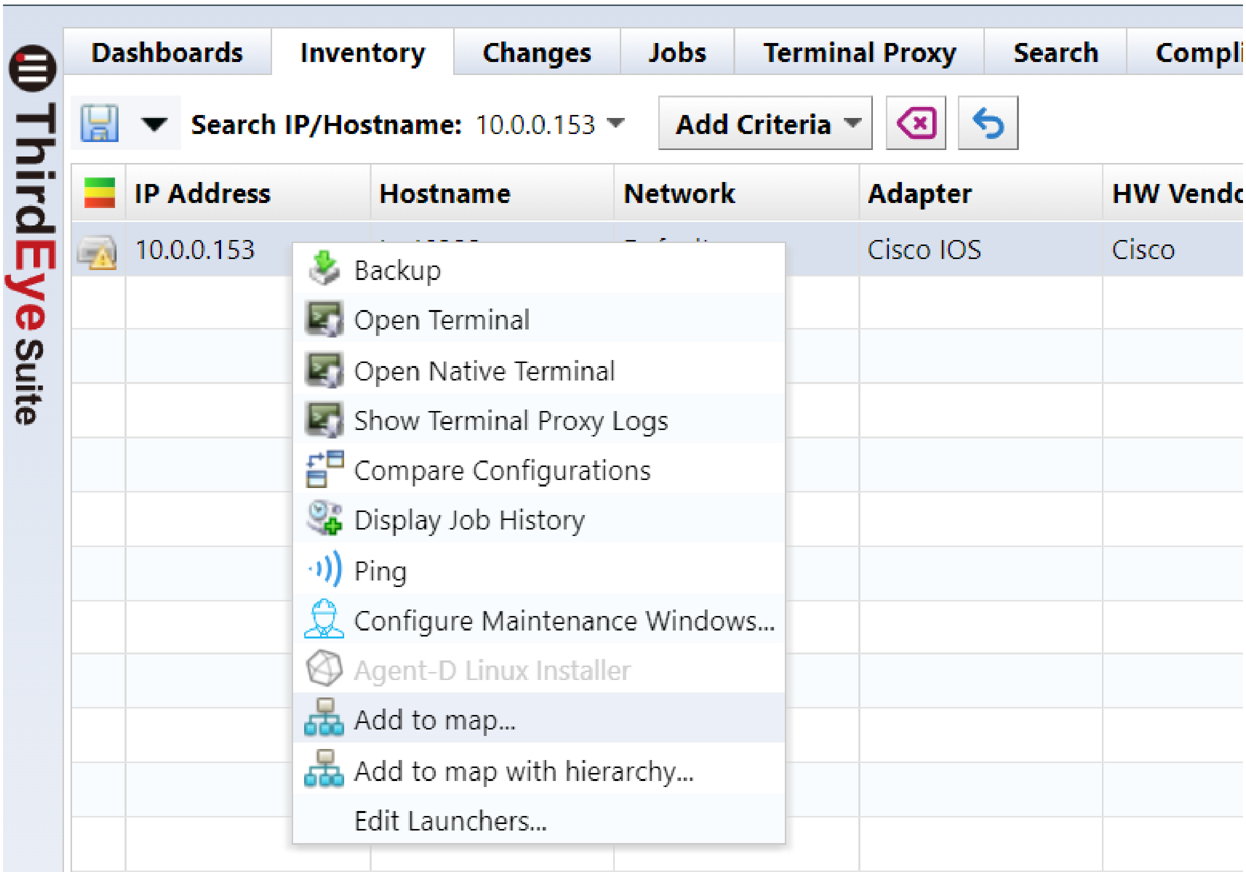
Preparation is now complete.

15.3.2 Start the Terminal Proxy

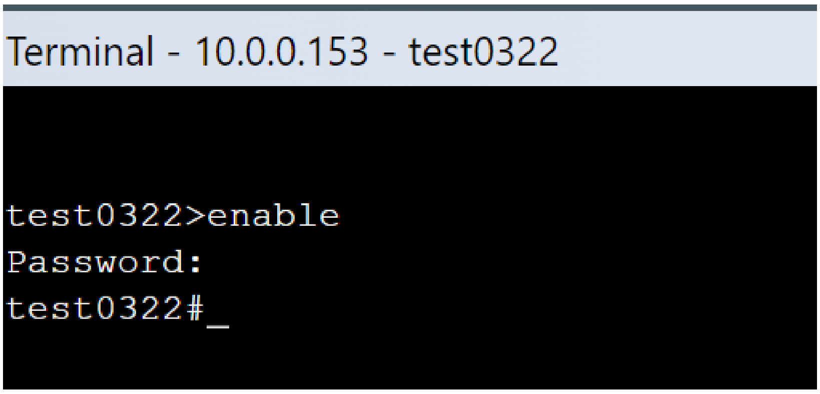
If a device configuration backup has been obtained when you start the terminal proxy, you can skip selecting the protocol and entering the user name/password after starting the terminal proxy.

15.3.3 Web Browser Setup

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.



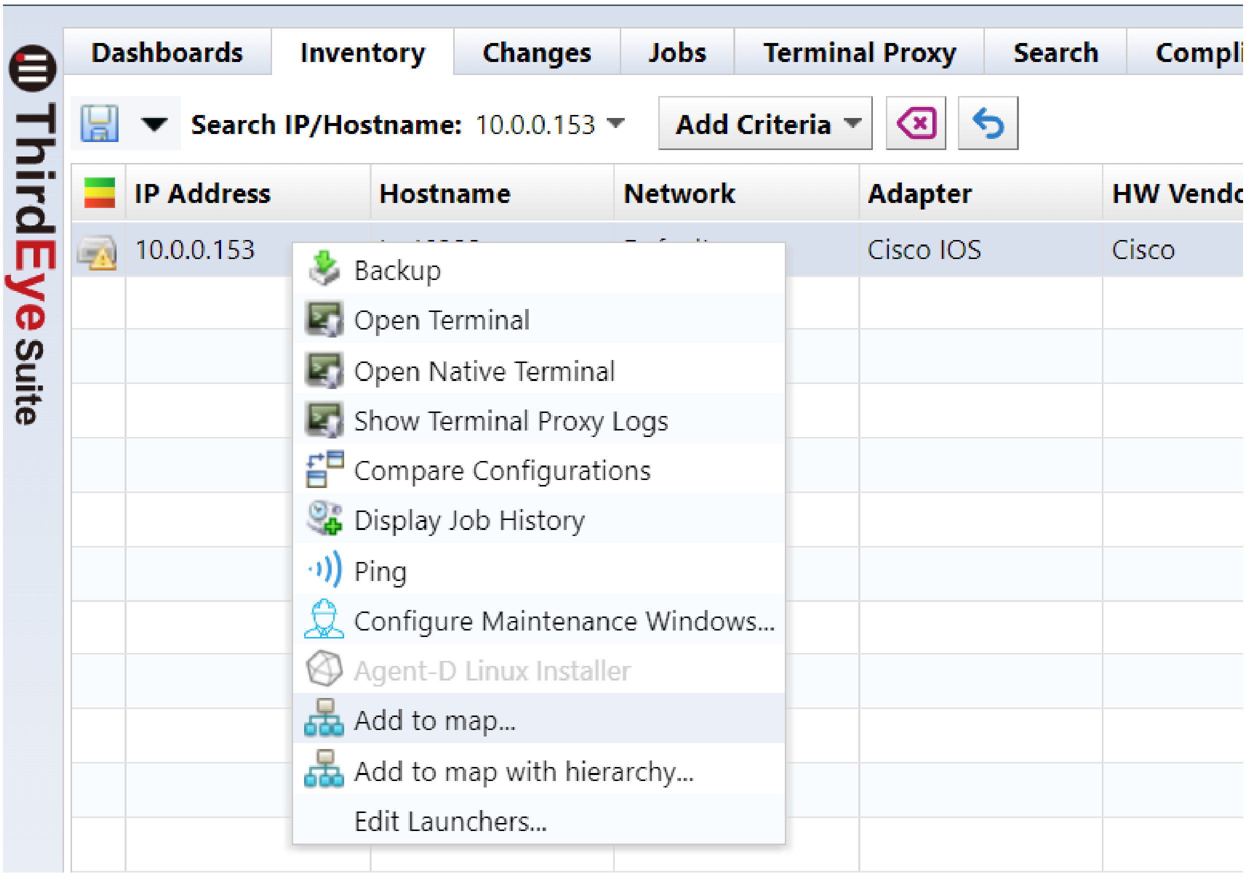
```
test0322>enable
Password:
test0322#_
```

15.3.4 Use Tera Term

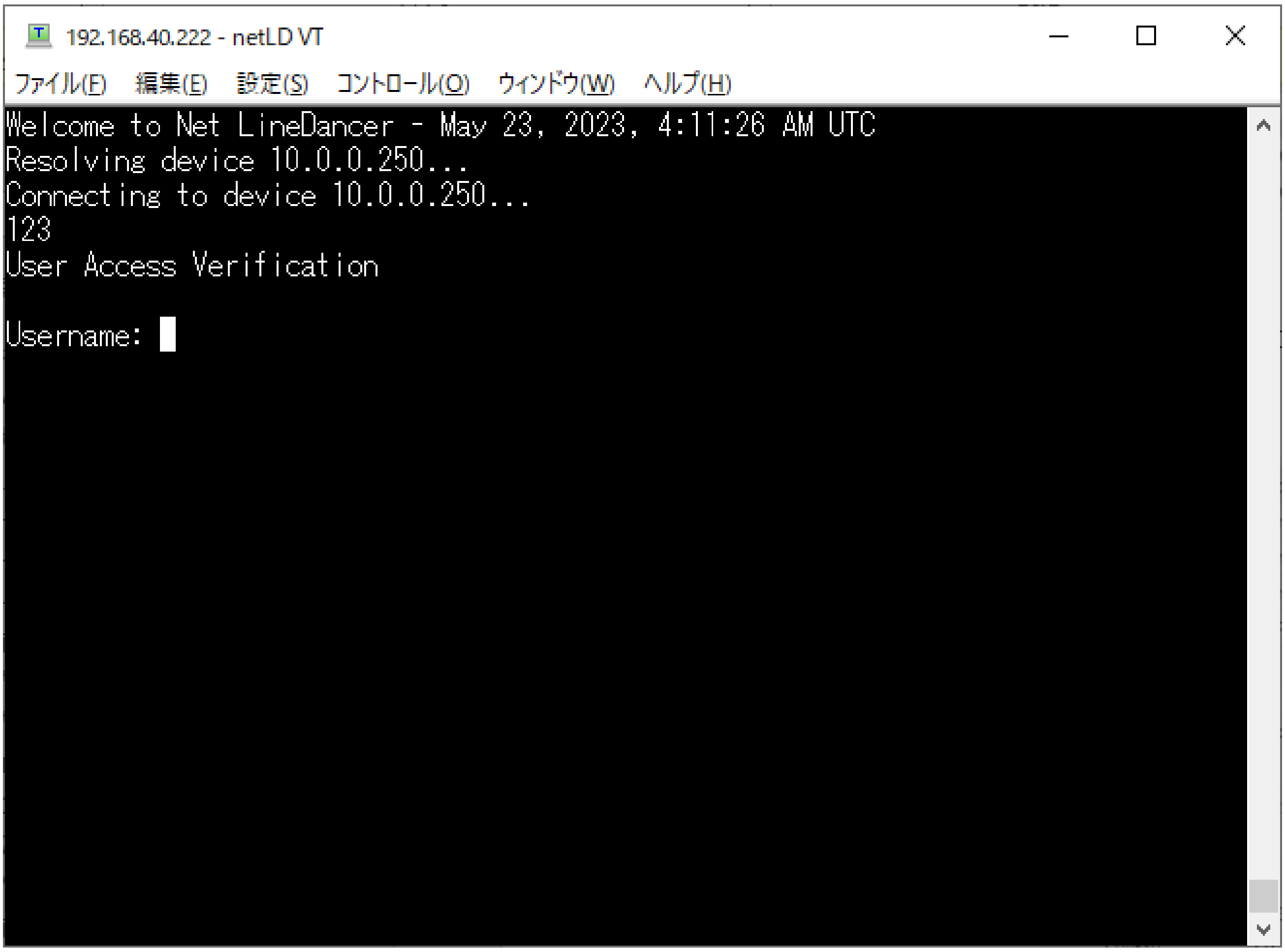
1. Select the [Inventory] tab.

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



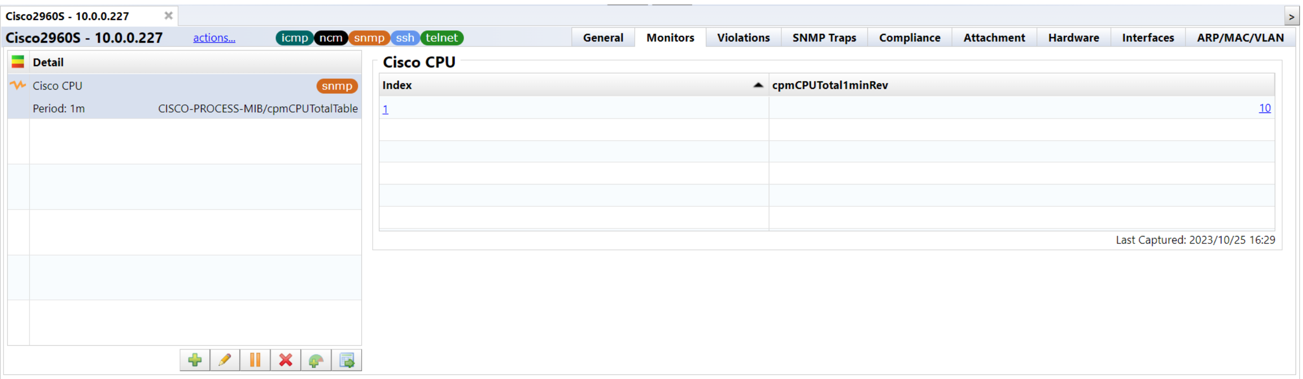
```
Welcome to Net LineDancer - May 23, 2023, 4:11:26 AM UTC
Resolving device 10.0.0.250...
Connecting to device 10.0.0.250...
123
User Access Verification

Username:
```

15.4 Configure 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].



Cisco CPU snmp

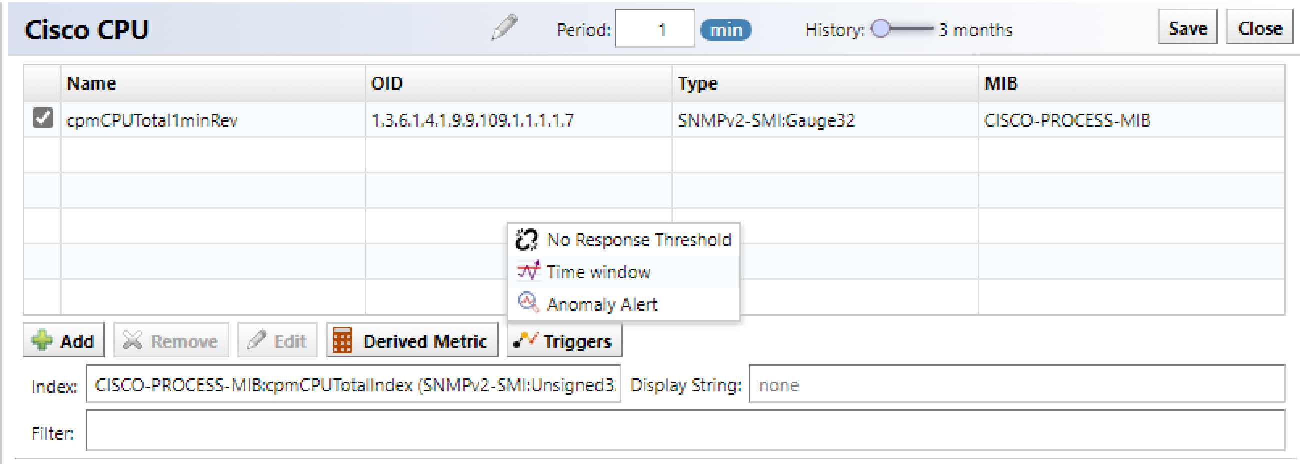
Period: 1m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU

Index	cpmCPUTotal1minRev
1	10

Last Captured: 2023/10/25 16:29

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



Cisco CPU

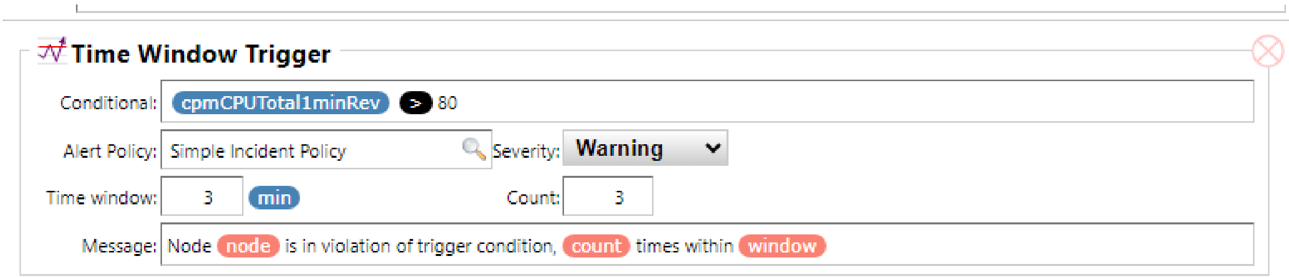
Period: 1 min History: 3 months

	Name	OID	Type	MIB
☑	cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Index: CISCO-PROCESS-MIB:cpmCPUTotalIndex (SNMPv2-SMI:Unsigned3 Display String: none

Filter:

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



Time Window Trigger

Conditional: cpmCPUTotal1minRev > 80

Alert Policy: Simple Incident Policy Severity: Warning

Time window: 3 min Count: 3

Message: Node node is in violation of trigger condition, count times within window

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`

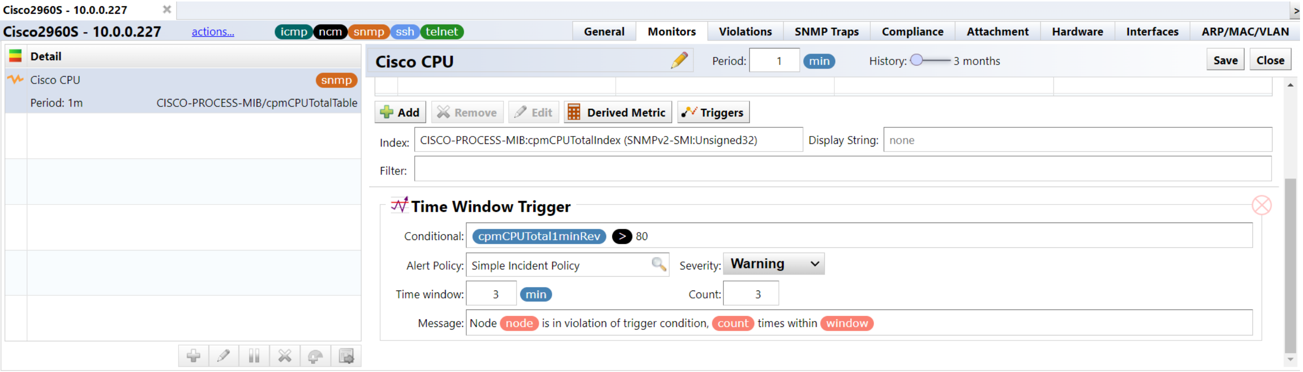
Alert Policy	Specify alert policy.
Severity	Select the severity from the following: (Initial value: warning): “Emergency”, “Alert”, “Critical”, “Error”, “Warning”, “Notification”, “Information”, “Debug”
Time window	Set the period for executing the process. (Minimum value: 30 seconds) The period that 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	ⓘ

Security level	Status	Severity status icon
	information	ⓘ
Low	**debug**	●

4. Click [Save].



Cisco CPU snmp

Period: 1m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU Period: 1 min History: 3 months

Index: CISCO-PROCESS-MIB:cpmCPUTotalIndex (SNMPv2-SMI:Unsigned32) Display String: none

Filter:

Time Window Trigger

Conditional: cpmCPUTotal1minRev > 80

Alert Policy: Simple Incident Policy Severity: Warning

Time window: 3 min Count: 3

Message: Node node is in violation of trigger condition, count times within window

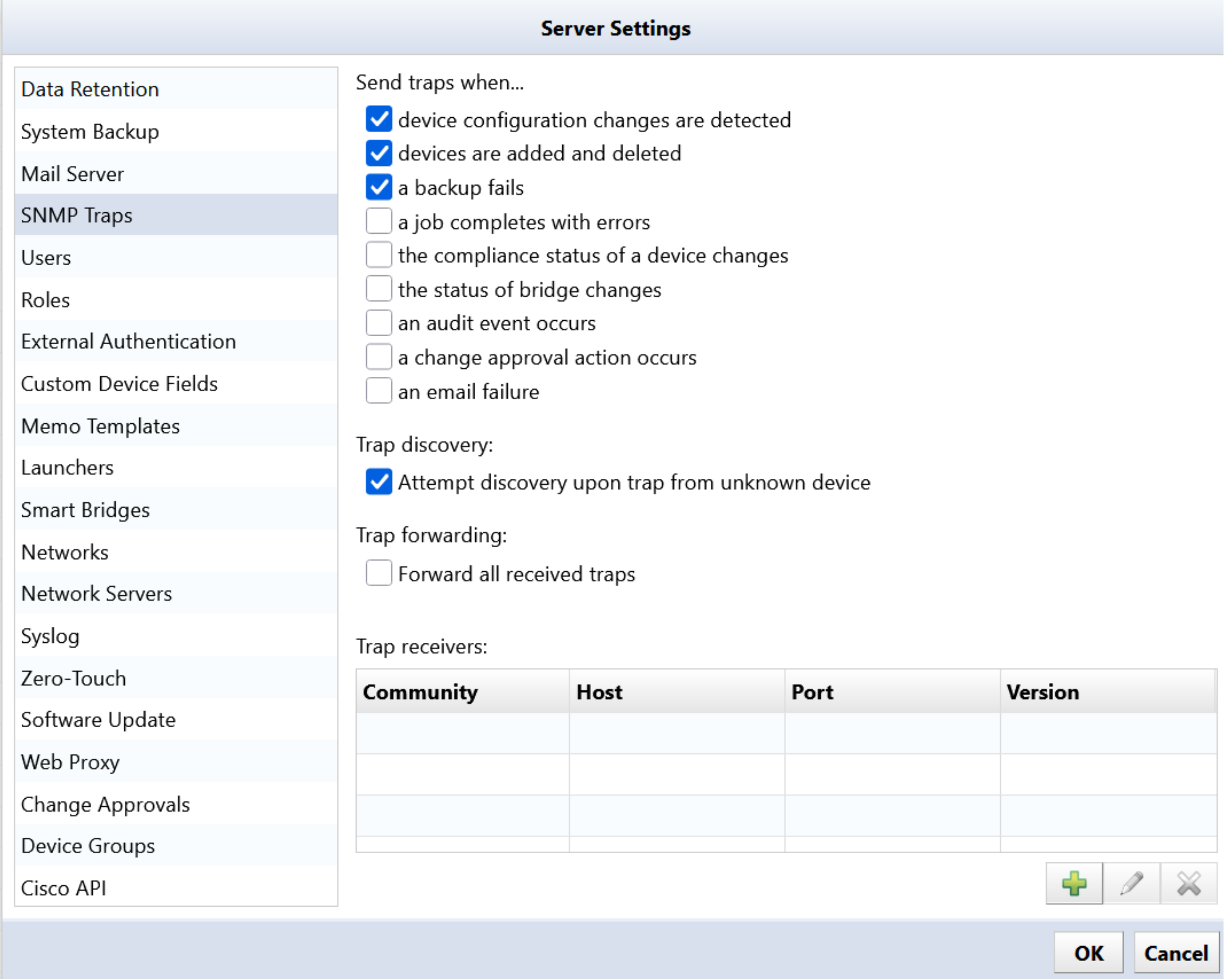
15.5 Configure SNMP Trap Handling

ThirdEye can send traps on certain events (e.g. when device configuration changes are detected) and execute actions when it receives traps (e.g. run discovery). This section describes how to configure ThirdEye to send and receive traps successfully.

15.5.1 Send traps on events

To send traps on events, select the events that you wish to subscribe to and specify where you want ThirdEye to send the traps to (trap destinations).

1. Click [Settings] on the Global Menu.
2. Click [SNMP Traps] and select the events.



Send traps when...

☑ device configuration changes are detected
☑ devices are added and deleted
☑ a backup fails
□ a job completes with errors
□ the compliance status of a device changes
□ the status of bridge changes
□ an audit event occurs
□ a change approval action occurs
□ an email failure

Trap discovery:

☑ Attempt discovery upon trap from unknown device

Trap forwarding:

□ Forward all received traps

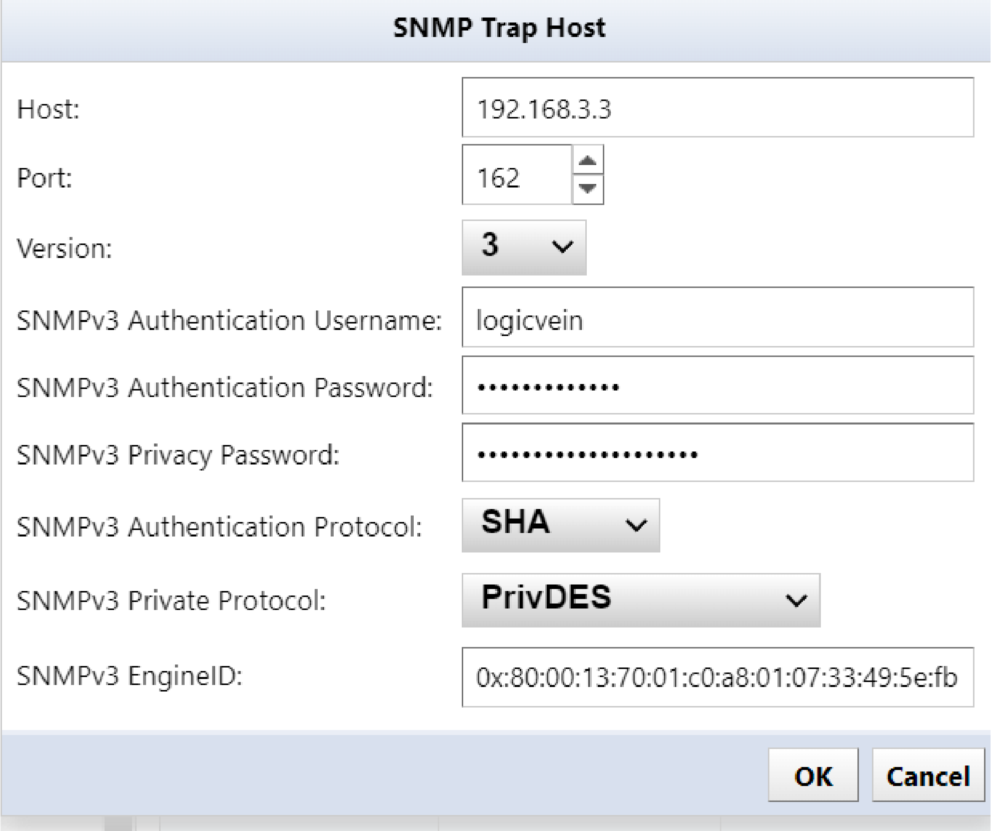
Trap receivers:

Community	Host	Port	Version

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.
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. To add a trap destination, click the + button.

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



SNMP Trap Host

Host: 192.168.3.3

Port: 162

Version: 3

SNMPv3 Authentication Username: logicvein

SNMPv3 Authentication Password: •••••••••••••

SNMPv3 Privacy Password: ••••••••••••••••••••

SNMPv3 Authentication Protocol: SHA

SNMPv3 Private Protocol: PrivDES

SNMPv3 EngineID: 0x:80:00:13:70:01:c0:a8:01:07:33:49:5e:fb

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 2c at Version)
(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`

Items	Explanation
(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)

15.5.2 Enable/disable trap-triggered discovery

The trap-triggered discovery feature allows ThirdEye to automatically discover and add previously unknown devices that send SNMP traps to the server. If there are multiple networks configured in the product, the server will employ heuristics to determine which network the device belongs to based on the source IP address of the trap. SNMP credentials for the network must be configured in advance for successful discovery. There are also delays of up to several minutes introduced to prevent excessive discovery attempts and to allow batch discovery of multiple traps from devices in the same network. Devices that fail discovery will have subsequent traps ignored for a period of five minutes before discovery can again be triggered. Devices that are discovered but subsequently deleted cannot trigger a discovery until the next time the server is restarted.

Enable or disable trap triggered discovery by using the checkbox “Attempt discovery upon trap from unknown device.”

15.5.3 Receive traps by SNMP v1/v2c

If there are no configured SNMP v1/v2 community strings, all SNMP v1/v2 traps will be accepted. However, if you wish to enforce that SNMP v1/v2 traps present only verified community strings, they must be specified in [Settings]. Once defined, only traps that present a matching community string will be accepted.

To add SNMP v1/v2c trap community strings:

1. Click [Settings] to open the [Server Settings] window and click the [SNMP Trap Users] item from the list on the left.
2. Click the + button at the bottom right, below the SNMP v1/v2 table, to begin.
3. Fill in the community string that will be used for authenticating incoming SNMP Traps.
4. Click the [OK] button at the bottom right.
5. To save changes, click the [OK] button at the bottom right of the [Server Settings] window.

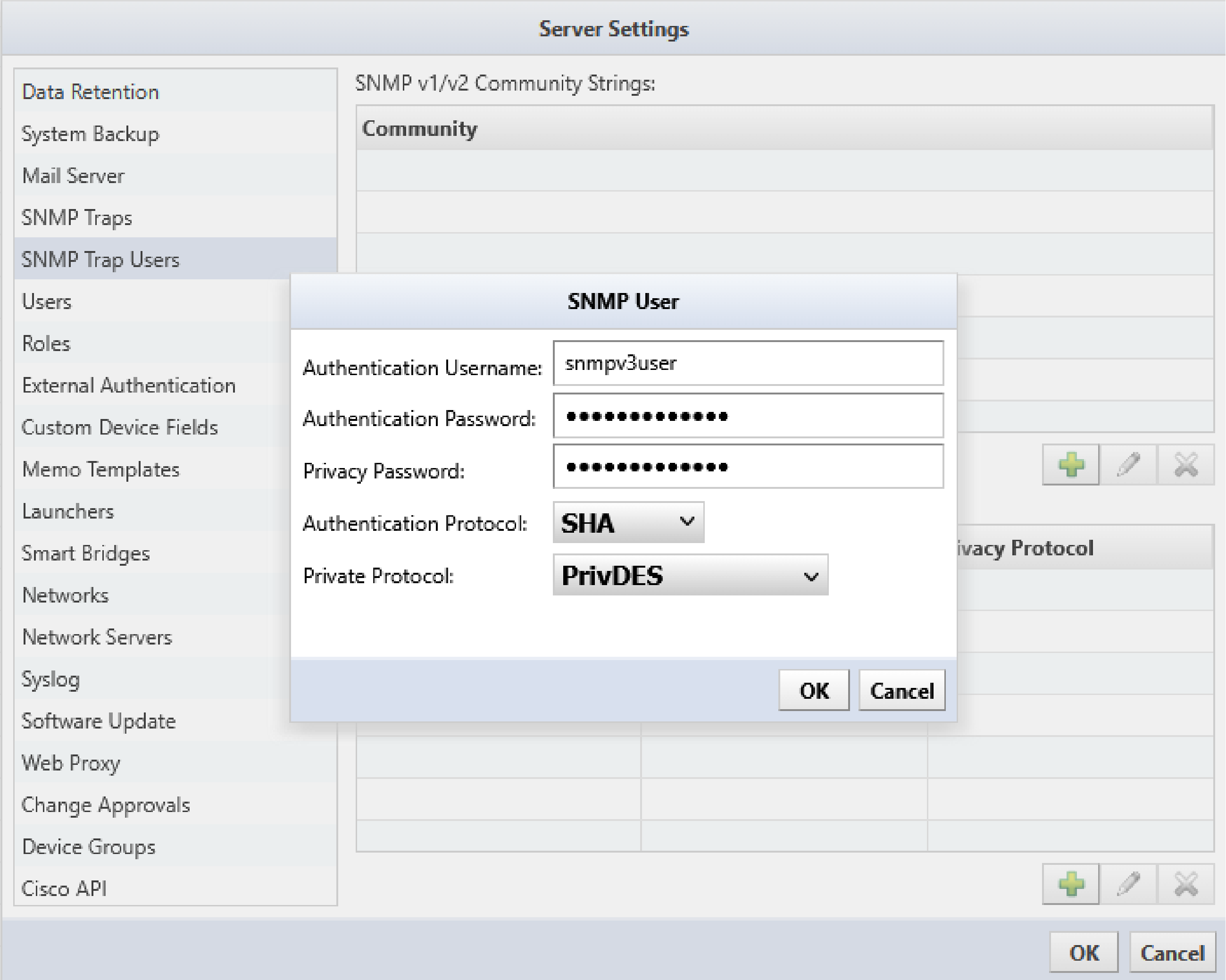
15.5.4 Receive traps by SNMPv3

To receive SNMP Traps by SNMPv3, it is required to set up credentials in advance so that ThirdEye can authenticate and/or decrypt incoming SNMP Traps.

1. Click [Settings] to open the [Server Settings] window and click the [SNMP Trap Users] item from the list on the left.
2. Click the + button at the bottom right, below the SNMP v3 table, to begin.
3. Fill in the SNMPv3 user information that will be used for authenticating and/or decrypting incoming SNMP Traps.

4. Click the [OK] button at the bottom right.

5. To save changes, click the [OK] button at the bottom right of the [Server Settings] window.



Authentication Username: snmpv3user

Authentication Password: •••••••••••••

Privacy Password: •••••••••••••

Authentication Protocol: SHA

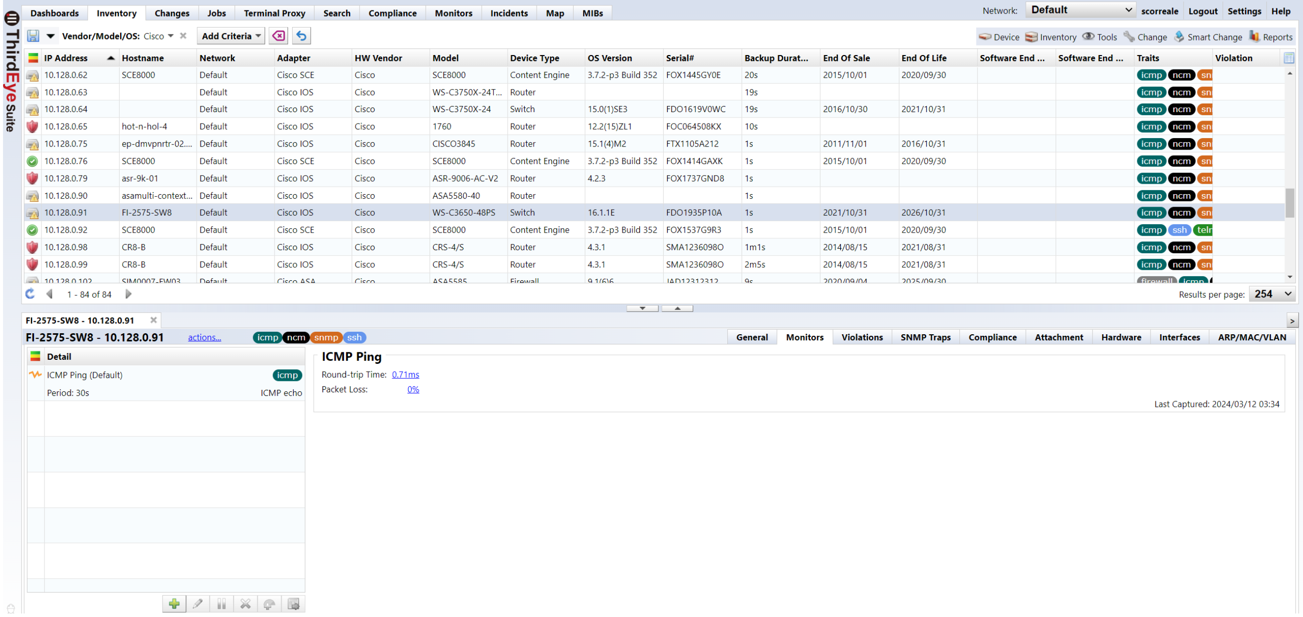
Private Protocol: PrivDES

15.6 Check the Up/Down Status of the Device Interface

You can check device details such as the status of device interfaces in the Editor of the [Inventory] main tab.

To use this function, SNMP communication with the monitored device must be possible.

1. From the list of monitored devices, doubleclick the device for which you want to check interfaces. This opens the [Inventory] Editor window at the bottom of the screen.



	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
⚠	10.128.0.62	SCE8000	Default	Cisco SCE	Cisco	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1445GY0E	20s	2015/10/01	2020/09/30			icmp ncm sn	
⚠	10.128.0.63		Default	Cisco IOS	Cisco	WS-C3750X-24T...	Router			19s					icmp ncm sn	
⚠	10.128.0.64		Default	Cisco IOS	Cisco	WS-C3750X-24	Switch	15.0(1)SE3	FDO1619V0WC	19s	2016/10/30	2021/10/31			icmp ncm sn	
⛨	10.128.0.65	hot-n-hol-4	Default	Cisco IOS	Cisco	1760	Router	12.2(15)ZL1	FOC064508KX	10s					icmp ncm sn	
⚠	10.128.0.75	ep-dmvpnrtr-02....	Default	Cisco IOS	Cisco	CISCO3845	Router	15.1(4)M2	FTX1105A212	1s	2011/11/01	2016/10/31			icmp ncm sn	
✓	10.128.0.76	SCE8000	Default	Cisco SCE	Cisco	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1414GAXK	1s	2015/10/01	2020/09/30			icmp ncm sn	
⛨	10.128.0.79	asr-9k-01	Default	Cisco IOS	Cisco	ASR-9006-AC-V2	Router	4.2.3	FOX1737GND8	1s					icmp ncm sn	
⚠	10.128.0.90	asamulti-context...	Default	Cisco IOS	Cisco	ASA5580-40	Router			1s					icmp ncm sn	
⚠	10.128.0.91	FI-2575-SW8	Default	Cisco IOS	Cisco	WS-C3650-48PS	Switch	16.1.1E	FDO1935P10A	1s	2021/10/31	2026/10/31			icmp ncm sn	
✓	10.128.0.92	SCE8000	Default	Cisco SCE	Cisco	SCE8000	Content Engine	3.7.2-p3 Build 352	FOX1537G9R3	1s	2015/10/01	2020/09/30			icmp ssh teln	
⛨	10.128.0.98	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	1m1s	2014/08/15	2021/08/31			icmp ncm sn	
⛨	10.128.0.99	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	2m5s	2014/08/15	2021/08/31			icmp ncm sn	
⚠	10.128.0.102	SIM0007-FW03	Default	Cisco ASA	Cisco	ASA5585	Firewall	9.1(6)6	JAD12312312	9s	2020/09/04	2025/09/30			firewall icmp	

1 - 84 of 84 Results per page: 254

FI-2575-SW8 - 10.128.0.91

FI-2575-SW8 - 10.128.0.91 actions... icmp ncm snmp ssh

Detail

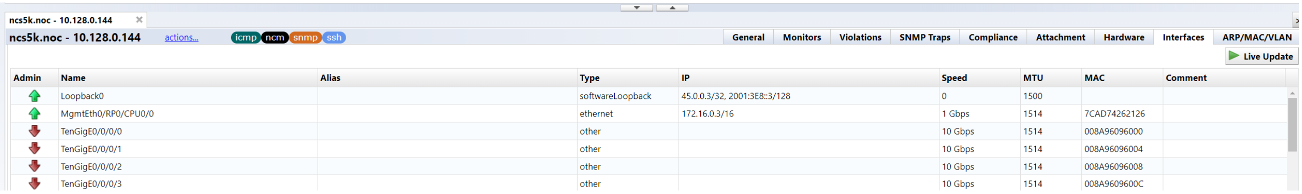
ICMP Ping (Default) icmp
Period: 30s ICMP echo

ICMP Ping
Round-trip Time: 0.71ms
Packet Loss: 0%

Last Captured: 2024/03/12 03:34

2. Click the [Interface] tab in the Editor window.

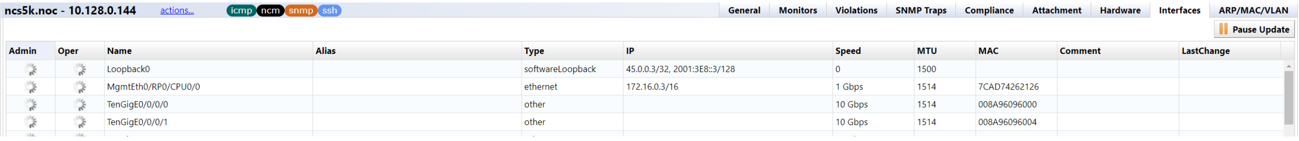
3. Click [Live Update] on the right side of the Editor window.


ncs5k.noc - 10.128.0.144

ncs5k.noc - 10.128.0.144 actions... icmp ncm snmp ssh

Admin	Name	Alias	Type	IP	Speed	MTU	MAC	Comment
⬆	Loopback0		softwareLoopback	45.0.0.3/32, 2001:3E8::3/128	0	1500		
⬆	MgmtEth0/RP0/CPU0/0		ethernet	172.16.0.3/16	1 Gbps	1514	7CAD74262126	
⬇	TenGigE0/0/0/0		other		10 Gbps	1514	008A96096000	
⬇	TenGigE0/0/0/1		other		10 Gbps	1514	008A96096004	
⬇	TenGigE0/0/0/2		other		10 Gbps	1514	008A96096008	
⬇	TenGigE0/0/0/3		other		10 Gbps	1514	008A9609600C	

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

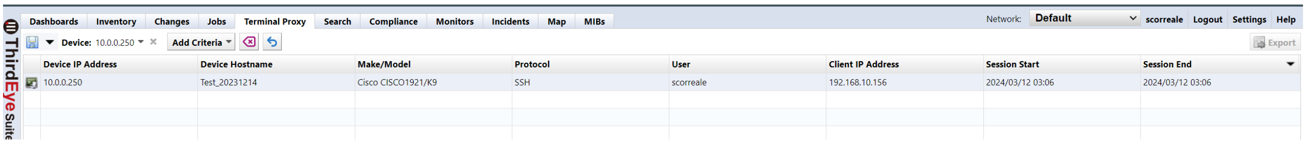

ncs5k.noc - 10.128.0.144 actions... icmp ncm snmp ssh

Admin	Oper	Name	Alias	Type	IP	Speed	MTU	MAC	Comment	LastChange
		Loopback0		softwareLoopback	45.0.0.3/32, 2001:3E8::3/128	0	1500			
		MgmtEth0/RP0/CPU0/0		ethernet	172.16.0.3/16	1 Gbps	1514	7CAD74262126		
		TenGigE0/0/0/0		other		10 Gbps	1514	008A96096000		
		TenGigE0/0/0/1		other		10 Gbps	1514	008A96096004		

To stop [Live Update], click [Pause Updates], or close the Editor window.

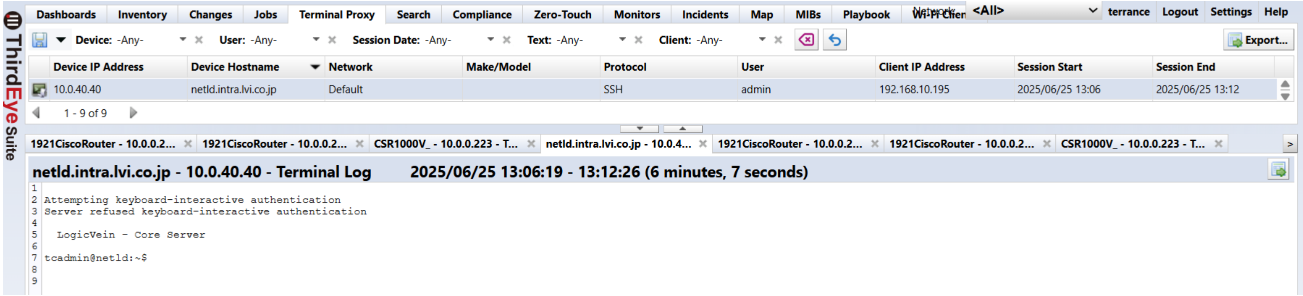
15.7 Check Operation Log

1. Select the [Terminal Proxy] tab.



Device IP Address	Device Hostname	Make/Model	Protocol	User	Client IP Address	Session Start	Session End
10.0.0.250	Test_20231214	Cisco CISCO1921/K9	SSH	scorreale	192.168.10.156	2024/03/12 03:06	2024/03/12 03:06

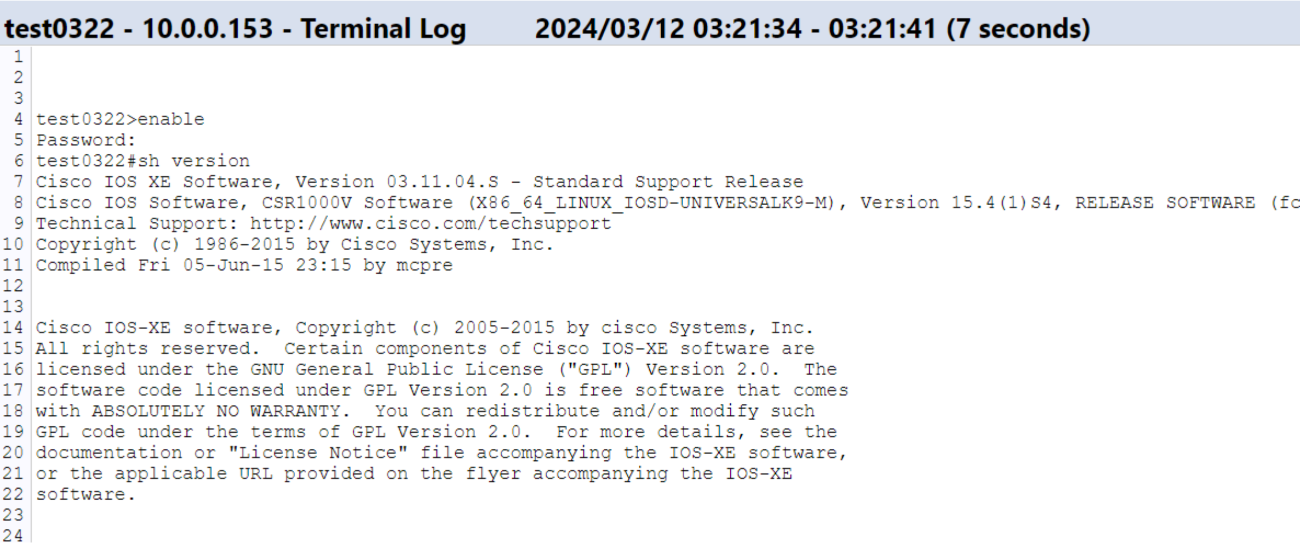
2. Doubleclick the log you want to view from the list. You cannot check the session log while connected.



Device IP Address	Device Hostname	Network	Make/Model	Protocol	User	Client IP Address	Session Start	Session End
10.0.40.40	netld.intra.lvi.co.jp	Default		SSH	admin	192.168.10.195	2025/06/25 13:06	2025/06/25 13:12

netld.intra.lvi.co.jp - 10.0.40.40 - Terminal Log   2025/06/25 13:06:19 - 13:12:26 (6 minutes, 7 seconds)

```

Attempting keyboard-interactive authentication
Server refused keyboard-interactive authentication

  LogicVein - Core Server

tcadmin@netld:~$


```

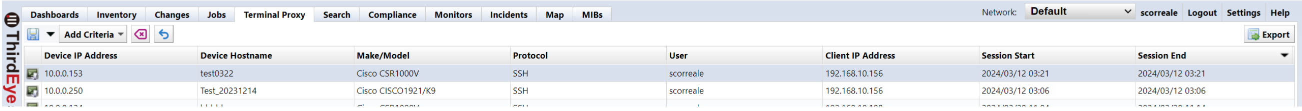


test0322 - 10.0.0.153 - Terminal Log   2024/03/12 03:21:34 - 03:21:41 (7 seconds)

```



test0322>enable
Password:
test0322#sh version
Cisco IOS XE Software, Version 03.11.04.S - Standard Support Release
Cisco IOS Software, CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.4(1)S4, RELEASE SOFTWARE (fc
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 05-Jun-15 23:15 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2015 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


```

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

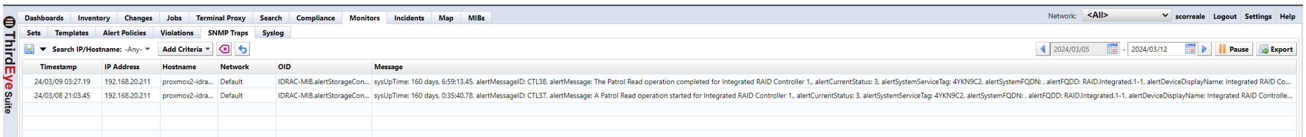
The file name is `termlogs".*YYYY-MM-DD*.zip` and is compiled in ZIP file format. `*YYYY-MM-DD*` indicates the date of saving.



Device IP Address	Device Hostname	Make/Model	Protocol	User	Client IP Address	Session Start	Session End
10.0.0.153	test0322	Cisco CSR1000V	SSH	scorreale	192.168.10.156	2024/03/12 03:21	2024/03/12 03:21
10.0.0.250	Test_20231214	Cisco CISCO1921/K9	SSH	scorreale	192.168.10.156	2024/03/12 03:06	2024/03/12 03:06

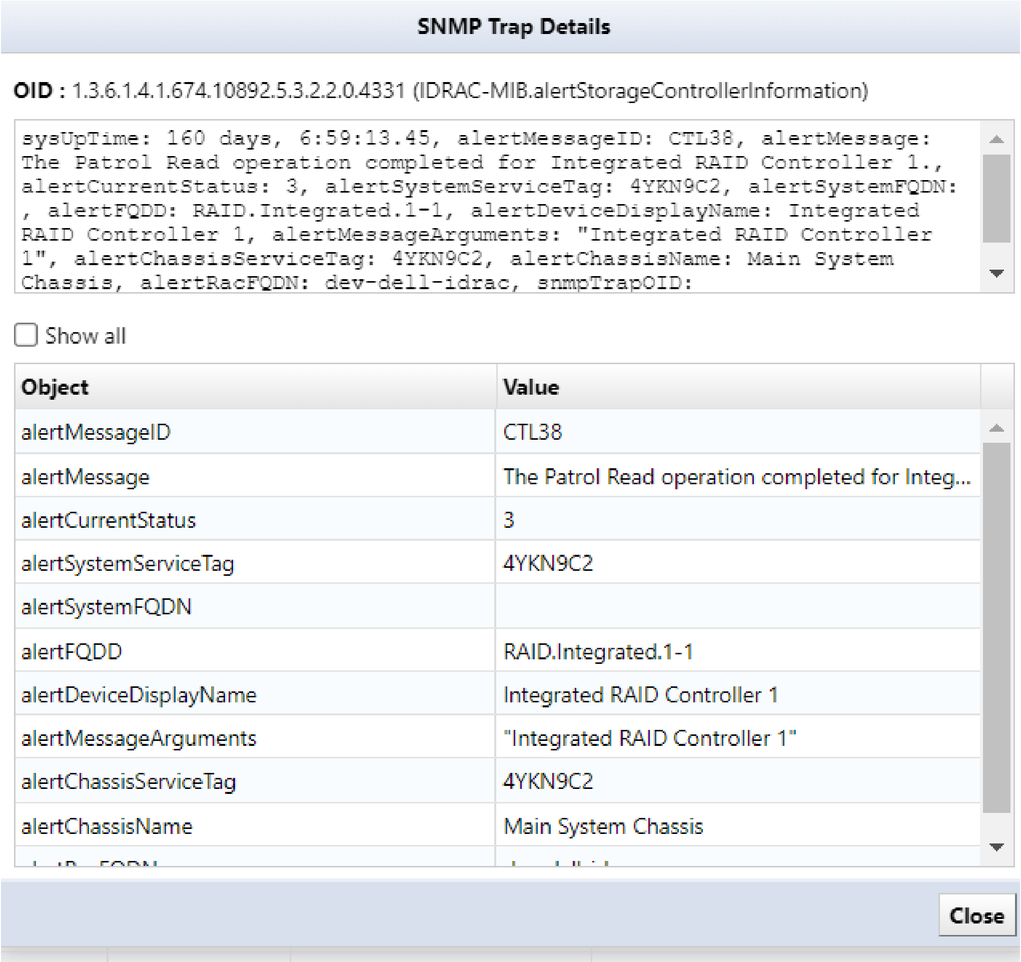
15.8 Check SNMP Traps From Registered Devices

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.



Timestamp	IP Address	Hostname	Network	OID	Message
24/03/09 03:27.19	192.168.20.211	proxmox2-idra...	Default	IDRAC-MIB.alertStorageCon...	sysUpTime: 160 days, 6:59:13.45, alertMessageID: CTL38, alertMessage: The Patrol Read operation completed for Integrated RAID Controller 1., alertCurrentStatus: 3, alertSystemServiceTag: 4YKN9C2, alertSystemFQDN: , alertFQDD: RAID.Integrated.1-1, alertDeviceDisplayName: Integrated RAID Co...
24/03/08 21:03.45	192.168.20.211	proxmox2-idra...	Default	IDRAC-MIB.alertStorageCon...	sysUpTime: 160 days, 0:35:40.78, alertMessageID: CTL37, alertMessage: A Patrol Read operation started for Integrated RAID Controller 1., alertCurrentStatus: 3, alertSystemServiceTag: 4YKN9C2, alertSystemFQDN: , alertFQDD: RAID.Integrated.1-1, alertDeviceDisplayName: Integrated RAID Controlle...

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.



OID : 1.3.6.1.4.1.674.10892.5.3.2.2.0.4331 (IDRAC-MIB.alertStorageControllerInformation)

```
sysUpTime: 160 days, 6:59:13.45, alertMessageID: CTL38, alertMessage:
The Patrol Read operation completed for Integrated RAID Controller 1.,
alertCurrentStatus: 3, alertSystemServiceTag: 4YKN9C2, alertSystemFQDN:
, alertFQDD: RAID.Integrated.1-1, alertDeviceDisplayName: Integrated
RAID Controller 1, alertMessageArguments: "Integrated RAID Controller
1", alertChassisServiceTag: 4YKN9C2, alertChassisName: Main System
Chassis, alertRacFQDN: dev-dell-idrac, snmpTrapOID:
```

☐ Show all

Object	Value
alertMessageID	CTL38
alertMessage	The Patrol Read operation completed for Integ...
alertCurrentStatus	3
alertSystemServiceTag	4YKN9C2
alertSystemFQDN	
alertFQDD	RAID.Integrated.1-1
alertDeviceDisplayName	Integrated RAID Controller 1
alertMessageArguments	"Integrated RAID Controller 1"
alertChassisServiceTag	4YKN9C2
alertChassisName	Main System Chassis

15.9 Check Collected SNMP Data

Data collected by SNMP monitors is stored in a database. You can export this data to graphs or Excel files.

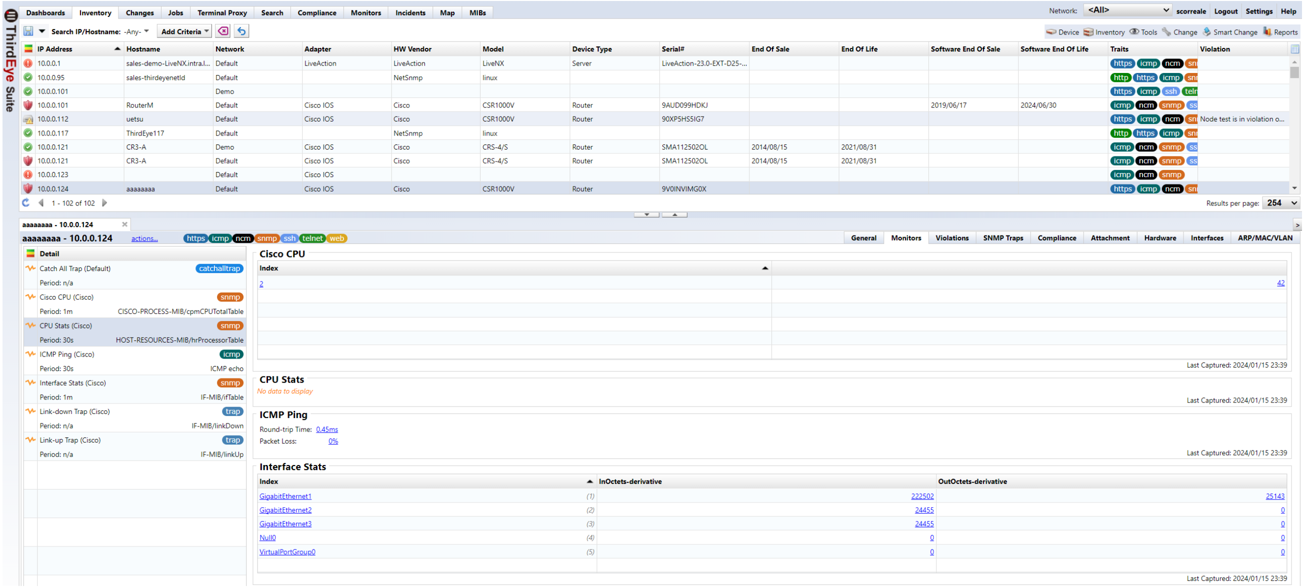
15.9.1 Add SNMP Graph Widget

Data collected by SNMP monitors can be viewed by adding a Graph Widget to your Dashboard. You can add a Graph Widget to your dashboard from the [Dashboard] main tab.

Refer to the **Add a Dashboard** section for more instructions on adding Dashboards.

To add a Dashboard:

1. Click the [Inventory] tab
2. From the list of monitored devices, doubleclick the device for which you want to set up a monitor. This opens the Editor at the bottom of the window. The Monitors information will be visible in the [Details] column in the left sidebar.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	Serial#	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life	Traits	Violation
10.0.0.1	sales-demo-LiveNX.intra.l...	Default	LiveAction	LiveAction	LiveNX	Server	LiveAction-23.0-EXT-D25-...					https icmp ncm sn	
10.0.0.95	sales-thirdeyenetld	Default		NetSnmp	linux							http https icmp sn	
10.0.0.101		Demo										https icmp ssh teln	
10.0.0.101	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	9AUD099HDKJ			2019/06/17	2024/06/30	icmp ncm snmp ss	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	90XP5HS5IG7					https icmp ncm sn	Node test is in violation o...
10.0.0.117	ThirdEye117	Default		NetSnmp	linux							http https icmp sn	
10.0.0.121	CR3-A	Demo	Cisco IOS	Cisco	CRS-4/S	Router	SMA112502OL	2014/08/15	2021/08/31			icmp ncm snmp ss	
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	SMA112502OL	2014/08/15	2021/08/31			icmp ncm snmp ss	
10.0.0.123		Default	Cisco IOS									icmp ncm snmp	
10.0.0.124	aaaaaaaa	Default	Cisco IOS	Cisco	CSR1000V	Router	9V0INVIMG0X					https icmp ncm sn	

Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
Cisco CPU (Cisco)	snmp
Period: 1m	CISCO-PROCESS-MIB/cpmCPUTotalTable
CPU Stats (Cisco)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping (Cisco)	icmp
Period: 30s	ICMP echo
Interface Stats (Cisco)	snmp
Period: 1m	IF-MIB/ifTable
Link-down Trap (Cisco)	trap
Period: n/a	IF-MIB/linkDown
Link-up Trap (Cisco)	trap
Period: n/a	IF-MIB/linkUp

Cisco CPU

Index	
2	42

Last Captured: 2024/01/15 23:39

CPU Stats

No data to display

Last Captured: 2024/01/15 23:39

ICMP Ping

Round-trip Time: 0.45ms

Packet Loss: 0%

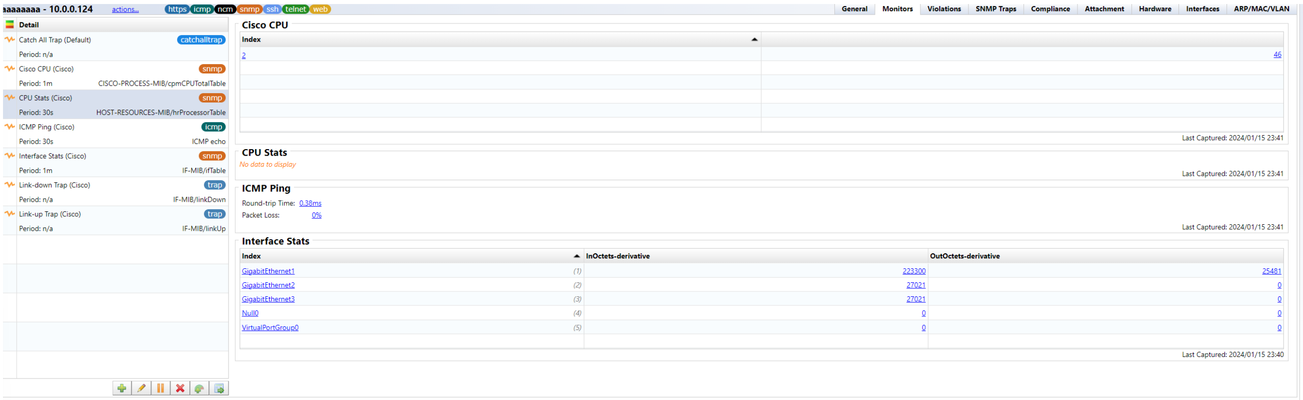
Last Captured: 2024/01/15 23:39

Interface Stats

Index		InOctets-derivative	OutOctets-derivative
GigabitEthernet1	(1)	222502	25143
GigabitEthernet2	(2)	24455	0
GigabitEthernet3	(3)	24455	0
Null0	(4)	0	0
VirtualPortGroup0	(5)	0	0

Last Captured: 2024/01/15 23:39

3. In the left sidebar, select the monitor whose data you want to check, and click [Add to Dashboard].



Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
Cisco CPU (Cisco)	snmp
Period: 1m	CISCO-PROCESS-MIB/cpmCPUTotalTable
CPU Stats (Cisco)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping (Cisco)	icmp
Period: 30s	ICMP echo
Interface Stats (Cisco)	snmp
Period: 1m	IF-MIB/ifTable
Link-down Trap (Cisco)	trap
Period: n/a	IF-MIB/linkDown
Link-up Trap (Cisco)	trap
Period: n/a	IF-MIB/linkUp

Cisco CPU

Index	
2	46

Last Captured: 2024/01/15 23:41

CPU Stats

No data to display

Last Captured: 2024/01/15 23:41

ICMP Ping

Round-trip Time: 0.38ms

Packet Loss: 0%

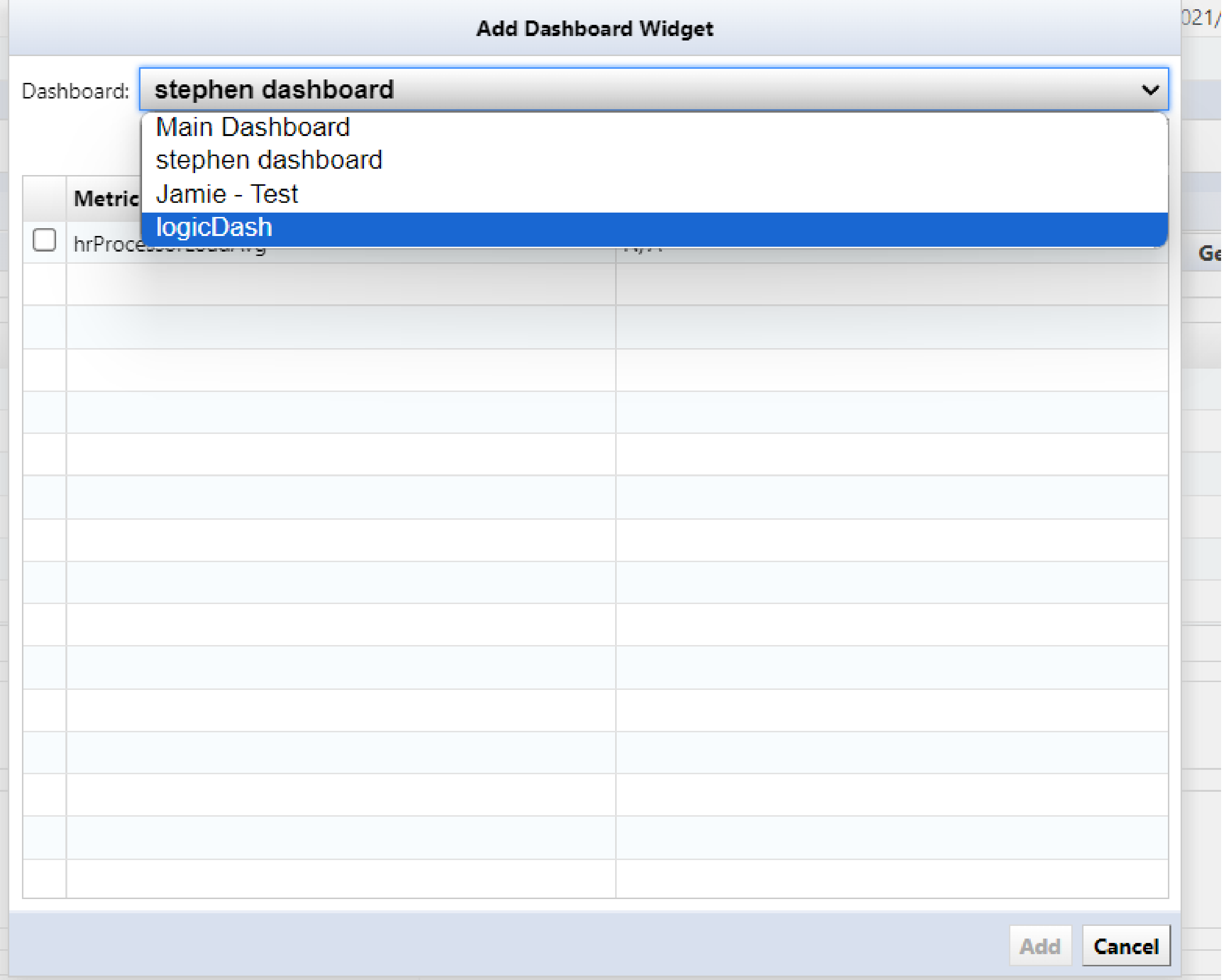
Last Captured: 2024/01/15 23:41

Interface Stats

Index		InOctets-derivative	OutOctets-derivative
GigabitEthernet1	(1)	223300	25481
GigabitEthernet2	(2)	27021	0
GigabitEthernet3	(3)	27021	0
Null0	(4)	0	0
VirtualPortGroup0	(5)	0	0

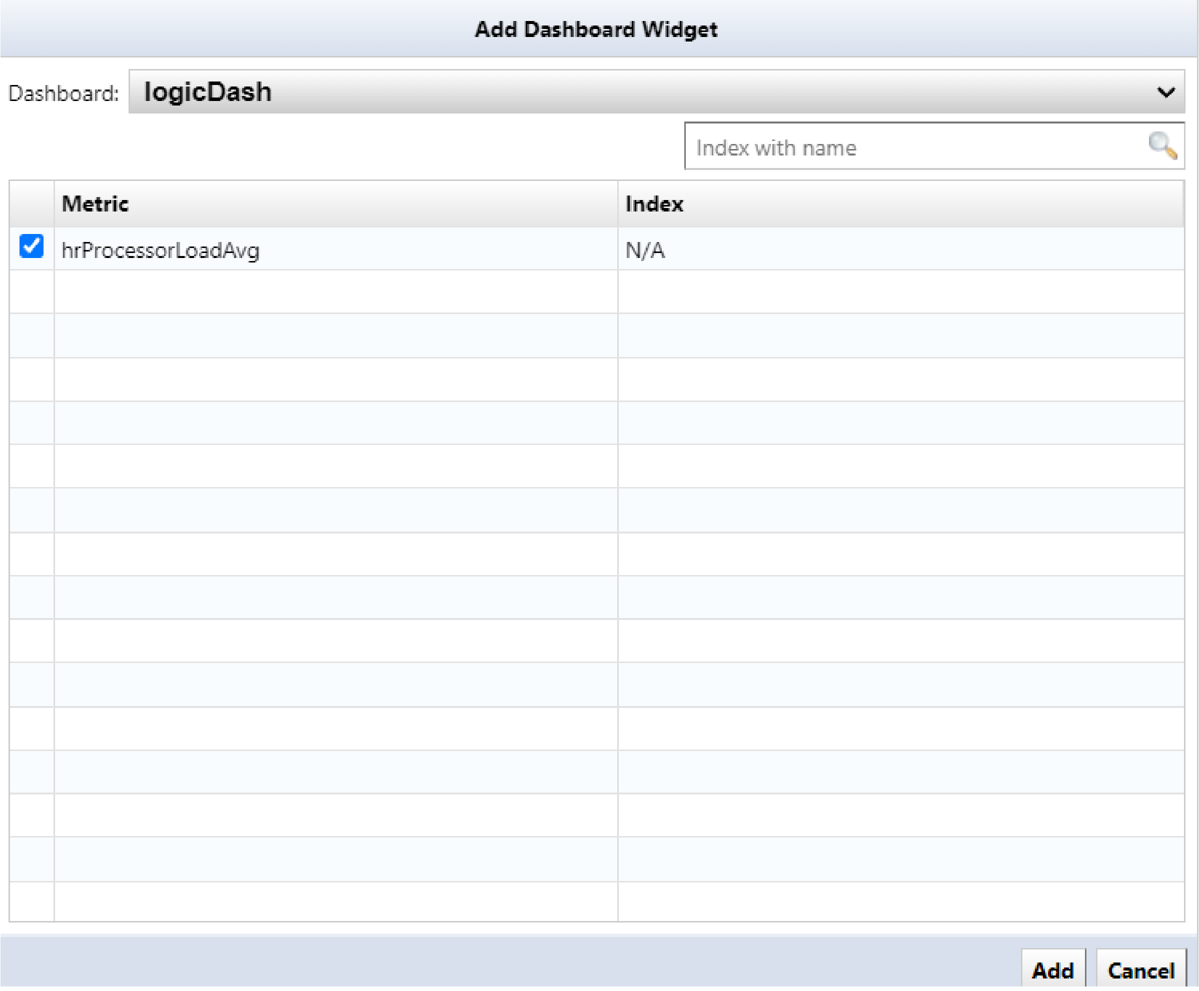
Last Captured: 2024/01/15 23:40

4. In the [Add Dashboard Widget] window, select the Dashboard you want to add the widget to.



5. Select the metrics you want to add to the graph and click [Add].

Depending on the data to be obtained, “Index” may not be displayed, and only “Metric” may be visible.



Add Dashboard Widget

Dashboard: logicDash

Index with name

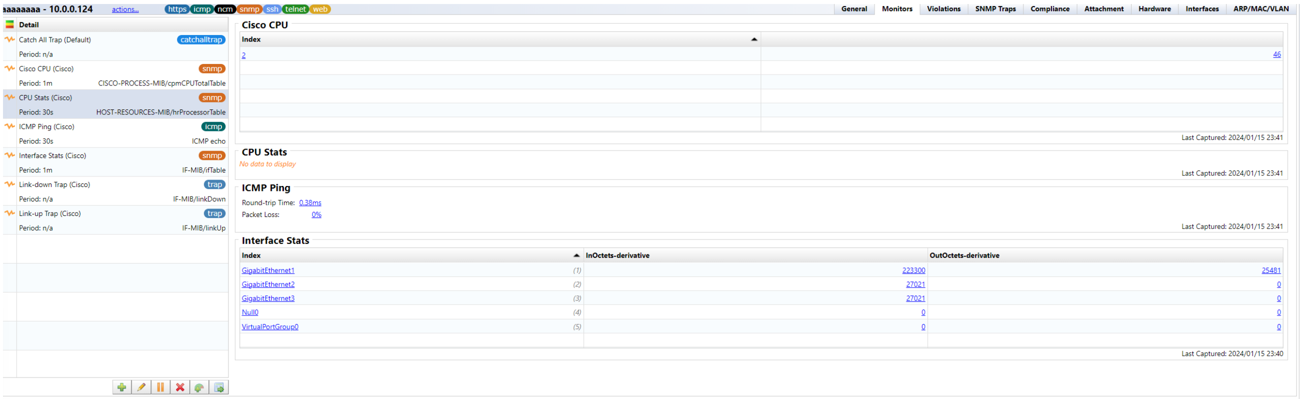
	Metric	Index
☑	hrProcessorLoadAvg	N/A

15.9.2 Export SNMP Data to CSV File

Data collected with SNMP can be exported to a CSV file.

1. From the list of monitored devices on the [Inventory] tab, doubleclick the device for which you want to set up a monitor. This opens the Editor at the bottom of the window. The Monitors information will be visible in the [Details] column in the left sidebar.

2. From the monitor's [Details] in the left sidebar, select the monitor whose data you want to check, and click [Export].



Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
Cisco CPU (Cisco)	snmp
Period: 1m	CISCO-PROCESS-MIB/cpmCPUTotalTable
CPU Stats (Cisco)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping (Cisco)	icmp
Period: 30s	ICMP echo
Interface Stats (Cisco)	snmp
Period: 1m	IF-MIB/ifTable
Link-down Trap (Cisco)	trap
Period: n/a	IF-MIB/linkDown
Link-up Trap (Cisco)	trap
Period: n/a	IF-MIB/linkUp

Cisco CPU

Index	
2	46

Last Captured: 2024/01/15 23:41

CPU Stats

No data to display

Last Captured: 2024/01/15 23:41

ICMP Ping

Round-trip Time: 0.38ms
Packet Loss: 0%

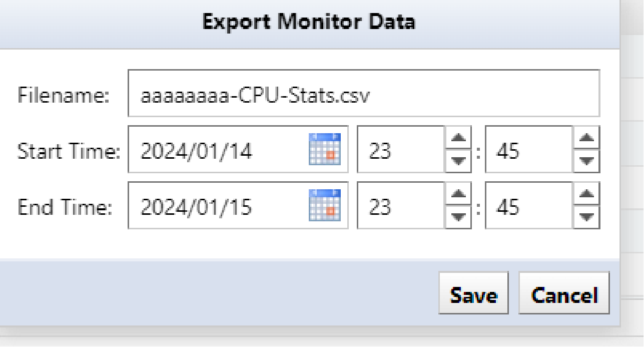
Last Captured: 2024/01/15 23:41

Interface Stats

Index		InOctets-derivative	OutOctets-derivative
GigabitEthernet1	(1)	223300	25481
GigabitEthernet2	(2)	27021	0
GigabitEthernet3	(3)	27021	0
Null0	(4)	0	0
VirtualPortGroup0	(5)	0	0

Last Captured: 2024/01/15 23:40

3. Enter the file name and data export period, and click [Save].



Filename: aaaaaaaa-CPU-Stats.csv

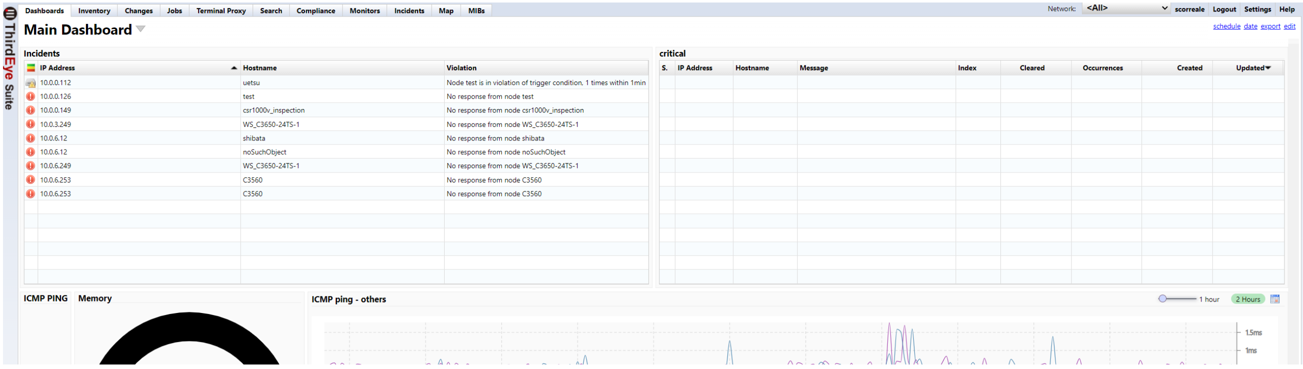
Start Time: 2024/01/14 23 : 45

End Time: 2024/01/15 23 : 45

After clicking [Save], the Excel file will be downloaded.

15.9.3 Publish PDF Dashboard Report

You can export the “inventory” and “line graph” displayed in the widget to a PDF file by clicking the [Export] button in the top right of the dashboard screen.



Incidents

	IP Address	Hostname	Violation
⚠	10.0.0.112	uetsu	Node test is in violation of trigger condition, 1 times within 1min
●	10.0.0.126	test	No response from node test
●	10.0.0.149	csr1000v_inspection	No response from node csr1000v_inspection
●	10.0.3.249	WS_C3650-24TS-1	No response from node WS_C3650-24TS-1
●	10.0.6.12	shibata	No response from node shibata
●	10.0.6.12	noSuchObject	No response from node noSuchObject
●	10.0.6.249	WS_C3650-24TS-1	No response from node WS_C3650-24TS-1
●	10.0.6.253	C3560	No response from node C3560
●	10.0.6.253	C3560	No response from node C3560

critical

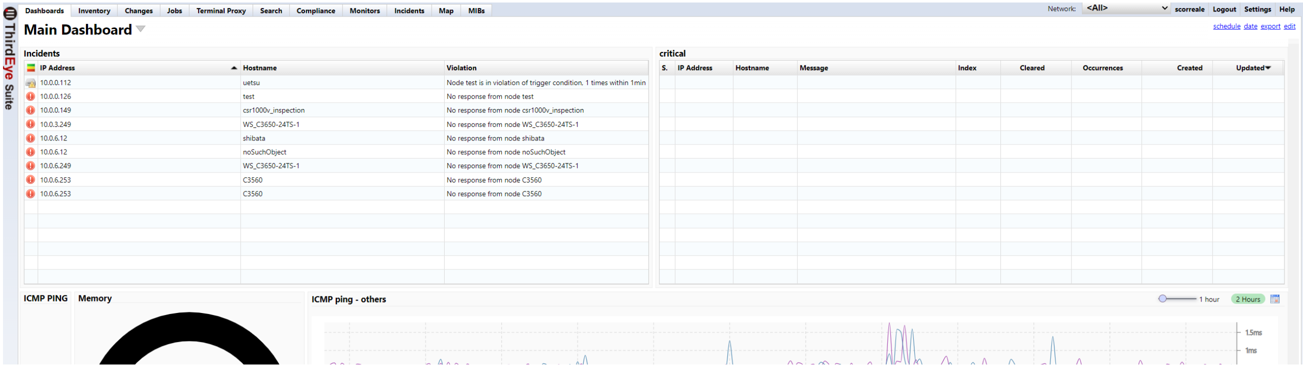
S.	IP Address	Hostname	Message	Index	Cleared	Occurrences	Created	Updated

15.9.4 Schedule Email Dashboard Reports

Dashboard reports can be emailed periodically.

To send email, you must first set up a mail server.

1. Click [Schedule].



Incidents

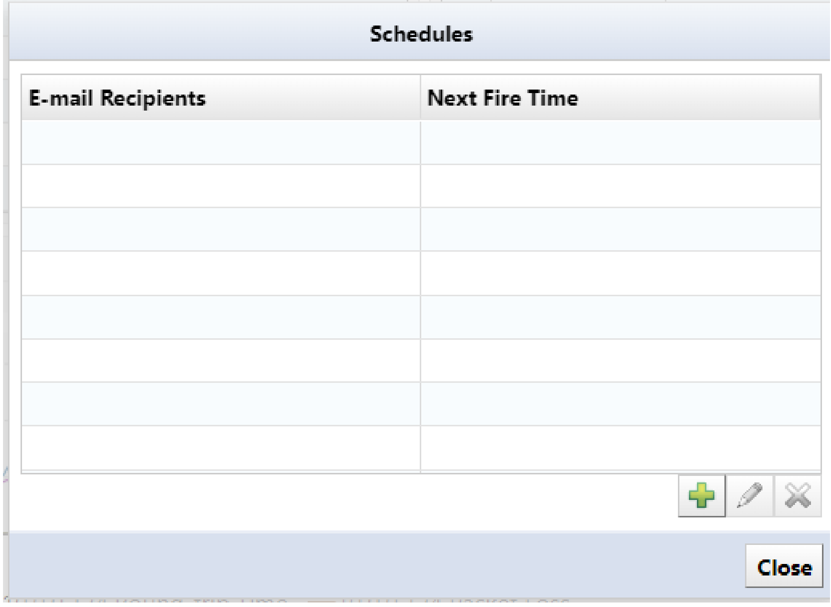
	IP Address	Hostname	Violation
⚠	10.0.0.112	uetsu	Node test is in violation of trigger condition, 1 times within 1min
●	10.0.0.126	test	No response from node test
●	10.0.0.149	csr1000v_inspection	No response from node csr1000v_inspection
●	10.0.3.249	WS_C3650-24TS-1	No response from node WS_C3650-24TS-1
●	10.0.6.12	shibata	No response from node shibata
●	10.0.6.12	noSuchObject	No response from node noSuchObject
●	10.0.6.249	WS_C3650-24TS-1	No response from node WS_C3650-24TS-1
●	10.0.6.253	C3560	No response from node C3560
●	10.0.6.253	C3560	No response from node C3560

critical

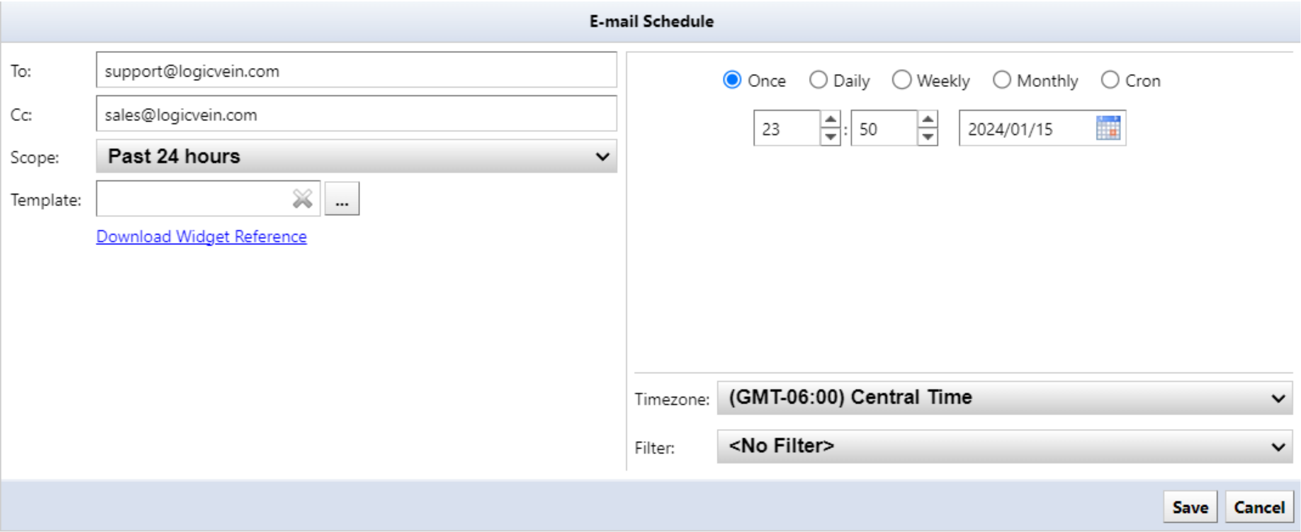
S.	IP Address	Hostname	Message	Index	Cleared	Occurrences	Created	Updated

This opens the [Schedules] window.

2. Click the ➕ button to open the email [Schedules] window.



3. Configure each item.



E-mail Schedule

To: support@logicvein.com

Cc: sales@logicvein.com

Scope: Past 24 hours

Template:

● Once ○ Daily ○ Weekly ○ Monthly ○ Cron

23 : 50 2024/01/15

Timezone: (GMT-06:00) Central Time

Filter: <No Filter>

Menu item	Explanation
To/Cc	Enter the email address.
Scope	Specify the report display period range from the dropdown menu: within 24 hours within a week within 30 days yesterday (00:00:00-23:59:59) last week (Monday to Sunday) last month (beginning of month to end of month) date range (user specifies any period)
Template	Dashboard graphs can be pasted into a Word file and sent as a report.
Schedule	Specify the schedule for publishing the report.
Timezone	Specify the time zone in which to publish the report.
Filter	Specifies execution time filter settings. Filter settings are made in [Job Management].
Save	Save your settings.
Cancel	Discards the settings and returns to the previous screen.

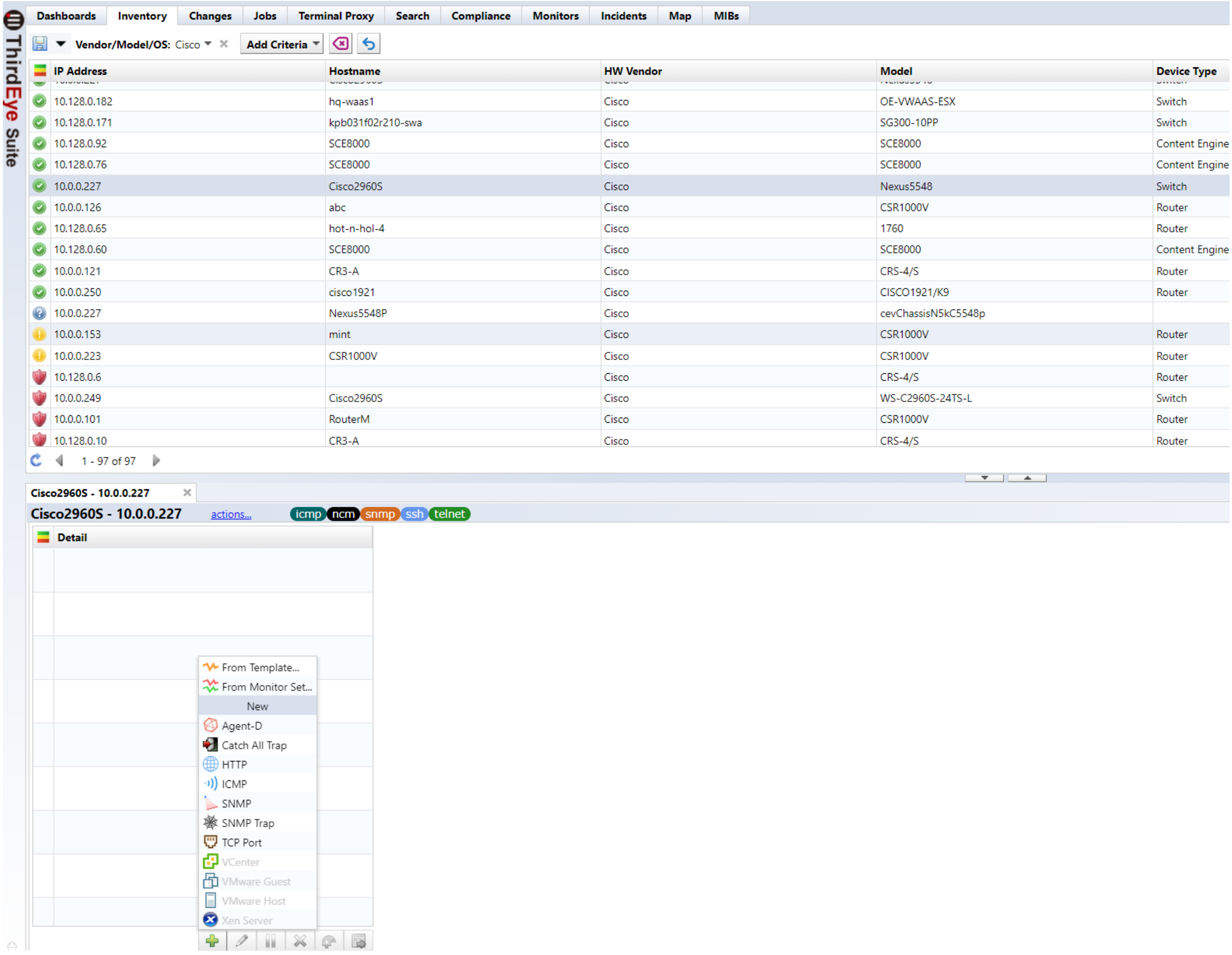
4. Click [Save].

15.10 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:

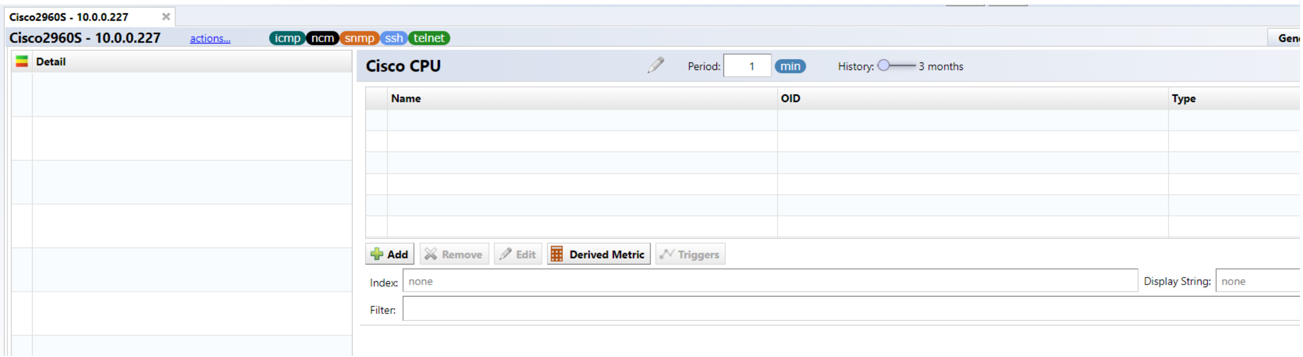
1. From the list of monitored devices on the [Inventory] tab, doubleclick the device for which you want to set up a monitor.
2. Click the ➕ button in the bottom left of the window, and then click [SNMP] in the pop up menu.



IP Address	Hostname	HW Vendor	Model	Device Type
10.128.0.182	hq-waas1	Cisco	OE-VWAAS-ESX	Switch
10.128.0.171	kpb031f02r210-swa	Cisco	SG300-10PP	Switch
10.128.0.92	SCE8000	Cisco	SCE8000	Content Engine
10.128.0.76	SCE8000	Cisco	SCE8000	Content Engine
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch
10.0.0.126	abc	Cisco	CSR1000V	Router
10.128.0.65	hot-n-hol-4	Cisco	1760	Router
10.128.0.60	SCE8000	Cisco	SCE8000	Content Engine
10.0.0.121	CR3-A	Cisco	CRS-4/S	Router
10.0.0.250	cisco1921	Cisco	CISCO1921/K9	Router
10.0.0.227	Nexus5548P	Cisco	cevChassisN5kC5548p	
10.0.0.153	mint	Cisco	CSR1000V	Router
10.0.0.223	CSR1000V	Cisco	CSR1000V	Router
10.128.0.6		Cisco	CRS-4/S	Router
10.0.0.249	Cisco2960S	Cisco	WS-C2960S-24TS-L	Switch
10.0.0.101	RouterM	Cisco	CSR1000V	Router
10.128.0.10	CR3-A	Cisco	CRS-4/S	Router

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.



Period: 1 min

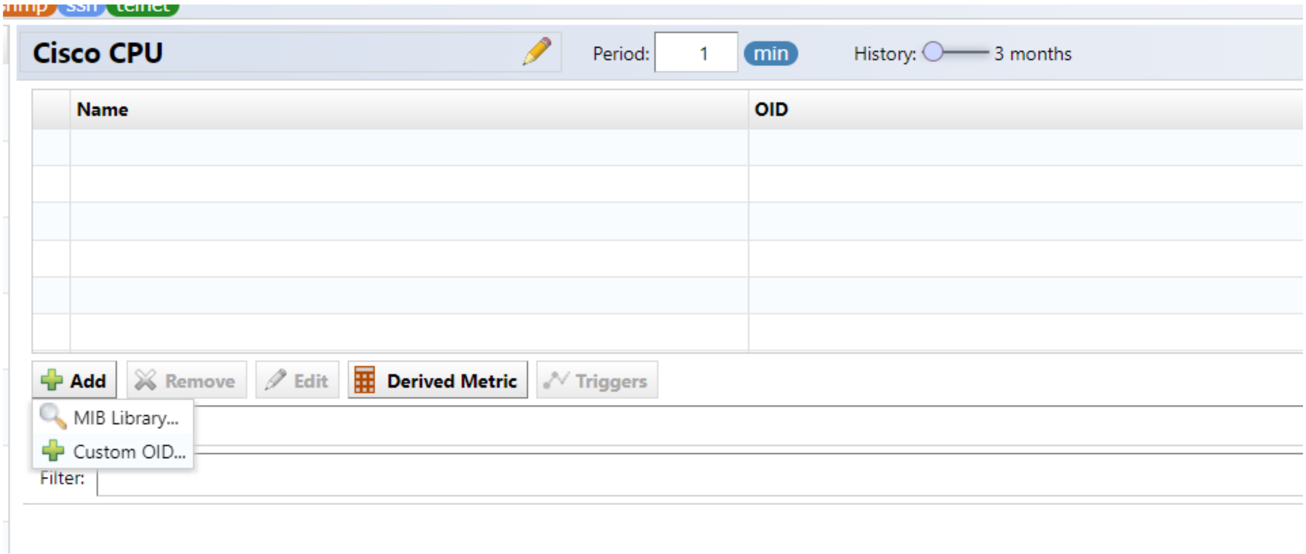
History: 3 months

Index: none

Display String: none

Filter:

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

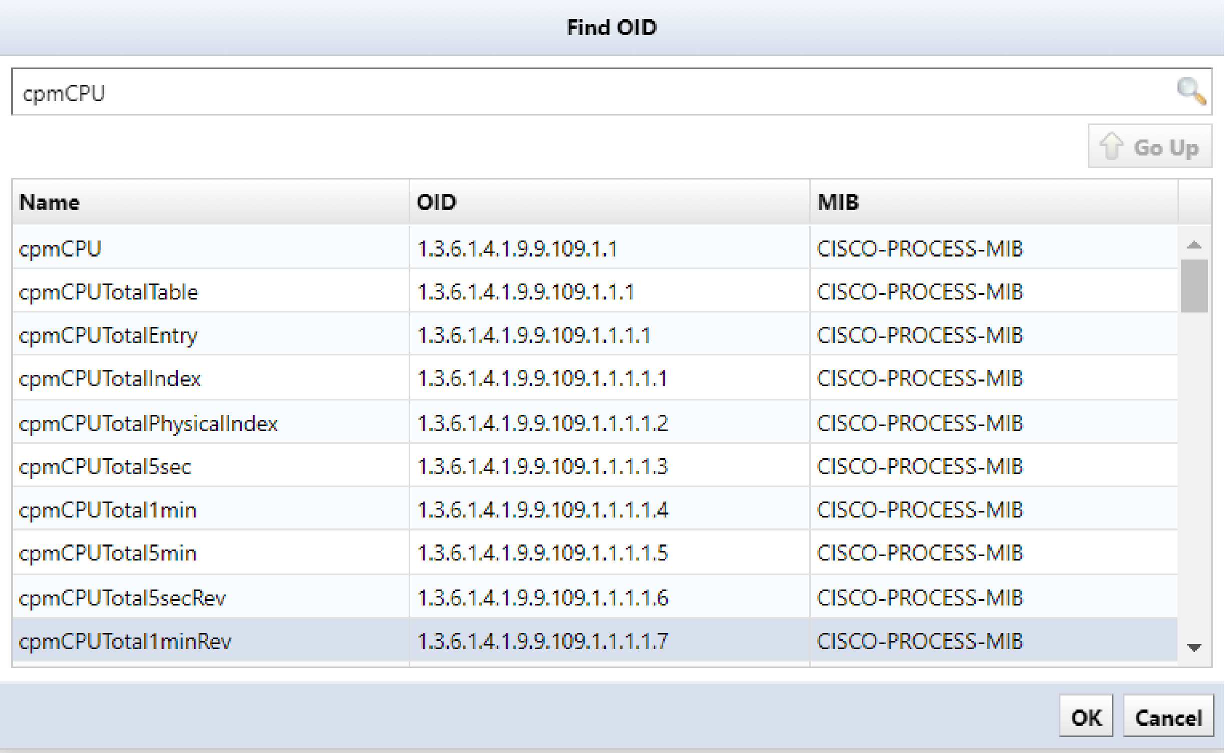


Period: 1 min

History: 3 months

Filter:

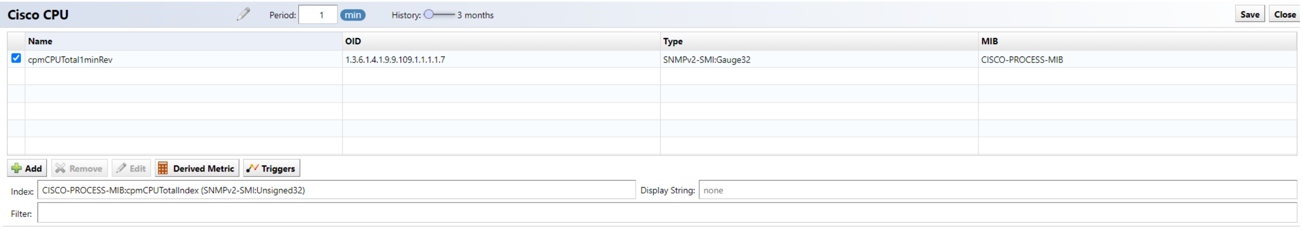
7. In the “Find OID” window, enter the MIB OID or name (“cpmCPU” in the example below) in the OID search field, select the MIB you want to add, and click [OK].



cpmCPU

Name	OID	MIB
cpmCPU	1.3.6.1.4.1.9.9.109.1.1	CISCO-PROCESS-MIB
cpmCPUTotalTable	1.3.6.1.4.1.9.9.109.1.1.1	CISCO-PROCESS-MIB
cpmCPUTotalEntry	1.3.6.1.4.1.9.9.109.1.1.1.1	CISCO-PROCESS-MIB
cpmCPUTotalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.1	CISCO-PROCESS-MIB
cpmCPUTotalPhysicalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.2	CISCO-PROCESS-MIB
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6	CISCO-PROCESS-MIB
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	CISCO-PROCESS-MIB

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



Cisco CPU

Period: 1 min

History: 3 months

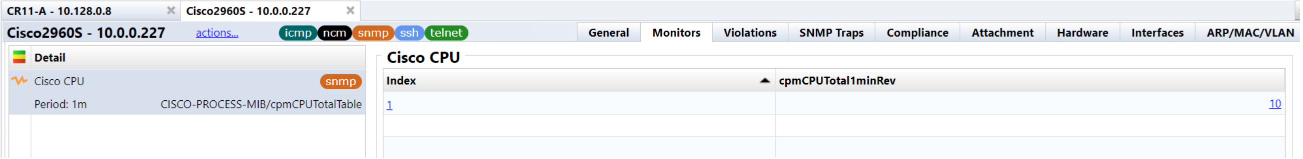
	Name	OID	Type	MIB
☑	cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Index: CISCO-PROCESS-MIB:cpmCPUTotalIndex (SNMPv2-SMI:Unsigned32)

Display String: none

Filter:

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



Period: 1m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU

Index	cpmCPUTotal1minRev
1	10

15.11 Monitor SNMP Traps

ThirdEye can receive SNMP traps and execute actions based on the received SNMP Traps. Depending on the SNMP version that you wish to use, you may need to configure credentials in advance.

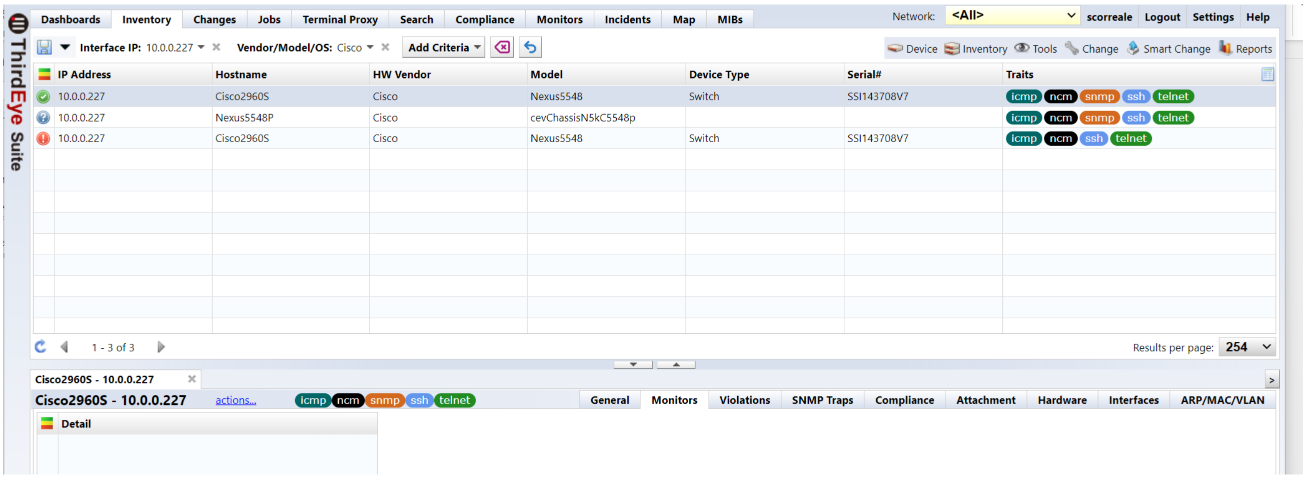
15.11.1 Set up credentials

Refer to **Configure SNMP Trap Handling** for instructions.

15.11.2 Monitor by OID

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, which is described in the next section.

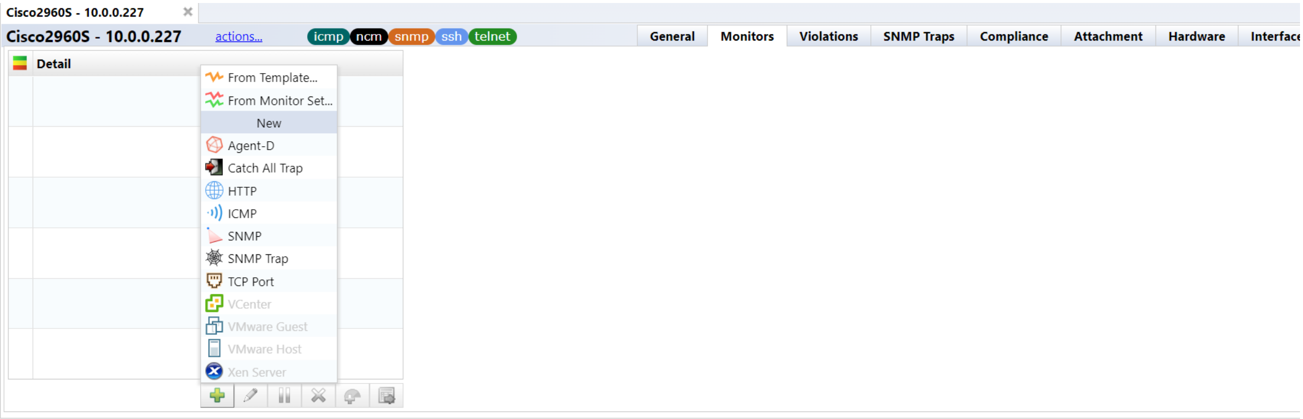
1. From the list of monitored devices on the [Inventory] tab, doubleclick the device for which you want to set up a monitor.



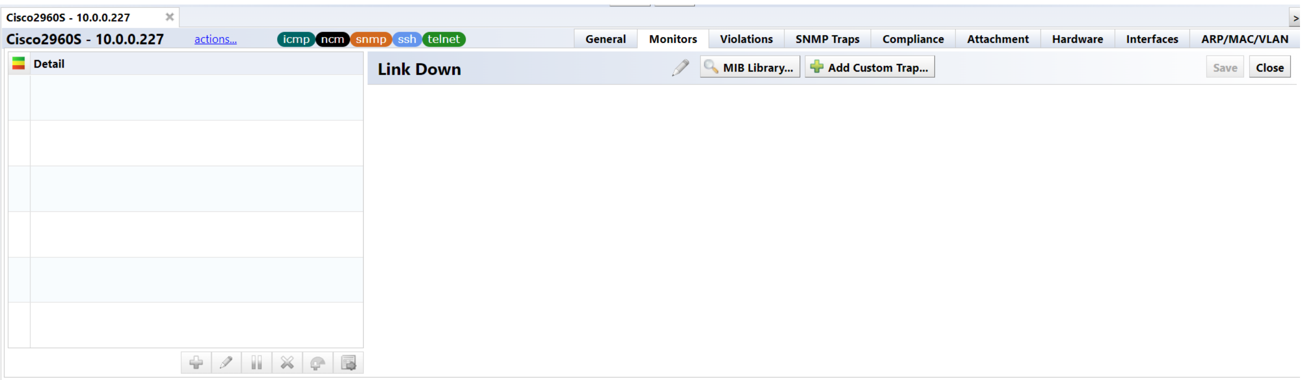
Interface IP: 10.0.0.227 Vendor/Model/OS: Cisco

IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7	icmp ncm snmp ssh telnet
10.0.0.227	Nexus5548P	Cisco	cevChassisN5kC5548p			icmp ncm snmp ssh telnet
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7	icmp ncm ssh telnet

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

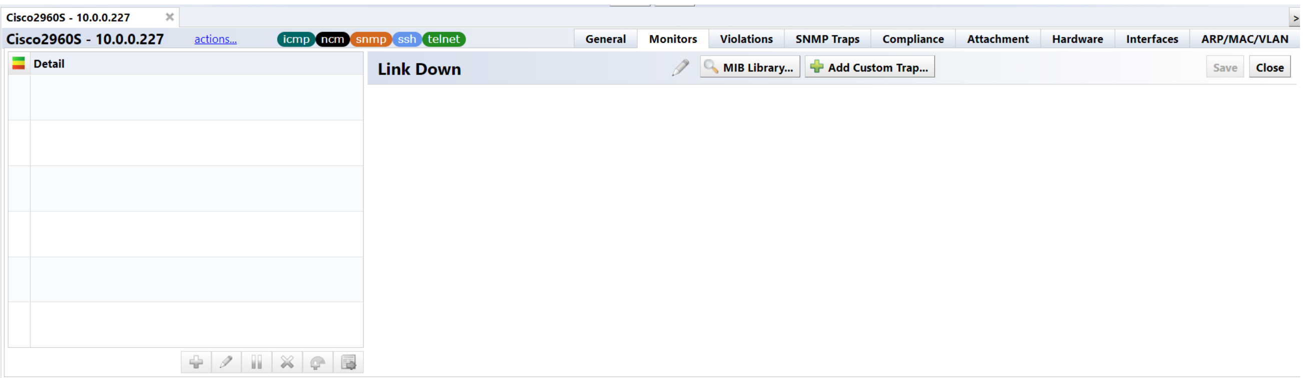


3. Enter any monitor name (“Link Down” in the example below).

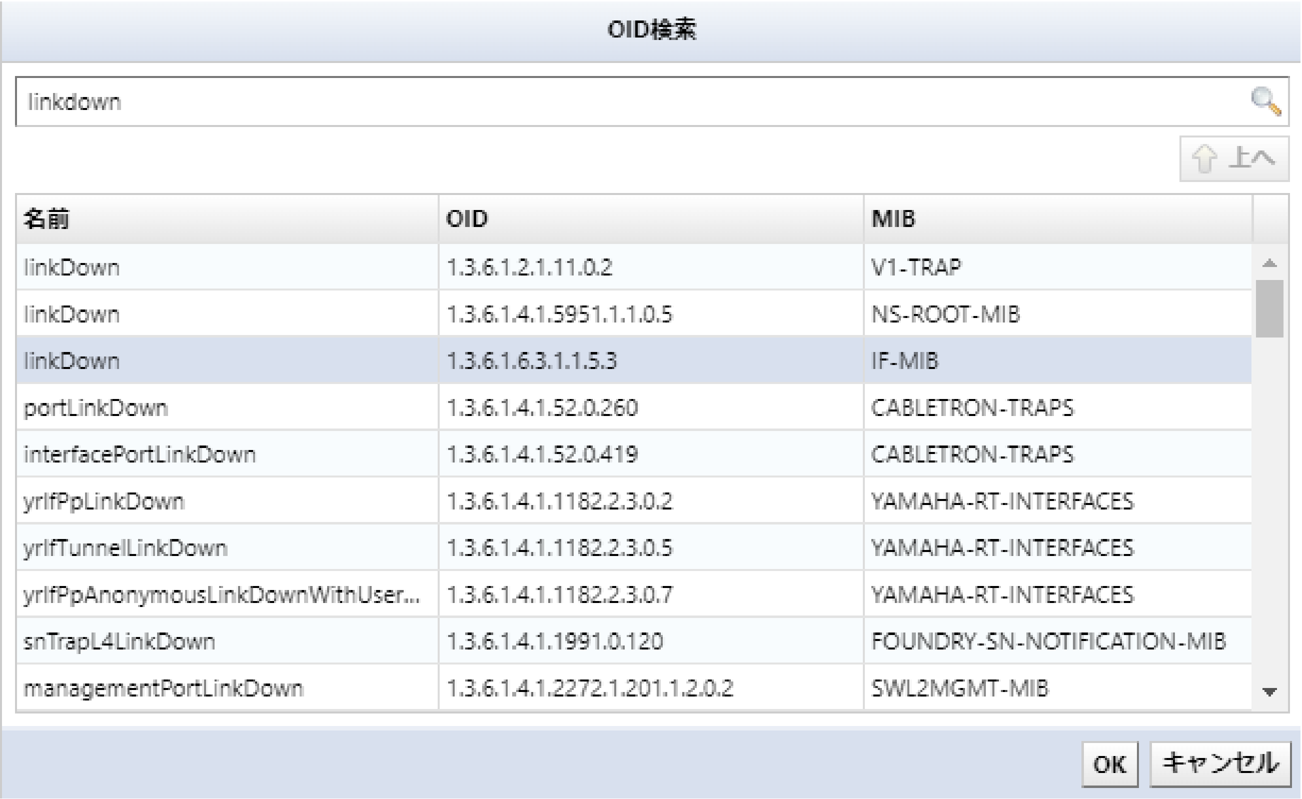


Link Down

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].

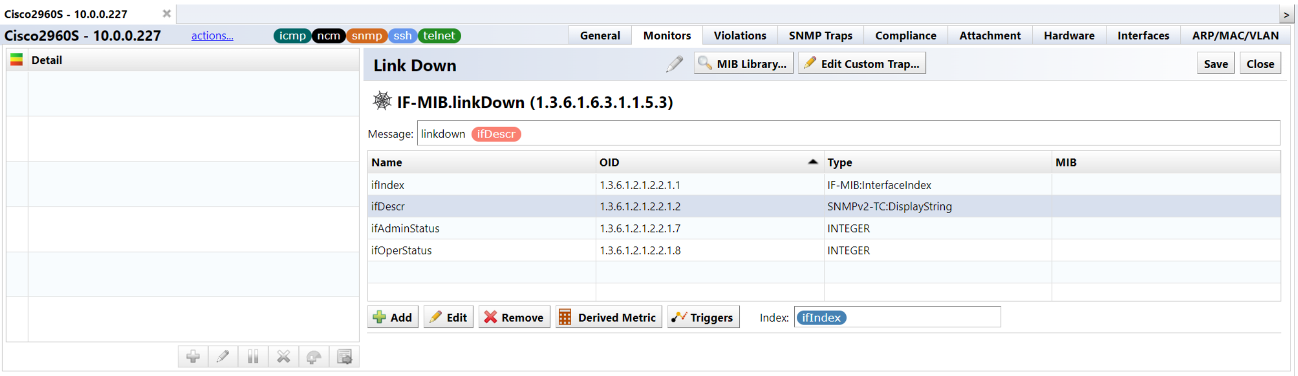


OID検索

linkdown

名前	OID	MIB
linkDown	1.3.6.1.2.1.11.0.2	V1-TRAP
linkDown	1.3.6.1.4.1.5951.1.1.0.5	NS-ROOT-MIB
linkDown	1.3.6.1.6.3.1.1.5.3	IF-MIB
portLinkDown	1.3.6.1.4.1.52.0.260	CABLETRON-TRAPS
interfacePortLinkDown	1.3.6.1.4.1.52.0.419	CABLETRON-TRAPS
yrIfPpLinkDown	1.3.6.1.4.1.1182.2.3.0.2	YAMAHA-RT-INTERFACES
yrIfTunnelLinkDown	1.3.6.1.4.1.1182.2.3.0.5	YAMAHA-RT-INTERFACES
yrIfPpAnonymousLinkDownWithUser...	1.3.6.1.4.1.1182.2.3.0.7	YAMAHA-RT-INTERFACES
snTrapL4LinkDown	1.3.6.1.4.1.1991.0.120	FOUNDRY-SN-NOTIFICATION-MIB
managementPortLinkDown	1.3.6.1.4.1.2272.1.201.1.2.0.2	SWL2MGMT-MIB

6. Enter a message for when a failure occurs.



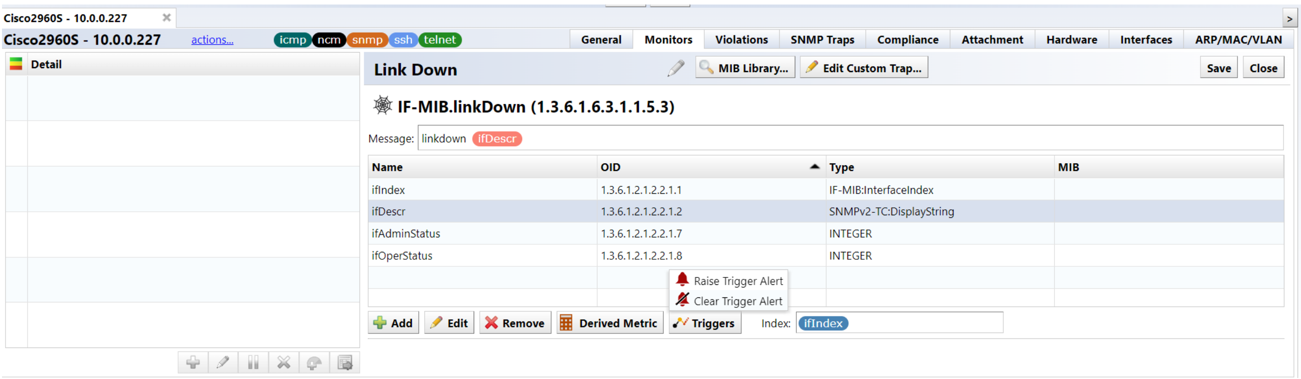
IF-MIB.linkDown (1.3.6.1.6.3.1.1.5.3)

Message: linkdown ifDescr

Name	OID	Type	MIB
ifIndex	1.3.6.1.2.1.2.2.1.1	IF-MIB:InterfaceIndex	
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString	
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	

Index: ifIndex

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



IF-MIB.linkDown (1.3.6.1.6.3.1.1.5.3)

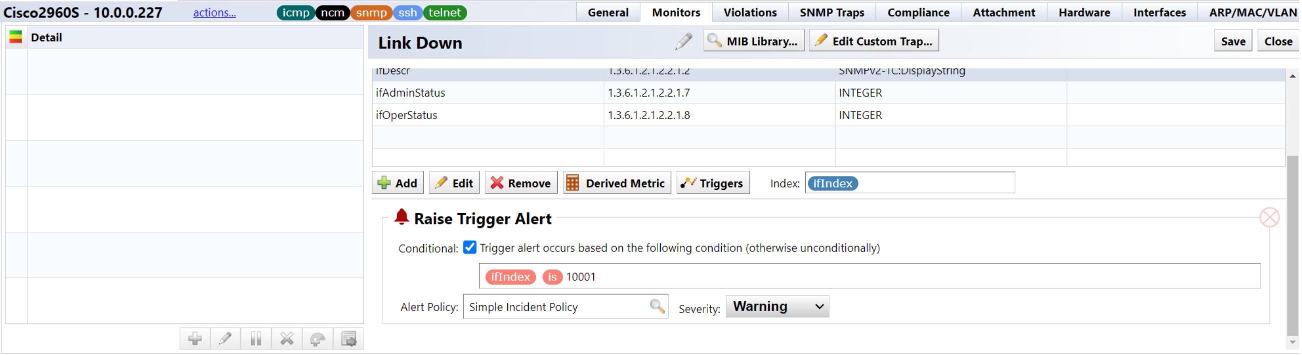
Message: linkdown ifDescr

Name	OID	Type	MIB
ifIndex	1.3.6.1.2.1.2.2.1.1	IF-MIB:InterfaceIndex	
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString	
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	

Index: ifIndex

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

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



ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER

Index: ifIndex

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

ifIndex is 10001

Alert Policy: Simple Incident Policy

Severity: Warning

Alert Setting	Explanation

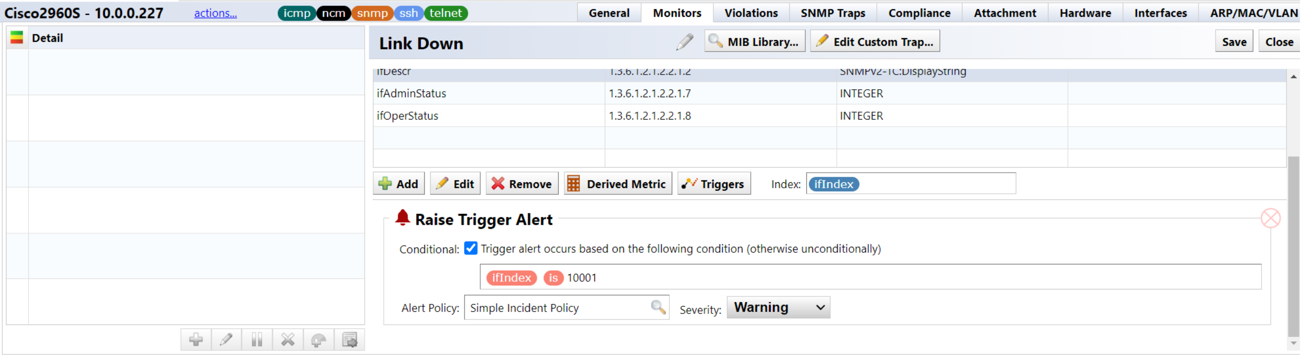
Conditional	If you check [Trigger alert occurs based on the following condition (otherwise unconditionally)], you can specify the conditions using the following items.
	`is` (equal)
	`is not` (not equal)
	`>` (less than, the value on the right is smaller)
	`<` (greater than, the value on the right is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



ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER

Index: ifIndex

Raise Trigger Alert

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

ifIndex is 10001

Alert Policy: Simple Incident Policy

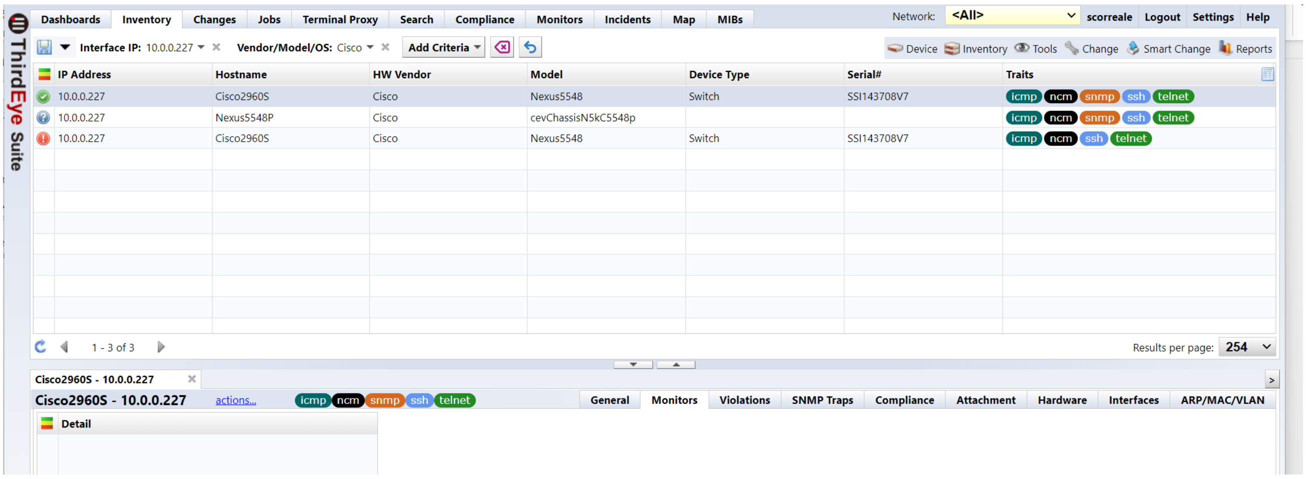
Severity: Warning

15.11.3 Monitor any OID

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.

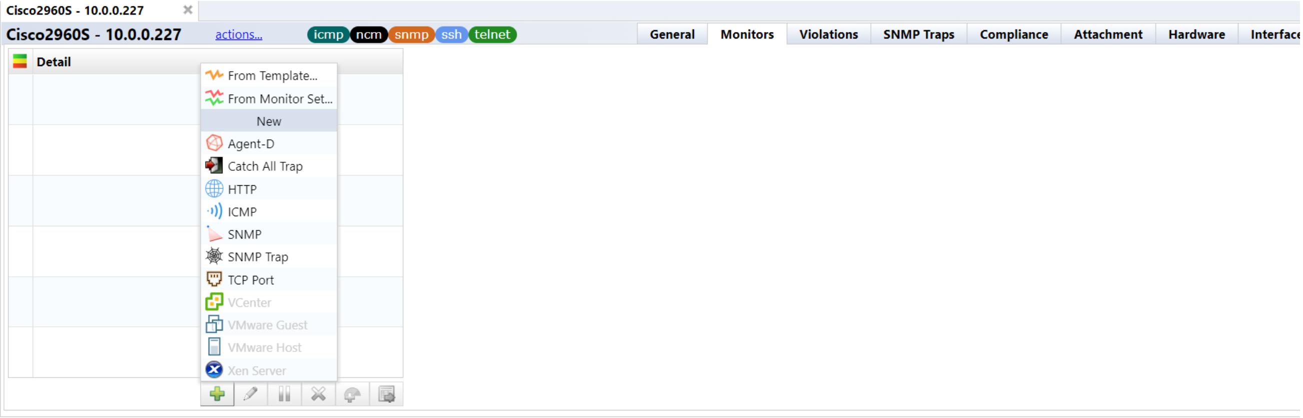
> **Note**
>
> The “SNMP Trap (All)” and “SNMP Trap (Optional)” settings can be used together. If used together, the “SNMP Trap (optional)” setting takes precedence.

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

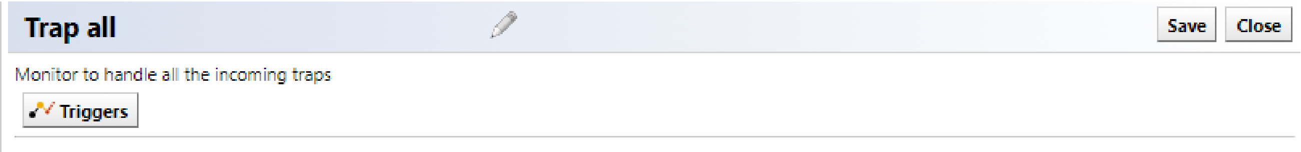


IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7	icmp ncm snmp ssh telnet
10.0.0.227	Nexus5548P	Cisco	cevChassisN5kC5548p			icmp ncm snmp ssh telnet
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7	icmp ncm ssh telnet

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



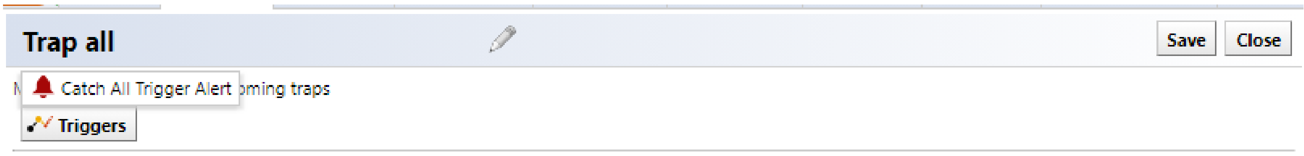
3. Enter any monitor name.



Trap all

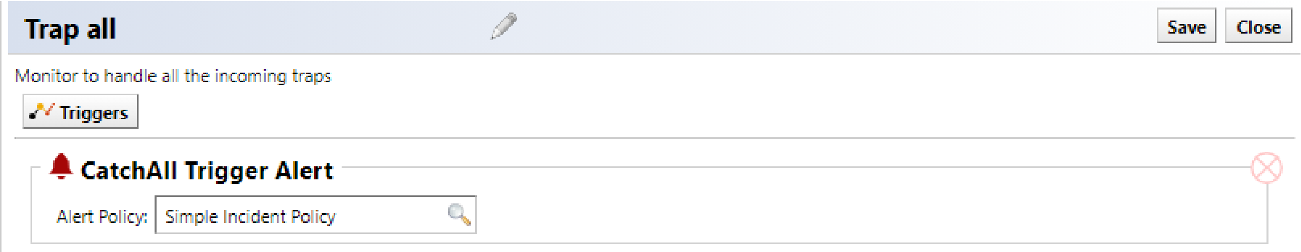
Monitor to handle all the incoming traps

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



Trap all

5. Specify the alert policy.



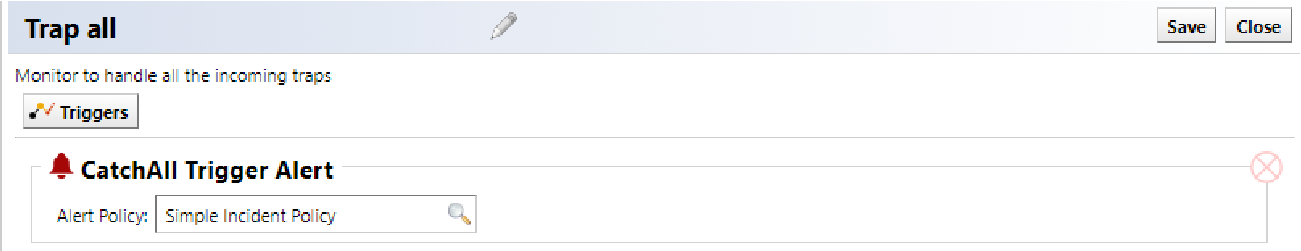
Trap all

Monitor to handle all the incoming traps

CatchAll Trigger Alert

Alert Policy: Simple Incident Policy

6. Click [Save].



Trap all

Monitor to handle all the incoming traps

CatchAll Trigger Alert

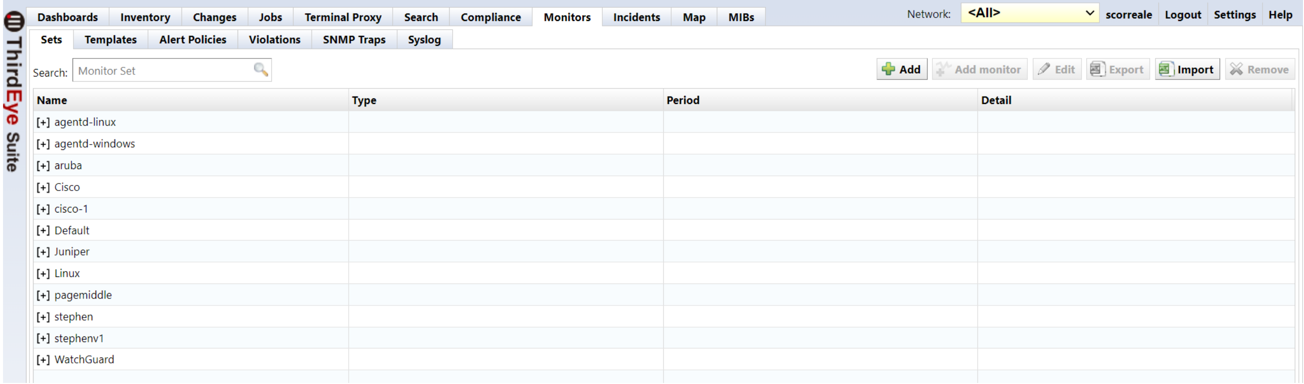
Alert Policy: Simple Incident Policy

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

15.12 Monitor Multiple Devices (Monitor Sets)

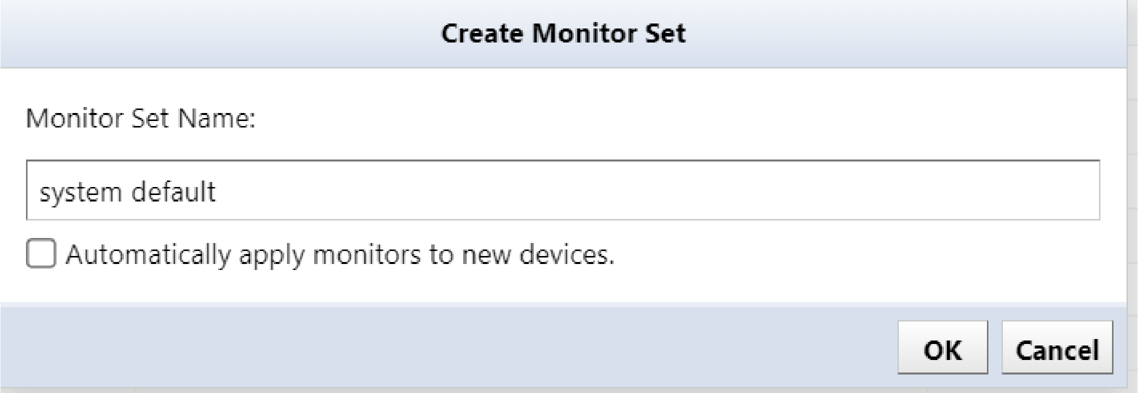
ThirdEye’s monitor settings include a function called “Monitor Set” that combines multiple monitors into one. Monitor Sets allow you to apply configured monitors to many devices at once.

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



Name	Type	Period	Detail
[+] agentd-linux			
[+] agentd-windows			
[+] aruba			
[+] Cisco			
[+] cisco-1			
[+] Default			
[+] Juniper			
[+] Linux			
[+] pagemiddle			
[+] stephen			
[+] stephenv1			
[+] WatchGuard			

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

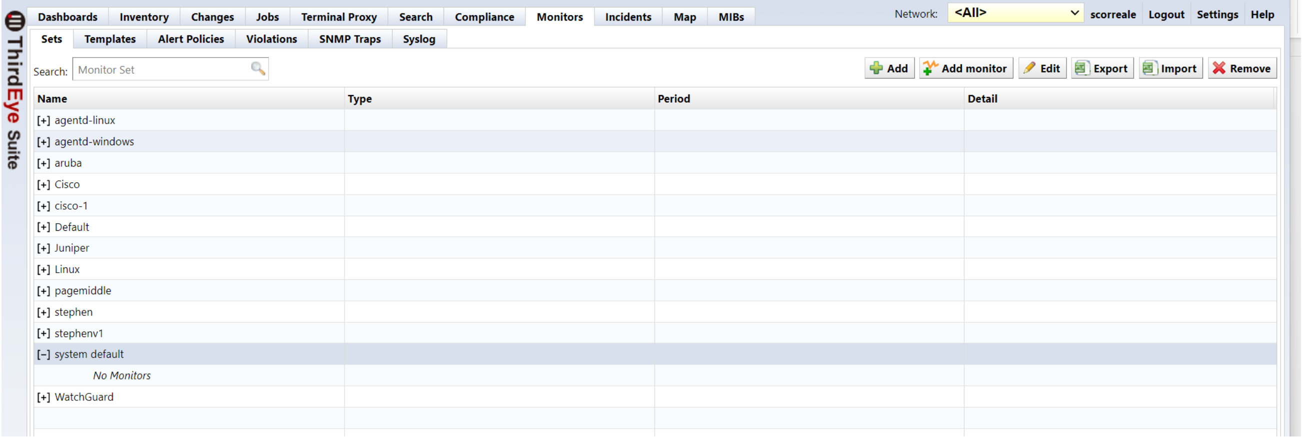


Monitor Set Name: system default

□ Automatically apply monitors to new devices.

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.

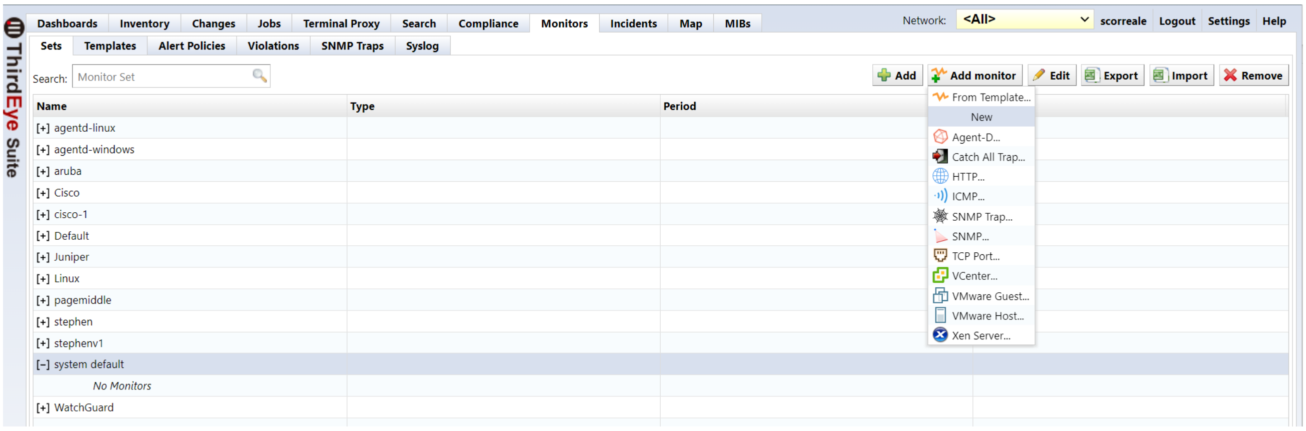
3. Select the monitor set you created.



Name	Type	Period	Detail
[+] agentd-linux			
[+] agentd-windows			
[+] aruba			
[+] Cisco			
[+] cisco-1			
[+] Default			
[+] Juniper			
[+] Linux			
[+] pagemiddle			
[+] stephen			
[+] stephenv1			
[−] system default			
No Monitors			
[+] WatchGuard			

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.

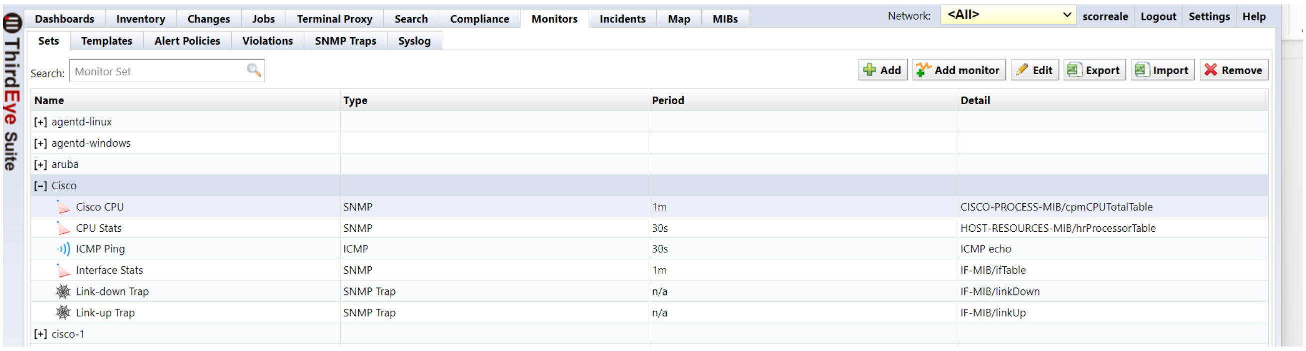


Name	Type	Period
[+] agentd-linux		
[+] agentd-windows		
[+] aruba		
[+] Cisco		
[+] cisco-1		
[+] Default		
[+] Juniper		
[+] Linux		
[+] pagemiddle		
[+] stephen		
[+] stephenv1		
[–] system default		
No Monitors		
[+] WatchGuard		

[Add Monitor] dropdown menu options:

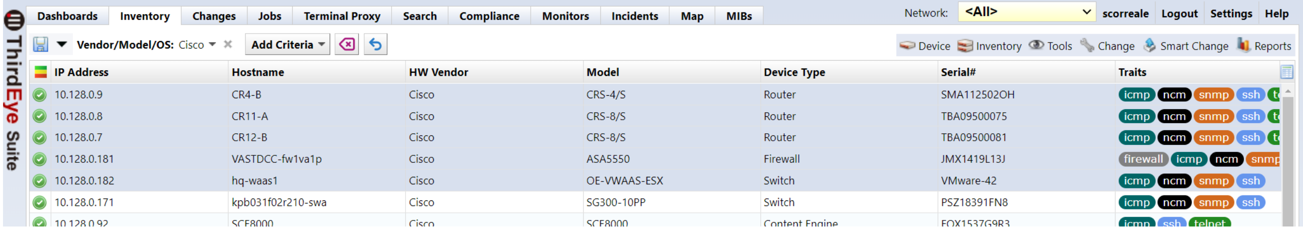
Menu option	Explanation
Add from template	Add a monitor from the created monitor templates to Template.
Agent-D	Add a monitor for Agent-D.
HTTP	Add a monitor for http or https.
ICMP	Add monitoring by ICMP Ping.
SNMP	Add a monitor to specify the MIB object to be monitored from the MIB table.
SNMP traps (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)



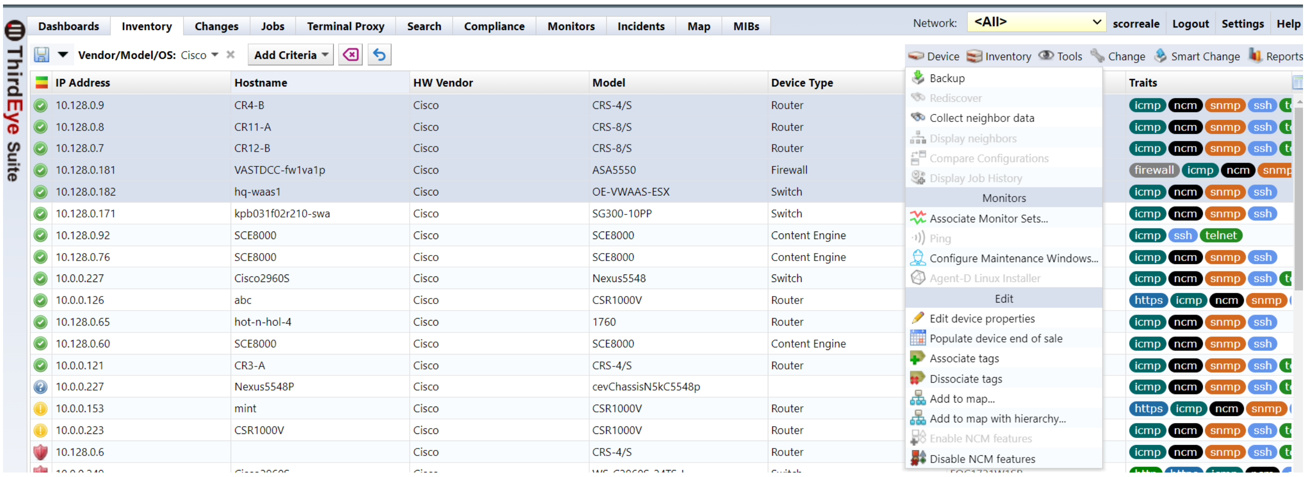
Name	Type	Period	Detail
[+] agentd-linux			
[+] agentd-windows			
[+] aruba			
[−] Cisco			
Cisco CPU	SNMP	1m	CISCO-PROCESS-MIB/cpmCPUTotalTable
CPU Stats	SNMP	30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping	ICMP	30s	ICMP echo
Interface Stats	SNMP	1m	IF-MIB/ifTable
Link-down Trap	SNMP Trap	n/a	IF-MIB/linkDown
Link-up Trap	SNMP Trap	n/a	IF-MIB/linkUp
[+] cisco-1			

5. Click the Editor’s [Devices] tab and select the device to which you want to assign the monitor set.



IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.128.0.9	CR4-B	Cisco	CRS-4/S	Router	SMA112502OH	icmp ncm snmp ssh t
10.128.0.8	CR11-A	Cisco	CRS-8/S	Router	TBA09500075	icmp ncm snmp ssh t
10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	TBA09500081	icmp ncm snmp ssh t
10.128.0.181	VASTDCC-fw1va1p	Cisco	ASA5550	Firewall	JMX1419L13J	firewall icmp ncm snmp
10.128.0.182	hq-waas1	Cisco	OE-VWAAS-ESX	Switch	VMware-42	icmp ncm snmp ssh
10.128.0.171	kpb031f02r210-swa	Cisco	SG300-10PP	Switch	PSZ18391FN8	icmp ncm snmp ssh
10.128.0.92	SCE8000	Cisco	SCE8000	Content Engine	FOX1537G9R3	icmp ssh telnet

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

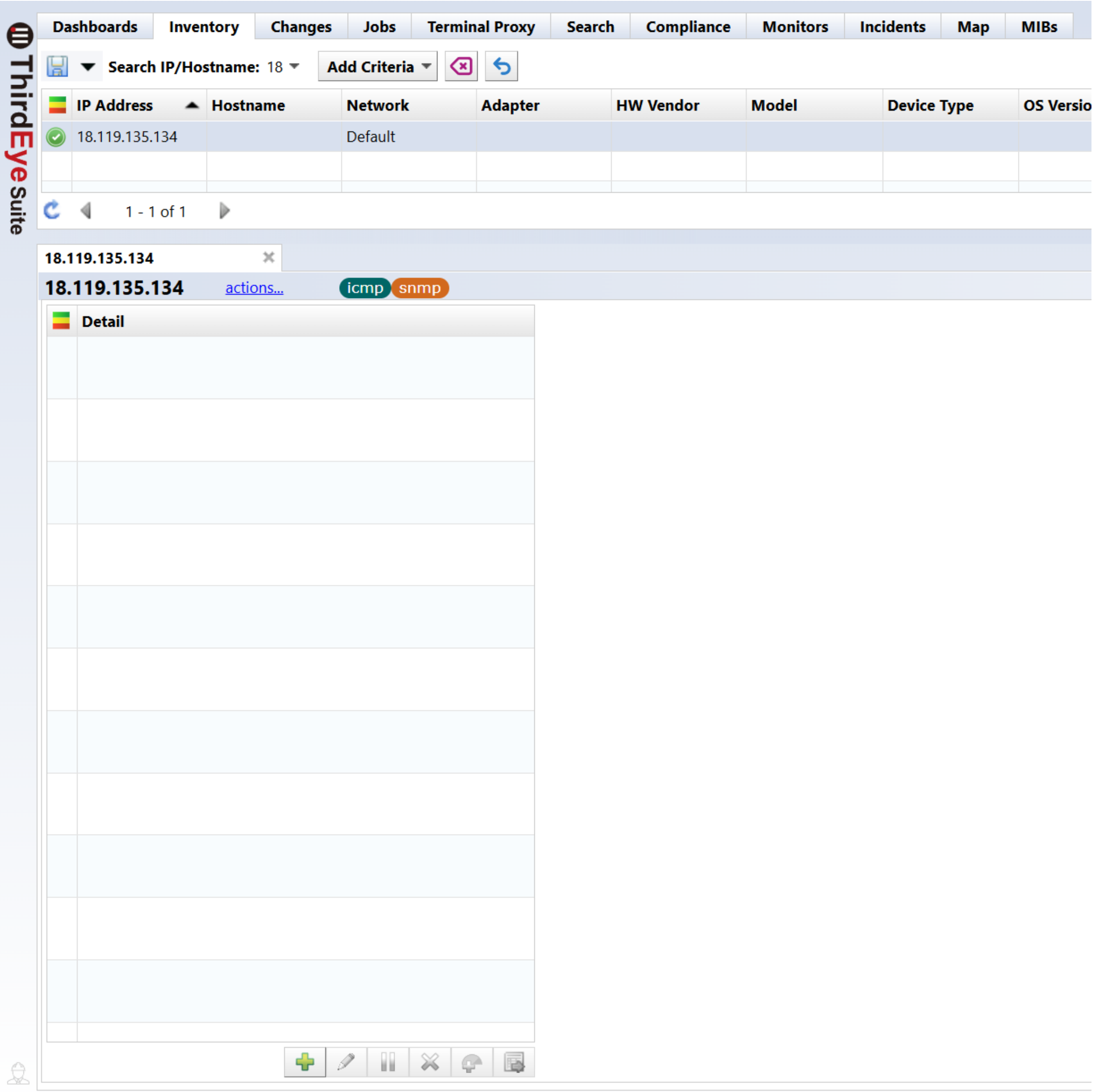


IP Address	Hostname	HW Vendor	Model	Device Type	Traits
10.128.0.9	CR4-B	Cisco	CRS-4/S	Router	icmp ncm snmp ssh t
10.128.0.8	CR11-A	Cisco	CRS-8/S	Router	icmp ncm snmp ssh t
10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	icmp ncm snmp ssh t
10.128.0.181	VASTDCC-fw1va1p	Cisco	ASA5550	Firewall	firewall icmp ncm snmp
10.128.0.182	hq-waas1	Cisco	OE-VWAAS-ESX	Switch	icmp ncm snmp ssh
10.128.0.171	kpb031f02r210-swa	Cisco	SG300-10PP	Switch	icmp ncm snmp ssh
10.128.0.92	SCE8000	Cisco	SCE8000	Content Engine	icmp ssh telnet
10.128.0.76	SCE8000	Cisco	SCE8000	Content Engine	icmp ncm snmp ssh
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	icmp ncm snmp ssh t
10.0.0.126	abc	Cisco	CSR1000V	Router	https icmp ncm snmp
10.128.0.65	hot-n-hol-4	Cisco	1760	Router	icmp ncm snmp ssh
10.128.0.60	SCE8000	Cisco	SCE8000	Content Engine	icmp ncm snmp ssh
10.0.0.121	CR3-A	Cisco	CRS-4/S	Router	icmp ncm snmp ssh t
10.0.0.227	Nexus5548P	Cisco	cevChassisN5kC5548p		icmp ncm snmp ssh t
10.0.0.153	mint	Cisco	CSR1000V	Router	https icmp ncm snmp
10.0.0.223	CSR1000V	Cisco	CSR1000V	Router	icmp ncm snmp ssh t
10.128.0.6		Cisco	CRS-4/S	Router	icmp ncm snmp ssh t

15.13 Monitor 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.

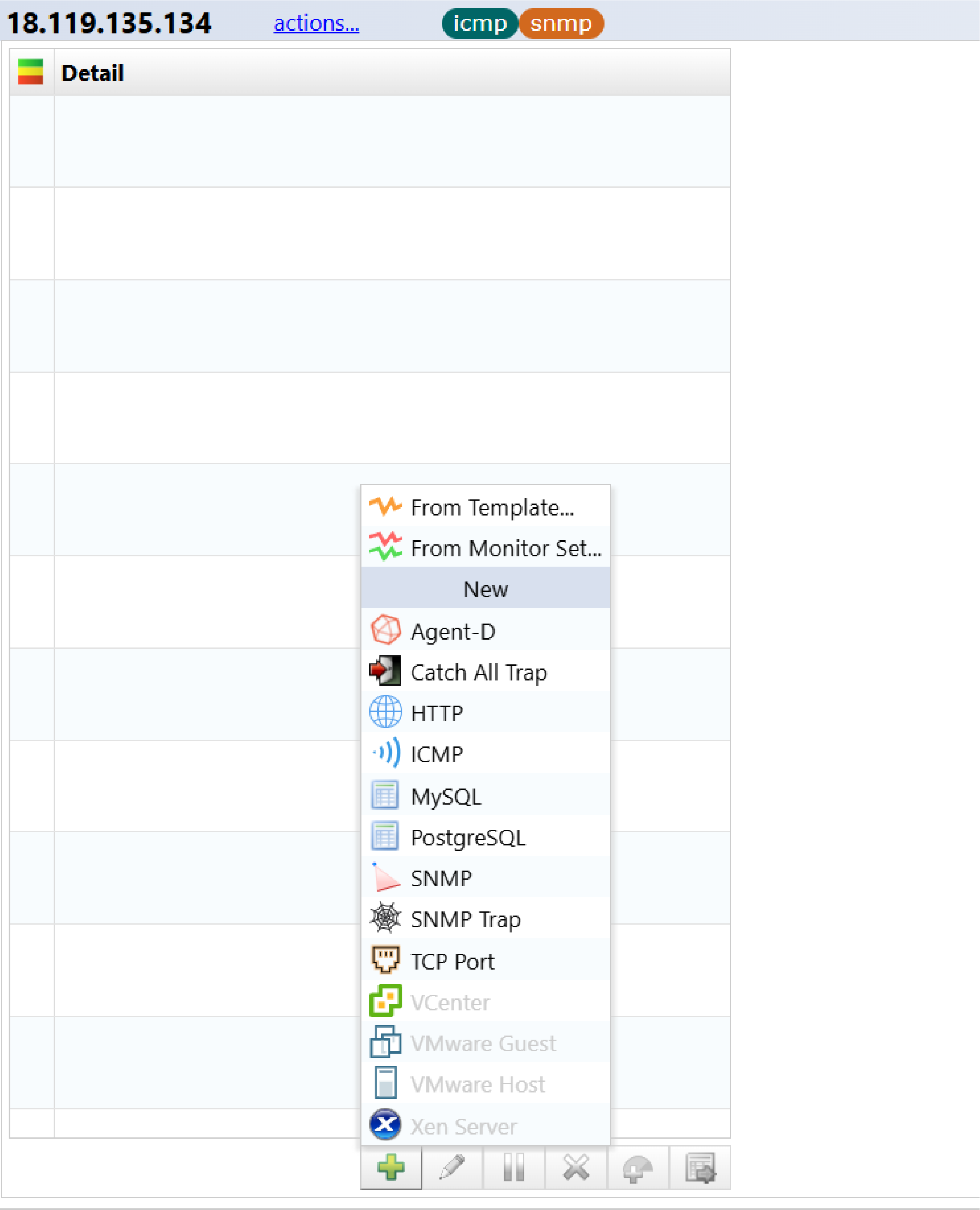


Search IP/Hostname: 18

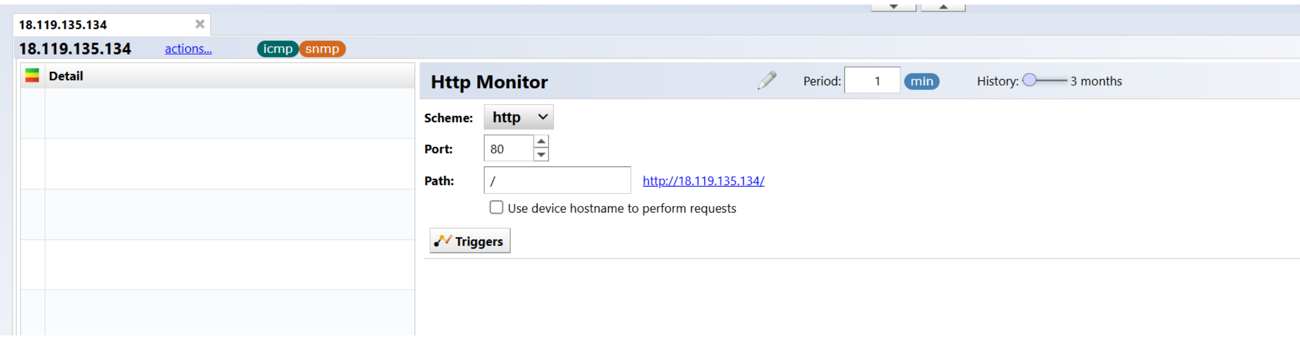
	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Versio
✓	18.119.135.134		Default					

18.119.135.134

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



3. Set any monitor name and interval.


18.119.135.134

18.119.135.134 actions... icmp snmp

Detail

Http Monitor

Period: 1 min

History: 3 months

Scheme: http

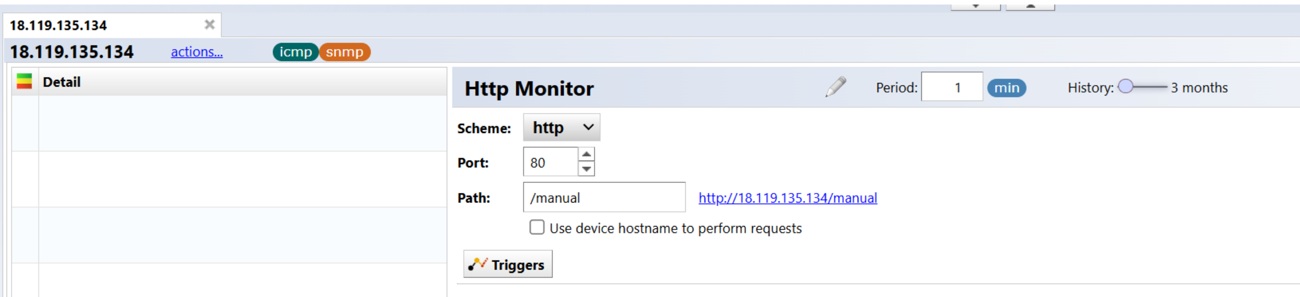
Port: 80

Path: / http://18.119.135.134/

□ Use device hostname to perform requests

Triggers

4. Enter the following items.


18.119.135.134

18.119.135.134 actions... icmp snmp

Detail

Http Monitor

Period: 1 min

History: 3 months

Scheme: http

Port: 80

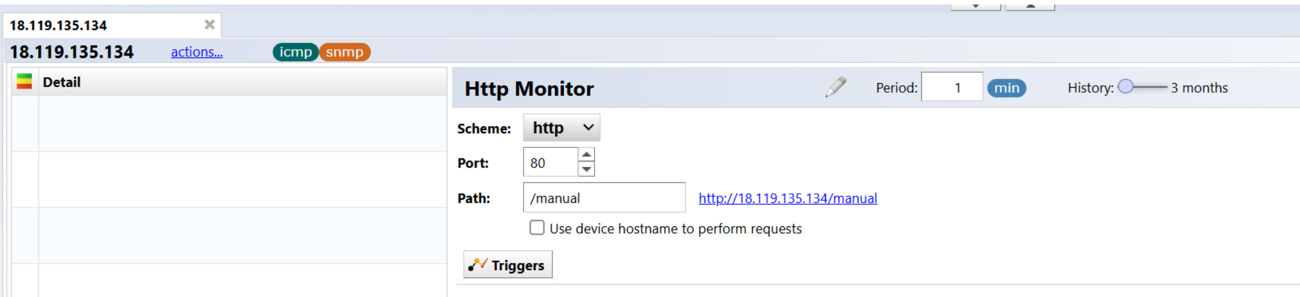
Path: /manual http://18.119.135.134/manual

□ Use device hostname to perform requests

Triggers

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].


