LogicVein

ThirdEye

User’s Manual

Contents

Contents

Contents

Revision History

Revision	Issued date	Contents
Rev.1	2/3/2019	First edition issued
Rev.2	8/4/2019	Revised explanations and images as functions were added
Rev.3	10/9/2019	Revised explanations and images as functions were added
Rev.4	3/9/2020	Chapter1 Add Configuration backup and generation management
Rev.5	02/2022	Updated documentation to include remediation and end of life
Rev .6	09/2022	Updated to modify end of sale/end of life

1. Introduction

This manual is for the network fault monitoring software "ThirdEye", which sets out to explain how to set up and operate ThirdEye.

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

- Monitoring Polling (ICMP Ping, SNMP Polling)
- Monitoring SNMP trap
- Monitoring Time Window
- Management incidents (Severity, Status, Priority, People, Event aggregation)
- Management dashboard (Display statistics graph, Customize widget)
- Management Inventory (Customize display, Sort, Search)
- Management Map (Setting the hierarchy, Map tree view, Incident notification)
- Set monitoring item /Set template
- Excel export of statistical information
- Set Maintenance Window
- Trail management by Terminal Proxy
- Email notification when incidents are updated
- Compiling the private MIB
- Configuration backup and generation management

1.1 Operating Environment

ThirdEye is provided as a virtual appliance (VA). To use ThirdEye, the following environment is required.

Item	Requirements
Virtualization Platform	VMWare ESXi 5.5 or higher Hyper-V (Windows Server 2012 R2 or later)
CPU	8 cores or more
Memory	8 GB or more
Hard Disk	HDD 1: 8 GB (system area) HDD 2: 50 GB or more (data area)
Supported Browsers (We recommend that you use the latest version of a compatible browser)	Google Chrome Mozilla Firefox Microsoft Edge

2. Installation

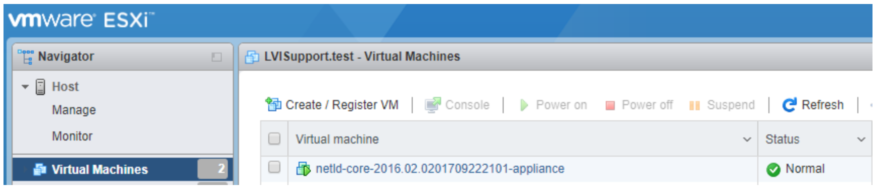
The installation process for ThirdEye is as follows.

2.1 Installation

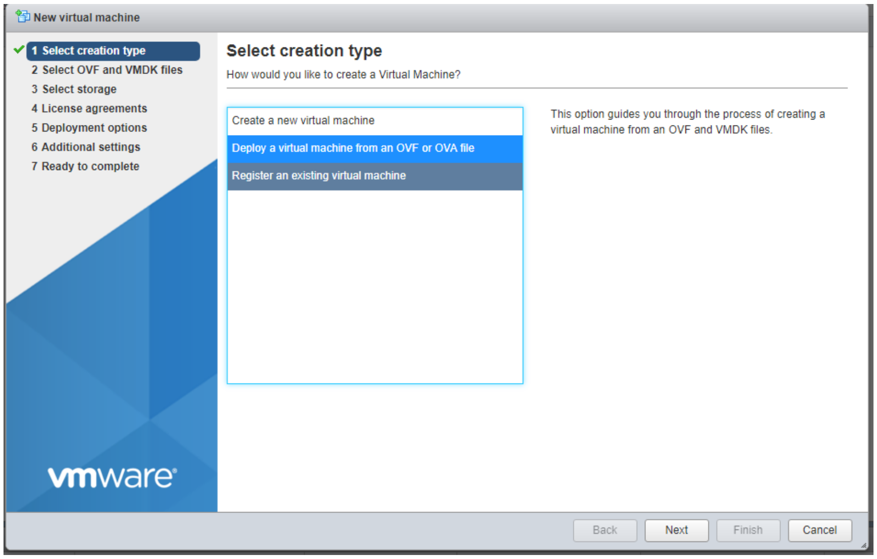
2.1.1 Deployment to VMware ESXi

This is the deployment procedure for VMWare ESXi. The following example is for ESXi 6.5.

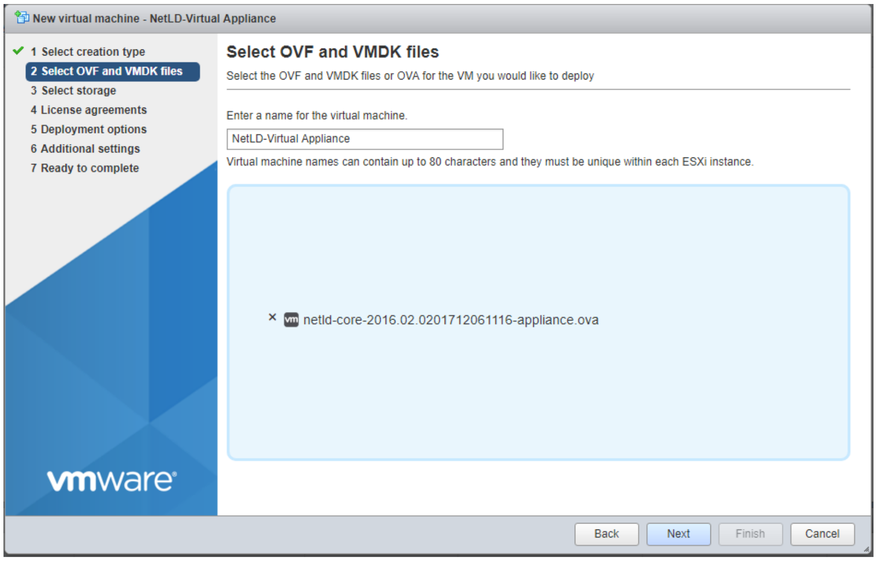
1. Login to Web UI, then click [Create/Register VM] from [Virtual Machines].



2. Select [Deploy a virtual machine from an OVF or OVA file], then 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.
vmware
Back
Next
Finish
Cancel

3. After entering the virtual machine’s name, drag and drop the LogicVein VA .ova file, then click [Next].



Select OVF and VMDK files

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

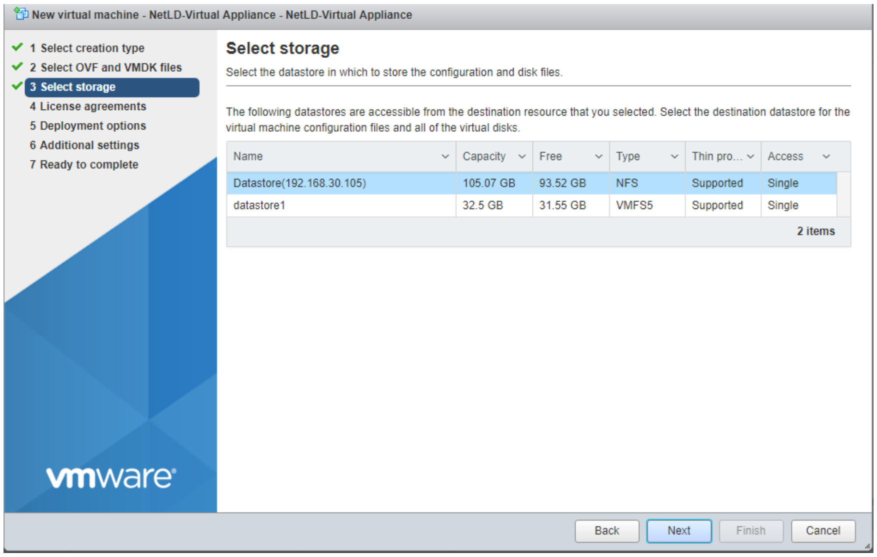
Enter a name for the virtual machine.

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

4. Select storage, then click [Next].



Select storage

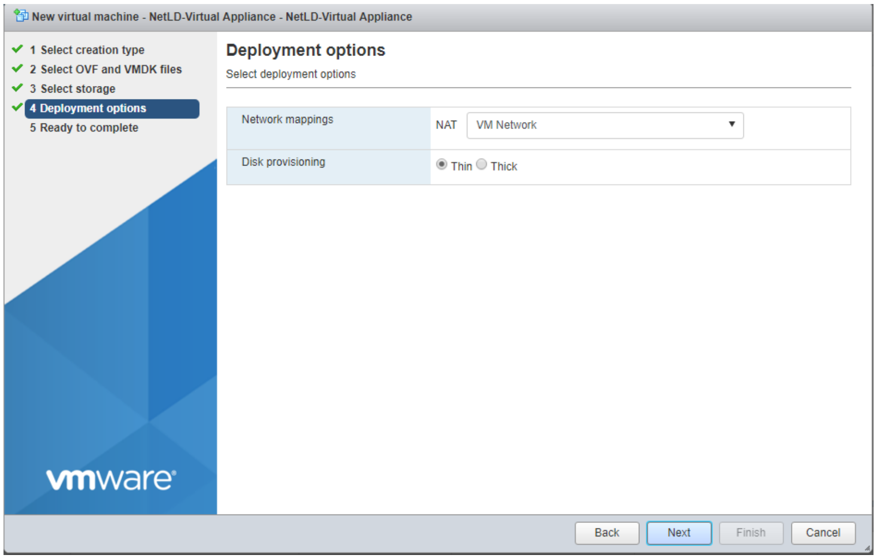
Select the datastore in which to store the configuration and disk files.

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

5. Select Network and Disk Provisioning, then click [Next]. *For [Disk Provisioning], [Thin] is recommended.



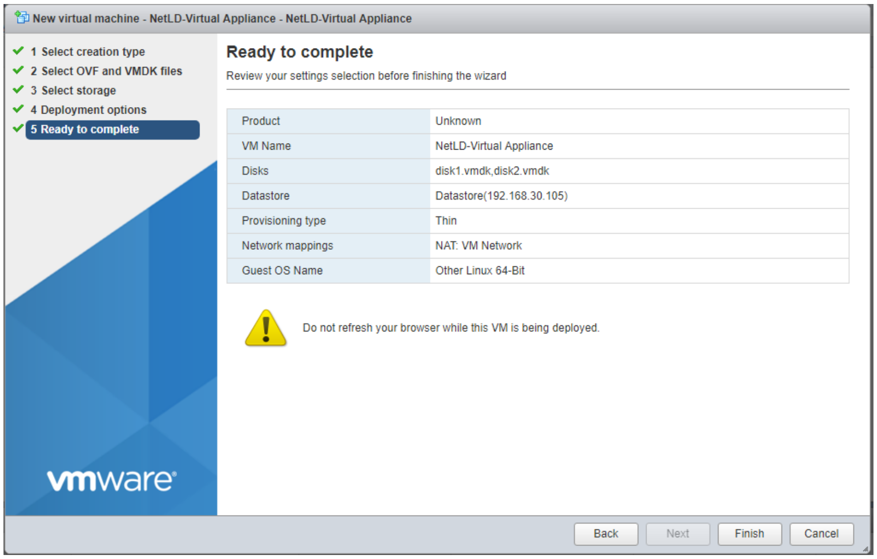
New virtual machine - NetLD-Virtual Appliance - NetLD-Virtual Appliance

Deployment options

Select deployment options

Network mappings	NAT VM Network
Disk provisioning	● Thin ○ Thick

6. Click [Finish].



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

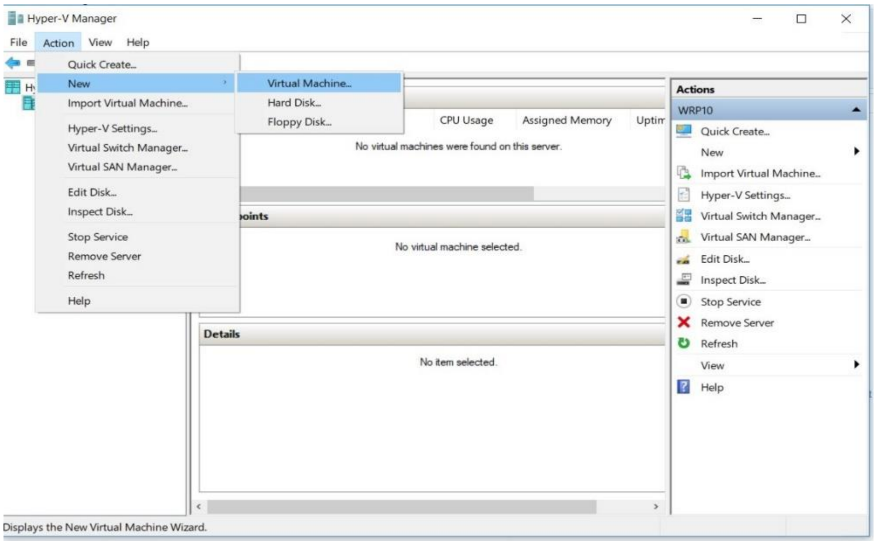
Do not refresh your browser while this VM is being deployed.

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

2.1.2 Windows Hyper-V Deployment

As an example, we will use Windows Server 2016, but you can use Windows 10 Pro also. Please change according to your environment.

1. Start Hyper-V Manager and click [Action] → [New] → [Virtual Machine] to display the New Virtual Machine Wizard.



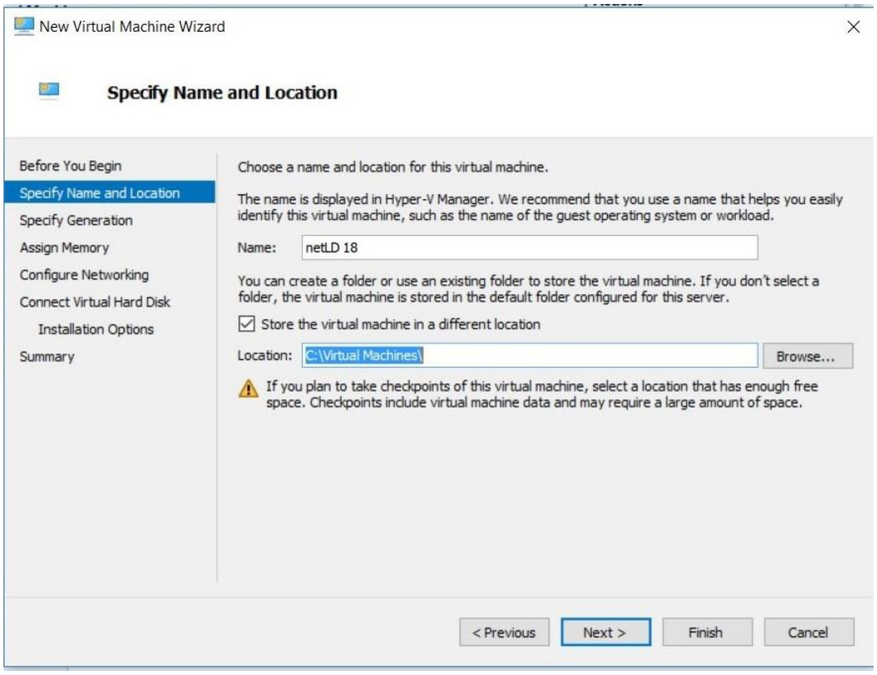
No virtual machines were found on this server.

No virtual machine selected.

No item selected.

Displays the New Virtual Machine Wizard.

2. Enter a name for the virtual machine. If desired, change the storage location. 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

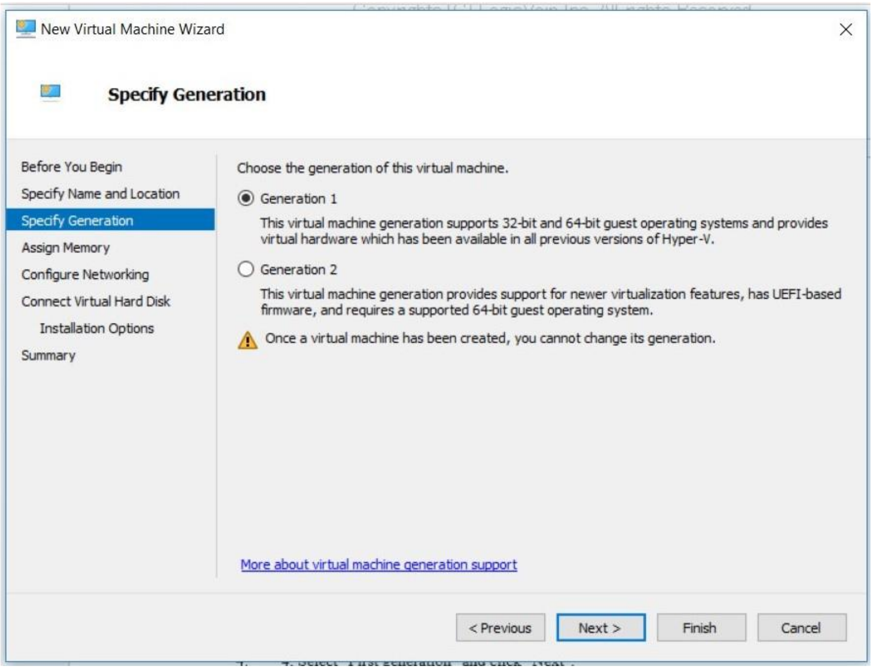
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ 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].



New Virtual Machine Wizard

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.

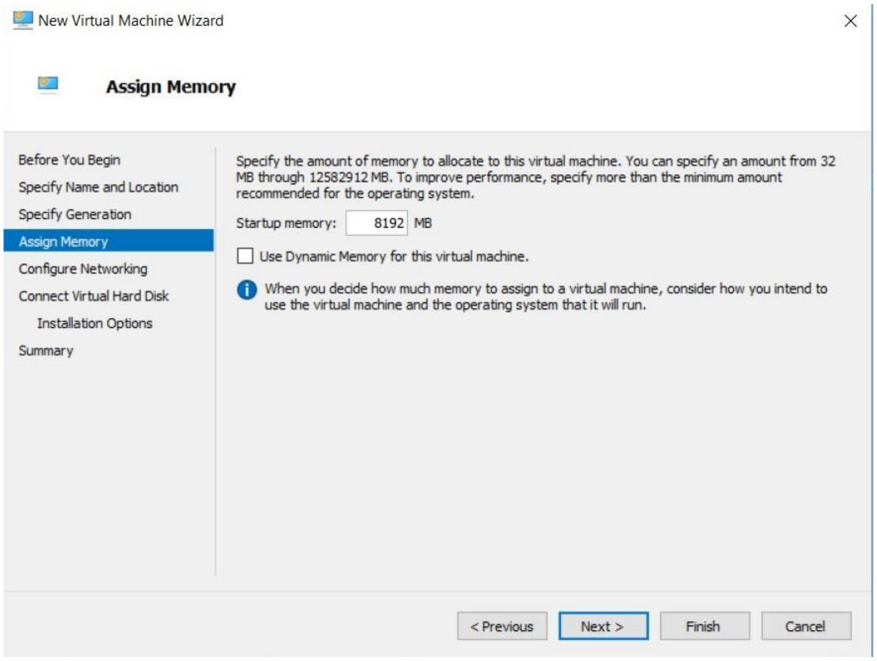
○ Generation 2

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].



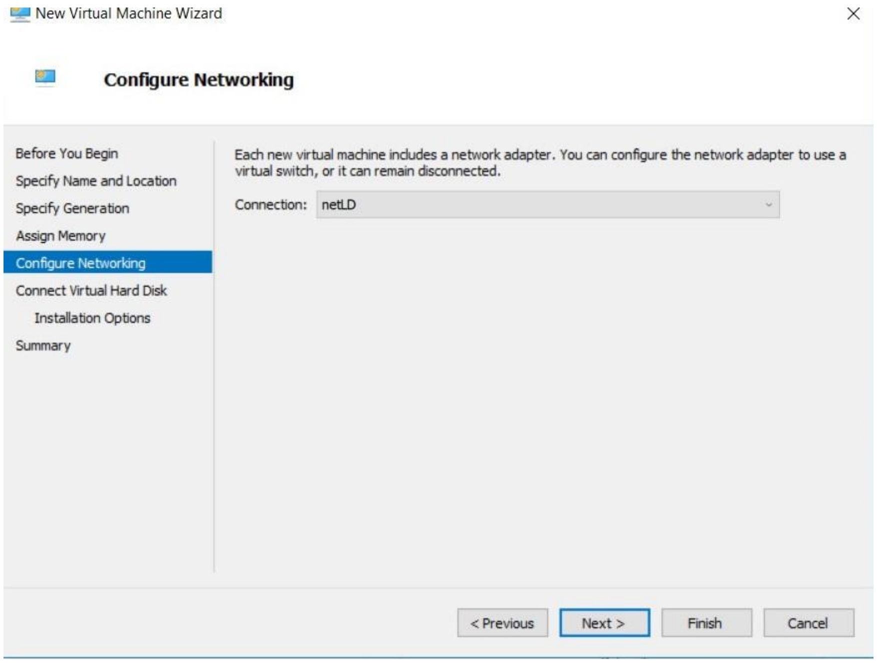
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

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.

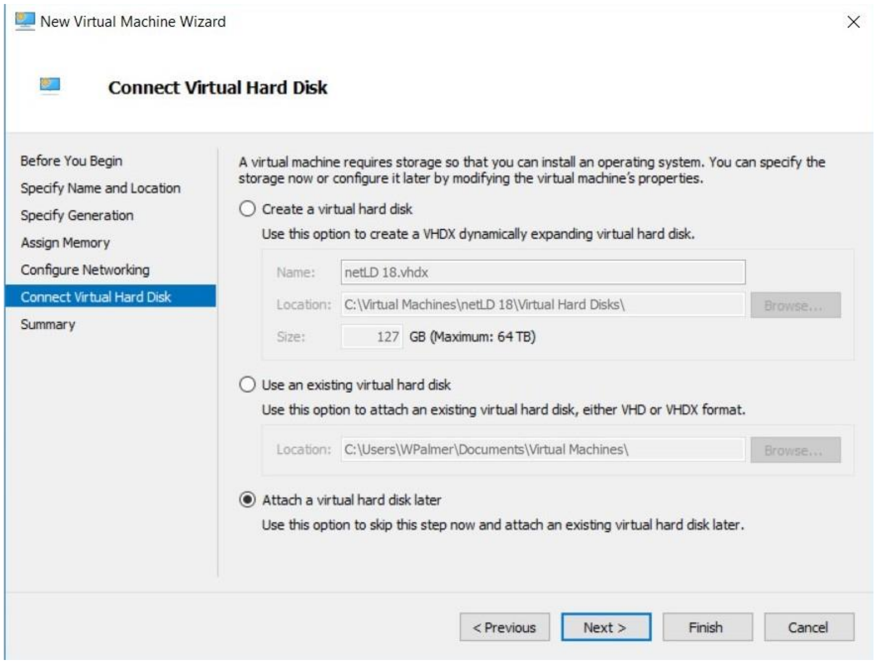
5. Next to [Connection:] select a virtual switch for the network connection and click [Next].



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 [Connect virtual hard disk later] and click [Next].


New Virtual Machine Wizard
Connect Virtual Hard Disk
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

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\

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

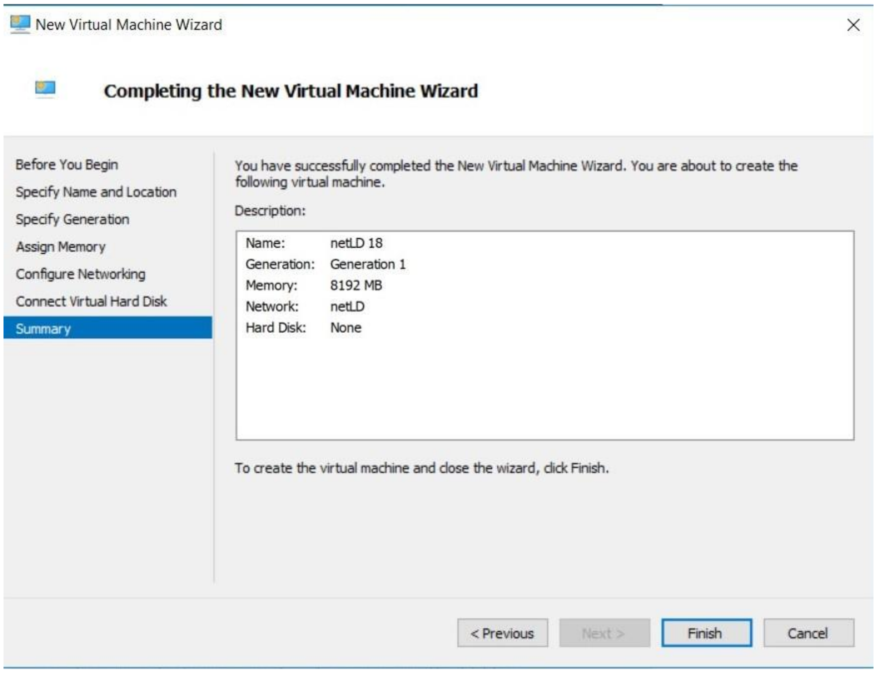
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

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

● 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].


New Virtual Machine Wizard
Completing the New Virtual Machine Wizard
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

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

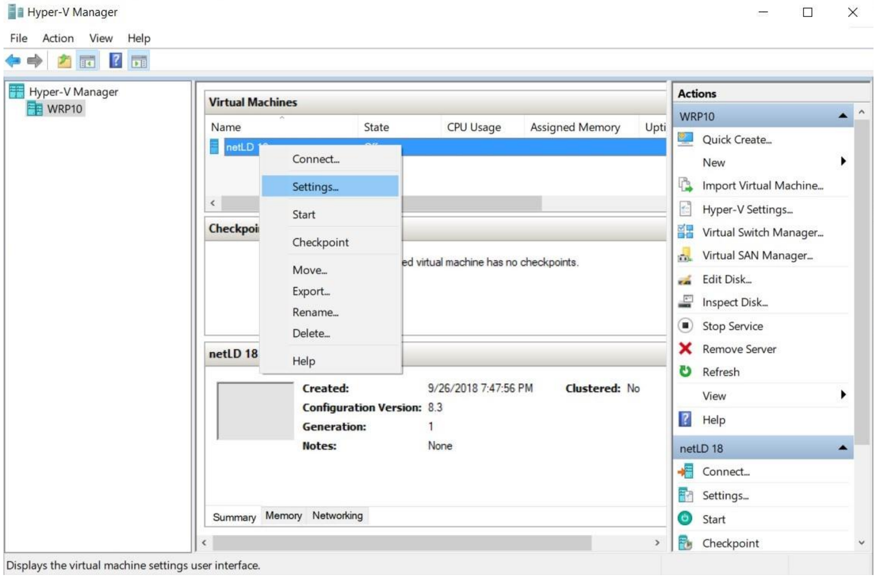
Description:

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.

< Previous
Next >
Finish
Cancel

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

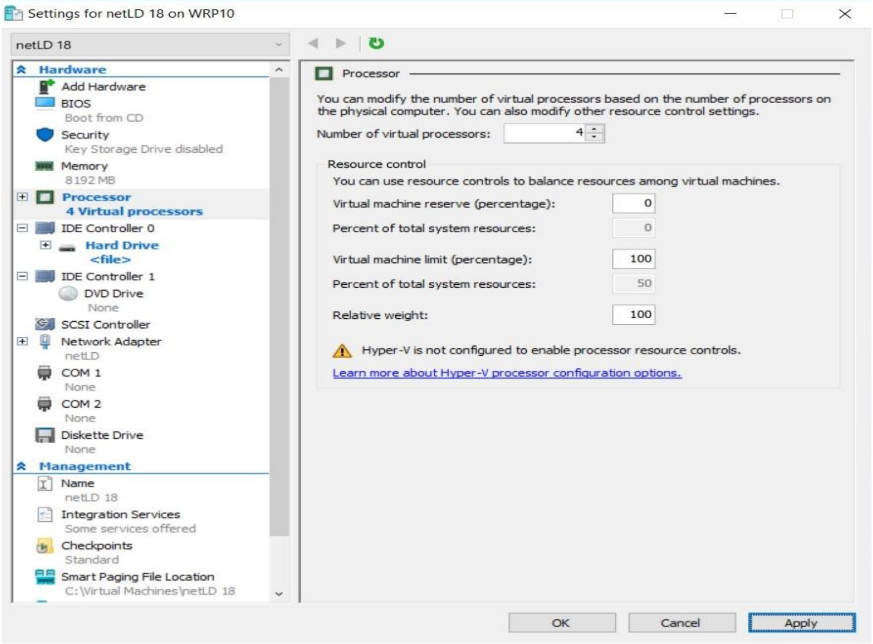


...ed virtual machine has no checkpoints.

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. Click [Processor] and change [Number of virtual processors].



BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
8192 MB
Processor
4 Virtual processors
IDE Controller 0
Hard Drive
<file>
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
netLD
COM 1
None
COM 2
None
Diskette Drive
None
Name
netLD 18
Integration Services
Some services offered
Checkpoints
Standard
Smart Paging File Location
C:\Virtual Machines\netLD 18

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

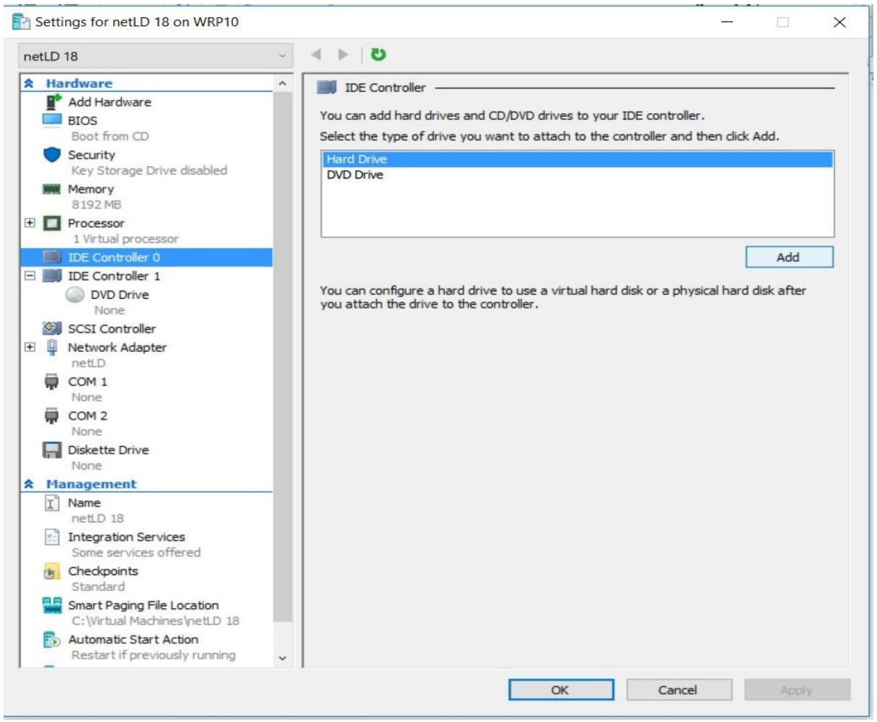
You can use resource controls to balance resources among virtual machines.

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. Click [IDE Controller 0], select [Hard Drive], and click [Add].



IDE Controller

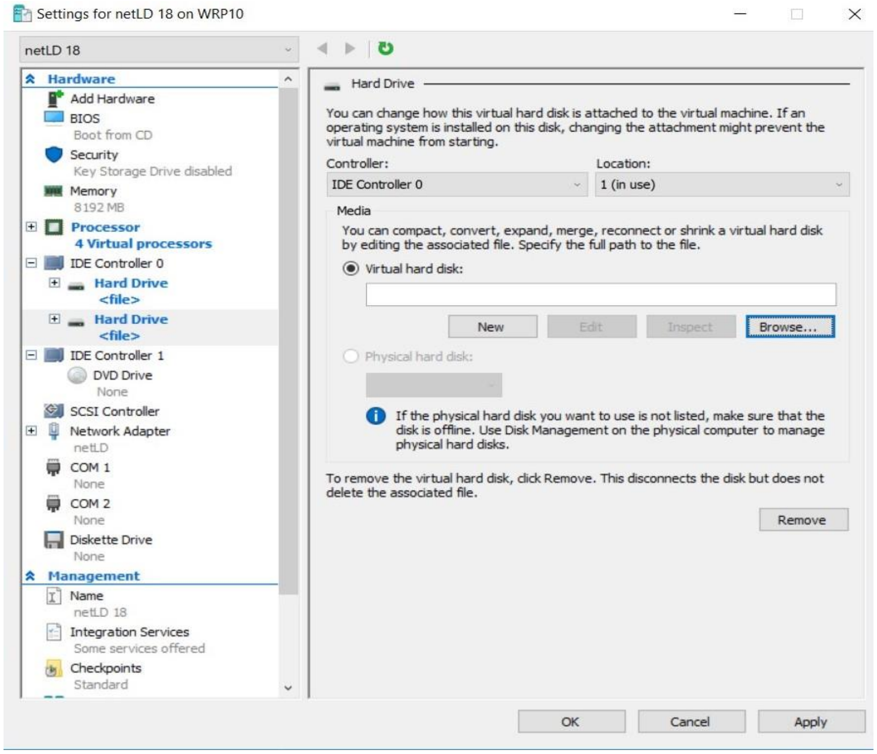
You can add hard drives and CD/DVD drives to your IDE controller.

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

Hard Drive
DVD Drive

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.

11. Click [Browse].



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.

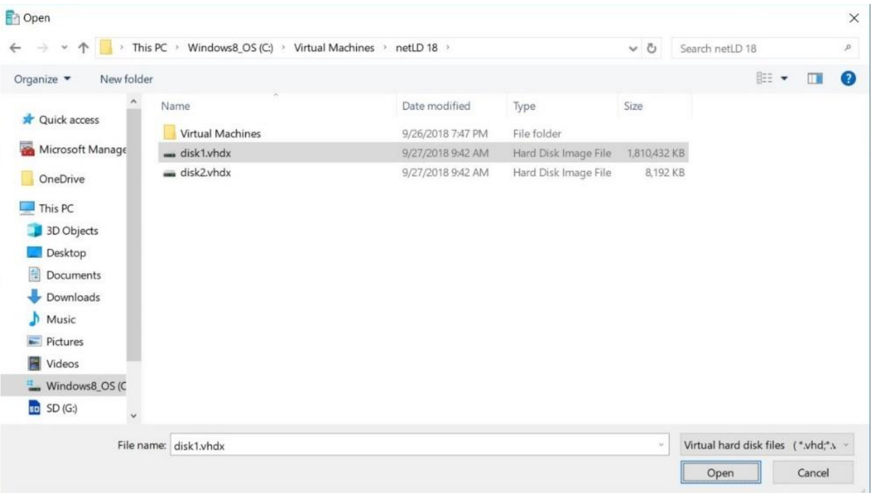
● Virtual hard disk:

○ 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. Browse to where you saved the downloaded .vhdx files, select disk1.vhdx, and click [Open].



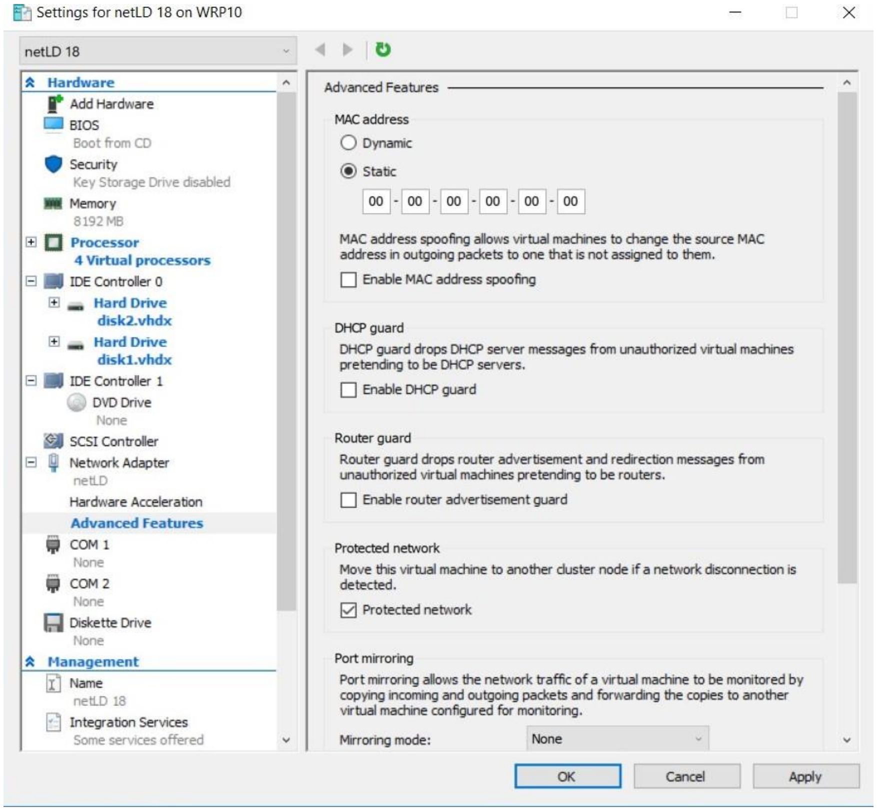
Name	Date modified	Type	Size
Virtual Machines	9/26/2018 7:47 PM	File folder	
disk1.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	1,810,432 KB
disk2.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	8,192 KB

File name: disk1.vhdx

Virtual hard disk files (*.vhd;*.v

13. Repeat steps 10 to 12 to add disk2.vhdx.

14. Click the [➕] next to [Network Adapter] and select [Advanced Features]. Add a static MAC address and 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

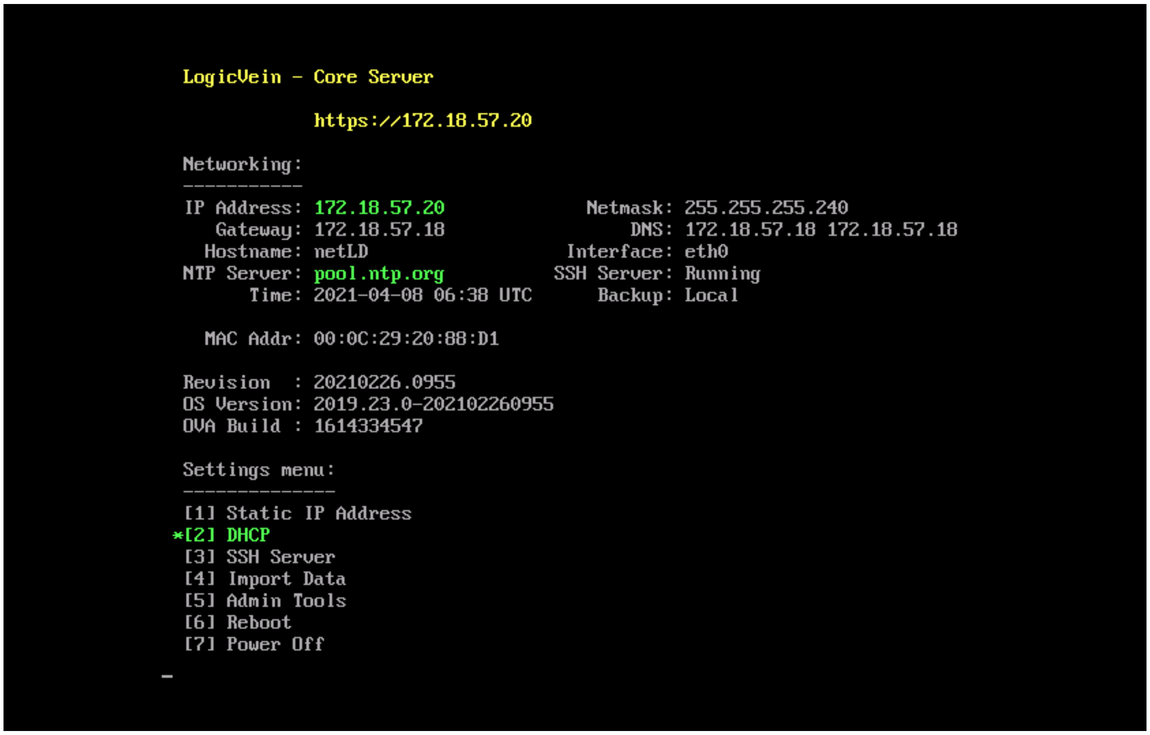
15. After the deployment is completed, please [Start] and [Connect] to the virtual machine.

2.2 Configuring network settings

After starting the VMware or Hyper-V virtual machine, some network settings are needed. By default ThirdEye receives its IP address and configuration from DHCP. Because DHCP only gives temporary IP addresses, or in an environment without a DHCP server, add a static IP address and configuration.

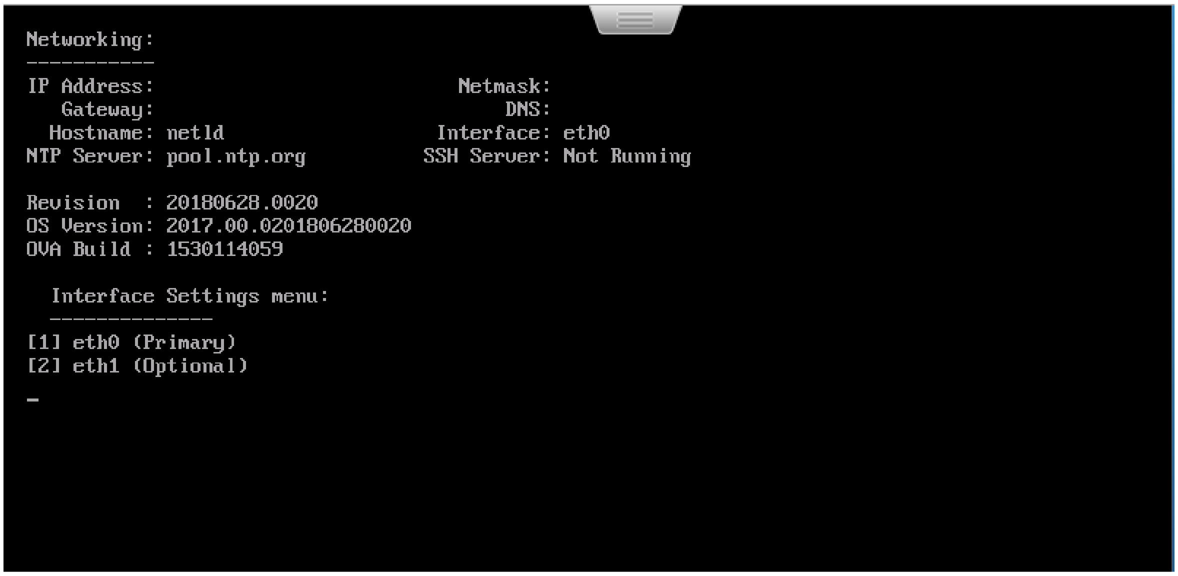
* All network settings are keyboard operations.

1. Type [1] to add a [Static IP Address].



```
 LogicVein - Core Server

             https://172.18.57.20

 Networking:
 -----------
 IP Address: 172.18.57.20           Netmask: 255.255.255.240
    Gateway: 172.18.57.18               DNS: 172.18.57.18 172.18.57.18
   Hostname: netLD                Interface: eth0
 NTP Server: pool.ntp.org        SSH Server: Running
       Time: 2021-04-08 06:38 UTC    Backup: Local

   MAC Addr: 00:0C:29:20:88:D1

 Revision  : 20210226.0955
 OS Version: 2019.23.0-202102260955
 OVA Build : 1614334547

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

_
```

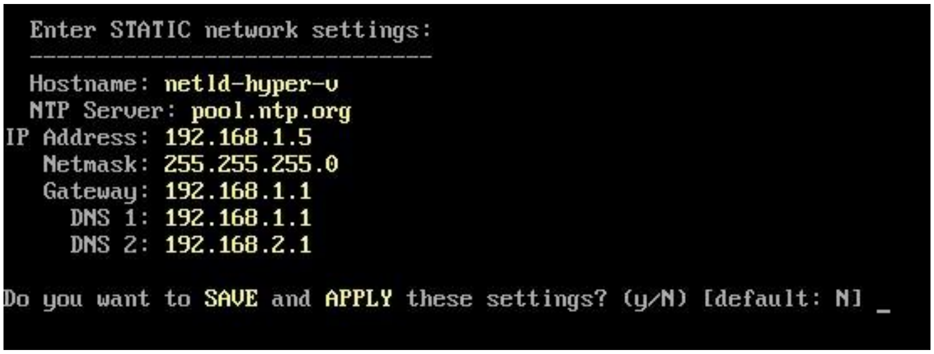
2. Type [1] to select [eth0 (Primary)].



```
Networking:
-----------
IP Address:                          Netmask:
   Gateway:                              DNS:
  Hostname: netld                  Interface: eth0
NTP Server: pool.ntp.org          SSH Server: Not Running

Revision  : 20180628.0020
OS Version: 2017.00.0201806280020
OVA Build : 1530114059

  Interface Settings menu:
  -------------
[1] eth0 (Primary)
[2] eth1 (Optional)
_
```

3. Enter the following items to match your network environment, and type [y] to save the setting.

Item	Description	Required
Hostname	Enter the desired hostname	✓
NTP Server	Enter DNS name or IP address of the NTP server	✓
IP Address	Enter the desired IP address	✓
Netmask	Enter your subnet mask	✓
Gateway	Enter the default gateway IP address	✓
DNS 1	Enter the IP address of your primary DNS server	✓
DNS 2 (Optional)	Enter the IP address of your secondary DNS server	×



```
  Enter STATIC network settings:
  ------------------------------
  Hostname: netld-hyper-v
  NTP Server: pool.ntp.org
IP Address: 192.168.1.5
   Netmask: 255.255.255.0
   Gateway: 192.168.1.1
     DNS 1: 192.168.1.1
     DNS 2: 192.168.2.1

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

After saving the setting, the service is automatically restarted.

2.3 Applying a license

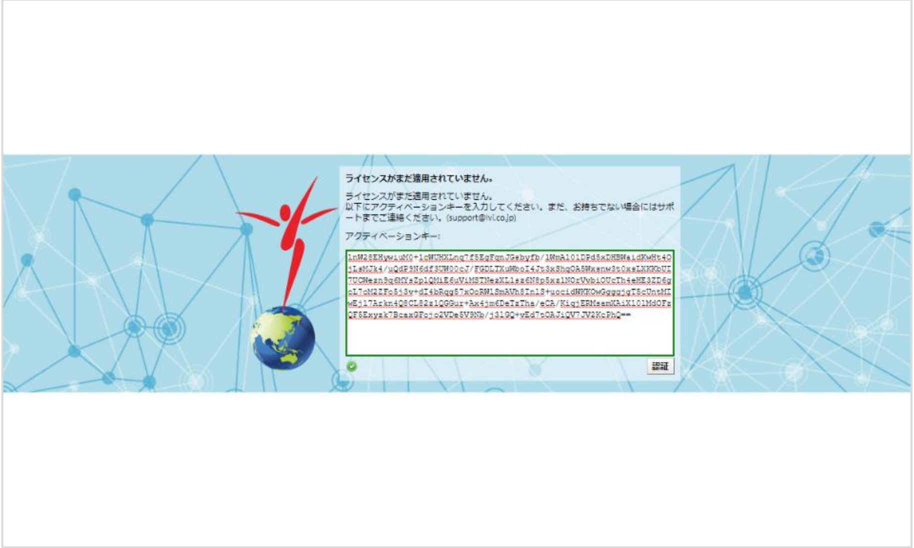
Apply the license and activate the product

1. Use a web browser to enter the ThirdEye address for access.

```
https://<IP_address>/
```

* Specify an IP address or FQDN (Fully Qualified Domain Name) for <IP_address>.

2. The license authentication screen is displayed. Copy and paste the activation key, enter it, and click [Authentication].



ライセンスがまだ適用されていません。

ライセンスがまだ適用されていません。
以下にアクティベーションキーを入力してください。また、お持ちでない場合にはサポートまでご連絡ください。(support@lvi.co.jp)

アクティベーションキー:

```
1nW28EHywiuM0+1cWUHXLnq7f5EgFqnJGebyfb/1WmA101DPd5xDHBWaidKwHt4O
jLeMJk4/uQdP9N6df3UW00cJ/FGDLTXuWboI4Jt3xShgOA5Wxenw3t0xeLXKKbUI
7UCNezn9q6MYeZplQMiE6uViMSTNezXL1ez6N8p5xz1NOrVvbiOUcTh4eHE3ZD6g
oL7cM2ZFo5j3v+dI4bRqg57xOcRW1SmAVh8In1S+uocidWKKOwGgggjgT5cUntMI
wEj17Arkn4Q8CL82z1QGGur+Ax4jm6DeTzThe/eCA/KiqjERMeemXAiX101MdOFz
QF5Exyzk7BcaxGFojo2VDe5V9Nb/j31GQ+vEd7tOAJiQV7JV2KcPhQ==
```

The service is automatically restarted, and licensing is complete.

3. Login / Logout

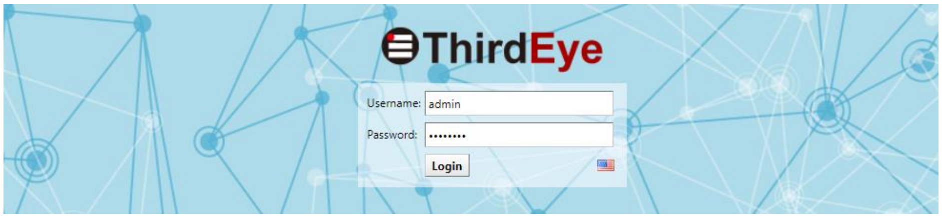
To log in / out, follow the steps below

3.1 Logging in

1. Open a web browser and enter the address of ThirdEye and access it.

   https://<IP_address> / or https://< Fully Qualified Domain Name>

2. On the login screen, enter the [Username] and [Password] and click [Login].



ThirdEye

Username: admin

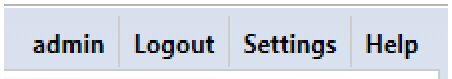
Password: ••••••••

* The default username is “admin” (Do not enter quotation marks.) and the password is “password”

When logging in, the top screen of ThirdEye is displayed.

3.2 Log out

1. Click [Logout] on the upper right of the screen.

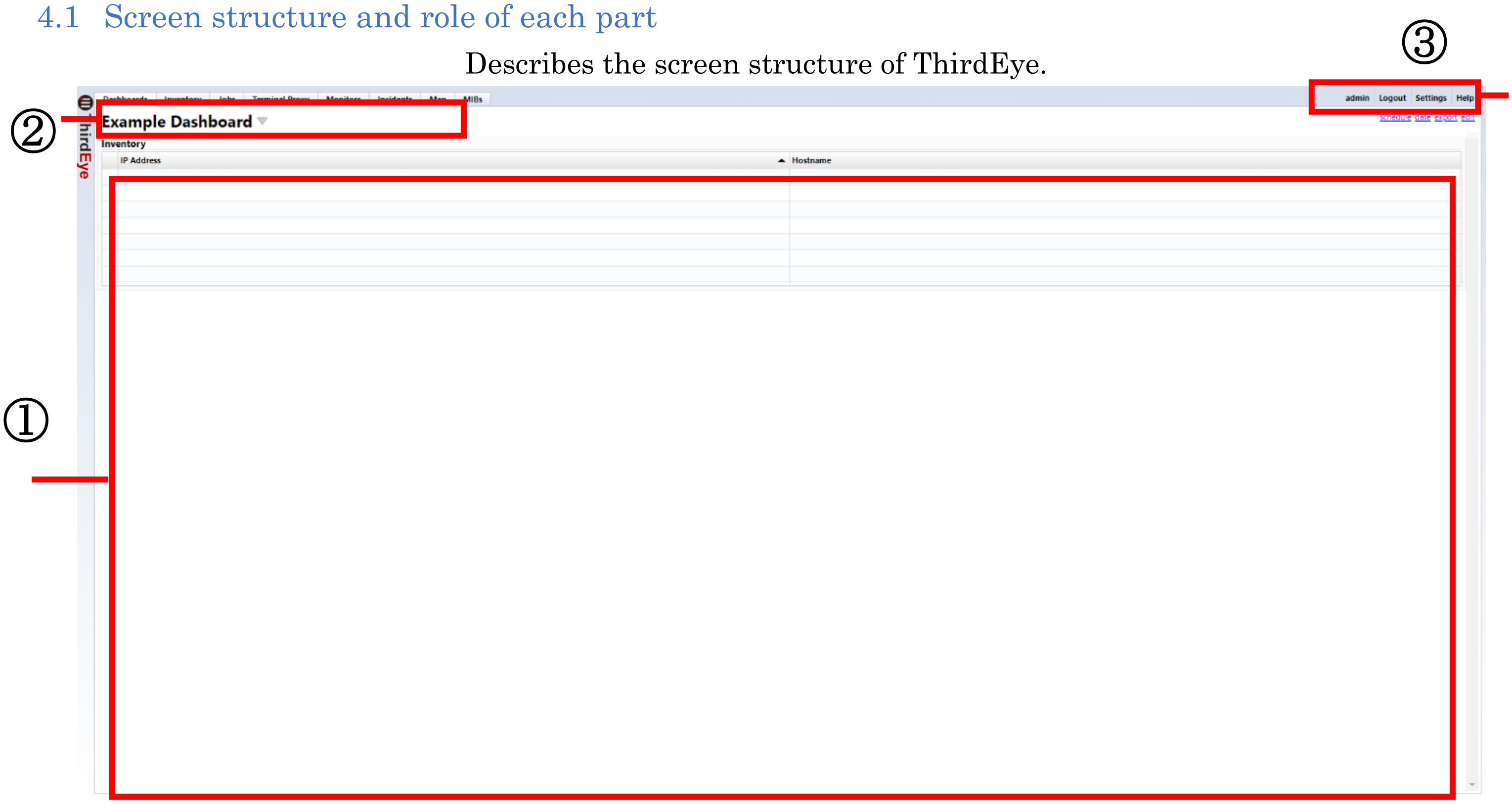


When logging out, the ThirdEye login screen is displayed.

4. Screen Structure

4.1 Screen structure and role of each part

Describes the screen structure of ThirdEye.



No.	Name	Explanation
①	**Main tab**	This tab switches the main screen.
②	**Main display**	The screen corresponding to the tab selected on the main tab is displayed.
③	**Global menu**	This menu is fixedly displayed in the upper right corner of the screen.

4.1.1 Main tab configuration

Tab	Explanation
Dashboard	Display the dashboard. For details, see 5.5 Creating a dashboard.
Inventory	Displays registered devices as an inventory (list).
Jobs	Displays a list of jobs.
Terminal Proxy	Displays a list of records when the terminal is connected to the device.

Tab	Explanation
Monitors	Configure monitoring settings.
Incidents	Displays a list of incidents.
Map	Display the map. In the map, you can create, edit, and delete maps.
MIBs	Search and browse MIBs.

4.1.2 Global menu structure

Name	Explanation
User	The current login username is displayed.
Logout	Log out of ThirdEye.
Setting	The various settings ([Server Settings]) screen is displayed.
Help	The help menu is displayed.

5. Basic Settings

This section discusses the basic settings for ThirdEye's monitoring.

5.1 Setting the SNMP community

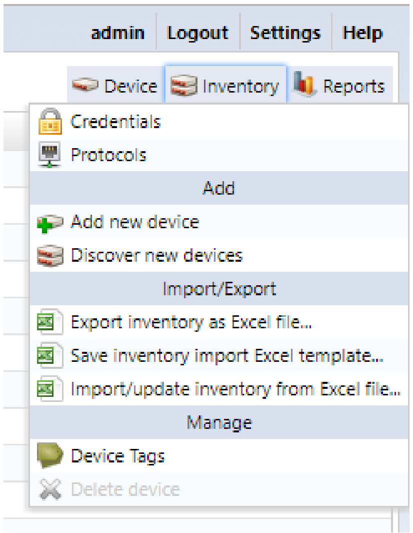
When monitoring from a monitored device using SNMP, it is necessary to set the SNMP community (hereinafter called “community name”) that has already been set to the monitored device to ThirdEye. Set the community name in [Inventory]-> [Credential] on the device tab. There are two ways to set credentials: "Dynamic" and "Static".

Description	Explanation
Dynamic	Set common credentials for the address range. This is useful when a common community name is 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 a different community name is set for each monitored device.

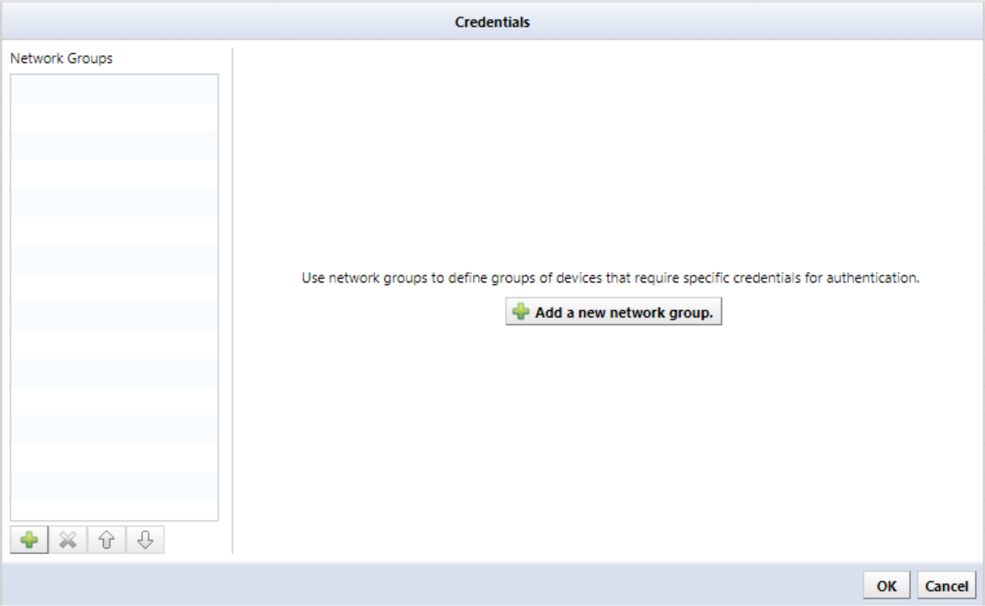
5.1.1 Setting a common SNMP community

If a common community name is set for the monitored devices, use "Dynamic".

1. Select the Inventory tab and click [Inventory] > [Credential].



Click [✚(Add)] or [Add New Network Group].

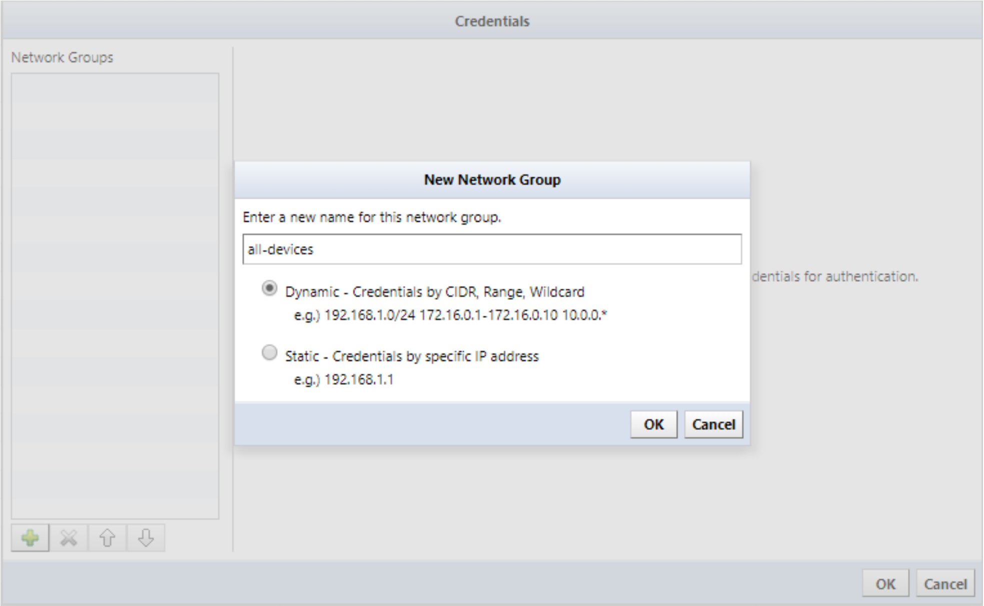


Credentials

Network Groups

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

2. Enter the network group name, select "Dynamic", and click [OK].



Credentials

Network Groups

New Network Group

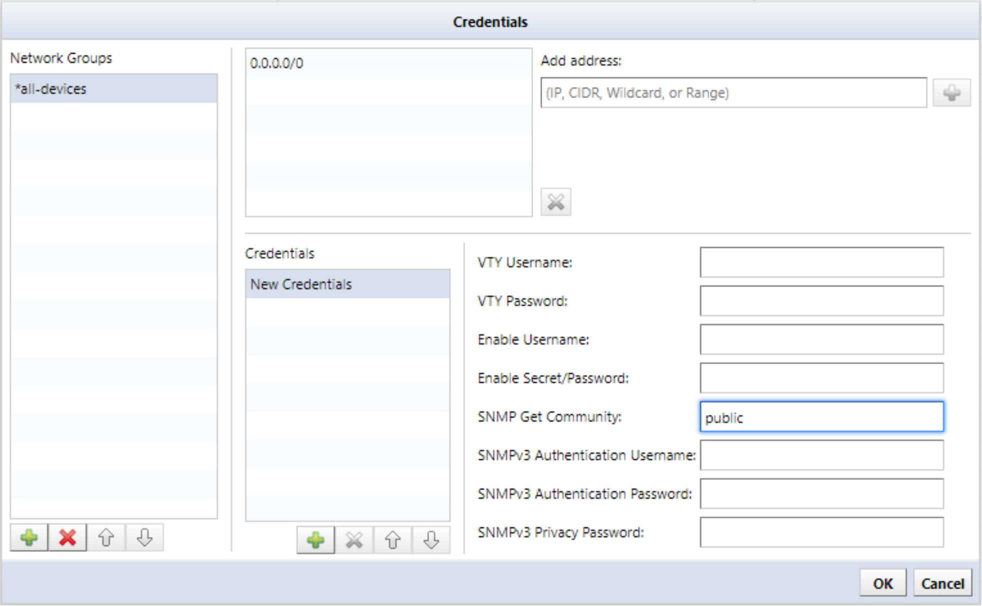
Enter a new name for this network group.

all-devices

● 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

3. Enter the network group address range in the [Add Address] field and click [+ (Add)]. Enter the community name of the monitored device in the “SNMP Get Community” field of the credential.



0.0.0.0/0

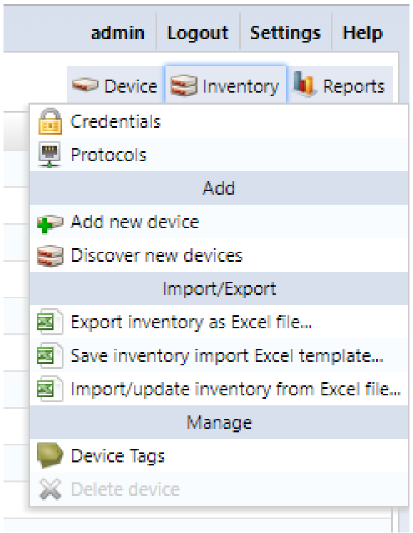
VTY Username:
VTY Password:
Enable Username:
Enable Secret/Password:
SNMP Get Community: public
SNMPv3 Authentication Username:
SNMPv3 Authentication Password:
SNMPv3 Privacy Password:

4. Click OK to save the settings.

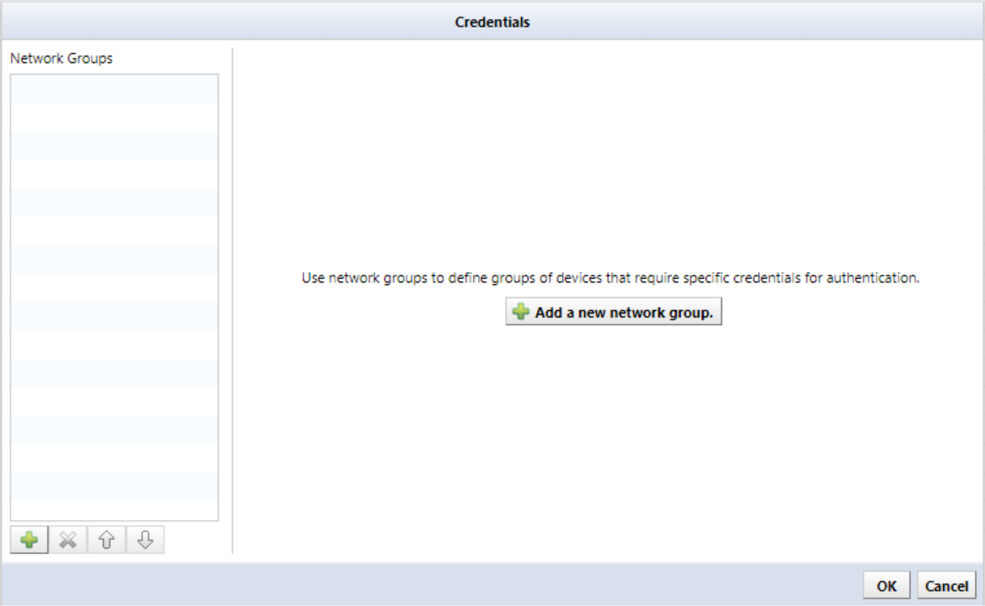
5.1.2 Set SNMP community for each device

If a different community name is set for each monitored device, use "Static".

1. Select the Inventory tab and click [Inventory] > [Credential].



2. Click [✚ (Add)] or [Add New Network Group].

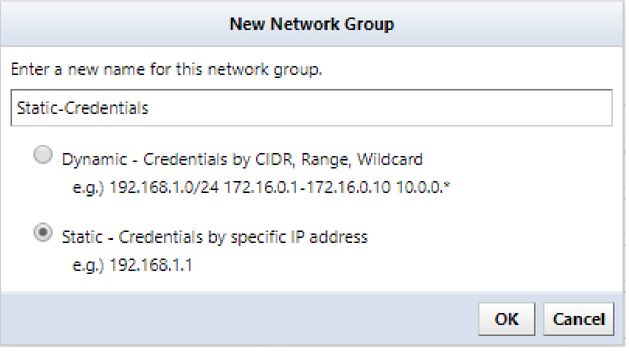


Credentials

Network Groups

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

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



New Network Group

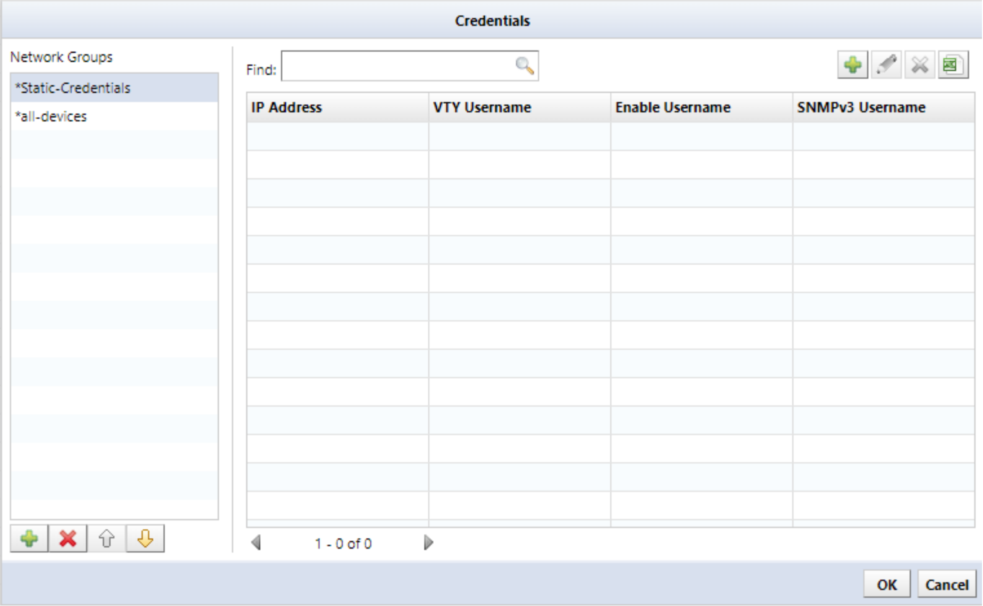
Enter a new name for this network group.

Static-Credentials

○ 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

4. Click [✚ (Add)] .



Credentials

Network Groups

*Static-Credentials

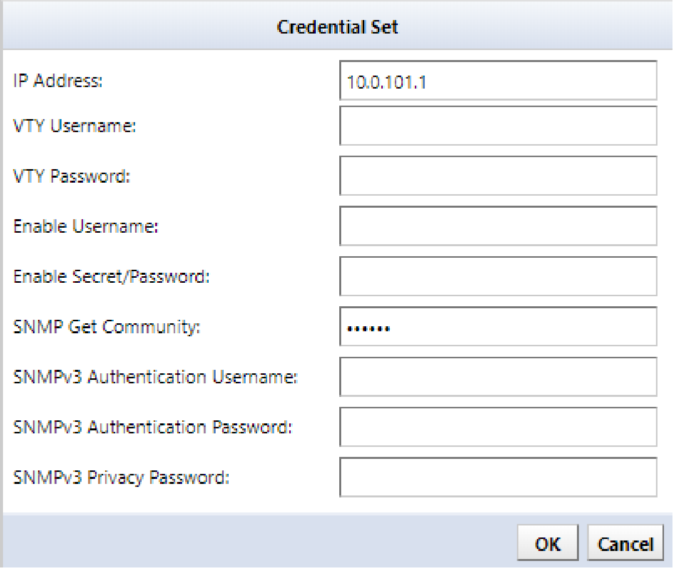
*all-devices

Find:

IP Address	VTY Username	Enable Username	SNMPv3 Username

1 - 0 of 0

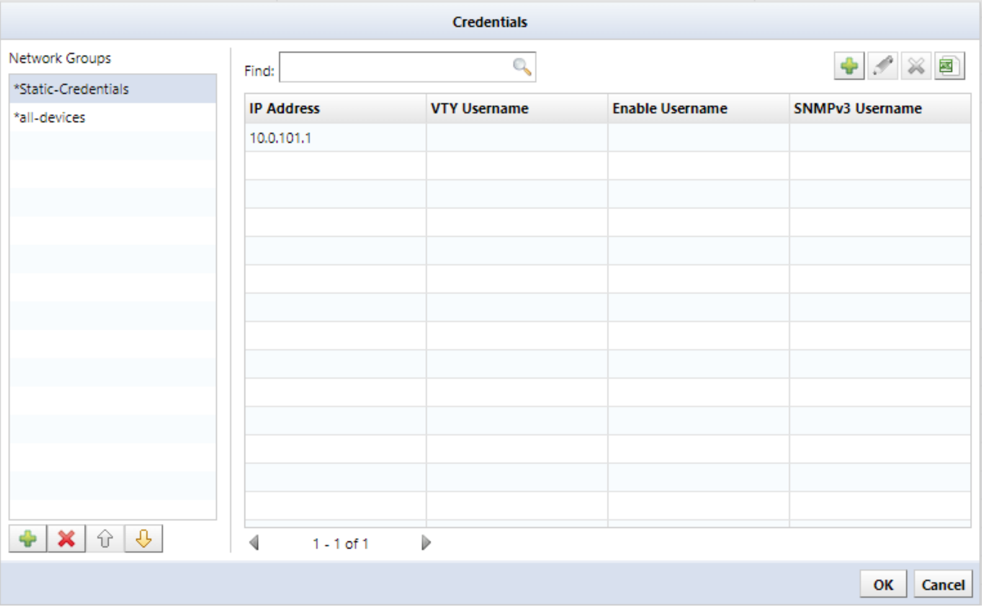
5. Enter the IP address, and enter the community name of the monitored device in the "SNMP Get Community" field.



Credential Set

IP Address:	10.0.101.1
VTY Username:	
VTY Password:	
Enable Username:	
Enable Secret/Password:	
SNMP Get Community:	••••••
SNMPv3 Authentication Username:	
SNMPv3 Authentication Password:	
SNMPv3 Privacy Password:	

6. Click [OK] to save the settings.



*Static-Credentials

*all-devices

IP Address	VTY Username	Enable Username	SNMPv3 Username
10.0.101.1			

5.2 Adding devices

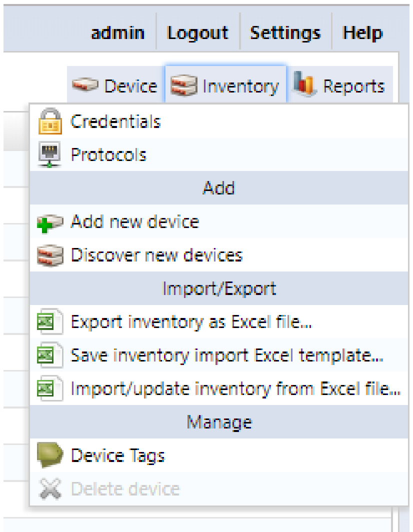
When adding a device to ThirdEye, use one of the following methods:

Description	Explanation
Manual	Enter the device IP address directly to add the device. Add one by one.
Discovery	Devices that are within the specified IP address range are automatically detected and added. * SNMP is used for discovery, so set the credentials in advance.
Import	This function reads device data from XLSX files. Export the template file for import and enter the monitored device information in the file.

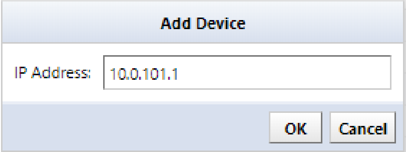
* When adding a device, the device is not displayed on the map. If you want to display a device icon on the map, add the device to the map. For details on how to add to the map, see "5.4.2 Inserting the device into the map" below.

5.2.1 Registering one by one

1. Select the [Inventory] tab and click [Inventory] > [Add Device].

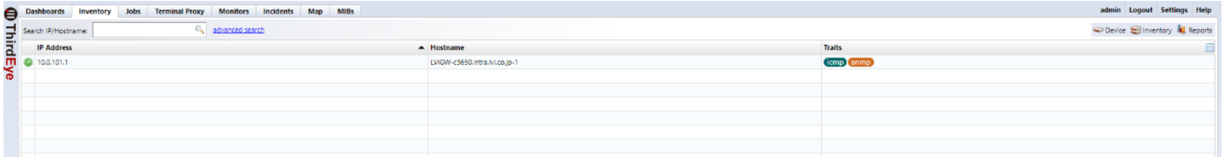


2. Enter the IP address of the device to be added and click [OK].



IP Address: 10.0.101.1

After clicking [OK], the device information is acquired from the monitored device and added to the device list.

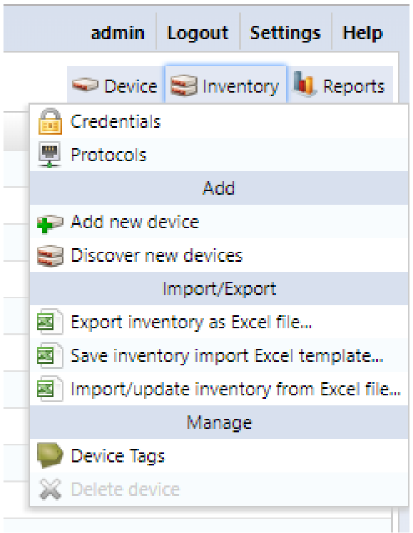


IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp

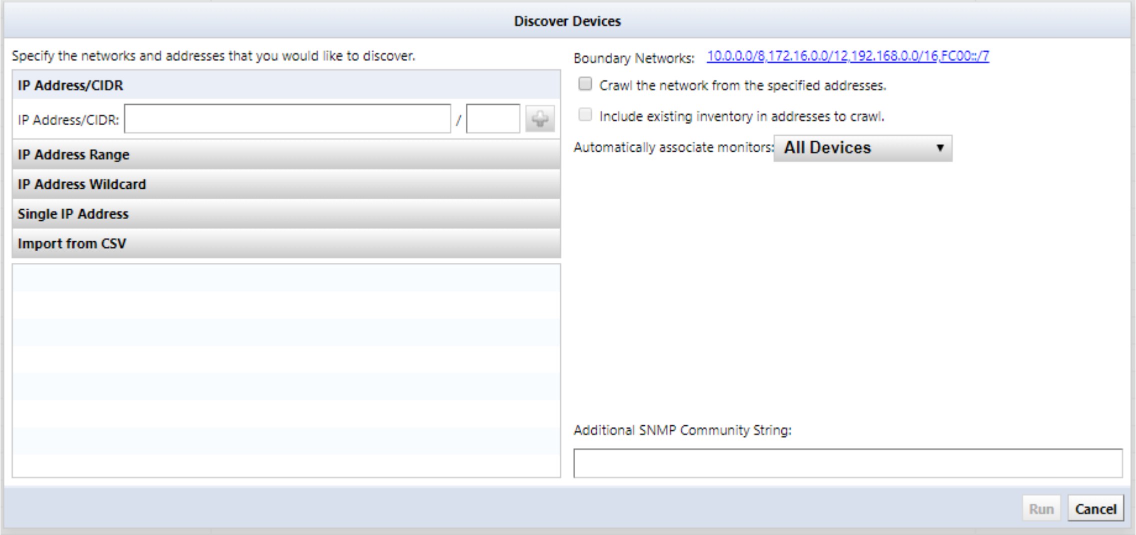
* If communication with the IP to be added is not possible, it will be added, but the host name and interface information cannot be acquired.

5.2.2 Registering devices on the network

1. Select the Inventory tab and click Inventory> Device Discovery.



2. Specify the IP address range to be discovered and click [(Add)].



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

IP Address/CIDR: /

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

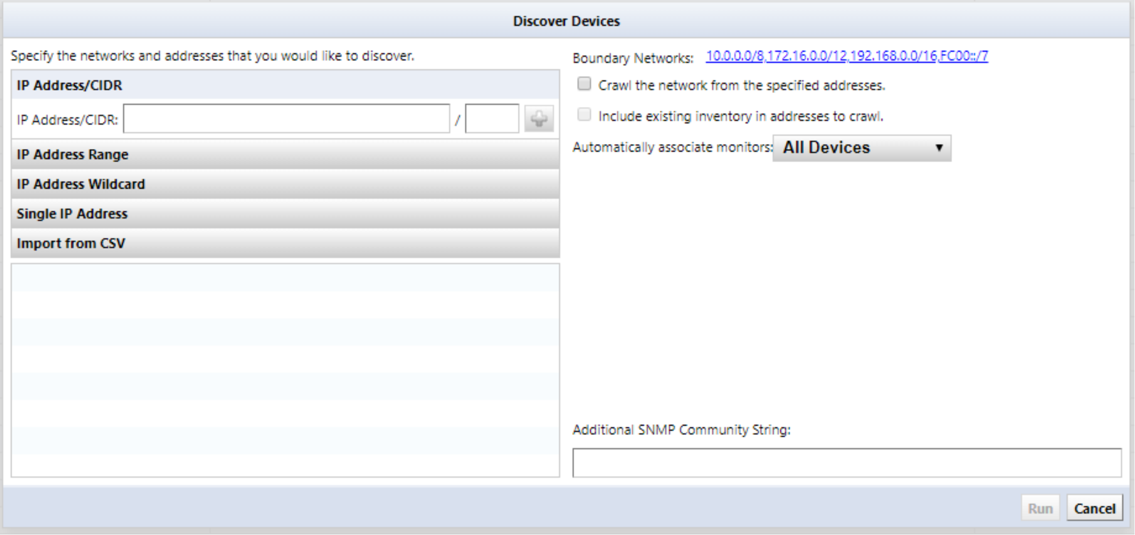
□ Crawl the network from the specified addresses.

□ Include existing inventory in addresses to crawl.

Automatically associate monitors: All Devices

Additional SNMP Community String:

3. Input information is added to the lower left of the screen. 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

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

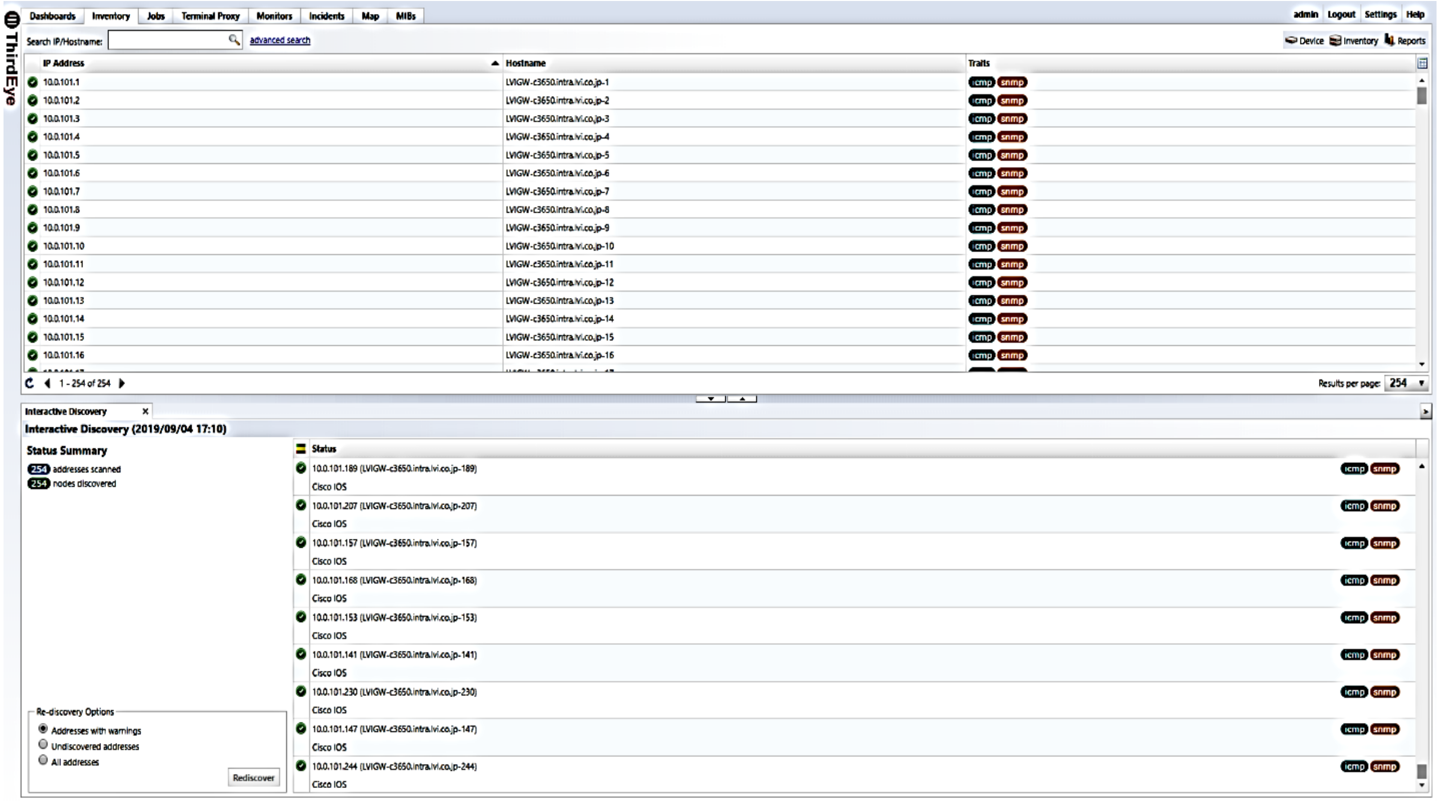
☐ Crawl the network from the specified addresses.

☐ Include existing inventory in addresses to crawl.

Automatically associate monitors: All Devices ▼

Additional SNMP Community String:

4. Discovery starts and the discovery result is displayed at the bottom of the screen.



Search IP/Hostname:

IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 254

Results per page: 254 ▼

Interactive Discovery ×

Interactive Discovery (2019/09/04 17:10)

Status Summary

254 addresses scanned

254 nodes discovered

Re-discovery Options

● Addresses with warnings

○ Undiscovered addresses

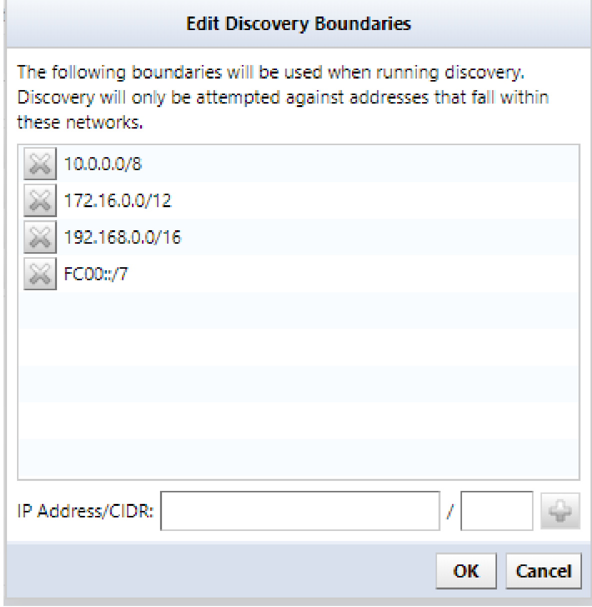
○ All addresses

Status	Traits
10.0.101.189 (LVIGW-c3650.intra.lvi.co.jp-189) Cisco IOS	icmp snmp
10.0.101.207 (LVIGW-c3650.intra.lvi.co.jp-207) Cisco IOS	icmp snmp
10.0.101.157 (LVIGW-c3650.intra.lvi.co.jp-157) Cisco IOS	icmp snmp
10.0.101.168 (LVIGW-c3650.intra.lvi.co.jp-168) Cisco IOS	icmp snmp
10.0.101.153 (LVIGW-c3650.intra.lvi.co.jp-153) Cisco IOS	icmp snmp
10.0.101.141 (LVIGW-c3650.intra.lvi.co.jp-141) Cisco IOS	icmp snmp
10.0.101.230 (LVIGW-c3650.intra.lvi.co.jp-230) Cisco IOS	icmp snmp
10.0.101.147 (LVIGW-c3650.intra.lvi.co.jp-147) Cisco IOS	icmp snmp
10.0.101.244 (LVIGW-c3650.intra.lvi.co.jp-244) Cisco IOS	icmp snmp

When discovery is complete, discovered devices are added automatically.

MEMO :

Only IP addresses that can be discovered can be discovered within the range displayed in the perimeter network. When discovering IP addresses outside the perimeter network range, add them to the perimeter network.



Edit Discovery Boundaries

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

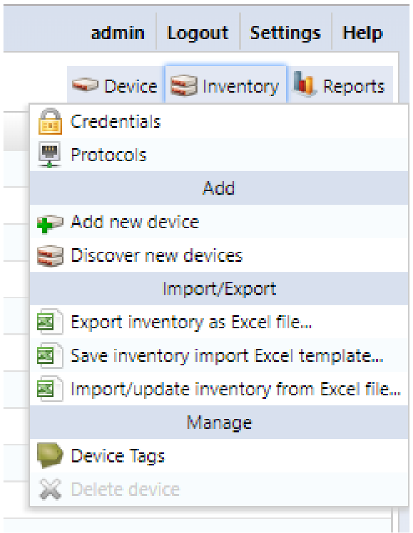
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- FC00::/7

IP Address/CIDR: /

5.2.3 Import registration from Excel file

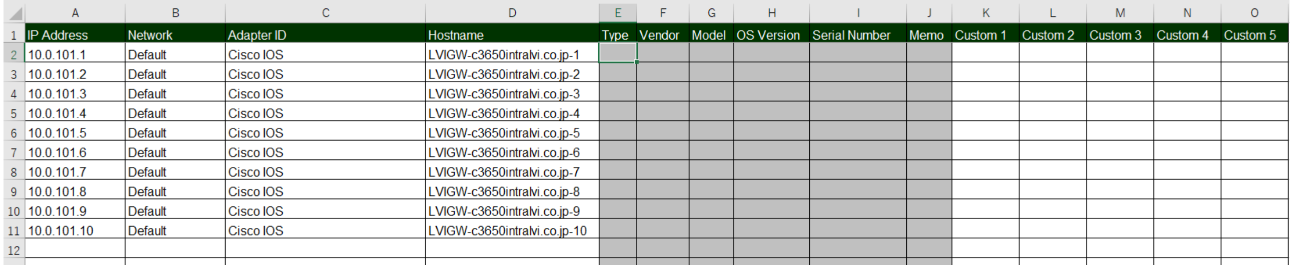
You can import monitored device information from an Excel file. An import template is provided. You can easily register it by exporting a file and filling in the information of monitored devices in the file.

1. Select the Inventory tab and click Inventory> Save Template for Inventory Import.



2. The file open screen is displayed. Select "Save File" and click [OK].
   * The file name will be "netLD-inventory YYYY-MM-DD.xlsx" and saved in the XLSX file format. "YYYY-MM-DD" represents the date.

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

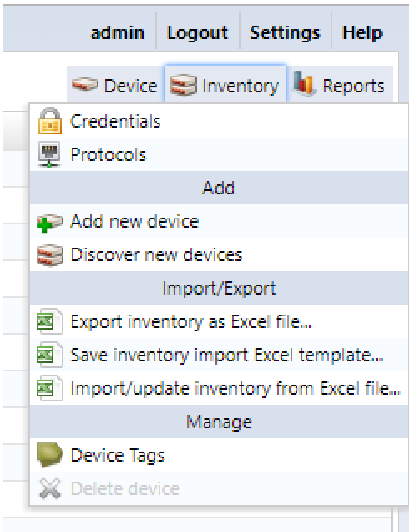


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	IP Address	Network	Adapter ID	Hostname	Type	Vendor	Model	OS Version	Serial Number	Memo	Custom 1	Custom 2	Custom 3	Custom 4	Custom 5
2	10.0.101.1	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-1											
3	10.0.101.2	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-2											
4	10.0.101.3	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-3											
5	10.0.101.4	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-4											
6	10.0.101.5	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-5											
7	10.0.101.6	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-6											
8	10.0.101.7	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-7											
9	10.0.101.8	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-8											
10	10.0.101.9	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-9											
11	10.0.101.10	Default	Cisco IOS	LVIGW-c3650intralvi.co.jp-10											
12															

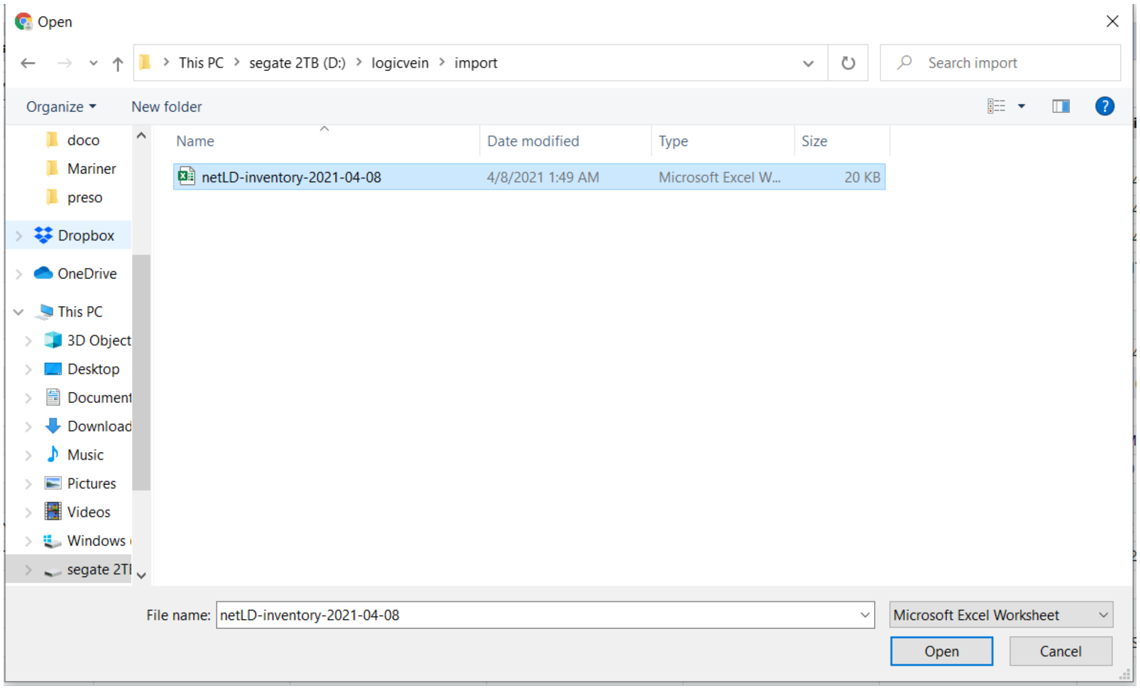
Description	Explanation	Required	Example
IP Address	Enter the IP address of the device.	✓	192.168.1.10
Network	Select "Default" from the pull-down list.	✓	Default
Adapter ID	Select the device adapter. * This item does not need to be specified in the current version.	×	Cisco IOS

Hostname	Enter the device hostname.	×	
Custom 1～5	Enter the information for "Custom Device Field".	×	

1. Click Inventory> Import / Update Inventory from Excel File.



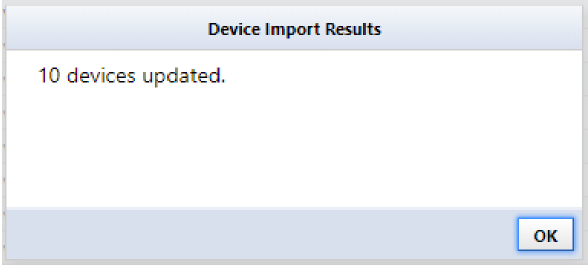
2. The file selection dialog is displayed. Select the edited file and click [Open].



Name	Date modified	Type	Size
netLD-inventory-2021-04-08	4/8/2021 1:49 AM	Microsoft Excel W...	20 KB

File name: netLD-inventory-2021-04-08

3. A confirmation message is displayed. Click [OK].



Device Import Results

10 devices updated.

5.3 Configure monitoring settings

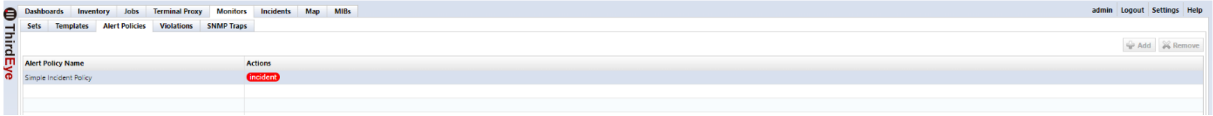
There are several methods of monitoring monitored devices, such as collecting information by SNMP and monitoring using ICMP Ping. This section describes the flow of basic monitoring settings. The flow to start monitoring is as follows.

I. Action settings (Alert policy function)
II. Monitoring item setting (Monitor function)
III. Trigger settings such as threshold (Trigger function)

5.3.1 Setting actions when an abnormality is detected

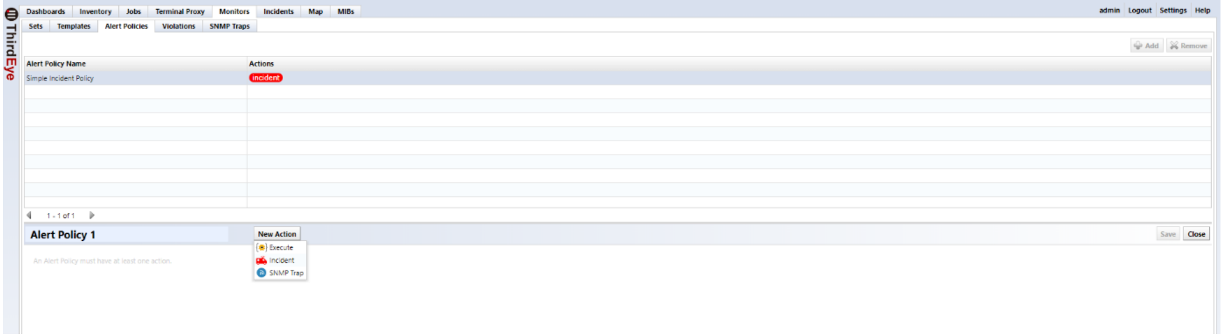
There are three types of actions to be taken when an abnormality is detected: incident registration, email transmission, program execution, and SNMP trap. Action settings are set on the Alert Policy tab under the Monitor tab. The procedure for creating a new alert policy is described below.

1. Select [Monitor] → [Alert Policy] and click [Add].



Alert Policy Name	Actions
Simple Incident Policy	incident

2. Enter the alert policy name. Click Add Action and select an action.
   * Multiple actions can be added.



Alert Policy Name	Actions
Simple Incident Policy	incident

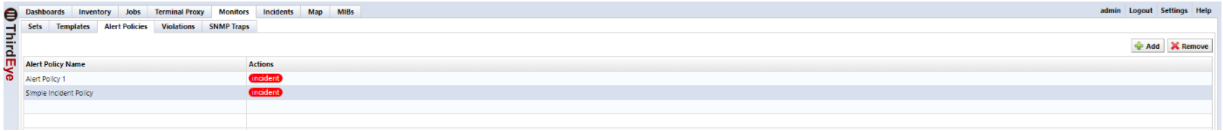
Alert Policy 1

An Alert Policy must have at least one action.

[Action content]

Description	Explanation
Execute	Executes a command on the remote host when a failure is detected.
Incident	Execute incident registration and email transmission when a failure is detected.
SNMP Trap	An SNMP trap is sent when a failure is detected.

3. Click [Save] and click [Close]

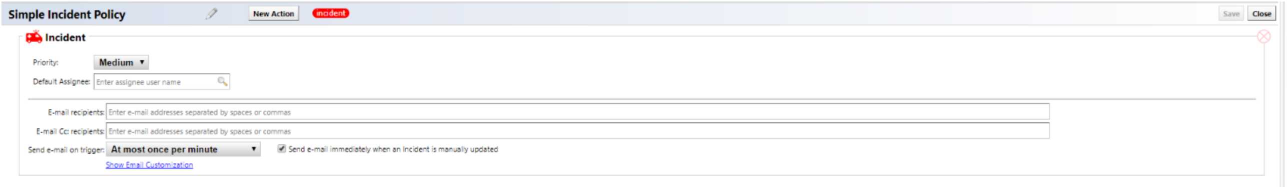


Alert Policy Name	Actions
Alert Policy 1	incident
Simple Incident Policy	incident

This completes the alert policy settings. Each action is described below.

i. Incident registration

In incident registration, an incident is created when a failure occurs. You can also send an email by entering an email address in Email destination / Cc.



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

Send e-mail on trigger: At most once per minute

☑ Send e-mail immediately when an Incident is manually updated

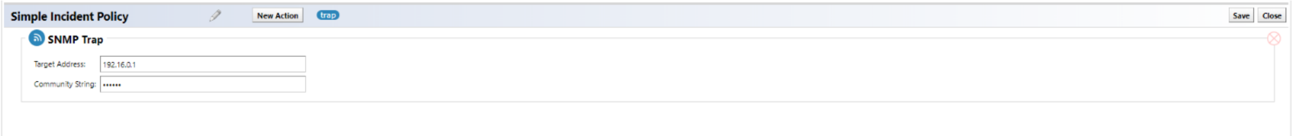
Show Email Customization

Description	Explanation
Priority	Specify the priority for incident registration.
Default Assignee	Specify the person responsible for the incident.
E-mail recipients	Set the email destination for incidents. * Email will not be sent if not entered.
E-mail Cc recipients	Set the CC email destination. * Email will not be sent if not entered.
Send e-mail on trigger	Specify when to notify by email. (Initial value: Send once every minute)
Send e-mail immediately when an incident is manually updated	Set whether to notify by e-mail when an incident is updated (close processing, etc.).

In order to send mail, it is necessary to set up a mail server in advance. Refer to "7.5 Setting Mail Server" for mail server settings.

ii. Send SNMP trap

Traps can be sent to other NMSs and alarm devices when a failure occurs.



Target Address: 192.16.0.1

Community String: ••••••

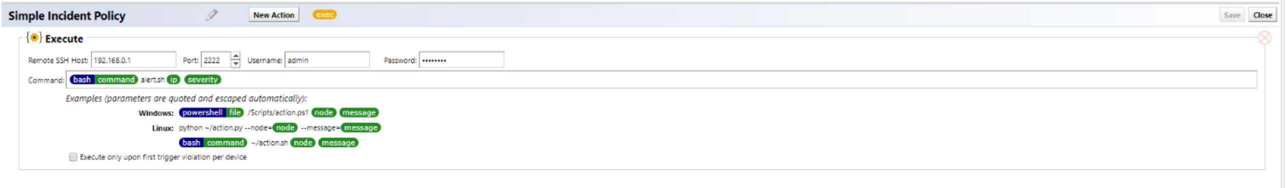
Description	Explanation
Target Address	Specify the destination of the SNMP trap that is sent when a failure occurs.
Community String	Specify the community name of the SNMP trap to be sent.

The traps sent from ThirdEye are as follows.

Description		Explanation
Trap name		triggerViolation
Trap OID		1.3.6.1.4.1.45654.2.1.1
Varbinds	**thirdEyeDeviceUuid**	UUID of the failed device (used inside ThirdEye)
	thirdEyeDeviceIpAddress	IP address of the failed device.
	thirdEyeManagedNetwork	The network to which the failed device belongs.
	thirdEyeDeviceHostname	Hostname of the failed device.
	thirdEyeMessage	Incident message
	thirdEyeMeasurement	Monitoring contents
	thirdEyeSeverity	Incident severity
	thirdEyeDeviceCustom1	Custom 1 contents of the failed device
	thirdEyeDeviceCustom2	Custom 2 contents of the failed device
	thirdEyeDeviceCustom3	Custom 3 contents of the failed device