18.119.135.134

18.119.135.134 actions... icmp snmp

Detail

Http Monitor Period: 1 min History: 3 months

Scheme: http

Port: 80

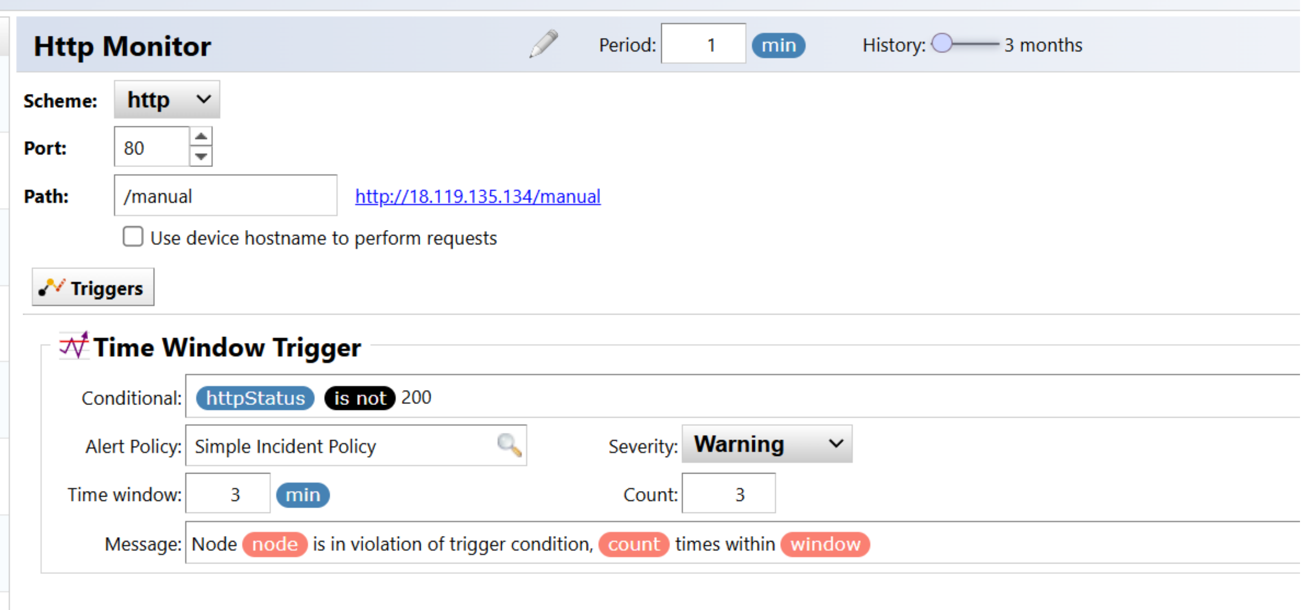
Path: /manual http://18.119.135.134/manual

□ Use device hostname to perform requests

Triggers

6. Set each item.

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


Http Monitor Period: 1 min History: 3 months

Scheme: http

Port: 80

Path: /manual http://18.119.135.134/manual

□ Use device hostname to perform requests

Triggers

Time Window Trigger

Conditional: httpStatus is not 200

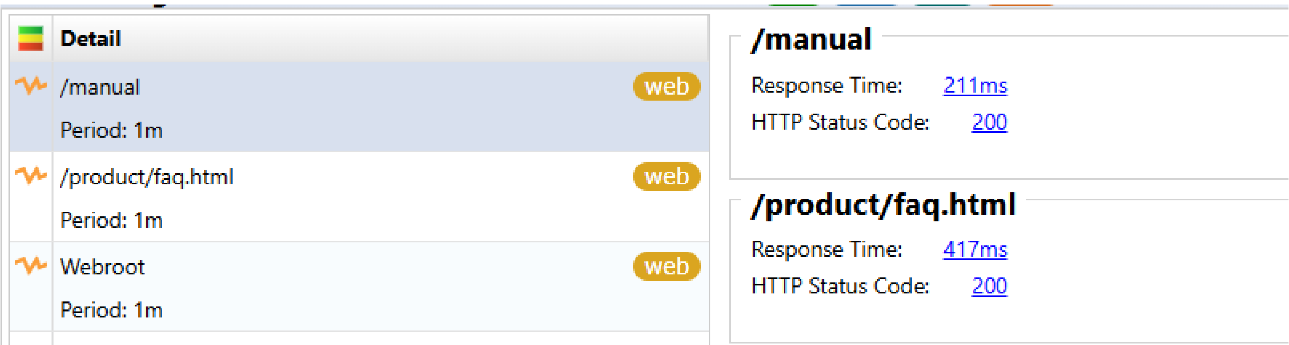
Alert Policy: Simple Incident Policy Severity: Warning

Time window: 3 min Count: 3

Message: Node node is in violation of trigger condition, count times within window

7. Click [Save].

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


Detail

/manual web
Period: 1m

/product/faq.html web
Period: 1m

Webroot web
Period: 1m

/manual

Response Time: 211ms

HTTP Status Code: 200

/product/faq.html

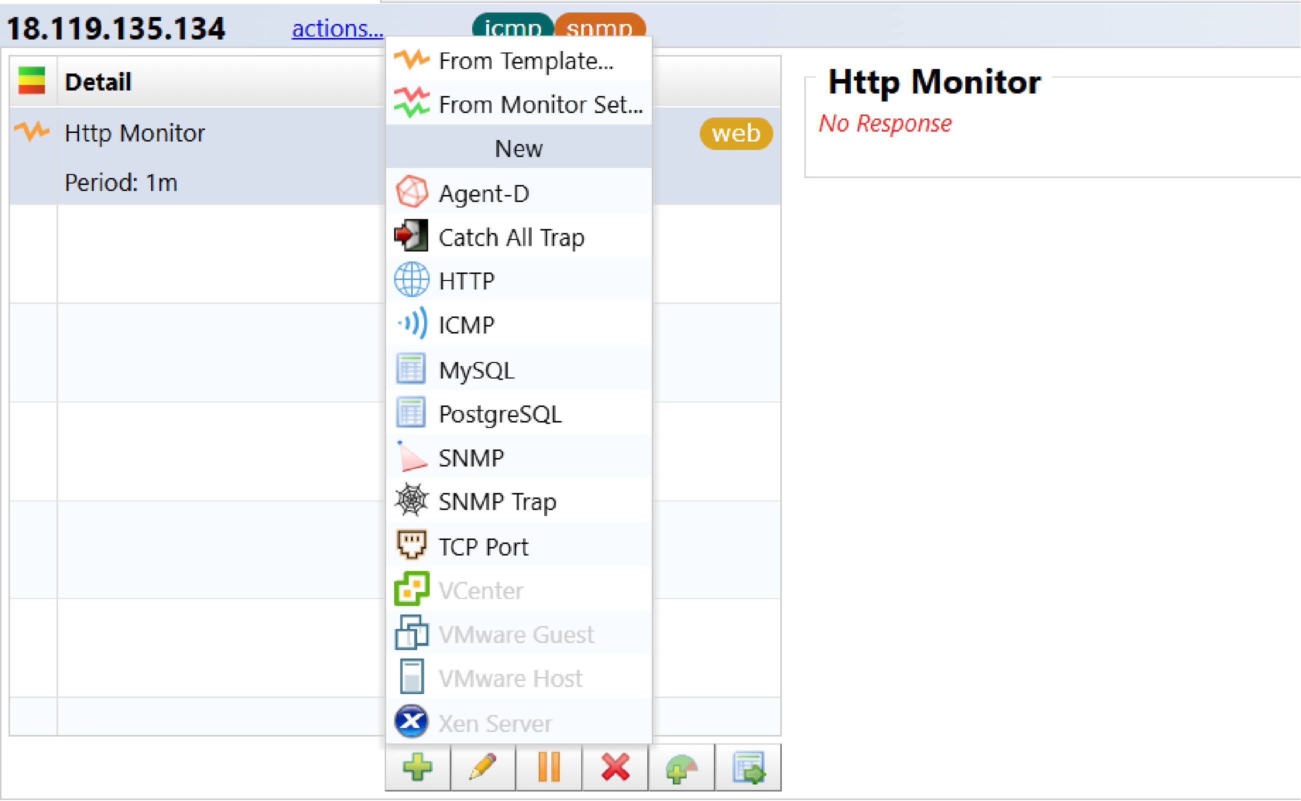
Response Time: 417ms

HTTP Status Code: 200

15.14 Monitor TCP Ports

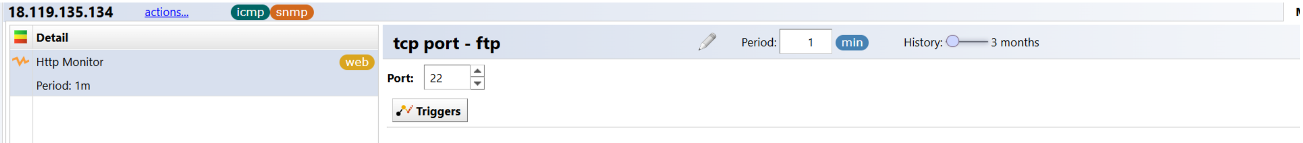
You can send a syn message to a TCP port and check if there is a response.

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



2. Set any monitor name, and select a Period.

3. Set the port number that must be monitored.



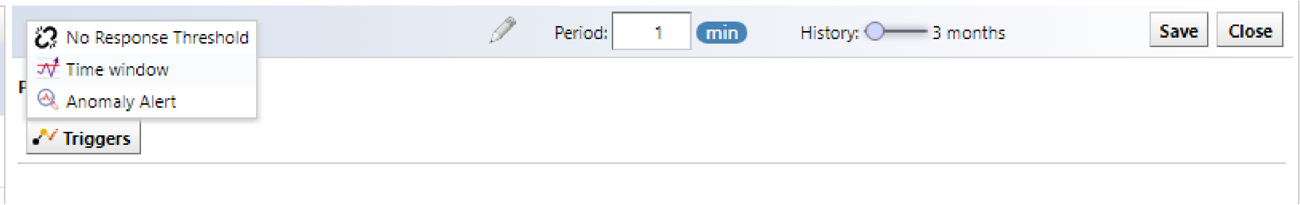
tcp port - ftp

Period: 1 min

History: 3 months

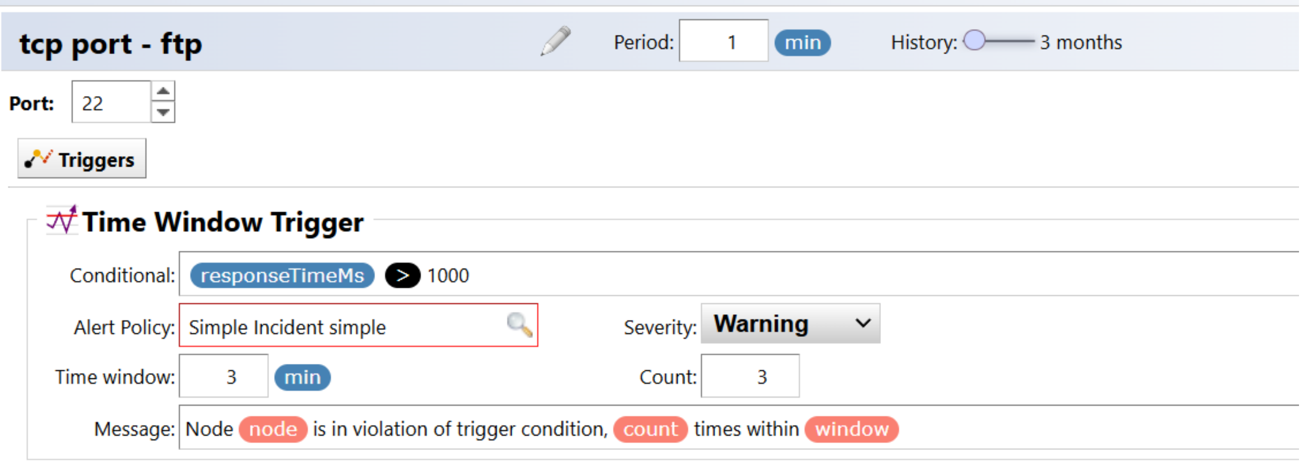
Port: 22

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



5. Configure each item in the “Time Window Trigger” window.

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



tcp port - ftp

Period: 1 min

History: 3 months

Port: 22

Time Window Trigger

Conditional: responseTimeMs > 1000

Alert Policy: Simple Incident simple

Severity: Warning

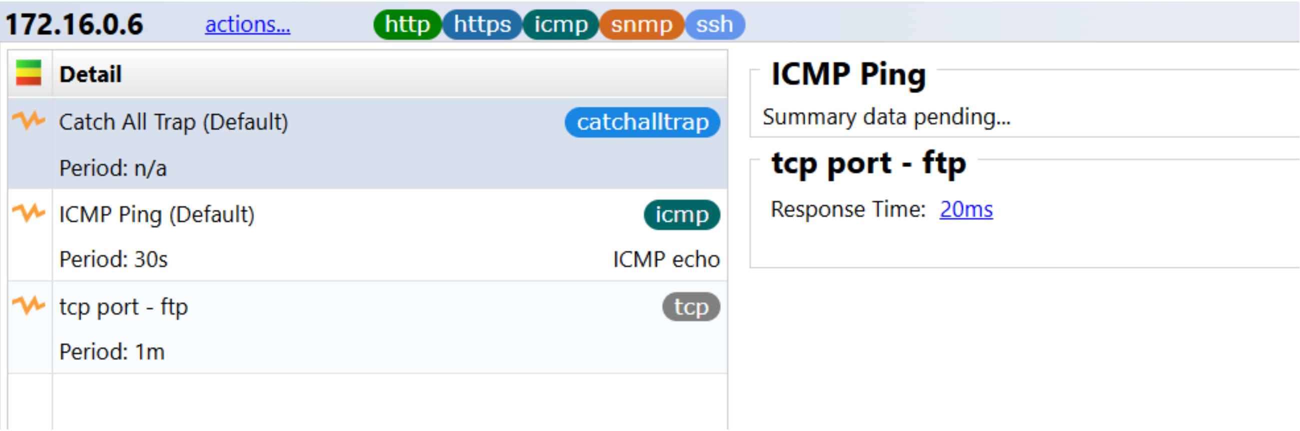
Time window: 3 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

6. Click [Save].

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



172.16.0.6 actions... http https icmp snmp ssh

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo
tcp port - ftp Period: 1m	tcp

ICMP Ping

Summary data pending...

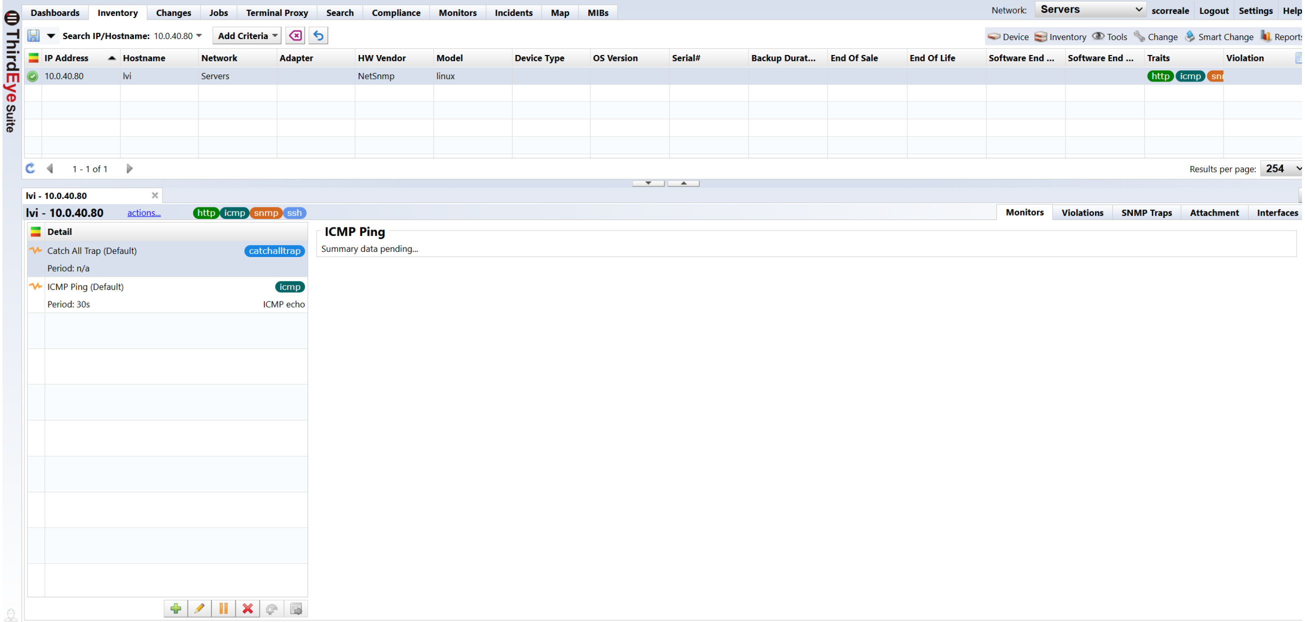
tcp port - ftp

Response Time: 20ms

15.15 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.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.40.80	lvi	Servers		NetSnmp	linux									http icmp sn	

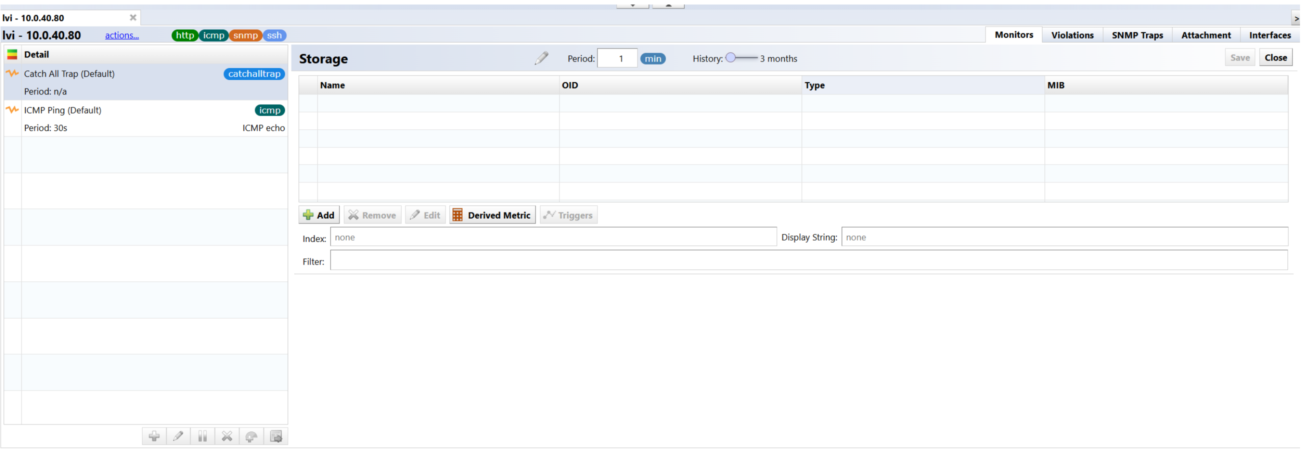
Catch All Trap (Default)
Period: n/a

ICMP Ping (Default)
Period: 30s ICMP echo

Summary data pending...

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

3. Set any monitor name and interval.



Catch All Trap (Default)
Period: n/a

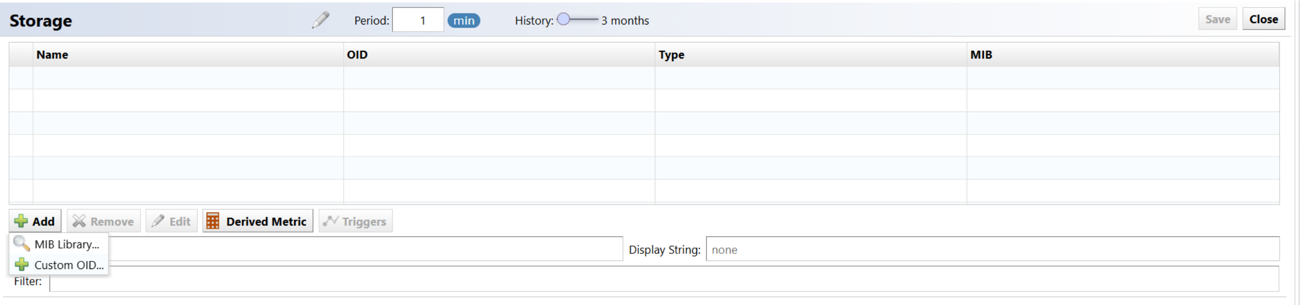
ICMP Ping (Default)
Period: 30s ICMP echo

Period: 1 min History: 3 months

Name	OID	Type	MIB

Index: none Display String: none
Filter:

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



Storage

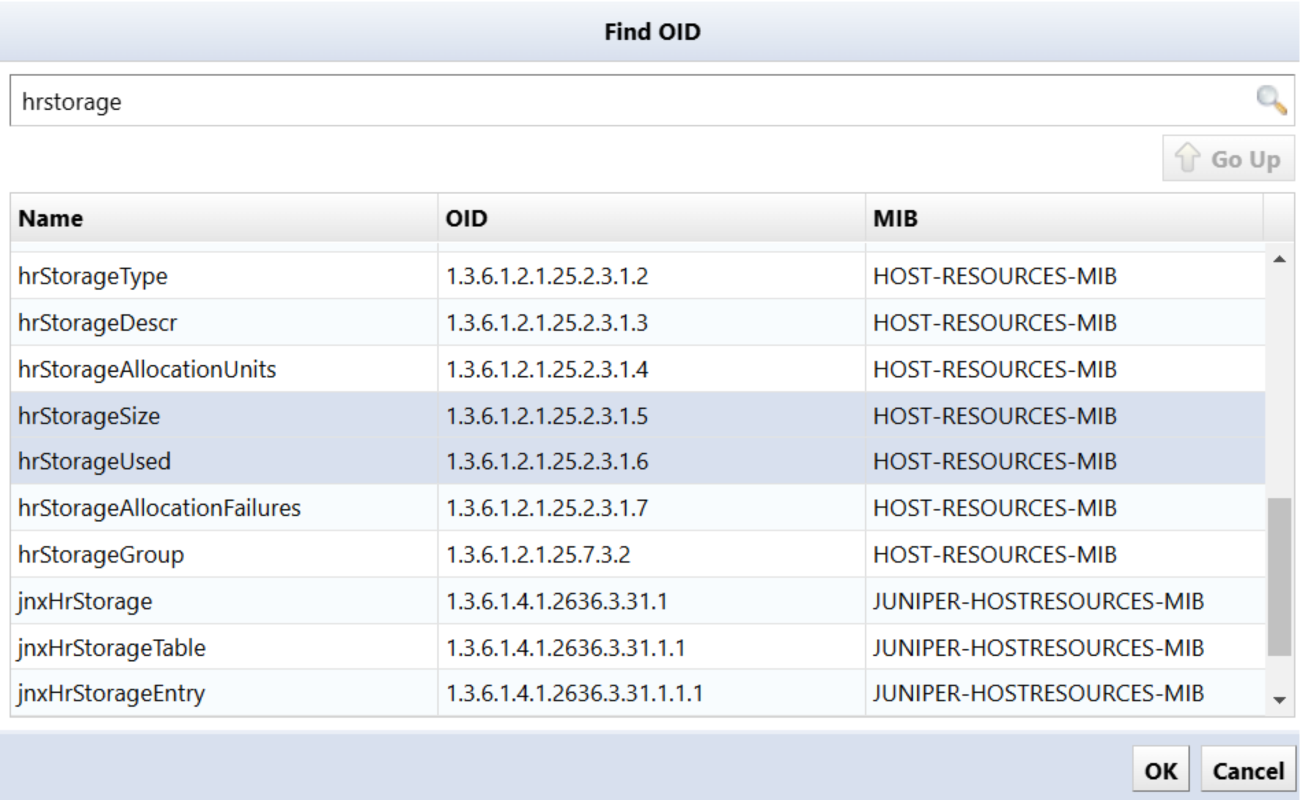
Period: 1 min History: 3 months

Name	OID	Type	MIB

Display String: none

Filter:

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

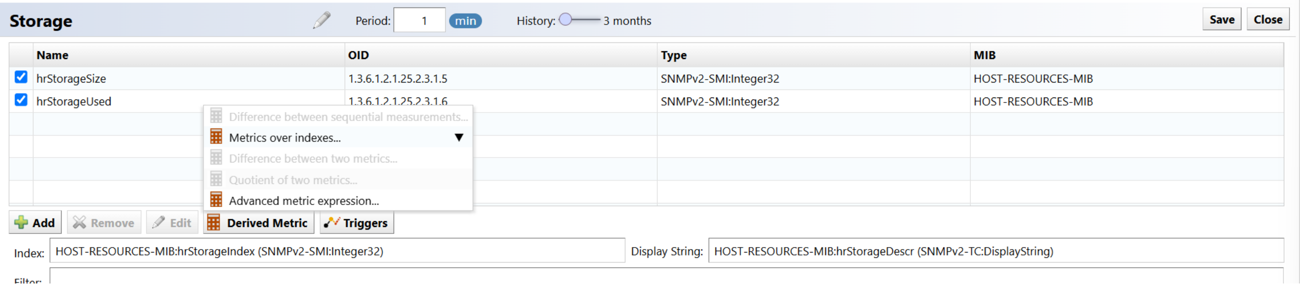


Find OID

hrstorage

Name	OID	MIB
hrStorageType	1.3.6.1.2.1.25.2.3.1.2	HOST-RESOURCES-MIB
hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3	HOST-RESOURCES-MIB
hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4	HOST-RESOURCES-MIB
hrStorageSize	1.3.6.1.2.1.25.2.3.1.5	HOST-RESOURCES-MIB
hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6	HOST-RESOURCES-MIB
hrStorageAllocationFailures	1.3.6.1.2.1.25.2.3.1.7	HOST-RESOURCES-MIB
hrStorageGroup	1.3.6.1.2.1.25.7.3.2	HOST-RESOURCES-MIB
jnxHrStorage	1.3.6.1.4.1.2636.3.31.1	JUNIPER-HOSTRESOURCES-MIB
jnxHrStorageTable	1.3.6.1.4.1.2636.3.31.1.1	JUNIPER-HOSTRESOURCES-MIB
jnxHrStorageEntry	1.3.6.1.4.1.2636.3.31.1.1.1	JUNIPER-HOSTRESOURCES-MIB

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



Storage

Period: 1 min History: 3 months

	Name	OID	Type	MIB
☑	hrStorageSize	1.3.6.1.2.1.25.2.3.1.5	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB

Index: HOST-RESOURCES-MIB:hrStorageIndex (SNMPv2-SMI:Integer32) Display String: HOST-RESOURCES-MIB:hrStorageDescr (SNMPv2-TC:DisplayString)

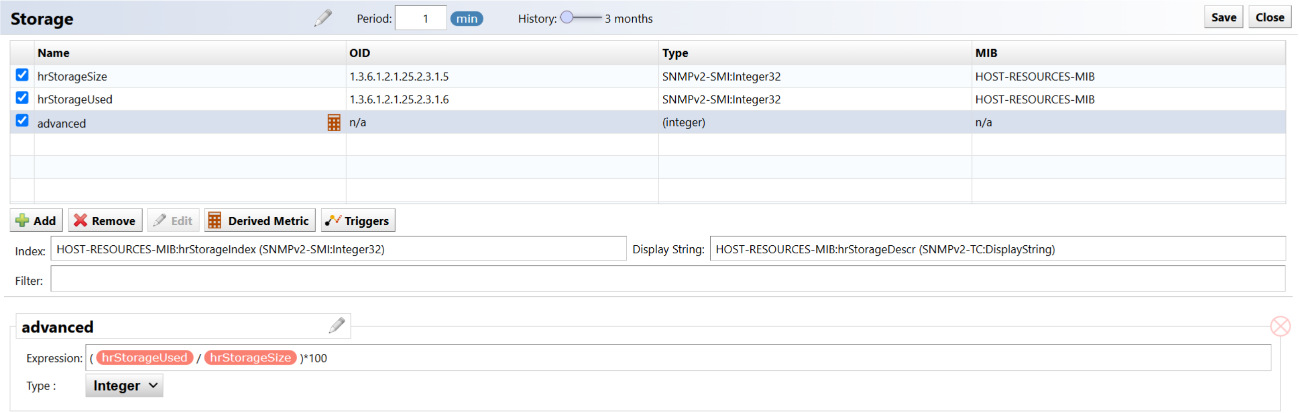
Filter:

Save
Close
Difference between sequential measurements...
Metrics over indexes...
Difference between two metrics...
Quotient of two metrics...
Advanced metric expression...
Add
Remove
Edit
Derived Metric
Triggers

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].



	Name	OID	Type	MIB
☑	hrStorageSize	1.3.6.1.2.1.25.2.3.1.5	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	advanced	n/a	(integer)	n/a

Index: HOST-RESOURCES-MIB:hrStorageIndex (SNMPv2-SMI:Integer32)

Display String: HOST-RESOURCES-MIB:hrStorageDescr (SNMPv2-TC:DisplayString)

Filter:

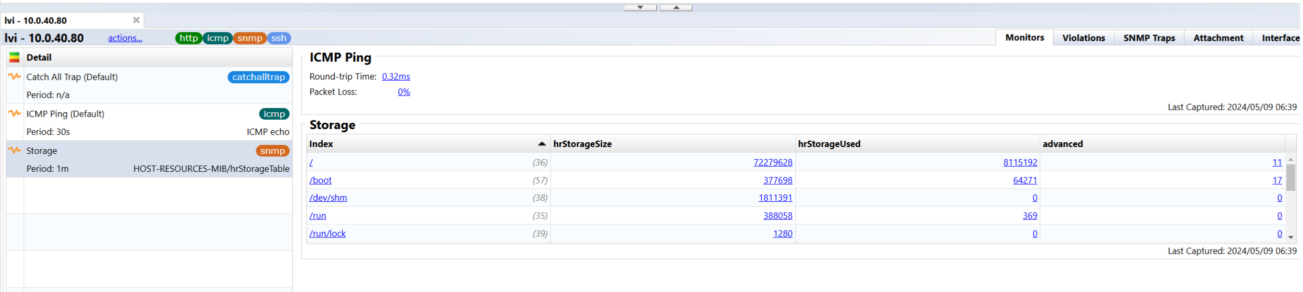
advanced

Expression: (hrStorageUsed / hrStorageSize)*100

Type : Integer

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

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



Catch All Trap (Default) catchalltrap
Period: n/a

ICMP Ping (Default) icmp
Period: 30s ICMP echo

Storage snmp
Period: 1m HOST-RESOURCES-MIB/hrStorageTable

ICMP Ping

Round-trip Time: 0.32ms

Packet Loss: 0%

Last Captured: 2024/05/09 06:39

Storage

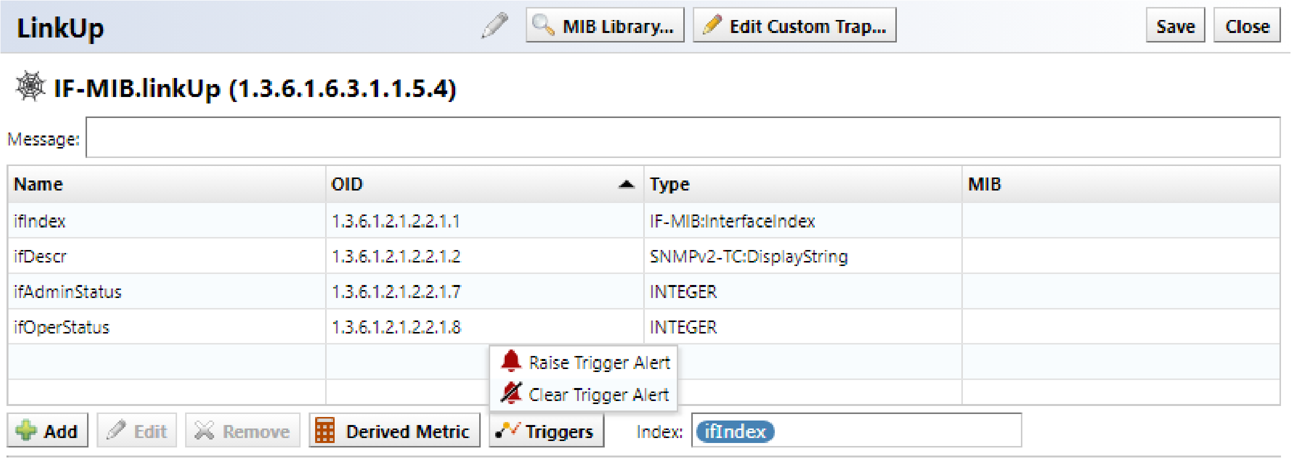
Index		hrStorageSize	hrStorageUsed	advanced
/	(36)	72279628	8115192	11
/boot	(57)	377698	64271	17
/dev/shm	(38)	1811391	0	0
/run	(35)	388058	369	0
/run/lock	(39)	1280	0	0

Last Captured: 2024/05/09 06:39

15.16 Automatically Clear Trap Incidents

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].



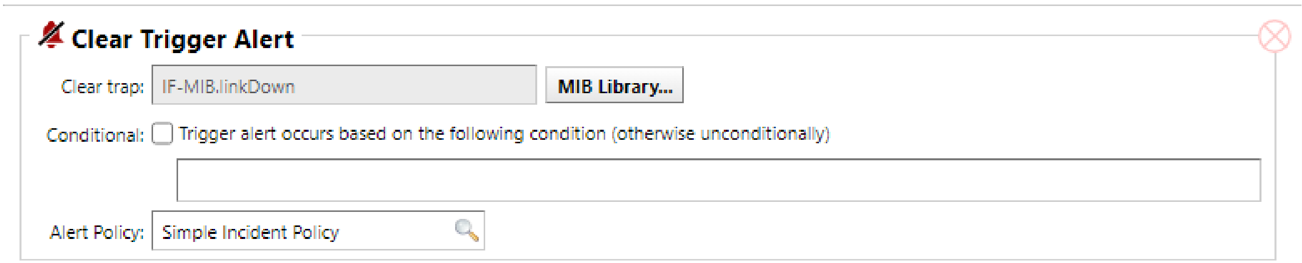
IF-MIB.linkUp (1.3.6.1.6.3.1.1.5.4)

Message:

Name	OID	Type	MIB
ifIndex	1.3.6.1.2.1.2.2.1.1	IF-MIB:InterfaceIndex	
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString	
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	

Index: ifIndex

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

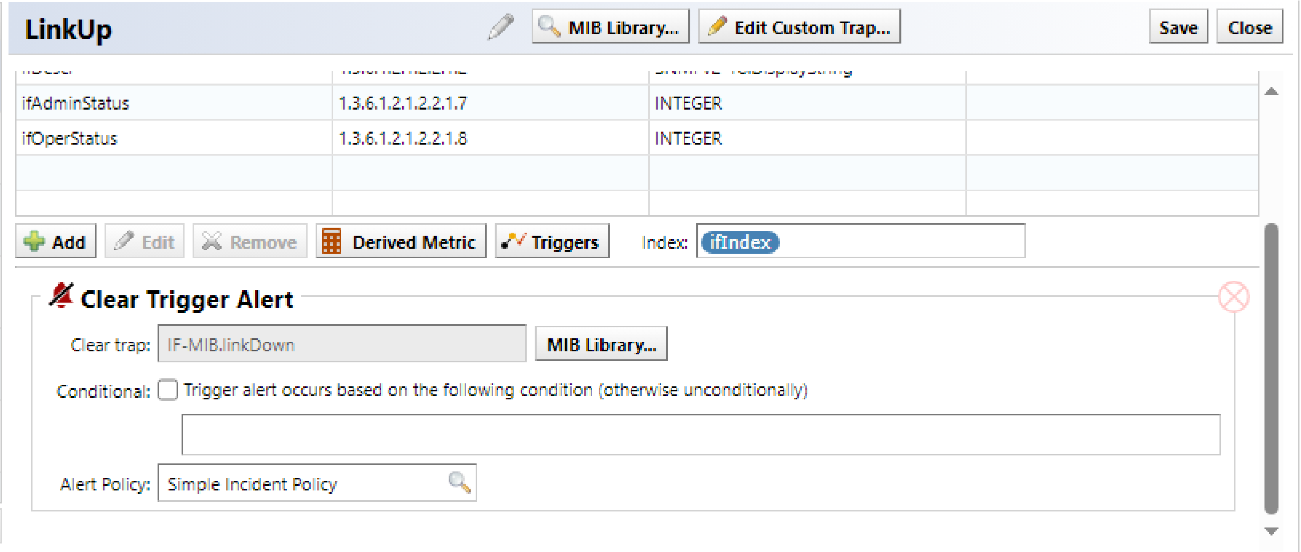


Clear trap: IF-MIB.linkDown

Conditional: ☐ Trigger alert occurs based on the following condition (otherwise unconditionally)

Alert Policy: Simple Incident Policy

5. Click [Save].



ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	

Index: ifIndex

Clear Trigger Alert

Clear trap: IF-MIB.linkDown

Conditional: □ Trigger alert occurs based on the following condition (otherwise unconditionally)

Alert Policy: Simple Incident Policy

15.17 Change Actions Based on the Trap Values

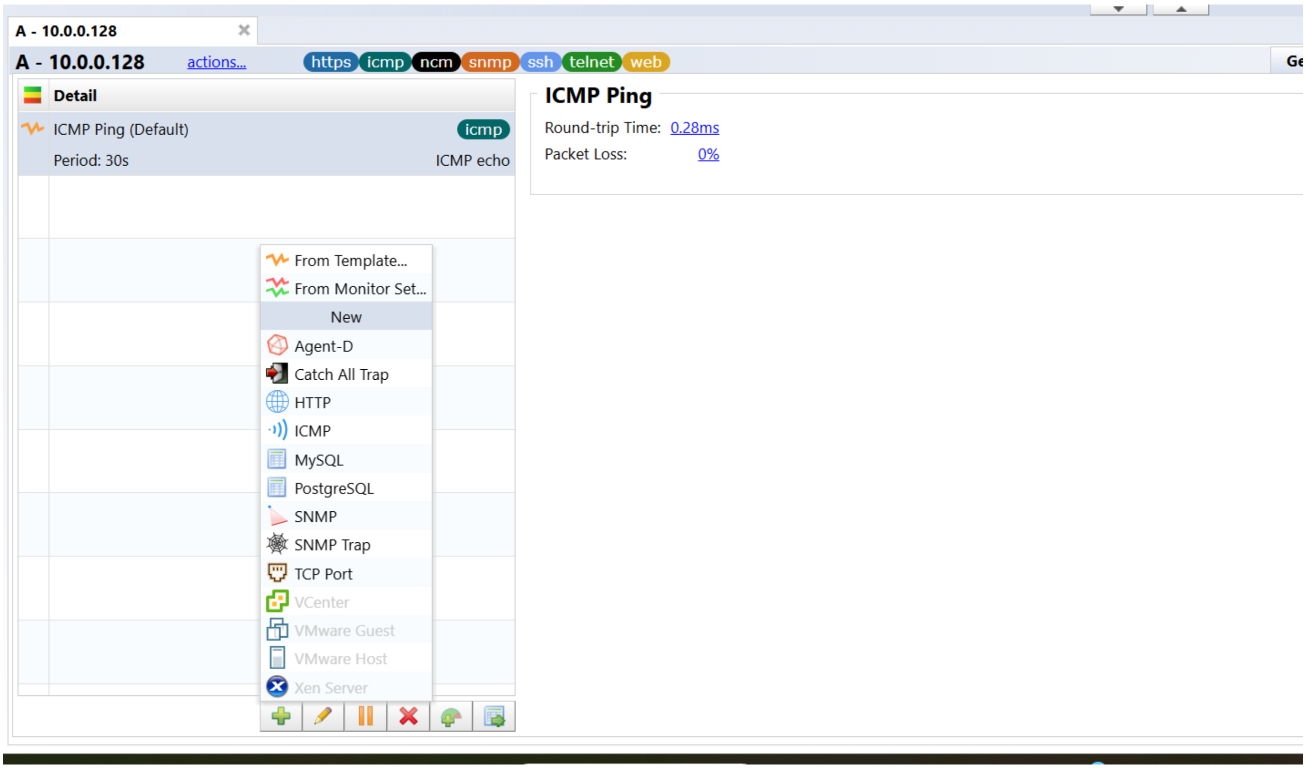
When the monitored device sends a trap, it puts various information into the trap and sends it. Depending on the content, you may not want to detect it as a failure. ThirdEye allows you to filter by specifying conditions.

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

1. In the [Inventory] main tab, doubleclick the target device.

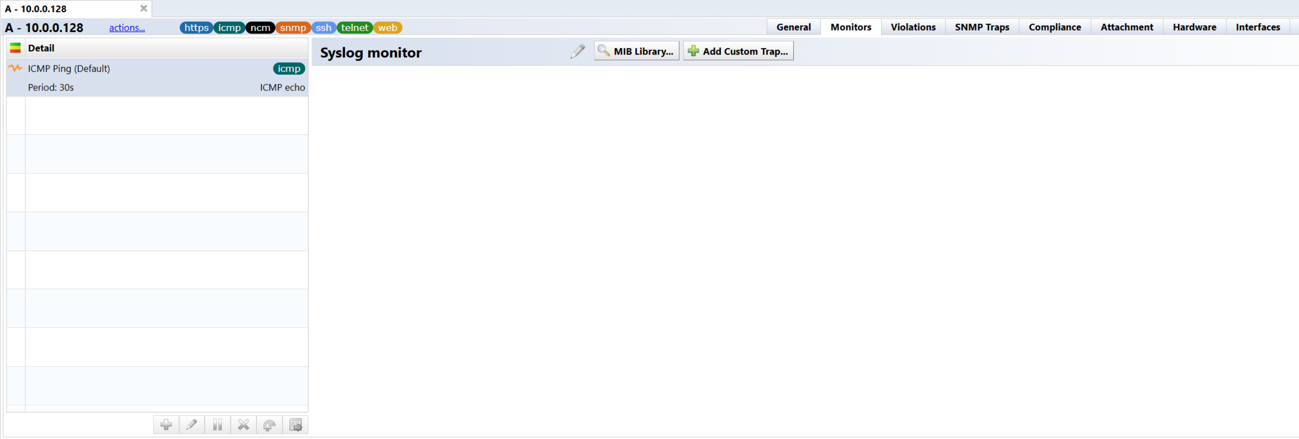
The device's Editor will open at the bottom of the screen.

2. Click the ➕ button in the left sidepanel of the Editor to open the options menu.
3. Click [SNMP Trap] to add an SNMP trap monitor to the device.



Round-trip Time: 0.28ms
Packet Loss: 0%

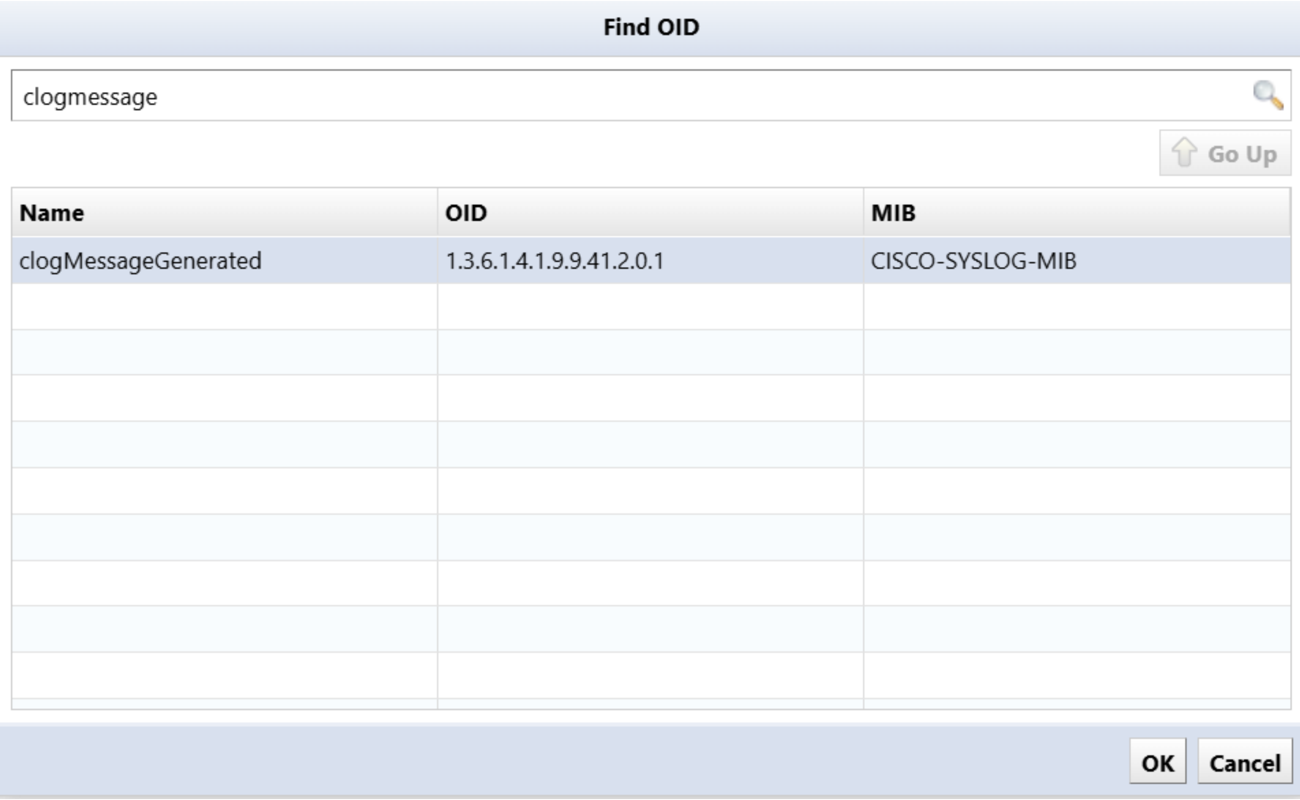
4. Enter a monitor name (“Syslog Monitor” in the example below).



ICMP Ping (Default) icmp
Period: 30s ICMP echo

Syslog monitor

5. Click the [MIB Library] button at the top of the Editor.
6. Enter `clogmessage` in the OID search, and select `clogMessageGenerated` from the search results.
7. Click [OK].

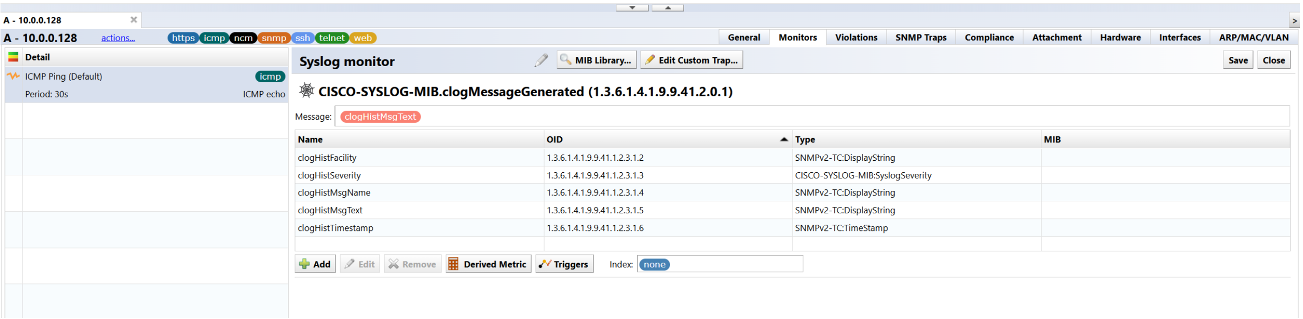


clogmessage

Name	OID	MIB
clogMessageGenerated	1.3.6.1.4.1.9.9.41.2.0.1	CISCO-SYSLOG-MIB

8. Enter a message for when a failure occurs.

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



Syslog monitor

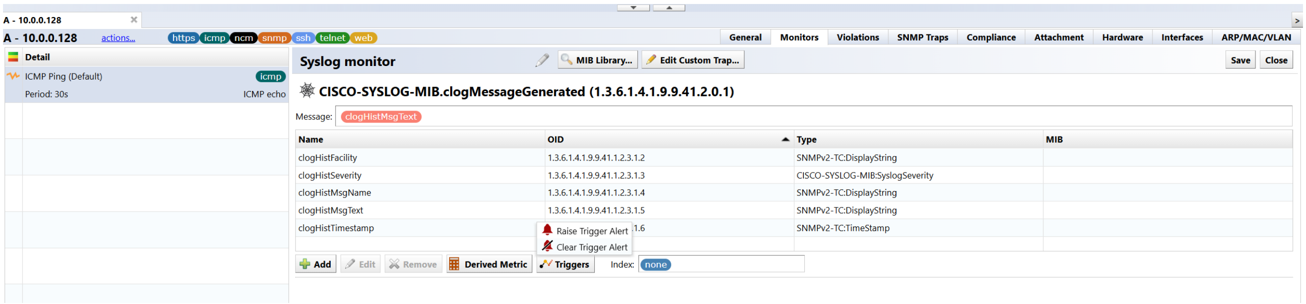
CISCO-SYSLOG-MIB.clogMessageGenerated (1.3.6.1.4.1.9.9.41.2.0.1)

Message: clogHistMsgText

Name	OID	Type	MIB
clogHistFacility	1.3.6.1.4.1.9.9.41.1.2.3.1.2	SNMPv2-TC:DisplayString	
clogHistSeverity	1.3.6.1.4.1.9.9.41.1.2.3.1.3	CISCO-SYSLOG-MIB:SyslogSeverity	
clogHistMsgName	1.3.6.1.4.1.9.9.41.1.2.3.1.4	SNMPv2-TC:DisplayString	
clogHistMsgText	1.3.6.1.4.1.9.9.41.1.2.3.1.5	SNMPv2-TC:DisplayString	
clogHistTimestamp	1.3.6.1.4.1.9.9.41.1.2.3.1.6	SNMPv2-TC:TimeStamp	

Index: none

9. Click [Trigger], then click [Raise Trigger Alert].



Syslog monitor

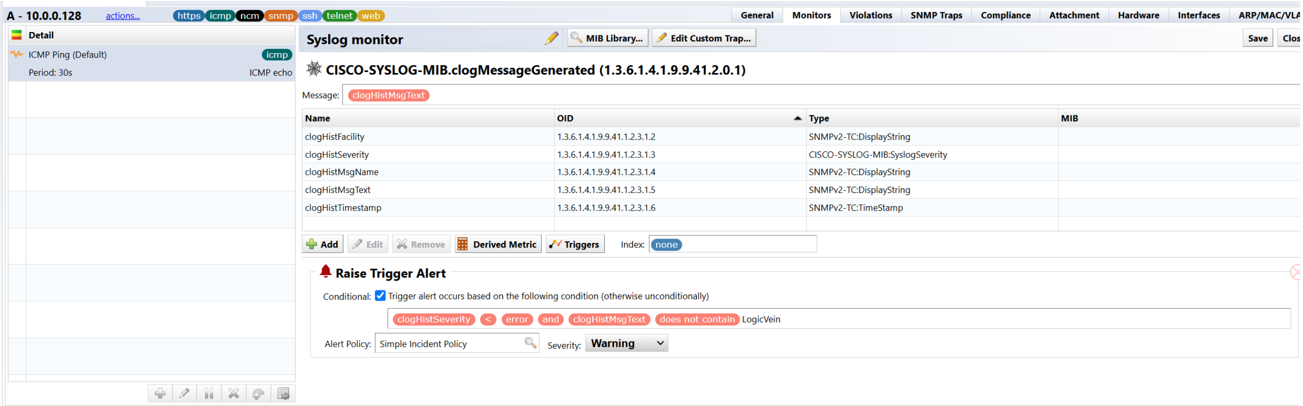
CISCO-SYSLOG-MIB.clogMessageGenerated (1.3.6.1.4.1.9.9.41.2.0.1)

Message: clogHistMsgText

Name	OID	Type	MIB
clogHistFacility	1.3.6.1.4.1.9.9.41.1.2.3.1.2	SNMPv2-TC:DisplayString	
clogHistSeverity	1.3.6.1.4.1.9.9.41.1.2.3.1.3	CISCO-SYSLOG-MIB:SyslogSeverity	
clogHistMsgName	1.3.6.1.4.1.9.9.41.1.2.3.1.4	SNMPv2-TC:DisplayString	
clogHistMsgText	1.3.6.1.4.1.9.9.41.1.2.3.1.5	SNMPv2-TC:DisplayString	
clogHistTimestamp	1.6	SNMPv2-TC:TimeStamp	

Index: none

10. Check the box next to “Conditional” and enter your Trigger Alert conditions.



Syslog monitor

CISCO-SYSLOG-MIB.clogMessageGenerated (1.3.6.1.4.1.9.9.41.2.0.1)

Message: clogHistMsgText

Name	OID	Type	MIB
clogHistFacility	1.3.6.1.4.1.9.9.41.1.2.3.1.2	SNMPv2-TC:DisplayString	
clogHistSeverity	1.3.6.1.4.1.9.9.41.1.2.3.1.3	CISCO-SYSLOG-MIB:SyslogSeverity	
clogHistMsgName	1.3.6.1.4.1.9.9.41.1.2.3.1.4	SNMPv2-TC:DisplayString	
clogHistMsgText	1.3.6.1.4.1.9.9.41.1.2.3.1.5	SNMPv2-TC:DisplayString	
clogHistTimestamp	1.3.6.1.4.1.9.9.41.1.2.3.1.6	SNMPv2-TC:TimeStamp	

Index: none

Raise Trigger Alert

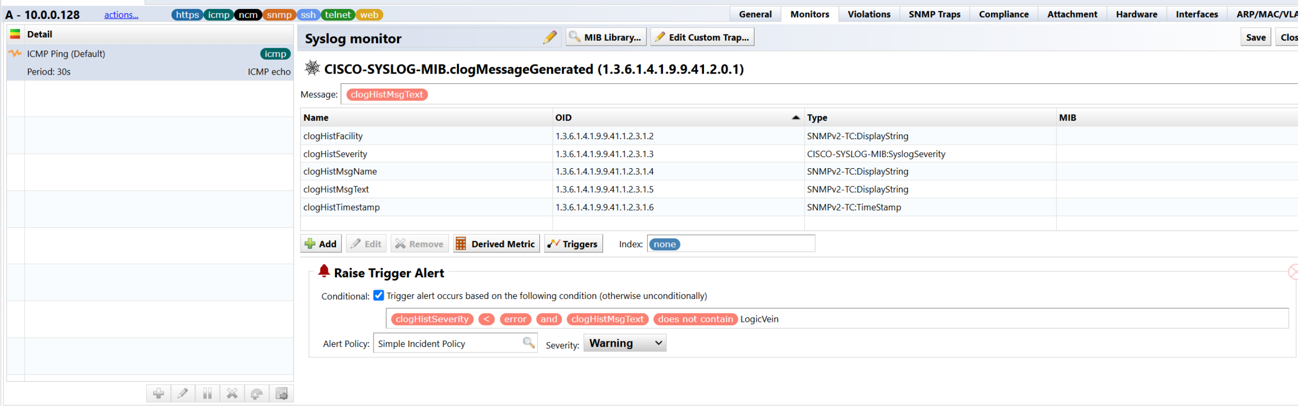
Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

clogHistSeverity < error and clogHistMsgText does not contain LogicVein

Alert Policy: Simple Incident Policy Severity: Warning

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.

11. Set the policy and severity.



CISCO-SYSLOG-MIB.clogMessageGenerated (1.3.6.1.4.1.9.9.41.2.0.1)

Message: clogHistMsgText

Name	OID	Type	MIB
clogHistFacility	1.3.6.1.4.1.9.9.41.1.2.3.1.2	SNMPv2-TC:DisplayString	
clogHistSeverity	1.3.6.1.4.1.9.9.41.1.2.3.1.3	CISCO-SYSLOG-MIB:SyslogSeverity	
clogHistMsgName	1.3.6.1.4.1.9.9.41.1.2.3.1.4	SNMPv2-TC:DisplayString	
clogHistMsgText	1.3.6.1.4.1.9.9.41.1.2.3.1.5	SNMPv2-TC:DisplayString	
clogHistTimestamp	1.3.6.1.4.1.9.9.41.1.2.3.1.6	SNMPv2-TC:TimeStamp	

Index: none

Raise Trigger Alert

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

clogHistSeverity < error and clogHistMsgText does not contain LogicVein

Alert Policy: Simple Incident Policy

Severity: Warning

12. Click [Save].

15.18 Compile the MIB

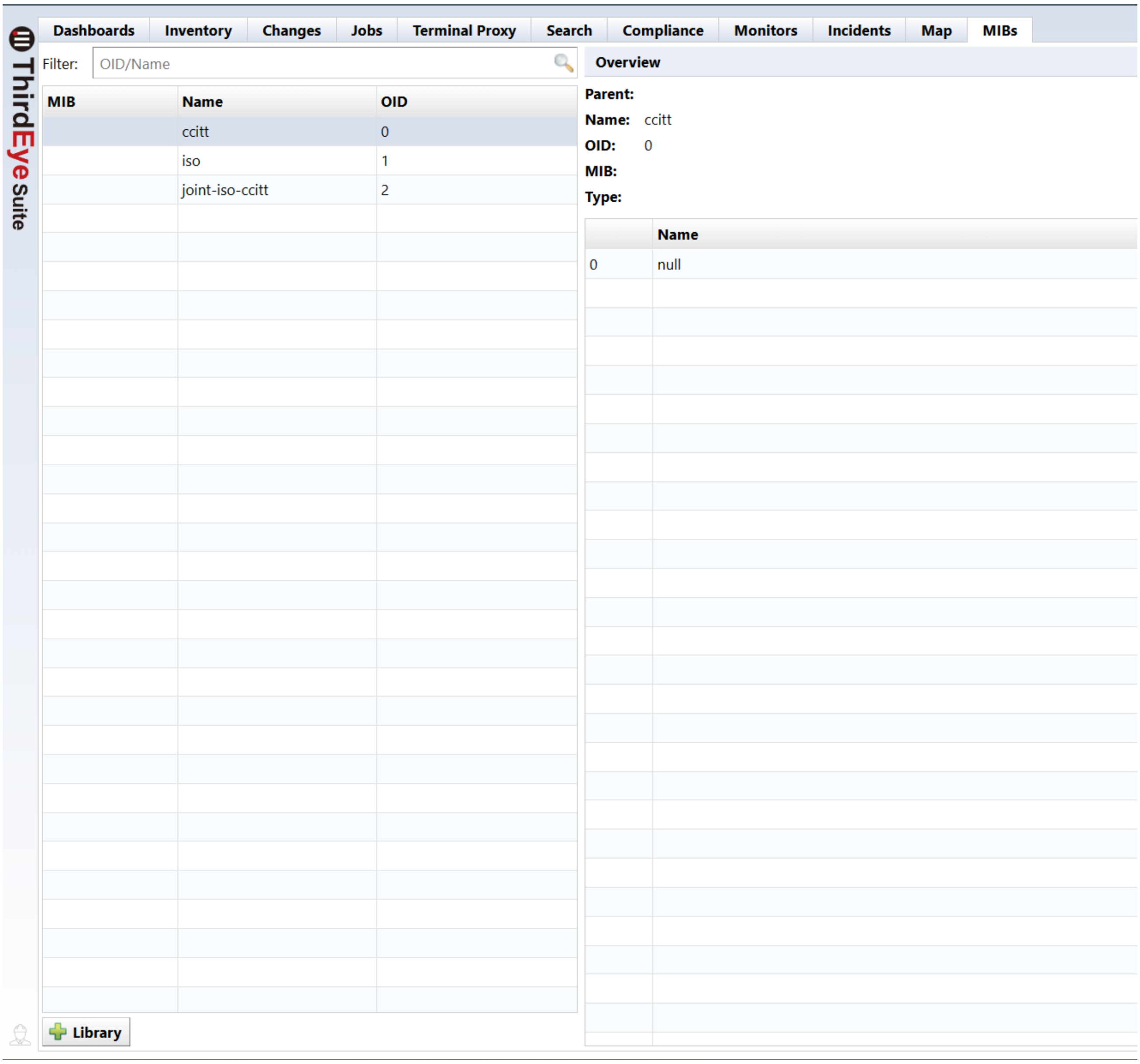
A Management Information Base (MIB) is a standardized framework that defines network device metrics. It uses Object Identifiers (OIDs) in a hierarchical tree structure. The MIB serve as a “dictionary” for SNMP monitoring systems, translating numerical OIDs into human-readable values.

Successful compilation makes the MIB searchable in tools like ThirdEye’s monitor configuration. Compiling a MIB processes its definitions:

- Validates syntax and dependencies
- Registers OIDs in the monitoring system
- Enables discovery for SNMP monitor creation

You can add uncompiled MIB files to ThirdEye.

1. Click the [MIBs] main tab.
2. Click the [Library] button at the bottom on the left sidepanel.



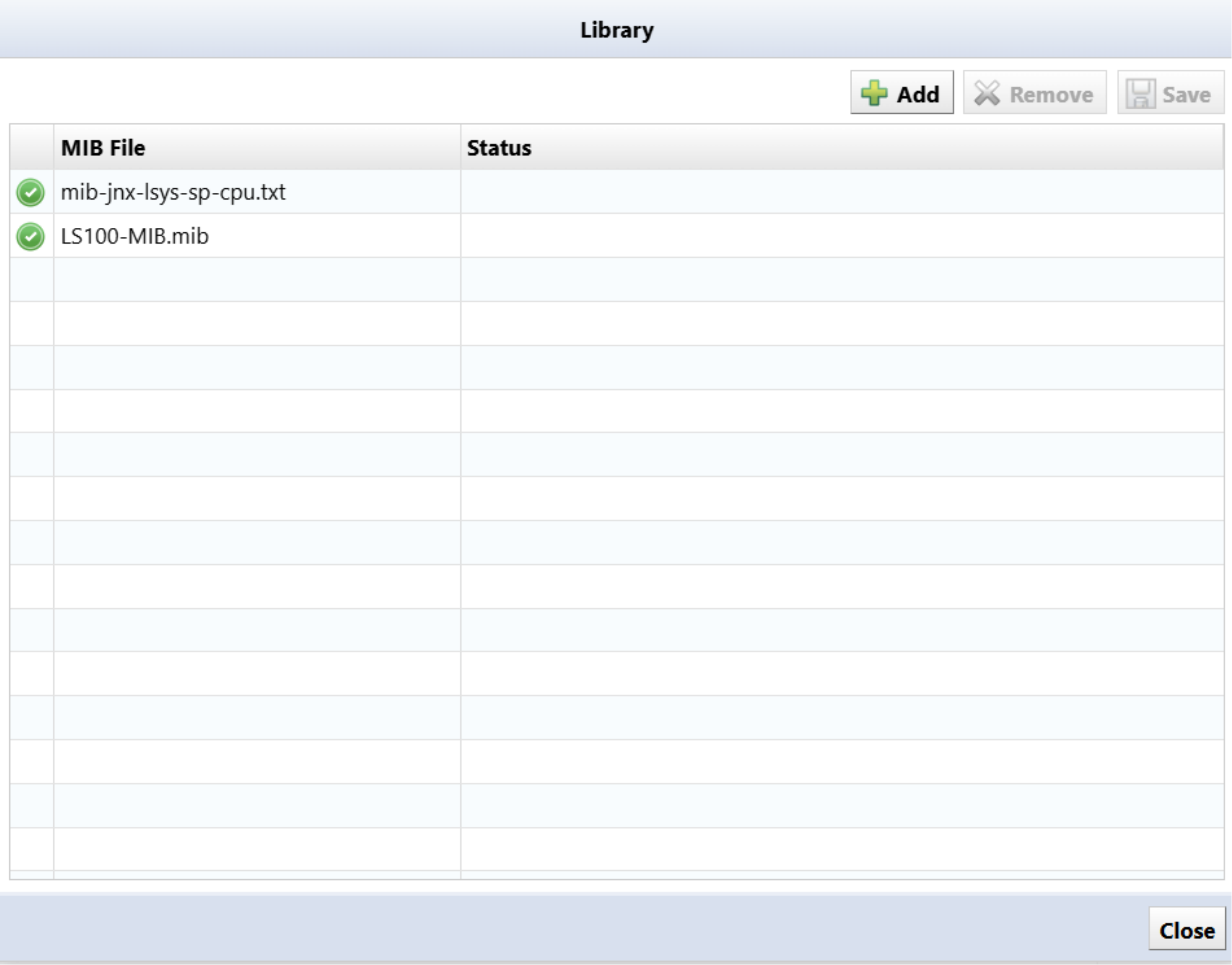
MIB	Name	OID
	ccitt	0
	iso	1
	joint-iso-ccitt	2

Parent:
Name: ccitt
OID: 0
MIB:
Type:

	Name
0	null

The library screen will be displayed.

3. Click the Add button to select a file.



	MIB File	Status
✓	mib-jnx-lsys-sp-cpu.txt	
✓	LS100-MIB.mib	

A file selection dialog will be displayed.

4. Select the MIB file to compile and click [Open].

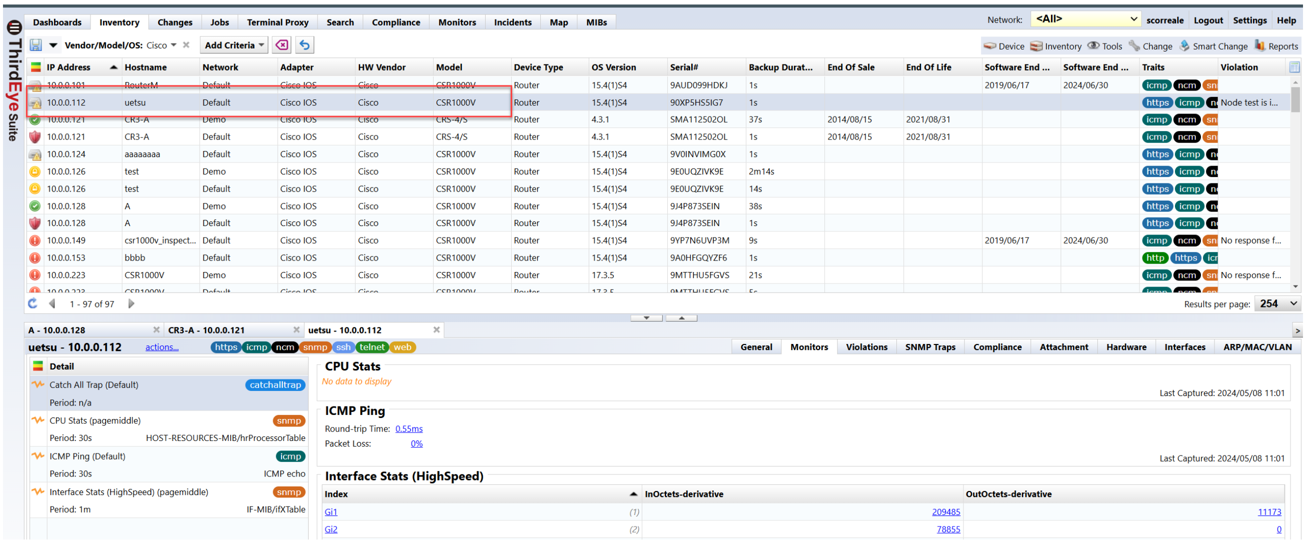
Compilation is complete when the MIB file is displayed in the list, and the ✓ icon is displayed to the left of the MIB file.

5. Click [Close].

15.19 Delete Monitor

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

This opens the Editor’s [Monitors] tab at the bottom of the window.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.101	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	1s			2019/06/17	2024/06/30	icmp ncm sn	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	1s					https icmp n	Node test is i...
10.0.0.121	CR3-A	Demo	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	37s	2014/08/15	2021/08/31			icmp ncm sn	
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31			icmp ncm sn	
10.0.0.124	aaaaaaaa	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	1s					https icmp n	
10.0.0.126	test	Demo	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	2m14s					https icmp n	
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	14s					https icmp n	
10.0.0.128	A	Demo	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	38s					https icmp n	
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	1s					https icmp n	
10.0.0.149	csr1000v_inspect...	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9YP7N6UVP3M	9s			2019/06/17	2024/06/30	icmp ncm sn	No response f...
10.0.0.153	bbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFGQYZF6	1s					http https ic	
10.0.0.223	CSR1000V	Demo	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	21s					icmp ncm sn	No response f...
10.0.0.223	CSR1000V	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	5s					icmp ncm sn	

1 - 97 of 97

Results per page: 254

A - 10.0.0.128 | CR3-A - 10.0.0.121 | uetsu - 10.0.0.112

uetsu - 10.0.0.112 actions... https icmp ncm snmp ssh telnet web

General | Monitors | Violations | SNMP Traps | Compliance | Attachment | Hardware | Interfaces | ARP/MAC/VLAN

Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
CPU Stats (pagemiddle)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Interface Stats (HighSpeed) (pagemiddle)	snmp
Period: 1m	IF-MIB/ifXTable

CPU Stats

No data to display

Last Captured: 2024/05/08 11:01

ICMP Ping

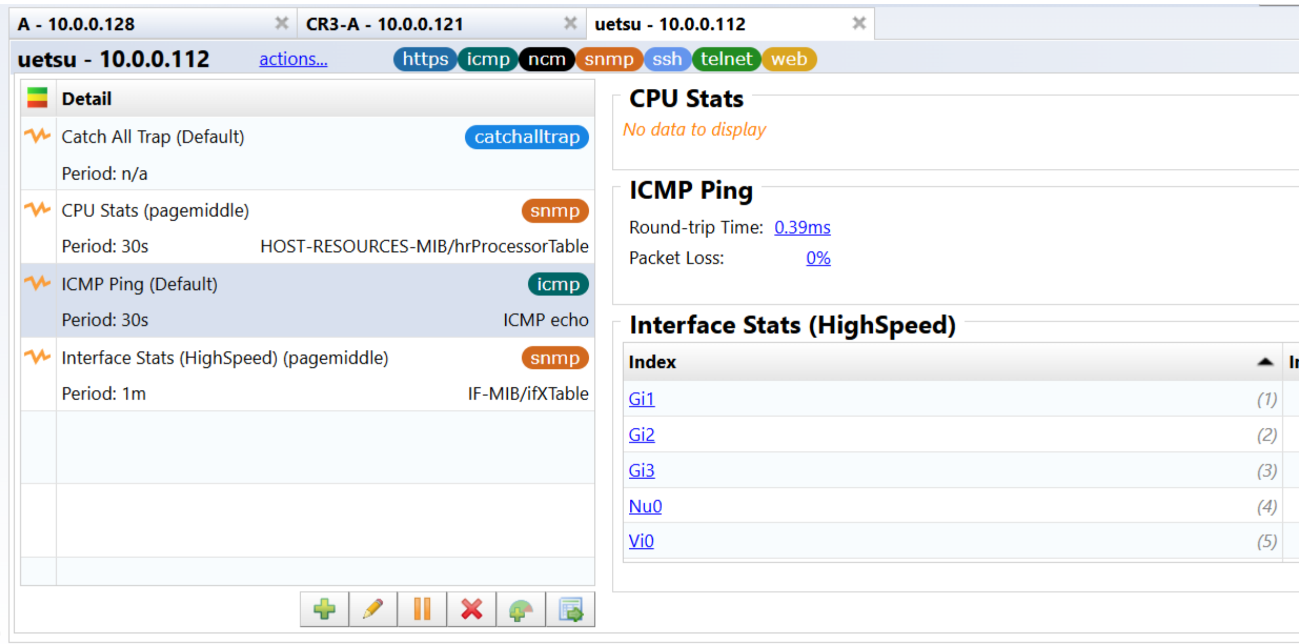
Round-trip Time: 0.55ms
Packet Loss: 0%

Last Captured: 2024/05/08 11:01

Interface Stats (HighSpeed)

Index		InOctets-derivative	OutOctets-derivative
Gi1	(1)	209485	11173
Gi2	(2)	78855	0

2. Select the monitor you want to delete from the monitor details and click the ☒ button at the bottom of the left sidepanel.



A - 10.0.0.128 | CR3-A - 10.0.0.121 | uetsu - 10.0.0.112

uetsu - 10.0.0.112 actions... https icmp ncm snmp ssh telnet web

Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
CPU Stats (pagemiddle)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Interface Stats (HighSpeed) (pagemiddle)	snmp
Period: 1m	IF-MIB/ifXTable

CPU Stats

No data to display

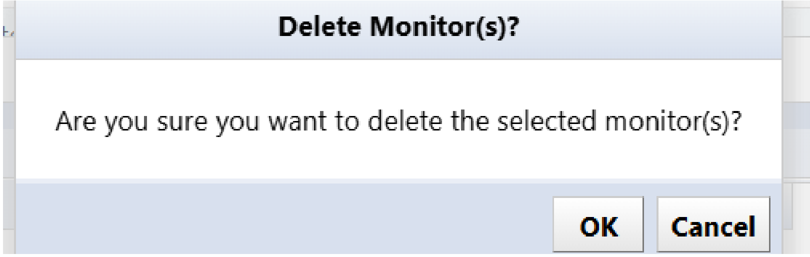
ICMP Ping

Round-trip Time: 0.39ms
Packet Loss: 0%

Interface Stats (HighSpeed)

Index	
Gi1	(1)
Gi2	(2)
Gi3	(3)
Nu0	(4)
Vi0	(5)

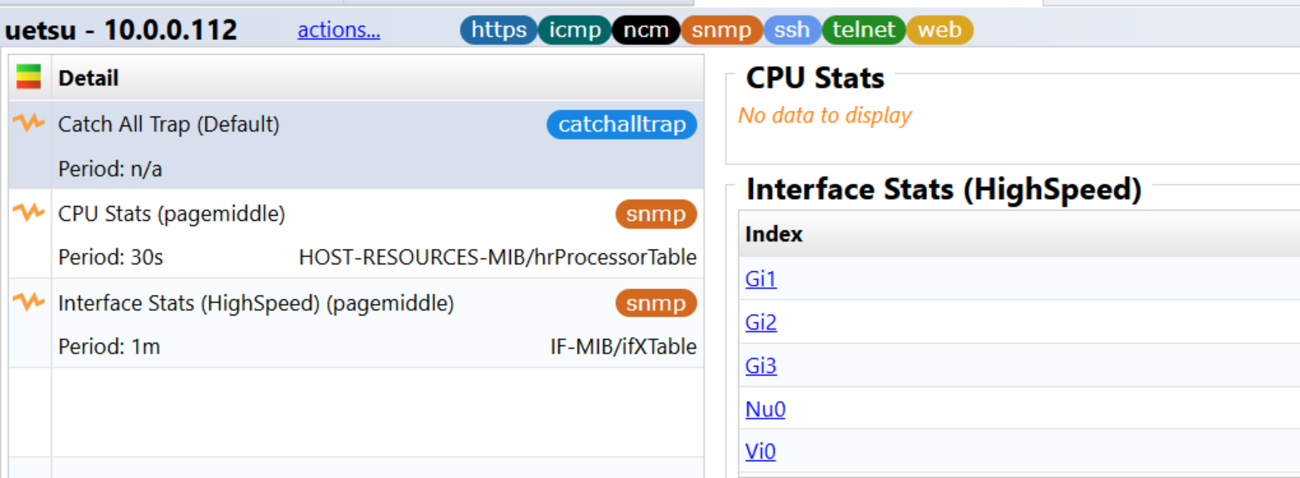
3. Click [OK] on the confirmation screen.



Delete Monitor(s)?

Are you sure you want to delete the selected monitor(s)?

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



uetsu - 10.0.0.112 actions...

Detail

Catch All Trap (Default) catchalltrap
Period: n/a

CPU Stats (pagemiddle) snmp
Period: 30s HOST-RESOURCES-MIB/hrProcessorTable

Interface Stats (HighSpeed) (pagemiddle) snmp
Period: 1m IF-MIB/ifXTable

CPU Stats

No data to display

Interface Stats (HighSpeed)

Index
Gi1
Gi2
Gi3
Nu0
Vi0

SECTION 16

PING MONITORING

Ping Monitoring is a method of checking if a device is reachable on a network by sending ICMP Echo Request packets and measuring response.

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.

16.1 Configure Ping Monitoring

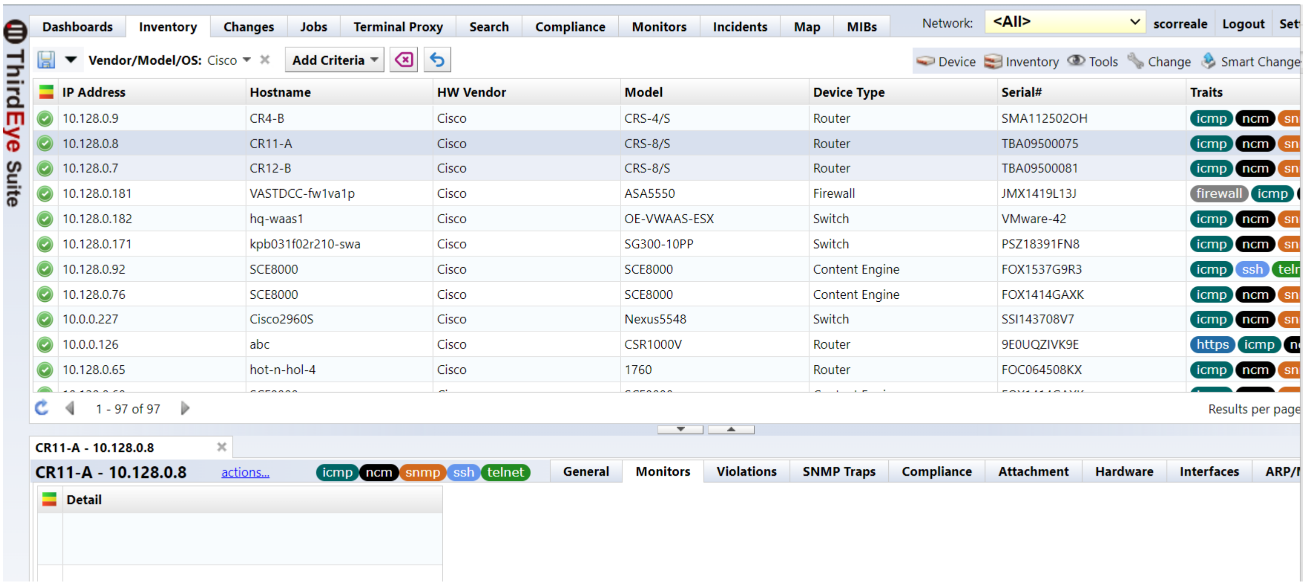
This section describes the steps to add a monitor with specific conditions to monitored devices.

Conditions:

Monitoring interval: 5 minutes

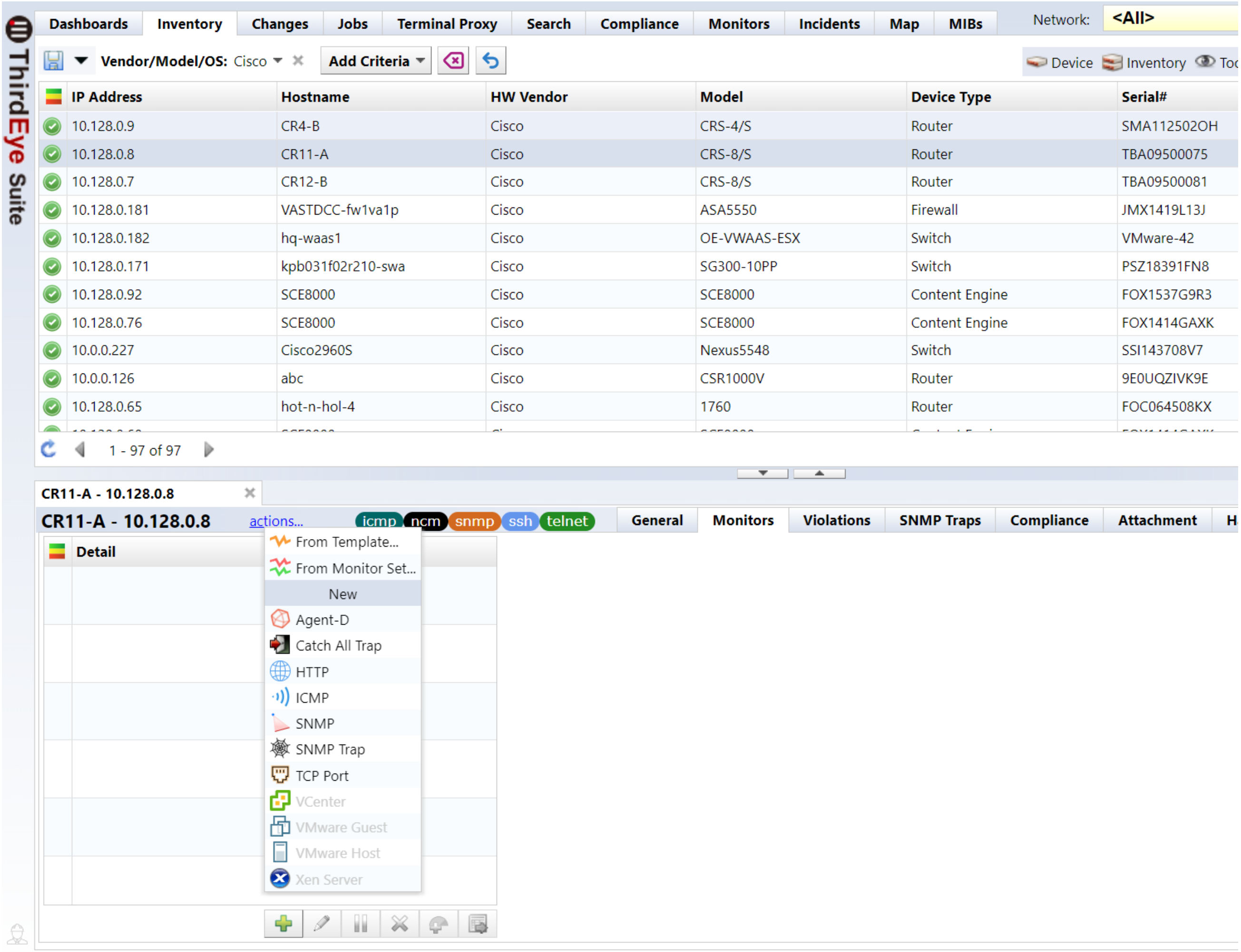
Alert condition: Twice in 10 minutes if there is no response.

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



IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.128.0.9	CR4-B	Cisco	CRS-4/S	Router	SMA112502OH	icmp ncm sn
10.128.0.8	CR11-A	Cisco	CRS-8/S	Router	TBA09500075	icmp ncm sn
10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	TBA09500081	icmp ncm sn
10.128.0.181	VASTDCC-fw1va1p	Cisco	ASA5550	Firewall	JMX1419L13J	firewall icmp
10.128.0.182	hq-waas1	Cisco	OE-VWAAS-ESX	Switch	VMware-42	icmp ncm sn
10.128.0.171	kpb031f02r210-swa	Cisco	SG300-10PP	Switch	PSZ18391FN8	icmp ncm sn
10.128.0.92	SCE8000	Cisco	SCE8000	Content Engine	FOX1537G9R3	icmp ssh teln
10.128.0.76	SCE8000	Cisco	SCE8000	Content Engine	FOX1414GAXK	icmp ncm sn
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7	icmp ncm sn
10.0.0.126	abc	Cisco	CSR1000V	Router	9E0UQZIVK9E	https icmp n
10.128.0.65	hot-n-hol-4	Cisco	1760	Router	FOC064508KX	icmp ncm sn

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



IP Address	Hostname	HW Vendor	Model	Device Type	Serial#
10.128.0.9	CR4-B	Cisco	CRS-4/S	Router	SMA112502OH
10.128.0.8	CR11-A	Cisco	CRS-8/S	Router	TBA09500075
10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	TBA09500081
10.128.0.181	VASTDCC-fw1va1p	Cisco	ASA5550	Firewall	JMX1419L13J
10.128.0.182	hq-waas1	Cisco	OE-VWAAS-ESX	Switch	VMware-42
10.128.0.171	kpb031f02r210-swa	Cisco	SG300-10PP	Switch	PSZ18391FN8
10.128.0.92	SCE8000	Cisco	SCE8000	Content Engine	FOX1537G9R3
10.128.0.76	SCE8000	Cisco	SCE8000	Content Engine	FOX1414GAXK
10.0.0.227	Cisco2960S	Cisco	Nexus5548	Switch	SSI143708V7
10.0.0.126	abc	Cisco	CSR1000V	Router	9E0UQZIVK9E
10.128.0.65	hot-n-hol-4	Cisco	1760	Router	FOC064508KX

1 - 97 of 97

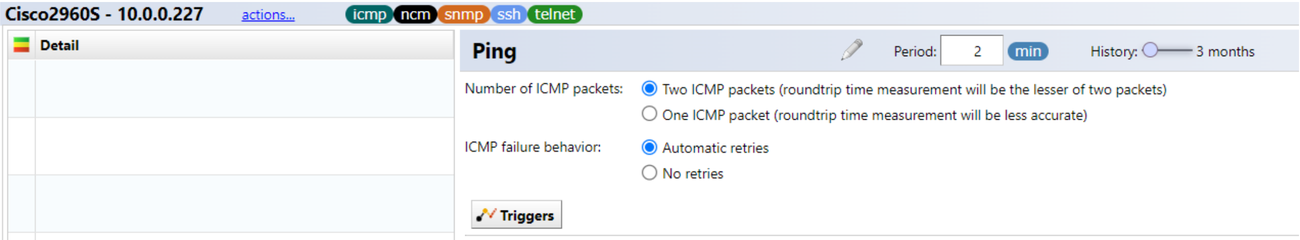
CR11-A - 10.128.0.8

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.



Cisco2960S - 10.0.0.227

Ping

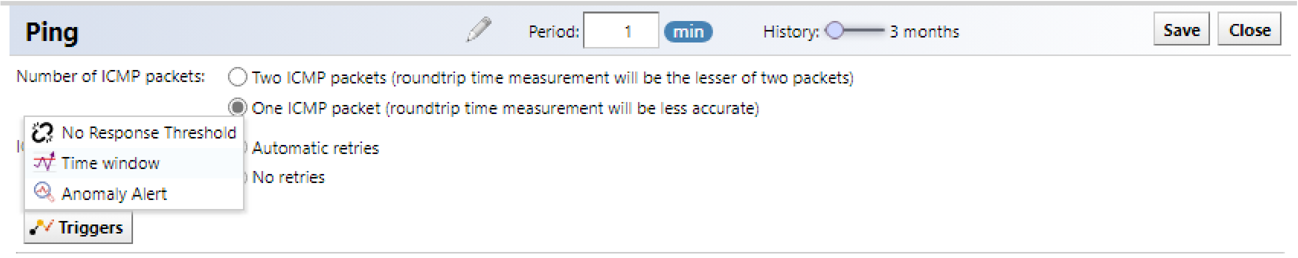
Period: 2 min

History: 3 months

Number of ICMP packets:
● Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
○ One ICMP packet (roundtrip time measurement will be less accurate)

ICMP failure behavior:
● Automatic retries
○ No retries

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



Ping

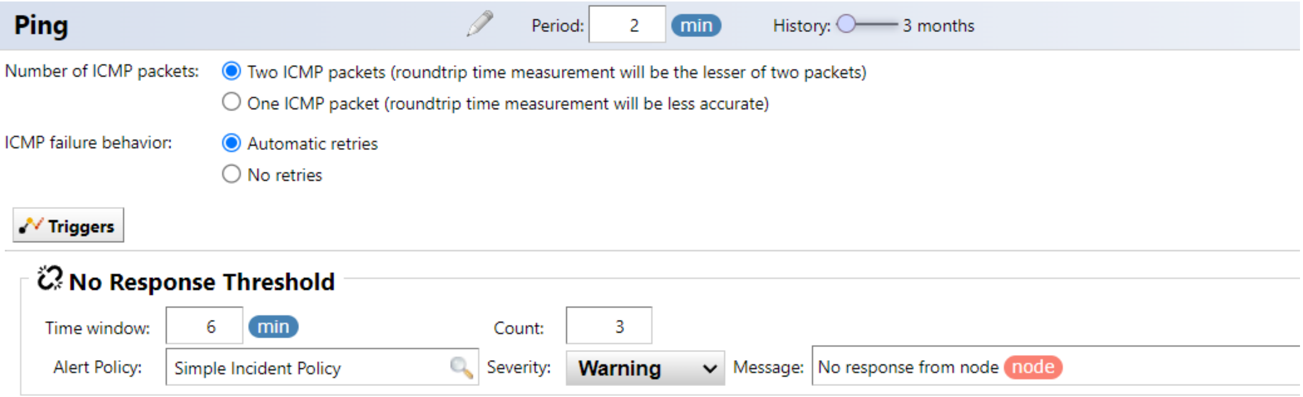
Period: 1 min

History: 3 months

Number of ICMP packets:
○ Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
● One ICMP packet (roundtrip time measurement will be less accurate)

Automatic retries
No retries

8. Configure the following items:



Ping

Period: 2 min

History: 3 months

Number of ICMP packets:
● Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
○ One ICMP packet (roundtrip time measurement will be less accurate)

ICMP failure behavior:
● Automatic retries
○ No retries

No Response Threshold

Time window: 6 min

Count: 3

Alert Policy: Simple Incident Policy

Severity: Warning

Message: No response from node node

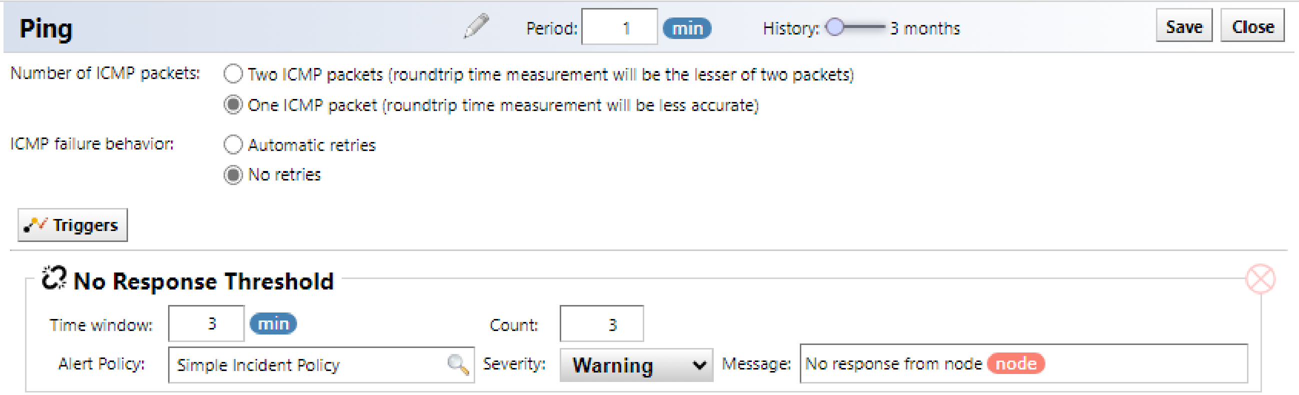
Monitor Setting	Explanation
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process 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**	❗

Security level	Status	Severity status icon
	warning	!
	notification	ⓘ
	information	ⓘ
Low	**debug**	●

9. Click [Save].



Period: 1 min

History: 3 months

Number of ICMP packets:
○ Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
● One ICMP packet (roundtrip time measurement will be less accurate)

ICMP failure behavior:
○ Automatic retries
● No retries

No Response Threshold

Time window: 3 min

Count: 3

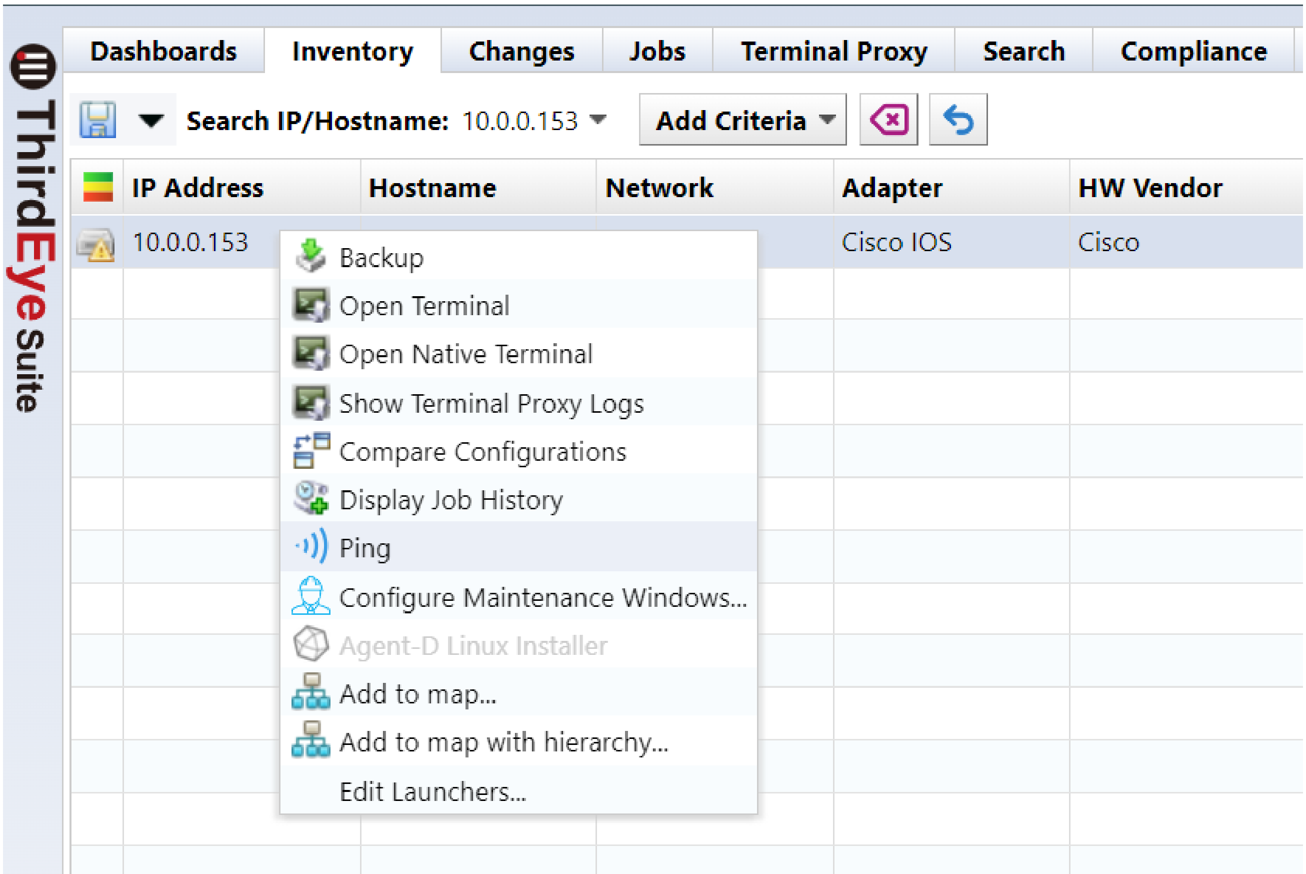
Alert Policy: Simple Incident Policy

Severity: Warning

Message: No response from node node

16.2 Real-Time Ping

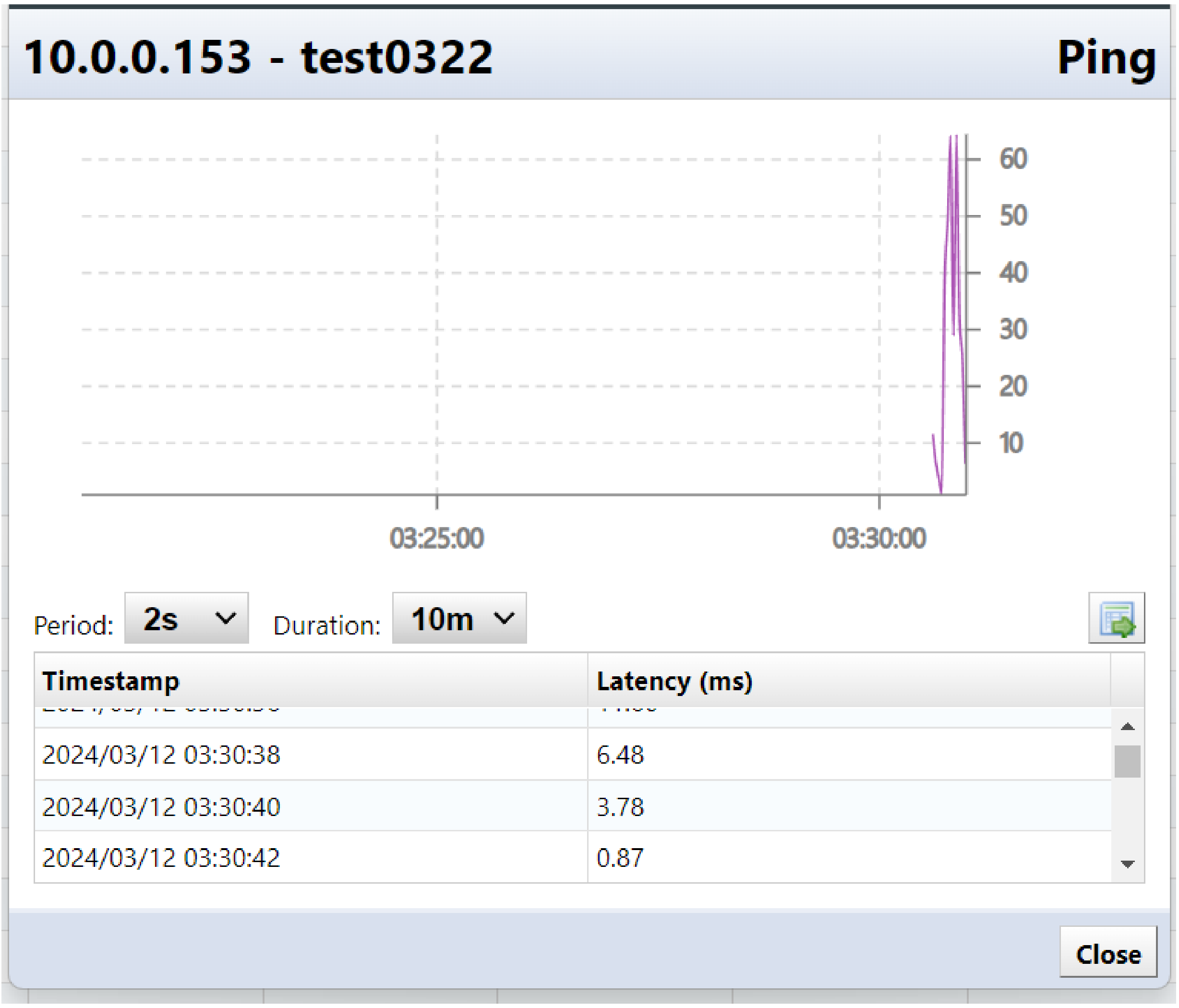
You can ping a monitored device from the device list or map from the right-click menu. The transmission interval is 2 seconds at startup, but you can change it from the screen that appears after executing Ping.



Search IP/Hostname: 10.0.0.153

IP Address	Hostname	Network	Adapter	HW Vendor
10.0.0.153			Cisco IOS	Cisco

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



Period: 2s

Duration: 10m

Timestamp	Latency (ms)
2024/03/12 03:30:38	6.48
2024/03/12 03:30:40	3.78
2024/03/12 03:30:42	0.87

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

16.3 ICMP Polling

ICMP polling is a network monitoring technique that uses ICMP (Internet Control Message Protocol) packets to check device availability and measure response times. The system uses the fastest response time from the packet batch for monitoring.

ThirdEye's ICMP monitoring system provides essential network availability tracking through optimized ping-based checks. It features configurable polling intervals (30s-5min,) and adaptive retry logic that automatically performs up to additional checks with dynamically calculated intervals when packet loss occurs. Key characteristics include:

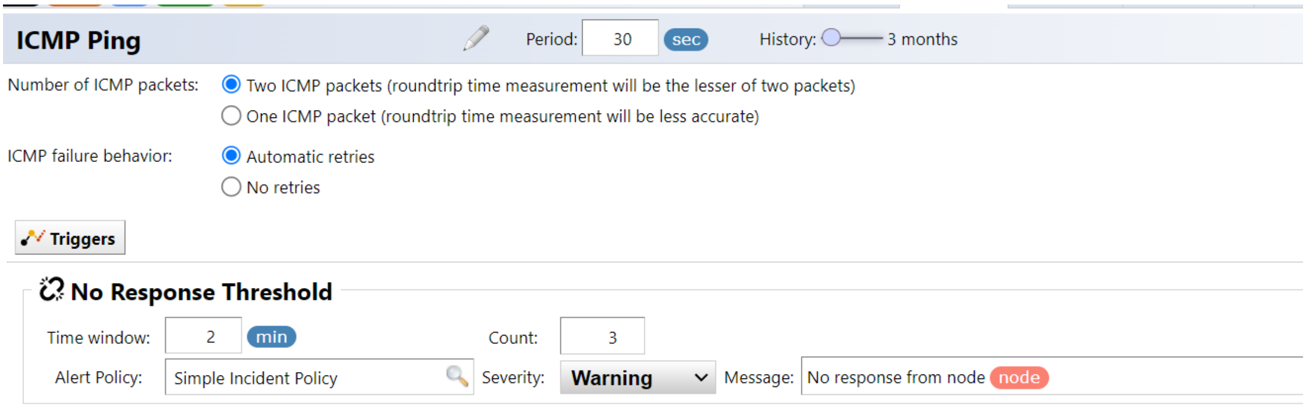
- **Dual-Packet Metrics**: Sends 1-2 ICMP packets per cycle, recording the fastest response time
- **Smart Retry System**: Auto-retries with geometrically increasing intervals during failures
- **Zero-Config Defaults**: Auto-assigns "ICMP Ping (Default)" monitor to new devices with immediate activation
- **Conditional Alerting**: Supports thresholds for consecutive failures and RTT limits

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:



ICMP Ping Period: 30 sec History: 3 months

Number of ICMP packets: ● Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
○ One ICMP packet (roundtrip time measurement will be less accurate)

ICMP failure behavior: ● Automatic retries
○ No retries

No Response Threshold

Time window: 2 min Count: 3

Alert Policy: Simple Incident Policy Severity: Warning Message: No response from node node

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**

16.3.1 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.

16.3.2 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:

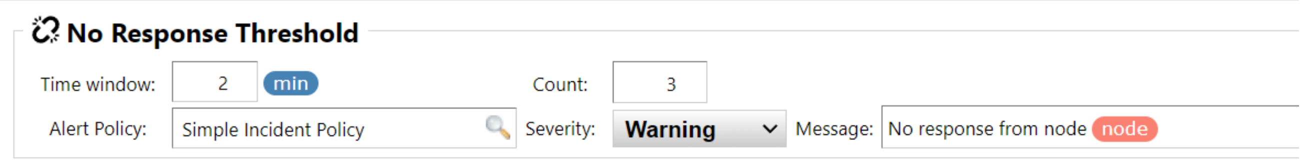
Theoretical value: 30 seconds (2+5.2*5+2) if the interval is set to 30 seconds.

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



No Response Threshold

Time window: 2 min

Count: 3

Alert Policy: Simple Incident Policy

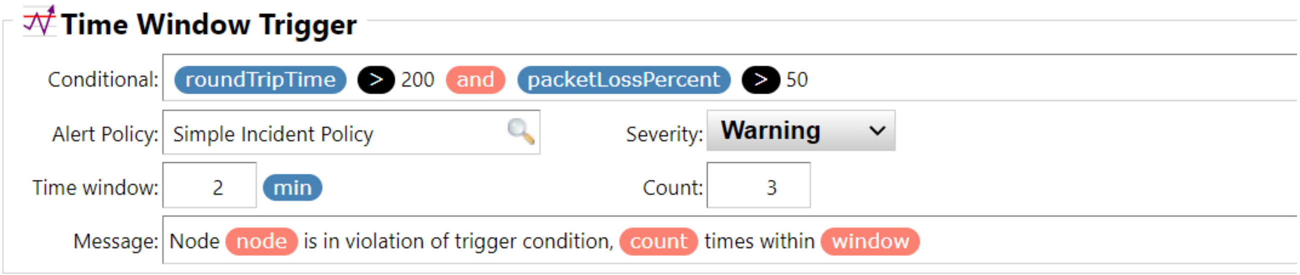
Severity: Warning

Message: No response from node node

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



Time Window Trigger

Conditional: roundTripTime > 200 and packetLossPercent > 50

Alert Policy: Simple Incident Policy

Severity: Warning

Time window: 2 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

SECTION 17

AGENT-D MONITORING

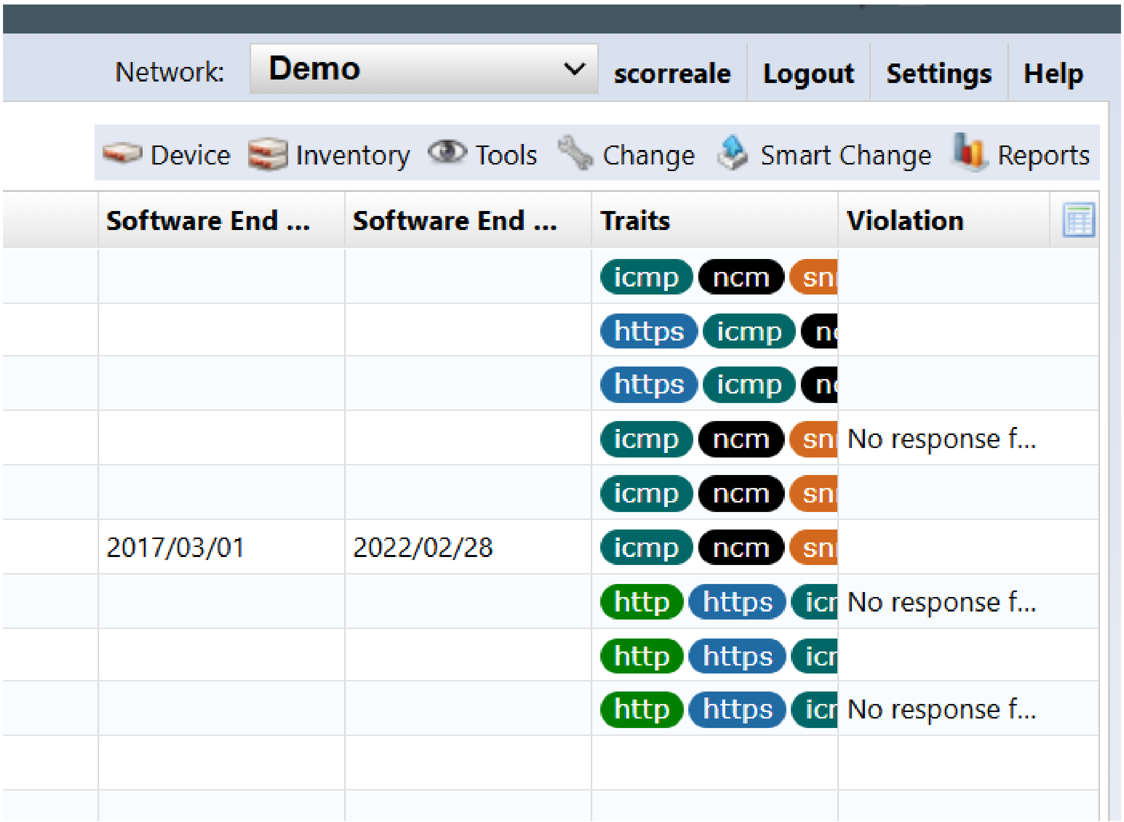
Agent-D is a server monitoring daemon for ThirdEye. By installing Agent-D on a Windows or Linux-based OS, you can monitor the server's CPU, memory, logs, etc.

Compared to traditional SNMP agents, Agent-D allows you to bulk distribute (install) on monitored devices, reducing installation time and simplifying management when there are many targets to be monitored.

17.1 Install on Linux

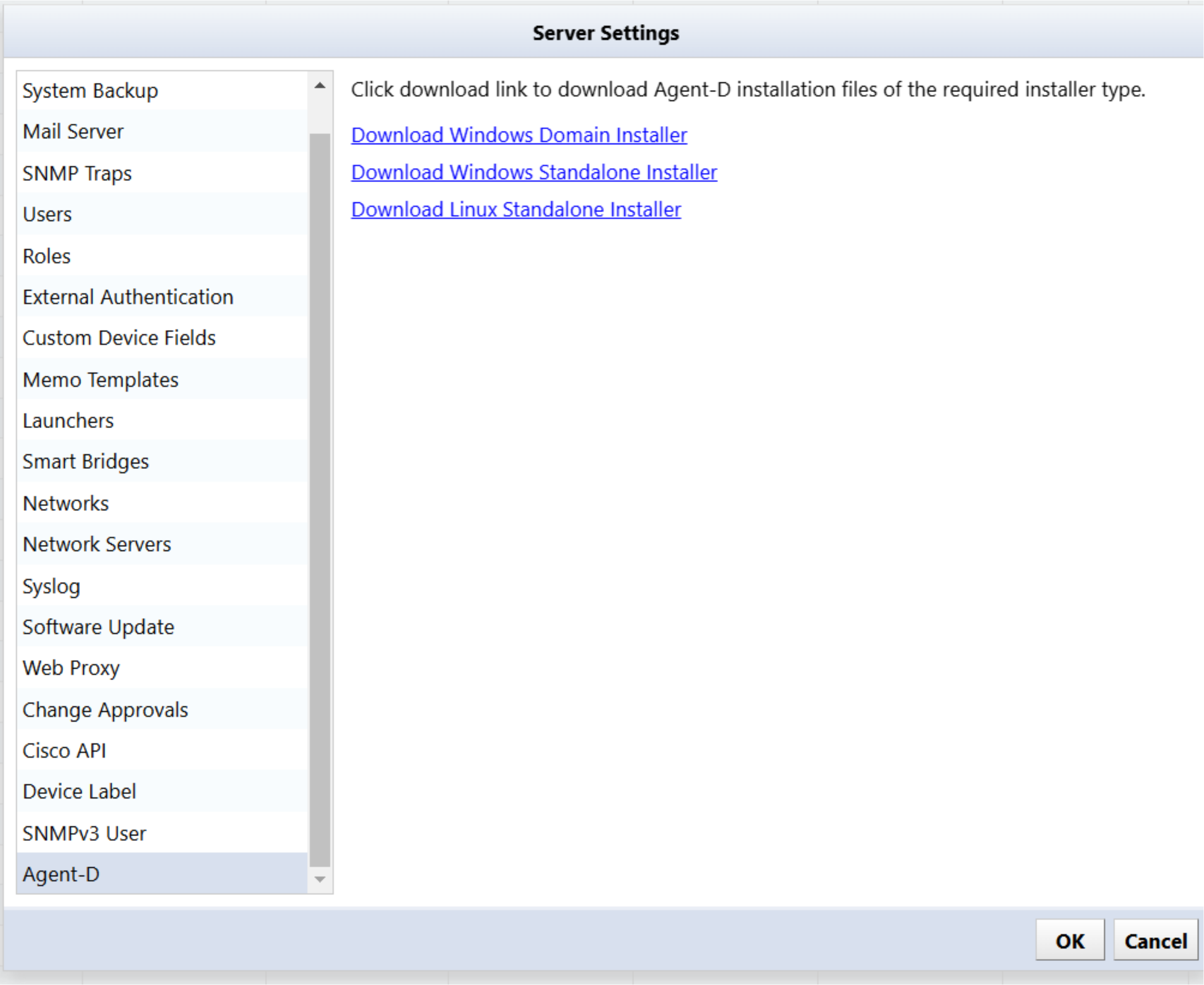
Download the installer from ThirdEye and install it on any Linux. Supported OS are RedHat Linux 7/8, CentOS 7/8, and Ubuntu.

1. Click [Settings] on the Global Menu.



	Software End ...	Software End ...	Traits	Violation
			icmp ncm sn	
			https icmp nc	
			https icmp nc	
			icmp ncm sn	No response f...
			icmp ncm sn	
	2017/03/01	2022/02/28	icmp ncm sn	
			http https icr	No response f...
			http https icr	
			http https icr	No response f...

2. Click [Agent-D] and the left sidepanel, then click [Download Linux Standalone Installer].



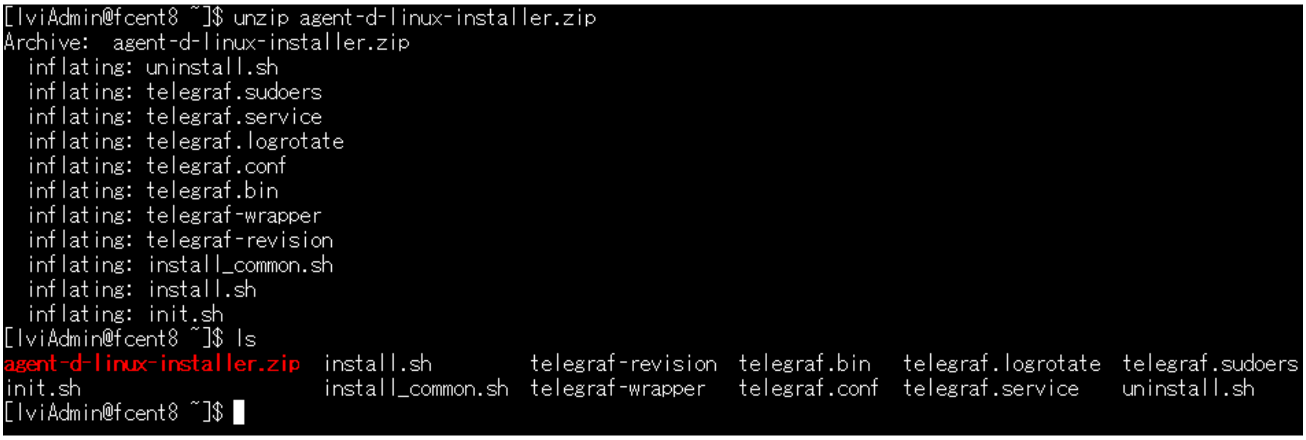
Click download link to download Agent-D installation files of the required installer type.

Download Windows Domain Installer

Download Windows Standalone Installer

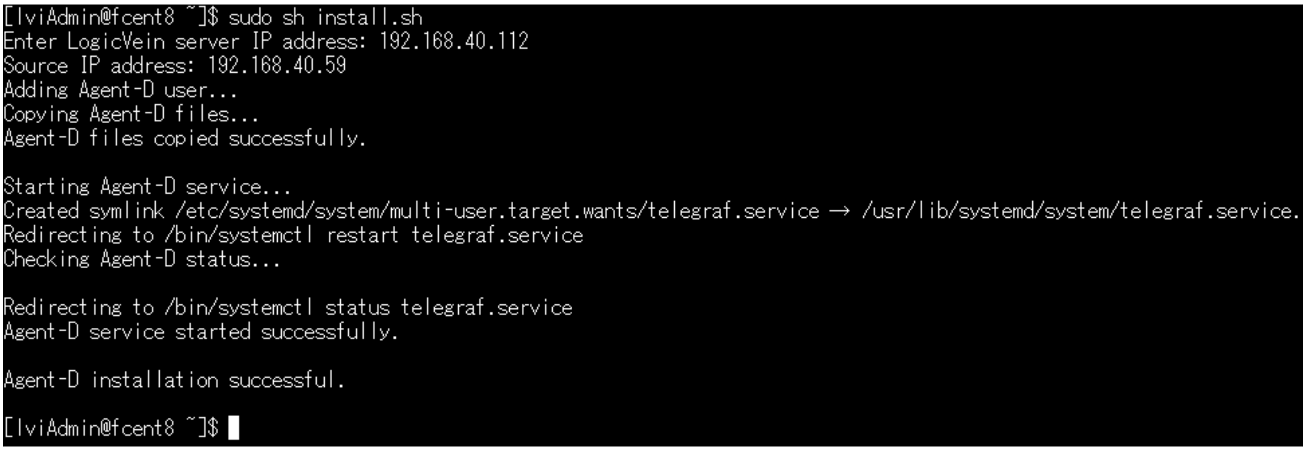
Download Linux Standalone Installer

3. Copy the downloaded file to the installation destination Linux server.
4. Unzip the downloaded file using the unzip command.



```
[lviAdmin@fcent8 ~]$ unzip agent-d-linux-installer.zip
Archive:  agent-d-linux-installer.zip
  inflating: uninstall.sh
  inflating: telegraf.sudoers
  inflating: telegraf.service
  inflating: telegraf.logrotate
  inflating: telegraf.conf
  inflating: telegraf.bin
  inflating: telegraf-wrapper
  inflating: telegraf-revision
  inflating: install_common.sh
  inflating: install.sh
  inflating: init.sh
[lviAdmin@fcent8 ~]$ ls
agent-d-linux-installer.zip  install.sh         telegraf-revision  telegraf.bin   telegraf.logrotate  telegraf.sudoers
init.sh                      install_common.sh  telegraf-wrapper   telegraf.conf  telegraf.service    uninstall.sh
[lviAdmin@fcent8 ~]$
```

5. Run `install.sh`.



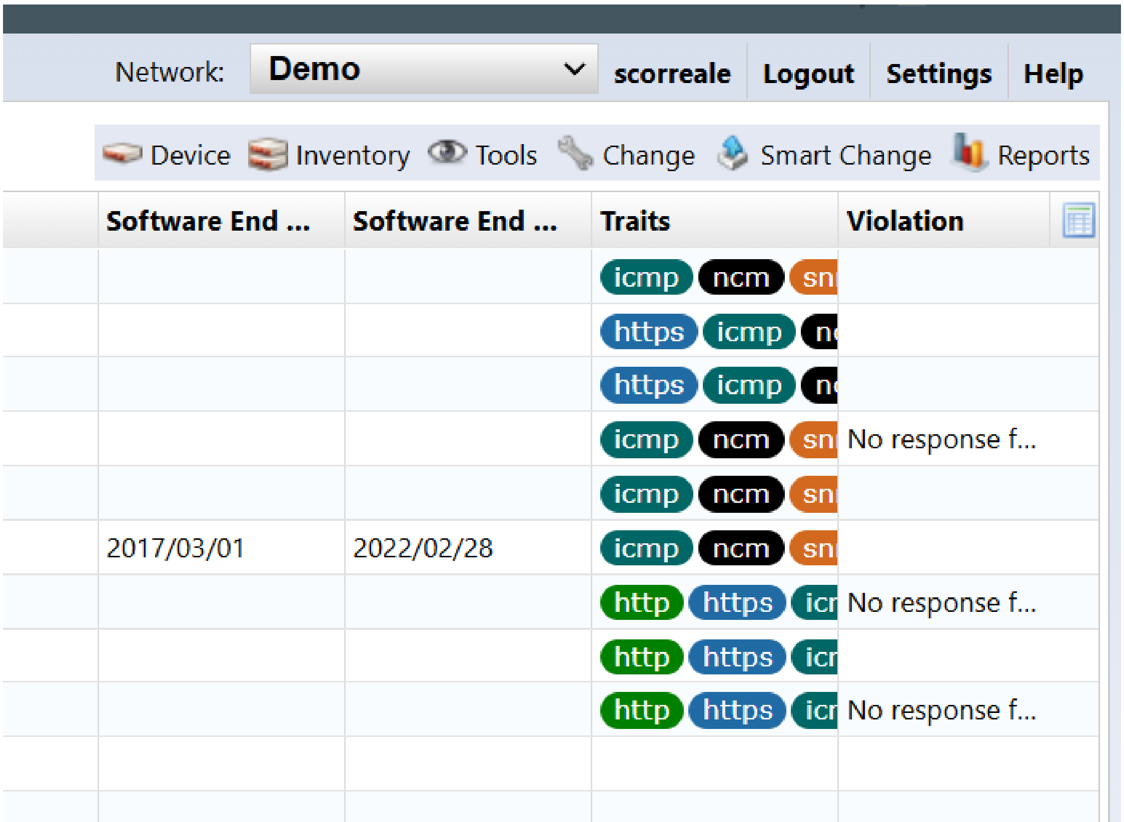
```
[lviAdmin@fcent8 ~]$ sudo sh install.sh
Enter LogicVein server IP address: 192.168.40.112
Source IP address: 192.168.40.59
Adding Agent-D user...
Copying Agent-D files...
Agent-D files copied successfully.

Starting Agent-D service...
Created symlink /etc/systemd/system/multi-user.target.wants/telegraf.service → /usr/lib/systemd/system/telegraf.service.
Redirecting to /bin/systemctl restart telegraf.service
Checking Agent-D status...

Redirecting to /bin/systemctl status telegraf.service
Agent-D service started successfully.

Agent-D installation successful.

[lviAdmin@fcent8 ~]$
```

6. Enter ThirdEye’s IP address and press the [Enter] key.

17.2 Install on Windows

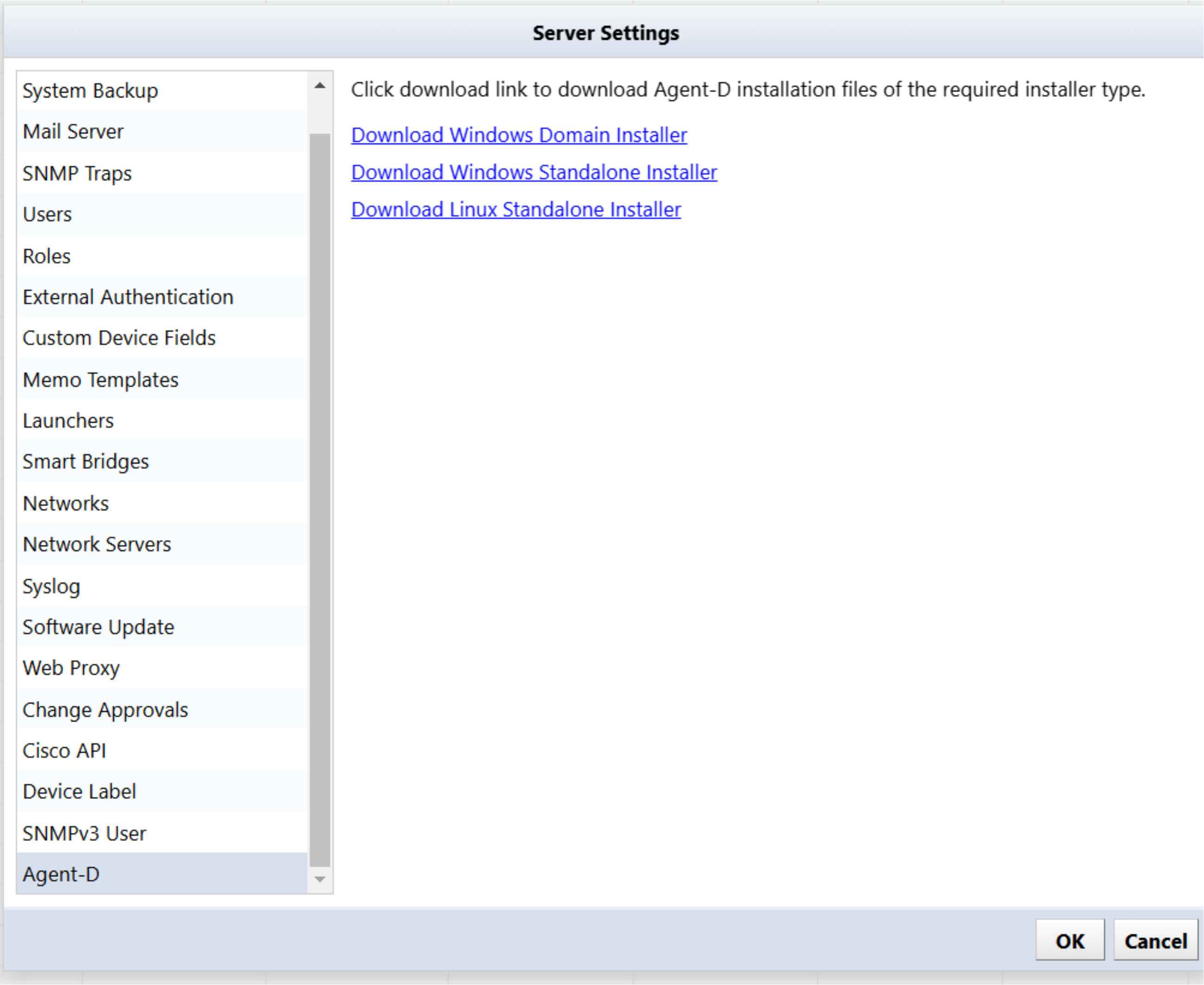
Download the installer from ThirdEye and install it on any Windows server. Windows OS Server versions 2016, 2019, and 2022 are supported.

1. Click [Settings] on the Global Menu.



	Software End ...	Software End ...	Traits	Violation
			icmp ncm sn	
			https icmp n	
			https icmp n	
			icmp ncm sn	No response f...
			icmp ncm sn	
	2017/03/01	2022/02/28	icmp ncm sn	
			http https icr	No response f...
			http https icr	
			http https icr	No response f...

2. Click [Agent-D] in the left sidebar, then click [Download Windows Standalone Installer].



Server Settings

Click download link to download Agent-D installation files of the required installer type.

Download Windows Domain Installer

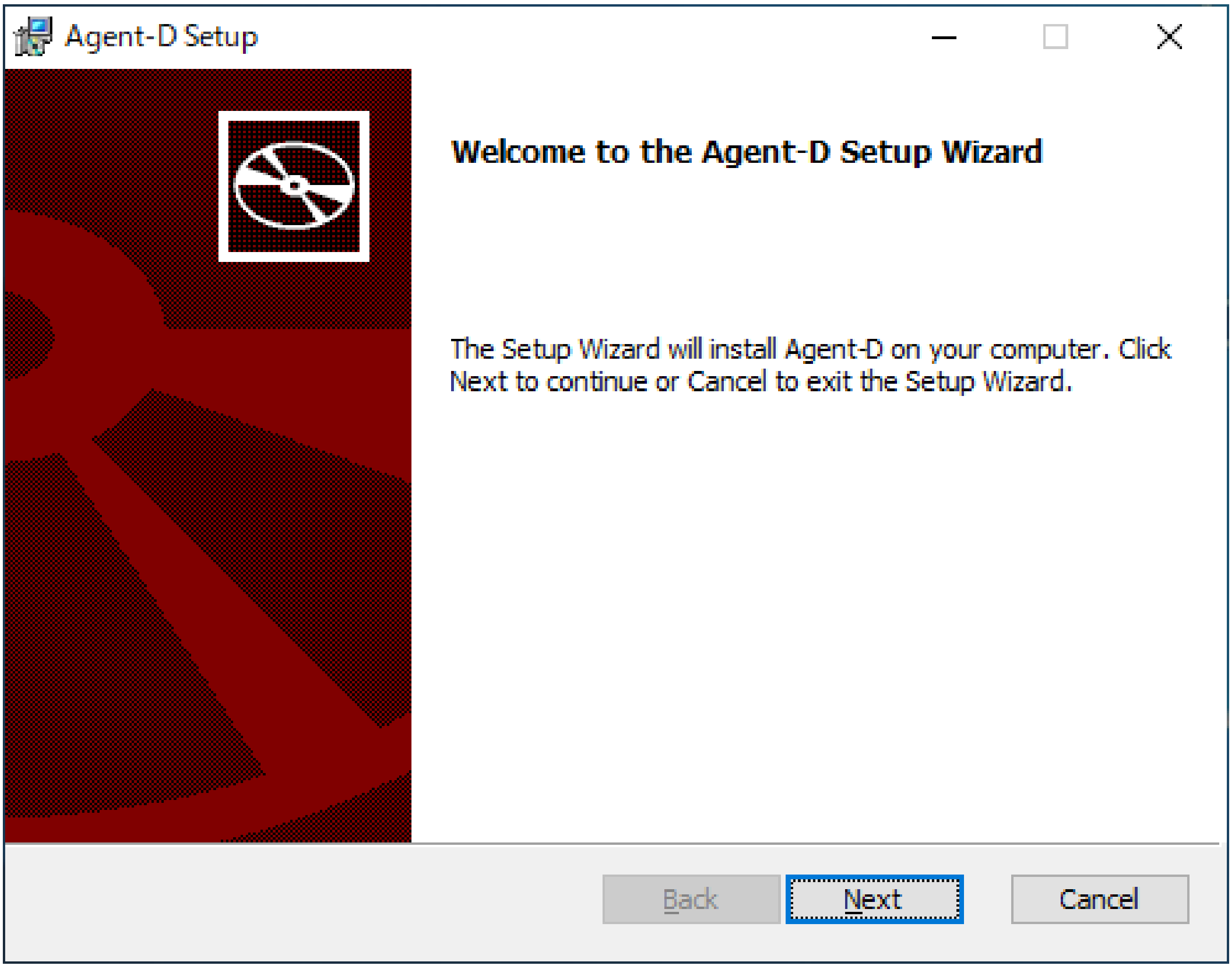
Download Windows Standalone Installer

Download Linux 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].

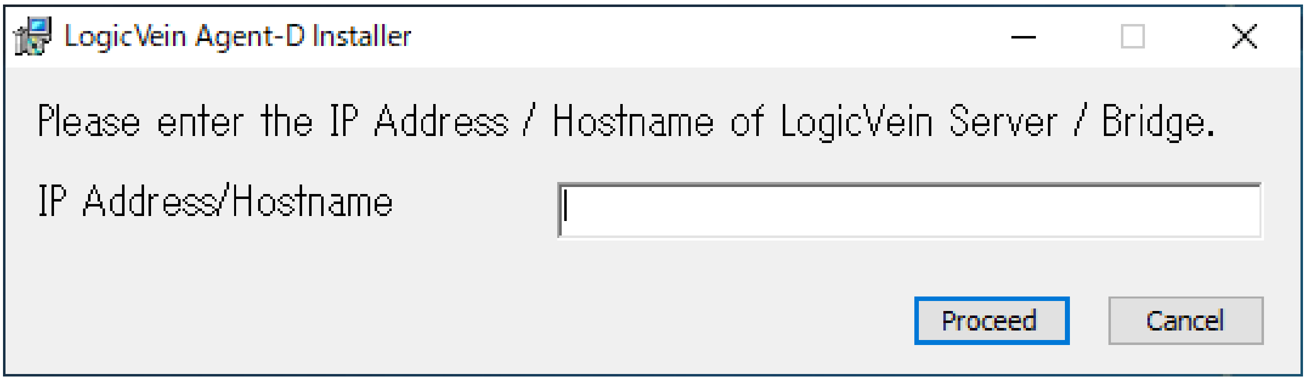


Agent-D Setup

Welcome to the Agent-D Setup Wizard

The Setup Wizard will install Agent-D on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

6. Enter ThirdEye's IP address or hostname and click [Proceed].

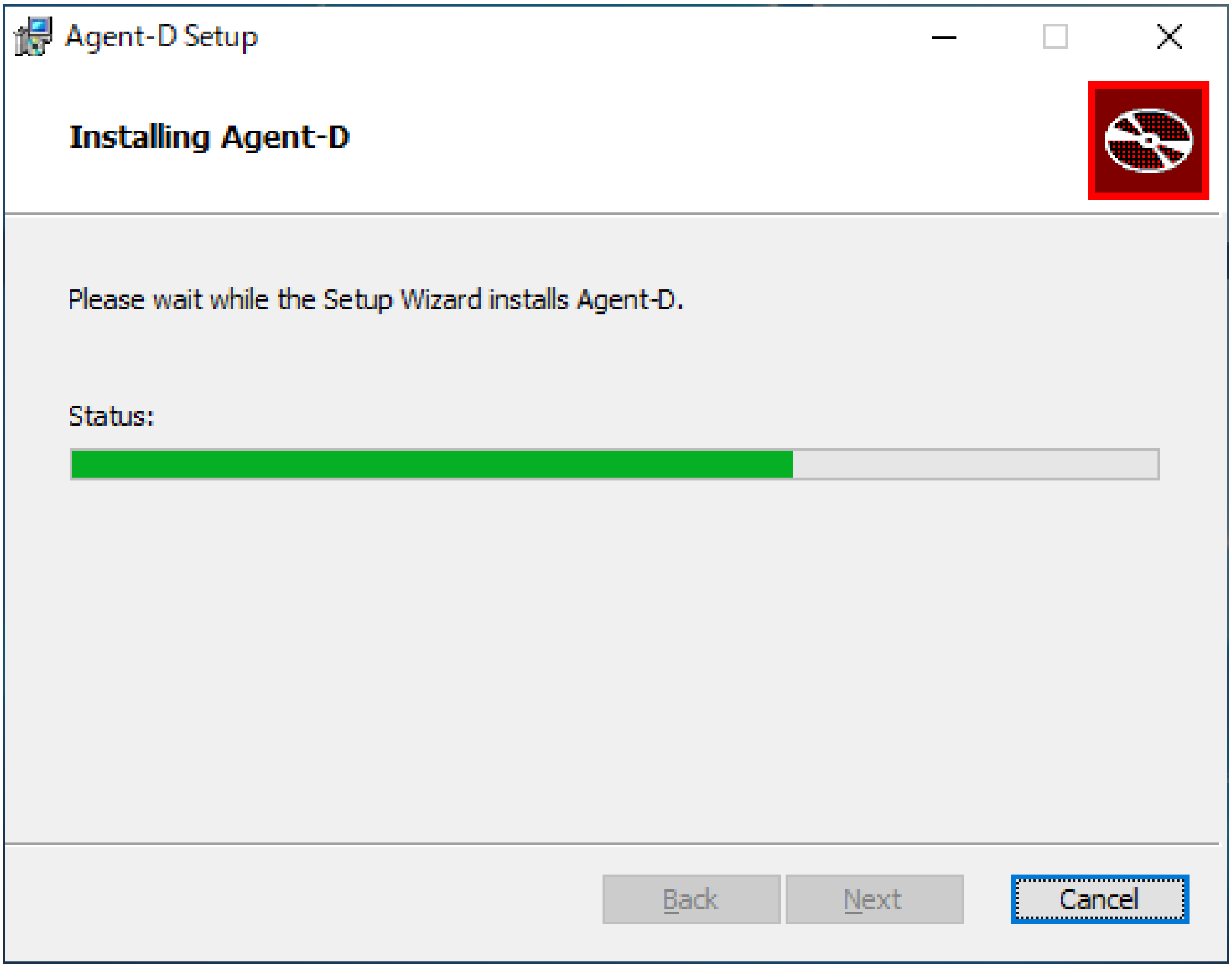


LogicVein Agent-D Installer

Please enter the IP Address / Hostname of LogicVein Server / Bridge.

IP Address/Hostname

Installation will begin.



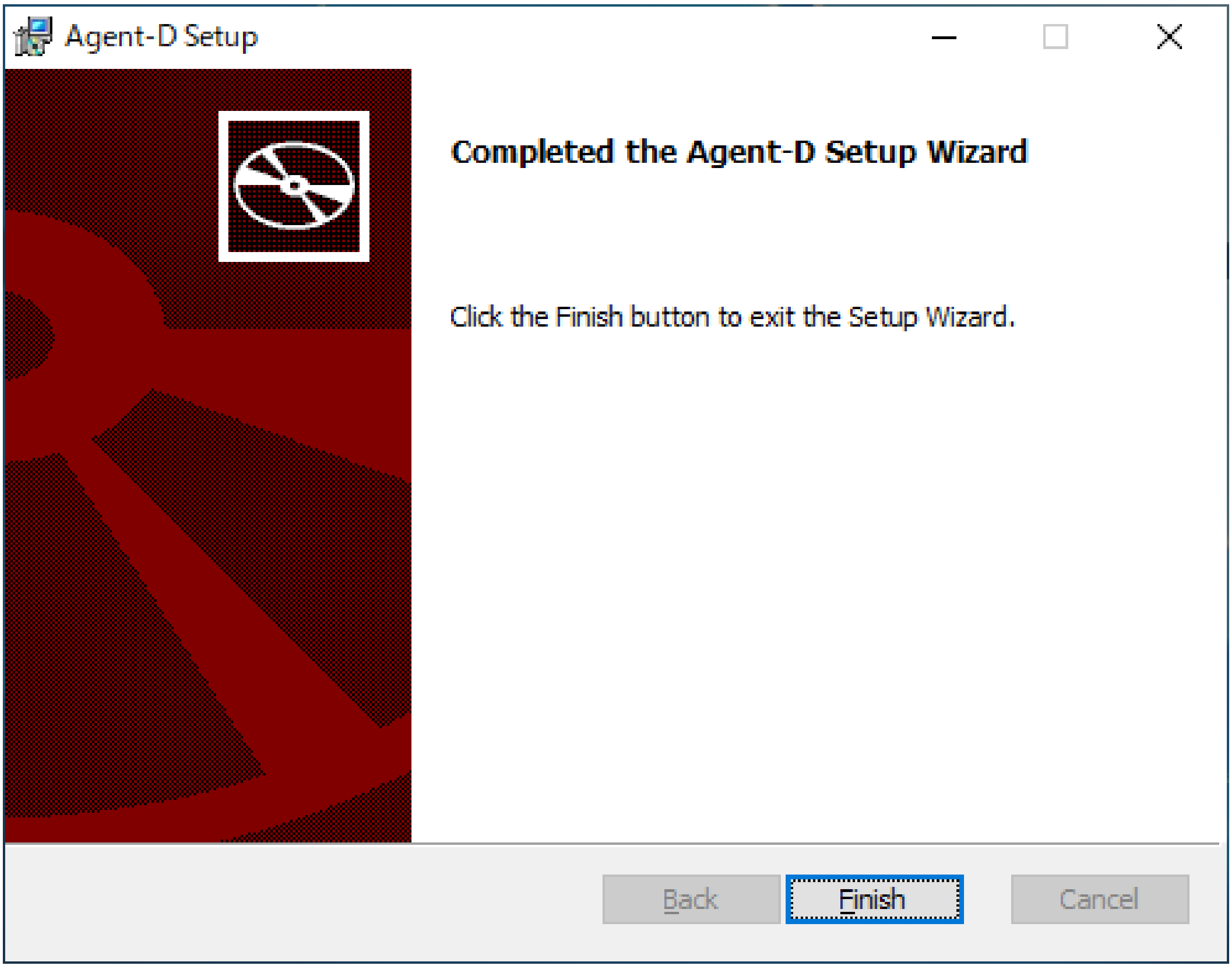
Agent-D Setup

Installing Agent-D

Please wait while the Setup Wizard installs Agent-D.

Status:

7. Click [Finish].



Completed the Agent-D Setup Wizard

Click the Finish button to exit the Setup Wizard.

17.3 Windows service monitoring

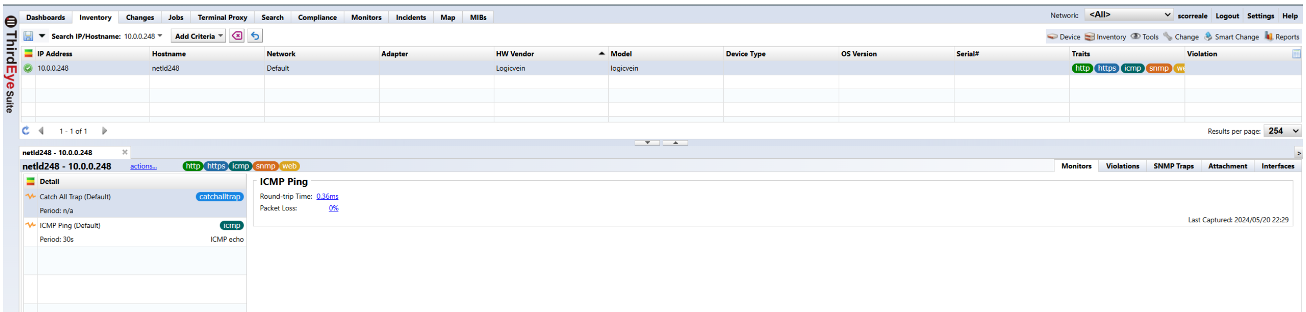
Use Agent-D to obtain information about Windows services on the installed Windows server. By setting thresholds for service status, you can issue an alert when the threshold is exceeded.

The following templates are registered in advance as monitors for HDD monitoring on the [Monitors] > [Templates] tab.

17.3.1 Windows Service Status

The 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.



Search IP/Hostname: 10.0.0.248

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Traits	Violation
10.0.0.248	netld248	Default		Logicvein	logicvein				http https icmp snmp we	

1 - 1 of 1

Results per page: 254

netld248 - 10.0.0.248

netld248 - 10.0.0.248 http https icmp snmp web

Detail

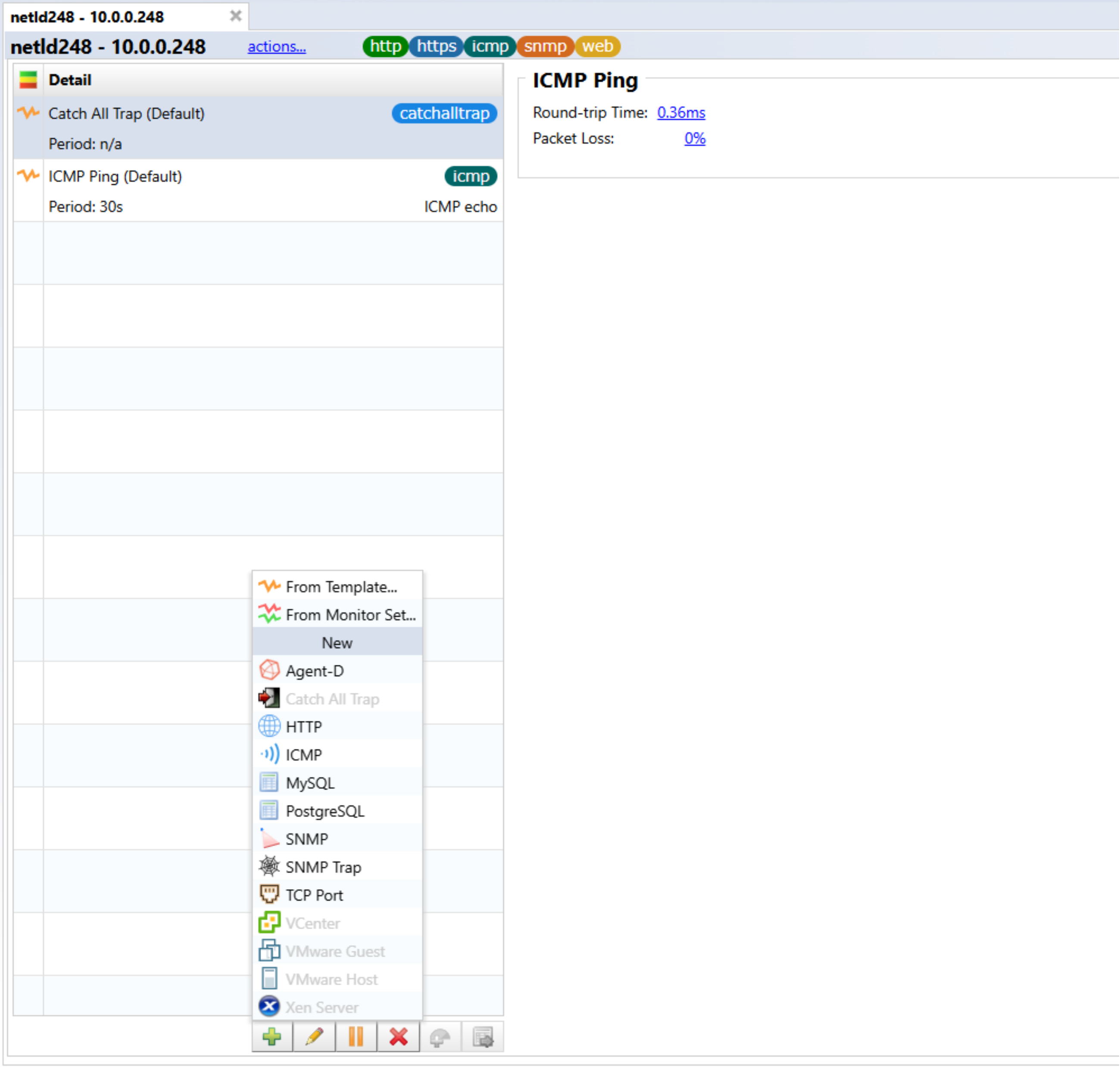
Catch All Trap (Default) catchalltrap
Period: n/a

ICMP Ping (Default) icmp
Period: 30s ICMP echo

ICMP Ping
Round-trip Time: 0.36ms
Packet Loss: 0%

Last Captured: 2024/05/20 22:29

2. Click the ✚ button, then click [Agent-D].



Catch All Trap (Default)
Period: n/a

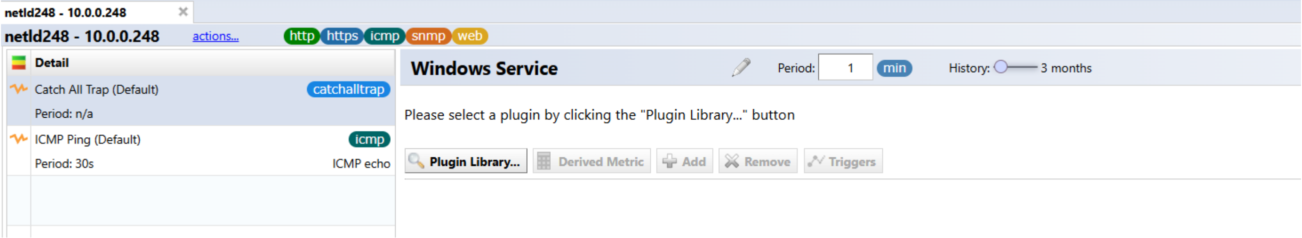
ICMP Ping (Default)
Period: 30s ICMP echo

ICMP Ping
Round-trip Time: 0.36ms
Packet Loss: 0%

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.



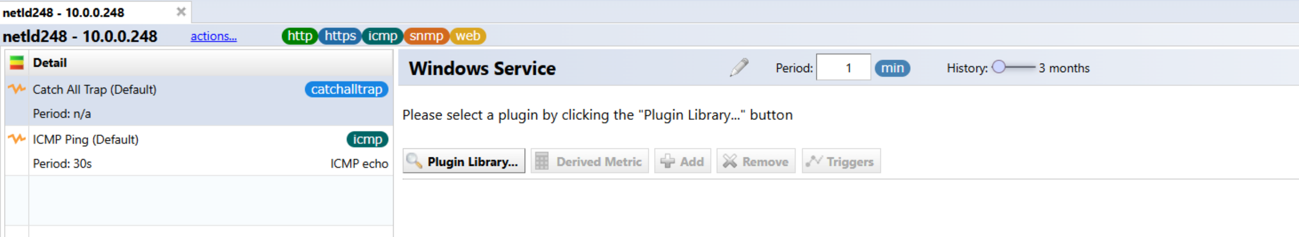
Catch All Trap (Default)
Period: n/a

ICMP Ping (Default)
Period: 30s ICMP echo

Windows Service
Period: 1 min
History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

4. Click [Plugin Library…].

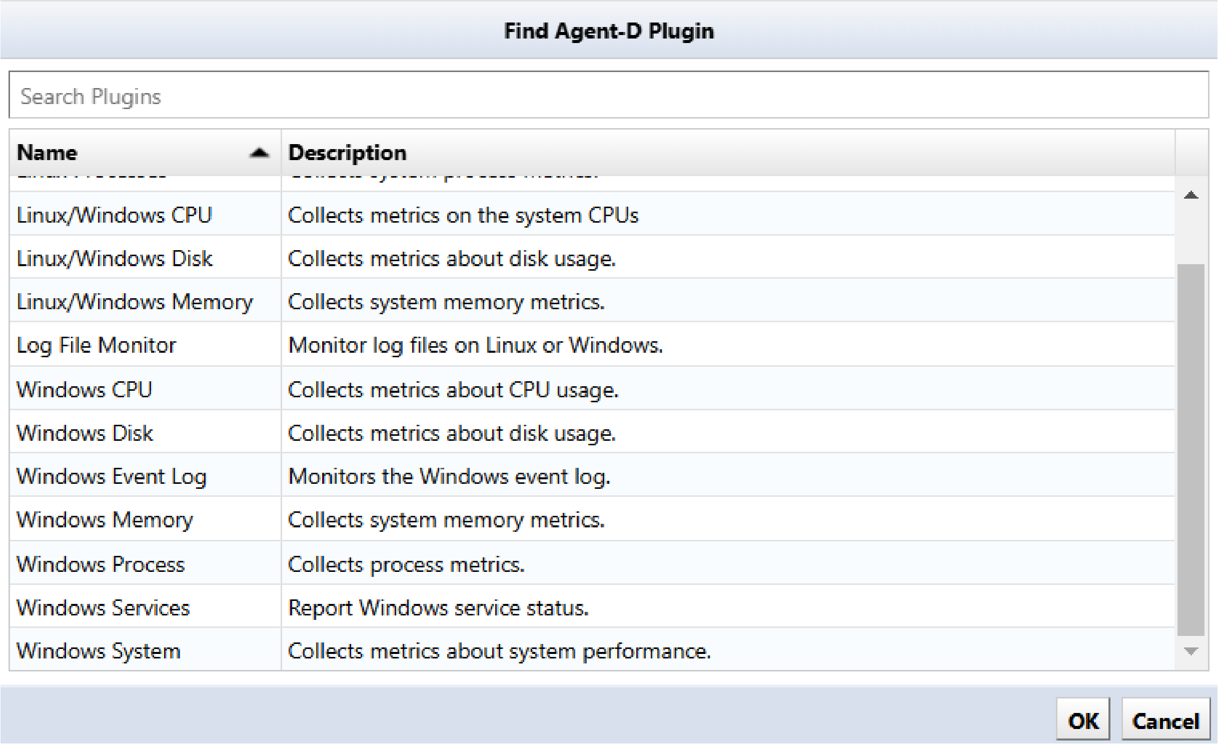


Period: 1 min

History: 3 months

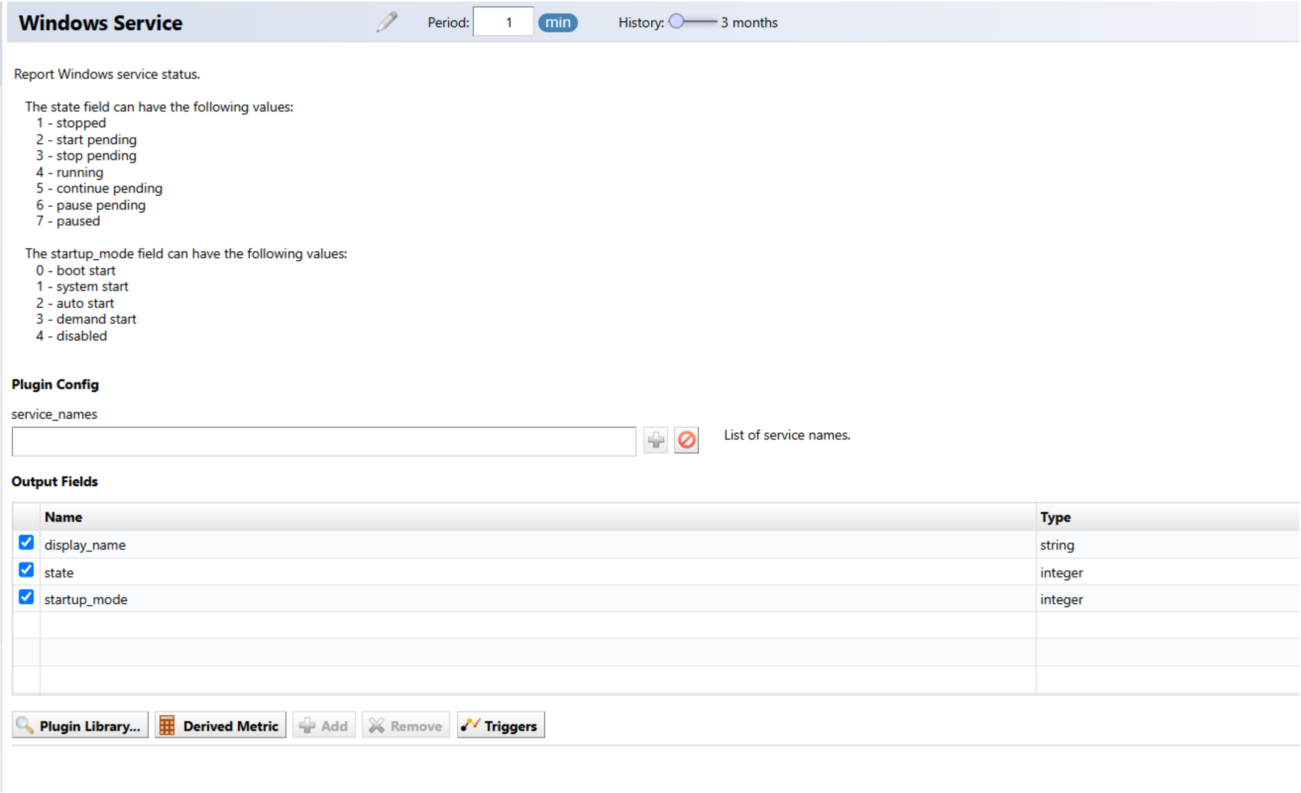
Please select a plugin by clicking the "Plugin Library..." button

5. Select [Windows Services] and click [OK].



Name	Description
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.
Windows Services	Report Windows service status.
Windows System	Collects metrics about system performance.

6. Add the service name to be monitored by entering it in the [service_names] field. The Service name is not uppercase and lowercase sensitive.



Report Windows service status.

The state field can have the following values:
1 - stopped
2 - start pending
3 - stop pending
4 - running
5 - continue pending
6 - pause pending
7 - paused

The startup_mode field can have the following values:
0 - boot start
1 - system start
2 - auto start
3 - demand start
4 - disabled

Plugin Config

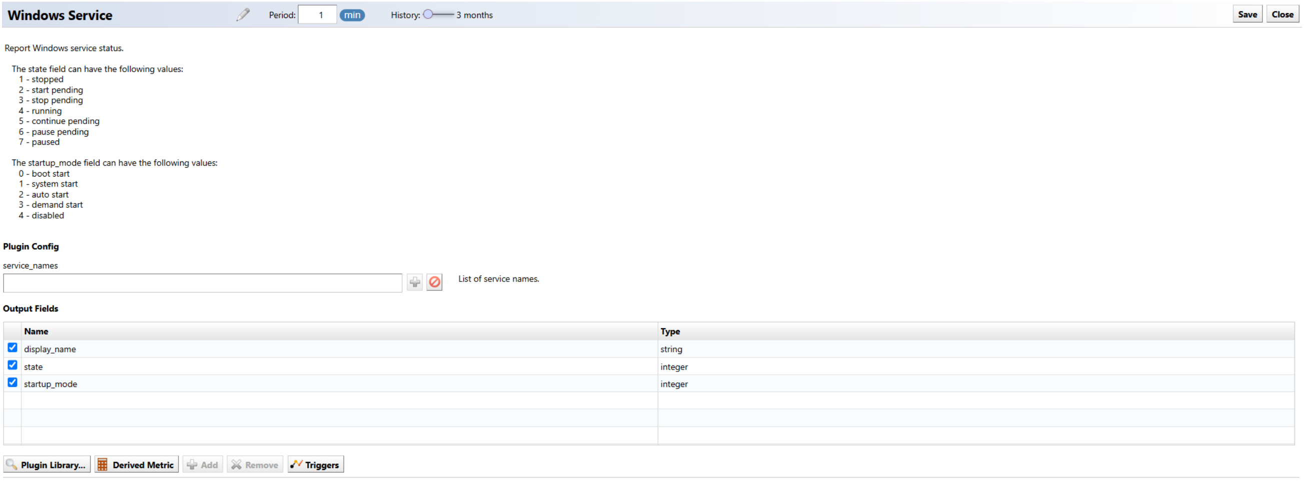
service_names

List of service names.

Output Fields

	Name	Type
☑	display_name	string
☑	state	integer
☑	startup_mode	integer

7. Check the items you want to obtain in [Output Fields] and click [Save].



Report Windows service status.

The state field can have the following values:
1 - stopped
2 - start pending
3 - stop pending
4 - running
5 - continue pending
6 - pause pending
7 - paused

The startup_mode field can have the following values:
0 - boot start
1 - system start
2 - auto start
3 - demand start
4 - disabled

Plugin Config

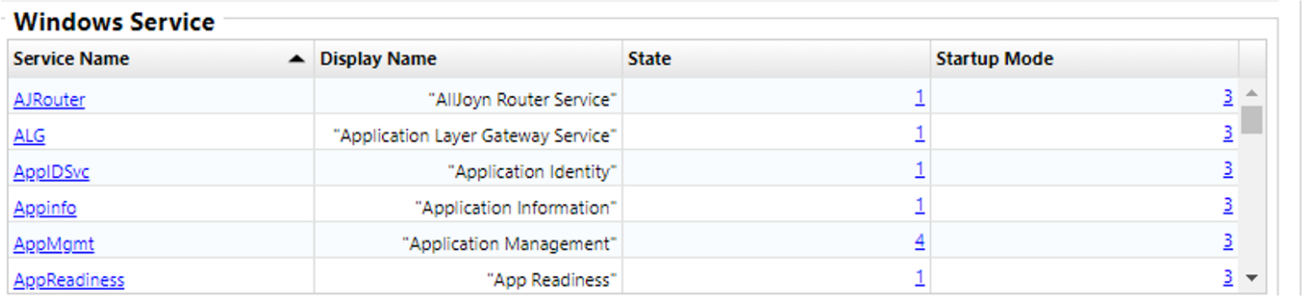
service_names

List of service names.

Output Fields

	Name	Type
☑	display_name	string
☑	state	integer
☑	startup_mode	integer

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

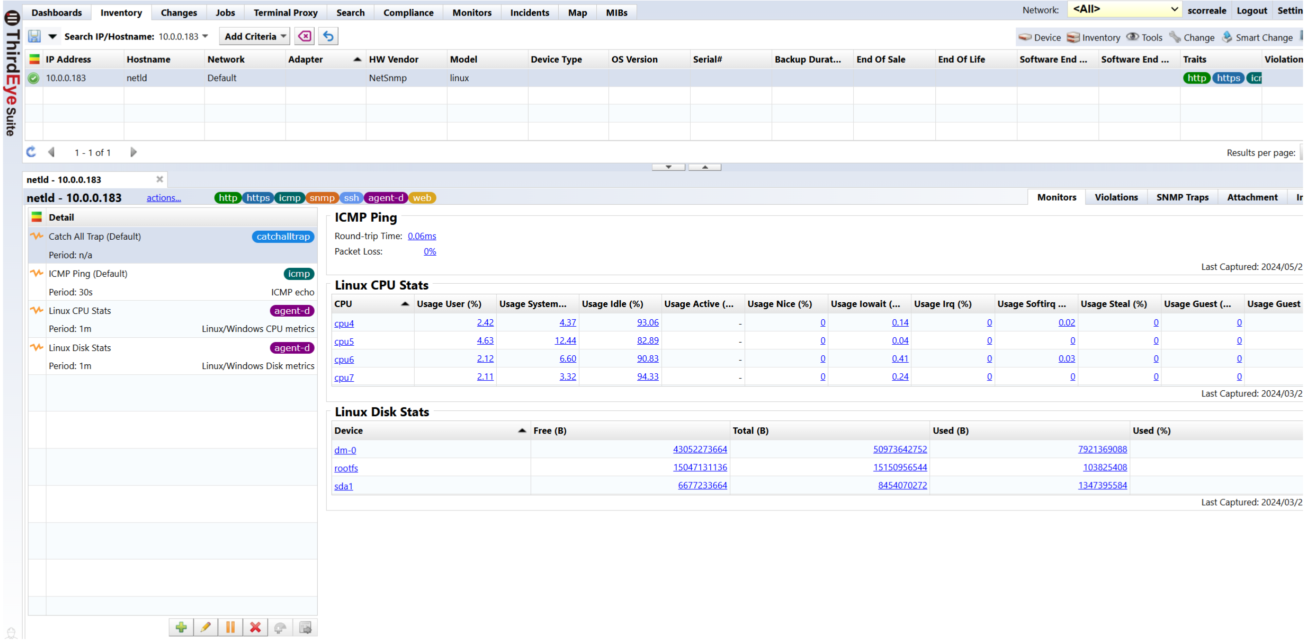
17.4 Windows Event Log Monitoring

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.



Search IP/Hostname: 10.0.0.183

	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
✓	10.0.0.183	netld	Default		NetSnmp	linux									http https icr	

1 - 1 of 1

netld - 10.0.0.183

netld - 10.0.0.183 http https icmp snmp ssh agent-d web

	Detail	
	Catch All Trap (Default) Period: n/a	catchalltrap
	ICMP Ping (Default) Period: 30s	icmp ICMP echo
	Linux CPU Stats Period: 1m	agent-d Linux/Windows CPU metrics
	Linux Disk Stats Period: 1m	agent-d Linux/Windows Disk metrics

ICMP Ping

Round-trip Time: 0.06ms

Packet Loss: 0%

Last Captured: 2024/05/2

Linux CPU Stats

CPU	Usage User (%)	Usage System...	Usage Idle (%)	Usage Active (...	Usage Nice (%)	Usage Iowait (...	Usage Irq (%)	Usage Softirq ...	Usage Steal (%)	Usage Guest (...	Usage Guest
cpu4	2.42	4.37	93.06	-	0	0.14	0	0.02	0	0	
cpu5	4.63	12.44	82.89	-	0	0.04	0	0	0	0	
cpu6	2.12	6.60	90.83	-	0	0.41	0	0.03	0	0	
cpu7	2.11	3.32	94.33	-	0	0.24	0	0	0	0	

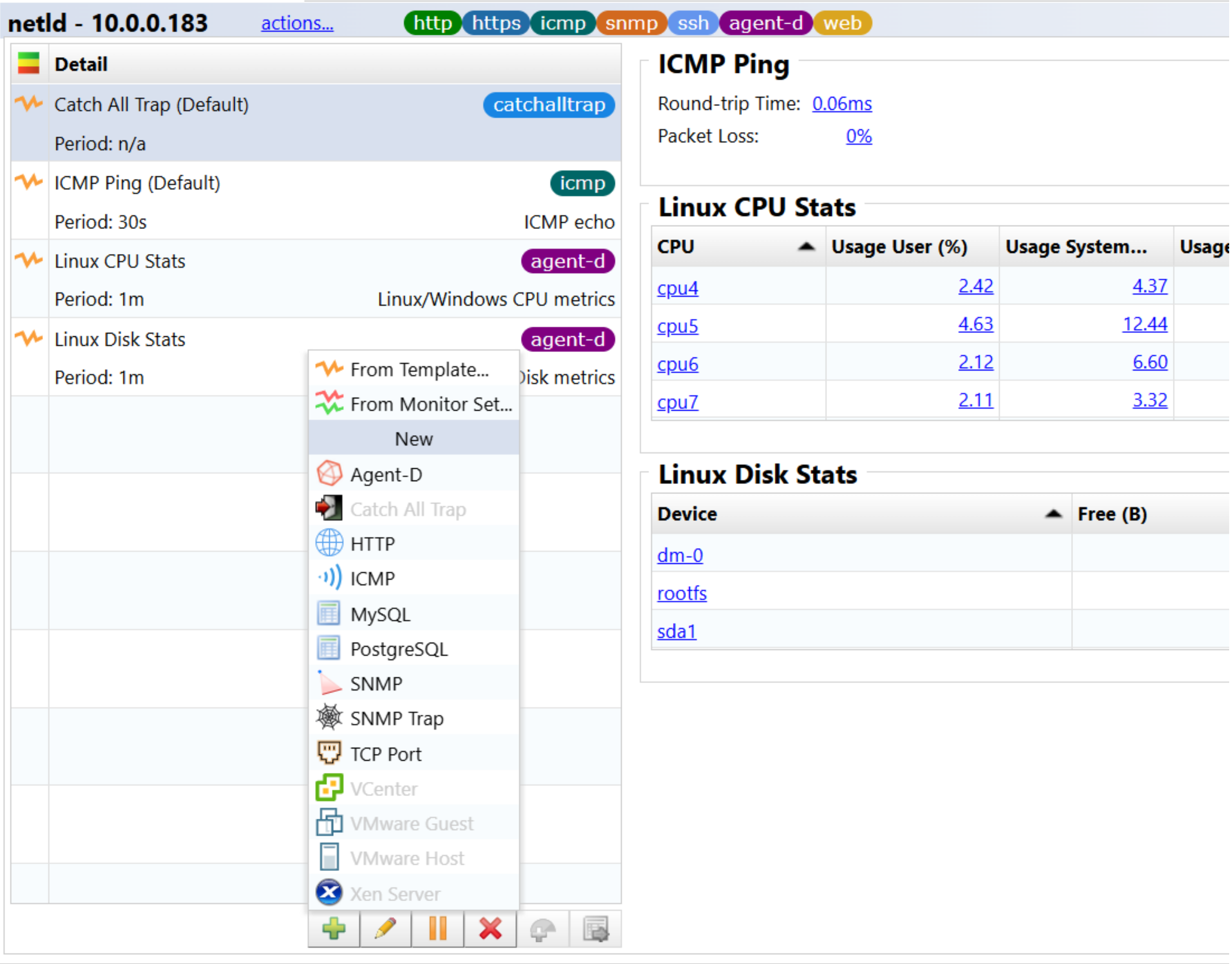
Last Captured: 2024/03/2

Linux Disk Stats

Device	Free (B)	Total (B)	Used (B)	Used (%)
dm-0	43052273664	50973642752	7921369088	
rootfs	15047131136	15150956544	103825408	
sda1	6677233664	8454070272	1347395584	

Last Captured: 2024/03/2

2. Click the ➕ button, then click [Agent-D].



netld - 10.0.0.183 actions...

Detail

Catch All Trap (Default) catchalltrap
Period: n/a

ICMP Ping (Default) icmp
Period: 30s ICMP echo

Linux CPU Stats agent-d
Period: 1m Linux/Windows CPU metrics

Linux Disk Stats agent-d
Period: 1m Disk metrics

ICMP Ping

Round-trip Time: 0.06ms
Packet Loss: 0%

Linux CPU Stats

CPU	Usage User (%)	Usage System...	Usage
cpu4	2.42	4.37	
cpu5	4.63	12.44	
cpu6	2.12	6.60	
cpu7	2.11	3.32	

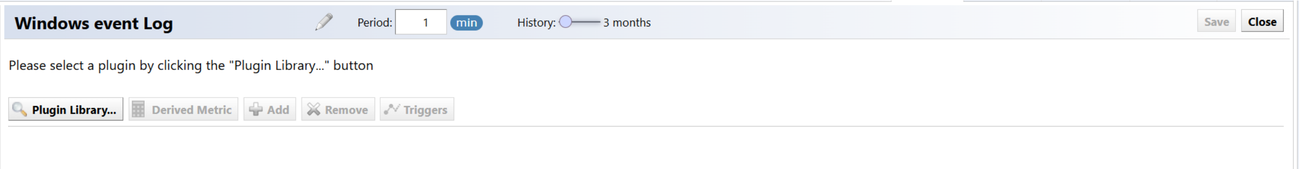
Linux Disk Stats

Device	Free (B)
dm-0	
rootfs	
sda1	

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

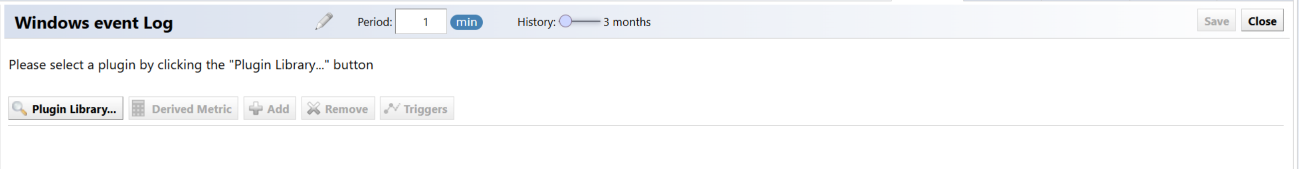
The [History] slider specifies a data retention period of 3, 6, or 12 months.



Windows event Log Period: 1 min History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

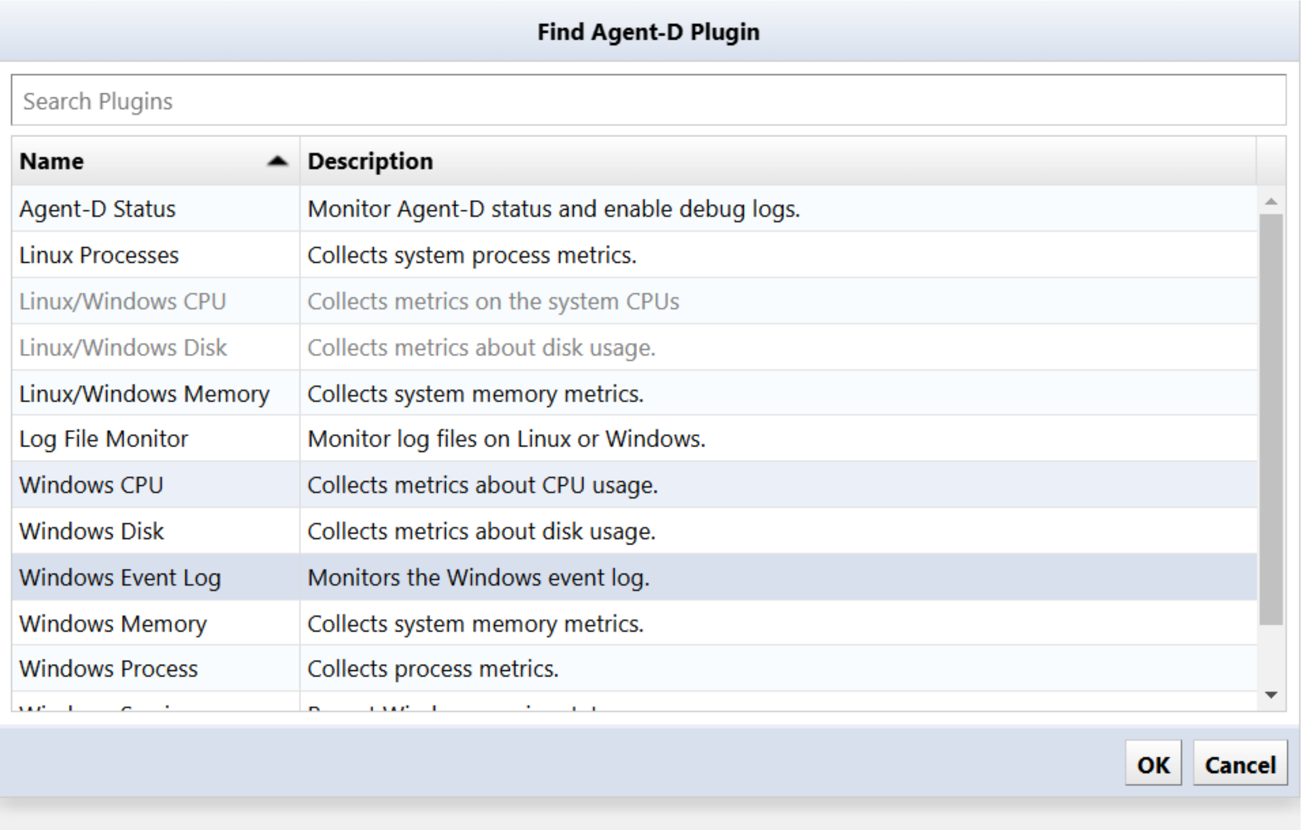
4. Click [Plugin Library …].



Windows event Log Period: 1 min History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

5. Click Windows Eventlog, then click [OK].

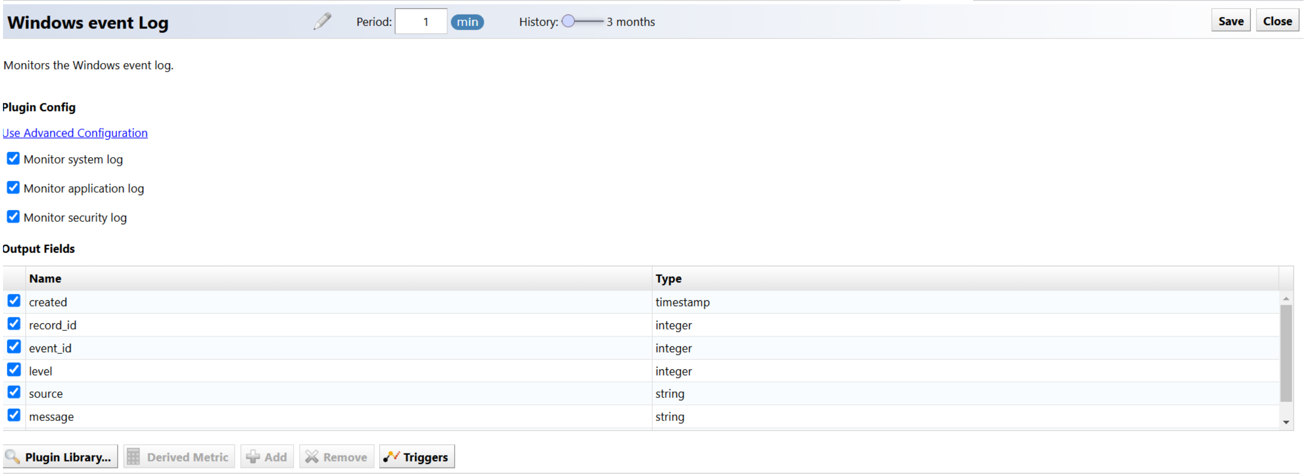


Find Agent-D Plugin

Search Plugins

Name	Description
Agent-D Status	Monitor Agent-D status and enable debug logs.
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.

6. Check the event logs you want to monitor.



Windows event Log

Period: 1 min

History: 3 months

Monitors the Windows event log.

Plugin Config

Use Advanced Configuration

☑ Monitor system log

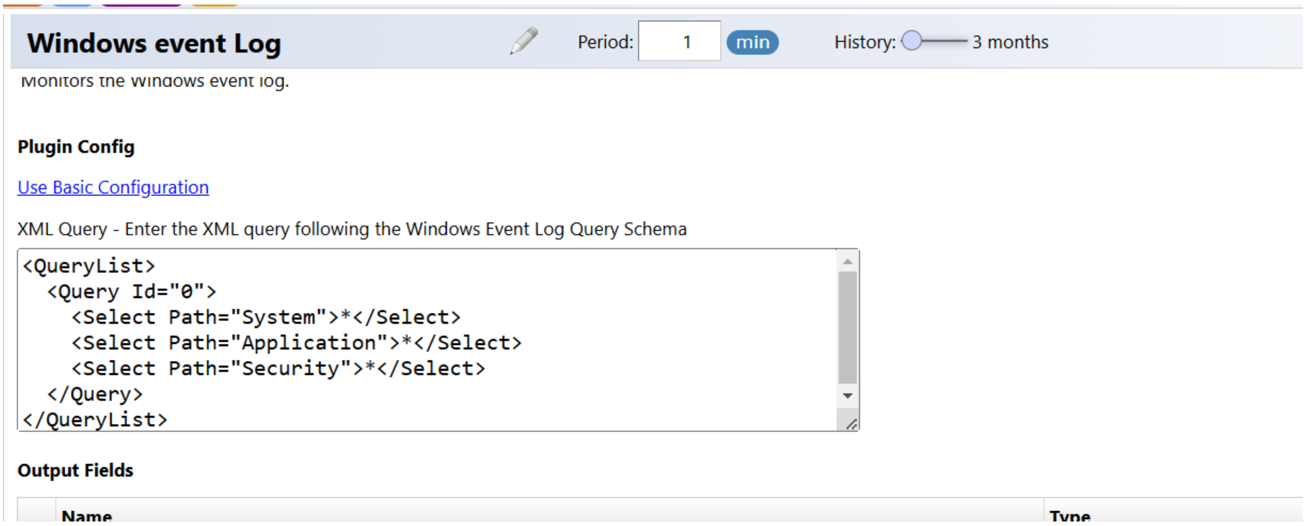
☑ Monitor application log

☑ Monitor security log

Output Fields

	Name	Type
☑	created	timestamp
☑	record_id	integer
☑	event_id	integer
☑	level	integer
☑	source	string
☑	message	string

7. Click [Use advanced settings] to specify in XML format.



Windows event Log

Period: 1 min History: 3 months

Monitors the windows event log.

Plugin Config

Use Basic Configuration

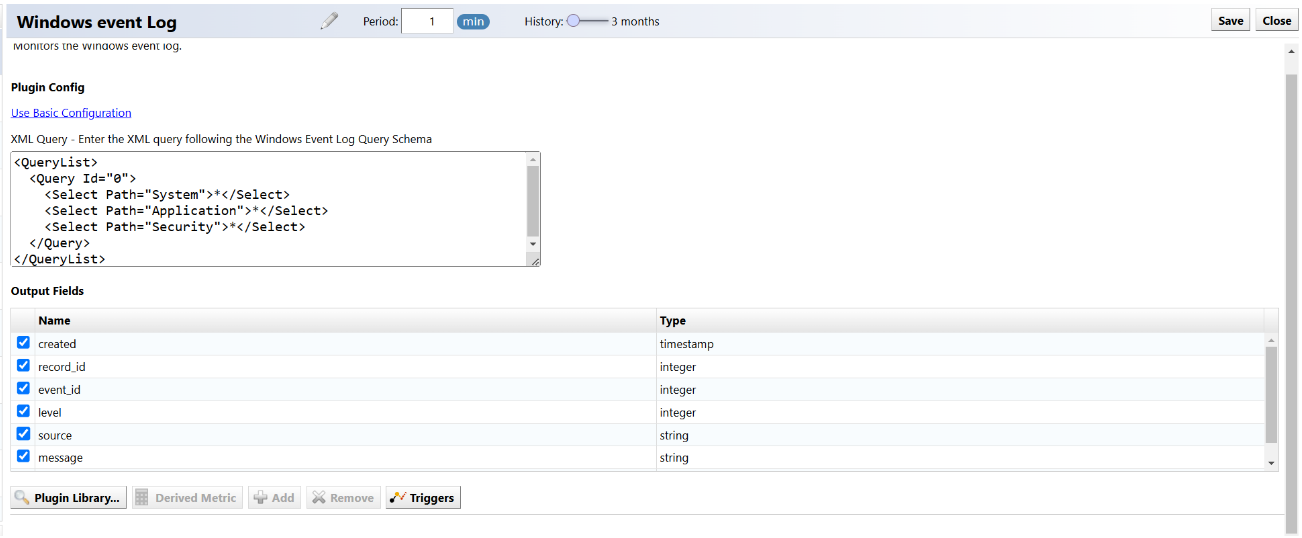
XML Query - Enter the XML query following the Windows Event Log Query Schema

```
<QueryList>
  <Query Id="0">
    <Select Path="System">*</Select>
    <Select Path="Application">*</Select>
    <Select Path="Security">*</Select>
  </Query>
</QueryList>
```

Output Fields

Name	Type

8. Check the items to be retrieved in [Output Fields].



Windows event Log

Period: 1 min History: 3 months

Monitors the windows event log.

Plugin Config

Use Basic Configuration

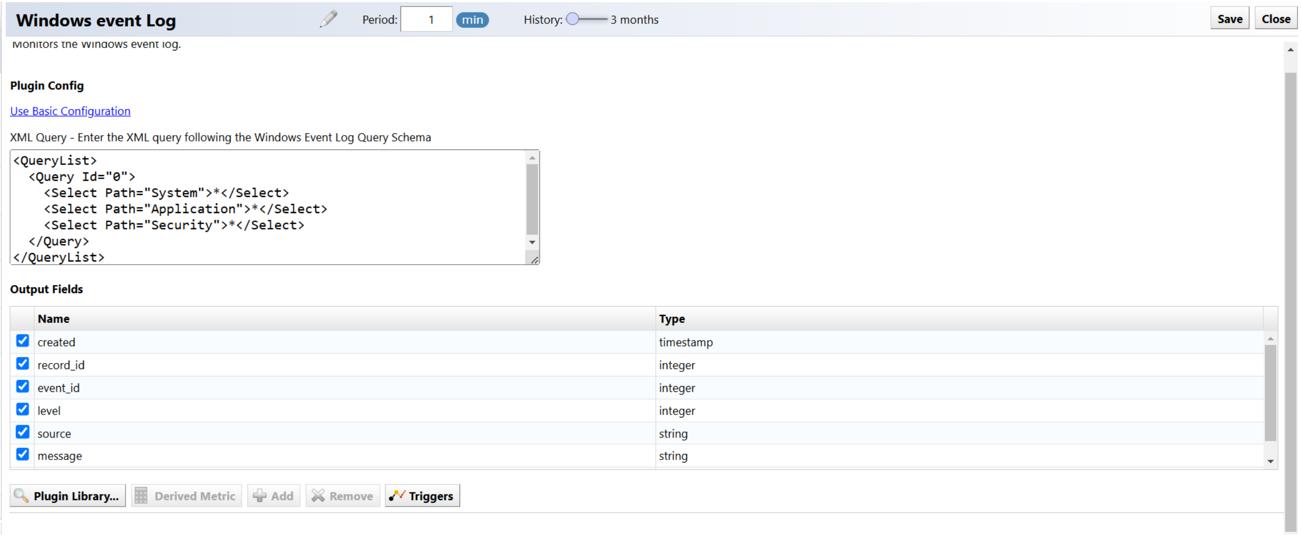
XML Query - Enter the XML query following the Windows Event Log Query Schema

```
<QueryList>
  <Query Id="0">
    <Select Path="System">*</Select>
    <Select Path="Application">*</Select>
    <Select Path="Security">*</Select>
  </Query>
</QueryList>
```

Output Fields

	Name	Type
☑	created	timestamp
☑	record_id	integer
☑	event_id	integer
☑	level	integer
☑	source	string
☑	message	string

9. Click [Save].



Monitors the windows event log.

Plugin Config

Use Basic Configuration

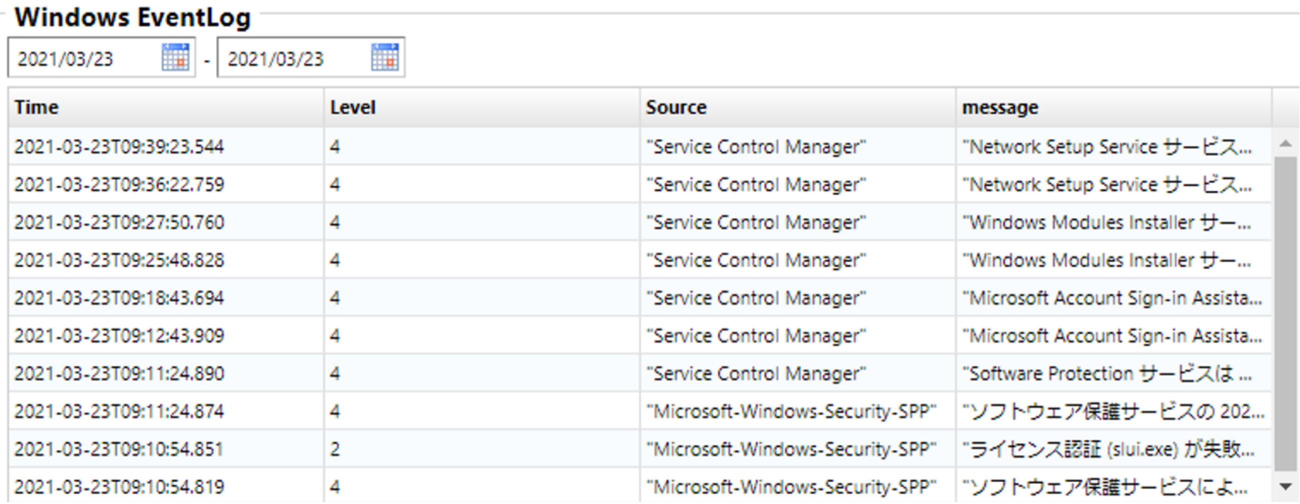
XML Query - Enter the XML query following the Windows Event Log Query Schema

```
<QueryList>
  <Query Id="0">
    <Select Path="System">*</Select>
    <Select Path="Application">*</Select>
    <Select Path="Security">*</Select>
  </Query>
</QueryList>
```

Output Fields

	Name	Type
☑	created	timestamp
☑	record_id	integer
☑	event_id	integer
☑	level	integer
☑	source	string
☑	message	string

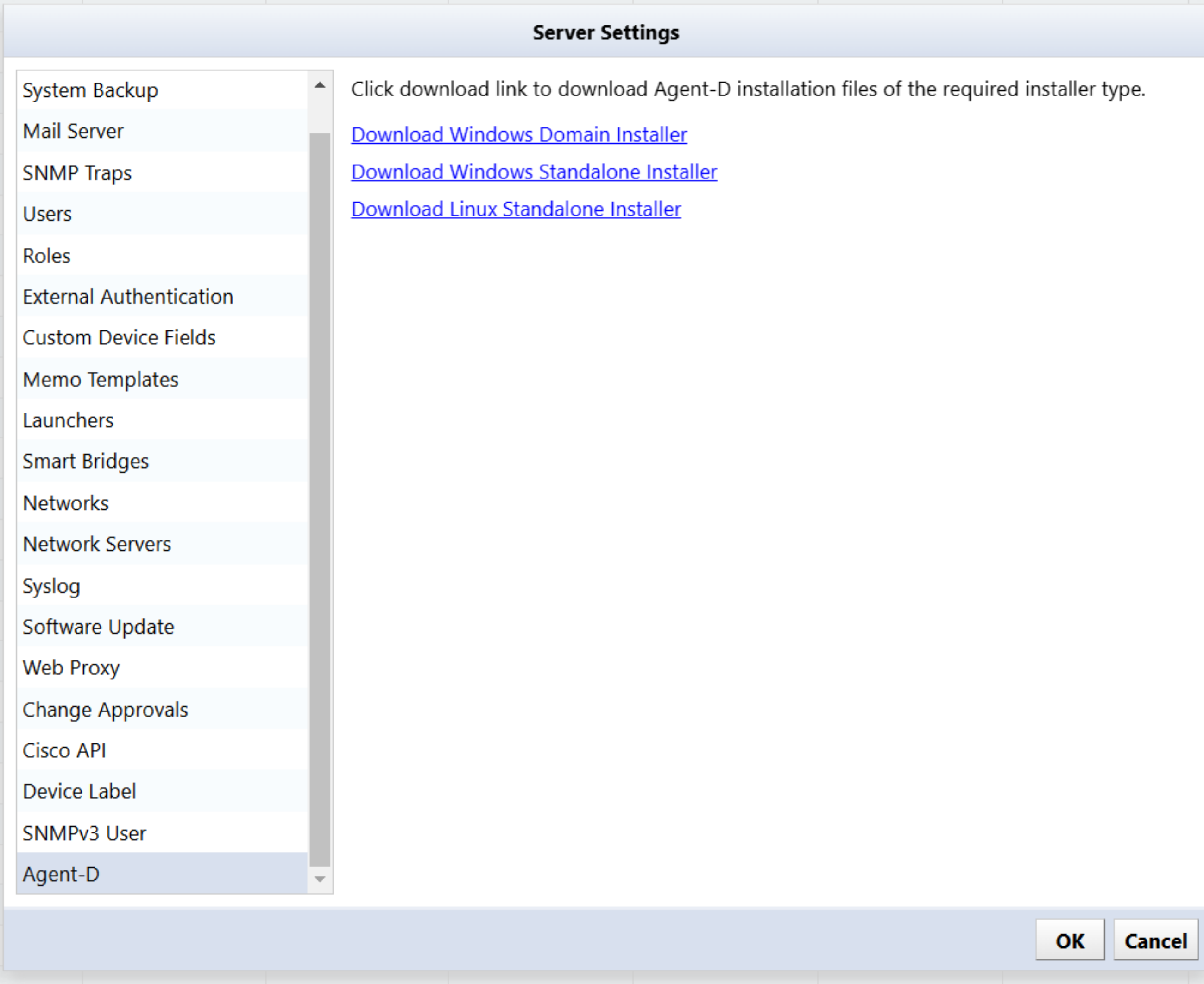
Now, the event log information will be sent from Agent-D and can be checked in the device details.



Time	Level	Source	message
2021-03-23T09:39:23.544	4	"Service Control Manager"	"Network Setup Service サービス...
2021-03-23T09:36:22.759	4	"Service Control Manager"	"Network Setup Service サービス...
2021-03-23T09:27:50.760	4	"Service Control Manager"	"Windows Modules Installer サー...
2021-03-23T09:25:48.828	4	"Service Control Manager"	"Windows Modules Installer サー...
2021-03-23T09:18:43.694	4	"Service Control Manager"	"Microsoft Account Sign-in Assista...
2021-03-23T09:12:43.909	4	"Service Control Manager"	"Microsoft Account Sign-in Assista...
2021-03-23T09:11:24.890	4	"Service Control Manager"	"Software Protection サービスは ...
2021-03-23T09:11:24.874	4	"Microsoft-Windows-Security-SPP"	"ソフトウェア保護サービスの 202...
2021-03-23T09:10:54.851	2	"Microsoft-Windows-Security-SPP"	"ライセンス認証 (slui.exe) が失敗...
2021-03-23T09:10:54.819	4	"Microsoft-Windows-Security-SPP"	"ソフトウェア保護サービスによ...

17.5 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.



Server Settings

Click download link to download Agent-D installation files of the required installer type.

Download Windows Domain Installer

Download Windows Standalone Installer

Download Linux Standalone Installer

Please check the Microsoft Docs guide “Install software remotely using Group Policy” for details:

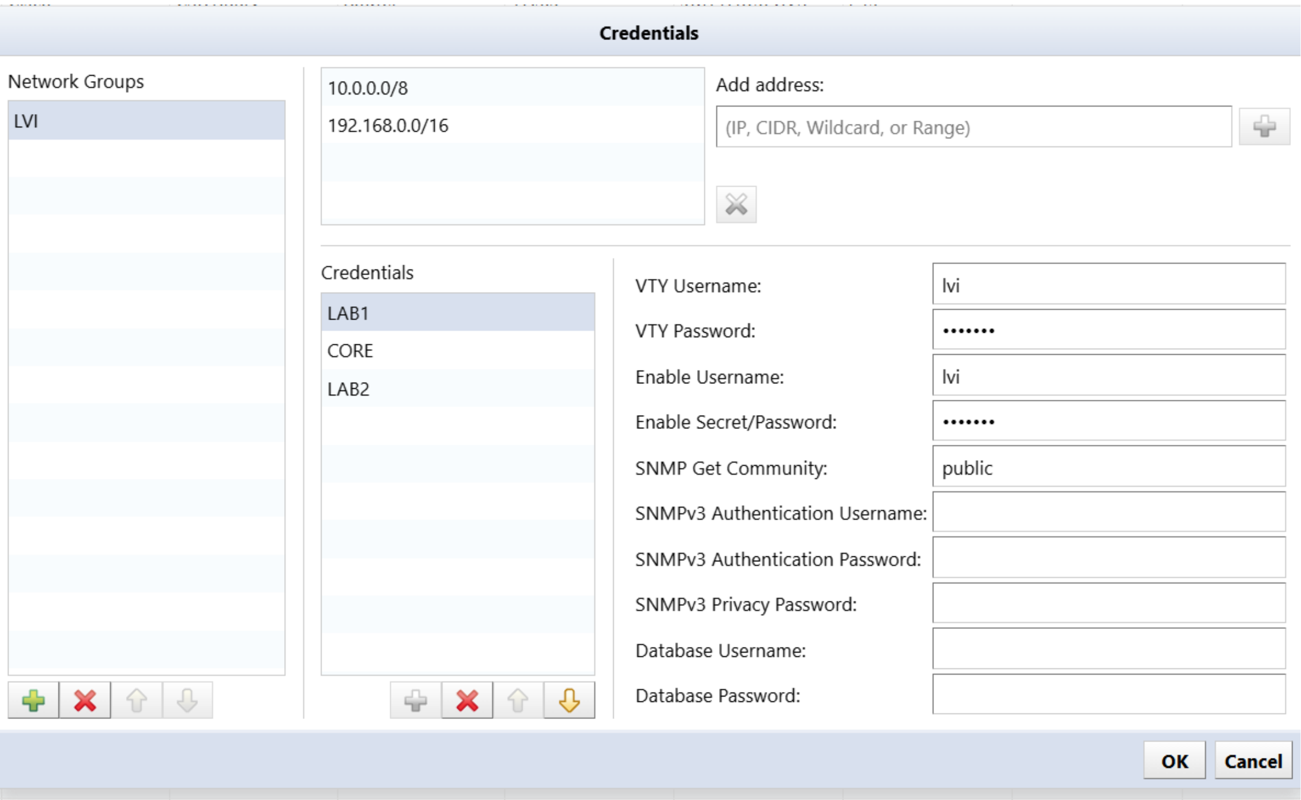
https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

17.6 Install on Linux

17.6.1 Distribute and Install Agent-D from ThirdEye

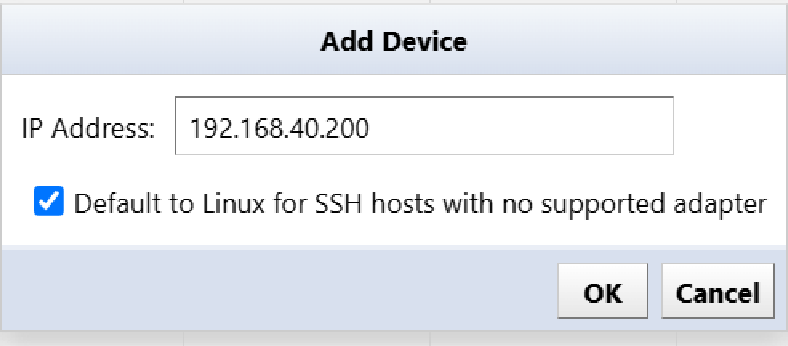
For Linux, if you are in an environment where you can SSH into Linux from ThirdEye, you can install Agent-D from the ThirdEye menu. By selecting devices at once, similar to configuration backup, you can distribute to many devices at once.

1. Set the authentication information (username/password) for SSH connection.



VTY Username:	lvi
VTY Password:	•••••••
Enable Username:	lvi
Enable Secret/Password:	•••••••
SNMP Get Community:	public
SNMPv3 Authentication Username:	
SNMPv3 Authentication Password:	
SNMPv3 Privacy Password:	
Database Username:	
Database Password:	

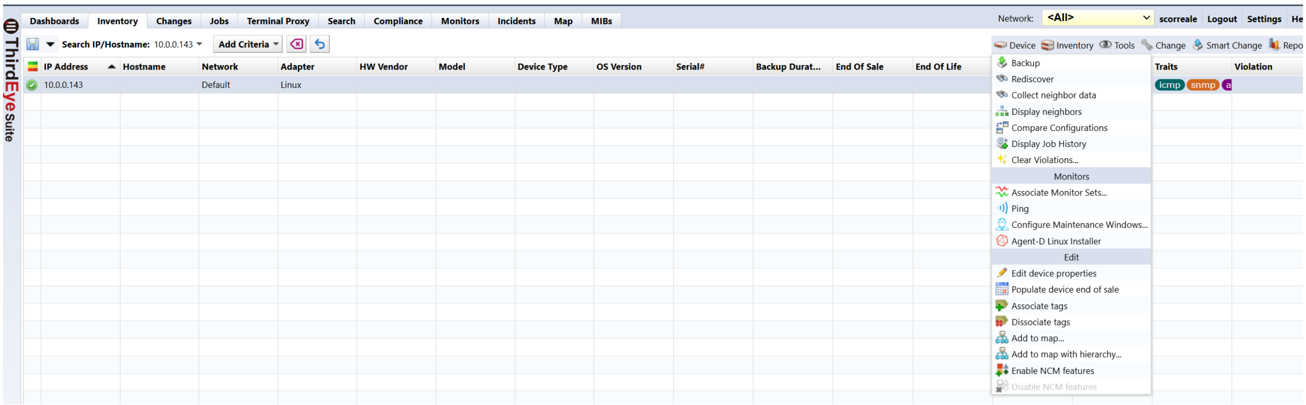
2. Add a Linux device to monitor.



IP Address: 192.168.40.200

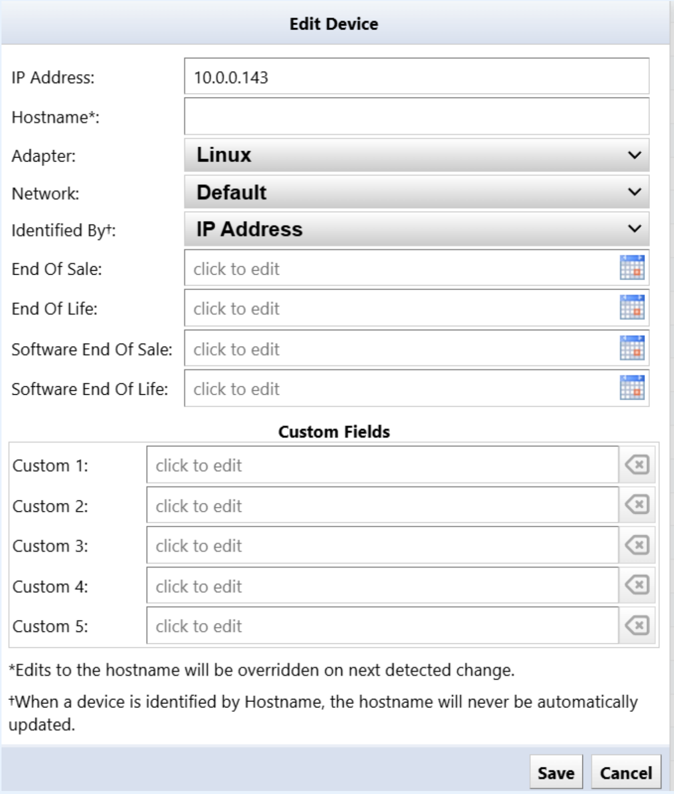
☑ Default to Linux for SSH hosts with no supported adapter

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] submenu:



Edit Device

IP Address:	10.0.0.143
Hostname*:	
Adapter:	Linux
Network:	Default
Identified By†:	IP Address
End Of Sale:	click to edit
End Of Life:	click to edit
Software End Of Sale:	click to edit
Software End Of Life:	click to edit

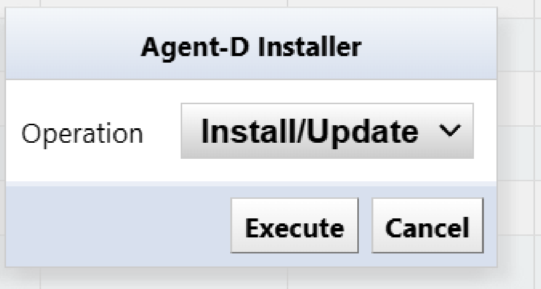
Custom Fields

Custom 1:	click to edit
Custom 2:	click to edit
Custom 3:	click to edit
Custom 4:	click to edit
Custom 5:	click to edit

*Edits to the hostname will be overridden on next detected change.

†When a device is identified by Hostname, the hostname will never be automatically updated.

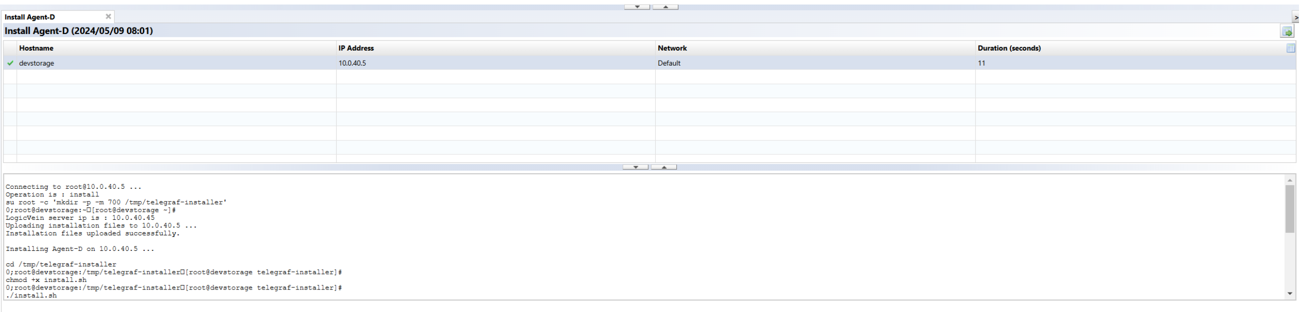
4. Click [Install/Update] > **Execute**.



Agent-D Installer

Operation Install/Update

5. The installation will execute and the results will be displayed in the bottom half of the screen.



Install Agent-D (2024/05/09 08:01)

	Hostname	IP Address	Network	Duration (seconds)
✓	devstorage	10.0.40.5	Default	11

```
Connecting to root@10.0.40.5 ...
Operation is : install
su root -c 'mkdir -p -m 700 /tmp/telegraf-installer'
0;root@devstorage:~□[root@devstorage ~]#
LogicVein server ip is : 10.0.40.45
Uploading installation files to 10.0.40.5 ...
Installation files uploaded successfully.

Installing Agent-D on 10.0.40.5 ...

cd /tmp/telegraf-installer
0;root@devstorage:/tmp/telegraf-installer□[root@devstorage telegraf-installer]#
chmod +x install.sh
0;root@devstorage:/tmp/telegraf-installer□[root@devstorage telegraf-installer]#
./install.sh
```

17.7 CPU Monitoring

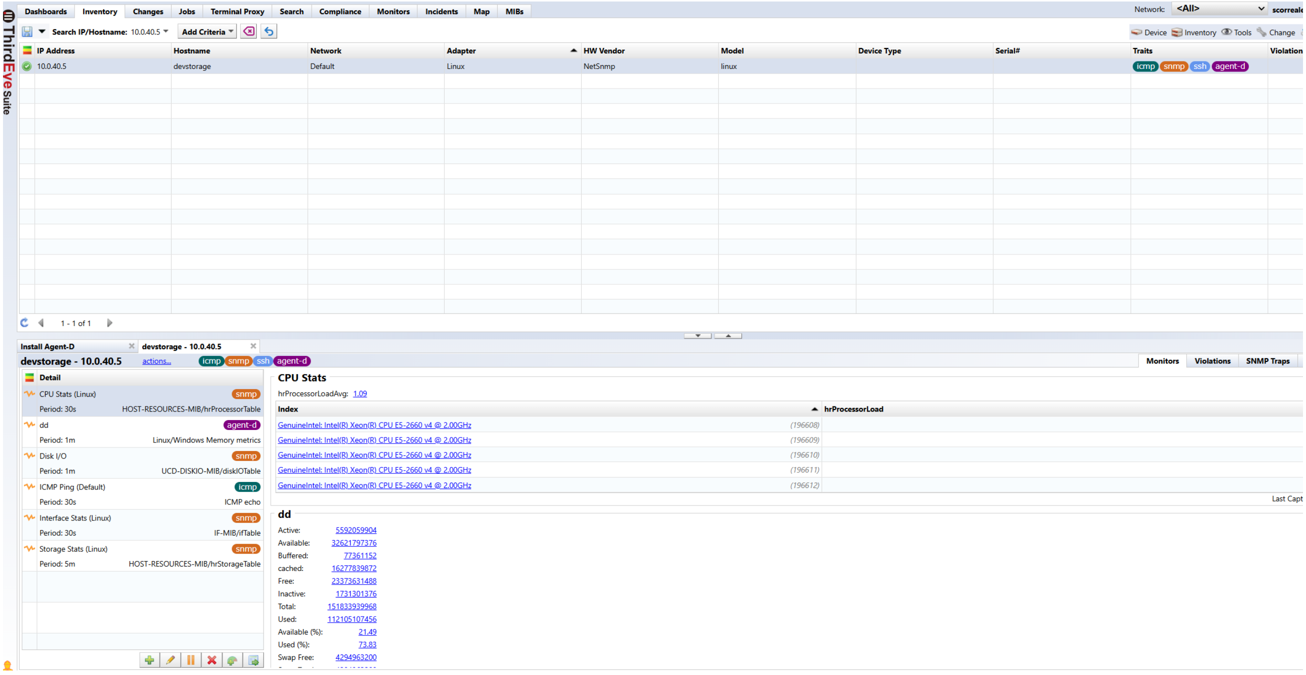
Use Agent-D to obtain CPU information for the installed server. By setting thresholds for CPU usage, etc., you can issue an alert when the threshold is exceeded.

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 be set up as a monitor for a CentOS device. For instructions, refer to the **Monitor SNMP Traps (all)** section.

1. Doubleclick the device for which you want to configure a monitor to open the device details.



Search IP/Hostname: 10.0.40.5

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	Serial#	Traits	Violation
10.0.40.5	devstorage	Default	Linux	NetSnmp	linux			icmp snmp ssh agent-d	

devstorage - 10.0.40.5 icmp snmp ssh agent-d

Detail	
CPU Stats (Linux)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
dd	agent-d
Period: 1m	Linux/Windows Memory metrics
Disk I/O	snmp
Period: 1m	UCD-DISKIO-MIB/diskIOTable
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Interface Stats (Linux)	snmp
Period: 30s	IF-MIB/ifTable
Storage Stats (Linux)	snmp
Period: 5m	HOST-RESOURCES-MIB/hrStorageTable

CPU Stats

hrProcessorLoadAvg: 1.09

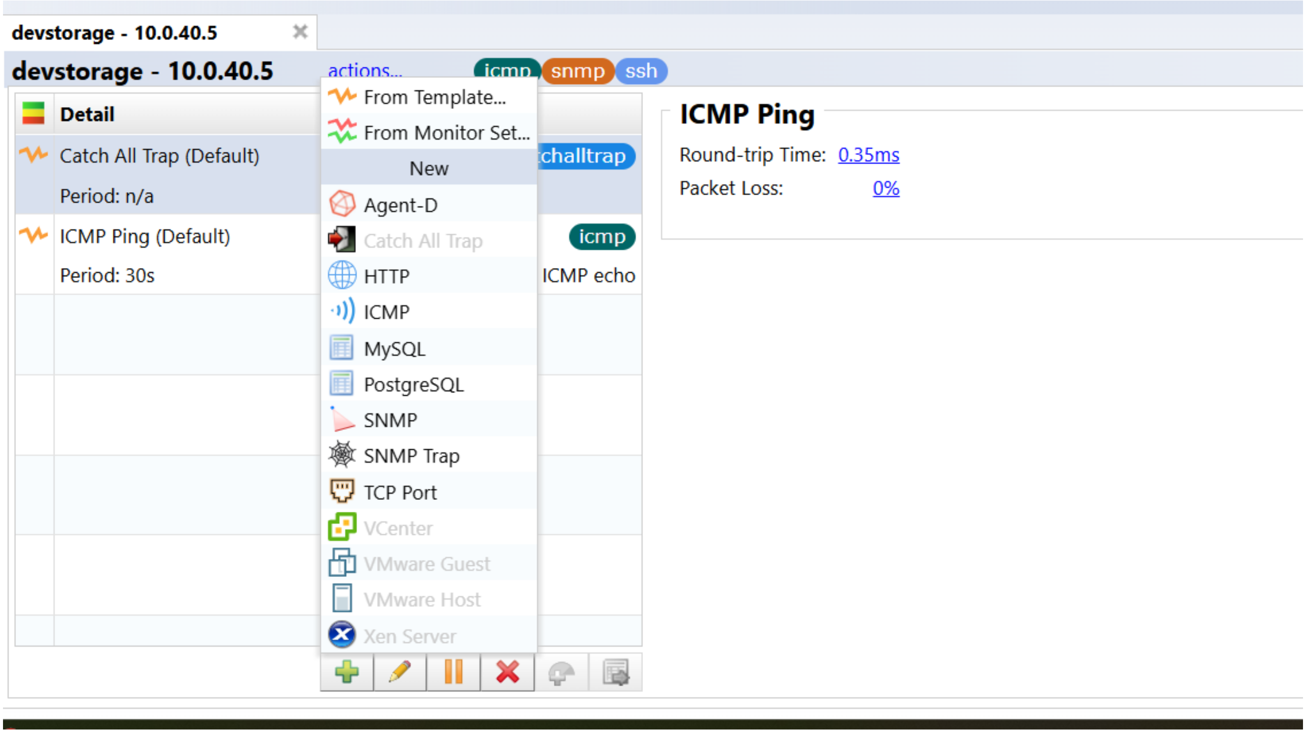
Index		hrProcessorLoad
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196608)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196609)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196610)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196611)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196612)	

Last Capt

dd

Active:	5592059904
Available:	32621797376
Buffered:	77361152
cached:	16277839872
Free:	23373631488
Inactive:	1731301376
Total:	151833939968
Used:	112105107456
Available (%):	21.49
Used (%):	73.83
Swap Free:	4294963200

2. Click the ➕ button, then click [Agent-D].



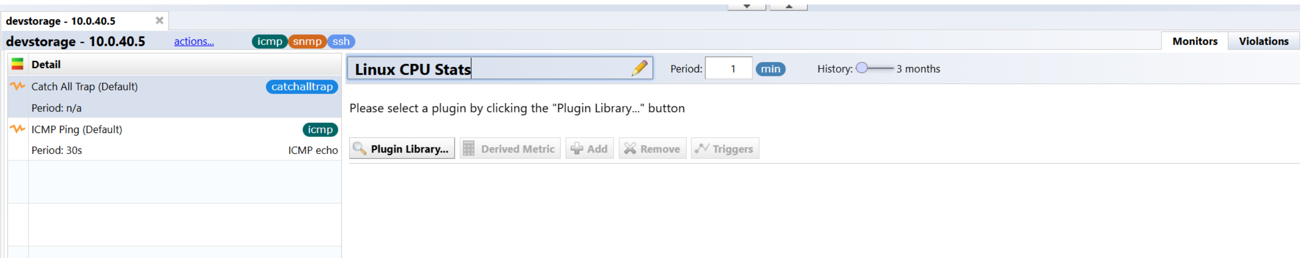
Round-trip Time: 0.35ms

Packet Loss: 0%

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.



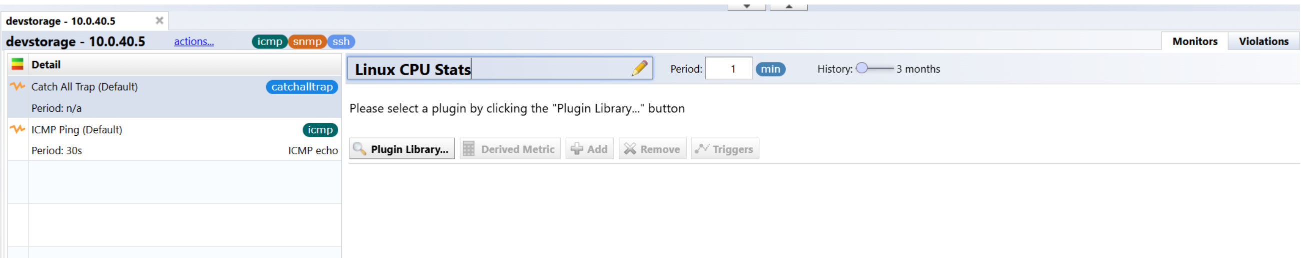
Linux CPU Stats

Period: 1 min

History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

4. Click [Plugin Library…].



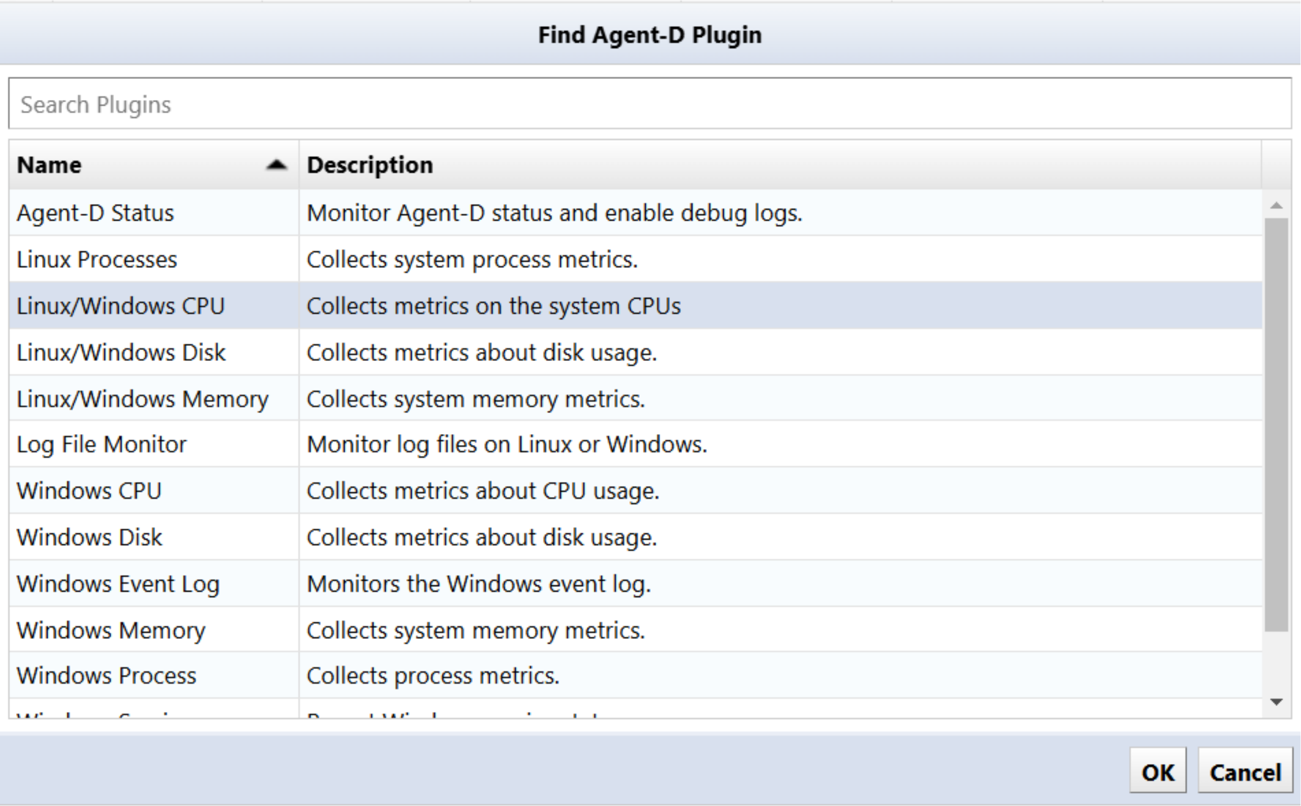
Linux CPU Stats

Period: 1 min

History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

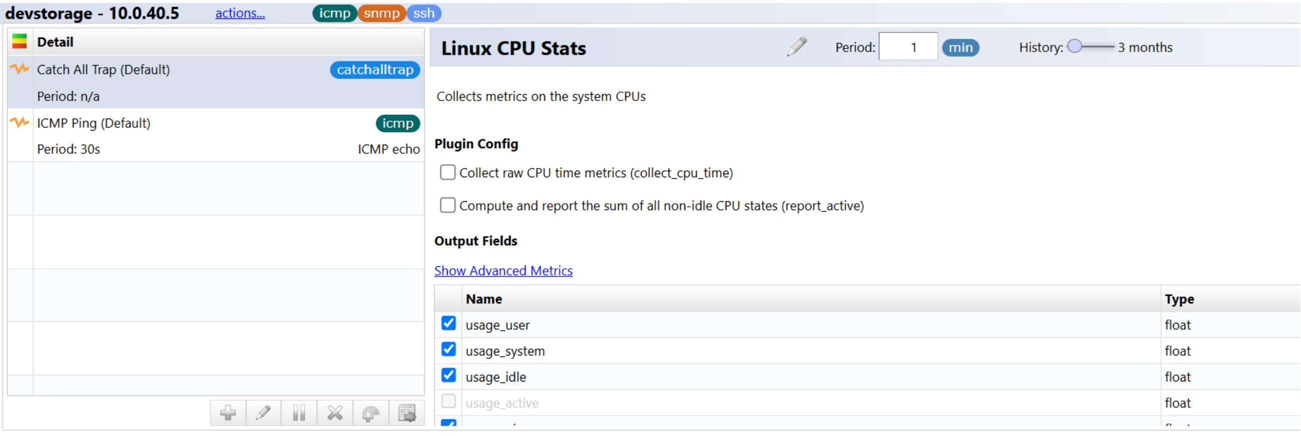
5. Select [Linux CPU] and click [OK].



Find Agent-D Plugin

Name ▲	Description
Agent-D Status	Monitor Agent-D status and enable debug logs.
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.

6. Check the items to be acquired in Plugin Config.



Linux CPU Stats

Period: 1 min History: 3 months

Collects metrics on the system CPUs

Plugin Config

□ Collect raw CPU time metrics (collect_cpu_time)

□ Compute and report the sum of all non-idle CPU states (report_active)

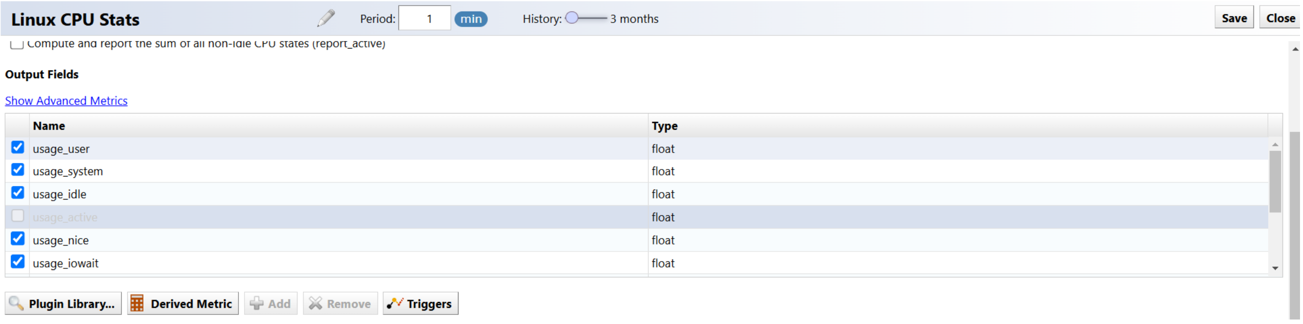
Output Fields

Show Advanced Metrics

	Name	Type
☑	usage_user	float
☑	usage_system	float
☑	usage_idle	float
□	usage_active	float

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].



Linux CPU Stats Period: 1 min History: 3 months Save Close

□ Compute and report the sum of all non-idle CPU states (report_active)

Output Fields

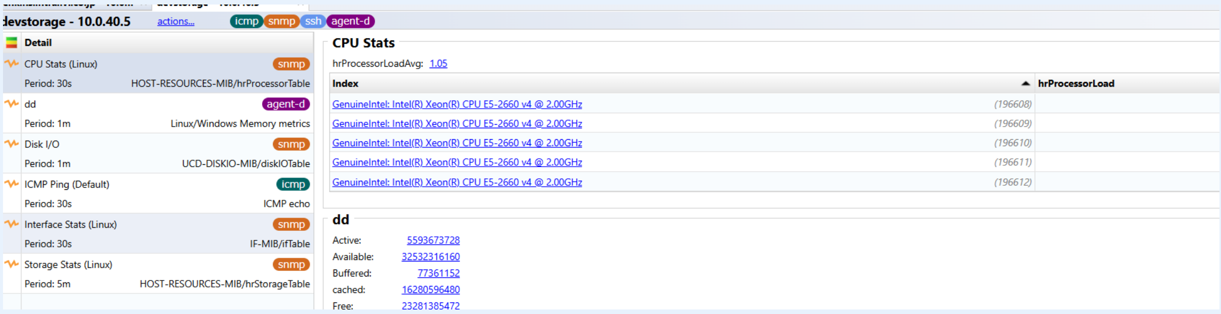
Show Advanced Metrics

	Name	Type
☑	usage_user	float
☑	usage_system	float
☑	usage_idle	float
□	usage_active	float
☑	usage_nice	float
☑	usage_iowait	float

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.



devstorage - 10.0.40.5 actions... icmp snmp ssh agent-d

Detail

CPU Stats (Linux)	snmp
Period: 30s	HOST-RESOURCES-MIB/hrProcessorTable
dd	agent-d
Period: 1m	Linux/Windows Memory metrics
Disk I/O	snmp
Period: 1m	UCD-DISKIO-MIB/diskIOTable
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Interface Stats (Linux)	snmp
Period: 30s	IF-MIB/ifTable
Storage Stats (Linux)	snmp
Period: 5m	HOST-RESOURCES-MIB/hrStorageTable

CPU Stats

hrProcessorLoadAvg: 1.05

Index		hrProcessorLoad
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196608)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196609)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196610)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196611)	
GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	(196612)	

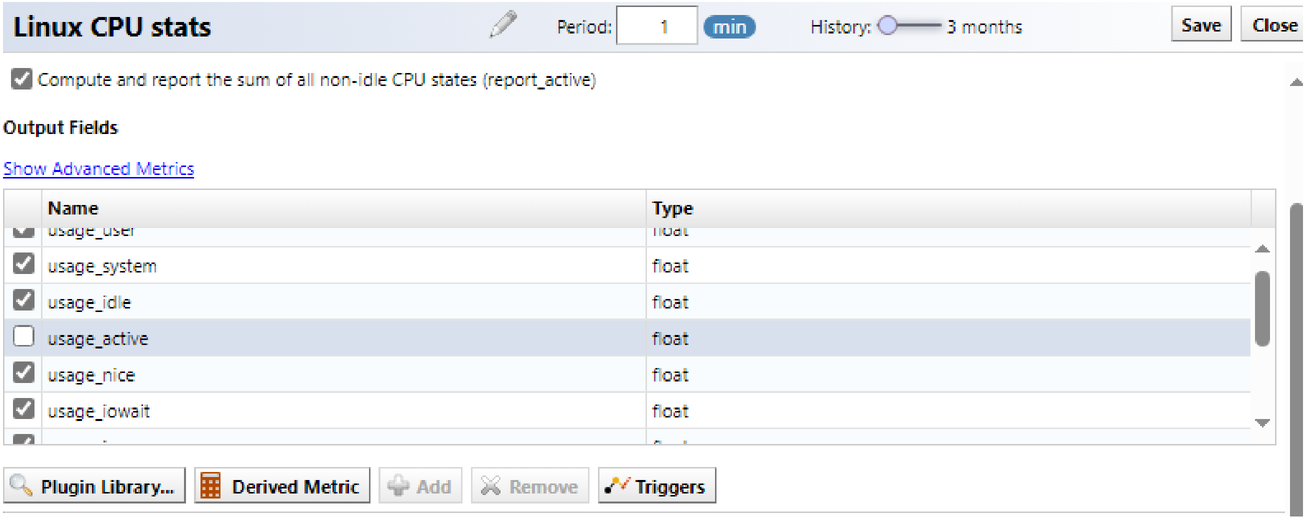
dd

Active:	5593673728
Available:	32532316160
Buffered:	77361152
cached:	16280596480
Free:	23281385472

17.8 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.



Linux CPU stats

Period: 1 min

History: 3 months

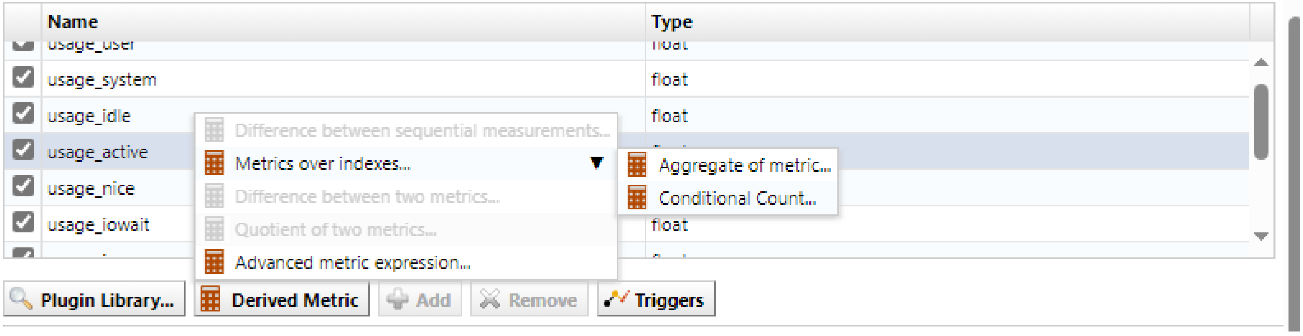
☑ Compute and report the sum of all non-idle CPU states (report_active)

Output Fields

Show Advanced Metrics

	Name	Type
☑	usage_user	float
☑	usage_system	float
☑	usage_idle	float
□	usage_active	float
☑	usage_nice	float
☑	usage_iowait	float

3. Click [Derived Metrics] > [Metrics over indexes] > [Aggregation of Multiple Indexes].



	Name	Type
☑	usage_user	float
☑	usage_system	float
☑	usage_idle	float
☑	usage_active	float
☑	usage_nice	float
☑	usage_iowait	float

Difference between sequential measurements...
Metrics over indexes...
Difference between two metrics...
Quotient of two metrics...
Advanced metric expression...
Aggregate of metric...
Conditional Count...
Plugin Library...
Derived Metric
Add
Remove
Triggers

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.

17.9 Memory Monitoring

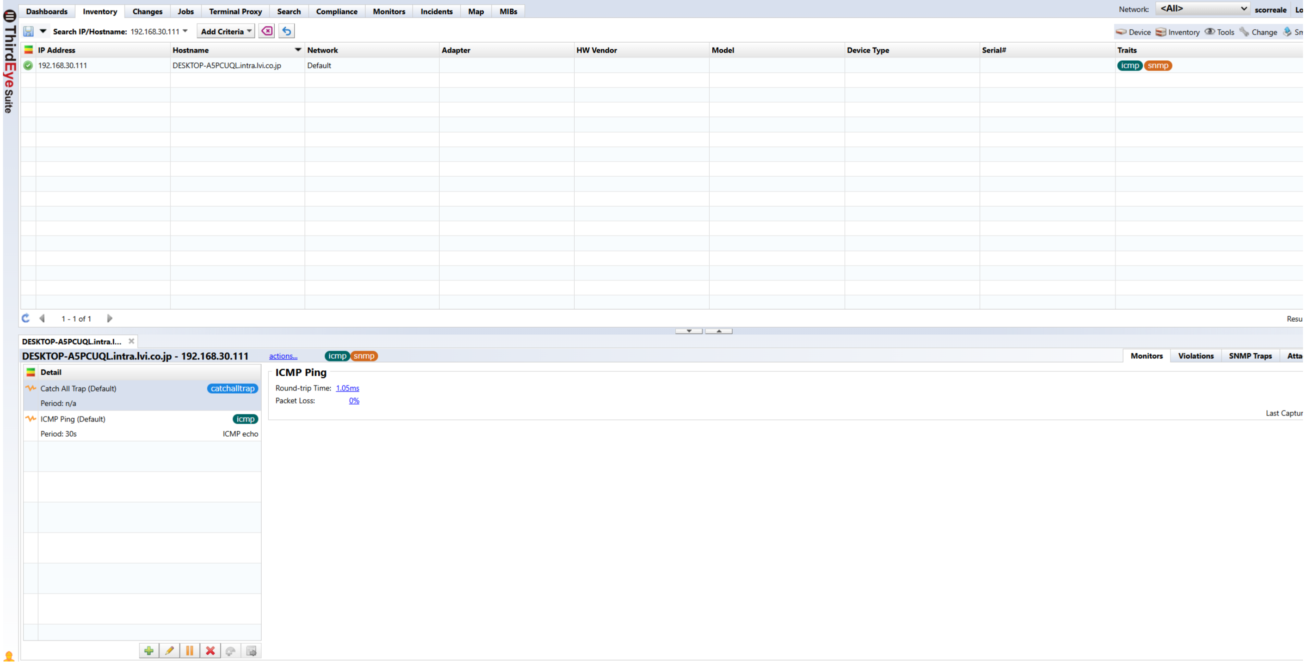
Use Agent-D to obtain memory information for installed servers. By setting thresholds for things like memory usage, you can issue an alert when the threshold is exceeded.

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.



Search IP/Hostname: 192.168.30.111

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	Serial#	Traits
192.168.30.111	DESKTOP-A5PCUQL.intra.lvi.co.jp	Default						icmp snmp

DESKTOP-A5PCUQL.intra.lvi.co.jp - 192.168.30.111 icmp snmp

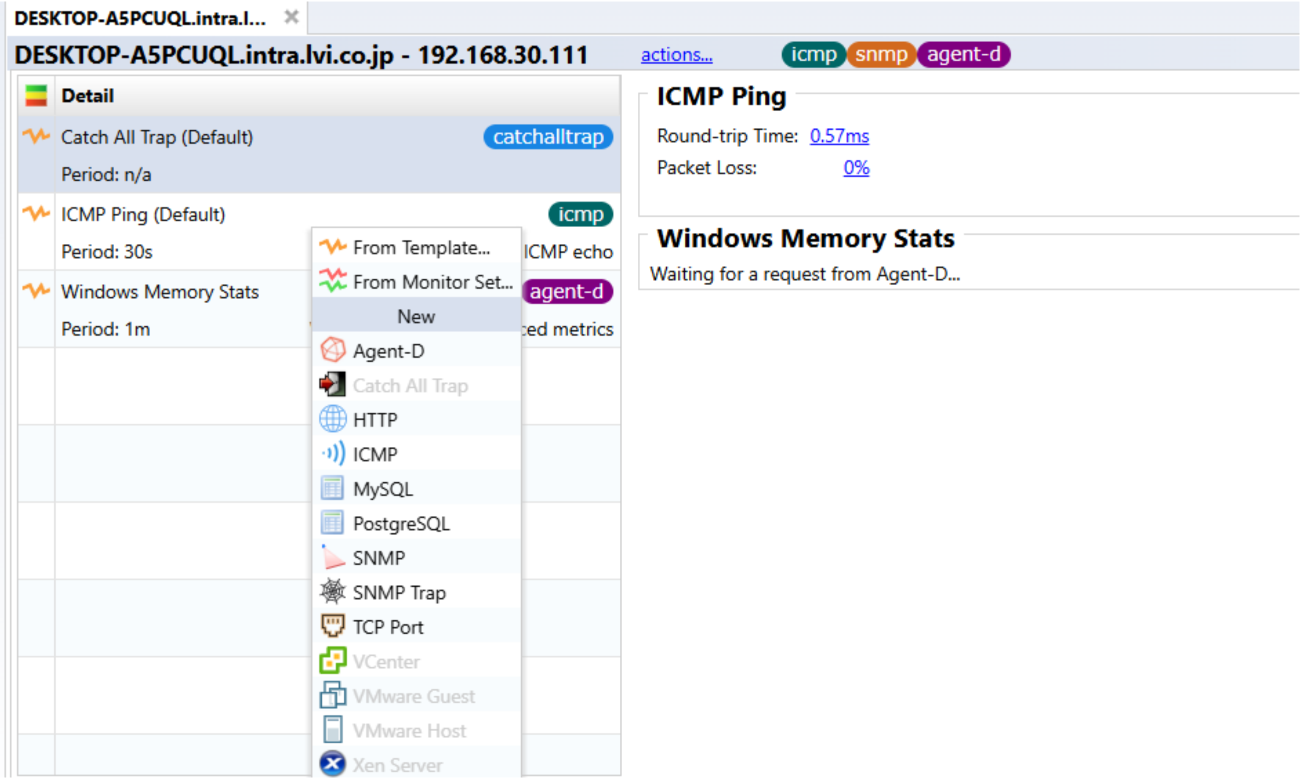
Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo

ICMP Ping

Round-trip Time: 1.05ms

Packet Loss: 0%

2. Click the ➕ button, then click [Agent-D].



DESKTOP-A5PCUQL.intra.l... ✕

DESKTOP-A5PCUQL.intra.lvi.co.jp - 192.168.30.111

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo
Windows Memory Stats Period: 1m	agent-d ...ced metrics

ICMP Ping

Round-trip Time: 0.57ms

Packet Loss: 0%

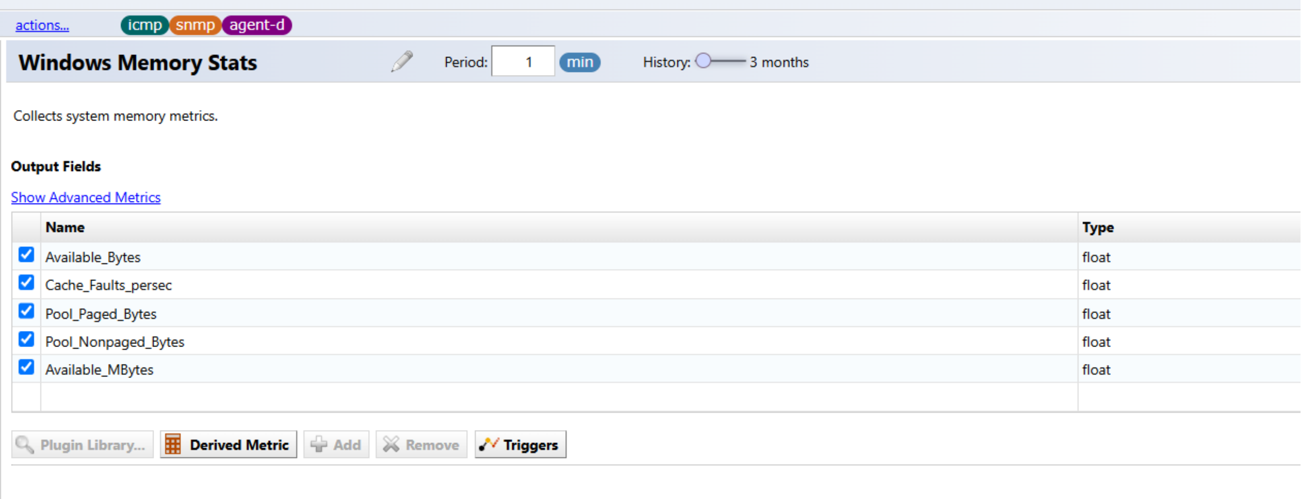
Windows Memory Stats

Waiting for a request from Agent-D...

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.



Windows Memory Stats

Period: 1 min

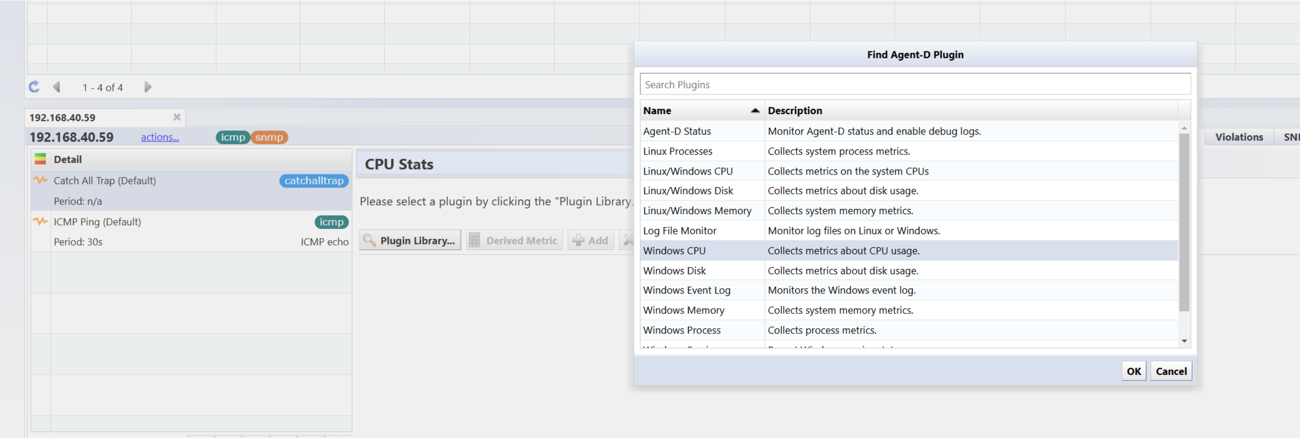
History: 3 months

Collects system memory metrics.

Output Fields

	Name	Type
☑	Available_Bytes	float
☑	Cache_Faults_persec	float
☑	Pool_Paged_Bytes	float
☑	Pool_Nonpaged_Bytes	float
☑	Available_MBytes	float

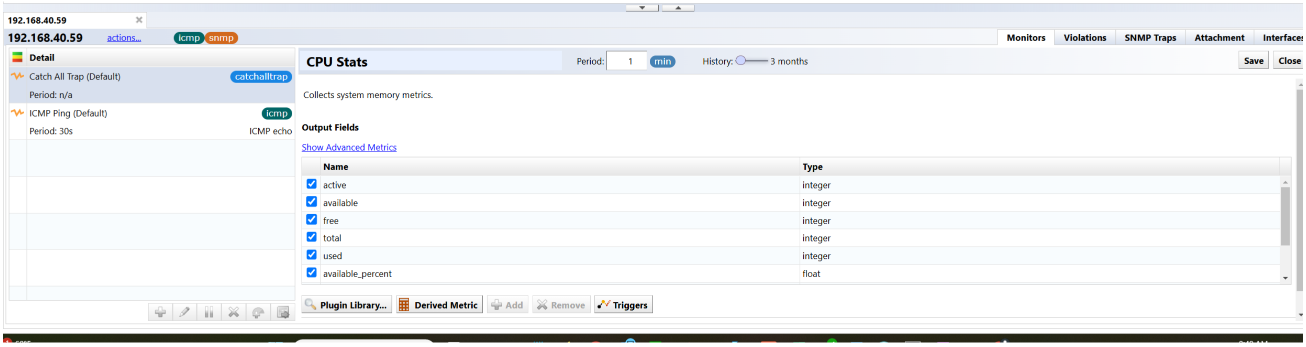
4. Click [Plugin Library…] and select [Windows Memory] and click [OK]



Please select a plugin by clicking the "Plugin Library

Name	Description
Agent-D Status	Monitor Agent-D status and enable debug logs.
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.

5. Check the items for which you want to obtain data in [Output Fields], and click [Save].



Period: 1 min

History: 3 months

Collects system memory metrics.

Output Fields

	Name	Type
☑	active	integer
☑	available	integer
☑	free	integer
☑	total	integer
☑	used	integer
☑	available_percent	float

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.

17.10 HDD Monitoring

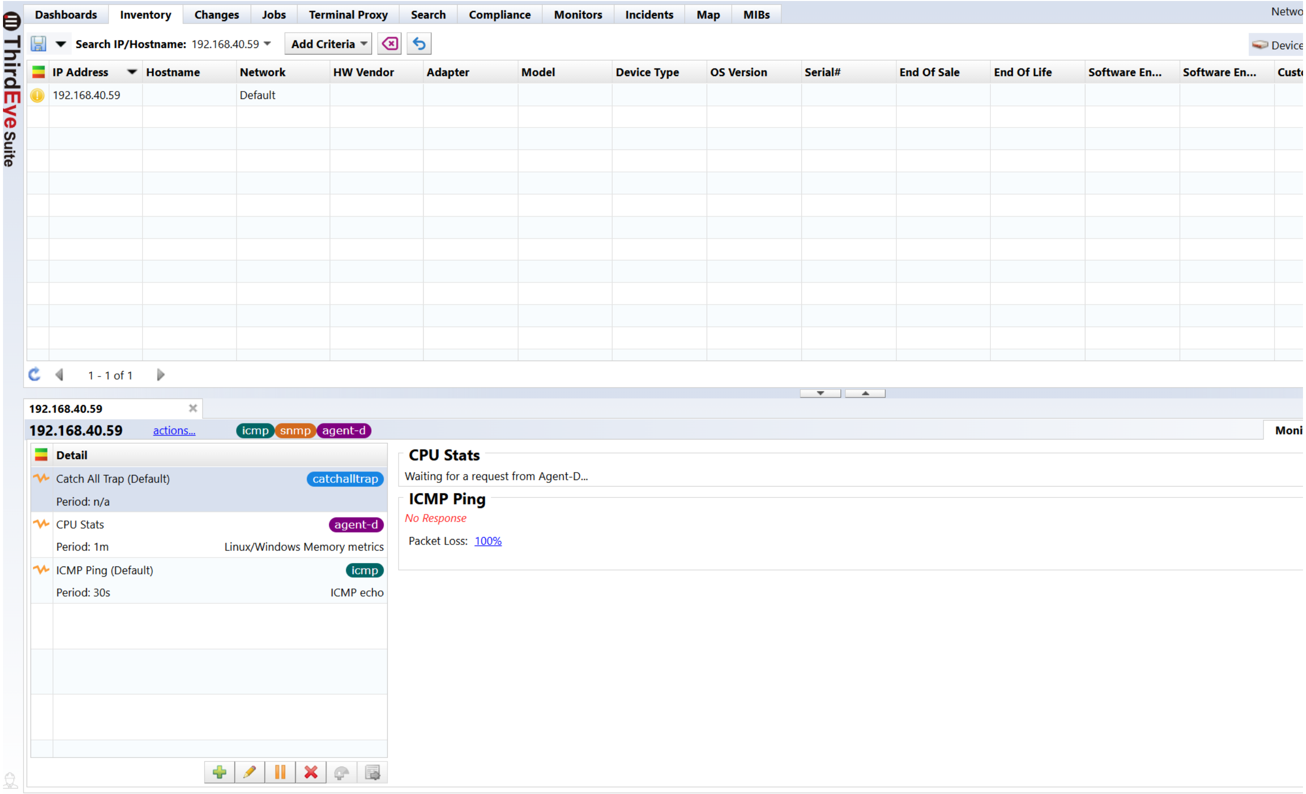
Use Agent-D to obtain the HDD information of the installed server. By setting thresholds for HDD free space, usage rate, etc., you can issue an alert when the thresholds are exceeded.

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.



Search IP/Hostname: 192.168.40.59

IP Address	Hostname	Network	HW Vendor	Adapter	Model	Device Type	OS Version	Serial#	End Of Sale	End Of Life	Software En...	Software En...	Custo
192.168.40.59		Default											

192.168.40.59

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
CPU Stats Period: 1m	agent-d Linux/Windows Memory metrics
ICMP Ping (Default) Period: 30s	icmp ICMP echo

CPU Stats

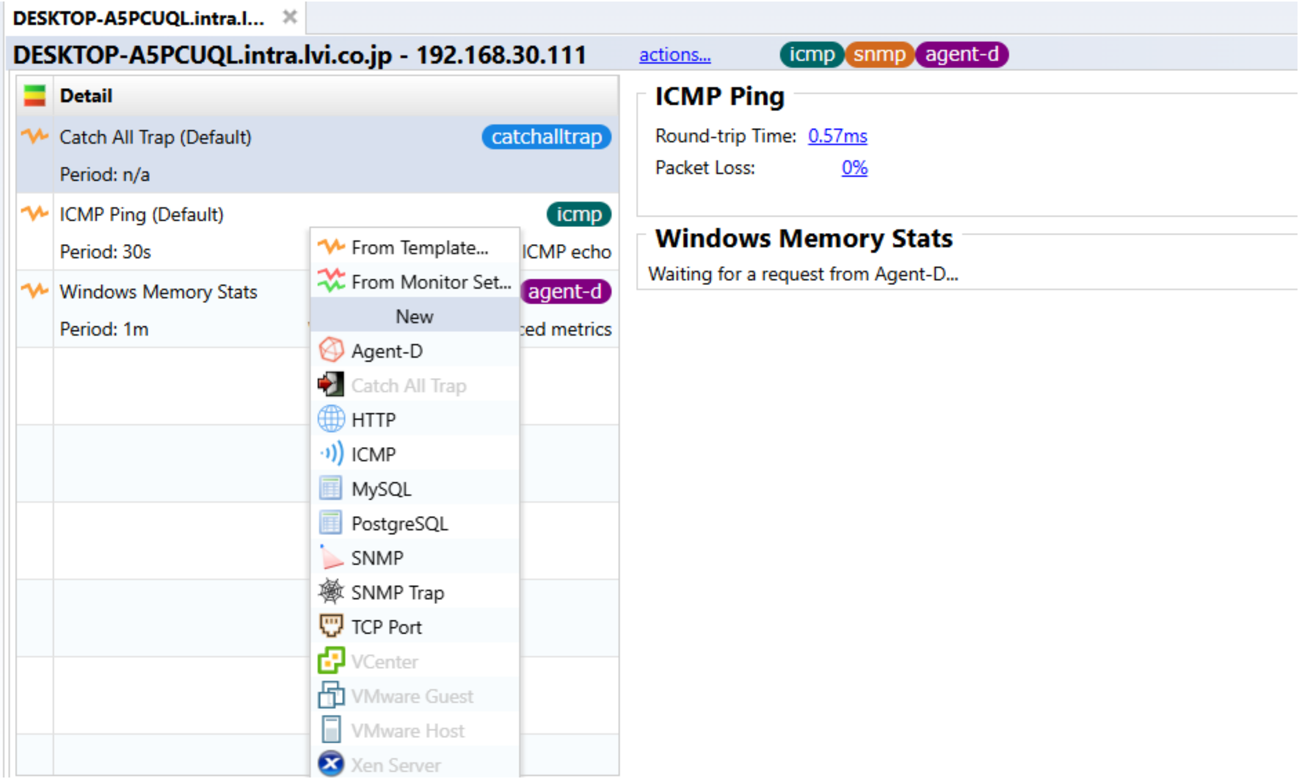
Waiting for a request from Agent-D...

ICMP Ping

No Response

Packet Loss: 100%

2. Click the + button, then click [Agent-D].



DESKTOP-A5PCUQL.intra.lvi.co.jp - 192.168.30.111

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo
Windows Memory Stats Period: 1m	agent-d …ced metrics

ICMP Ping

Round-trip Time: 0.57ms

Packet Loss: 0%

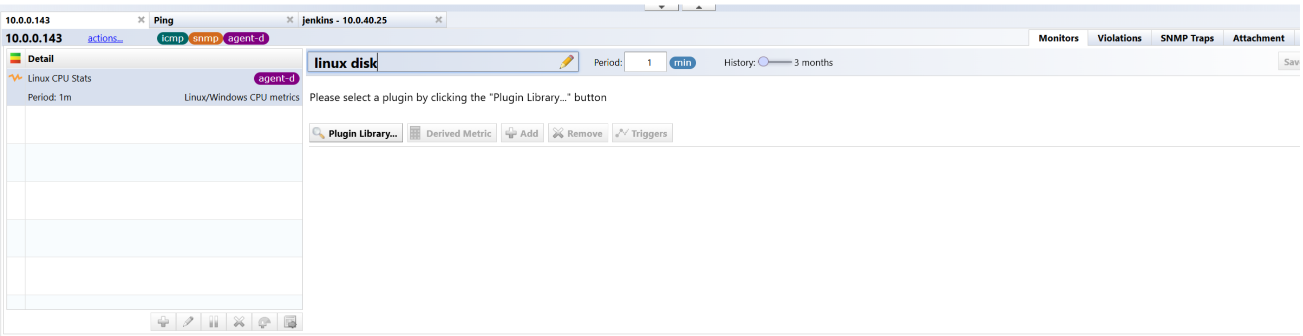
Windows Memory Stats

Waiting for a request from Agent-D...

3. Enter any monitor name, and set the interval and data retention period.

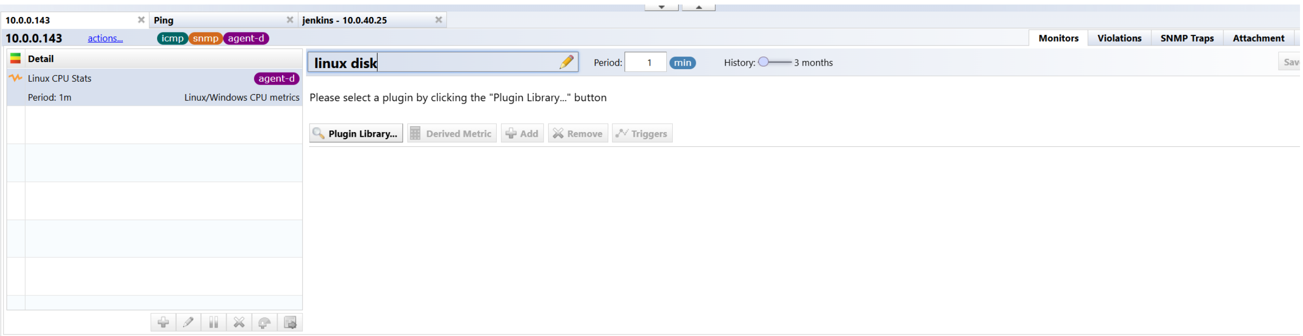
The [Period] field, specifies the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.



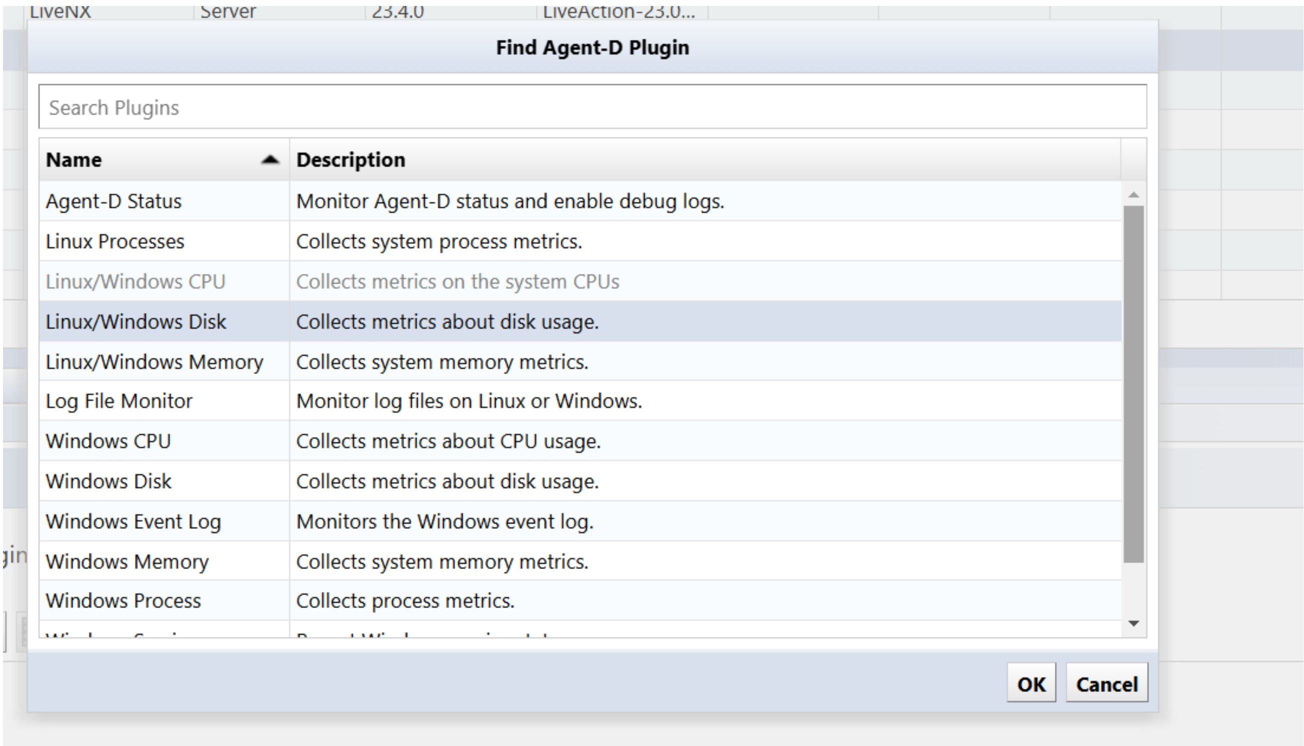
Please select a plugin by clicking the "Plugin Library..." button

4. Click [Plugin Library…].



Please select a plugin by clicking the "Plugin Library..." button

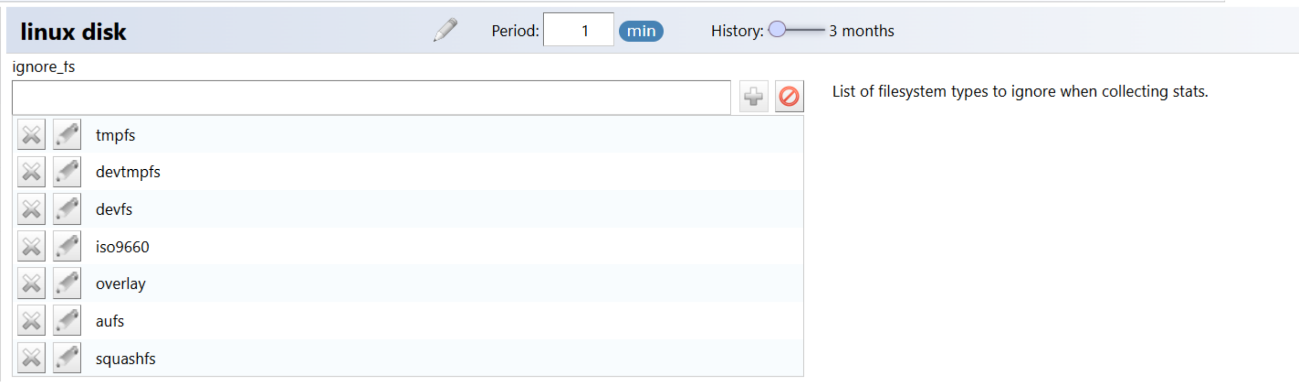
5. Select [Linux/Windows Disk] and click [OK].



Name	Description
Agent-D Status	Monitor Agent-D status and enable debug logs.
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.

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.



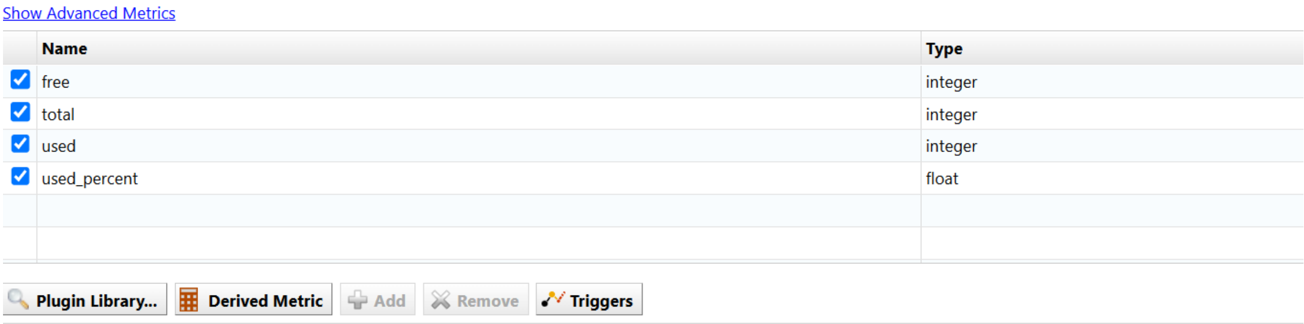
linux disk Period: 1 min History: 3 months

ignore_fs

List of filesystem types to ignore when collecting stats.

- tmpfs
- devtmpfs
- devfs
- iso9660
- overlay
- aufs
- squashfs

7. Check the items you want to obtain in [Output Fields] and click [Save].



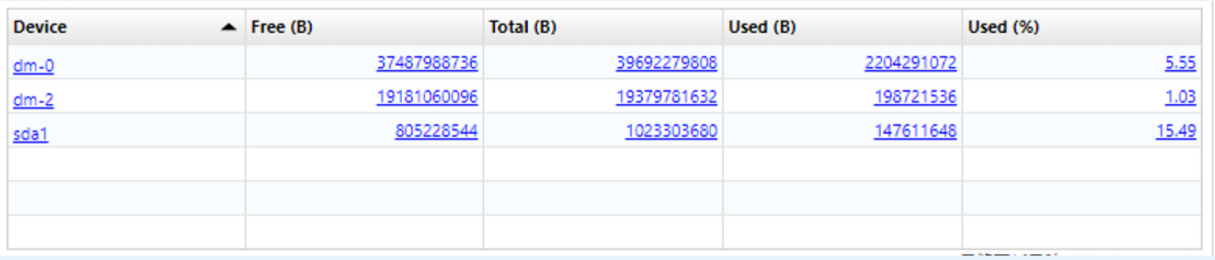
Show Advanced Metrics

	Name	Type
☑	free	integer
☑	total	integer
☑	used	integer
☑	used_percent	float

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

17.11 Process Monitoring

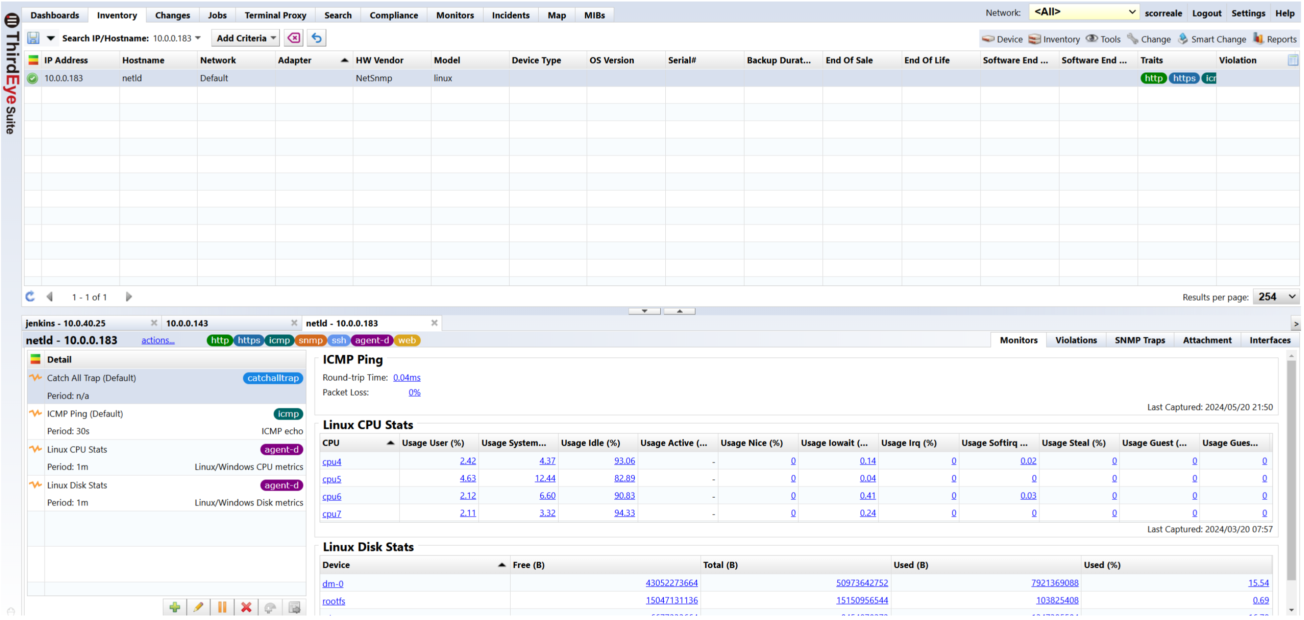
Use Agent-D to obtain information about installed server processes. By setting thresholds for process status, memory usage, etc., you can issue alerts when thresholds are exceeded.

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.



Search IP/Hostname: 10.0.0.183

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.183	netld	Default		NetSnmp	linux									http https icr	

netld - 10.0.0.183

Detail	
Catch All Trap (Default)	catchalltrap
Period: n/a	
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Linux CPU Stats	agent-d
Period: 1m	Linux/Windows CPU metrics
Linux Disk Stats	agent-d
Period: 1m	Linux/Windows Disk metrics

ICMP Ping

Round-trip Time: 0.04ms
Packet Loss: 0%

Last Captured: 2024/05/20 21:50

Linux CPU Stats

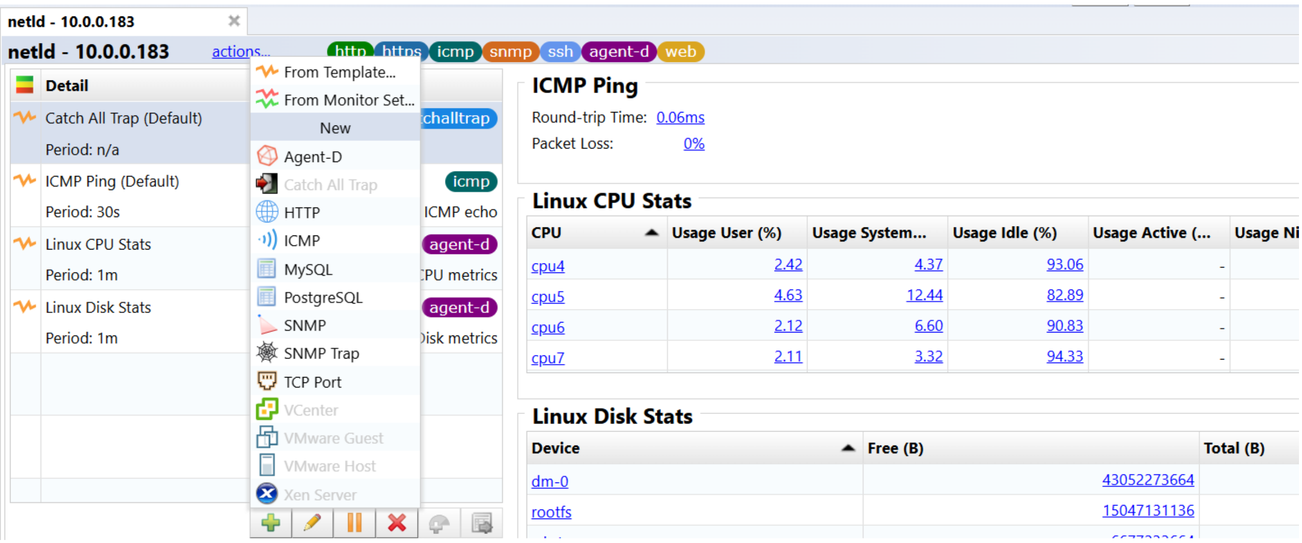
CPU	Usage User (%)	Usage System...	Usage Idle (%)	Usage Active (...	Usage Nice (%)	Usage Iowait (...	Usage Irq (%)	Usage Softirq ...	Usage Steal (%)	Usage Guest (...	Usage Gues...
cpu4	2.42	4.37	93.06	-	0	0.14	0	0.02	0	0	0
cpu5	4.63	12.44	82.89	-	0	0.04	0	0	0	0	0
cpu6	2.12	6.60	90.83	-	0	0.41	0	0.03	0	0	0
cpu7	2.11	3.32	94.33	-	0	0.24	0	0	0	0	0

Last Captured: 2024/03/20 07:57

Linux Disk Stats

Device	Free (B)	Total (B)	Used (B)	Used (%)
dm-0	43052273664	50973642752	7921369088	15.54
rootfs	15047131136	15150956544	103825408	0.69

2. Click the ➕ button, then click [Agent-D].



ICMP Ping

Round-trip Time: 0.06ms

Packet Loss: 0%

Linux CPU Stats

CPU	Usage User (%)	Usage System...	Usage Idle (%)	Usage Active (...	Usage Ni
cpu4	2.42	4.37	93.06	-	
cpu5	4.63	12.44	82.89	-	
cpu6	2.12	6.60	90.83	-	
cpu7	2.11	3.32	94.33	-	

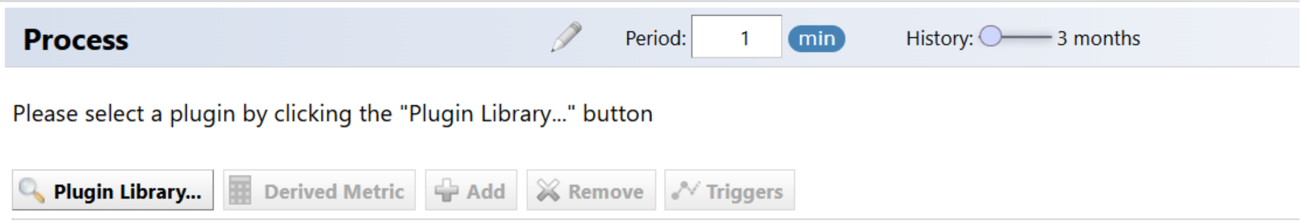
Linux Disk Stats

Device	Free (B)	Total (B)
dm-0	43052273664	
rootfs	15047131136	

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

The [History] slider specifies a data retention period of 3, 6, or 12 months.

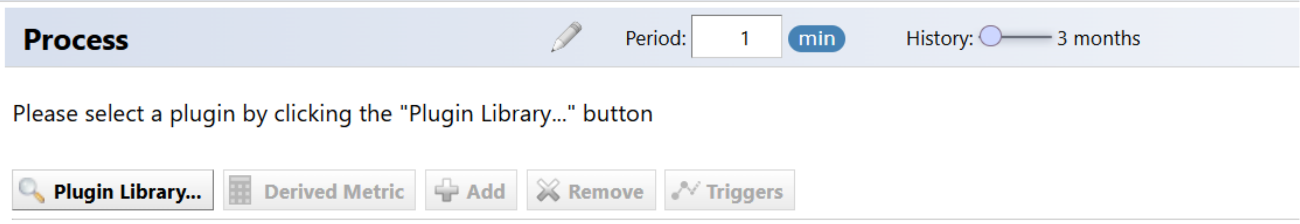


Process

Period: 1 min History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

4. Click [Plugin Library…].

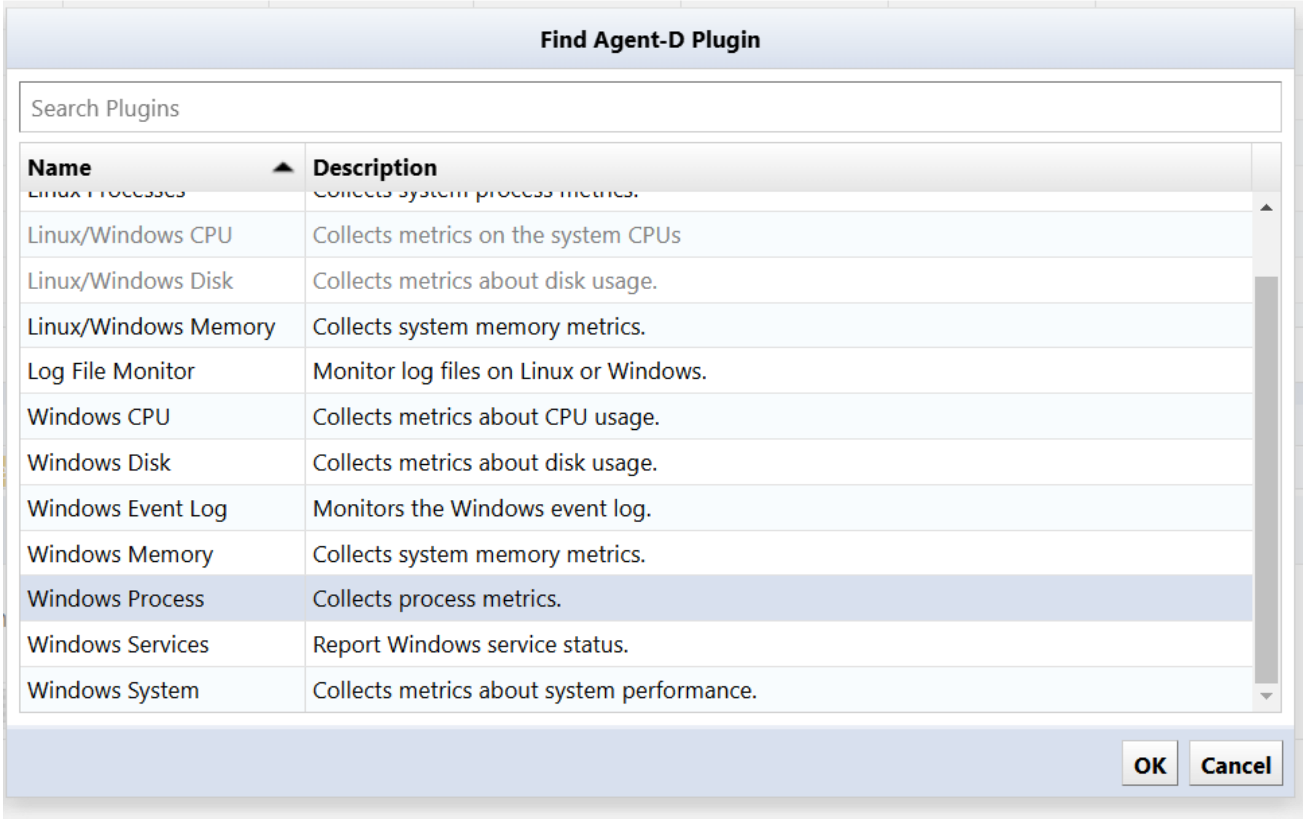


Process

Period: 1 min History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

5. Select Window Process and click [OK].

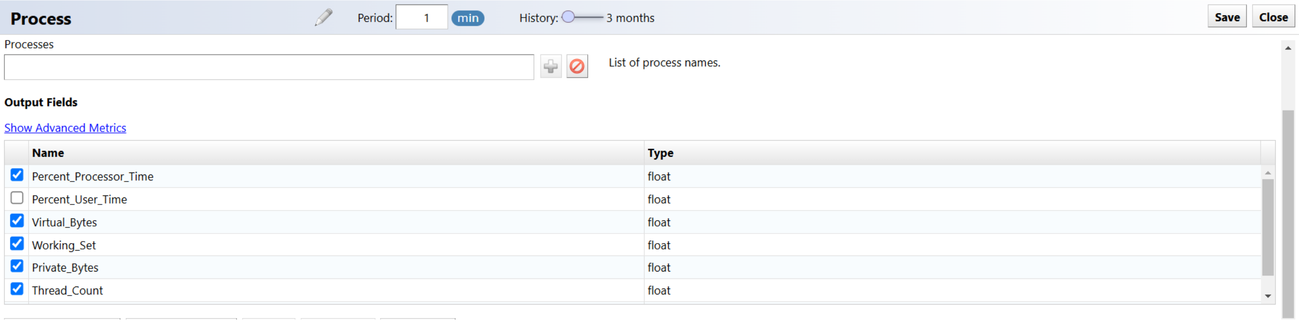


Find Agent-D Plugin

Search Plugins

Name	Description
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.
Windows Services	Report Windows service status.
Windows System	Collects metrics about system performance.

6. Add the process name to be monitored by entering it in the [Processes] field.



Process

Period: 1 min

History: 3 months

Processes

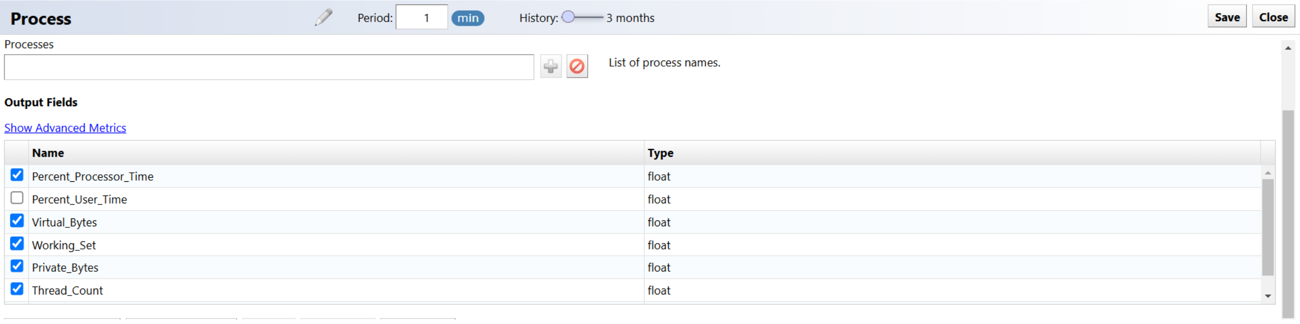
List of process names.

Output Fields

Show Advanced Metrics

	Name	Type
☑	Percent_Processor_Time	float
□	Percent_User_Time	float
☑	Virtual_Bytes	float
☑	Working_Set	float
☑	Private_Bytes	float
☑	Thread_Count	float

7. Check the items you want to obtain in [Output Fields] and click [Save].



Process Period: 1 min History: 3 months Save Close

Processes

List of process names.

Output Fields

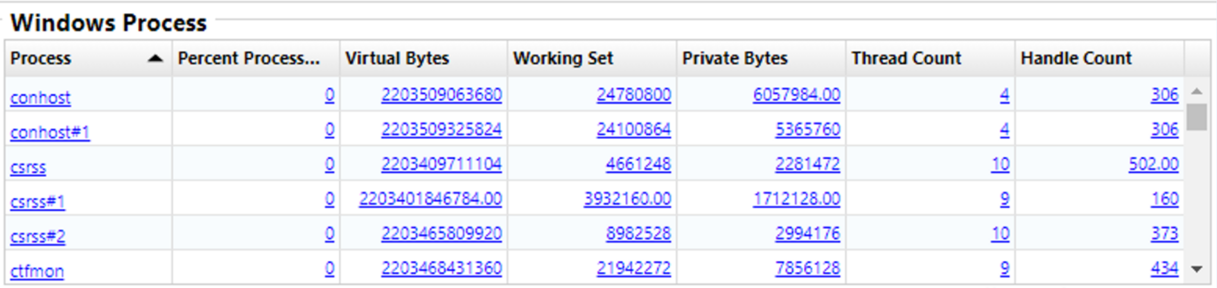
Show Advanced Metrics

	Name	Type
☑	Percent_Processor_Time	float
□	Percent_User_Time	float
☑	Virtual_Bytes	float
☑	Working_Set	float
☑	Private_Bytes	float
☑	Thread_Count	float

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.



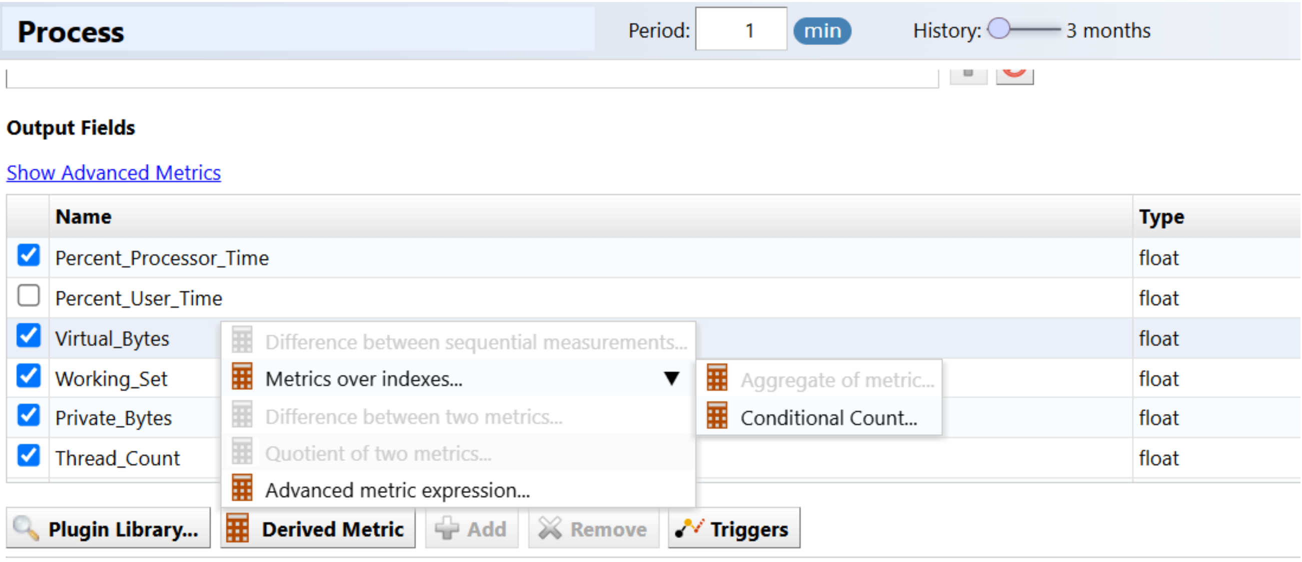
Windows Process

Process	Percent Process...	Virtual Bytes	Working Set	Private Bytes	Thread Count	Handle Count
conhost	0	2203509063680	24780800	6057984.00	4	306
conhost#1	0	2203509325824	24100864	5365760	4	306
csrss	0	2203409711104	4661248	2281472	10	502.00
csrss#1	0	2203401846784.00	3932160.00	1712128.00	9	160
csrss#2	0	2203465809920	8982528	2994176	10	373
ctfmon	0	2203468431360	21942272	7856128	9	434

17.12 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].



Process

Period: 1 min History: 3 months

Output Fields

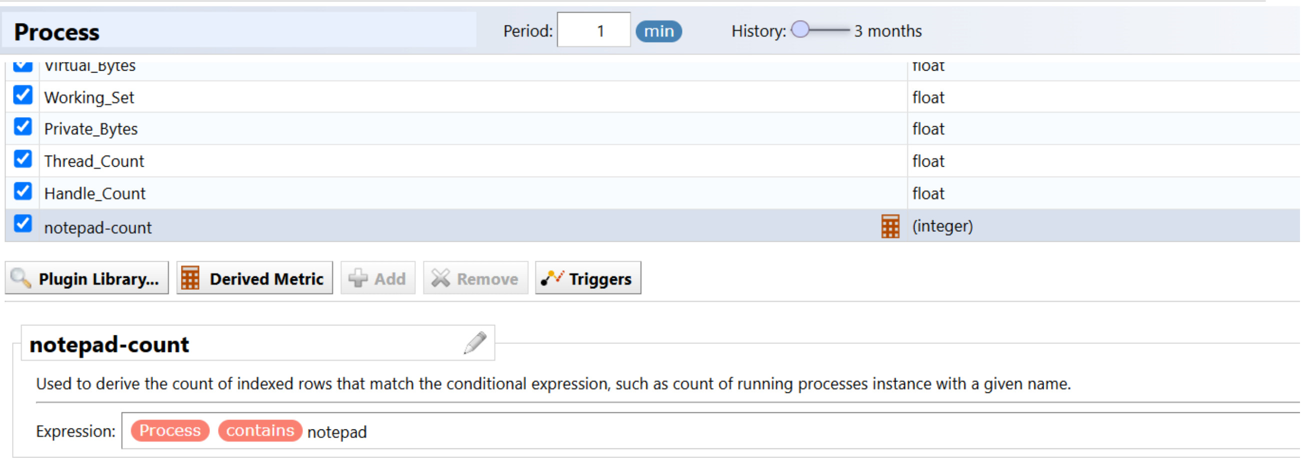
Show Advanced Metrics

	Name	Type
☑	Percent_Processor_Time	float
□	Percent_User_Time	float
☑	Virtual_Bytes	float
☑	Working_Set	float
☑	Private_Bytes	float
☑	Thread_Count	float

Difference between sequential measurements...
Metrics over indexes...
Difference between two metrics...
Quotient of two metrics...
Advanced metric expression...
Aggregate of metric...
Conditional Count...
Plugin Library...
Derived Metric
Add
Remove
Triggers

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`)



Process   Period: 1 min   History: 3 months

☑	Virtual_Bytes	float
☑	Working_Set	float
☑	Private_Bytes	float
☑	Thread_Count	float
☑	Handle_Count	float
☑	notepad-count	(integer)

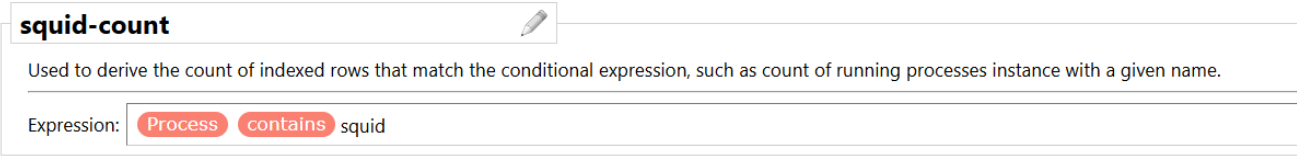
notepad-count

Used to derive the count of indexed rows that match the conditional expression, such as count of running processes instance with a given name.

Expression: Process contains notepad

- **For Windows**, set the process name to “Process”.

Setting calculation formula example: `process contains {Process name}`



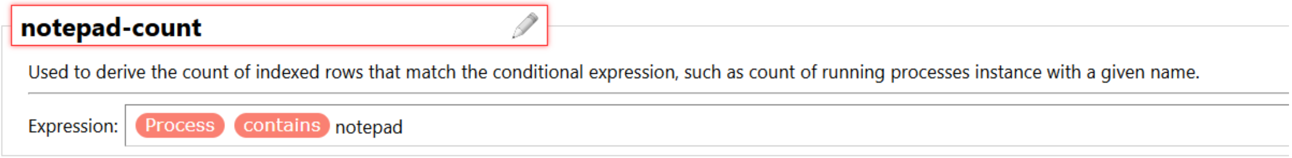
squid-count

Used to derive the count of indexed rows that match the conditional expression, such as count of running processes instance with a given name.

Expression: Process contains squid

- **For Linux**, set the process name to “process_name”.

Setting calculation formula example: `process_name contains {Process name}`

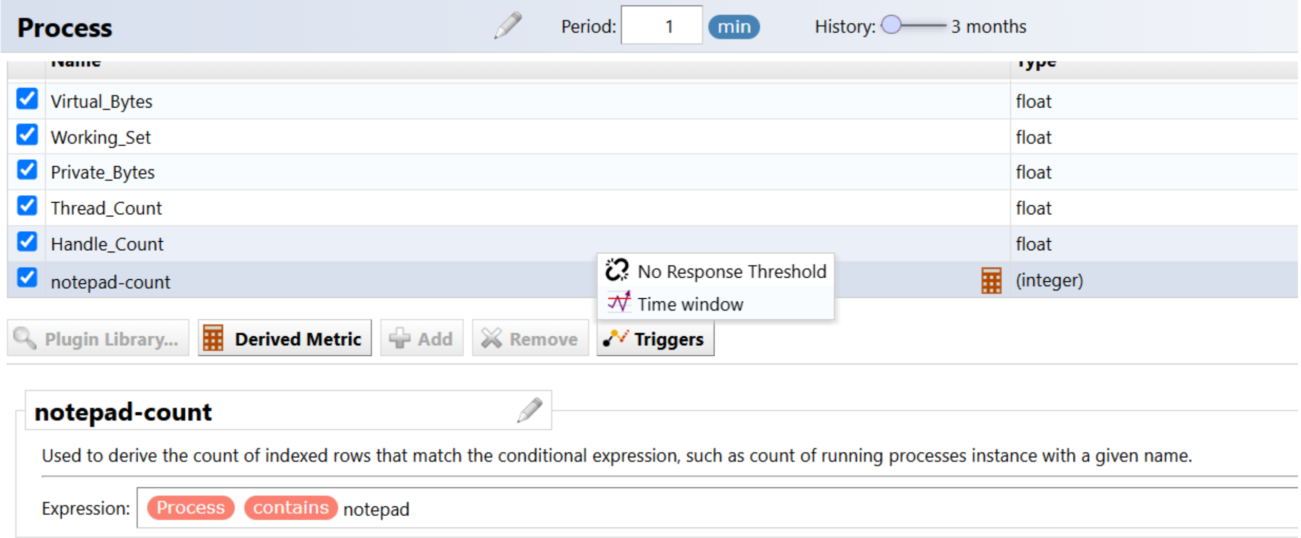


notepad-count

Used to derive the count of indexed rows that match the conditional expression, such as count of running processes instance with a given name.

Expression: Process contains notepad

4. Click [Trigger] > [Time Window].



Process

Period: 1 min

History: 3 months

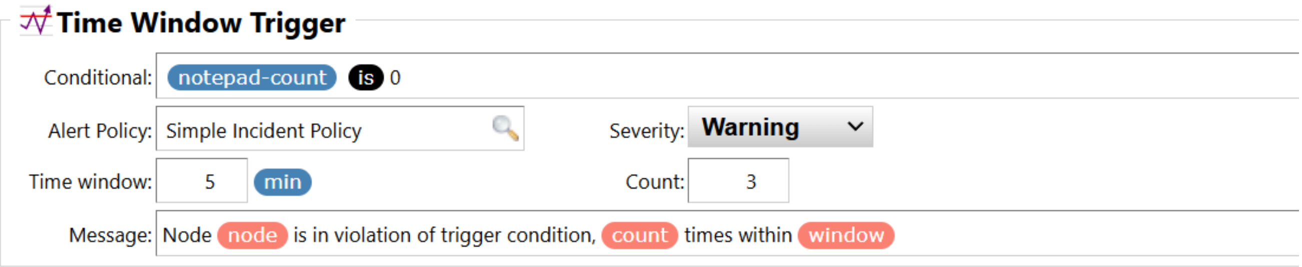
	Name	Type
☑	Virtual_Bytes	float
☑	Working_Set	float
☑	Private_Bytes	float
☑	Thread_Count	float
☑	Handle_Count	float
☑	notepad-count	(integer)

notepad-count

Used to derive the count of indexed rows that match the conditional expression, such as count of running processes instance with a given name.

Expression: Process contains notepad

5. Once the Count has been set, set conditions using metrics.



Time Window Trigger

Conditional: notepad-count is 0

Alert Policy: Simple Incident Policy

Severity: Warning

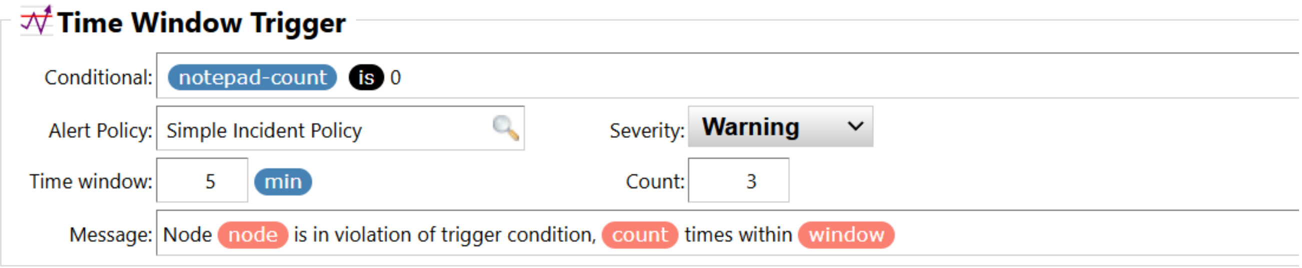
Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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”).



Time Window Trigger

Conditional: notepad-count is 0

Alert Policy: Simple Incident Policy

Severity: Warning

Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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].

17.13 Text Log Monitoring

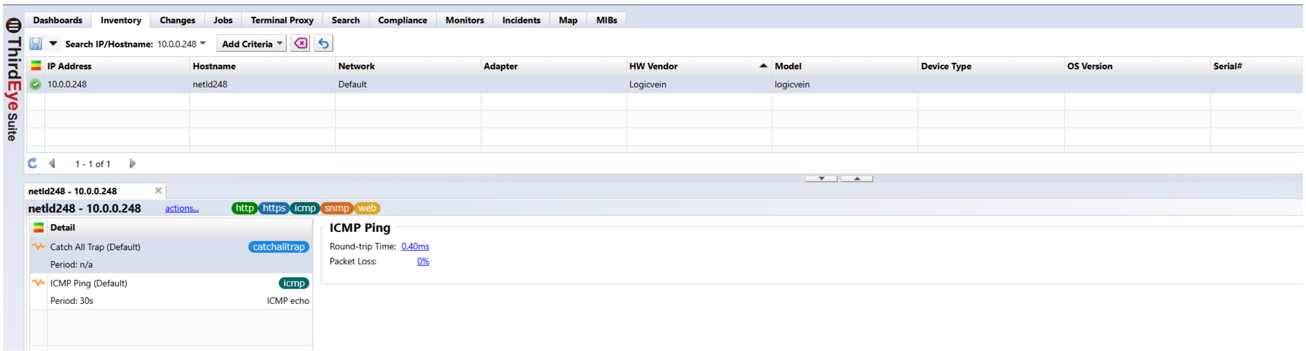
Use Agent-D to obtain log information for the installed server. You can issue an alert when a log containing a specific string is detected.

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.



Search IP/Hostname: 10.0.0.248

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#
10.0.0.248	netld248	Default		Logicvein	logicvein			

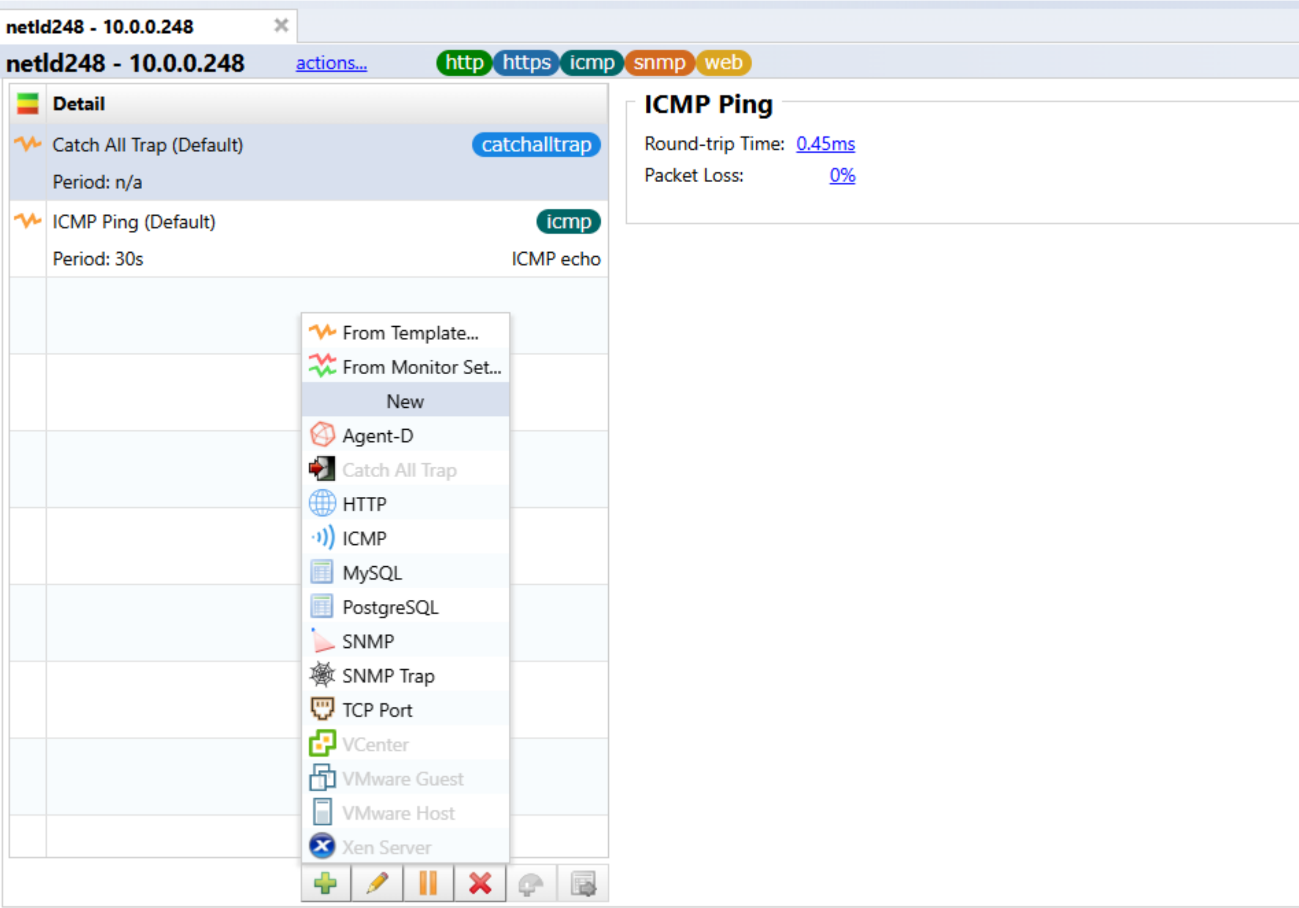
netld248 - 10.0.0.248

Catch All Trap (Default)
Period: n/a

ICMP Ping (Default)
Period: 30s ICMP echo

ICMP Ping
Round-trip Time: 0.40ms
Packet Loss: 0%

2. click the ✚ button, then click [Agent-D].



Catch All Trap (Default)
Period: n/a

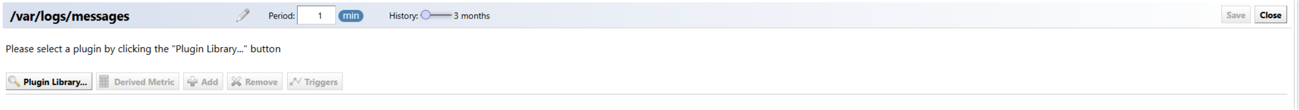
ICMP Ping (Default)
Period: 30s
ICMP echo

ICMP Ping
Round-trip Time: 0.45ms
Packet Loss: 0%

3. Enter any monitor name, and set the interval and data retention period.

The [Period] field, specifies the interval.

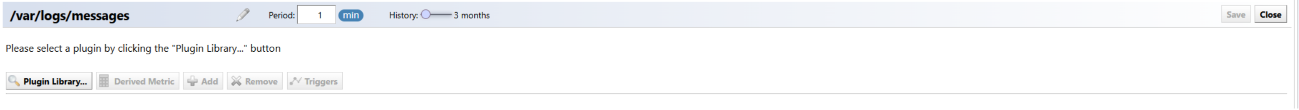
The [History] slider specifies a data retention period of 3, 6, or 12 months.



/var/logs/messages
Period: 1 min
History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

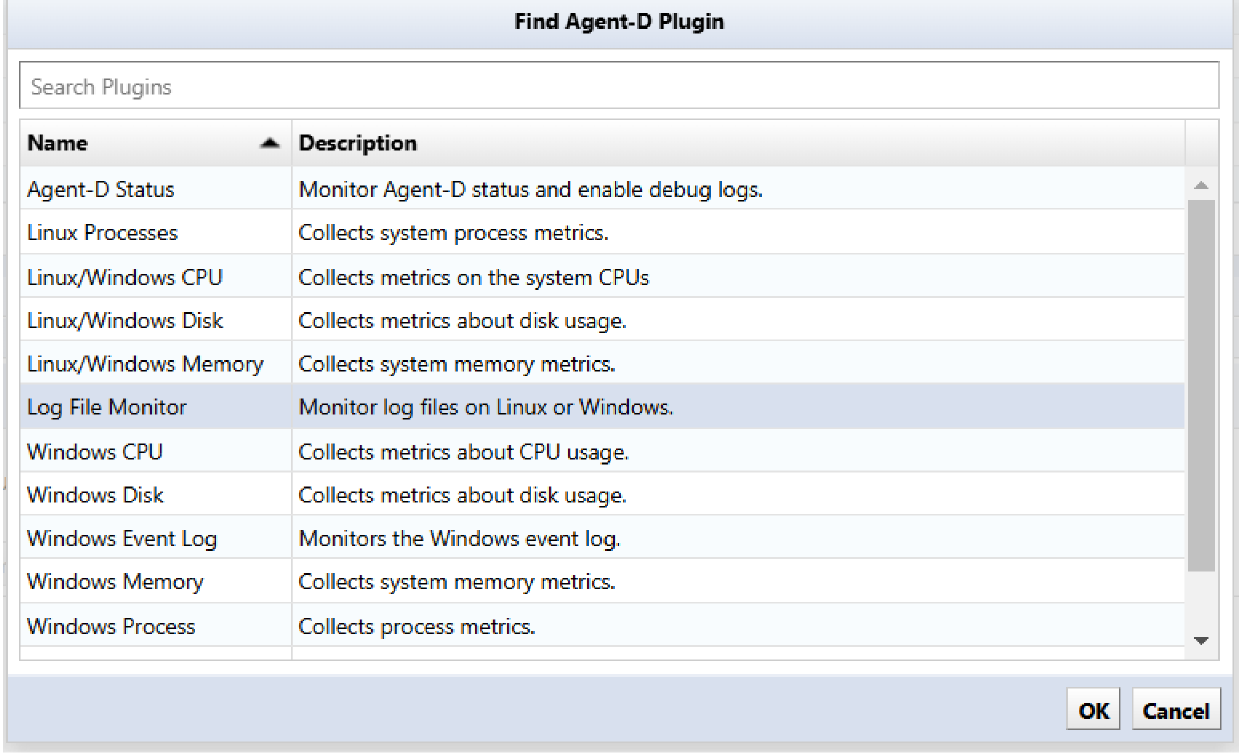
4. Click [Plugin Library …].



/var/logs/messages
Period: 1 min
History: 3 months

Please select a plugin by clicking the "Plugin Library..." button

5. Select [Log Fie Monitor] and click [OK].

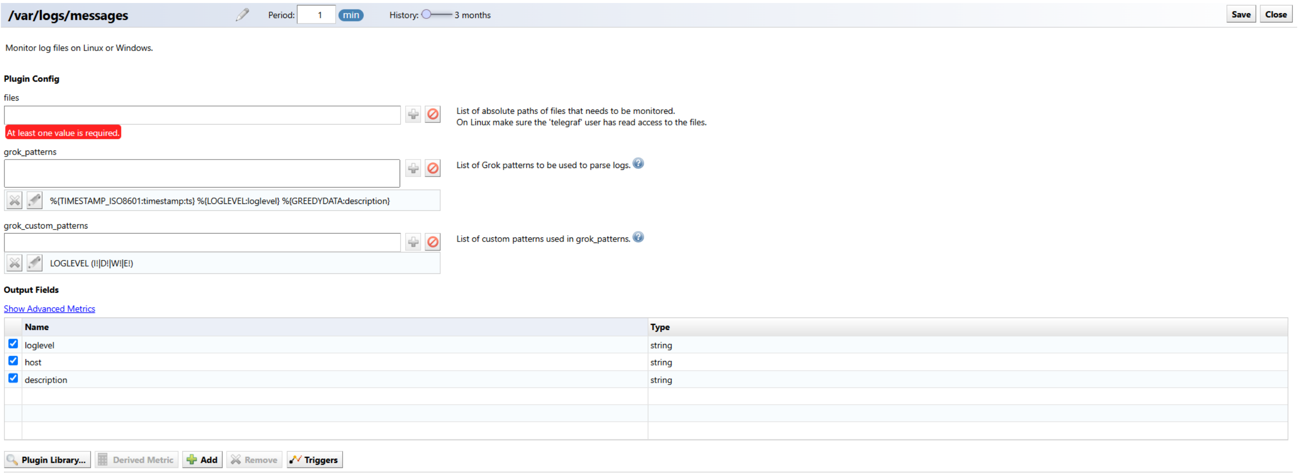


Find Agent-D Plugin

Name	Description
Agent-D Status	Monitor Agent-D status and enable debug logs.
Linux Processes	Collects system process metrics.
Linux/Windows CPU	Collects metrics on the system CPUs
Linux/Windows Disk	Collects metrics about disk usage.
Linux/Windows Memory	Collects system memory metrics.
Log File Monitor	Monitor log files on Linux or Windows.
Windows CPU	Collects metrics about CPU usage.
Windows Disk	Collects metrics about disk usage.
Windows Event Log	Monitors the Windows event log.
Windows Memory	Collects system memory metrics.
Windows Process	Collects process metrics.

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.



/var/logs/messages

Period: 1 min History: 3 months

Monitor log files on Linux or Windows.

Plugin Config

files

At least one value is required.

List of absolute paths of files that needs to be monitored.
On Linux make sure the 'telegraf' user has read access to the files.

grok_patterns

%{TIMESTAMP_ISO8601:timestamp:ts} %{LOGLEVEL:loglevel} %{GREEDYDATA:description}

List of Grok patterns to be used to parse logs.

grok_custom_patterns

LOGLEVEL (I!|D!|W!|E!)

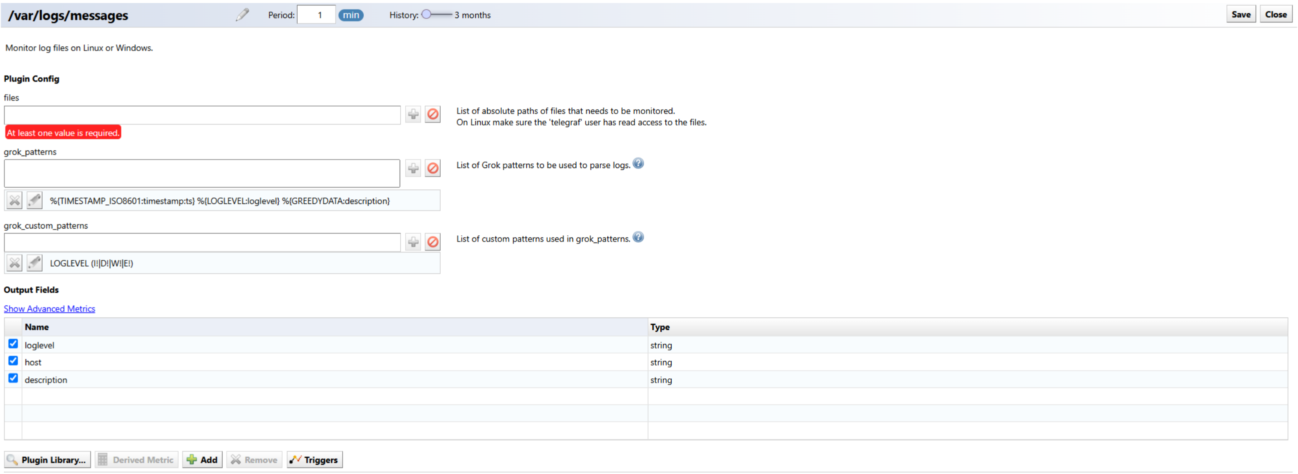
List of custom patterns used in grok_patterns.

Output Fields

Show Advanced Metrics

	Name	Type
☑	loglevel	string
☑	host	string
☑	description	string

7. Enter grok_patterns and grok_custom_patterns.



Monitor log files on Linux or Windows.

Plugin Config

files

At least one value is required.

List of absolute paths of files that needs to be monitored.
On Linux make sure the 'telegraf' user has read access to the files.

grok_patterns

```
%{TIMESTAMP_ISO8601:timestamp:ts} %{LOGLEVEL:loglevel} %{GREEDYDATA:description}
```

List of Grok patterns to be used to parse logs.

grok_custom_patterns

```
LOGLEVEL (I!|D!|W!|E!)
```

List of custom patterns used in grok_patterns.

Output Fields

Show Advanced Metrics

	Name	Type
☑	loglevel	string
☑	host	string
☑	description	string

17.14 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.

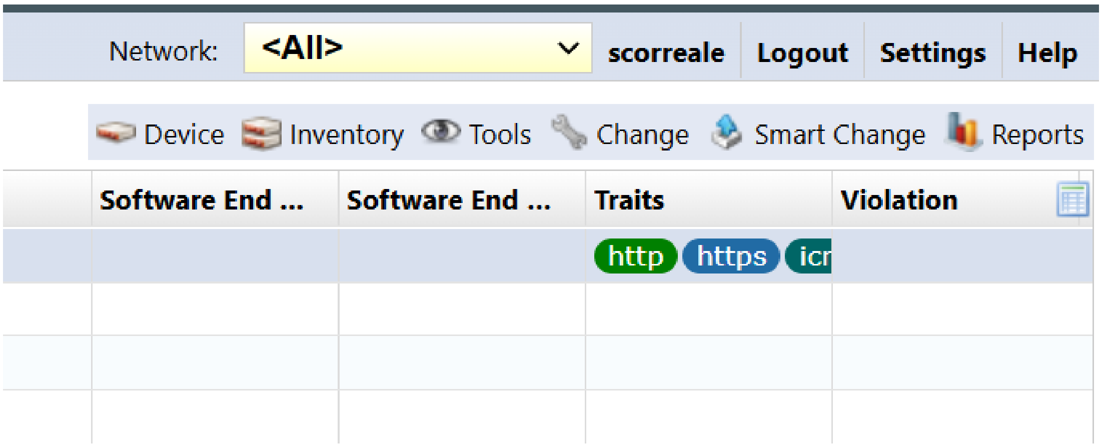
The following templates are registered in advance as monitors for HDD monitoring on the [Monitors] > [Templates] tab.

- ThirdEye Syslog Monitor

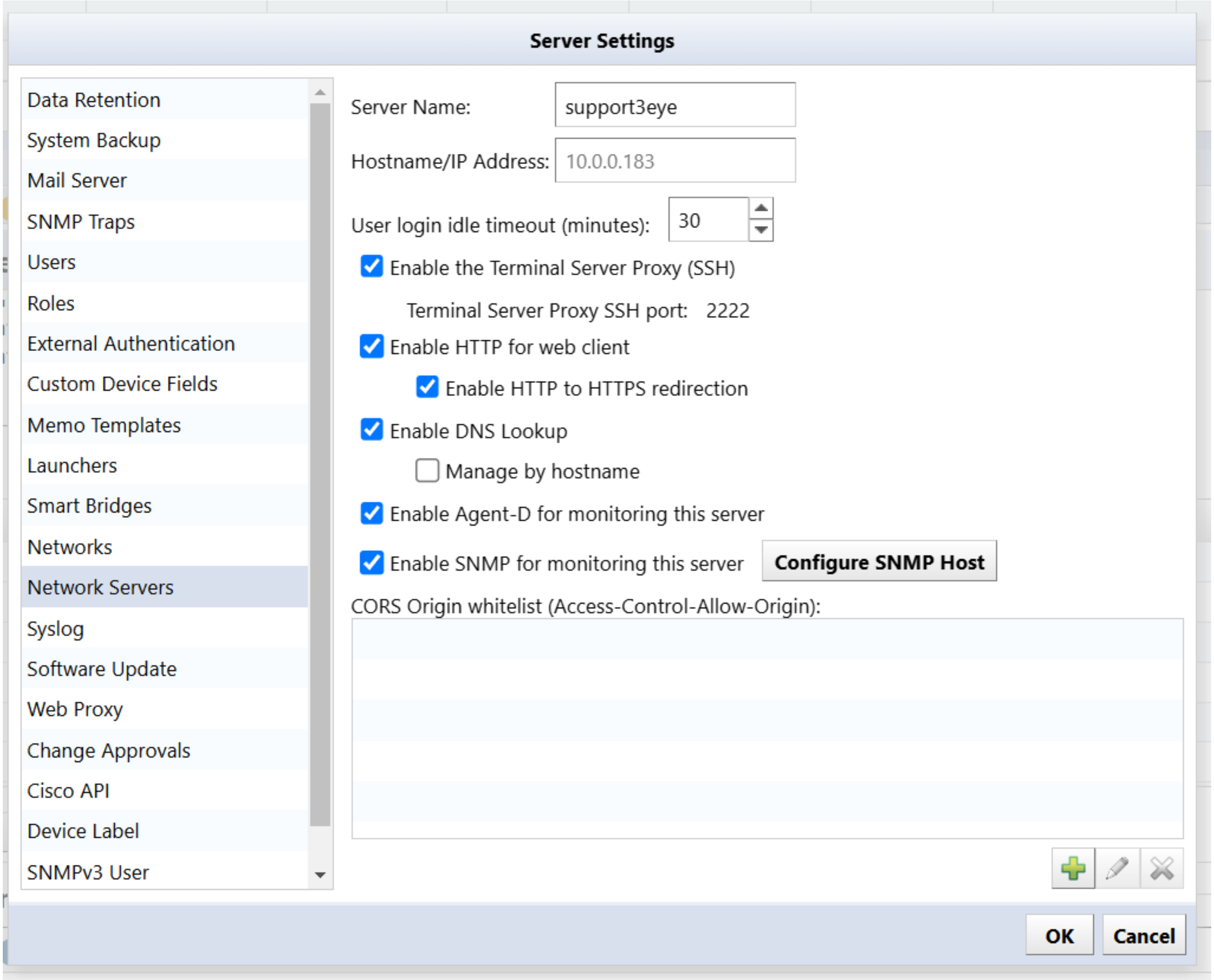
Agent-D is pre-installed on ThirdEye, but is disabled by default. If you want to enable/disable Agent-D, you must restart ThirdEye.

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].