	thirdEyeDeviceCustom4	Custom 4 contents of the failed device
	thirdEyeDeviceCustom5	Custom 5 contents of the failed device

iii. Execute the program from the remote host

Log in to the specified remote host using SSH and execute the specified command from the remote host.



Simple Incident Policy

Execute

Remote SSH Host: 192.168.0.1 Port: 2222 Username: admin 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

□ Execute only upon first trigger violation per device

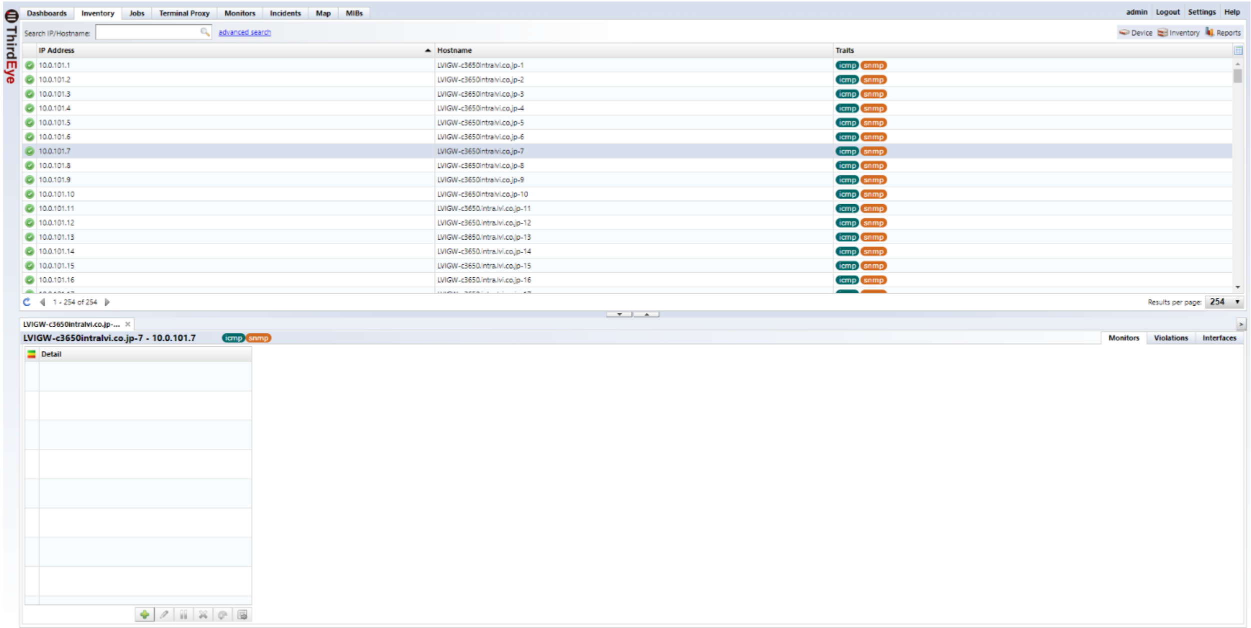
Description	Explanation
Remote SSH Host	Specify the remote host (external server) to execute the command.
Username	The username used to log in to the remote host.
Password	The password of the user specified by "Username".
Command	A command to be executed on the remote host.
Execute only upon first trigger violation per device	Executes the command for each device only at the first violation.

5.3.2 Setting up Ping monitoring

To perform Ping monitoring, add an ICMP monitor. Monitored devices registered by manual addition or discovery are automatically assigned as an "ICMP Ping (Default)" monitor, and Ping monitoring starts immediately after registration. This section describes the procedure for adding a monitored device under the following conditions.

[Conditions]
Monitoring period: 5 minutes
Alert condition: No response twice in 10 minutes
* Refer to "" for details of ThirdEye's ICMP polling.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.

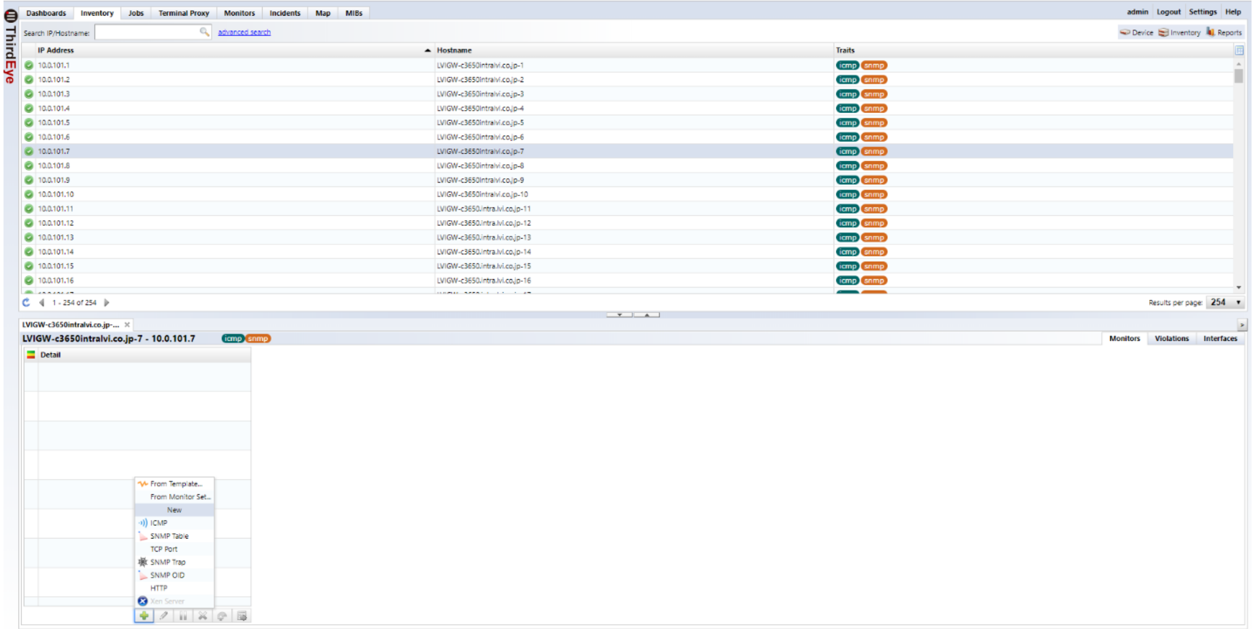


IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

2. Click [(Add)] in the lower left, and then click "ICMP".



Search IP/Hostname:

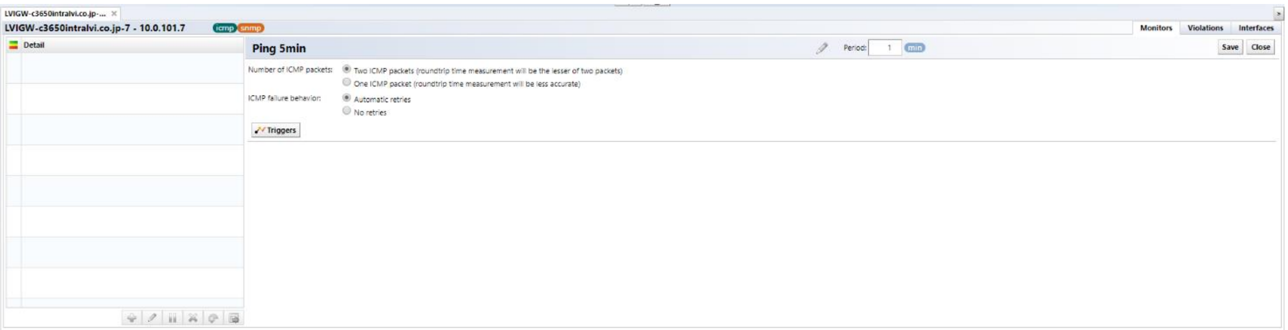
IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 254

LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

3. Enter any monitor name.



LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

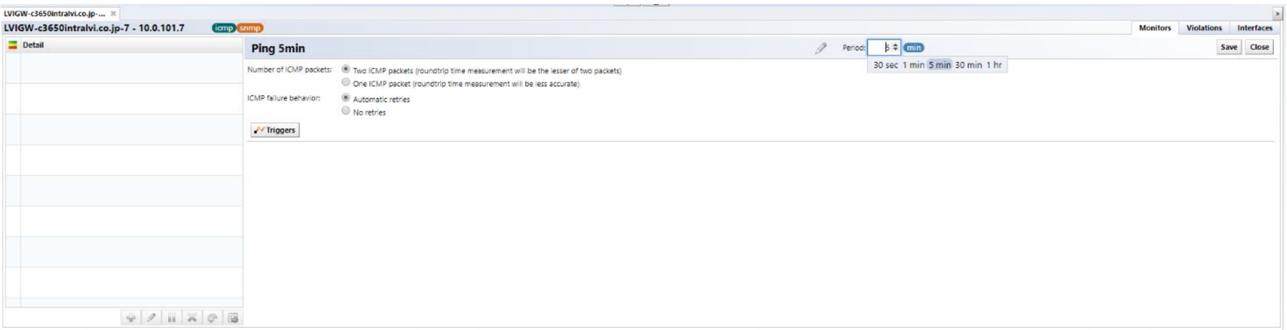
Ping 5min

Period: 1 min

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

4. Specify the “Period”.



LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

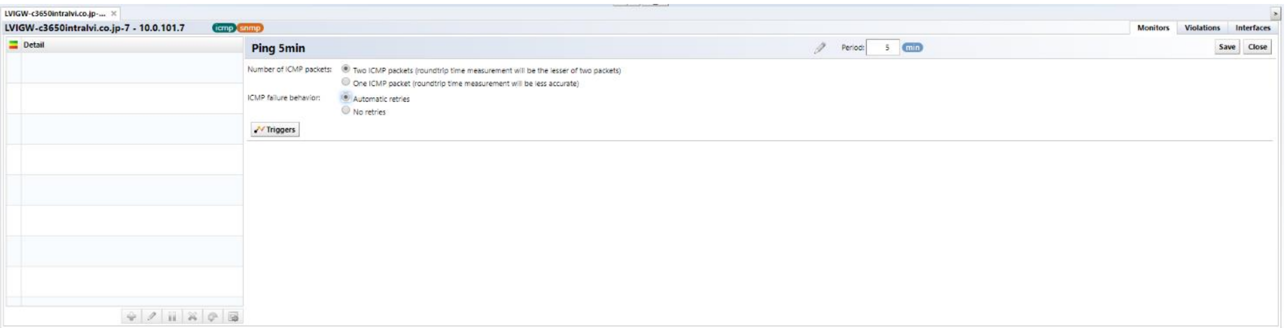
Ping 5min

Period: 5 min

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

5. Select the number of ICMP packets and retry.



LVIGW-c3650intralvi.co.jp-...
LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7
icmp
snmp
Detail
Monitors
Violations
Interfaces
Save
Close
Triggers

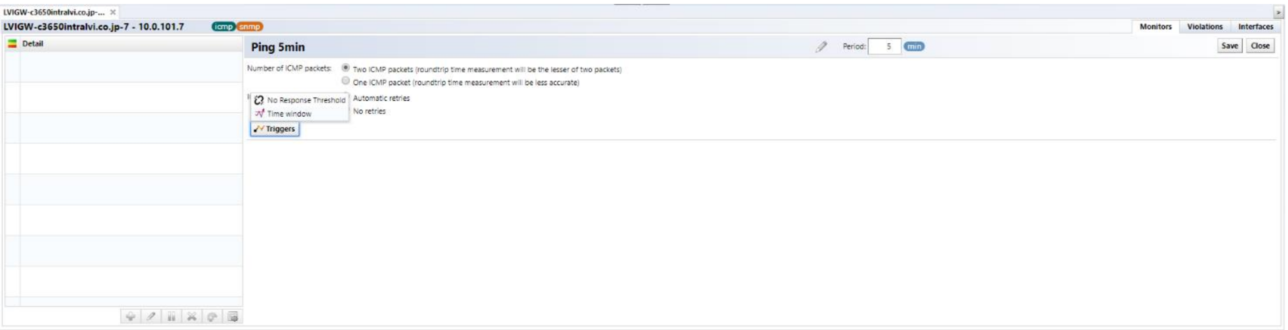
Ping 5min

Period: 5 min

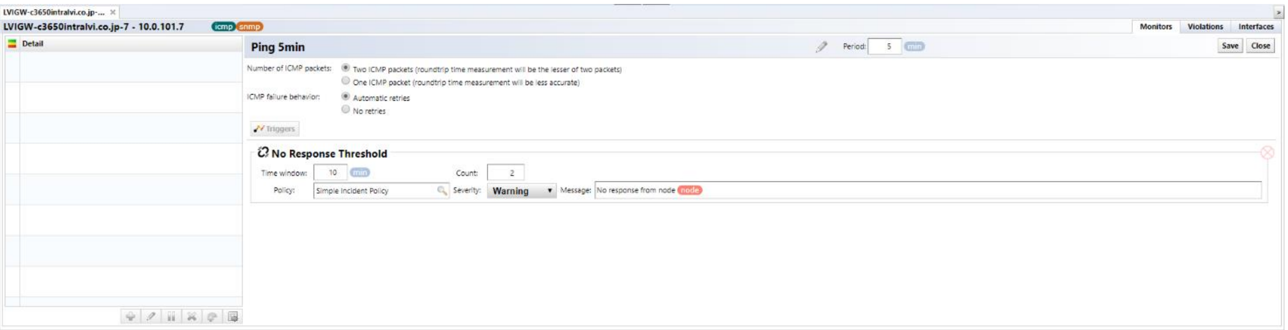
Number of ICMP packets: ● Two ICMP packets (roundtrip time measurement will be the lesser of two packets) ○ One ICMP packet (roundtrip time measurement will be less accurate)

ICMP failure behavior: ● Automatic retries ○ No retries

6. Click [Triggers] and click [No Response Threshold].



7. Enter the following items.



No Response Threshold

Time window: 10 min

Count: 2

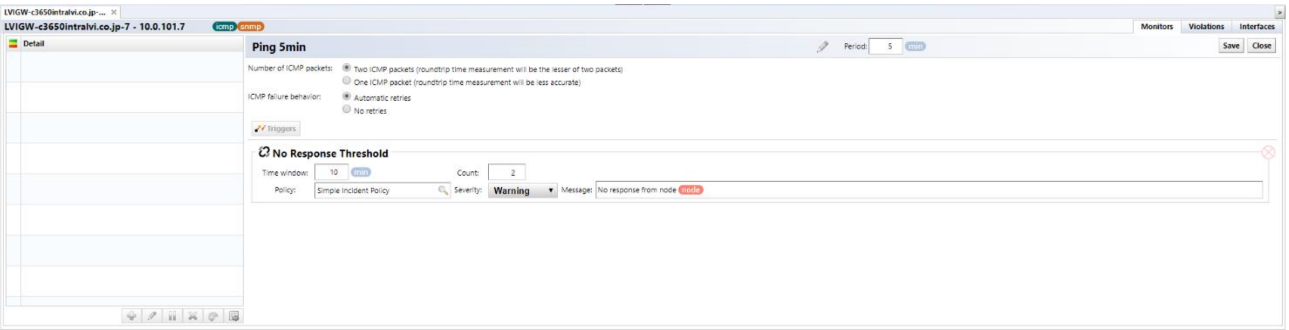
Policy: Simple Incident Policy

Severity: Warning

Message: No response from node node

Description	Explanation
Time window	Set the period for executing the process. (Minimum value: 1 minute) A period that is used as a reference for counting how many times a failure (count) has occurred within a set period of time, the process defined in the policy is executed.
Count	Set how many times the process fails within the set period. (Minimum value: 1)
Policy	Specify the alert policy.
Severity	Select a severity from the follows: (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 "Register Incident" action must be defined in the alert policy.

8. Click [Save].



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7

Ping 5min

Period: 5 min

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

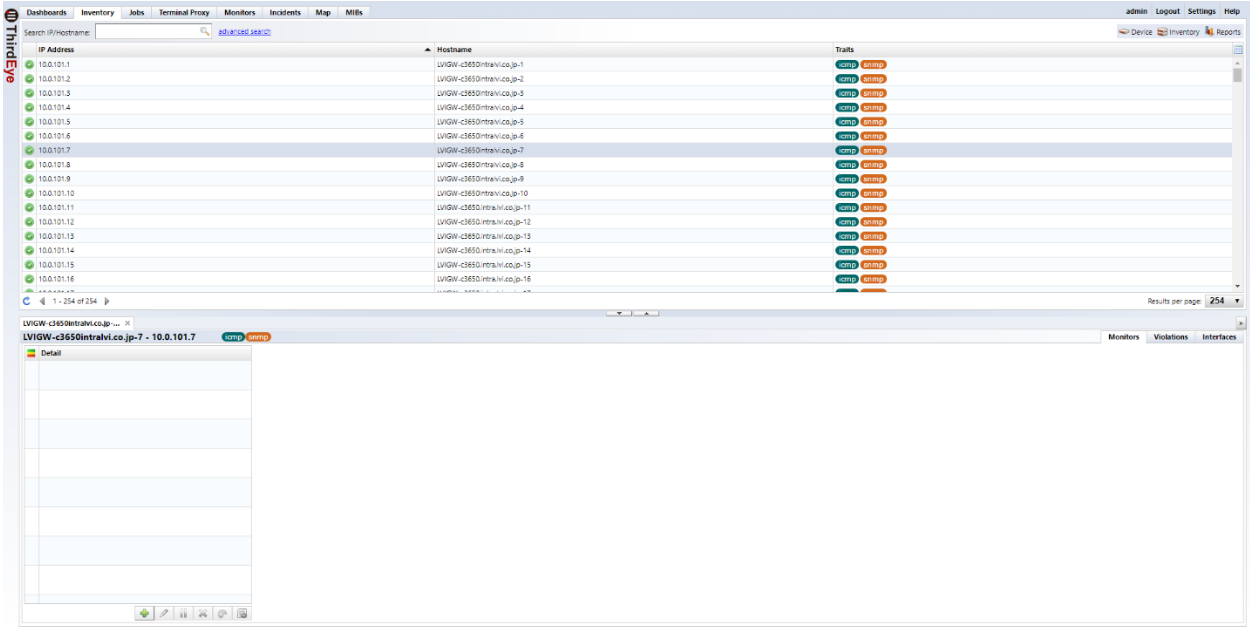
Time window: 10 min Count: 2

Policy: Simple Incident Policy Severity: Warning Message: No response from node node

5.3.3 Collecting SNMP information

Add an SNMP monitor to obtain MIB information such as CPU usage and traffic volume from monitored devices. This section describes the procedure for obtaining the CPU usage rate (cpmCPUTotal1minRev) of the following Cisco devices for the monitored device.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.

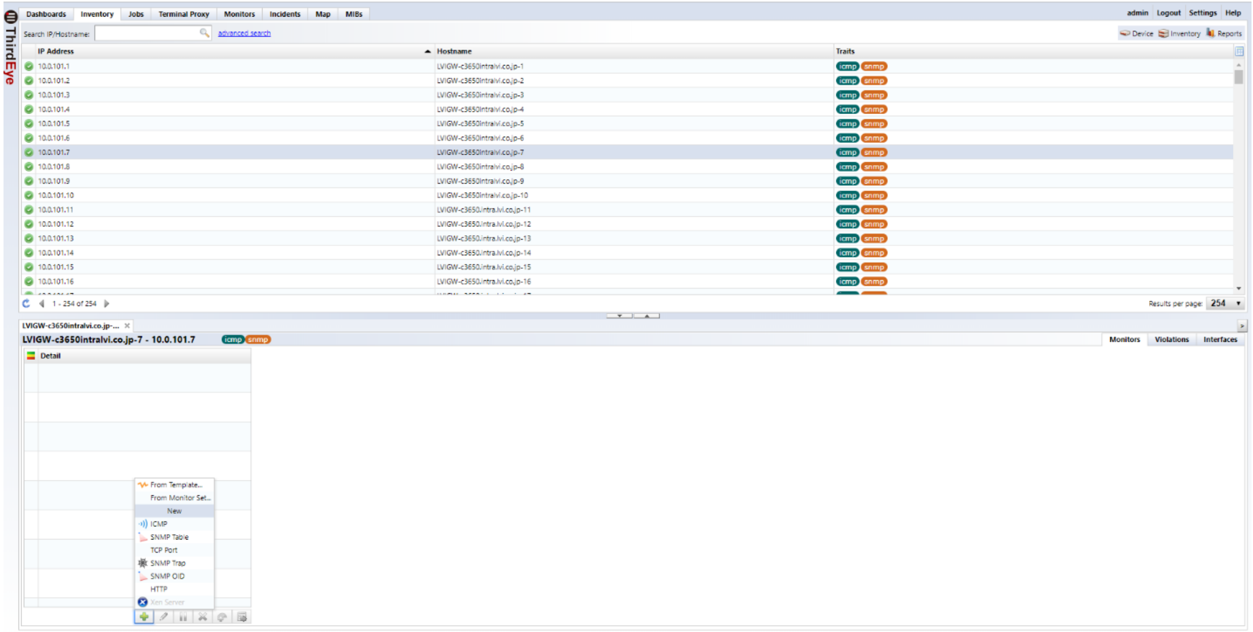


IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 254 Results per page: 254

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7

2. Click [(Add)] in the lower left and click “SNMP Table”.



IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

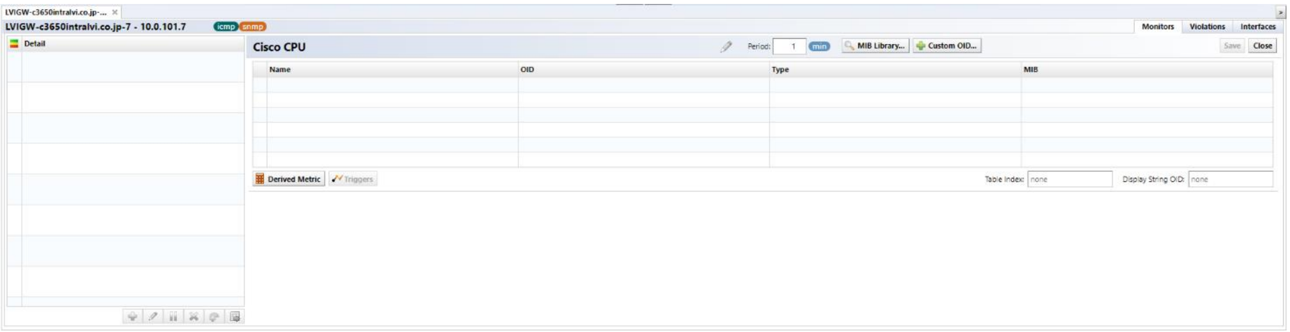
1 - 254 of 254

Results per page: 254

LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

3. Enter any monitor name.



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

Cisco CPU

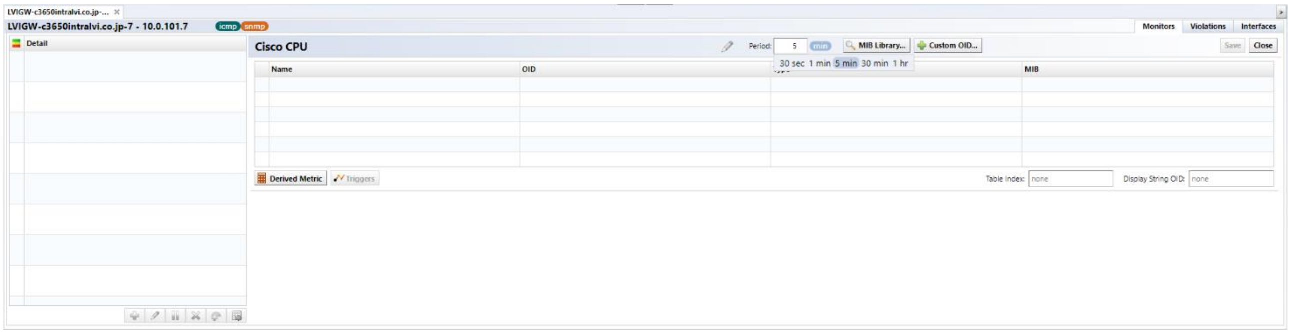
Period: 1 min

Name	OID	Type	MIB

Table Index: none

Display String OID: none

4. Specify the period.



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

Cisco CPU

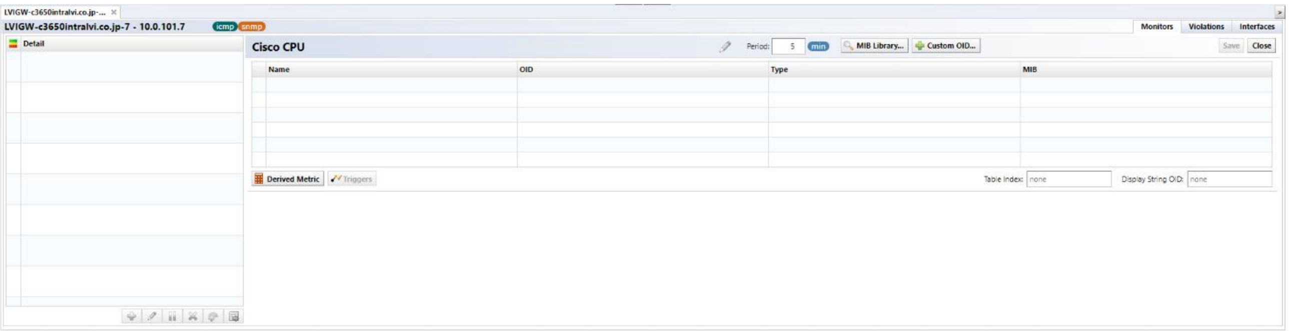
Period: 5 min

Name	OID		MIB

Table Index: none

Display String OID: none

5. Click [MIB Library].



Cisco CPU

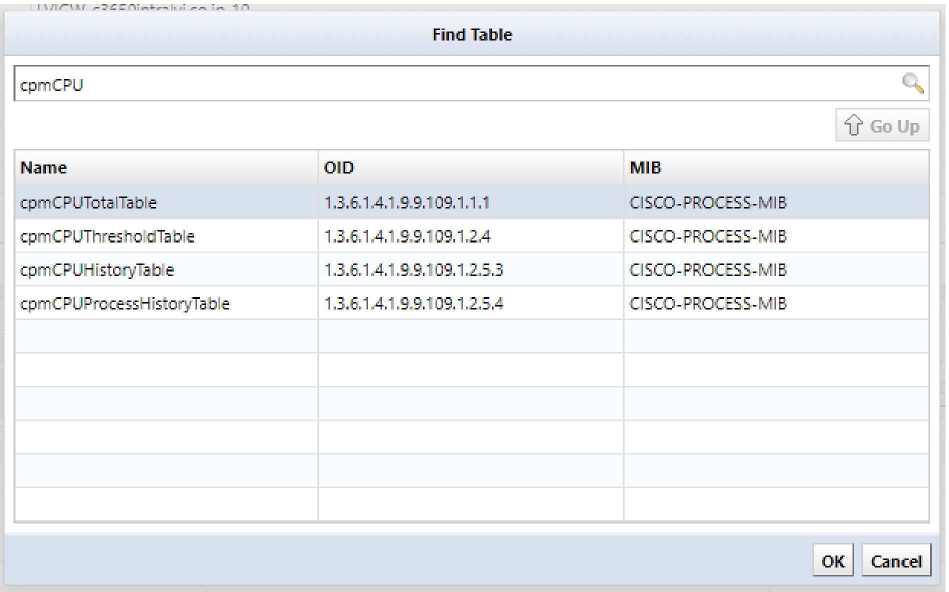
Period: 5 min

Name	OID	Type	MIB

Table Index: none

Display String OID: none

6. Enter the OID or name of the MIB in the OID search, select the MIB table to add, and click [OK].

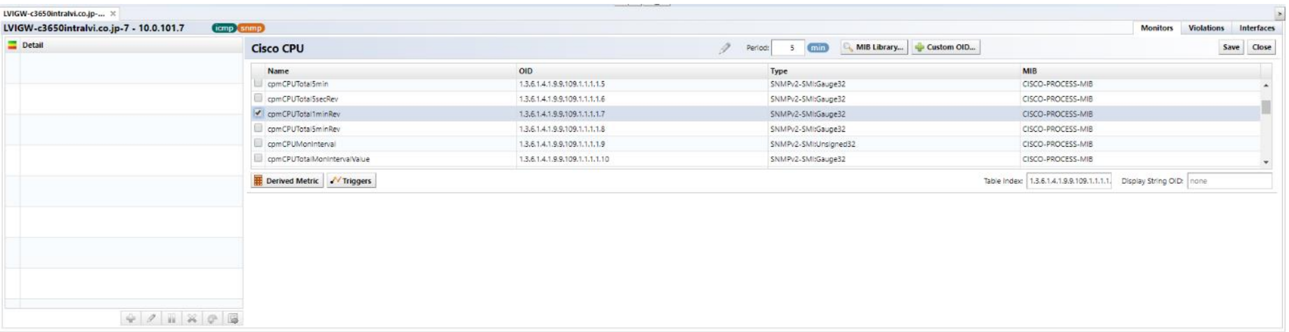


Find Table

cpmCPU

Name	OID	MIB
cpmCPUTotalTable	1.3.6.1.4.1.9.9.109.1.1.1	CISCO-PROCESS-MIB
cpmCPUThresholdTable	1.3.6.1.4.1.9.9.109.1.2.4	CISCO-PROCESS-MIB
cpmCPUHistoryTable	1.3.6.1.4.1.9.9.109.1.2.5.3	CISCO-PROCESS-MIB
cpmCPUProcessHistoryTable	1.3.6.1.4.1.9.9.109.1.2.5.4	CISCO-PROCESS-MIB

7. Insert a check into the MIB that you want to retrieve.



Cisco CPU

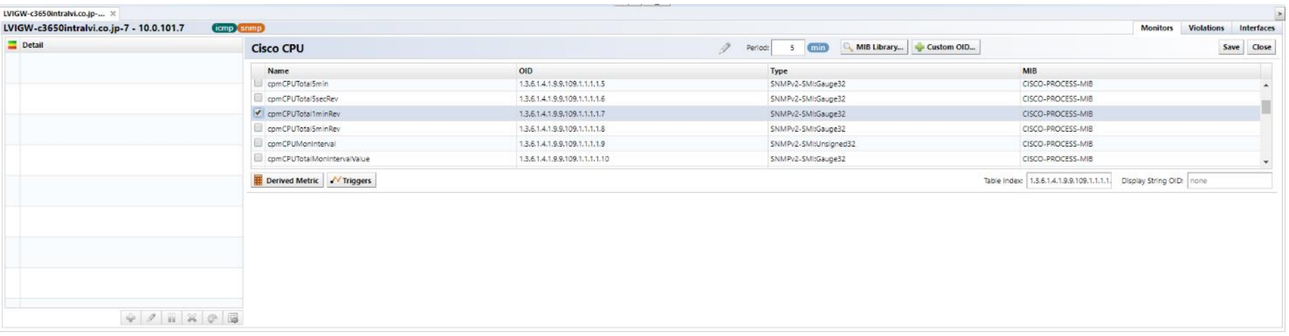
Period: 5 min

	Name	OID	Type	MIB
□	cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
☑	cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUMonInterval	1.3.6.1.4.1.9.9.109.1.1.1.1.9	SNMPv2-SMI:Unsigned32	CISCO-PROCESS-MIB
□	cpmCPUTotalMonIntervalValue	1.3.6.1.4.1.9.9.109.1.1.1.1.10	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Table Index: 1.3.6.1.4.1.9.9.109.1.1.1.1.

Display String OID: none

8. Click [Save].

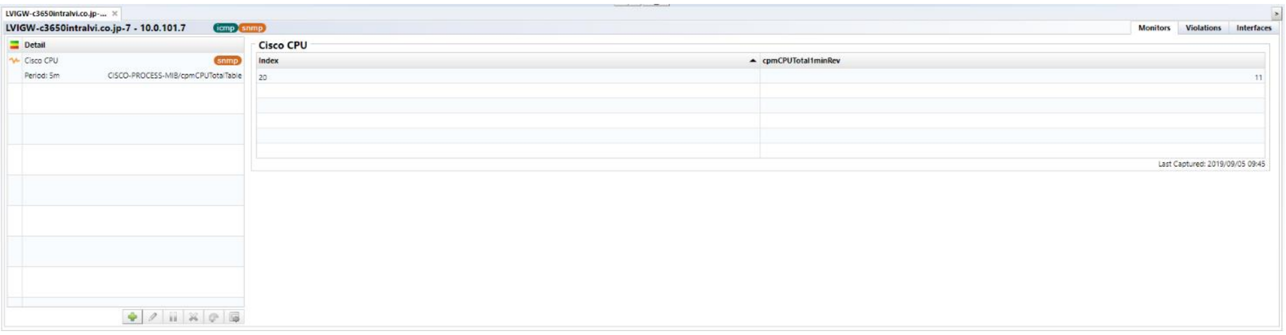


Period: 5 min

	Name	OID	Type	MIB
□	cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
☑	cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUMonInterval	1.3.6.1.4.1.9.9.109.1.1.1.1.9	SNMPv2-SMI:Unsigned32	CISCO-PROCESS-MIB
□	cpmCPUTotalMonIntervalValue	1.3.6.1.4.1.9.9.109.1.1.1.1.10	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Table Index: 1.3.6.1.4.1.9.9.109.1.1.1.1. Display String OID: none

After saving, data collection is started, and if it can be acquired normally, the data will be displayed on the device details screen.


LVIGW-c3650intralvi.co.jp-...
LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7
icmp
snmp
Monitors
Violations
Interfaces
Detail
Cisco CPU
snmp

Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU

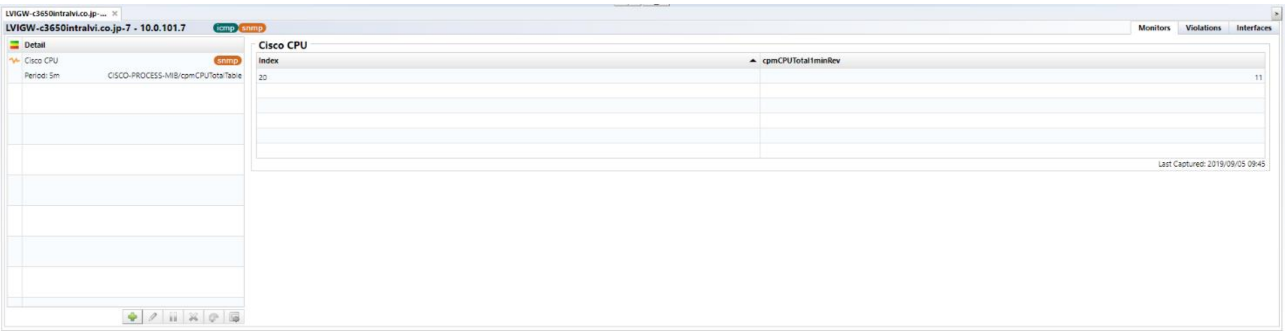
Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/05 09:45

5.3.4 Setting and monitoring thresholds

You can set a threshold for the data to be acquired and raise an alert when a violation occurs. Here, set the threshold value for the SNMP monitor created in 5.3.3.

1. From the details table, double-click the monitor for which a threshold is to be set or click [Edit].


LVIGW-c3650intralvi.co.jp-...
LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7
icmp
snmp
Monitors
Violations
Interfaces
Detail
Cisco CPU
snmp

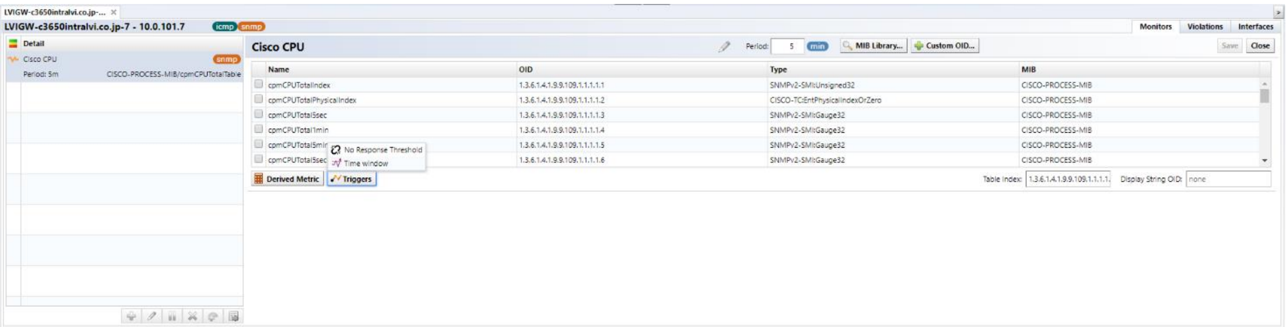
Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU

Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/05 09:45

2. Click [Triggers], and click [Time window]



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7

Detail

Cisco CPU — Period: 5m — CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU — Period: 5 min

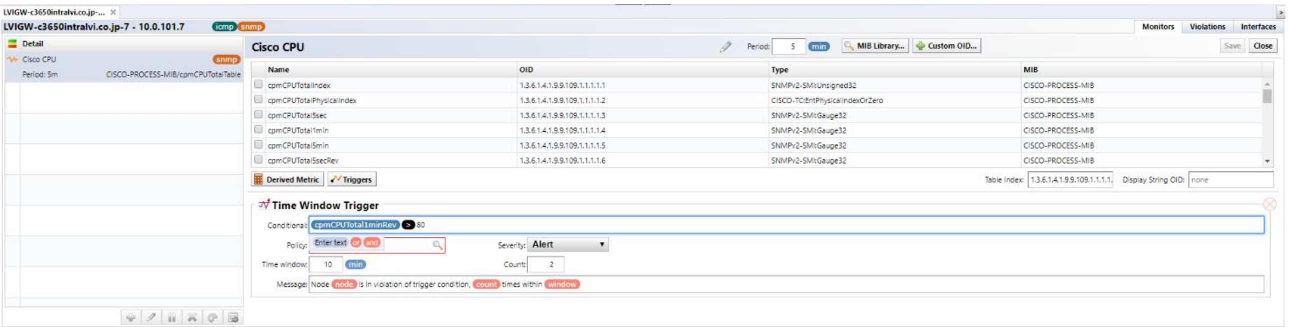
Name	OID	Type	MIB
cpmCPUTotalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.1	SNMPv2-SMI:Unsigned32	CISCO-PROCESS-MIB
cpmCPUTotalPhysicalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.2	CISCO-TC:EntPhysicalIndexOrZero	CISCO-PROCESS-MIB
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal5mir	1.3.6.1.4.1.9.9.109.1.1.1.1.5	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.6	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Table Index: 1.3.6.1.4.1.9.9.109.1.1.1.1.

Display String OID: none

3. Enter the following items.

   In the following example, the alert is targeted when the CPU is greater than 80%.



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7

Detail

Cisco CPU — Period: 5m — CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU — Period: 5 min

Name	OID	Type	MIB
cpmCPUTotalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.1	SNMPv2-SMI:Unsigned32	CISCO-PROCESS-MIB
cpmCPUTotalPhysicalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.2	CISCO-TC:EntPhysicalIndexOrZero	CISCO-PROCESS-MIB
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Table Index: 1.3.6.1.4.1.9.9.109.1.1.1.1.

Display String OID: none

Time Window Trigger

Conditional: cpmCPUTotal1minRev > 80

Policy: Enter text or and

Severity: Alert

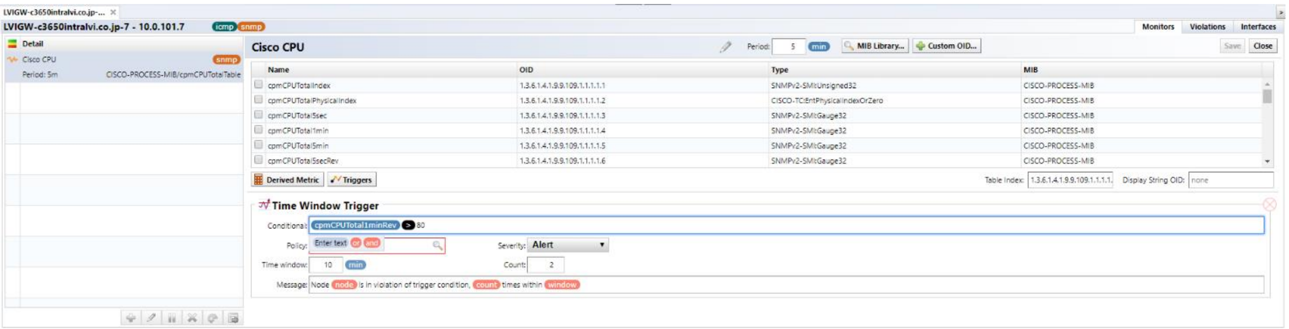
Time window: 10 min

Count: 2

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

Description	Explanation
Conditional	You can specify conditions using the following items: • is (equal) • is not (not equal) • < (greater than the right value) • < (smaller than the right value) • contains • not contains
Policy	Specify the alert policy.
Severity	Select a 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: 1 minute) A period that is used as a reference for counting how many times a failure (count) has occurred within a set period of time, the process defined in the policy is executed.
Count	Set how many times the process fails within the set period. (* Minimum value: 1)
Message	Set a message for executing the process.

4. Click [Save].



LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7

Cisco CPU — snmp — Period: 5m — CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU — Period: 5 min

	Name	OID	Type	MIB
□	cpmCPUTotalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.1	SNMPv2-SMI:Unsigned32	CISCO-PROCESS-MIB
□	cpmCPUTotalPhysicalIndex	1.3.6.1.4.1.9.9.109.1.1.1.1.2	CISCO-TC:EntPhysicalIndexOrZero	CISCO-PROCESS-MIB
□	cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB
□	cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6	SNMPv2-SMI:Gauge32	CISCO-PROCESS-MIB

Table Index: 1.3.6.1.4.1.9.9.109.1.1.1.1. Display String OID: none

Time Window Trigger

Conditional: cpmCPUTotal1minRev > 80

Policy: Enter text or and

Severity: Alert

Time window: 10 min

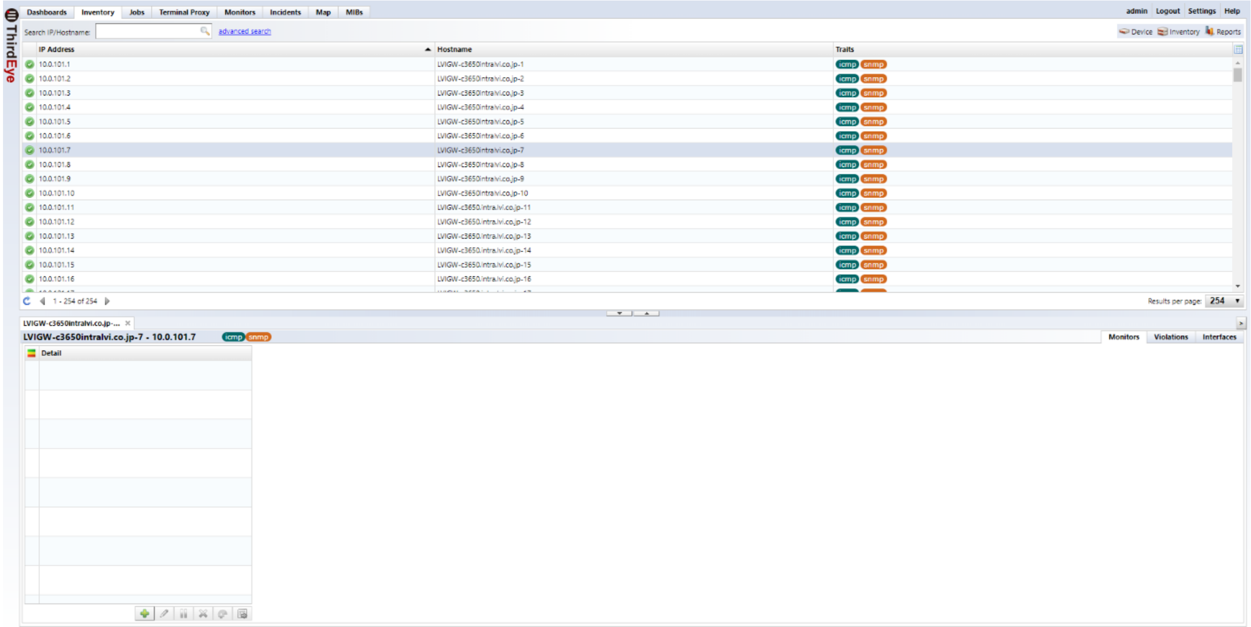
Count: 2

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

5.3.5 Monitoring SNMP traps

In ThirdEye, it is necessary to register the trap to be monitored as a monitor. If you do not register it as a monitor, you can receive traps and check them from the [Monitor] tab > [SNMP Trap], but you cannot perform actions such as incident registration or email transmission.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.

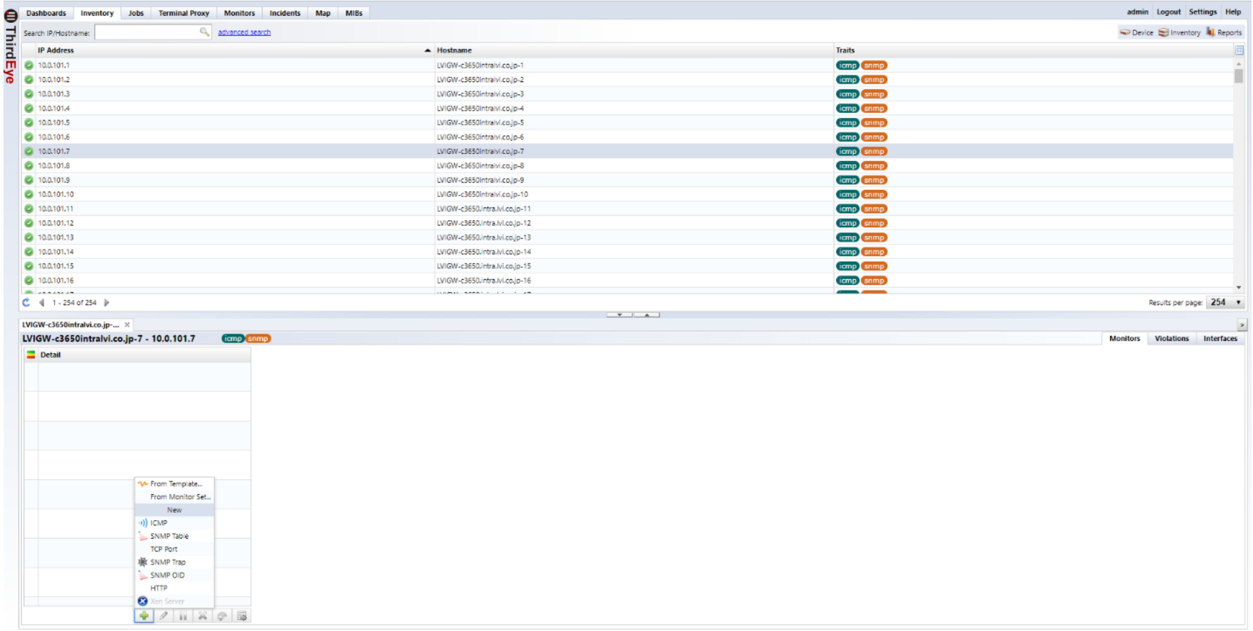


IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 254 Results per page: 254

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

2. Click [(Add)] in the lower left and click “SNMP Trap”.

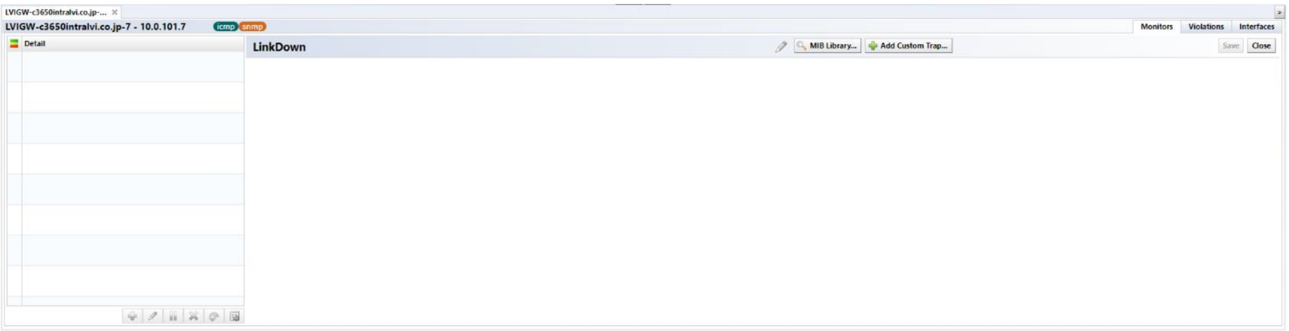


IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 254

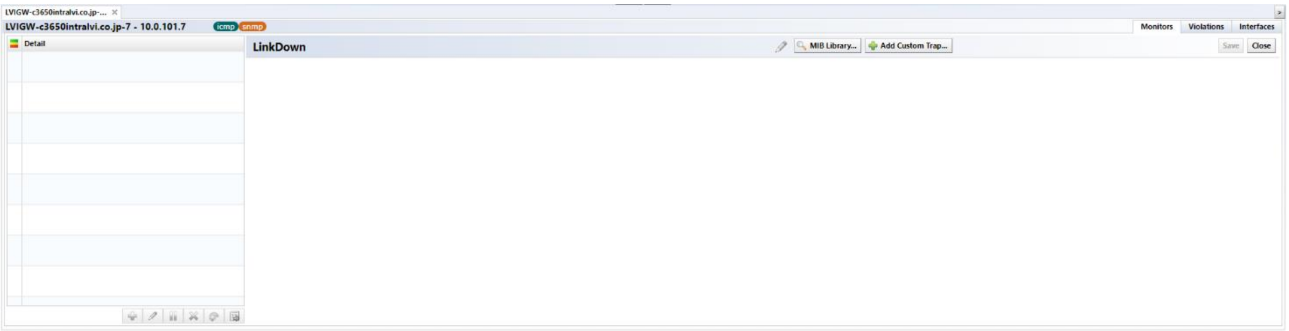
LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

3. Enter any monitor name.



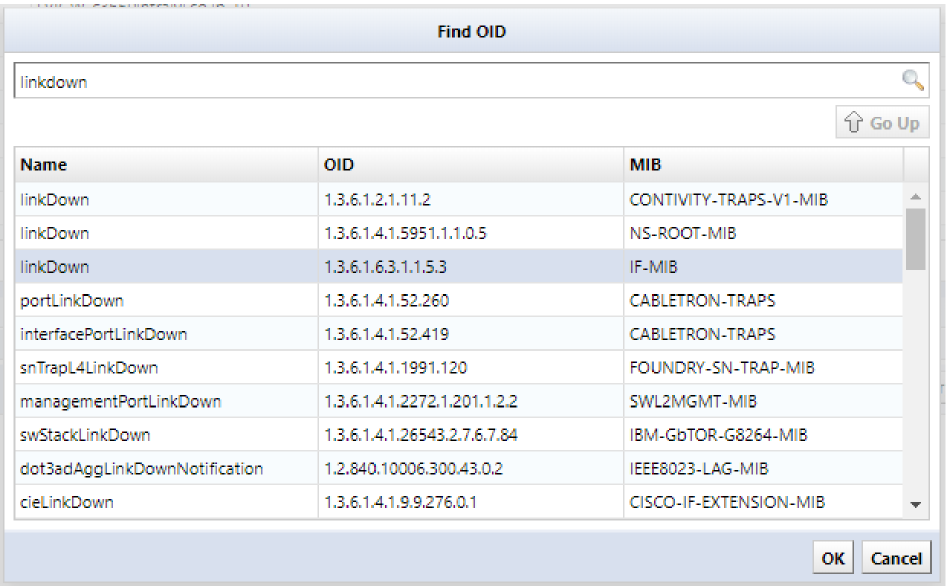
LinkDown

4. Click [MIB Library].



LinkDown

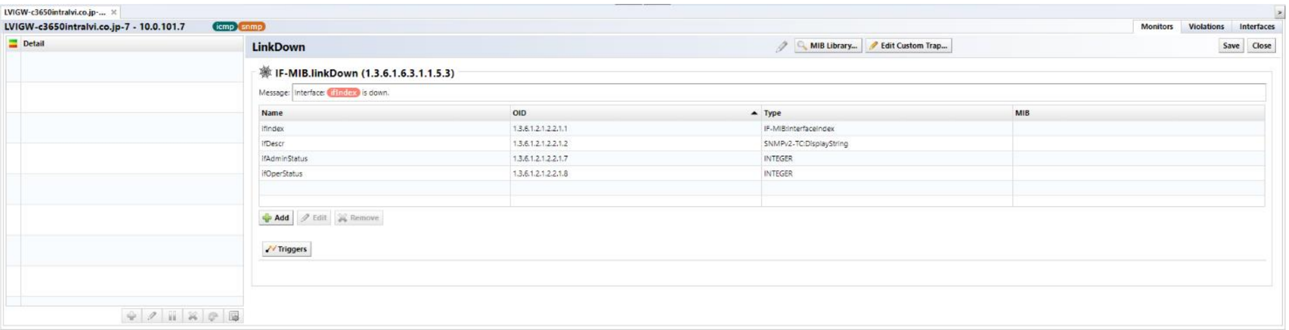
5. Enter the trap OID or name in the OID search, select the trap to be monitored, and click [OK].



linkdown

Name	OID	MIB
linkDown	1.3.6.1.2.1.11.2	CONTIVITY-TRAPS-V1-MIB
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	1.3.6.1.4.1.52.260	CABLETRON-TRAPS
interfacePortLinkDown	1.3.6.1.4.1.52.419	CABLETRON-TRAPS
snTrapL4LinkDown	1.3.6.1.4.1.1991.120	FOUNDRY-SN-TRAP-MIB
managementPortLinkDown	1.3.6.1.4.1.2272.1.201.1.2.2	SWL2MGMT-MIB
swStackLinkDown	1.3.6.1.4.1.26543.2.7.6.7.84	IBM-GbTOR-G8264-MIB
dot3adAggLinkDownNotification	1.2.840.10006.300.43.0.2	IEEE8023-LAG-MIB
cieLinkDown	1.3.6.1.4.1.9.9.276.0.1	CISCO-IF-EXTENSION-MIB

6. Enter a message when a failure occurs.

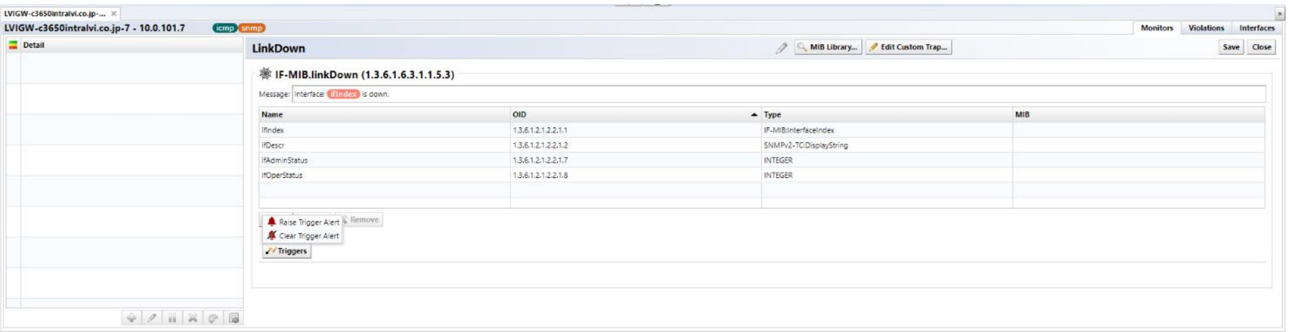


IF-MIB.linkDown (1.3.6.1.6.3.1.1.5.3)

Message: Interface: ifIndex is down.

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	

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

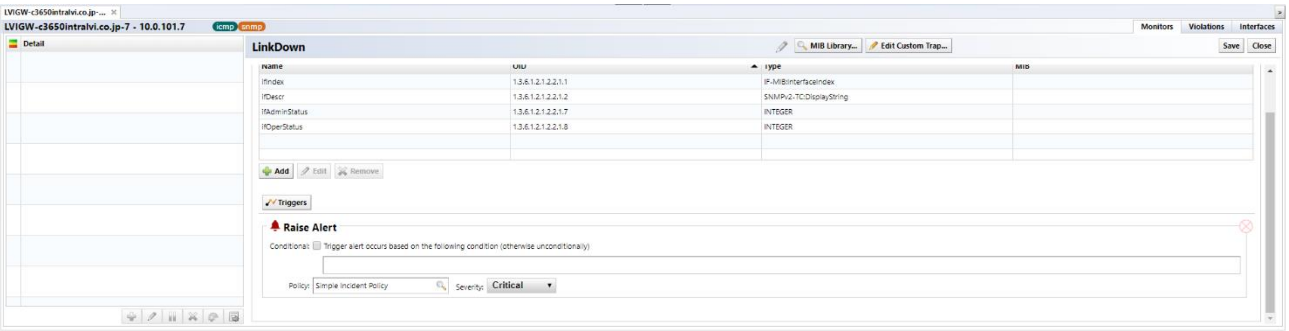


IF-MIB.linkDown (1.3.6.1.6.3.1.1.5.3)

Message: Interface: ifIndex is down.

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	

8. Enter the following items.



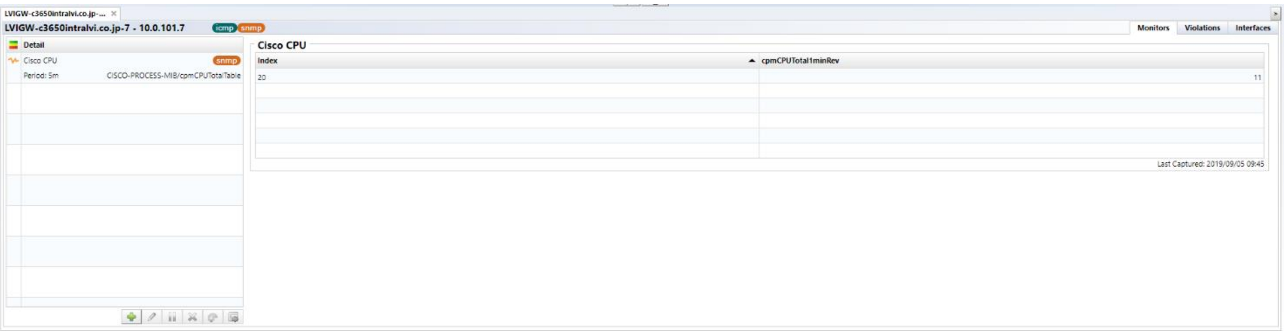
Name	OID	Type	MIB
ifIndex	1.3.6.1.2.1.2.2.1.1	IF-MIB:interfaceIndex	
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString	
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	

Conditional: □ Trigger alert occurs based on the following condition (otherwise unconditionally)

Policy: Simple Incident Policy Severity: Critical

Description	Explanation
Conditional	When [Specify the following conditions for the trigger] is checked, you can specify the conditions using the following items. • is (equal) • is not (not equal) • < (greater than the right value) • < (smaller than the right value) • contains • not contains
Policy	Specify the alert policy.
Severity	Select a severity from the following: (Initial value: warning) "Emergency", "Alert", "Critical", "Error", "Warning", "Notification", "Information", "Debug"
Message	Set a message for executing the process.

9. Click [Save].

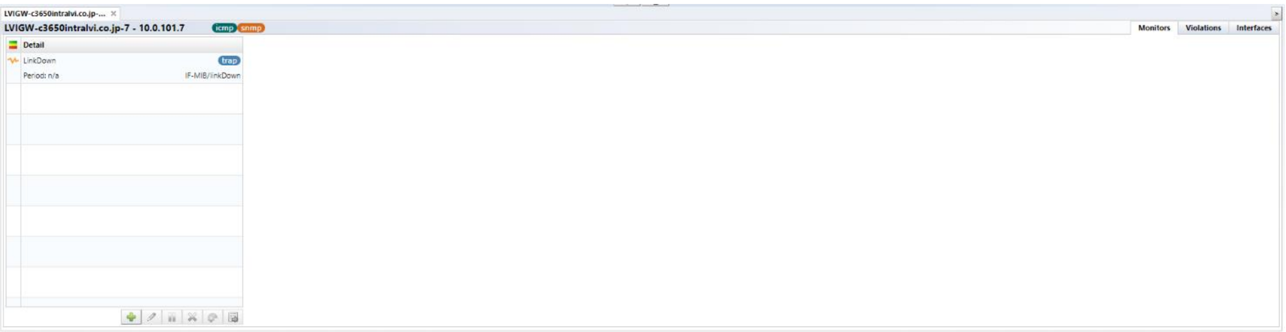

LVIGW-c3650intralvi.co.jp-...
LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7
icmp
snmp
Monitors
Violations
Interfaces
Detail
Cisco CPU
snmp
Cisco CPU

Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable

Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/05 09:45

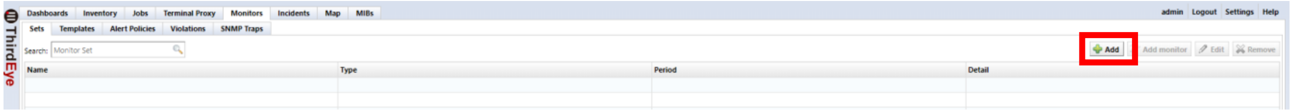
It is added to the monitor details table and monitoring is executed.



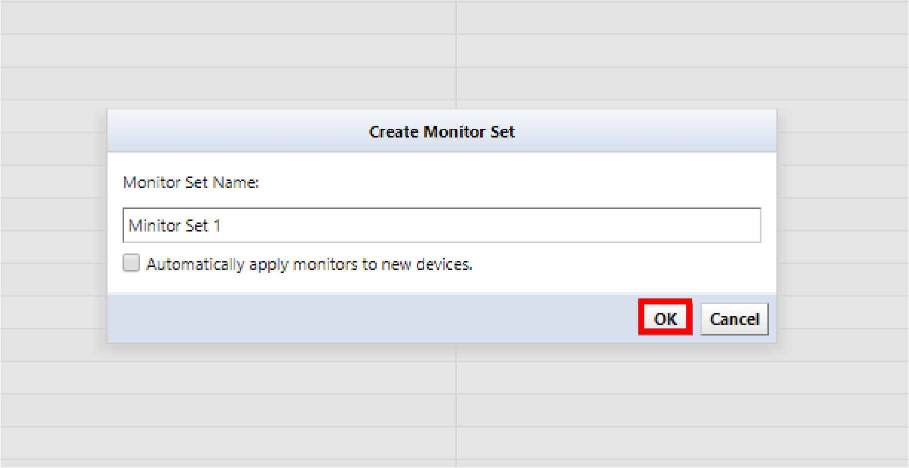
5.3.6 Configuring monitoring settings for many devices using a monitor set

With ThirdEye, monitoring items can be grouped as a monitor set, and monitors can be set for many monitored devices at once.

1. Select [Monitors] → [Sets] and click [Add].



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

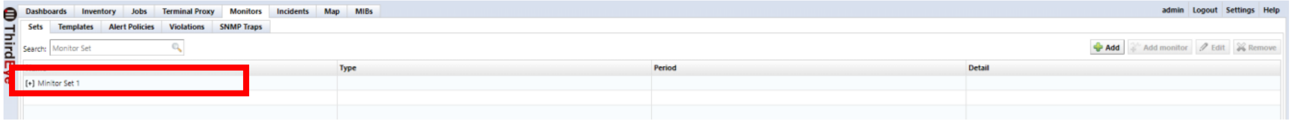

Create Monitor Set

Monitor Set Name:

Minitor Set 1

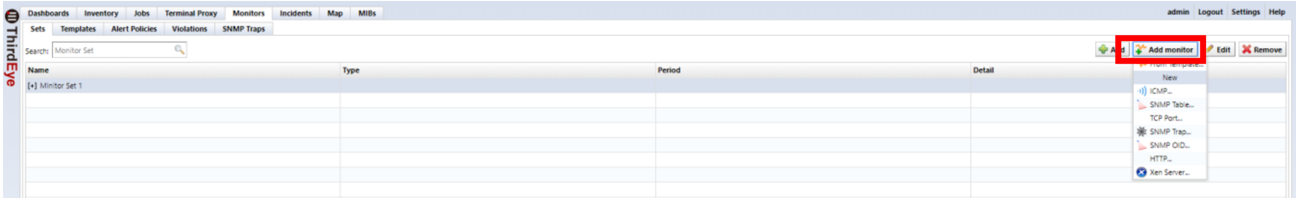
☐ Automatically apply monitors to new devices.

3. Select the created monitor set.



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

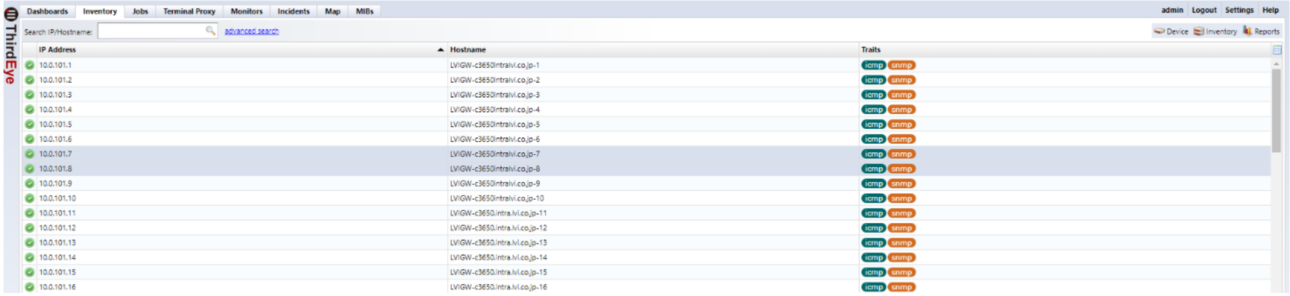
* Monitor creation methods can be added in the same way as individual monitor settings.



Name	Type	Period	Detail
[+] Minitor Set 1			

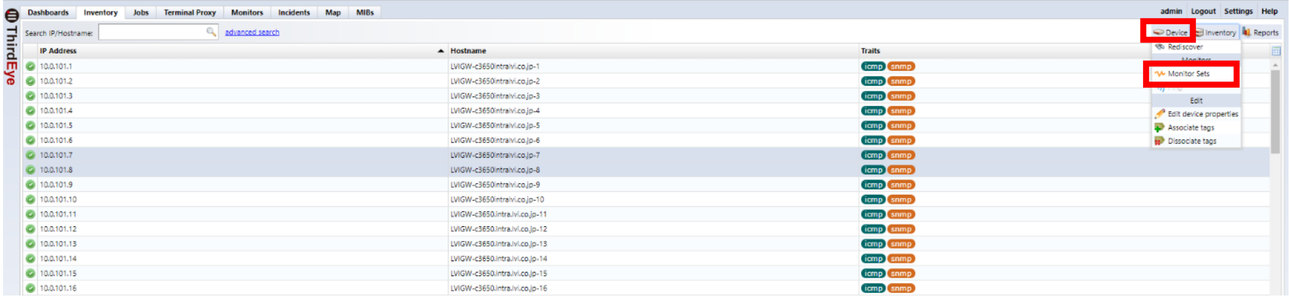
Description	Explanation
From Template	Add a monitor from the created monitor templates to [Template].
ICMP	Add a monitor by ICMP Ping.
SNMP Table	Specify the MIB table and the MIB object to be monitored.
SNMP Trap	Specify the TrapOID to be monitored and add a monitor.
SNMP OID	Specify the MIB object to be monitored.
HTTP	Monitors http or https.
Xen Server	Add a monitor to check the memory usage of Citrix Xen Server.

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



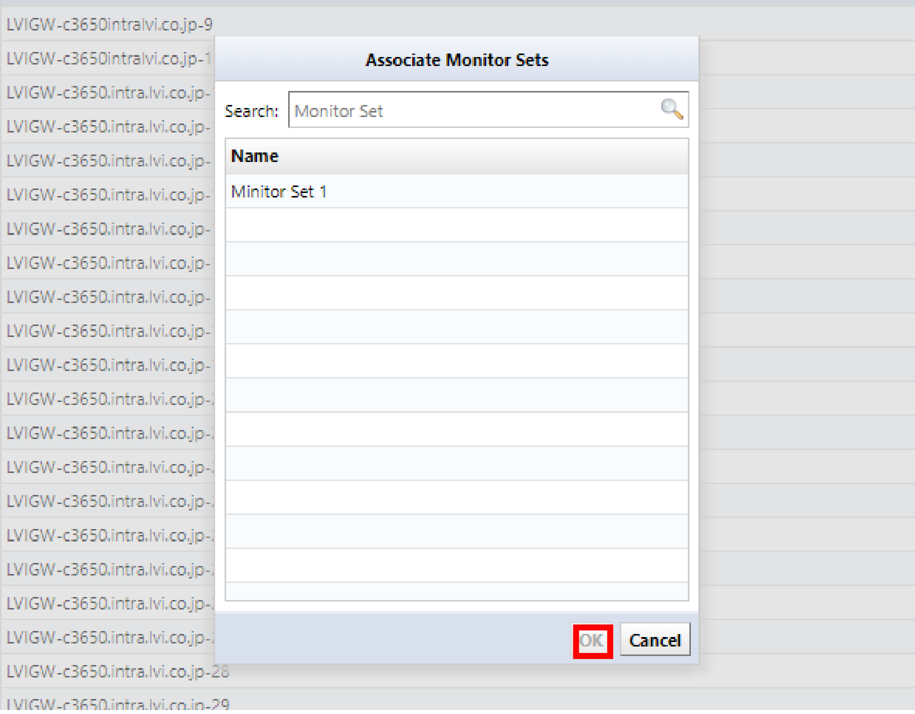
IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

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



IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

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


LVIGW-c3650intralvi.co.jp-9
LVIGW-c3650intralvi.co.jp-1