Server Settings

Server Name: support3eye

Hostname/IP Address: 10.0.0.183

User login idle timeout (minutes): 30

☑ Enable the Terminal Server Proxy (SSH)

Terminal Server Proxy SSH port: 2222

☑ Enable HTTP for web client

☑ Enable HTTP to HTTPS redirection

☑ Enable DNS Lookup

□ Manage by hostname

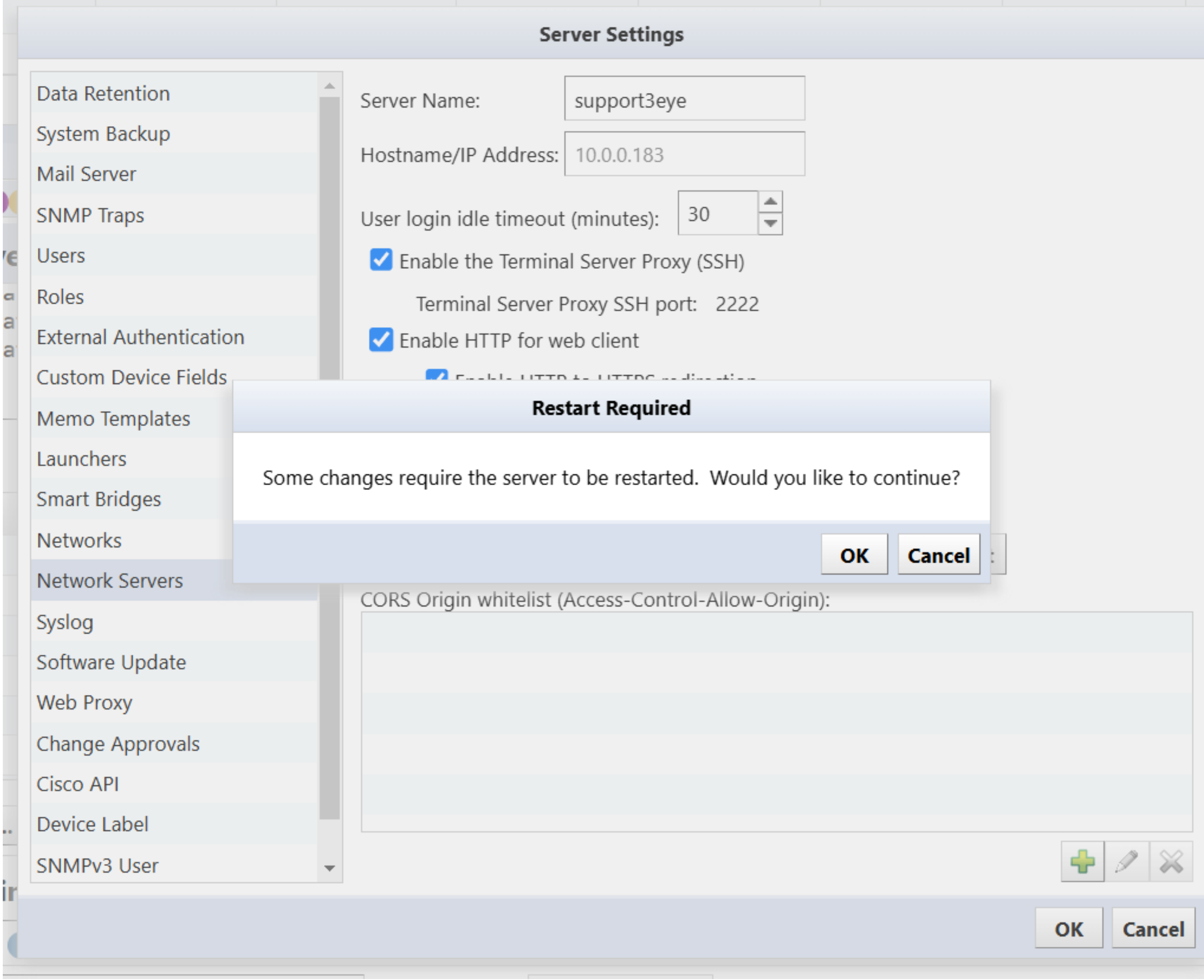
☑ Enable Agent-D for monitoring this server

☑ Enable SNMP for monitoring this server

CORS Origin whitelist (Access-Control-Allow-Origin):

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.



Server Settings

Server Name: support3eye

Hostname/IP Address: 10.0.0.183

User login idle timeout (minutes): 30

☑ Enable the Terminal Server Proxy (SSH)

Terminal Server Proxy SSH port: 2222

☑ Enable HTTP for web client

CORS Origin whitelist (Access-Control-Allow-Origin):

Restart Required

Some changes require the server to be restarted. Would you like to continue?

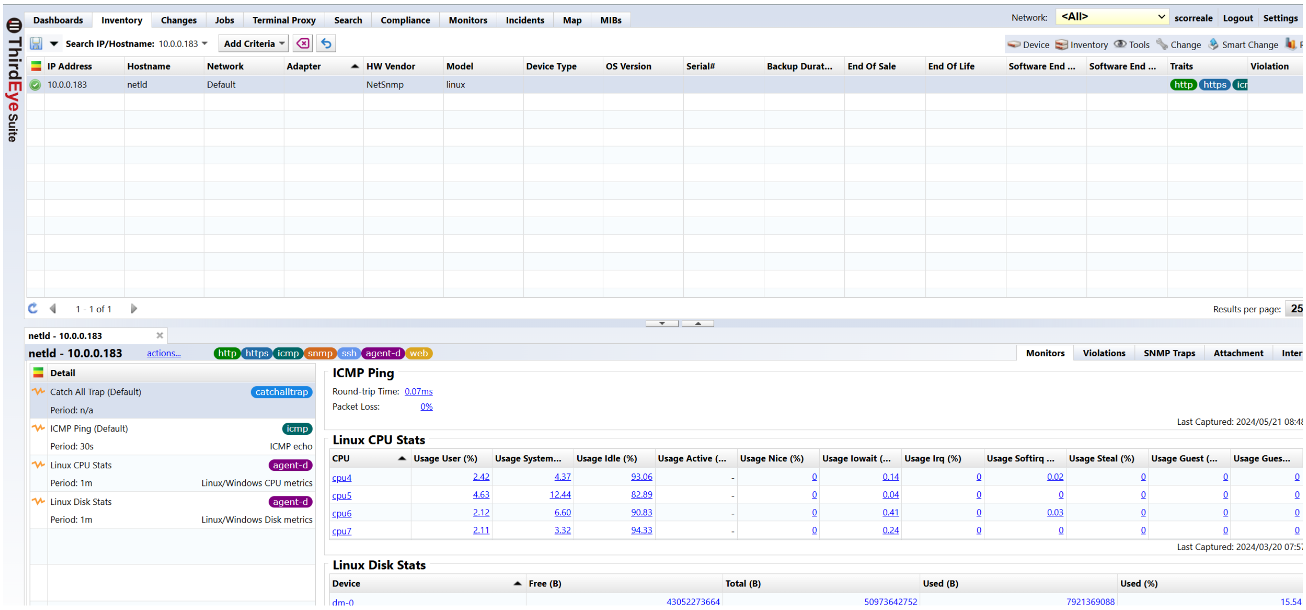
4. Check for the message "Restarting services …" and wait a few minutes.

A login screen will be displayed.

5. After logging in, click the [Inventory] main tab.

6. Register ThirdEye's own IP address as a monitored device from [Inventory] > [Add Device].

7. Doubleclick to open device details.



Search IP/Hostname: 10.0.0.183

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.183	netld	Default		NetSnmp	linux									http https icr	

1 - 1 of 1

Results per page: 25

netld - 10.0.0.183

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo
Linux CPU Stats Period: 1m	agent-d Linux/Windows CPU metrics
Linux Disk Stats Period: 1m	agent-d Linux/Windows Disk metrics

ICMP Ping

Round-trip Time: 0.07ms

Packet Loss: 0%

Last Captured: 2024/05/21 08:4

Linux CPU Stats

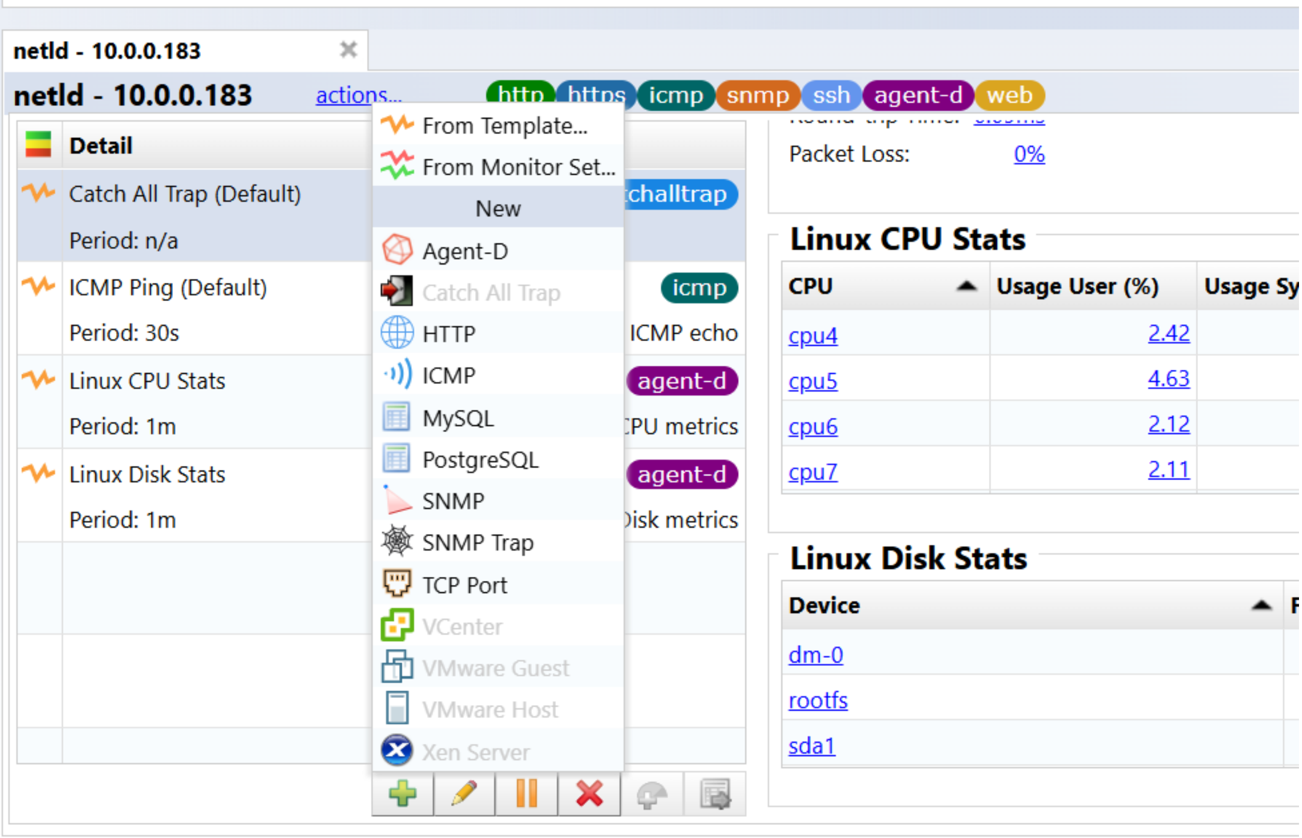
CPU	Usage User (%)	Usage System...	Usage Idle (%)	Usage Active (...	Usage Nice (%)	Usage Iowait (...	Usage Irq (%)	Usage Softirq ...	Usage Steal (%)	Usage Guest (...	Usage Gues...
cpu4	2.42	4.37	93.06	-	0	0.14	0	0.02	0	0	0
cpu5	4.63	12.44	82.89	-	0	0.04	0	0	0	0	0
cpu6	2.12	6.60	90.83	-	0	0.41	0	0.03	0	0	0
cpu7	2.11	3.32	94.33	-	0	0.24	0	0	0	0	0

Last Captured: 2024/03/20 07:5

Linux Disk Stats

Device	Free (B)	Total (B)	Used (B)	Used (%)
dm-0	43052273664	50973642752	7921369088	15.54

8. click the ✚ button, and then click [Add from Template].



netld - 10.0.0.183

Detail	
Catch All Trap (Default) Period: n/a	catchalltrap
ICMP Ping (Default) Period: 30s	icmp ICMP echo
Linux CPU Stats Period: 1m	agent-d CPU metrics
Linux Disk Stats Period: 1m	agent-d Disk metrics

Packet Loss: 0%

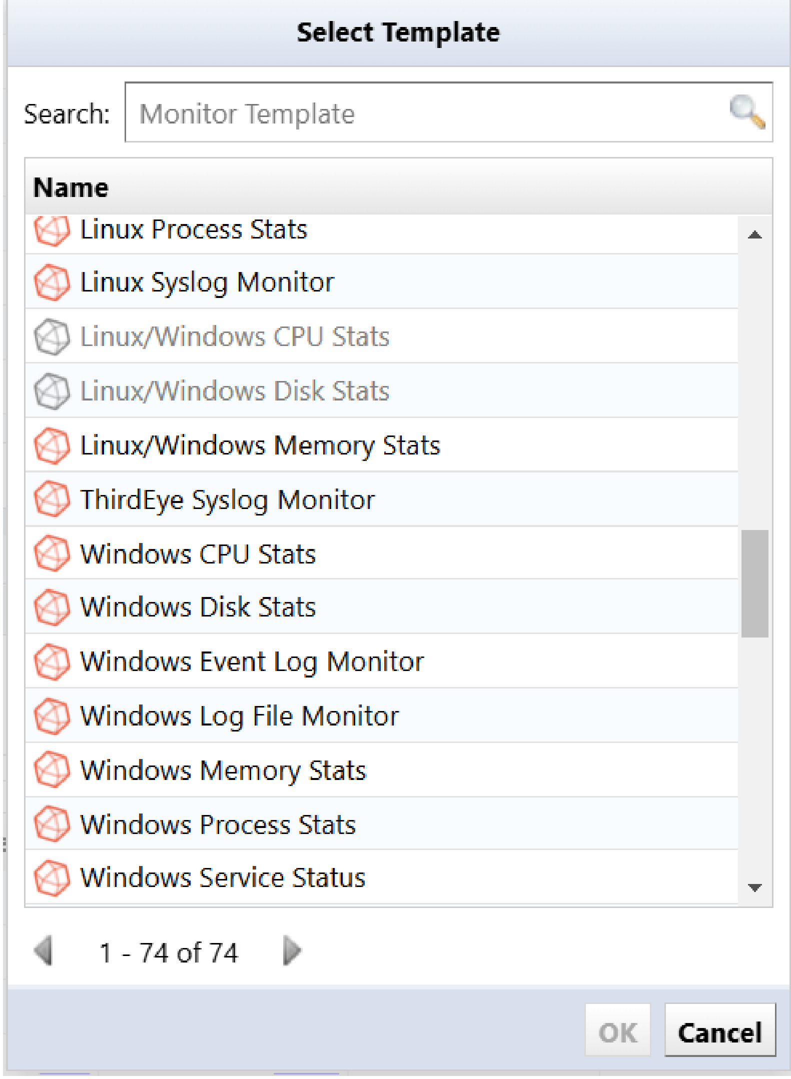
Linux CPU Stats

CPU	Usage User (%)	Usage Sy
cpu4	2.42	
cpu5	4.63	
cpu6	2.12	
cpu7	2.11	

Linux Disk Stats

Device	F
dm-0	
rootfs	
sda1	

9. Select ThirdEye Syslog Monitor and click [OK].



Select Template

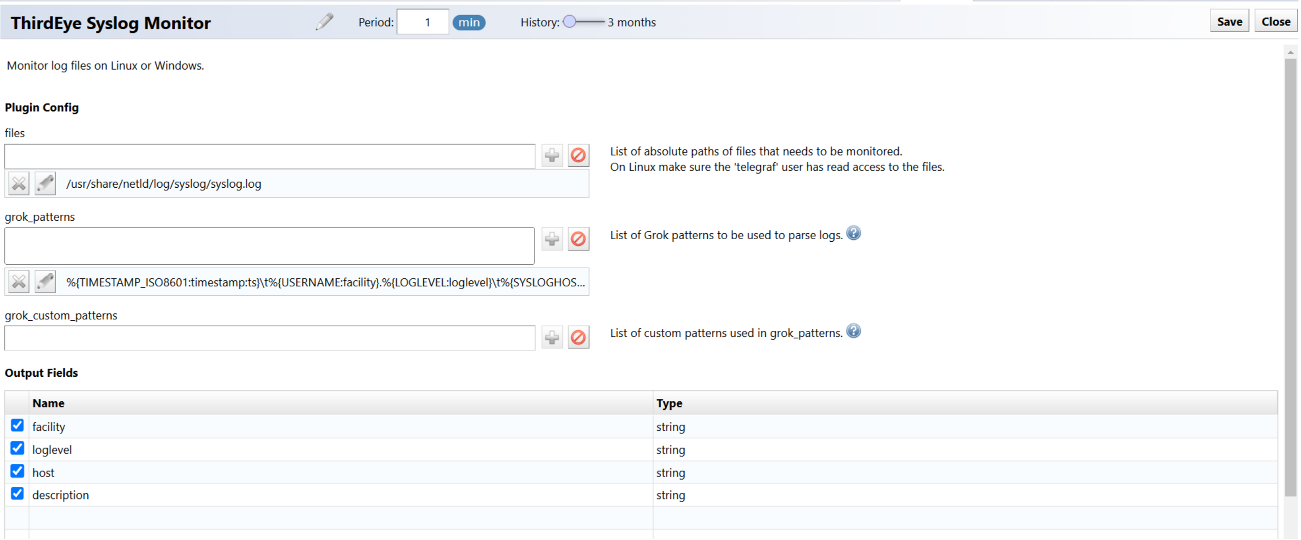
Search: Monitor Template

Name
Linux Process Stats
Linux Syslog Monitor
Linux/Windows CPU Stats
Linux/Windows Disk Stats
Linux/Windows Memory Stats
ThirdEye Syslog Monitor
Windows CPU Stats
Windows Disk Stats
Windows Event Log Monitor
Windows Log File Monitor
Windows Memory Stats
Windows Process Stats
Windows Service Status

1 - 74 of 74

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.



ThirdEye Syslog Monitor

Period: 1 min

History: 3 months

Monitor log files on Linux or Windows.

Plugin Config

files

/usr/share/netld/log/syslog/syslog.log

List of absolute paths of files that needs to be monitored.
On Linux make sure the 'telegraf' user has read access to the files.

grok_patterns

%{TIMESTAMP_ISO8601:timestamp:ts}\t%{USERNAME:facility}.%{LOGLEVEL:loglevel}\t%{SYSLOGHOS...

List of Grok patterns to be used to parse logs.

grok_custom_patterns

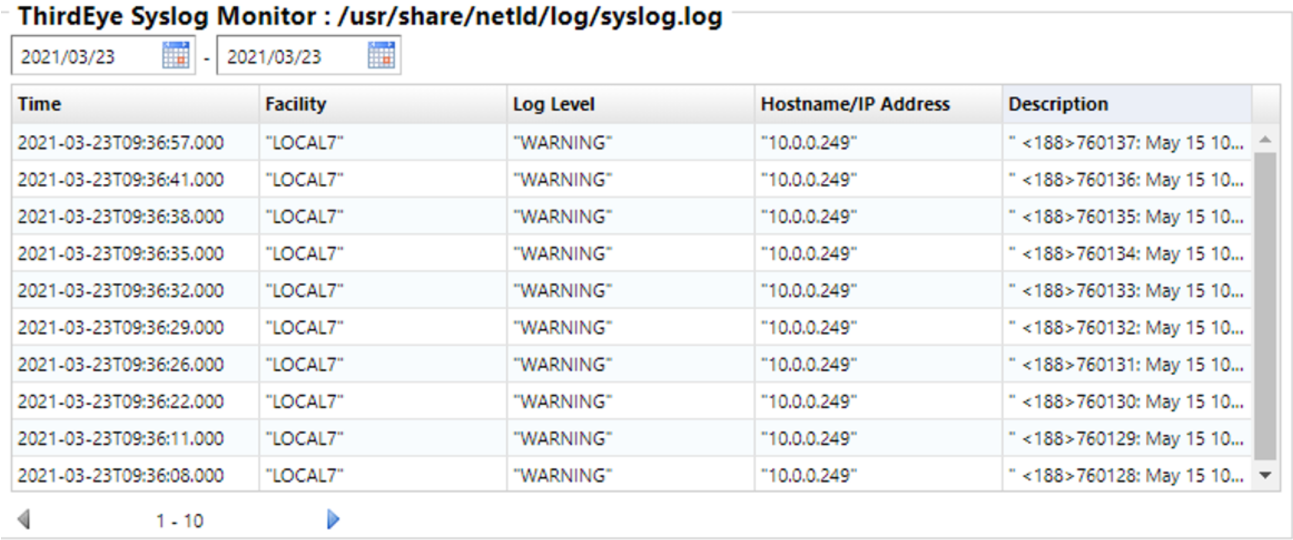
List of custom patterns used in grok_patterns.

Output Fields

	Name	Type
☑	facility	string
☑	loglevel	string
☑	host	string
☑	description	string

With the above steps, you can obtain the Syslog information sent to ThirdEye.

Syslog messages are displayed in the “Conditional” field.



ThirdEye Syslog Monitor : /usr/share/netld/log/syslog.log

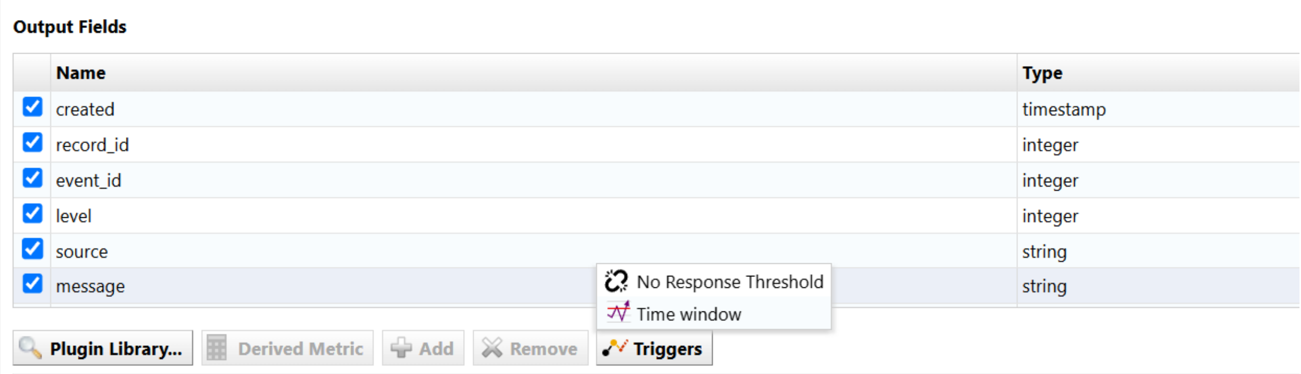
2021/03/23 - 2021/03/23

Time	Facility	Log Level	Hostname/IP Address	Description
2021-03-23T09:36:57.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760137: May 15 10...
2021-03-23T09:36:41.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760136: May 15 10...
2021-03-23T09:36:38.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760135: May 15 10...
2021-03-23T09:36:35.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760134: May 15 10...
2021-03-23T09:36:32.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760133: May 15 10...
2021-03-23T09:36:29.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760132: May 15 10...
2021-03-23T09:36:26.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760131: May 15 10...
2021-03-23T09:36:22.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760130: May 15 10...
2021-03-23T09:36:11.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760129: May 15 10...
2021-03-23T09:36:08.000	"LOCAL7"	"WARNING"	"10.0.0.249"	" <188>760128: May 15 10...

17.15 Trigger Message Alert

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.

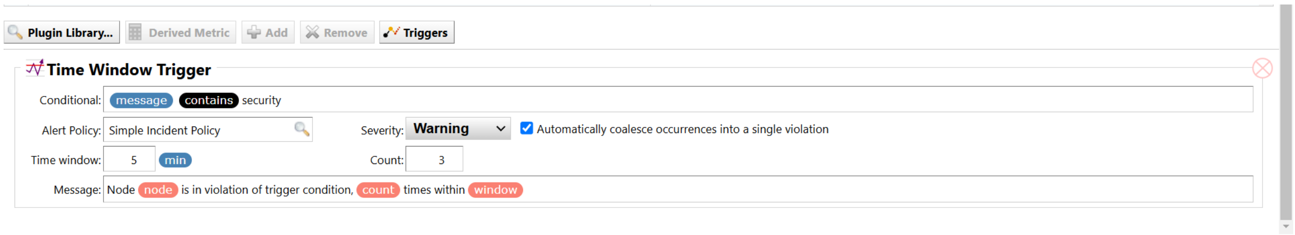
1. Doubleclick the event log monitor to open it.
2. Click [Trigger] > [Time window].



Output Fields

	Name	Type
☑	created	timestamp
☑	record_id	integer
☑	event_id	integer
☑	level	integer
☑	source	string
☑	message	string

3. Set conditions in the "Conditional" field.



Time Window Trigger

Conditional: message contains security

Alert Policy: Simple Incident Policy

Severity: Warning

☑ Automatically coalesce occurrences into a single violation

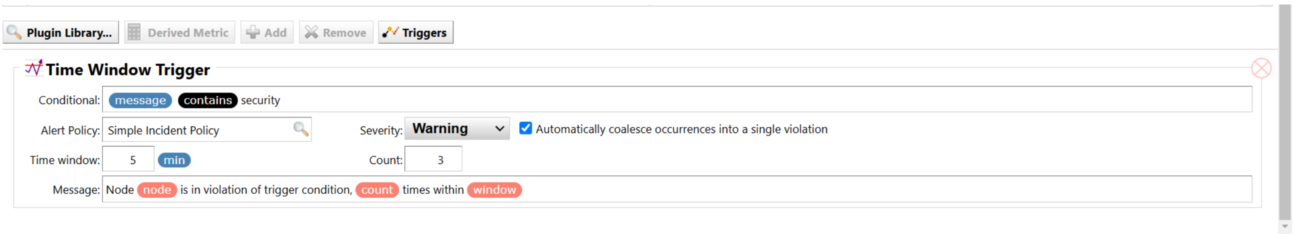
Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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”).



Time Window Trigger

Conditional: message contains security

Alert Policy: Simple Incident Policy

Severity: Warning

☑ Automatically coalesce occurrences into a single violation

Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

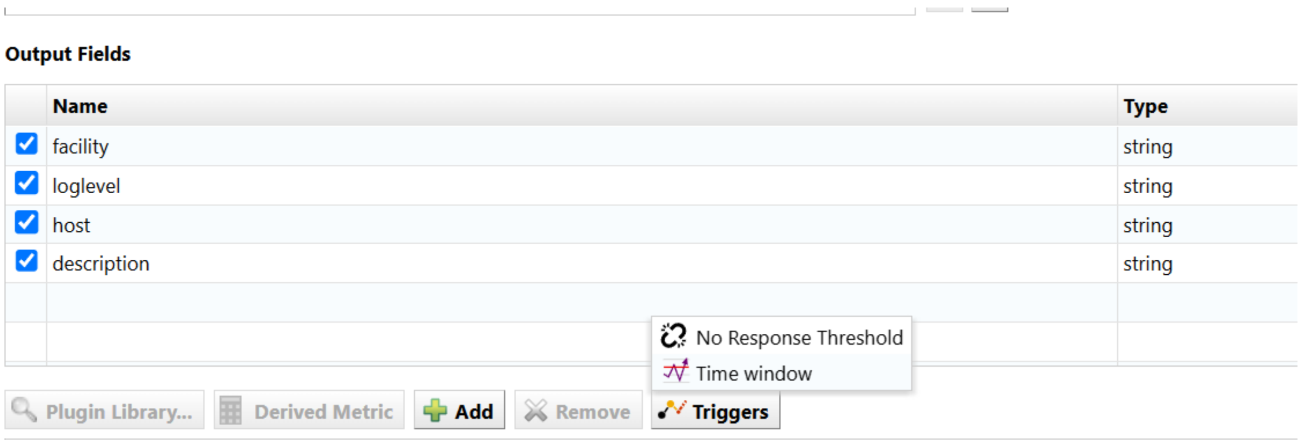
Item	Description
Time window	Set the period for executing the process. (Minimum value: 1 minute) The period that is used as the basis for counting how many times the process defined in the policy must be executed within a specified period of failure.
Count	Set the number of times the process must fail 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].

17.16 Trigger Description Alert

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.

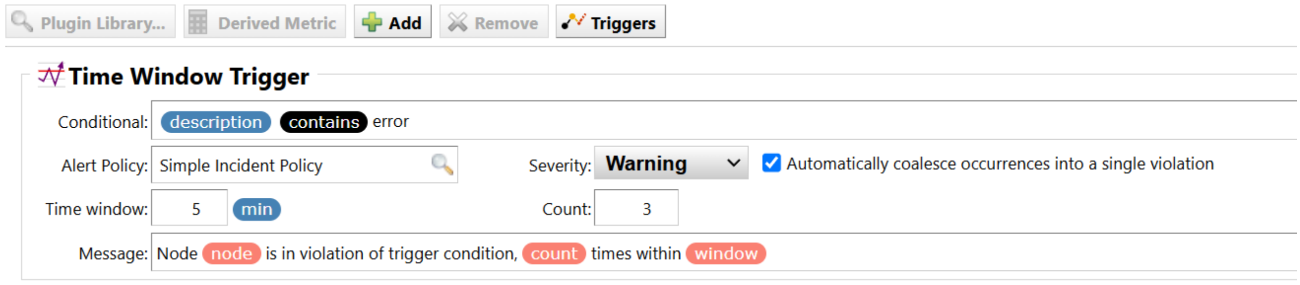
1. Doubleclick the [ThirdEye Syslog Monitor] monitor to open it.
2. Click [Trigger] > [Time window].



Output Fields

	Name	Type
☑	facility	string
☑	loglevel	string
☑	host	string
☑	description	string

3. Set the “Conditionnal” using `description`.



Time Window Trigger

Conditional: description contains error

Alert Policy: Simple Incident Policy

Severity: Warning

☑ Automatically coalesce occurrences into a single violation

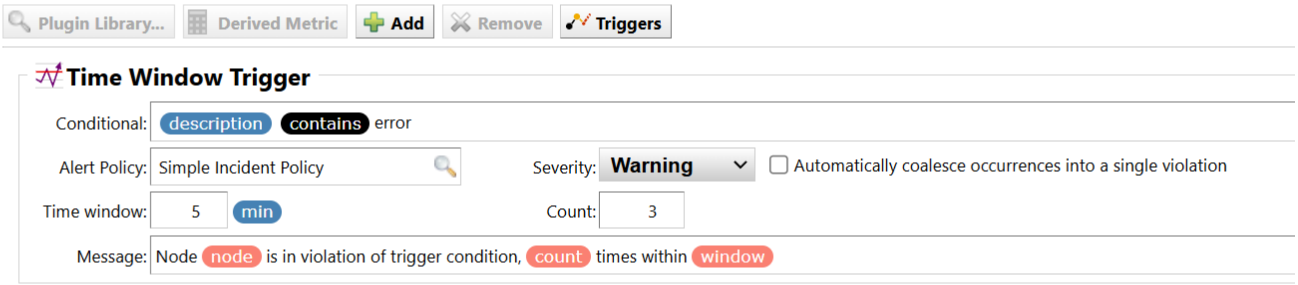
Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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”.



Time Window Trigger

Conditional: description contains error

Alert Policy: Simple Incident Policy

Severity: Warning

□ Automatically coalesce occurrences into a single violation

Time window: 5 min

Count: 3

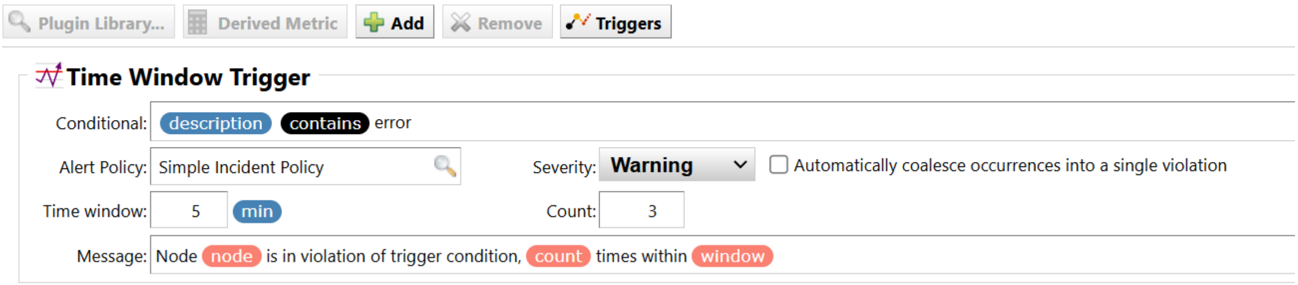
Message: Node node is in violation of trigger condition, count times within window

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”).



Time Window Trigger

Conditional: description contains error

Alert Policy: Simple Incident Policy

Severity: Warning

□ Automatically coalesce occurrences into a single violation

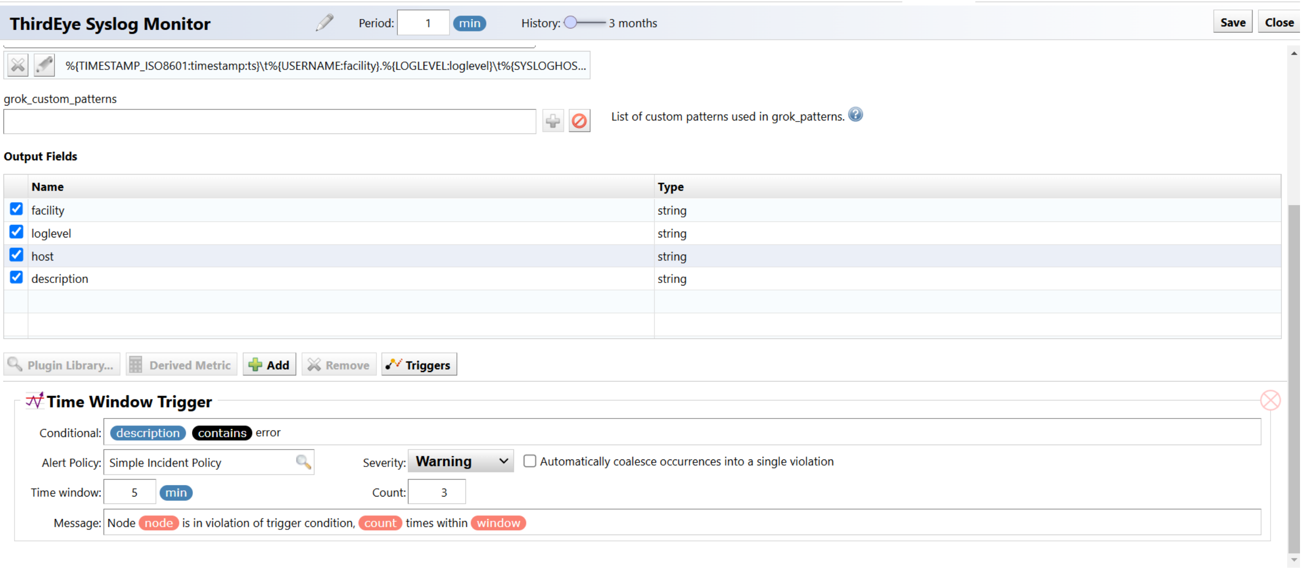
Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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].



ThirdEye Syslog Monitor

Period: 1 min History: 3 months

%{TIMESTAMP_ISO8601:timestamp:ts}\t%{USERNAME:facility}.%{LOGLEVEL:loglevel}\t%{SYSLOGHOS...

grok_custom_patterns

List of custom patterns used in grok_patterns.

Output Fields

	Name	Type
☑	facility	string
☑	loglevel	string
☑	host	string
☑	description	string

Time Window Trigger

Conditional: description contains error

Alert Policy: Simple Incident Policy

Severity: Warning

□ Automatically coalesce occurrences into a single violation

Time window: 5 min

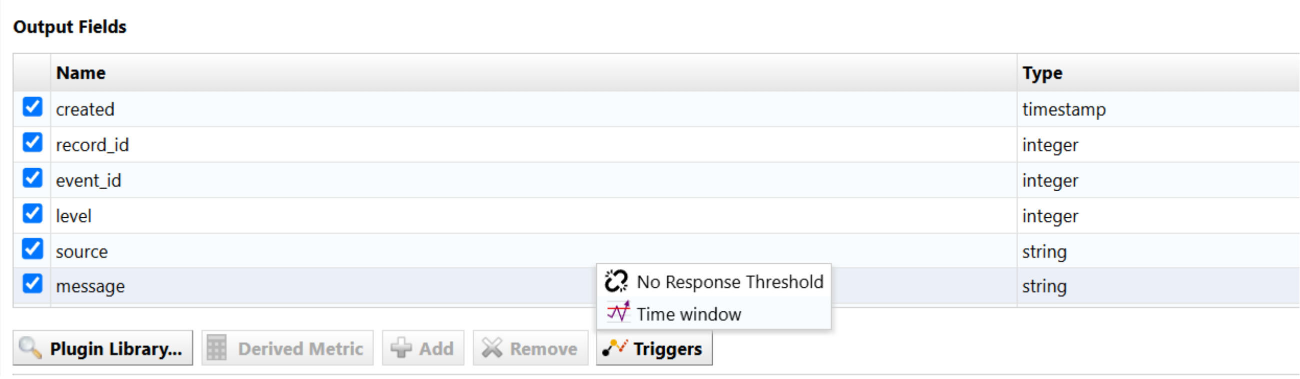
Count: 3

Message: Node node is in violation of trigger condition, count times within window

17.17 Log Level Alert

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.

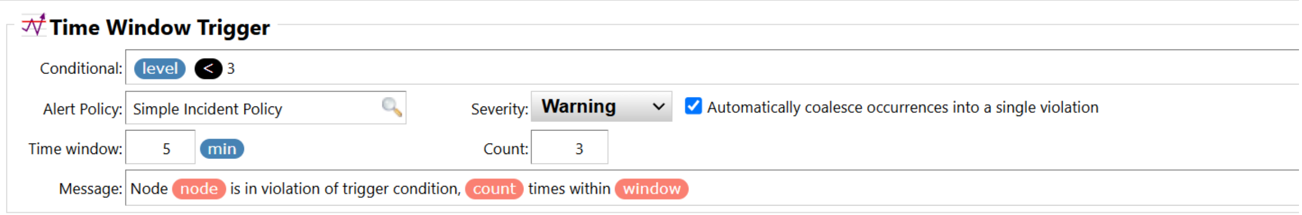
1. Doubleclick the event log monitor to open it.
2. Click [Trigger] > [Time window].



Output Fields

	Name	Type
☑	created	timestamp
☑	record_id	integer
☑	event_id	integer
☑	level	integer
☑	source	string
☑	message	string

3. Set the condition using Agent-D’s “level”.



Time Window Trigger

Conditional: level < 3

Alert Policy: Simple Incident Policy

Severity: Warning

☑ Automatically coalesce occurrences into a single violation

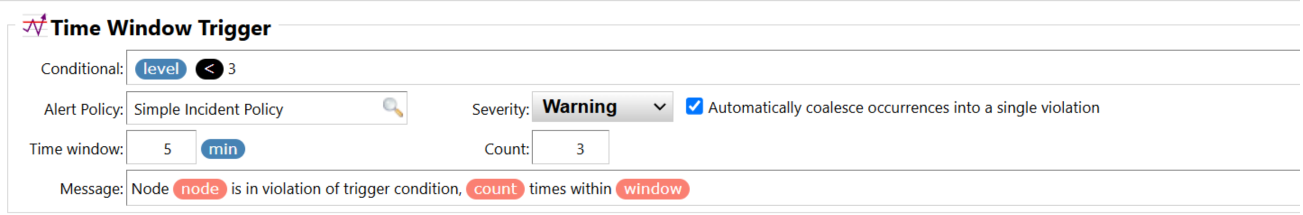
Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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”).



Time Window Trigger

Conditional: level < 3

Alert Policy: Simple Incident Policy

Severity: Warning

☑ Automatically coalesce occurrences into a single violation

Time window: 5 min

Count: 3

Message: Node node is in violation of trigger condition, count times within window

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].

17.18 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:mess
```

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` .

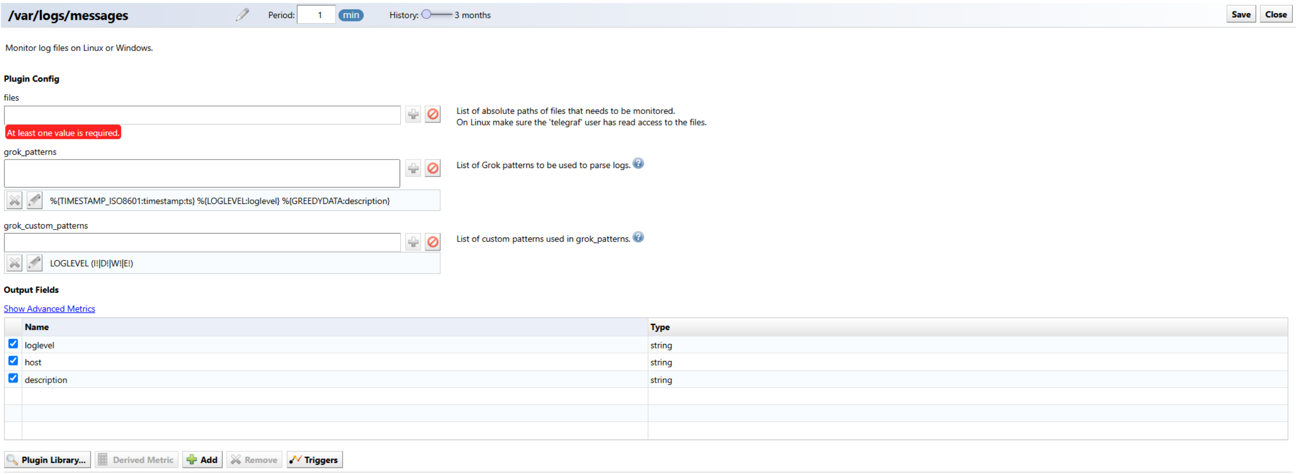
grok_pattern: `%{GREEDYDATA:message}`

17.19 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].



/var/logs/messages

Period: 1 min

History: 3 months

Monitor log files on Linux or Windows.

Plugin Config

files

At least one value is required.

List of absolute paths of files that needs to be monitored.
On Linux make sure the 'telegraf' user has read access to the files.

grok_patterns

%{TIMESTAMP_ISO8601:timestamp:ts} %{LOGLEVEL:loglevel} %{GREEDYDATA:description}

List of Grok patterns to be used to parse logs.

grok_custom_patterns

LOGLEVEL (I!|D!|W!|E!)

List of custom patterns used in grok_patterns.

Output Fields

Show Advanced Metrics

	Name	Type
☑	loglevel	string
☑	host	string
☑	description	string

Now, Agent-D will send log information and you can check it in the device details.

SECTION 18

WMI (WINDOWS MANAGEMENT INSTRUMENTATION) MONITORING

WMI Monitoring is the process of collecting system information from Windows devices using Windows Management Instrumentation, including metrics like CPU, memory, disk, and service status.

ThirdEye uses the HTTP/SOAP based WS-Management protocol to retrieve Windows Management Instrumentation(WMI) objects.

The following objects can be retrieved currently:

- Win32_PerfFormattedData_PerfOS_Processor (CPU Monitoring)
- Win32_PerfFormattetedData_PerfDisk_LogicalDisk (Disk Monitor)
- Win32_PerfFormattedData_PerfOS_Memory (Memory Monitoring)
- Win32_PerfFormattedData_PerfProc_Process (Process Monitoring)

18.1 WinRM (Windows Remote Management)

18.1.1 Default Configuration

The Windows Remote Management (WinRM) service is required to remotely manage Windows systems. Currently, WinRM is already installed on systems supported by Microsoft.

First, run `winrm quickconfig` from the command prompt or Powershell to set the default configuration for WinRMConfiguration:

After executing, 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
```

18.1.2 Non-Secure HTTP Connections

By default, only encrypted traffic is allowed. If you want to monitor using HTTP, execute the following to allow unencrypted traffic:

```
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

```
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
```

18.1.3 Basic Authentication Settings

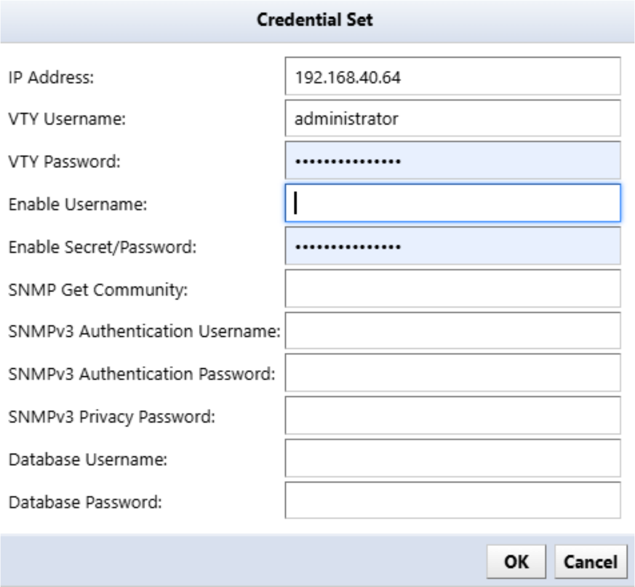
If you want to use Basic authentication, run `winrm set winrm/config/service/auth '@{Basic="true}'` . If the system is not joined to a domain (WORKGROUP), enable Basic authentication:

```
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
```

18.2 WMI 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".



Credential Set

IP Address:	192.168.40.64
VTY Username:	administrator
VTY Password:	•••••••••••••••
Enable Username:	
Enable Secret/Password:	•••••••••••••••
SNMP Get Community:	
SNMPv3 Authentication Username:	
SNMPv3 Authentication Password:	
SNMPv3 Privacy Password:	
Database Username:	
Database Password:	

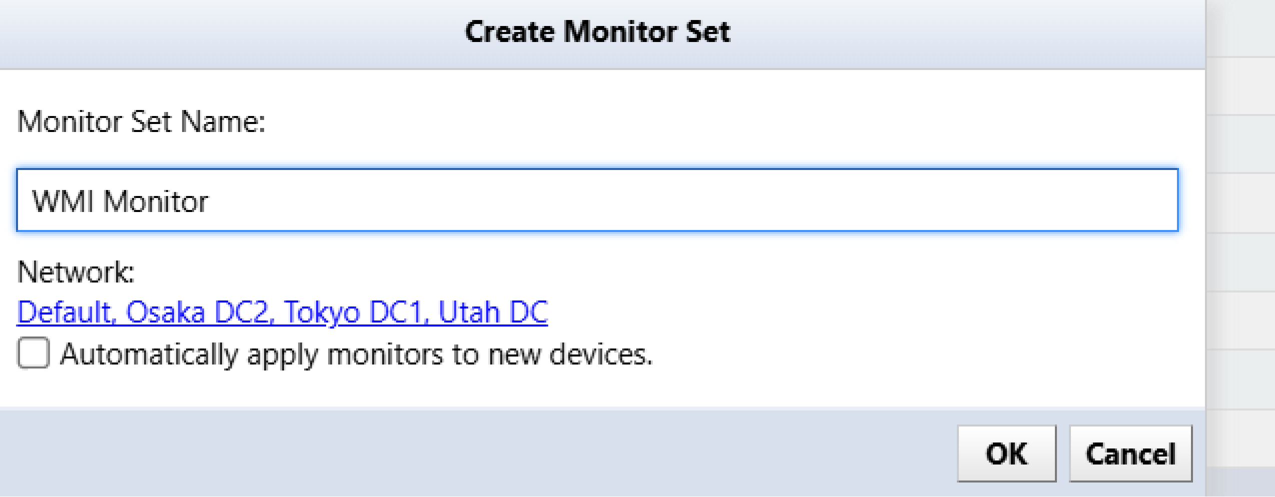
Monitors using WMI support the following monitoring functions:

- Windows Disk (collects disk usage metrics)
- Windows Memory (collects system memory metrics)
- Windows Processor (collect CPU usage metrics)
- Windows Process (Collect metrics for processes)

18.3 Add WMI Monitor

Monitors can be added to the device details screen and monitor sets in the same way as other monitors. The following describes the procedure for adding monitors using monitor sets.

1. Click the [Monitor] main tab.
2. Click the [Sets] subtab.
3. Click **Add** to open the [Create Monitor Set] window, and add a monitor set.



Create Monitor Set

Monitor Set Name:

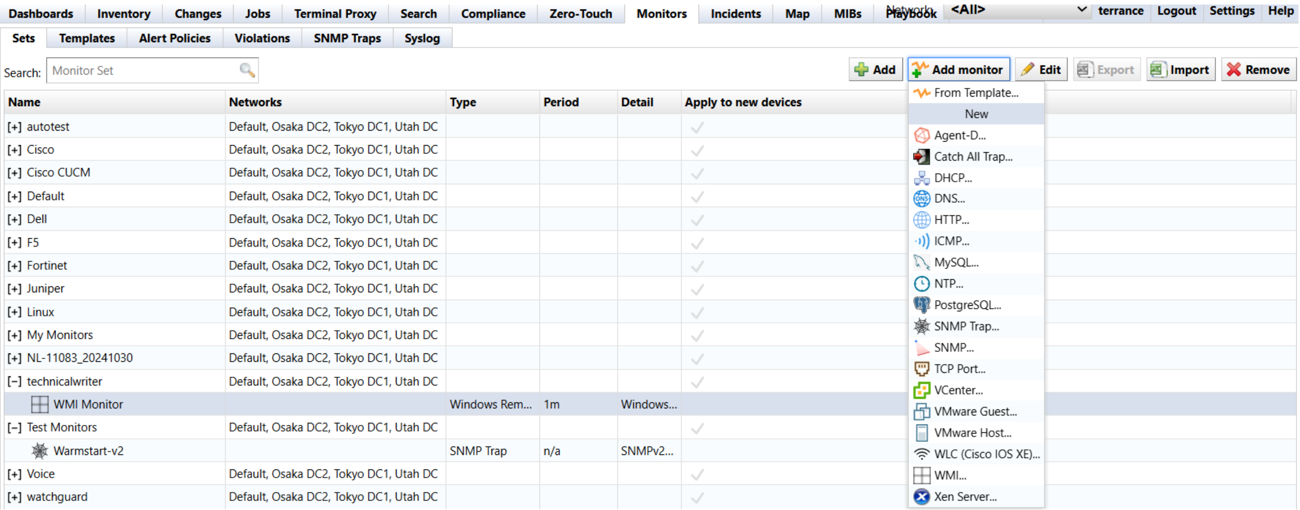
WMI Monitor

Network:

Default, Osaka DC2, Tokyo DC1, Utah DC

□ Automatically apply monitors to new devices.

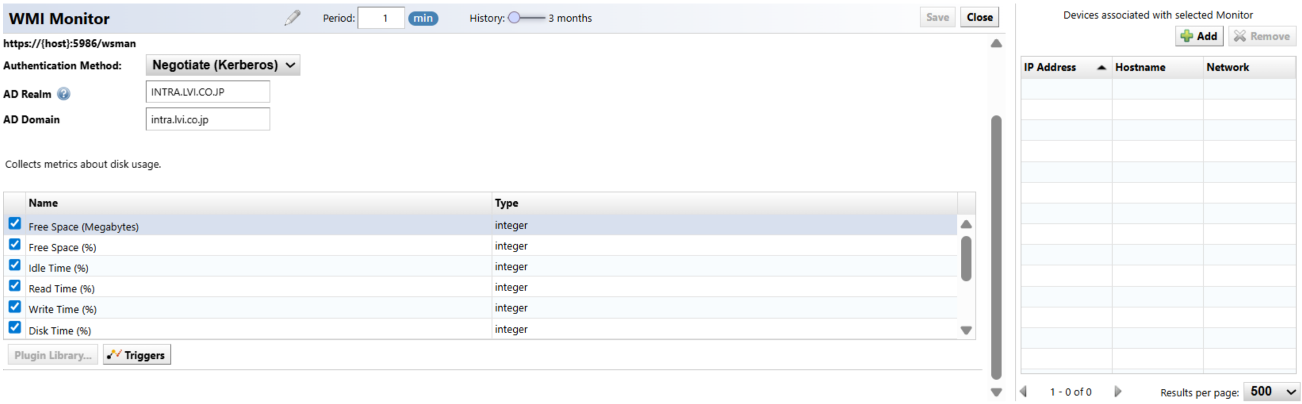
4. Click the added monitor set, then click [Add Monitor] > [WMI].



Search: Monitor Set

Name	Networks	Type	Period	Detail	Apply to new devices
[+] autotest	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Cisco	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Cisco CUCM	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Default	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Dell	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] F5	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Fortinet	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Juniper	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] Linux	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] My Monitors	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] NL-11083_20241030	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[–] technicalwriter	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
WMI Monitor		Windows Rem...	1m	Windows...	
[–] Test Monitors	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
Warmstart-v2		SNMP Trap	n/a	SNMPv2...	
[+] Voice	Default, Osaka DC2, Tokyo DC1, Utah DC				✓
[+] watchguard	Default, Osaka DC2, Tokyo DC1, Utah DC				✓

5. Set the monitor name, interval, data storage period, and optional triggers.



Period: 1 min

History: 3 months

https://{host}:5986/wsman

Authentication Method: Negotiate (Kerberos)

AD Realm: INTRA.LVI.CO.JP

AD Domain: intra.lvi.co.jp

Collects metrics about disk usage.

	Name	Type
☑	Free Space (Megabytes)	integer
☑	Free Space (%)	integer
☑	Idle Time (%)	integer
☑	Read Time (%)	integer
☑	Write Time (%)	integer
☑	Disk Time (%)	integer

IP Address	Hostname	Network

1 - 0 of 0

Results per page: 500

The following metrics can be obtained by each plugin for a monitor:

Plugin	Metric	Description
Windows Disk		Uses Win32_PerfFormattedData_PerfDisk_Logic class
	Free Space (Megabytes)	Refers to “FreeMegabytes”
	Free Space (%)	Refers to “PercentFreeSpace”
	Idle Time (%)	Refers to “PercentIdleTime”
	Read Time (%)	Refers to “PercentDiskReadTime”
	Write Time (%)	Refers to “PercentDiskWriteTime”
	Disk Time (%)	Refers to “PercentDiskTime”
	Bytes Per Second	Refers to “DiskBytesPersec”
	Bytes Read Per Second	Refers to “DiskReadBytesPersec”
	Bytes Written Per Second	Refers to “DiskWriteBytesPersec”
	Reads Per Second	Refers to “DiskReadsPersec”
	Writes Per Second	Refers to “DiskWritesPersec”
Windows Memory		Uses Win32_PerfFormattedData_PerfOS_Memo class

Plugin	Metric	Description
	Bytes Available	Refers to “AvailableBytes”
	Bytes Cached	Refers to “CacheBytes”
	Bytes Committed	Refers to “CommittedBytes”
	Page Faults	Refers to “PageFaultsPersec”
Windows Processor		Uses Win32_PerfRawData_PerfProc_Process class
	Idle Time (%)	Refers to “PercentIdleTime”
	Interrupts Time (%)	Refers to “PercentInterruptTime”
	Privileged Time (%)	Refers to “PercentPrivilegedTime”
	Processor Time (%)	Refers to “PercentProcessorTime”
	User Time (%)	Refers to “PercentUserTime”

6. Click [Plugin Library] to select plugin.
7. Click [OK] > [Save].

18.4 WMI Live Service Monitor

The WMI Live Service Monitor in Thirdeye provides real-time visibility into Windows process activity through WMI (Windows Management Instrumentation). It tracks process creation/termination events, resource utilization (CPU/memory), and parent-child process relationships. This monitor acts as a critical security and operational tool, detecting unauthorized processes, identifying resource bottlenecks, and maintaining compliance through granular process auditing. Integrated with Thirdeye's alerting system, it triggers notifications for abnormal process patterns while correlating data with other system metrics for root cause analysis.

Columns (Metrics)

- Service Name
- Description
- Status
- Startup Type
- Assigned Application

Tooltips

You can mouseover the Service Name for Tooltips that offer further information about the service. Tooltips contains the following information about the Service:

- Name
- Description
- Process Id
- Log On As
- Path
- Services which are dependent on this service

Operations

- Start Service
- Restart Service
- Stop Service

Timing Data

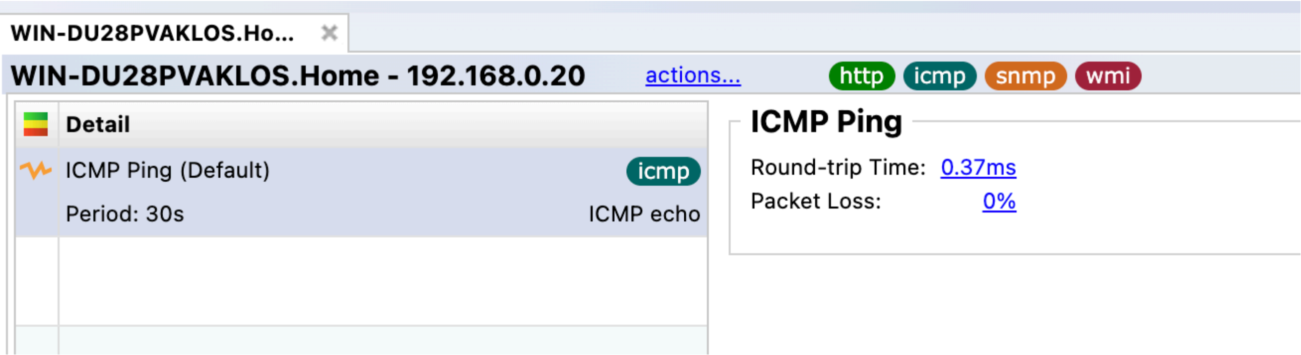
- **Open Live Process Monitor Page**: Monitor setup time about 120s
- **Live Monitor Refresh interval**: Refresh interval about 30s
- **Device Single Process Monitor** (Process instance stopped / started): Poll interval about 30s

18.4.1 Windows Server Credentials

You can configure credentials for the Windows Server in the device credentials settings. Hostname is used for the connection, so the IP address of the Windows VM must be used as the device hostname. Process monitoring is also performed using the Windows server host name.

18.4.2 WinRM Configuration

WMI Live Service Monitor is available for Windows servers that have WinRM enabled and configured. When WinRM is enabled on the Windows Server, performing discovery will add a `wmi` trait to the device.



ICMP Ping (Default)

Period: 30s

ICMP echo

ICMP Ping

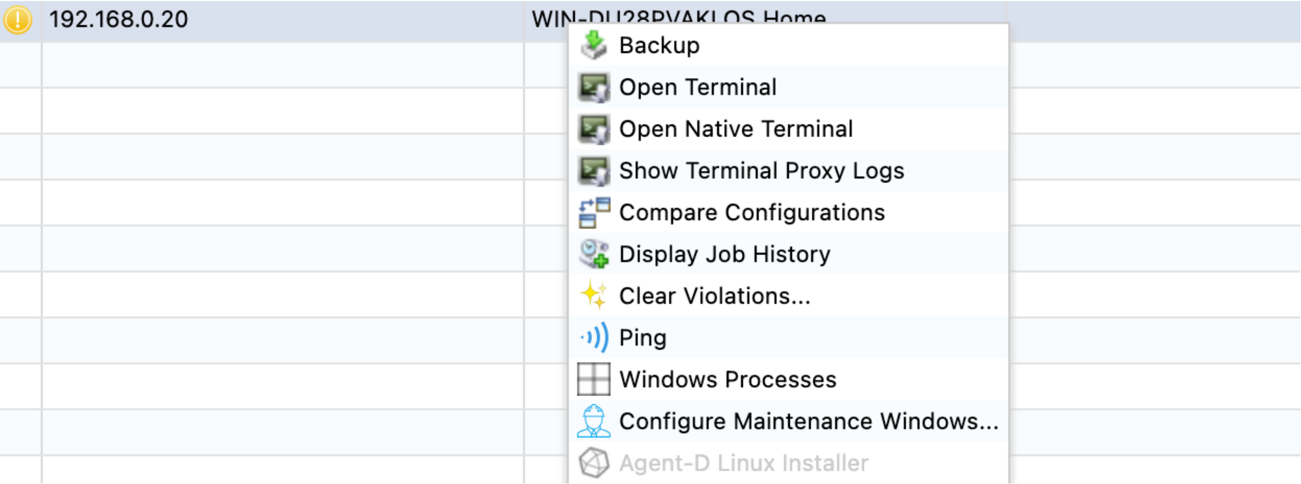
Round-trip Time: 0.37ms

Packet Loss: 0%

18.4.3 Access WMI Live Service Monitor

To access WMI Live Service Monitor:

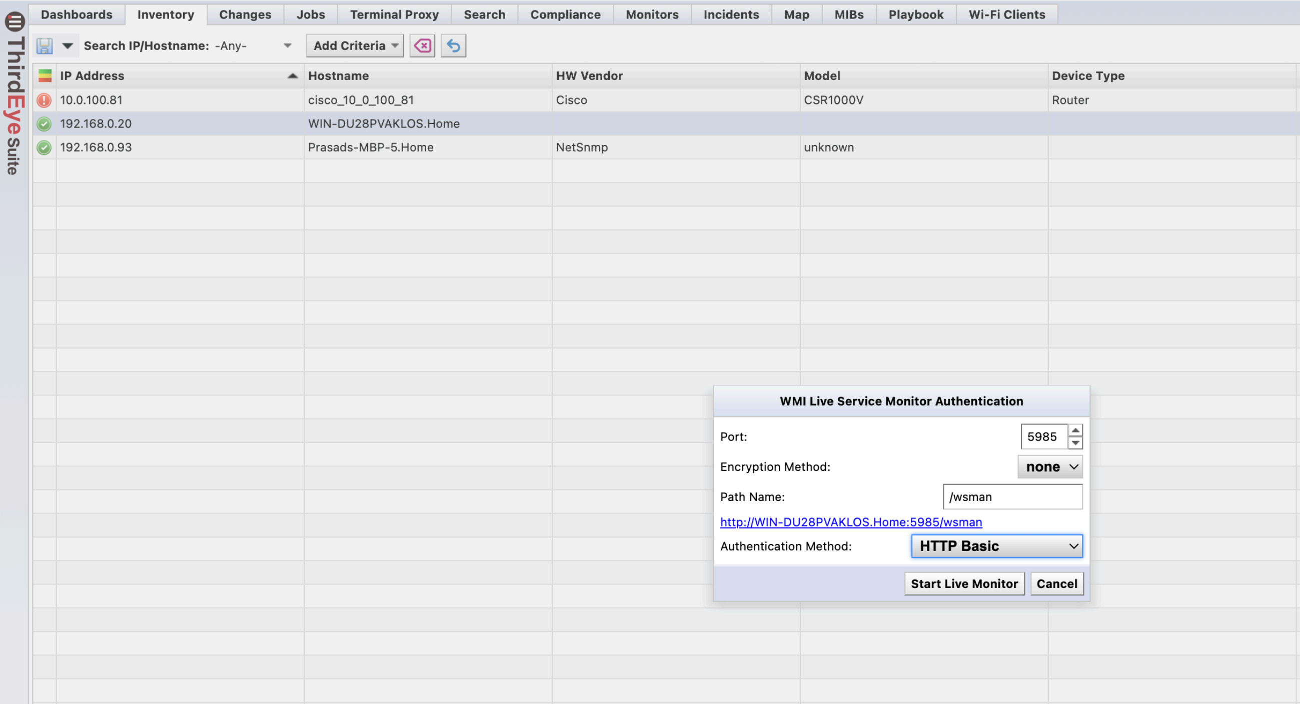
1. Click the [Inventory] main tab.
2. Rightclick the Windows Server.
3. Click [Windows Processes] to open the “WMI Live Service Monitor Authentication” window.



> **Note**
>
> the `Windows Processes` menu item will only be available on right click if the device has a `wmi` trait.

18.4.4 Configure WMI Live Service Monitor

1. Configure WinRM Authentication settings in the “WMI Live Service Monitor Authentication window.



Search IP/Hostname: -Any-

IP Address	Hostname	HW Vendor	Model	Device Type
10.0.100.81	cisco_10_0_100_81	Cisco	CSR1000V	Router
192.168.0.20	WIN-DU28PVAKLOS.Home			
192.168.0.93	Prasads-MBP-5.Home	NetSnmp	unknown	

WMI Live Service Monitor Authentication

Port: 5985

Encryption Method: none

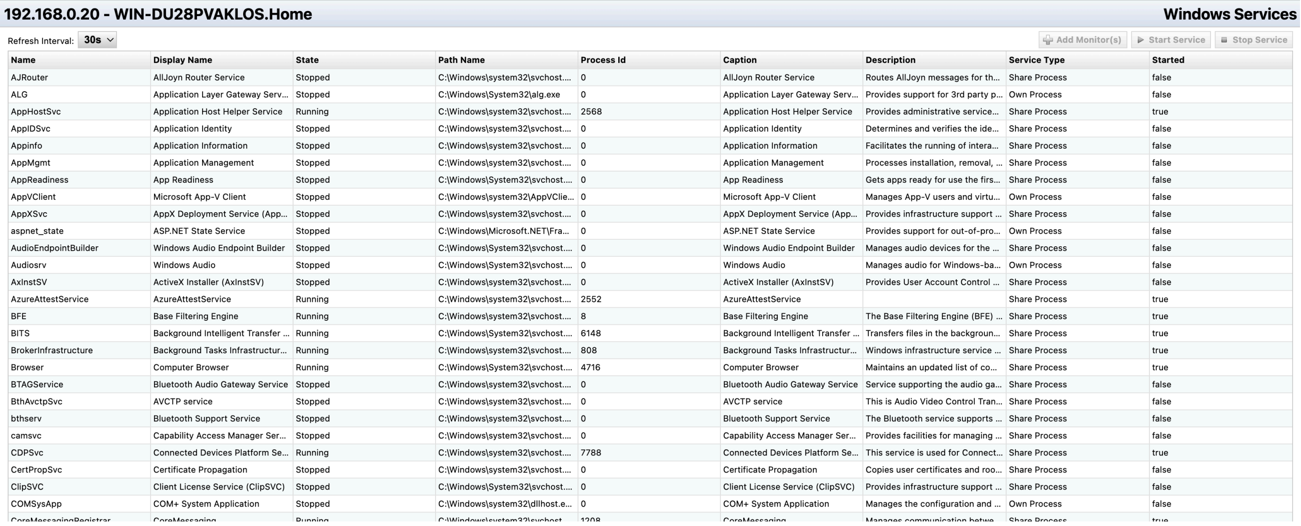
Path Name: /wsman

http://WIN-DU28PVAKLOS.Home:5985/wsman

Authentication Method: HTTP Basic

Item	Description
Port	Specify the WMI port. By default, “5986” is used when encryption is set to “https”, and “5985” when set to “None”.
Encryption Method	Select “https” or “None” based on your environment.
Path Name	Change the path if it has been modified on the server side. The default is “/wsman”.
Authentication Method	Select “Negotiate” or “Http Basic” based on your environment.
AD Realm	Enter the realm. (Only when the authentication method is “Negotiate”)
AD Domain	Enter the domain. (Only when the authentication method is “Negotiate”)

2. Click on [Start Live Monitor] to open the “Windows Services” window.



192.168.0.20 - WIN-DU28PVAKLOS.Home

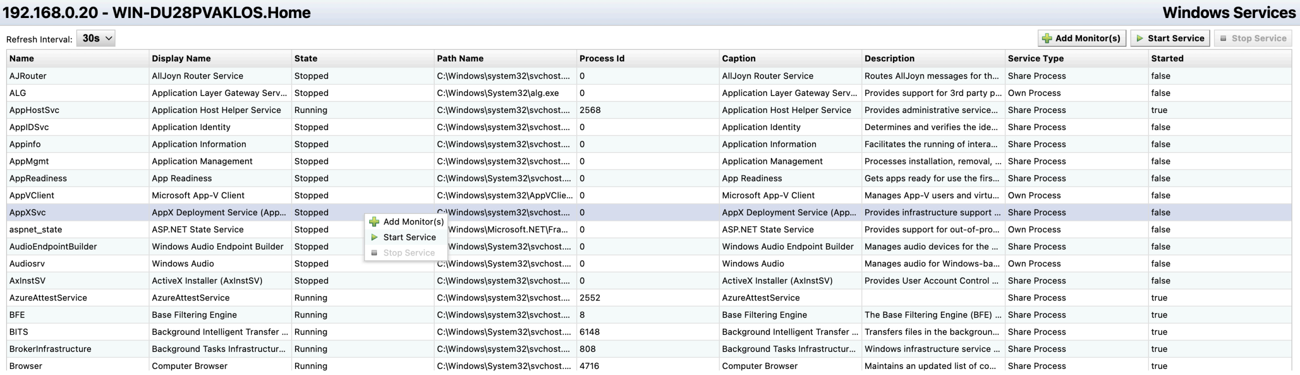
Windows Services

Refresh Interval: 30s

Name	Display Name	State	Path Name	Process Id	Caption	Description	Service Type	Started
AJRouter	AllJoyn Router Service	Stopped	C:\Windows\system32\svchost....	0	AllJoyn Router Service	Routes AllJoyn messages for th...	Share Process	false
ALG	Application Layer Gateway Serv...	Stopped	C:\Windows\System32\alg.exe	0	Application Layer Gateway Serv...	Provides support for 3rd party p...	Own Process	false
AppHostSvc	Application Host Helper Service	Running	C:\Windows\system32\svchost....	2568	Application Host Helper Service	Provides administrative service...	Share Process	true
AppIDSvc	Application Identity	Stopped	C:\Windows\system32\svchost....	0	Application Identity	Determines and verifies the ide...	Share Process	false
Appinfo	Application Information	Stopped	C:\Windows\system32\svchost....	0	Application Information	Facilitates the running of intera...	Share Process	false
AppMgmt	Application Management	Stopped	C:\Windows\system32\svchost....	0	Application Management	Processes installation, removal, ...	Share Process	false
AppReadiness	App Readiness	Stopped	C:\Windows\System32\svchost....	0	App Readiness	Gets apps ready for use the firs...	Share Process	false
AppVClient	Microsoft App-V Client	Stopped	C:\Windows\system32\AppVClie...	0	Microsoft App-V Client	Manages App-V users and virtu...	Own Process	false
AppXSvc	AppX Deployment Service (App...	Stopped	C:\Windows\system32\svchost....	0	AppX Deployment Service (App...	Provides infrastructure support ...	Share Process	false
aspnet_state	ASP.NET State Service	Stopped	C:\Windows\Microsoft.NET\Fra...	0	ASP.NET State Service	Provides support for out-of-pro...	Own Process	false
AudioEndpointBuilder	Windows Audio Endpoint Builder	Stopped	C:\Windows\System32\svchost....	0	Windows Audio Endpoint Builder	Manages audio devices for the ...	Share Process	false
Audiosrv	Windows Audio	Stopped	C:\Windows\System32\svchost....	0	Windows Audio	Manages audio for Windows-ba...	Own Process	false
AxInstSV	ActiveX Installer (AxInstSV)	Stopped	C:\Windows\system32\svchost....	0	ActiveX Installer (AxInstSV)	Provides User Account Control ...	Share Process	false
AzureAttestService	AzureAttestService	Running	C:\Windows\system32\svchost....	2552	AzureAttestService		Share Process	true
BFE	Base Filtering Engine	Running	C:\Windows\system32\svchost....	8	Base Filtering Engine	The Base Filtering Engine (BFE) ...	Share Process	true
BITS	Background Intelligent Transfer ...	Running	C:\Windows\System32\svchost....	6148	Background Intelligent Transfer ...	Transfers files in the backgroun...	Share Process	true
BrokerInfrastructure	Background Tasks Infrastructur...	Running	C:\Windows\system32\svchost....	808	Background Tasks Infrastructur...	Windows infrastructure service ...	Share Process	true
Browser	Computer Browser	Running	C:\Windows\System32\svchost....	4716	Computer Browser	Maintains an updated list of co...	Share Process	true
BTAGService	Bluetooth Audio Gateway Service	Stopped	C:\Windows\system32\svchost....	0	Bluetooth Audio Gateway Service	Service supporting the audio ga...	Share Process	false
BthAvctpSvc	AVCTP service	Stopped	C:\Windows\system32\svchost....	0	AVCTP service	This is Audio Video Control Tran...	Share Process	false
bthserv	Bluetooth Support Service	Stopped	C:\Windows\system32\svchost....	0	Bluetooth Support Service	The Bluetooth service supports ...	Share Process	false
camsvc	Capability Access Manager Ser...	Stopped	C:\Windows\system32\svchost....	0	Capability Access Manager Ser...	Provides facilities for managing ...	Share Process	false
CDPSvc	Connected Devices Platform Se...	Running	C:\Windows\system32\svchost....	7788	Connected Devices Platform Se...	This service is used for Connect...	Share Process	true
CertPropSvc	Certificate Propagation	Stopped	C:\Windows\system32\svchost....	0	Certificate Propagation	Copies user certificates and roo...	Share Process	false
ClipSVC	Client License Service (ClipSVC)	Stopped	C:\Windows\System32\svchost....	0	Client License Service (ClipSVC)	Provides infrastructure support ...	Share Process	false
COMSysApp	COM+ System Application	Stopped	C:\Windows\system32\dllhost.e...	0	COM+ System Application	Manages the configuration and ...	Own Process	false
CoreMessagingRegistrar	CoreMessaging	Running	C:\Windows\system32\svchost....	1208	CoreMessaging	Manages communication betwe...	Share Process	true

18.4.5 Start/Stop WMI Services

You can Start/Stop Services by clicking the buttons in the upper right right of the window, or by rightclicking the service.

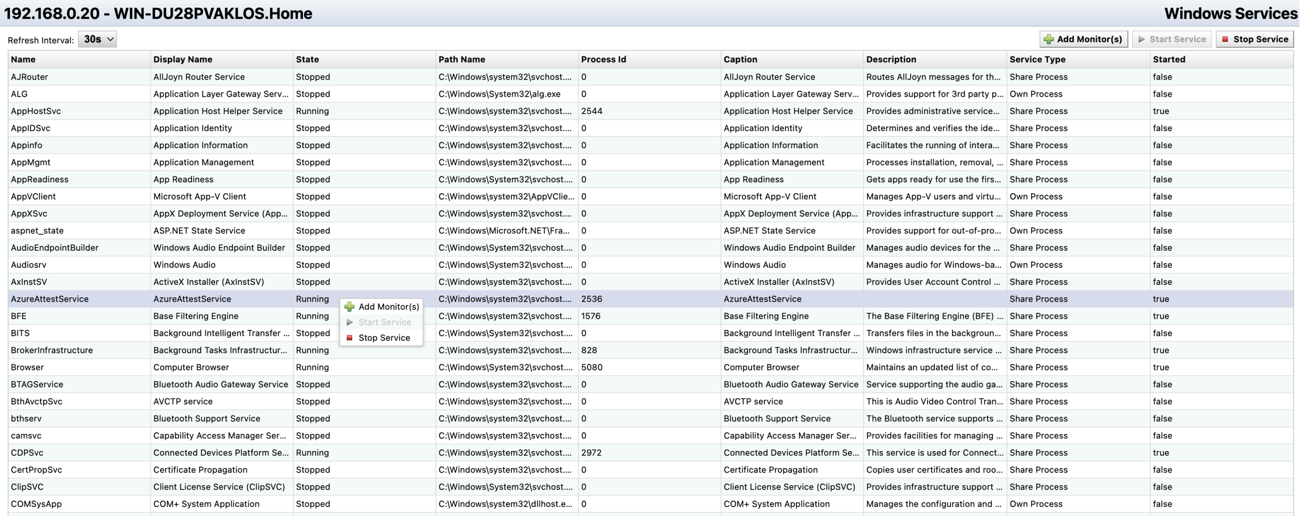


192.168.0.20 - WIN-DU28PVAKLOS.Home

Windows Services

Refresh Interval: 30s

Name	Display Name	State	Path Name	Process Id	Caption	Description	Service Type	Started
AJRouter	AllJoyn Router Service	Stopped	C:\Windows\system32\svchost....	0	AllJoyn Router Service	Routes AllJoyn messages for th...	Share Process	false
ALG	Application Layer Gateway Serv...	Stopped	C:\Windows\System32\alg.exe	0	Application Layer Gateway Serv...	Provides support for 3rd party p...	Own Process	false
AppHostSvc	Application Host Helper Service	Running	C:\Windows\system32\svchost....	2568	Application Host Helper Service	Provides administrative service...	Share Process	true
AppIDSvc	Application Identity	Stopped	C:\Windows\system32\svchost....	0	Application Identity	Determines and verifies the ide...	Share Process	false
Appinfo	Application Information	Stopped	C:\Windows\system32\svchost....	0	Application Information	Facilitates the running of intera...	Share Process	false
AppMgmt	Application Management	Stopped	C:\Windows\system32\svchost....	0	Application Management	Processes installation, removal, ...	Share Process	false
AppReadiness	App Readiness	Stopped	C:\Windows\System32\svchost....	0	App Readiness	Gets apps ready for use the firs...	Share Process	false
AppVClient	Microsoft App-V Client	Stopped	C:\Windows\system32\AppVClie...	0	Microsoft App-V Client	Manages App-V users and virtu...	Own Process	false
AppXSvc	AppX Deployment Service (App...	Stopped	C:\Windows\system32\svchost....	0	AppX Deployment Service (App...	Provides infrastructure support ...	Share Process	false
aspnet_state	ASP.NET State Service	Stopped	Windows\Microsoft.NET\Fra...	0	ASP.NET State Service	Provides support for out-of-pro...	Own Process	false
AudioEndpointBuilder	Windows Audio Endpoint Builder	Stopped	Windows\System32\svchost....	0	Windows Audio Endpoint Builder	Manages audio devices for the ...	Share Process	false
Audiosrv	Windows Audio	Stopped	C:\Windows\System32\svchost....	0	Windows Audio	Manages audio for Windows-ba...	Own Process	false
AxInstSV	ActiveX Installer (AxInstSV)	Stopped	C:\Windows\system32\svchost....	0	ActiveX Installer (AxInstSV)	Provides User Account Control ...	Share Process	false
AzureAttestService	AzureAttestService	Running	C:\Windows\system32\svchost....	2552	AzureAttestService		Share Process	true
BFE	Base Filtering Engine	Running	C:\Windows\system32\svchost....	8	Base Filtering Engine	The Base Filtering Engine (BFE) ...	Share Process	true
BITS	Background Intelligent Transfer ...	Running	C:\Windows\System32\svchost....	6148	Background Intelligent Transfer ...	Transfers files in the backgroun...	Share Process	true
BrokerInfrastructure	Background Tasks Infrastructur...	Running	C:\Windows\system32\svchost....	808	Background Tasks Infrastructur...	Windows infrastructure service ...	Share Process	true
Browser	Computer Browser	Running	C:\Windows\System32\svchost....	4716	Computer Browser	Maintains an updated list of co...	Share Process	true



192.168.0.20 - WIN-DU28PVAKLOS.Home

Windows Services

Refresh Interval: 30s

Name	Display Name	State	Path Name	Process Id	Caption	Description	Service Type	Started
AJRouter	AllJoyn Router Service	Stopped	C:\Windows\system32\svchost....	0	AllJoyn Router Service	Routes AllJoyn messages for th...	Share Process	false
ALG	Application Layer Gateway Serv...	Stopped	C:\Windows\System32\alg.exe	0	Application Layer Gateway Serv...	Provides support for 3rd party p...	Own Process	false
AppHostSvc	Application Host Helper Service	Running	C:\Windows\system32\svchost....	2544	Application Host Helper Service	Provides administrative service...	Share Process	true
AppIDSvc	Application Identity	Stopped	C:\Windows\system32\svchost....	0	Application Identity	Determines and verifies the ide...	Share Process	false
Appinfo	Application Information	Stopped	C:\Windows\system32\svchost....	0	Application Information	Facilitates the running of intera...	Share Process	false
AppMgmt	Application Management	Stopped	C:\Windows\system32\svchost....	0	Application Management	Processes installation, removal, ...	Share Process	false
AppReadiness	App Readiness	Stopped	C:\Windows\System32\svchost....	0	App Readiness	Gets apps ready for use the firs...	Share Process	false
AppVClient	Microsoft App-V Client	Stopped	C:\Windows\system32\AppVClie...	0	Microsoft App-V Client	Manages App-V users and virtu...	Own Process	false
AppXSvc	AppX Deployment Service (App...	Stopped	C:\Windows\system32\svchost....	0	AppX Deployment Service (App...	Provides infrastructure support ...	Share Process	false
aspnet_state	ASP.NET State Service	Stopped	C:\Windows\Microsoft.NET\Fra...	0	ASP.NET State Service	Provides support for out-of-pro...	Own Process	false
AudioEndpointBuilder	Windows Audio Endpoint Builder	Stopped	C:\Windows\System32\svchost....	0	Windows Audio Endpoint Builder	Manages audio devices for the ...	Share Process	false
Audiosrv	Windows Audio	Stopped	C:\Windows\System32\svchost....	0	Windows Audio	Manages audio for Windows-ba...	Own Process	false
AxInstSV	ActiveX Installer (AxInstSV)	Stopped	C:\Windows\system32\svchost....	0	ActiveX Installer (AxInstSV)	Provides User Account Control ...	Share Process	false
AzureAttestService	AzureAttestService	Running	C:\Windows\system32\svchost....	2536	AzureAttestService		Share Process	true
BFE	Base Filtering Engine	Running	C:\Windows\system32\svchost....	1576	Base Filtering Engine	The Base Filtering Engine (BFE) ...	Share Process	true
BITS	Background Intelligent Transfer ...	Stopped	C:\Windows\System32\svchost....	0	Background Intelligent Transfer ...	Transfers files in the backgroun...	Share Process	false
BrokerInfrastructure	Background Tasks Infrastructur...	Running	C:\Windows\system32\svchost....	828	Background Tasks Infrastructur...	Windows infrastructure service ...	Share Process	true
Browser	Computer Browser	Running	C:\Windows\System32\svchost....	5080	Computer Browser	Maintains an updated list of co...	Share Process	true
BTAGService	Bluetooth Audio Gateway Service	Stopped	C:\Windows\system32\svchost....	0	Bluetooth Audio Gateway Service	Service supporting the audio ga...	Share Process	false
BthAvctpSvc	AVCTP service	Stopped	C:\Windows\system32\svchost....	0	AVCTP service	This is Audio Video Control Tran...	Share Process	false
bthserv	Bluetooth Support Service	Stopped	C:\Windows\system32\svchost....	0	Bluetooth Support Service	The Bluetooth service supports ...	Share Process	false
camsvc	Capability Access Manager Ser...	Stopped	C:\Windows\system32\svchost....	0	Capability Access Manager Ser...	Provides facilities for managing ...	Share Process	false
CDPSvc	Connected Devices Platform Se...	Running	C:\Windows\system32\svchost....	2972	Connected Devices Platform Se...	This service is used for Connect...	Share Process	true
CertPropSvc	Certificate Propagation	Stopped	C:\Windows\system32\svchost....	0	Certificate Propagation	Copies user certificates and roo...	Share Process	false
ClipSVC	Client License Service (ClipSVC)	Stopped	C:\Windows\System32\svchost....	0	Client License Service (ClipSVC)	Provides infrastructure support ...	Share Process	false
COMSysApp	COM+ System Application	Stopped	C:\Windows\system32\dllhost.e...	0	COM+ System Application	Manages the configuration and ...	Own Process	false

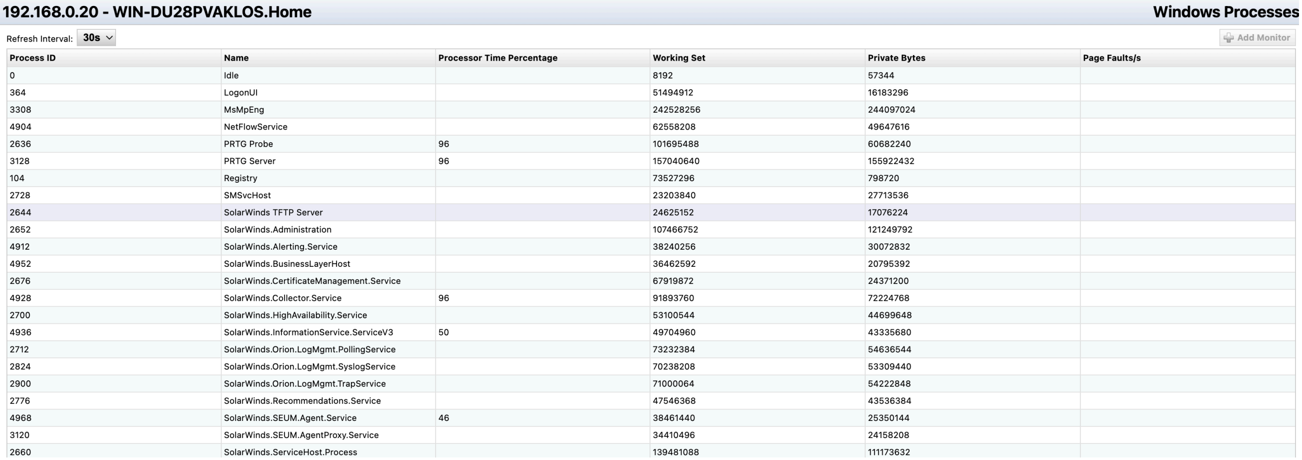
Note

The [Start Service] and [Stop Service] buttons are enabled depending on the current status of the service.

18.4.6 Add WMI Monitor

WMI Service monitors can be directly added to a device in a similar way to other monitors.

1. Click [Start Live Monitor] to open a Live Monitor page.

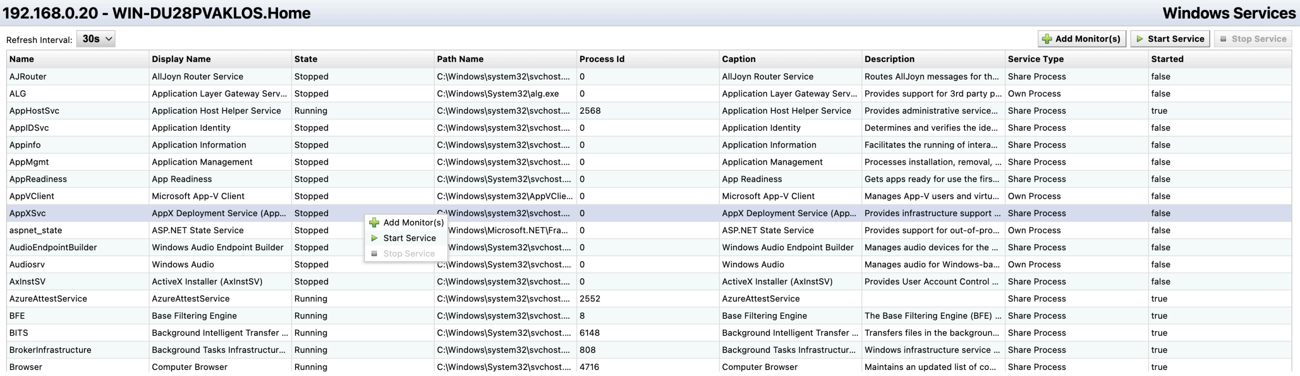


192.168.0.20 - WIN-DU28PVAKLOS.Home — Windows Processes

Refresh Interval: 30s

Process ID	Name	Processor Time Percentage	Working Set	Private Bytes	Page Faults/s
0	Idle		8192	57344	
364	LogonUI		51494912	16183296	
3308	MsMpEng		242528256	244097024	
4904	NetFlowService		62558208	49647616	
2636	PRTG Probe	96	101695488	60682240	
3128	PRTG Server	96	157040640	155922432	
104	Registry		73527296	798720	
2728	SMSvcHost		23203840	27713536	
2644	SolarWinds TFTP Server		24625152	17076224	
2652	SolarWinds.Administration		107466752	121249792	
4912	SolarWinds.Alerting.Service		38240256	30072832	
4952	SolarWinds.BusinessLayerHost		36462592	20795392	
2676	SolarWinds.CertificateManagement.Service		67919872	24371200	
4928	SolarWinds.Collector.Service	96	91893760	72224768	
2700	SolarWinds.HighAvailability.Service		53100544	44699648	
4936	SolarWinds.InformationService.ServiceV3	50	49704960	43335680	
2712	SolarWinds.Orion.LogMgmt.PollingService		73232384	54636544	
2824	SolarWinds.Orion.LogMgmt.SyslogService		70238208	53309440	
2900	SolarWinds.Orion.LogMgmt.TrapService		71000064	54222848	
2776	SolarWinds.Recommendations.Service		47546368	43536384	
4968	SolarWinds.SEUM.Agent.Service	46	38461440	25350144	
3120	SolarWinds.SEUM.AgentProxy.Service		34410496	24158208	
2660	SolarWinds.ServiceHost.Process		139481088	111173632	

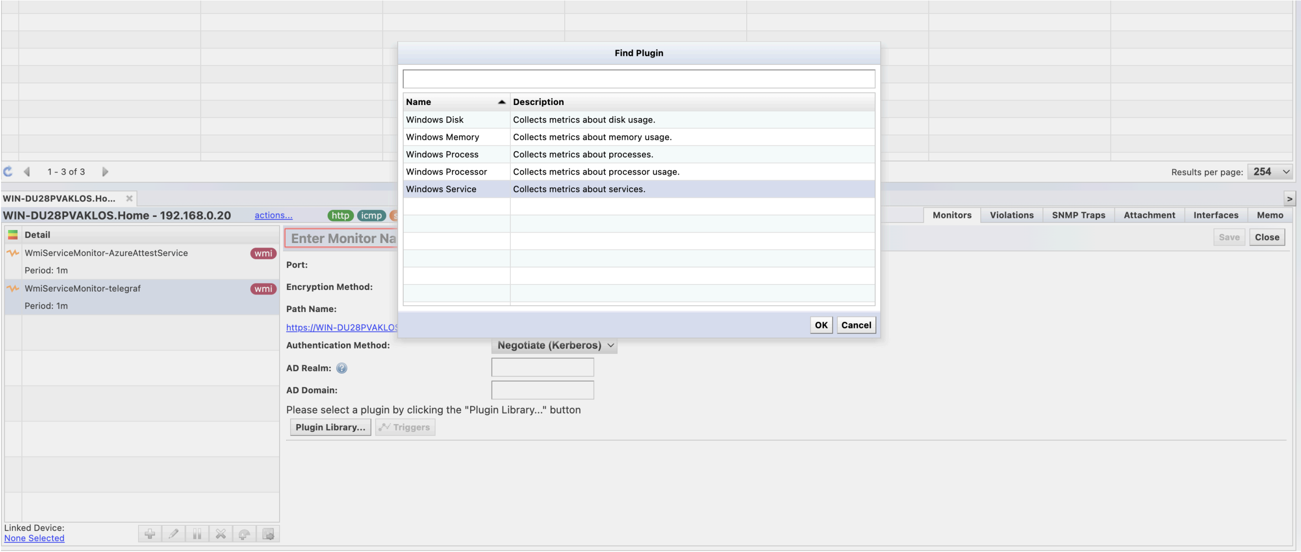
2. Click the [Add Monitor(s)] button to add a monitor to the device for the selected Service(s).



192.168.0.20 - WIN-DU28PVAKLOS.Home — Windows Services

Refresh Interval: 30s

Name	Display Name	State	Path Name	Process Id	Caption	Description	Service Type	Started
AJRouter	AllJoyn Router Service	Stopped	C:\Windows\system32\svchost....	0	AllJoyn Router Service	Routes AllJoyn messages for th...	Share Process	false
ALG	Application Layer Gateway Serv...	Stopped	C:\Windows\System32\alg.exe	0	Application Layer Gateway Serv...	Provides support for 3rd party p...	Own Process	false
AppHostSvc	Application Host Helper Service	Running	C:\Windows\system32\svchost....	2568	Application Host Helper Service	Provides administrative service...	Share Process	true
AppIDSvc	Application Identity	Stopped	C:\Windows\system32\svchost....	0	Application Identity	Determines and verifies the ide...	Share Process	false
Appinfo	Application Information	Stopped	C:\Windows\system32\svchost....	0	Application Information	Facilitates the running of intera...	Share Process	false
AppMgmt	Application Management	Stopped	C:\Windows\system32\svchost....	0	Application Management	Processes installation, removal, ...	Share Process	false
AppReadiness	App Readiness	Stopped	C:\Windows\System32\svchost....	0	App Readiness	Gets apps ready for use the firs...	Share Process	false
AppVClient	Microsoft App-V Client	Stopped	C:\Windows\system32\AppVClie...	0	Microsoft App-V Client	Manages App-V users and virtu...	Own Process	false
AppXSvc	AppX Deployment Service (App...	Stopped	C:\Windows\system32\svchost....	0	AppX Deployment Service (App...	Provides infrastructure support ...	Share Process	false
aspnet_state	ASP.NET State Service	Stopped	Windows\Microsoft.NET\Fra...	0	ASP.NET State Service	Provides support for out-of-pro...	Own Process	false
AudioEndpointBuilder	Windows Audio Endpoint Builder	Stopped	Windows\System32\svchost....	0	Windows Audio Endpoint Builder	Manages audio devices for the ...	Share Process	false
Audiosrv	Windows Audio	Stopped	C:\Windows\System32\svchost....	0	Windows Audio	Manages audio for Windows-ba...	Own Process	false
AxInstSV	ActiveX Installer (AxInstSV)	Stopped	C:\Windows\system32\svchost....	0	ActiveX Installer (AxInstSV)	Provides User Account Control ...	Share Process	false
AzureAttestService	AzureAttestService	Running	C:\Windows\system32\svchost....	2552	AzureAttestService		Share Process	true
BFE	Base Filtering Engine	Running	C:\Windows\system32\svchost....	8	Base Filtering Engine	The Base Filtering Engine (BFE) ...	Share Process	true
BITS	Background Intelligent Transfer ...	Running	C:\Windows\System32\svchost....	6148	Background Intelligent Transfer ...	Transfers files in the backgroun...	Share Process	true
BrokerInfrastructure	Background Tasks Infrastructur...	Running	C:\Windows\system32\svchost....	808	Background Tasks Infrastructur...	Windows infrastructure service ...	Share Process	true
Browser	Computer Browser	Running	C:\Windows\System32\svchost....	4716	Computer Browser	Maintains an updated list of co...	Share Process	true



Find Plugin

Name	Description
Windows Disk	Collects metrics about disk usage.
Windows Memory	Collects metrics about memory usage.
Windows Process	Collects metrics about processes.
Windows Processor	Collects metrics about processor usage.
Windows Service	Collects metrics about services.

WIN-DU28PVAKLOS.Home - 192.168.0.20

WmiServiceMonitor-AzureAttestService
Period: 1m

WmiServiceMonitor-telegraf
Period: 1m

Enter Monitor Na

Port:

Encryption Method:

Path Name:

https://WIN-DU28PVAKLO

Authentication Method: Negotiate (Kerberos)

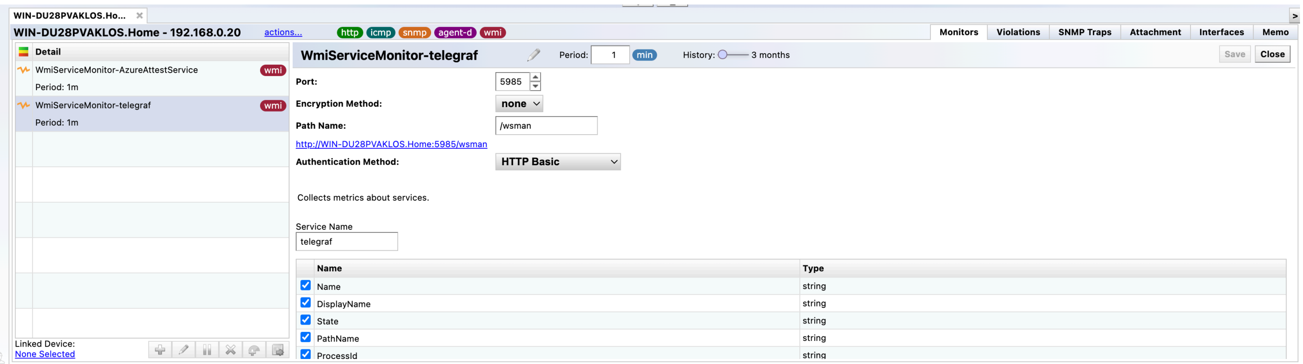
AD Realm:

AD Domain:

Please select a plugin by clicking the "Plugin Library..." button

Linked Device:
None Selected

WinRM authentication should be configured as usual.



WIN-DU28PVAKLOS.Home - 192.168.0.20

Detail

WmiServiceMonitor-AzureAttestService wmi
Period: 1m

WmiServiceMonitor-telegraf wmi
Period: 1m

Linked Device: None Selected

WmiServiceMonitor-telegraf — Period: 1 min — History: 3 months

Port: 5985

Encryption Method: none

Path Name: /wsman

http://WIN-DU28PVAKLOS.Home:5985/wsman

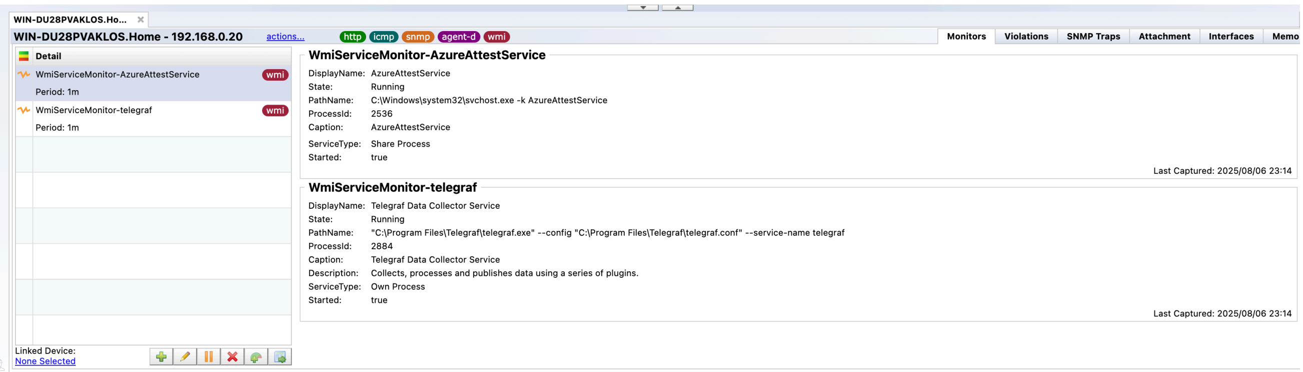
Authentication Method: HTTP Basic

Collects metrics about services.

Service Name: telegraf

	Name	Type
☑	Name	string
☑	DisplayName	string
☑	State	string
☑	PathName	string
☑	ProcessId	string

The monitor will be added to the device, and monitoring will begin.



WIN-DU28PVAKLOS.Home - 192.168.0.20

Detail

WmiServiceMonitor-AzureAttestService wmi
Period: 1m

WmiServiceMonitor-telegraf wmi
Period: 1m

Linked Device: None Selected

WmiServiceMonitor-AzureAttestService

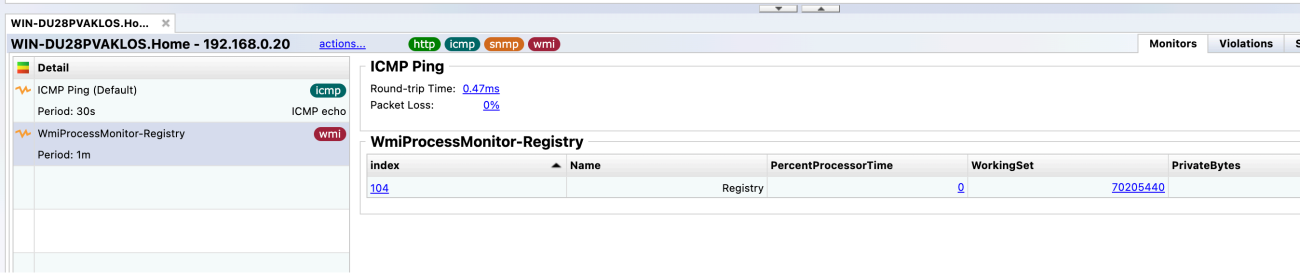
```
DisplayName:  AzureAttestService
State:        Running
PathName:     C:\Windows\system32\svchost.exe -k AzureAttestService
ProcessId:    2536
Caption:      AzureAttestService
ServiceType:  Share Process
Started:      true
```

Last Captured: 2025/08/06 23:14

WmiServiceMonitor-telegraf

```
DisplayName:  Telegraf Data Collector Service
State:        Running
PathName:     "C:\Program Files\Telegraf\telegraf.exe" --config "C:\Program Files\Telegraf\telegraf.conf" --service-name telegraf
ProcessId:    2884
Caption:      Telegraf Data Collector Service
Description:  Collects, processes and publishes data using a series of plugins.
ServiceType:  Own Process
Started:      true
```

Last Captured: 2025/08/06 23:14



WIN-DU28PVAKLOS.Home - 192.168.0.20

Detail

ICMP Ping (Default) icmp
Period: 30s ICMP echo

WmiProcessMonitor-Registry wmi
Period: 1m

ICMP Ping

Round-trip Time: 0.47ms
Packet Loss: 0%

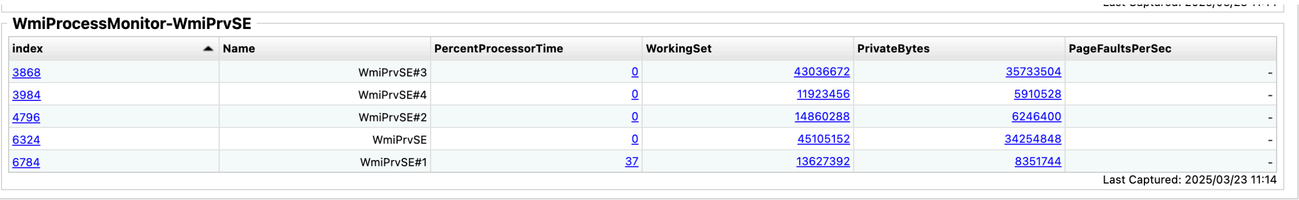
WmiProcessMonitor-Registry

index	Name	PercentProcessorTime	WorkingSet	PrivateBytes
104	Registry	0	70205440	

> **Note**
>
> A monitor can only monitor one service at a time. To monitor multiple services, multiple monitors can be added to the same device.

If the selected process has multiple instances, the added monitor will monitor all instances of the process. The instances will be indicated by `<process name>`, `<process name>#1`, `<process name>#2`, etc.

In the example below, the process monitor `WmiPrvSE` has different instances of the same process with the names `WmiPrvSE`, `WmiPrvSE#1`, and `WmiPrvSE#2`.

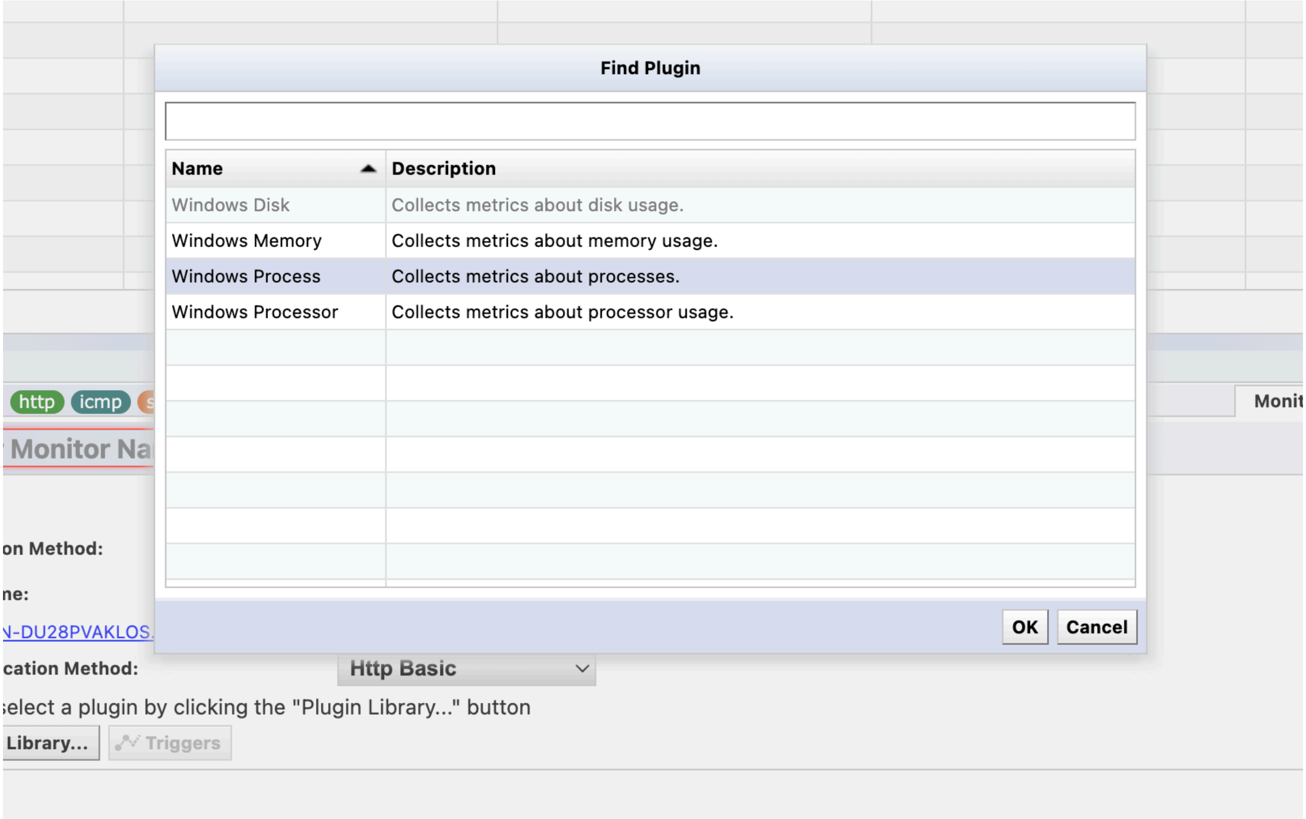


WmiProcessMonitor-WmiPrvSE

index	Name	PercentProcessorTime	WorkingSet	PrivateBytes	PageFaultsPerSec
3868	WmiPrvSE#3	0	43036672	35733504	-
3984	WmiPrvSE#4	0	11923456	5910528	-
4796	WmiPrvSE#2	0	14860288	6246400	-
6324	WmiPrvSE	0	45105152	34254848	-
6784	WmiPrvSE#1	37	13627392	8351744	-

Last Captured: 2025/03/23 11:14

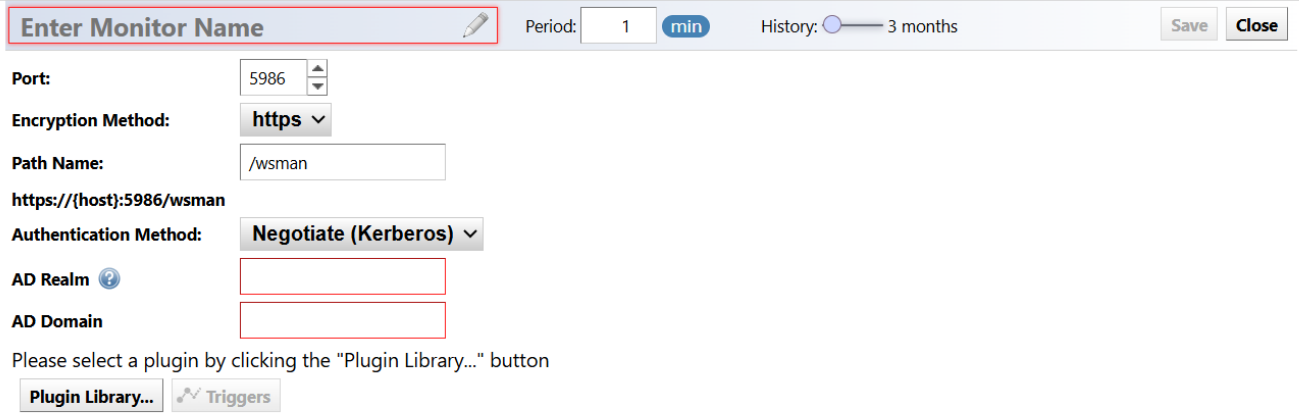
As with other monitors, WMI Process monitors can be manually added directly to the device.



Find Plugin

Name	Description
Windows Disk	Collects metrics about disk usage.
Windows Memory	Collects metrics about memory usage.
Windows Process	Collects metrics about processes.
Windows Processor	Collects metrics about processor usage.

The process name to be monitored must be set manually. If the selected process has multiple instances, all instances will be monitored. You can edit the process name of monitors added via the Live Monitor page.



Port: 5986

Encryption Method: https

Path Name: /wsman

https://{host}:5986/wsman

Authentication Method: Negotiate (Kerberos)

AD Realm

AD Domain

Please select a plugin by clicking the "Plugin Library..." button

SECTION 19

WIRELESS LAN CONTROLLER MONITORING

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.

19.1 WLC Monitor Configuration

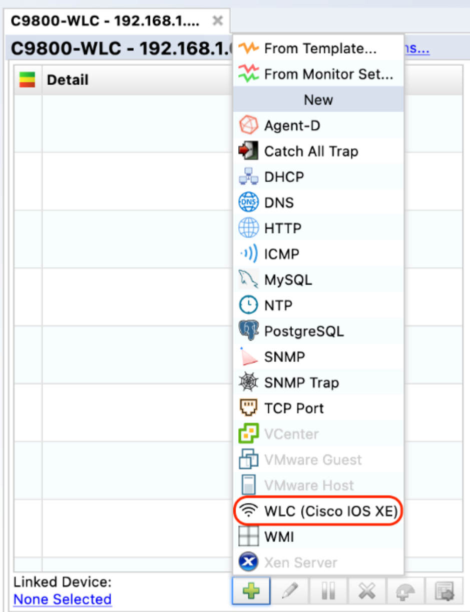
1. Add your Wireless Lan Controller, and its associated Access Points to the inventory.
2. Ensure that their hostnames are correct, and that their Device Adapters are set to Cisco IOS.

Access Points reported from the Wireless Lan Controller will automatically be given an AP tag. This identification is based on both the Managed Network and Hostname of the device in inventory. So please make sure that the APs are in the same Managed Network as the controller and that the hostnames in inventory match the hostnames configured in the Controller.

3. Make sure your Wireless Lan Controller has credentials configured for it in the Credential Manager.

   `VTY Username` and `VTY Password` are used for authentication.

4. Add a WLC (Cisco IOS XE) Monitor to the Wireless Lan Controller.

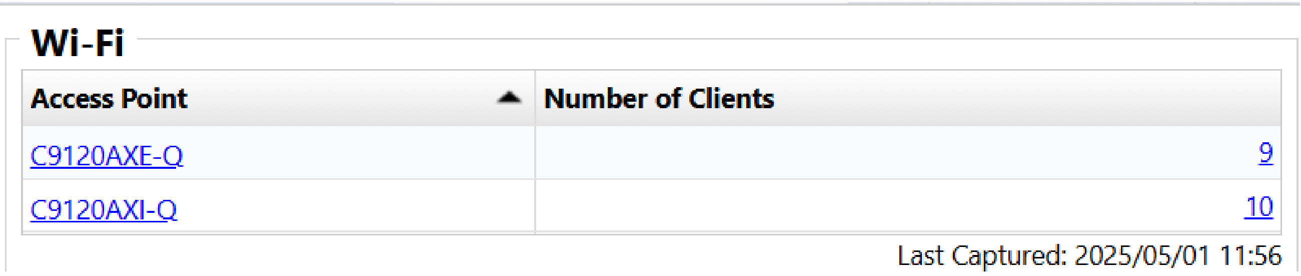


Configure the monitor settings.

5. Set the monitor name, interval, data storage period, and optional triggers.

6. Click [Save].

When data collection is complete, a table displaying collected Access Point Names & the number of currently connected devices will be displayed:

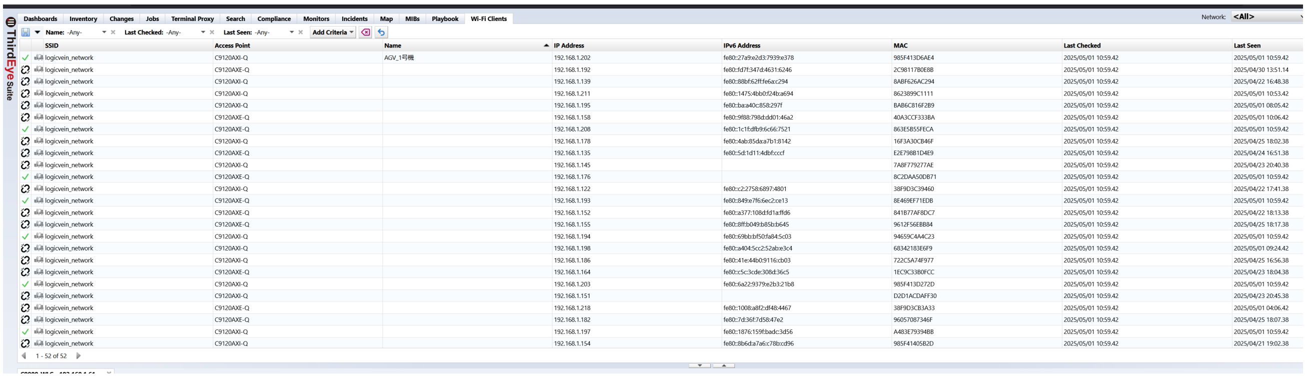


Wi-Fi

Access Point ▲	Number of Clients
C9120AXE-Q	9
C9120AXI-Q	10

Last Captured: 2025/05/01 11:56

The [Wi-Fi Clients] tab provides details on the clients acquired by the WLC monitor.



Name: -Any- Last Checked: -Any- Last Seen: -Any-

Network: <All>

		SSID	Access Point	Name	IP Address	IPv6 Address	MAC	Last Checked	Last Seen
✓		logicvein_network	C9120AXI-Q	AGV_1号機	192.168.1.202	fe80::27a9:e2d3:7939:e378	985F413D6AE4	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXE-Q		192.168.1.192	fe80::fd7f:347d:4631:6246	2C98117B0E8B	2025/05/01 10:59.42	2025/04/30 13:51.14
🔗		logicvein_network	C9120AXI-Q		192.168.1.139	fe80::88bf:62ff:fe6a:c294	8ABF626AC294	2025/05/01 10:59.42	2025/04/22 16:48.38
🔗		logicvein_network	C9120AXI-Q		192.168.1.211	fe80::1475:4bb0:f24b:a694	8623899C1111	2025/05/01 10:59.42	2025/05/01 10:53.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.195	fe80::ba:a40c:858:297f	BAB6C816F2B9	2025/05/01 10:59.42	2025/05/01 08:05.42
🔗		logicvein_network	C9120AXE-Q		192.168.1.158	fe80::9f88:798d:dd01:46a2	40A3CCF333BA	2025/05/01 10:59.42	2025/05/01 10:06.42
✓		logicvein_network	C9120AXE-Q		192.168.1.208	fe80::1c1f:dfb9:6c66:7521	863E5B55FECA	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.178	fe80::4ab:85da:a7b1:8142	16F3A30CB46F	2025/05/01 10:59.42	2025/04/25 18:02.38
🔗		logicvein_network	C9120AXE-Q		192.168.1.135	fe80::5d:1d11:4dbf:cccf	E2E798B1D4E9	2025/05/01 10:59.42	2025/04/24 16:51.38
🔗		logicvein_network	C9120AXI-Q		192.168.1.145		7A8F779277AE	2025/05/01 10:59.42	2025/04/23 20:40.38
✓		logicvein_network	C9120AXE-Q		192.168.1.176		8C2DAA50DB71	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.122	fe80::c2:2758:6897:4801	38F9D3C39460	2025/05/01 10:59.42	2025/04/22 17:41.38
✓		logicvein_network	C9120AXE-Q		192.168.1.193	fe80::849:e7f6:6ec2:ce13	8E469EF71EDB	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXE-Q		192.168.1.152	fe80::a377:108d:fd1a:ffd6	841B77AF8DC7	2025/05/01 10:59.42	2025/04/22 18:13.38
🔗		logicvein_network	C9120AXE-Q		192.168.1.155	fe80::8ff:b049:b85b:b645	9612F56EBB84	2025/05/01 10:59.42	2025/04/25 18:17.38
✓		logicvein_network	C9120AXI-Q		192.168.1.194	fe80::69bb:bf50:fa84:5c03	94659C4A4C23	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.198	fe80::a404:5cc2:52ab:e3c4	68342183E6F9	2025/05/01 10:59.42	2025/05/01 09:24.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.186	fe80::41e:44b0:9116:cb03	722C5A74F977	2025/05/01 10:59.42	2025/04/25 16:56.38
🔗		logicvein_network	C9120AXE-Q		192.168.1.164	fe80::c5c:3cde:308d:36c5	1EC9C33B0FCC	2025/05/01 10:59.42	2025/04/23 18:04.38
✓		logicvein_network	C9120AXI-Q		192.168.1.203	fe80::6a22:9379:e2b3:21b8	985F413D272D	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.151		D2D1ACDAFF30	2025/05/01 10:59.42	2025/04/23 20:45.38
🔗		logicvein_network	C9120AXE-Q		192.168.1.218	fe80::1008:a8f2:df48:4467	38F9D3CB3A33	2025/05/01 10:59.42	2025/05/01 04:06.42
🔗		logicvein_network	C9120AXE-Q		192.168.1.182	fe80::7d:36f:7d58:47e2	96057087346F	2025/05/01 10:59.42	2025/04/25 18:07.38
✓		logicvein_network	C9120AXI-Q		192.168.1.197	fe80::1876:159f:badc:3d56	A483E79394BB	2025/05/01 10:59.42	2025/05/01 10:59.42
🔗		logicvein_network	C9120AXI-Q		192.168.1.154	fe80::8b6d:a7a6:c78b:cd96	985F41405B2D	2025/05/01 10:59.42	2025/04/21 19:02.38

1 - 52 of 52

Item	Description
Status	The following two types of icons are displayed: ✓ Indicates that the client is currently connected to. 🔗 Indicates that the client has been recognized as a client at least once in the past but is not currently connected.
Icon	A customizable 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 currently connected.
Access Point	Displays the name of the access point to which the client is connected.
Name	A customizable 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.

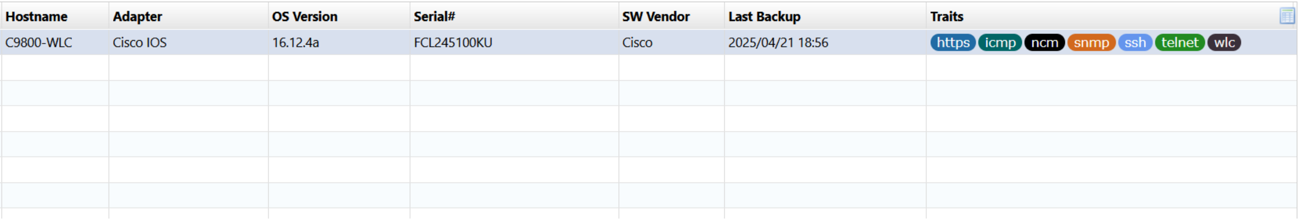
The name and icon can be customized by clicking the [Edit] button in the upper right corner. Since this customization is associated with the client's MAC address, the customization will be applied even if the client has a new IP address.

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.

19.2 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.
- Verify that the access point has been given an “ap” trait.



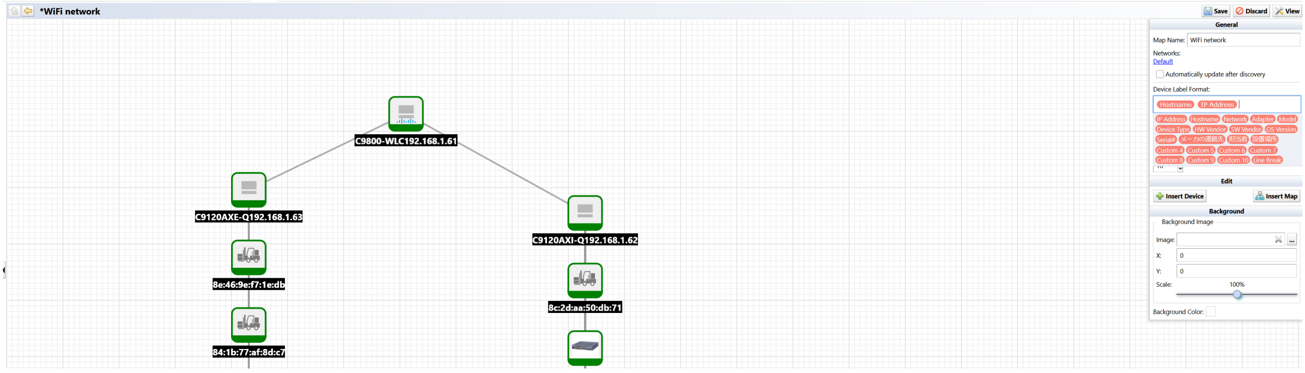
Hostname	Adapter	OS Version	Serial#	SW Vendor	Last Backup	Traits
C9800-WLC	Cisco IOS	16.12.4a	FCL245100KU	Cisco	2025/04/21 18:56	https icmp ncm snmp ssh telnet wlc

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.

2. 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.

3. Select the access point and activate the “Show Wi-Fi Clients” option.



Map Name: WiFi network

Networks:
Default

☐ Automatically update after discovery

Device Label Format: Hostname IP Address

Image:

X: 0

Y: 0

Scale: 100%

Background Color:

4. Save the map.

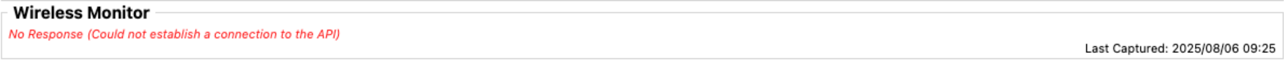
The name set in the [Wi-Fi Clients] tab will be used to label the clients that appear on the map. If no name is set, the client’s MAC address will be displayed. The name and icon can be edited in the [Wi-Fi Clients] tab or by right-clicking on the client icon on the map. The client icon on the map will also be automatically updated when the client is disconnected or moved to another access point.

19.3 WLC Error Messages

The following errors are possible when monitoring Cisco Wi-Fi devices with a WLC monitor:

- `No Response (Could not establish a connection to the API)`

Connection cannot be established:



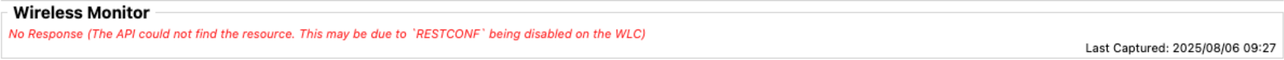
Wireless Monitor

No Response (Could not establish a connection to the API)

Last Captured: 2025/08/06 09:25

- `No Response (The API could not find the resource. This may be due to RESTCONFIG being`

Connection can be established, but RESTCONF is disabled. Enable RESTCONF to locate the resources.



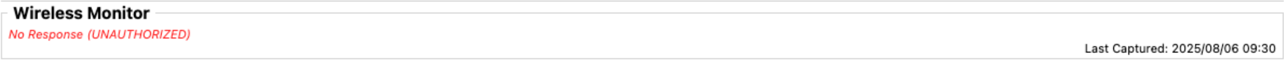
Wireless Monitor

No Response (The API could not find the resource. This may be due to `RESTCONF` being disabled on the WLC)

Last Captured: 2025/08/06 09:27

- `No Response (UNAUTHORIZED)`

Incorrect credentials used for access attempt:



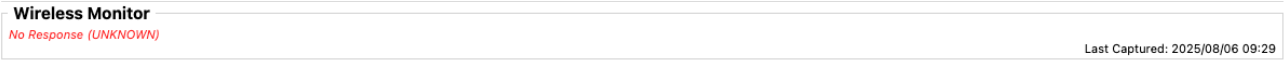
Wireless Monitor

No Response (UNAUTHORIZED)

Last Captured: 2025/08/06 09:30

- `UNKNOWN`

Other issue.



Wireless Monitor

No Response (UNKNOWN)

Last Captured: 2025/08/06 09:29

SECTION 20

VRF (VIRTUAL ROUTING AND FORWARDING)

VRFs use multiple virtual routing tables instead of using a single global routing table. Each VRF instance operates as a separate virtual router, maintaining its own routing table and forwarding decisions, isolated from other VRFs. This allows multiple instances of a routing table to coexist within the same router simultaneously. They are commonly used for MPLS (Multiprotocol Label Switching) deployments.

VRFs enables network segmentation and supports features such as:

- **Network Isolation:** VRFs create separate virtual networks within a single physical router, ensuring traffic from different customers, departments, or networks remains isolated.
- **Multi-Tenancy:** Commonly used in service provider environments to manage multiple customers' traffic on shared infrastructure without interference.
- **Overlapping IP Addresses:** VRFs allow the same IP address space to be reused across different VRF instances, as each instance is independent.
- **VPN Support:** VRF is a key component in MPLS VPNs, enabling secure, isolated communication over shared networks.

20.1 VRF Cisco Support

ThirdEye can collect VRF data from a Cisco device.

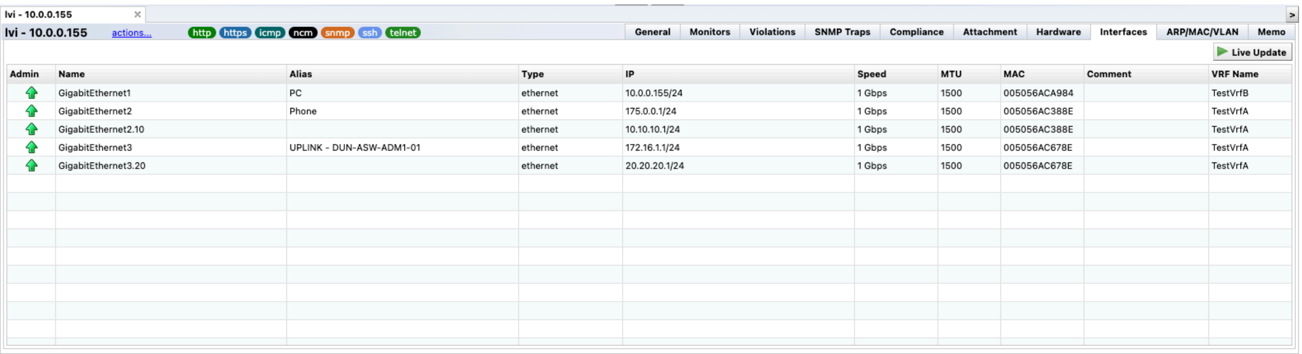
> **Note**
>
> A single interface on a Cisco device cannot be a member of multiple VRFs (Virtual Routing and Forwarding instances) simultaneously. Each interface, physical or logical (such as a subinterface) can be associated with only one VRF at a time.

20.2 Viewing VRF Data

You can view a device's VRF data in the [Inventory] main tab, and sort devices using their "VRF Name".

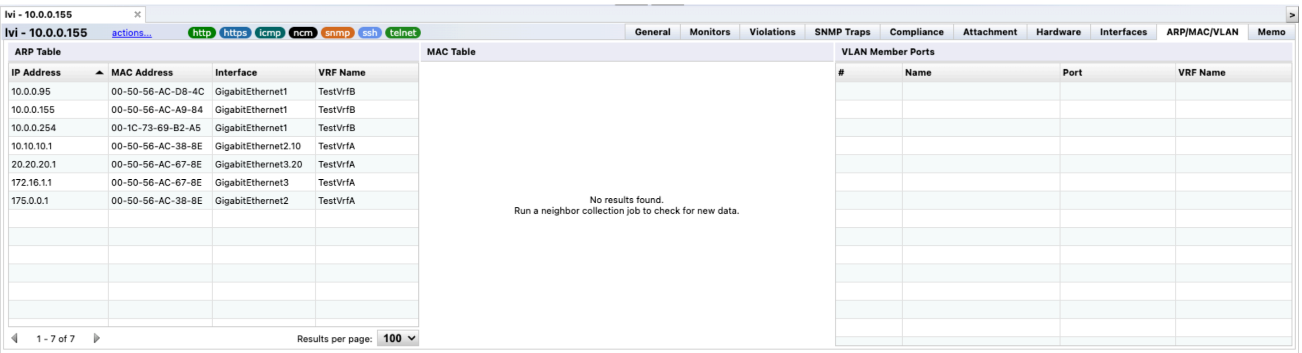
1. Click the [Inventory] main tab.
2. Doubleclick a device to open its Editor at the bottom of the window.

The device's VRF data will be visible in the Editor's [Interfaces] and [ARP/MAC/VLAN] tabs:



Admin	Name	Alias	Type	IP	Speed	MTU	MAC	Comment	VRF Name
⇧	GigabitEthernet1	PC	ethernet	10.0.0.155/24	1 Gbps	1500	005056ACA984		TestVrfB
⇧	GigabitEthernet2	Phone	ethernet	175.0.0.1/24	1 Gbps	1500	005056AC388E		TestVrfA
⇧	GigabitEthernet2.10		ethernet	10.10.10.1/24	1 Gbps	1500	005056AC388E		TestVrfA
⇧	GigabitEthernet3	UPLINK - DUN-ASW-ADM1-01	ethernet	172.16.1.1/24	1 Gbps	1500	005056AC678E		TestVrfA
⇧	GigabitEthernet3.20		ethernet	20.20.20.1/24	1 Gbps	1500	005056AC678E		TestVrfA

> **Note**
>
> These columns will be empty if there is no VRF information associated with the device.



ARP Table

IP Address	MAC Address	Interface	VRF Name
10.0.0.95	00-50-56-AC-D8-4C	GigabitEthernet1	TestVrfB
10.0.0.155	00-50-56-AC-A9-84	GigabitEthernet1	TestVrfB
10.0.0.254	00-1C-73-69-B2-A5	GigabitEthernet1	TestVrfB
10.10.10.1	00-50-56-AC-38-8E	GigabitEthernet2.10	TestVrfA
20.20.20.1	00-50-56-AC-67-8E	GigabitEthernet3.20	TestVrfA
172.16.1.1	00-50-56-AC-67-8E	GigabitEthernet3	TestVrfA
175.0.0.1	00-50-56-AC-38-8E	GigabitEthernet2	TestVrfA

1 - 7 of 7

MAC Table

No results found.
Run a neighbor collection job to check for new data.

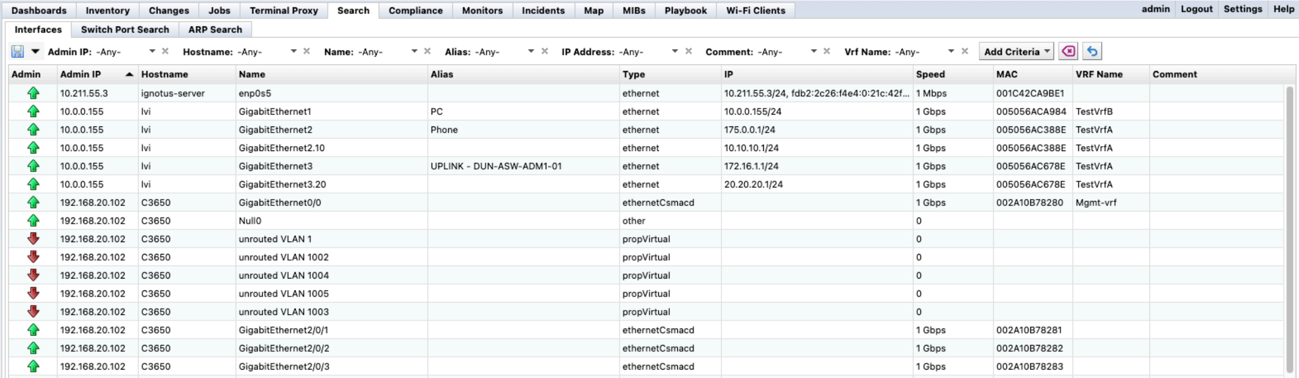
VLAN Member Ports

#	Name	Port	VRF Name

You can also view a device’s VRF data in the [Search] main tab:

1. Click the [Search] main tab.
2. Click the [Interfaces] subtab.

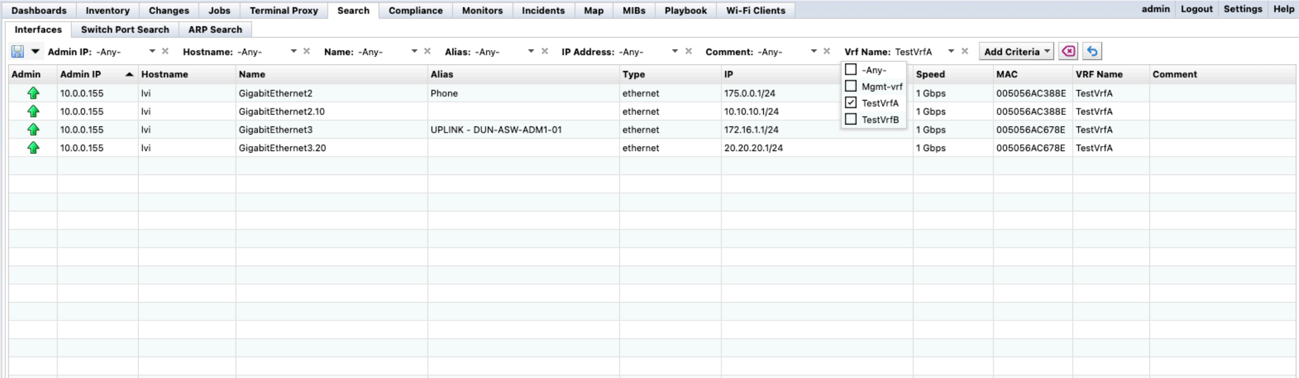
The device’s “VRF Name” will be displayed in a column on the righthand side of the window.



Admin IP: -Any- Hostname: -Any- Name: -Any- Alias: -Any- IP Address: -Any- Comment: -Any- Vrf Name: -Any-

Admin	Admin IP	Hostname	Name	Alias	Type	IP	Speed	MAC	VRF Name	Comment
↑	10.211.55.3	ignotus-server	enp0s5		ethernet	10.211.55.3/24, fdb2:2c26:f4e4:0:21c:42f...	1 Mbps	001C42CA9BE1		
↑	10.0.0.155	lvi	GigabitEthernet1	PC	ethernet	10.0.0.155/24	1 Gbps	005056ACA984	TestVrfB	
↑	10.0.0.155	lvi	GigabitEthernet2	Phone	ethernet	175.0.0.1/24	1 Gbps	005056AC388E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet2.10		ethernet	10.10.10.1/24	1 Gbps	005056AC388E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet3	UPLINK - DUN-ASW-ADM1-01	ethernet	172.16.1.1/24	1 Gbps	005056AC678E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet3.20		ethernet	20.20.20.1/24	1 Gbps	005056AC678E	TestVrfA	
↑	192.168.20.102	C3650	GigabitEthernet0/0		ethernetCsmacd		1 Gbps	002A10B78280	Mgmt-vrf	
↑	192.168.20.102	C3650	Null0		other		0			
↓	192.168.20.102	C3650	unrouted VLAN 1		propVirtual		0			
↓	192.168.20.102	C3650	unrouted VLAN 1002		propVirtual		0			
↓	192.168.20.102	C3650	unrouted VLAN 1004		propVirtual		0			
↓	192.168.20.102	C3650	unrouted VLAN 1005		propVirtual		0			
↓	192.168.20.102	C3650	unrouted VLAN 1003		propVirtual		0			
↑	192.168.20.102	C3650	GigabitEthernet2/0/1		ethernetCsmacd		1 Gbps	002A10B78281		
↑	192.168.20.102	C3650	GigabitEthernet2/0/2		ethernetCsmacd		1 Gbps	002A10B78282		
↑	192.168.20.102	C3650	GigabitEthernet2/0/3		ethernetCsmacd		1 Gbps	002A10B78283		

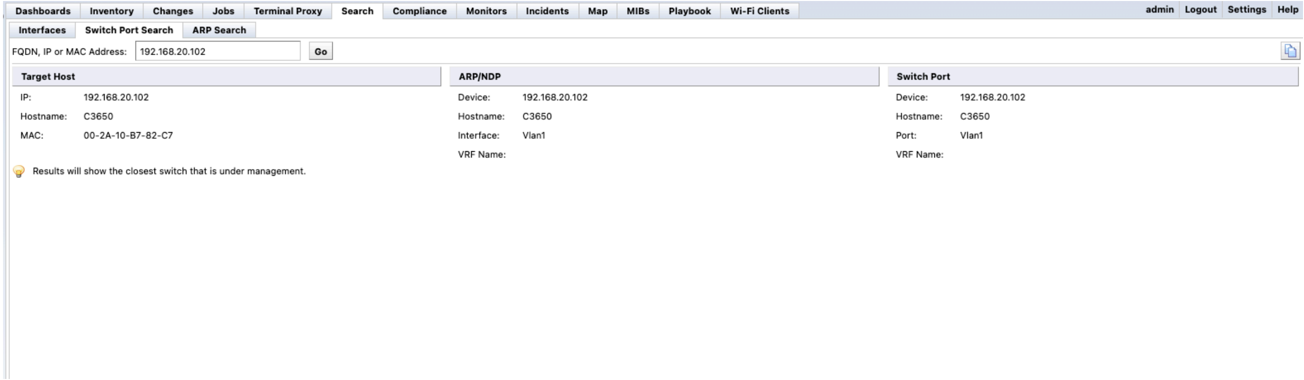
In the [Interfaces] subtab, you can also filter VRF devices by clicking the dropdown menu next to “VRF Name” in the [Interfaces] subtab’s top menu bar:



Admin IP: -Any- Hostname: -Any- Name: -Any- Alias: -Any- IP Address: -Any- Comment: -Any- Vrf Name: TestVrfA

Admin	Admin IP	Hostname	Name	Alias	Type	IP	Speed	MAC	VRF Name	Comment
↑	10.0.0.155	lvi	GigabitEthernet2	Phone	ethernet	175.0.0.1/24	1 Gbps	005056AC388E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet2.10		ethernet	10.10.10.1/24	1 Gbps	005056AC388E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet3	UPLINK - DUN-ASW-ADM1-01	ethernet	172.16.1.1/24	1 Gbps	005056AC678E	TestVrfA	
↑	10.0.0.155	lvi	GigabitEthernet3.20		ethernet	20.20.20.1/24	1 Gbps	005056AC678E	TestVrfA	

Click the [Switch Port Search] subtab to search for a device by address, and view its “ARP/NDP” and “Switch Port” information:



FQDN, IP or MAC Address: 192.168.20.102

Target Host

IP: 192.168.20.102
Hostname: C3650
MAC: 00-2A-10-B7-82-C7

ARP/NDP

Device: 192.168.20.102
Hostname: C3650
Interface: Vlan1
VRF Name:

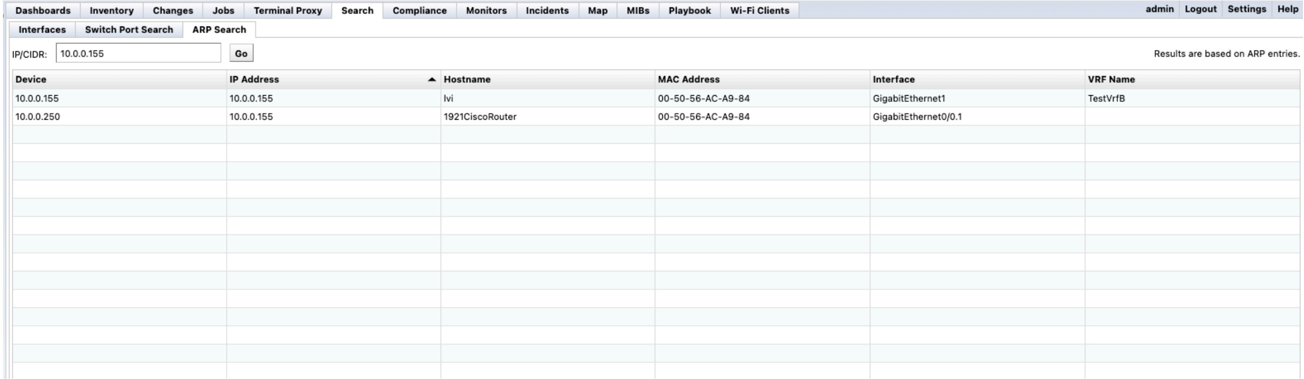
Switch Port

Device: 192.168.20.102
Hostname: C3650
Port: Vlan1
VRF Name:

Results will show the closest switch that is under management.

Click the [ARP] subtab to search for a device, and view its “VRF Name” in the rightmost column.

You can sort devices using their “VRF Name”.



IP/CIDR: 10.0.0.155

Results are based on ARP entries.

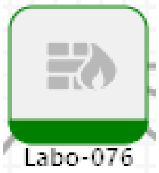
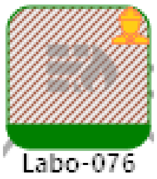
Device	IP Address ▲	Hostname	MAC Address	Interface	VRF Name
10.0.0.155	10.0.0.155	lvi	00-50-56-AC-A9-84	GigabitEthernet1	TestVrfB
10.0.0.250	10.0.0.155	1921CiscoRouter	00-50-56-AC-A9-84	GigabitEthernet0/0.1	

SECTION 21

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:

Monitoring mode	Maintenance mode
	

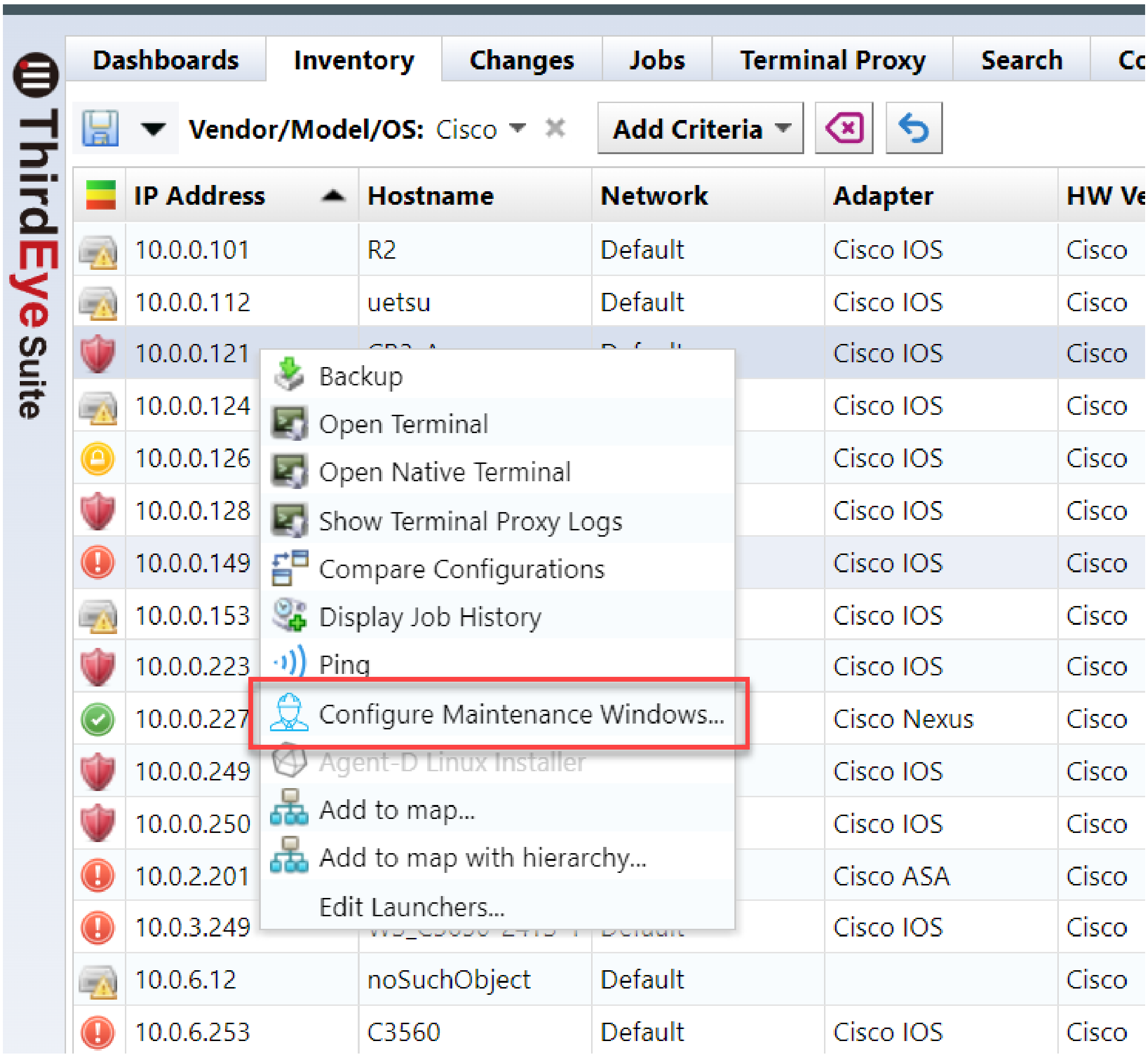
21.1 Manual Maintenance Mode

1. Click the [Inventory] main tab.

2. Select and rightclick the device for which you want to set maintenance mode.

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

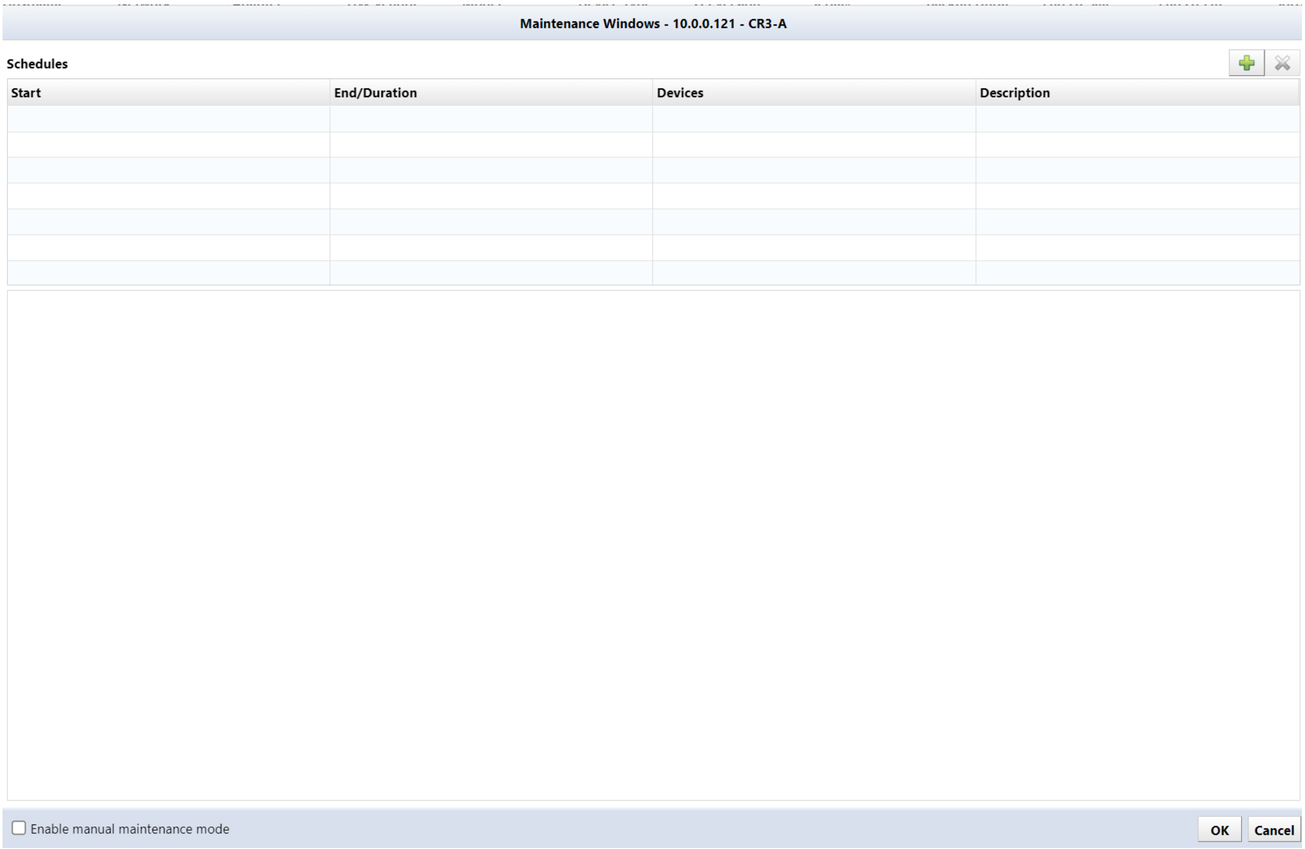
2. Click [Configure Maintenance Windows…].



	IP Address	Hostname	Network	Adapter	HW Ve
	10.0.0.101	R2	Default	Cisco IOS	Cisco
	10.0.0.112	uetsu	Default	Cisco IOS	Cisco
	10.0.0.121			Cisco IOS	Cisco
	10.0.0.124			Cisco IOS	Cisco
	10.0.0.126			Cisco IOS	Cisco
	10.0.0.128			Cisco IOS	Cisco
	10.0.0.149			Cisco IOS	Cisco
	10.0.0.153			Cisco IOS	Cisco
	10.0.0.223			Cisco IOS	Cisco
	10.0.0.227			Cisco Nexus	Cisco
	10.0.0.249			Cisco IOS	Cisco
	10.0.0.250			Cisco IOS	Cisco
	10.0.2.201			Cisco ASA	Cisco
	10.0.3.249			Cisco IOS	Cisco
	10.0.6.12	noSuchObject	Default		Cisco
	10.0.6.253	C3560	Default	Cisco IOS	Cisco

4. Check [Enable manual maintenance mode]

5. Click [OK].



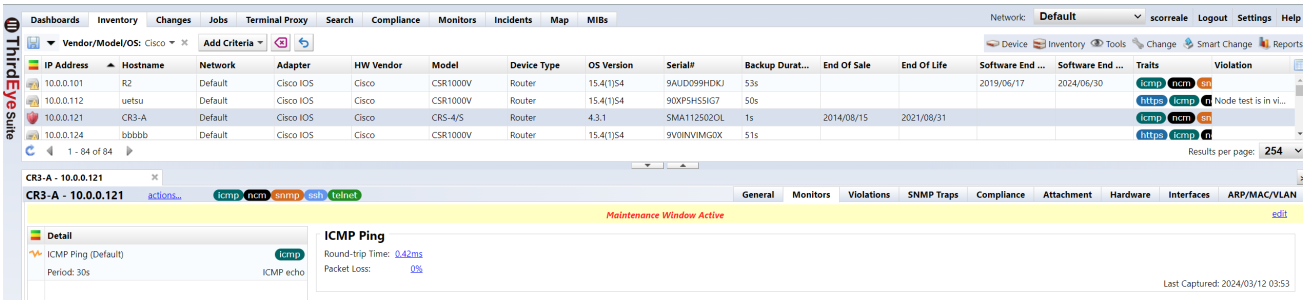
Maintenance Windows - 10.0.0.121 - CR3-A

Schedules

Start	End/Duration	Devices	Description

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.



Vendor/Model/OS: Cisco

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	53s			2019/06/17	2024/06/30	icmp ncm sn	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	50s					https icmp n	Node test is in vi...
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31			icmp ncm sn	
10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	51s					https icmp n	

1 - 84 of 84

Results per page: 254

CR3-A - 10.0.0.121

CR3-A - 10.0.0.121 actions... icmp ncm snmp ssh telnet

Maintenance Window Active edit

Detail

ICMP Ping (Default) icmp

Period: 30s ICMP echo

ICMP Ping

Round-trip Time: 0.42ms

Packet Loss: 0%

Last Captured: 2024/03/12 03:53

To cancel maintenance mode:

1. Uncheck “Enable manual maintenance mode” in Step 4.

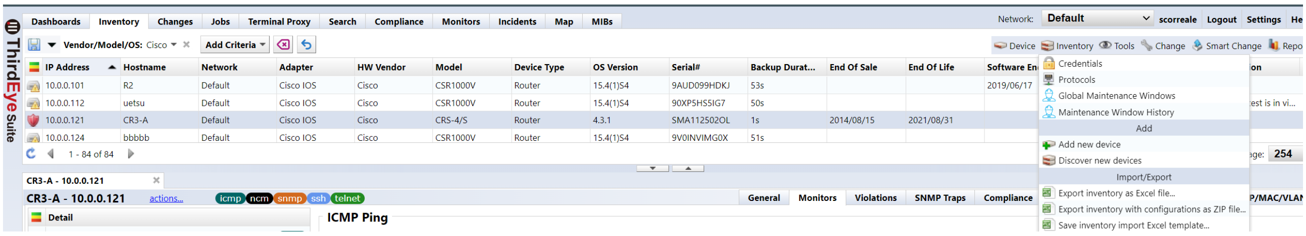
2. Click [OK].

21.2 Scheduled Maintenance Mode

1. Click the [Inventory] main tab.

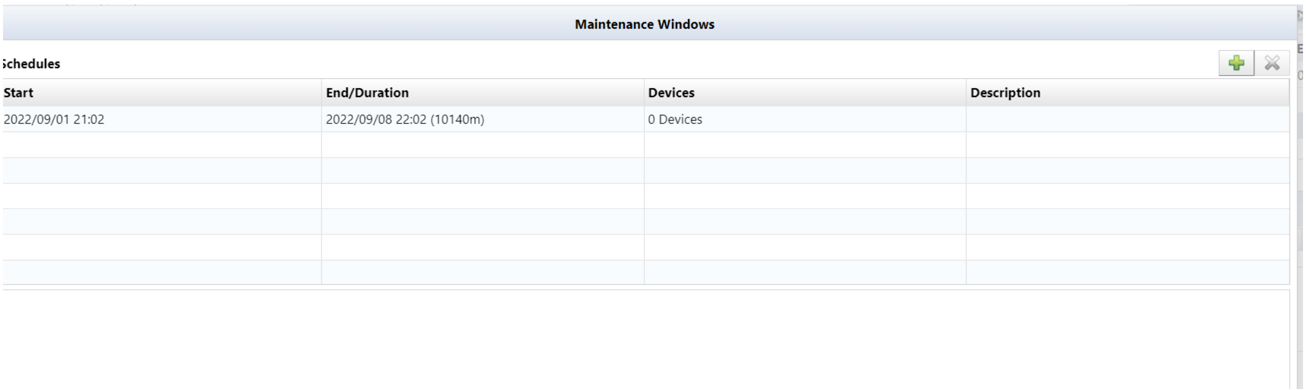
2. Click [Inventory] in the menu bar.

3. Click [Global Maintenance Windows].



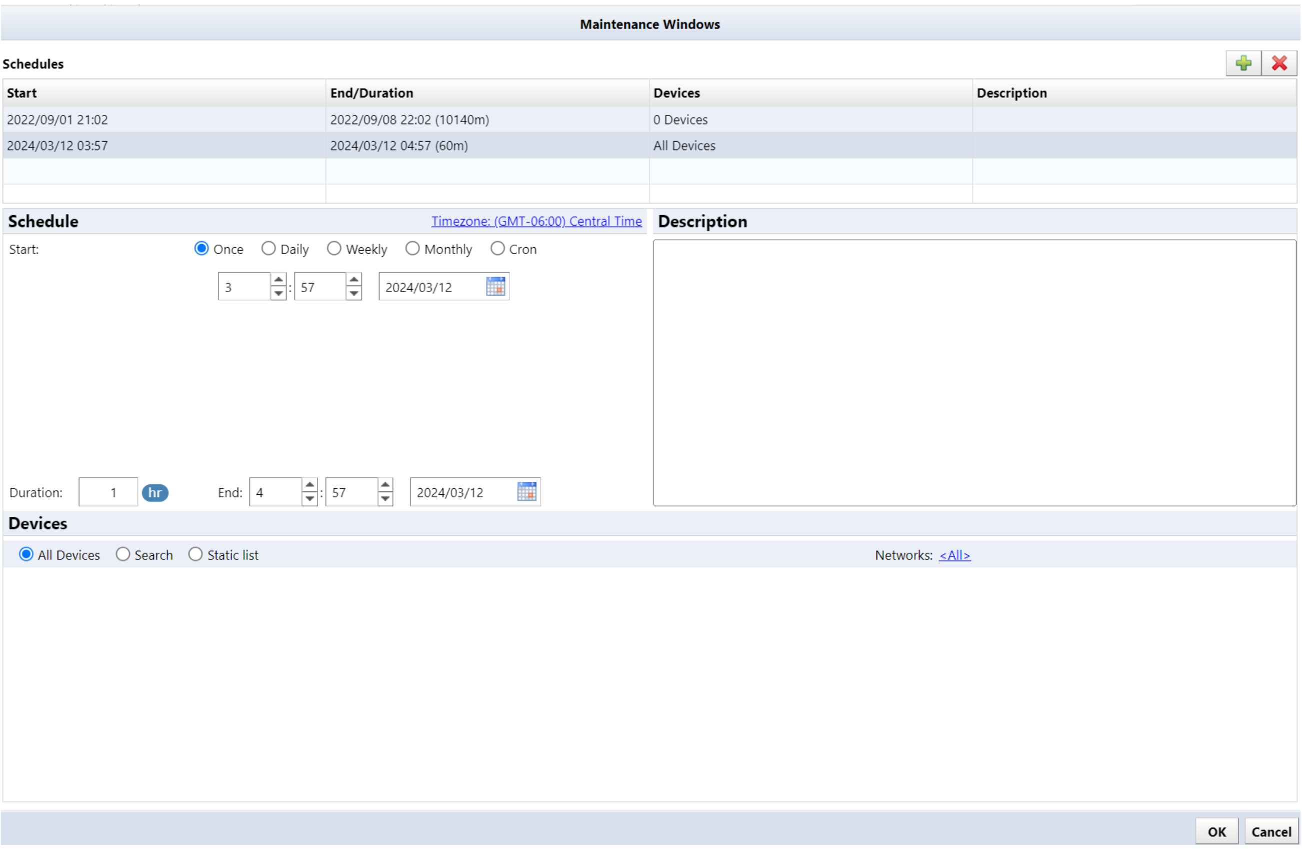
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software En	on
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	53s			2019/06/17	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	50s				est is in vi...
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31		
10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	51s				

4. Click the ✚ button.



Start	End/Duration	Devices	Description
2022/09/01 21:02	2022/09/08 22:02 (10140m)	0 Devices	

5. Set the schedule and devices.



Maintenance Windows

Schedules

Start	End/Duration	Devices	Description
2022/09/01 21:02	2022/09/08 22:02 (10140m)	0 Devices	
2024/03/12 03:57	2024/03/12 04:57 (60m)	All Devices	

Schedule — Timezone: (GMT-06:00) Central Time

Start: ● Once ○ Daily ○ Weekly ○ Monthly ○ Cron

3 : 57 2024/03/12

Duration: 1 hr End: 4 : 57 2024/03/12

Description

Devices

● All Devices ○ Search ○ Static list Networks: <All>

[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.

Menu Item	Submenu Item	Explanation
		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”.
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

6. Click [OK].

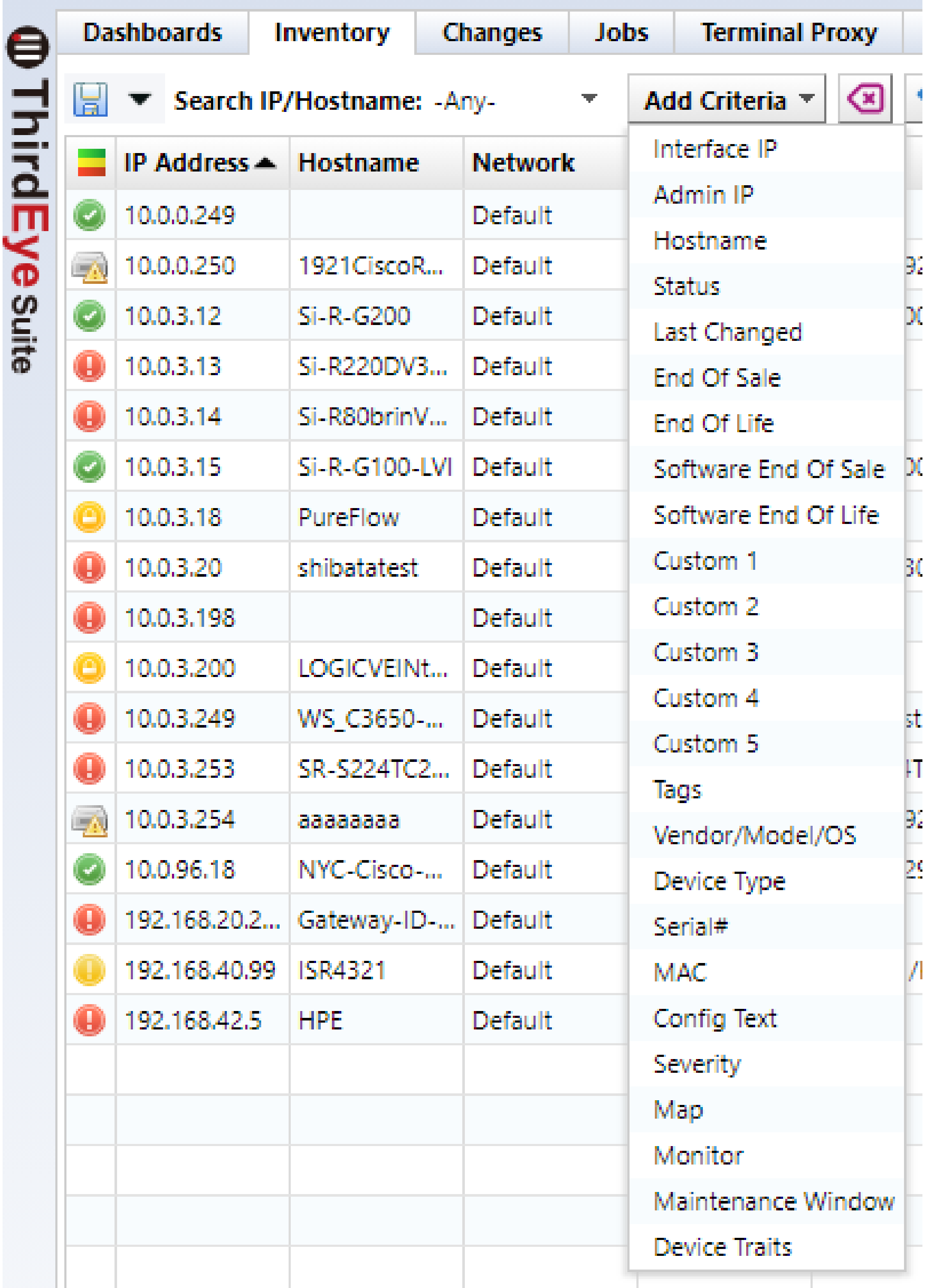
With the above operations, the device will be placed in a non-monitoring state according to the time set in the schedule.

21.3 Find Non-Monitored Devices

You can search devices that maintenance using the search criteria on the [Inventory] main tab.

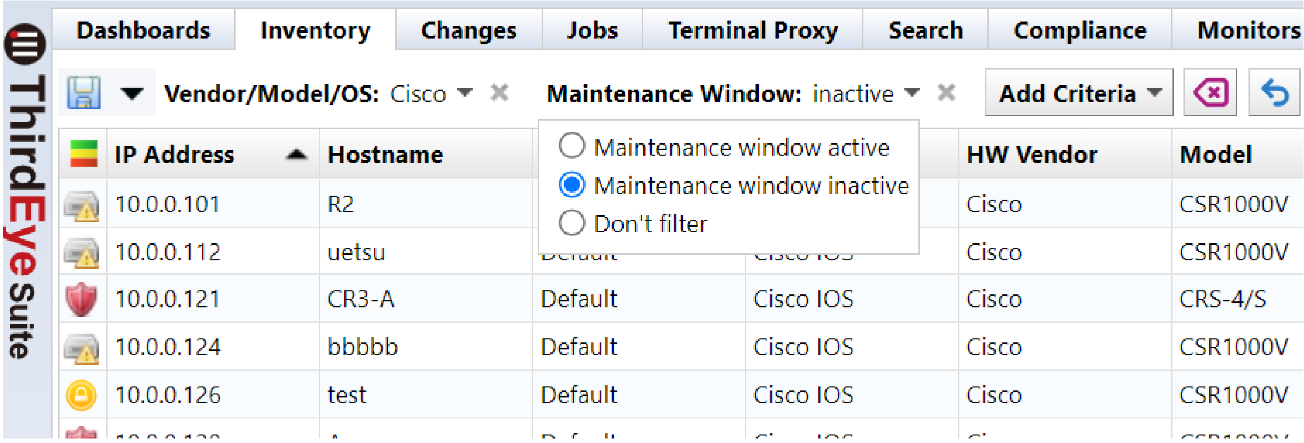
1. Click the [Inventory] main tab.

2. Click [Add criteria] > [Maintenance Window].



	IP Address ▲	Hostname	Network
✓	10.0.0.249		Default
⚠	10.0.0.250	1921CiscoR...	Default
✓	10.0.3.12	Si-R-G200	Default
❗	10.0.3.13	Si-R220DV3...	Default
❗	10.0.3.14	Si-R80brinV...	Default
✓	10.0.3.15	Si-R-G100-LVI	Default
🔒	10.0.3.18	PureFlow	Default
❗	10.0.3.20	shibatatest	Default
❗	10.0.3.198		Default
🔒	10.0.3.200	LOGICVEINt...	Default
❗	10.0.3.249	WS_C3650-...	Default
❗	10.0.3.253	SR-S224TC2...	Default
⚠	10.0.3.254	aaaaaaaa	Default
✓	10.0.96.18	NYC-Cisco-...	Default
❗	192.168.20.2...	Gateway-ID-...	Default
!	192.168.40.99	ISR4321	Default
❗	192.168.42.5	HPE	Default

2. Select [Maintenance window inactive].



Vendor/Model/OS: Cisco

Maintenance Window: inactive

○ Maintenance window active
● Maintenance window inactive
○ Don't filter

	IP Address	Hostname			HW Vendor	Model
⚠	10.0.0.101	R2			Cisco	CSR1000V
⚠	10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V
	10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S
⚠	10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V
	10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V

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

SECTION 22

POLICY ACTIONS

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

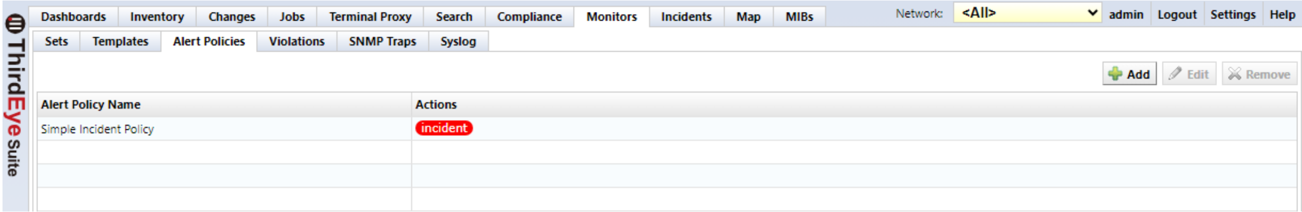
- Incident registration/sending emails
- Program execution
- SNMP trap

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.

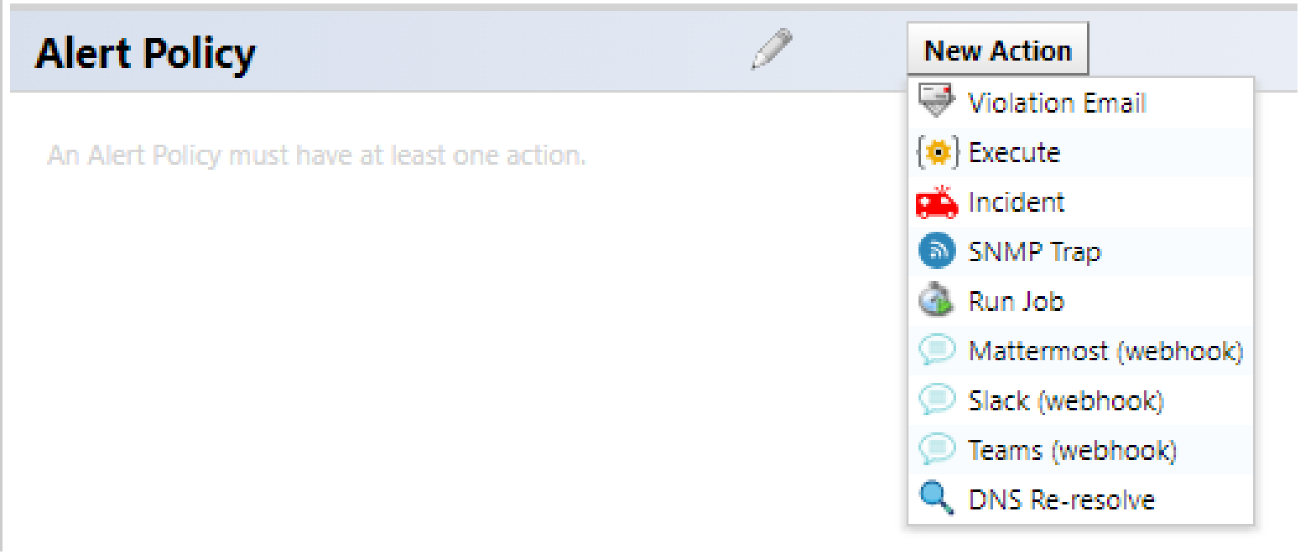
To create a new alert policy:

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



Alert Policy Name	Actions
Simple Incident Policy	incident

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



An Alert Policy must have at least one action.

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

Action details

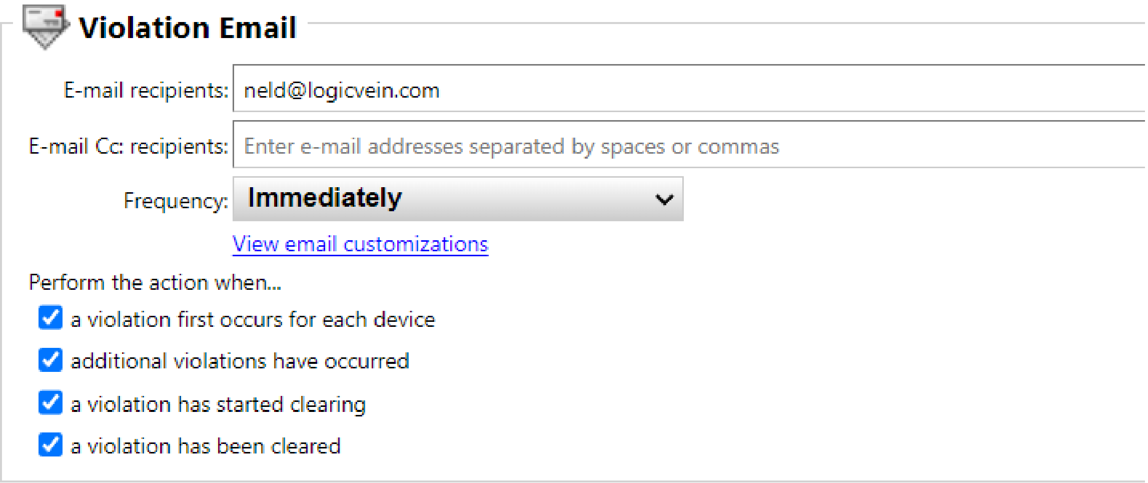
Action	Explanation
Execution	Executes a command on a remote host when a failure is detected.
Incident	Registers an incident and sends an email when a failure is detected.
SNMP Trap	Sends an SNMP trap when a failure is detected.
Run job	Execute the registered job.
Violation mail	Sends an email when a 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.
PagerDuty	Notify PagerDuty 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. The following sections explain each action in detail.

22.1 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

E-mail recipients: neld@logicvein.com

E-mail Cc: recipients: Enter e-mail addresses separated by spaces or commas

Frequency: Immediately

View email customizations

Perform the action when...

☑ a violation first occurs for each device

☑ additional violations have occurred

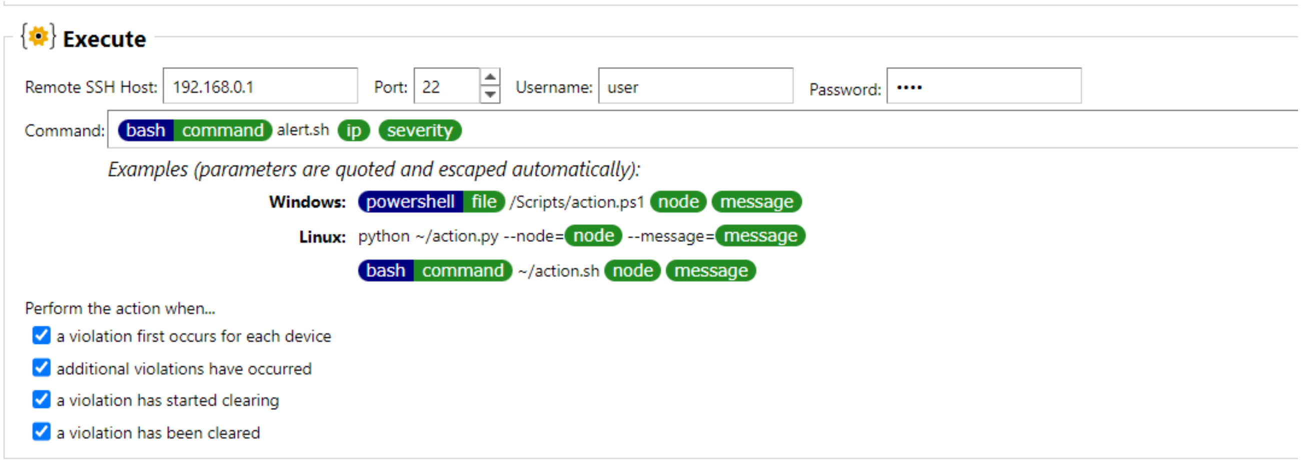
☑ a violation has started clearing

☑ a violation has been cleared

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”.

22.2 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

Remote SSH Host: 192.168.0.1 Port: 22 Username: user Password: ••••

Command: bash command alert.sh ip severity

Examples (parameters are quoted and escaped automatically):

Windows: powershell file /Scripts/action.ps1 node message

Linux: python ~/action.py --node= node --message= message

bash command ~/action.sh node message

Perform the action when...

☑ a violation first occurs for each device

☑ additional violations have occurred

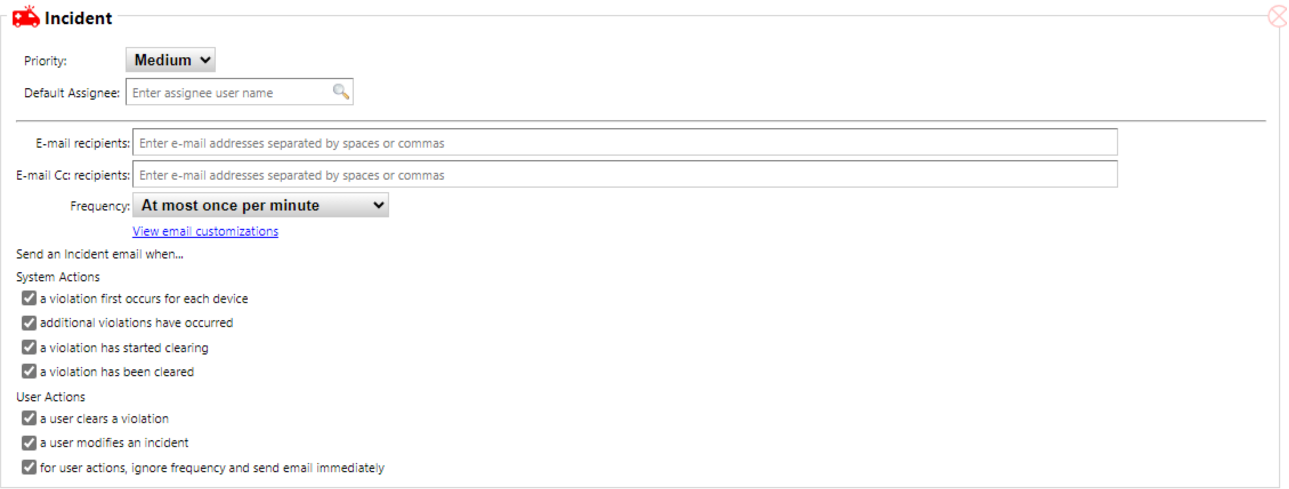
☑ a violation has started clearing

☑ a violation has been cleared

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”.

22.3 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

Priority: Medium

Default Assignee: Enter assignee user name

E-mail recipients: Enter e-mail addresses separated by spaces or commas

E-mail Cc: recipients: Enter e-mail addresses separated by spaces or commas

Frequency: At most once per minute

View email customizations

Send an Incident email when...

System Actions

- ☑ a violation first occurs for each device
- ☑ additional violations have occurred
- ☑ a violation has started clearing
- ☑ a violation has been cleared

User Actions

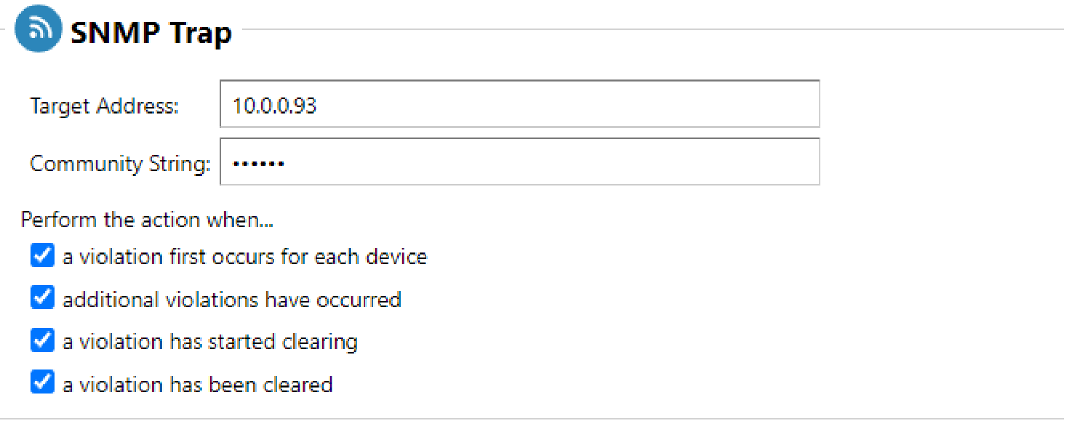
- ☑ a user clears a violation
- ☑ a user modifies an incident
- ☑ for user actions, ignore frequency and send email immediately

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”.

Incident Setting	Explanation
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.

22.4 Send SNMP Trap To Devices

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



SNMP Trap

Target Address: 10.0.0.93

Community String: ••••••

Perform the action when...

☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

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

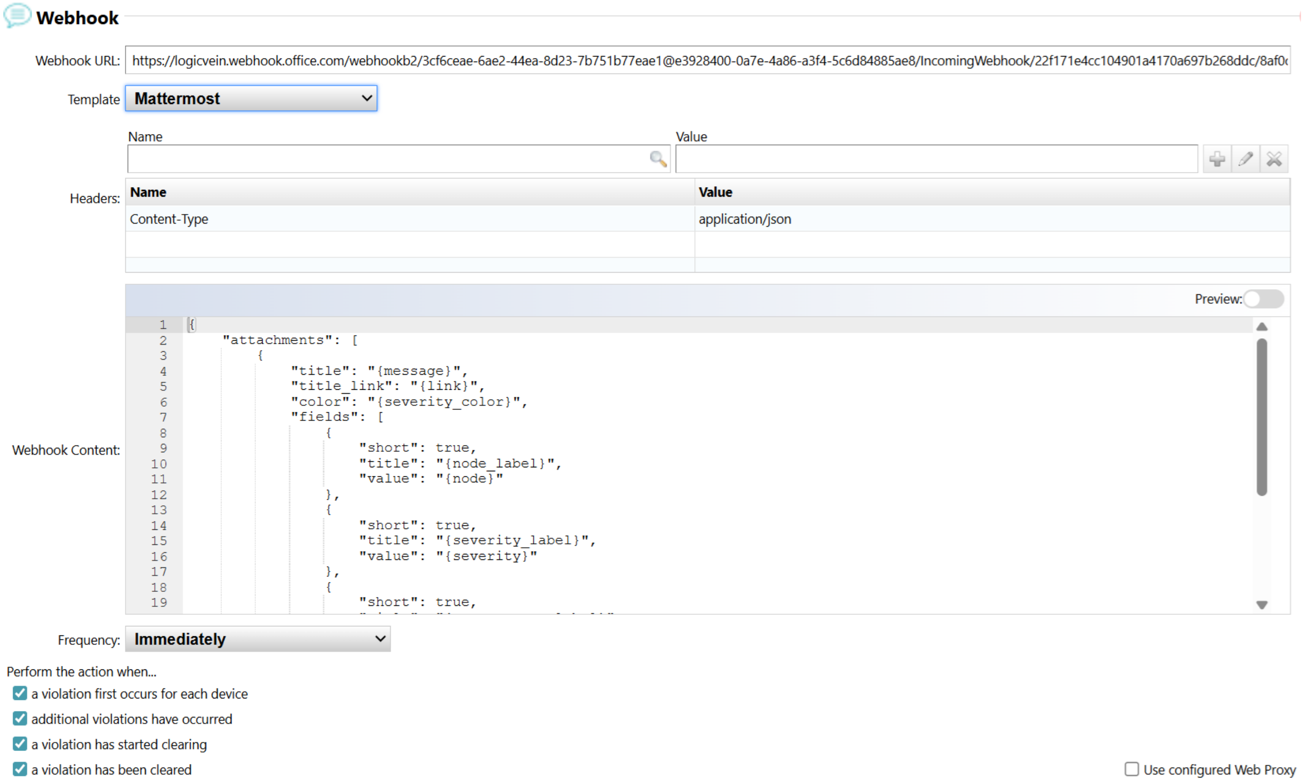
Trap Variables	Variable Name	Explanation
	thirdEyeDeviceUuid	UUID of the failed device (used internally by ThirdEye)

Trap Variables	Variable Name	Explanation
	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
	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

22.5 Webhooks

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

Mattermost:



Webhook

Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: Mattermost

Headers:

Name	Value
Content-Type	application/json

Webhook Content:

Preview: ○

```
{
    "attachments": [
        {
            "title": "{message}",
            "title_link": "{link}",
            "color": "{severity_color}",
            "fields": [
                {
                    "short": true,
                    "title": "{node_label}",
                    "value": "{node}"
                },
                {
                    "short": true,
                    "title": "{severity_label}",
                    "value": "{severity}"
                },
                {
                    "short": true,
```

Frequency: Immediately

Perform the action when...

☑ a violation first occurs for each device

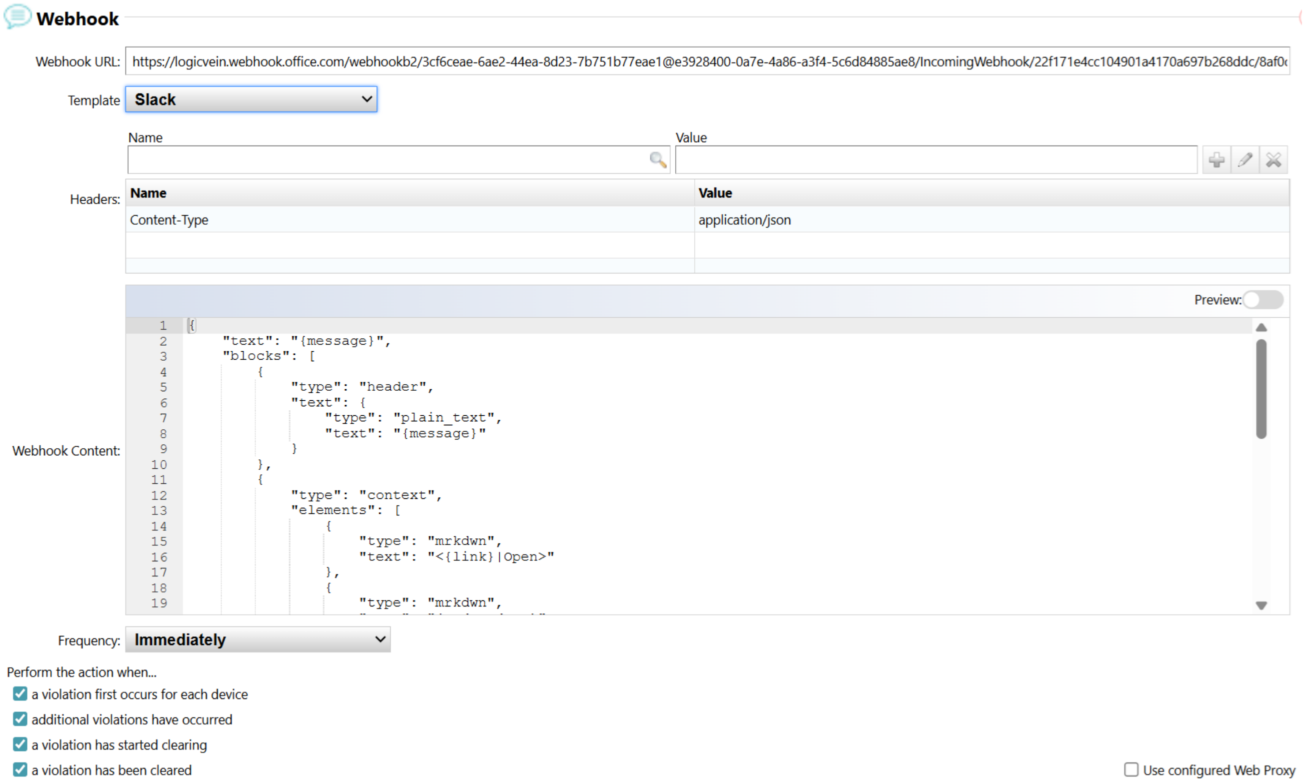
☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

□ Use configured Web Proxy

Slack:



Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: Slack

Headers:

Name	Value
Content-Type	application/json

Webhook Content:

```
{
    "text": "{message}",
    "blocks": [
        {
            "type": "header",
            "text": {
                "type": "plain_text",
                "text": "{message}"
            }
        },
        {
            "type": "context",
            "elements": [
                {
                    "type": "mrkdwn",
                    "text": "<{link}|Open>"
                },
                {
                    "type": "mrkdwn",
```

Frequency: Immediately

Perform the action when...

☑ a violation first occurs for each device

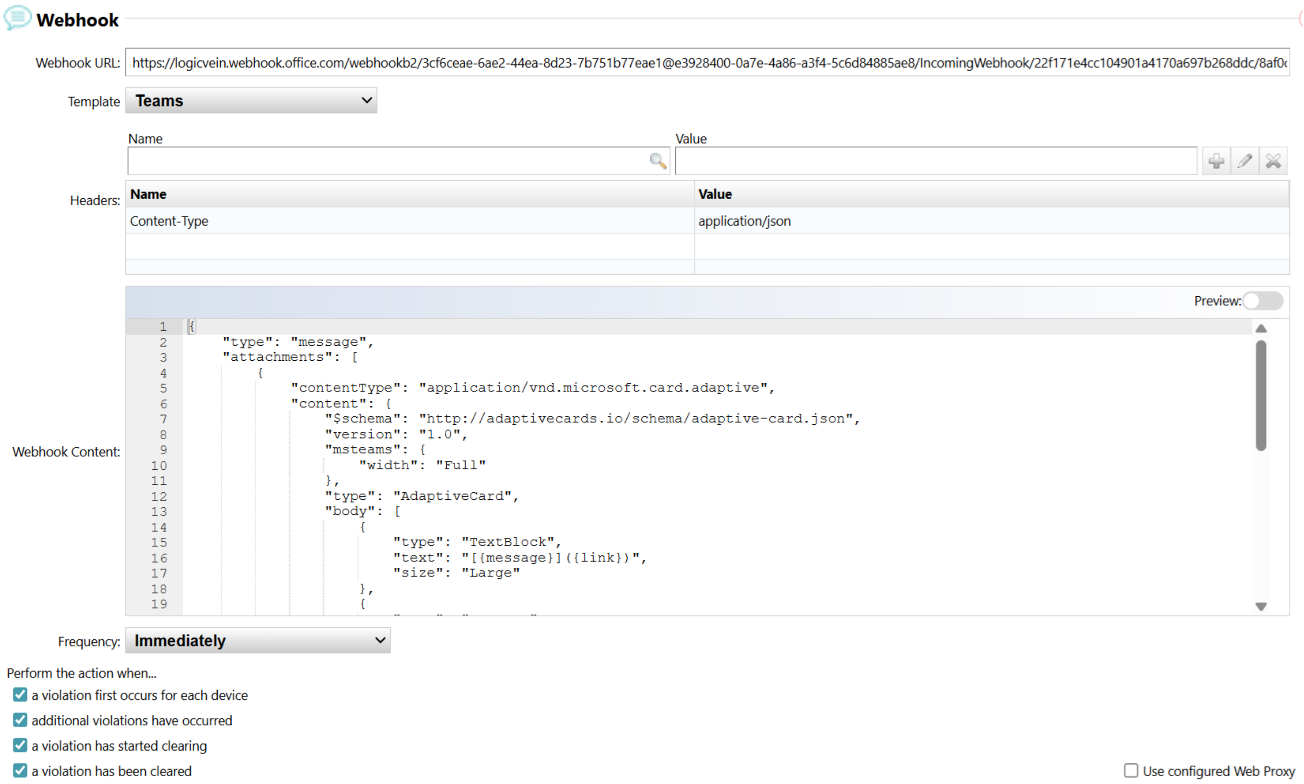
☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

☐ Use configured Web Proxy

Teams:



Webhook

Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: Teams

Headers:

Name	Value
Content-Type	application/json

Preview: ○

Webhook Content:

```
{
    "type": "message",
    "attachments": [
        {
            "contentType": "application/vnd.microsoft.card.adaptive",
            "content": {
                "$schema": "http://adaptivecards.io/schema/adaptive-card.json",
                "version": "1.0",
                "msteams": {
                    "width": "Full"
                },
                "type": "AdaptiveCard",
                "body": [
                    {
                        "type": "TextBlock",
                        "text": "[{message}]({link})",
                        "size": "Large"
                    },
                    {
```

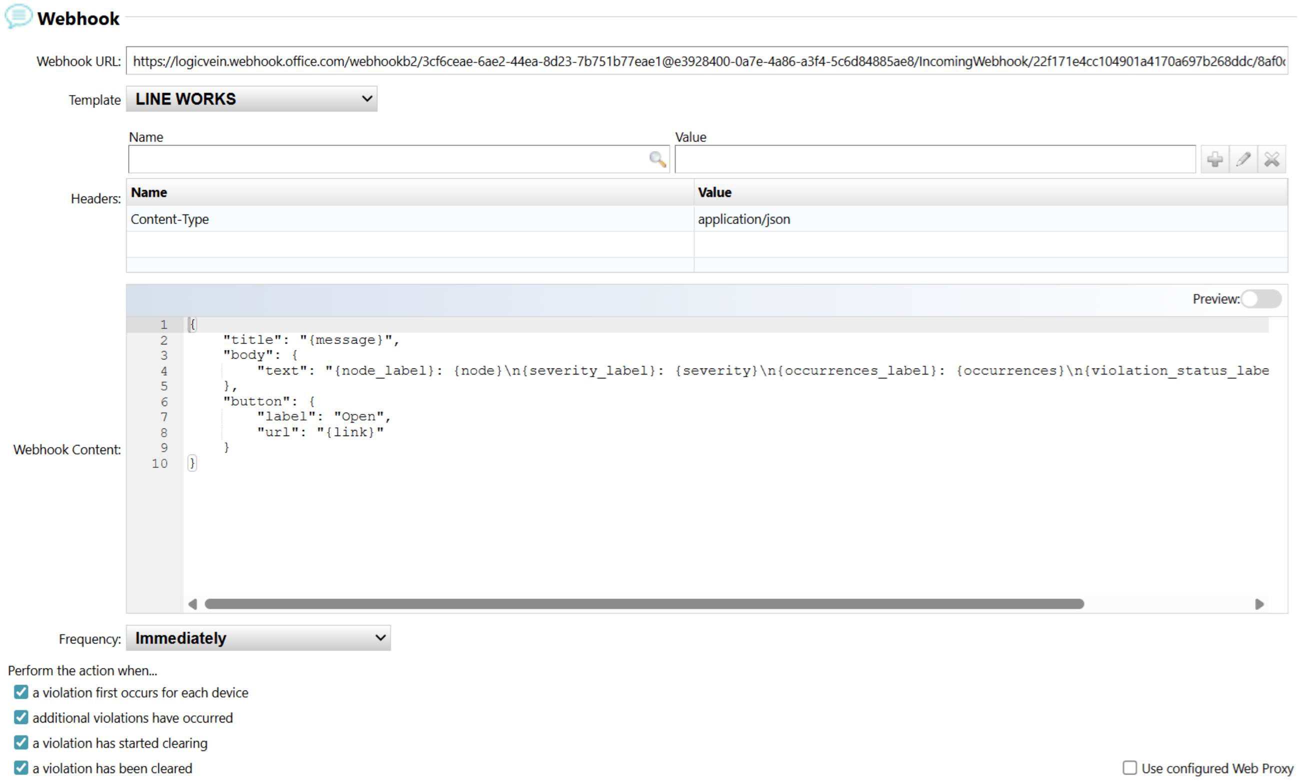
Frequency: Immediately

Perform the action when...

- ☑ a violation first occurs for each device
- ☑ additional violations have occurred
- ☑ a violation has started clearing
- ☑ a violation has been cleared

☐ Use configured Web Proxy

Line:



Webhook

Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: LINE WORKS

Headers:

Name	Value
Content-Type	application/json

Preview: ○

Webhook Content:

```
{
    "title": "{message}",
    "body": {
        "text": "{node_label}: {node}\n{severity_label}: {severity}\n{occurrences_label}: {occurrences}\n{violation_status_labe
    },
    "button": {
        "label": "Open",
        "url": "{link}"
    }
}
```

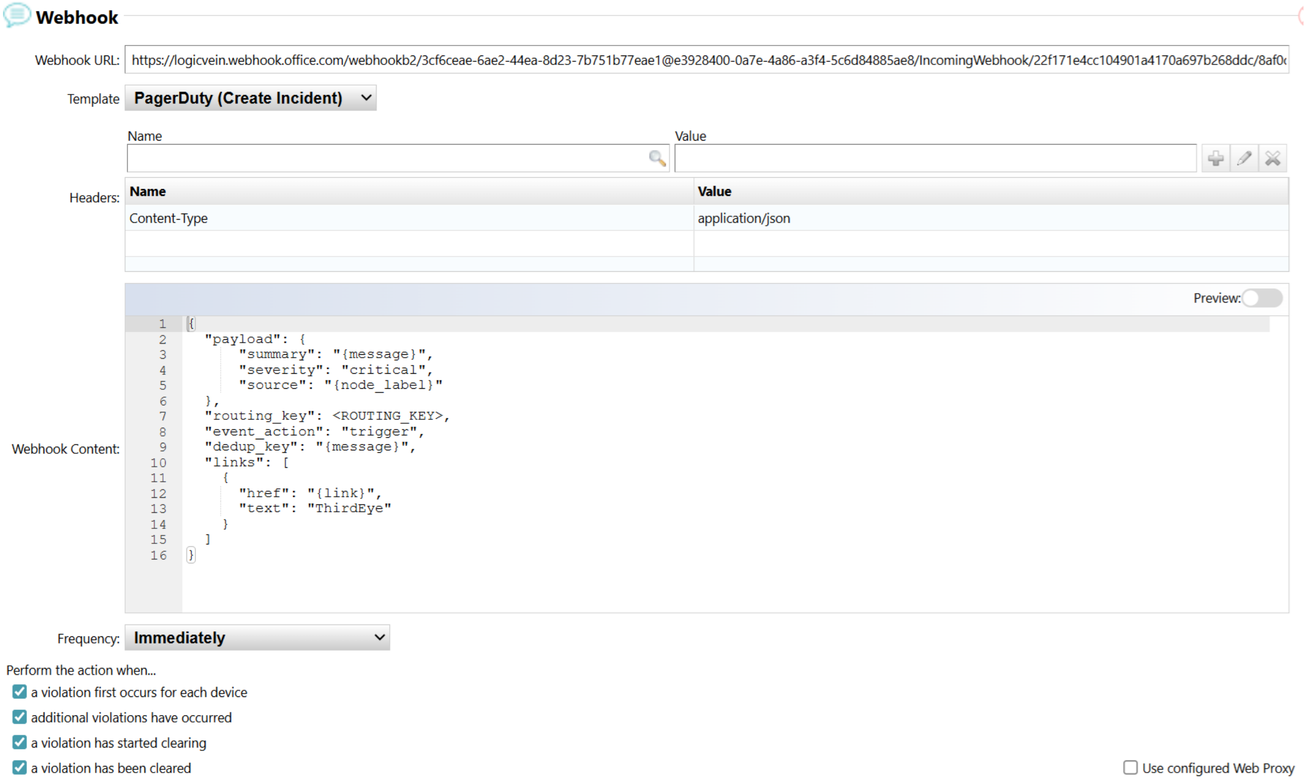
Frequency: Immediately

Perform the action when...

- ☑ a violation first occurs for each device
- ☑ additional violations have occurred
- ☑ a violation has started clearing
- ☑ a violation has been cleared

☐ Use configured Web Proxy

PagerDuty



Webhook

Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: PagerDuty (Create Incident)

Headers:

Name	Value
Content-Type	application/json

Webhook Content:

```
{
  "payload": {
      "summary": "{message}",
      "severity": "critical",
      "source": "{node_label}"
  },
  "routing_key": <ROUTING_KEY>,
  "event_action": "trigger",
  "dedup_key": "{message}",
  "links": [
    {
      "href": "{link}",
      "text": "ThirdEye"
    }
  ]
}
```

Frequency: Immediately

Perform the action when...

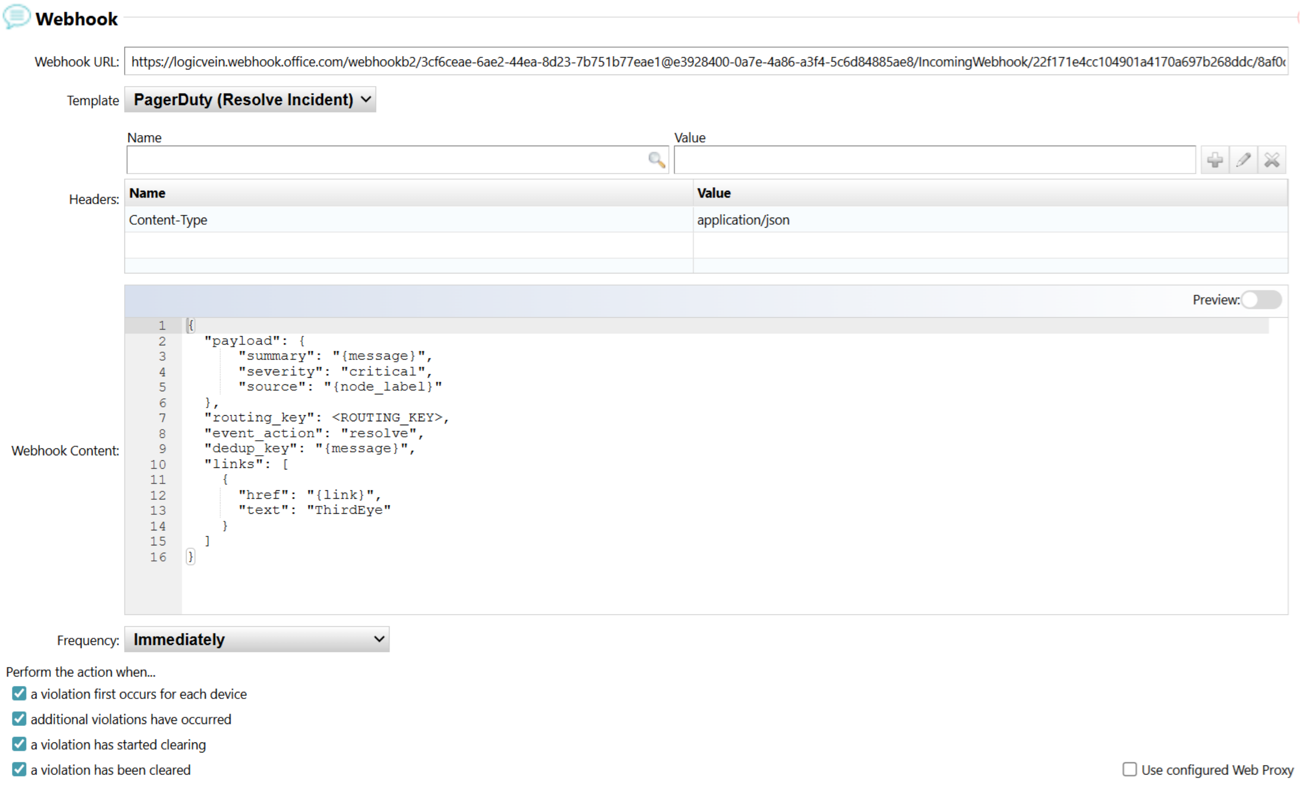
☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

□ Use configured Web Proxy



Webhook

Webhook URL: https://logicvein.webhook.office.com/webhookb2/3cf6ceae-6ae2-44ea-8d23-7b751b77eae1@e3928400-0a7e-4a86-a3f4-5c6d84885ae8/IncomingWebhook/22f171e4cc104901a4170a697b268ddc/8af0

Template: PagerDuty (Resolve Incident)

Headers:

Name	Value
Content-Type	application/json

Webhook Content:

```
{
  "payload": {
      "summary": "{message}",
      "severity": "critical",
      "source": "{node_label}"
  },
  "routing_key": <ROUTING_KEY>,
  "event_action": "resolve",
  "dedup_key": "{message}",
  "links": [
    {
      "href": "{link}",
      "text": "ThirdEye"
    }
  ]
}
```

Frequency: Immediately

Perform the action when...

☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

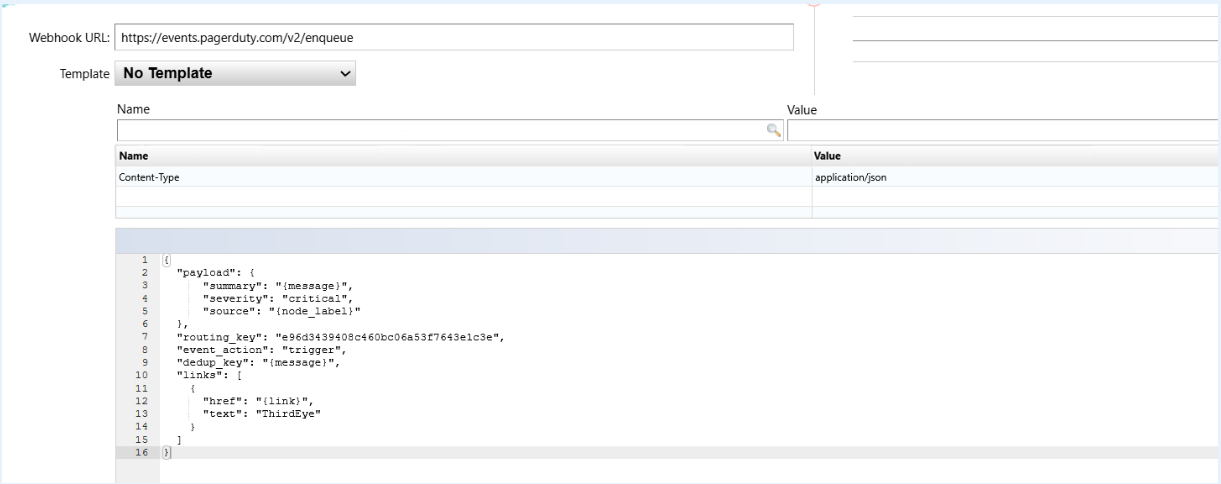
□ Use configured Web Proxy

Webhook Setting	Explanation
webhook url	Enter the URL generated on Mattermost/Slack/Teams/Line/PagerDuty.
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”.
Use configured Web Proxy	Select whether to use a Web Proxy.

Note

PagerDuty requires the user to enter a routing key when setting up a Webhook.

Without a routing key, “No Template” will be shown in the Template option field.



Webhook URL: https://events.pagerduty.com/v2/enqueue

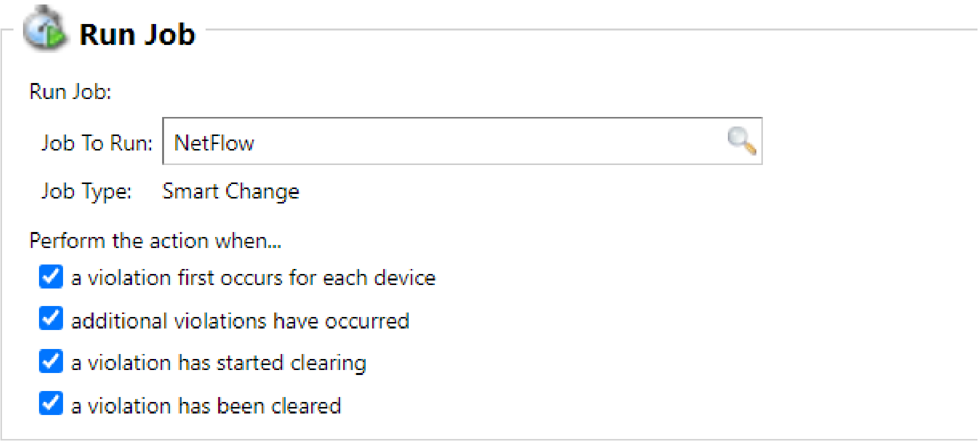
Template: No Template

Name	Value
Content-Type	application/json

```
{
  "payload": {
      "summary": "{message}",
      "severity": "critical",
      "source": "{node_label}"
  },
  "routing_key": "e96d3439408c460bc06a53f7643e1c3e",
  "event_action": "trigger",
  "dedup_key": "{message}",
  "links": [
    {
      "href": "{link}",
      "text": "ThirdEye"
    }
  ]
}
```

22.6 Run Jobs 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

Run Job:

Job To Run: NetFlow

Job Type: Smart Change

Perform the action when...

☑ a violation first occurs for each device

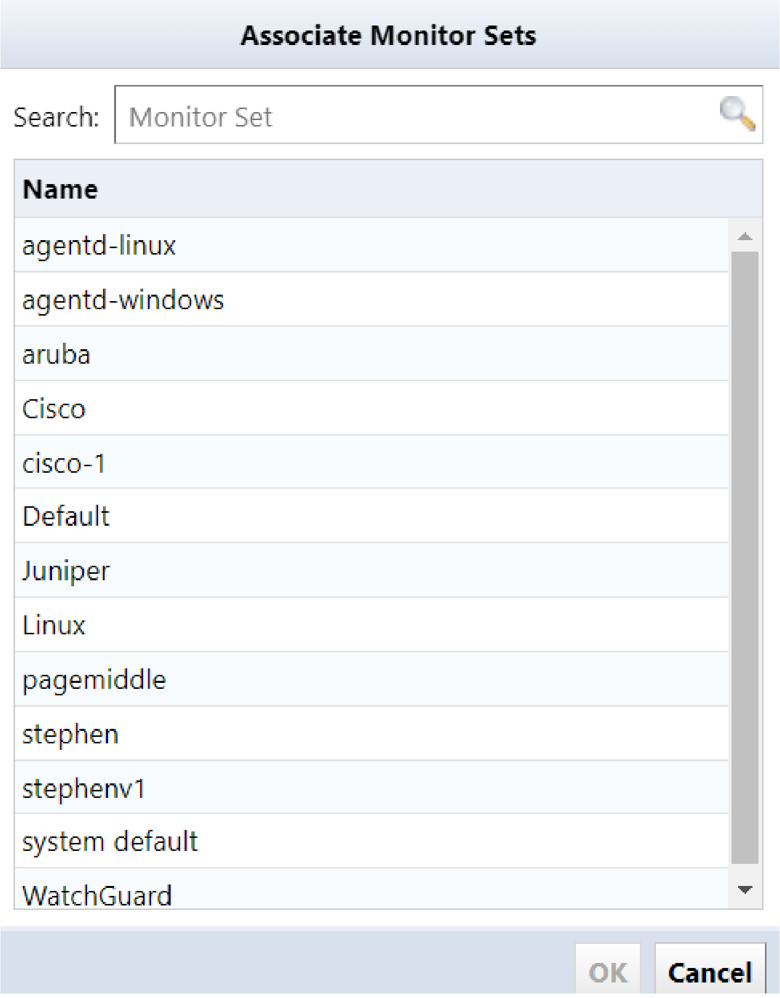
☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

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”.

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



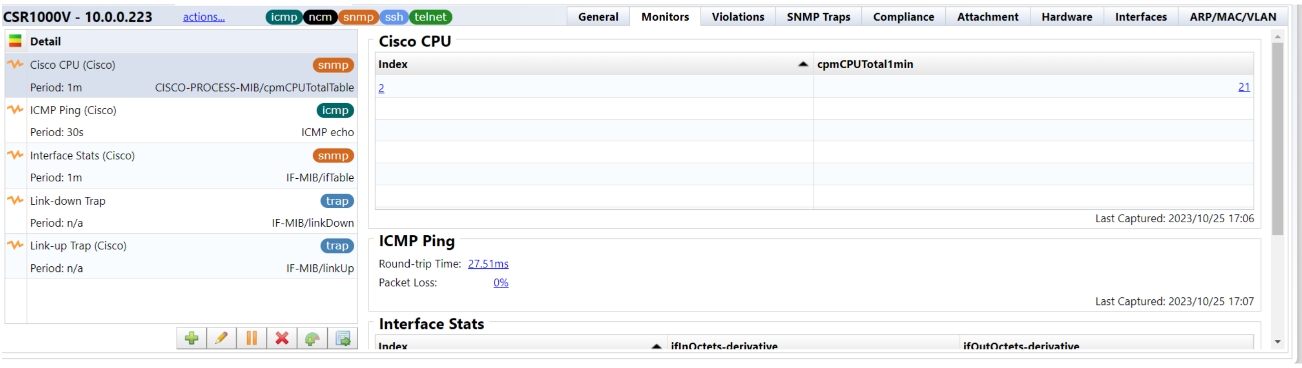
Associate Monitor Sets

Search: Monitor Set

Name
agentd-linux
agentd-windows
aruba
Cisco
cisco-1
Default
Juniper
Linux
pagemiddle
stephen
stephenv1
system default
WatchGuard

With the above operations, the application of the monitor set is completed.

The [Details] column in the 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.



Detail	
Cisco CPU (Cisco)	snmp
Period: 1m	CISCO-PROCESS-MIB/cpmCPUTotalTable
ICMP Ping (Cisco)	icmp
Period: 30s	ICMP echo
Interface Stats (Cisco)	snmp
Period: 1m	IF-MIB/ifTable
Link-down Trap	trap
Period: n/a	IF-MIB/linkDown
Link-up Trap (Cisco)	trap
Period: n/a	IF-MIB/linkUp

Cisco CPU

Index	cpmCPUTotal1min
2	21

Last Captured: 2023/10/25 17:06

ICMP Ping

Round-trip Time: 27.51ms
Packet Loss: 0%

Last Captured: 2023/10/25 17:07

Interface Stats

Index	ifInOctets-derivative	ifOutOctets-derivative

22.7 Anomaly Alerts

Anomaly alerts are automated monitoring systems that detect deviations from established normal patterns in network operations. They employ statistical analysis to create baseline thresholds through a 14-day learning period, analyzing metric distributions (min/max values, standard deviation) across different time intervals. They then determine the parameters for an alert.

These alerts enable you to identify potential issues in network infrastructure before they escalate. Anomaly alerts are particularly useful for detecting zero-day anomalies and subtle performance degradation.

After the learning phase, violations trigger when metrics exceed statistically calculated ranges.

Key characteristics:

- **Automatic Thresholding**: Eliminates manual configuration by learning normal patterns
- **Pattern Recognition**: Analyzes daily/weekly cycles and seasonal variations
- **Proactive Detection**: Flags unusual activity like traffic spikes, resource anomalies, or performance deviations
- **Multi-Metric Analysis**: Processes 50+ device metrics simultaneously

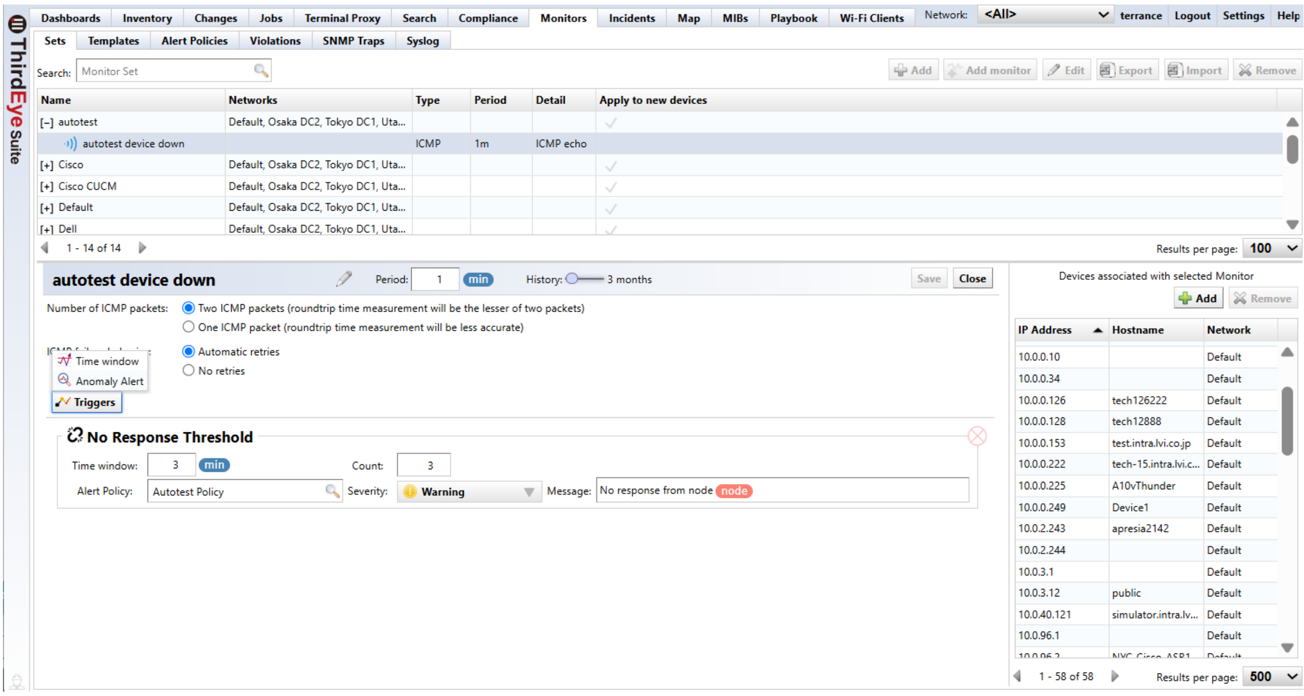
22.8 Enabling a device

1. Select the device in the [Inventory] tab.

2. In the [Monitors] tab, double click to select the incident to which the anomaly alert will be applied.

3. Click the [Triggers] button.

4. Click [Anomaly Alert].



Search: Monitor Set

Name	Networks	Type	Period	Detail	Apply to new devices
[–] autotest	Default, Osaka DC2, Tokyo DC1, Uta...				✓
autotest device down		ICMP	1m	ICMP echo	
[+] Cisco	Default, Osaka DC2, Tokyo DC1, Uta...				✓
[+] Cisco CUCM	Default, Osaka DC2, Tokyo DC1, Uta...				✓
[+] Default	Default, Osaka DC2, Tokyo DC1, Uta...				✓
[+] Dell	Default, Osaka DC2, Tokyo DC1, Uta...				✓

1 - 14 of 14 Results per page: 100

autotest device down Period: 1 min History: 3 months

Number of ICMP packets: ● Two ICMP packets (roundtrip time measurement will be the lesser of two packets)
○ One ICMP packet (roundtrip time measurement will be less accurate)

● Automatic retries
○ No retries

No Response Threshold

Time window: 3 min Count: 3

Alert Policy: Autotest Policy Severity: Warning Message: No response from node node

Devices associated with selected Monitor

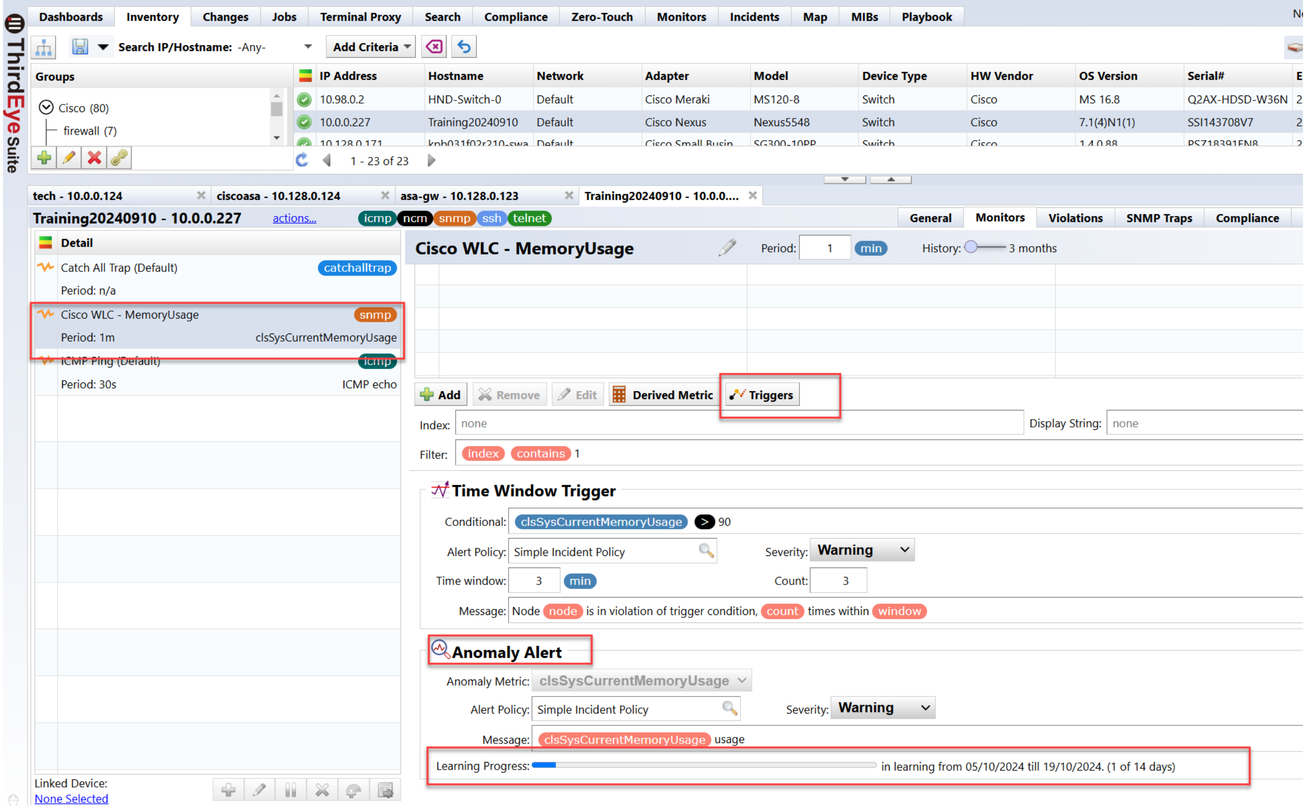
IP Address	Hostname	Network
10.0.0.10		Default
10.0.0.34		Default
10.0.0.126	tech126222	Default
10.0.0.128	tech12888	Default
10.0.0.153	test.intra.lvi.co.jp	Default
10.0.0.222	tech-15.intra.lvi.c...	Default
10.0.0.225	A10vThunder	Default
10.0.0.249	Device1	Default
10.0.2.243	apresia2142	Default
10.0.2.244		Default
10.0.3.1		Default
10.0.3.12	public	Default
10.0.40.121	simulator.intra.lv...	Default
10.0.96.1		Default

1 - 58 of 58 Results per page: 500

5. Add in your message

6. 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.



Search IP/Hostname: -Any-

IP Address	Hostname	Network	Adapter	Model	Device Type	HW Vendor	OS Version	Serial#
10.98.0.2	HND-Switch-0	Default	Cisco Meraki	MS120-8	Switch	Cisco	MS 16.8	Q2AX-HDSD-W36N
10.0.0.227	Training20240910	Default	Cisco Nexus	Nexus5548	Switch	Cisco	7.1(4)N1(1)	SSI143708V7
10.128.0.171	knb031f02r210-swa	Default	Cisco Small Busin	SG300-10PP	Switch	Cisco	1.4.0.88	PSZ18391FN8

Training20240910 - 10.0.0.227

Catch All Trap (Default) catchalltrap
Period: n/a

Cisco WLC - MemoryUsage snmp
Period: 1m clsSysCurrentMemoryUsage

ICMP Ping (Default) icmp
Period: 30s ICMP echo

Cisco WLC - MemoryUsage

Period: 1 min History: 3 months

Index: none Display String: none

Filter: index contains 1

Time Window Trigger

Conditional: clsSysCurrentMemoryUsage > 90

Alert Policy: Simple Incident Policy Severity: Warning

Time window: 3 min Count: 3

Message: Node node is in violation of trigger condition, count times within window

Anomaly Alert

Anomaly Metric: clsSysCurrentMemoryUsage

Alert Policy: Simple Incident Policy Severity: Warning

Message: clsSysCurrentMemoryUsage usage

Learning Progress: in learning from 05/10/2024 till 19/10/2024. (1 of 14 days)

SECTION 23

DRAFT CONFIGURATIONS

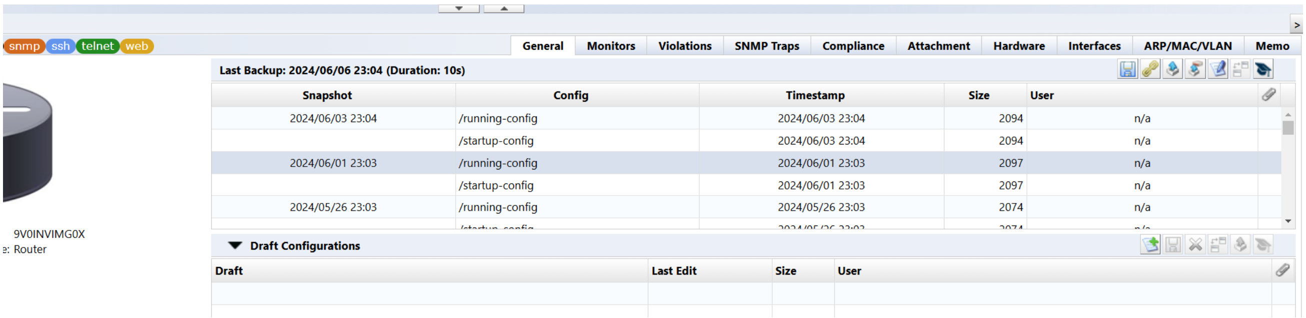
Suite

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.

23.1 Create 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 ✎ button.



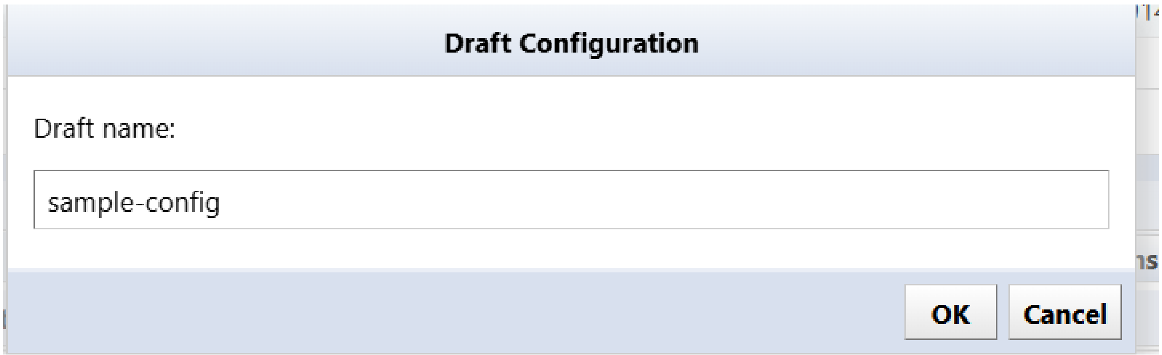
Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a

Draft Configurations

Draft	Last Edit	Size	User

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

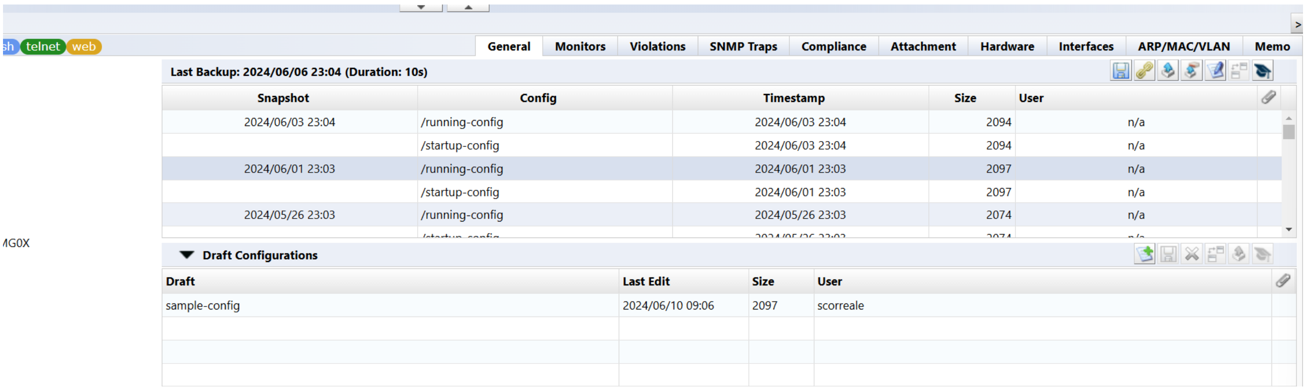


Draft Configuration

Draft name:

sample-config

4. Doubleclick the created draft configuration.



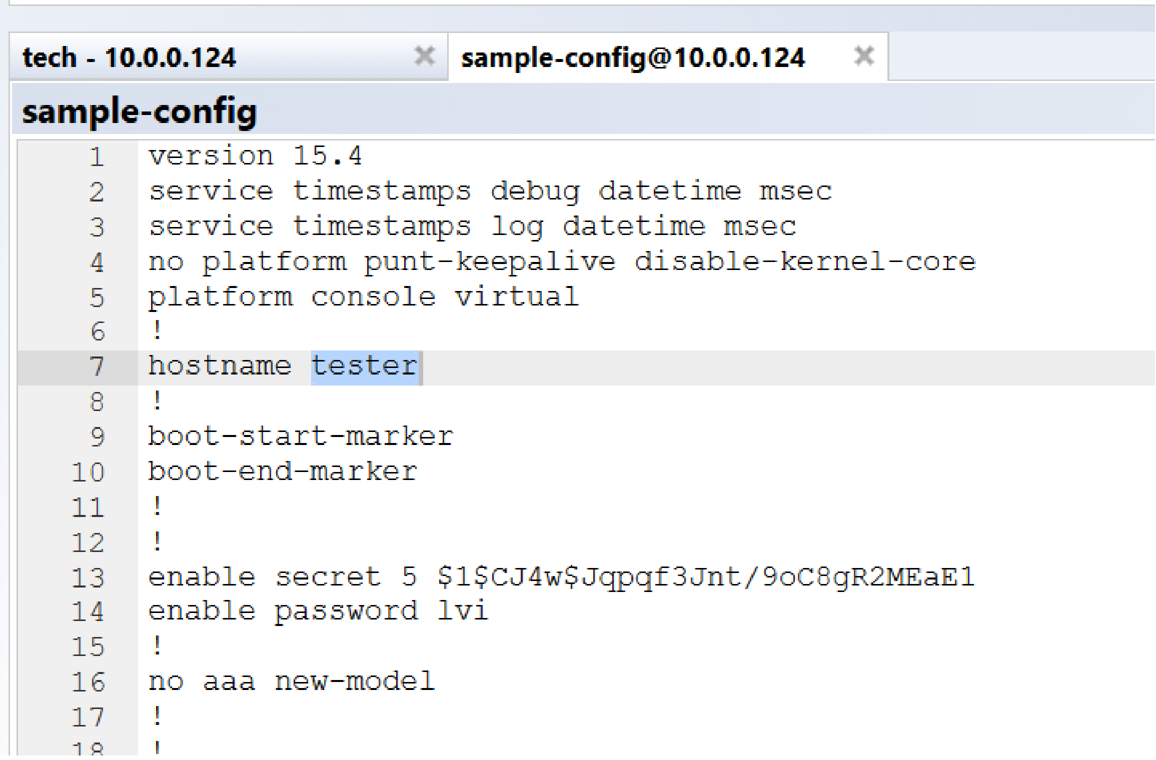
Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a
	/startup-config	2024/05/26 23:03	2074	n/a

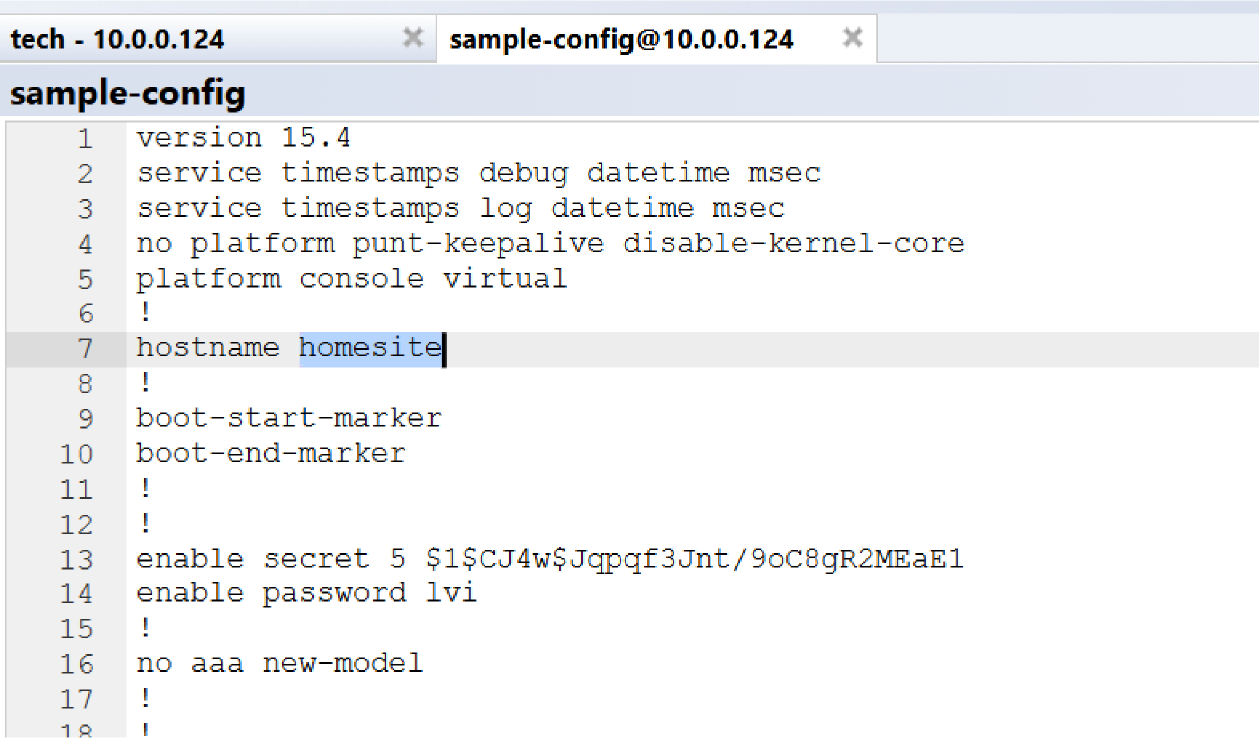
Draft Configurations

Draft	Last Edit	Size	User
sample-config	2024/06/10 09:06	2097	scorreale

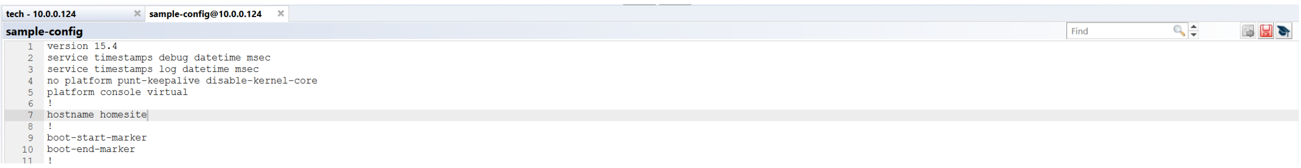
5. Edit the configuration and click the 💾 button to save.



```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname tester
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$CJ4w$Jqpqf3Jnt/9oC8gR2MEaE1
enable password lvi
!
no aaa new-model
!
!
```



```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname homesite
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$CJ4w$Jqpqf3Jnt/9oC8gR2MEaE1
enable password lvi
!
no aaa new-model
!
!
```

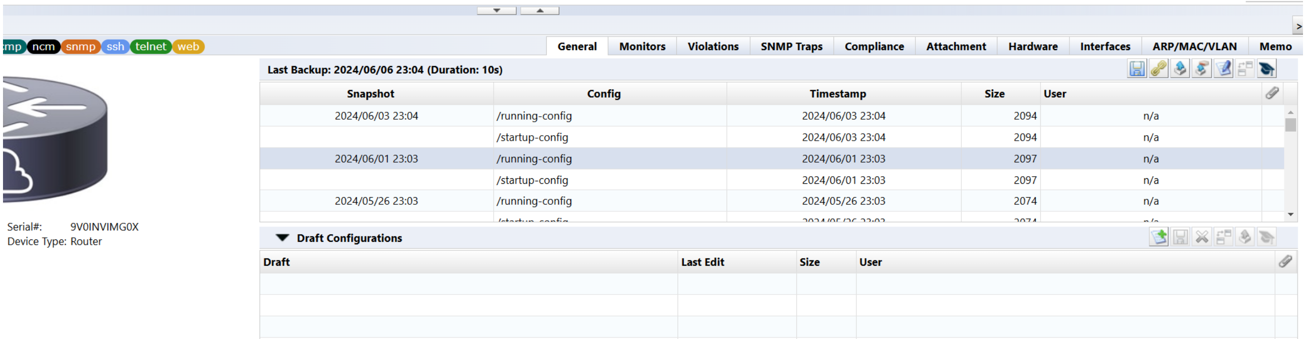


```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname homesite
!
boot-start-marker
boot-end-marker
!
```

23.2 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 backup status panel, click the button.



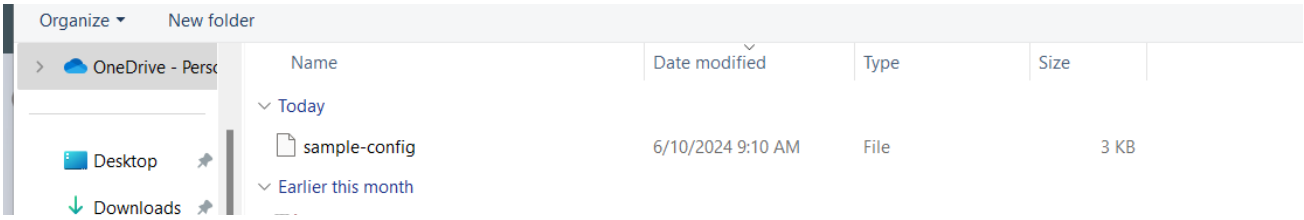
Serial#: 9V0INVIMG0X
Device Type: Router

Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a

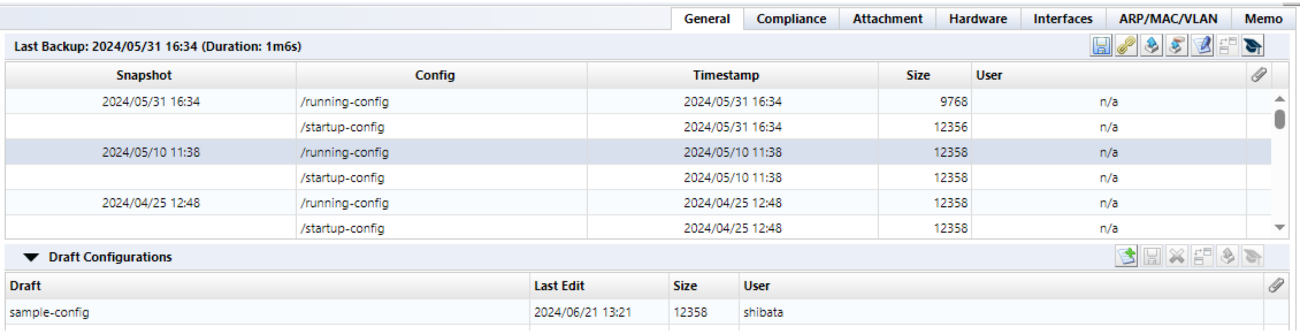
Draft	Last Edit	Size	User

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



Name	Date modified	Type	Size
Today			
sample-config	6/10/2024 9:10 AM	File	3 KB
Earlier this month			

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



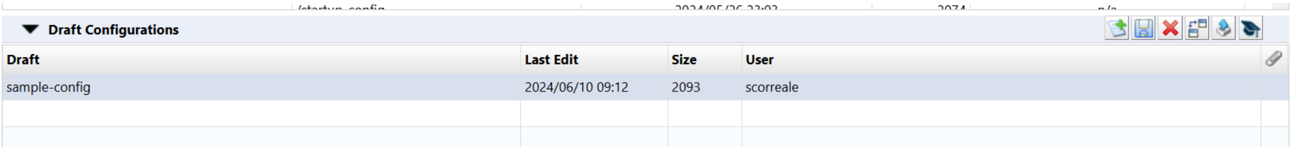
Last Backup: 2024/05/31 16:34 (Duration: 1m6s)

Snapshot	Config	Timestamp	Size	User
2024/05/31 16:34	/running-config	2024/05/31 16:34	9768	n/a
	/startup-config	2024/05/31 16:34	12356	n/a
2024/05/10 11:38	/running-config	2024/05/10 11:38	12358	n/a
	/startup-config	2024/05/10 11:38	12358	n/a
2024/04/25 12:48	/running-config	2024/04/25 12:48	12358	n/a
	/startup-config	2024/04/25 12:48	12358	n/a

Draft	Last Edit	Size	User
sample-config	2024/06/21 13:21	12358	shibata

23.3 Apply Draft Configuration

Applying drafts can be done using the same procedure as applying (restoring) backup configurations. However, you must select the draft configuration to upload, then click the button.

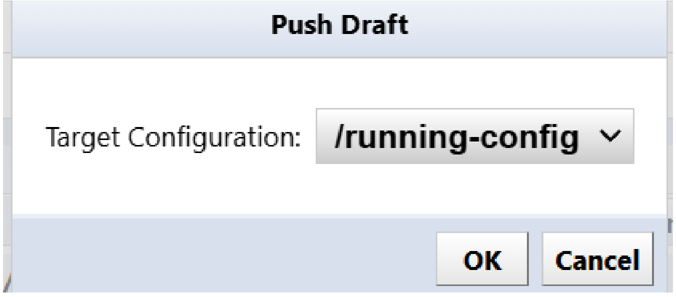


Draft Configurations

Draft	Last Edit	Size	User
sample-config	2024/06/10 09:12	2093	scorreale

Next, select which draft configuration you would like to upload to.

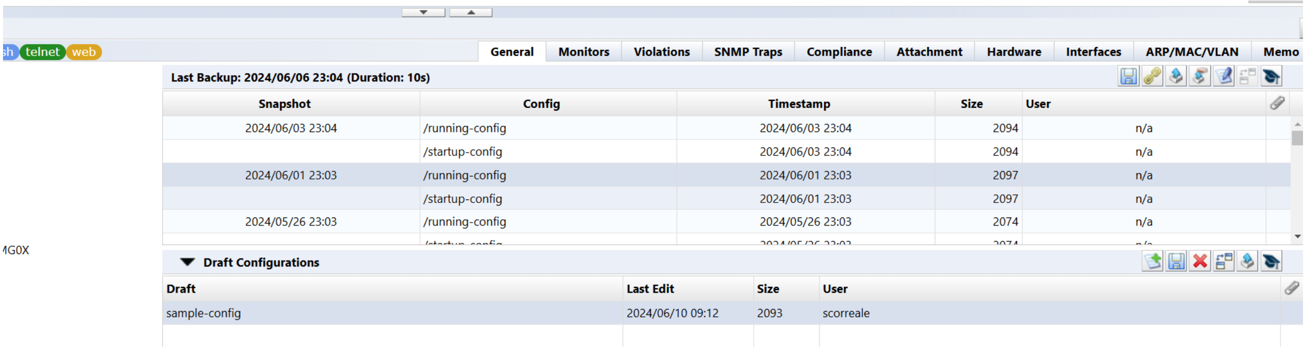
> **Note**
>
> This is different from history upload. When uploading history,running-config and startup-config will also be uploaded.



Push Draft

Target Configuration: /running-config

Click [OK] to start uploading.



Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a

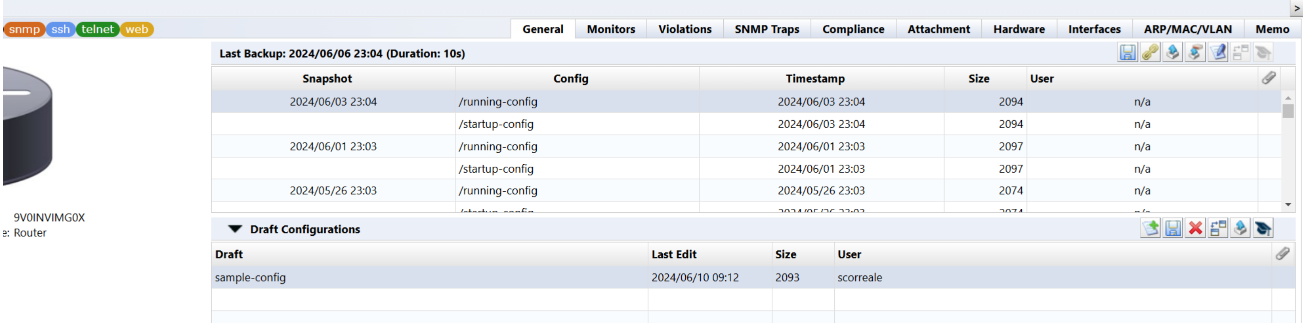
Draft Configurations

Draft	Last Edit	Size	User
sample-config	2024/06/10 09:12	2093	scorreale

23.4 Compare Draft Configurations

To compare draft configurations, click the button.

You can use the same comparison functions in draft configurations as in regular configurations.



Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a

Draft Configurations

Draft	Last Edit	Size	User
sample-config	2024/06/10 09:12	2093	scorreale

23.5 Export Draft Configuration

To export a draft configuration, click the button.

23.6 Delete Draft Configuration

To delete a draft configuration, click the the button.

SECTION 24

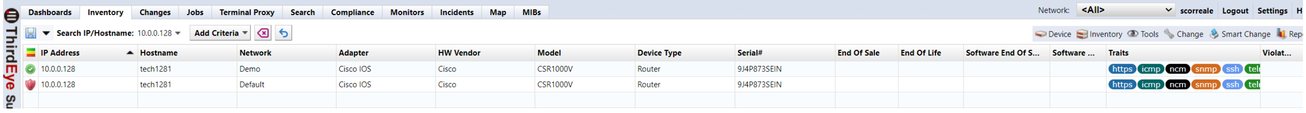
CONFIGURATION BACKUP

ThirdEye allows you to use the functionality of the **Net LineDancer** config management tool.

In ThirdEye, obtaining the device configuration is called a "**Configuration Backup**". For configuration backup, ThirdEye connects to the device via SSH or Telnet and retrieves the configuration using show commands, TFTP commands, etc.

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 ***Credentials*** *section to make sure the credentials are set.*
- The model supports configuration backup by ThirdEye.
  For a list of supported devices, visit https://logicvein.com/supported-devices.
- The NCM (Network Configuration Management) function is enabled. The target of configuration backup is the device with `ncm` displayed in the trait column.



	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	Serial#	End Of Sale	End Of Life	Software End Of S...	Software ...	Traits	Violat...
✓	10.0.0.128	tech1281	Demo	Cisco IOS	Cisco	CSR1000V	Router	9J4P873SEIN					https icmp ncm snmp ssh tel	
🛡	10.0.0.128	tech1281	Default	Cisco IOS	Cisco	CSR1000V	Router	9J4P873SEIN					https icmp ncm snmp ssh tel	

24.1 NCM (Network Configuration Management)

The Network Configuration Management (NCM) in ThirdEye functions as a monitoring-centric tool that automatically tracks device configuration states as part of its network surveillance system. Implemented as an optional module, it focuses on preserving configuration integrity for already-deployed devices within monitored networks.

In ThirdEye, the NCM performs the following functions:

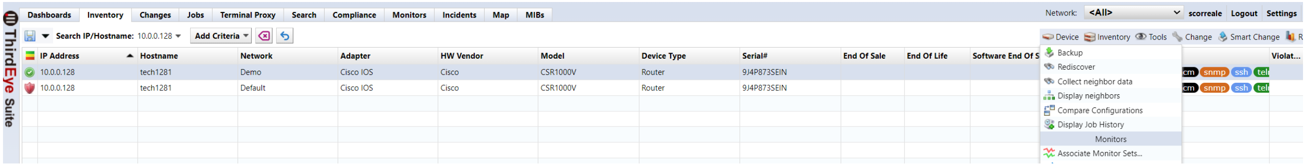
- Provides historical versioning of configurations
- Detects unauthorized changes through SNMP-triggered alerts
- Supports compliance checks against predefined baselines

To enable NCM functionality, click the target device in the [Inventory] main tab, and click [Enable NCM functionality] in the menu bar's [Device] menu.

24.2 Perform a Backup

1. Click the [Inventory] main tab.
2. Click the target device.
3. Click the [Device] menu.
4. Click [Backup].

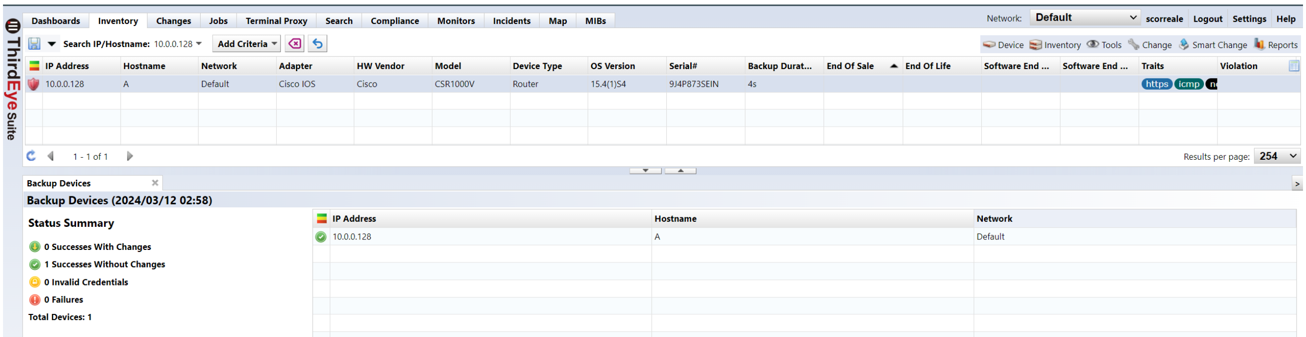
If no device is selected, execute for devices with NCM function is enabled.



Search IP/Hostname: 10.0.0.128

	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	Serial#	End Of Sale	End Of Life	Software End Of S		Violat...
✓	10.0.0.128	tech1281	Demo	Cisco IOS	Cisco	CSR1000V	Router	9J4P873SEIN				cm snmp ssh tel	
	10.0.0.128	tech1281	Default	Cisco IOS	Cisco	CSR1000V	Router	9J4P873SEIN				cm snmp ssh tel	

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



Search IP/Hostname: 10.0.0.128

	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
	10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	4s					https icmp n	

1 - 1 of 1

Results per page: 254

Backup Devices (2024/03/12 02:58)

Status Summary

- 0 Successes With Changes
- 1 Successes Without Changes
- 0 Invalid Credentials
- 0 Failures

Total Devices: 1

	IP Address	Hostname	Network
✓	10.0.0.128	A	Default

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.

24.3 Backup Status

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.

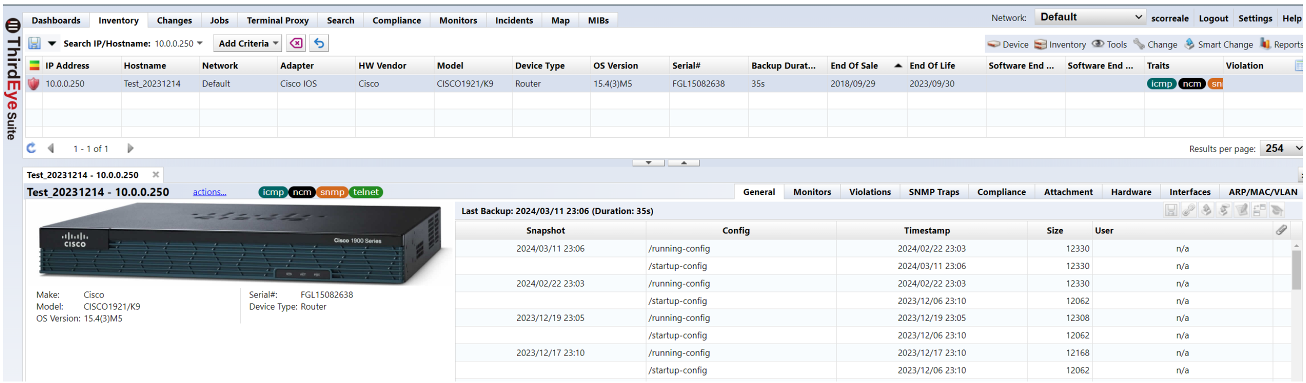
Icon	Status	Condition Description
✓	**Backup complete**	Configuration acquisition has completed successfully.
⚠	**Configuration mismatch**	There are differences between the device's running-config and startup-config. Doubleclick the icon to see the comparison results.
🔒	**Credential mismatch**	You cannot 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	Compliance Status Icon
High	**Emergency**	🔥	-	-
	Alert	▨	-	-
	Backup failure	-	❗	-
	Critical	⊗	-	-
	Credential mismatch	-	🔒	-
	Config mismatch	-	⚠	-
Priority	**Compliance error**	-	-	🛡
	Error	❗	-	-
	Compliance warning	-	-	🛡
	Warning	❗	-	-
	Notify	ⓘ	-	-
	Backup not executed	-	❓	-
	Information	ⓘ	-	-
Low	**Debug**	●	-	-

24.4 Acquired Configuration

You can check the acquired configuration from the device details screen.



Search IP/Hostname: 10.0.0.250

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.250	Test_20231214	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	35s	2018/09/29	2023/09/30			icmp ncm sn	

Test_20231214 - 10.0.0.250

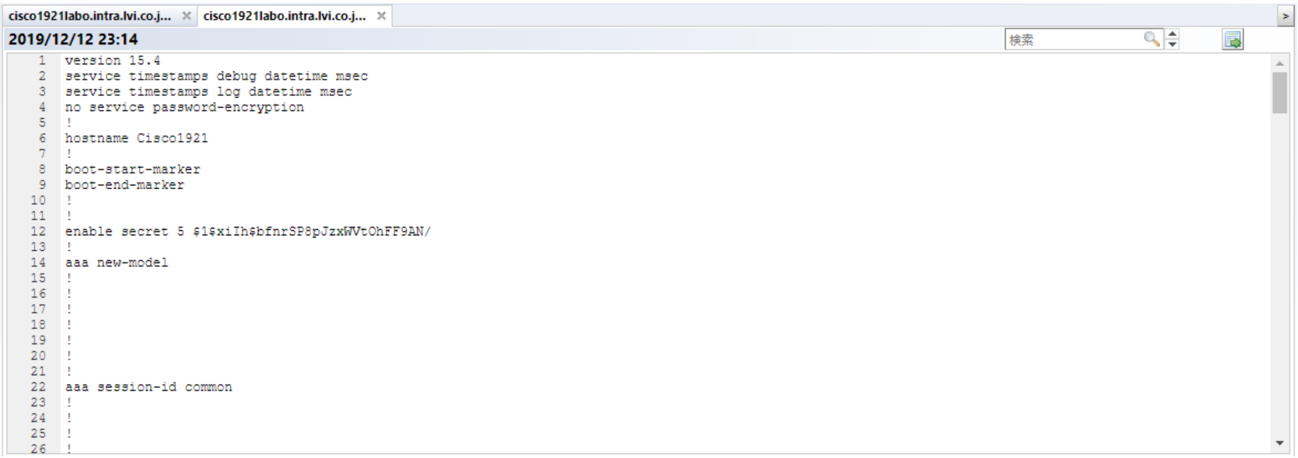
Make: Cisco
Model: CISCO1921/K9
OS Version: 15.4(3)M5

Serial#: FGL15082638
Device Type: Router

Last Backup: 2024/03/11 23:06 (Duration: 35s)

Snapshot	Config	Timestamp	Size	User
2024/03/11 23:06	/running-config	2024/02/22 23:03	12330	n/a
	/startup-config	2024/03/11 23:06	12330	n/a
2024/02/22 23:03	/running-config	2024/02/22 23:03	12330	n/a
	/startup-config	2023/12/06 23:10	12062	n/a
2023/12/19 23:05	/running-config	2023/12/19 23:05	12308	n/a
	/startup-config	2023/12/06 23:10	12062	n/a
2023/12/17 23:10	/running-config	2023/12/17 23:10	12168	n/a
	/startup-config	2023/12/06 23:10	12062	n/a

You can check the contents by double-clicking on the [Config] button.


cisco1921labo.intra.lvi.co.j...
cisco1921labo.intra.lvi.co.j...
検索

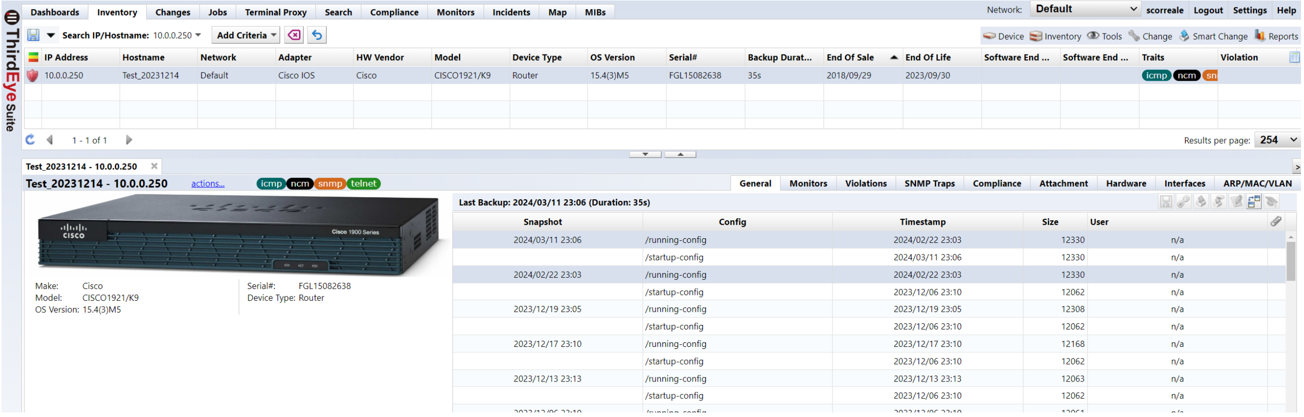
2019/12/12 23:14

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco1921
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$xiIh$bfnrSP8pJzxWVtOhFF9AN/
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
!
!
!
!
```

24.5 Compare Configurations

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.



Search IP/Hostname: 10.0.0.250

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.250	Test_20231214	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	35s	2018/09/29	2023/09/30			icmp ncm sn	

Test_20231214 - 10.0.0.250

Test_20231214 - 10.0.0.250 icmp ncm snmp telnet

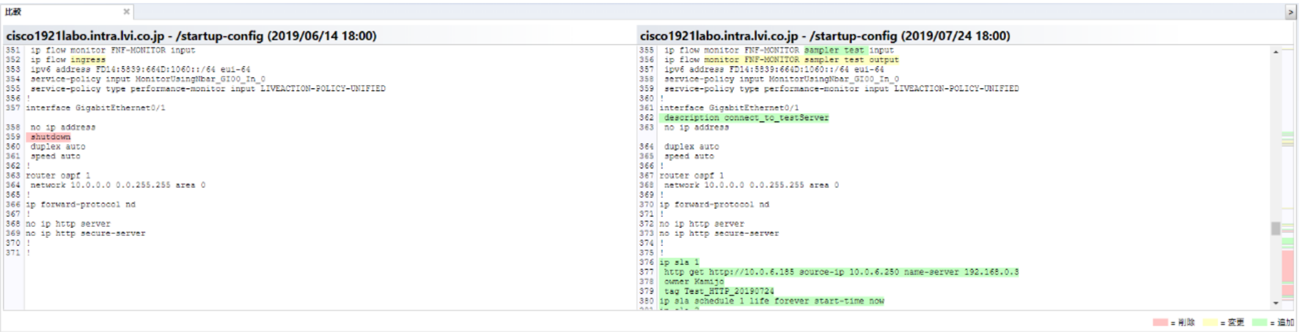
Make: Cisco
Model: CISCO1921/K9
OS Version: 15.4(3)M5

Serial#: FGL15082638
Device Type: Router

Last Backup: 2024/03/11 23:06 (Duration: 35s)

Snapshot	Config	Timestamp	Size	User
2024/03/11 23:06	/running-config	2024/02/22 23:03	12330	n/a
	/startup-config	2024/03/11 23:06	12330	n/a
2024/02/22 23:03	/running-config	2024/02/22 23:03	12330	n/a
	/startup-config	2023/12/06 23:10	12062	n/a
2023/12/19 23:05	/running-config	2023/12/19 23:05	12308	n/a
	/startup-config	2023/12/06 23:10	12062	n/a
2023/12/17 23:10	/running-config	2023/12/17 23:10	12168	n/a
	/startup-config	2023/12/06 23:10	12062	n/a
2023/12/13 23:13	/running-config	2023/12/13 23:13	12063	n/a
	/startup-config	2023/12/06 23:10	12062	n/a

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.



cisco1921labo.intra.lvi.co.jp - /startup-config (2019/06/14 18:00)

```
 ip flow monitor FNF-MONITOR input
 ip flow ingress
 ipv6 address FD14:5839:664D:1060::/64 eui-64
 service-policy input MonitorUsingNbar_GI00_In_0
 service-policy type performance-monitor input LIVEACTION-POLICY-UNIFIED
!
interface GigabitEthernet0/1

 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
```

cisco1921labo.intra.lvi.co.jp - /startup-config (2019/07/24 18:00)

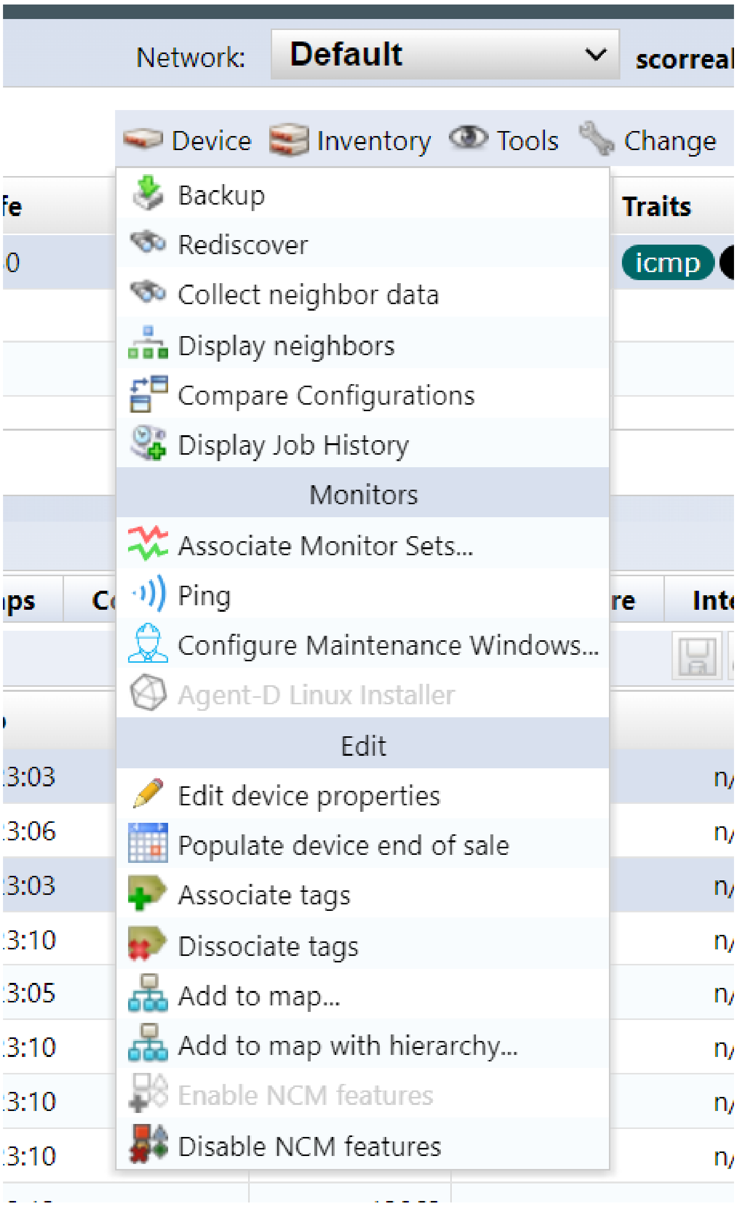
```
 ip flow monitor FNF-MONITOR sampler test input
 ip flow monitor FNF-MONITOR sampler test output
 ipv6 address FD14:5839:664D:1060::/64 eui-64
 service-policy input MonitorUsingNbar_GI00_In_0
 service-policy type performance-monitor input LIVEACTION-POLICY-UNIFIED
!
interface GigabitEthernet0/1
 description connect_to_testServer
 no ip address

 duplex auto
 speed auto
!
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip sla 1
 http get http://10.0.6.185 source-ip 10.0.6.250 name-server 192.168.0.8
 owner Kamijo
 tag Test_HTTP_20190724
ip sla schedule 1 life forever start-time now
```

24.6 Disable Configuration Backup

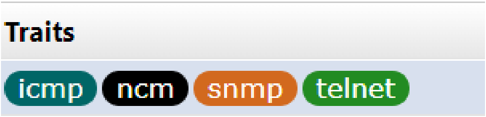
Even if the model supports configuration backup, if you do not want to acquire the configuration, you can exclude it from the backup target by disabling the NCM function.

To disable NCM functionality.

1. Click the target device in the [Inventory] main tab.
2. Click [Disable NCM functionality] in the Menu Bar's [Device] menu.

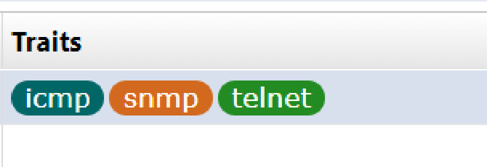


Disabling the NCM feature will remove the “ncm” trait from the device’s properties, and “ncm” will no longer appear in the device’s traits.



Traits

icmp ncm snmp telnet



Traits

icmp snmp telnet

24.7 Enable Configuration Backup

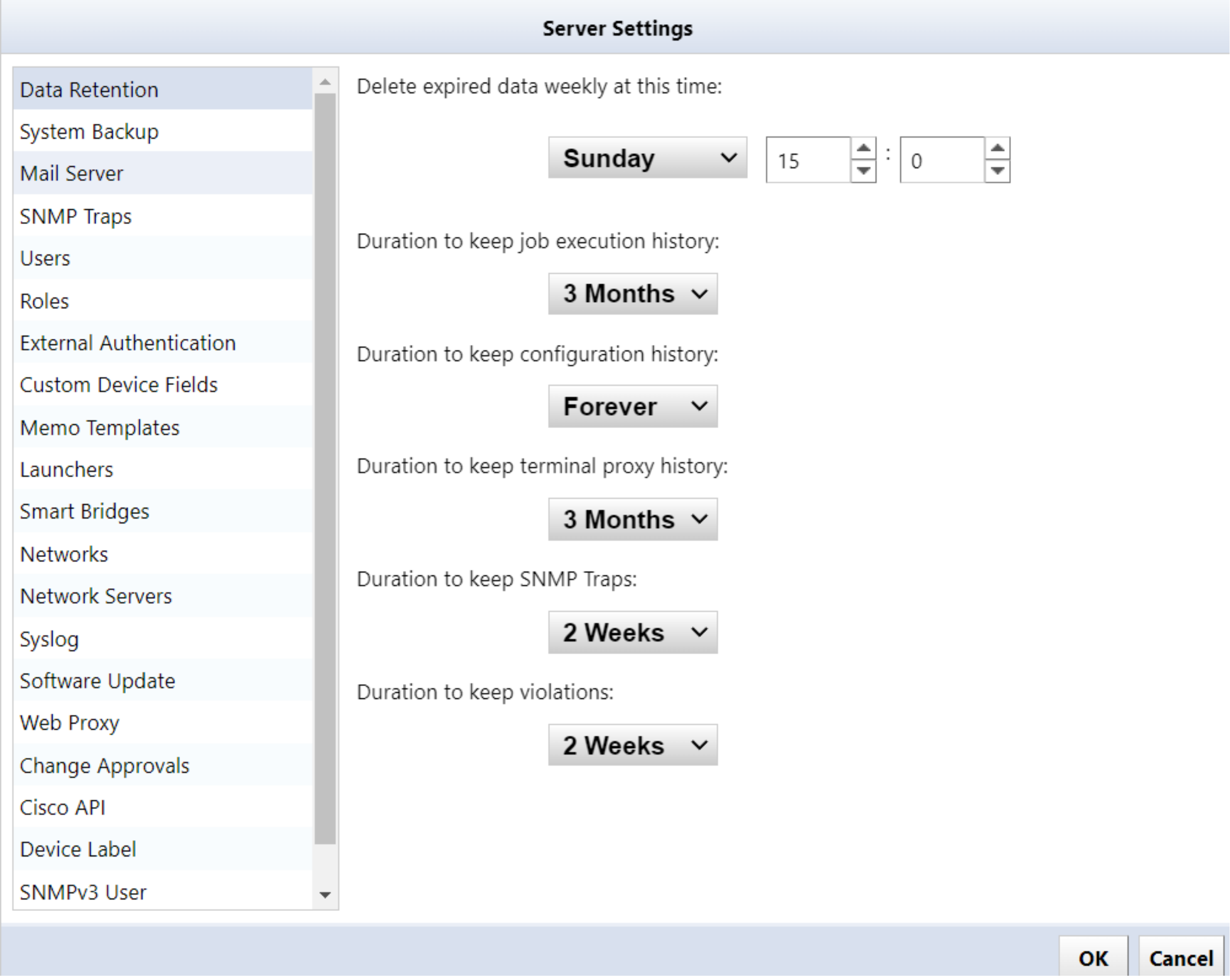
To enable the NCM function:

1. Select the target device.
2. Click [Enable NCM function] in the [Device] submenu.

Enabling the NCM feature will add the “ncm” trait to the device’s properties, and “ncm” will appear in the device’s traits.

24.8 Change Data Retention Period

Click [Data Retention] to set the data retention period and automatic deletion timing.



Delete expired data weekly at this time: Sunday 15 : 0

Duration to keep job execution history: 3 Months

Duration to keep configuration history: Forever

Duration to keep terminal proxy history: 3 Months

Duration to keep SNMP Traps: 2 Weeks

Duration to keep violations: 2 Weeks

Item	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)

Item	Explanation
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`
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: Forever) `Forever`, `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: Forever) `Forever`, `2 weeks`, `3 Months`, `6 Months`, `1 Year`

SECTION 25

RULES

Rules define specific configuration requirements that network devices must meet, such as security settings or operational parameters.

Rules are organized into **Rulesets** which group related checks (e.g., all authentication-related rules), and provide logical organization.

Multiple Rulesets are then combined into **Compliance Policies** which determine enforcement parameters that include target devices, violation severity levels.

This hierarchy allows policies to activate standardized rule groupings across network infrastructure.

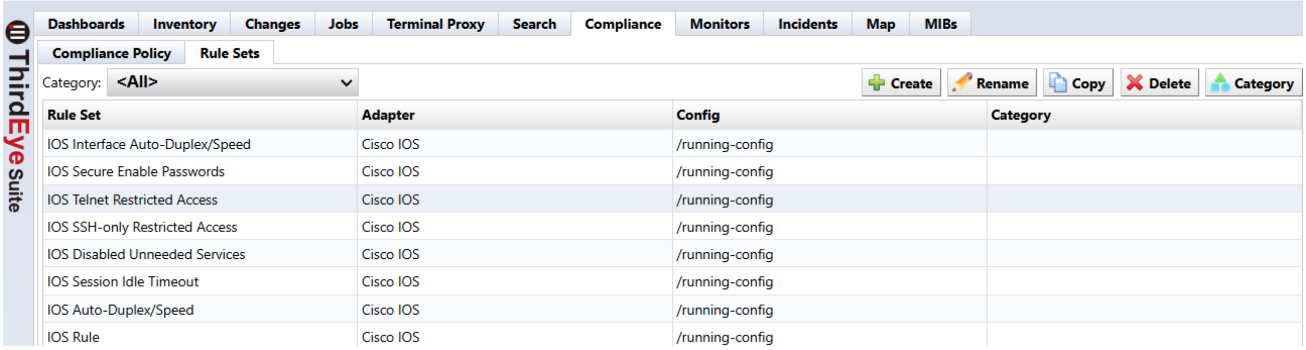
25.1 Create a Rule

In this section we will explain how to create a new rule with screenshots. The examples below will generate a violation when the SNMP community setting is "public" in the Cisco IOS device configuration.

1. Click the [Compliance] main tab.

2. Click the [Rule Sets] subtab.

3. Click the [Create] button.

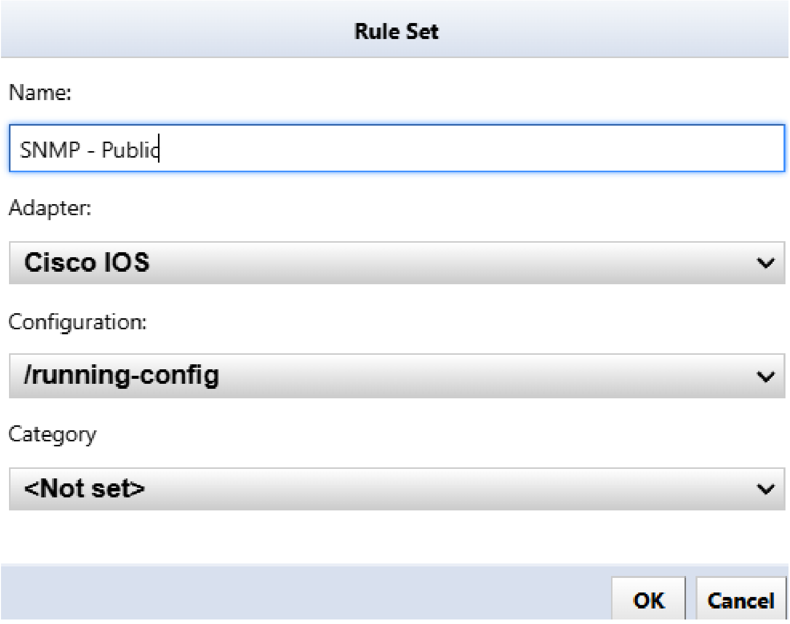


Category: <All>

Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Rule	Cisco IOS	/running-config	

4. Enter the name of the rule, and configure the target Adapter (model classification), Configuration, and Category.

5. Click [OK].



Rule Set

Name: SNMP - Public

Adapter: Cisco IOS

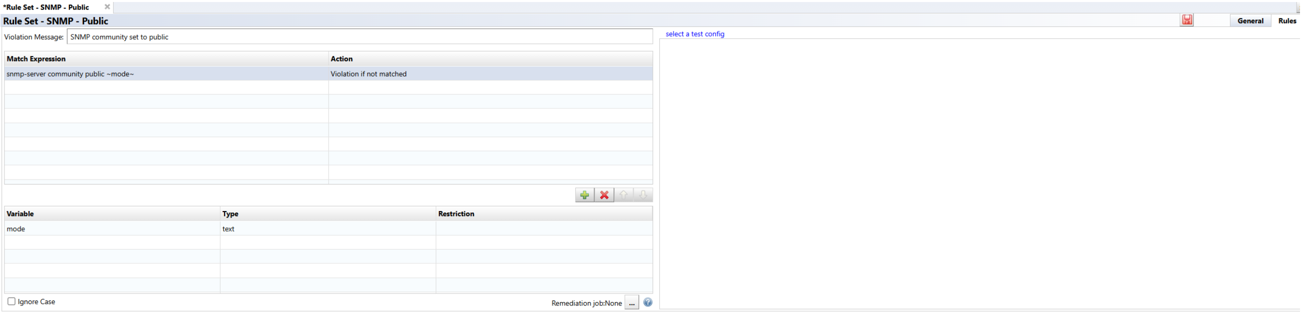
Configuration: /running-config

Category <Not set>

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

7. Click the ✚ button.

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



Rule Set - SNMP - Public

Violation Message: SNMP community set to public

Match Expression	Action
snmp-server community public ~mode~	Violation if not matched

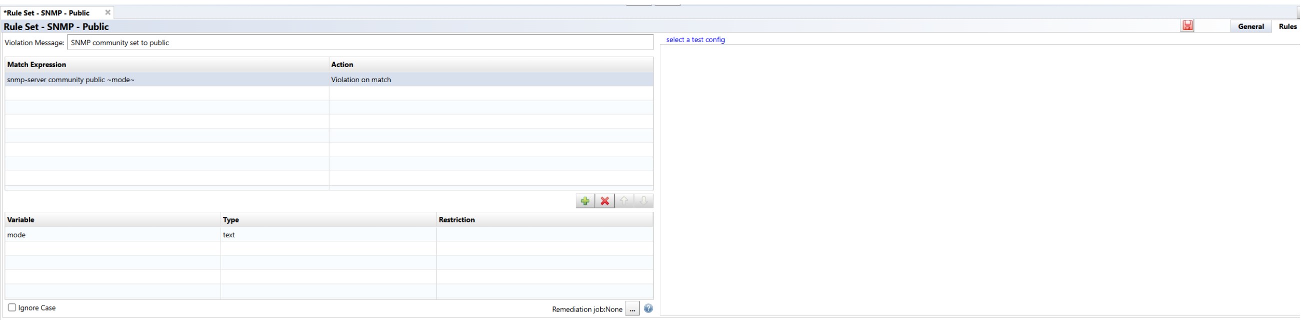
Variable	Type	Restriction
mode	text	

□ Ignore Case

Remediation job:None

8. In the [Match Expression] column, enter the text that is a violation.

9. In the [Action] column select [Violate on match].



Rule Set - SNMP - Public

Violation Message: SNMP community set to public

Match Expression	Action
snmp-server community public ~mode~	Violation on match

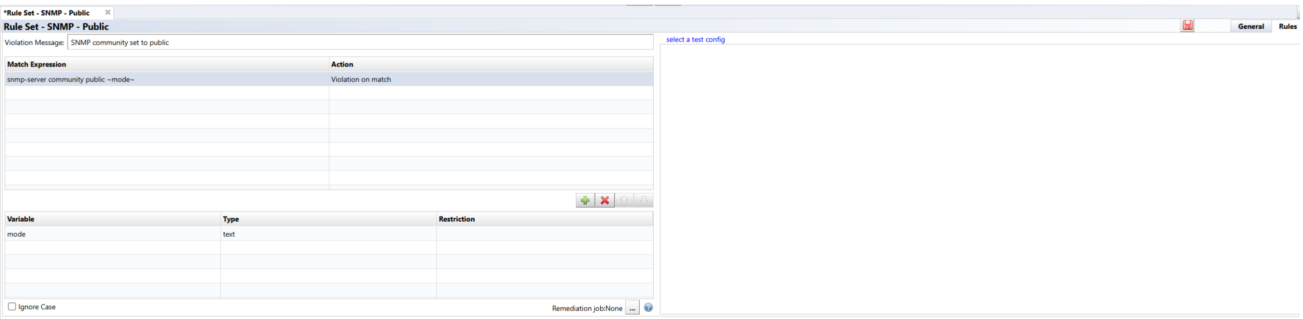
Variable	Type	Restriction
mode	text	

□ Ignore Case

Remediation job:None

If you want to test the rule you created:

10. Click [Select a configuration] in the upper right to test and select a configuration from your inventory.



Rule Set - SNMP - Public

Violation Message: SNMP community set to public

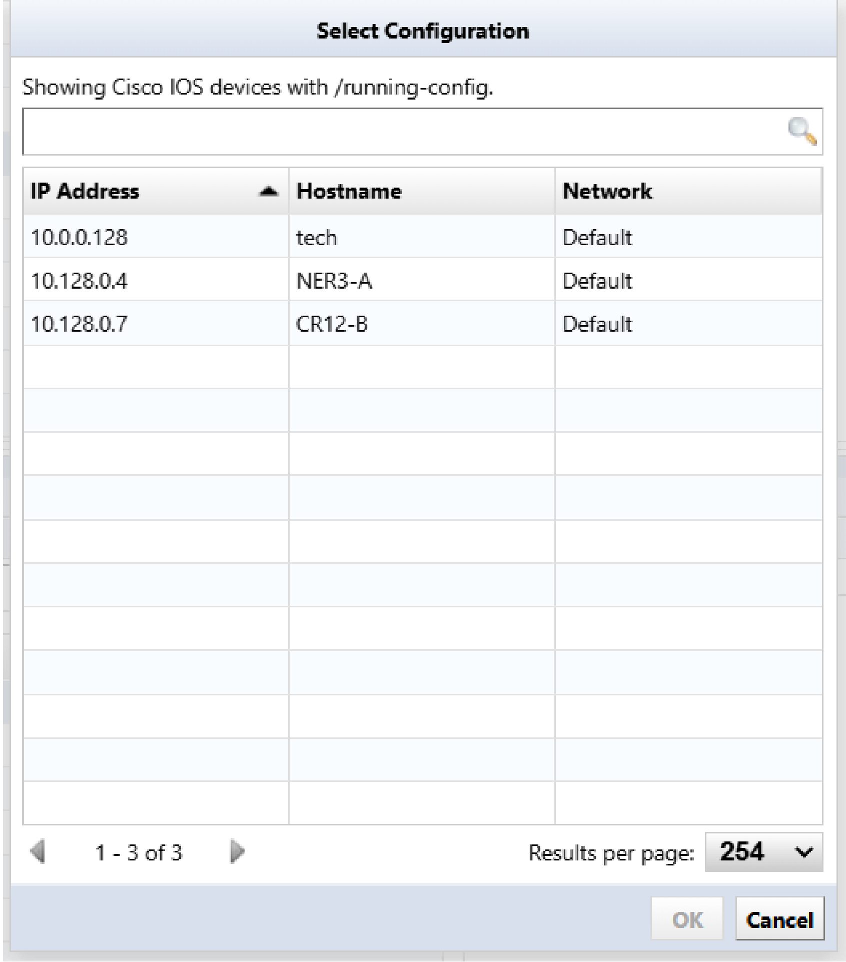
Match Expression	Action
snmp-server community public ~mode~	Violation on match

Variable	Type	Restriction
mode	text	

□ Ignore Case

Remediation job:None

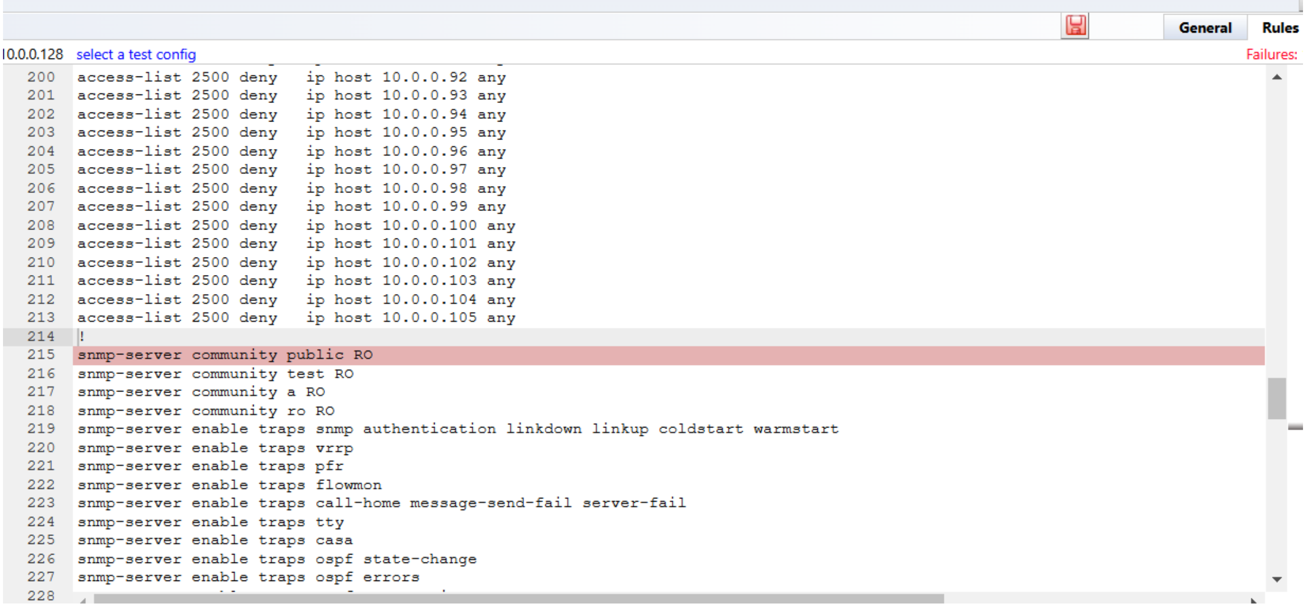
The configuration selection window displays a list of devices that apply to the adapter you selected when creating the rule. This column only displays devices that match the IOS adapter you originally selected.



Showing Cisco IOS devices with /running-config.

IP Address	Hostname	Network
10.0.0.128	tech	Default
10.128.0.4	NER3-A	Default
10.128.0.7	CR12-B	Default

Violations will be searched for against this text rule. If violations are found, they will be displayed in red.



```
access-list 2500 deny   ip host 10.0.0.92 any
access-list 2500 deny   ip host 10.0.0.93 any
access-list 2500 deny   ip host 10.0.0.94 any
access-list 2500 deny   ip host 10.0.0.95 any
access-list 2500 deny   ip host 10.0.0.96 any
access-list 2500 deny   ip host 10.0.0.97 any
access-list 2500 deny   ip host 10.0.0.98 any
access-list 2500 deny   ip host 10.0.0.99 any
access-list 2500 deny   ip host 10.0.0.100 any
access-list 2500 deny   ip host 10.0.0.101 any
access-list 2500 deny   ip host 10.0.0.102 any
access-list 2500 deny   ip host 10.0.0.103 any
access-list 2500 deny   ip host 10.0.0.104 any
access-list 2500 deny   ip host 10.0.0.105 any
!
snmp-server community public RO
snmp-server community test RO
snmp-server community a RO
snmp-server community ro RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
```

25.2 Compliance Policies

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 device compliance 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.

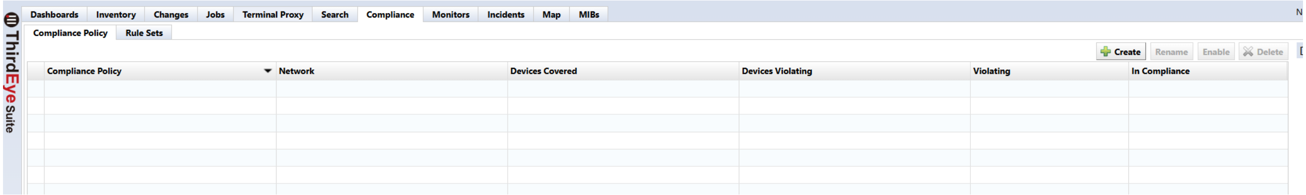
25.3 Create Compliance Policy

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

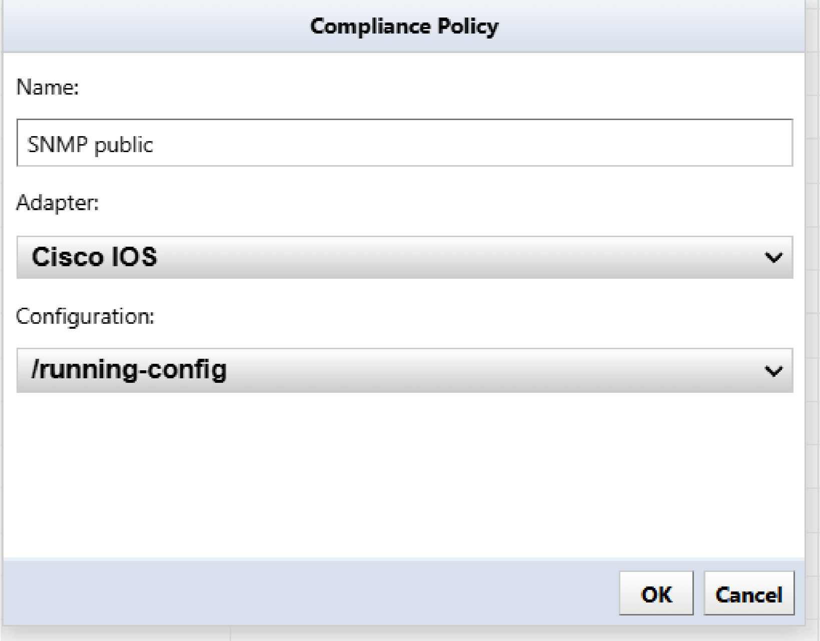
1. Click the [Compliance] main tab.

2. Click the [Compliance Policy] subtab.

3. Click the [Create] button.



4. Enter the policy "Name", "Adapter" target , and "Configuration" type, then click [OK].

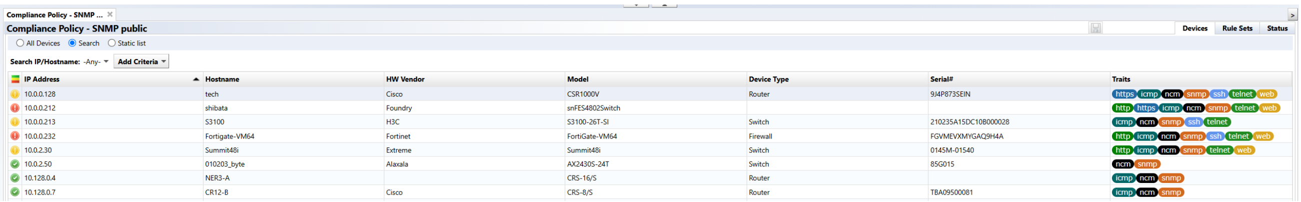


Name: SNMP public

Adapter: Cisco IOS

Configuration: /running-config

In this example, “Search” is selected in the Editor window’s [Devices] tab.



Compliance Policy - SNMP public

○ All Devices ● Search ○ Static list

Search IP/Hostname: -Any-

	IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
⚠	10.0.0.128	tech	Cisco	CSR1000V	Router	9J4P873SEIN	https icmp ncm snmp ssh telnet web
❗	10.0.0.212	shibata	Foundry	snFES4802Switch			http https icmp ncm snmp telnet web
⚠	10.0.0.213	S3100	H3C	S3100-26T-SI	Switch	210235A15DC10B000028	icmp ncm snmp ssh telnet
❗	10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGVMEVXMYGAQ9H4A	http icmp ncm snmp ssh telnet web
⚠	10.0.2.30	Summit48i	Extreme	Summit48i	Switch	0145M-01540	http icmp ncm snmp telnet web
✓	10.0.2.50	010203_byte	Alaxala	AX2430S-24T	Switch	85G015	ncm snmp
✓	10.128.0.4	NER3-A		CRS-16/S	Router		icmp ncm snmp
✓	10.128.0.7	CR12-B	Cisco	CRS-8/S	Router	TBA09500081	icmp ncm snmp

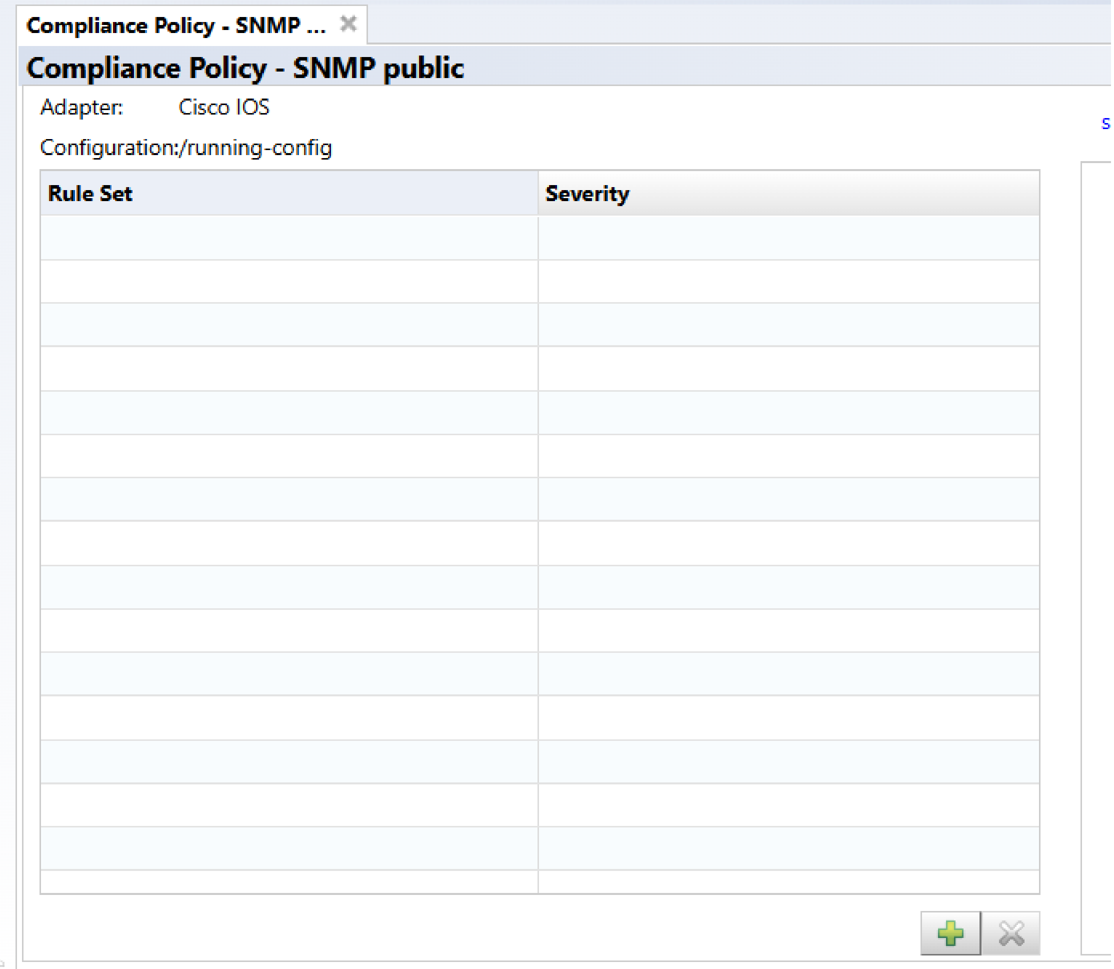
Note

The setting behavior for “Search” and “Static list” in the [Compliance] main tab > [Compliance Policy] subtab Editor window and the [Jobs] maintab > [Job Management] subtab Editor window is identical.

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

The search result is not saved when creating policy.

5. In the Editor window, click the [Rule Set] subtab.
6. Click the ✚ button.



Compliance Policy - SNMP public

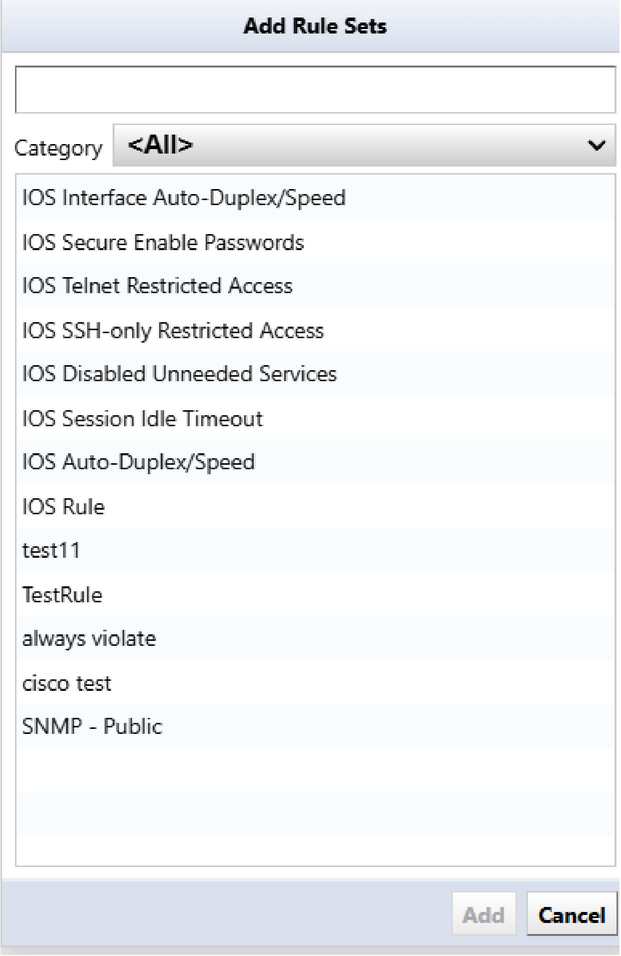
Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity

7. Select a Rule Set and click [Add].

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

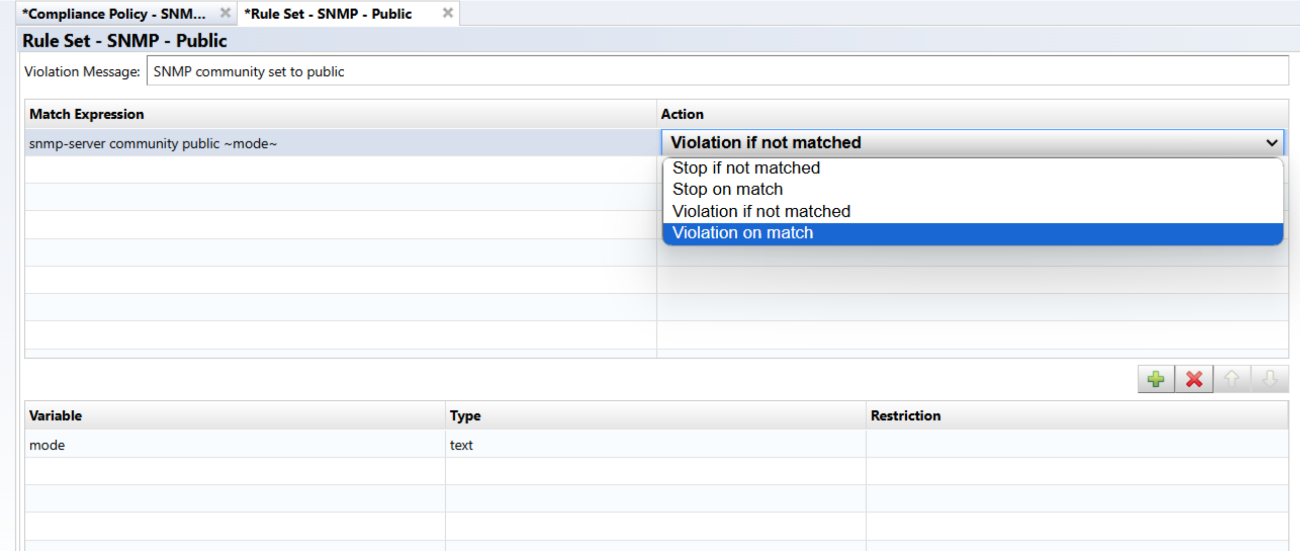


Add Rule Sets
Category
<All>
IOS Interface Auto-Duplex/Speed
IOS Secure Enable Passwords
IOS Telnet Restricted Access
IOS SSH-only Restricted Access
IOS Disabled Unneeded Services
IOS Session Idle Timeout
IOS Auto-Duplex/Speed
IOS Rule
test11
TestRule
always violate
cisco test
SNMP - Public
Add
Cancel

8. 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.



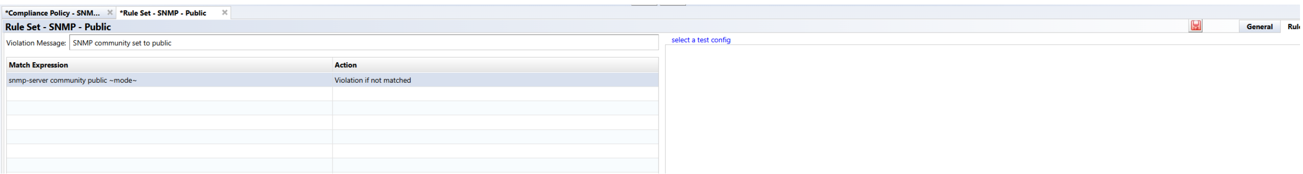
Rule Set - SNMP - Public

Violation Message: SNMP community set to public

Match Expression	Action
snmp-server community public ~mode~	Violation if not matched

Variable	Type	Restriction
mode	text	

9. Save the policy.



Rule Set - SNMP - Public

Violation Message: SNMP community set to public

Match Expression	Action
snmp-server community public ~mode~	Violation if not matched

Note

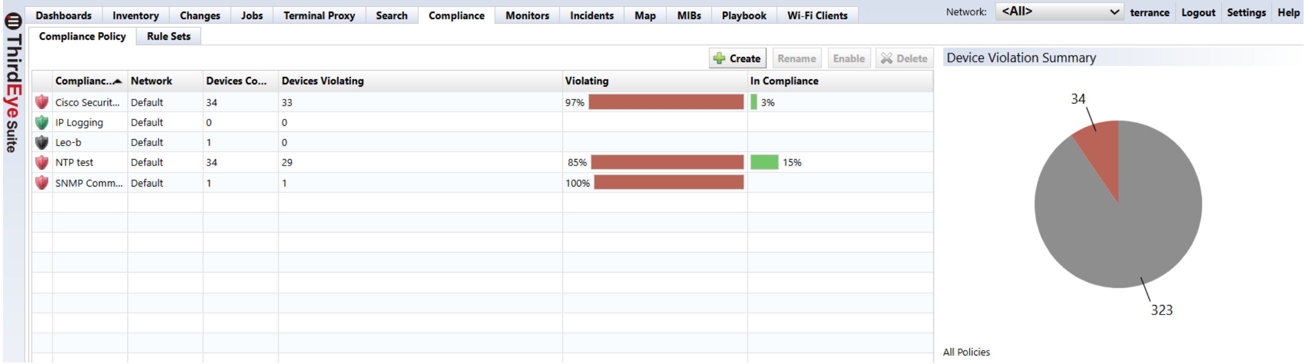
Activate the policy after saving. Simply creating a policy does not check for violations.

25.4 Applying a Compliance Policy

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

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

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

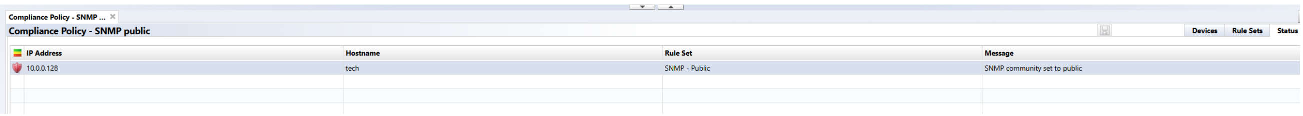


Complianc...	Network	Devices Co...	Devices Violating	Violating	In Compliance
Cisco Securit...	Default	34	33	97%	3%
IP Logging	Default	0	0		
Leo-b	Default	1	0		
NTP test	Default	34	29	85%	15%
SNMP Comm...	Default	1	1	100%	

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.

For more information about severity icons, refer to the **Perform a Backup** and **Backup Status** sections.

Doubleclick the changed icon to open the Editor, and view more details about the violation.



IP Address	Hostname	Rule Set	Message
10.0.0.128	tech	SNMP - Public	SNMP community set to public

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

25.5 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.

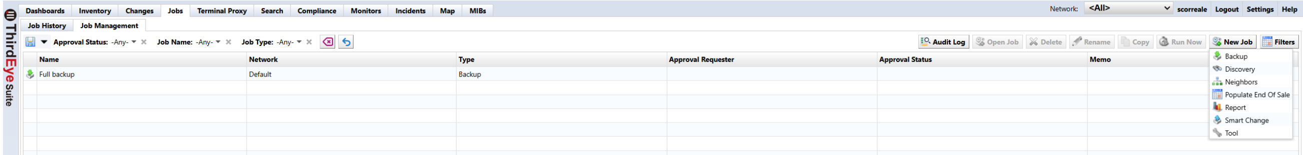
Setting Process

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.

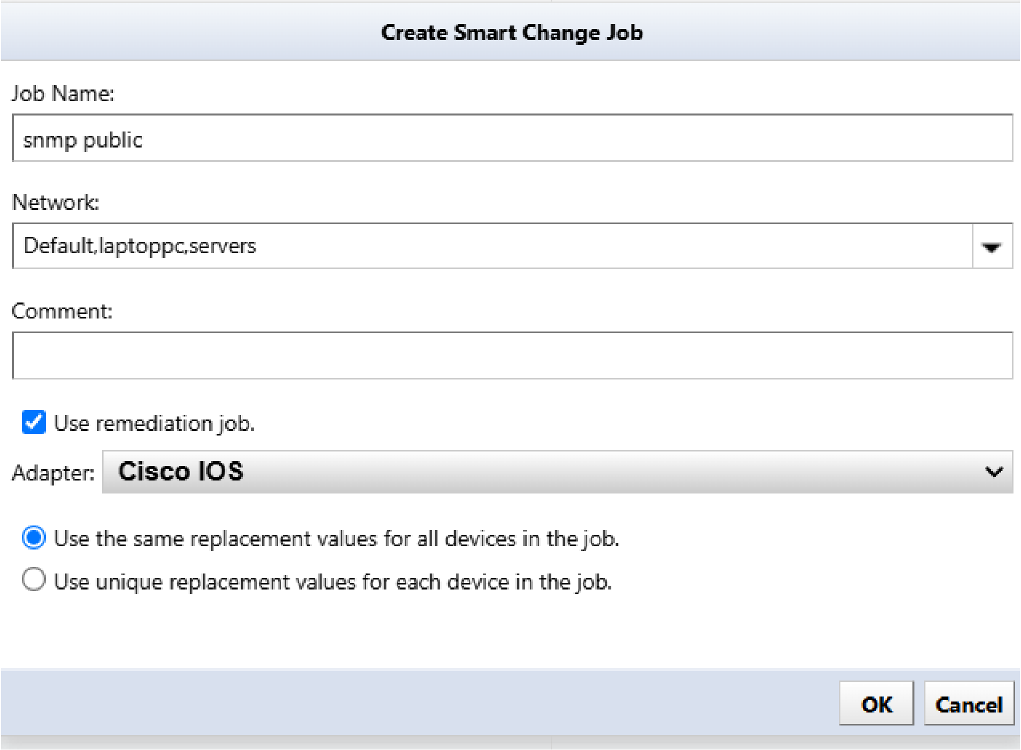
25.5.1 Case 1: When the use of Read-Write authority is prohibited in the SNMP community settings

1. Click the [Jobs] main tab > [Job Management] subtab.
2. Click [New Job] > [Smart Change].



Name	Network	Type	Approval Requester	Approval Status	Memo
Full backup	Default	Backup			

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



Create Smart Change Job

Job Name: snmp public

Network: Default,laptoppc,servers

Comment:

☑ Use remediation job.

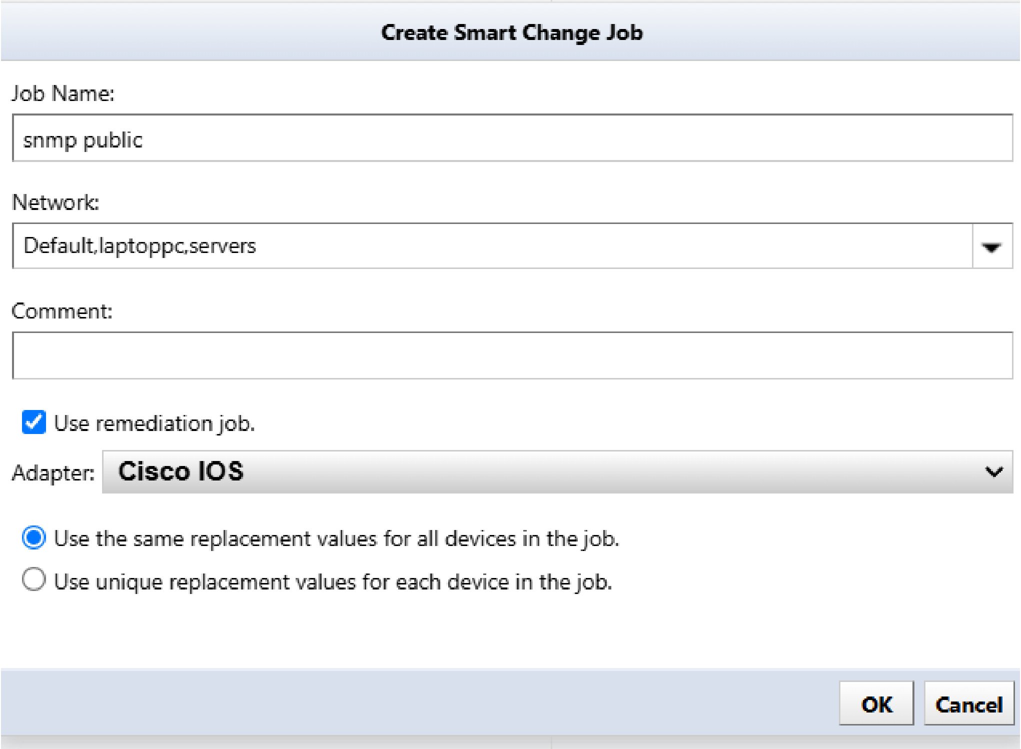
Adapter: Cisco IOS

● Use the same replacement values for all devices in the job.

○ Use unique replacement values for each device in the job.

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

This is used for linking with Rule Sets.



Create Smart Change Job

Job Name: snmp public

Network: Default,laptoppc,servers

Comment:

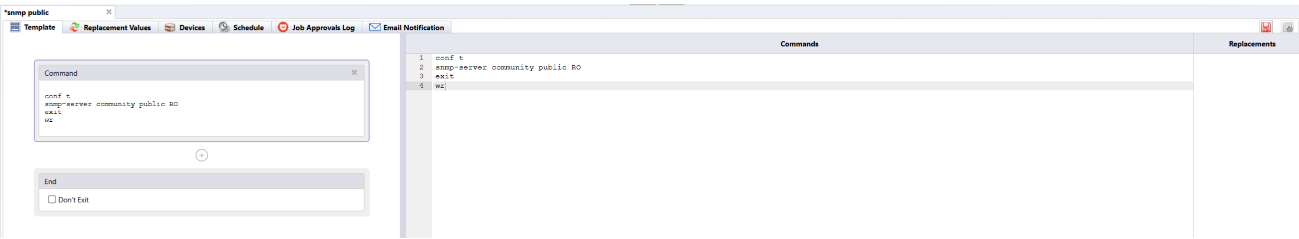
☑ Use remediation job.

Adapter: Cisco IOS

● Use the same replacement values for all devices in the job.

○ Use unique replacement values for each device in the job.

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



```
conf t
snmp-server community public RO
exit
wr
```

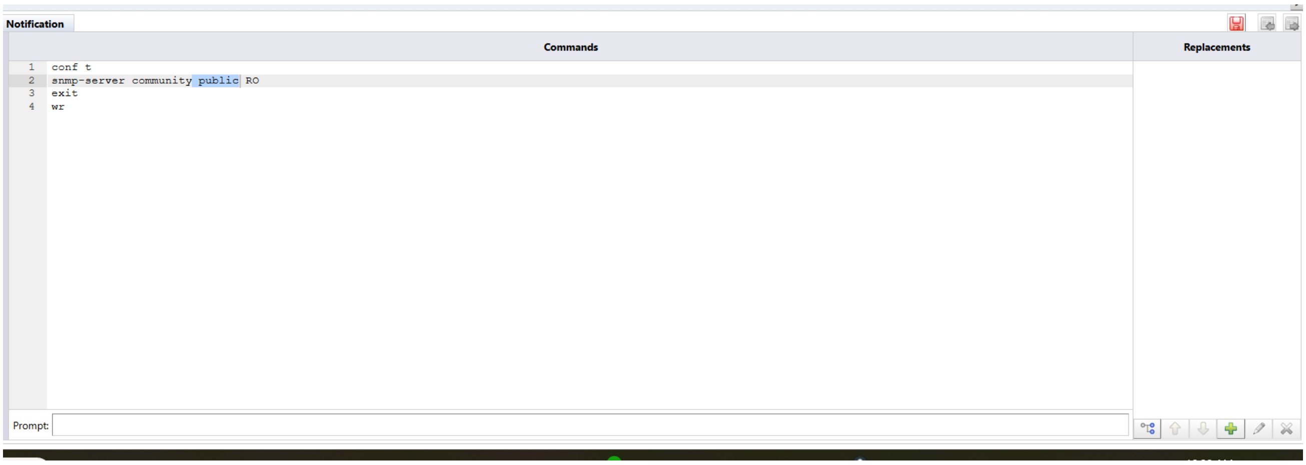
□ Don't Exit

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

Note

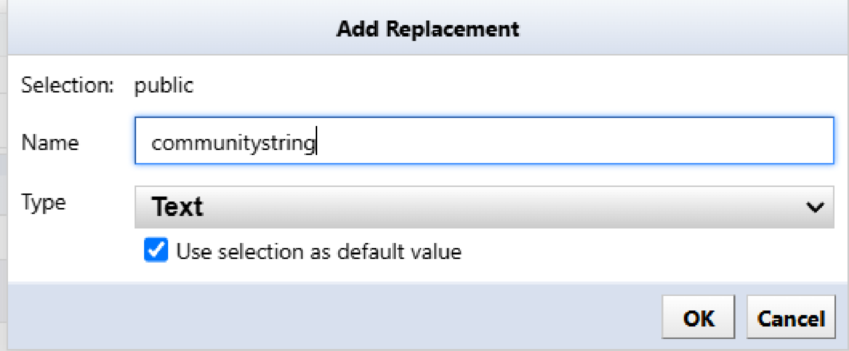
Skip this step if you want to execute the command as is without converting it to a variable.