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-
LVIGW-c3650.intra.lvi.co.jp-28
LVIGW-c3650.intra.lvi.co.jp-29

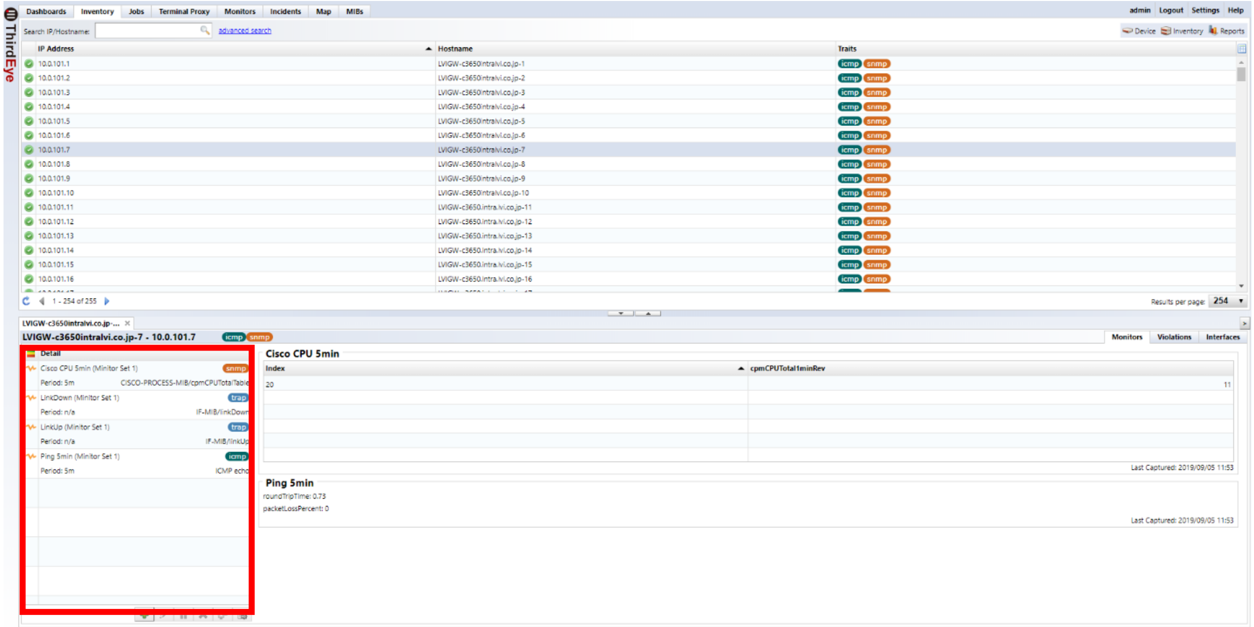
Associate Monitor Sets

Search: Monitor Set

Name
Minitor Set 1

This completes the application of the monitor sets.

The [Detail] column on the left of the device details display area displays a list of monitored monitors. Double-click the device to expand it, and check whether the settings are reflected in the [Detail] column.



Search IP/Hostname: advanced search

IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650intralvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650intralvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650intralvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650intralvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650intralvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650intralvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650intralvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650intralvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650intralvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650intralvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 255

Results per page: 254

LVIGW-c3650intralvi.co.jp-...

LVIGW-c3650intralvi.co.jp-7 - 10.0.101.7 icmp snmp

Detail

- Cisco CPU 5min (Minitor Set 1) snmp
  Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable
- LinkDown (Minitor Set 1) trap
  Period: n/a IF-MIB/linkDown
- LinkUp (Minitor Set 1) trap
  Period: n/a IF-MIB/linkUp
- Ping 5min (Minitor Set 1) icmp
  Period: 5m ICMP echo

Cisco CPU 5min

Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/05 11:53

Ping 5min

roundTripTime: 0.73
packetLossPercent: 0

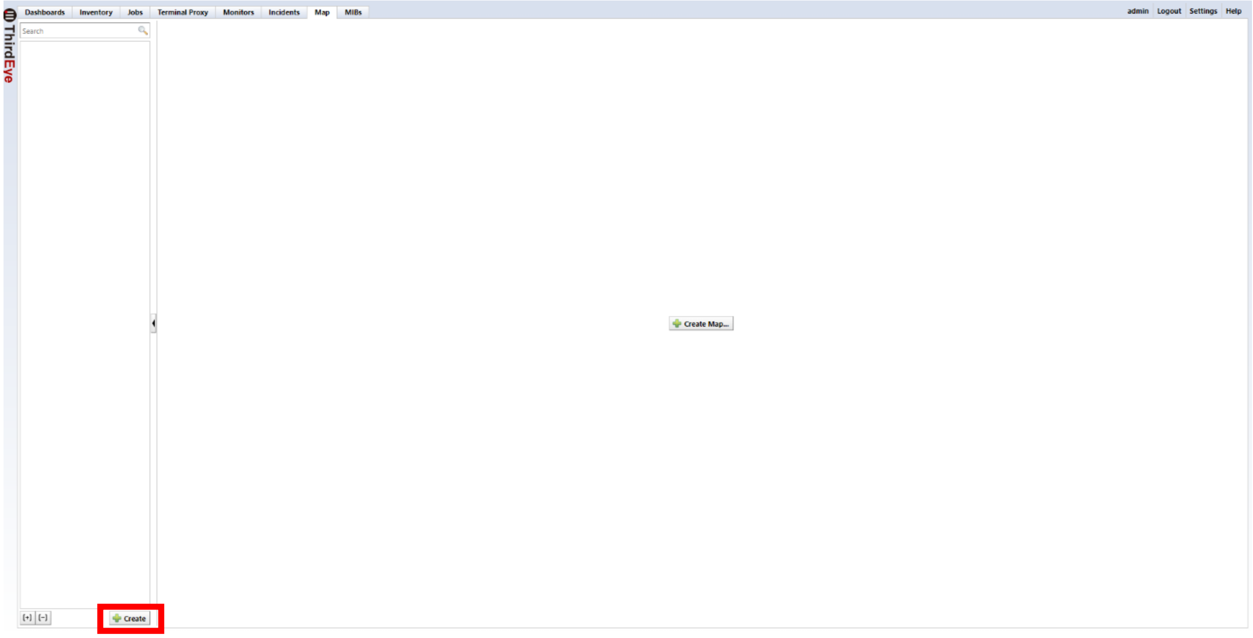
Last Captured: 2019/09/05 11:53

5.4 Creating a map

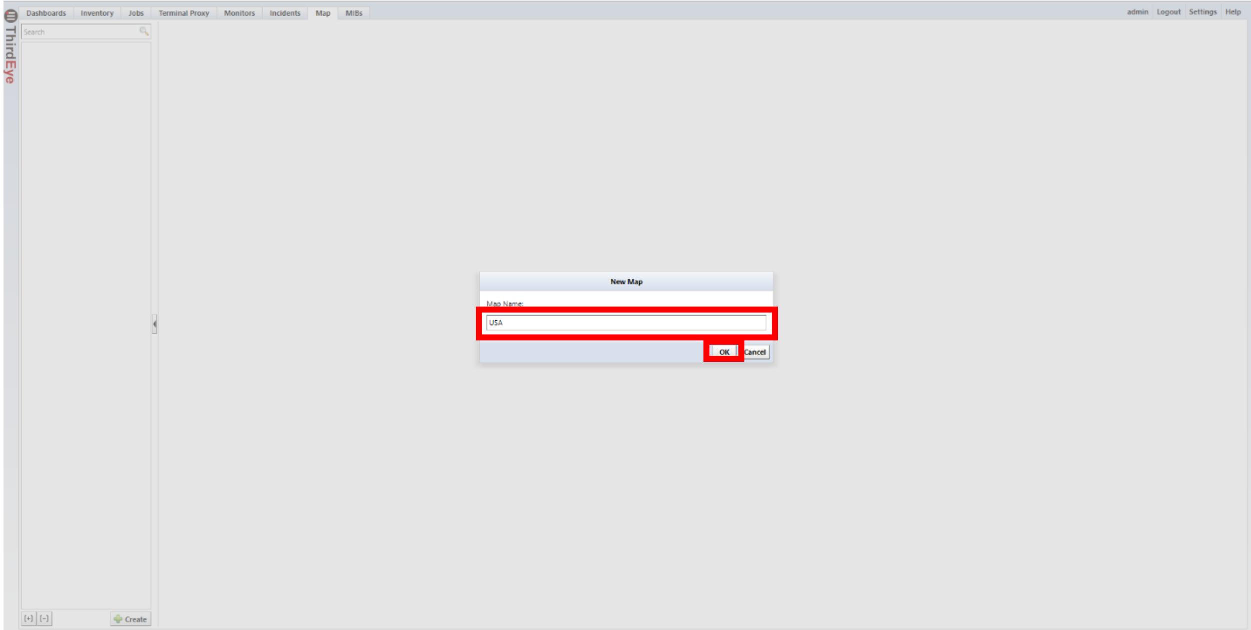
Create a map for visual monitoring. On the map screen, monitored devices are displayed as icons. When a failure occurs, the background color of the icon changes or an icon indicating the importance level is displayed. A hierarchical map can also be created by creating multiple maps.

5.4.1 Creating a map

1. Click [Create] at the bottom left of the screen.

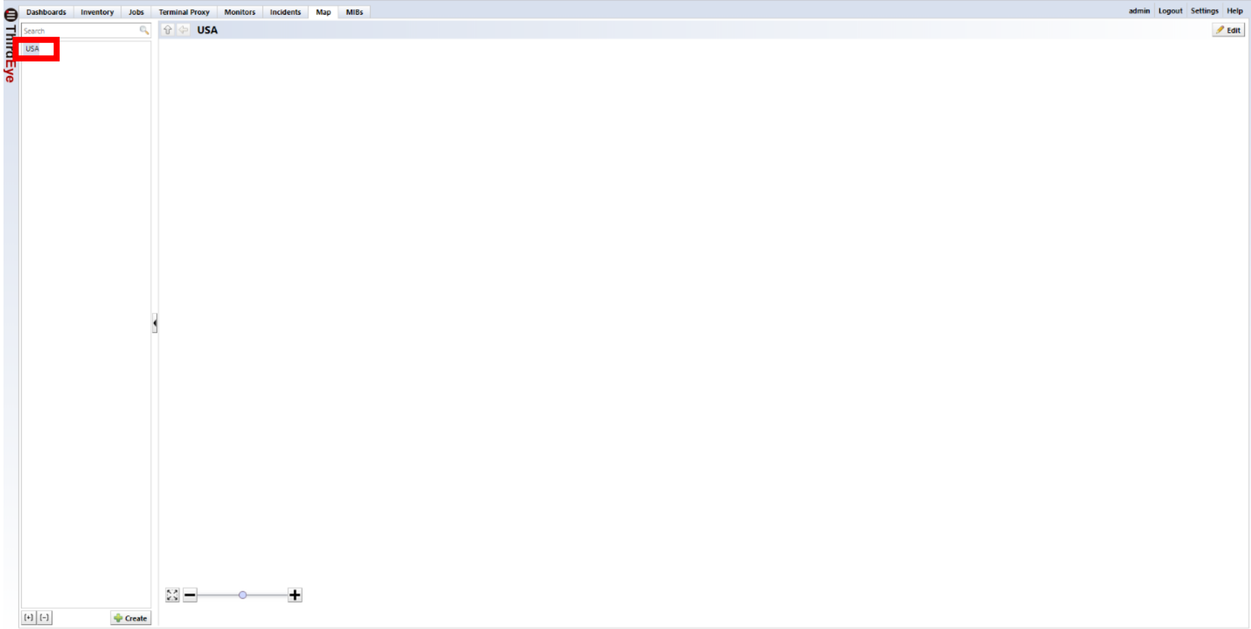


2. The New Map screen is displayed. Enter a map name and click [OK].



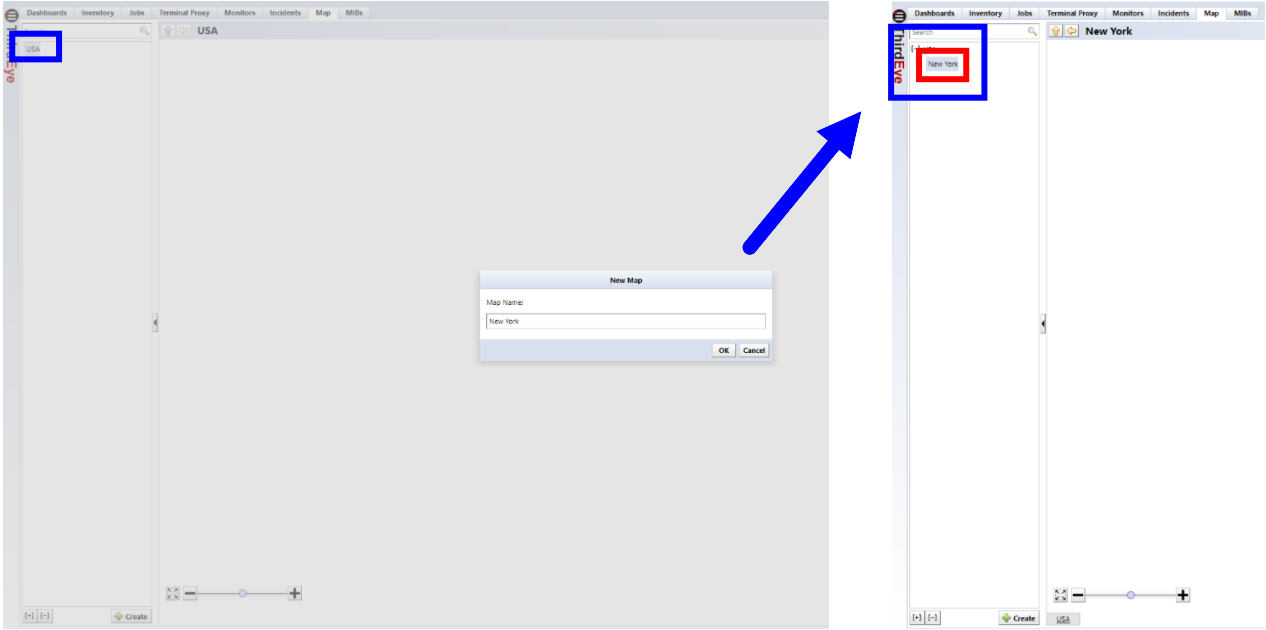
Map Name: USA

3. The saved map is displayed in the map list on the left side of the screen.



【Supplement】

If you create a new map with the map selected in the map list on the left side of the screen, you can create a new map below the selected map.



New Map

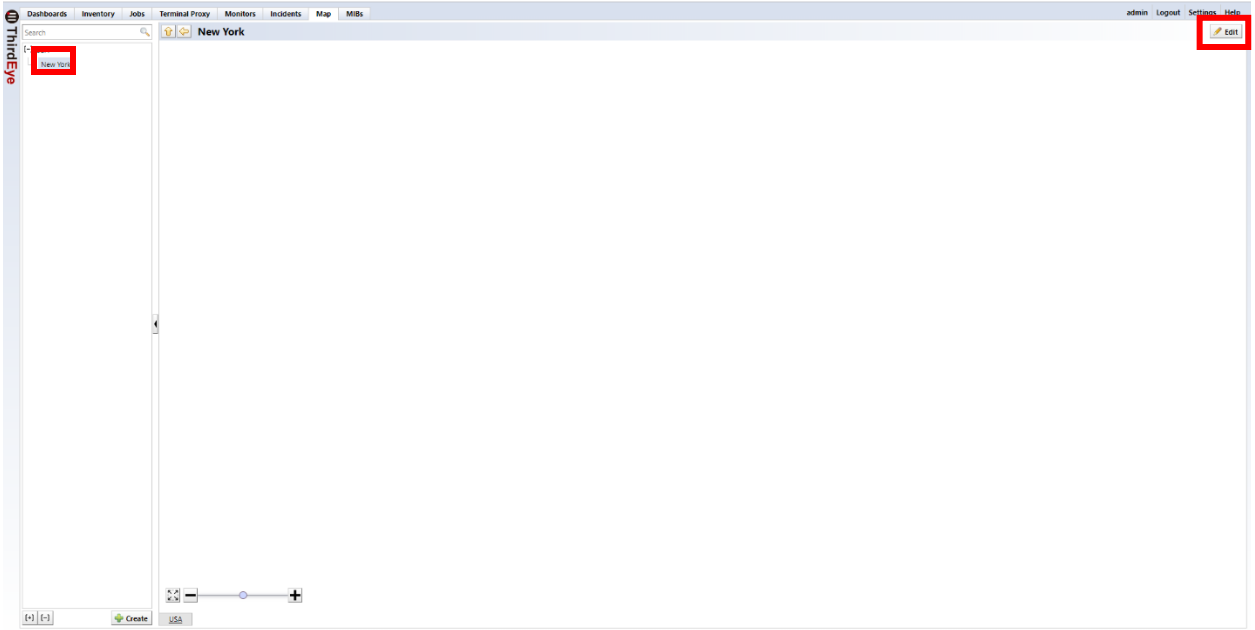
Map Name: New York

OK Cancel

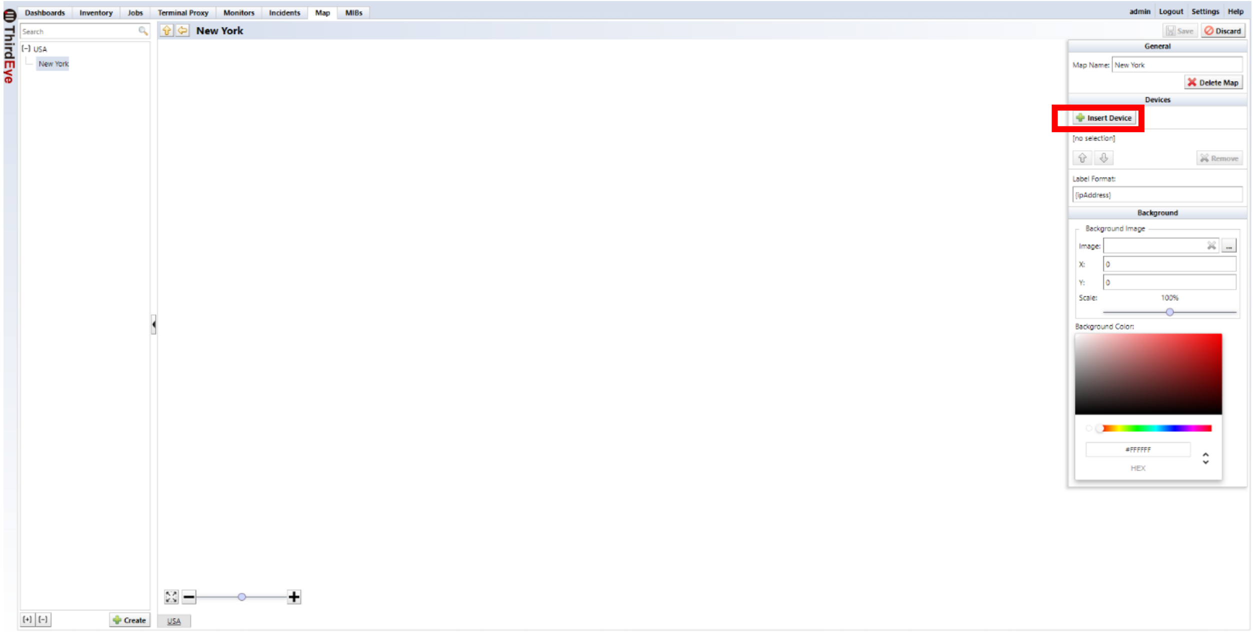
5.4.2 Inserting a device into the map

If you want to display the device as an icon on the map, insert the device into the map.

1. Double-click the map to which you want to add a device from the map list on the left side of the screen and click [Edit].



2. Click [Insert Device].



New York

Map Name: New York

[no selection]

Label Format: {ipAddress}

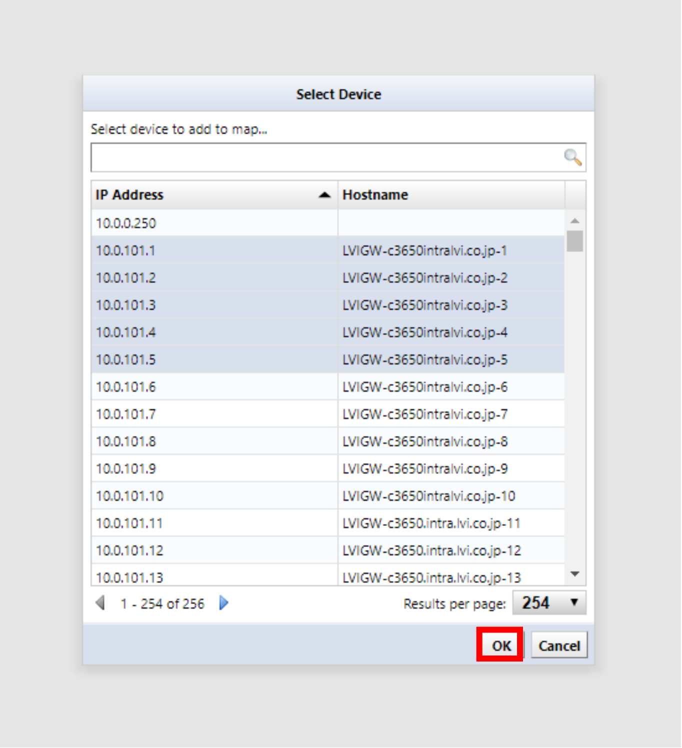
X: 0

Y: 0

Scale: 100%

#FFFFFF

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



Select Device

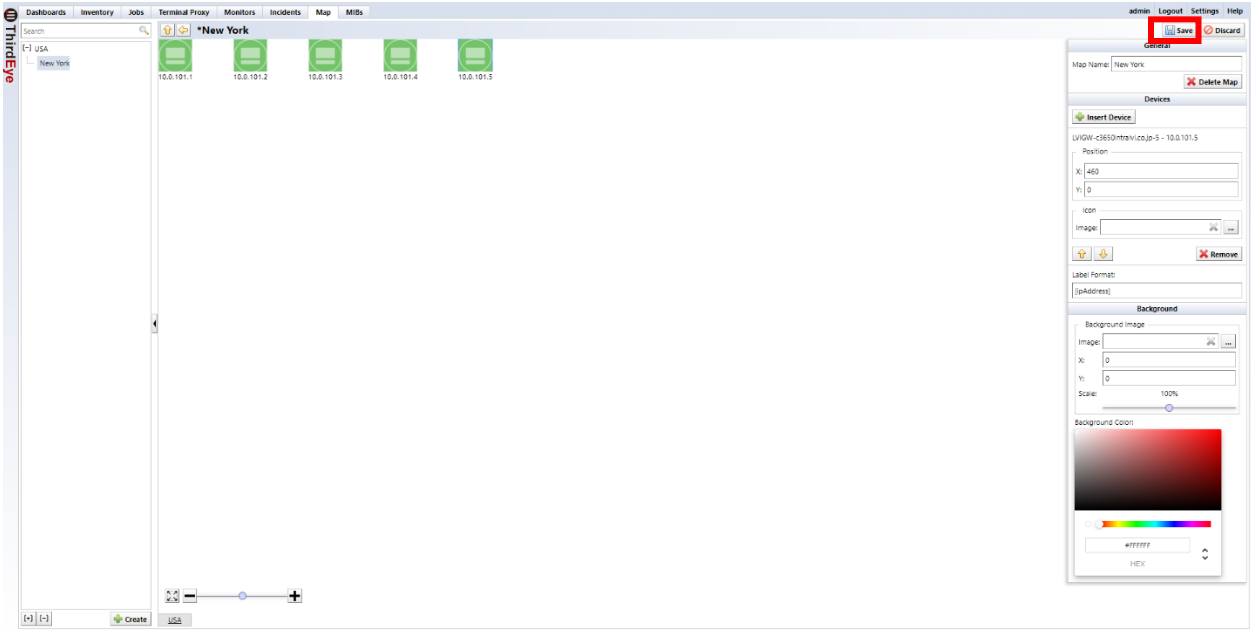
Select device to add to map...

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650intralvi.co.jp-1
10.0.101.2	LVIGW-c3650intralvi.co.jp-2
10.0.101.3	LVIGW-c3650intralvi.co.jp-3
10.0.101.4	LVIGW-c3650intralvi.co.jp-4
10.0.101.5	LVIGW-c3650intralvi.co.jp-5
10.0.101.6	LVIGW-c3650intralvi.co.jp-6
10.0.101.7	LVIGW-c3650intralvi.co.jp-7
10.0.101.8	LVIGW-c3650intralvi.co.jp-8
10.0.101.9	LVIGW-c3650intralvi.co.jp-9
10.0.101.10	LVIGW-c3650intralvi.co.jp-10
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13

1 - 254 of 256

Results per page: 254

4. The device icon is inserted. Click [Save] to complete editing.



Map Name: New York

LVIGW-c3650intralvi.co.jp-5 - 10.0.101.5

Position

X: 460

Y: 0

Icon

Image:

Label Format: {ipAddress}

Background Image

Image:

X: 0

Y: 0

Scale: 100%

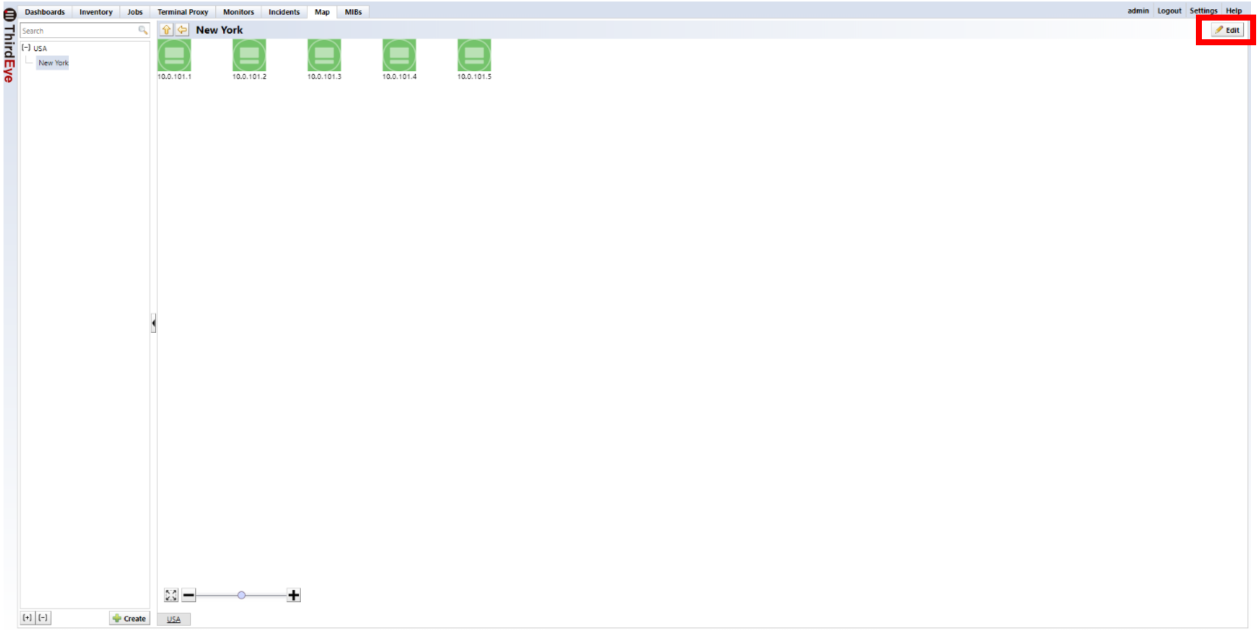
Background Color: #FFFFFF

5.4.3 Connect two icons with a line

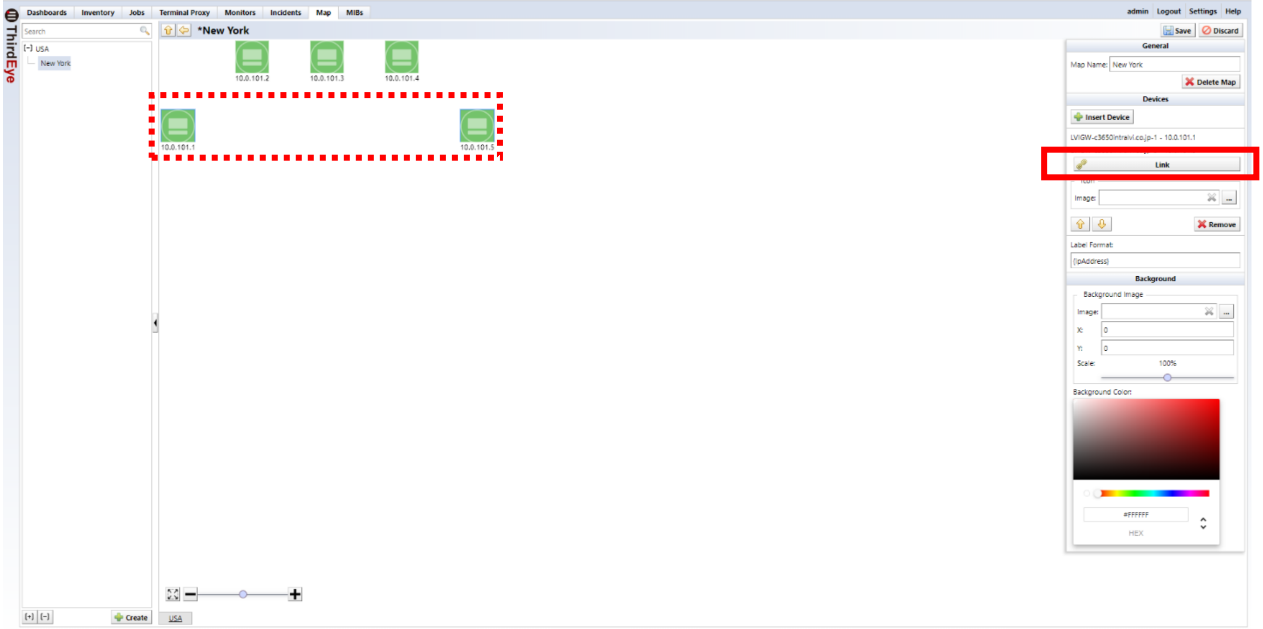
You can connect map and device icons with link lines.

* Line thickness cannot be changed. Also, the line color does not change.

1. Open the map by double-clicking it and click [Edit].



2. While holding down the “Ctrl” key on the keyboard, click to select the two devices connected by the link line. With the device selected, click [Link].



Map Name: New York

LVIGW-c3650intralvi.co.jp-1 - 10.0.101.1

Image:

Label Format: {ipAddress}

Image:

X: 0

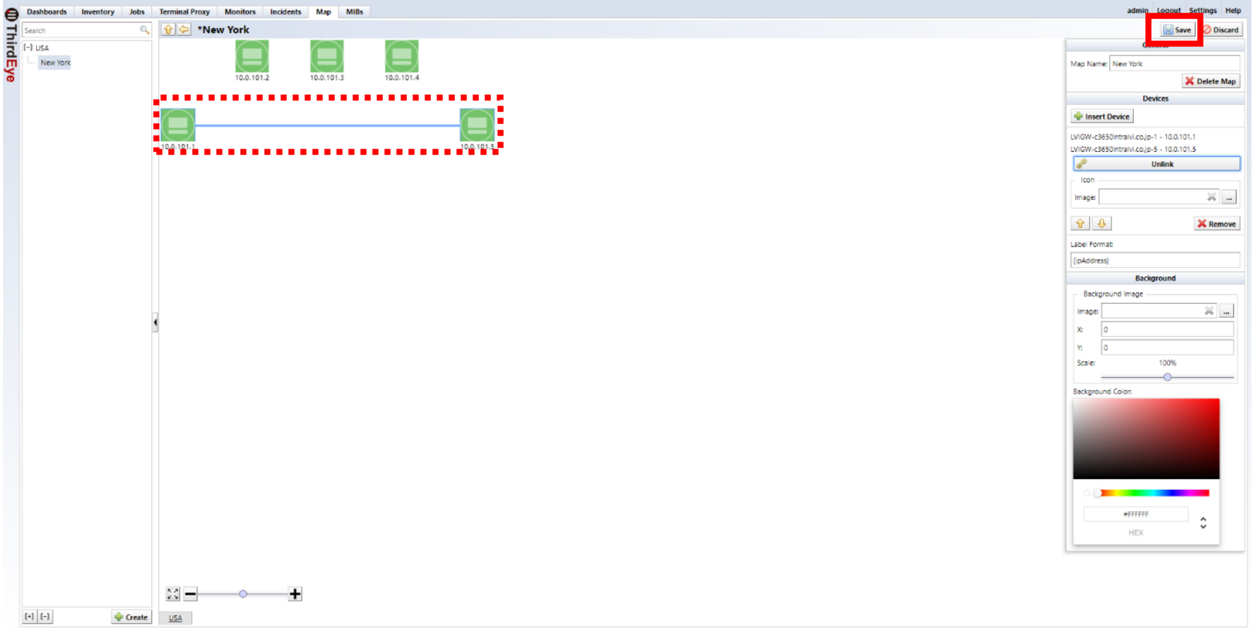
Y: 0

Scale: 100%

#FFFFFF

3. A link line is inserted. Click [Save] to complete editing.

* To delete a link line, click [Remove] with two devices selected.



Map Name: New York

LVIGW-c3650intralvi.co.jp-1 - 10.0.101.1

LVIGW-c3650intralvi.co.jp-5 - 10.0.101.5

Image:

Label Format: {ipAddress}

Image:

X: 0

Y: 0

Scale: 100%

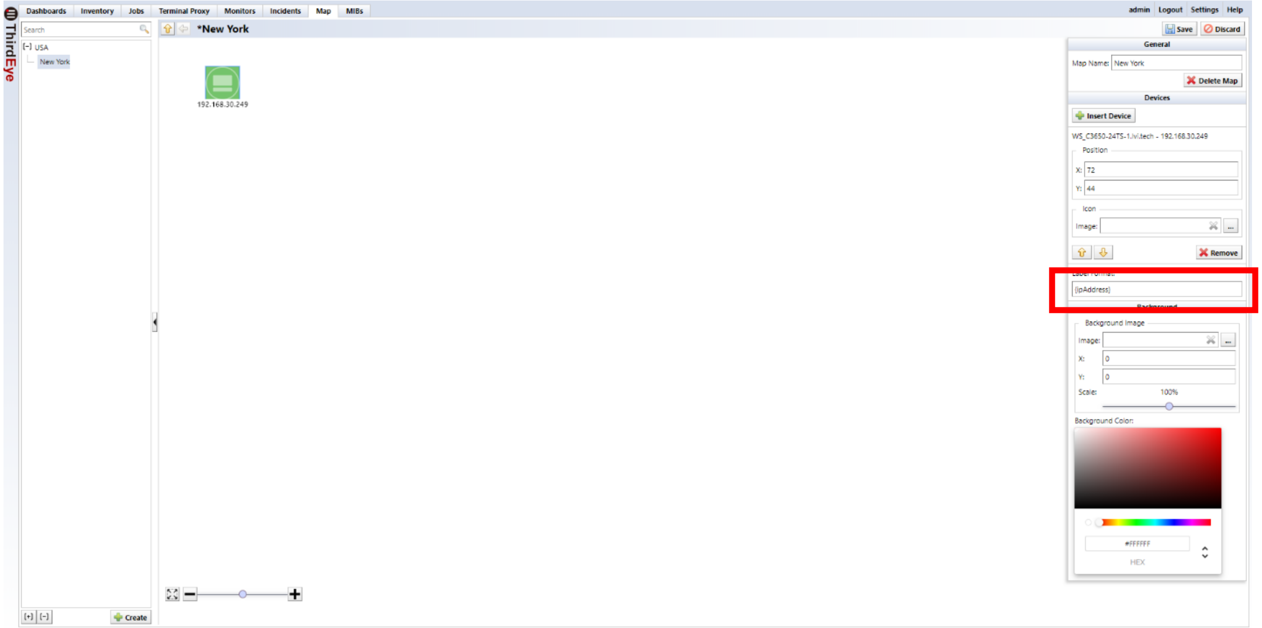
#FFFFFF

5.4.4 Setting the map label format

A label is a character string displayed on a device icon on the map. Labels can be set in map units by setting the label format.

1. Open the map by double-clicking it and click [Edit].

2. Change the [Label Format] setting.
   Here, the label display is changed from IP address to host name.



Map Name: New York

WS_C3650-24TS-1.lvi.tech - 192.168.30.249

Position
X: 72
Y: 44

Icon
Image:

Label Format:
{ipAddress}

Background

Background Image
Image:
X: 0
Y: 0
Scale: 100%

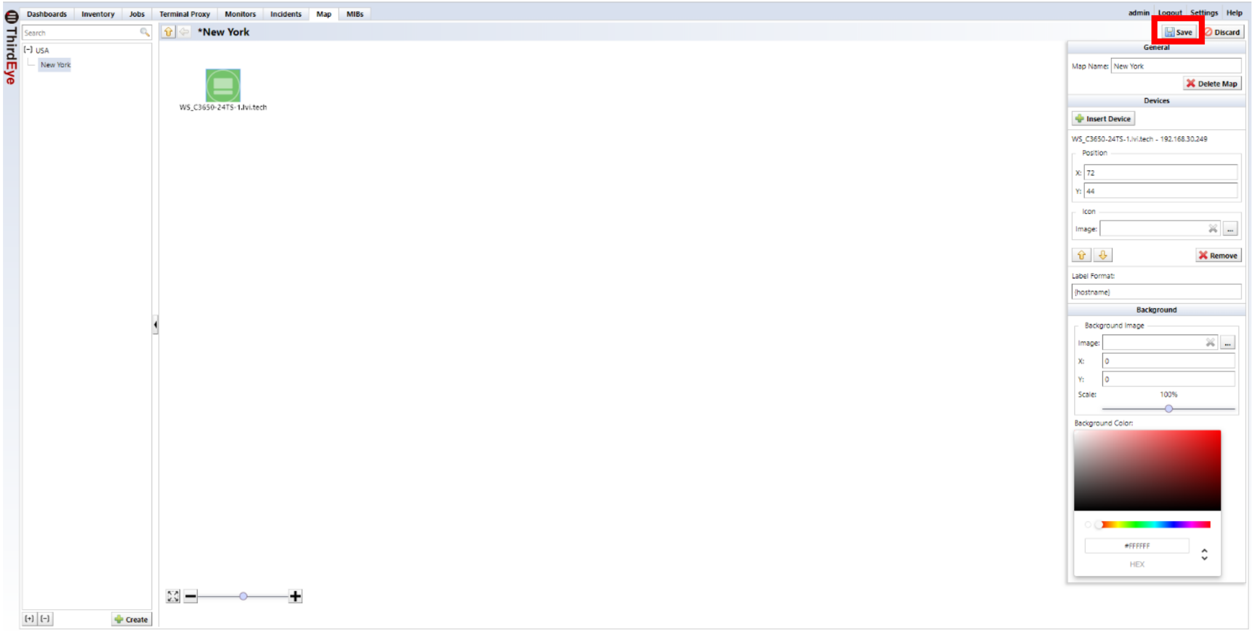
Background Color:
#FFFFFF
HEX

The following arguments can be used for the label format. You can also specify any string.

【Label format】

Description	Explanation
{ipAddress}	Displays the device IP address. (initial value)
{hostname}	Displays the device host name.
{custom1}	Display custom 1 information for the device.
{custom2}	Display custom 2 information for the device.
{custom3}	Display custom 3 information for the device.
{custom4}	Display custom 4 information for the device.
{custom5}	Display custom 5 information for the device.

3. Click [Save] to complete the edit.



Map Name: New York

WS_C3650-24TS-1.lvi.tech - 192.168.30.249

X: 72

Y: 44

Label Format: {hostname}

X: 0

Y: 0

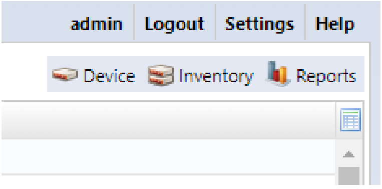
Scale: 100%

#FFFFFF

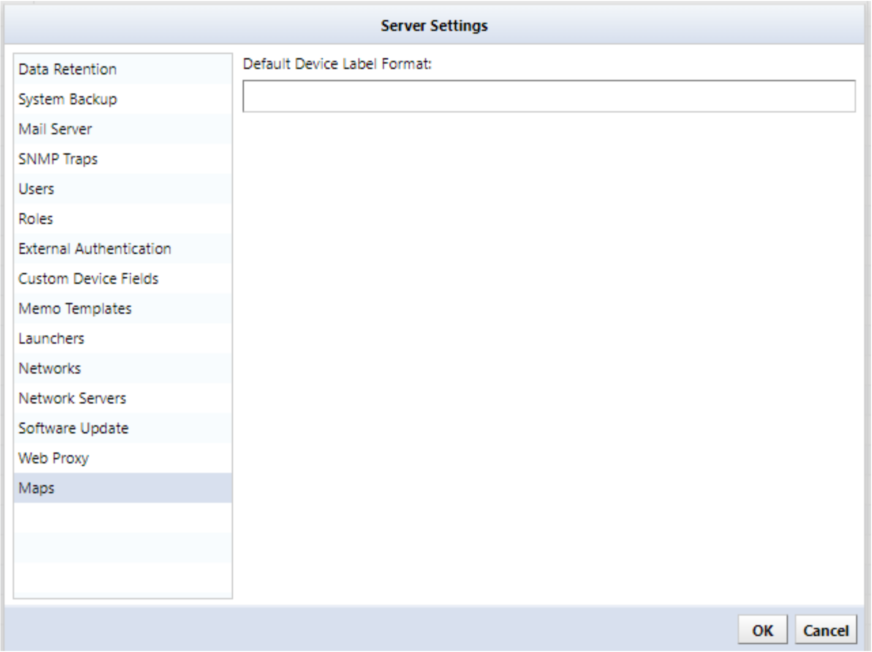
5.4.5 Setting the default label format for maps

You can specify the label format (default) when creating a new map.

1. Click [Settings] in the global menu.



2. Click [Maps] and set the label-specific format to “Default Device Label Format”.

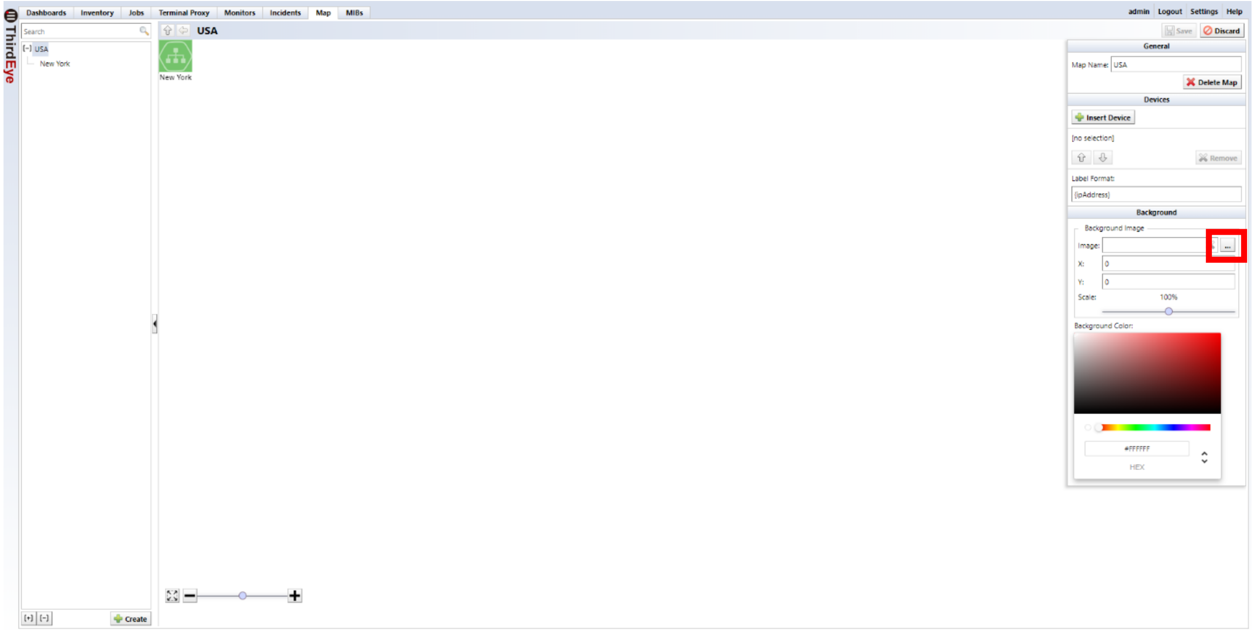


The initial value is not filled in. If not filled in, the map label format will be "{ipAddress}".

5.4.6 Setting the map background image

You can set the background image from the [Edit] menu of the map.

1. Open the map by double-clicking it and click [Edit].
2. From the setting menu on the right side of the screen, click [...] to the right of the [Background image] field in the background section.



Map Name: USA

Label Format: {ipAddress}

Image:

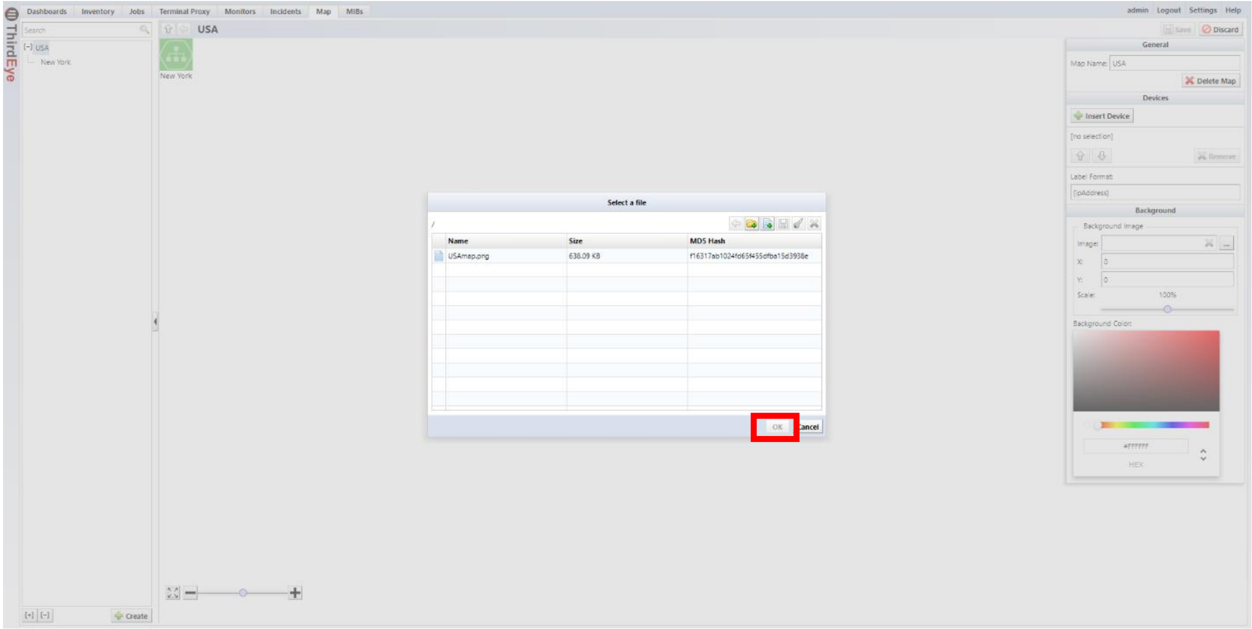
X: 0

Y: 0

Scale: 100%

#FFFFFF

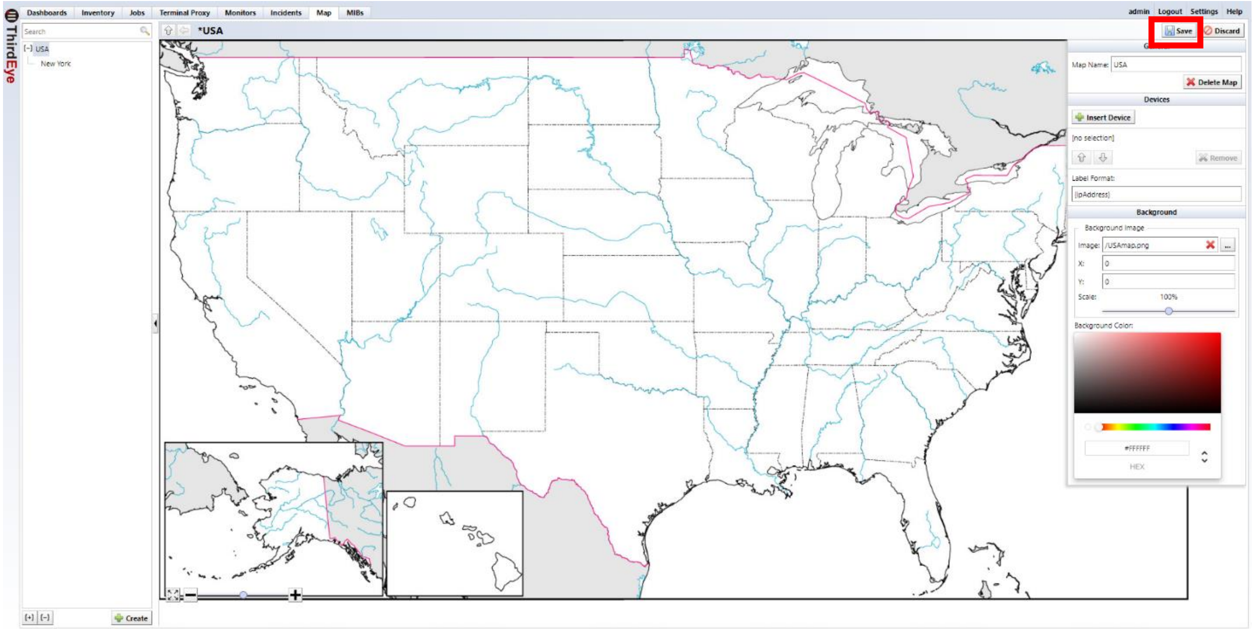
3. The file selection screen is displayed. Select the file you want to set as the background image and click [OK].



Name	Size	MD5 Hash
USAmap.png	638.09 KB	f16317ab1024fd65f455dfba15d3938e

* Client files can be uploaded to the ThirdEye server. Click [📄] to display the client side file selection dialog. Select the file to upload and click [Open].

4. Click [Save] to complete the edit.



Map Name: USA

[no selection]

Label Format: {ipAddress}

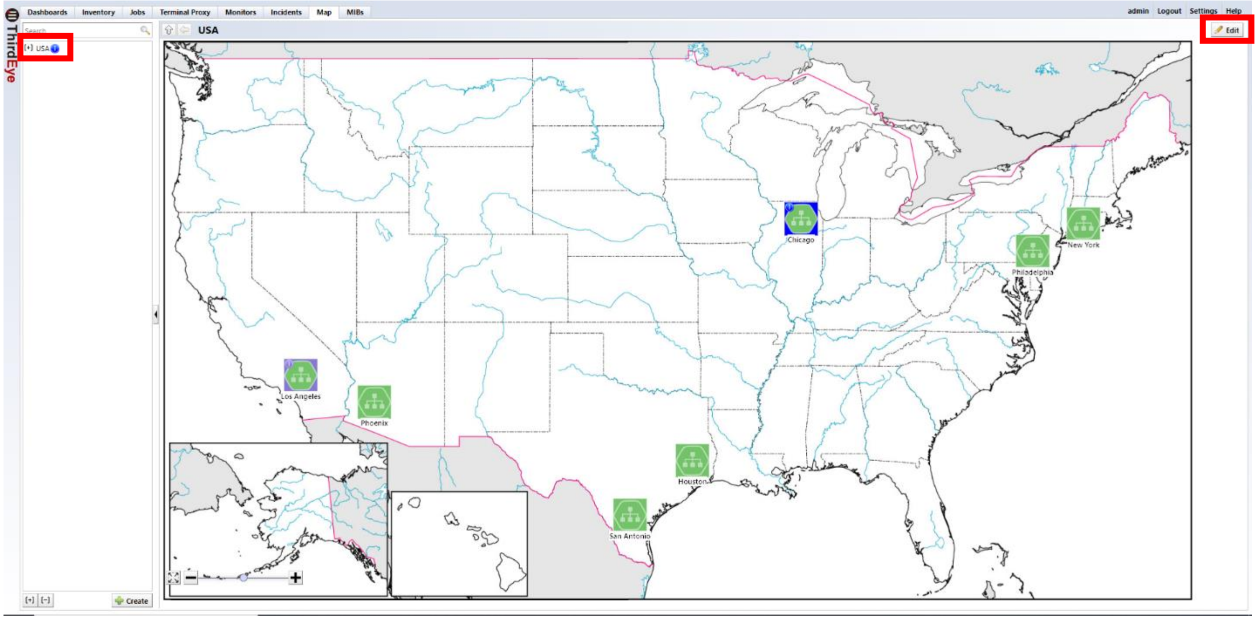
Background Image
Image: /USAmap.png
X: 0
Y: 0
Scale: 100%

Background Color: #FFFFFF HEX

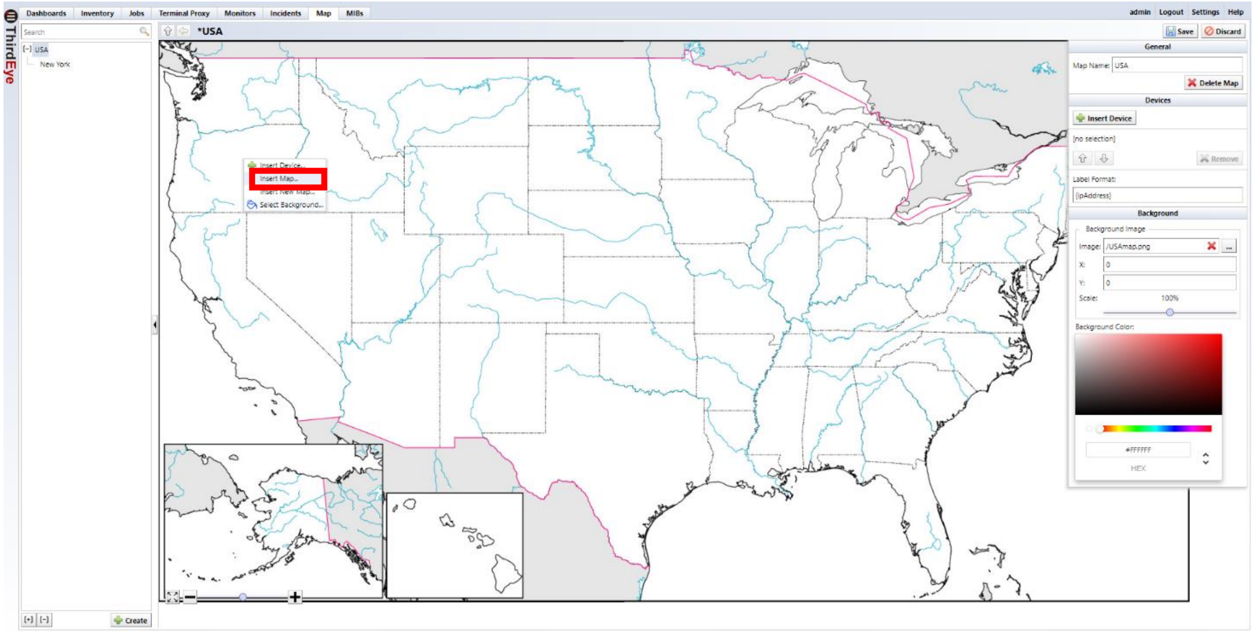
5.4.7 Setting the map hierarchy

If you want to display the map in a hierarchical structure, you can configure it by inserting the lower hierarchy map into the upper hierarchy map of the hierarchy structure.

1. From the map list on the left side of the screen, double-click the map that will be the upper layer, and click [Edit].



2. Right-click on the map screen. Select [Insert Map] from the right-click menu.



Map Name: USA

[no selection]

Label Format: {ipAddress}

Image: /USAmap.png

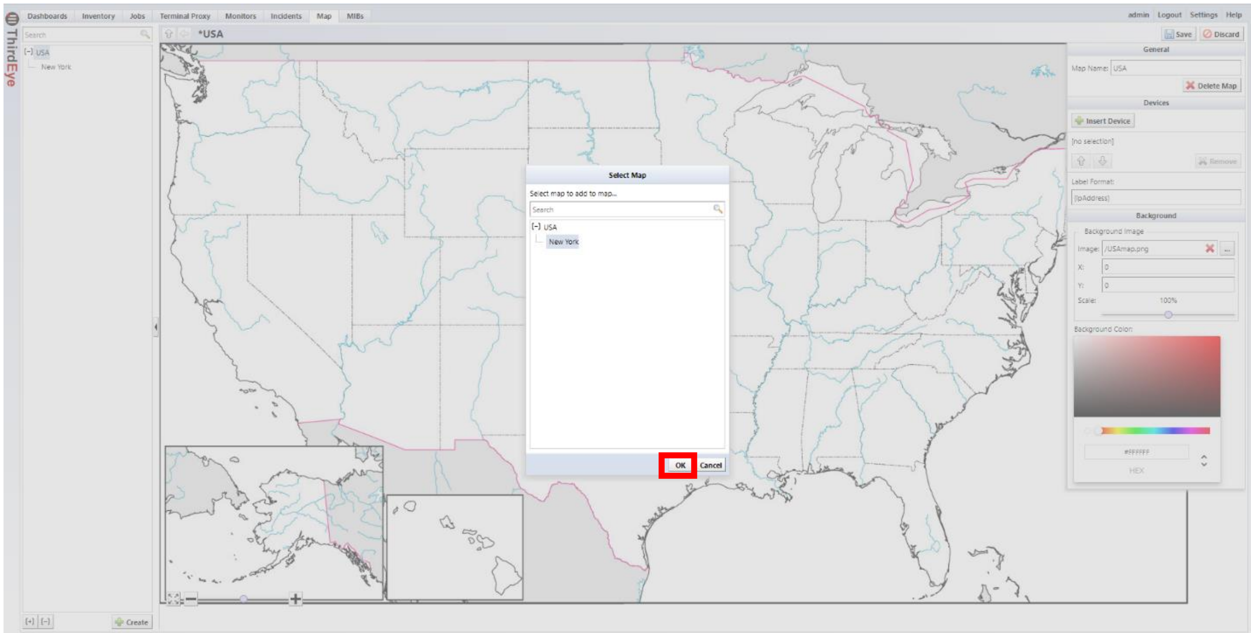
X: 0

Y: 0

Scale: 100%

Background Color: #FFFFFF

3. The file selection screen is displayed. Select the file you want to set as the background image and click [OK].



Map Name: USA

[no selection]

Label Format: {IpAddress}

Image: /USAmap.png

X: 0

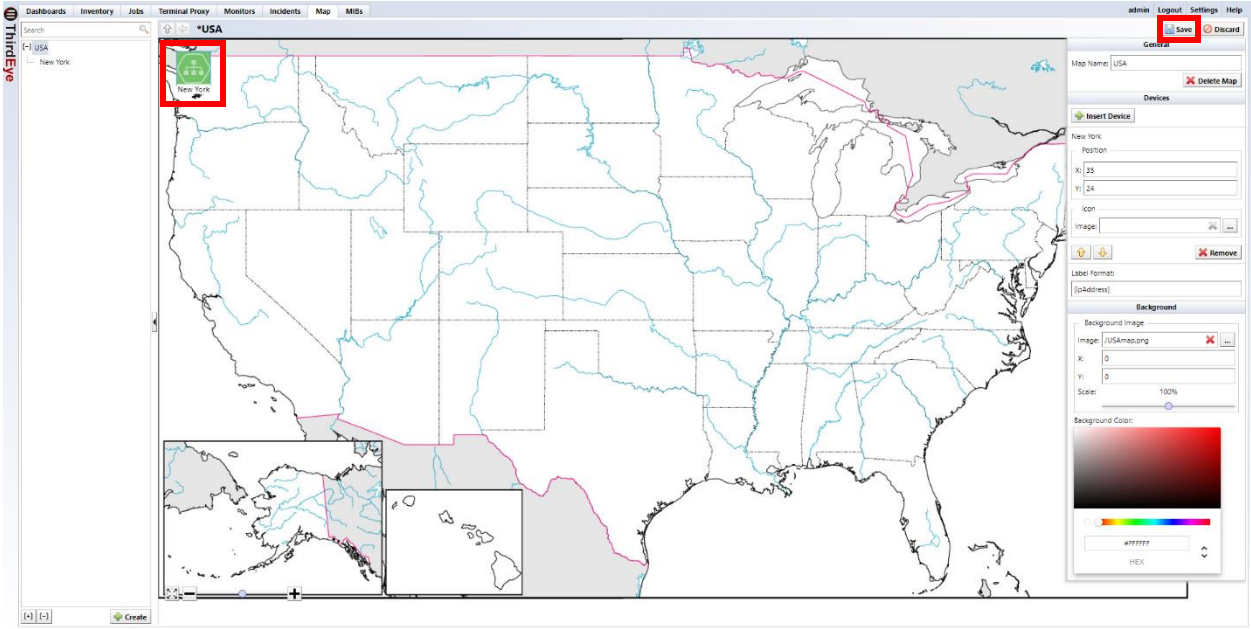
Y: 0

Scale: 100%

#FFFFFF

Select map to add to map...

4. Click [Save] to complete the edit.



Map Name: USA

New York

Position

X: 35

Y: 24

Icon

Image:

Label Format:

{ipAddress}

Image: /USAmap.png

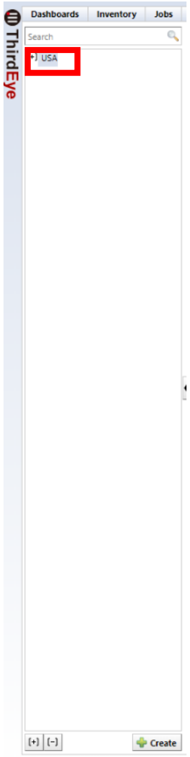
X: 0

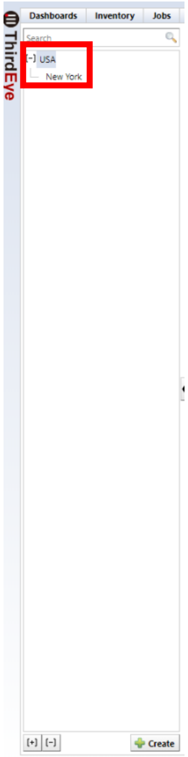
Y: 0

Scale: 100%

#FFFFFF

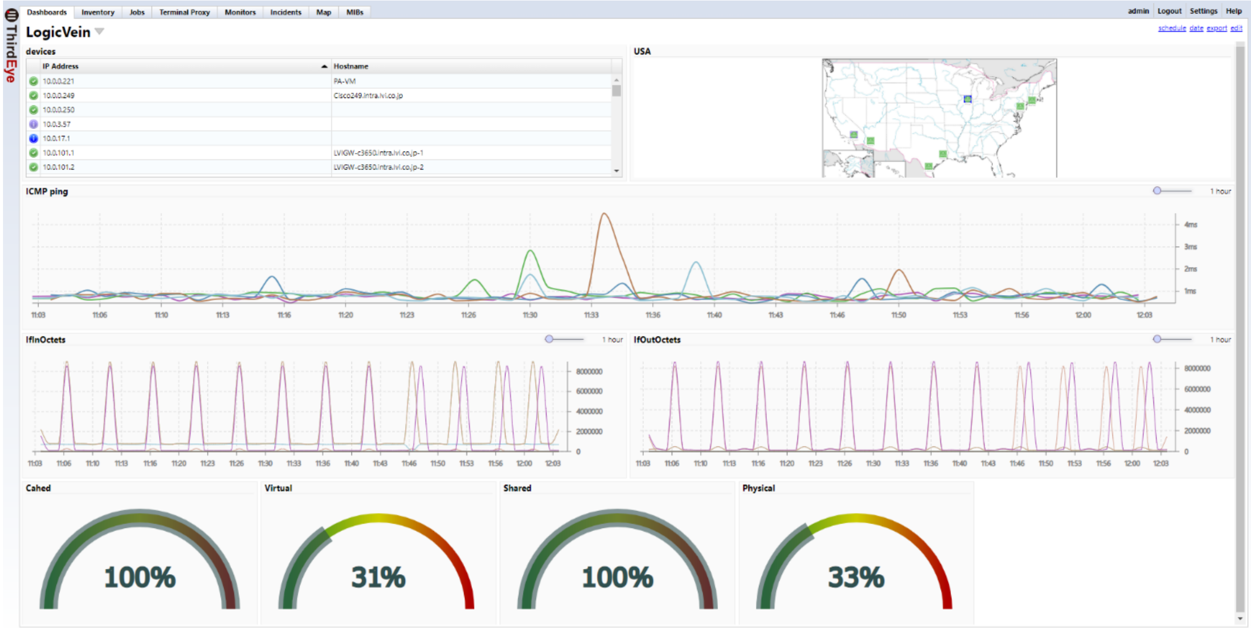
When the hierarchical structure is created, the map list on the left side of the screen changes to a tree view. By clicking the symbol [+] / [-] to the left of the map name, you can expand or collapse the map.





5.5 Create a dashboard

The dashboard is an interface that allows you to configure a single monitoring screen by embedding various items on the screen. Each embedded item is called a "widget". Users can create new dashboards and add / reorder widgets.

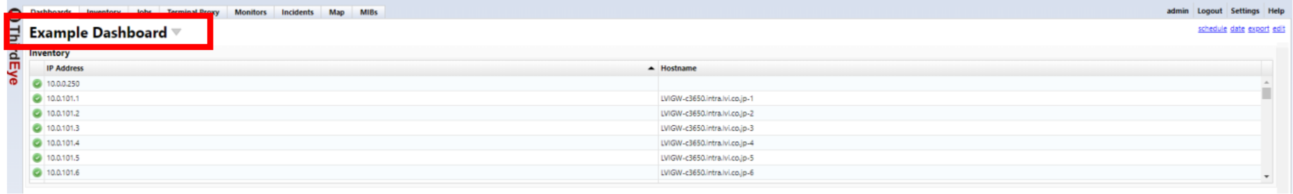


devices

	IP Address	Hostname
✓	10.0.0.221	PA-VM
✓	10.0.0.249	Cisco249.intra.lvi.co.jp
✓	10.0.0.250	
i	10.0.3.57	
i	10.0.17.1	
✓	10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
✓	10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2

5.5.1 Adding a dashboard

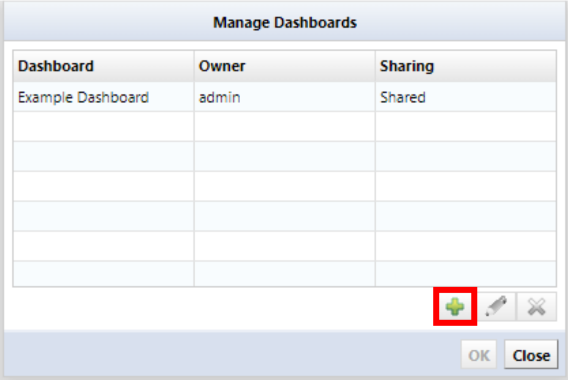
1. Click the "Dashboard Name" (in the figure below, "Example Dashboard") under the Dashboard tab and select [Manage Dashboards].



Inventory

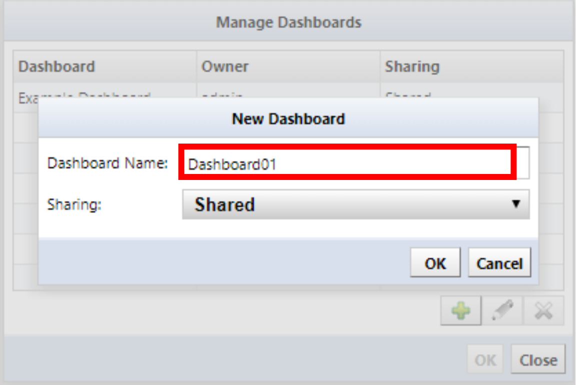
	IP Address	Hostname
✓	10.0.0.250	
✓	10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
✓	10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
✓	10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
✓	10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
✓	10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
✓	10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

2. Click [✚ (Add)].


Manage Dashboards

Dashboard	Owner	Sharing
Example Dashboard	admin	Shared

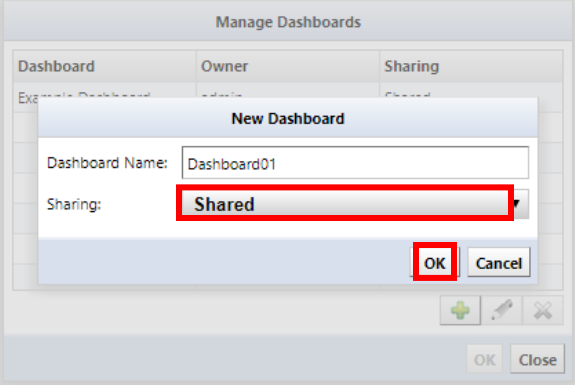
3. Enter the dashboard name.


New Dashboard

Dashboard Name: Dashboard01

Sharing: Shared

4. Select the dashboard type for the share and click [OK].


New Dashboard

Dashboard Name: Dashboard01

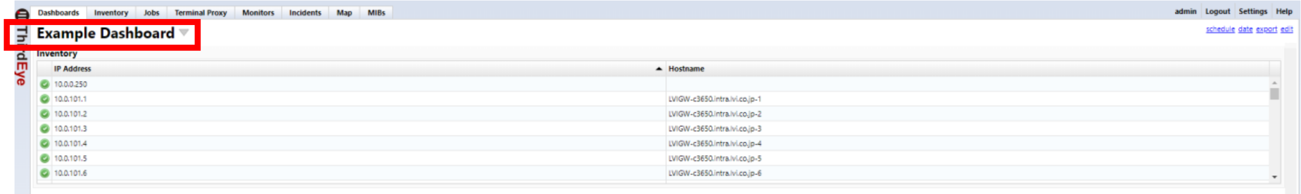
Sharing: Shared

Sharing	Explanation
Shared	Add dashboards that other users can view.
Private	Add a dashboard that only the created user can view.

5. The dashboard is added to the list.

5.5.2 Switching dashboards

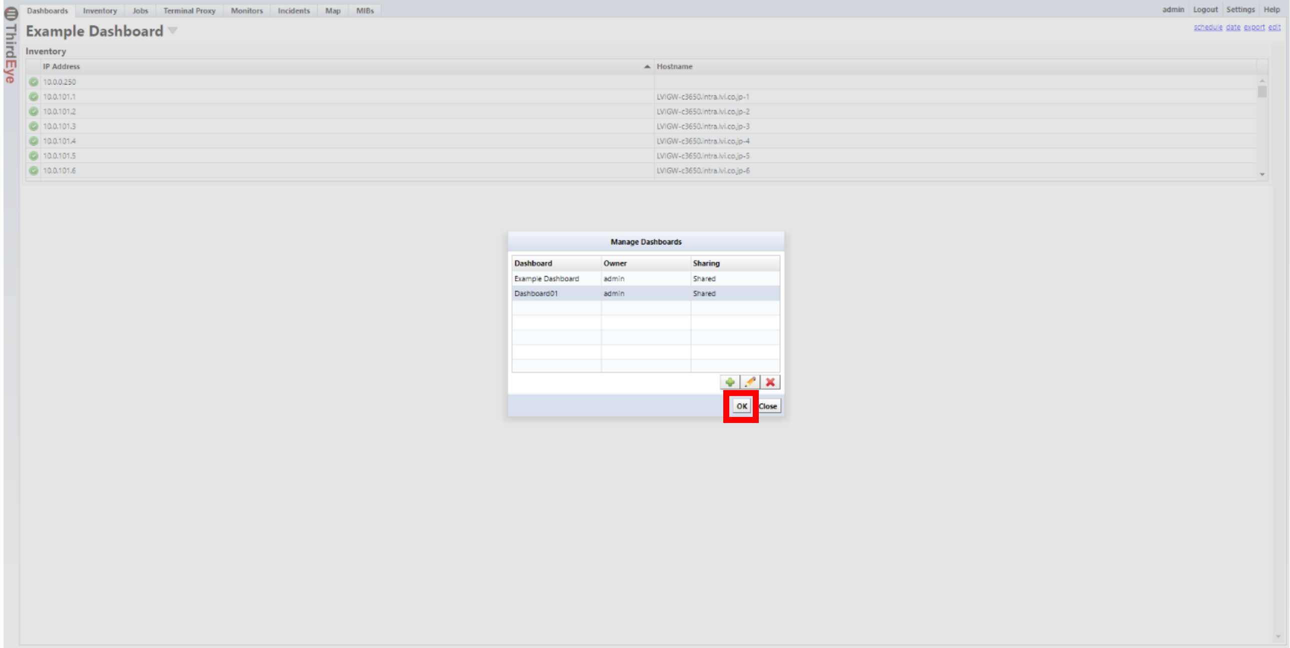
1. Click the "Dashboard Name" (in the figure below, "Example Dashboard") under the Dashboard tab and select [Manage Dashboards].



Inventory

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

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



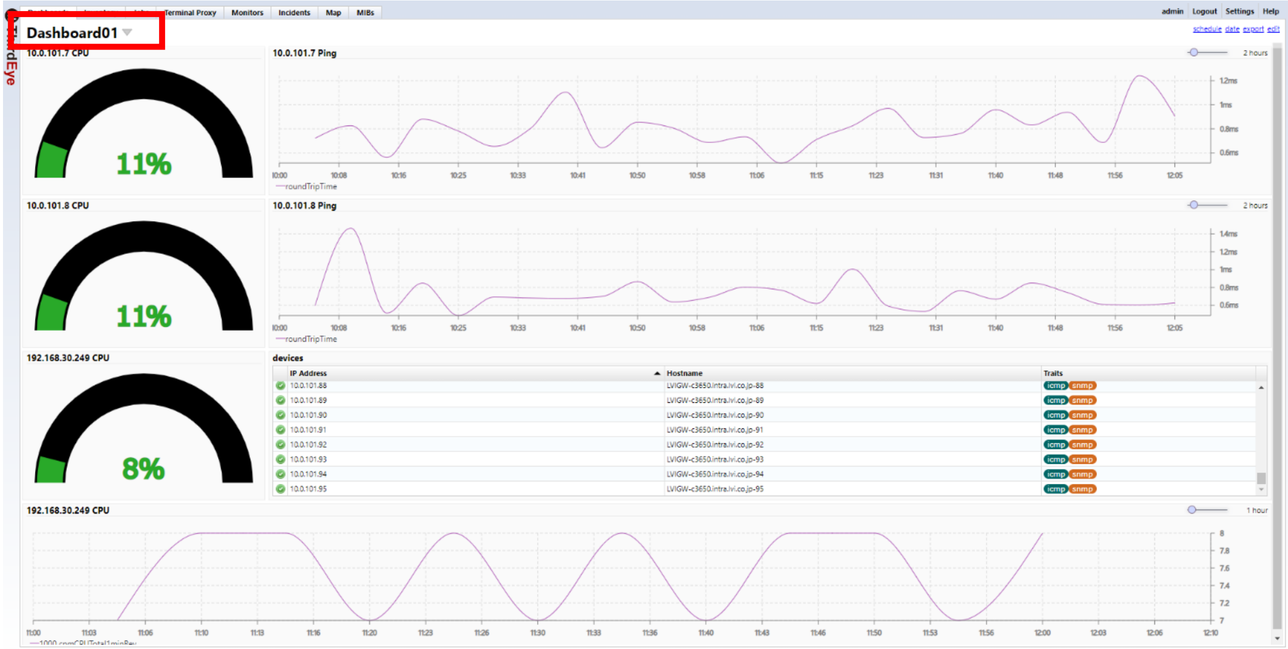
Inventory

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

Manage Dashboards

Dashboard	Owner	Sharing
Example Dashboard	admin	Shared
Dashboard01	admin	Shared

3. Switch to the selected dashboard screen.

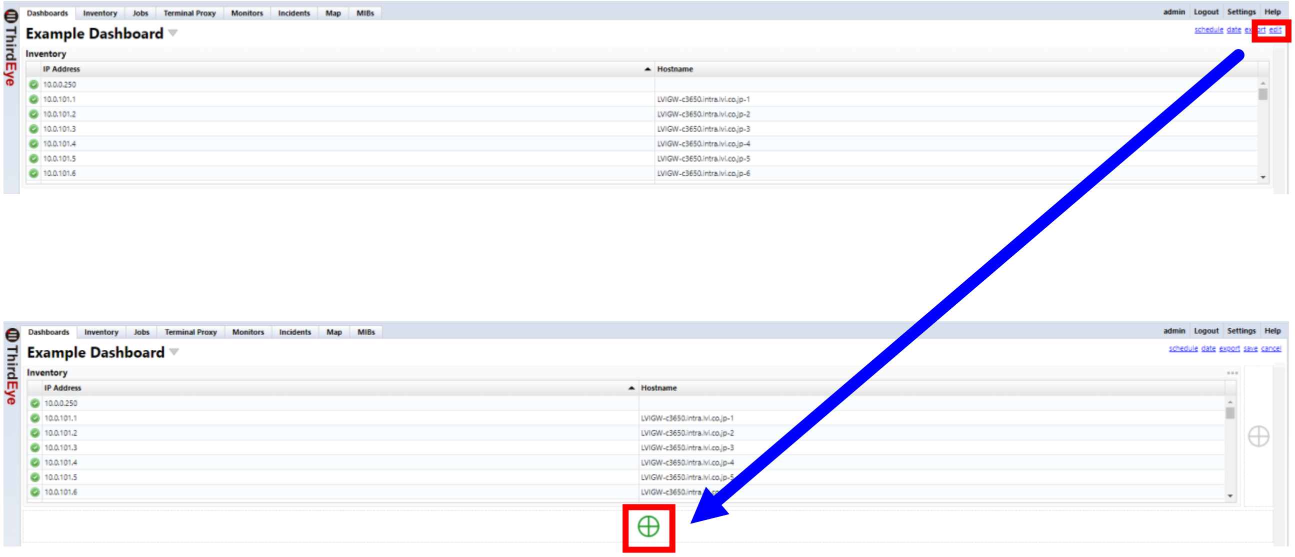


devices

IP Address	Hostname	Traits
10.0.101.88	LVIGW-c3650.intra.lvi.co.jp-88	icmp snmp
10.0.101.89	LVIGW-c3650.intra.lvi.co.jp-89	icmp snmp
10.0.101.90	LVIGW-c3650.intra.lvi.co.jp-90	icmp snmp
10.0.101.91	LVIGW-c3650.intra.lvi.co.jp-91	icmp snmp
10.0.101.92	LVIGW-c3650.intra.lvi.co.jp-92	icmp snmp
10.0.101.93	LVIGW-c3650.intra.lvi.co.jp-93	icmp snmp
10.0.101.94	LVIGW-c3650.intra.lvi.co.jp-94	icmp snmp
10.0.101.95	LVIGW-c3650.intra.lvi.co.jp-95	icmp snmp

5.5.3 Adding widgets

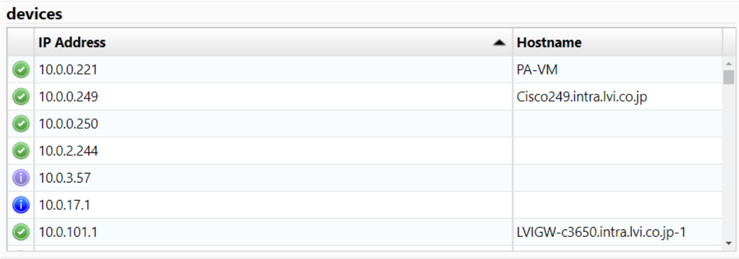
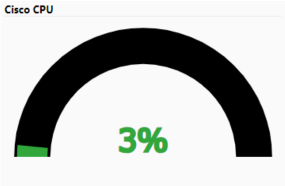
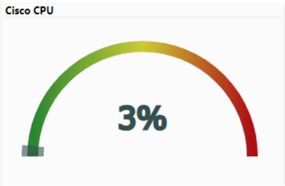
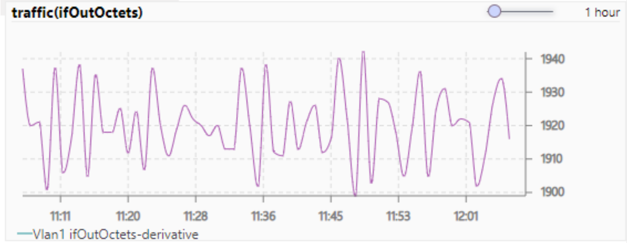
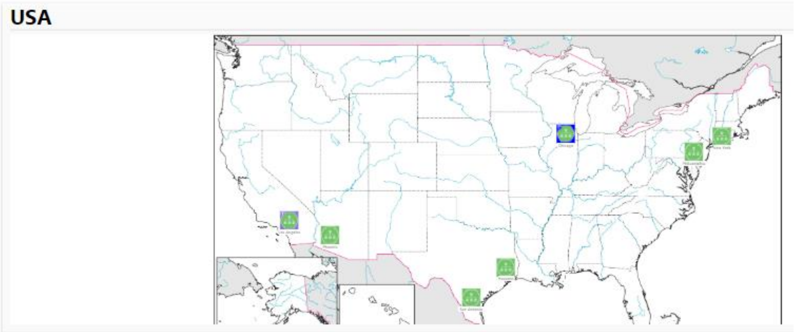
A widget is a component that displays content on a dashboard. Add widgets to your dashboard for quick access to the information you want to see. You can add widgets by clicking [⊕ (Add)] from [Edit] in the upper right of the dashboard screen.



Inventory

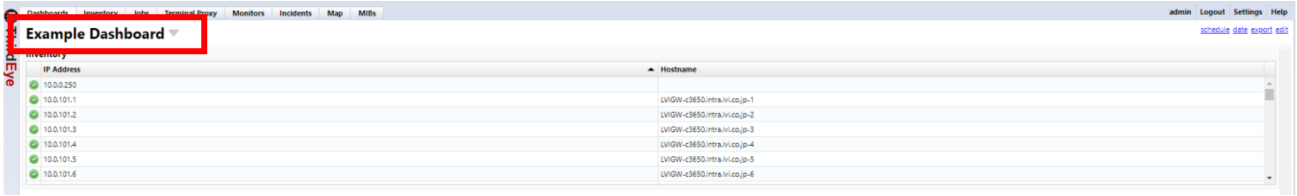
IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

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

Type if widgets	Explanation
Inventory	View inventory.  devices IP Address ▲ | Hostname ✓ 10.0.0.221 | PA-VM ✓ 10.0.0.249 | Cisco249.intra.lvi.co.jp ✓ 10.0.0.250 | ✓ 10.0.2.244 | ⓘ 10.0.3.57 | ⓘ 10.0.17.1 | ✓ 10.0.101.1 | LVIGW-c3650.intra.lvi.co.jp-1 * The maximum number of displays is 100. If the number exceeds 100, you can check it from the [Inventory] tab.
Gauge graph	Display Gauge graph.  
Histogram	Display a Histogram. 
Map	Display the map. 

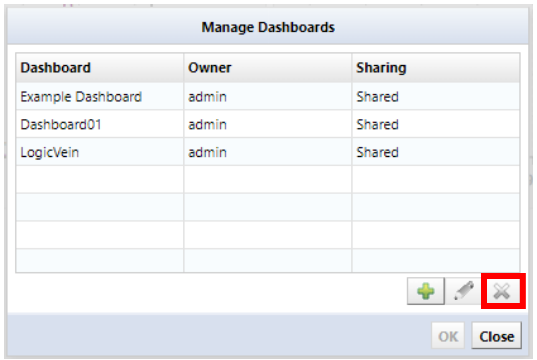
5.5.4 Deleting a dashboard

1. Click the "Dashboard Name" (in the figure below, "Example Dashboard") under the Dashboard tab and select [Manage Dashboards].



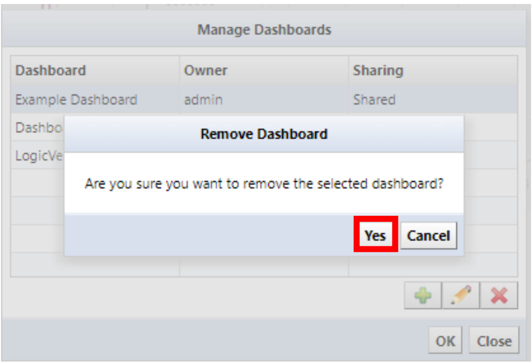
IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

2. Select the dashboard you want to delete and click [✖ (Remove)].



Dashboard	Owner	Sharing
Example Dashboard	admin	Shared
Dashboard01	admin	Shared
LogicVein	admin	Shared

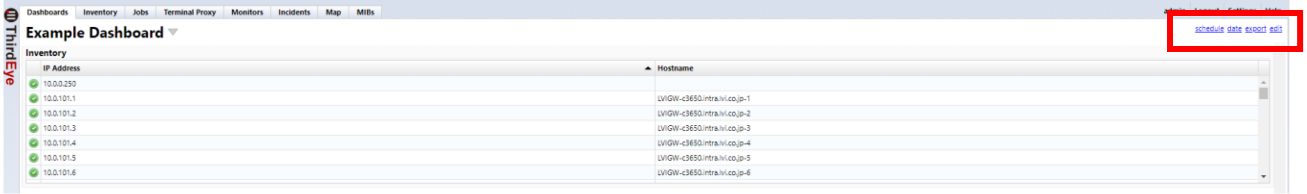
3. A confirmation message is displayed. Click [Yes].



Are you sure you want to remove the selected dashboard?

5.5.5 Dashboard edit menu

【Normal】

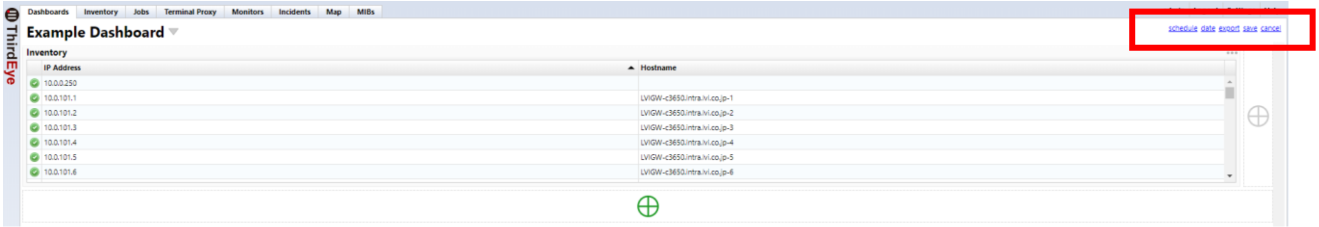


Example Dashboard

Inventory

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

【Editing】



Example Dashboard

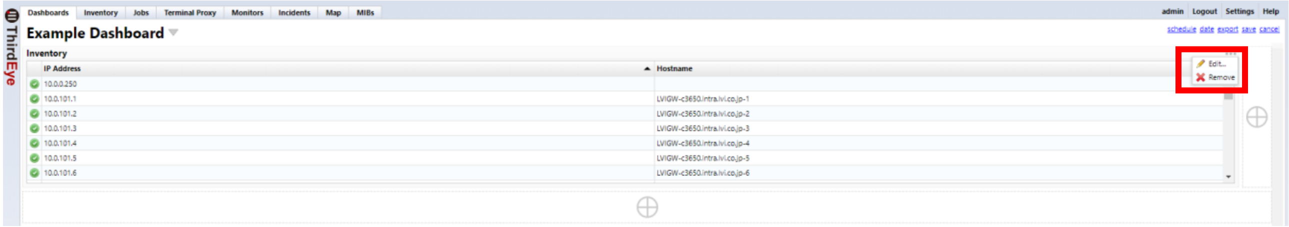
Inventory

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

Description	Explanation
schedule	Schedule email reports for dashboard PDF reports. * Schedule is for "Inventory" and "Histogram" widgets.
date	You can change the display period of the line graph on the dashboard at once. * The date is for the "Histogram" widget.
export	Create a PDF report of the displayed dashboard. Export is for "Inventory" and "Histogram" widgets.
edit	Switch to dashboard edit mode.
save	Save the dashboard changes and return from edit mode.
cancel	Cancels the dashboard edit mode.
⊕ **(add)**	Add a widget to the dashboard.

5.5.6 Edit widget menu

You can add / edit / remove widgets while in dashboard edit mode.



Example Dashboard

Inventory

IP Address	Hostname
10.0.0.250	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6

Description	Explanation
・・・	A three-point leader (“…”) mark displayed on the right side of the widget title. Click “…” to display the widget editing menu.
Edit	Edit the widget.
Remove	Remove the widget.

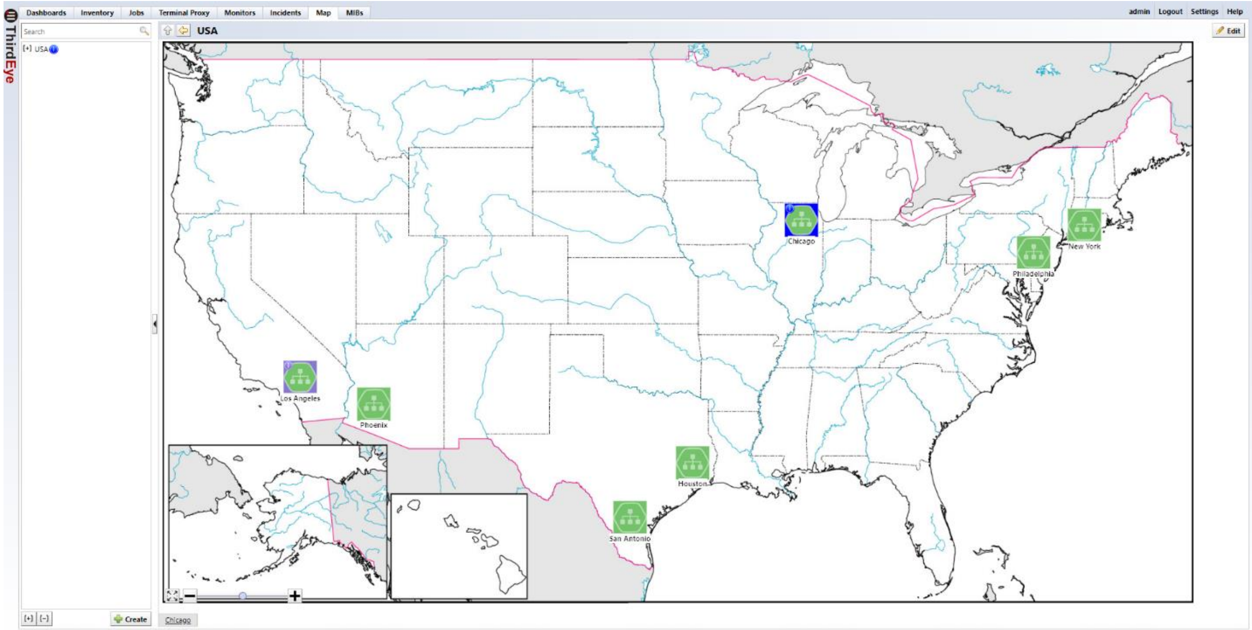
6. Operation

This section describes the operations used in daily operations.

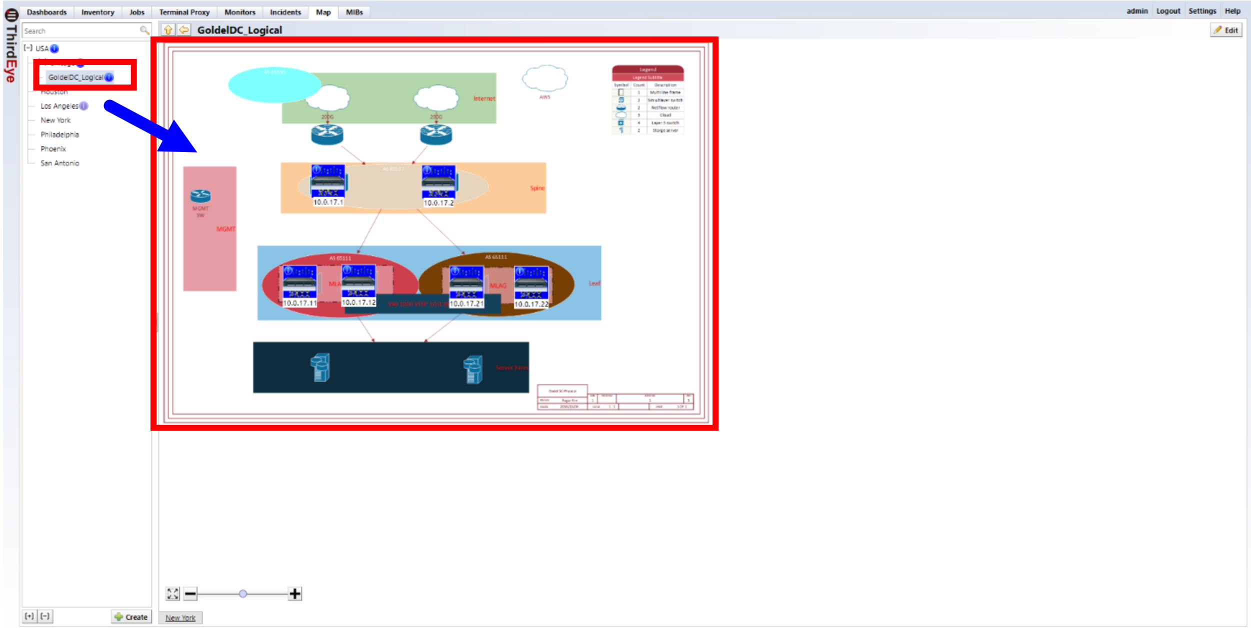
6.1 Troubleshooting

6.1.1 Checking the failed device

When a failure is detected, the background color of the icon on the map changes to a color corresponding to the severity set for the monitor, and a status icon indicating the severity is displayed in the upper left. This behavior is the same for maps registered as widgets in the dashboard.

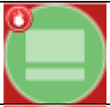
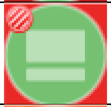
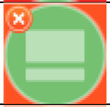
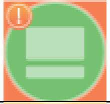
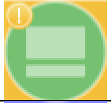
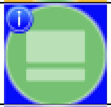
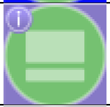
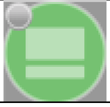