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



```
conf t
snmp-server community public RO
exit
wr
```

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



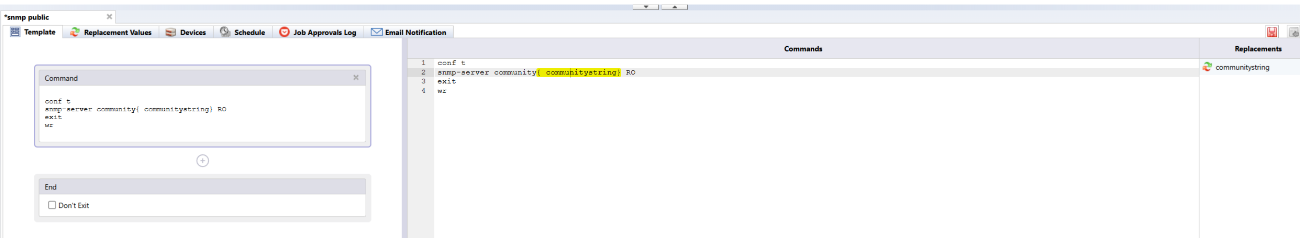
Selection: public

Name: communitystring

Type: Text

☑ Use selection as default value

8. Save the settings.

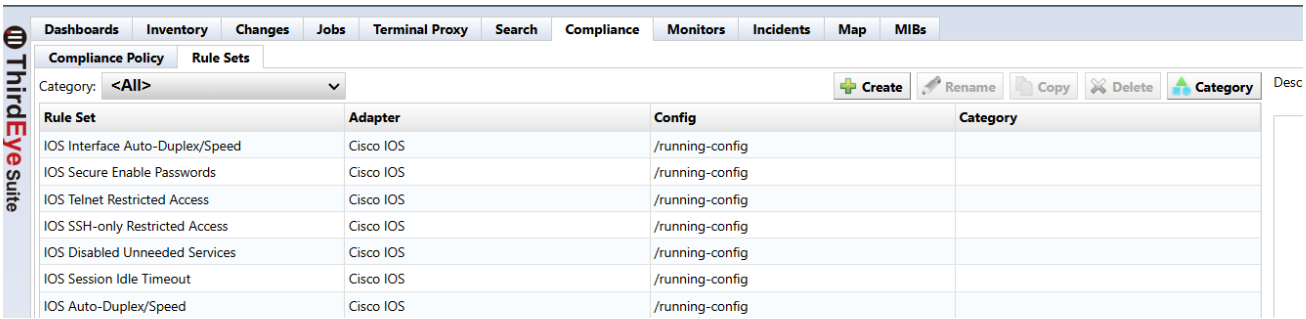


```
conf t
snmp-server community{ communitystring} RO
exit
wr
```

☐ Don't Exit

Replacements: communitystring

9. Click the [Compliance] main tab > [Rule Sets] subtab, and click [Create].

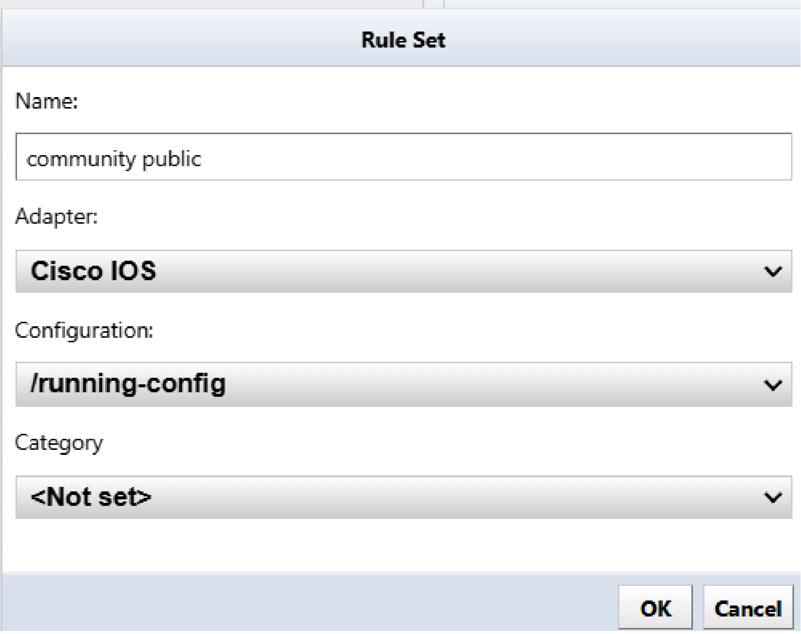


Category: <All>

Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	

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

Please select the adapter you selected when creating the Smart Change.



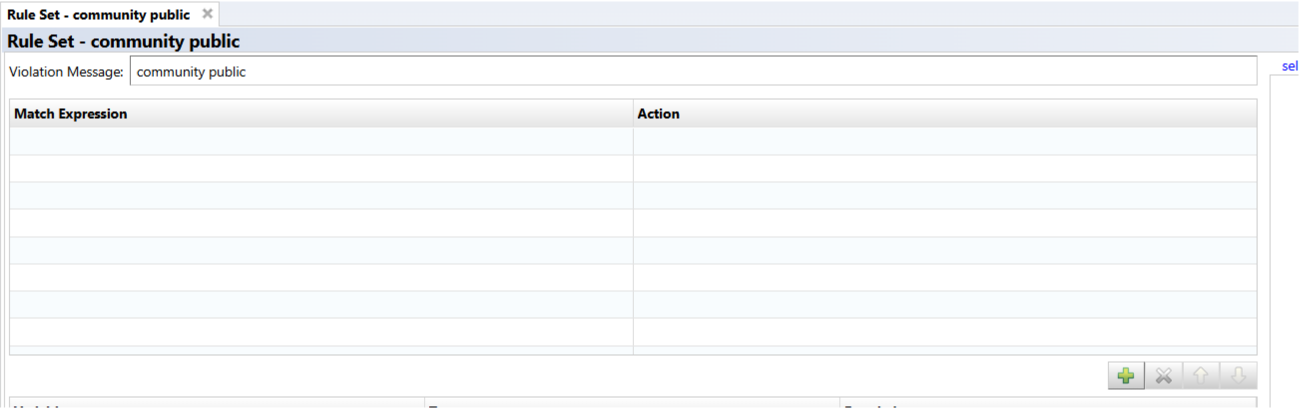
Name: community public

Adapter: Cisco IOS

Configuration: /running-config

Category <Not set>

11. Click the ✚ button to add "Match Expression".

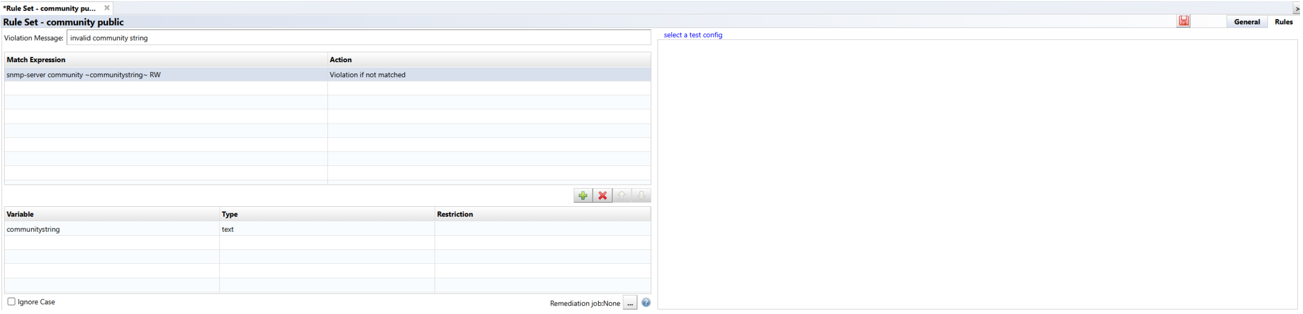

Rule Set - community public

Violation Message: community public

Match Expression	Action

12. In the "Variable" section in the bottom half of the page, specify the community name as the Smart Change Variable.

13. In the "Match Expression" section in the top half of the page, add ~ before and after the variable name.


*Rule Set - community pu...

Rule Set - community public

Violation Message: invalid community string

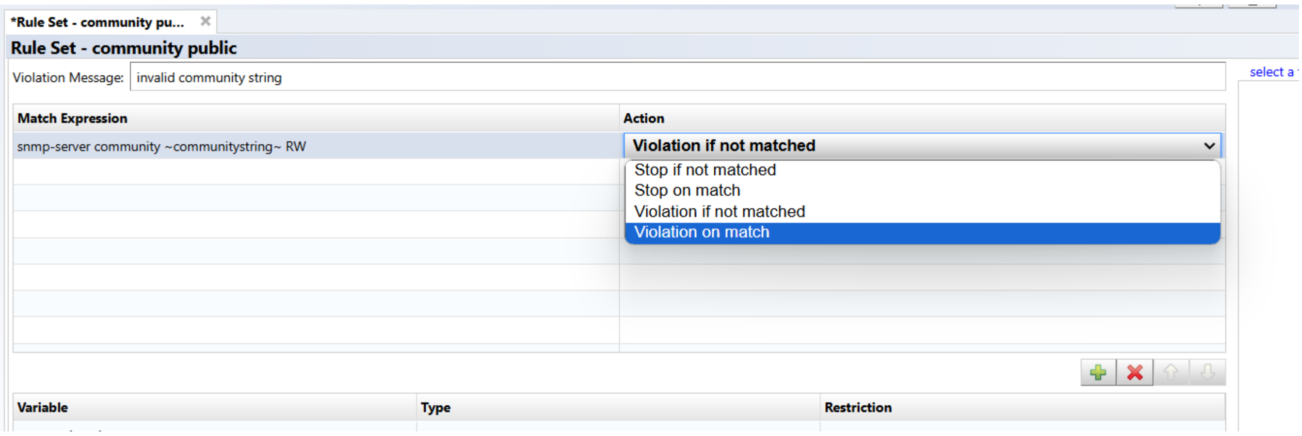
Match Expression	Action
snmp-server community ~communitystring~ RW	Violation if not matched

Variable	Type	Restriction
communitystring	text	

☐ Ignore Case

Remediation job:None

14. Set the Action to "Violation on match."

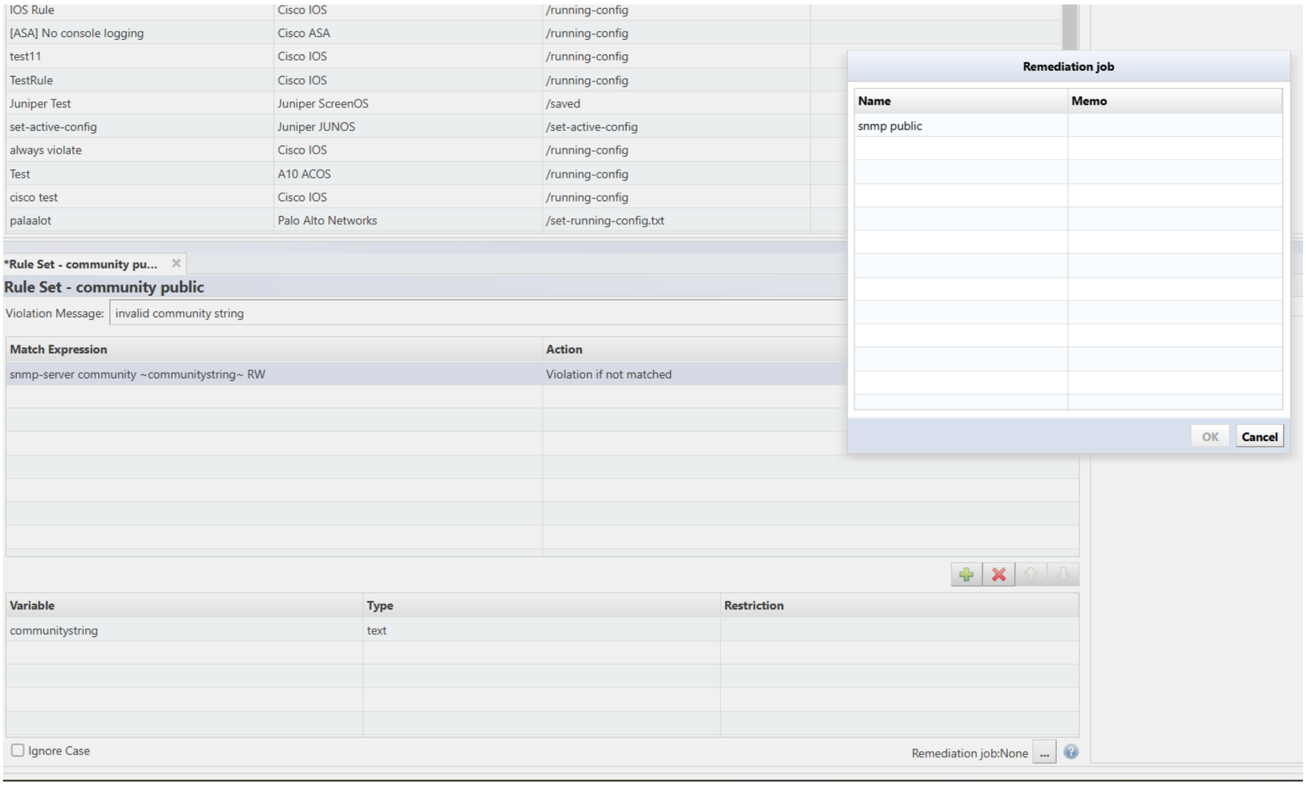

*Rule Set - community pu...

Rule Set - community public

Violation Message: invalid community string

Match Expression	Action
snmp-server community ~communitystring~ RW	Violation if not matched

15. 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.



IOS Rule	Cisco IOS	/running-config
[ASA] No console logging	Cisco ASA	/running-config
test11	Cisco IOS	/running-config
TestRule	Cisco IOS	/running-config
Juniper Test	Juniper ScreenOS	/saved
set-active-config	Juniper JUNOS	/set-active-config
always violate	Cisco IOS	/running-config
Test	A10 ACOS	/running-config
cisco test	Cisco IOS	/running-config
palaalot	Palo Alto Networks	/set-running-config.txt

*Rule Set - community pu...

Rule Set - community public

Violation Message: invalid community string

Match Expression	Action
snmp-server community ~communitystring~ RW	Violation if not matched

Variable	Type	Restriction
communitystring	text	

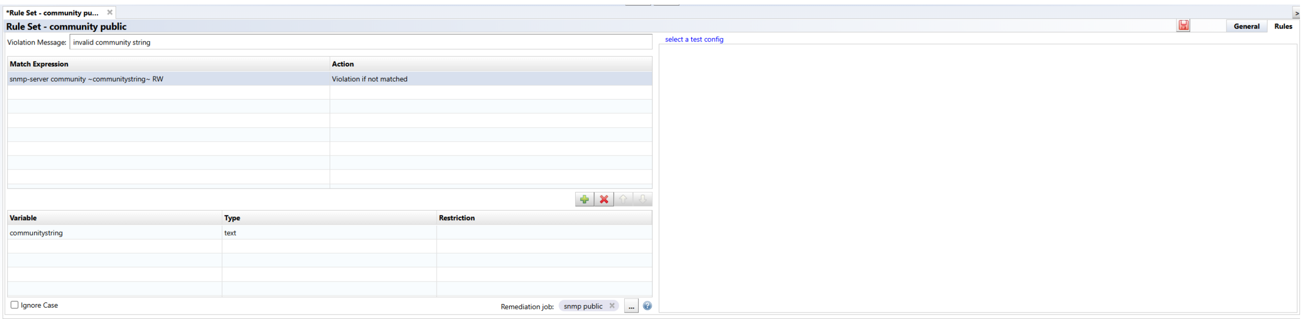
□ Ignore Case

Remediation job:None

Remediation job

Name	Memo
snmp public	

16. Save your settings.



*Rule Set - community pu...

Rule Set - community public

Violation Message: invalid community string

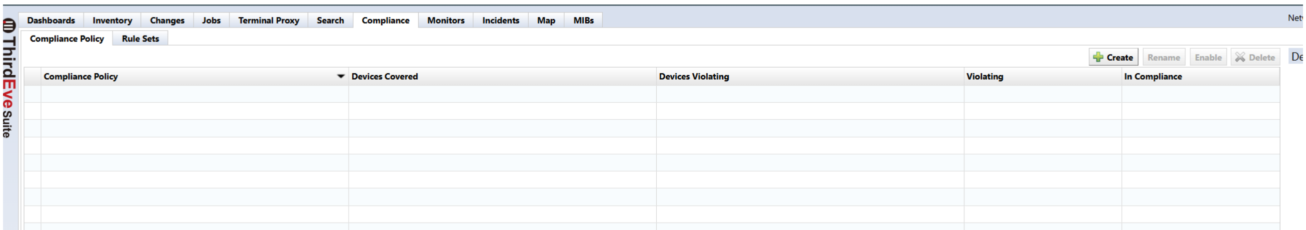
Match Expression	Action
snmp-server community ~communitystring~ RW	Violation if not matched

Variable	Type	Restriction
communitystring	text	

□ Ignore Case

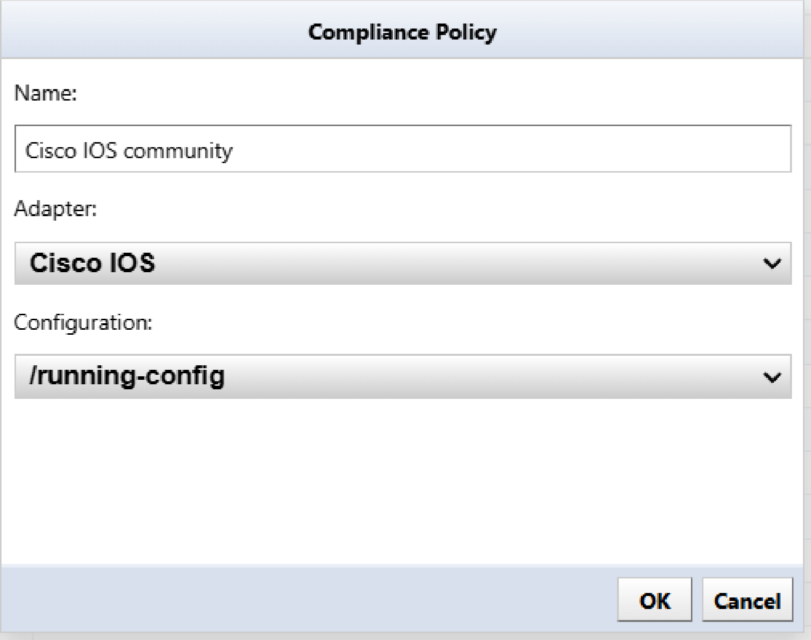
Remediation job: snmp public

17. Click the [Compliance] main tab > [Compliance Policy] subtab, and click [Create].



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance

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



Compliance Policy

Name:

Cisco IOS community

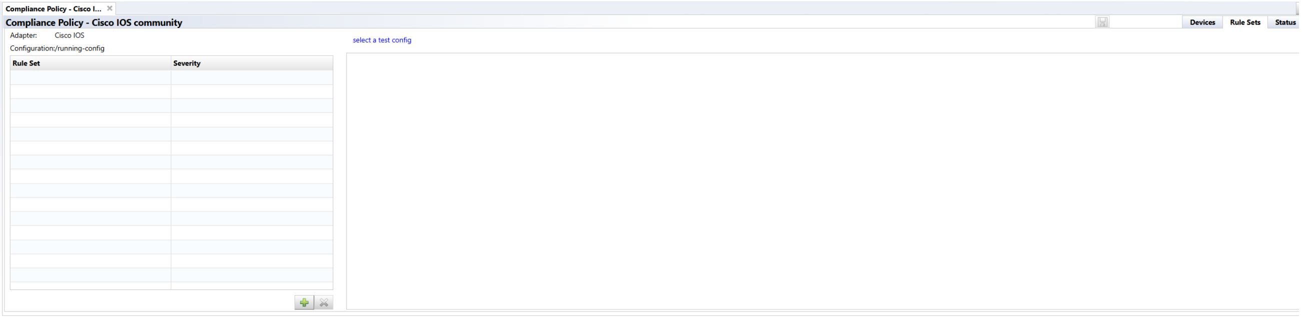
Adapter:

Cisco IOS

Configuration:

/running-config

19. Click the + button.



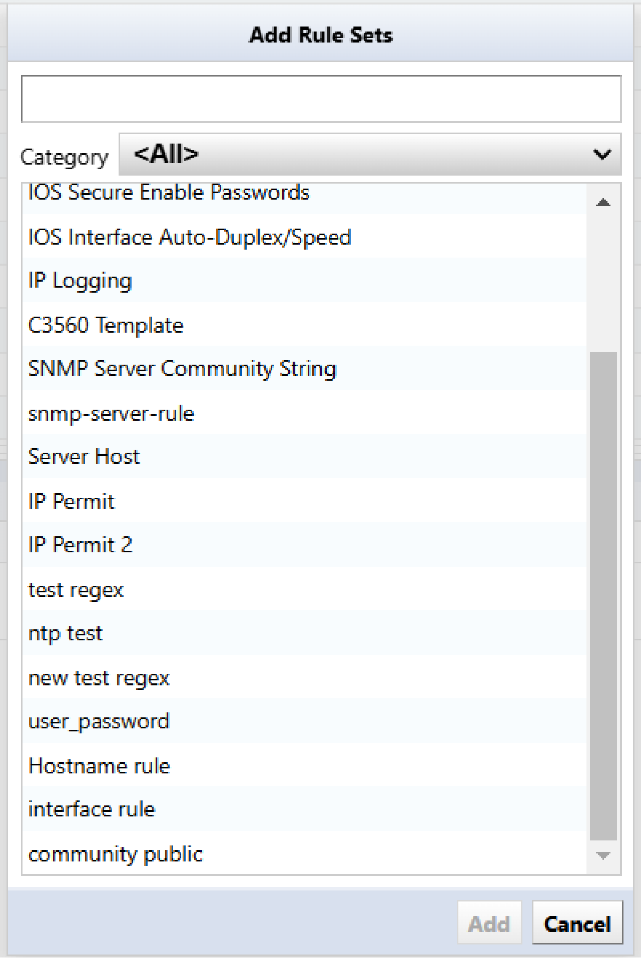
Compliance Policy - Cisco IOS community

Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity

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

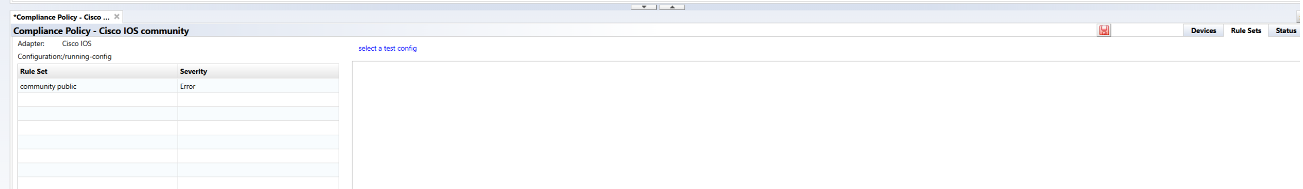


Add Rule Sets

Category <All>

IOS Secure Enable Passwords
IOS Interface Auto-Duplex/Speed
IP Logging
C3560 Template
SNMP Server Community String
snmp-server-rule
Server Host
IP Permit
IP Permit 2
test regex
ntp test
new test regex
user_password
Hostname rule
interface rule
community public

21. Click [Save].



*Compliance Policy - Cisco ...

Compliance Policy - Cisco IOS community

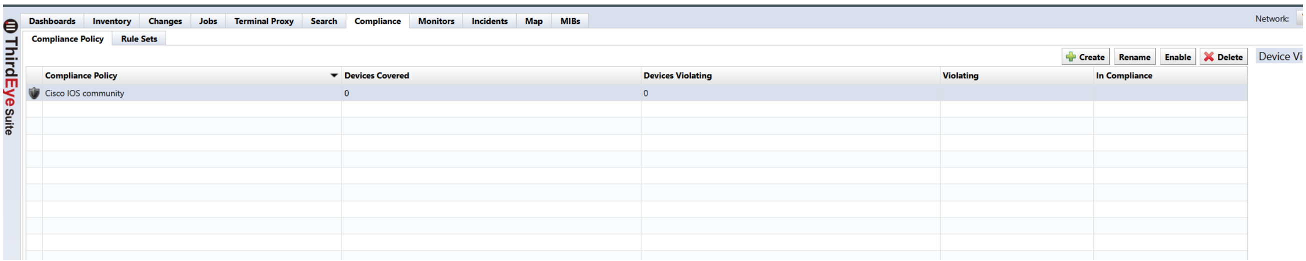
Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity
community public	Error

select a test config

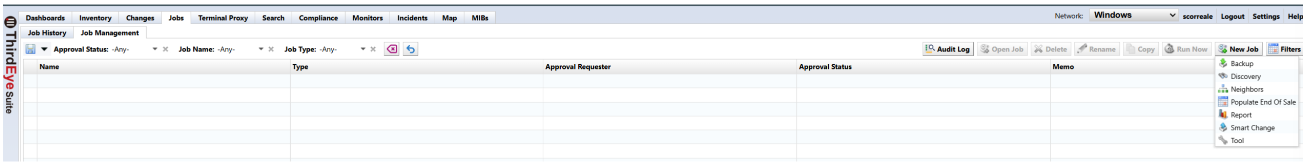
22. Select the compliance policy you created and click [Enable].



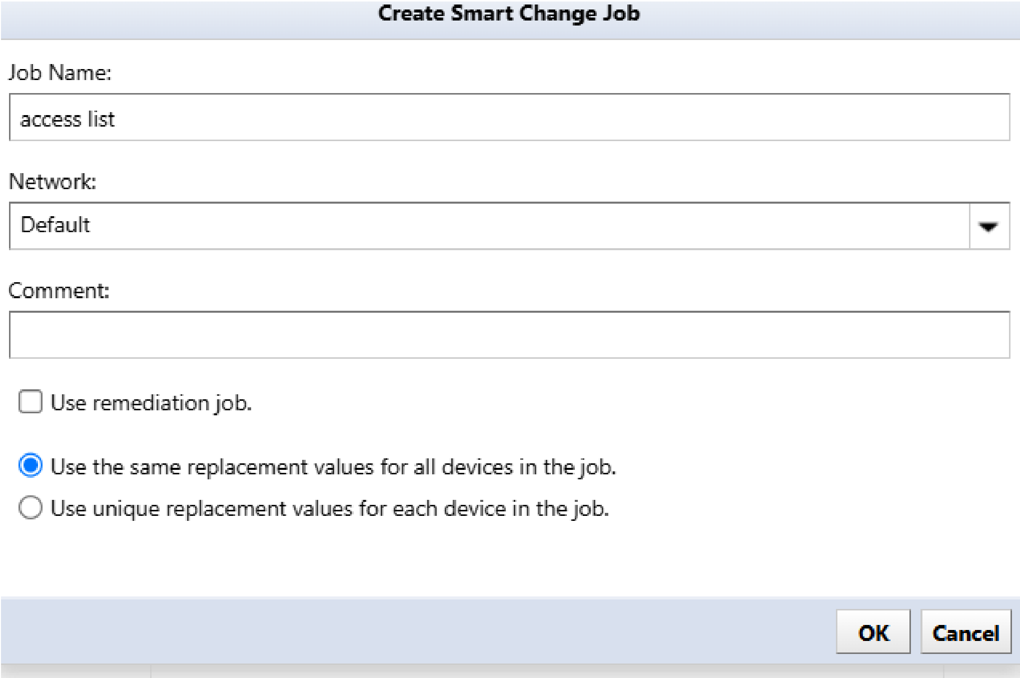
Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS community	0	0		

25.5.2 Case 2: No access list added to the interface

1. Click [Jobs] main tab > [Job Management] subtab > [New Job] > [Smart Change].



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



Create Smart Change Job

Job Name:

access list

Network:

Default

Comment:

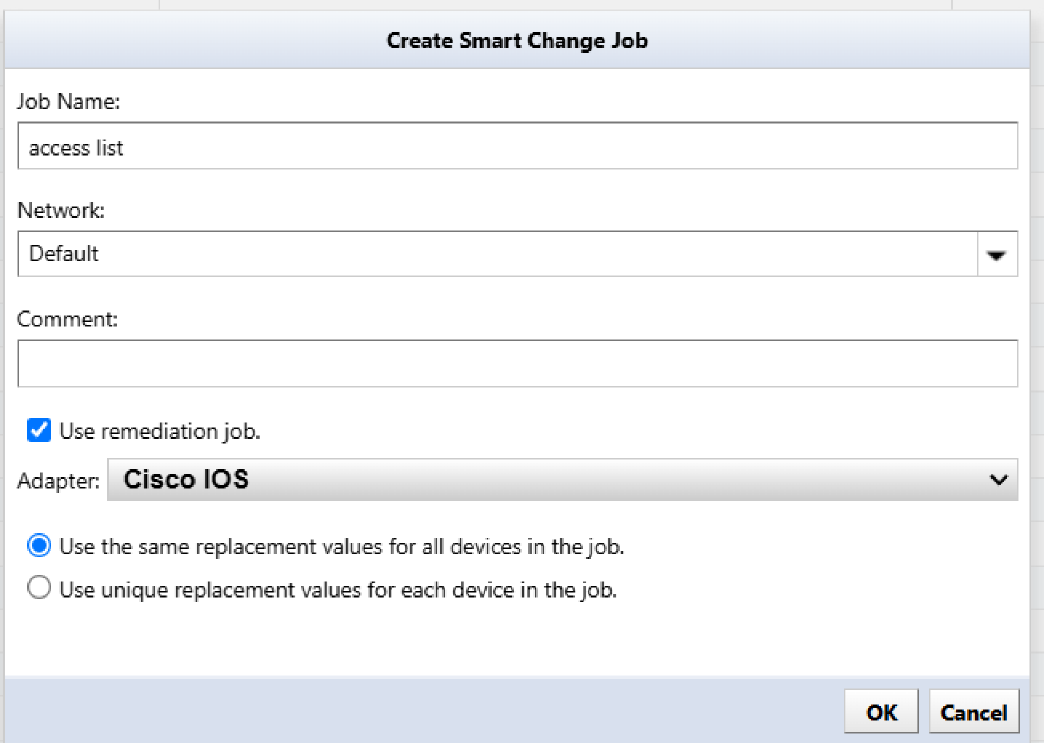
□ Use remediation job.

● Use the same replacement values for all devices in the job.

○ Use unique replacement values for each device in the job.

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

This is used for linking with Rule Sets.



Create Smart Change Job

Job Name: access list

Network: Default

Comment:

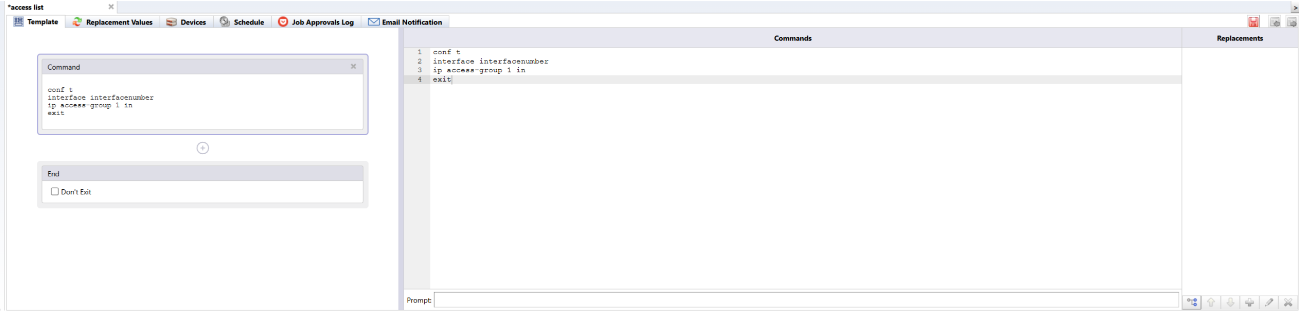
☑ Use remediation job.

Adapter: Cisco IOS

● Use the same replacement values for all devices in the job.

○ Use unique replacement values for each device in the job.

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



Command

```
conf t
interface interfacenumber
ip access-group 1 in
exit
```

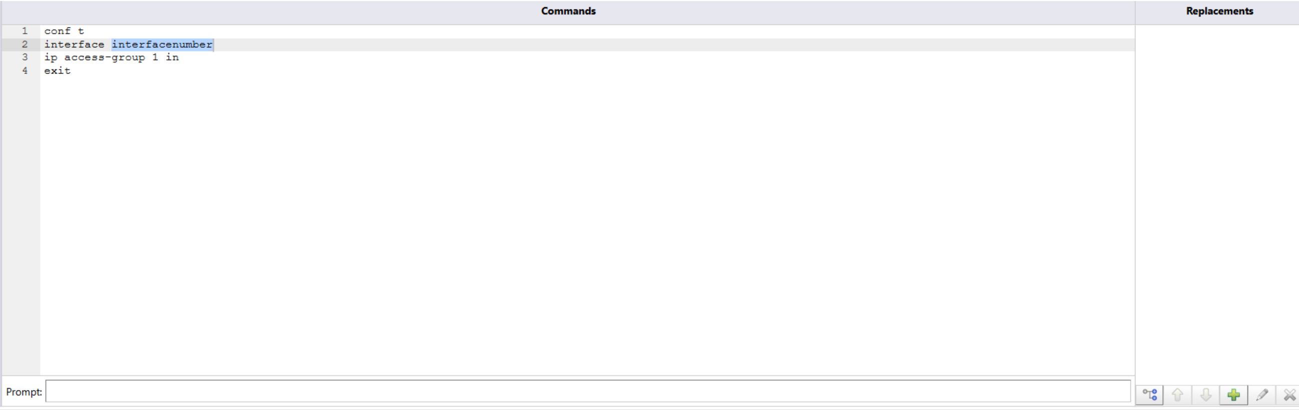
End

□ Don't Exit

Prompt:

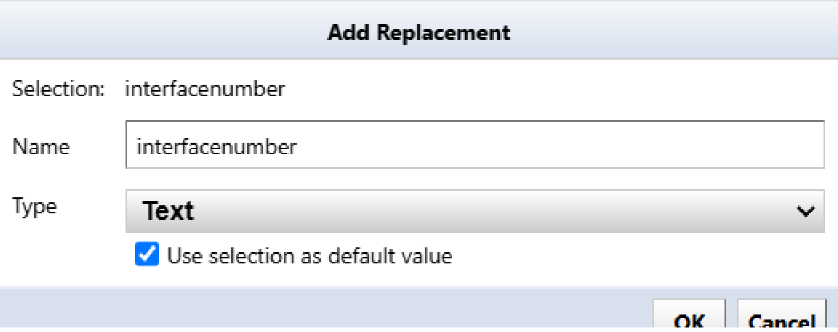
5. Select the part you want to convert into a variable and click the ✚ button.

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



```
conf t
interface interfacenumber
ip access-group 1 in
exit
```

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



Selection: interfacenumber

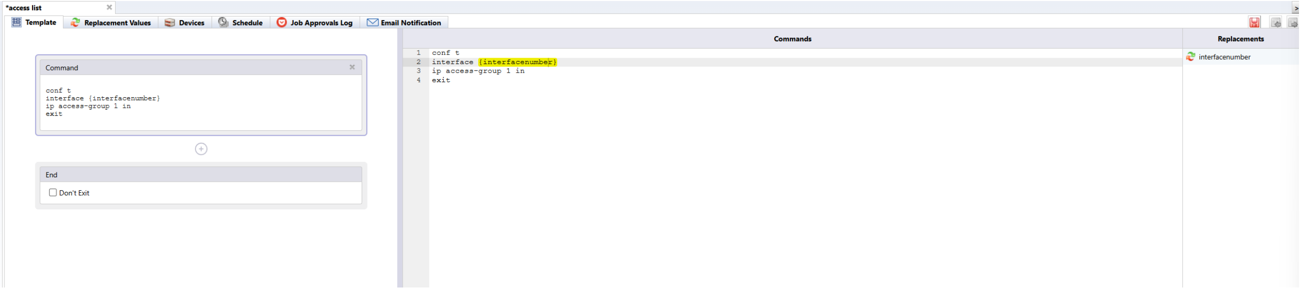
Name: interfacenumber

Type: Text

☑ Use selection as default value

{n}

7. Click [Save].

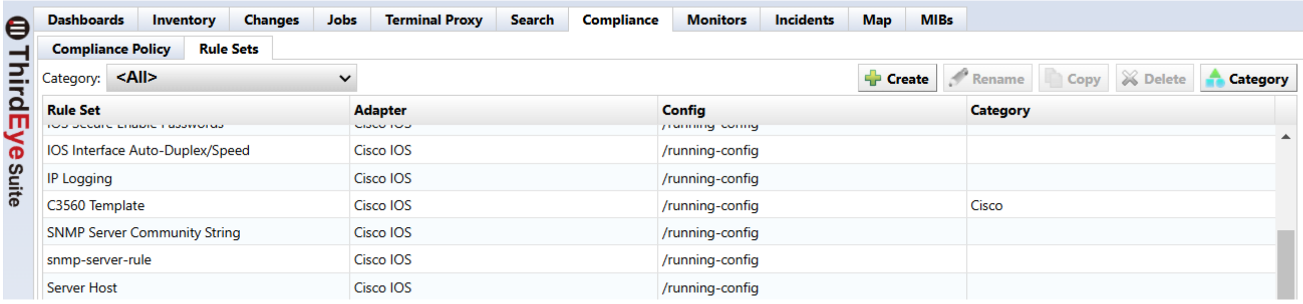


```
conf t
interface {interfacenumber}
ip access-group 1 in
exit
```

□ Don't Exit

Replacements: interfacenumber

8. Click the [Compliance] main tab > [Rule Sets] subtab, and click [Create].

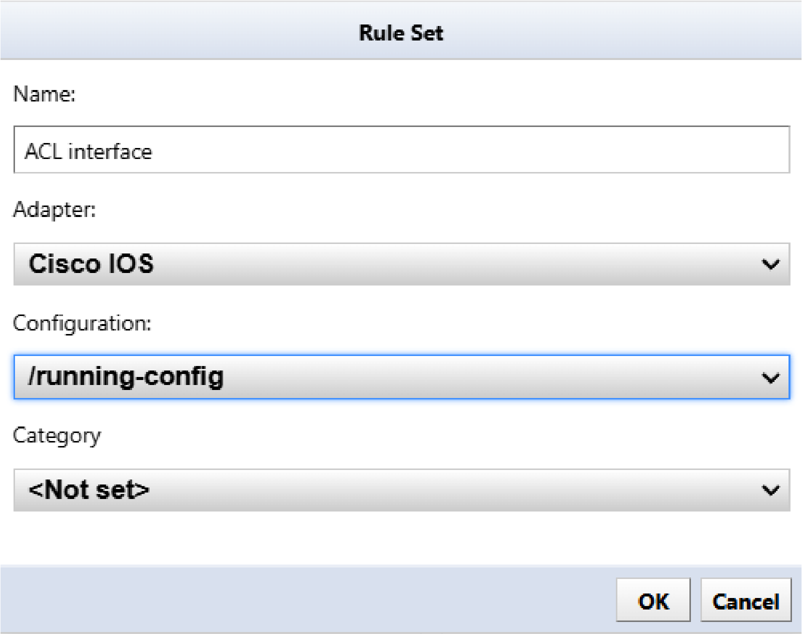


Category: <All>

Rule Set	Adapter	Config	Category
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IP Logging	Cisco IOS	/running-config	
C3560 Template	Cisco IOS	/running-config	Cisco
SNMP Server Community String	Cisco IOS	/running-config	
snmp-server-rule	Cisco IOS	/running-config	
Server Host	Cisco IOS	/running-config	

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

Select the adapter you selected when creating the Smart Change.



Rule Set

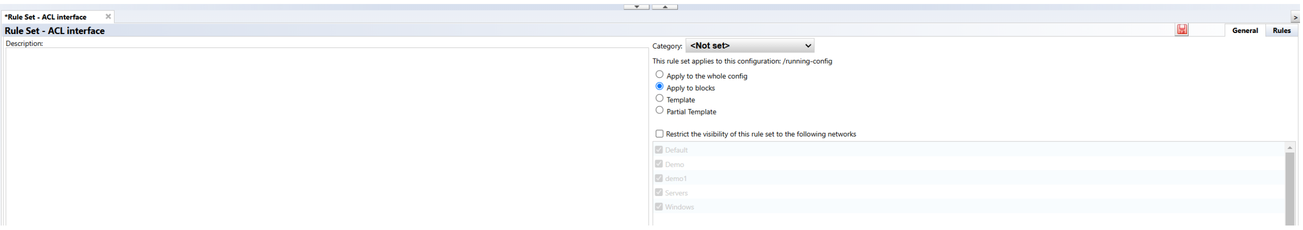
Name: ACL interface

Adapter: Cisco IOS

Configuration: /running-config

Category <Not set>

10. In the Editor at the bottom of the page, click the [General] tab, and select “Apply to Blocks”.



Rule Set - ACL interface

Description:

Category: <Not set>

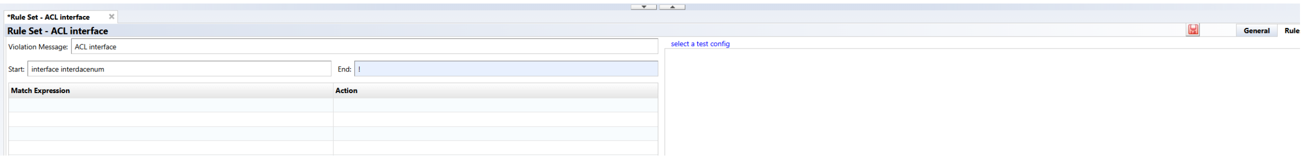
This rule set applies to this configuration: /running-config

○ Apply to the whole config
● Apply to blocks
○ Template
○ Partial Template

□ Restrict the visibility of this rule set to the following networks

☑ Default
☑ Demo
☑ demo1
☑ Servers
☑ Windows

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



Violation Message: ACL interface

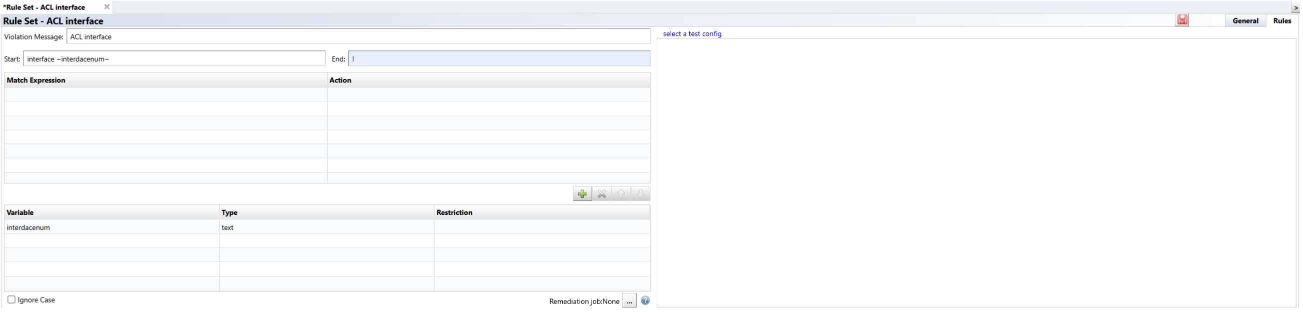
Start: interface interdacenum

End: !

Match Expression	Action

12. In the “Variable” section in the bottom half of the Editor, 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.



Violation Message: ACL interface

Start: interface ~interdacenum~

End: !

Match Expression	Action

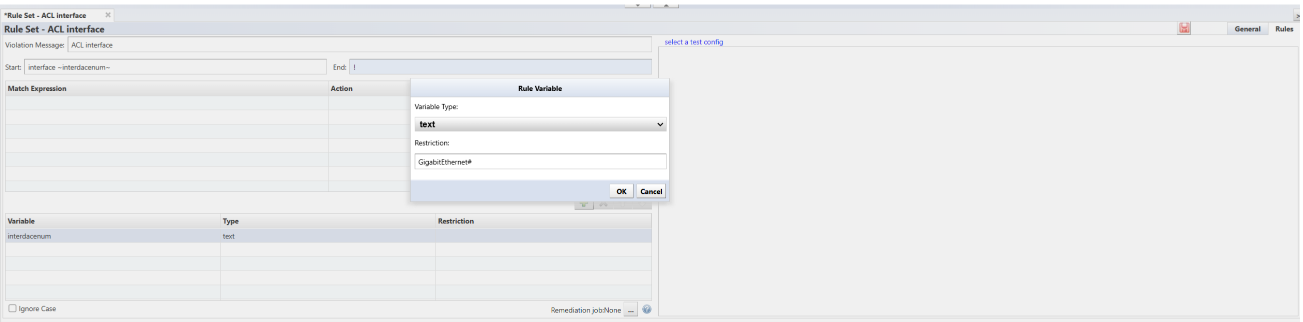
Variable	Type	Restriction
interdacenum	text	

□ Ignore Case

Remediation job:None

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

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



Rule Set - ACL interface

Violation Message: ACL interface

Start: interface ~interdacenum~ End: !

Match Expression	Action

Rule Variable

Variable Type: text

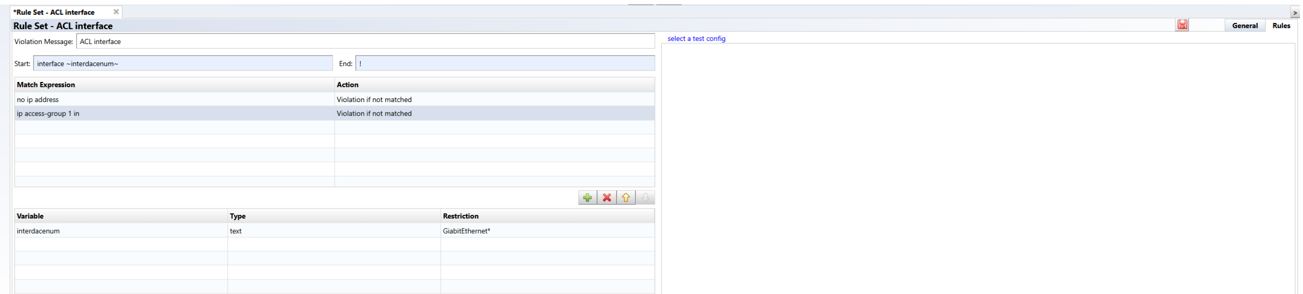
Restriction: GigabitEthernet#

Variable	Type	Restriction
interdacenum	text	

□ Ignore Case

Remediation job:None ...

14. Click the ✚ button to add matching conditions.



Rule Set - ACL interface

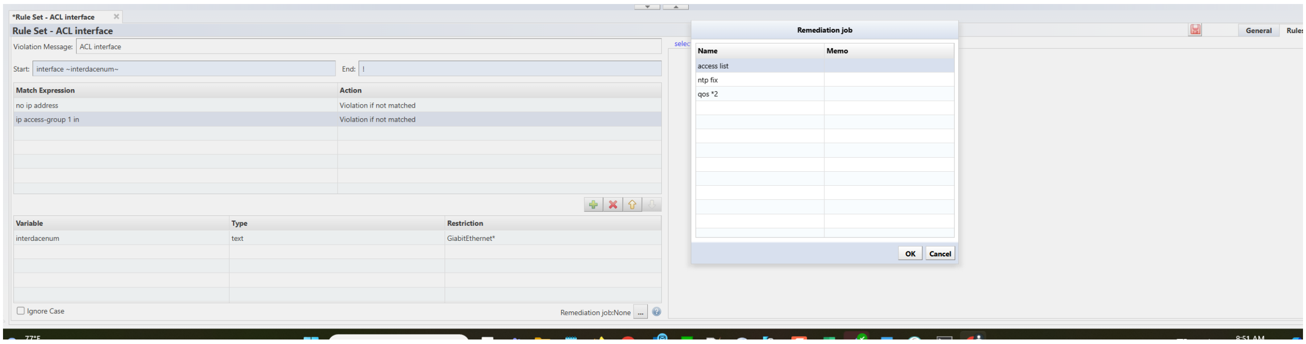
Violation Message: ACL interface

Start: interface ~interdacenum~ End: !

Match Expression	Action
no ip address	Violation if not matched
ip access-group 1 in	Violation if not matched

Variable	Type	Restriction
interdacenum	text	GiabitEthernet*

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



Rule Set - ACL interface

Violation Message: ACL interface

Start: interface ~interdacenum~ End: !

Match Expression	Action
no ip address	Violation if not matched
ip access-group 1 in	Violation if not matched

Variable	Type	Restriction
interdacenum	text	GiabitEthernet*

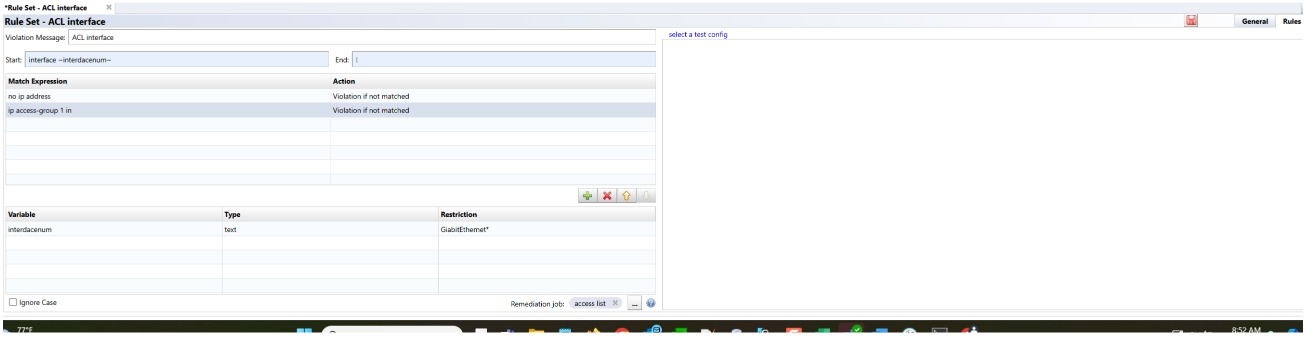
□ Ignore Case

Remediation job:None ...

Remediation job

Name	Memo
access list	
ntp fix	
qos *2	

16. Save your settings.



Rule Set - ACL interface

Violation Message: ACL interface

Start: interface ~interdacenum~

End: !

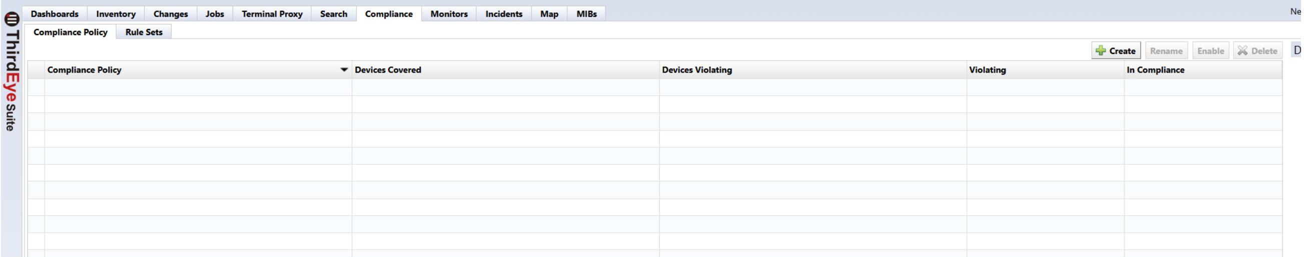
Match Expression	Action
no ip address	Violation if not matched
ip access-group 1 in	Violation if not matched

Variable	Type	Restriction
interdacenum	text	GiabitEthernet*

□ Ignore Case

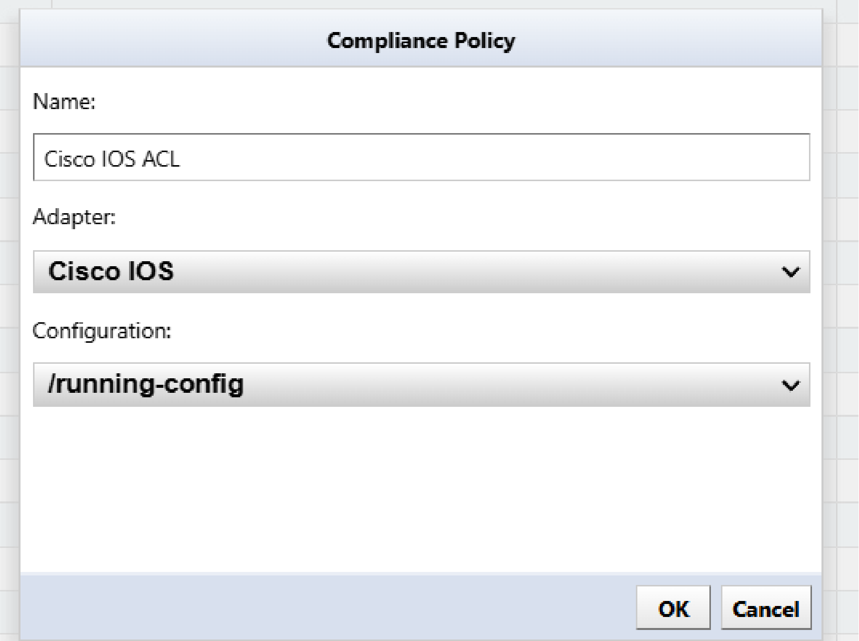
Remediation job: access list

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



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance

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



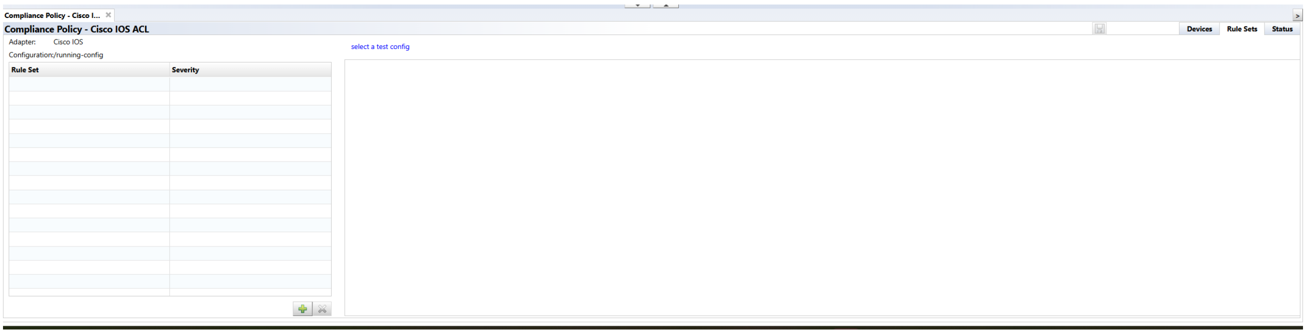
Compliance Policy

Name: Cisco IOS ACL

Adapter: Cisco IOS

Configuration: /running-config

19. Click the ➕ button.



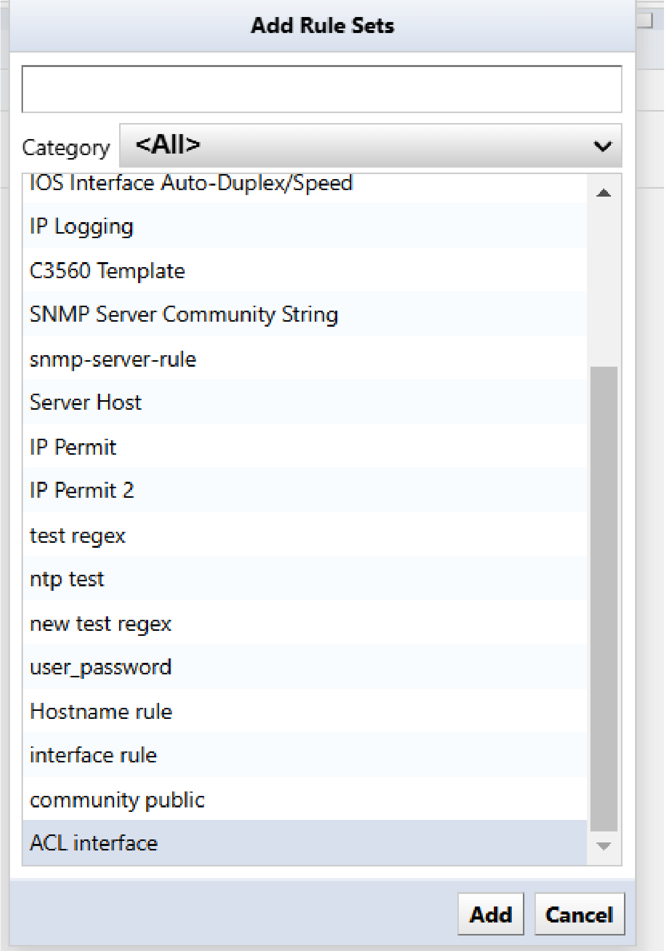
Compliance Policy - Cisco IOS ACL

Adapter: Cisco IOS

Configuration:/running-config

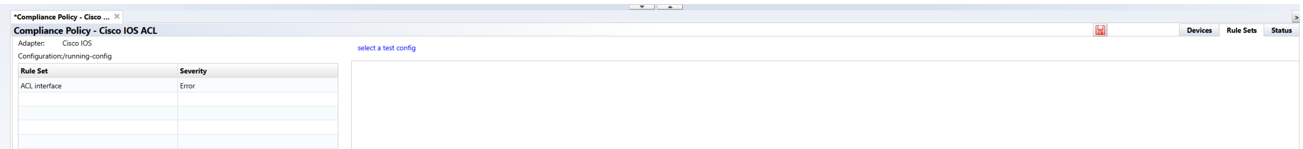
Rule Set	Severity

20. Add a Rule Set.



IOS Interface Auto-Duplex/Speed
IP Logging
C3560 Template
SNMP Server Community String
snmp-server-rule
Server Host
IP Permit
IP Permit 2
test regex
ntp test
new test regex
user_password
Hostname rule
interface rule
community public
ACL interface

21. Click [Save].



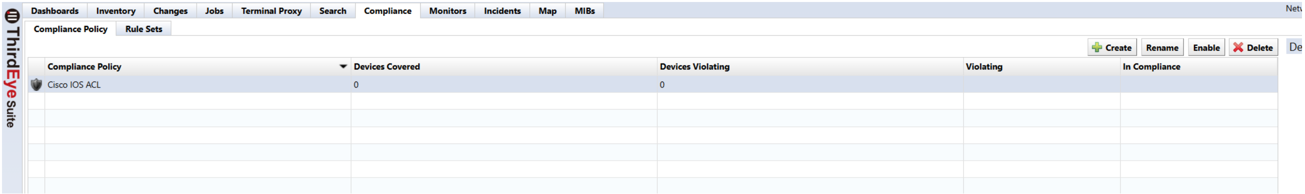
Compliance Policy - Cisco IOS ACL

Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity
ACL interface	Error

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



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS ACL	0	0		

SECTION 26

CHANGE ADVISOR

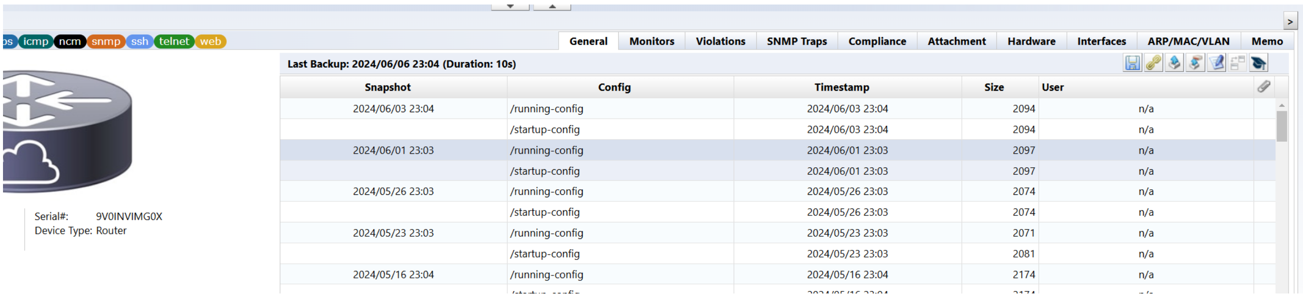
Suite

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.

To start Change Advisor:

1. Doubleclick the device in the device view.
2. Select a configuration from configuration history or draft.
3. Click the button.

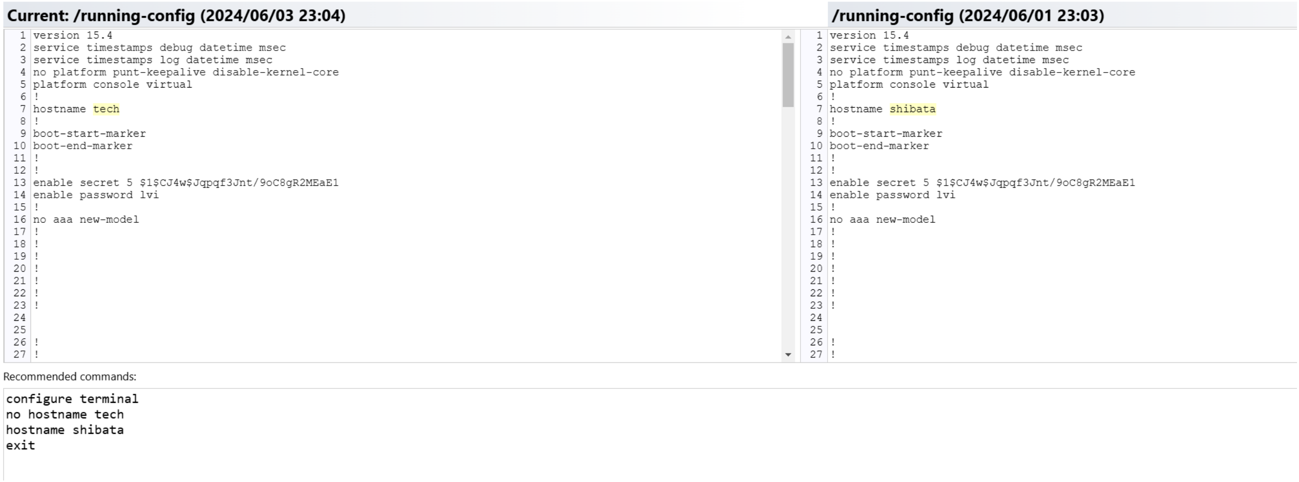


Serial#: 9V0INVIMG0X
Device Type: Router

Last Backup: 2024/06/06 23:04 (Duration: 10s)

Snapshot	Config	Timestamp	Size	User
2024/06/03 23:04	/running-config	2024/06/03 23:04	2094	n/a
	/startup-config	2024/06/03 23:04	2094	n/a
2024/06/01 23:03	/running-config	2024/06/01 23:03	2097	n/a
	/startup-config	2024/06/01 23:03	2097	n/a
2024/05/26 23:03	/running-config	2024/05/26 23:03	2074	n/a
	/startup-config	2024/05/26 23:03	2074	n/a
2024/05/23 23:03	/running-config	2024/05/23 23:03	2071	n/a
	/startup-config	2024/05/23 23:03	2081	n/a
2024/05/16 23:04	/running-config	2024/05/16 23:04	2174	n/a

4. Change Advisor starts and presents commands in the lower panel.



Current: /running-config (2024/06/03 23:04)

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname tech
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$CJ4w$Jqpqf3Jnt/9oC8gR2MEaE1
enable password lvi
!
no aaa new-model
!
!
!
!
!
!
!


!
!
```

/running-config (2024/06/01 23:03)

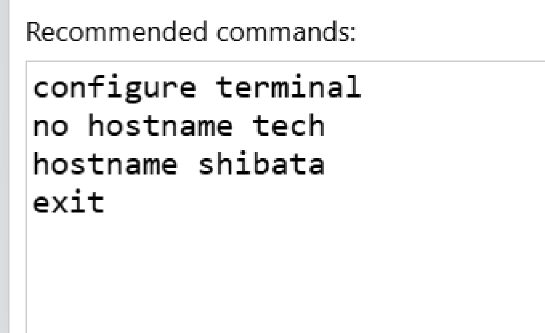
```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname shibata
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$CJ4w$Jqpqf3Jnt/9oC8gR2MEaE1
enable password lvi
!
no aaa new-model
!
!
!
!
!
!
!


!
!
```

Recommended commands:

```
configure terminal
no hostname tech
hostname shibata
exit
```

26.1 Execute Commands Using Change Advisor

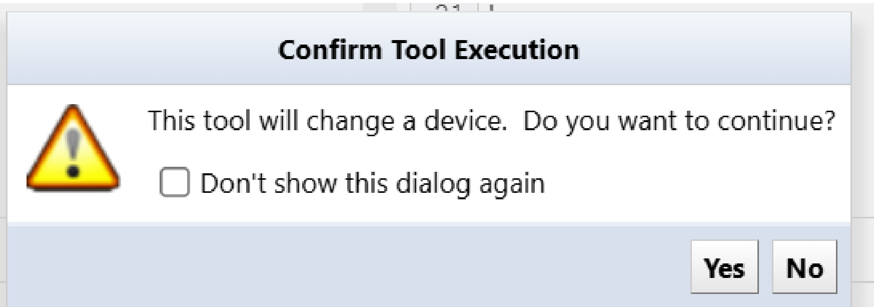
Commands output by Change Advisor can be executed on the device. Double check the command you want to run before executing the suggested command. If an incorrect command is antered, you can directly edit the output command.



Recommended commands:

```
configure terminal
no hostname tech
hostname shibata
exit
```

To proceed, click [Run], then [Yes].

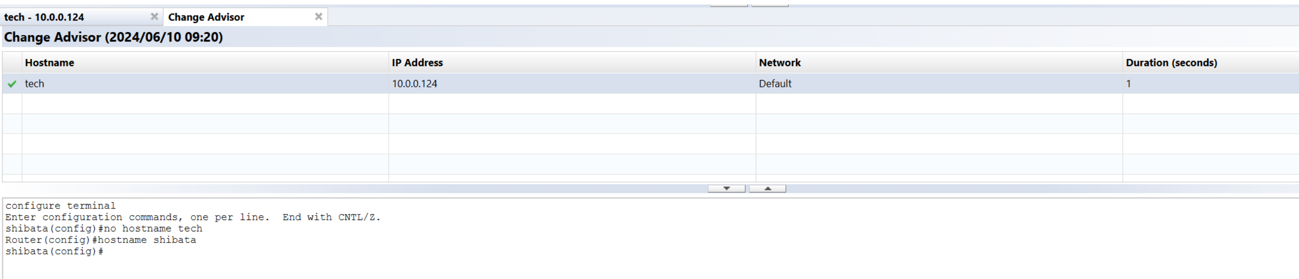


Confirm Tool Execution

This tool will change a device. Do you want to continue?

□ Don't show this dialog again

You can check the result after executing the command. Change Advisor execution results and history are also displayed in the job history.



Change Advisor (2024/06/10 09:20)

Hostname	IP Address	Network	Duration (seconds)
✓ tech	10.0.0.124	Default	1

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shibata(config)#no hostname tech
Router(config)#hostname shibata
shibata(config)#
```

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.

SECTION 27

JOBS

Jobs are automated workflows that execute network operations and complex workflows across the ThirdEye platform while maintaining audit histories.

Jobs put the following into operation:

- **Rules** (individual compliance checks)
- **Rulesets** (grouped policies)
- **Playbooks** (visual automation sequences)

27.1 Create A Job

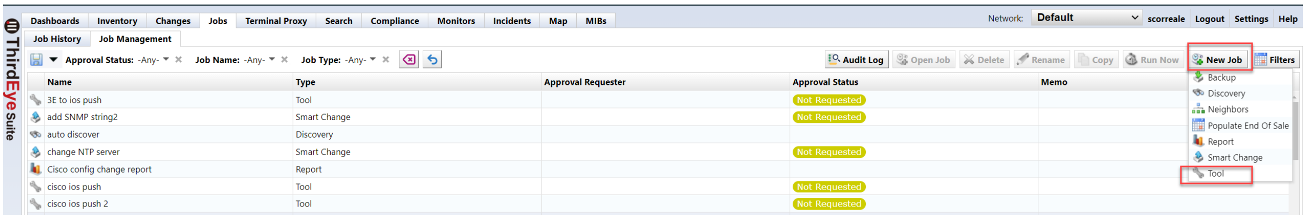
The general flow of creating a job remains the same regardless of the type of job:

1. Click the [Jobs] main tab.
2. Click the [Job Management] subtab.
3. Click the New Job button.
4. Enter a job name and select the functions you want to use.
5. Enter the required parameters.
6. Select the target device.
7. Enter the job trigger.

Example

Below, we will create a job as an example, and explain the steps screen by screen.

1. In the [Jobs] main tab, click [New Job] > [Tool].



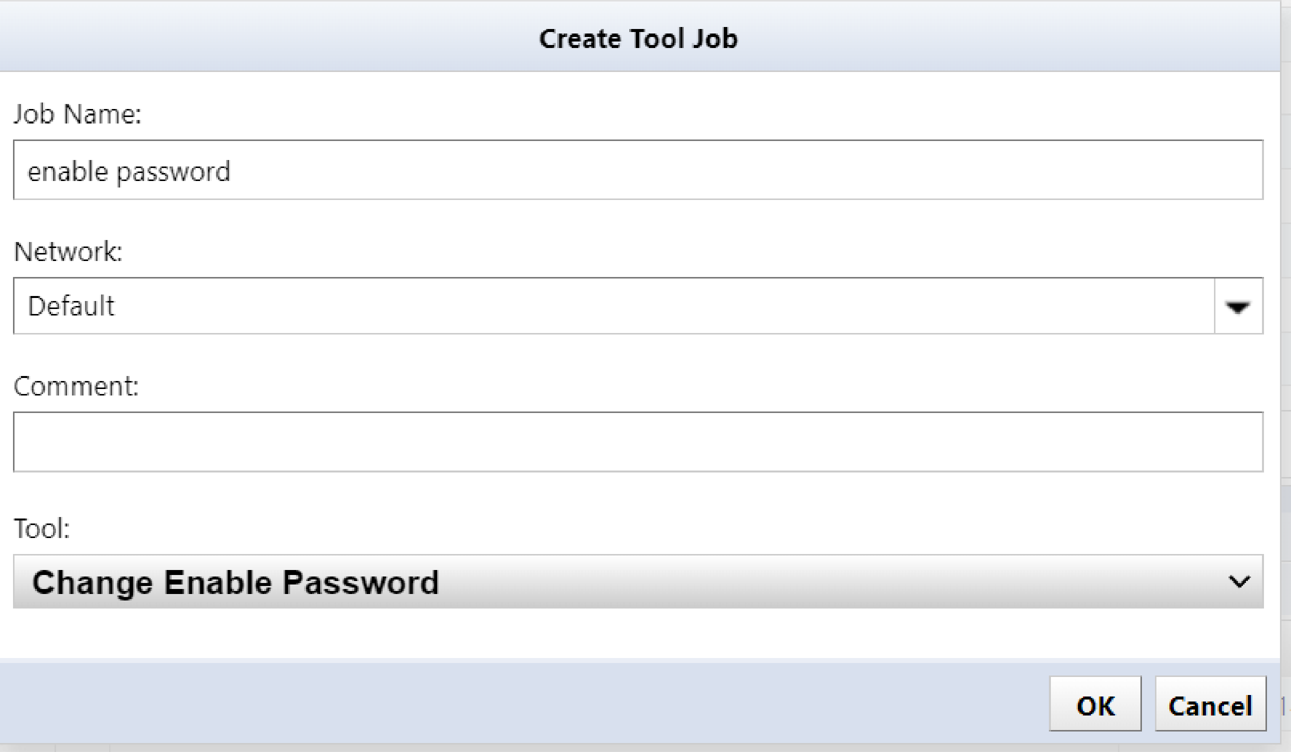
Approval Status: -Any- Job Name: -Any- Job Type: -Any-

Name	Type	Approval Requester	Approval Status	Memo
3E to ios push	Tool		Not Requested	
add SNMP string2	Smart Change		Not Requested	
auto discover	Discovery			
change NTP server	Smart Change		Not Requested	
Cisco config change report	Report			
cisco ios push	Tool		Not Requested	
cisco ios push 2	Tool		Not Requested	

2. In the [Create Tool Job] window, enter a job name and/or function:
3. Select a Network.
4. Add comments section that will be easy for others to understand later.

5. Select a Tool.

6. For this example, click [Change Enable Password].



Create Tool Job

Job Name:

enable password

Network:

Default

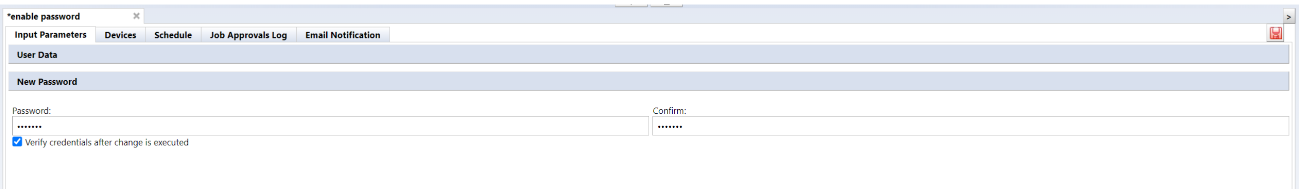
Comment:

Tool:

Change Enable Password

7. In the [*enable password] window, click the [Input Parameters] tab.

8. Enter the password string to be changed in the password field.



*enable password

User Data

New Password

Password: •••••••

Confirm: •••••••

☑ Verify credentials after change is executed

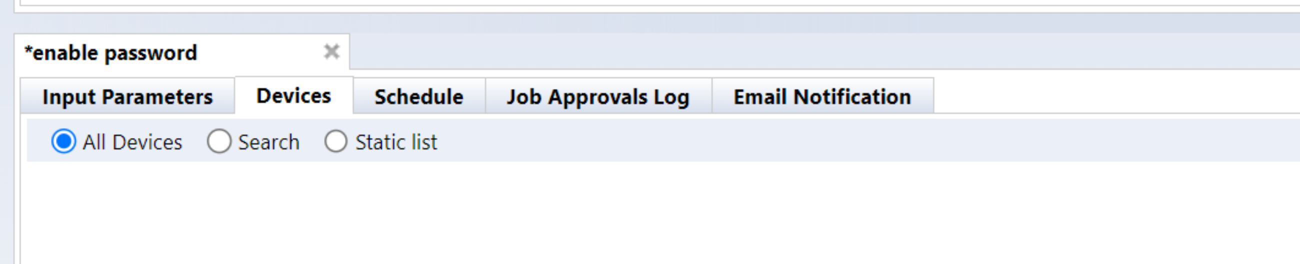
9. In the [*enable password] window, click the [Devices] tab.

10. Check one of the following to select the device on which you want to run the job:

- “All devices”
- “Search”
- “Static list”

All Devices

This applies to all registered devices.



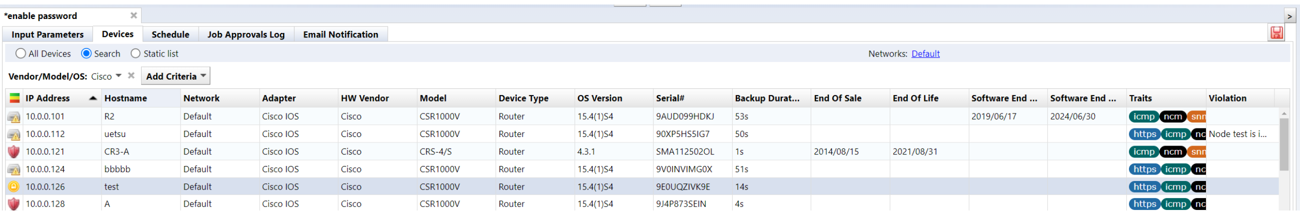
● All Devices ○ Search ○ Static list

Search

Devices that match the search criteria will be targeted.

Note

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



○ All Devices ● Search ○ Static list

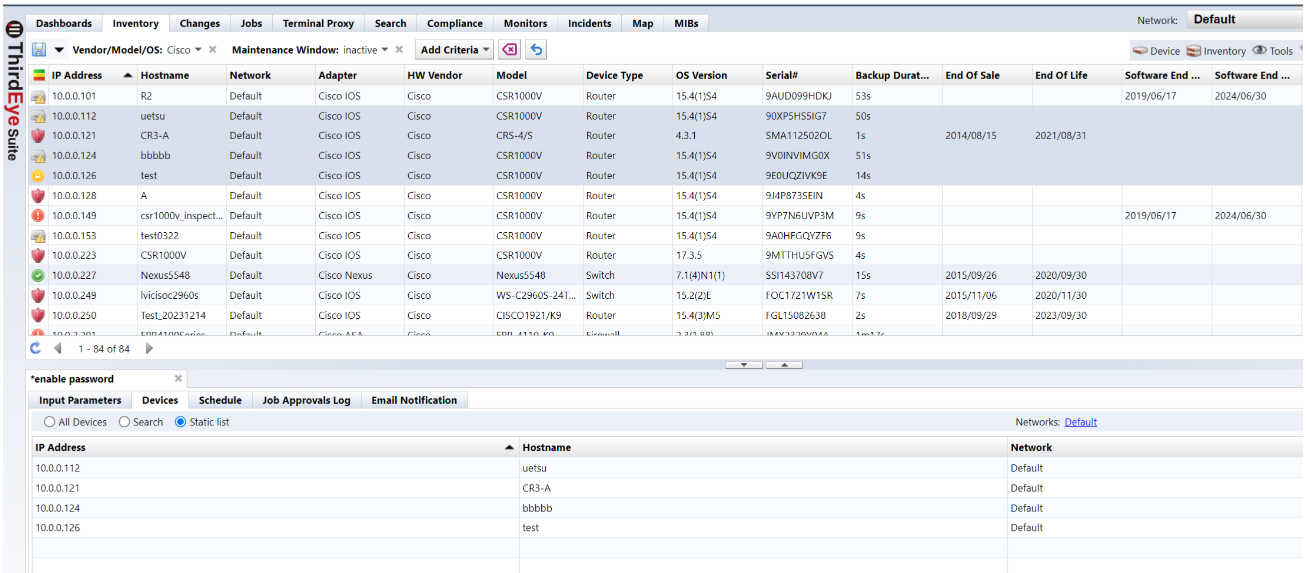
Networks: Default

Vendor/Model/OS: Cisco

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	53s			2019/06/17	2024/06/30	icmp ncm snr	
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	50s					https icmp nc	Node test is i...
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31			icmp ncm snr	
10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	51s					https icmp nc	
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	14s					https icmp nc	
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	4s					https icmp nc	

Static list

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



Vendor/Model/OS: Cisco   Maintenance Window: inactive

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	53s			2019/06/17	2024/06/30
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	50s				
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31		
10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	51s				
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	14s				
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	4s				
10.0.0.149	csr1000v_inspect...	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9YP7N6UVP3M	9s			2019/06/17	2024/06/30
10.0.0.153	test0322	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFGQYZF6	9s				
10.0.0.223	CSR1000V	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	4s				
10.0.0.227	Nexus5548	Default	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	15s	2015/09/26	2020/09/30		
10.0.0.249	lvicisoc2960s	Default	Cisco IOS	Cisco	WS-C2960S-24T...	Switch	15.2(2)E	FOC1721W1SR	7s	2015/11/06	2020/11/30		
10.0.0.250	Test_20231214	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	2s	2018/09/29	2023/09/30		

*enable password

Input Parameters | Devices | Schedule | Job Approvals Log | Email Notification

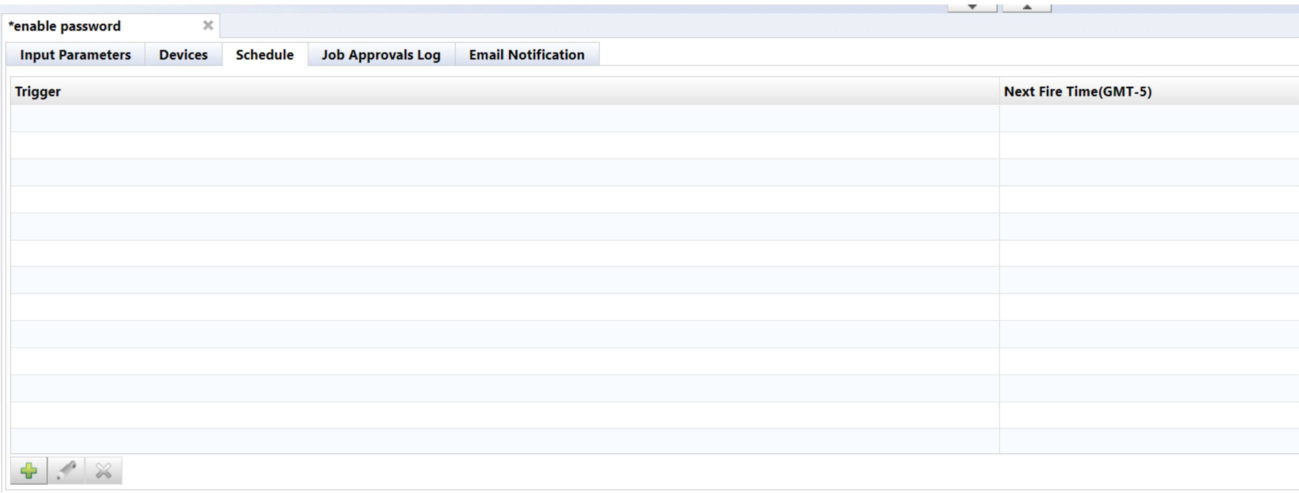
○ All Devices ○ Search ● Static list   Networks: Default

IP Address	Hostname	Network
10.0.0.112	uetsu	Default
10.0.0.121	CR3-A	Default
10.0.0.124	bbbbb	Default
10.0.0.126	test	Default

Finally, add the trigger:

11. In the [*enable password] window, click the [Schedule] tab.

12. Add new triggers using the ➕ button.



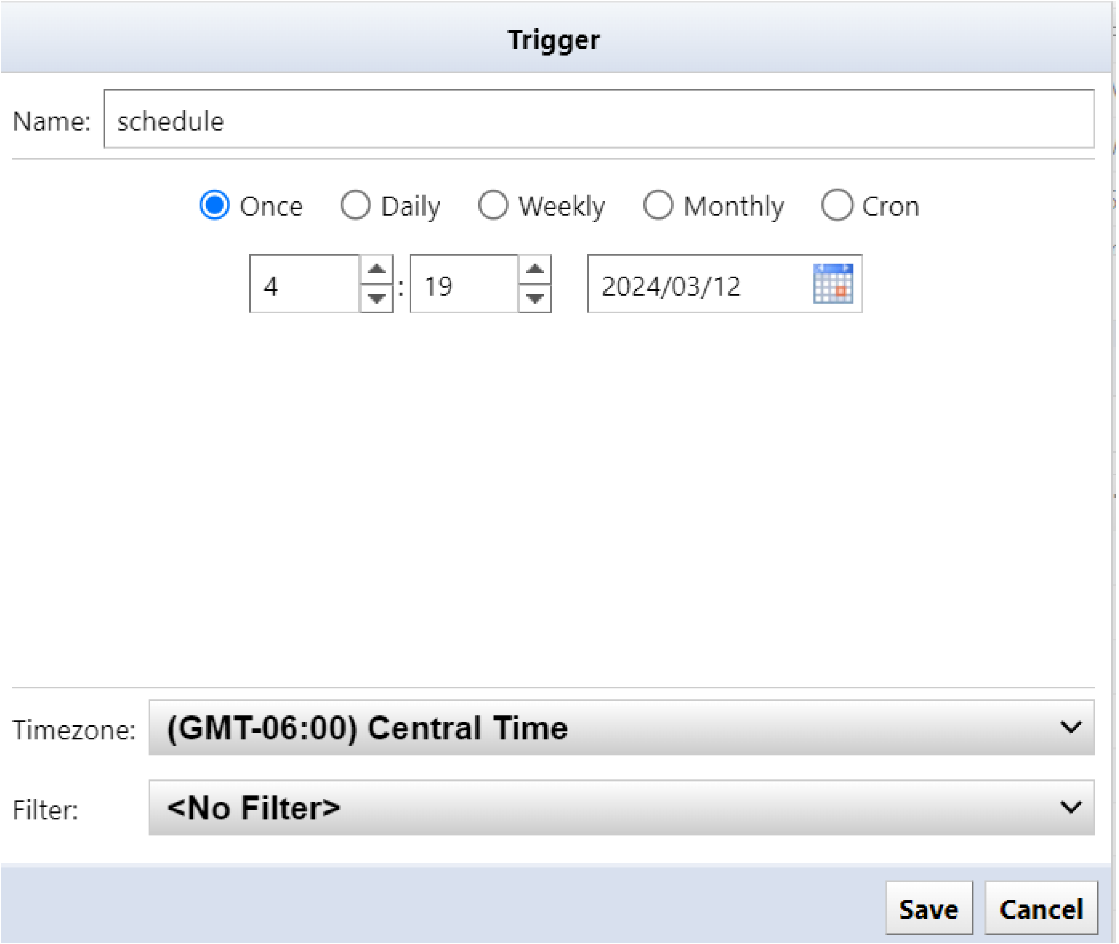
*enable password

Input Parameters | Devices | Schedule | Job Approvals Log | Email Notification

Trigger	Next Fire Time(GMT-5)

13. Set the date and repeat frequency.

14. When you have finished entering all information, click the [Save] button.



Trigger

Name: schedule

● Once ○ Daily ○ Weekly ○ Monthly ○ Cron

4 : 19 2024/03/12

Timezone: (GMT-06:00) Central Time

Filter: <No Filter>

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.

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

27.2 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.

> Note
>
> 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.
2. The person in charge of approval checks the relevant job request in the [Job Approval Log].
3. The person in charge of approvals selects [Approval], [Reject], or [Comment] from the confirmation screen, and contacts the applicant.
4. After clicking [Approval], the applicant can execute the corresponding job.

27.3 Approval Function Permissions

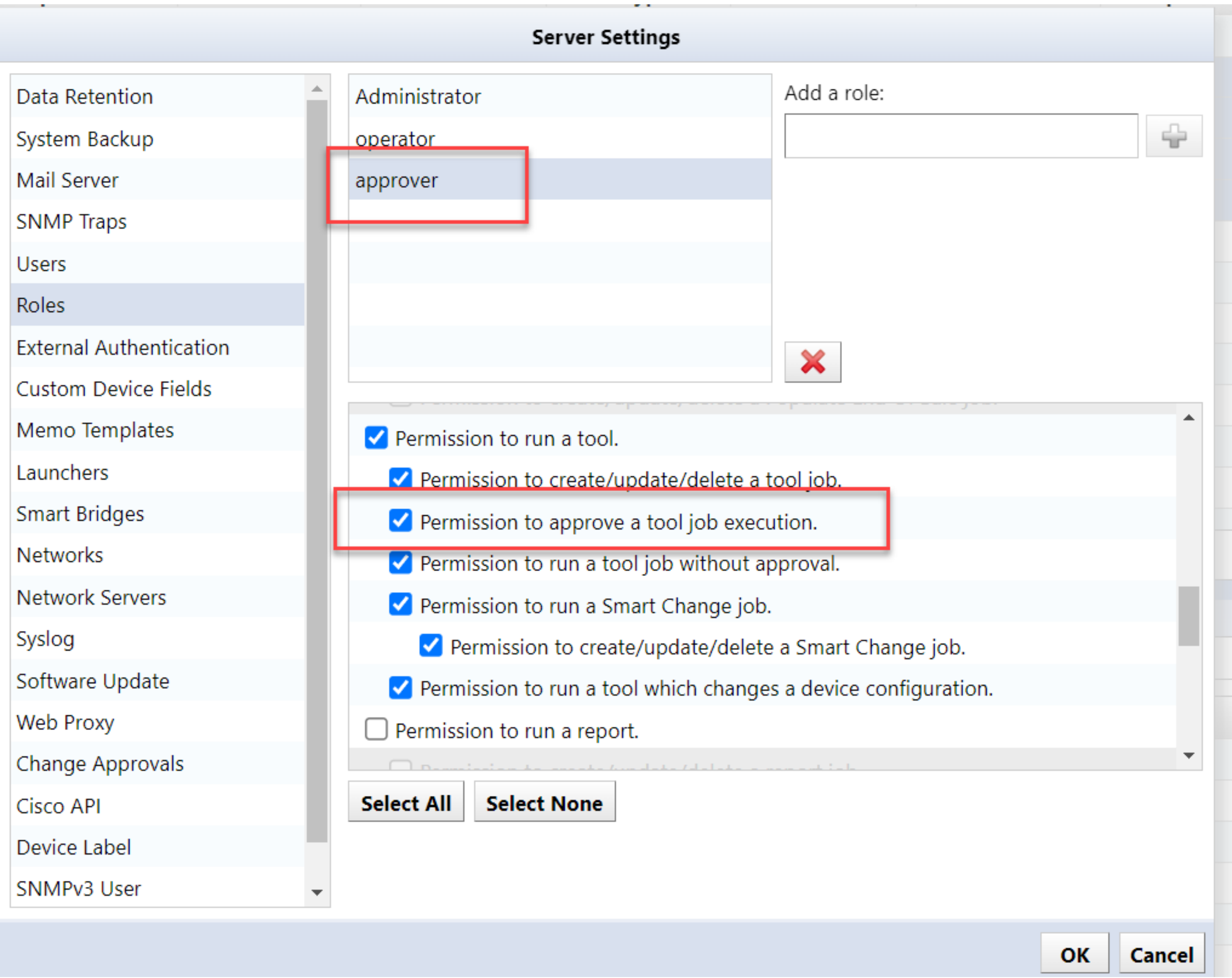
You can register approvers with configured permissions to approve jobs.

1. Click [Settings].
2. Click [Permissions]
3. Specify the desired permissions and permission details.
4. 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).

When setting the **approver's** authority, ensure that **"Permission to approve a tool job execution"** is checked.



Server Settings

Roles: Administrator, operator, approver

Add a role:

☑ Permission to run a tool.

☑ Permission to create/update/delete a tool job.

☑ Permission to approve a tool job execution.

☑ Permission to run a tool job without approval.

☑ Permission to run a Smart Change job.

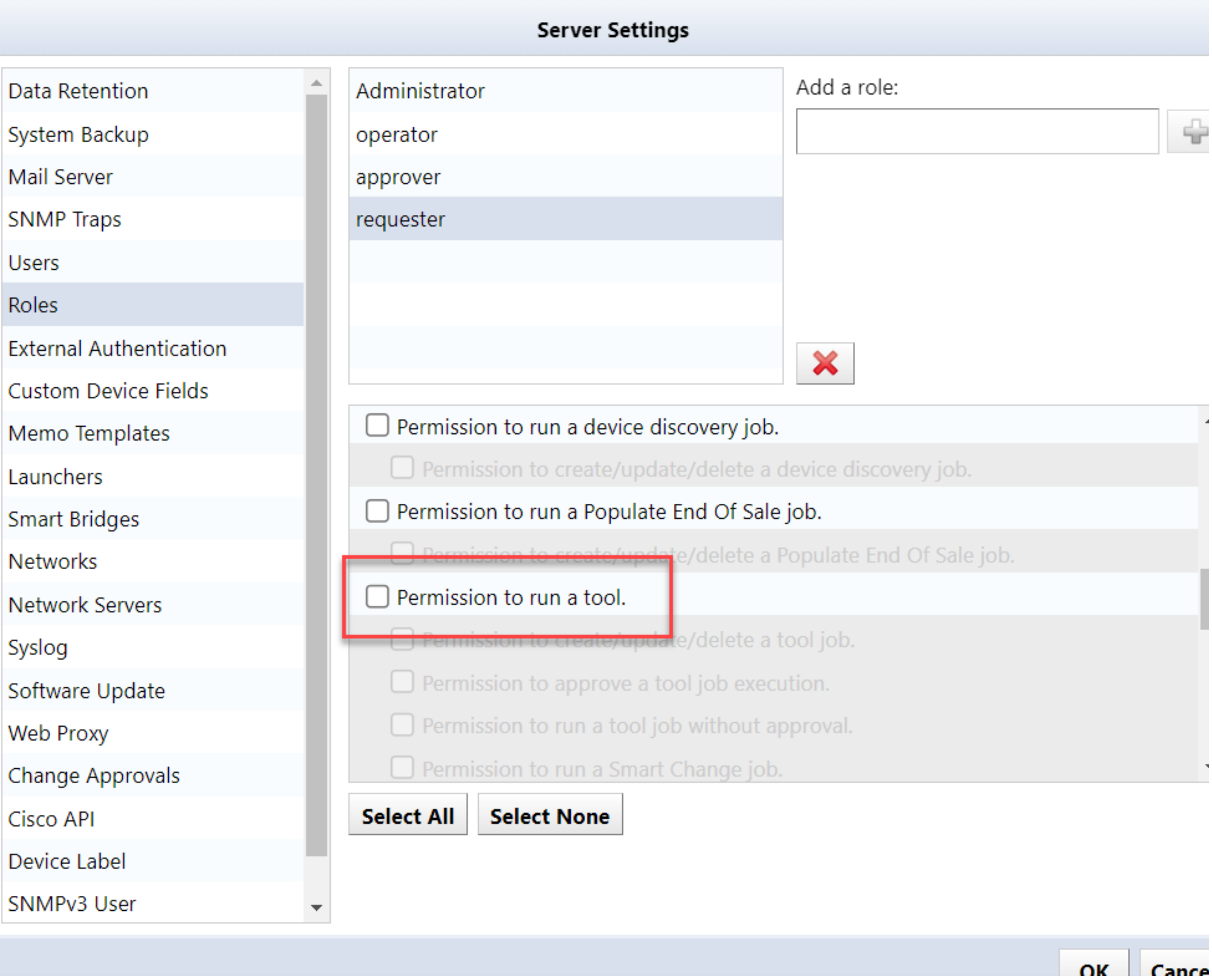
☑ Permission to create/update/delete a Smart Change job.

☑ Permission to run a tool which changes a device configuration.

☐ Permission to run a report.

Permission	Explanation
Permission to run a tool job without approval.	Authority to execute a job without requesting approval.

When setting the **applicant's** authority, ensure that **"Permission to run a tool"** is unchecked.



□ Permission to run a device discovery job.

□ Permission to create/update/delete a device discovery job.

□ Permission to run a Populate End Of Sale job.

□ Permission to create/update/delete a Populate End Of Sale job.

□ Permission to run a tool.

□ Permission to create/update/delete a tool job.

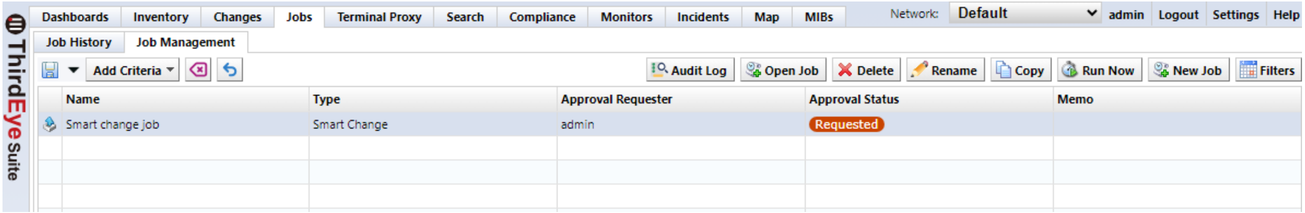
□ Permission to approve a tool job execution.

□ Permission to run a tool job without approval.

□ Permission to run a Smart Change job.

27.4 Job Approval Requests

1. Click [Jobs] > [Job History] > [Job Approval Logs].
2. Enter a message in the “Comments” field.
3. Click [Request Approval].
4. When the application is completed, “Requested” is displayed in the [Approval Status] column.



Name	Type	Approval Requester	Approval Status	Memo
Smart change job	Smart Change	admin	Requested	

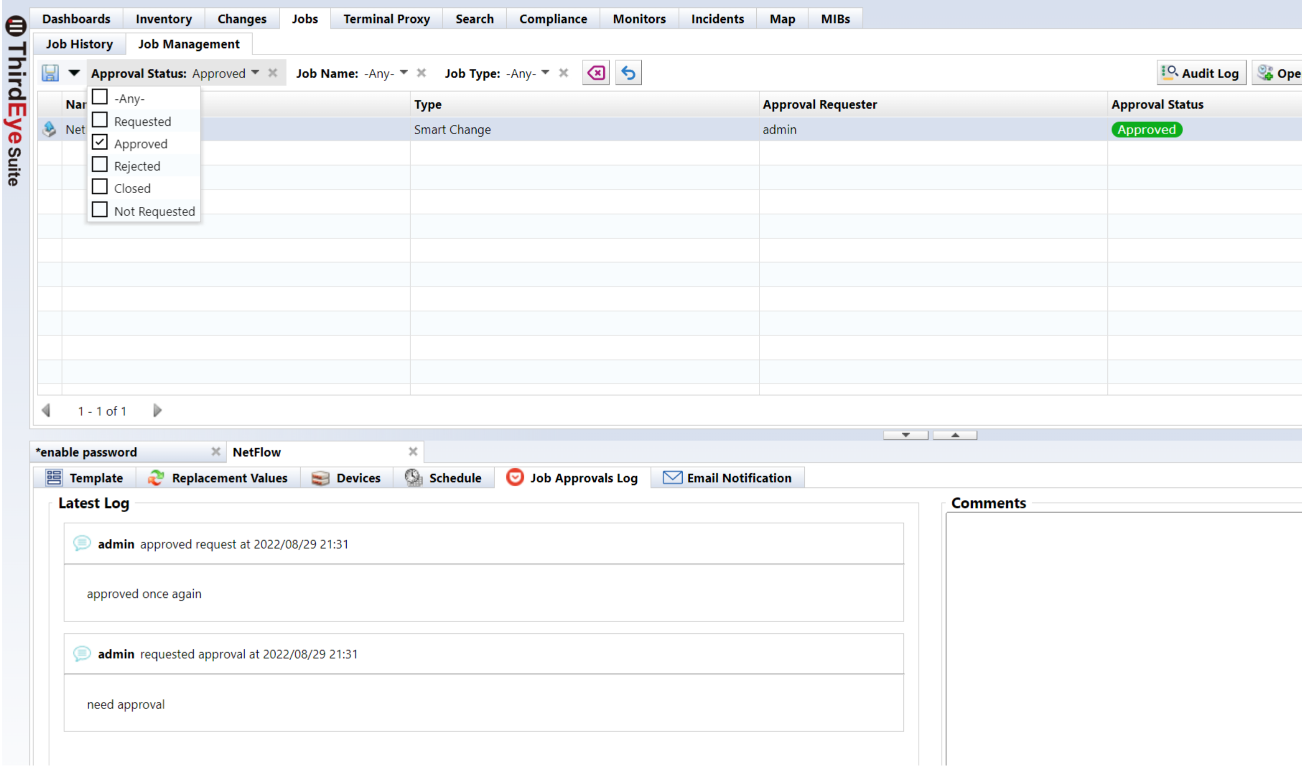
Job Approval Status	Explanation
Not Requested	Job approval request is not set.
Requested	Job execution approval is requested.
Approved	Job execution is approved.
Rejected	Job approval request has been rejected.
Closed	Job is closed. This status is set when: 1. Job is executed 2. Closed by administrator/job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

27.5 Approving Requests

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

2. Open the job that has been requested for approval.

You can use the [Job Execution Approval Status] button to filter the jobs.



Approval Status: Approved Job Name: -Any- Job Type: -Any-

□ -Any-
□ Requested
☑ Approved
□ Rejected
□ Closed
□ Not Requested

Nar	Type	Approval Requester	Approval Status
Net	Smart Change	admin	Approved

1 - 1 of 1

Latest Log

admin approved request at 2022/08/29 21:31

approved once again

admin requested approval at 2022/08/29 21:31

need approval

Comments

3. Check the job details and open the [Job Approval Log] tab.

4. Enter your message in the message field and click [Approve], [Reject], or [Comment].

27.6 Check Pre-Approval Record

1. Click [Jobs] > [Job History].

2. Select the target job, and click [Job Approval Log] to check the record (messages) up to approval.

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

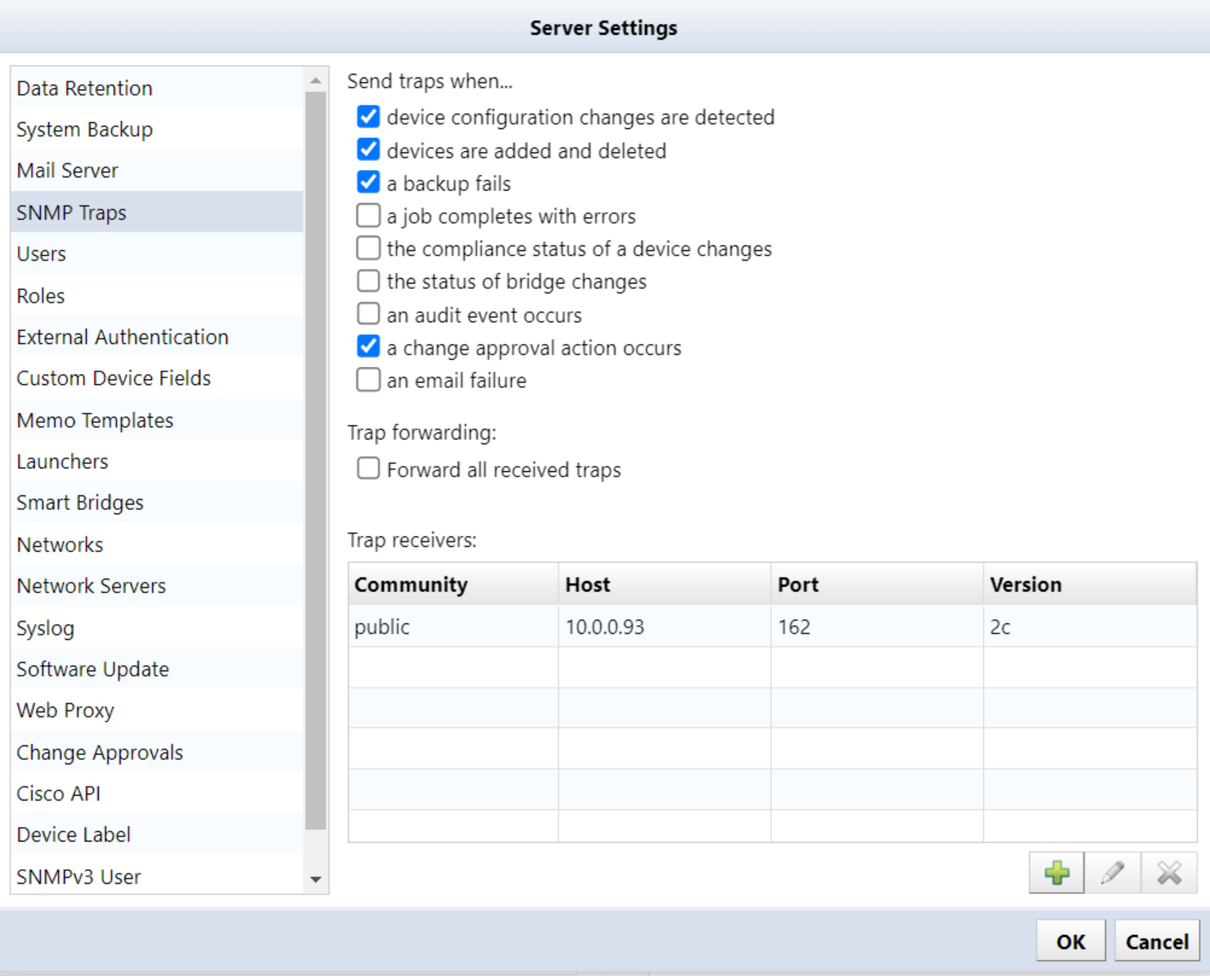
27.7 Approval Notifications

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

27.8 SNMP Trap Notifications

In the Global Menu, click [Server Settings] > [SNMP Traps].

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



Send traps when...

☑ device configuration changes are detected
☑ devices are added and deleted
☑ a backup fails
☐ a job completes with errors
☐ the compliance status of a device changes
☐ the status of bridge changes
☐ an audit event occurs
☑ a change approval action occurs
☐ an email failure

Trap forwarding:

☐ Forward all received traps

Trap receivers:

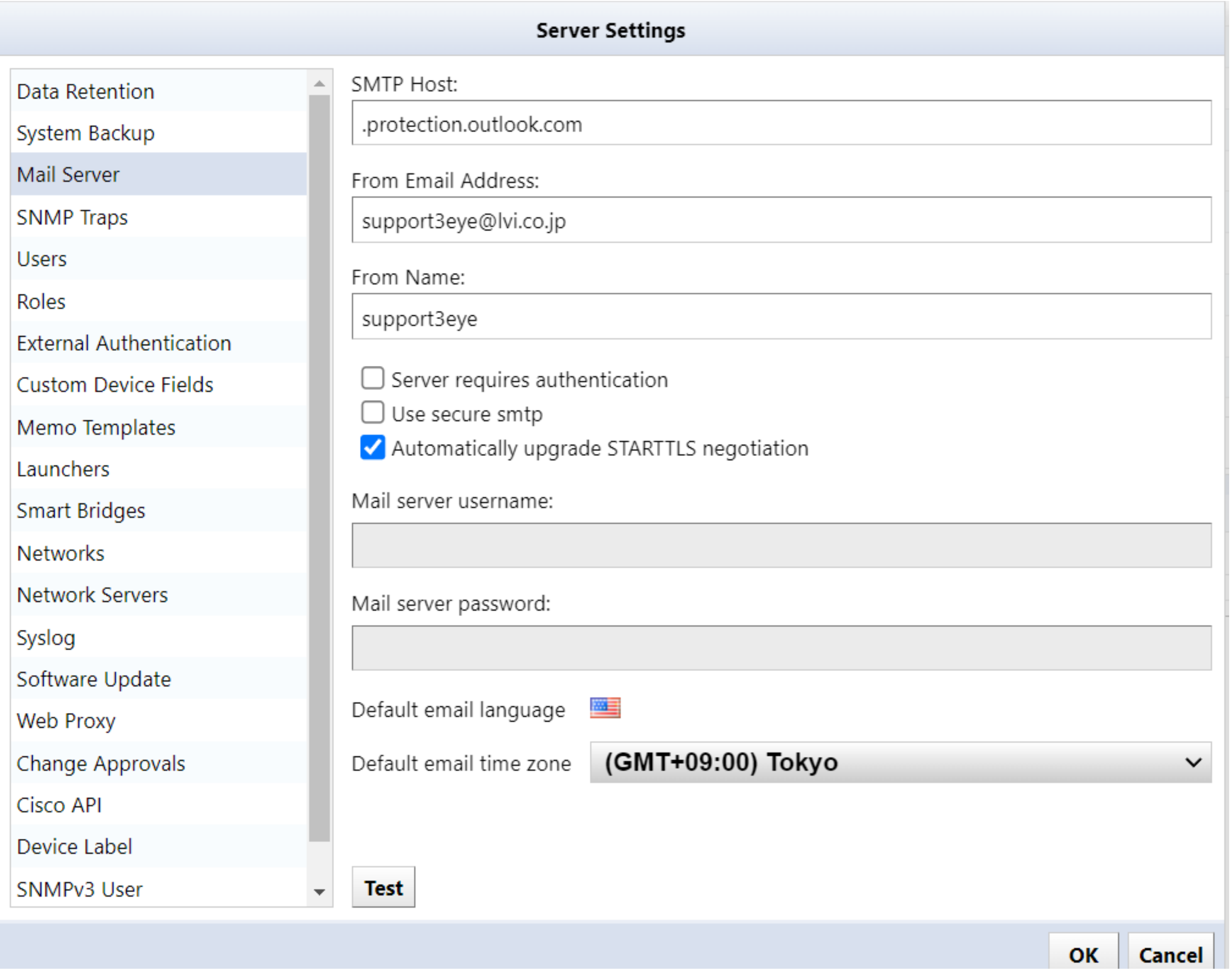
Community	Host	Port	Version
public	10.0.0.93	162	2c

27.9 Email Notifications

In the Global Menu, click[Server Settings] > [Mail Server].

An email will be sent when a job is requested/submitted/approved/rejected/closed.

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



SMTP Host: .protection.outlook.com

From Email Address: support3eye@lvi.co.jp

From Name: support3eye

□ Server requires authentication

□ Use secure smtp

☑ Automatically upgrade STARTTLS negotiation

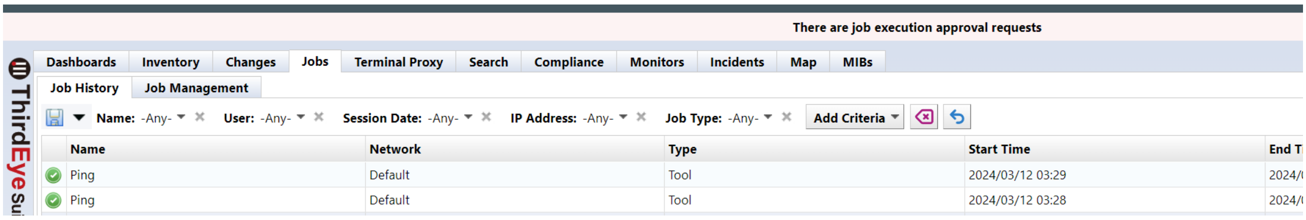
Mail server username:

Mail server password:

Default email language 🇺🇸

Default email time zone (GMT+09:00) Tokyo

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



There are job execution approval requests

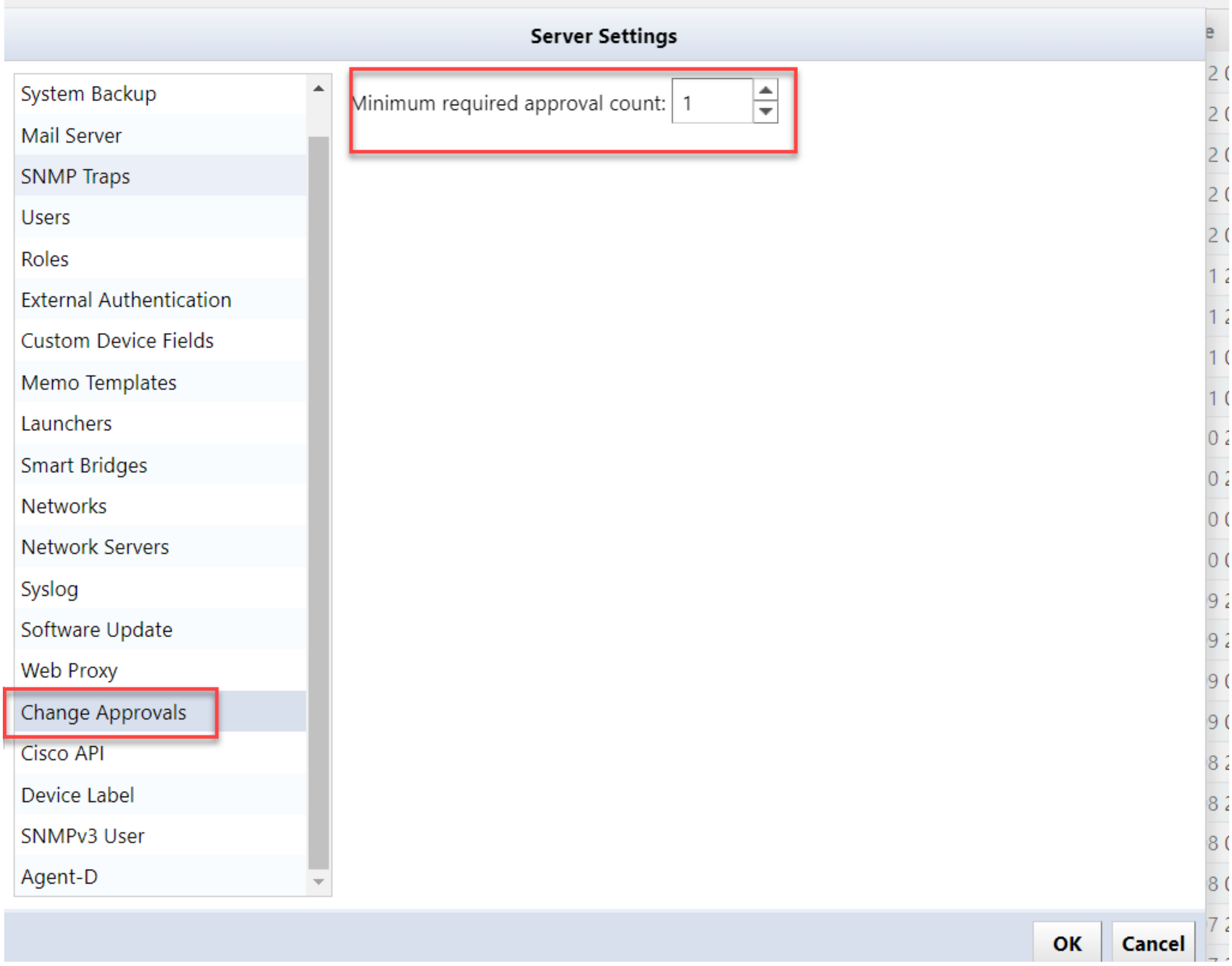
Name: -Any- User: -Any- Session Date: -Any- IP Address: -Any- Job Type: -Any-

	Name	Network	Type	Start Time	End T
✓	Ping	Default	Tool	2024/03/12 03:29	2024/(
✓	Ping	Default	Tool	2024/03/12 03:28	2024/(

27.10 Change Required Approvals Number

You can specify the number of approvals required before a job created or edited by an applicant can be executed.

In the Global Menu, click [Settings] > [Change Approvals]. The configurable range is 1 to 3.



Minimum required approval count: 1

27.11 Check Past Job History

Click the [Jobs] > [Job History] tabs to view the jobs that have been executed. Doubleclick on a published report to view the job type:

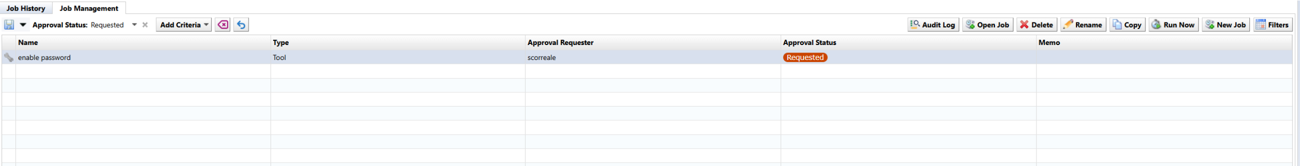
- Report
- Discover
- Neighbor
- Backup
- Agent-D
- Tool
- Information such as “when”, “who”, and “what was done”

[Column list]

Item	Explanation
Name	Displays the name of the job.
Network	Displays the name of the network.
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.

27.12 Delete Job

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

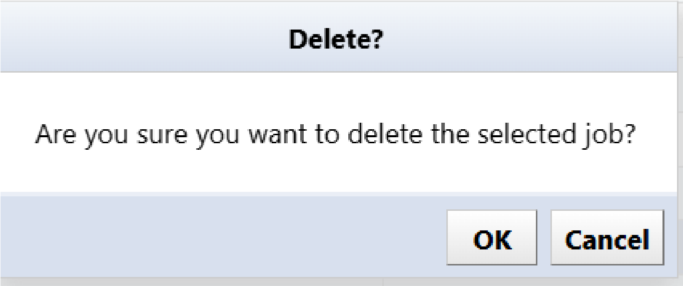


Approval Status: Requested

Name	Type	Approval Requester	Approval Status	Memo
enable password	Tool	scorreale	Requested	

2. Select the job you want to delete, and click [Delete].

3. Click [Yes] on the confirmation screen.



Are you sure you want to delete the selected job?

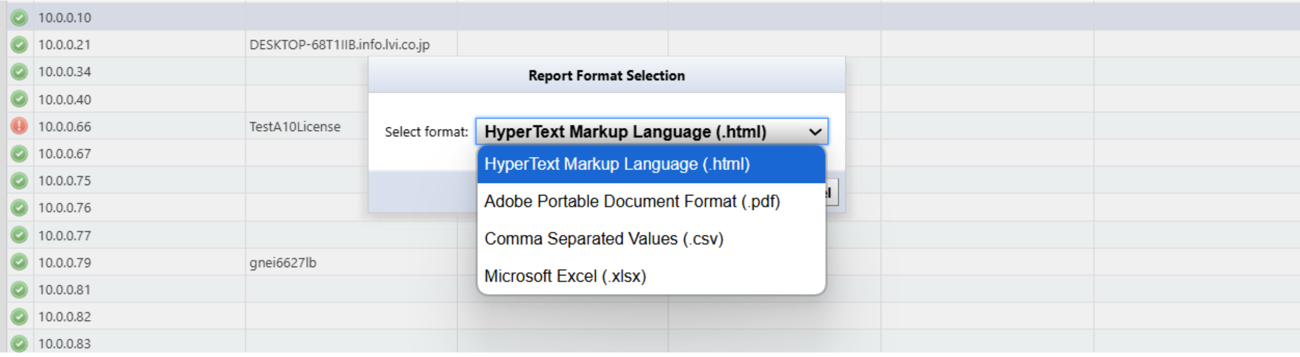
The selected job will be deleted from the job management list.

SECTION 28

REPORTS

ThirdEye provides a variety of customizable reports that can be run on-demand as well as with schedules.

Reports support export in multiple formats (PDF, HTML, Excel, CSV), and can be scheduled for automated email delivery.



✓	10.0.0.10	
✓	10.0.0.21	DESKTOP-68T1IIB.info.lvi.co.jp
✓	10.0.0.34	
✓	10.0.0.40	
!	10.0.0.66	TestA10License
✓	10.0.0.67	
✓	10.0.0.75	
✓	10.0.0.76	
✓	10.0.0.77	
✓	10.0.0.79	gnei6627lb
✓	10.0.0.81	
✓	10.0.0.82	
✓	10.0.0.83	

Report Format Selection

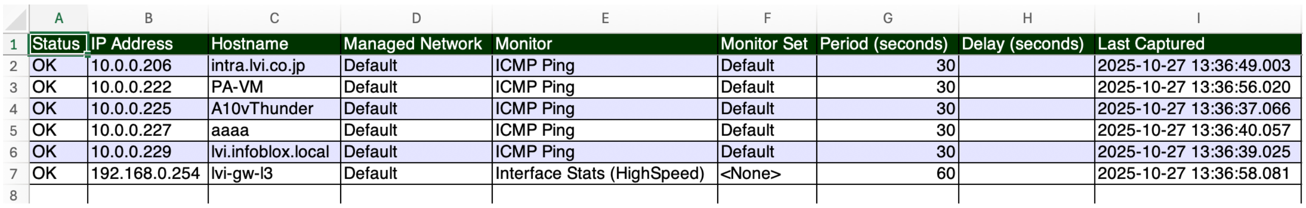
Select format: HyperText Markup Language (.html)

HyperText Markup Language (.html)
Adobe Portable Document Format (.pdf)
Comma Separated Values (.csv)
Microsoft Excel (.xlsx)

28.1 Monitor Health Report

Supported Output Formats: Excel and CSV (*comma separated values*)

The monitor health report allows you to easily confirm that the ThirdEye monitoring systems are functioning properly. The report will take a device selection and show a single status row for each monitor associated with each device. Only "polling" monitors will be included.



Status	IP Address	Hostname	Managed Network	Monitor	Monitor Set	Period (seconds)	Delay (seconds)	Last Captured
OK	10.0.0.206	intra.lvi.co.jp	Default	ICMP Ping	Default	30		2025-10-27 13:36:49.003
OK	10.0.0.222	PA-VM	Default	ICMP Ping	Default	30		2025-10-27 13:36:56.020
OK	10.0.0.225	A10vThunder	Default	ICMP Ping	Default	30		2025-10-27 13:36:37.066
OK	10.0.0.227	aaaa	Default	ICMP Ping	Default	30		2025-10-27 13:36:40.057
OK	10.0.0.229	lvi.infoblox.local	Default	ICMP Ping	Default	30		2025-10-27 13:36:39.025
OK	192.168.0.254	lvi-gw-l3	Default	Interface Stats (HighSpeed)	<None>	60		2025-10-27 13:36:58.081

This report works by checking if there is any data saved within the last polling period for the device. For example, an ICMP monitor with a polling period of 30 seconds is expected to have at least some data persisted every 30 seconds. For the purposes of this report, a "No Response" data point is still considered sufficient to be considered healthy. The purpose of this report is not to determine the health of the devices themselves, but rather that the ThirdEye monitoring sub-systems are running properly.

Data for *push monitors* like **SNMP Trap** and **Agent-D syslog** are not included. These monitors do not run on any regular schedule so the logic used by this report to determine health of the monitor is not applicable.

If there are no devices found based on the search criteria or if there are no applicable monitors in any of the selected devices, the report will be empty. In the case of an empty report, no email will be sent.

28.1.1 Columns

The following columns are included in the output of the **Monitor Health Report**:

Status
The health of the **Monitor**

Paused
The **Monitor** associated with the device is in the manual **Paused** state.

Maintenance Window
A Maintenance Window is active for this device, so no data is being collected.

Never
No data has ever been captured for this monitor.

Delayed
There appears to be a delay or the monitoring is not running normally.

OK Monitoring is running normally.

IP Address
The **IP Address** of the monitored device.

Managed Network
The **Managed Network** that the monitored device is in.

Monitor
The name of the **Monitor**

Monitor Set
The name of the **Monitor Set** that this **Monitor** is a member of (or `<None>` if it is not in a **Monitor Set**)

Period
The time in seconds that this **Monitor** is configured to collect data.

Delay
In the case that the **Monitor** is not `OK`, this column will show the amount of seconds since the last collection attempt.

Last Captured
The last time that **Monitor** executed. This includes both successful and unsuccessful collection attempts.

SECTION 29

SMART CHANGE

Suite

Smart Change is LogicVein’s template-based automation solution for network device management that eliminates repetitive manual configuration.

With Smart Change you can:

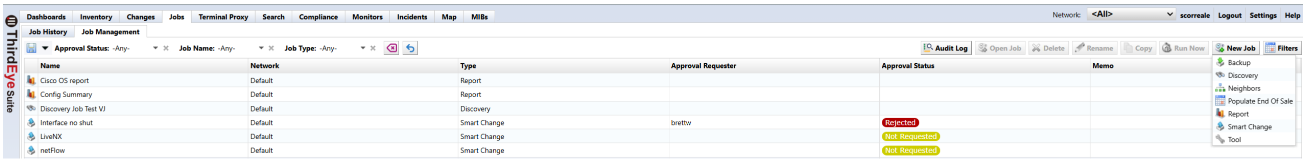
- Creates reusable command templates with variables
- Perform batch execution with different values per device in single job
- Integrate Excel for bulk value imports/exports
- Customize execution parameters through template interface

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.

29.1 Create a Smart Change Job

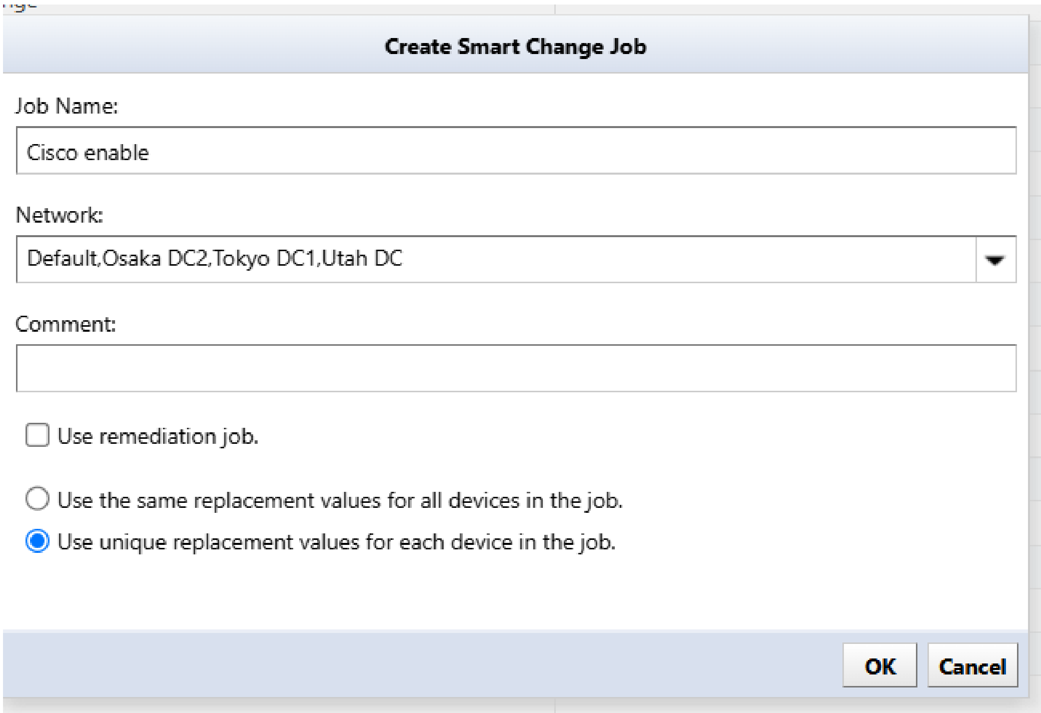
1. Click the [Jobs] main tab > [Job Management] subtab > [New Job] > [Smart Change].



Approval Status: -Any- Job Name: -Any- Job Type: -Any-

Name	Network	Type	Approval Requester	Approval Status	Memo
Cisco OS report	Default	Report			
Config Summary	Default	Report			
Discovery Job Test VJ	Default	Discovery			
Interface no shut	Default	Smart Change	brettw	Rejected	
LiveNX	Default	Smart Change		Not Requested	
netFlow	Default	Smart Change		Not Requested	

2. Enter the job name and comment, select the function, and click [OK].



Create Smart Change Job

Job Name: Cisco enable

Network: Default,Osaka DC2,Tokyo DC1,Utah DC

Comment:

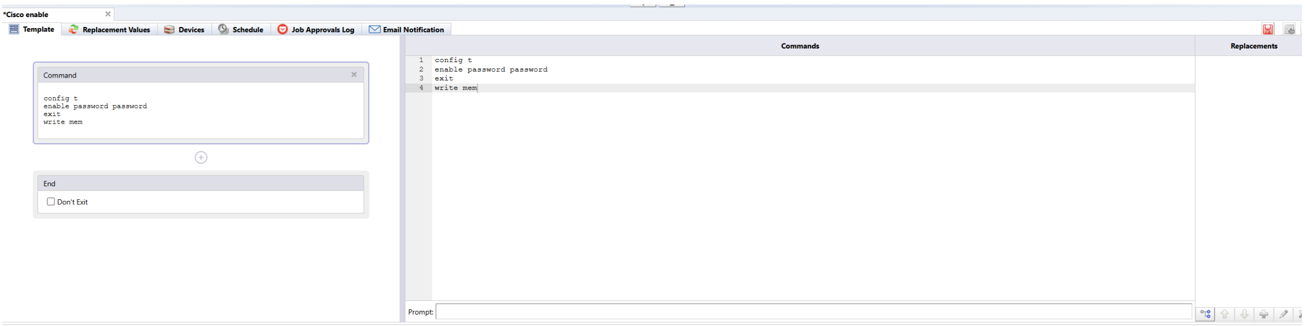
□ Use remediation job.

○ Use the same replacement values for all devices in the job.

● Use unique replacement values for each device in the job.

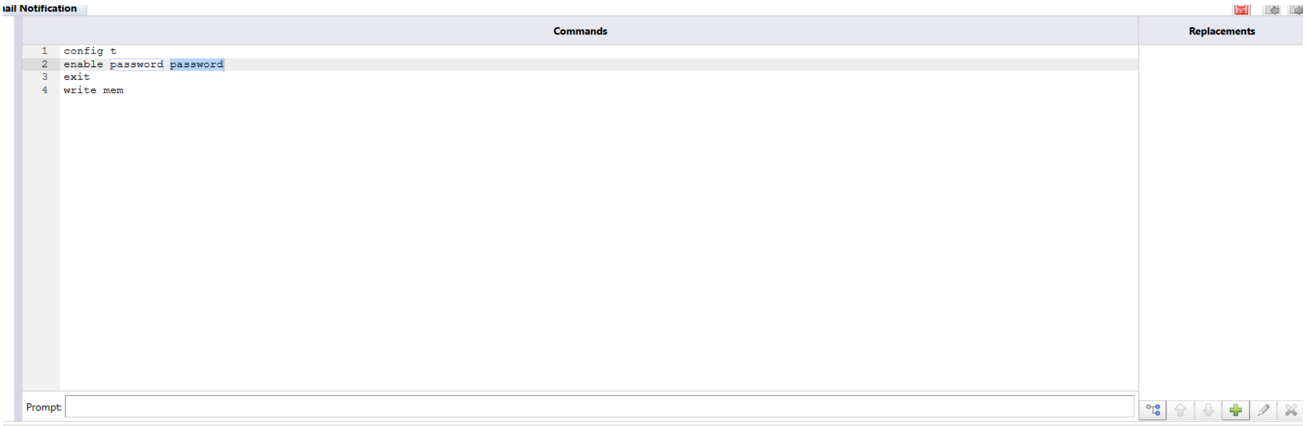
Item	Explanation
Job name	Enter the name of the Smart Change job.
Comment	Enter a comment (description) for the Smart Change job.
Use remediation job	Select whether to use Smart Change jobs as repair jobs. If selected, additionally select an adapter.
Use the same replacement values for all devices in 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.



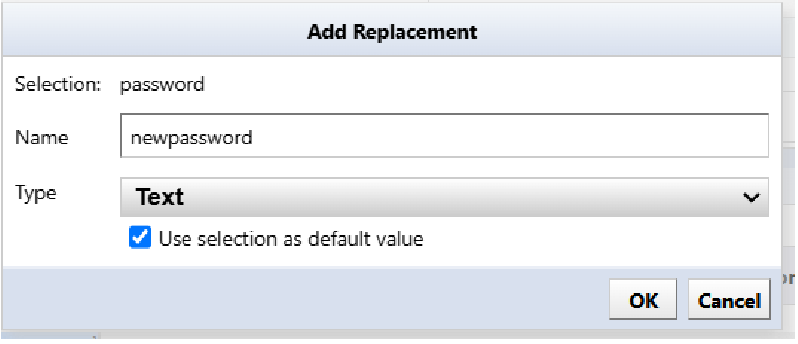
```
config t
enable password password
exit
write mem
```

4. Select the part you want to change as an alternative value, click the + button.



```
config t
enable password password
exit
write mem
```

5. Enter a name for the alternative value and select a type.



Add Replacement

Selection: password

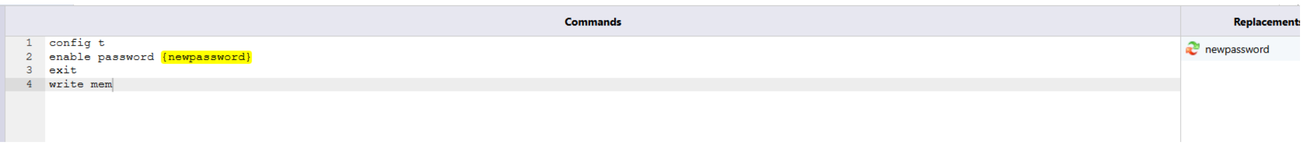
Name: newpassword

Type: Text

☑ Use selection as default value

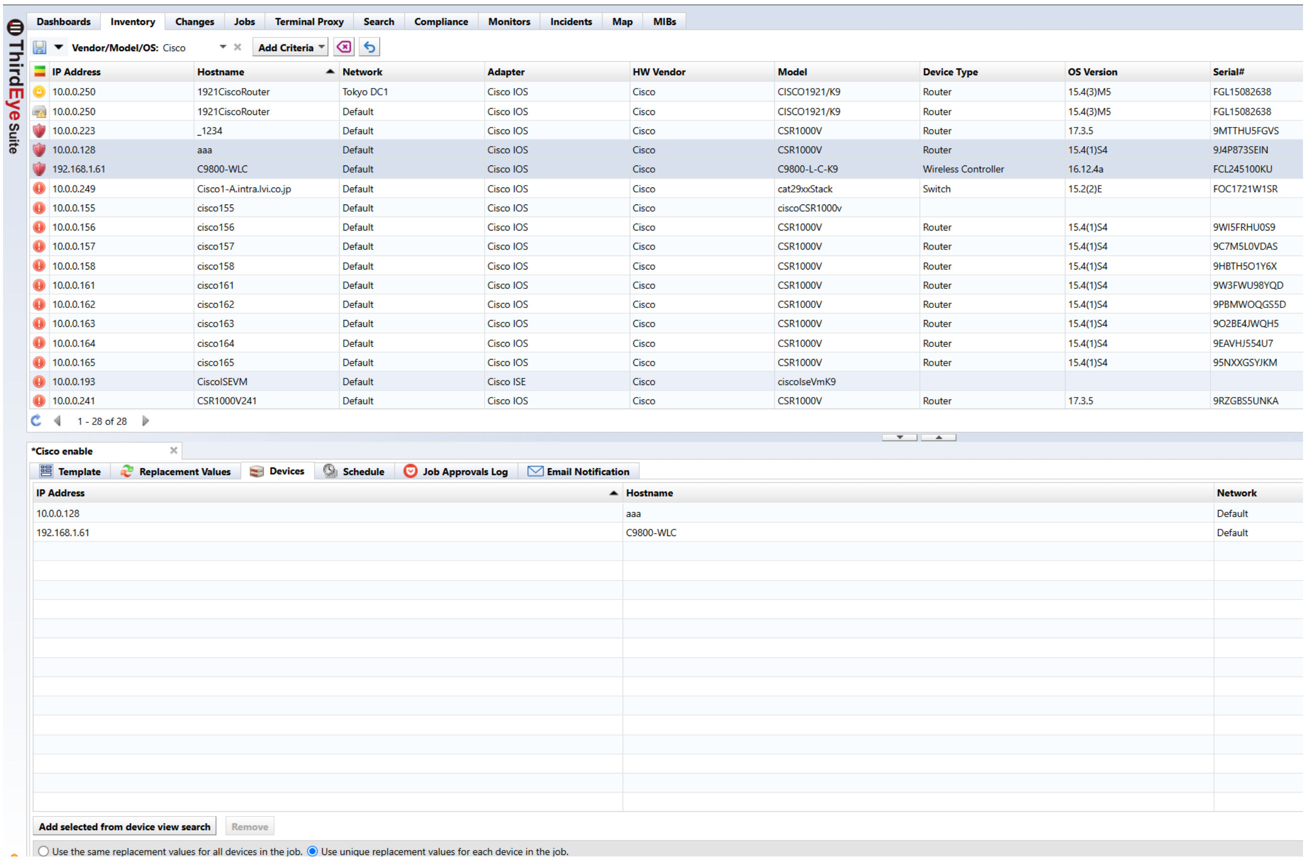
Item	Explanation
Text	Any text
IP address	IP address. If a value other than the correct IPv4 or IPv6 format is entered, an error will be reported.
Hostname	Hostname
IP address or hostname	IP address or host name
Choice	When entering an alternative value, you will be able to select it from a drop-down 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.



```
config t
enable password {newpassword}
exit
write mem
```

Add the device you want to run in the [Inventory] main tab Editor at the bottom of the window.



Vendor/Model/OS: Cisco

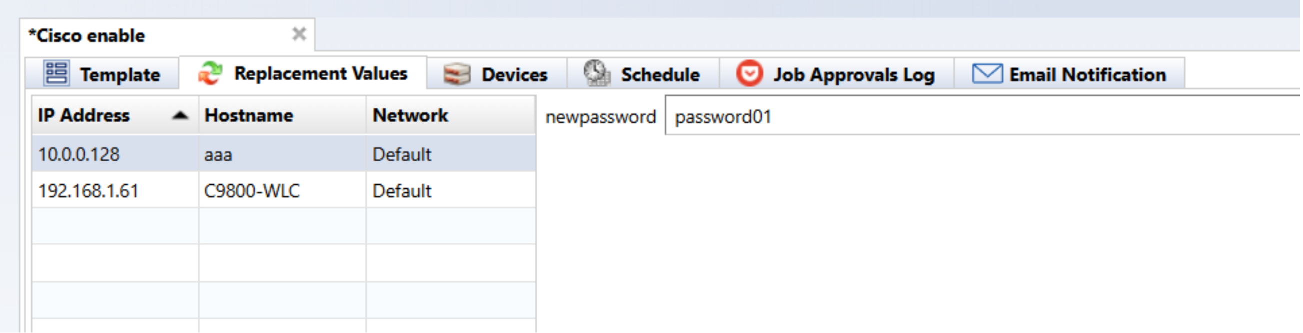
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#
10.0.0.250	1921CiscoRouter	Tokyo DC1	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638
10.0.0.223	_1234	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS
10.0.0.128	aaa	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN
192.168.1.61	C9800-WLC	Default	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU
10.0.0.249	Cisco1-A.intra.lvi.co.jp	Default	Cisco IOS	Cisco	cat29xxStack	Switch	15.2(2)E	FOC1721W1SR
10.0.0.155	cisco155	Default	Cisco IOS	Cisco	ciscoCSR1000v			
10.0.0.156	cisco156	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9WI5FRHU0S9
10.0.0.157	cisco157	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9C7M5L0VDAS
10.0.0.158	cisco158	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9HBTH5O1Y6X
10.0.0.161	cisco161	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W3FWU98YQD
10.0.0.162	cisco162	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9PBMWOQGS5D
10.0.0.163	cisco163	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9O2BE4JWQH5
10.0.0.164	cisco164	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9EAVHJ554U7
10.0.0.165	cisco165	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	95NXXGSYJKM
10.0.0.193	CiscoISEVM	Default	Cisco ISE	Cisco	ciscoIseVmK9			
10.0.0.241	CSR1000V241	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9RZGBS5UNKA

*Cisco enable

IP Address	Hostname	Network
10.0.0.128	aaa	Default
192.168.1.61	C9800-WLC	Default

○ Use the same replacement values for all devices in the job. ● Use unique replacement values for each device in the job.

6. Click the Editor's [Replacement Values] tab and enter the values.



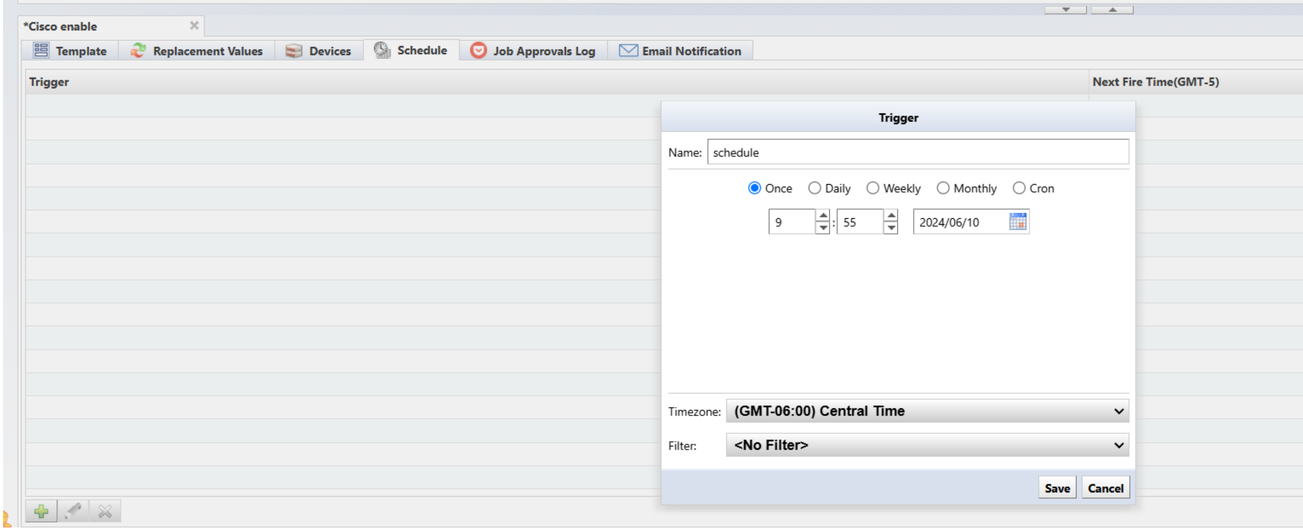
*Cisco enable

IP Address	Hostname	Network
10.0.0.128	aaa	Default
192.168.1.61	C9800-WLC	Default

newpassword password01

Alternative data can be can be imported/exported via Excel file using the (export) or (import) buttons.

7. On the Editor’s [Schedule] tab, click the ➕ button in the lower lefthand corner of the window to add Triggers.



Trigger

Name: schedule

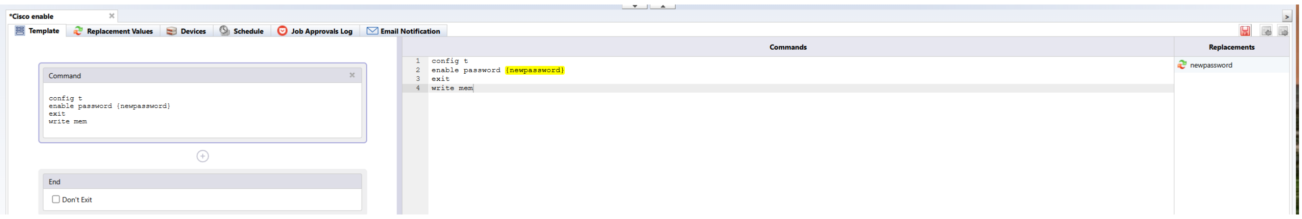
● Once ○ Daily ○ Weekly ○ Monthly ○ Cron

9 : 55 2024/06/10

Timezone: (GMT-06:00) Central Time

Filter: <No Filter>

8. Click the 💾 button to save the job.



```
config t
enable password {newpassword}
exit
write mem
```

□ Don't Exit

```
config t
enable password {newpassword}
exit
write mem
```

newpassword

SECTION 30

PLAYBOOKS

Suite

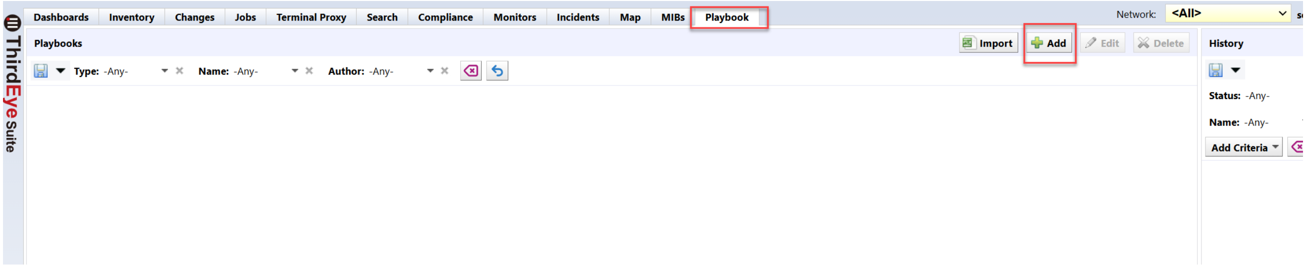
Playbooks are visual automation workflows that orchestrate complex network operations through conditional logic and multi-step processes. They combine device commands, data analysis, and decision nodes to create intelligent automation sequences. With Playbooks you can:

- Execute corrective configurations based on real-time device outputs
- Trigger alerts/notifications when specific conditions are detected
- Initialize backup processes before making critical changes

Playbooks are composed of interconnected Nodes. Each Node performs a specific network operation task, with connections defining the execution flow path.

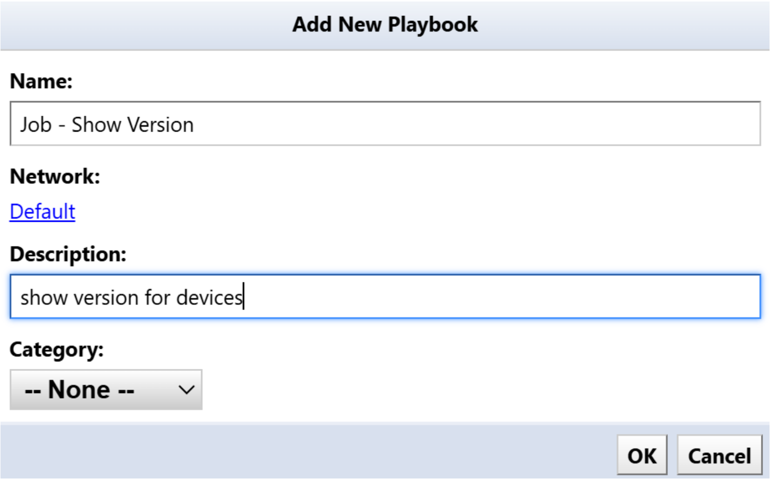
30.1 Add New Playbook

1. Click on the [Playbook] main tab.
2. Click on the Add button.



Type: -Any-
Name: -Any-
Author: -Any-
Status: -Any-
Name: -Any-

3. In the [Add New Playbook] popup window, enter the “Name” of the job, and a corresponding “Description”.
4. Click [OK].



Add New Playbook

Name:

Job - Show Version

Network:

Default

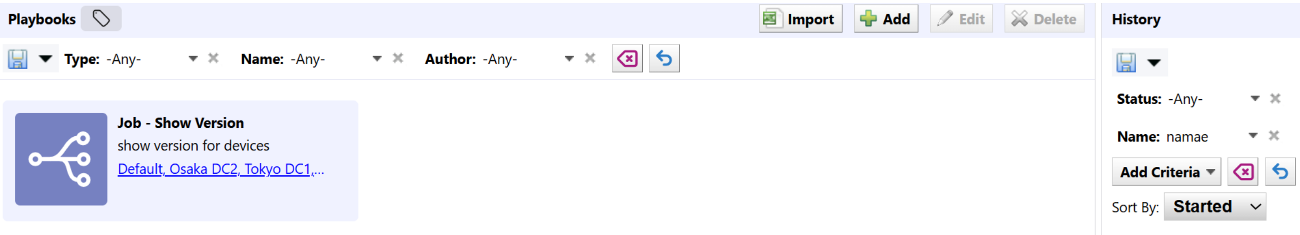
Description:

show version for devices

Category:

-- None --

The new Playbook will be visible in the Playbook Field.



Type: -Any-

Name: -Any-

Author: -Any-

Job - Show Version

show version for devices

Default, Osaka DC2, Tokyo DC1,...

Status: -Any-

Name: namae

Sort By: Started

30.2 Create Playbook

To create a Playbook:

1. Click on the [Playbook] main tab.
2. Doubleclick your new Playbook.

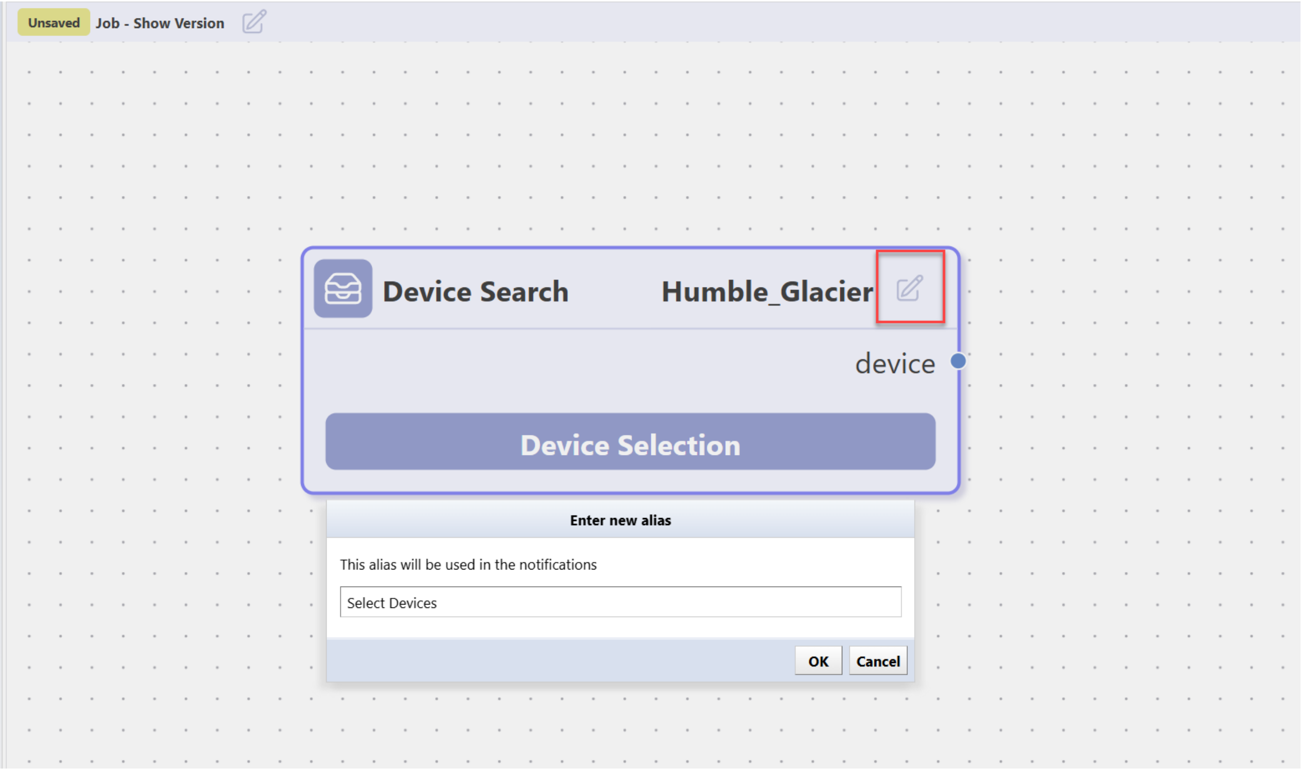
The [Node] panel will appear on the right side of the screen.

3. Click and hold a Node from the [Node] panel on the right side of the window, and drag it to the Playbook Field.

30.3 Nodes

Nodes are individual components that perform specific tasks, such as device communication, data processing, or conditional logic. They can be visually connected to create complex operational sequences called Playbooks.

Once a Node is in the Playbook Field, click the ✎ button in the top right corner of the node to change the descriptive Alias of the Node.



This alias will be used in the notifications

Select Devices

30.3.1 Node List

The [Node] panel is on the right side of the screen. These are the different options to configure a job to run.

Node Option	Explanation
And	Only proceed after both inputs have received a signal
Backup Device	Run a device backup
Chat App (Webhook)	Webhook to send messages to either Teams/Slack/Mattermost/Webex/Line/PagerDuty
Compliance Remediation	Get information from a Compliance Rule Set configured to run this playbook
Merge by Device	Combine to a single output per device
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
Load Configuration	Set Adapter and Configuration
Memo	Save a note
Raise Compliance Violation	Set severity of Violations, and add error message
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	Set or update variables before forwarding input
Set Variables	Schedule this playbook to run automatically
Sleep	Delay for a number of milliseconds before forwarding input
SSH Exec	Execute a command on remote SSH host
To CSV	Serialize data to CSV string
To Json	Serialize data to JSON string
Upload File	Send a file to your devices

30.3.2 Node Types by Position

Nodes are classified into “Start”, “Middle”, and “Terminal” based on their input/output terminals:

Start Nodes (Initiate processes)

- **Device Search:** Selects devices from inventory
- **Compliance Remediation:** Triggers on policy violations
- **Incident:** Starts with alert policy triggers
- **Schedule:** Time-based activation

Middle Nodes (Process data/decisions)

- **And Gate:** Requires multiple input conditions
- **Regex Match:** Filters text outputs
- **Run Code:** Executes Python/JS scripts
- **Run Code With Automatic Retry:** Run a block of code on your device a number of times or until it is successful
- **Ruleset:** Run a ruleset against the output of a node
- **Set variables:** Set or update variables before forwarding input
- **Merge by Device:** Combines device data streams
- **Sleep:** Adds timed delays (1s-24h)
- **SSH Exec:** Runs CLI commands
- **Load Configuration:** Device configuration deployment mechanism. It is often followed by verification nodes
- **Backup Device:** Run a device backup Set Variables
- **To CSV:** Serialize data to CSV string
- **To Json:** Serialize data to JSON string
- **Upload File:** Send a file to your devices

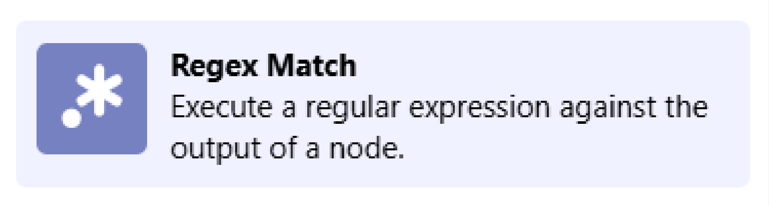
Terminal Nodes (Final outputs)

- **Email Notification:** Sends SMTP alerts
- **Chat Webhook:** Posts to Teams/Slack
- **Raise Compliance Violation:** Sends Compliance Violation notifications

Note

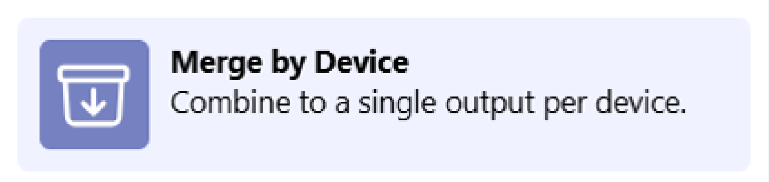
There have been recent changes to the Nodes side panel:

- The icon for the [Regex Match], Node has been updated:



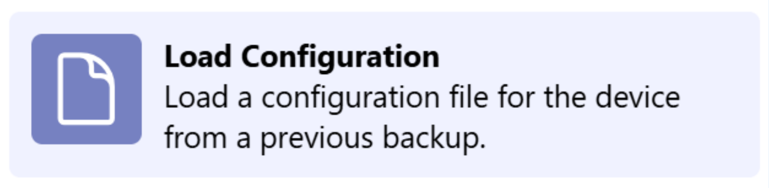
Regex Match
Execute a regular expression against the output of a node.

- A new node, [Merge by Device], has been added:



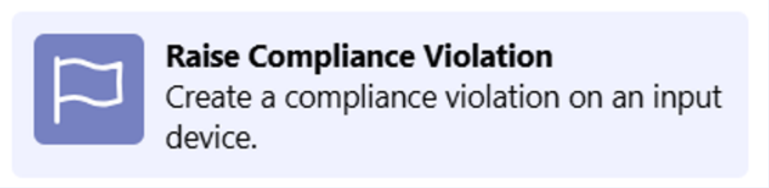
Merge by Device
Combine to a single output per device.

- A new node, [Load Configuration], has been added:



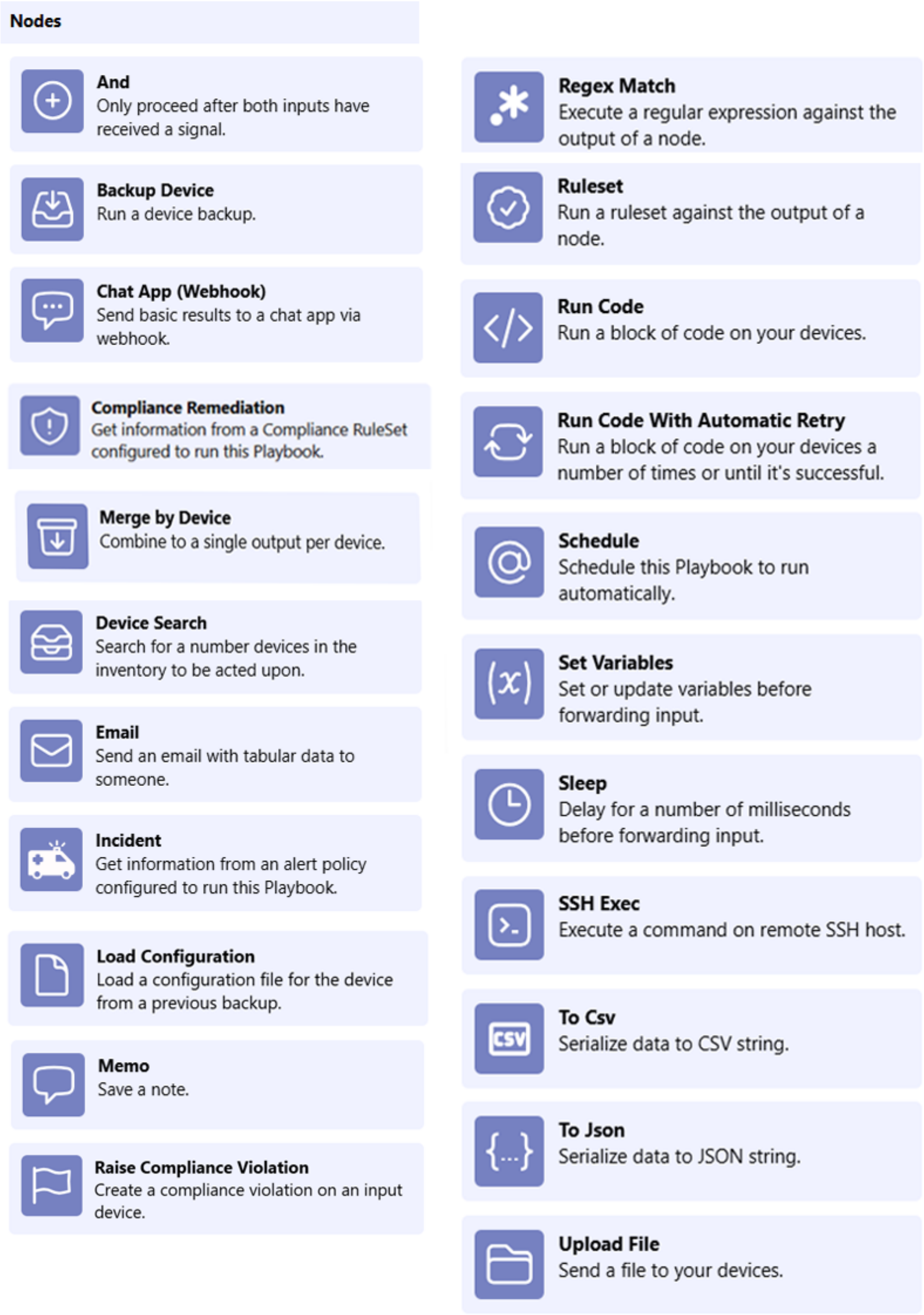
Load Configuration
Load a configuration file for the device from a previous backup.

- A new node, [Raise Compliance Violation], has been added:



Raise Compliance Violation
Create a compliance violation on an input device.

This is the full list of current nodes. More will be added in future releases.



Nodes

And
Only proceed after both inputs have received a signal.

Backup Device
Run a device backup.

Chat App (Webhook)
Send basic results to a chat app via webhook.

Compliance Remediation
Get information from a Compliance RuleSet configured to run this Playbook.

Merge by Device
Combine to a single output per device.

Device Search
Search for a number devices in the inventory to be acted upon.

Email
Send an email with tabular data to someone.

Incident
Get information from an alert policy configured to run this Playbook.

Load Configuration
Load a configuration file for the device from a previous backup.

Memo
Save a note.

Raise Compliance Violation
Create a compliance violation on an input device.

Regex Match
Execute a regular expression against the output of a node.

Ruleset
Run a ruleset 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's successful.

Schedule
Schedule this Playbook to run automatically.

Set Variables
Set or update variables before forwarding input.

Sleep
Delay for a number of milliseconds before forwarding input.

SSH Exec
Execute a command on remote SSH host.

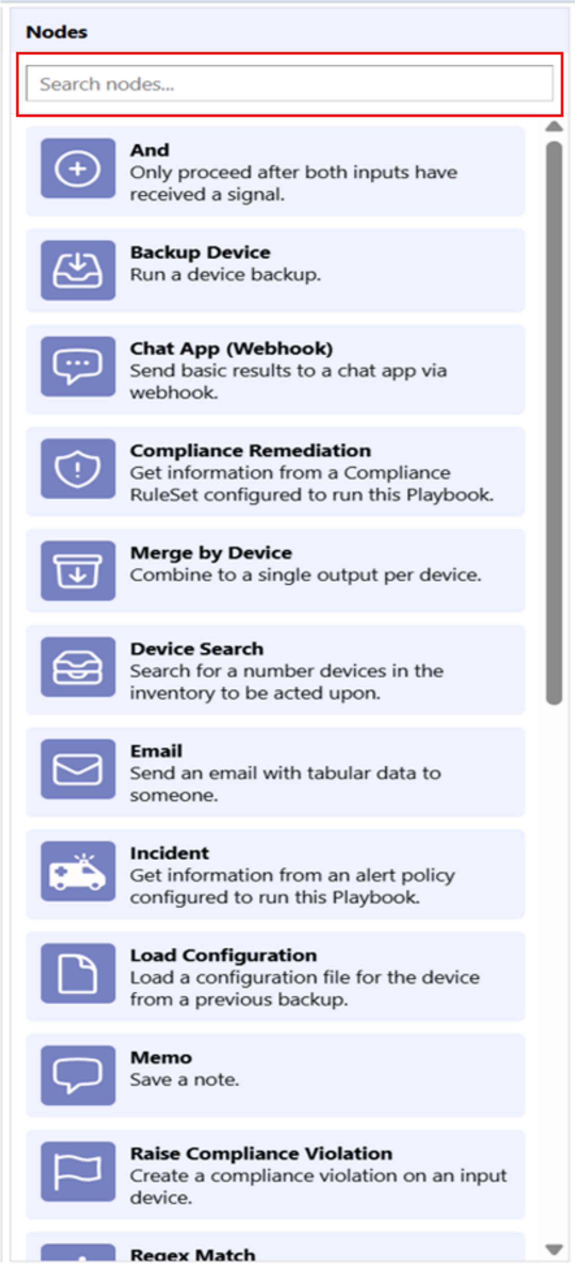
To Csv
Serialize data to CSV string.

To Json
Serialize data to JSON string.

Upload File
Send a file to your devices.

30.3.3 Node Search

You can search for Nodes that you want to add by name, or filter the Nodes that are visible in the Nodes list by using the Nodes Search function at the top of the right sidepanel.



Nodes

Search nodes...

And
Only proceed after both inputs have received a signal.

Backup Device
Run a device backup.

Chat App (Webhook)
Send basic results to a chat app via webhook.

Compliance Remediation
Get information from a Compliance RuleSet configured to run this Playbook.

Merge by Device
Combine to a single output per device.

Device Search
Search for a number devices in the inventory to be acted upon.

Email
Send an email with tabular data to someone.

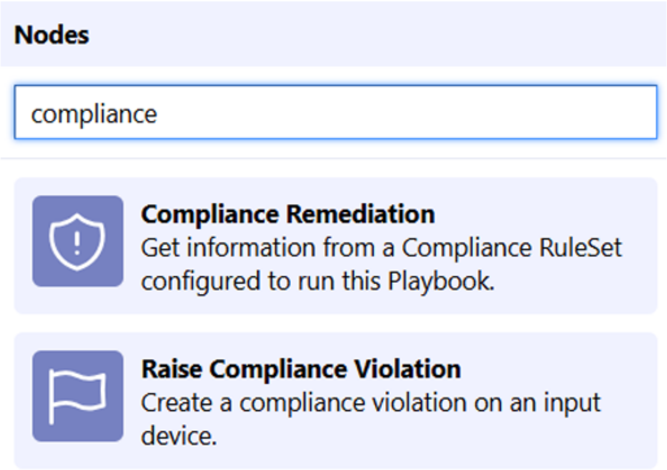
Incident
Get information from an alert policy configured to run this Playbook.

Load Configuration
Load a configuration file for the device from a previous backup.

Memo
Save a note.

Raise Compliance Violation
Create a compliance violation on an input device.

Regex Match



Nodes

compliance

Compliance Remediation
Get information from a Compliance RuleSet configured to run this Playbook.

Raise Compliance Violation
Create a compliance violation on an input device.

30.3.4 Add Node

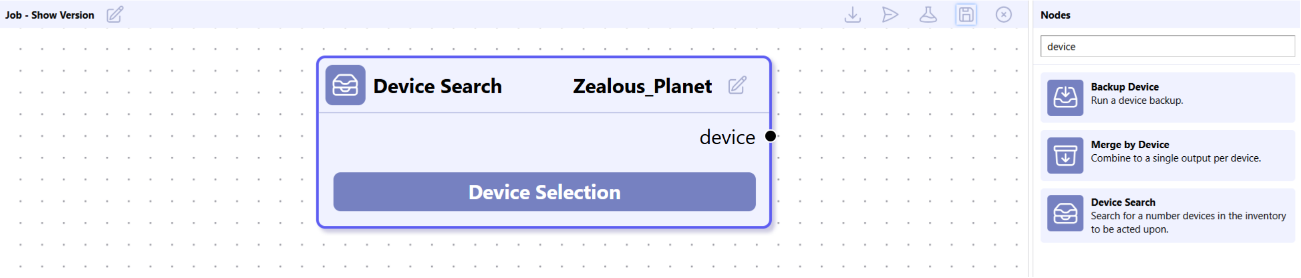
To add a Node:

1. Click the [Playbook] main tab.
2. Doubleclick the Playbook to which the Node will be added.
3. Click and drag a Node from the Node list in the righthand panel, to the Playbook Field.

30.3.5 Select Device

To select a device:

1. Click the [Playbook] main tab.
2. Create or open a Playbook.
3. Add a “Device Search” Node to you workflow from the Node list on the right side of the window.
4. On the “Device Search” Node, click [Device Selection].



Job - Show Version

Device Search Zealous_Planet

device

Device Selection

Nodes

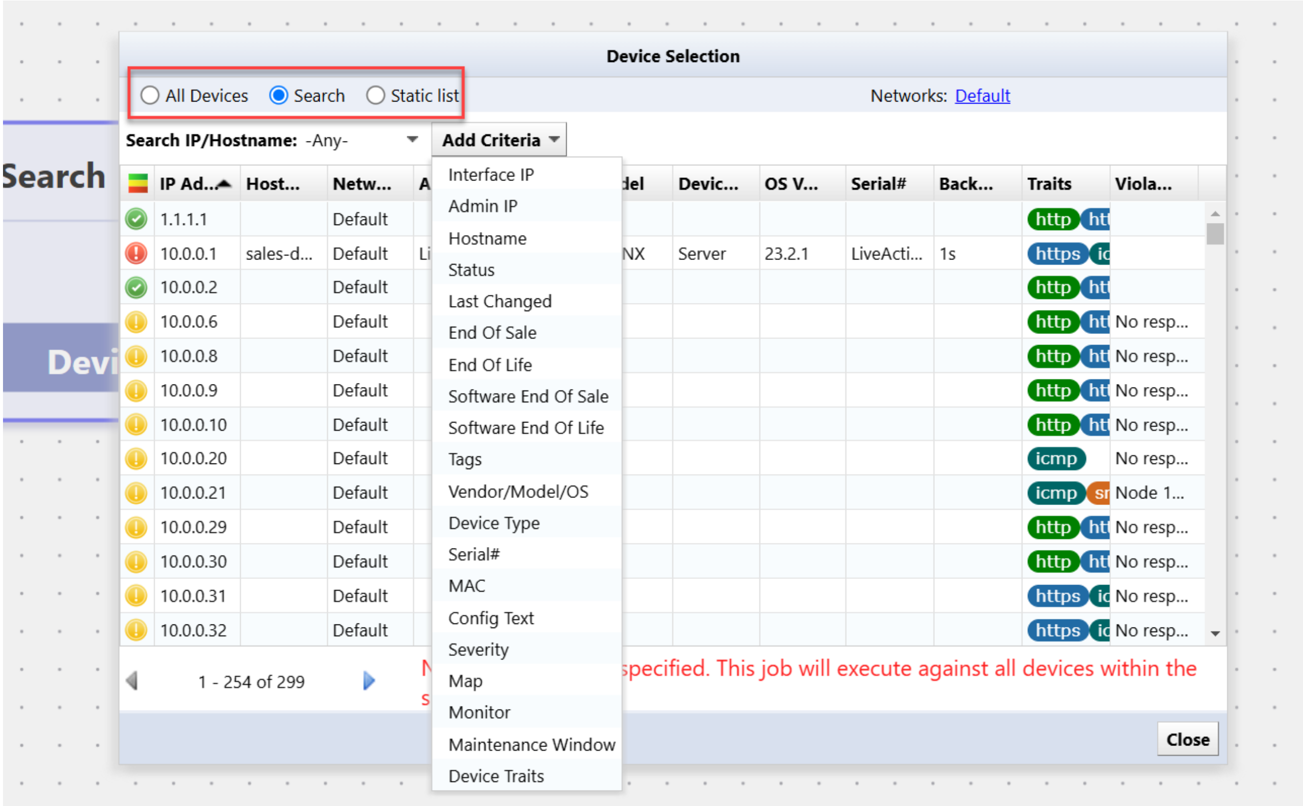
device

Backup Device
Run a device backup.

Merge by Device
Combine to a single output per device.

Device Search
Search for a number devices in the inventory to be acted upon.

There are three options in the [Device Selection] window:



Device Selection

○ All Devices ● Search ○ Static list

Networks: Default

Search IP/Hostname: -Any-

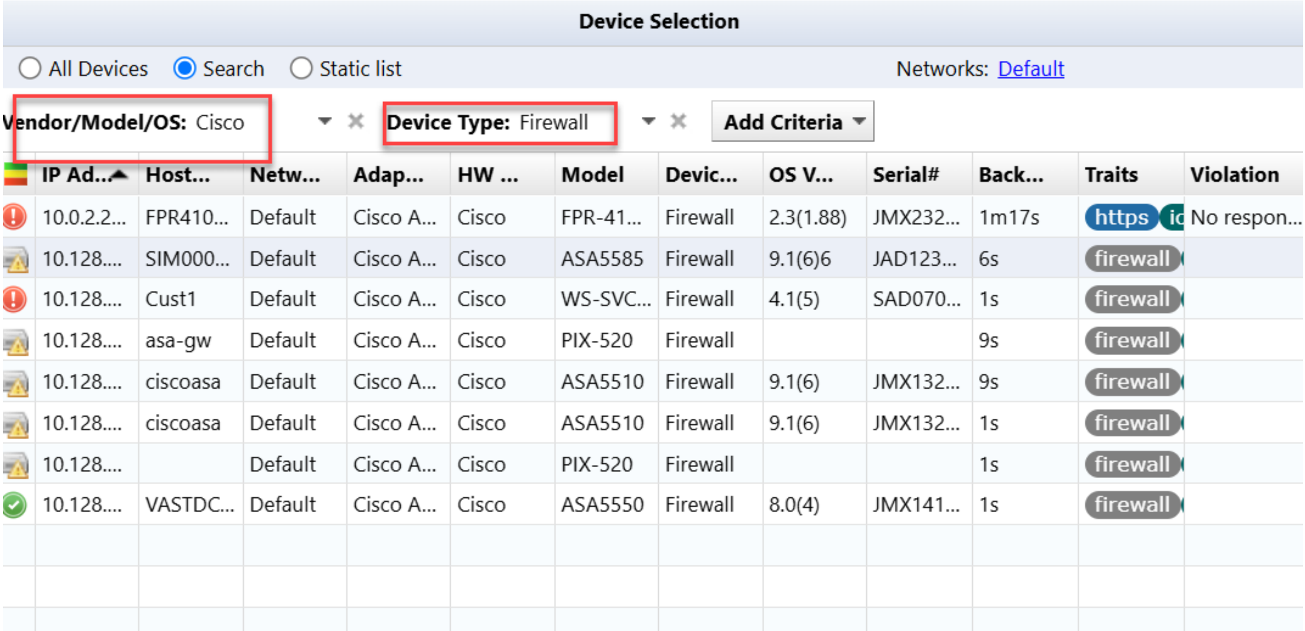
	IP Ad...	Host...	Netw...	A	del	Devic...	OS V...	Serial#	Back...	Traits	Viola...
✓	1.1.1.1		Default							http ht	
!	10.0.0.1	sales-d...	Default	Li	NX	Server	23.2.1	LiveActi...	1s	https ic	
✓	10.0.0.2		Default							http ht	
!	10.0.0.6		Default							http ht	No resp...
!	10.0.0.8		Default							http ht	No resp...
!	10.0.0.9		Default							http ht	No resp...
!	10.0.0.10		Default							http ht	No resp...
!	10.0.0.20		Default							icmp	No resp...
!	10.0.0.21		Default							icmp sr	Node 1...
!	10.0.0.29		Default							http ht	No resp...
!	10.0.0.30		Default							http ht	No resp...
!	10.0.0.31		Default							https ic	No resp...
!	10.0.0.32		Default							https ic	No resp...

1 - 254 of 299

N specified. This job will execute against all devices within the
s

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

Selecting “Search” allows you to narrow your search using multiple criteria.



Device Selection

○ All Devices ● Search ○ Static list Networks: Default

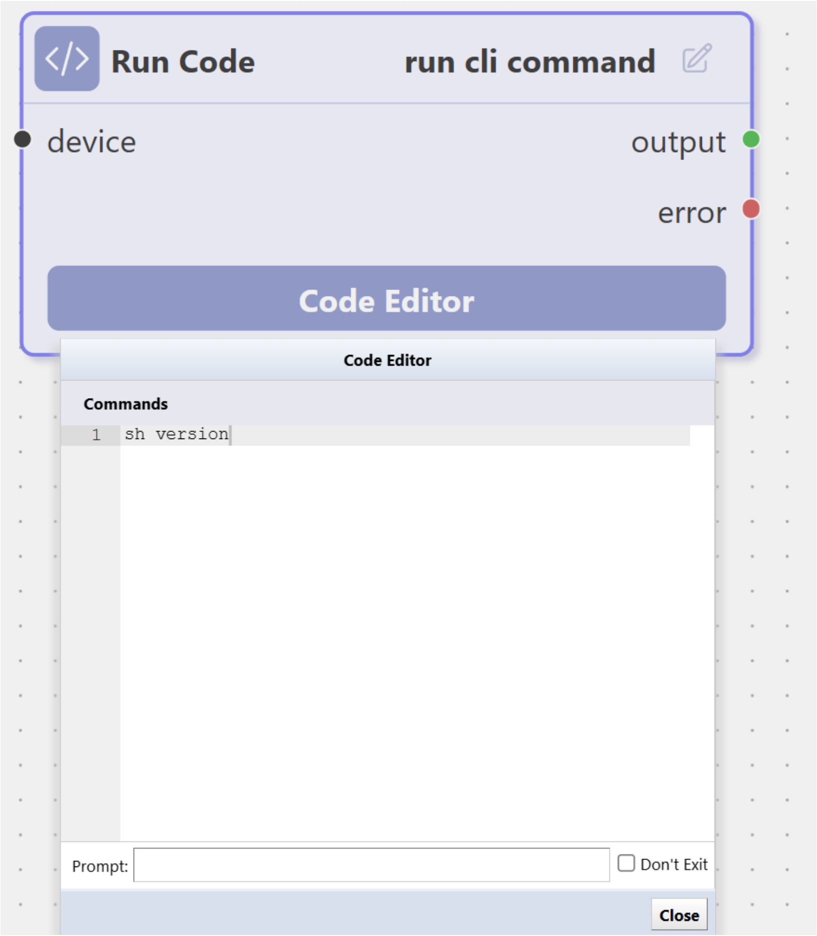
Vendor/Model/OS: Cisco Device Type: Firewall

	IP Ad...	Host...	Netw...	Adap...	HW ...	Model	Devic...	OS V...	Serial#	Back...	Traits	Violation
!	10.0.2.2...	FPR410...	Default	Cisco A...	Cisco	FPR-41...	Firewall	2.3(1.88)	JMX232...	1m17s	https id	No respon...
⚠	10.128....	SIM000...	Default	Cisco A...	Cisco	ASA5585	Firewall	9.1(6)6	JAD123...	6s	firewall	
!	10.128....	Cust1	Default	Cisco A...	Cisco	WS-SVC...	Firewall	4.1(5)	SAD070...	1s	firewall	
⚠	10.128....	asa-gw	Default	Cisco A...	Cisco	PIX-520	Firewall			9s	firewall	
⚠	10.128....	ciscoasa	Default	Cisco A...	Cisco	ASA5510	Firewall	9.1(6)	JMX132...	9s	firewall	
⚠	10.128....	ciscoasa	Default	Cisco A...	Cisco	ASA5510	Firewall	9.1(6)	JMX132...	1s	firewall	
⚠	10.128....		Default	Cisco A...	Cisco	PIX-520	Firewall			1s	firewall	
✓	10.128....	VASTDC...	Default	Cisco A...	Cisco	ASA5550	Firewall	8.0(4)	JMX141...	1s	firewall	

30.3.6 Run Code

To run code on a device:

1. Add a “Run Code” Node to you workflow from the Node list on the right side of the window.
2. Click the [Code Editor] button.
3. Enter a `cli` command for the devices you have selected.

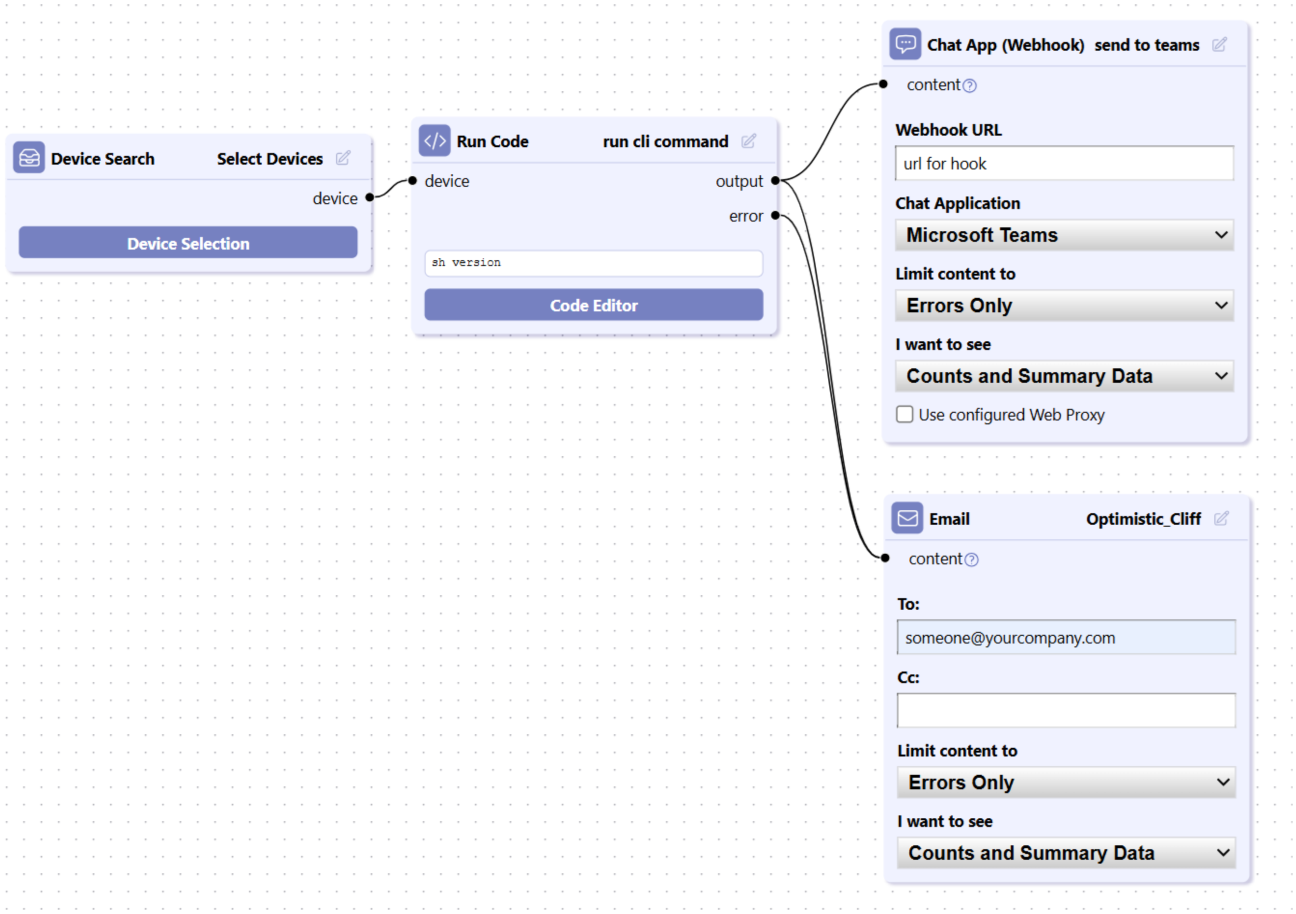


```
sh version
```

30.3.7 Raise Compliance Violation

The [Raise Compliance Violation] Node sends Compliance Violation notifications to users via four methods:

- Email
- Webhook to Teams/Slack/Webex/Line/PagerDuty
- Both email and Webhook
- Notifications in ThirdEye's [Inventory] main tab > Editor [Compliance] tab.



```
sh version
```

Webhook URL
url for hook

Chat Application
Microsoft Teams

Limit content to
Errors Only

I want to see
Counts and Summary Data

□ Use configured Web Proxy

To:
someone@yourcompany.com

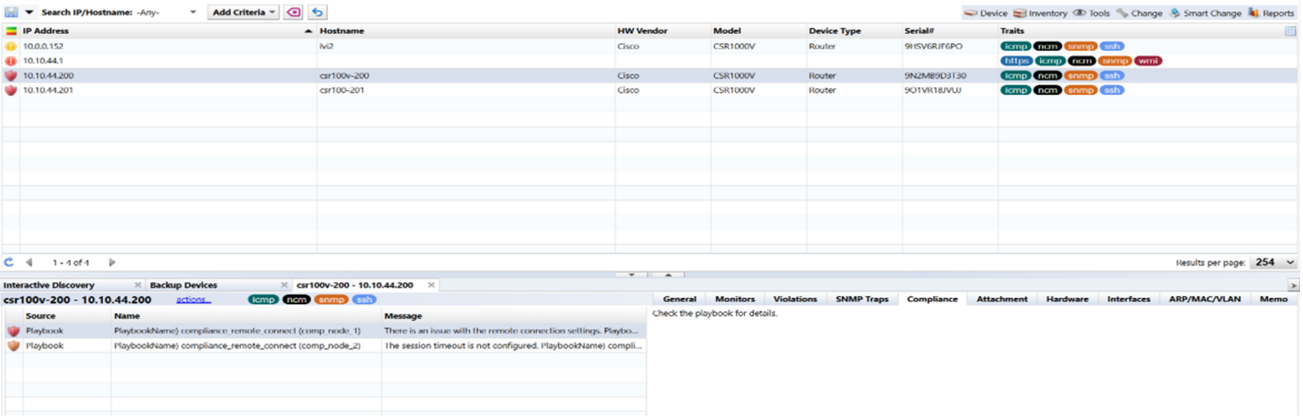
Cc:

Limit content to
Errors Only

I want to see
Counts and Summary Data

To view the details of the Violation in ThirdEye‘s [Compliance] tab:

1. Click the [Inventory] main tab.
2. Doubleclick the device to open the its Editor window at the bottom of the screen.
3. Click the Editor’s [Compliance] tab.



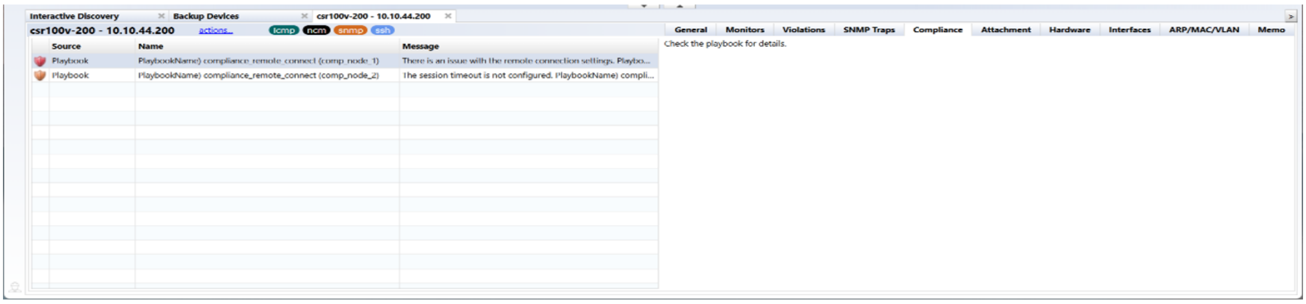
IP Address	Hostname	HW Vendor	Model	Device Type	Serial#	Traits
10.0.0.152	lvi2	Cisco	CSR1000V	Router	9HSV6RJF6PO	icmp ncm snmp ssh
10.10.44.1						https icmp ncm snmp wmi
10.10.44.200	csr100v-200	Cisco	CSR1000V	Router	9N2MB9D3T30	icmp ncm snmp ssh
10.10.44.201	csr100-201	Cisco	CSR1000V	Router	9O1VR18JVUJ	icmp ncm snmp ssh

csr100v-200 - 10.10.44.200 icmp ncm snmp ssh

Source	Name	Message
Playbook	PlaybookName) compliance_remote_connect (comp_node_1)	There is an issue with the remote connection settings. Playbo...
Playbook	PlaybookName) compliance_remote_connect (comp_node_2)	The session timeout is not configured. PlaybookName) compli...

Check the playbook for details.

The source of the Violation severity icon, Compliance Violation, Compliance Policy Name, and Violation message are displayed in the left sidepanel of the Editor.



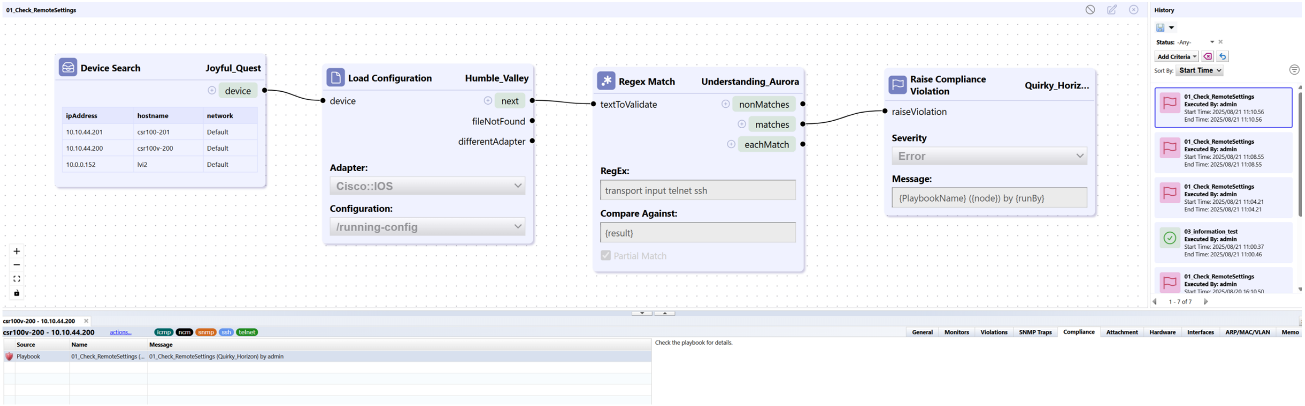
csr100v-200 - 10.10.44.200 icmp ncm snmp ssh

Source	Name	Message
Playbook	PlaybookName) compliance_remote_connect (comp_node_1)	There is an issue with the remote connection settings. Playbo...
Playbook	PlaybookName) compliance_remote_connect (comp_node_2)	The session timeout is not configured. PlaybookName) compli...

Check the playbook for details.

For more information about the Violation, you can click the [Playbook] main tab to check the Violation History.

The History is located in the right sidepanel.



ipAddress	hostname	network
10.10.44.201	csr100-201	Default
10.10.44.200	csr100v-200	Default
10.0.0.152	lvi2	Default

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:10.56
End Time: 2025/08/21 11:10.56

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:08.55
End Time: 2025/08/21 11:08.55

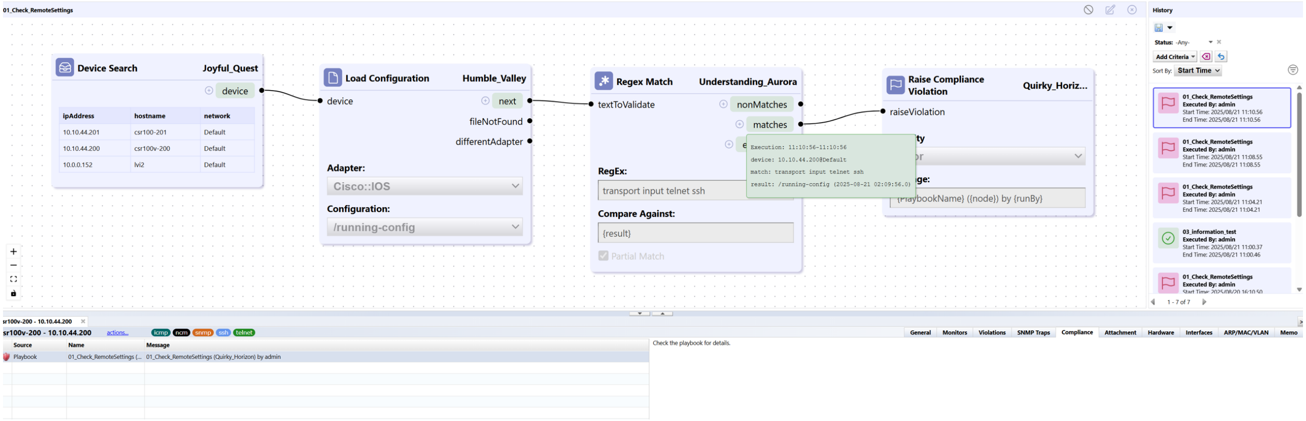
01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:04.21
End Time: 2025/08/21 11:04.21

03_information_test
Executed By: admin
Start Time: 2025/08/21 11:00.37
End Time: 2025/08/21 11:00.46

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/20 16:10.50

Source	Name	Message
Playbook	01_Check_RemoteSettings (...	01_Check_RemoteSettings (Quirky_Horizon) by admin

Check the playbook for details.



```
Execution: 11:10:56-11:10:56
device: 10.10.44.200@Default
match: transport input telnet ssh
result: /running-config (2025-08-21 02:09:56.0)
```

ipAddress	hostname	network
10.10.44.201	csr100-201	Default
10.10.44.200	csr100v-200	Default
10.0.0.152	lvi2	Default

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:10.56
End Time: 2025/08/21 11:10.56

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:08.55
End Time: 2025/08/21 11:08.55

01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/21 11:04.21
End Time: 2025/08/21 11:04.21

03_information_test
Executed By: admin
Start Time: 2025/08/21 11:00.37
End Time: 2025/08/21 11:00.46

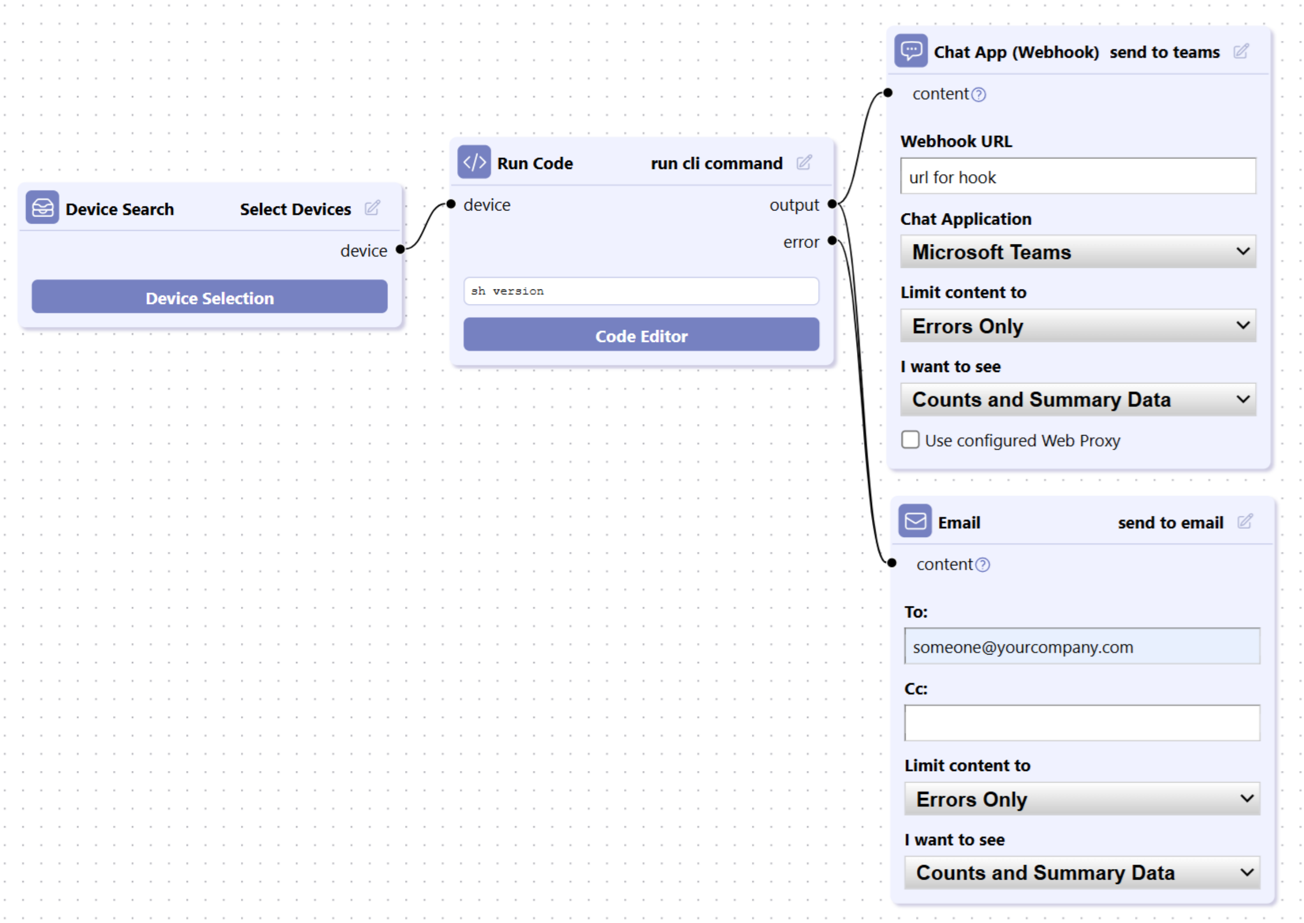
01_Check_RemoteSettings
Executed By: admin
Start Time: 2025/08/20 16:10.50

Source	Name	Message
Playbook	01_Check_RemoteSettings (...	01_Check_RemoteSettings (Quirky_Horizon) by admin

Check the playbook for details.

30.3.8 Connect Nodes

You can connect Nodes to create Playbook.



```
sh version
```

Webhook URL: url for hook

Chat Application: Microsoft Teams

Limit content to: Errors Only

I want to see: Counts and Summary Data

□ Use configured Web Proxy

To: someone@yourcompany.com

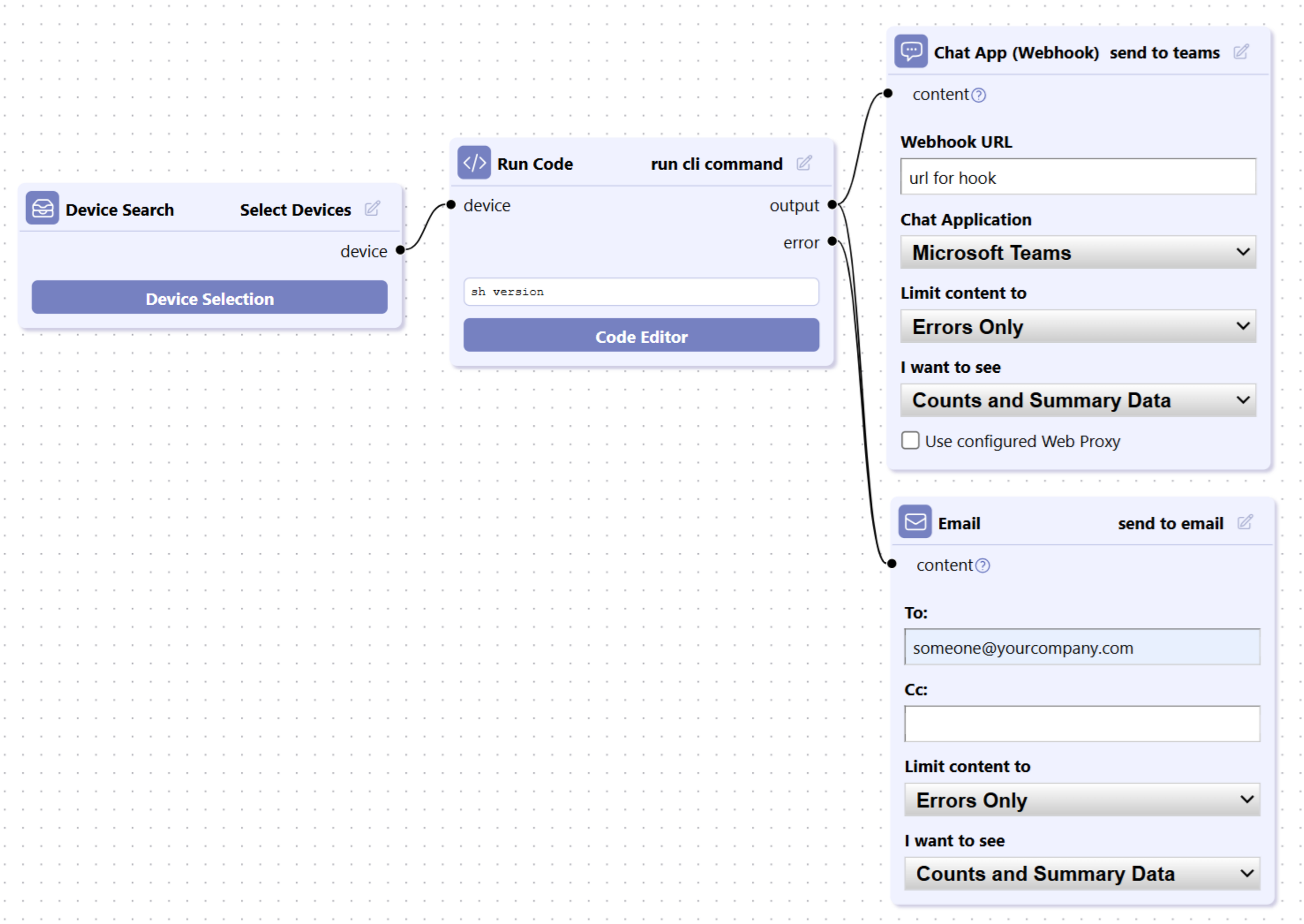
Cc:

Limit content to: Errors Only

I want to see: Counts and Summary Data

To connect nodes, click and drag from an output port (right side) of one Node, to an input port (left side) of another node.

Press [Backspace] on your keyboard to remove unwanted connections.



```
sh version
```

Webhook URL: url for hook

Chat Application: Microsoft Teams

Limit content to: Errors Only

I want to see: Counts and Summary Data

☐ Use configured Web Proxy

To: someone@yourcompany.com

Cc:

Limit content to: Errors Only

I want to see: Counts and Summary Data

30.3.9 Remove Nodes or Connection

To remove a node, or a connection, select the desired item, and click on [Backspace] on your keyboard.

30.4 Import Playbook

To import a Playbook:

1. Click the [Playbook] main tab.
2. Click the Import button in the menu bar at the top of the window.
3. Doubleclick the Playbook .json file you want to import.
4. The Playbook file will appear in the [Playbook] interface.

30.5 Export Playbook

To export a Playbook:

1. Click the [Playbook] main tab.
2. Doubleclick the [Playbook] you want to export.
3. Click the click the [Export] ⤓ button in the menu bar at the top of the window.
4. Download the Playbook as a .json file.
5. Click the [Close Playbook] ⊗ button in the menu bar at the top of the window.

30.6 Playbook Categories

The Playbook Category Feature introduces organizational improvements for Playbook management.

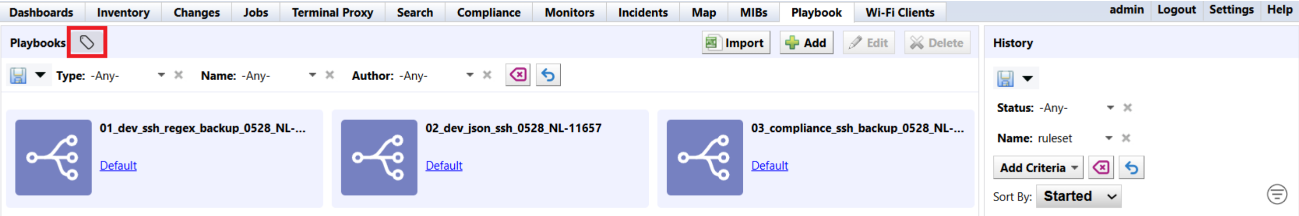
With Playbook Categories you can:

- Create and edit custom categories
- label using colored tags in Playbook lists
- Create multiple categories within one playbook

30.7 Create Playbook Category

To create a Playbook Category:

1. Click the [Playbook] main tab.
2. Click the 🏷 button next to the “Playbook” main tab title to open the [Categories] window.



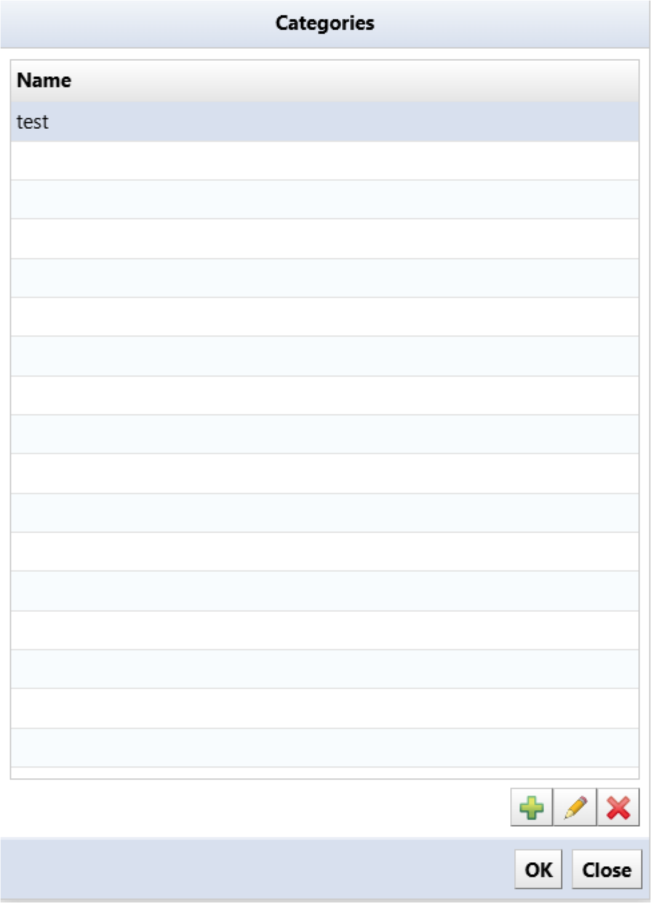
Type: -Any-
Name: -Any-
Author: -Any-

01_dev_ssh_regex_backup_0528_NL-...
Default

02_dev_json_ssh_0528_NL-11657
Default

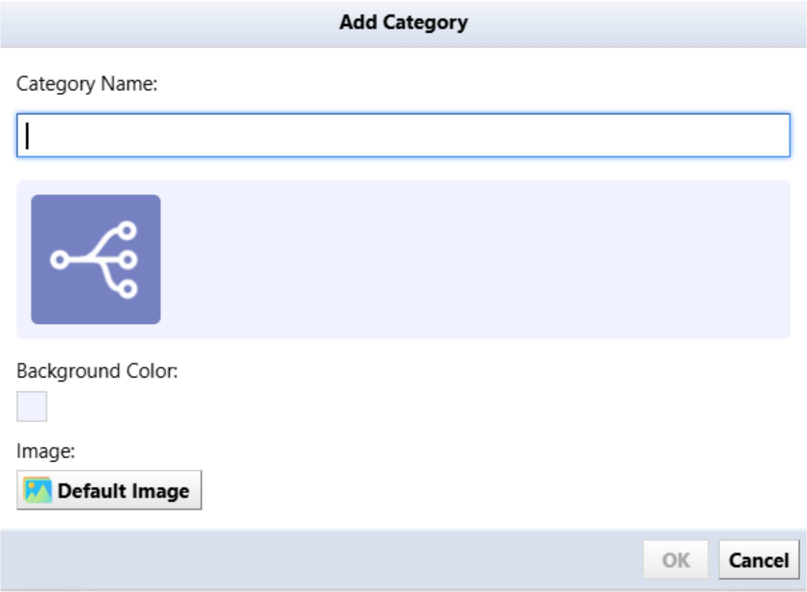
03_compliance_ssh_backup_0528_NL-...
Default

Status: -Any-
Name: ruleset
Sort By: Started

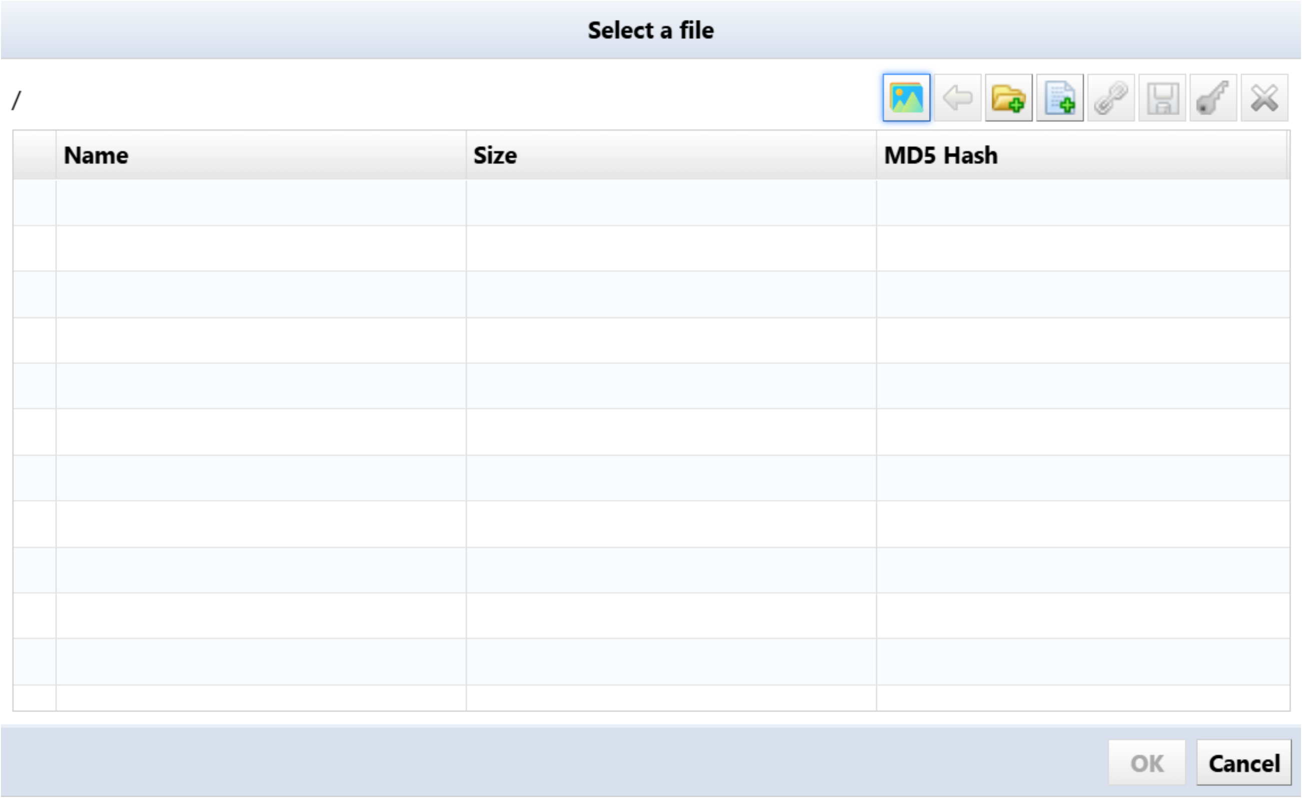


Name
test

3. Click the ➕ button to open the [Add Category] window.



4. Click the **Default Image** button to select a .svg image for the Category.

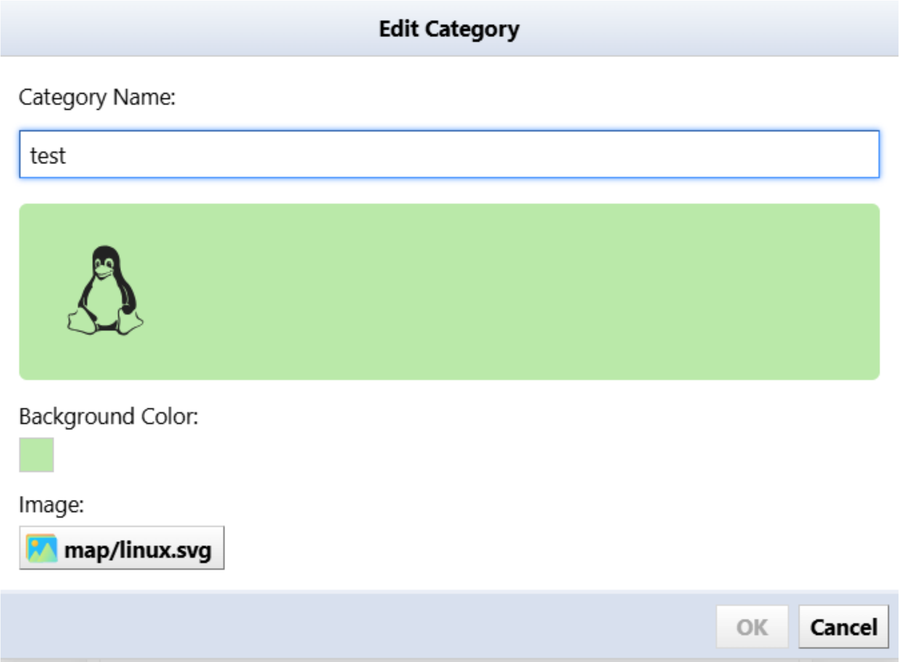


5. Enter a name for the Category.

6. Click [OK] > [Close].

30.8 Edit Playbook Category

1. Click the 🏷 button next to the “Playbook” main tab title to open the [Categories] window.
2. Click the category name in the [Categories] window.
3. Click the ✏ button to open the [Edit Category] window.



Category Name: test

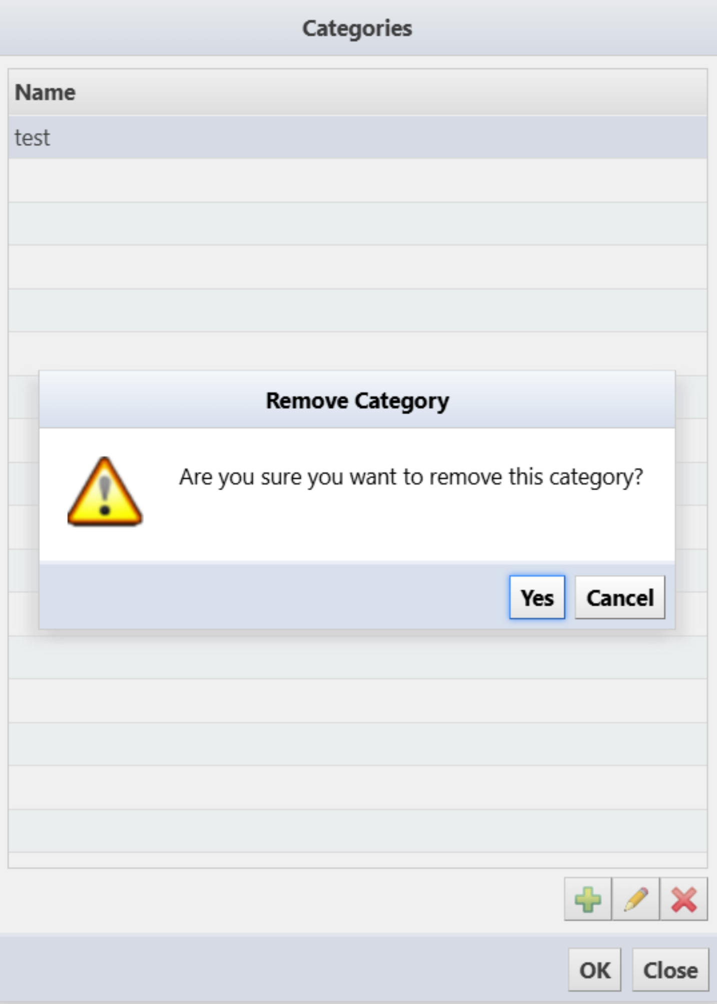
Background Color: 🟩

Image: map/linux.svg

4. Click [OK] after editing.

30.9 Delete Playbook Category

1. Click the 🏷 button next to the “Playbook” main tab title to open the [Categories] window.
2. Click the category name in the [Categories] window.
3. Click the ❌ button to open the [Remove Category] window.



Are you sure you want to remove this category?

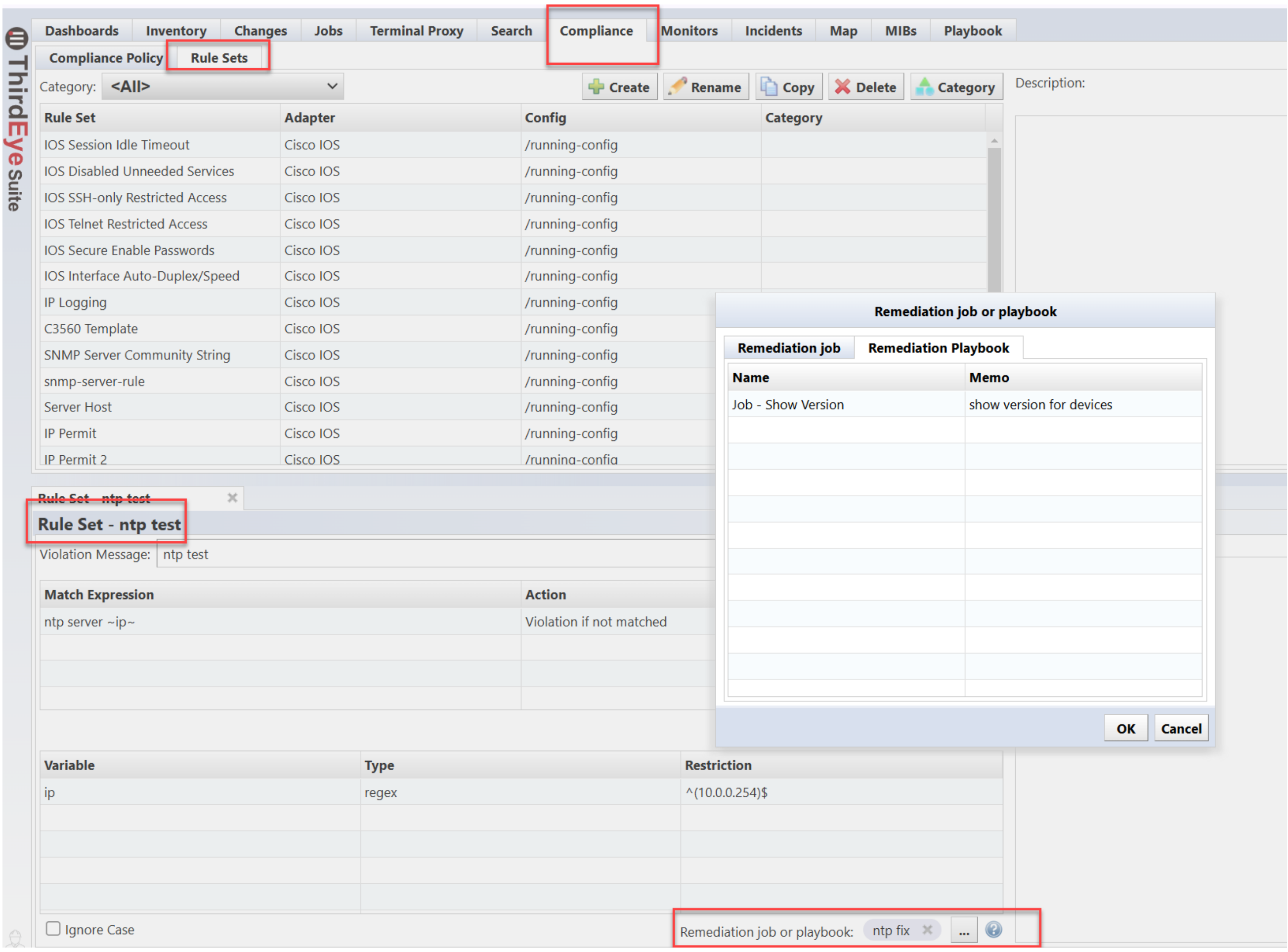
4. Click [Yes].

30.10 Compliance and 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. Doubleclick a [Rule Set] to open the “Rule Set - ntp test” window in the Editor at the bottom of the page.
3. Click the “Remediation job or playbook” ... button in the lower right of the page.



Category: <All>

Rule Set	Adapter	Config	Category
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IP Logging	Cisco IOS	/running-config	
C3560 Template	Cisco IOS	/running-config	
SNMP Server Community String	Cisco IOS	/running-config	
snmp-server-rule	Cisco IOS	/running-config	
Server Host	Cisco IOS	/running-config	
IP Permit	Cisco IOS	/running-config	
IP Permit 2	Cisco IOS	/running-config	

Remediation job or playbook

Remediation job | Remediation Playbook

Name	Memo
Job - Show Version	show version for devices

Violation Message: ntp test

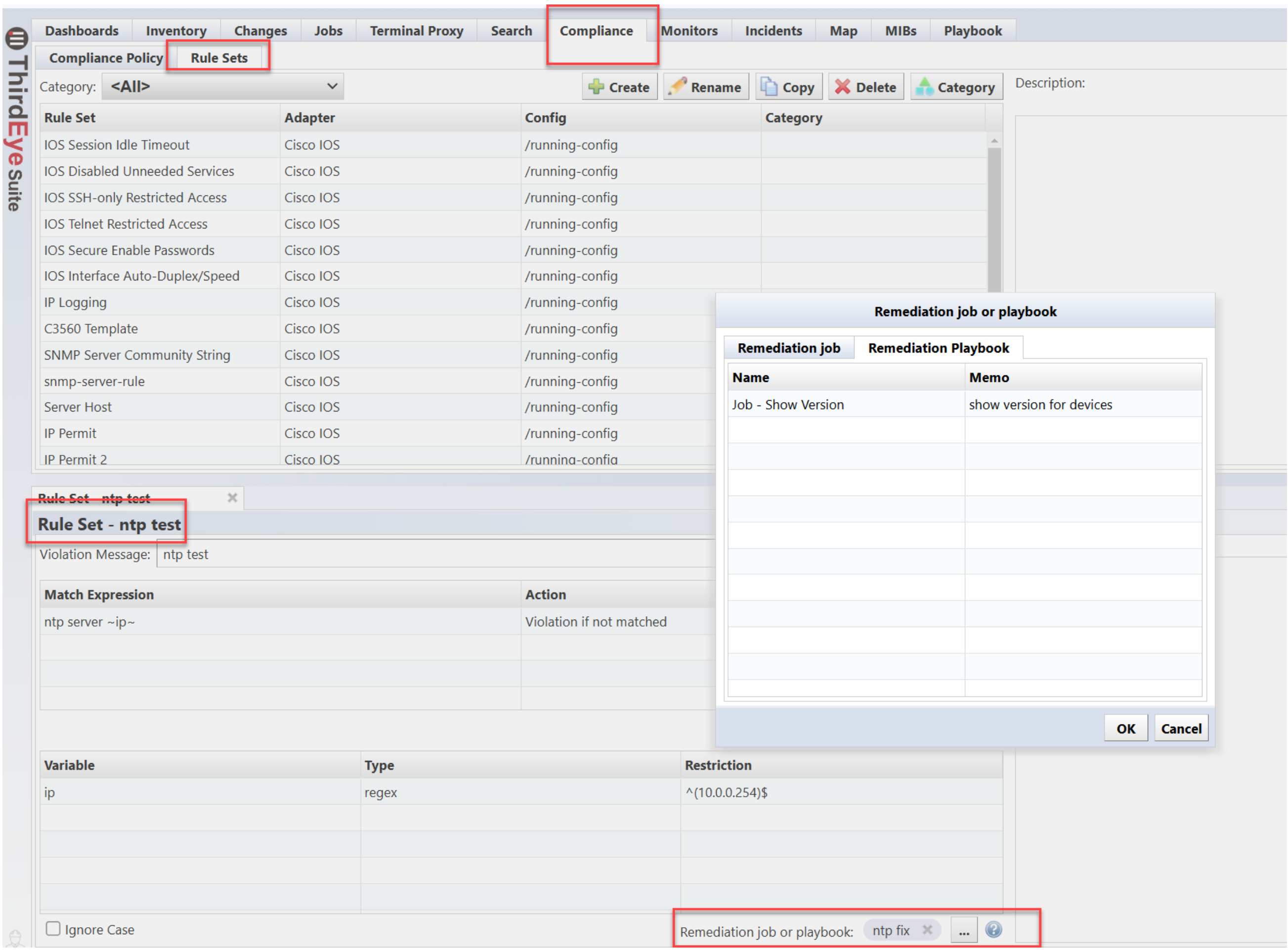
Match Expression	Action
ntp server ~ip~	Violation if not matched

Variable	Type	Restriction
ip	regex	^(10.0.0.254)$

□ Ignore Case

Remediation job or playbook: ntp fix ✕ ...

Compliance example:



Category: <All>

Rule Set	Adapter	Config	Category
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IP Logging	Cisco IOS	/running-config	
C3560 Template	Cisco IOS	/running-config	
SNMP Server Community String	Cisco IOS	/running-config	
snmp-server-rule	Cisco IOS	/running-config	
Server Host	Cisco IOS	/running-config	
IP Permit	Cisco IOS	/running-config	
IP Permit 2	Cisco IOS	/running-config	

Remediation job or playbook

Name	Memo
Job - Show Version	show version for devices

Rule Set - ntp test

Violation Message: ntp test

Match Expression	Action
ntp server ~ip~	Violation if not matched

Variable	Type	Restriction
ip	regex	^(10.0.0.254)$

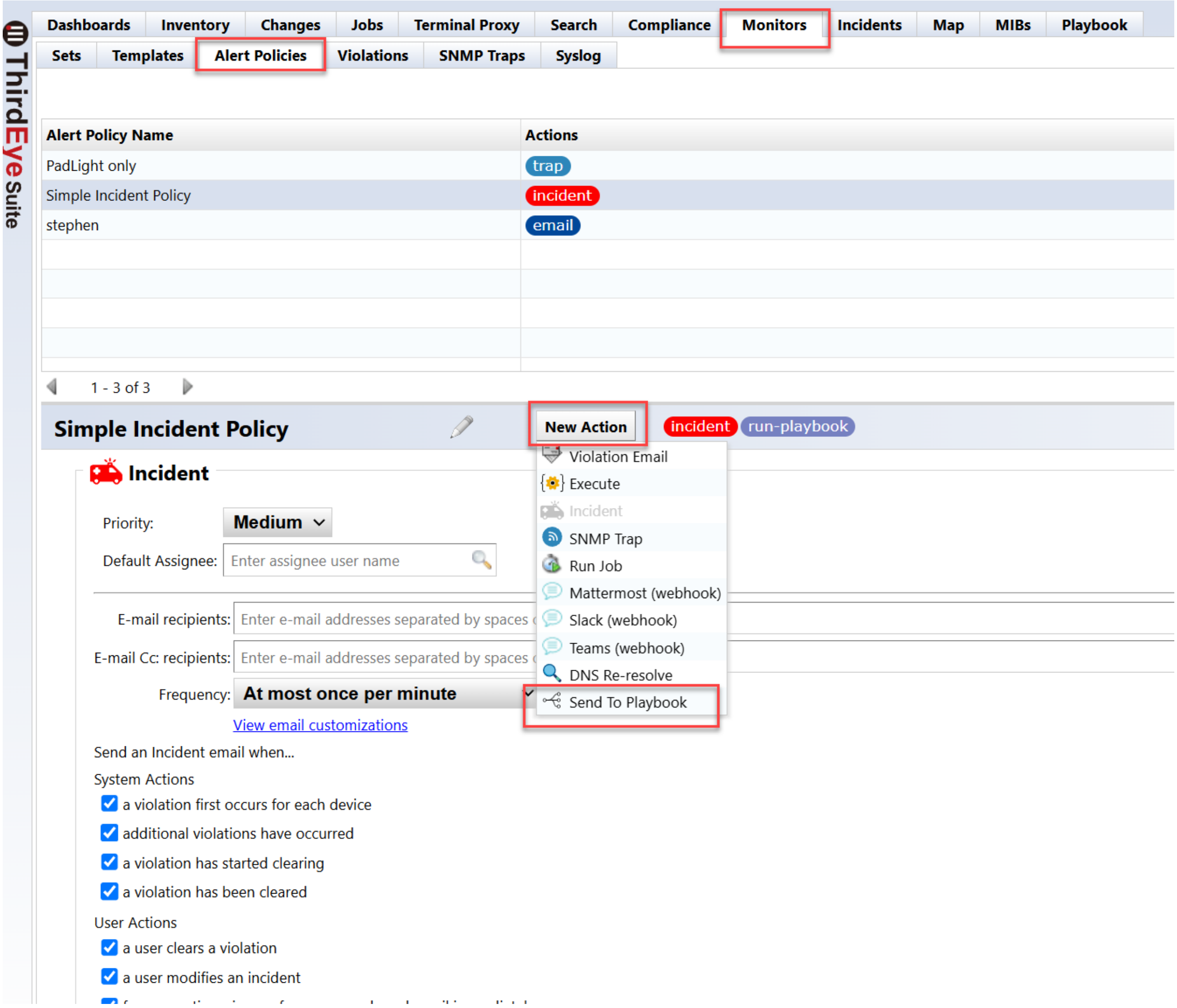
☐ Ignore Case

Remediation job or playbook: ntp fix ✕

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 click [Send to Playbook].



Alert Policy Name	Actions
PadLight only	trap
Simple Incident Policy	incident
stephen	email

Simple Incident Policy

Incident

Priority: Medium

Default Assignee: Enter assignee user name

E-mail recipients: Enter e-mail addresses separated by spaces

E-mail Cc: recipients: Enter e-mail addresses separated by spaces

Frequency: At most once per minute

Send an Incident email when...

System Actions

☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

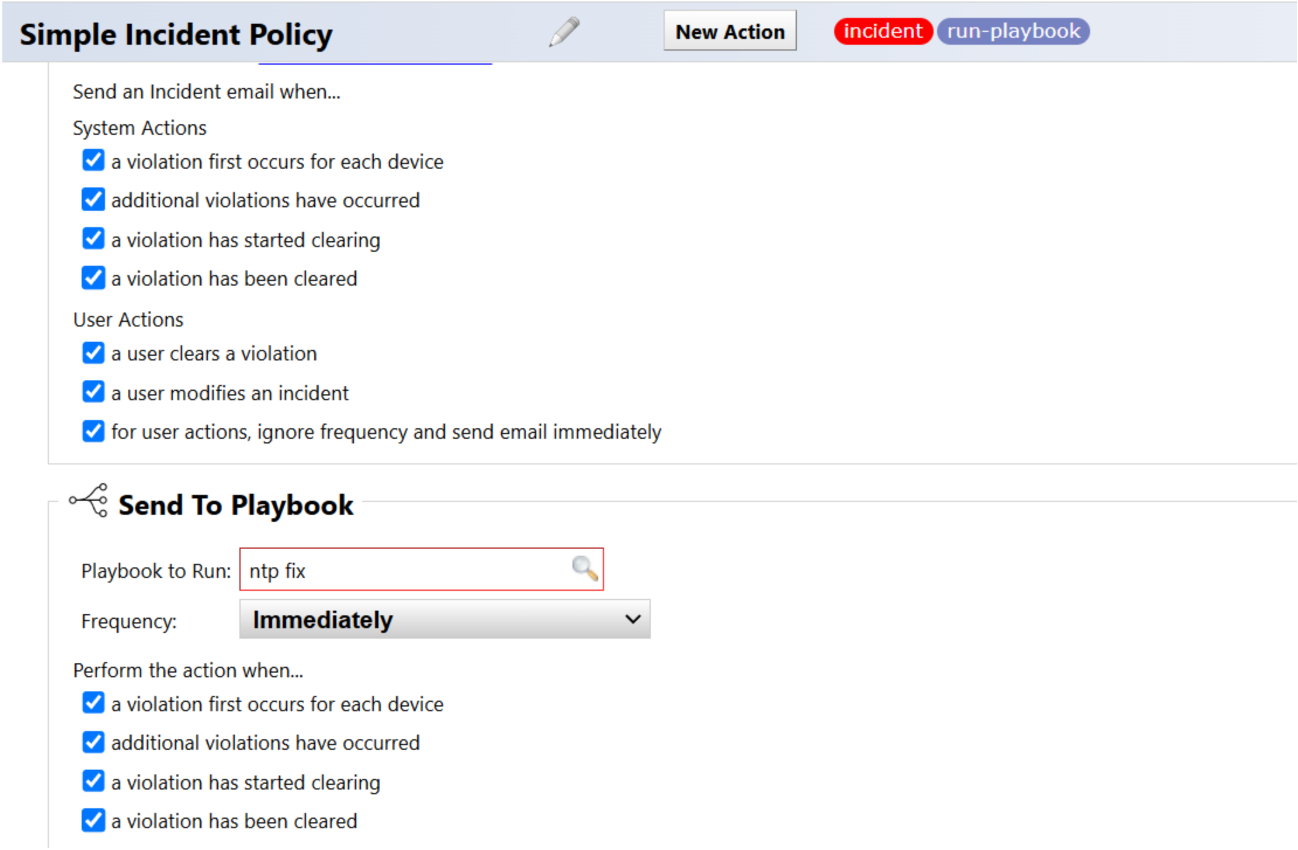
☑ a violation has been cleared

User Actions

☑ a user clears a violation

☑ a user modifies an incident

Once added, select “Playbook to Run”, Frequency” and “Perform the action when…”.



Send an Incident email when...

System Actions

☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

☑ a violation has been cleared

User Actions

☑ a user clears a violation

☑ a user modifies an incident

☑ for user actions, ignore frequency and send email immediately

Send To Playbook

Playbook to Run: ntp fix

Frequency: Immediately

Perform the action when...

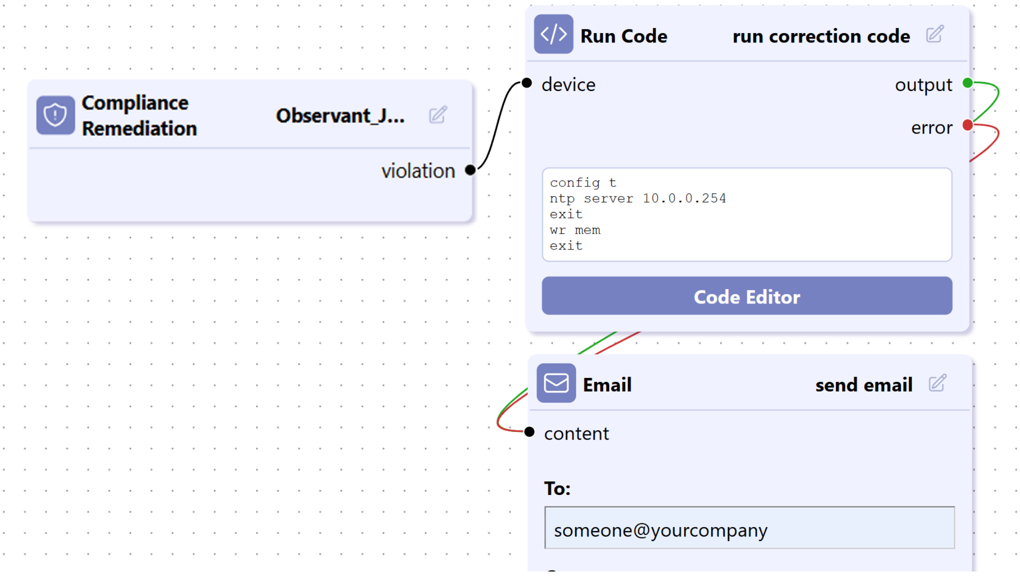
☑ a violation first occurs for each device

☑ additional violations have occurred

☑ a violation has started clearing

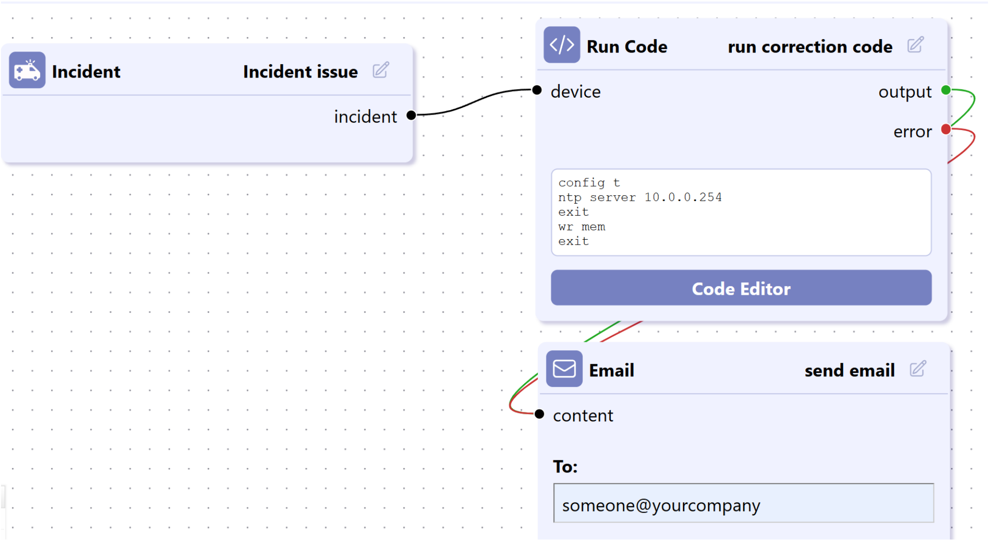
☑ a violation has been cleared

Compliance example:



```
config t
ntp server 10.0.0.254
exit
wr mem
exit
```

Incident example:



```
config t
ntp server 10.0.0.254
exit
wr mem
exit
```

SECTION 31

SYSTEM BACKUP/RESTORE

A system backup is a backup of the entire ThirdEye. You can backup/restore various settings and monitor data (polling, SNMP traps, etc.).

To perform a system backup, click [Settings] > [System Backup] .

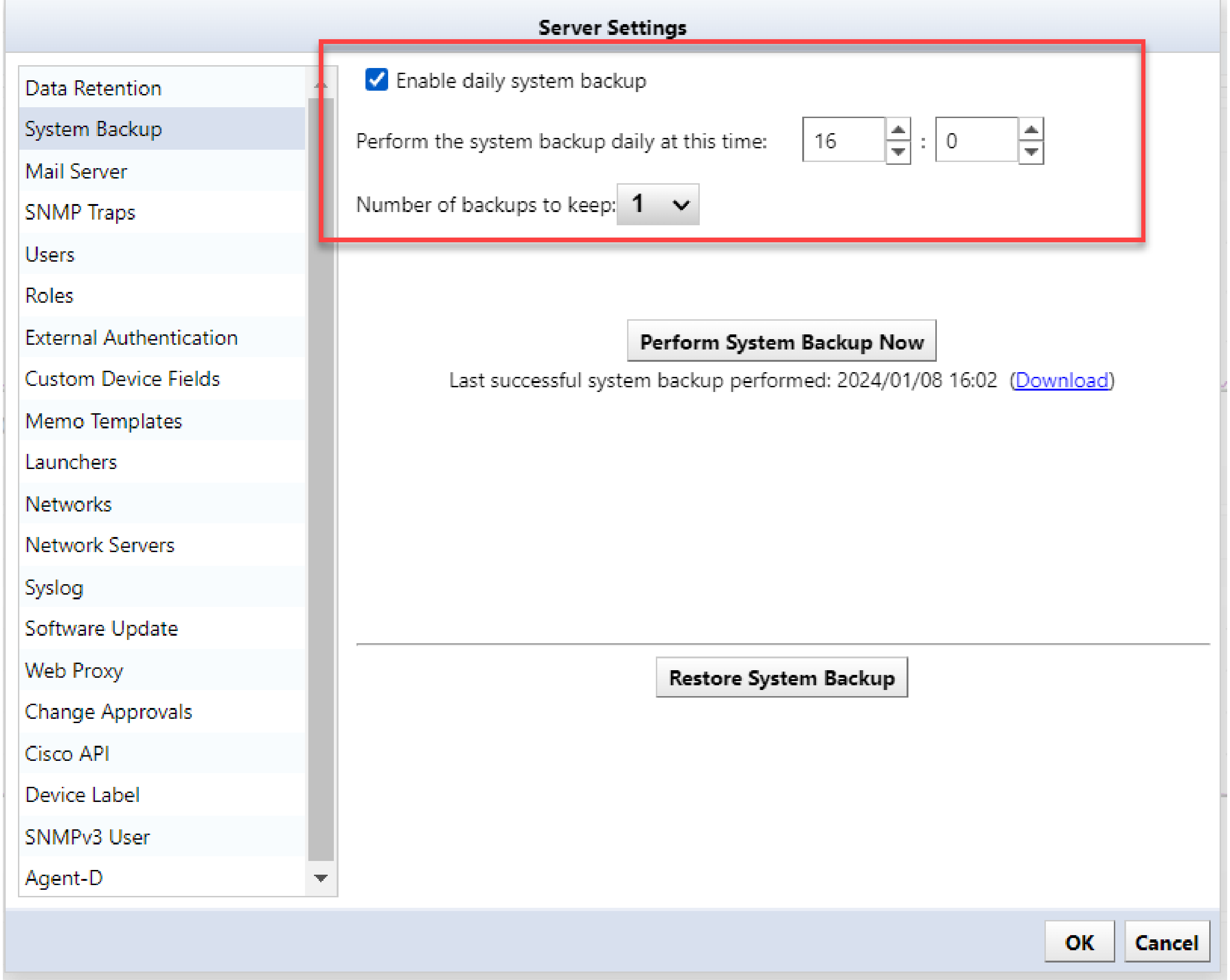
31.1 Automatic System Backup

Automatic system backups are enabled by default.

To disable or change the time for automatic system backups:

1. Click [Settings] in the Global Menu.
2. Click [System Backup] in the left sidemenu to open the [Server Settings] window.

3. Uncheck “Enable daily system backup”, or change the settings the scheduled time or number of backups.



☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

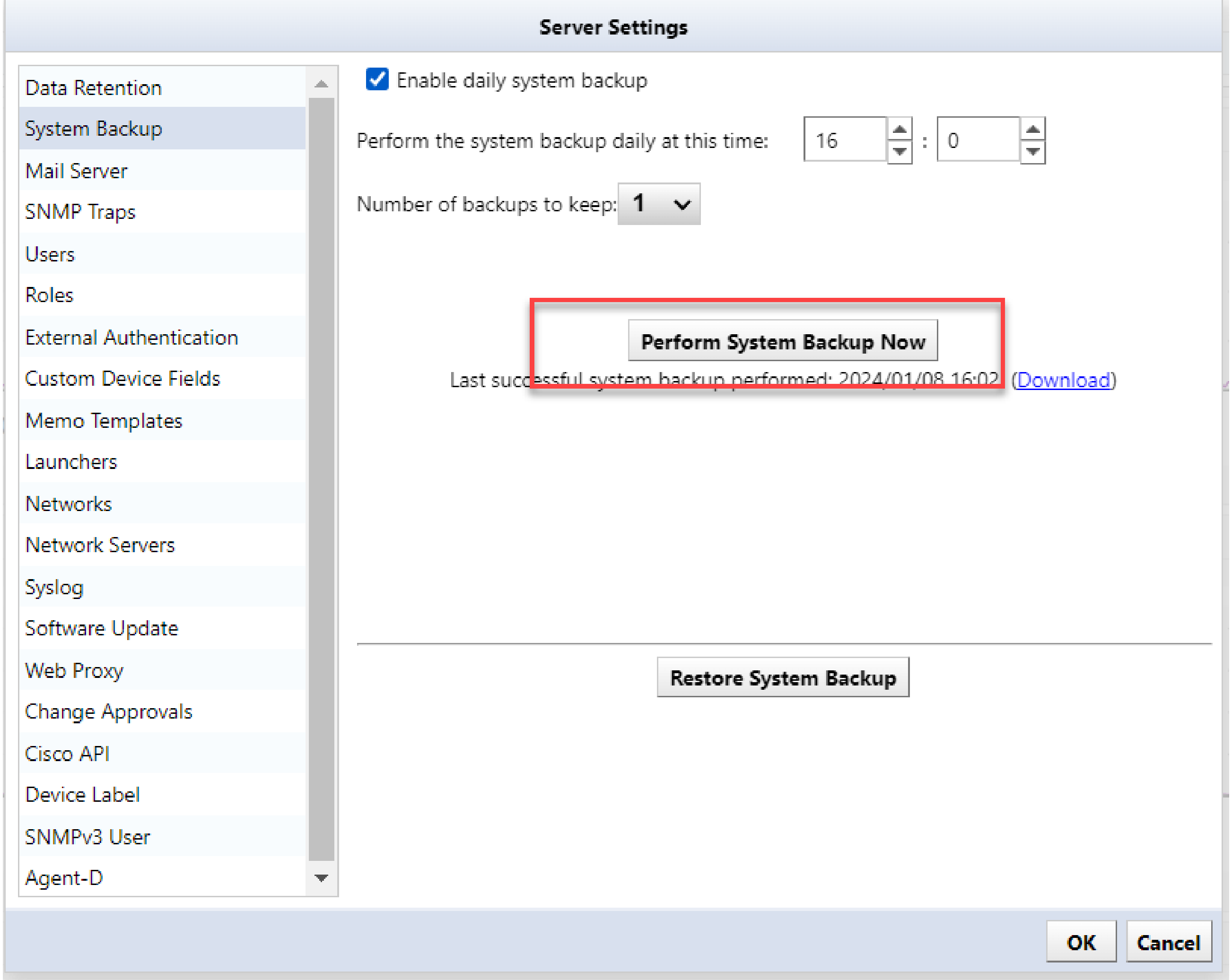
Last successful system backup performed: 2024/01/08 16:02 (Download)

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`)

31.2 Manual System Backup

To perform a manual system backup:

1. Click [Settings] in the Global Menu to open the [Server Settings] window.
2. Click [Perform System Backup].



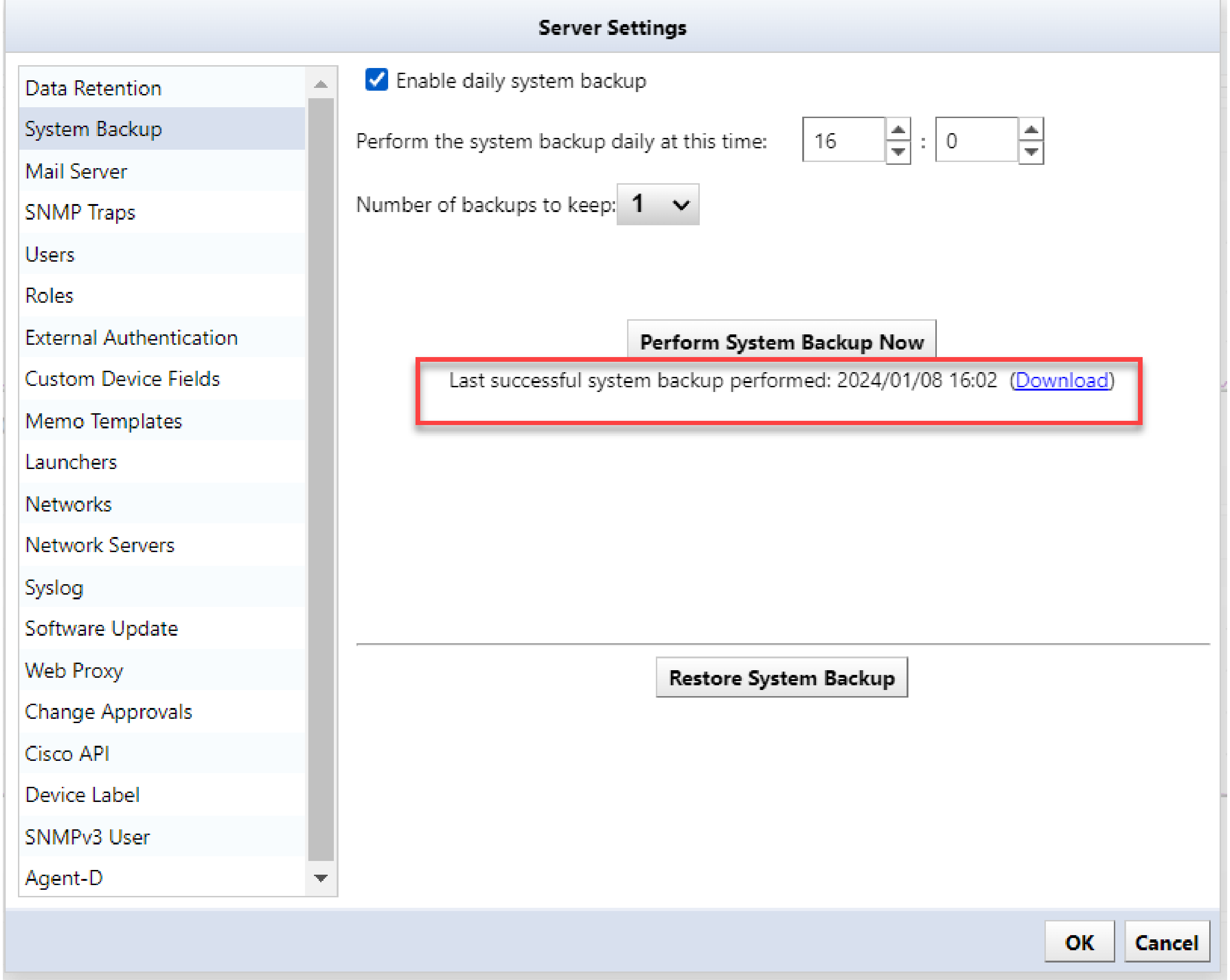
☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

Last successful system backup performed: 2024/01/08 16:02 (Download)

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.



☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

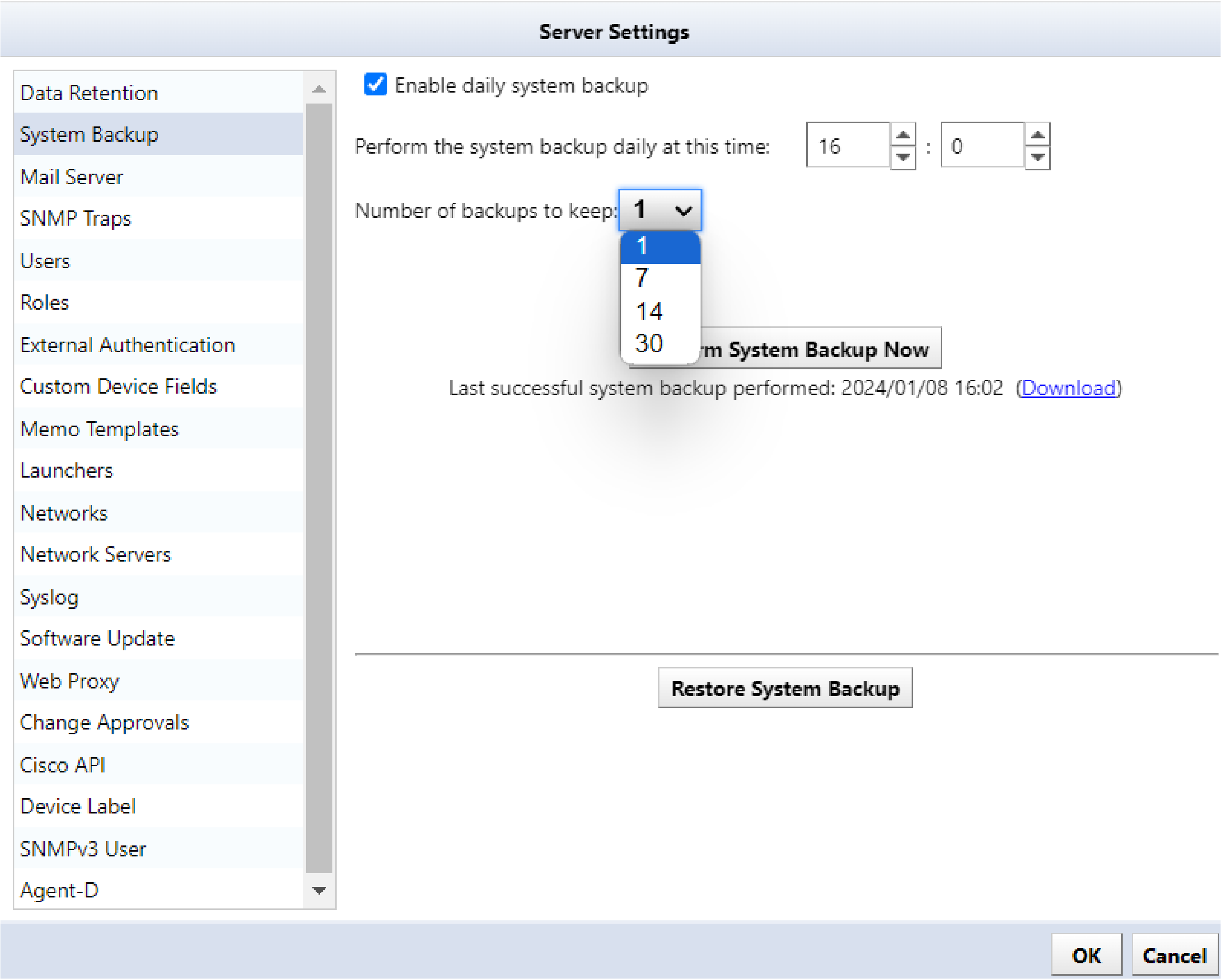
Last successful system backup performed: 2024/01/08 16:02 (Download)

31.3 Change Number of System Backups

You can select the number of system backups. The default value is 7.

> **Note**
>
> 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 accumulate, and consume up disk space. Disk space usage can be reduced by reducing the number of system backups.



Server Settings

☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

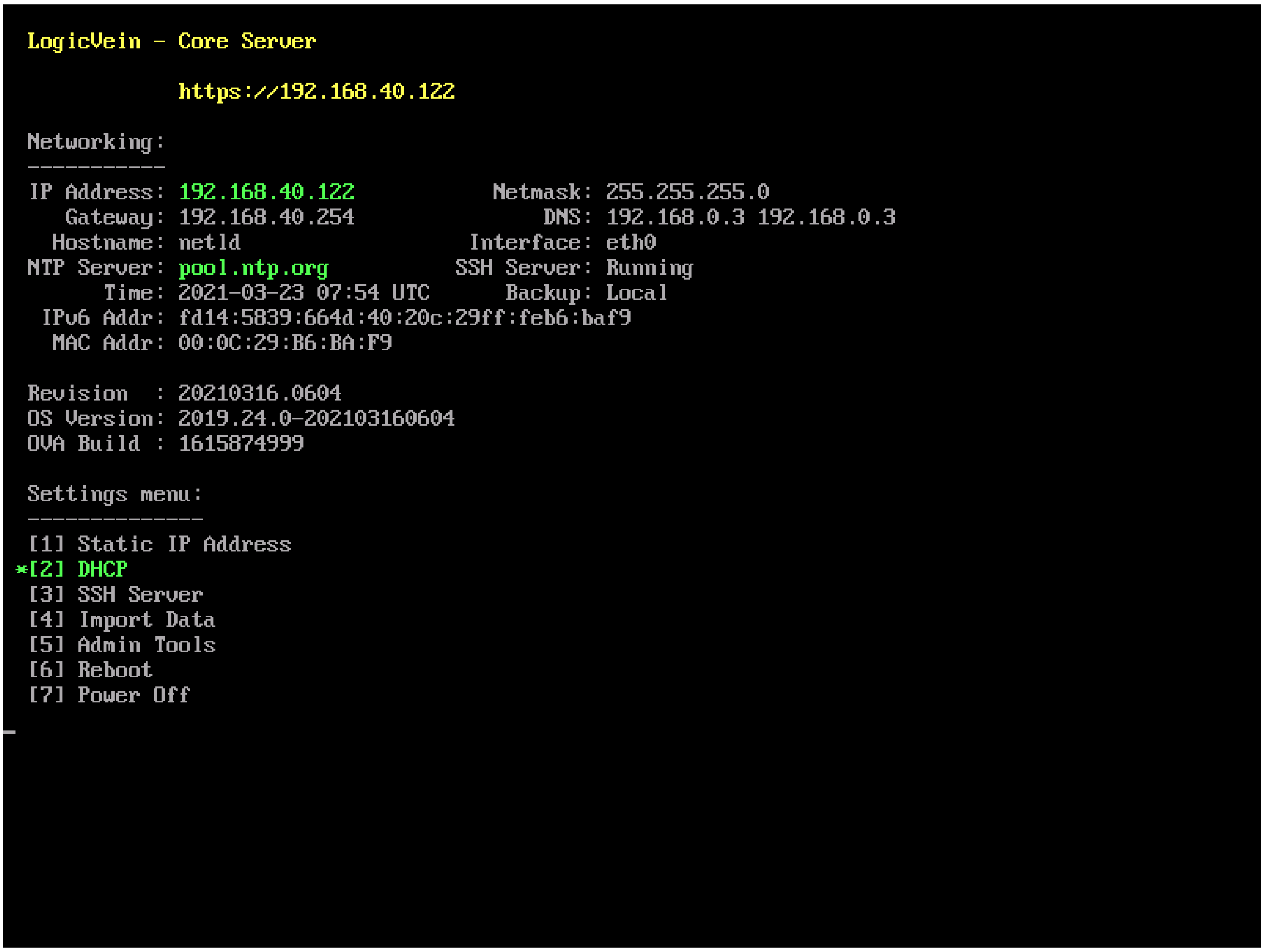
Last successful system backup performed: 2024/01/08 16:02 (Download)

31.4 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.

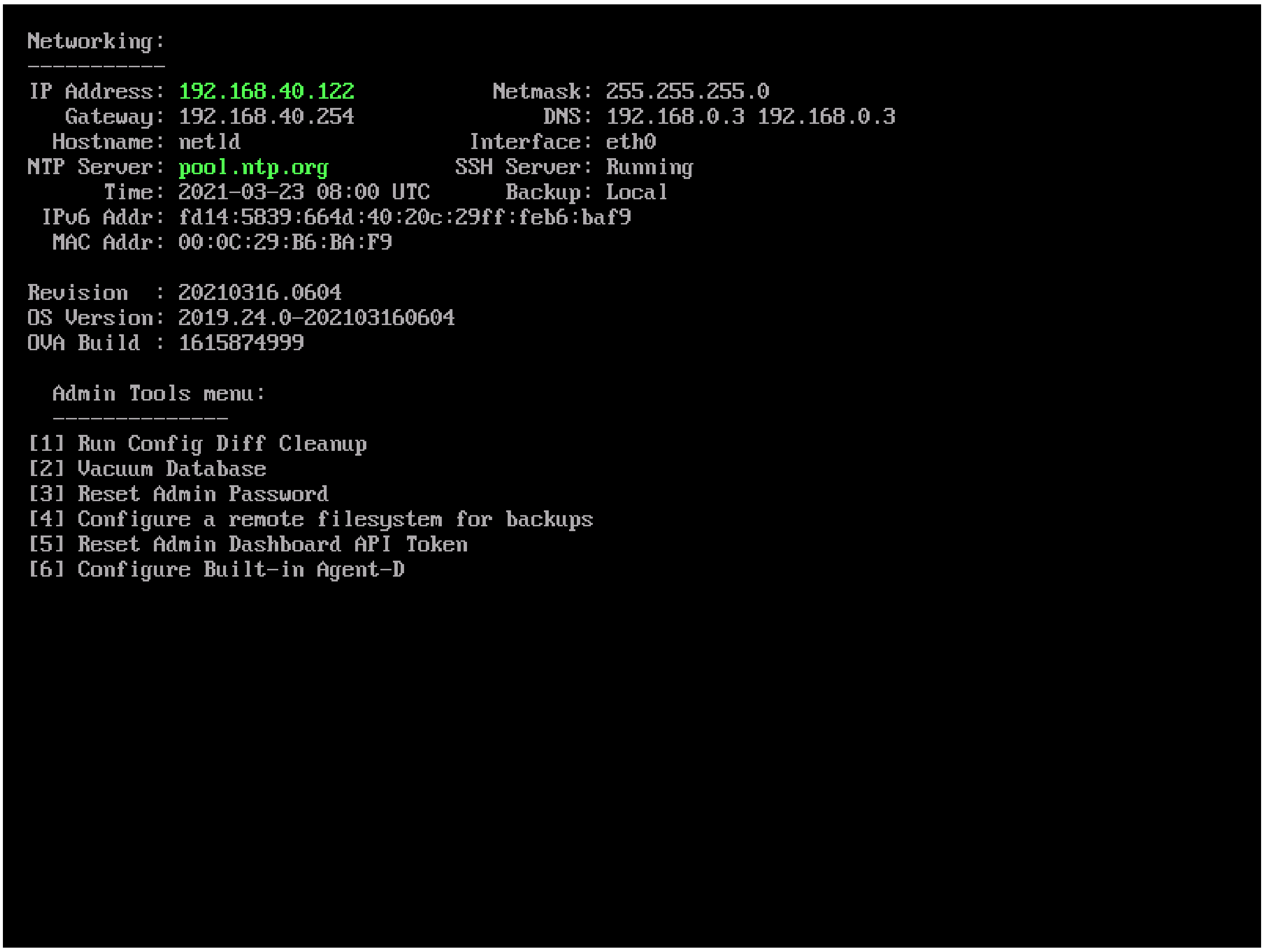
To set up external storage:

1. Click the [5] key on your keyboard, and select [Admin Tools].



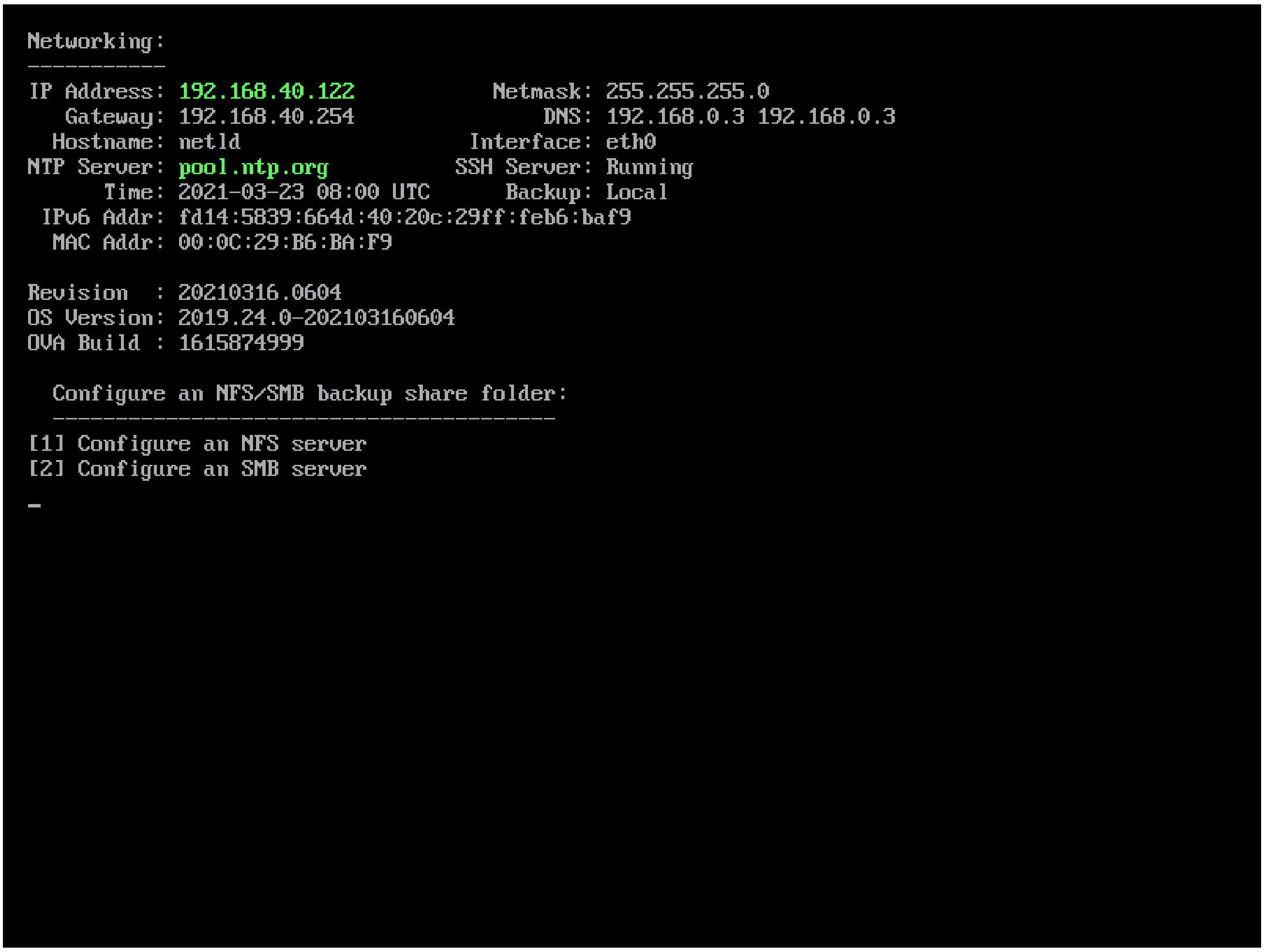
```
LogicVein - Core Server

            https://192.168.40.122

Networking:
-----------
IP Address: 192.168.40.122          Netmask: 255.255.255.0
   Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Running
      Time: 2021-03-23 07:54 UTC     Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
  MAC Addr: 00:0C:29:B6:BA:F9

Revision  : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

Settings menu:
--------------
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
_
```

2. Click the [4] key on your keyboard, and select [Configure a remote filesystem for backups].



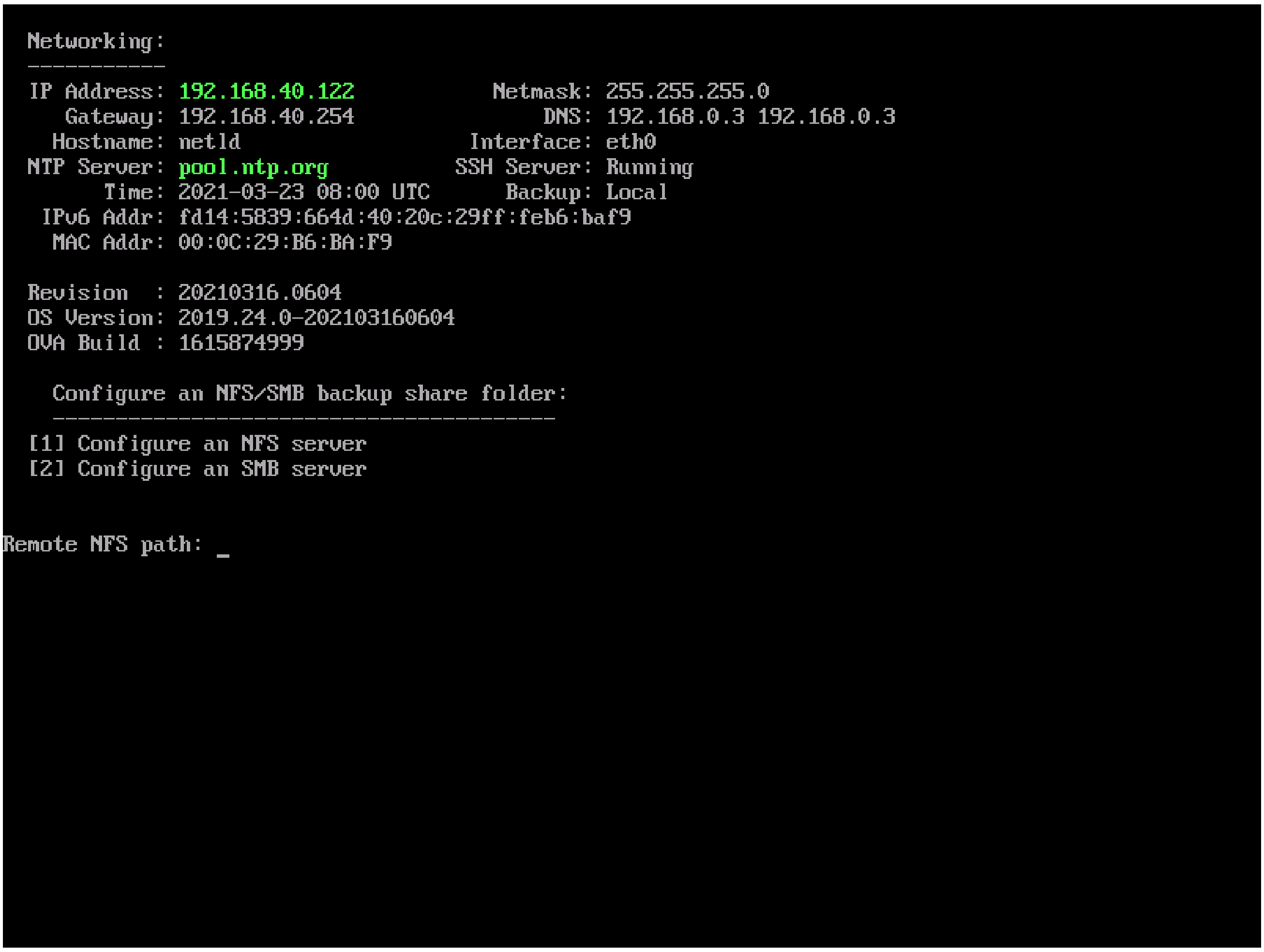
```
Networking:
-----------
IP Address: 192.168.40.122          Netmask: 255.255.255.0
   Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Running
      Time: 2021-03-23 08:00 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
  MAC Addr: 00:0C:29:B6:BA:F9

Revision  : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

  Admin Tools menu:
  --------------
[1] Run Config Diff Cleanup
[2] Vacuum Database
[3] Reset Admin Password
[4] Configure a remote filesystem for backups
[5] Reset Admin Dashboard API Token
[6] Configure Built-in Agent-D
```

3. Select the server type.



```
Networking:
-----------
IP Address: 192.168.40.122          Netmask: 255.255.255.0
   Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Running
      Time: 2021-03-23 08:00 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
  MAC Addr: 00:0C:29:B6:BA:F9

Revision  : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

  Configure an NFS/SMB backup share folder:
  ----------------------------------------
[1] Configure an NFS server
[2] Configure an SMB server

_
```

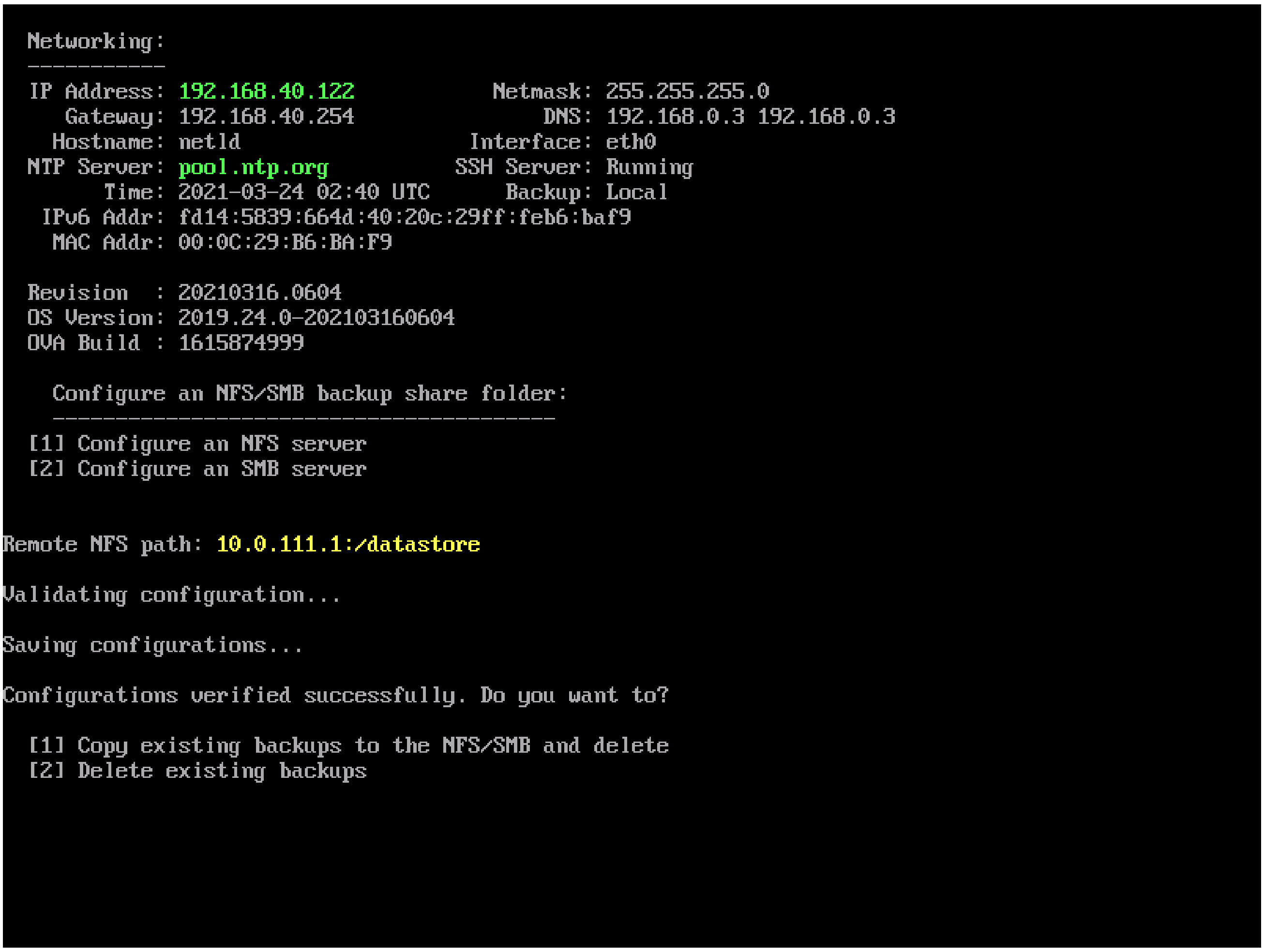
4. Enter the required information and press [Enter].



```
 Networking:
 -----------
 IP Address: 192.168.40.122          Netmask: 255.255.255.0
    Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                 Interface: eth0
 NTP Server: pool.ntp.org         SSH Server: Running
       Time: 2021-03-23 08:00 UTC     Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

   Configure an NFS/SMB backup share folder:
   ----------------------------------------
 [1] Configure an NFS server
 [2] Configure an SMB server


Remote NFS path: _
```

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].

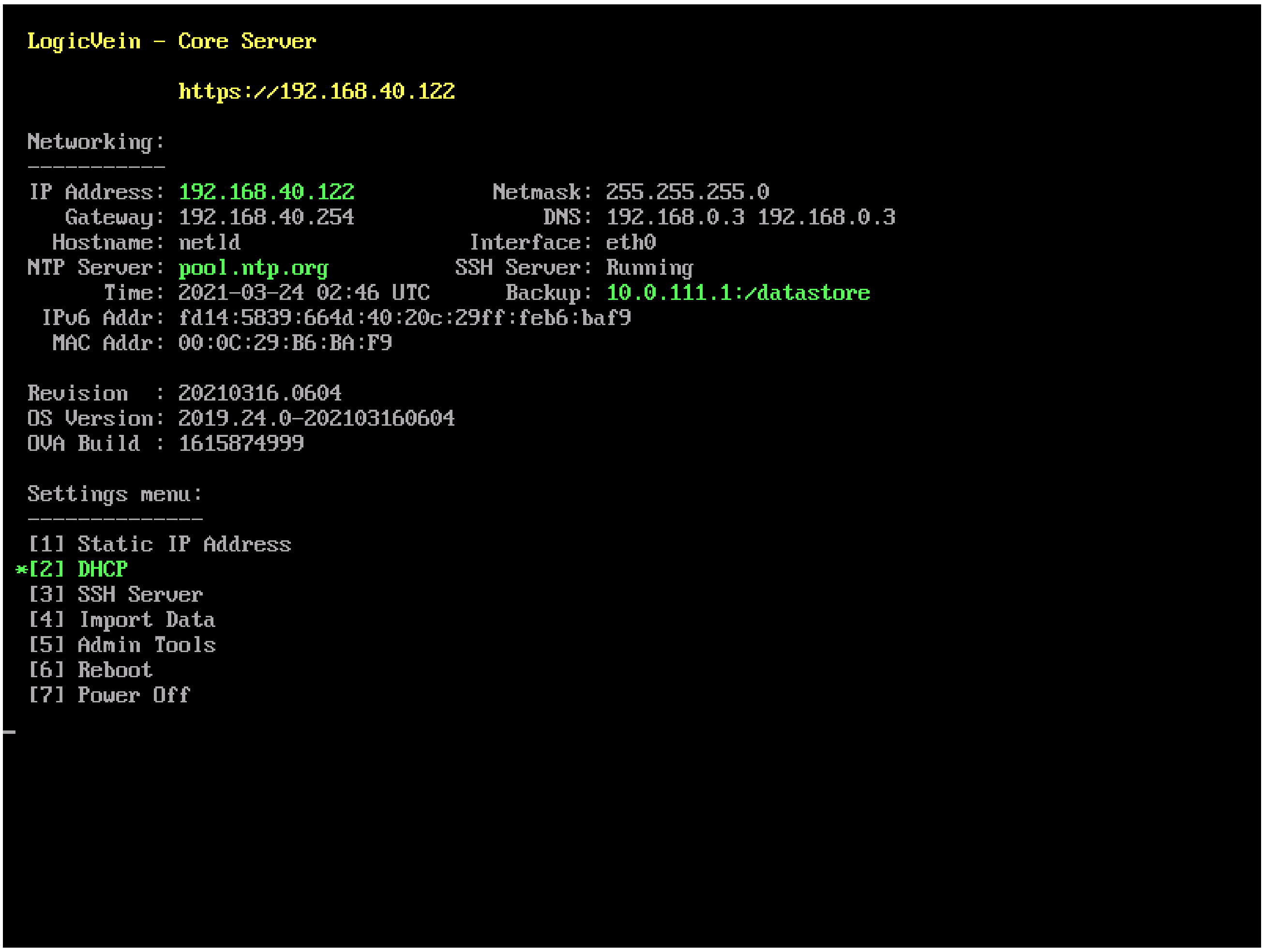


```
  Networking:
  -----------
  IP Address: 192.168.40.122          Netmask: 255.255.255.0
     Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
    Hostname: netld                 Interface: eth0
  NTP Server: pool.ntp.org         SSH Server: Running
        Time: 2021-03-24 02:40 UTC     Backup: Local
   IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
    MAC Addr: 00:0C:29:B6:BA:F9

  Revision  : 20210316.0604
  OS Version: 2019.24.0-202103160604
  OVA Build : 1615874999

    Configure an NFS/SMB backup share folder:
    ----------------------------------------
  [1] Configure an NFS server
  [2] Configure an SMB server


Remote NFS path: 10.0.111.1:/datastore

Validating configuration...

Saving configurations...

Configurations verified successfully. Do you want to?

  [1] Copy existing backups to the NFS/SMB and delete
  [2] Delete existing backups
```

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.

ThirdEye will restart automatically, and you can check the settings on the console screen.



```
 LogicVein - Core Server

             https://192.168.40.122

 Networking:
 -----------
 IP Address: 192.168.40.122          Netmask: 255.255.255.0
    Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                 Interface: eth0
 NTP Server: pool.ntp.org         SSH Server: Running
       Time: 2021-03-24 02:46 UTC     Backup: 10.0.111.1:/datastore
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

 Settings menu:
 --------------
 [1] Static IP Address
*[2] DHCP
 [3] SSH Server
 [4] Import Data
 [5] Admin Tools
 [6] Reboot
 [7] Power Off
_
```

31.5 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:

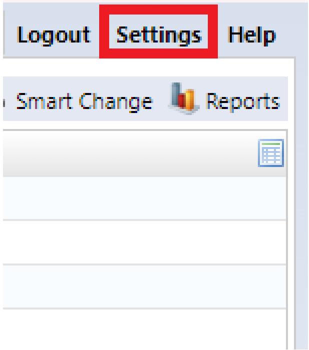
- `pgsql` (folder)
- `version.txt` (file)
- `complete` (file)

31.6 Restore System Backup from Zip File

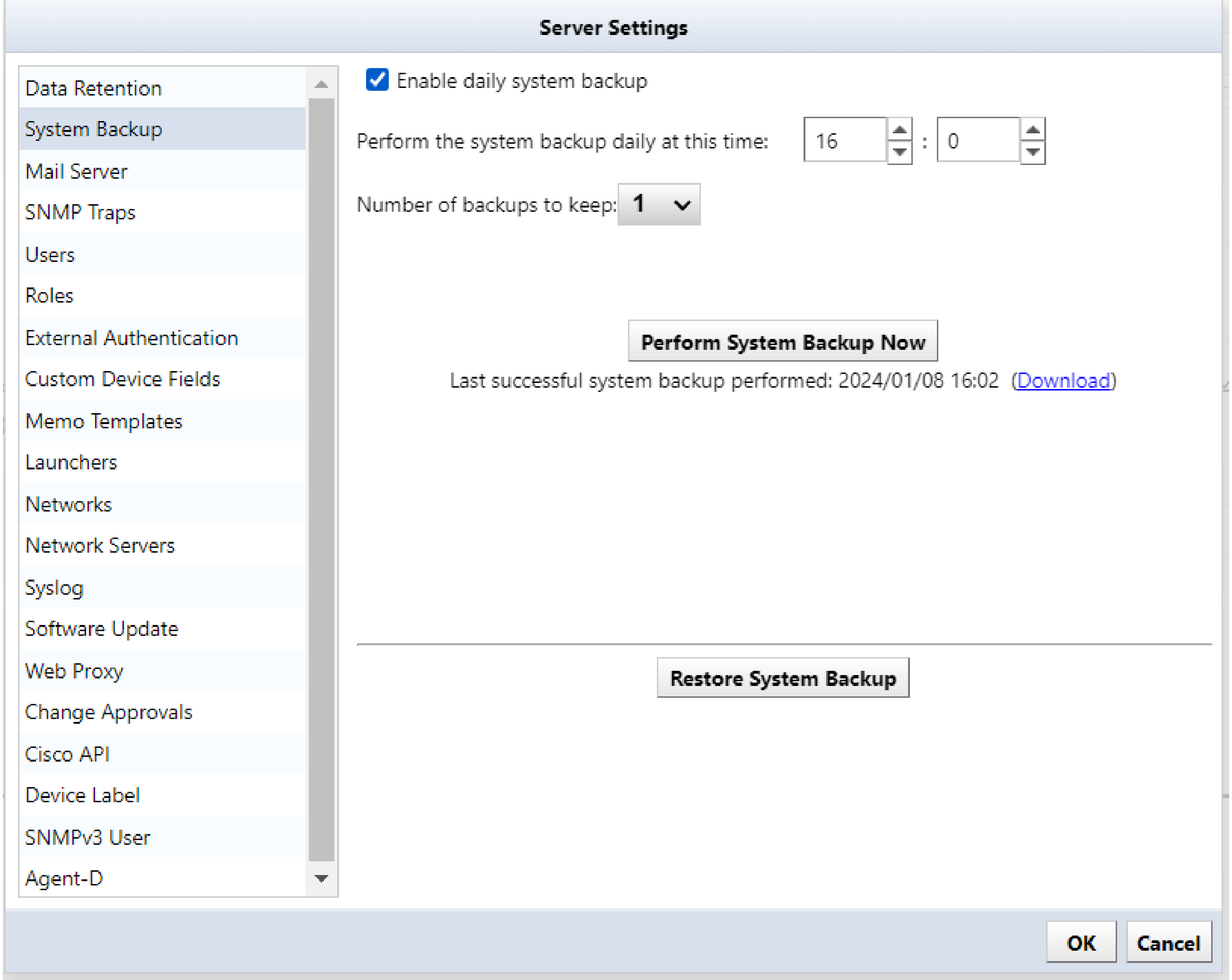
To restore system backup from a zip file, select the backup source and restore destination. It must be the same version (revision).

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].



Server Settings

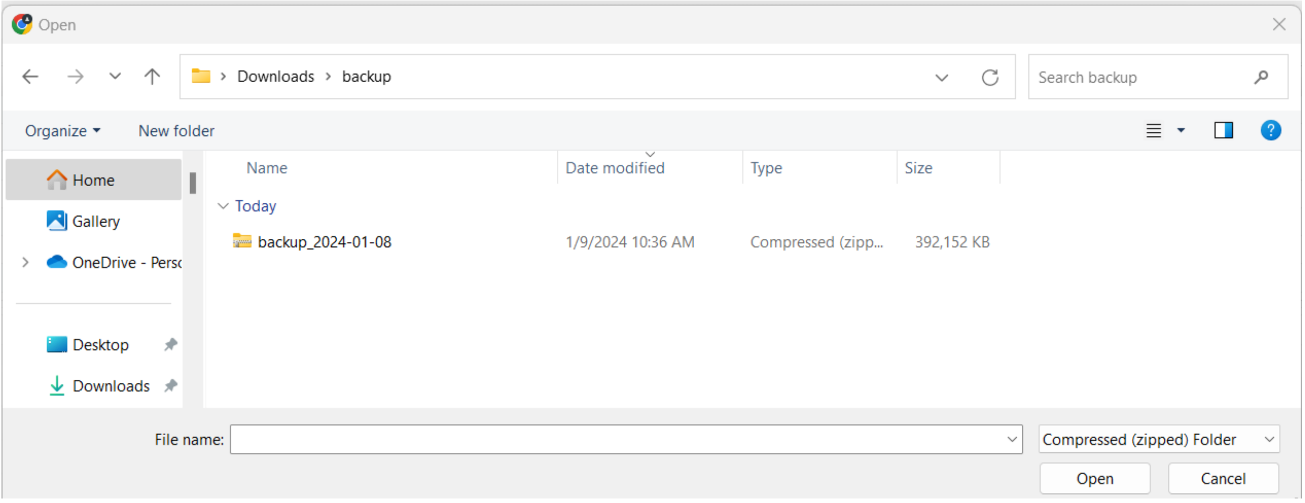
☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

Last successful system backup performed: 2024/01/08 16:02 (Download)

4. Select the file you want to restore, and click [Open].

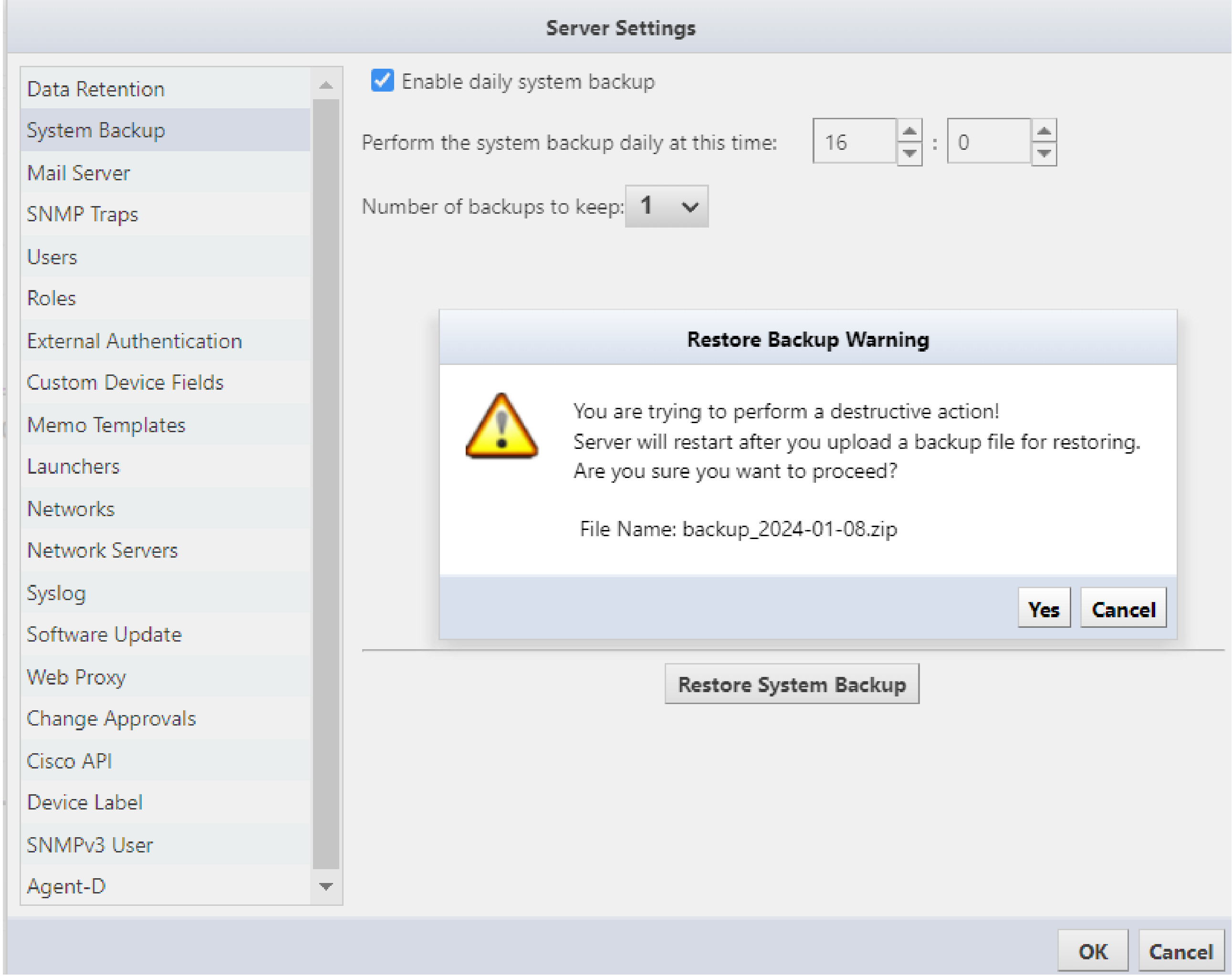


Name	Date modified	Type	Size
backup_2024-01-08	1/9/2024 10:36 AM	Compressed (zipp...	392,152 KB

File name:

Compressed (zipped) Folder

5. Click [Yes] on the warning screen.



Server Settings

☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

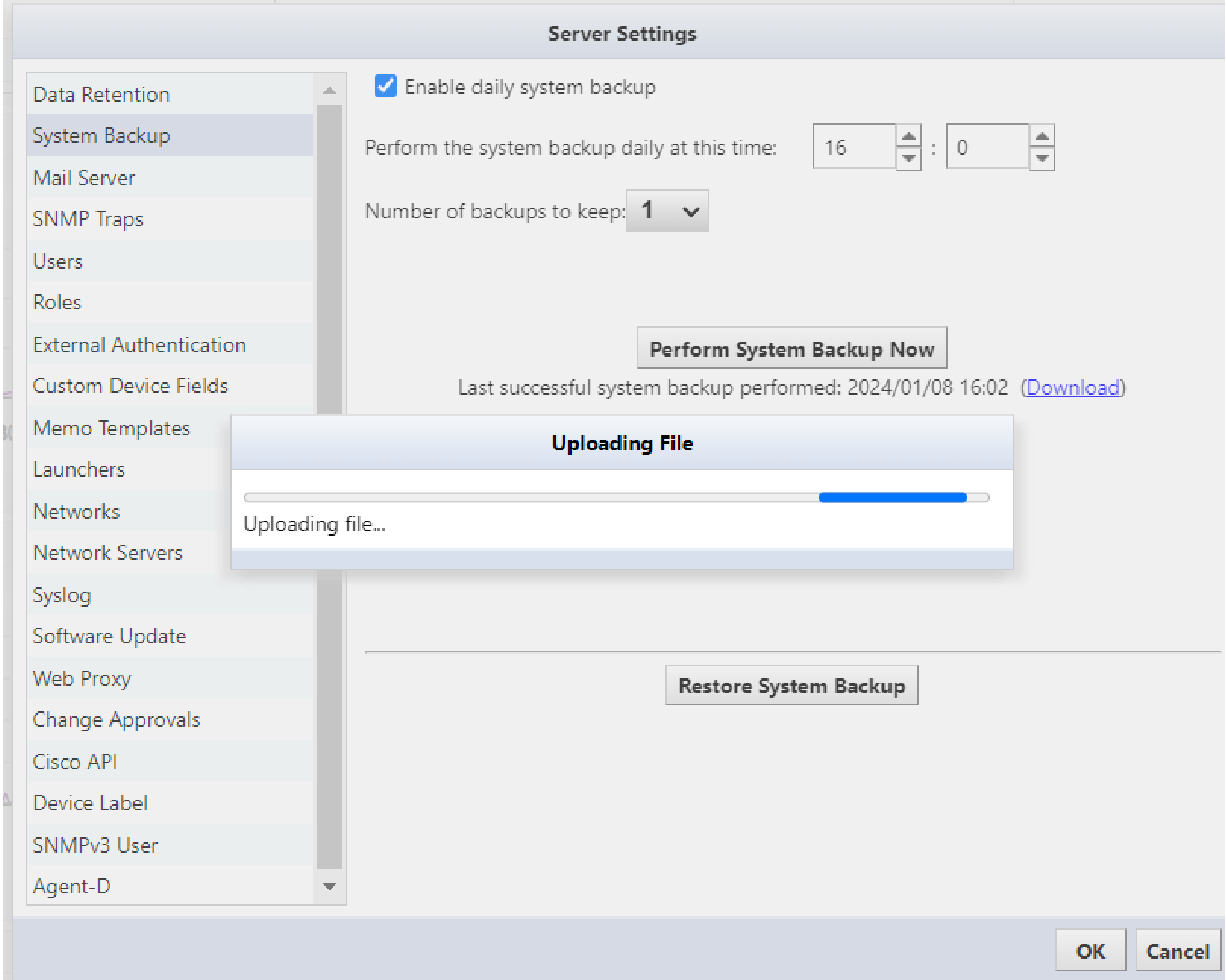
Number of backups to keep: 1

Restore Backup Warning

You are trying to perform a destructive action!
Server will restart after you upload a backup file for restoring.
Are you sure you want to proceed?

File Name: backup_2024-01-08.zip

6. The file will be uploaded, and the restoration will begin.



☑ Enable daily system backup

Perform the system backup daily at this time: 16 : 0

Number of backups to keep: 1

Last successful system backup performed: 2024/01/08 16:02 (Download)

Uploading File

Uploading file...

System backup/restore is now complete.

After uploading, the service will automatically restart and return to the login screen.

SECTION 32

SMART BRIDGES (OPTIONAL)

SmartBridges are secure communication gateways designed to connect distributed network infrastructure to centralized management systems. They primarily serve to:

- Establish encrypted tunnels through corporate firewalls without requiring inbound port openings
- Support Bridge-to-Server (outbound HTTPS connections) and Server-to-Bridge (for specific use cases)
- Enable secure management of devices across multiple network boundaries
- Function as lightweight virtual appliances
- Use unique authentication tokens for secure pairing

ThirdEye supports two modes for the connection of Smart Bridges to the core server:

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

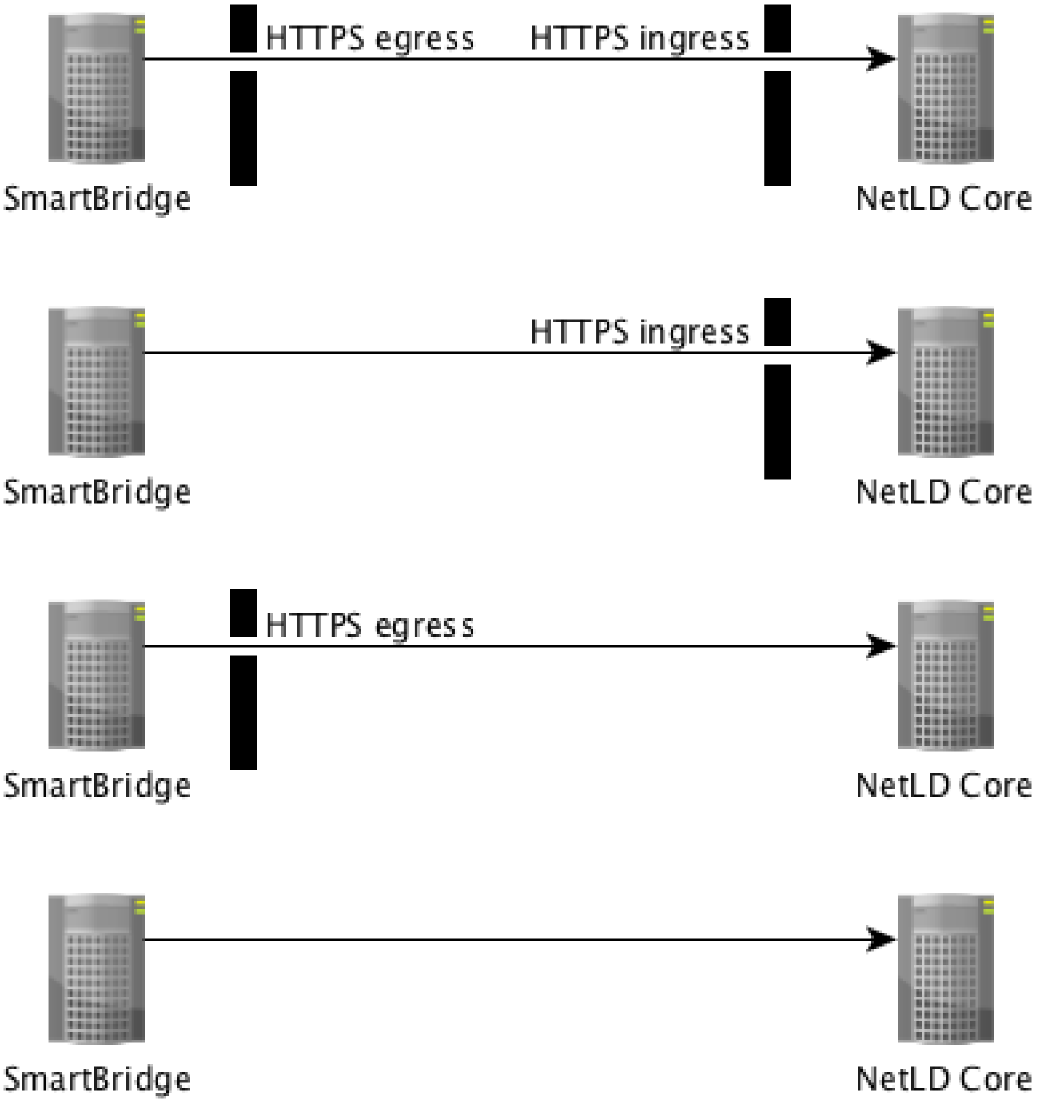
All connections are via HTTPS, so wire traffic is encrypted end-to-end.

32.1 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.

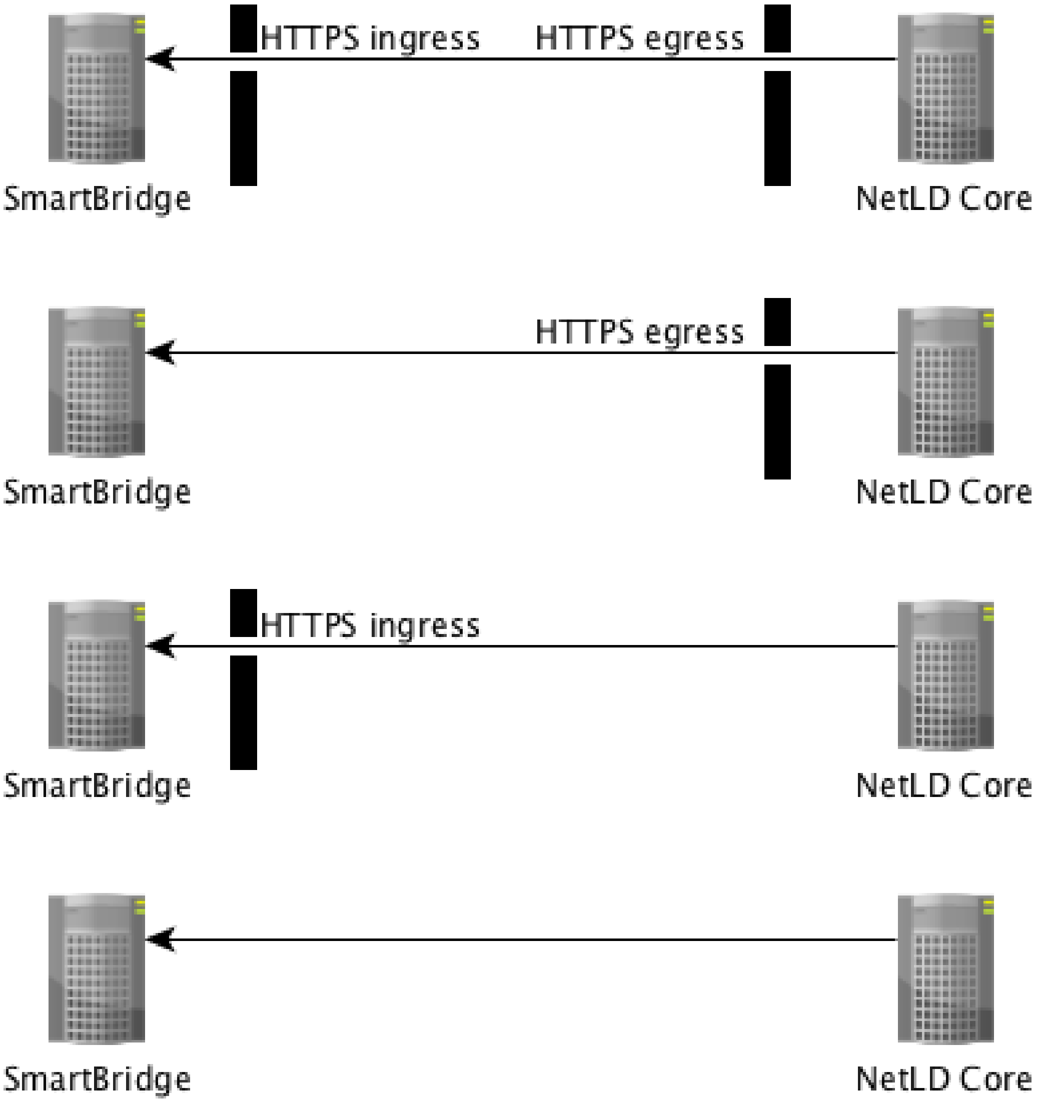


32.2 Server-to-Bridge

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 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.



32.3 Connection Token

LogicVein introduces the concept of a *Connection Token*. This is 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.

32.4 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`

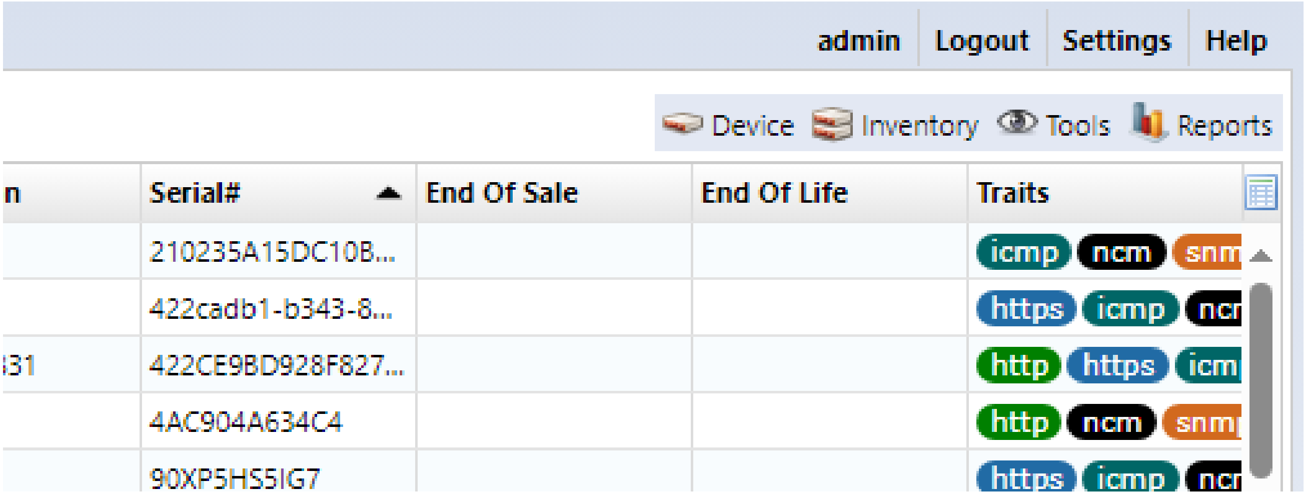
Smart bridge file name: `lvi-bridge-2024.03.0-202406180814-appliance.ova`

After installation, refer to the **Configuring Network Settings** for instructions on configuring the network.

32.5 Add SmartBridge to Core Server

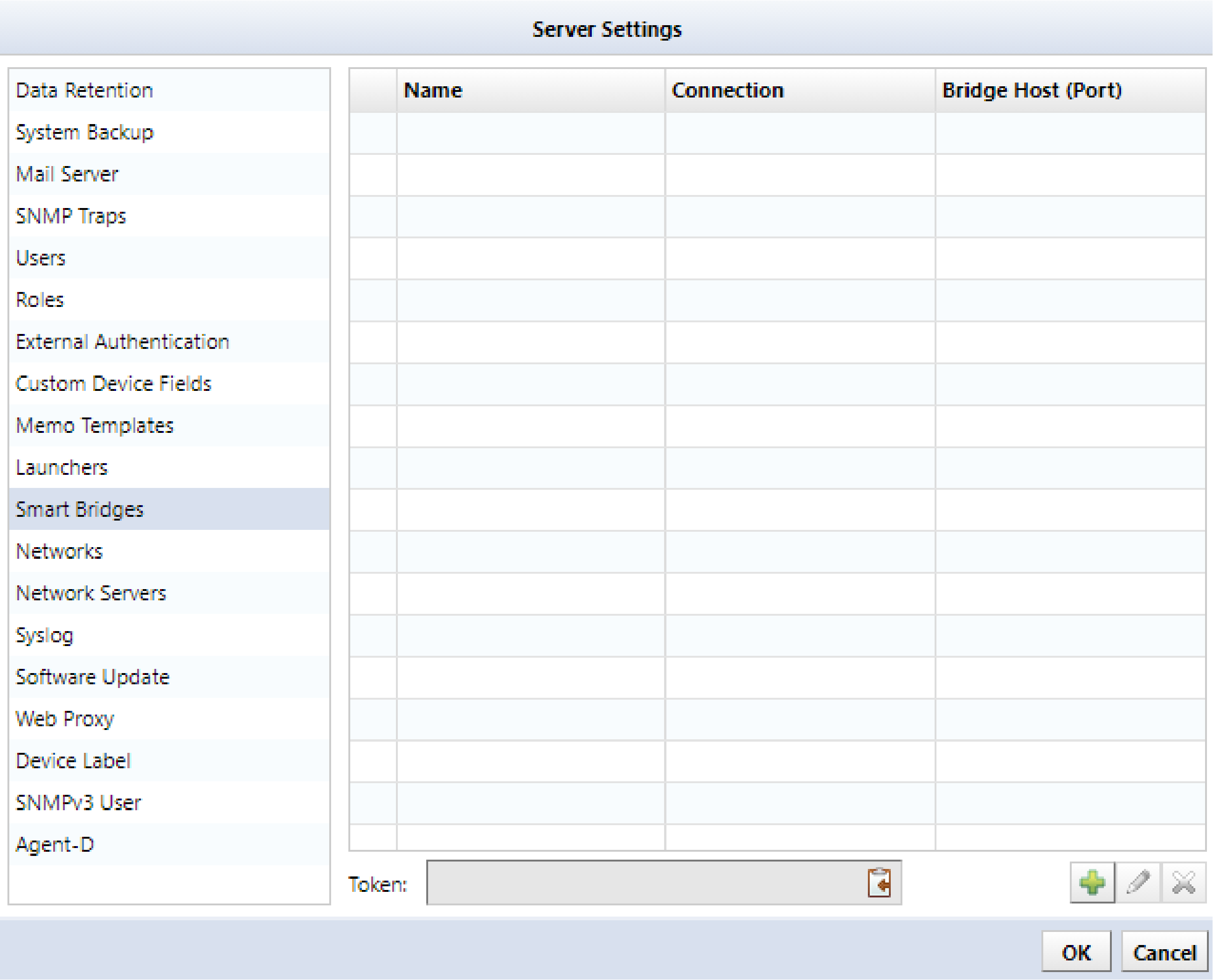
Register SmartBridge on the core server. After registering SmartBridge, a token will be automatically generated.

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

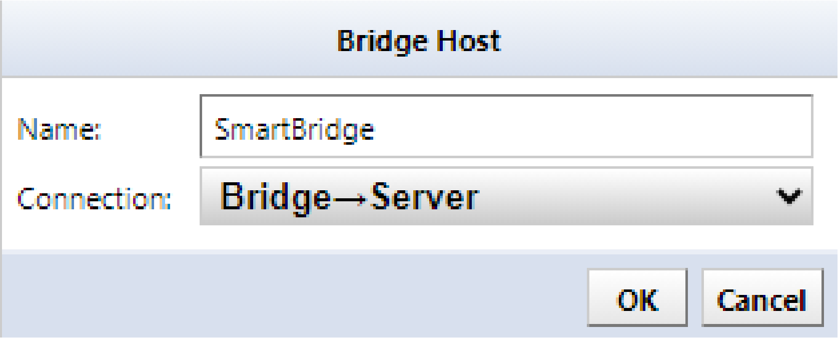


n	Serial#	End Of Sale	End Of Life	Traits
	210235A15DC10B...			icmp ncm snm
	422cadb1-b343-8...			https icmp ncr
31	422CE9BD928F827...			http https icm
	4AC904A634C4			http ncm snmj
	90XP5HS5IG7			https icmp ncr

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

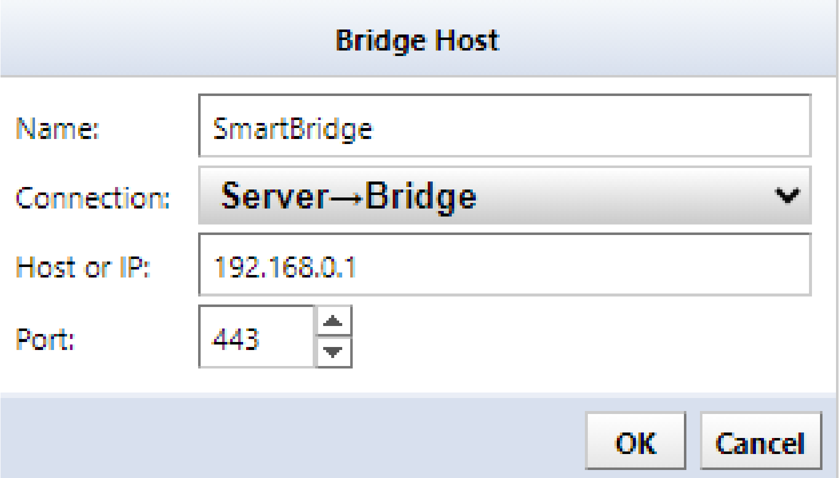


Name: SmartBridge

Connection: Bridge→Server

4. Click [Connection].

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



Bridge Host

Name: SmartBridge

Connection: Server→Bridge

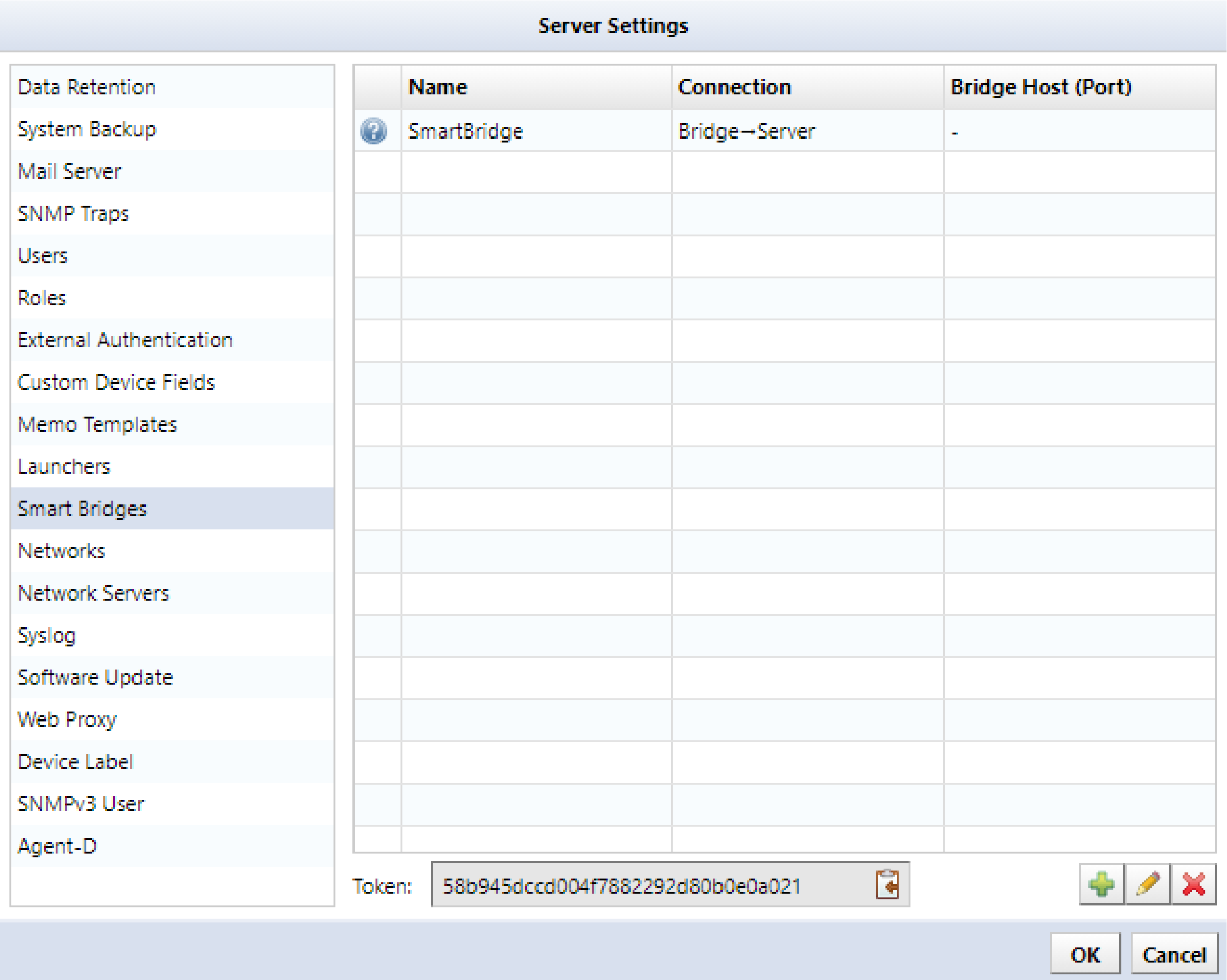
Host or IP: 192.168.0.1

Port: 443

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.