If you double-click the map icon whose status has changed, you will move to the lower layer. In addition, you can easily display the desired map by using the map tree.


ThirdEye
Dashboards
Inventory
Jobs
Terminal Proxy
Monitors
Incidents
Map
MIBs
admin
Logout
Settings
Help
Search
GoldelDC_Logical
Edit
[-] USA
GoldelDC_Logical
Los Angeles
New York
Philadelphia
Phoenix
San Antonio
Internet
AWS
200G
200G
Legend
Spine
10.0.17.1
10.0.17.2
MGMT SW
MGMT
AS 65111
AS 65111
MLAG
MLAG
Leaf
10.0.17.11
10.0.17.12
10.0.17.21
10.0.17.22
[+] [-]
Create
New York

MEMO :

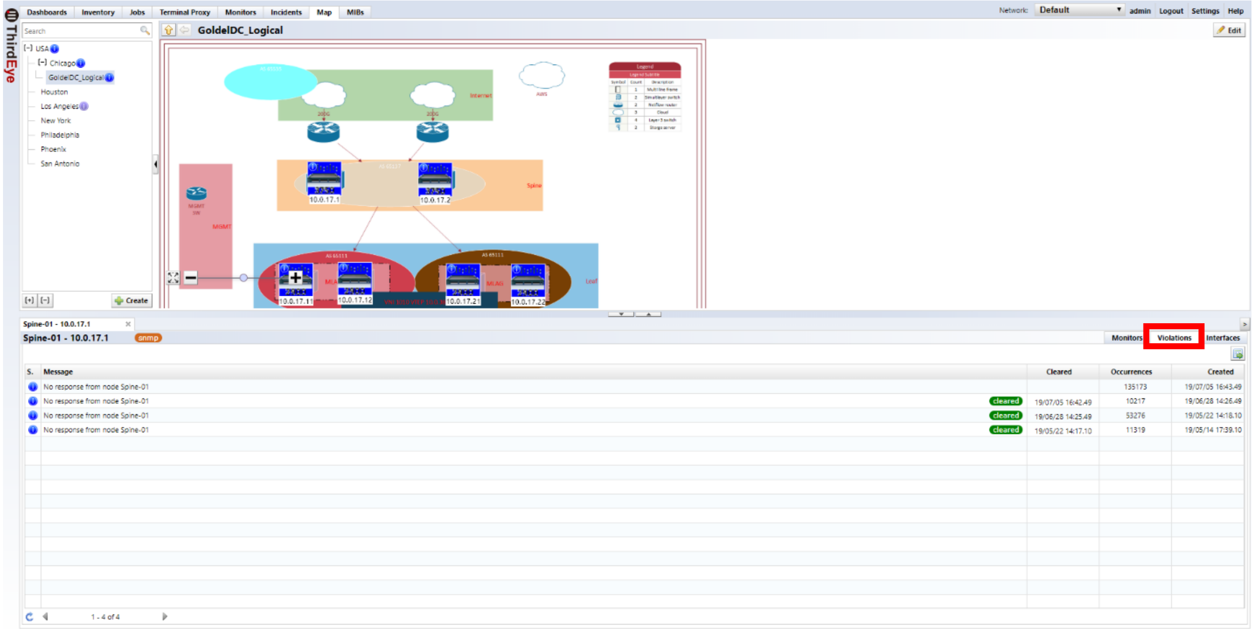
Refer to the following table for the background color / status icon types depending on the scheme severity.

Severity	Map（Image)	Status Icon
Emergency		🔴
Alert		🔴
Critical		🟠
Error		🟠
Warning		🟡
Notice		🔵
Info		🟣
Debug		⚪

*If multiple incidents occur on one device, the one with the highest severity is displayed.

6.1.2 Checking the details of the failure

Once you have identified the location of the failure, you need to know what the failure is. You can display the device details screen by double-clicking the icon where the fault has occurred from the map. In the [Violations] tab of the device details screen, you can check the fault that has occurred in the monitored device.



Spine-01 - 10.0.17.1

S.	Message		Cleared	Occurrences	Created
●	No response from node Spine-01			135173	19/07/05 16:43.49
●	No response from node Spine-01	cleared	19/07/05 16:42.49	10217	19/06/28 14:26.49
●	No response from node Spine-01	cleared	19/06/28 14:25.49	53276	19/05/22 14:18.10
●	No response from node Spine-01	cleared	19/05/22 14:17.10	11319	19/05/14 17:39.10

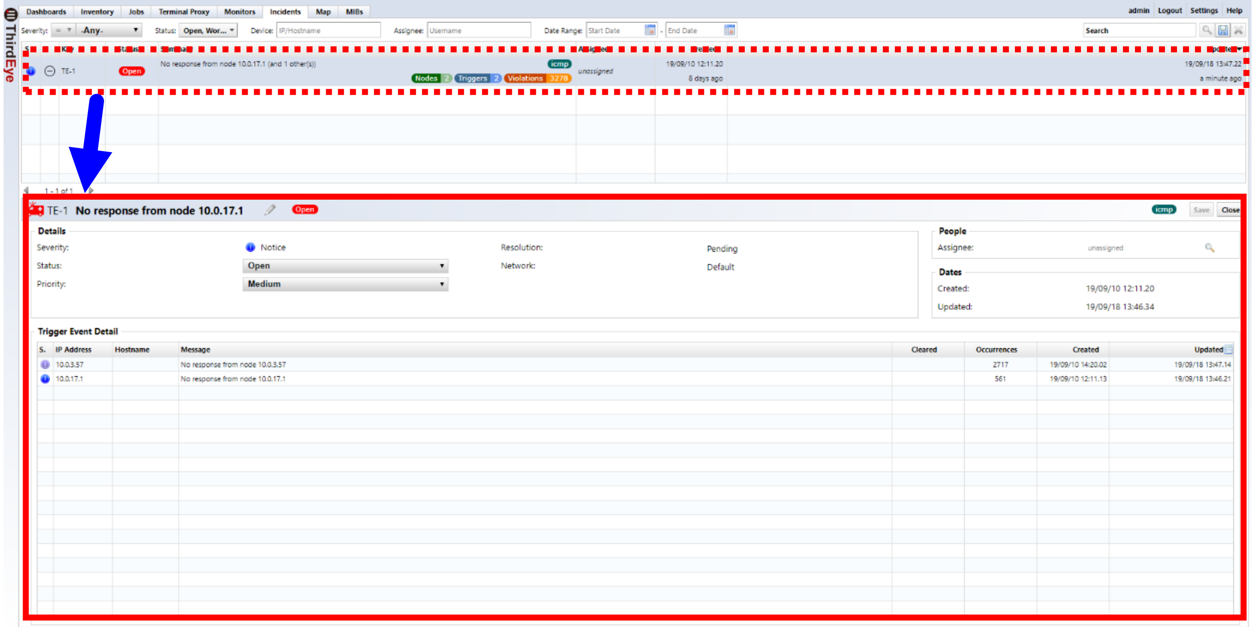
In addition, ThirdEye has an incident function. On the incident screen, you can check the details of the failure. On the incident screen, detected events are displayed based on the alert policy settings.

The incident status indicates the response status of the incident. An incident occurs at the first event detection and is displayed in the incident.

Subsequent events for the same monitor and policy are associated with the same open incident. New incidents configured with the same monitors and policies will not be generated unless the original incident is closed ("resolved").

If the incident is not closed, new alerts are aggregated into the existing incident. Incidents cannot be deleted by user operations.

1. Double-click the incident line you want to check.
2. The incident details screen is displayed at the bottom of the screen. Check the event details in the event details.



Severity: -Any- Status: Open, Wor... Device: IP/Hostname Assignee: Username Date Range: Start Date - End Date

S	P	Key	Status	Summary	Assignee	Created	Updated
		TE-1	Open	No response from node 10.0.17.1 (and 1 other(s)) icmp Nodes 2 Triggers 2 Violations 3278	unassigned	19/09/10 12:11.20 8 days ago	19/09/18 13:47.22 a minute ago

1 - 1 of 1

TE-1 No response from node 10.0.17.1 Open

Details

Severity:	Notice	Resolution:	Pending
Status:	Open	Network:	Default
Priority:	Medium		

People

Assignee: unassigned

Dates

Created: 19/09/10 12:11.20

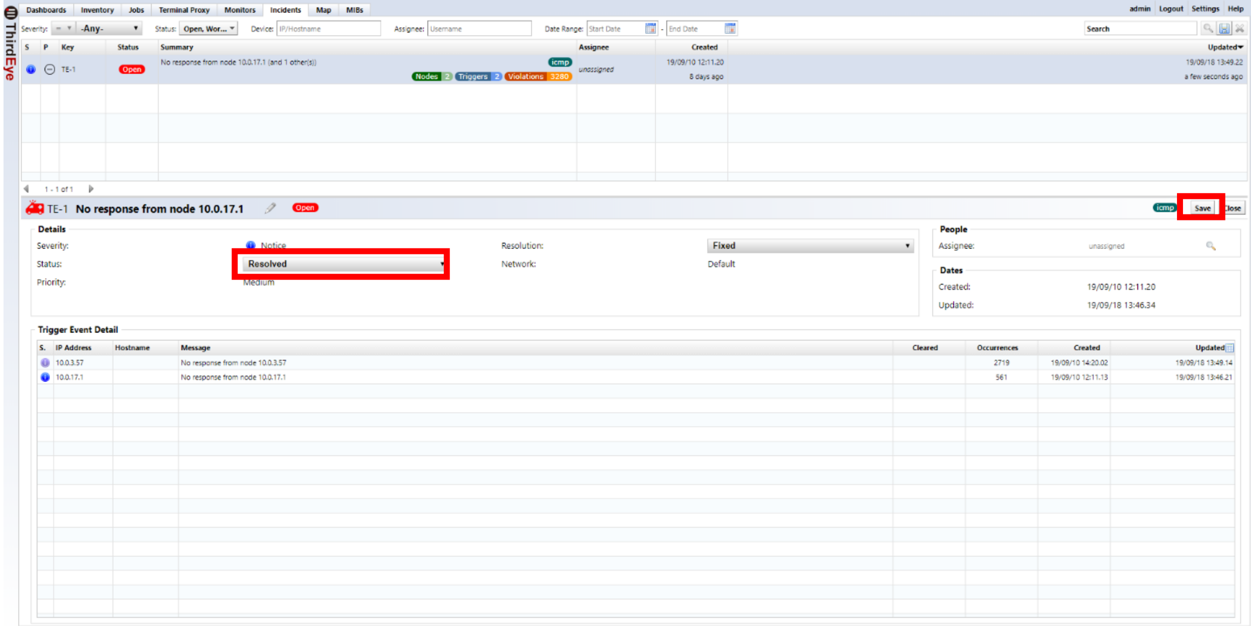
Updated: 19/09/18 13:46.34

Trigger Event Detail

S.	IP Address	Hostname	Message	Cleared	Occurrences	Created	Updated
	10.0.3.57		No response from node 10.0.3.57		2717	19/09/10 14:20.02	19/09/18 13:47.14
	10.0.17.1		No response from node 10.0.17.1		561	19/09/10 12:11.13	19/09/18 13:46.21

6.1.3 After handling the failure, make the incident “resolved”

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



Severity: -Any- Status: Open, Wor... Device: IP/Hostname Assignee: Username Date Range: Start Date - End Date

S	P	Key	Status	Summary	Assignee	Created	Updated
		TE-1	Open	No response from node 10.0.17.1 (and 1 other(s)) icmp Nodes 2 Triggers 2 Violations 3280	unassigned	19/09/10 12:11.20 8 days ago	19/09/18 13:49.22 a few seconds ago

1 - 1 of 1

TE-1 No response from node 10.0.17.1 Open

Details

Severity:	Notice	Resolution:	Fixed
Status:	Resolved	Network:	Default
Priority:	Medium		

People

Assignee: unassigned

Dates

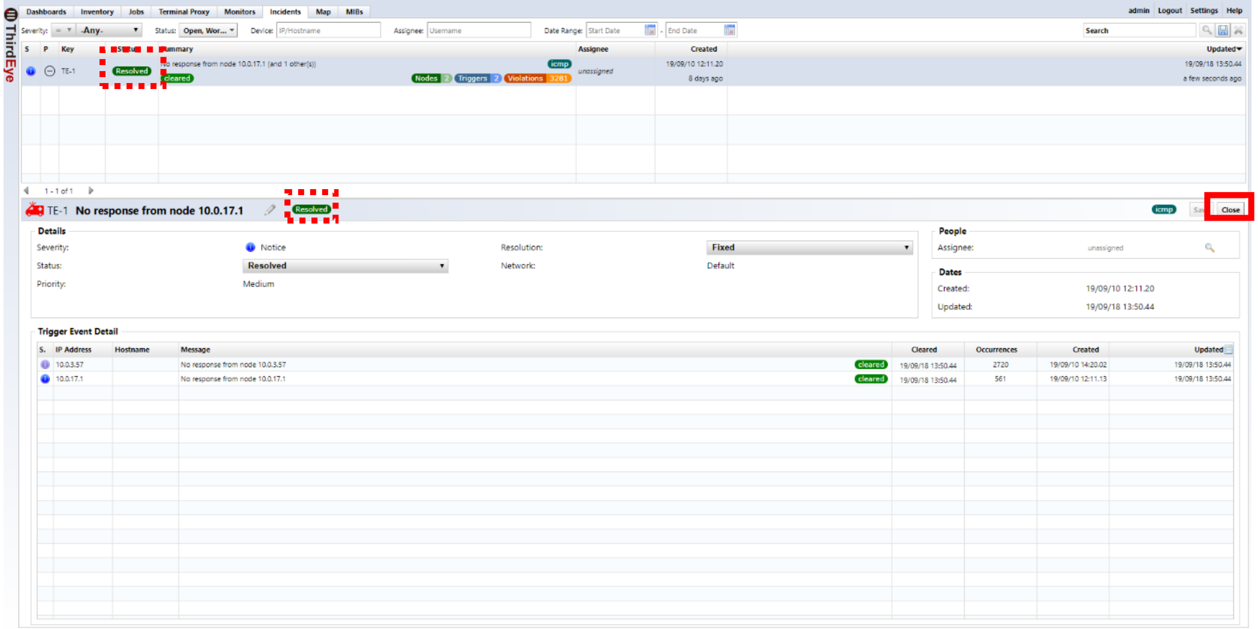
Created: 19/09/10 12:11.20

Updated: 19/09/18 13:46.34

Trigger Event Detail

S.	IP Address	Hostname	Message	Cleared	Occurrences	Created	Updated
	10.0.3.57		No response from node 10.0.3.57		2719	19/09/10 14:20.02	19/09/18 13:49.14
	10.0.17.1		No response from node 10.0.17.1		561	19/09/10 12:11.13	19/09/18 13:46.21

The status display changes to “Resolved” and the close process is complete. Click [Close] to close the incident details screen.



Severity: = -Any- Status: Open, Wor... Device: IP/Hostname Assignee: Username Date Range: Start Date - End Date

S	P	Key	Status	Summary	Assignee	Created	Updated
●	⊖	TE-1	Resolved	No response from node 10.0.17.1 (and 1 other(s)) icmp cleared Nodes 2 Triggers 2 Violations 3281	unassigned	19/09/10 12:11.20 8 days ago	19/09/18 13:50.44 a few seconds ago

1 - 1 of 1

TE-1 No response from node 10.0.17.1 Resolved

Details

Severity:	● Notice	Resolution:	Fixed
Status:	Resolved	Network:	Default
Priority:	Medium		

People

Assignee: unassigned

Dates

Created: 19/09/10 12:11.20

Updated: 19/09/18 13:50.44

Trigger Event Detail

S.	IP Address	Hostname	Message	Cleared	Occurrences	Created	Updated
●	10.0.3.57		No response from node 10.0.3.57 cleared	19/09/18 13:50.44	2720	19/09/10 14:20.02	19/09/18 13:50.44
●	10.0.17.1		No response from node 10.0.17.1 cleared	19/09/18 13:50.44	561	19/09/10 12:11.13	19/09/18 13:50.44

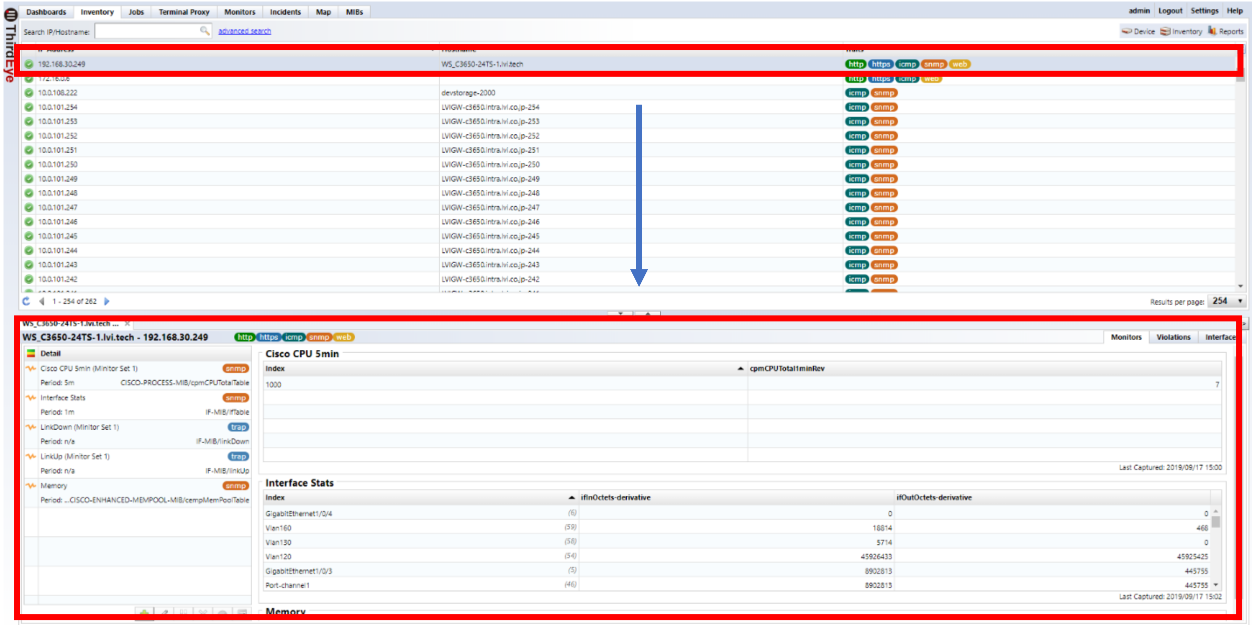
6.2 Checking data collected by SNMP

Data collected by the SNMP monitor is saved in the database. You can create a graph from past data or export it to an Excel file.

6.2.1 Displaying a graph from the console

Data collected by SNMP can be confirmed by adding it to the dashboard widget. The procedure for adding to a dashboard is described in "5.5.1 Adding a dashboard", but it can also be easily added to the dashboard from the device details screen.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.



Search IP/Hostname: advanced search

192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
172.16.0.6		http https icmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

1 - 254 of 262 Results per page: 254

WS_C3650-24TS-1.lvi.tech ...

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Detail	
Cisco CPU 5min (Minitor Set 1)	snmp
Period: 5m	CISCO-PROCESS-MIB/cpmCPUTotalTable
Interface Stats	snmp
Period: 1m	IF-MIB/ifTable
LinkDown (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkDown
LinkUp (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkUp
Memory	snmp
Period: ...CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable	

Cisco CPU 5min

Index	cpmCPUTotal1minRev
1000	7

Last Captured: 2019/09/17 15:00

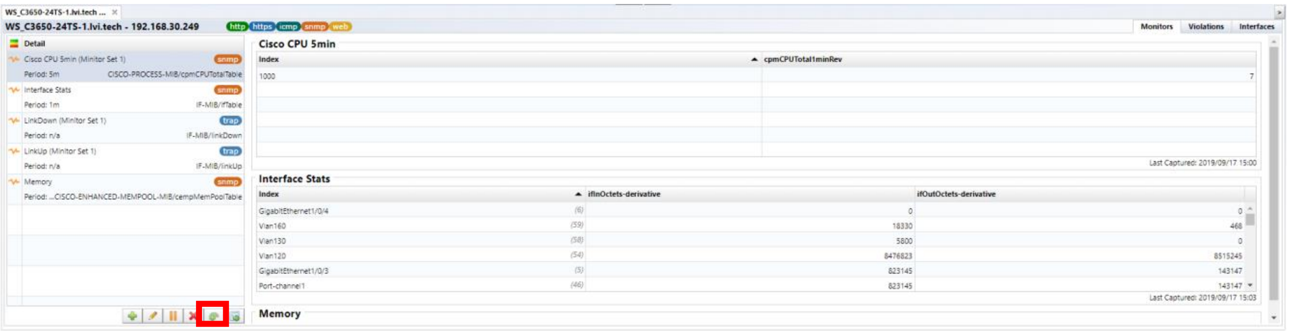
Interface Stats

Index		ifInOctets-derivative	ifOutOctets-derivative
GigabitEthernet1/0/4	(6)	0	0
Vlan160	(59)	18814	468
Vlan130	(58)	5714	0
Vlan120	(54)	45926433	45925425
GigabitEthernet1/0/3	(5)	8902813	445755
Port-channel1	(46)	8902813	445755

Last Captured: 2019/09/17 15:02

Memory

2. From the monitor details, select the monitor whose data you want to check, and click [Add monitor to a Dashboard].



WS_C3650-24TS-1.lvi.tech ...

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Detail	
Cisco CPU 5min (Minitor Set 1)	snmp
Period: 5m	CISCO-PROCESS-MIB/cpmCPUTotalTable
Interface Stats	snmp
Period: 1m	IF-MIB/ifTable
LinkDown (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkDown
LinkUp (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkUp
Memory	snmp
Period: ...CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable	

Cisco CPU 5min

Index	cpmCPUTotal1minRev
1000	7

Last Captured: 2019/09/17 15:00

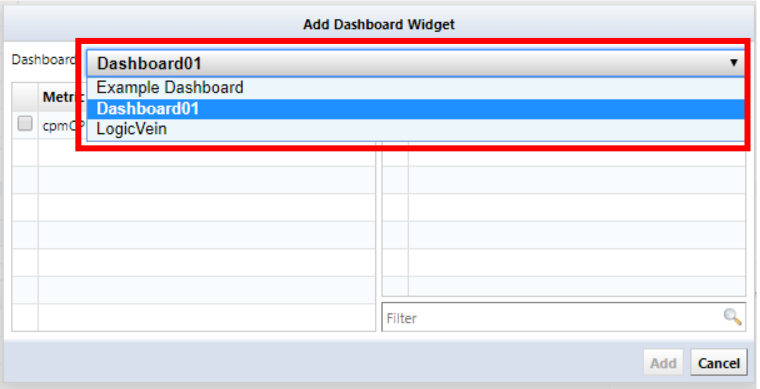
Interface Stats

Index		ifInOctets-derivative	ifOutOctets-derivative
GigabitEthernet1/0/4	(6)	0	0
Vlan160	(59)	18330	468
Vlan130	(58)	5800	0
Vlan120	(54)	8476823	8515245
GigabitEthernet1/0/3	(5)	823145	143147
Port-channel1	(46)	823145	143147

Last Captured: 2019/09/17 15:03

Memory

3. Select the dashboard to which you want to add the widget.

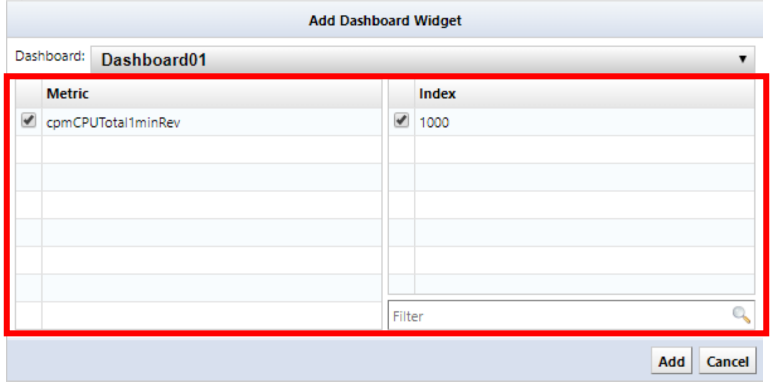


Add Dashboard Widget

Dashboard: Dashboard01

4. Select the metrics and indexes to add to the graph and click [Add].

* Only metrics are displayed depending on the data to be acquired.



Add Dashboard Widget

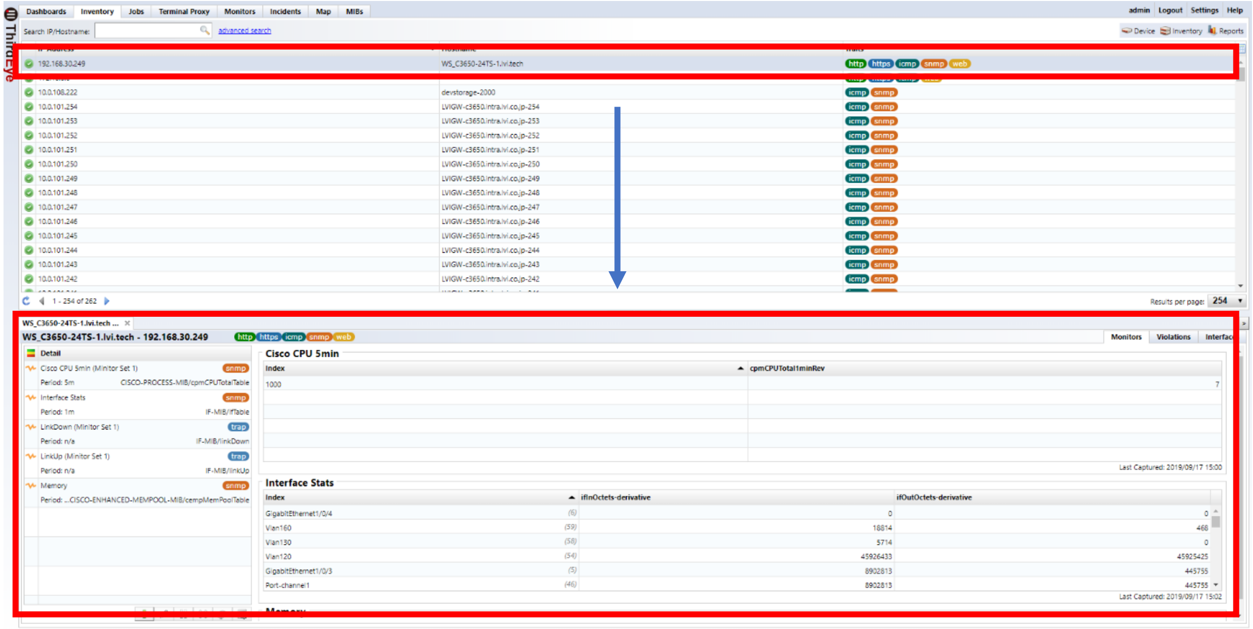
Dashboard: Dashboard01

Metric	Index
☑ cpmCPUTotal1minRev	☑ 1000

6.2.2 Export to Excel file

Data collected by SNMP can be exported to an Excel file.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.



192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Detail

- Cisco CPU 5min (Minitor Set 1) snmp — Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable
- Interface Stats snmp — Period: 1m IF-MIB/ifTable
- LinkDown (Minitor Set 1) trap — Period: n/a IF-MIB/linkDown
- LinkUp (Minitor Set 1) trap — Period: n/a IF-MIB/linkUp
- Memory snmp — Period: ...CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable

Cisco CPU 5min

Index	cpmCPUTotal1minRev
1000	7

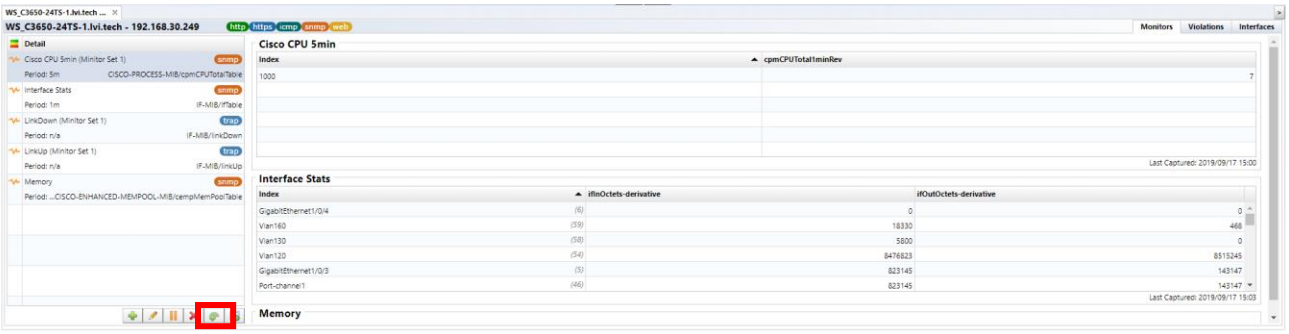
Last Captured: 2019/09/17 15:00

Interface Stats

Index		ifInOctets-derivative	ifOutOctets-derivative
GigabitEthernet1/0/4	(6)	0	0
Vlan160	(59)	18814	468
Vlan130	(58)	5714	0
Vlan120	(54)	45926433	45925425
GigabitEthernet1/0/3	(5)	8902813	445755
Port-channel1	(46)	8902813	445755

Last Captured: 2019/09/17 15:02

2. From the monitor details, select the monitor whose data you want to check, and click [Add monitor to a Dashboard].



WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Detail

- Cisco CPU 5min (Minitor Set 1) snmp — Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable
- Interface Stats snmp — Period: 1m IF-MIB/ifTable
- LinkDown (Minitor Set 1) trap — Period: n/a IF-MIB/linkDown
- LinkUp (Minitor Set 1) trap — Period: n/a IF-MIB/linkUp
- Memory snmp — Period: ...CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable

Cisco CPU 5min

Index	cpmCPUTotal1minRev
1000	7

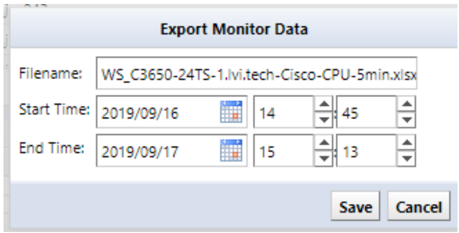
Last Captured: 2019/09/17 15:00

Interface Stats

Index		ifInOctets-derivative	ifOutOctets-derivative
GigabitEthernet1/0/4	(6)	0	0
Vlan160	(59)	18330	468
Vlan130	(58)	5800	0
Vlan120	(54)	8476823	8515245
GigabitEthernet1/0/3	(5)	823145	143147
Port-channel1	(46)	823145	143147

Last Captured: 2019/09/17 15:03

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



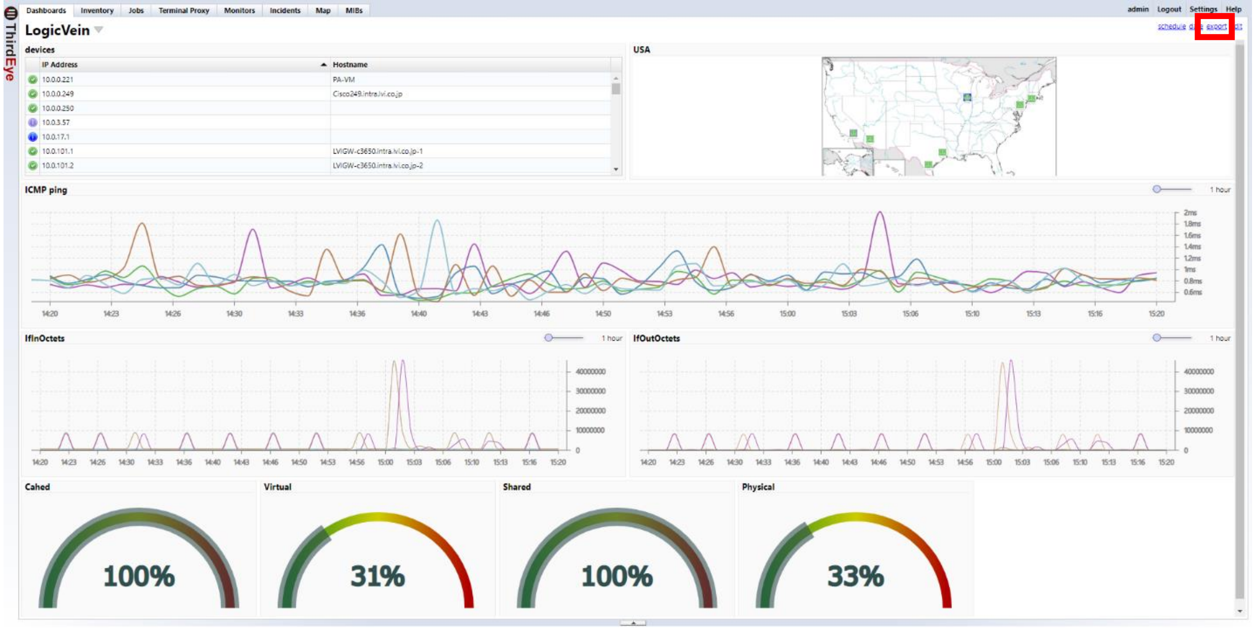
Export Monitor Data

Filename: WS_C3650-24TS-1.lvi.tech-Cisco-CPU-5min.xlsx
Start Time: 2019/09/16 14 : 45
End Time: 2019/09/17 15 : 13

After clicking Save, the Excel file will be downloaded.

6.2.3 Publish dashboard reports

The "Inventory" and "Line graph" displayed in the widget can be exported to a PDF file. Click [Export] at the top right of the dashboard screen to export.



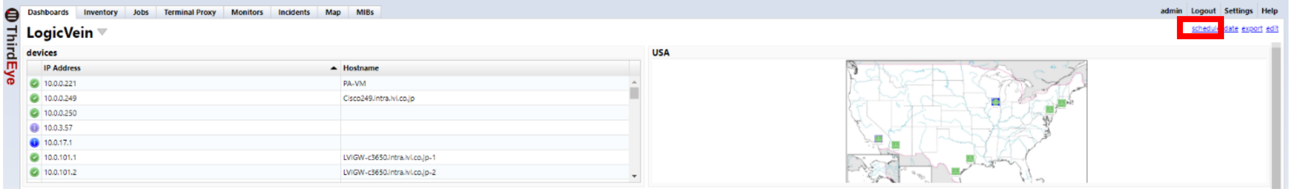
IP Address	Hostname
10.0.0.221	PA-VM
10.0.0.249	Cisco249.intra.lvi.co.jp
10.0.0.250	
10.0.3.57	
10.0.17.1	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2

6.2.4 Send dashboard reports regularly by email

You can email dashboard reports regularly.

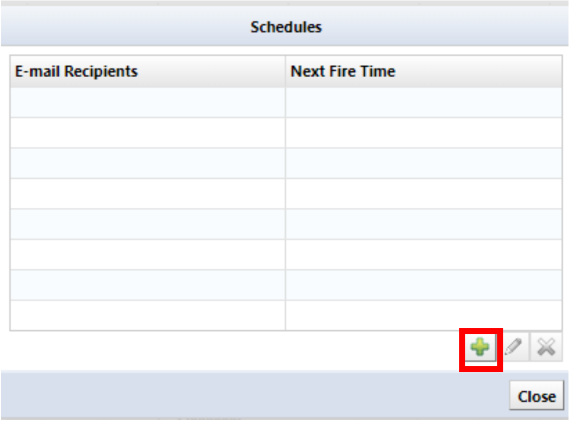
* To send mail, the mail server must be set up first. For details on mail server settings, refer to "7.5 Setting Mail Server".

1. Click [schedule].

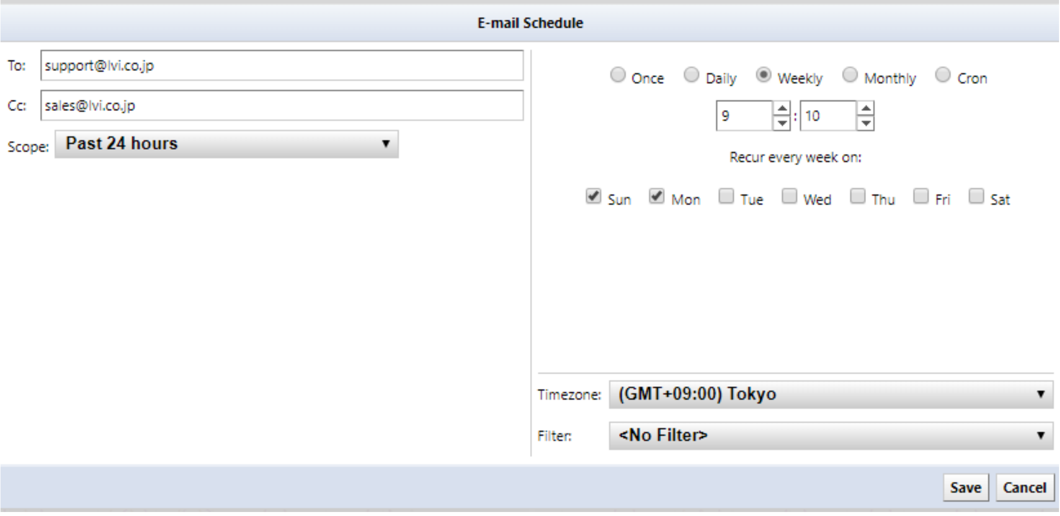


IP Address	Hostname
10.0.0.221	PA-VM
10.0.0.249	Cisco249.intra.lvi.co.jp
10.0.0.250	
10.0.3.57	
10.0.17.1	
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2

2. The Schedule screen is displayed. Click [✚ (Add)].



3. [The [E-mail Schedule] screen appears. Enter / select each item.



To: support@lvi.co.jp

Cc: sales@lvi.co.jp

Scope: Past 24 hours

○ Once ○ Daily ● Weekly ○ Monthly ○ Cron

9 : 10

Recur every week on:

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

Timezone: (GMT+09:00) Tokyo

Filter: <No Filter>

Description	Explanation
To/Cc	Enter the email destination address.
Scope	Specify the range of the report display period. Within 24 hours Within a week Within 30 days Yesterday (00: 00: 00-23: 59: 59) Last week (Monday to Sunday) Last month (from the beginning of the month to the end of the month) Date range (user can specify any period)
Schedule	Specify the schedule for issuing reports.
Time zone	Specify the time zone to publish the report.
Filter	Specify filter settings for execution time. * Set the filter in "Job Management".
Save	Save your settings.
Cancel	Discards the settings and returns to the previous screen.

6.3 SSH / Telnet connection to the device

SSH / Telnet connection can be made to the monitored device from the device list or map. This function is called “terminal proxy” in ThirdEye. When using a terminal proxy, commands executed on the terminal and output results are automatically saved.

6.3.1 Preparations before use

The following preparations are required to use the terminal proxy.

- Install Tera Term on the terminal to be operated

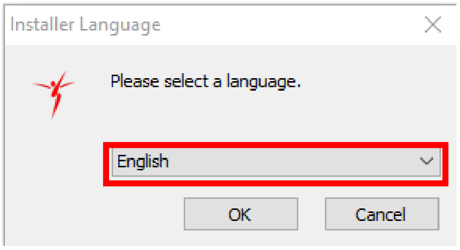
  The following preparations are required to use the terminal proxy.
- Install browser integration

  It is necessary to associate Tera Term with the browser connected to ThirdEye.

You can do this from the screen that appears when you start Terminal Proxy for the first time. The following describes the installation of Step 2 browser integration. For information on installing Tera Term, see the Tera Term manual.

1. Click [Install Integration].
2. Run the downloaded ttinstall.exe.

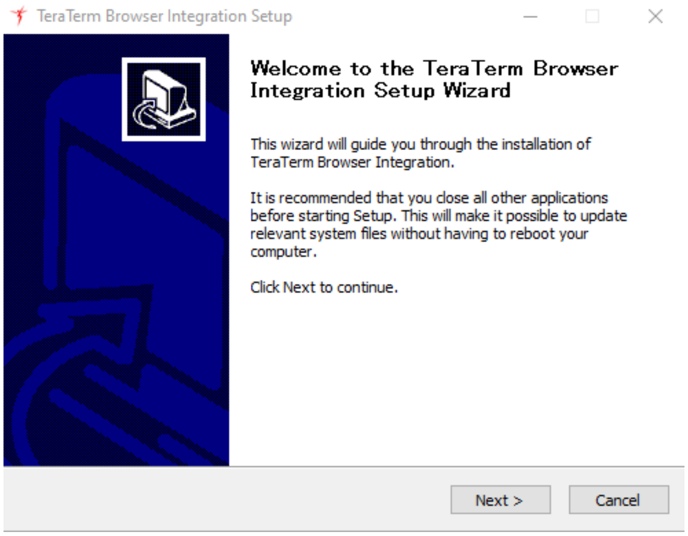
3. Select a language.


Installer Language

Please select a language.

English

4. Click [Next].



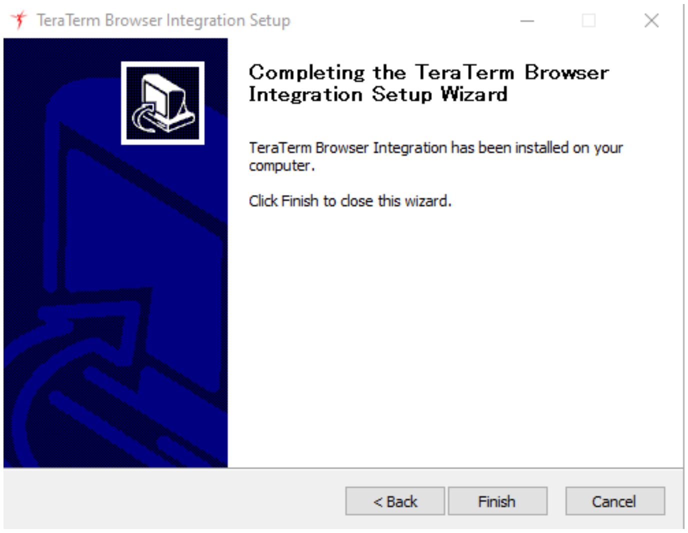
Welcome to the TeraTerm Browser Integration Setup Wizard

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.

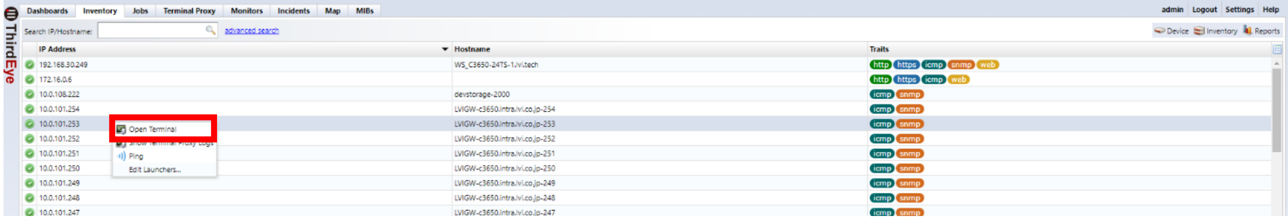
Click Finish to close this wizard.

Preparation is now complete.

For Step2, you may need to reset it when you clear the browser cache or update ThirdEye.

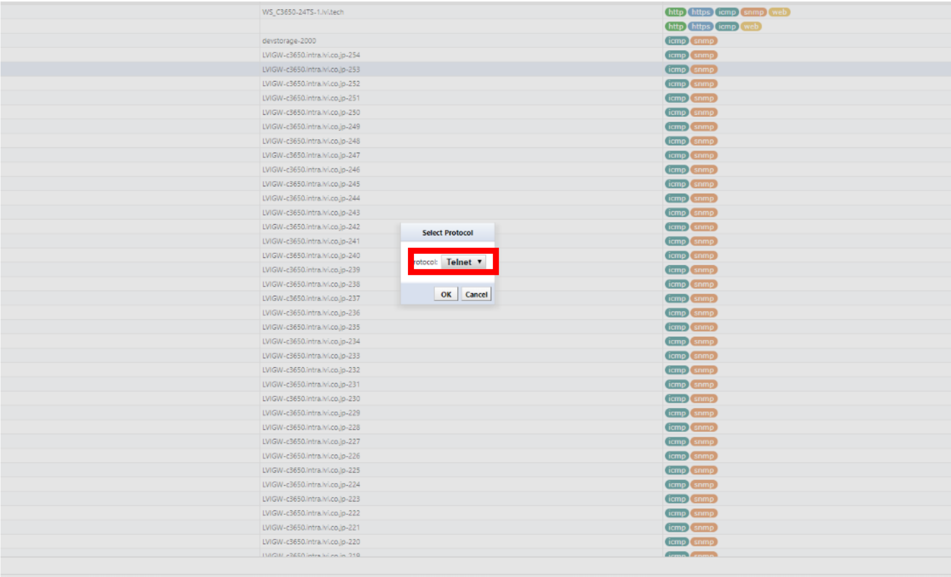
6.3.2 Starting the terminal

1. Select the [Inventory] tab.
2. Right-click the device to be connected to the terminal and select [Open Terminal].



IP Address	Hostname	Traits
192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
172.16.0.6		http https icmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp

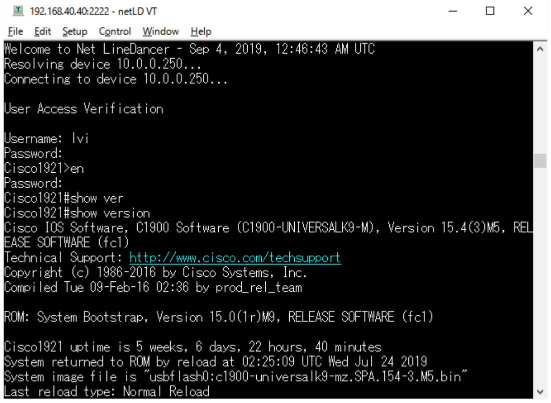
3. [Select Protocol] screen is displayed. Select the connection protocol and click [OK].



WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
	http https icmp web
devstorage-2000	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-241	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-240	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-239	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-238	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-237	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-236	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-235	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-234	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-233	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-232	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-231	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-230	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-229	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-228	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-227	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-226	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-225	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-224	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-223	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-222	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-221	icmp snmp
LVIGW-c3650.intra.lvi.co.jp-220	icmp snmp

4. The terminal software "Tera Term" starts up and the device login screen appears.

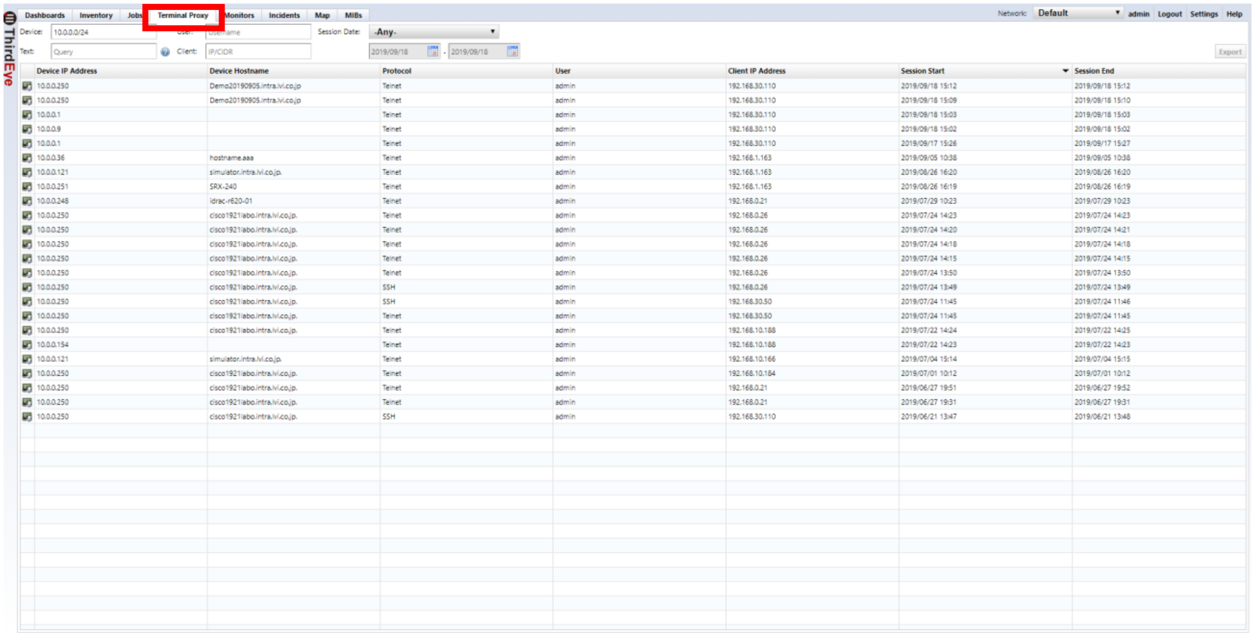
* Log out of the device when you are finished.