	Name	Connection	Bridge Host (Port)
?	SmartBridge	Bridge→Server	-

Token: 58b945dccd004f7882292d80b0e0a021

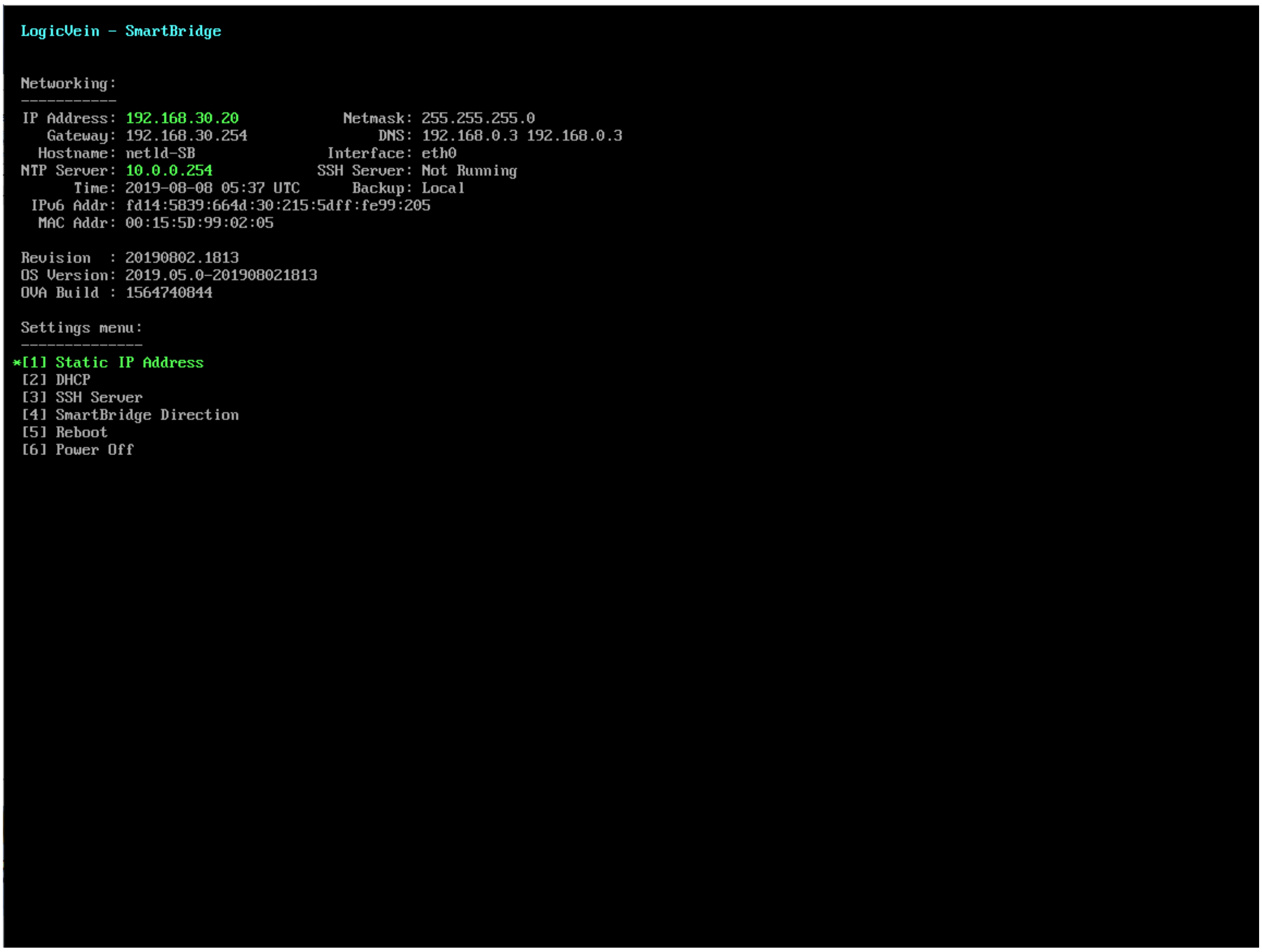
7. Click [OK].

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

32.6 SmartBridge Settings

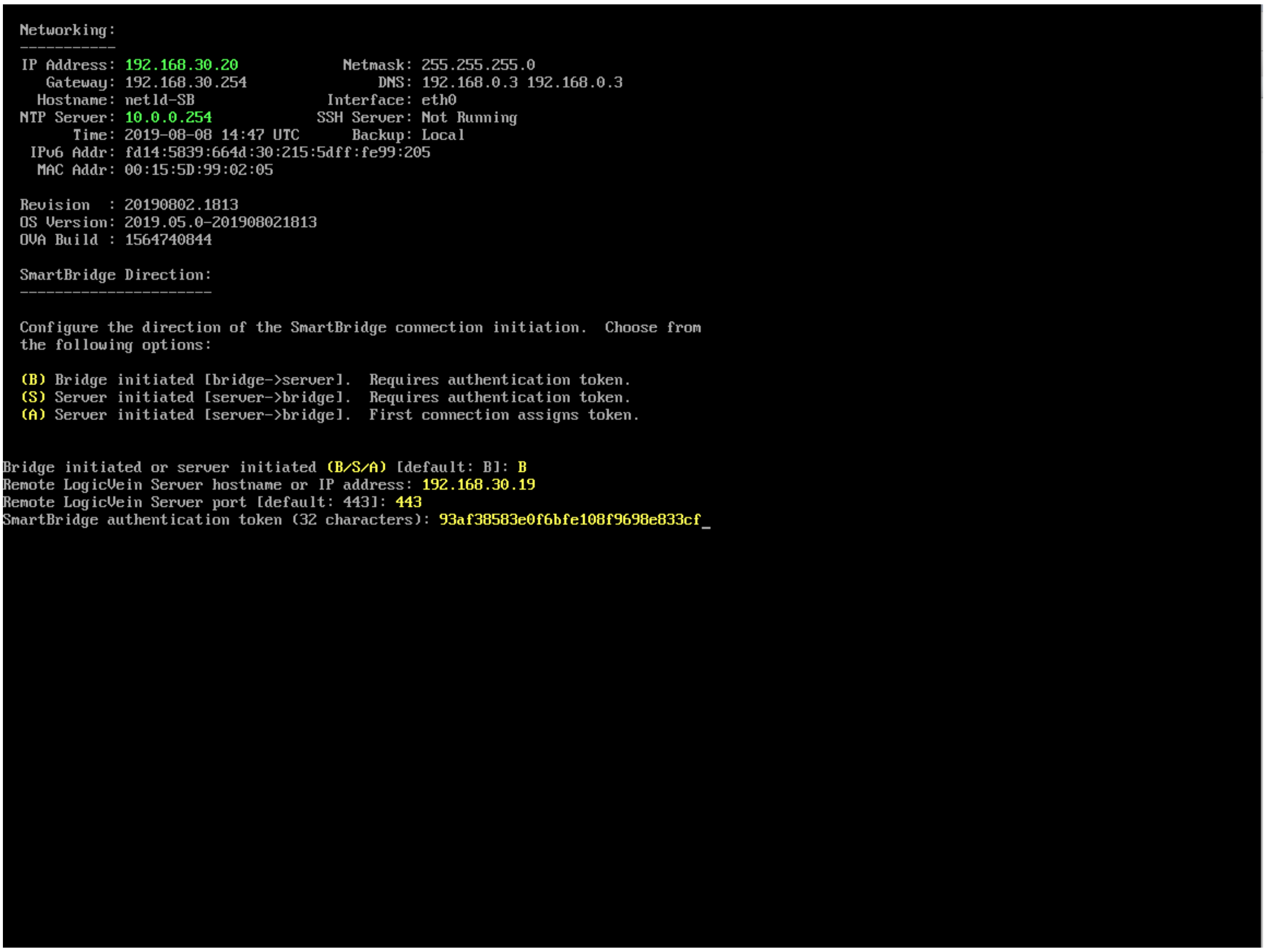
Set the core server information and token in SmartBridge. SmartBridge does not have a web console, so you will need to use the OVA console.

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



```
 LogicVein - SmartBridge


 Networking:
 -----------
  IP Address: 192.168.30.20            Netmask: 255.255.255.0
     Gateway: 192.168.30.254               DNS: 192.168.0.3 192.168.0.3
    Hostname: netld-SB               Interface: eth0
 NTP Server: 10.0.0.254             SSH Server: Not Running
        Time: 2019-08-08 05:37 UTC      Backup: Local
   IPv6 Addr: fd14:5839:664d:30:215:5dff:fe99:205
    MAC Addr: 00:15:5D:99:02:05

 Revision  : 20190802.1813
 OS Version: 2019.05.0-201908021813
 OVA Build : 1564740844

 Settings menu:
 --------------
*[1] Static IP Address
 [2] DHCP
 [3] SSH Server
 [4] SmartBridge Direction
 [5] Reboot
 [6] Power Off
```

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



```
 Networking:
 -----------
  IP Address: 192.168.30.20           Netmask: 255.255.255.0
     Gateway: 192.168.30.254              DNS: 192.168.0.3 192.168.0.3
    Hostname: netld-SB              Interface: eth0
  NTP Server: 10.0.0.254           SSH Server: Not Running
        Time: 2019-08-08 14:47 UTC     Backup: Local
   IPv6 Addr: fd14:5839:664d:30:215:5dff:fe99:205
    MAC Addr: 00:15:5D:99:02:05

 Revision  : 20190802.1813
 OS Version: 2019.05.0-201908021813
 OVA Build : 1564740844

 SmartBridge Direction:
 ----------------------

 Configure the direction of the SmartBridge connection initiation.  Choose from
 the following options:

 (B) Bridge initiated [bridge->server].  Requires authentication token.
 (S) Server initiated [server->bridge].  Requires authentication token.
 (A) Server initiated [server->bridge].  First connection assigns token.


Bridge initiated or server initiated (B/S/A) [default: B]: B
Remote LogicVein Server hostname or IP address: 192.168.30.19
Remote LogicVein Server port [default: 443]: 443
SmartBridge authentication token (32 characters): 93af38583e0f6bfe108f9698e833cf_
```

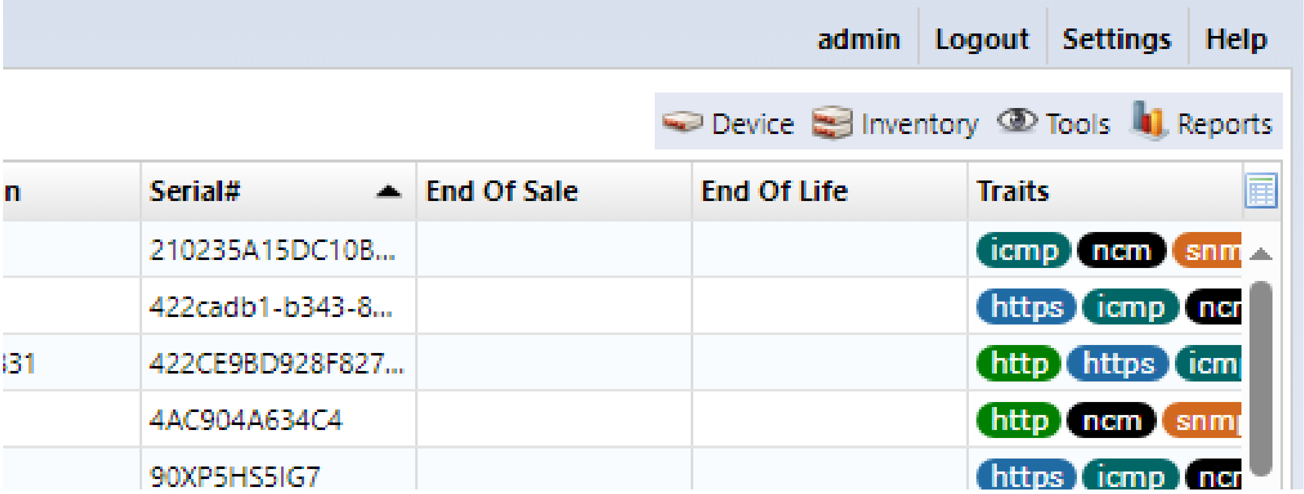
Project	Explanation	Keyboard Selction
Connection Initiation	Connection direction	
	Connect from Bridge to Server (with token)	[B]
	Connect from Server to Bridge (with token)	[S]
	Connect from Server to Bridge (without token)	[A]
Hostname or IP address	Core server (ThirdEye) IP address	`192.168.30.19`
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.

32.7 Managing Devices via SmartBridge

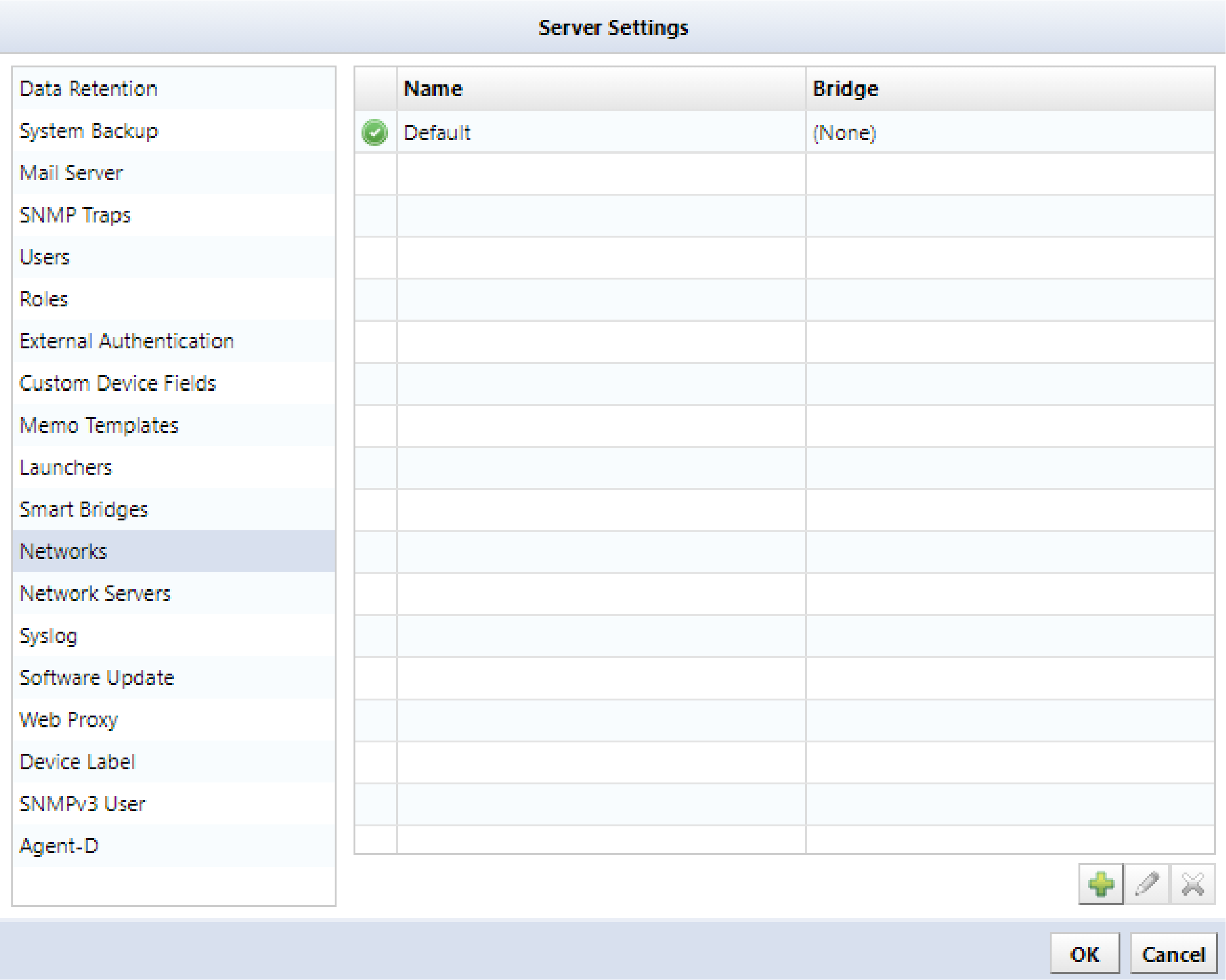
When you want to manage devices with SmartBridge, you will use the Network feature, any devices added to that network will be monitored/managed via SmartBridge.

1. click [Settings].



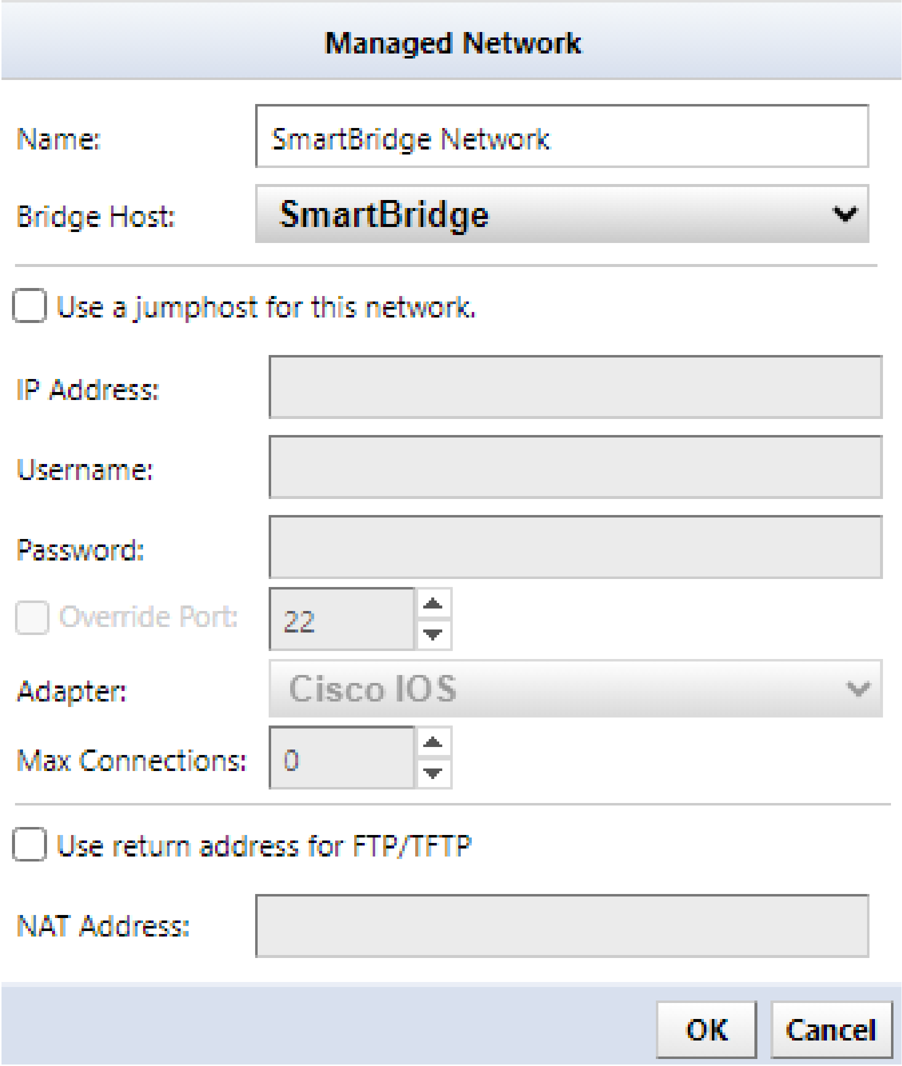
n	Serial#	End Of Sale	End Of Life	Traits
	210235A15DC10B...			icmp ncm snm
	422cadb1-b343-8...			https icmp ncr
31	422CE9BD928F827...			http https icm
	4AC904A634C4			http ncm snm
	90XP5HS5IG7			https icmp ncr

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



	Name	Bridge
✓	Default	(None)

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



Managed Network

Name: SmartBridge Network

Bridge Host: SmartBridge

□ Use a jumphost for this network.

IP Address:

Username:

Password:

□ Override Port: 22

Adapter: Cisco IOS

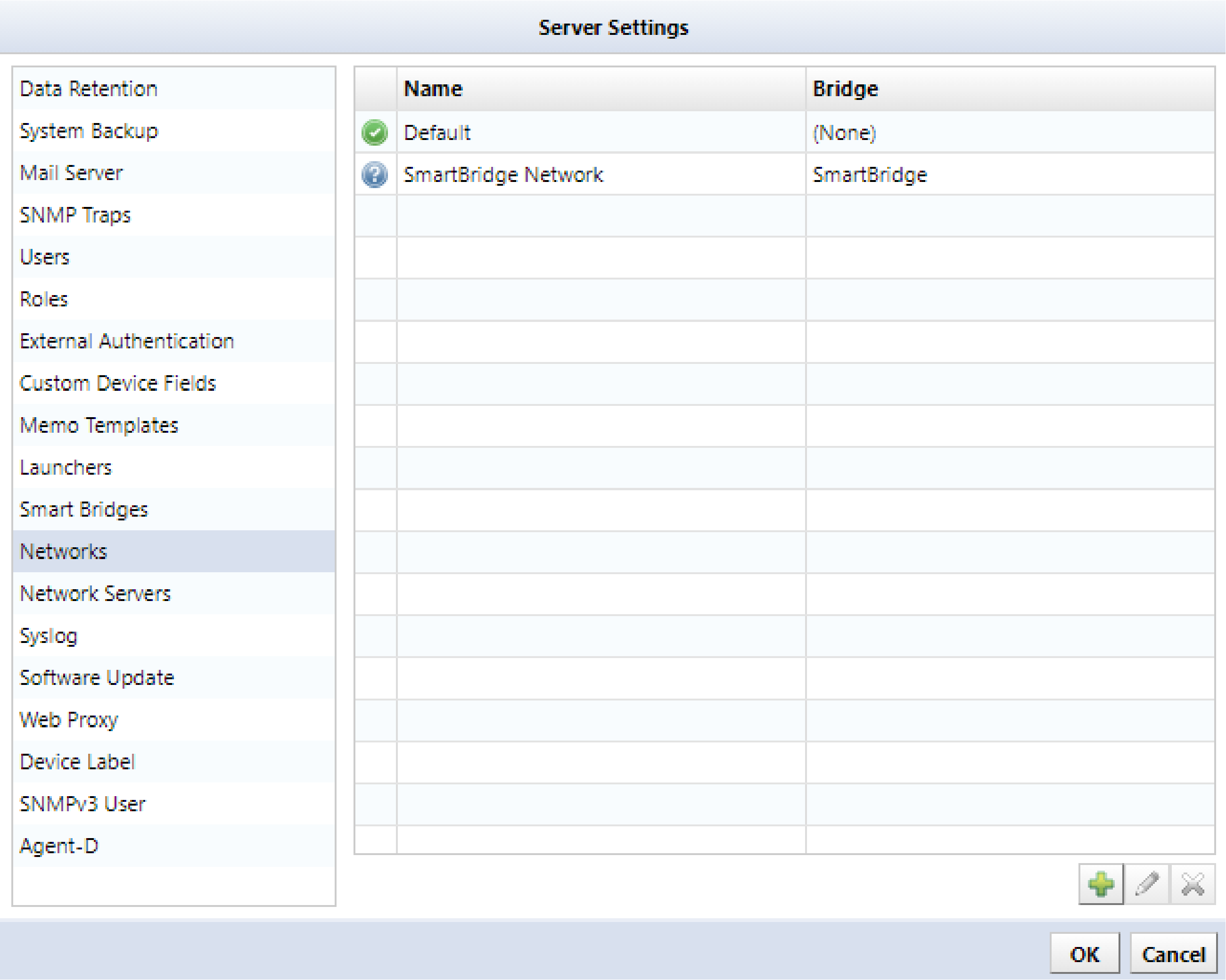
Max Connections: 0

□ Use return address for FTP/TFTP

NAT Address:

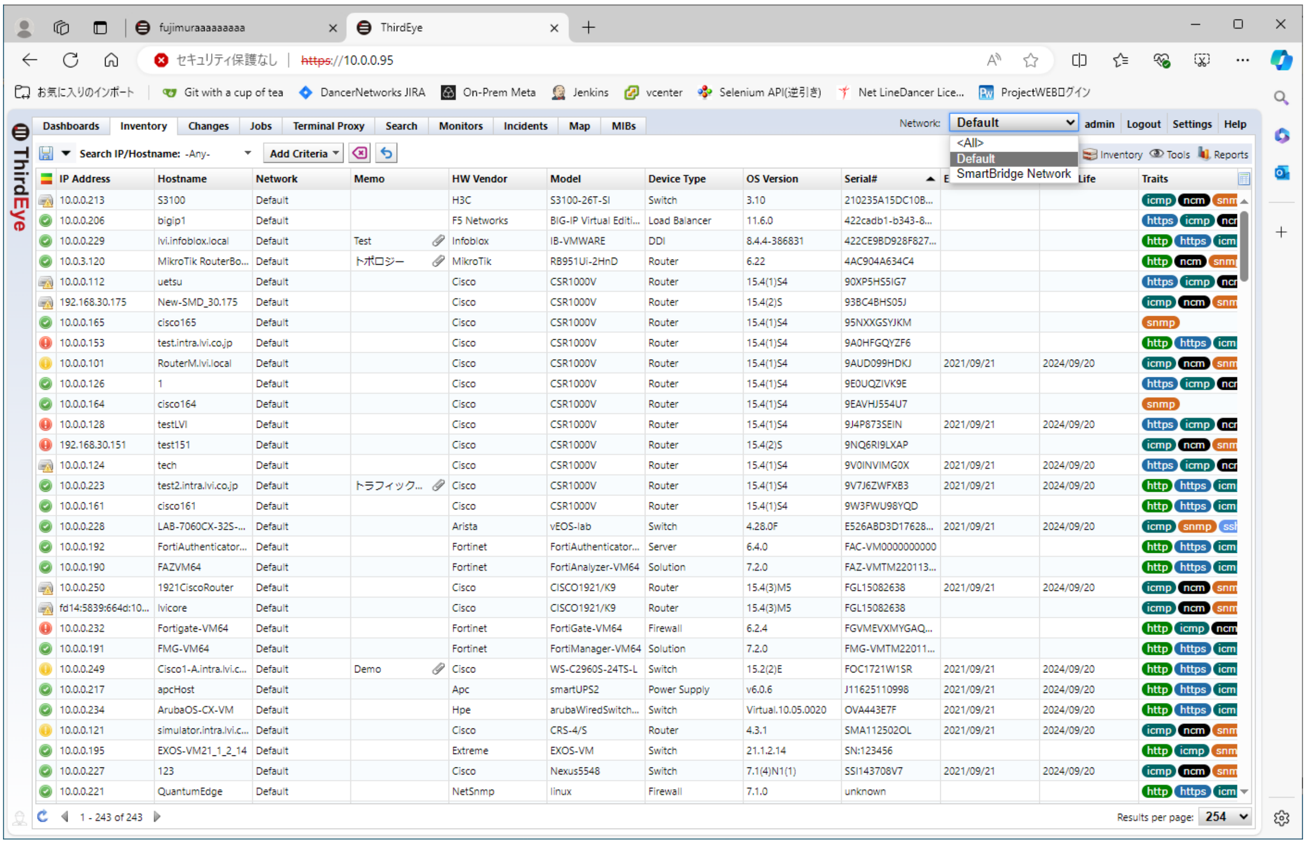
4. Click [OK]

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



	Name	Bridge
✓	Default	(None)
?	SmartBridge Network	SmartBridge

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.



Network: Default

<All>
Default
SmartBridge Network

Search IP/Hostname: -Any-

	IP Address	Hostname	Network	Memo	HW Vendor	Model	Device Type	OS Version	Serial# ▲	E	Life	Traits
⚠	10.0.0.213	S3100	Default		H3C	S3100-26T-SI	Switch	3.10	210235A15DC10B...			icmp ncm snm
✓	10.0.0.206	bigip1	Default		F5 Networks	BIG-IP Virtual Editi...	Load Balancer	11.6.0	422cadb1-b343-8...			https icmp ncr
✓	10.0.0.229	lvi.infoblox.local	Default	Test	Infoblox	IB-VMWARE	DDI	8.4.4-386831	422CE9BD928F827...			http https icm
✓	10.0.3.120	MikroTik RouterBo...	Default	トポロジー	MikroTik	RB951Ui-2HnD	Router	6.22	4AC904A634C4			http ncm snm
⚠	10.0.0.112	uetsu	Default		Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7			https icmp ncr
⚠	192.168.30.175	New-SMD_30.175	Default		Cisco	CSR1000V	Router	15.4(2)S	93BC4BHS05J			icmp ncm snm
✓	10.0.0.165	cisco165	Default		Cisco	CSR1000V	Router	15.4(1)S4	95NXXGSYJKM			snmp
❗	10.0.0.153	test.intra.lvi.co.jp	Default		Cisco	CSR1000V	Router	15.4(1)S4	9A0HFGQYZF6			http https icm
!	10.0.0.101	RouterM.lvi.local	Default		Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	2021/09/21	2024/09/20	icmp ncm snm
✓	10.0.0.126	1	Default		Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E			https icmp ncr
✓	10.0.0.164	cisco164	Default		Cisco	CSR1000V	Router	15.4(1)S4	9EAVHJ554U7			snmp
❗	10.0.0.128	testLVI	Default		Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEIN	2021/09/21	2024/09/20	https icmp ncr
❗	192.168.30.151	test151	Default		Cisco	CSR1000V	Router	15.4(2)S	9NQ6RI9LXAP			icmp ncm snm
⚠	10.0.0.124	tech	Default		Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	2021/09/21	2024/09/20	https icmp ncr
✓	10.0.0.223	test2.intra.lvi.co.jp	Default	トラフィック...	Cisco	CSR1000V	Router	15.4(1)S4	9V7J6ZWFXB3	2021/09/21	2024/09/20	http https icm
✓	10.0.0.161	cisco161	Default		Cisco	CSR1000V	Router	15.4(1)S4	9W3FWU98YQD			http https icm
✓	10.0.0.228	LAB-7060CX-32S-...	Default		Arista	vEOS-lab	Switch	4.28.0F	E526ABD3D17628...	2021/09/21	2024/09/20	icmp snmp ssh
✓	10.0.0.192	FortiAuthenticator...	Default		Fortinet	FortiAuthenticator...	Server	6.4.0	FAC-VM0000000000			http https icm
✓	10.0.0.190	FAZVM64	Default		Fortinet	FortiAnalyzer-VM64	Solution	7.2.0	FAZ-VMTM220113...			http https icm
⚠	10.0.0.250	1921CiscoRouter	Default		Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	2021/09/21	2024/09/20	icmp ncm snm
⚠	fd14:5839:664d:10...	lvicore	Default		Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638			icmp ncm snm
❗	10.0.0.232	Fortigate-VM64	Default		Fortinet	FortiGate-VM64	Firewall	6.2.4	FGVMEVXMYGAQ...			http icmp ncm
✓	10.0.0.191	FMG-VM64	Default		Fortinet	FortiManager-VM64	Solution	7.2.0	FMG-VMTM22011...			http https icm
!	10.0.0.249	Cisco1-A.intra.lvi.c...	Default	Demo	Cisco	WS-C2960S-24TS-L	Switch	15.2(2)E	FOC1721W1SR	2021/09/21	2024/09/20	http https icm
✓	10.0.0.217	apcHost	Default		Apc	smartUPS2	Power Supply	v6.0.6	J11625110998	2021/09/21	2024/09/20	http https icm
✓	10.0.0.234	ArubaOS-CX-VM	Default		Hpe	arubaWiredSwitch...	Switch	Virtual.10.05.0020	OVA443E7F	2021/09/21	2024/09/20	http https icm
!	10.0.0.121	simulator.intra.lvi.c...	Default		Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	2021/09/21	2024/09/20	icmp ncm snm
✓	10.0.0.195	EXOS-VM21_1_2_14	Default		Extreme	EXOS-VM	Switch	21.1.2.14	SN:123456			http icmp snm
✓	10.0.0.227	123	Default		Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	2021/09/21	2024/09/20	icmp ncm snm
✓	10.0.0.221	QuantumEdge	Default		NetSnmp	linux	Firewall	7.1.0	unknown			http https icm

1 - 243 of 243

Results per page: 254

SECTION 33

HA (ACTIVE/STANDBY)

ThirdEye has supported the High Availability (HA) Active/Standby feature since r20241218.0941.

HA provides system redundancy through paired primary (active) and standby servers. The primary server handles all monitoring and configuration operations, while the standby maintains real-time synchronization. Attached files are synchronized per 120 seconds with standby server.

HA uses **active** and **standby** as a roles.

For **active** server, ThirdEye manages devices or monitor devices.

For **standby** server, it receives transaction log (WAL) from active server and performs synchronization by recovering it.

33.1 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.

33.2 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

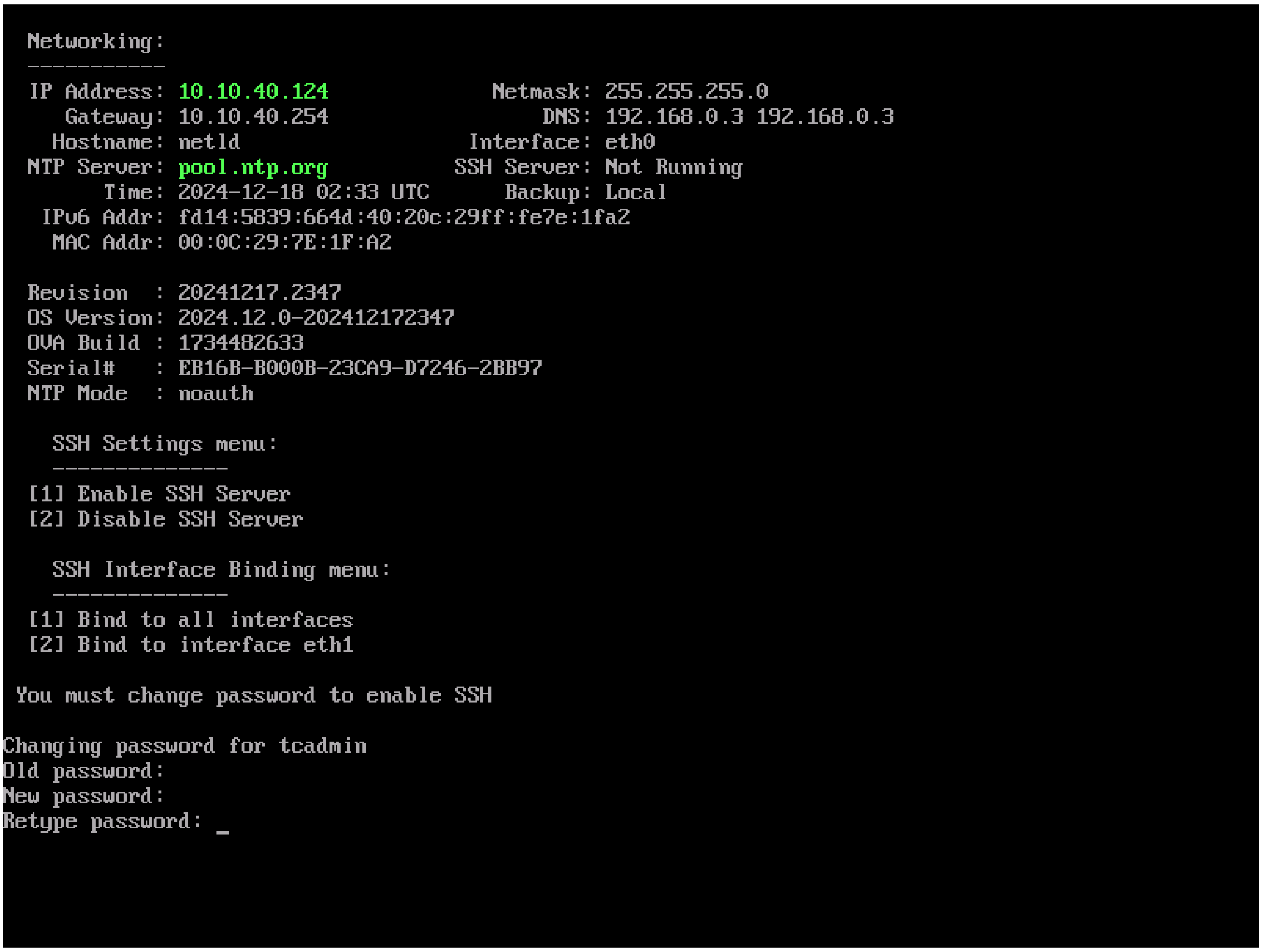
33.3 Settings

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

33.4 Procedure

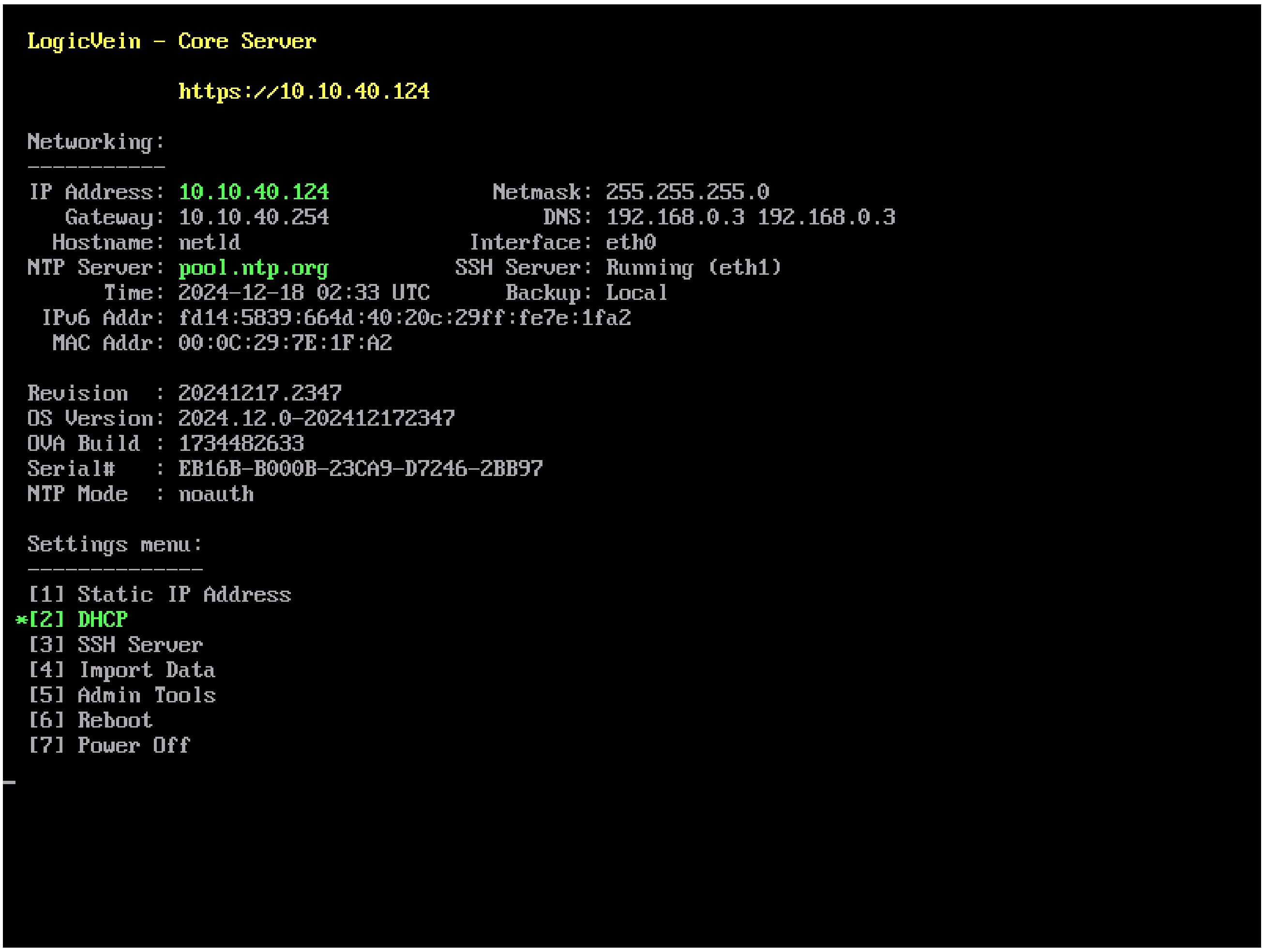
Before configuring, set IP addresses on the eth1 interfaces of the primary and standby server so that communication is possible between eth1.

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.



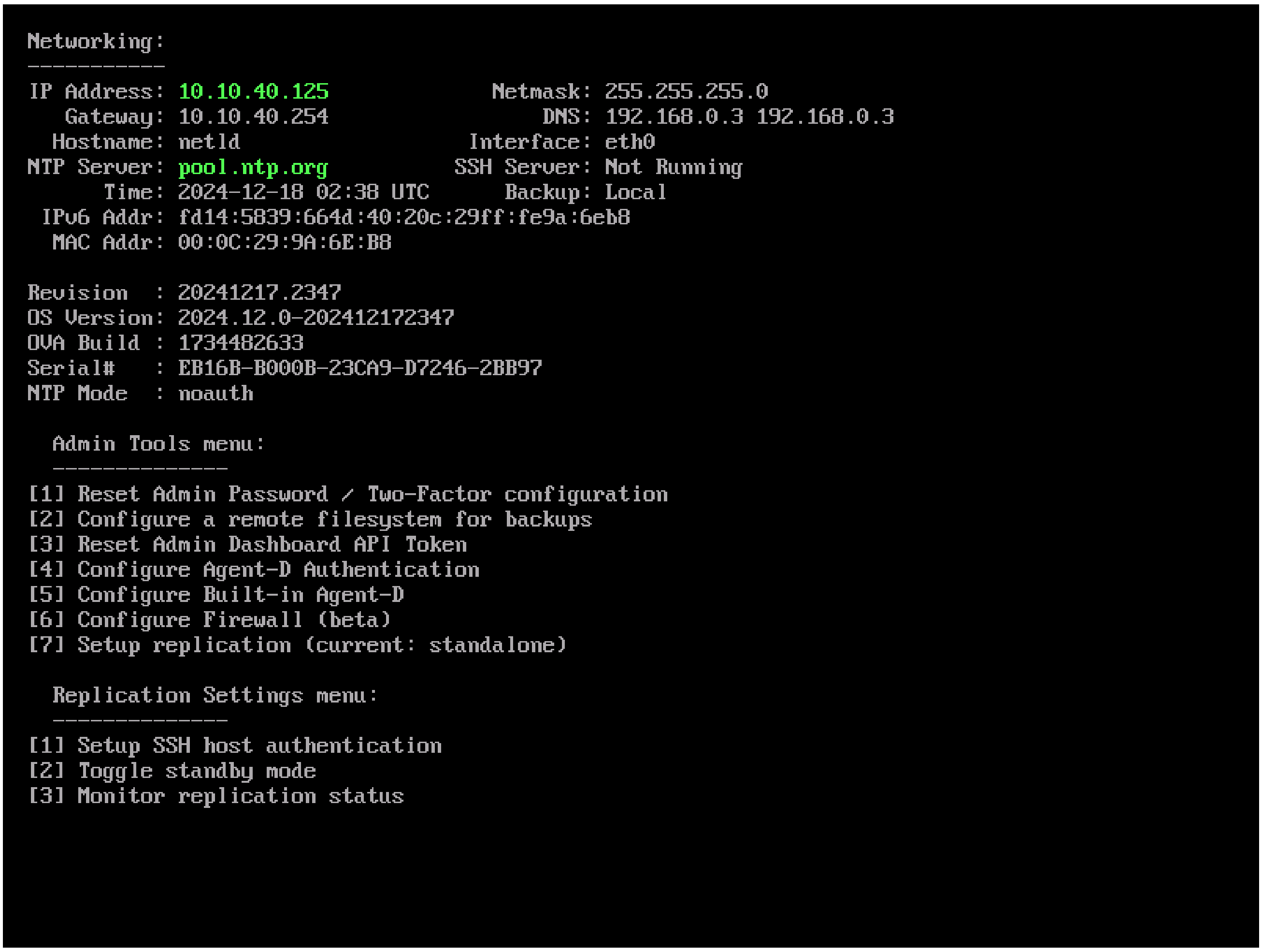
```
 Networking:
 -----------
 IP Address: 10.10.40.124             Netmask: 255.255.255.0
    Gateway: 10.10.40.254                 DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                  Interface: eth0
 NTP Server: pool.ntp.org          SSH Server: Not Running
       Time: 2024-12-18 02:33 UTC      Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe7e:1fa2
   MAC Addr: 00:0C:29:7E:1F:A2

 Revision  : 20241217.2347
 OS Version: 2024.12.0-202412172347
 OVA Build : 1734482633
 Serial#   : EB16B-B000B-23CA9-D7246-2BB97
 NTP Mode  : noauth

   SSH Settings menu:
   --------------
 [1] Enable SSH Server
 [2] Disable SSH Server

   SSH Interface Binding menu:
   ------------
 [1] Bind to all interfaces
 [2] Bind to interface eth1

 You must change password to enable SSH

Changing password for tcadmin
Old password:
New password:
Retype password: _
```

3. Confirm that the SSH Server is Running.



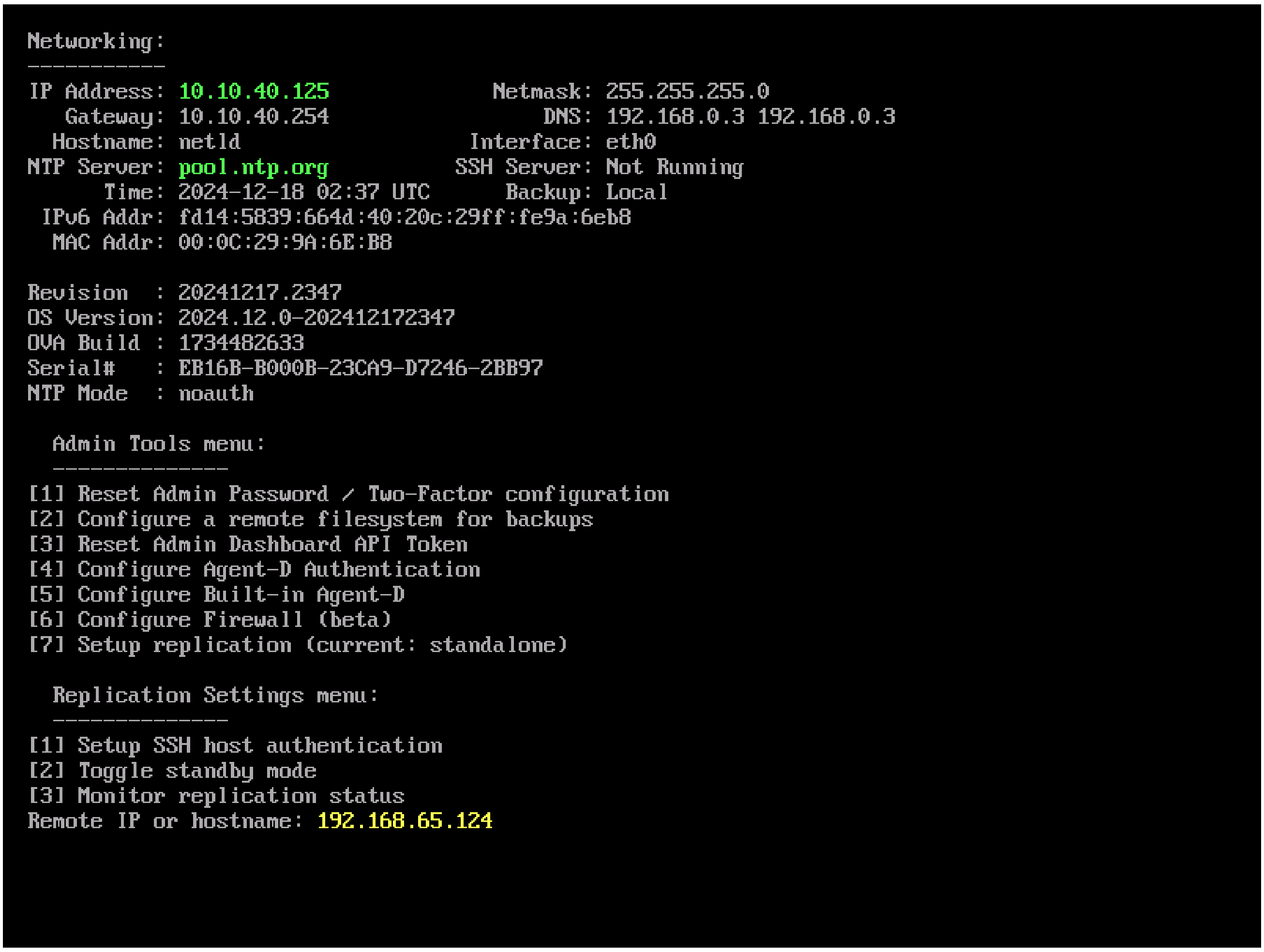
```
LogicVein - Core Server

            https://10.10.40.124

Networking:
-----------
IP Address: 10.10.40.124            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Running (eth1)
      Time: 2024-12-18 02:33 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe7e:1fa2
  MAC Addr: 00:0C:29:7E:1F:A2

Revision  : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

Settings menu:
--------------
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
```

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.



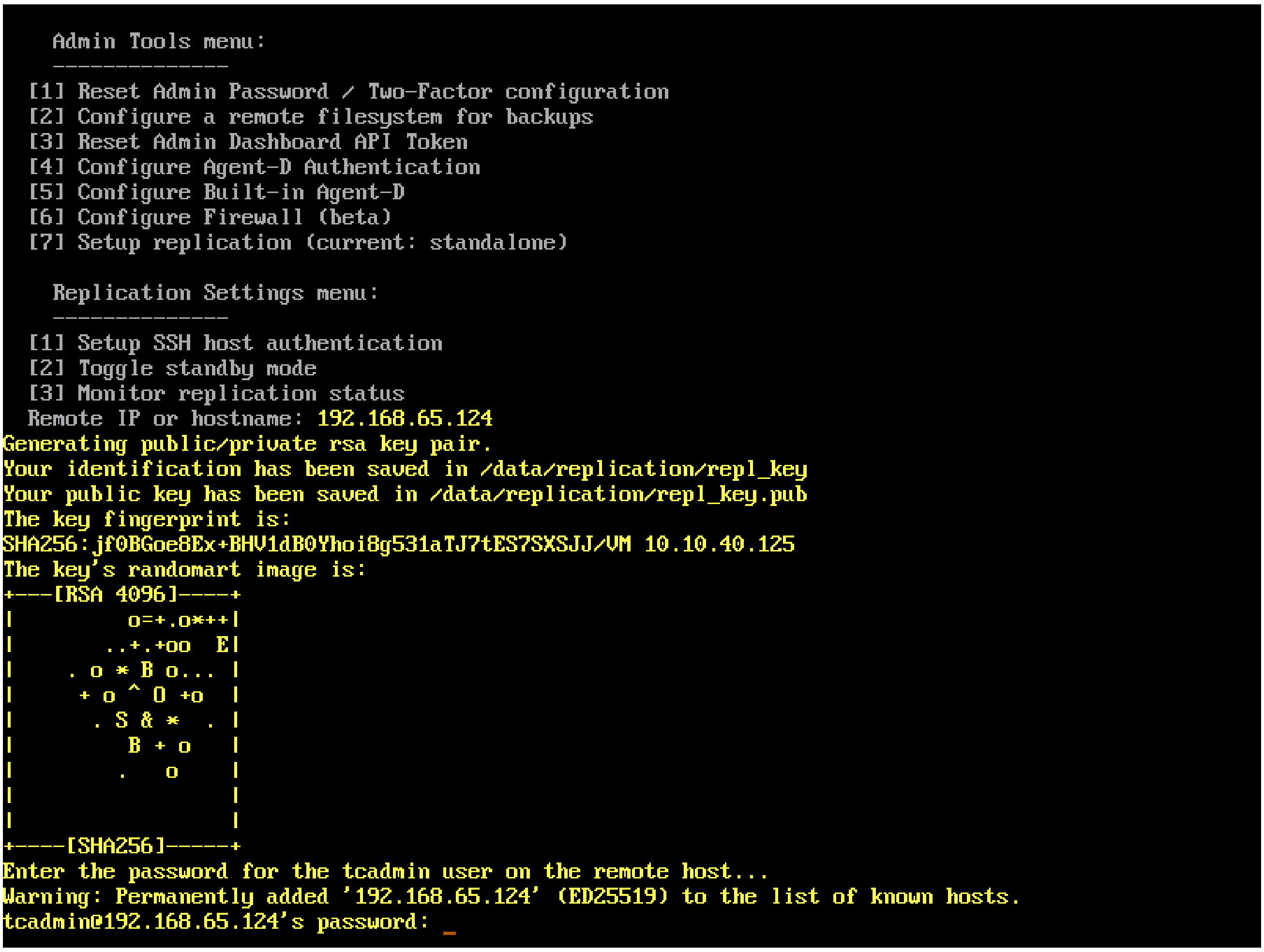
```
Networking:
-----------
IP Address: 10.10.40.125            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 02:38 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8
  MAC Addr: 00:0C:29:9A:6E:B8

Revision  : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
```

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



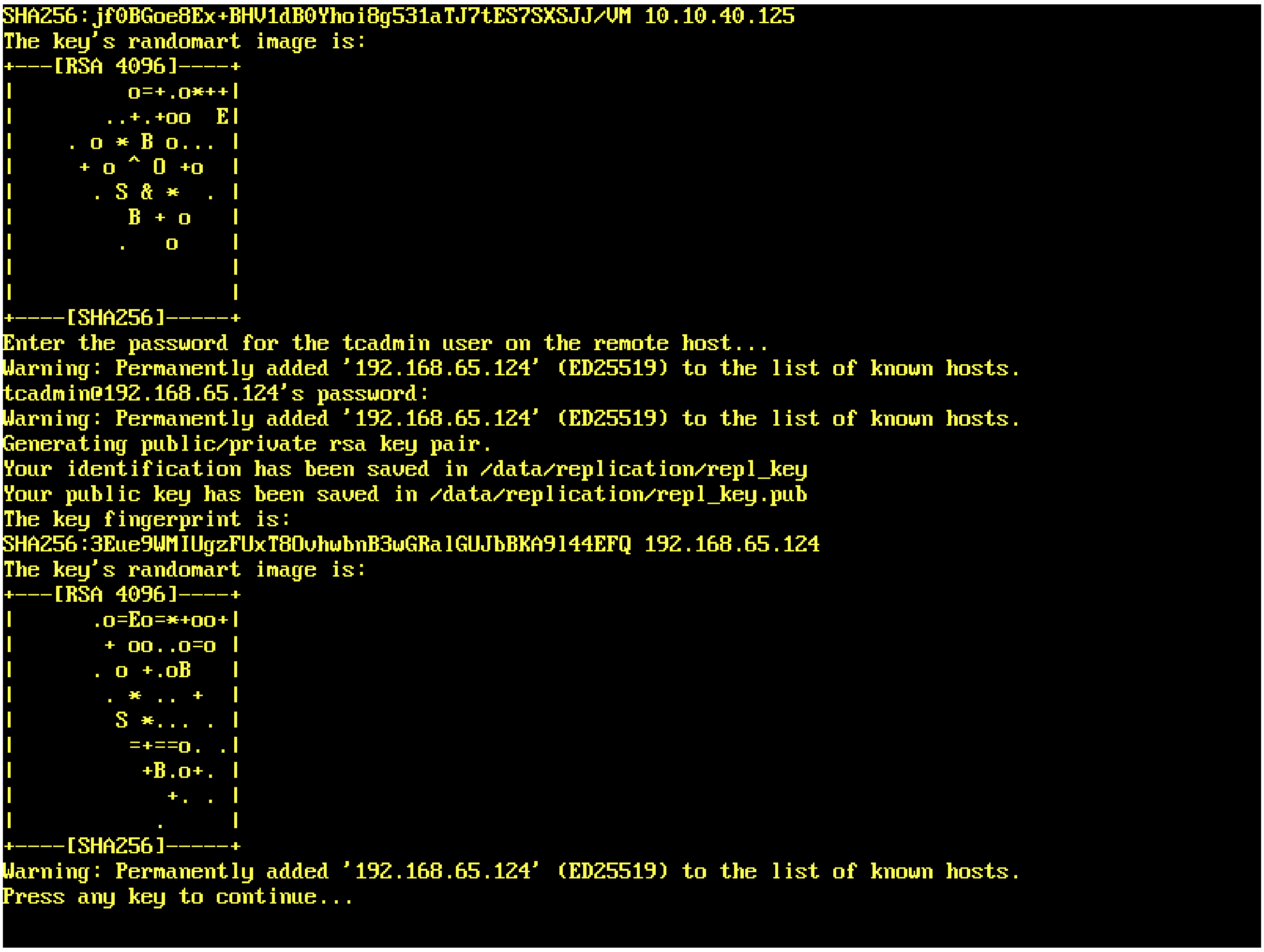
```
Networking:
-----------
IP Address: 10.10.40.125            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 02:37 UTC      Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8
  MAC Addr: 00:0C:29:9A:6E:B8

Revision  : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
Remote IP or hostname: 192.168.65.124
```

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



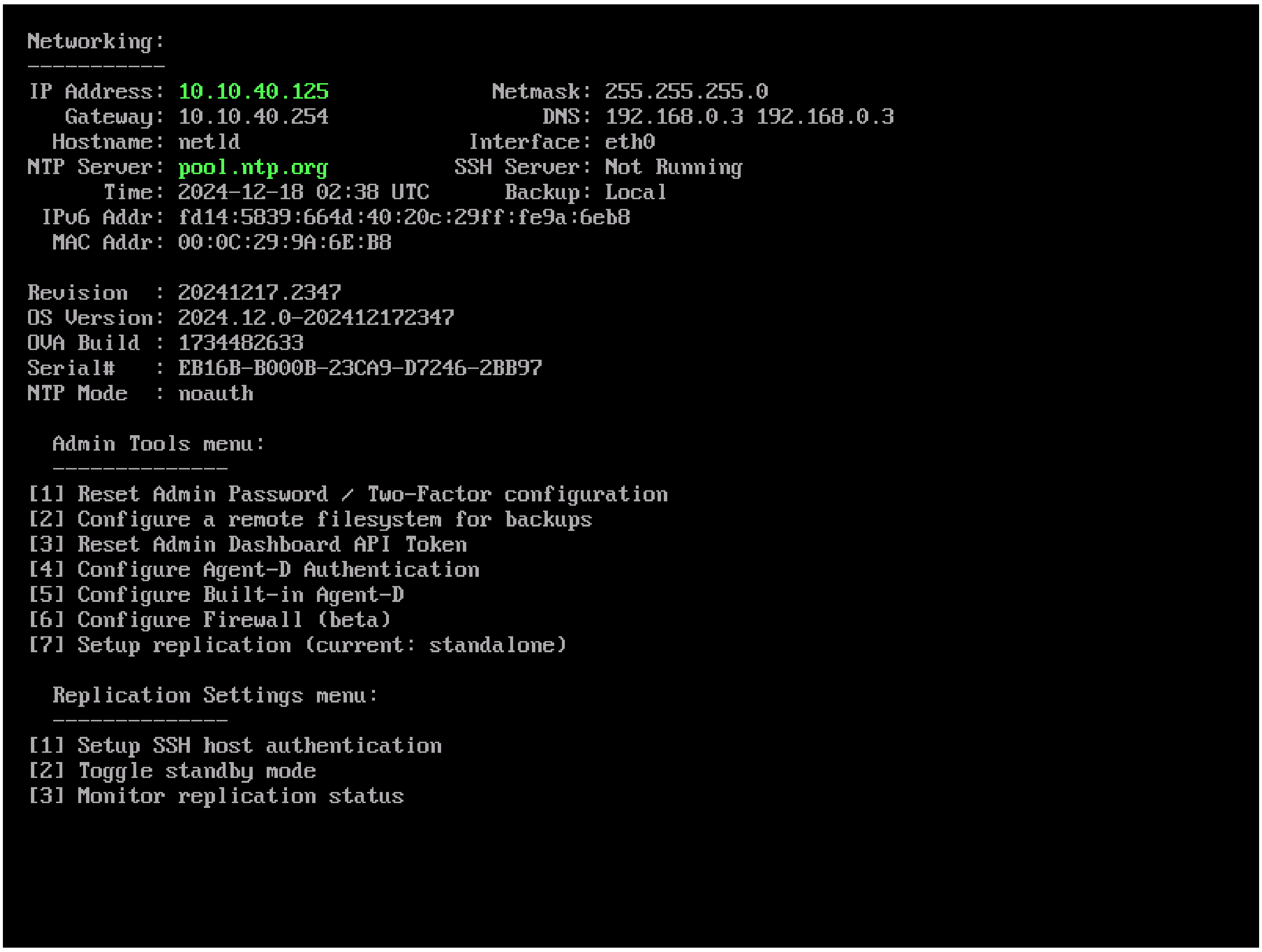
```
    Admin Tools menu:
    ---------------
  [1] Reset Admin Password / Two-Factor configuration
  [2] Configure a remote filesystem for backups
  [3] Reset Admin Dashboard API Token
  [4] Configure Agent-D Authentication
  [5] Configure Built-in Agent-D
  [6] Configure Firewall (beta)
  [7] Setup replication (current: standalone)

    Replication Settings menu:
    ---------------
  [1] Setup SSH host authentication
  [2] Toggle standby mode
  [3] Monitor replication status
  Remote IP or hostname: 192.168.65.124
Generating public/private rsa key pair.
Your identification has been saved in /data/replication/repl_key
Your public key has been saved in /data/replication/repl_key.pub
The key fingerprint is:
SHA256:jf0BGoe8Ex+BHV1dB0Yhoi8g531aTJ7tES7SXSJJ/VM 10.10.40.125
The key's randomart image is:
+---[RSA 4096]----+
|         o=+.o*++|
|       ..+.+oo  E|
|    . o * B o... |
|     + o ^ O +o  |
|      . S & *  . |
|         B + o   |
|        .   o    |
|                 |
|                 |
+----[SHA256]-----+
Enter the password for the tcadmin user on the remote host...
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
tcadmin@192.168.65.124's password: _
```

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



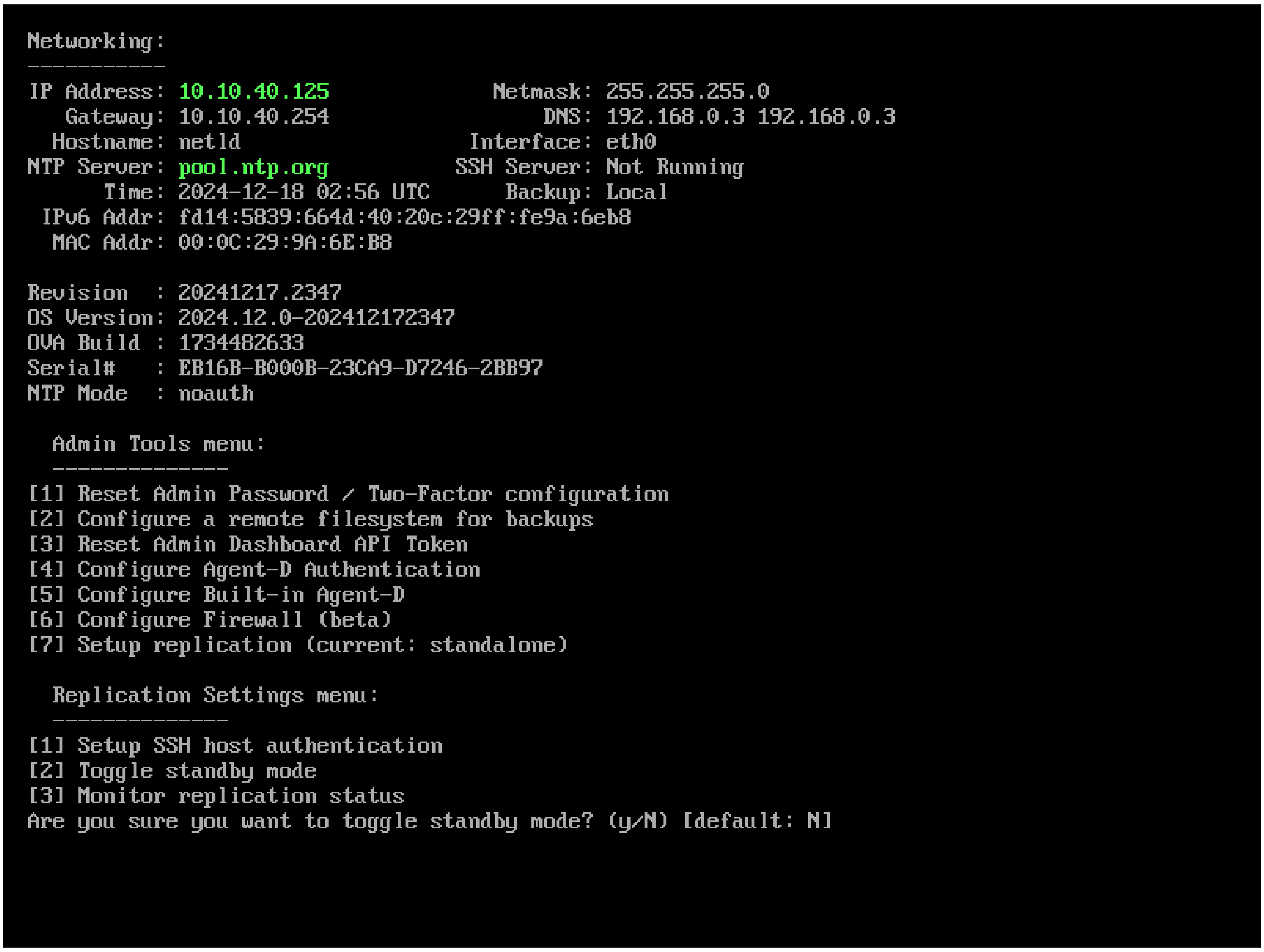
```
SHA256:jf0BGoe8Ex+BHV1dB0Yhoi8g531aTJ7tES7SXSJJ/VM 10.10.40.125
The key's randomart image is:
+---[RSA 4096]----+
|         o=+.o*++|
|       ..+.+oo  E|
|    . o * B o... |
|     + o ^ O +o  |
|      . S & *  . |
|         B + o   |
|        .   o    |
|                 |
|                 |
+----[SHA256]-----+
Enter the password for the tcadmin user on the remote host...
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
tcadmin@192.168.65.124's password:
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
Generating public/private rsa key pair.
Your identification has been saved in /data/replication/repl_key
Your public key has been saved in /data/replication/repl_key.pub
The key fingerprint is:
SHA256:3Eue9WMIUgzFUxT8OvhwbnB3wGRalGUJbBKA9l44EFQ 192.168.65.124
The key's randomart image is:
+---[RSA 4096]----+
|      .o=Eo=*+oo+|
|       + oo..o=o |
|      . o +.oB   |
|       . * .. +  |
|        S *... . |
|         =+==o. .|
|          +B.o+. |
|            +. . |
|           .     |
+----[SHA256]-----+
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
Press any key to continue...
```

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.



```
Networking:
-----------
IP Address: 10.10.40.125            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 02:38 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8
  MAC Addr: 00:0C:29:9A:6E:B8

Revision  : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
```

10. Press [Y].



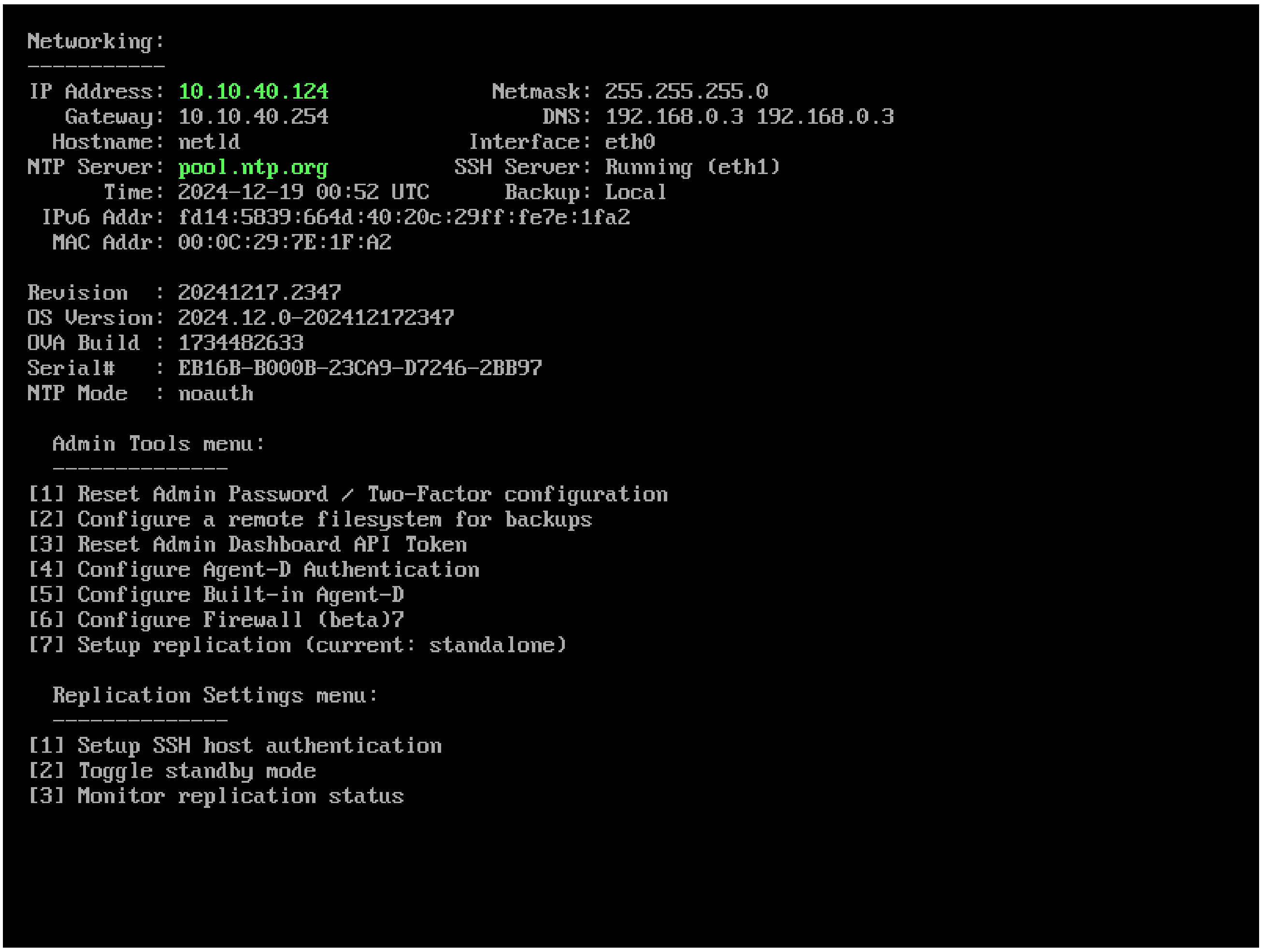
```
Networking:
-----------
IP Address: 10.10.40.125            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 02:56 UTC      Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8
  MAC Addr: 00:0C:29:9A:6E:B8

Revision  : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
Are you sure you want to toggle standby mode? (y/N) [default: N]
```

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

33.5 Confirm Status

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

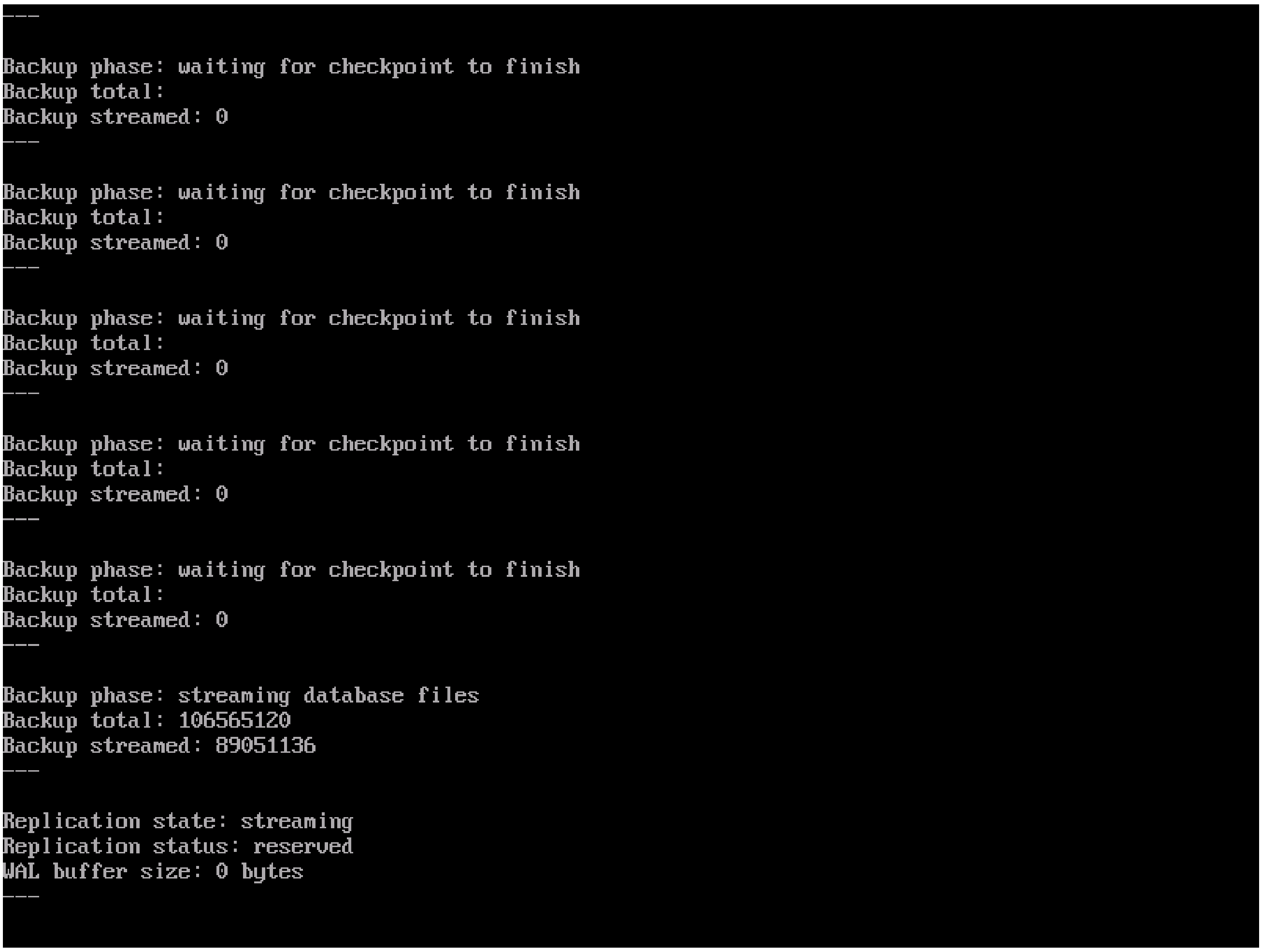
1. Connect to the OVA console of the primary server.
2. Press [5] (Admin Tools) > [7] (Setup replication) > [3] (Monitor replication status) on the keyboard to check the status.



```
Networking:
-----------
IP Address: 10.10.40.124             Netmask: 255.255.255.0
   Gateway: 10.10.40.254                 DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                  Interface: eth0
NTP Server: pool.ntp.org          SSH Server: Running (eth1)
      Time: 2024-12-19 00:52 UTC      Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe7e:1fa2
  MAC Addr: 00:0C:29:7E:1F:A2

Revision   : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build  : 1734482633
Serial#    : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode   : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)7
[7] Setup replication (current: standalone)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
```

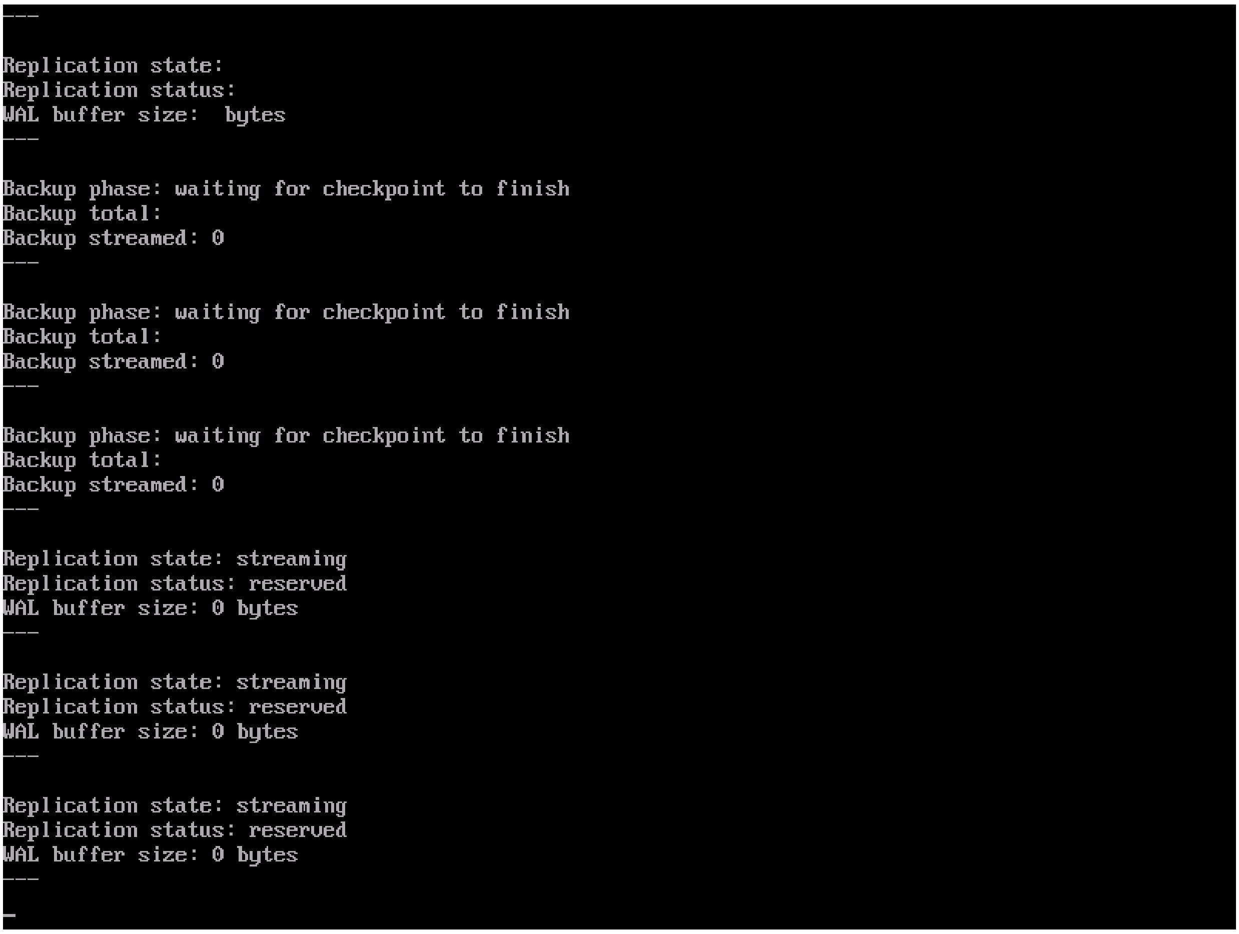
The status will be updated automatically when it is displayed. To close the status screen, press [Ctrl+C].

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.



```
---

Replication state:
Replication status:
WAL buffer size:  bytes
---

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
---

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

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

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

_
```

33.6 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.

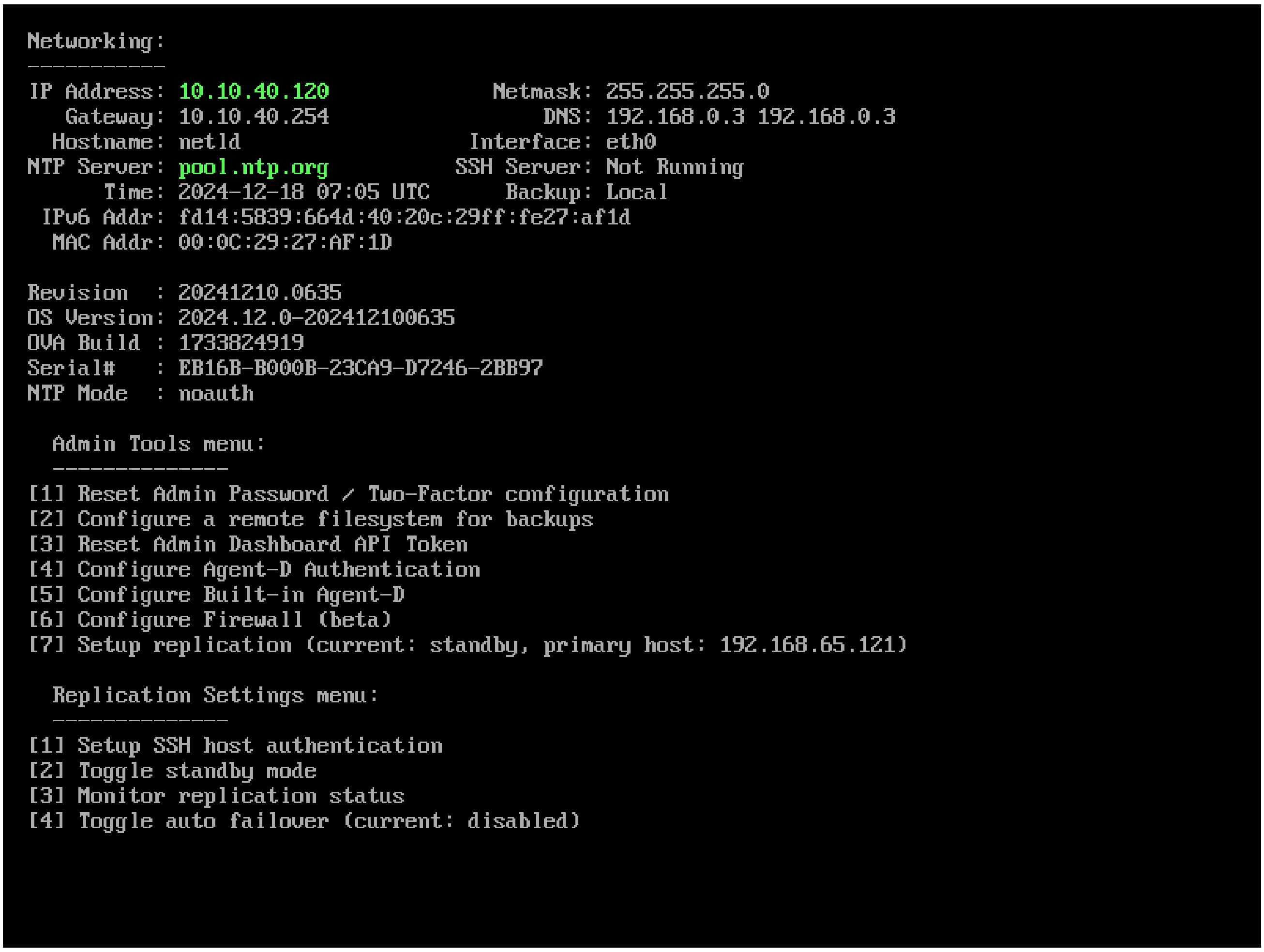
33.7 Failover

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.

33.7.1 Manual Failover

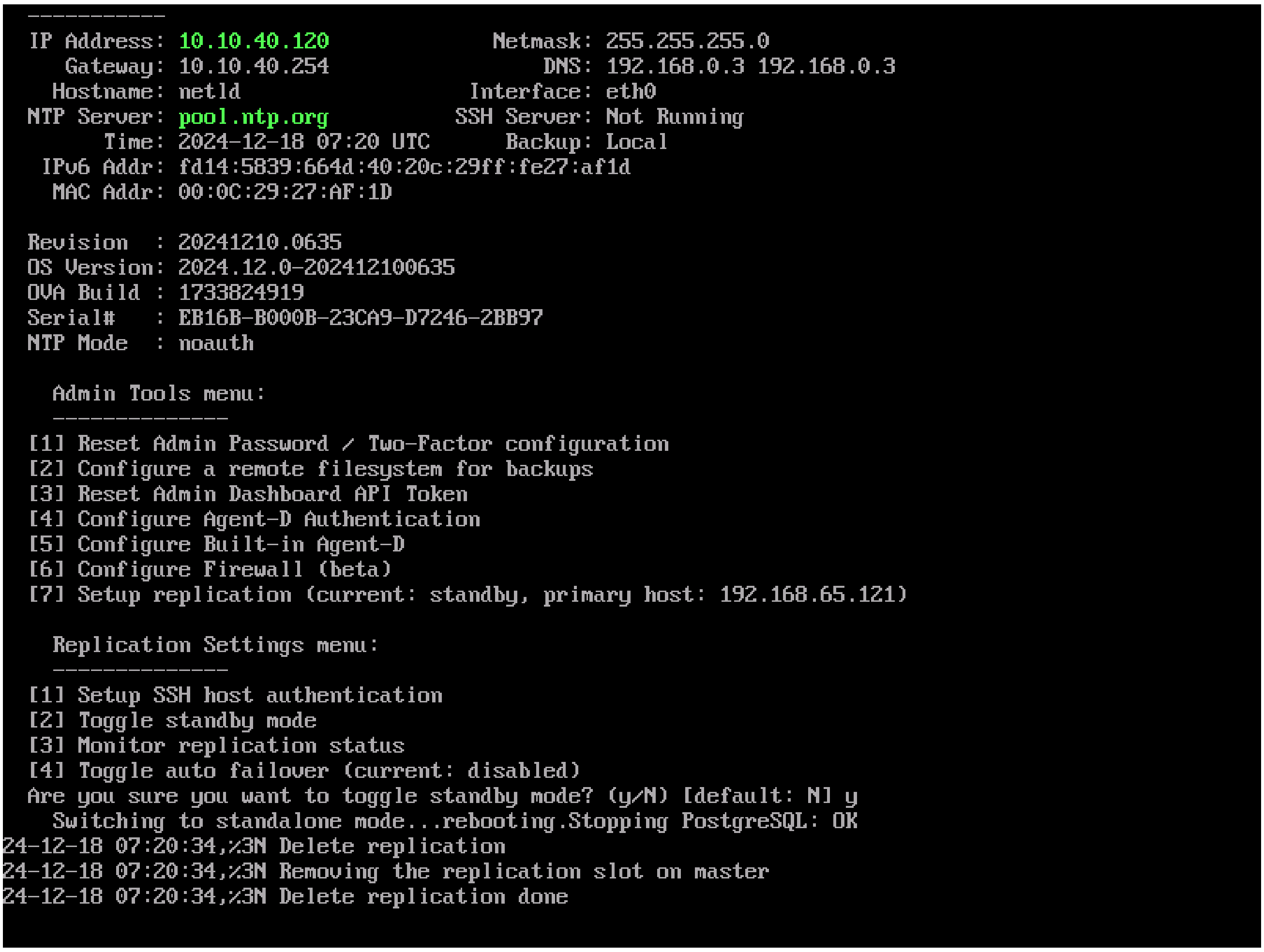
To monitor on an active server, change the role from standby to active. The change procedure is as follows.

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.



```
Networking:
-----------
IP Address: 10.10.40.120            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 07:05 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
  MAC Addr: 00:0C:29:27:AF:1D

Revision  : 20241210.0635
OS Version: 2024.12.0-202412100635
OVA Build : 1733824919
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standby, primary host: 192.168.65.121)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
[4] Toggle auto failover (current: disabled)
```

3. Press [Y].



```
  -----------
  IP Address: 10.10.40.120            Netmask: 255.255.255.0
     Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
    Hostname: netld                 Interface: eth0
  NTP Server: pool.ntp.org         SSH Server: Not Running
        Time: 2024-12-18 07:20 UTC     Backup: Local
    IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
    MAC Addr: 00:0C:29:27:AF:1D

  Revision  : 20241210.0635
  OS Version: 2024.12.0-202412100635
  OVA Build : 1733824919
  Serial#   : EB16B-B000B-23CA9-D7246-2BB97
  NTP Mode  : noauth

    Admin Tools menu:
    --------------
  [1] Reset Admin Password / Two-Factor configuration
  [2] Configure a remote filesystem for backups
  [3] Reset Admin Dashboard API Token
  [4] Configure Agent-D Authentication
  [5] Configure Built-in Agent-D
  [6] Configure Firewall (beta)
  [7] Setup replication (current: standby, primary host: 192.168.65.121)

    Replication Settings menu:
    --------------
  [1] Setup SSH host authentication
  [2] Toggle standby mode
  [3] Monitor replication status
  [4] Toggle auto failover (current: disabled)
  Are you sure you want to toggle standby mode? (y/N) [default: N] y
    Switching to standalone mode...rebooting.Stopping PostgreSQL: OK
24-12-18 07:20:34,%3N Delete replication
24-12-18 07:20:34,%3N Removing the replication slot on master
24-12-18 07:20:34,%3N Delete replication done
```

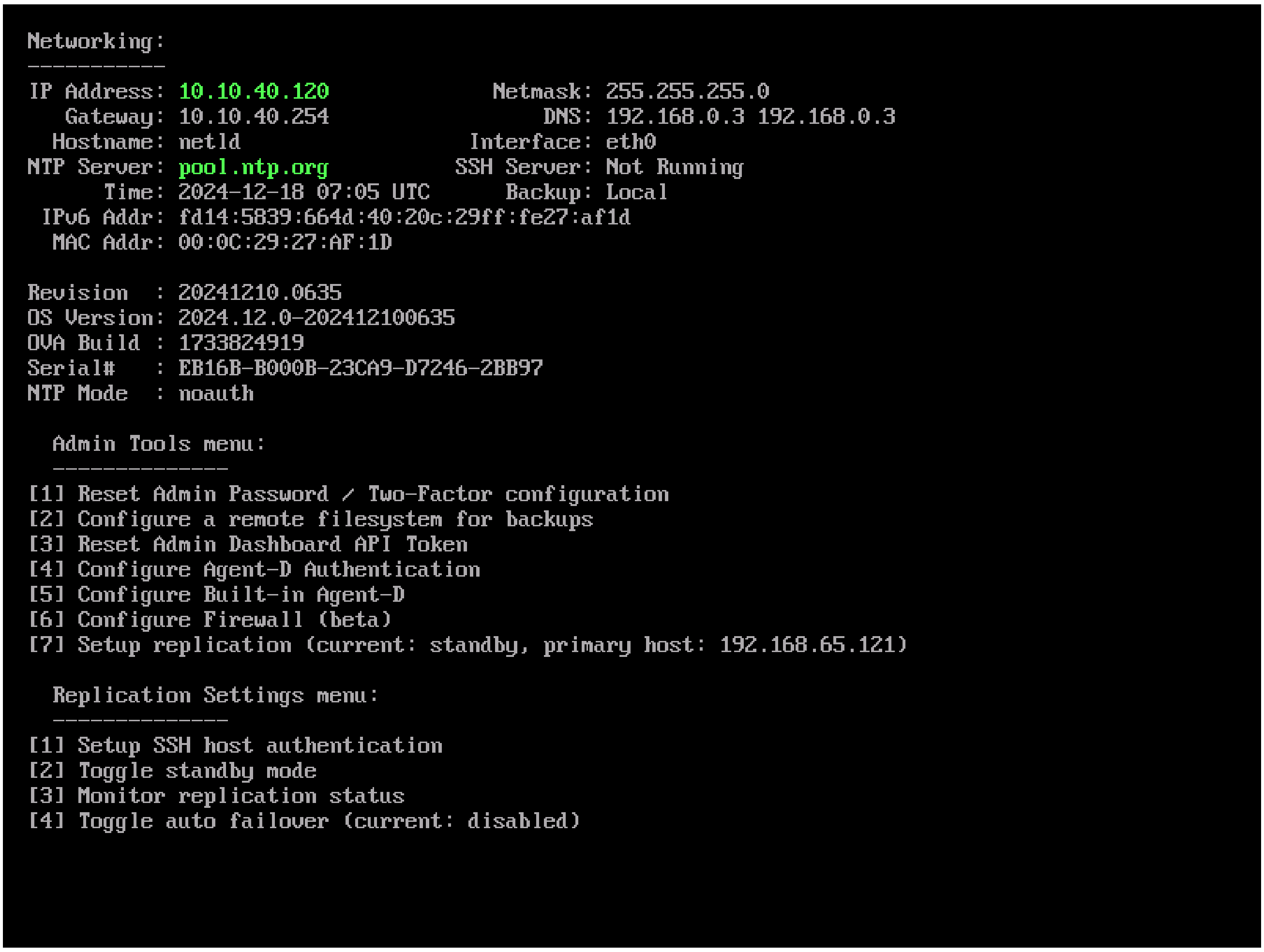
Press [Y] to automatically restart the standby server. After restarting, please log in from a web browser.

33.7.2 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.

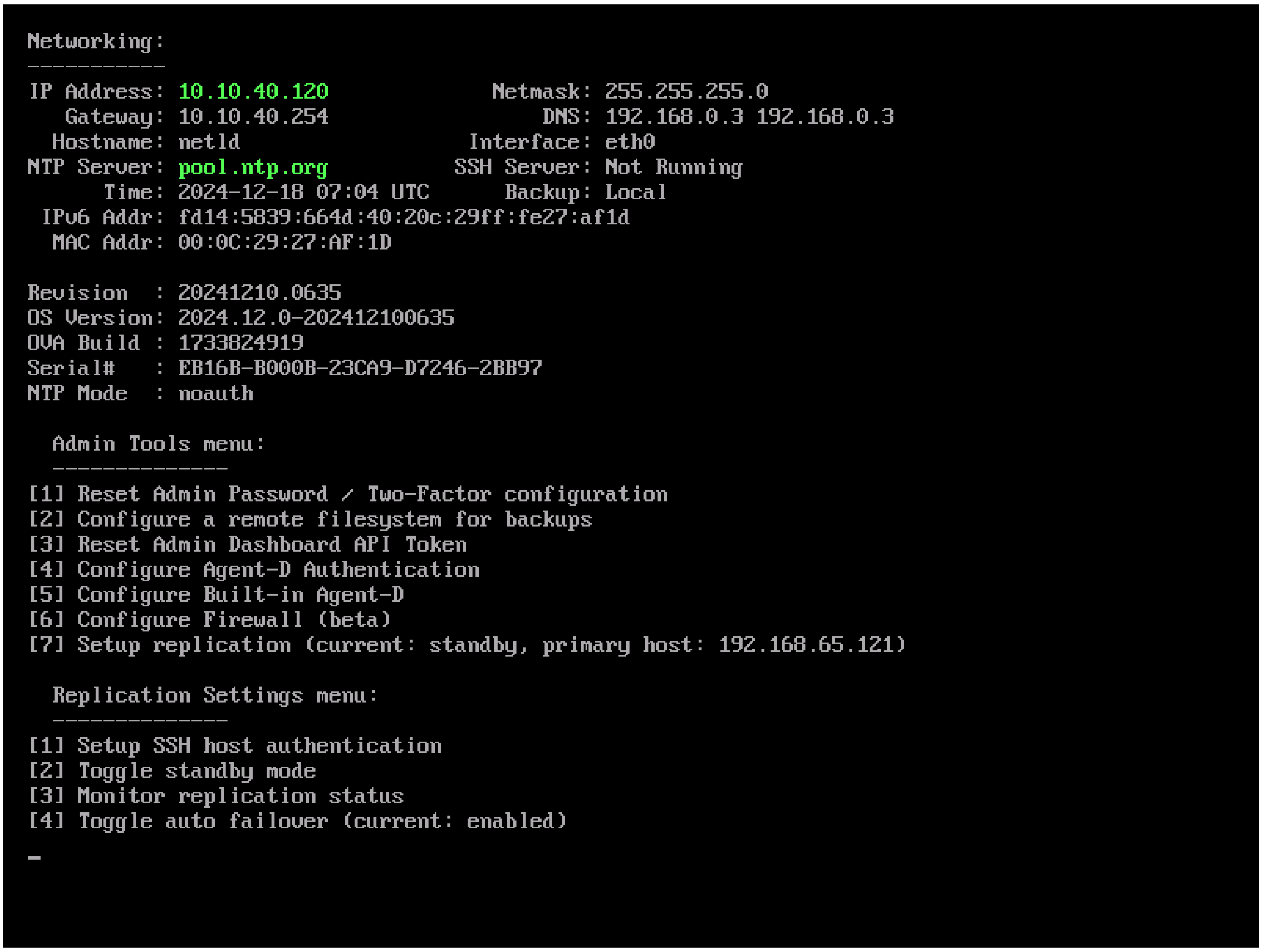
By default, auto failover is disabled. To have the standby server automatically take over monitoring if the primary server fails, follow these steps to enable auto failover.

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.



```
Networking:
-----------
IP Address: 10.10.40.120            Netmask: 255.255.255.0
   Gateway: 10.10.40.254                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                 Interface: eth0
NTP Server: pool.ntp.org         SSH Server: Not Running
      Time: 2024-12-18 07:05 UTC     Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
  MAC Addr: 00:0C:29:27:AF:1D

Revision  : 20241210.0635
OS Version: 2024.12.0-202412100635
OVA Build : 1733824919
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standby, primary host: 192.168.65.121)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
[4] Toggle auto failover (current: disabled)
```

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”.

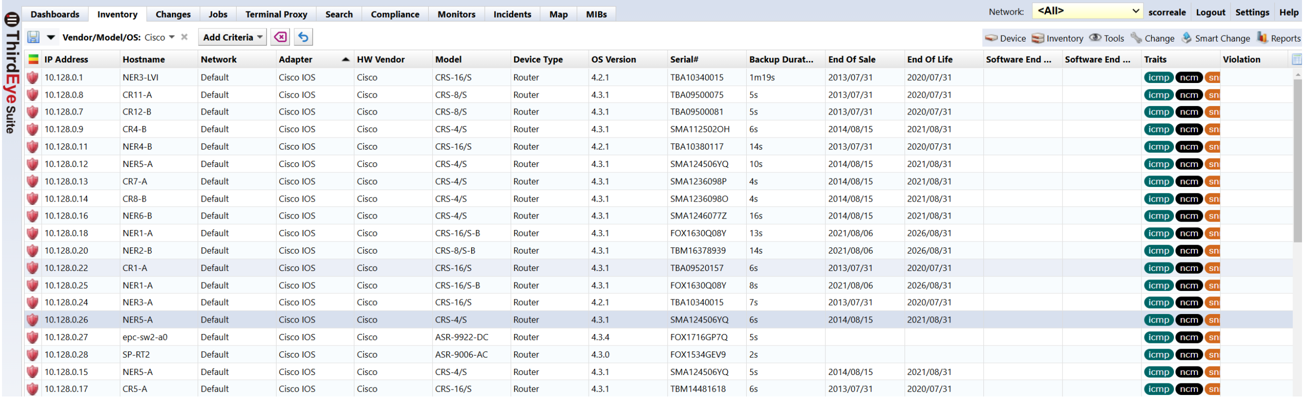


```
Networking:
-----------
IP Address: 10.10.40.120              Netmask: 255.255.255.0
   Gateway: 10.10.40.254                  DNS: 192.168.0.3 192.168.0.3
  Hostname: netld                   Interface: eth0
NTP Server: pool.ntp.org           SSH Server: Not Running
      Time: 2024-12-18 07:04 UTC       Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
  MAC Addr: 00:0C:29:27:AF:1D

Revision  : 20241210.0635
OS Version: 2024.12.0-202412100635
OVA Build : 1733824919
Serial#   : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode  : noauth

  Admin Tools menu:
  --------------
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standby, primary host: 192.168.65.121)

  Replication Settings menu:
  --------------
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
[4] Toggle auto failover (current: enabled)
_
```

SECTION 34

DEVICE EOS/EOL MANAGEMENT

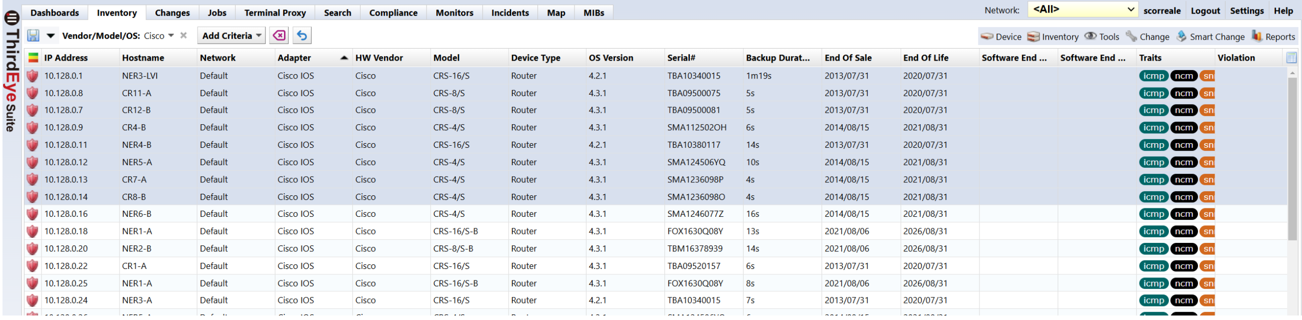
To manage EOS/EOL, “End of Sales (EOS)”/“End of Life (EOL)” columns have been added to the inventory. EOS/EOL information can be configured manually or by importing from an Excel file, or automatically configured for Cisco devices using the Cisco Support API.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.25	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	8s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.24	NER3-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	7s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.26	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	6s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.27	epc-sw2-a0	Default	Cisco IOS	Cisco	ASR-9922-DC	Router	4.3.4	FOX1716GP7Q	5s					icmp ncm sn	
10.128.0.28	SP-RT2	Default	Cisco IOS	Cisco	ASR-9006-AC	Router	4.3.0	FOX1534GEV9	2s					icmp ncm sn	
10.128.0.15	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	5s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.17	CR5-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBM14481618	6s	2013/07/31	2020/07/31			icmp ncm sn	

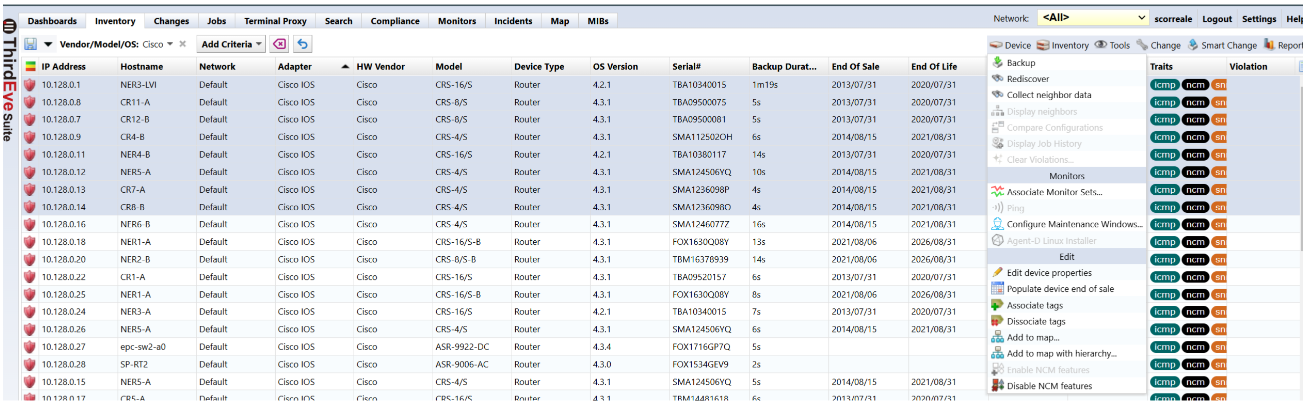
34.1 Manual Configuration

1. Click the [Inventory] tab.
2. Select the device for which to set EOS/EOL.



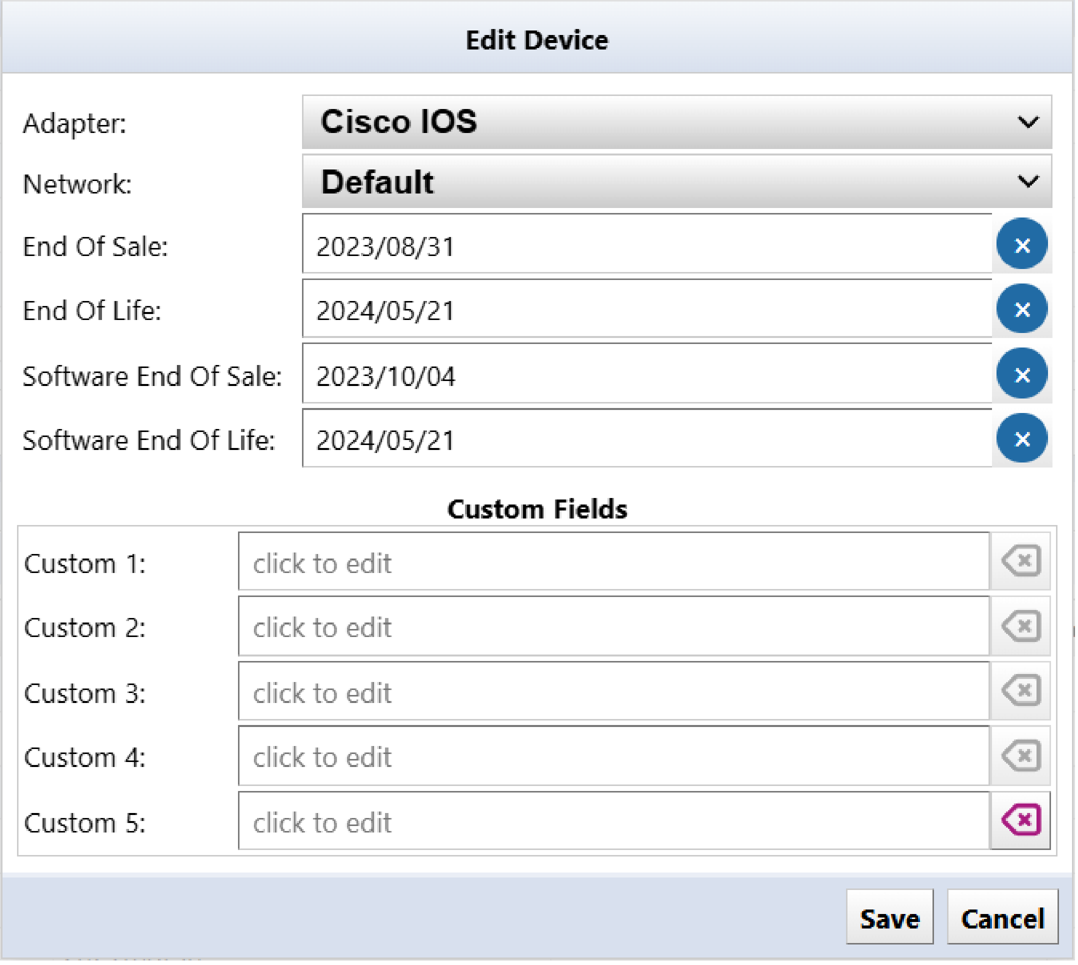
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.25	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	8s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.24	NER3-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	7s	2013/07/31	2020/07/31			icmp ncm sn	

3. Click [Device] in the [Inventory] menu bar.
4. Click [Edit device properties].



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31	icmp ncm sn	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31	icmp ncm sn	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.25	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	8s	2021/08/06	2026/08/31	icmp ncm sn	
10.128.0.24	NER3-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	7s	2013/07/31	2020/07/31	icmp ncm sn	
10.128.0.26	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	6s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.27	epc-sw2-a0	Default	Cisco IOS	Cisco	ASR-9922-DC	Router	4.3.4	FOX1716GP7Q	5s			icmp ncm sn	
10.128.0.28	SP-RT2	Default	Cisco IOS	Cisco	ASR-9006-AC	Router	4.3.0	FOX1534GEV9	2s			icmp ncm sn	
10.128.0.15	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	5s	2014/08/15	2021/08/31	icmp ncm sn	
10.128.0.17	CR5-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBM14481618	6s	2013/07/31	2020/07/31	icmp ncm sn	

3. Select the product EOS/EOL dates and click the [Save] button.



Edit Device

Adapter: Cisco IOS

Network: Default

End Of Sale: 2023/08/31

End Of Life: 2024/05/21

Software End Of Sale: 2023/10/04

Software End Of Life: 2024/05/21

Custom Fields

Custom 1: click to edit

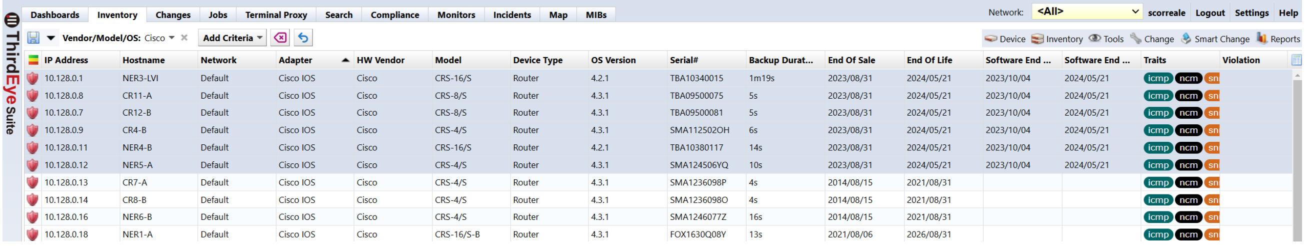
Custom 2: click to edit

Custom 3: click to edit

Custom 4: click to edit

Custom 5: click to edit

The date set in the column will be displayed.



Network: <All>

Vendor/Model/OS: Cisco

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31			icmp ncm sn	

34.2 Automatic Configuration Suite

Automatic Configuration enables the automated retrieval of critical device lifecycle information through integration with Cisco's Smart Net Total Care (SNTC) service. This feature supports both online and offline workflows. Automatic Configuration allows you to:

- Automatically populate End-of-Sale/End-of-Life (EOS/EOL) data
- Maintain updated device lifecycle records through API integration
- Handle offline scenarios with .csv-based data exchange

ThirdEye requires the following for Automatic Configuration:

- Valid Cisco Smart Net Total Care (SNTC) is required.
- You must log in with your Cisco account and obtain an API key and secret code before accessing Cisco Smart Net Total Care.

For information on obtaining API, visit https://developer.cisco.com/docs/support-apis/#!user-onboarding-process.

> Note
>
> ThirdEye must be able to connect to the Internet to retrieve the End-of-Sale (EOS) date from the Cisco server.

34.2.1 Offline Environment

If ThirdEye cannot connect to the Internet, it will not be able to retrieve the EOS 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 also export a .csv file from your Cisco service, and import it into ThirdEye to update the EOS date.

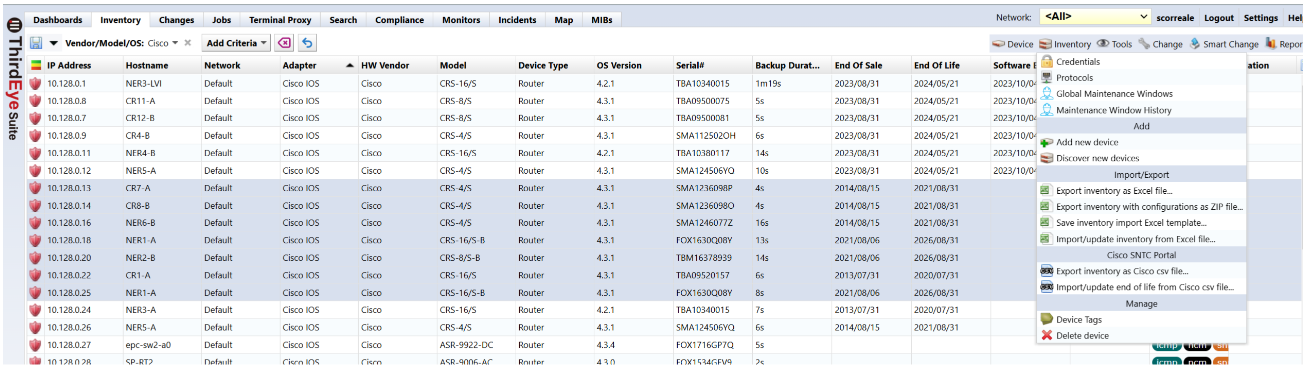
> Note
>
> Cisco services do not include the end-of-sale date in the export file.

34.2.2 Export Device Inventory

To export a .csv file that can be used for import into Cisco services:

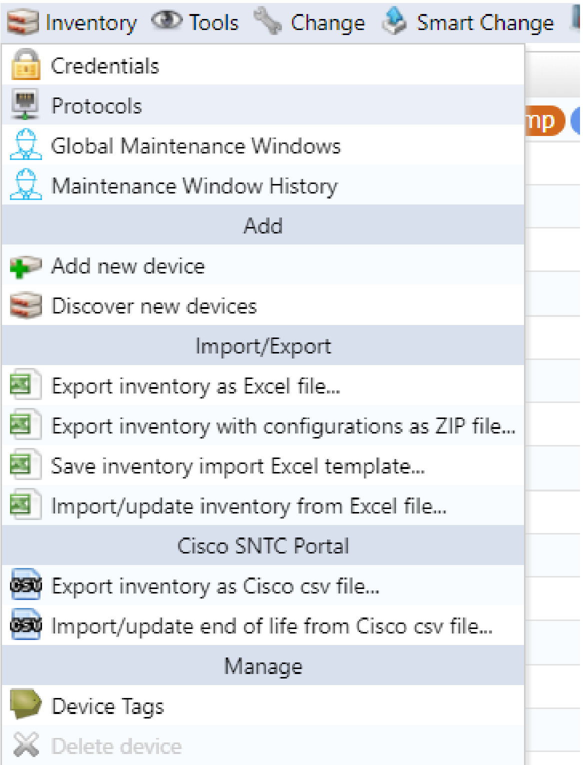
1. Click the [Inventory] main tab.

2. Click [Inventory] in the menu bar.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software E
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2023/08/31	2024/05/21	2023/10/04
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2023/08/31	2024/05/21	2023/10/04
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2023/08/31	2024/05/21	2023/10/04
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2023/08/31	2024/05/21	2023/10/04
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2023/08/31	2024/05/21	2023/10/04
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2023/08/31	2024/05/21	2023/10/04
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31	
10.128.0.25	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	8s	2021/08/06	2026/08/31	
10.128.0.24	NER3-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	7s	2013/07/31	2020/07/31	
10.128.0.26	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	6s	2014/08/15	2021/08/31	
10.128.0.27	epc-sw2-a0	Default	Cisco IOS	Cisco	ASR-9922-DC	Router	4.3.4	FOX1716GP7Q	5s			
10.128.0.28	SP-RT2	Default	Cisco IOS	Cisco	ASR-9006-AC	Router	4.3.0	FOX1534GEV9	2s			

3. Click [Export Inventory as Cisco .csv file..].


Inventory
Tools
Change
Smart Change
Credentials
Protocols
Global Maintenance Windows
Maintenance Window History
Add
Add new device
Discover new devices
Import/Export
Export inventory as Excel file...
Export inventory with configurations as ZIP file...
Save inventory import Excel template...
Import/update inventory from Excel file...
Cisco SNTC Portal
Export inventory as Cisco csv file...
Import/update end of life from Cisco csv file...
Manage
Device Tags
Delete device
mp

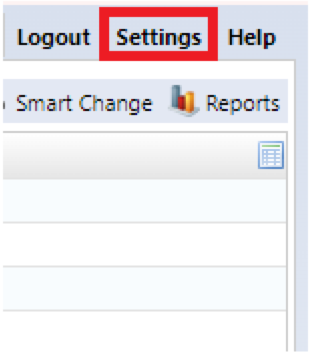
34.2.3 Import Cisco CSV File

1. Repeat steps 1 and 2 above.

2. Click [Import/update end of life from Cisco csv file…].

34.2.4 Obtain Device EOS/EOL

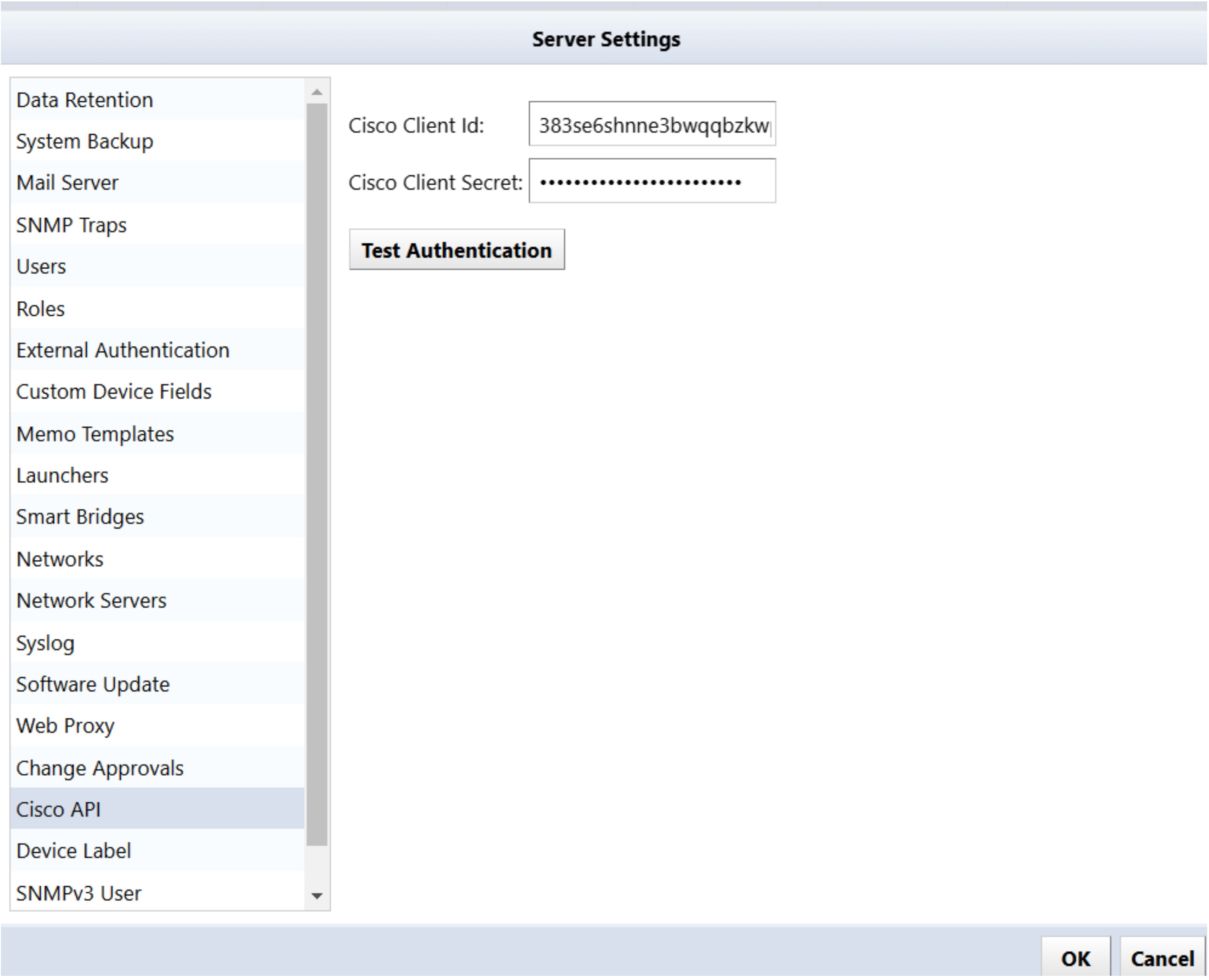
1. Click [Settings] in the Global Menu.



2. Click [Cisco API] in the left sidebar.

3. Enter your API key and secret code and click [OK].

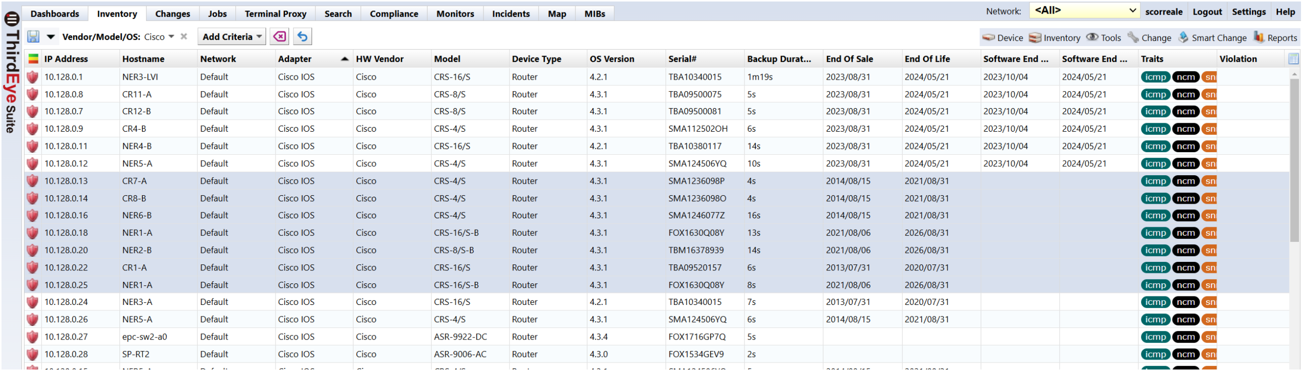
(Clicking [Test Authentication] checks the validity of the ID and Secret code.)



Cisco Client Id: 383se6shnne3bwqqbzkw

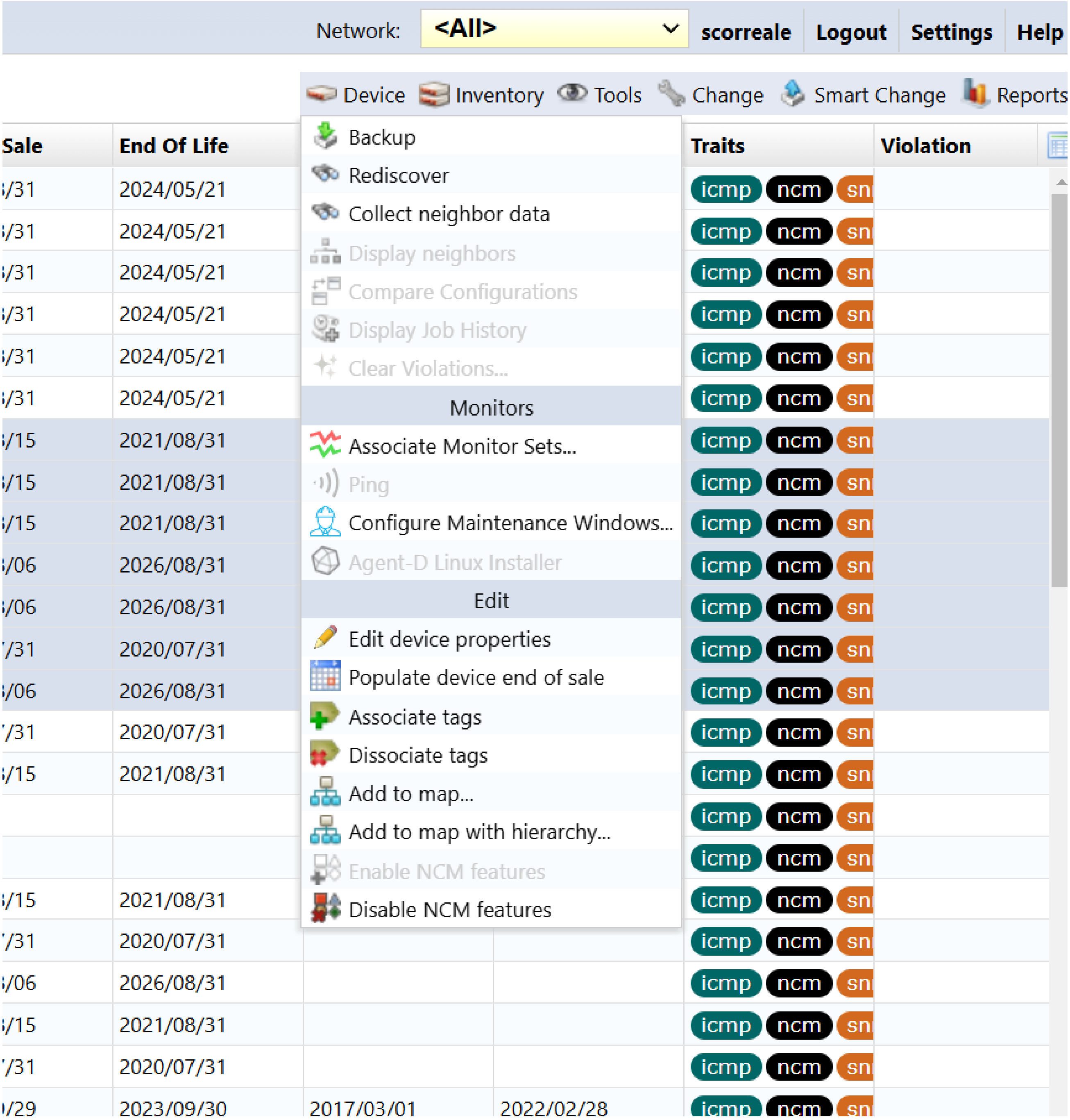
Cisco Client Secret: ••••••••••••••••••••••••

4. Select the device to obtain EOS/EOL.



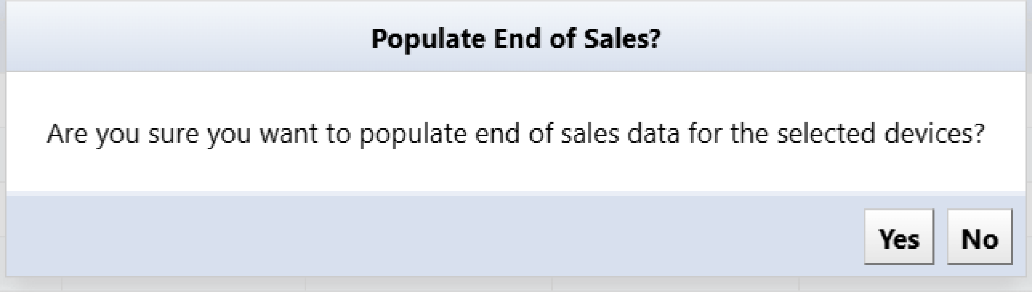
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.25	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	8s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.24	NER3-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	7s	2013/07/31	2020/07/31			icmp ncm sn	
10.128.0.26	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	6s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.27	epc-sw2-a0	Default	Cisco IOS	Cisco	ASR-9922-DC	Router	4.3.4	FOX1716GP7Q	5s					icmp ncm sn	
10.128.0.28	SP-RT2	Default	Cisco IOS	Cisco	ASR-9006-AC	Router	4.3.0	FOX1534GEV9	2s					icmp ncm sn	

5. Click [Populate device end of sale] in the [Device] submenu.



Sale	End Of Life			Traits	Violation
/31	2024/05/21			icmp ncm sn	
/31	2024/05/21			icmp ncm sn	
/31	2024/05/21			icmp ncm sn	
/31	2024/05/21			icmp ncm sn	
/31	2024/05/21			icmp ncm sn	
/31	2024/05/21			icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
/06	2026/08/31			icmp ncm sn	
/06	2026/08/31			icmp ncm sn	
/31	2020/07/31			icmp ncm sn	
/06	2026/08/31			icmp ncm sn	
/31	2020/07/31			icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
				icmp ncm sn	
				icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
/31	2020/07/31			icmp ncm sn	
/06	2026/08/31			icmp ncm sn	
/15	2021/08/31			icmp ncm sn	
/31	2020/07/31			icmp ncm sn	
/29	2023/09/30	2017/03/01	2022/02/28	icmp ncm sn	

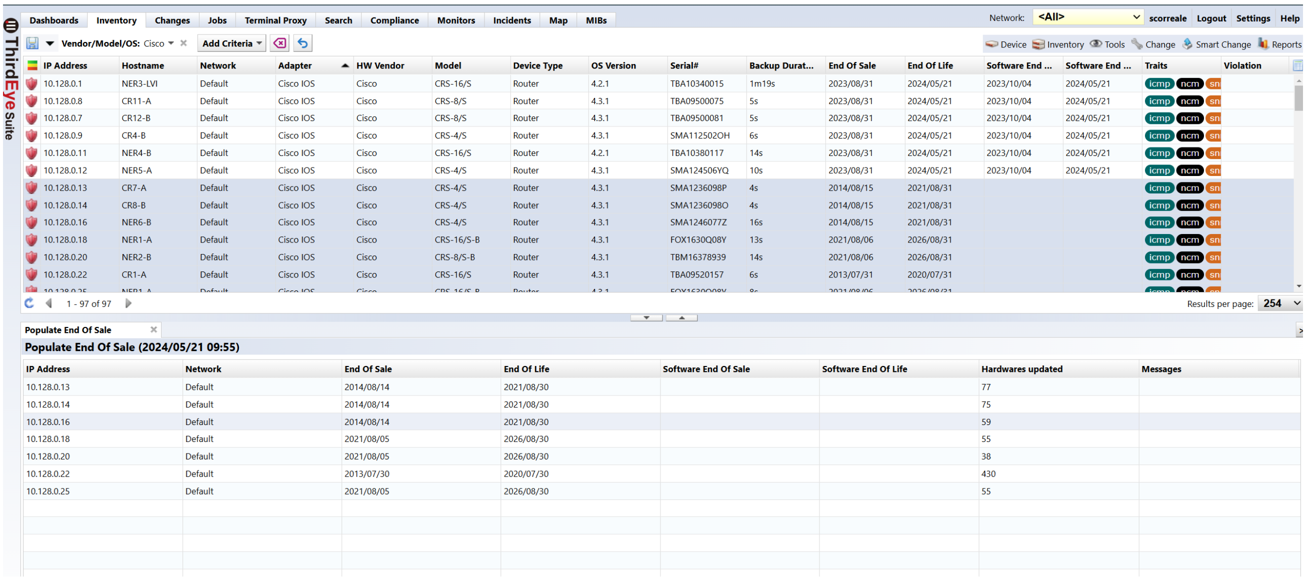
6. On the “Populate End of Sales” screen, click [Yes].



Populate End of Sales?

Are you sure you want to populate end of sales data for the selected devices?

EOS/EOL information will be automatically acquired and registered in the column.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.128.0.1	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	1m19s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.8	CR11-A	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500075	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.7	CR12-B	Default	Cisco IOS	Cisco	CRS-8/S	Router	4.3.1	TBA09500081	5s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.9	CR4-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OH	6s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.11	NER4-B	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10380117	14s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.12	NER5-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA124506YQ	10s	2023/08/31	2024/05/21	2023/10/04	2024/05/21	icmp ncm sn	
10.128.0.13	CR7-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098P	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.14	CR8-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1236098O	4s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.16	NER6-B	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA1246077Z	16s	2014/08/15	2021/08/31			icmp ncm sn	
10.128.0.18	NER1-A	Default	Cisco IOS	Cisco	CRS-16/S-B	Router	4.3.1	FOX1630Q08Y	13s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.20	NER2-B	Default	Cisco IOS	Cisco	CRS-8/S-B	Router	4.3.1	TBM16378939	14s	2021/08/06	2026/08/31			icmp ncm sn	
10.128.0.22	CR1-A	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.3.1	TBA09520157	6s	2013/07/31	2020/07/31			icmp ncm sn	

1 - 97 of 97

Results per page: 254

Populate End Of Sale

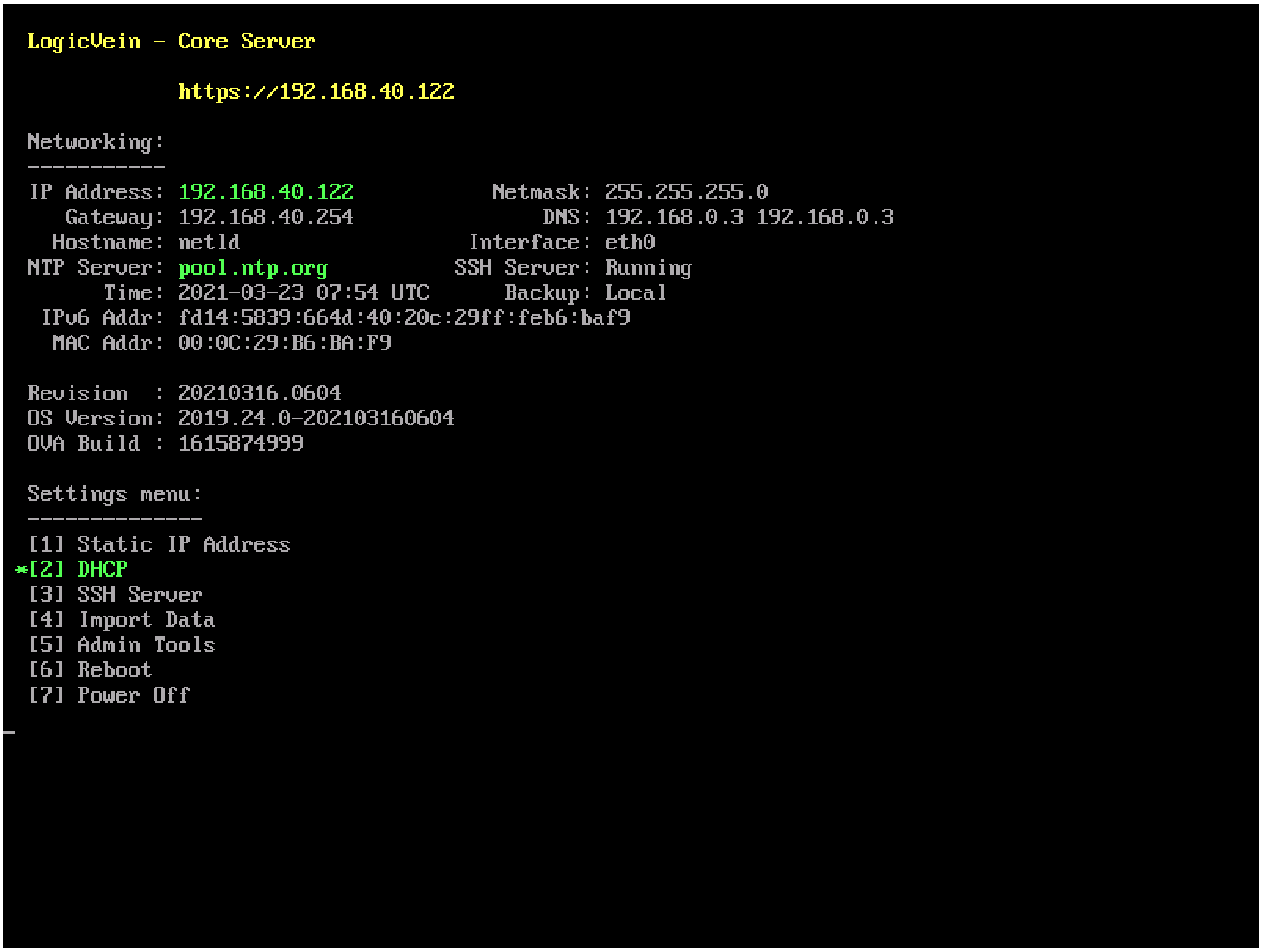
Populate End Of Sale (2024/05/21 09:55)

IP Address	Network	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life	Hardwares updated	Messages
10.128.0.13	Default	2014/08/14	2021/08/30			77	
10.128.0.14	Default	2014/08/14	2021/08/30			75	
10.128.0.16	Default	2014/08/14	2021/08/30			59	
10.128.0.18	Default	2021/08/05	2026/08/30			55	
10.128.0.20	Default	2021/08/05	2026/08/30			38	
10.128.0.22	Default	2013/07/30	2020/07/30			430	
10.128.0.25	Default	2021/08/05	2026/08/30			55	

SECTION 35

REBOOT/SHUTDOWN

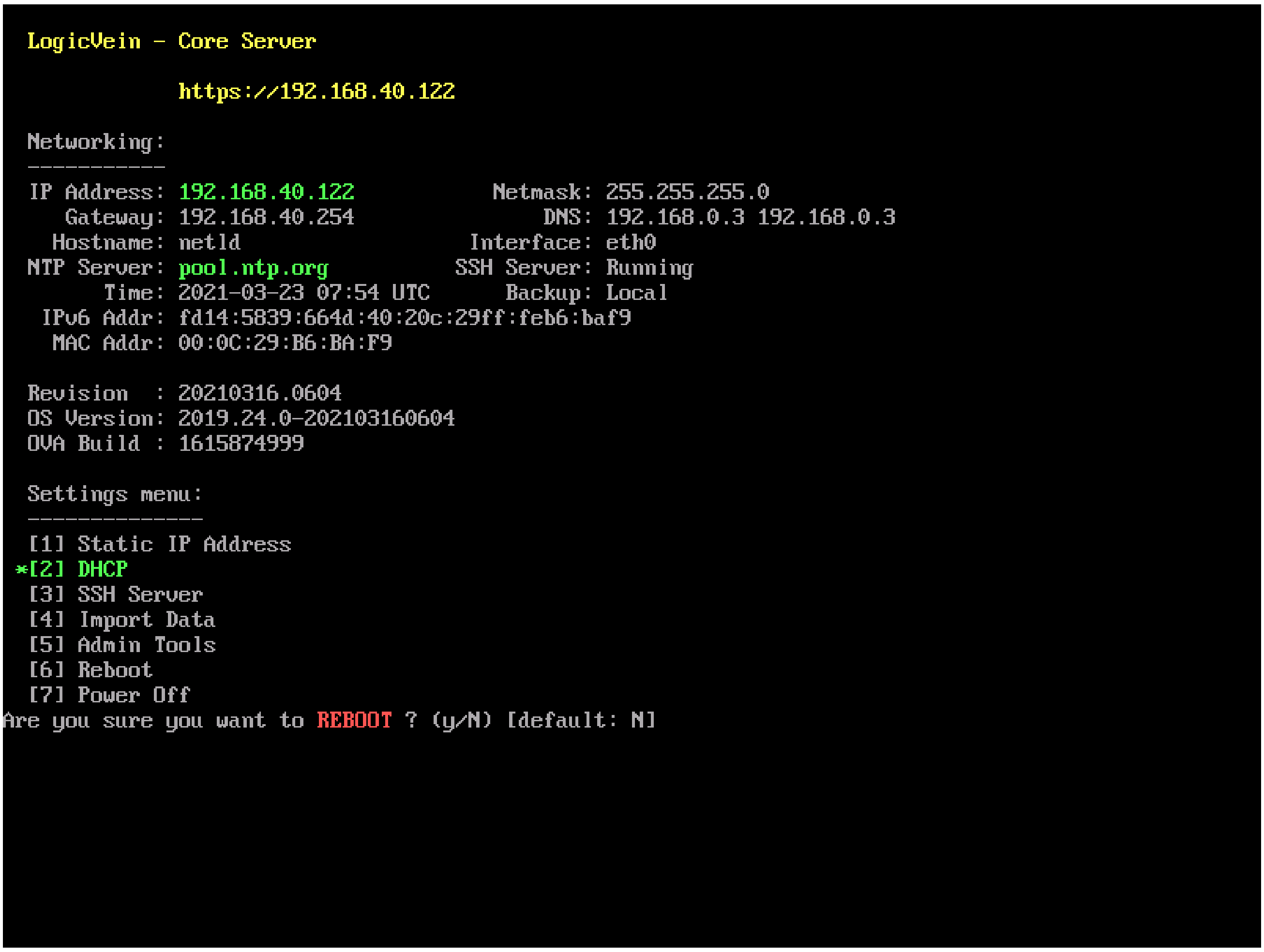
Reboot and shutdown operations are performed using the keyboard on the virtual machine console.



```
 LogicVein - Core Server

             https://192.168.40.122

 Networking:
 -----------
 IP Address: 192.168.40.122          Netmask: 255.255.255.0
    Gateway: 192.168.40.254              DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                 Interface: eth0
 NTP Server: pool.ntp.org         SSH Server: Running
       Time: 2021-03-23 07:54 UTC     Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

 Settings menu:
 --------------
 [1] Static IP Address
*[2] DHCP
 [3] SSH Server
 [4] Import Data
 [5] Admin Tools
 [6] Reboot
 [7] Power Off
_
```

35.1 Restart Procedure:

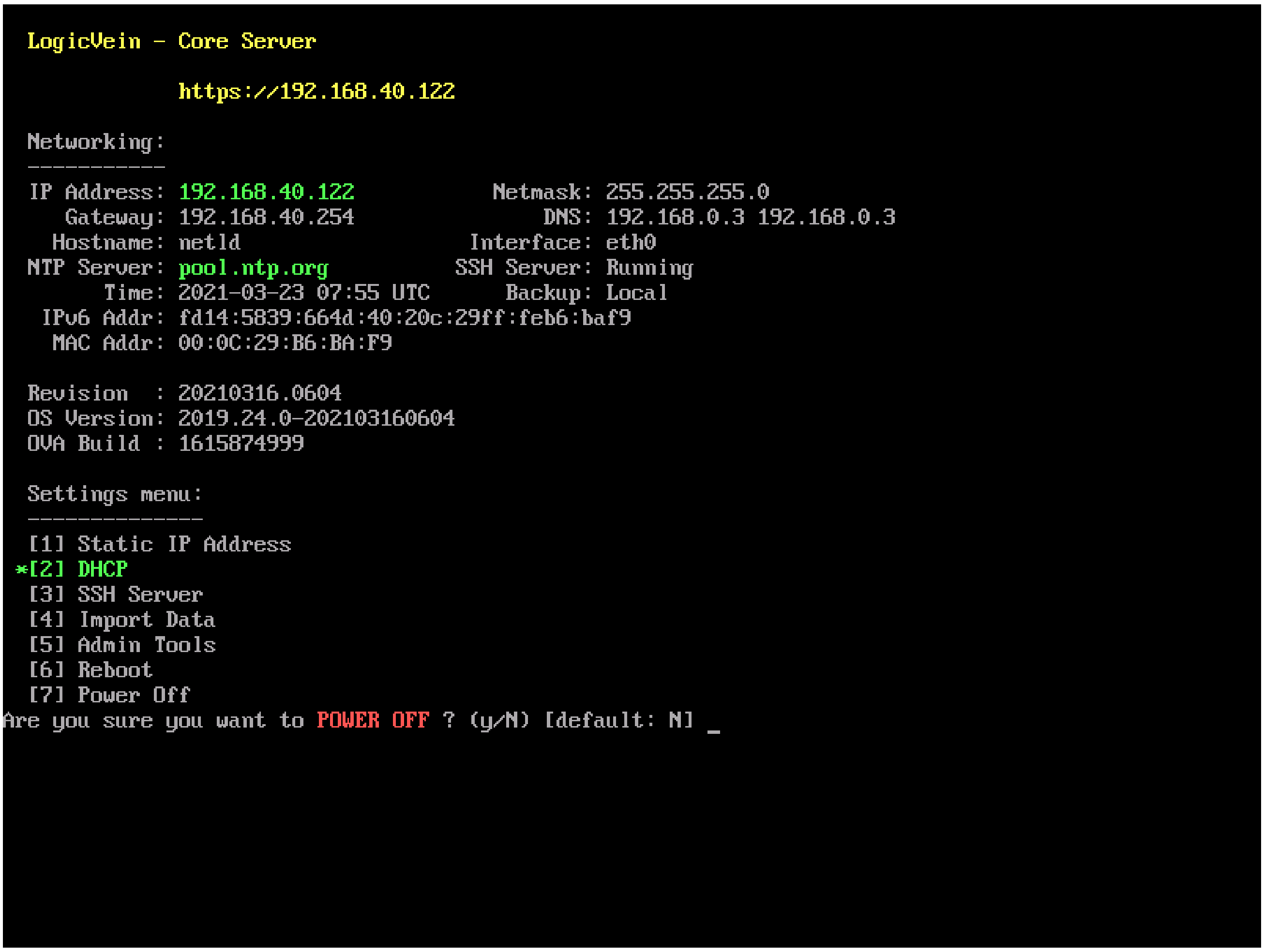
1. Click the [6] key on your keyboard.
2. Choose [Reboot].
3. Press the [Y] key on your keyboard to execute.



```
 LogicVein - Core Server

             https://192.168.40.122

 Networking:
 -----------
 IP Address: 192.168.40.122           Netmask: 255.255.255.0
    Gateway: 192.168.40.254               DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                  Interface: eth0
 NTP Server: pool.ntp.org          SSH Server: Running
       Time: 2021-03-23 07:54 UTC      Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

 Settings menu:
 --------------
 [1] Static IP Address
*[2] DHCP
 [3] SSH Server
 [4] Import Data
 [5] Admin Tools
 [6] Reboot
 [7] Power Off
Are you sure you want to REBOOT ? (y/N) [default: N]
```

35.2 Shutdown Procedure:

1. Click the [7] key on your keyboard.
2. Choose [Power Off].
3. Press the [Y] key on your keyboard to execute.



```
 LogicVein - Core Server

             https://192.168.40.122

 Networking:
 -----------
 IP Address: 192.168.40.122           Netmask: 255.255.255.0
    Gateway: 192.168.40.254               DNS: 192.168.0.3 192.168.0.3
   Hostname: netld                  Interface: eth0
 NTP Server: pool.ntp.org          SSH Server: Running
       Time: 2021-03-23 07:55 UTC      Backup: Local
  IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
   MAC Addr: 00:0C:29:B6:BA:F9

 Revision  : 20210316.0604
 OS Version: 2019.24.0-202103160604
 OVA Build : 1615874999

 Settings menu:
 --------------
 [1] Static IP Address
*[2] DHCP
 [3] SSH Server
 [4] Import Data
 [5] Admin Tools
 [6] Reboot
 [7] Power Off
Are you sure you want to POWER OFF ? (y/N) [default: N] _
```

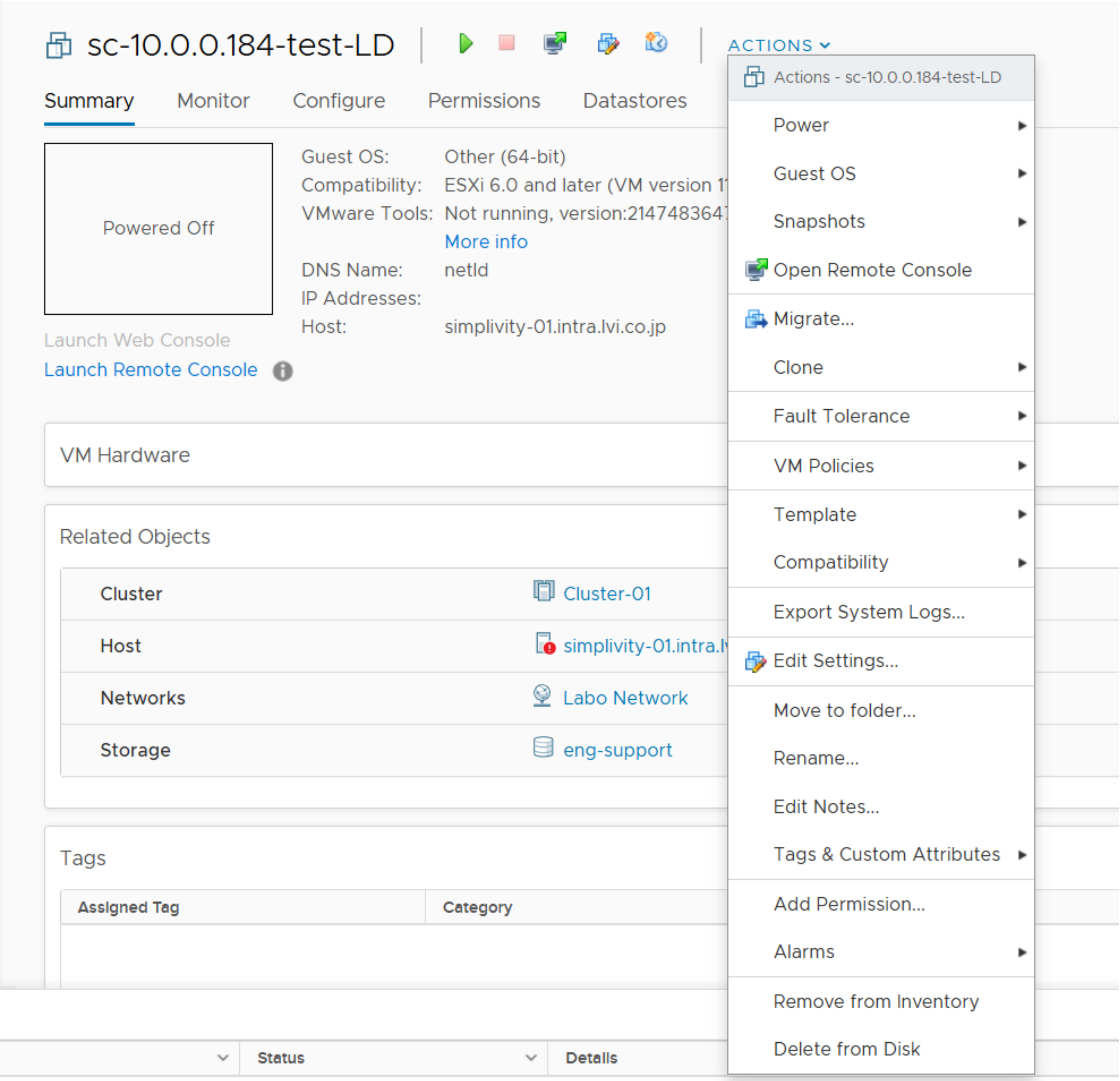
SECTION 36

UNINSTALL

36.1 Uninstall

1. Shut down ThirdEye.
2. After the shutdown is complete, delete the ThirdEye virtual machine from the virtual host OS.

Example of deletion screen in VMware ESXi:



Guest OS: Other (64-bit)

Compatibility: ESXi 6.0 and later (VM version 1

VMware Tools: Not running, version:214748364

More info

DNS Name: netld

IP Addresses:

Host: simplivity-01.intra.lvi.co.jp

VM Hardware

Related Objects

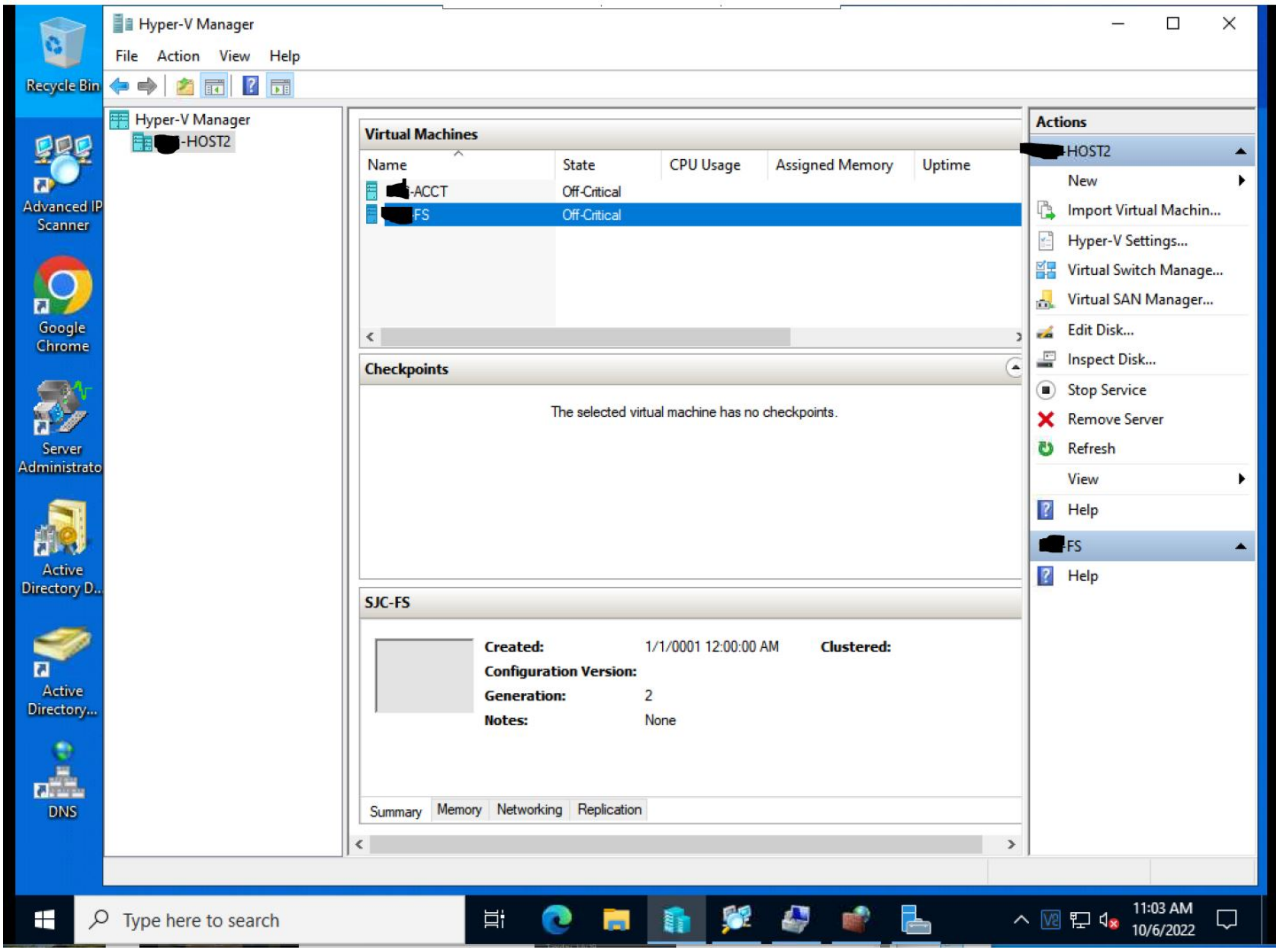
Cluster	Cluster-01
Host	simplivity-01.intra.l
Networks	Labo Network
Storage	eng-support

Tags

Assigned Tag	Category

	Status	Details

Example of deletion screen in Windows Hyper-V:



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
[redacted]-ACCT	Off-Critical			
[redacted]FS	Off-Critical			

Checkpoints

The selected virtual machine has no checkpoints.

SJC-FS

Created: 1/1/0001 12:00:00 AM **Clustered:**

Configuration Version:

Generation: 2

Notes: None

This completes the uninstallation of ThirdEye.

SECTION 37

INQUIRIES

If you have any problems or questions while using ThirdEye, 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 (ThirdEye license information)
4. Specific issue(s) and questions.
5. A screenshot of the issue (if possible).