```
Welcome to Net LineDancer - Sep 4, 2019, 12:46:43 AM UTC
Resolving device 10.0.0.250...
Connecting to device 10.0.0.250...

User Access Verification

Username: lvi
Password:
Cisco1921>en
Password:
Cisco1921#show ver
Cisco1921#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M5, REL
EASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 09-Feb-16 02:36 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

Cisco1921 uptime is 5 weeks, 6 days, 22 hours, 40 minutes
System returned to ROM by reload at 02:25:09 UTC Wed Jul 24 2019
System image file is "usbflash0:c1900-universalk9-mz.SPA.154-3.M5.bin"
Last reload type: Normal Reload
```

6.3.3 Checking operation logs

1. Select the [Terminal Proxy] tab.



Network: Default

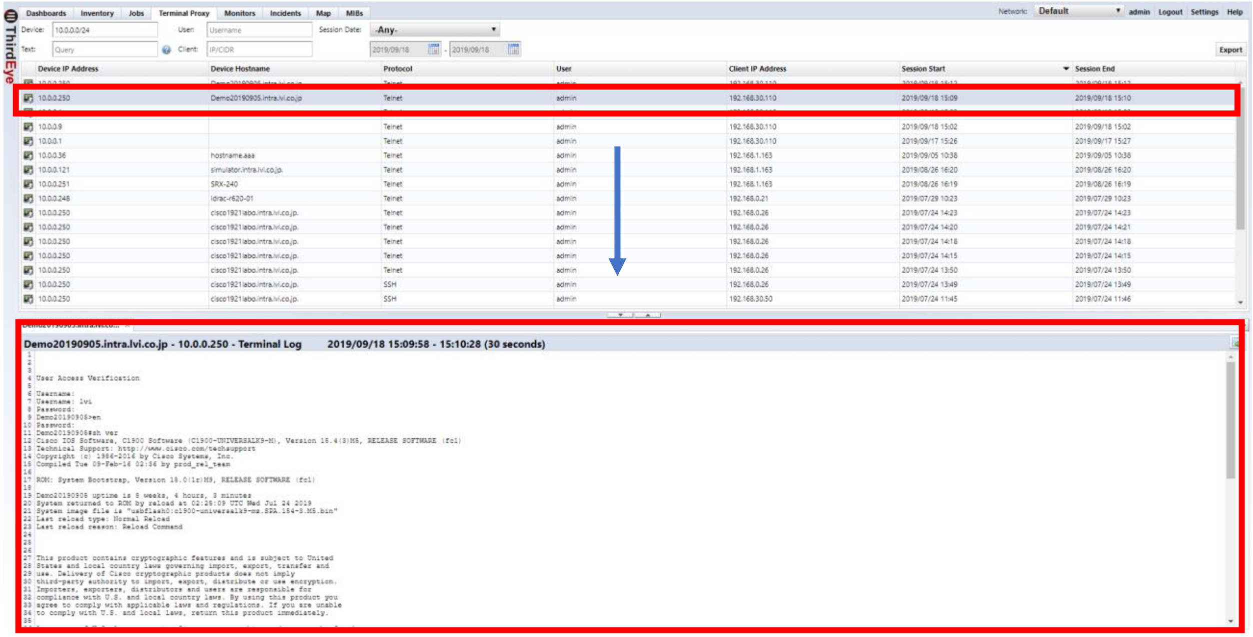
Device: 10.0.0.0/24 User: Username Session Date: -Any-

Text: Query Client: IP/CIDR 2019/09/18 - 2019/09/18

Device IP Address	Device Hostname	Protocol	User	Client IP Address	Session Start	Session End
10.0.0.250	Demo20190905.intra.lvi.co.jp	Telnet	admin	192.168.30.110	2019/09/18 15:12	2019/09/18 15:12
10.0.0.250	Demo20190905.intra.lvi.co.jp	Telnet	admin	192.168.30.110	2019/09/18 15:09	2019/09/18 15:10
10.0.0.1		Telnet	admin	192.168.30.110	2019/09/18 15:03	2019/09/18 15:03
10.0.0.9		Telnet	admin	192.168.30.110	2019/09/18 15:02	2019/09/18 15:02
10.0.0.1		Telnet	admin	192.168.30.110	2019/09/17 15:26	2019/09/17 15:27
10.0.0.36	hostname.aaa	Telnet	admin	192.168.1.163	2019/09/05 10:38	2019/09/05 10:38
10.0.0.121	simulator.intra.lvi.co.jp.	Telnet	admin	192.168.1.163	2019/08/26 16:20	2019/08/26 16:20
10.0.0.251	SRX-240	Telnet	admin	192.168.1.163	2019/08/26 16:19	2019/08/26 16:19
10.0.0.248	idrac-r620-01	Telnet	admin	192.168.0.21	2019/07/29 10:23	2019/07/29 10:23
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:23	2019/07/24 14:23
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:20	2019/07/24 14:21
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:18	2019/07/24 14:18
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:15	2019/07/24 14:15
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 13:50	2019/07/24 13:50
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	SSH	admin	192.168.0.26	2019/07/24 13:49	2019/07/24 13:49
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	SSH	admin	192.168.30.50	2019/07/24 11:45	2019/07/24 11:46
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.30.50	2019/07/24 11:45	2019/07/24 11:45
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.10.188	2019/07/22 14:24	2019/07/22 14:25
10.0.0.154		Telnet	admin	192.168.10.188	2019/07/22 14:23	2019/07/22 14:23
10.0.0.121	simulator.intra.lvi.co.jp.	Telnet	admin	192.168.10.166	2019/07/04 15:14	2019/07/04 15:15
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.10.184	2019/07/01 10:12	2019/07/01 10:12
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.21	2019/06/27 19:51	2019/06/27 19:52
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.21	2019/06/27 19:31	2019/06/27 19:31
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	SSH	admin	192.168.30.110	2019/06/21 13:47	2019/06/21 13:48

2. Double-click the log you want to view from the list.

You cannot check the session log during connection.



Network: Default

Device: 10.0.0.0/24 User: Username Session Date: -Any-

Text: Query Client: IP/CIDR 2019/09/18 - 2019/09/18

Device IP Address	Device Hostname	Protocol	User	Client IP Address	Session Start	Session End
10.0.0.250	Demo20190905.intra.lvi.co.jp	Telnet	admin	192.168.30.110	2019/09/18 15:09	2019/09/18 15:10
10.0.0.9		Telnet	admin	192.168.30.110	2019/09/18 15:02	2019/09/18 15:02
10.0.0.1		Telnet	admin	192.168.30.110	2019/09/17 15:26	2019/09/17 15:27
10.0.0.36	hostname.aaa	Telnet	admin	192.168.1.163	2019/09/05 10:38	2019/09/05 10:38
10.0.0.121	simulator.intra.lvi.co.jp.	Telnet	admin	192.168.1.163	2019/08/26 16:20	2019/08/26 16:20
10.0.0.251	SRX-240	Telnet	admin	192.168.1.163	2019/08/26 16:19	2019/08/26 16:19
10.0.0.248	idrac-r620-01	Telnet	admin	192.168.0.21	2019/07/29 10:23	2019/07/29 10:23
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:23	2019/07/24 14:23
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:20	2019/07/24 14:21
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:18	2019/07/24 14:18
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 14:15	2019/07/24 14:15
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	Telnet	admin	192.168.0.26	2019/07/24 13:50	2019/07/24 13:50
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	SSH	admin	192.168.0.26	2019/07/24 13:49	2019/07/24 13:49
10.0.0.250	cisco1921labo.intra.lvi.co.jp.	SSH	admin	192.168.30.50	2019/07/24 11:45	2019/07/24 11:46

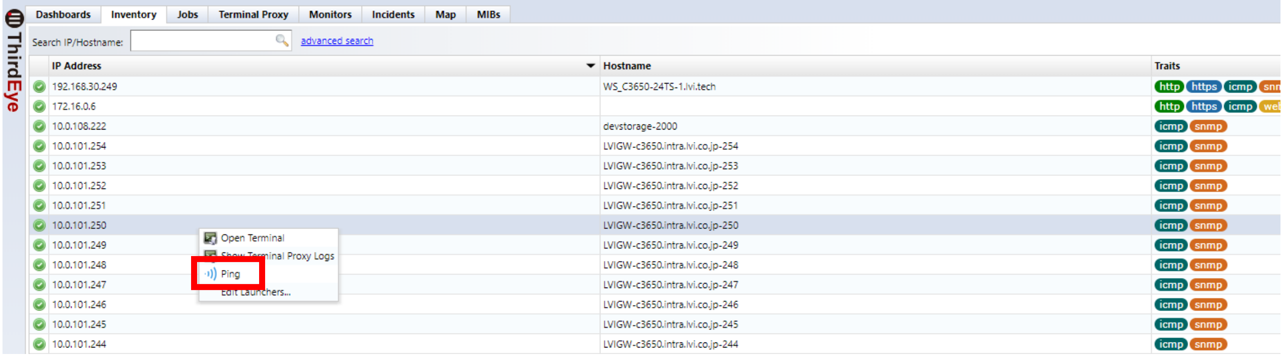
Demo20190905.intra.lvi.co.jp - 10.0.0.250 - Terminal Log   2019/09/18 15:09:58 - 15:10:28 (30 seconds)

```



User Access Verification

Username:
Username: lvi
Password:
Demo20190905>en
Password:
Demo20190905#sh ver
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 09-Feb-16 02:36 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

Demo20190905 uptime is 8 weeks, 4 hours, 3 minutes
System returned to ROM by reload at 02:26:09 UTC Wed Jul 24 2019
System image file is "usbflash0:c1900-universalk9-mz.SPA.154-3.M5.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

```

You can save the session data as a text file by clicking (Export)] in the upper right of the log screen. The file name will be “netLD-termlogs YYYY-MM-DD.zip” and will be collected in the ZIP file format. “YYYY-MM-DD” represents the date of saving.

6.4 Real time Ping

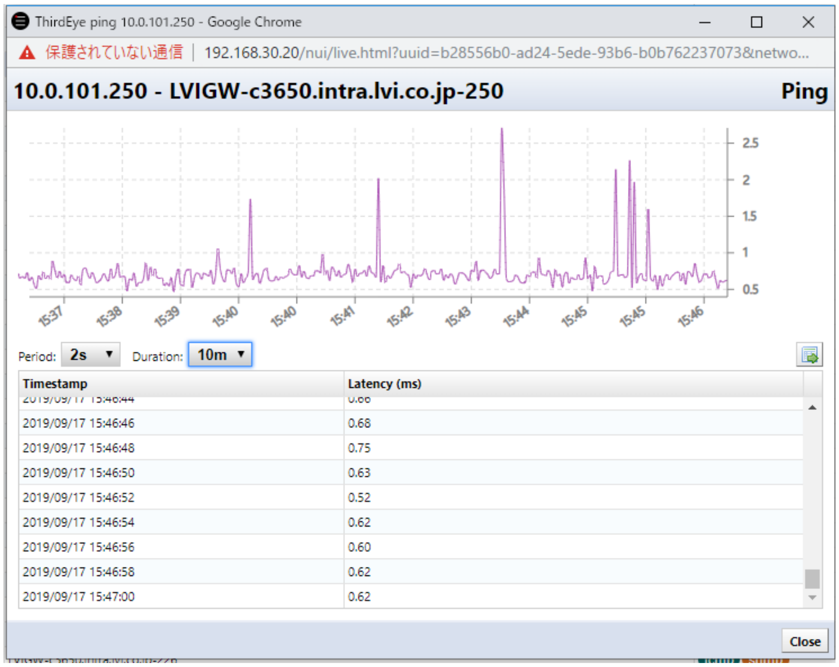
From the device list or map, you can easily ping a monitored device from the right-click menu. The transmission interval is 2 seconds at startup but can be changed from the screen displayed after Ping.



Search IP/Hostname: advanced search

IP Address	Hostname	Traits
192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snı
172.16.0.6		http https icmp wel
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp

When you click Ping, the following screen is displayed, and the Ping result is displayed.



ThirdEye ping 10.0.101.250 - Google Chrome

保護されていない通信 | 192.168.30.20/nui/live.html?uuid=b28556b0-ad24-5ede-93b6-b0b762237073&netwo...

10.0.101.250 - LVIGW-c3650.intra.lvi.co.jp-250 **Ping**

Period: 2s Duration: 10m

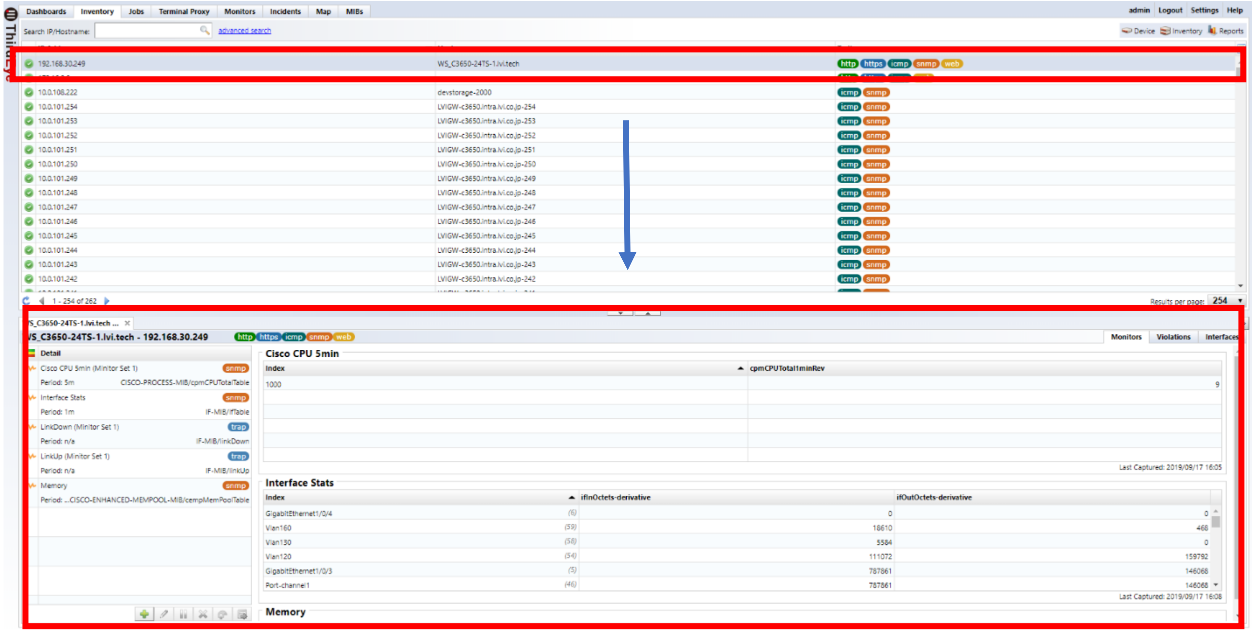
Timestamp	Latency (ms)
2019/09/17 15:46:44	0.66
2019/09/17 15:46:46	0.68
2019/09/17 15:46:48	0.75
2019/09/17 15:46:50	0.63
2019/09/17 15:46:52	0.52
2019/09/17 15:46:54	0.62
2019/09/17 15:46:56	0.60
2019/09/17 15:46:58	0.62
2019/09/17 15:47:00	0.62

Click [(Export)] on the right side of the screen to export the Ping result to a CSV file.

6.5 Checking the Up / Down status of the device interface

On the device details screen, you can check the interface status of the device. To use this function, it is necessary to be able to communicate with the monitored device via SNMP.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.



192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

1 - 254 of 262

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Detail	
Cisco CPU 5min (Minitor Set 1)	snmp
Period: 5m	CISCO-PROCESS-MIB/cpmCPUTotalTable
Interface Stats	snmp
Period: 1m	IF-MIB/ifTable
LinkDown (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkDown
LinkUp (Minitor Set 1)	trap
Period: n/a	IF-MIB/linkUp
Memory	snmp
Period: ...CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable	

Cisco CPU 5min

Index	cpmCPUTotal1minRev
1000	9

Last Captured: 2019/09/17 16:05

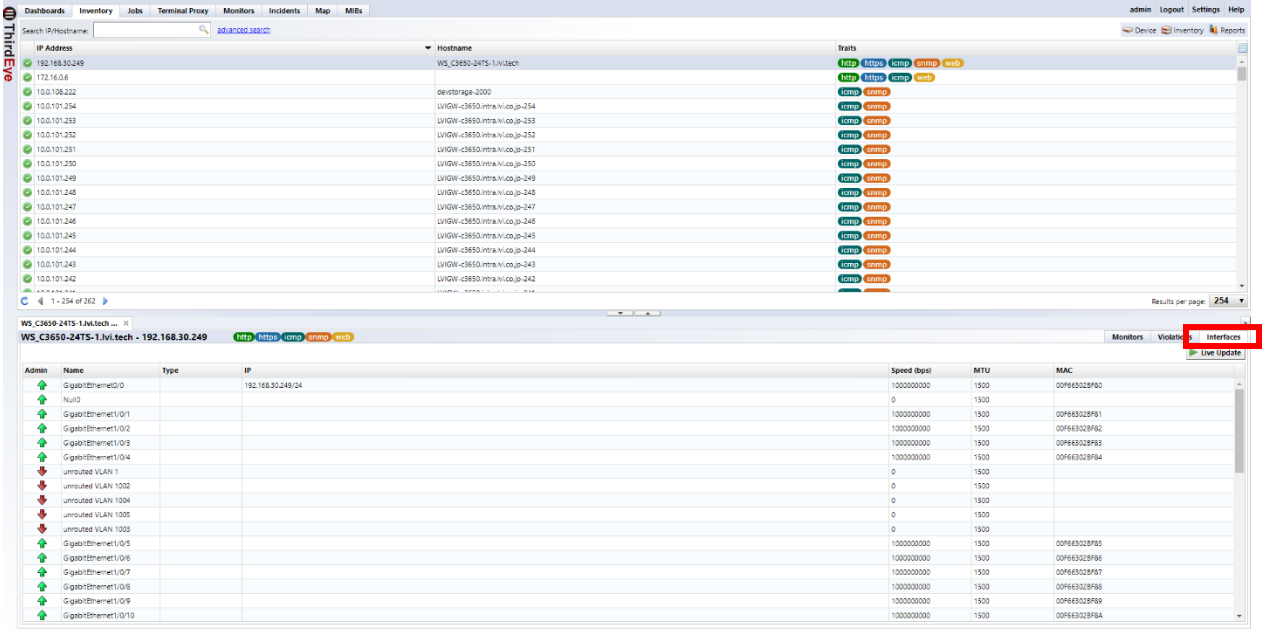
Interface Stats

Index		ifInOctets-derivative	ifOutOctets-derivative
GigabitEthernet1/0/4	(6)	0	0
Vlan160	(59)	18610	468
Vlan130	(58)	5584	0
Vlan120	(54)	111072	159792
GigabitEthernet1/0/3	(5)	787861	146068
Port-channel1	(46)	787861	146068

Last Captured: 2019/09/17 16:08

Memory

2. Click the [Interfaces] tab in the device details screen.



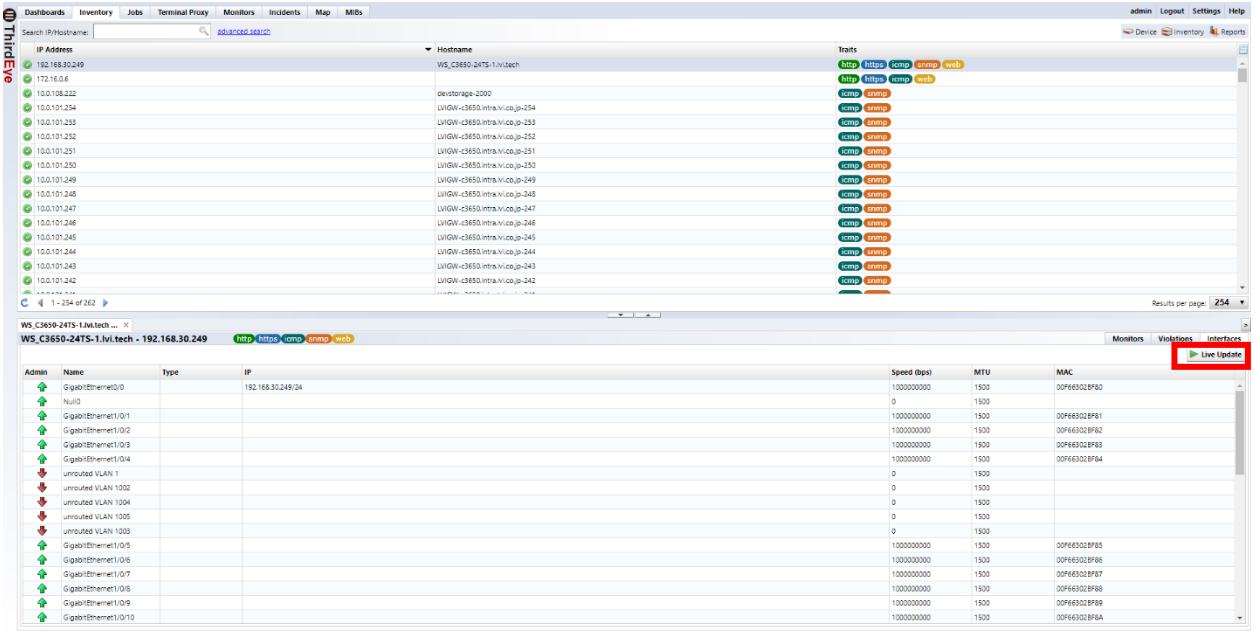
IP Address	Hostname	Traits
192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
172.16.0.6		http https icmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

1 - 254 of 262

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Admin	Name	Type	IP	Speed (bps)	MTU	MAC
↑	GigabitEthernet0/0		192.168.30.249/24	1000000000	1500	00F66302BF80
↑	Null0			0	1500	
↑	GigabitEthernet1/0/1			1000000000	1500	00F66302BF81
↑	GigabitEthernet1/0/2			1000000000	1500	00F66302BF82
↑	GigabitEthernet1/0/3			1000000000	1500	00F66302BF83
↑	GigabitEthernet1/0/4			1000000000	1500	00F66302BF84
↓	unrouted VLAN 1			0	1500	
↓	unrouted VLAN 1002			0	1500	
↓	unrouted VLAN 1004			0	1500	
↓	unrouted VLAN 1005			0	1500	
↓	unrouted VLAN 1003			0	1500	
↑	GigabitEthernet1/0/5			1000000000	1500	00F66302BF85
↑	GigabitEthernet1/0/6			1000000000	1500	00F66302BF86
↑	GigabitEthernet1/0/7			1000000000	1500	00F66302BF87
↑	GigabitEthernet1/0/8			1000000000	1500	00F66302BF88
↑	GigabitEthernet1/0/9			1000000000	1500	00F66302BF89
↑	GigabitEthernet1/0/10			1000000000	1500	00F66302BF8A

3. Click [Live Update].



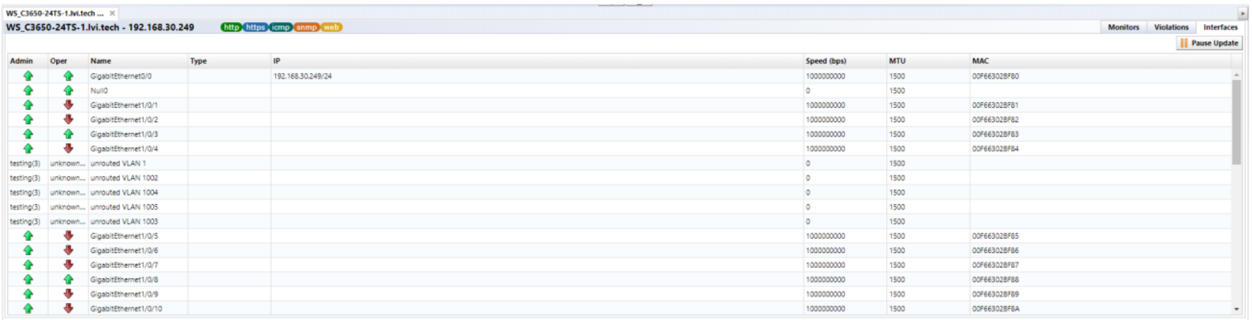
IP Address	Hostname	Traits
192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
172.16.0.6		http https icmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.254	LVIGW-c3650.intra.lvi.co.jp-254	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

1 - 254 of 262

WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

Admin	Name	Type	IP	Speed (bps)	MTU	MAC
⬆	GigabitEthernet0/0		192.168.30.249/24	1000000000	1500	00F66302BF80
⬆	Null0			0	1500	
⬆	GigabitEthernet1/0/1			1000000000	1500	00F66302BF81
⬆	GigabitEthernet1/0/2			1000000000	1500	00F66302BF82
⬆	GigabitEthernet1/0/3			1000000000	1500	00F66302BF83
⬆	GigabitEthernet1/0/4			1000000000	1500	00F66302BF84
⬇	unrouted VLAN 1			0	1500	
⬇	unrouted VLAN 1002			0	1500	
⬇	unrouted VLAN 1004			0	1500	
⬇	unrouted VLAN 1005			0	1500	
⬇	unrouted VLAN 1003			0	1500	
⬆	GigabitEthernet1/0/5			1000000000	1500	00F66302BF85
⬆	GigabitEthernet1/0/6			1000000000	1500	00F66302BF86
⬆	GigabitEthernet1/0/7			1000000000	1500	00F66302BF87
⬆	GigabitEthernet1/0/8			1000000000	1500	00F66302BF88
⬆	GigabitEthernet1/0/9			1000000000	1500	00F66302BF89
⬆	GigabitEthernet1/0/10			1000000000	1500	00F66302BF8A

4. After clicking Automatic Update, you can periodically acquire the interface information on the monitored device and check the current status.



WS_C3650-24TS-1.lvi.tech - 192.168.30.249 http https icmp snmp web

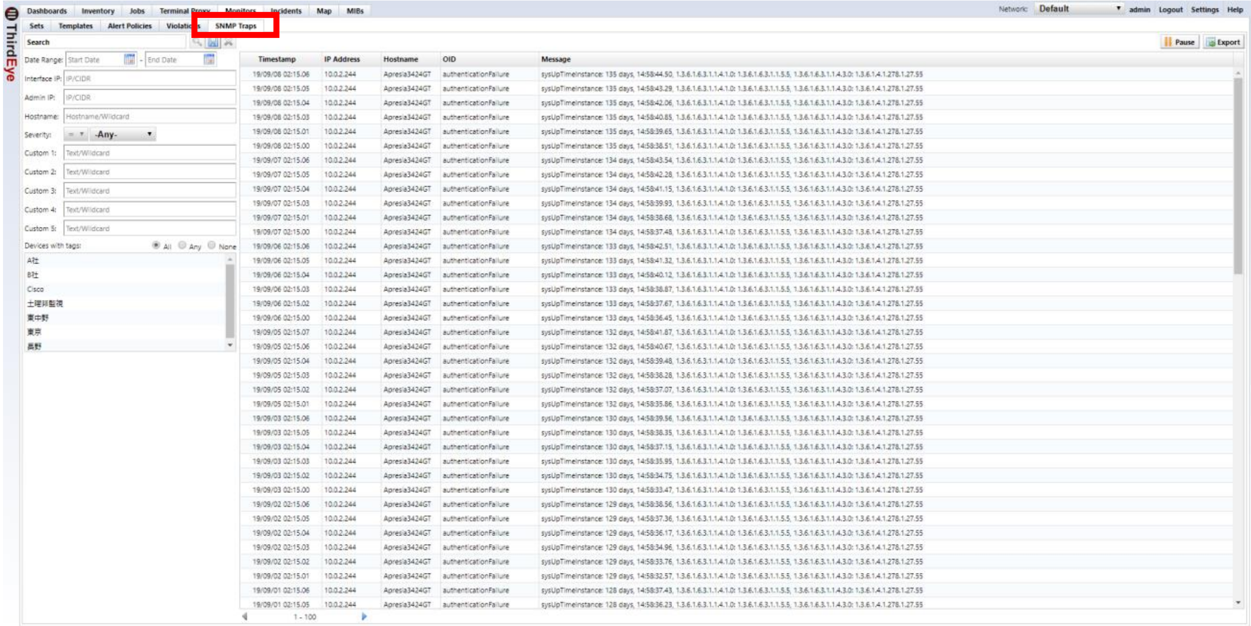
Admin	Oper	Name	Type	IP	Speed (bps)	MTU	MAC
⬆	⬆	GigabitEthernet0/0		192.168.30.249/24	1000000000	1500	00F66302BF80
⬆	⬆	Null0			0	1500	
⬆	⬇	GigabitEthernet1/0/1			1000000000	1500	00F66302BF81
⬆	⬇	GigabitEthernet1/0/2			1000000000	1500	00F66302BF82
⬆	⬆	GigabitEthernet1/0/3			1000000000	1500	00F66302BF83
⬆	⬇	GigabitEthernet1/0/4			1000000000	1500	00F66302BF84
testing(3)	unknown...	unrouted VLAN 1			0	1500	
testing(3)	unknown...	unrouted VLAN 1002			0	1500	
testing(3)	unknown...	unrouted VLAN 1004			0	1500	
testing(3)	unknown...	unrouted VLAN 1005			0	1500	
testing(3)	unknown...	unrouted VLAN 1003			0	1500	
⬆	⬇	GigabitEthernet1/0/5			1000000000	1500	00F66302BF85
⬆	⬇	GigabitEthernet1/0/6			1000000000	1500	00F66302BF86
⬆	⬇	GigabitEthernet1/0/7			1000000000	1500	00F66302BF87
⬆	⬆	GigabitEthernet1/0/8			1000000000	1500	00F66302BF88
⬆	⬇	GigabitEthernet1/0/9			1000000000	1500	00F66302BF89
⬆	⬇	GigabitEthernet1/0/10			1000000000	1500	00F66302BF8A

To stop, close the device details screen or click [Pause Update]

6.6 Checking SNMP traps that are not registered for monitoring

When a trap that is not registered as an SNMP trap monitor is received, it can be confirmed from the [Monitors] tab → [SNMP Traps] tab. You can also display traps for a specific device using the search function.

* The SNMP trap displayed here must be registered in the device as a monitored device.



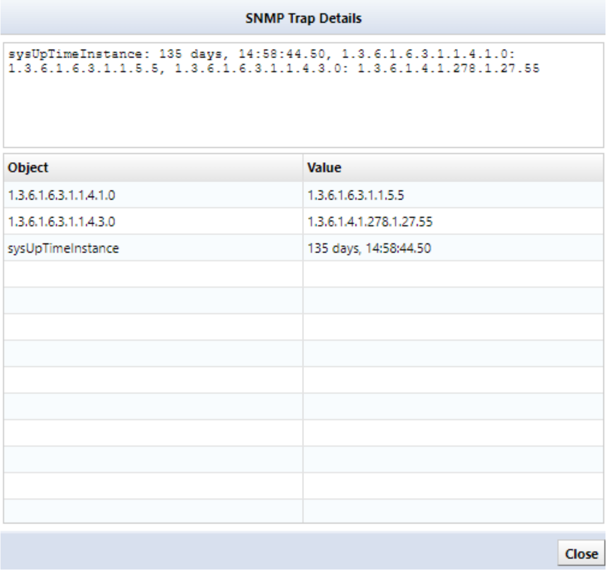
Date Range: Start Date - End Date
Interface IP: IP/CIDR
Admin IP: IP/CIDR
Hostname: Hostname/Wildcard
Severity: = -Any-
Custom 1: Text/Wildcard
Custom 2: Text/Wildcard
Custom 3: Text/Wildcard
Custom 4: Text/Wildcard
Custom 5: Text/Wildcard
Devices with tags: ● All ○ Any ○ None

A社
B社
Cisco
土曜日監視
東中野
東京
長野

Timestamp	IP Address	Hostname	OID	Message
19/09/08 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:44.50, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/08 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:43.29, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/08 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:42.06, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/08 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:40.85, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/08 02:15.01	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:39.65, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/08 02:15.00	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 135 days, 14:58:38.51, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:43.54, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:42.28, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:41.15, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:39.93, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.01	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:38.68, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/07 02:15.00	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 134 days, 14:58:37.48, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:42.51, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:41.32, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:40.12, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:38.87, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.02	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:37.67, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/06 02:15.00	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 133 days, 14:58:36.45, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.07	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:41.87, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:40.67, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:39.48, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:38.28, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.02	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:37.07, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/05 02:15.01	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 132 days, 14:58:35.86, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:39.56, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:38.35, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:37.15, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:35.95, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.02	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:34.75, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/03 02:15.00	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 130 days, 14:58:33.47, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:38.56, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:37.36, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.04	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:36.17, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.03	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:34.96, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.02	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:33.76, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/02 02:15.01	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 129 days, 14:58:32.57, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/01 02:15.06	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 128 days, 14:58:37.43, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
19/09/01 02:15.05	10.0.2.244	Apresia3424GT	authenticationFailure	sysUpTimeInstance: 128 days, 14:58:36.23, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55

You can check the details of the trap by double-clicking.

The displayed traps can be exported to a CSV file from the [Export] button.



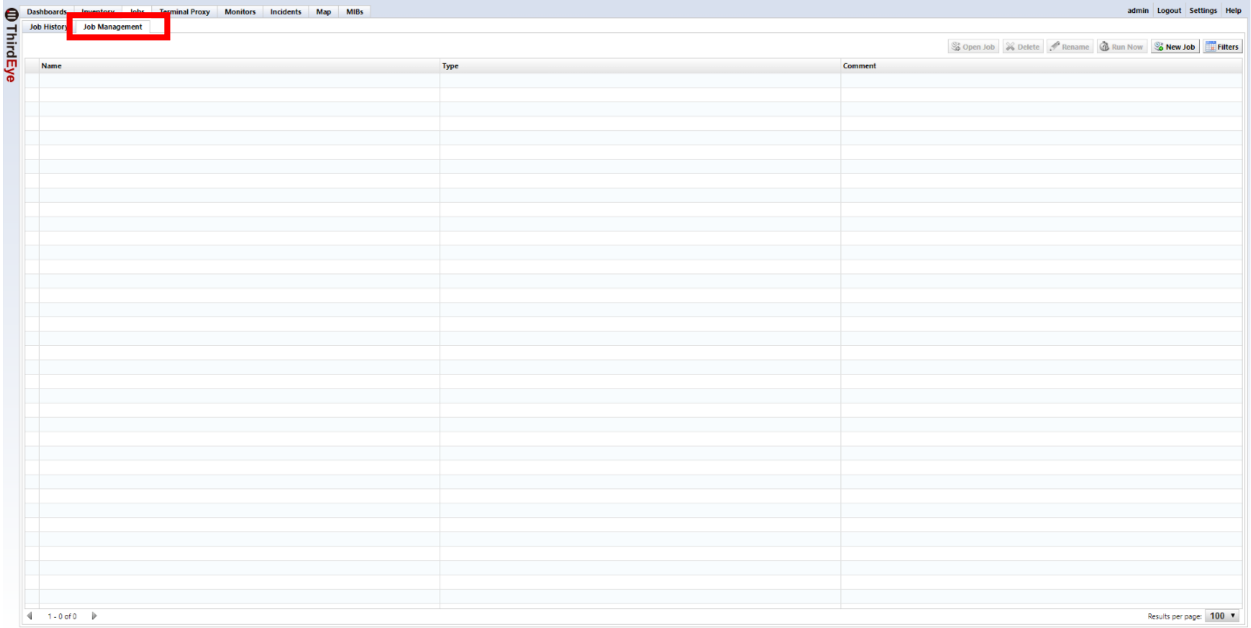
```
sysUpTimeInstance: 135 days, 14:58:44.50, 1.3.6.1.6.3.1.1.4.1.0:
1.3.6.1.6.3.1.1.5.5, 1.3.6.1.6.3.1.1.4.3.0: 1.3.6.1.4.1.278.1.27.55
```

Object	Value
1.3.6.1.6.3.1.1.4.1.0	1.3.6.1.6.3.1.1.5.5
1.3.6.1.6.3.1.1.4.3.0	1.3.6.1.4.1.278.1.27.55
sysUpTimeInstance	135 days, 14:58:44.50

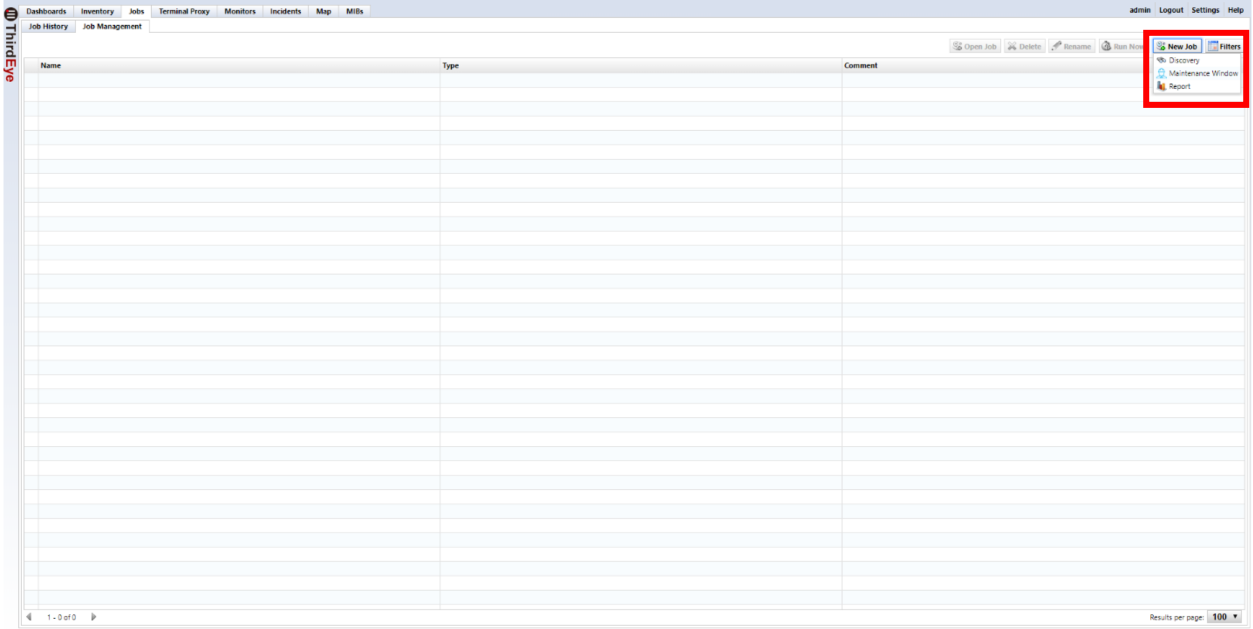
6.7 Stop monitoring temporarily

Use the job function to temporarily put the monitored device into the unmonitored state.

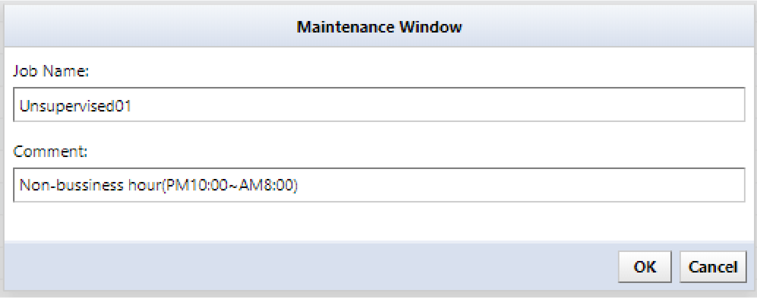
1. Click the [Jobs] tab → [Job Management].



2. Click [New Job] → [Maintenance Window].



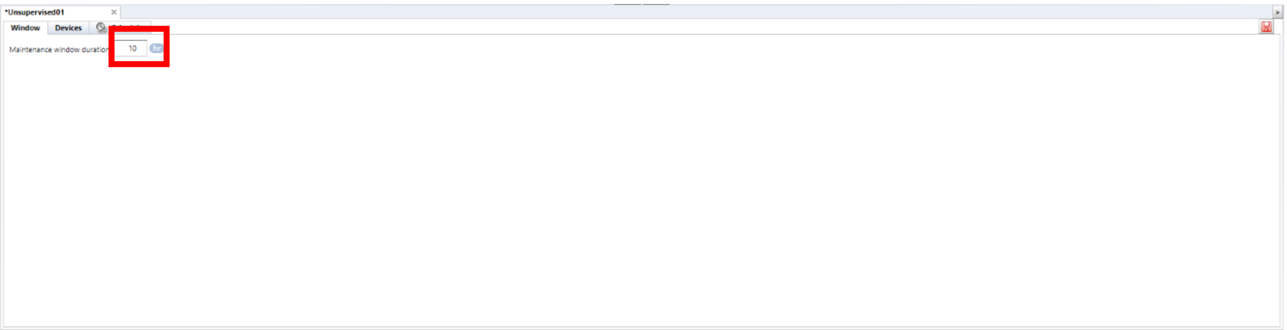
3. Enter the job name and comment and click [OK].



Job Name: Unsupervised01

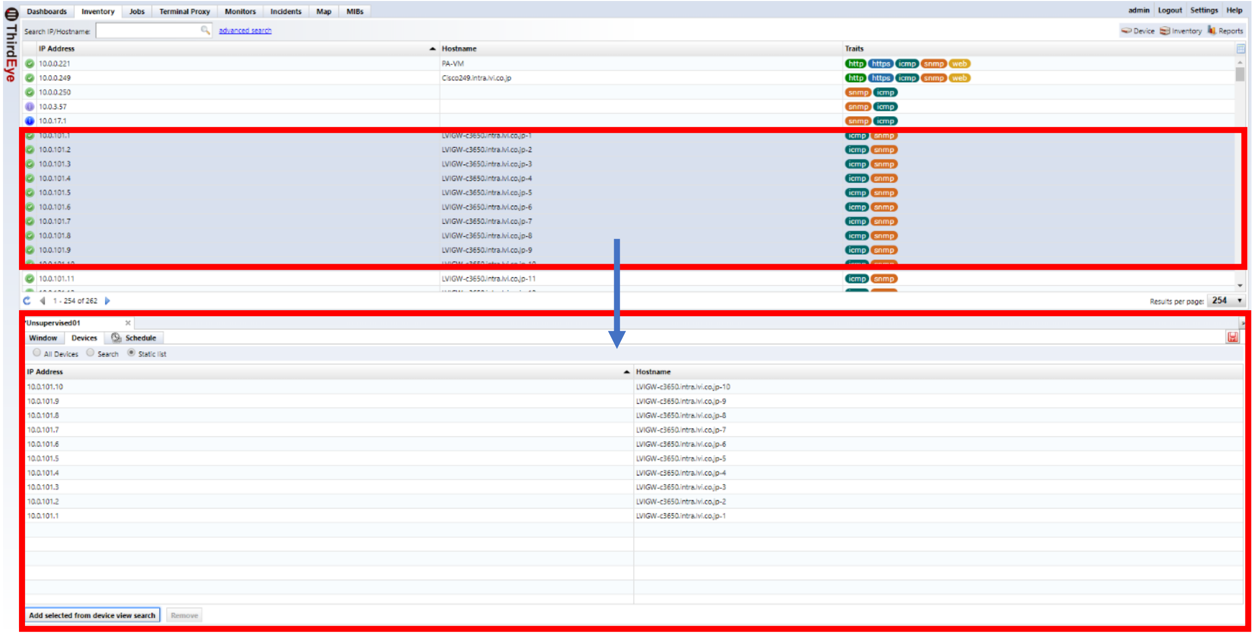
Comment: Non-bussiness hour(PM10:00~AM8:00)

4. Click the Period tab and set the period to be unmonitored.



Maintenance window duration: 10 hr

5. Click the Device tab and add a device to be monitored.

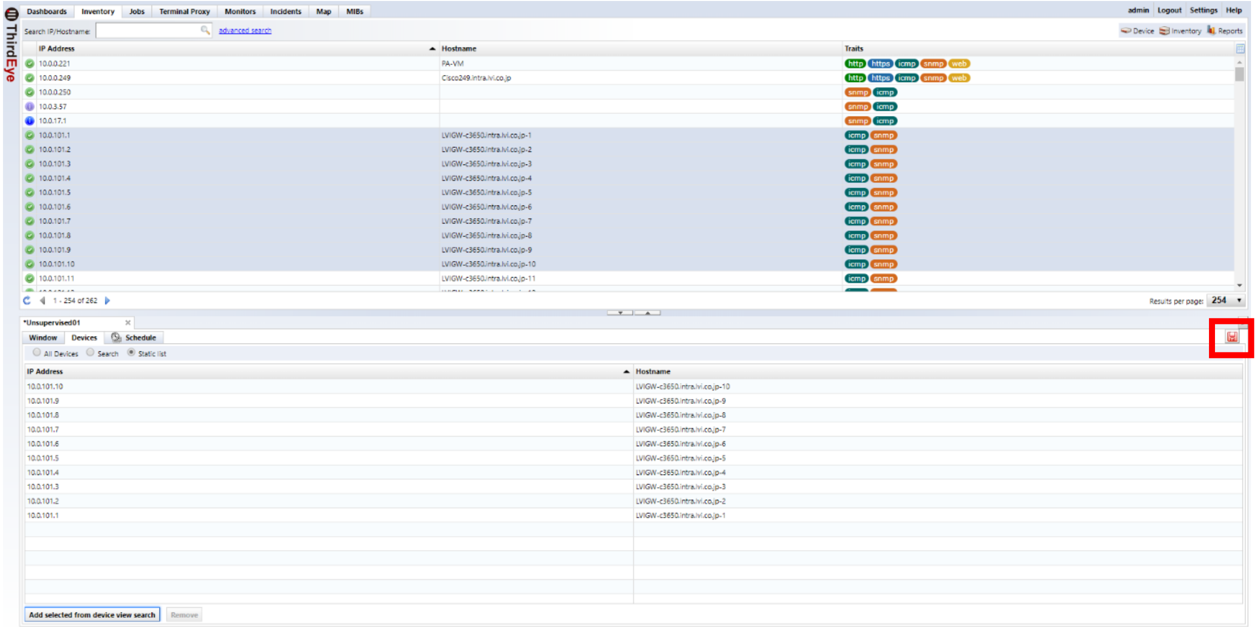


IP Address	Hostname	Traits
10.0.0.221	PA-VM	http https icmp snmp web
10.0.0.249	Cisco249.intra.lvi.co.jp	http https icmp snmp web
10.0.0.250		snmp icmp
10.0.3.57		snmp icmp
10.0.17.1		snmp icmp
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp

○ All Devices ○ Search ● Static list

IP Address	Hostname
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1

6. Click [Save].



IP Address	Hostname	Traits
10.0.0.221	PA-VM	http https icmp snmp web
10.0.0.249	Cisco249.intra.lvi.co.jp	http https icmp snmp web
10.0.0.250		snmp icmp
10.0.3.57		snmp icmp
10.0.17.1		snmp icmp
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp

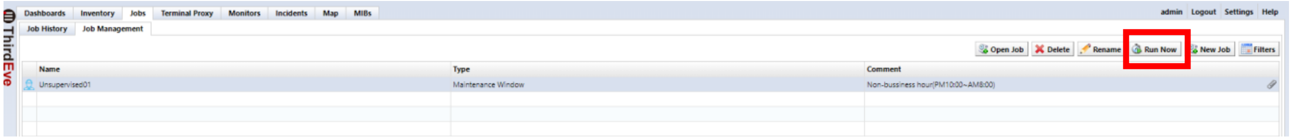
1 - 254 of 262

*Unsupervised01

○ All Devices ○ Search ● Static list

IP Address	Hostname
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1

7. Click [Run Now].



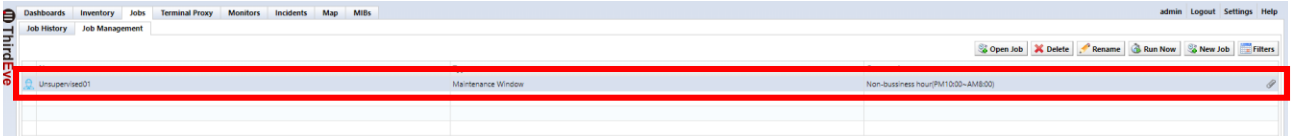
Name	Type	Comment
Unsupervised01	Maintenance Window	Non-bussiness hour(PM10:00~AM8:00)

That's all for the operation. After clicking [Run Now], it will be unmonitored for the time specified on the Period tab. Refer to "6.8 Temporarily Stop Monitoring Using a Schedule" when executing on a schedule.

6.8 Stop monitoring temporarily using a schedule

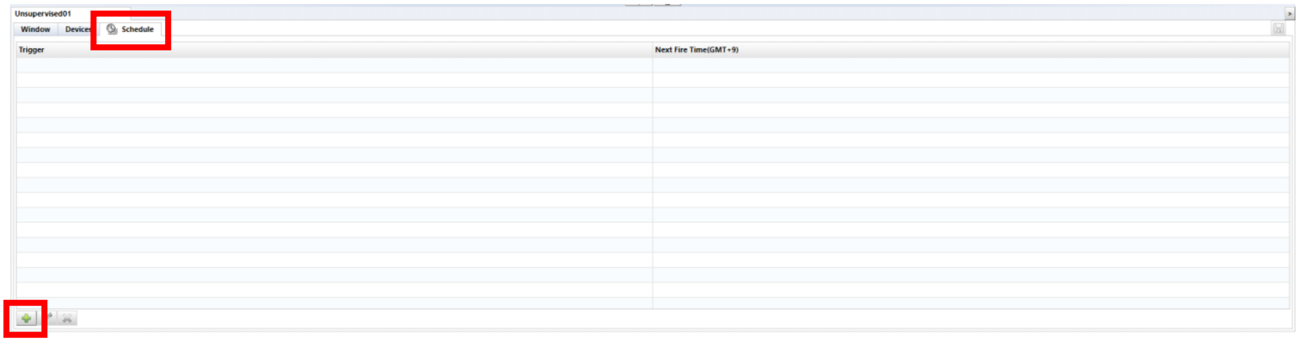
Runs non-monitoring on a schedule. A non-monitoring job is executed at a specified date and time and can be put into a non-monitoring state for a specified period. Here, set the schedule for the non-monitoring job set in 6.10.

1. Double-click the job to set the schedule or click [Open Job].



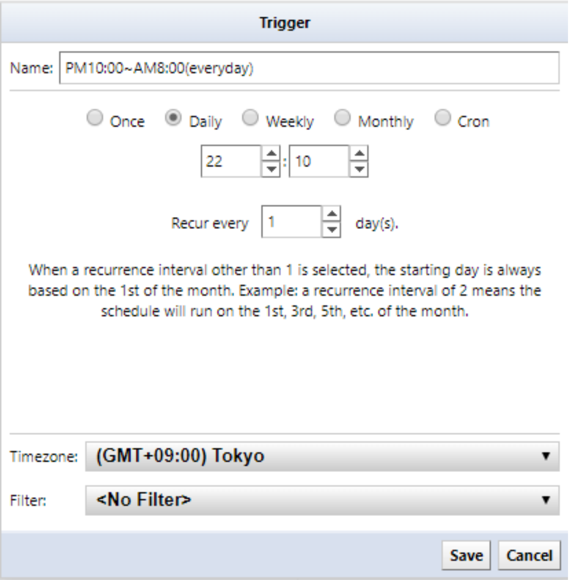
Unsupervised01	Maintenance Window	Non-bussiness hour(PM10:00~AM8:00)

2. Click the Schedule tab and click [Add].



Trigger	Next Fire Time(GMT+9)

3. Specify a name and execution schedule and click [Save].



Name: PM10:00~AM8:00(everyday)

○ Once ● Daily ○ Weekly ○ Monthly ○ Cron

22 : 10

Recur every 1 day(s).

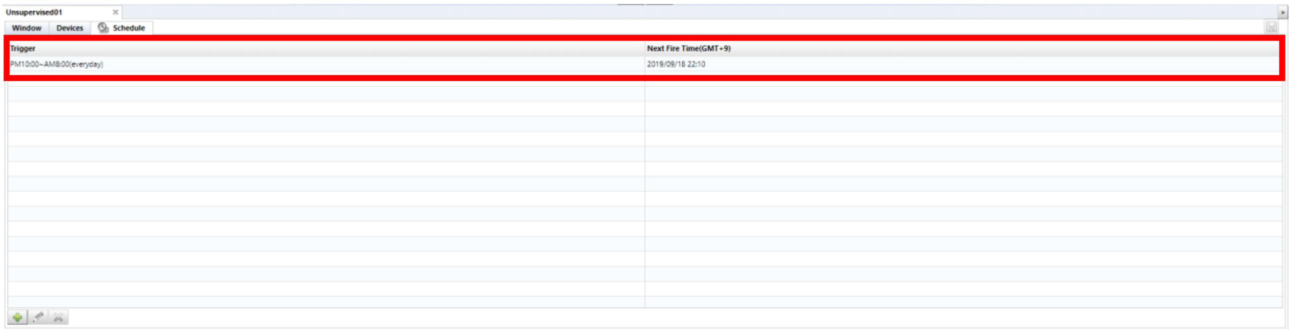
When a recurrence interval other than 1 is selected, the starting day is always based on the 1st of the month. Example: a recurrence interval of 2 means the schedule will run on the 1st, 3rd, 5th, etc. of the month.

Timezone: (GMT+09:00) Tokyo

Filter: <No Filter>

Description	Explanation
Schedule	Select one of the following five execution schedules. Once ... Execute once at the time and date set for the time Daily: Run every n days (Starting on the 1st of the current month) Weekly: Run on a specific day of the week Monthly: Run every specified month Cron ... Executes at the date and time specified in coulomb format
Time zone	Specify the time zone.
Filter	Select the schedule filter registered in "Filter settings". Timing that matches this filter is removed from the trigger. For details, see “Scheduler Filter”.

Click Save to add the schedule. In addition, the date and time will be displayed in “Next Fire Time”.



Trigger	Next Fire Time(GMT+9)
PM10:00~AM8:00(everyday)	2019/09/18 22:10

6.9 Checking the past job history

The job history can be confirmed from the [Jobs] tab → [Job History], and the jobs executed so far are displayed. Jobs can be reported / discovered / unmonitored to see when and who executed them. For report jobs, you can double-click to view a published report.

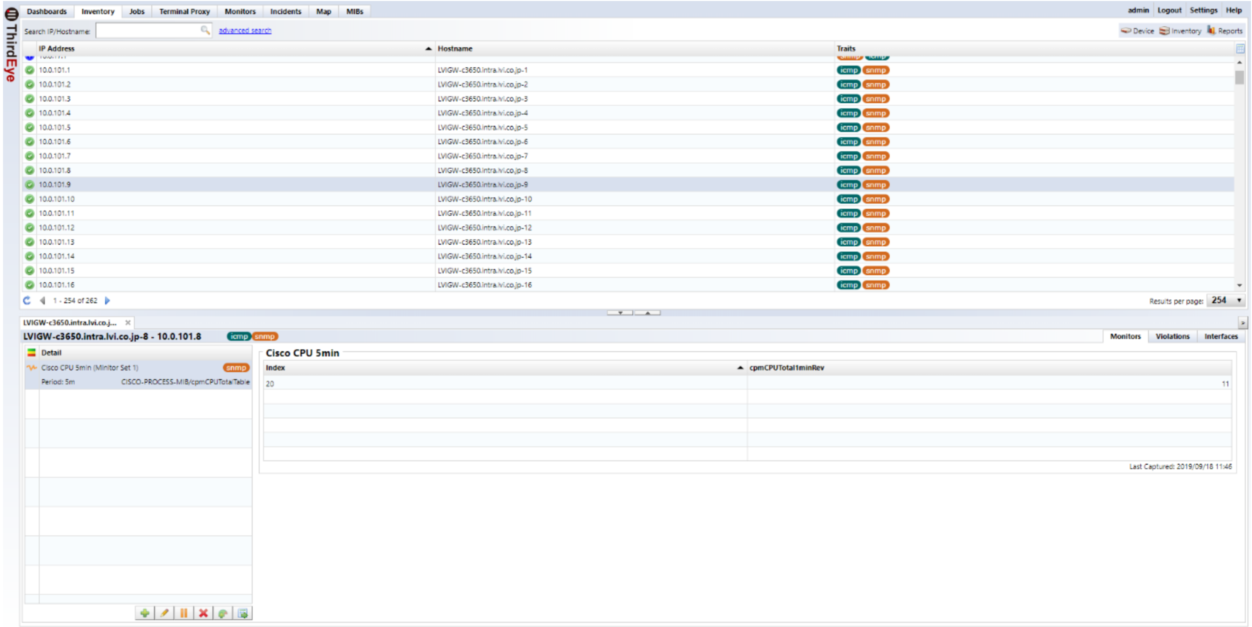
【Column list】

Description	Explanation
Name	Displays the name of the job.
Type	The job type is displayed.
Start time	Displays the date and time when the job was executed.
End time	Displays the end date and time when the job ended.
User	Displays the name of the user who executed the job.

6.10 Canceling monitoring settings

6.10.1 Deleting a monitor

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.



Search IP/Hostname: advanced search

IP Address	Hostname	Traits
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10	icmp snmp
10.0.101.11	LVIGW-c3650.intra.lvi.co.jp-11	icmp snmp
10.0.101.12	LVIGW-c3650.intra.lvi.co.jp-12	icmp snmp
10.0.101.13	LVIGW-c3650.intra.lvi.co.jp-13	icmp snmp
10.0.101.14	LVIGW-c3650.intra.lvi.co.jp-14	icmp snmp
10.0.101.15	LVIGW-c3650.intra.lvi.co.jp-15	icmp snmp
10.0.101.16	LVIGW-c3650.intra.lvi.co.jp-16	icmp snmp

1 - 254 of 262 Results per page: 254

LVIGW-c3650.intra.lvi.co.j...

LVIGW-c3650.intra.lvi.co.jp-8 - 10.0.101.8 icmp snmp

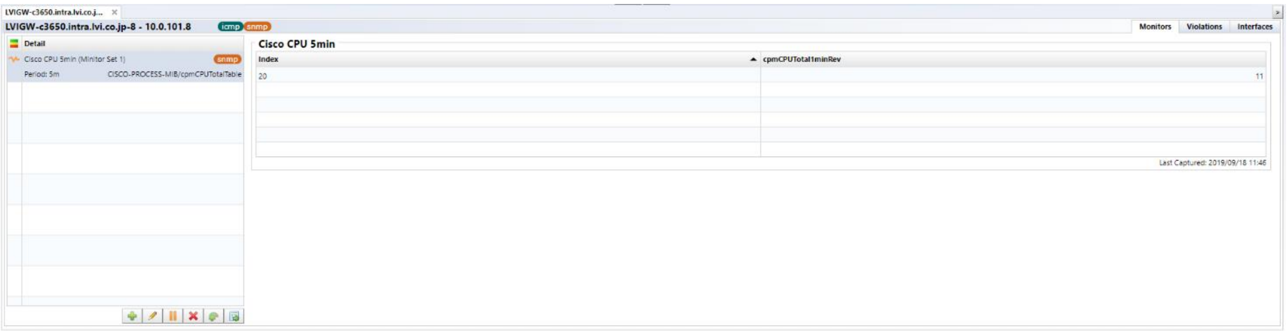
Detail
Cisco CPU 5min (Minitor Set 1) snmp
Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU 5min

Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/18 11:46

2. Select the monitor to be deleted from the monitor details and click [Remove].



LVIGW-c3650.intra.lvi.co.j...

LVIGW-c3650.intra.lvi.co.jp-8 - 10.0.101.8 icmp snmp

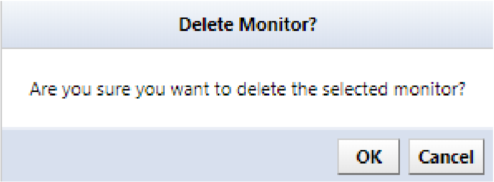
Detail
Cisco CPU 5min (Minitor Set 1) snmp
Period: 5m CISCO-PROCESS-MIB/cpmCPUTotalTable

Cisco CPU 5min

Index	cpmCPUTotal1minRev
20	11

Last Captured: 2019/09/18 11:46

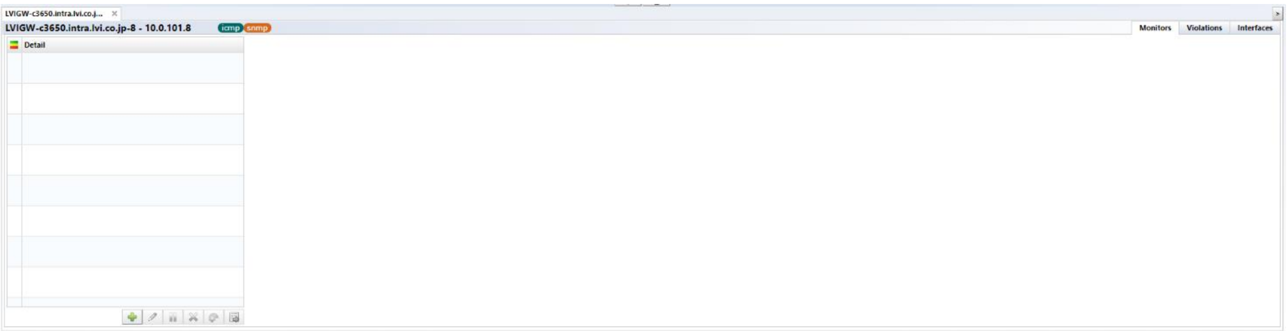
3. Click [Yes] on the confirmation screen.



Delete Monitor?

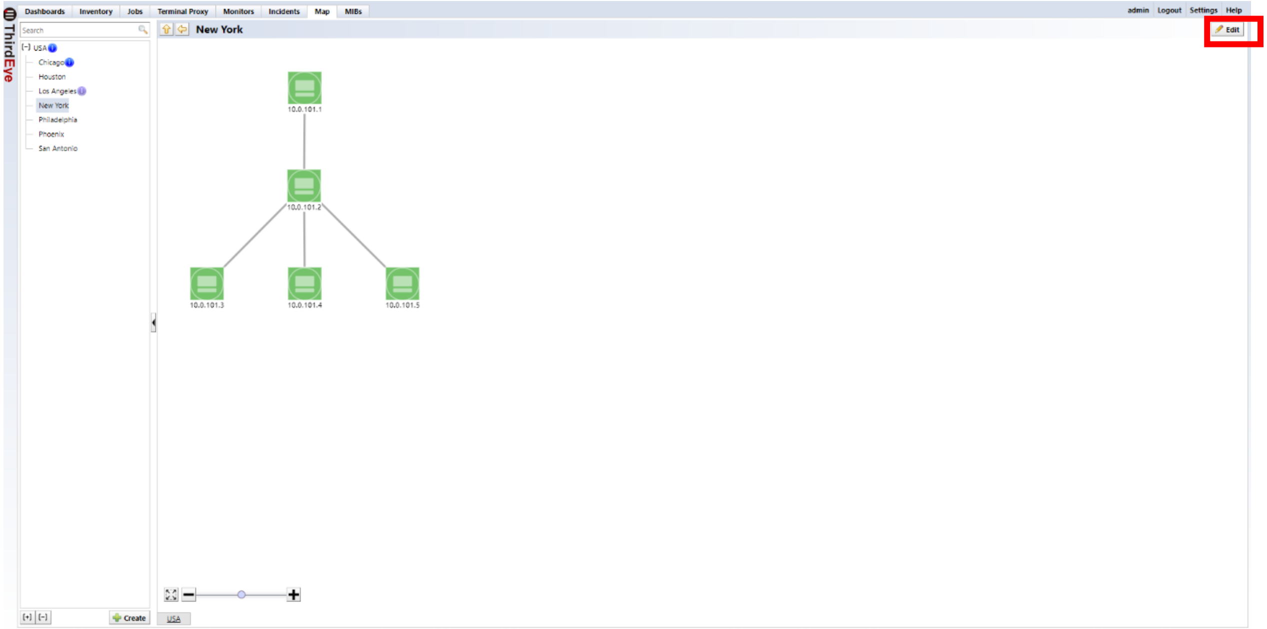
Are you sure you want to delete the selected monitor?

The monitor will be deleted from the monitor details and data will not be collected.

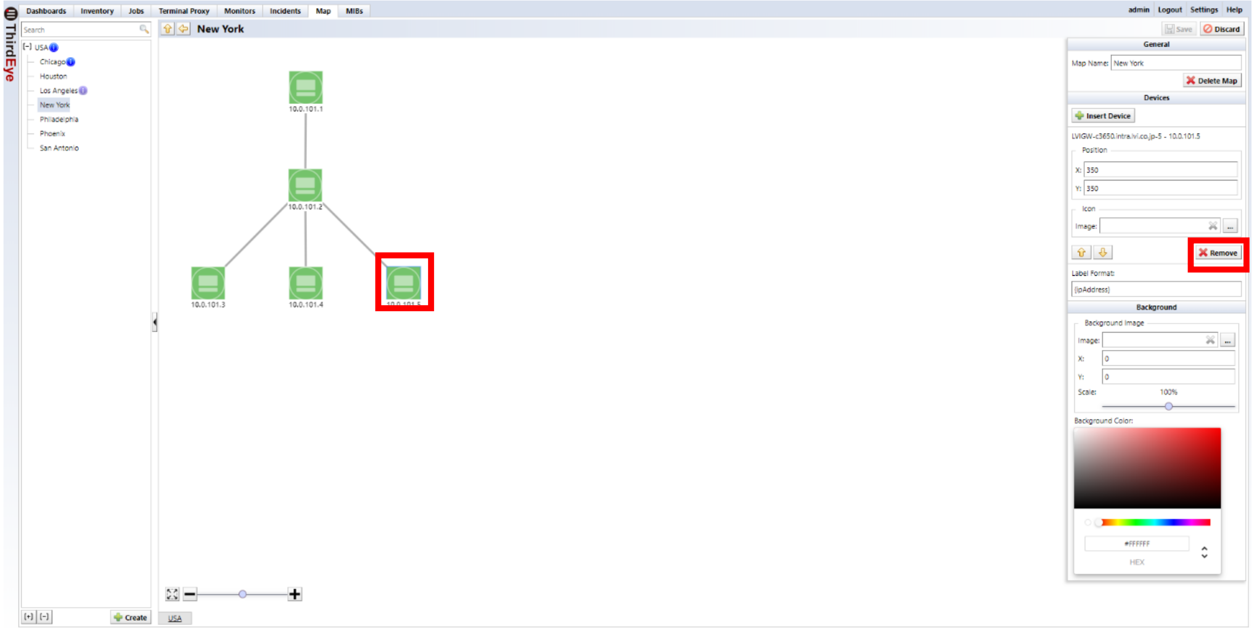

LVIGW-c3650.intra.lvi.co.j...
LVIGW-c3650.intra.lvi.co.jp-8 - 10.0.101.8
icmp
snmp
Monitors
Violations
Interfaces
Detail

6.10.2 Deleting icons (device / map) from the map

1. Double-click the map from the map list on the left side of the screen and click [Edit].



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



Map Name: New York

LVIGW-c3650.intra.lvi.co.jp-5 - 10.0.101.5

X: 350

Y: 350

Label Format: {ipAddress}

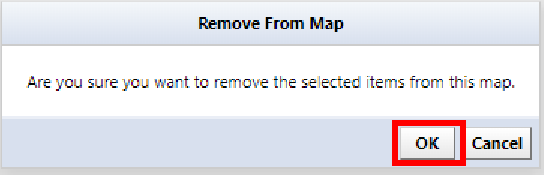
X: 0

Y: 0

Scale: 100%

#FFFFFF

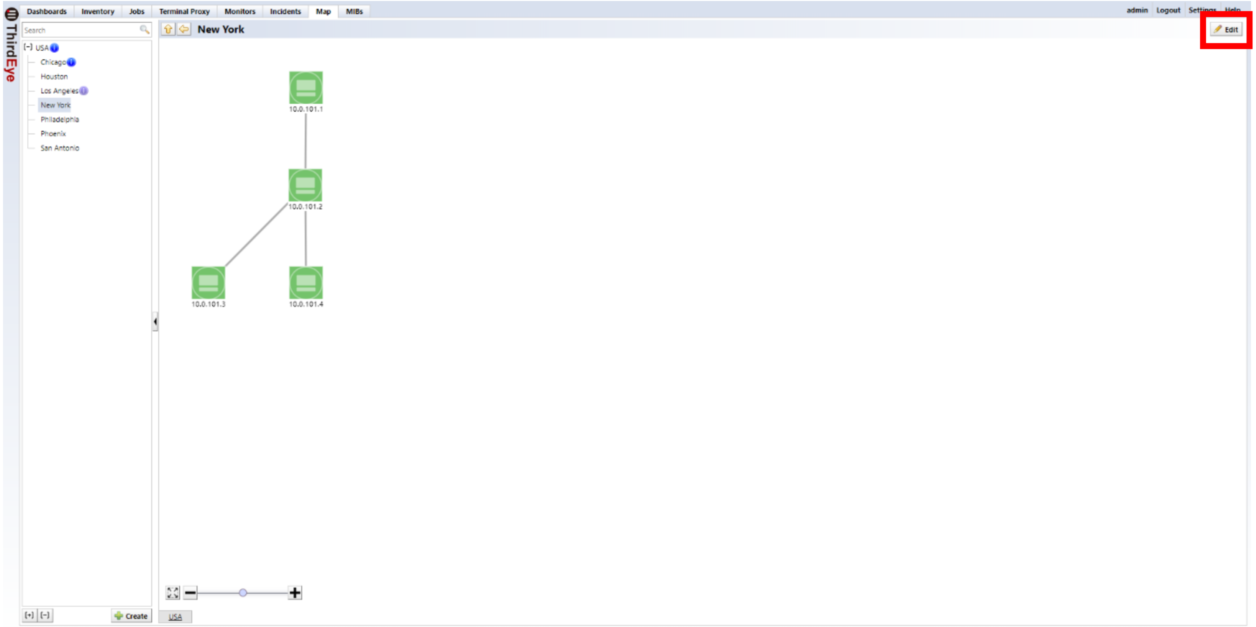
3. A confirmation message is displayed. Click [OK].



Remove From Map

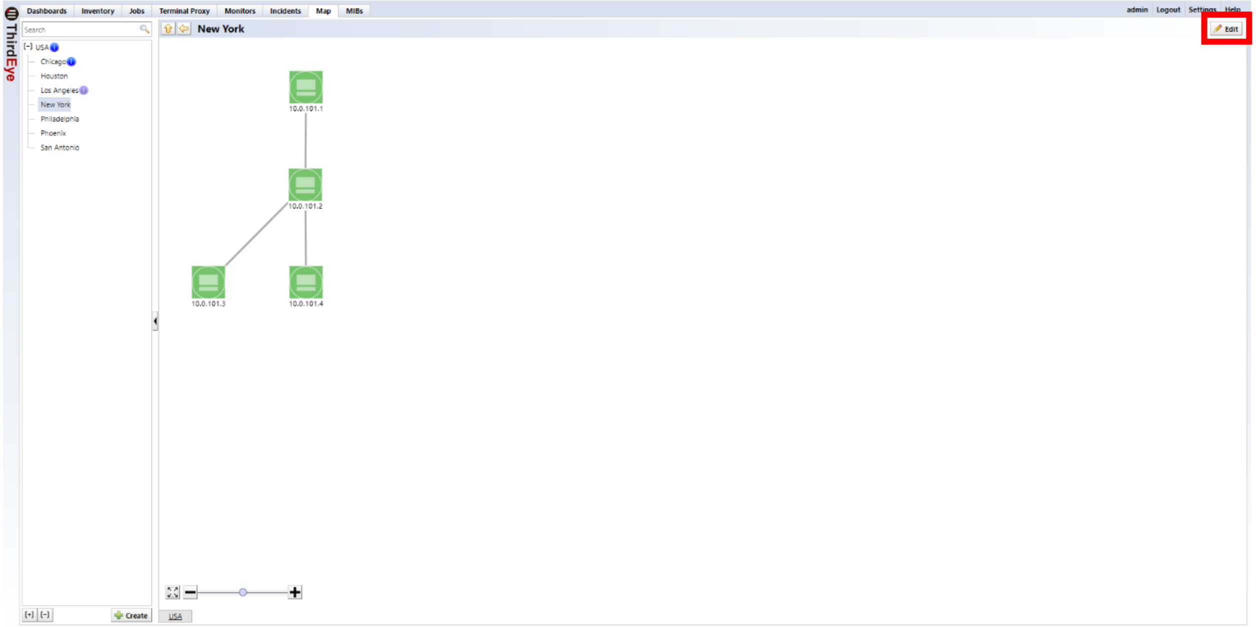
Are you sure you want to remove the selected items from this map.

4. The device is deleted. Click [Save] to complete editing.

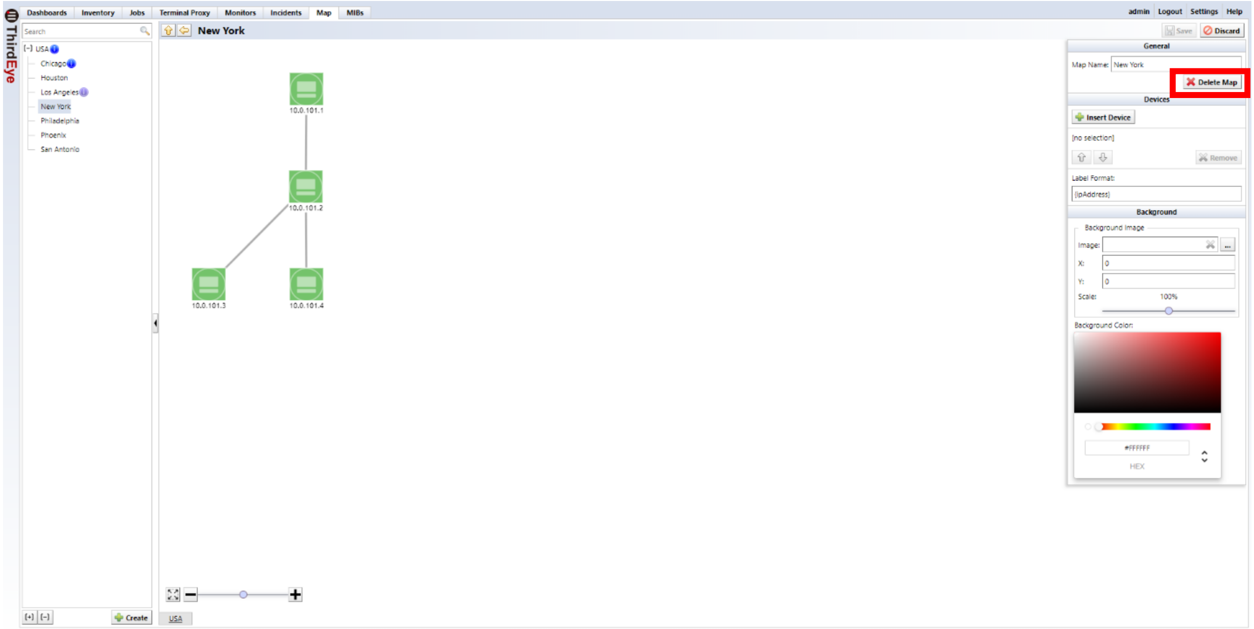


6.10.3 Deleting a map

1. Double-click the map you want to delete and click [Edit].



2. The setting screen is displayed on the right side of the screen. Click [Delete Map].



Map Name: New York

[no selection]

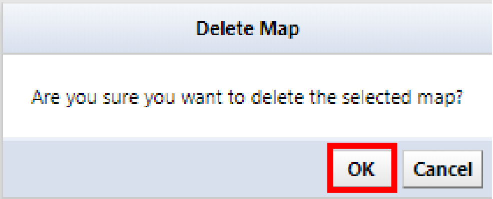
Label Format: {ipAddress}

X: 0

Y: 0

#FFFFFF

3. A confirmation message is displayed. Click [OK].

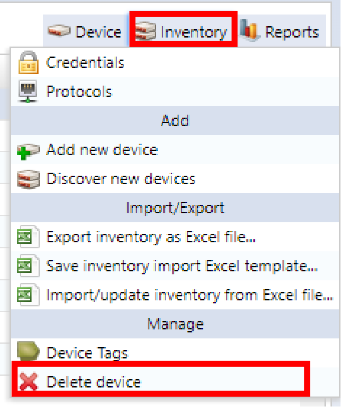


Delete Map

Are you sure you want to delete the selected map?

6.10.4 Deleting a device

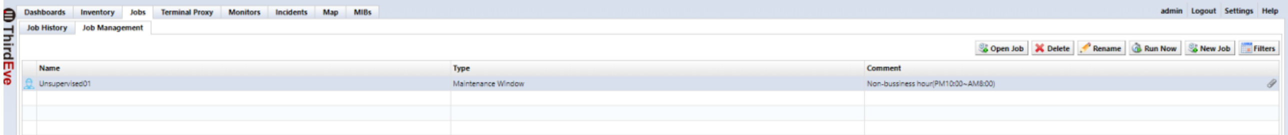
1. In the [Inventory] tab, select the device that you want to delete. * Multiple selection is possible
2. With the device selected, click [Inventory]> [Delete Device].



3. A confirmation message is displayed. Click [Yes].

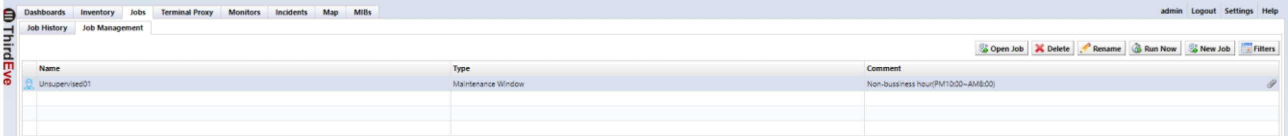
6.10.5 Deleting a job

1. Click the [Jobs] tab → [Job Management].



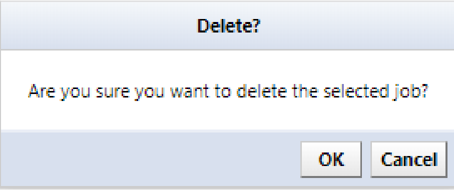
Name	Type	Comment
Unsupervised01	Maintenance Window	Non-bussiness hour(PM10:00~AM8:00)

2. Select the job you want to delete and click [Delete].



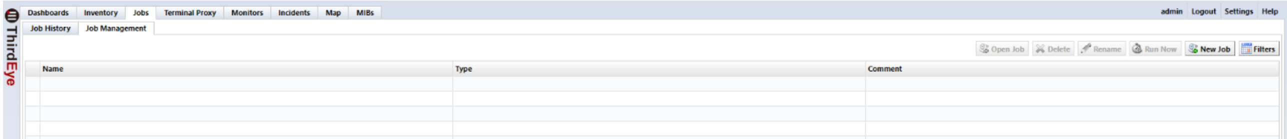
Name	Type	Comment
Unsupervised01	Maintenance Window	Non-bussiness hour(PM10:00~AM8:00)

3. Click [OK] on the confirmation screen.


Delete?

Are you sure you want to delete the selected job?

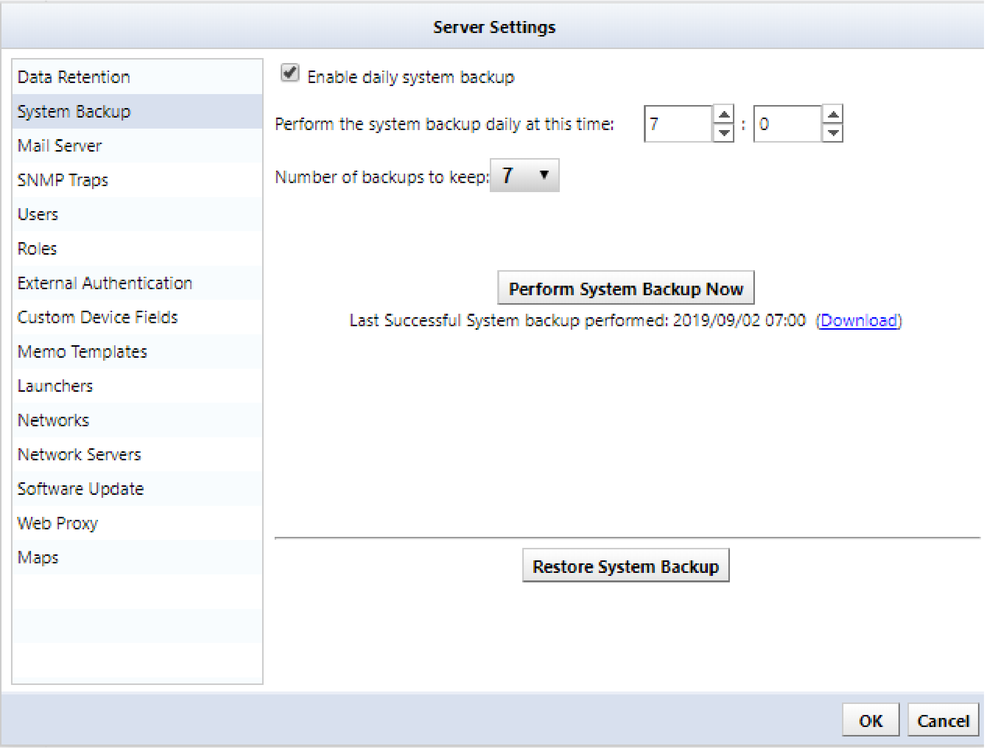
The selected job is deleted from the job management list.



Name	Type	Comment

6.11 Backing up ThirdEye configuration information

In system backup, the settings of ThirdEye are backed up. The acquired system backup file can be restored from [Restore System Backup].



☑ Enable daily system backup

Perform the system backup daily at this time: 7 : 0

Number of backups to keep: 7

Last Successful System backup performed: 2019/09/02 07:00 (Download)

Description	Explanation
Enable daily system backup	Enable daily system backup. 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 of daily system backup. (Initial value: 7:00)
Number of backups to keep	Specify the number of system backup generations maintained by the ThirdEye server from the following. (Initial value: 7) "7", "14", "30"
Perform System Backup Now	Perform a system backup manually.
Download	The backup file at the time of the last system backup can be downloaded. The file name will be "backup_YYYY-MM-DD ***. Zip" and will be collected in the ZIP file format. * The file name "YYYY-MM-DD" represents the Coordinated Universal Time (UTC) date.
Restore System Backup	Restore the system backup. * Select the backup file in the ZIP file format.

7. Advanced Settings

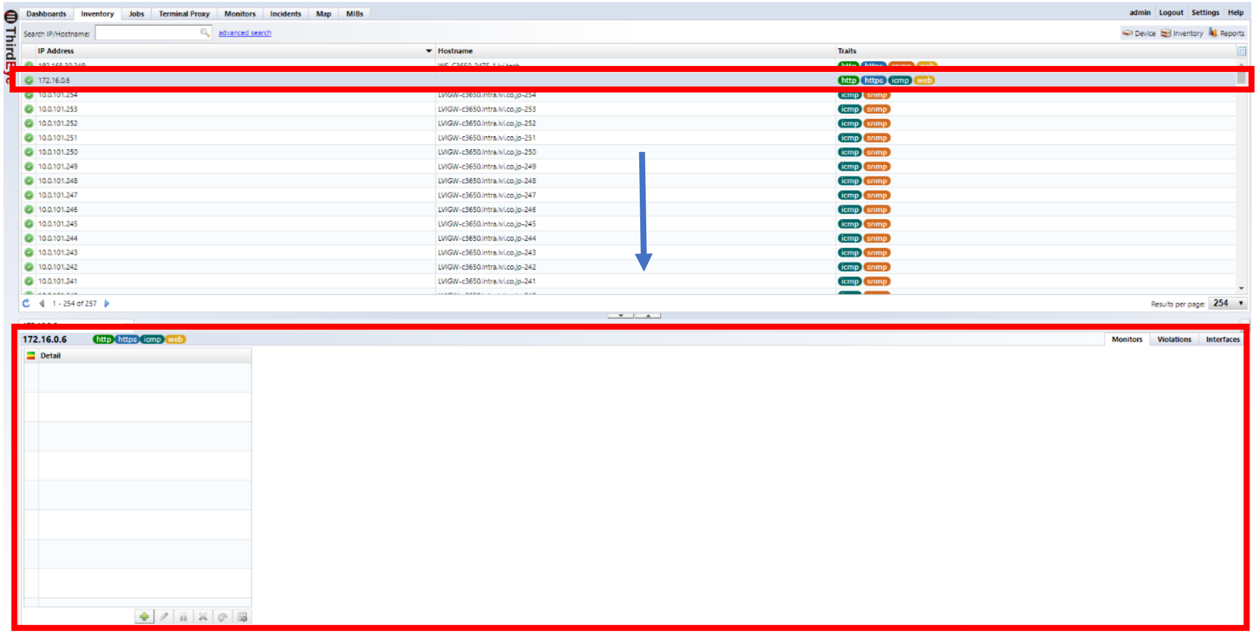
This section introduces monitoring settings that are more detailed than backup, global settings,

7.1 Setting various monitoring settings

7.1.1 Monitoring a website

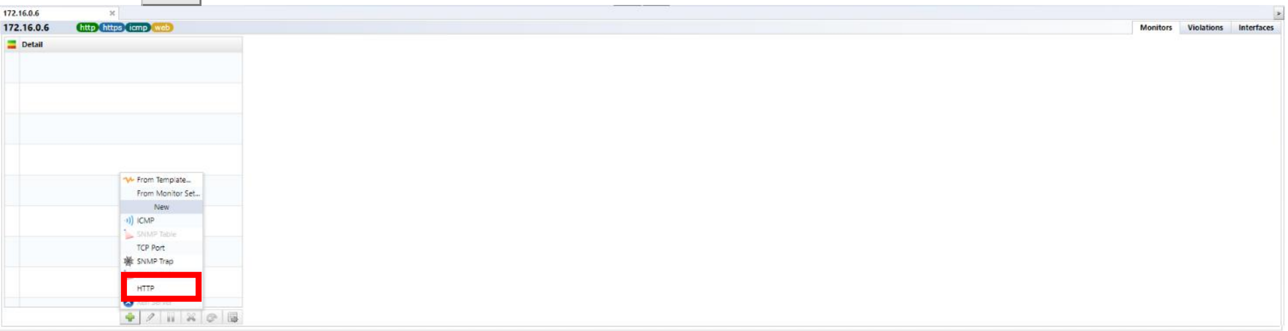
You can send HTTP requests to monitor web ports or specific sites.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.

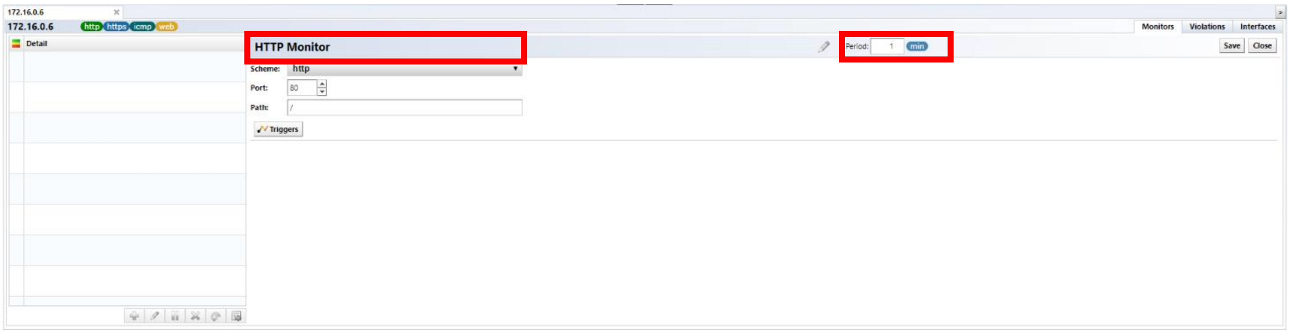


IP Address	Hostname	Traits
172.16.0.6		http https icmp web
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp
10.0.101.241	LVIGW-c3650.intra.lvi.co.jp-241	icmp snmp

2. Click [+ (Add)] in the lower left and click [HTTP].



3. Set the desired monitor name and interval.



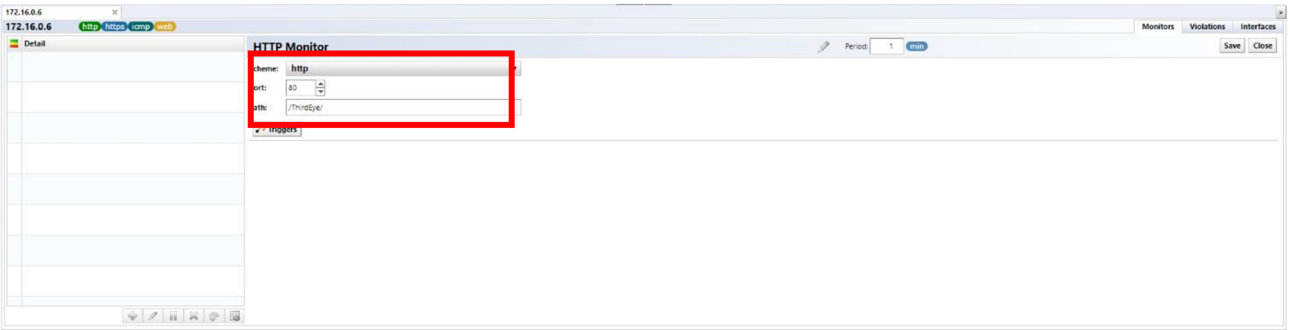
Scheme: http

Port: 80

Path: /

Period: 1 min

4. Enter the following items.



Period: 1 min

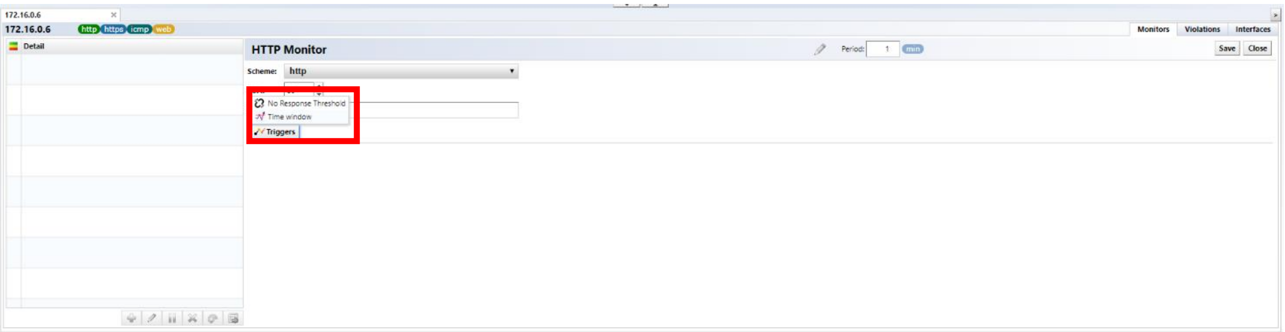
Scheme: http

Port: 80

Path: /ThirdEye/

Description	Explanation
Scheme	Select HTTP or HTTPS.
Port	Specify the web port.
Pass	Enter the path of the site to be monitored.

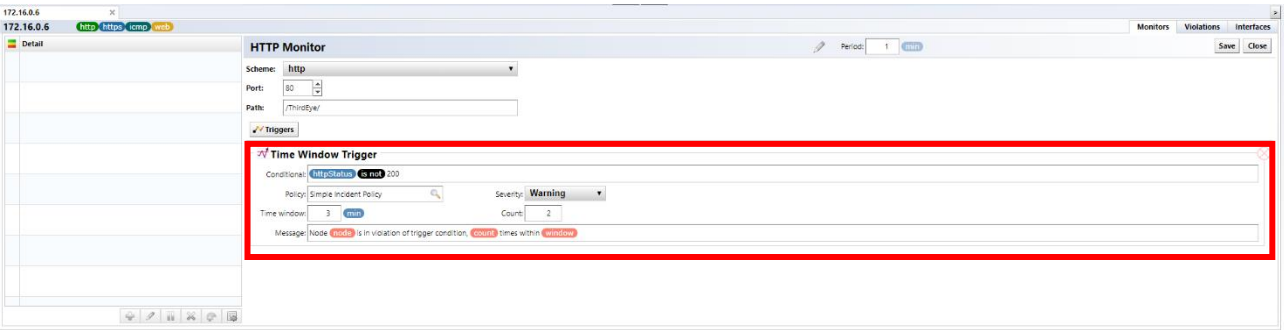
5. Click [Triggers] and click [Time Window].



Period: 1 min

Scheme: http

6. Set the conditions and policies in the same way as the threshold settings.
   In the conditions of the following screens, alert status is applicable when the status code is other than "200".



HTTP Monitor

Period: 1 min

Scheme: http

Port: 80

Path: /ThirdEye/

Time Window Trigger

Conditional: httpStatus is not 200

Policy: Simple Incident Policy

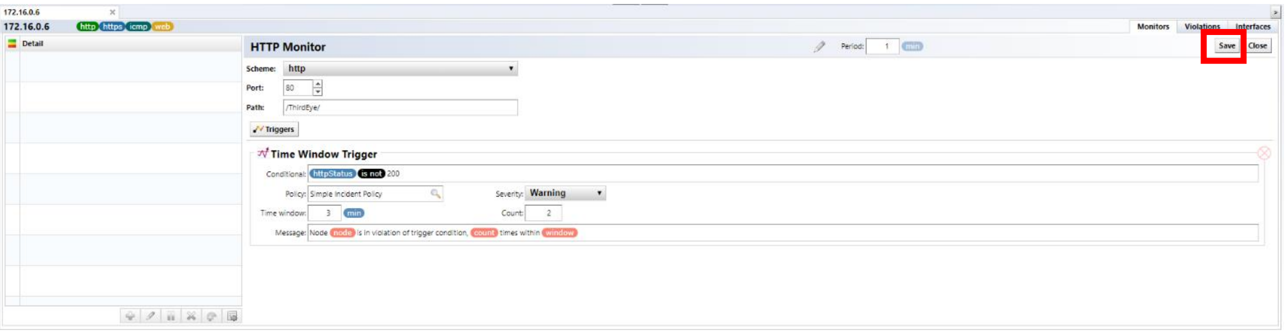
Severity: Warning

Time window: 3 min

Count: 2

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

7. Click [Save].



HTTP Monitor

Period: 1 min

Scheme: http

Port: 80

Path: /ThirdEye/

Time Window Trigger

Conditional: httpStatus is not 200

Policy: Simple Incident Policy

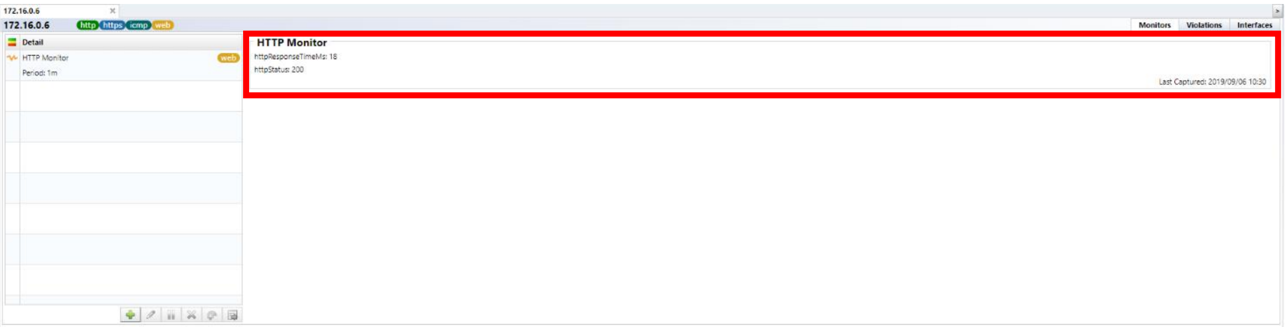
Severity: Warning

Time window: 3 min

Count: 2

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

After saving, if the request is started and can be acquired normally, the data will be displayed on the device details screen.



HTTP Monitor

httpResponseTimeMs: 18

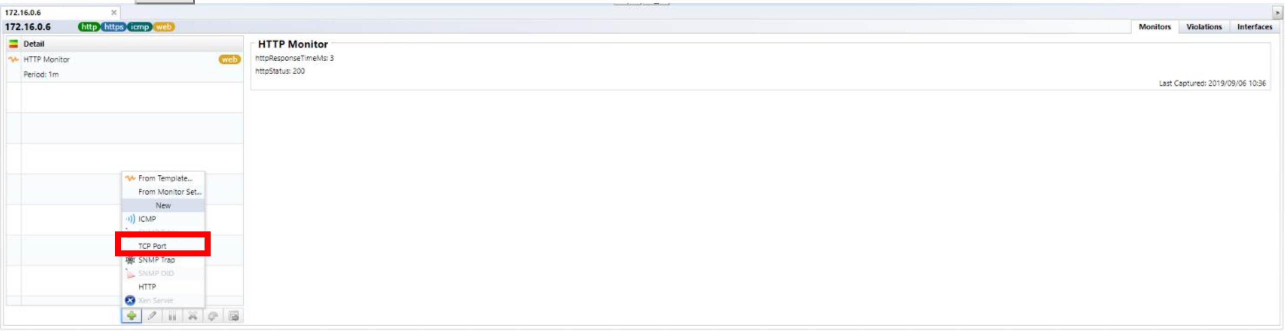
httpStatus: 200

Last Captured: 2019/09/06 10:30

7.1.2 Monitoring TCP ports

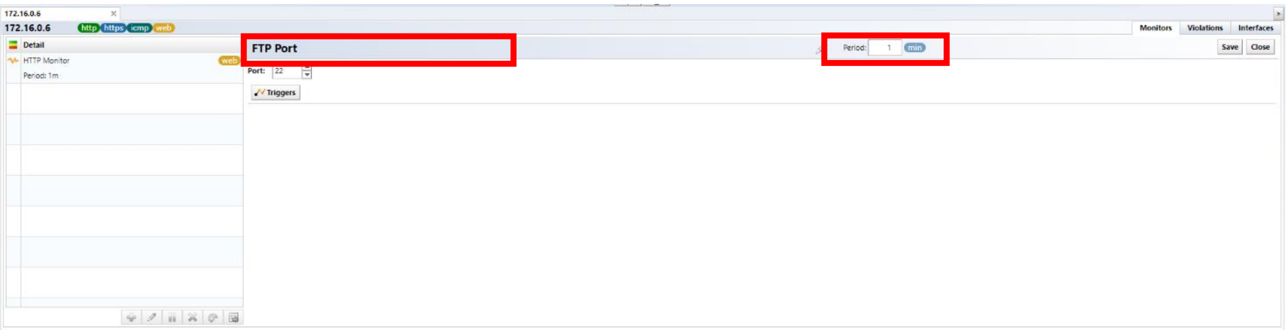
You can send a syn message to the TCP port and check if there is a response.

1. Click [✚ (Add)] in the lower left and click [TCP Port].



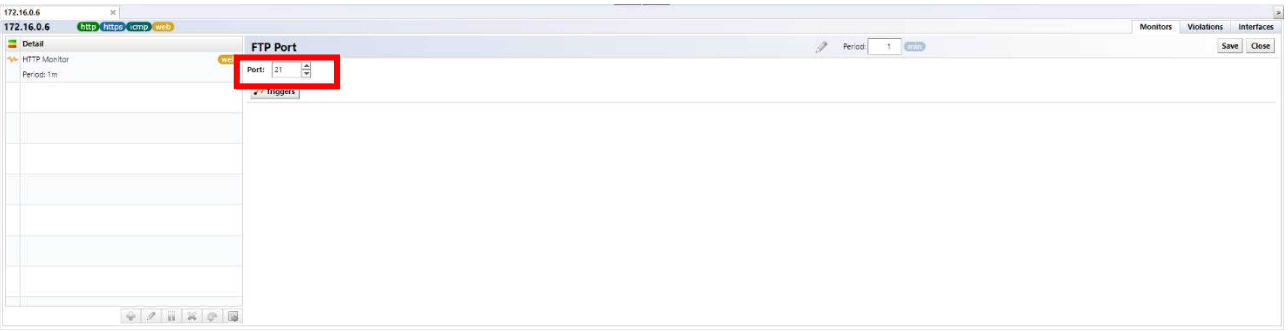
HTTP Monitor
httpResponseTimeMs: 3
httpStatus: 200
Last Captured: 2019/09/06 10:36

2. Set any monitor name and interval.



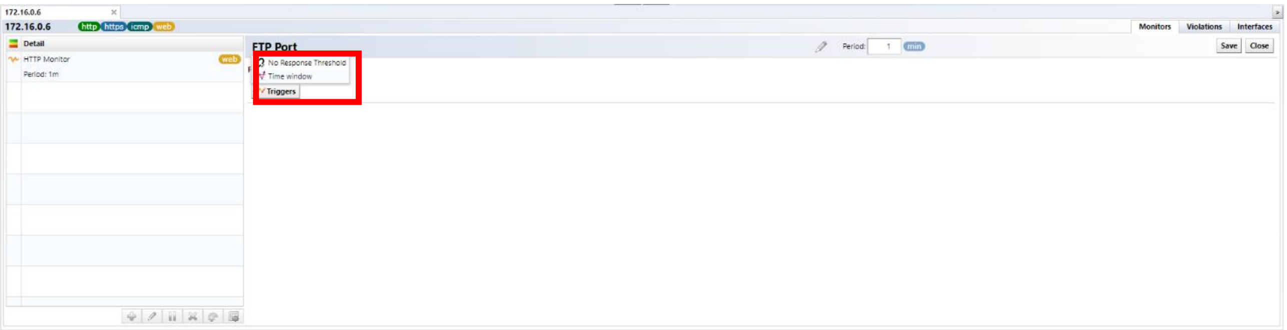
FTP Port
Period: 1 min
Port: 22

3. Set the port number to be monitored.

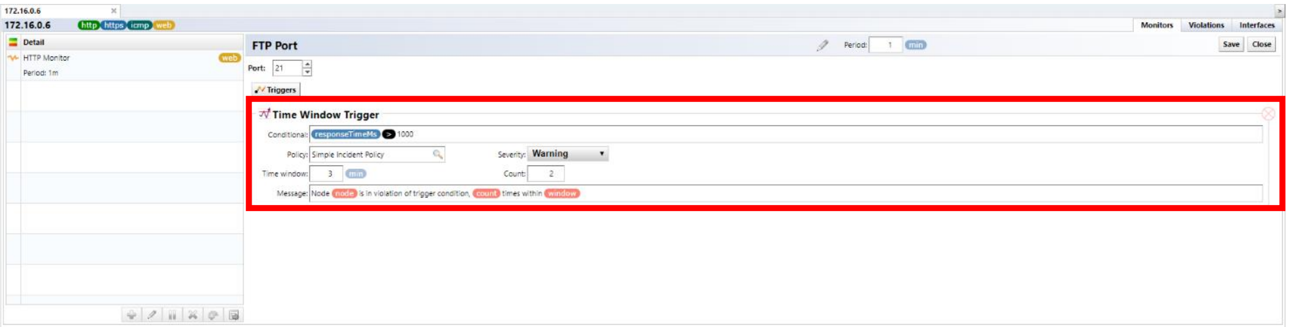


FTP Port
Period: 1 min
Port: 21

4. Click [Triggers] and click [Time Window].



5. Set the conditions and policies in the same way as the threshold settings.
In the following screen conditions, alerts will be alerted if the response is greater than 1000 milliseconds.



FTP Port

Period: 1 min

Port: 21

Time Window Trigger

Conditional: responseTimeMs > 1000

Policy: Simple Incident Policy

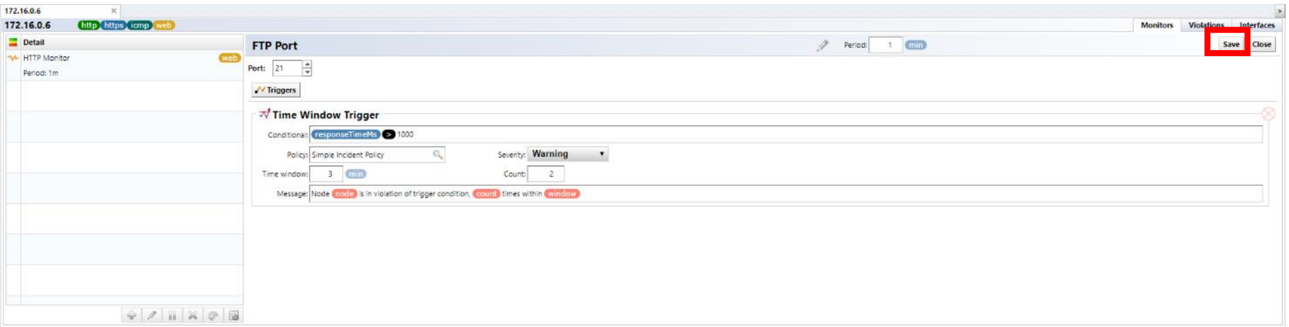
Severity: Warning

Time window: 3 min

Count: 2

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

6. Click [Save].



FTP Port

Period: 1 min

Port: 21

Time Window Trigger

Conditional: responseTimeMs > 1000

Policy: Simple Incident Policy

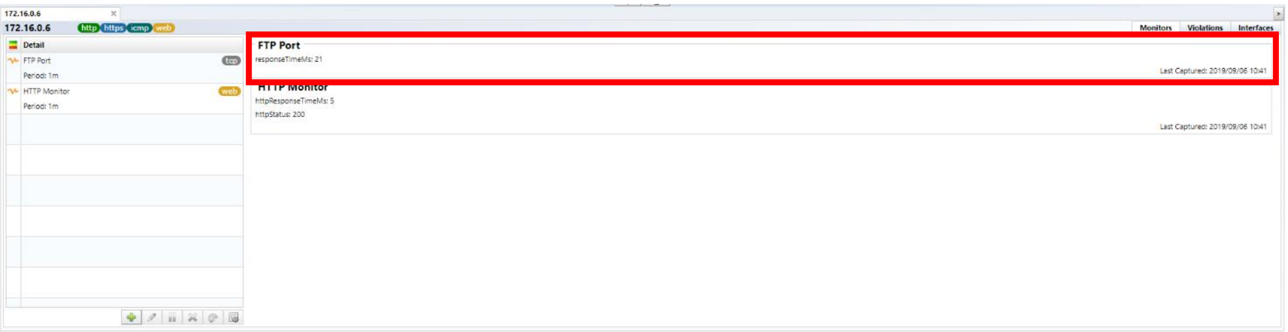
Severity: Warning

Time window: 3 min

Count: 2

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

After saving, if the request is started and can be acquired normally, the data will be displayed on the device details screen.



172.16.0.6

FTP Port
Period: 1m

HTTP Monitor
Period: 1m

FTP Port
responseTimeMs: 21
Last Captured: 2019/09/06 10:41

HTTP Monitor
httpResponseTimeMs: 5
httpStatus: 200
Last Captured: 2019/09/06 10:41

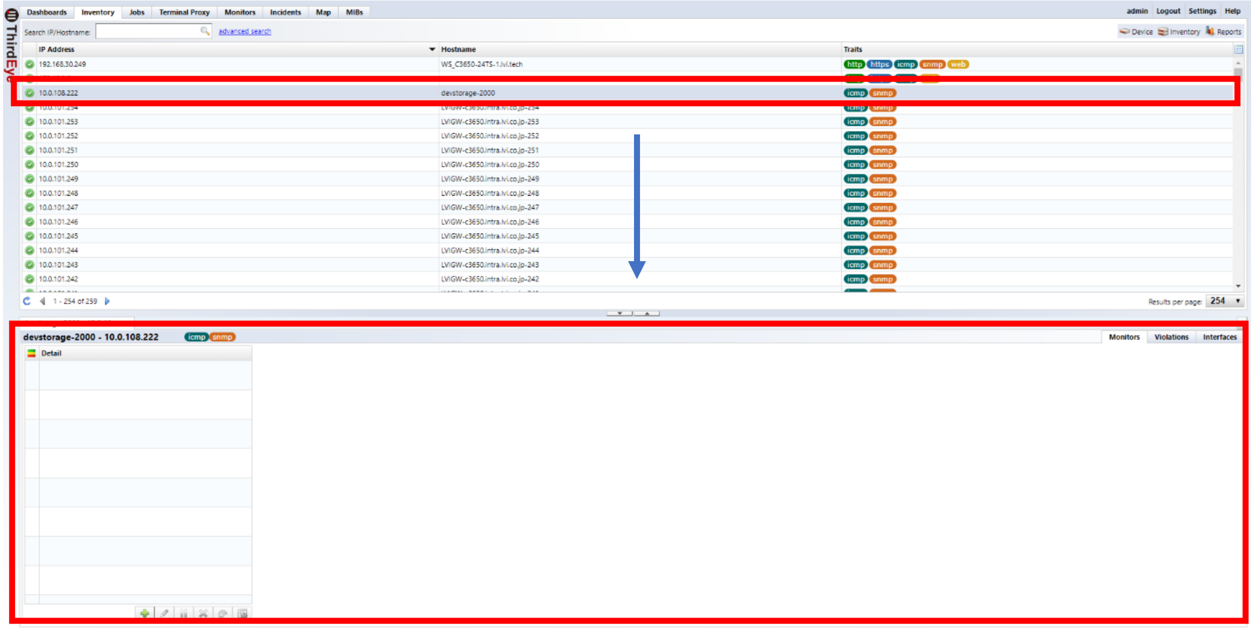
7.1.3 Monitoring using formulas

ThirdEye can automatically calculate the data obtained using a custom formula. For example, in the standard MIB HOST-RESOURCE-MIB, there are MIBs for server disk size and usage, but there is no MIB for usage (%).

By using a custom formula, you can calculate the disk size and usage to get the usage rate.

This section describes the procedure using HOST-RESOURCE-MIB as an example.

1. From the list of monitored devices on the [Inventory] tab, double-click the device for which you want to set the monitor.



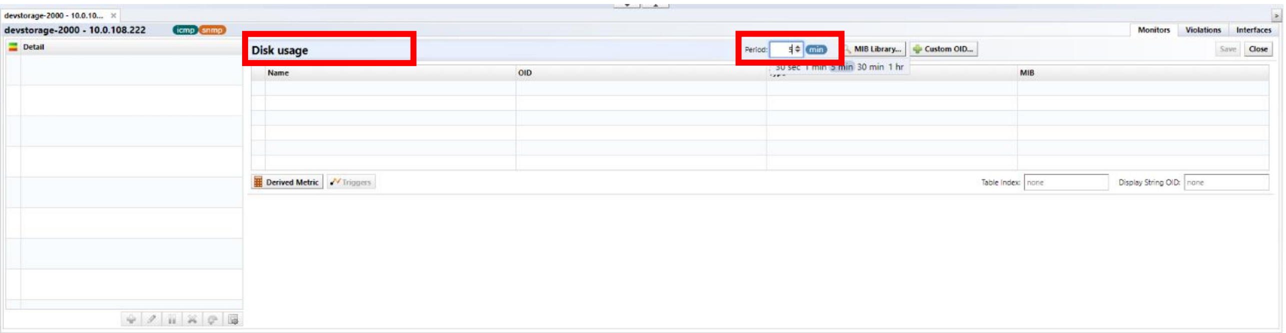
IP Address	Hostname	Traits
192.168.30.249	WS_C3650-24TS-1.lvi.tech	http https icmp snmp web
10.0.108.222	devstorage-2000	icmp snmp
10.0.101.253	LVIGW-c3650.intra.lvi.co.jp-253	icmp snmp
10.0.101.252	LVIGW-c3650.intra.lvi.co.jp-252	icmp snmp
10.0.101.251	LVIGW-c3650.intra.lvi.co.jp-251	icmp snmp
10.0.101.250	LVIGW-c3650.intra.lvi.co.jp-250	icmp snmp
10.0.101.249	LVIGW-c3650.intra.lvi.co.jp-249	icmp snmp
10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
10.0.101.247	LVIGW-c3650.intra.lvi.co.jp-247	icmp snmp
10.0.101.246	LVIGW-c3650.intra.lvi.co.jp-246	icmp snmp
10.0.101.245	LVIGW-c3650.intra.lvi.co.jp-245	icmp snmp
10.0.101.244	LVIGW-c3650.intra.lvi.co.jp-244	icmp snmp
10.0.101.243	LVIGW-c3650.intra.lvi.co.jp-243	icmp snmp
10.0.101.242	LVIGW-c3650.intra.lvi.co.jp-242	icmp snmp

1 - 254 of 259

devstorage-2000 - 10.0.108.222 icmp snmp

2. Click [✚ (Add)] in the lower left and click "SNMP Table".

3. Set the desired monitor name and interval.



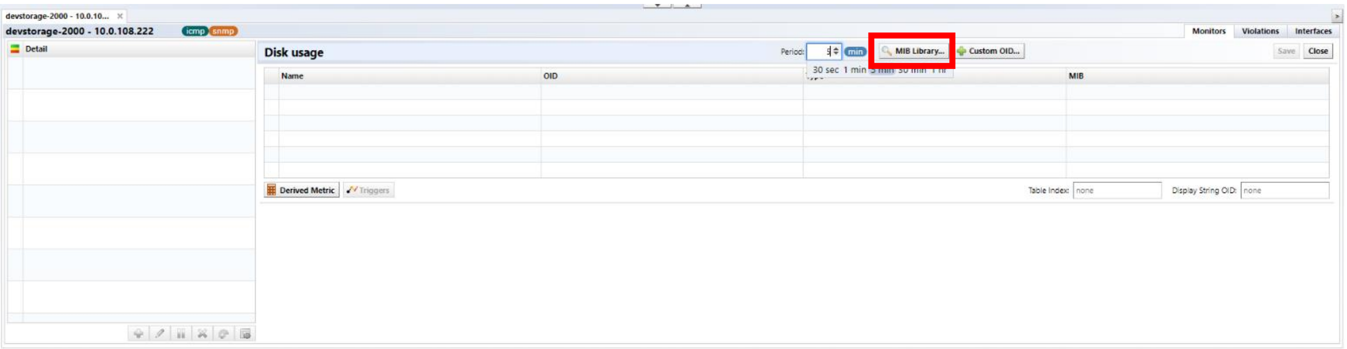
Disk usage

Period: 5 min

Table Index: none

Display String OID: none

4. Click [MIB Library].



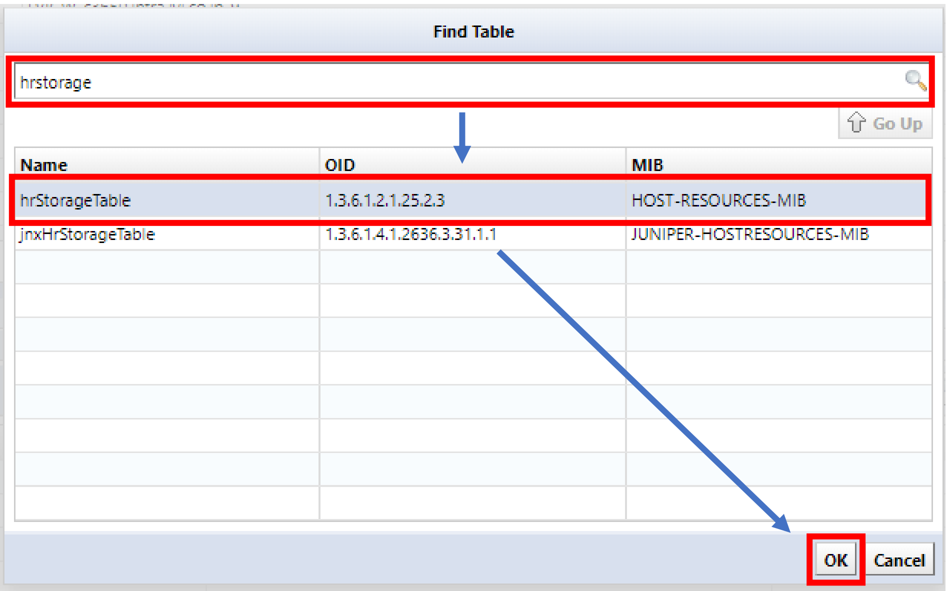
Disk usage

Period: 5 min

Table Index: none

Display String OID: none

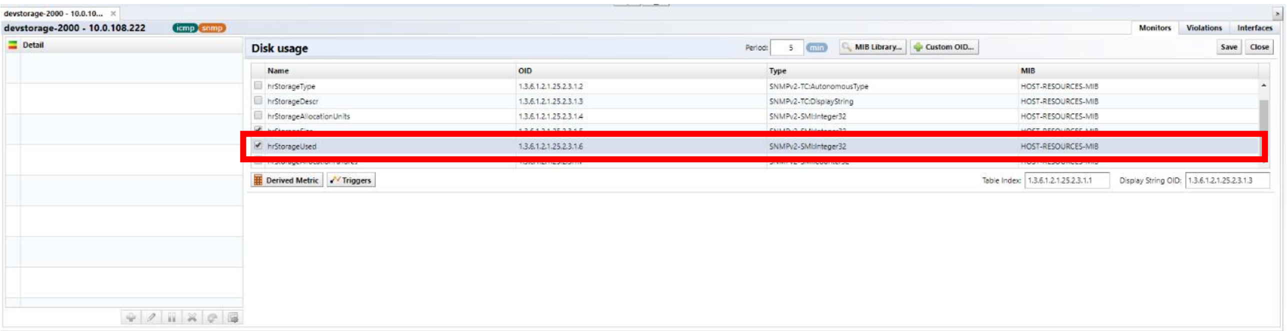
5. Enter [hrstorage] in the OID search, select "hrStorageTable" from the search results, and click [OK].



hrstorage

Name	OID	MIB
hrStorageTable	1.3.6.1.2.1.25.2.3	HOST-RESOURCES-MIB
jnxHrStorageTable	1.3.6.1.4.1.2636.3.31.1.1	JUNIPER-HOSTRESOURCES-MIB

6. Check “hrStorageSize / hrStorageUsed” from the table.



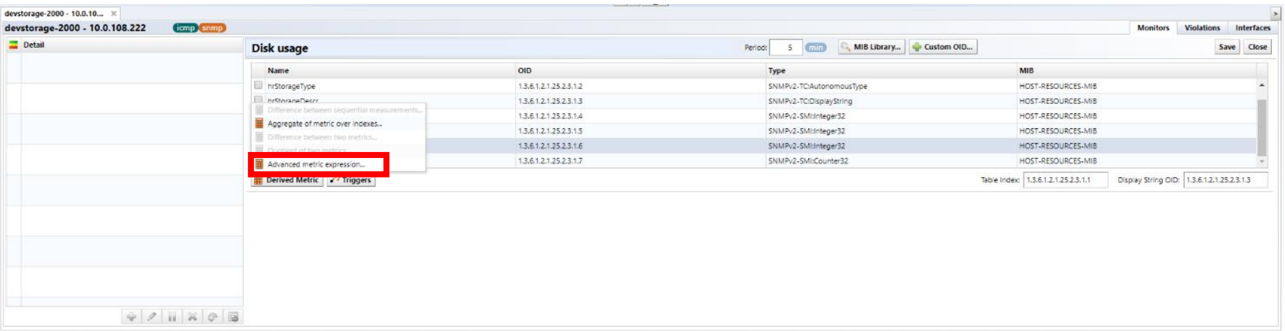
devstorage-2000 - 10.0.108.222

Disk usage Period: 5 min

	Name	OID	Type	MIB
□	hrStorageType	1.3.6.1.2.1.25.2.3.1.2	SNMPv2-TC:AutonomousType	HOST-RESOURCES-MIB
□	hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3	SNMPv2-TC:DisplayString	HOST-RESOURCES-MIB
□	hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4	SNMPv2-SMI:Integer32	HOST-RESOURCES-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

Table Index: 1.3.6.1.2.1.25.2.3.1.1 Display String OID: 1.3.6.1.2.1.25.2.3.1.3

7. Click Derived Metric → Advanced metric expression.



devstorage-2000 - 10.0.108.222

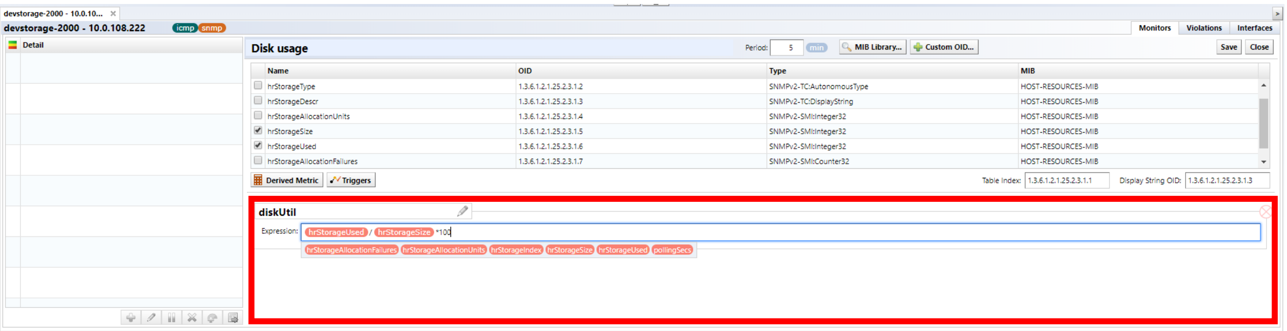
Disk usage Period: 5 min

	Name	OID	Type	MIB
□	hrStorageType	1.3.6.1.2.1.25.2.3.1.2	SNMPv2-TC:AutonomousType	HOST-RESOURCES-MIB
□	hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3	SNMPv2-TC:DisplayString	HOST-RESOURCES-MIB
		1.3.6.1.2.1.25.2.3.1.4	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
		1.3.6.1.2.1.25.2.3.1.5	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
		1.3.6.1.2.1.25.2.3.1.6	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
		1.3.6.1.2.1.25.2.3.1.7	SNMPv2-SMI:Counter32	HOST-RESOURCES-MIB

Table Index: 1.3.6.1.2.1.25.2.3.1.1 Display String OID: 1.3.6.1.2.1.25.2.3.1.3

devstorage-2000 - 10.0.10...
icmp
snmp
Monitors
Violations
Interfaces
Detail
MIB Library...
Custom OID...
Save
Close
Difference between sequential measurements...
Aggregate of metric over indexes...
Difference between two metrics...
Quotient of two metrics...
Advanced metric expression...
Derived Metric
Triggers

8. Enter a name and formula.



devstorage-2000 - 10.0.108.222

Disk usage Period: 5 min

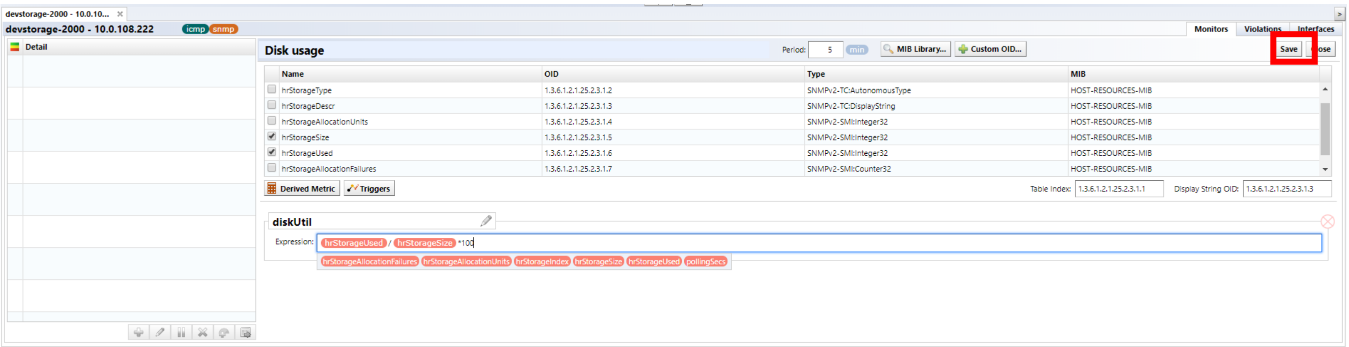
	Name	OID	Type	MIB
□	hrStorageType	1.3.6.1.2.1.25.2.3.1.2	SNMPv2-TC:AutonomousType	HOST-RESOURCES-MIB
□	hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3	SNMPv2-TC:DisplayString	HOST-RESOURCES-MIB
□	hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageSize	1.3.6.1.2.1.25.2.3.1.5	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
□	hrStorageAllocationFailures	1.3.6.1.2.1.25.2.3.1.7	SNMPv2-SMI:Counter32	HOST-RESOURCES-MIB

Table Index: 1.3.6.1.2.1.25.2.3.1.1 Display String OID: 1.3.6.1.2.1.25.2.3.1.3

diskUtil

Expression: hrStorageUsed / hrStorageSize *100

9. Click [Save].



devstorage-2000 - 10.0.108.222

Disk usage Period: 5 min

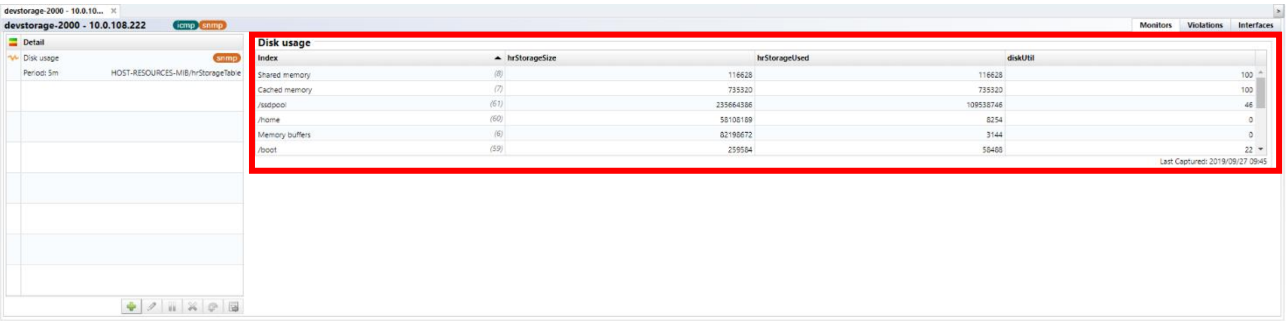
	Name	OID	Type	MIB
□	hrStorageType	1.3.6.1.2.1.25.2.3.1.2	SNMPv2-TC:AutonomousType	HOST-RESOURCES-MIB
□	hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3	SNMPv2-TC:DisplayString	HOST-RESOURCES-MIB
□	hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageSize	1.3.6.1.2.1.25.2.3.1.5	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
☑	hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6	SNMPv2-SMI:Integer32	HOST-RESOURCES-MIB
□	hrStorageAllocationFailures	1.3.6.1.2.1.25.2.3.1.7	SNMPv2-SMI:Counter32	HOST-RESOURCES-MIB

Table Index: 1.3.6.1.2.1.25.2.3.1.1 Display String OID: 1.3.6.1.2.1.25.2.3.1.3

diskUtil

Expression: hrStorageUsed / hrStorageSize *100

After saving, data collection starts, and the results are displayed.


devstorage-2000 - 10.0.10...
devstorage-2000 - 10.0.108.222
icmp
snmp
Monitors
Violations
Interfaces
Detail
Disk usage
snmp
Period: 5m
HOST-RESOURCES-MIB/hrStorageTable

Disk usage

Index		hrStorageSize	hrStorageUsed	diskUtil
Shared memory	(8)	116628	116628	100
Cached memory	(7)	735320	735320	100
/ssdpool	(61)	235664386	109538746	46
/home	(60)	58108189	8254	0
Memory buffers	(6)	82198672	3144	0
/boot	(59)	259584	58488	22

Last Captured: 2019/09/27 09:45

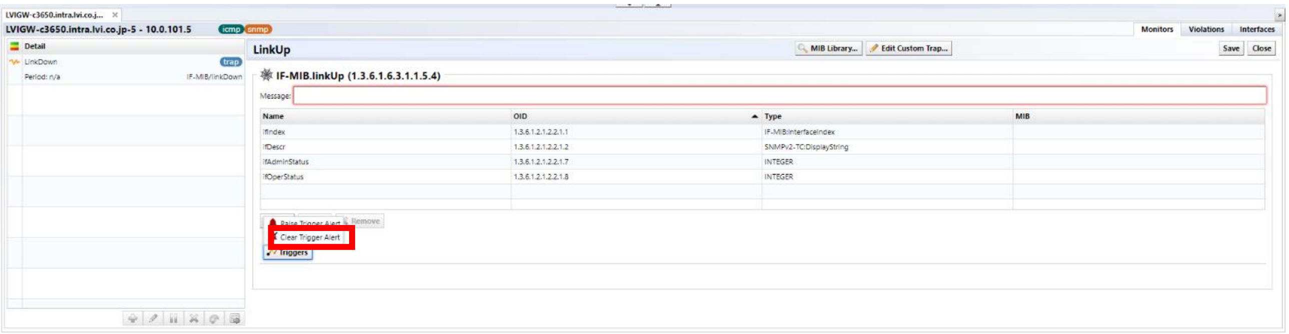
You can also set a threshold for the calculated value using a custom formula. For details on threshold settings, see 5.3.4 Setting and monitoring thresholds.

7.1.4 Automatically clear a specific trap incident when a trap is received

When a correlated trap is received, the fault is automatically cleared, and the icon color and status icon on the map can be returned to the normal state.

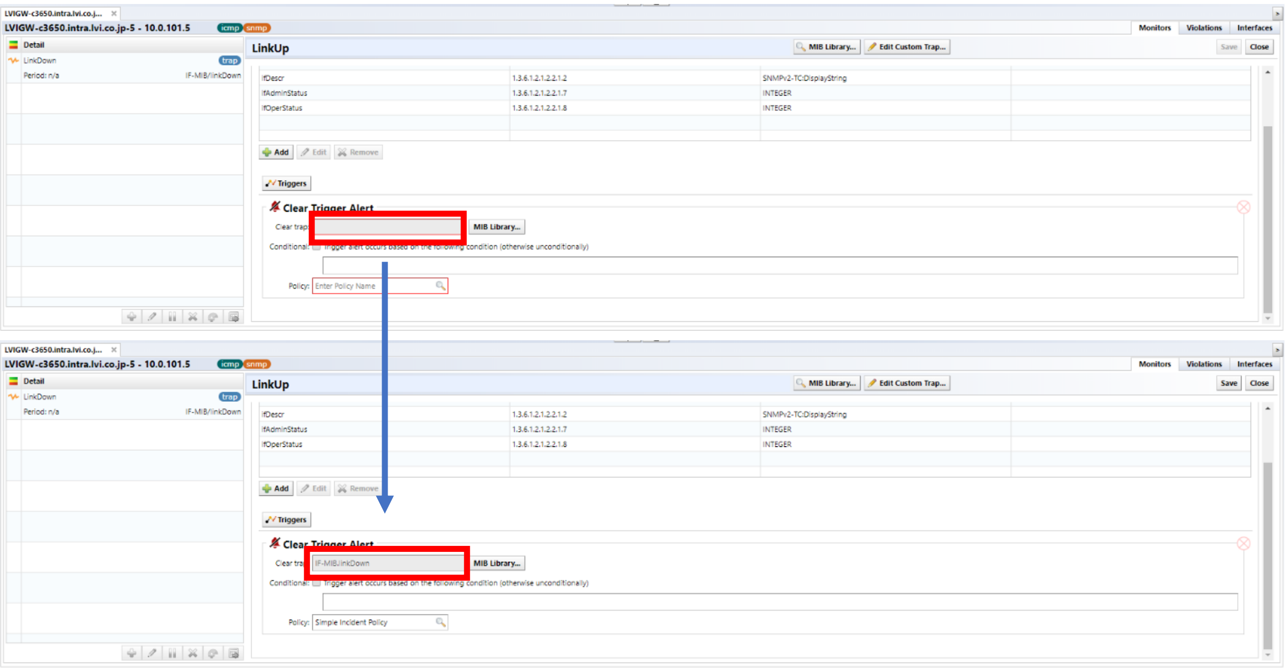
For example, LinkDown trap and LinkUp trap. After the LinkDown trap is received and an incident occurs as a failure, the LinkDown trap is cleared when the LinkUp trap is received.

1. Create a LinkDown trap monitor.
2. Create an SNMP trap monitor for LinkUp.
3. Click [Trigger] and click [Time window].



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	

4. Click [MIB Library] of the trap to be released and add a LinkDown trap.



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

Clear trap:

Conditional: □ Trigger alert occurs based on the following condition (otherwise unconditionally)

Policy: Enter Policy Name

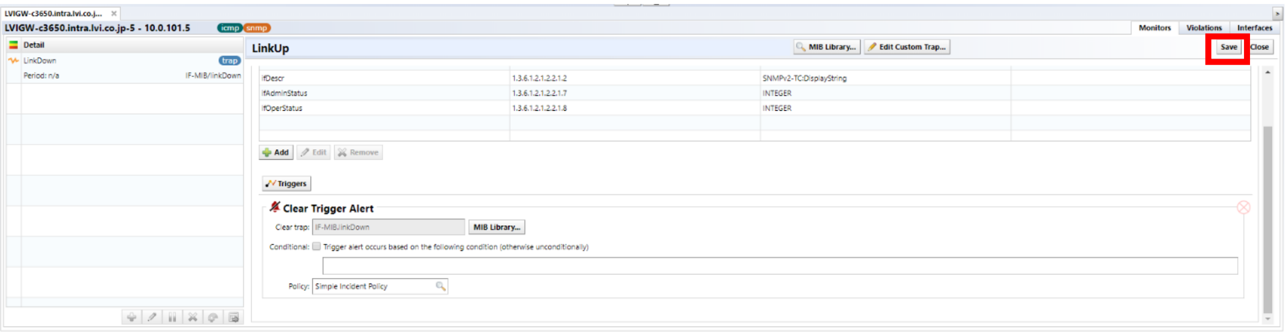
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv2-TC:DisplayString
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER
ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER

Clear trap: IF-MIB.linkDown

Conditional: □ Trigger alert occurs based on the following condition (otherwise unconditionally)

Policy: Simple Incident Policy

5. 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

Clear trap: IF-MIB.linkDown

Conditional: □ Trigger alert occurs based on the following condition (otherwise unconditionally)

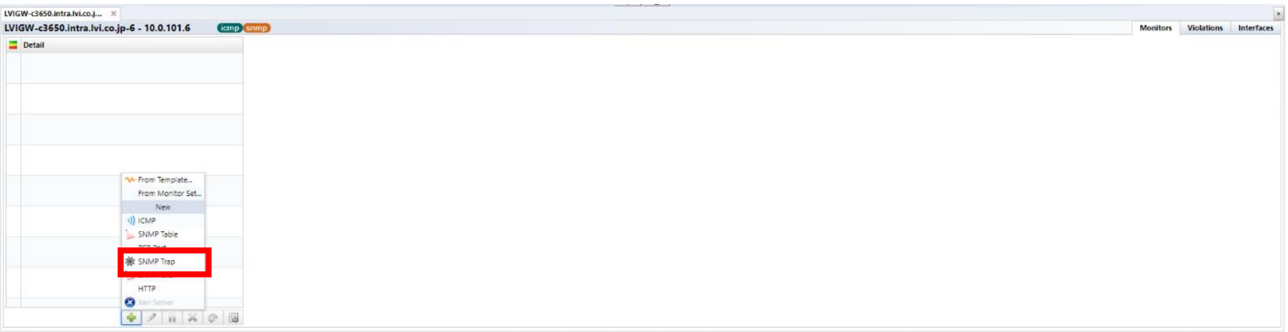
Policy: Simple Incident Policy

7.1.5 Changing the action with the value contained in the trap

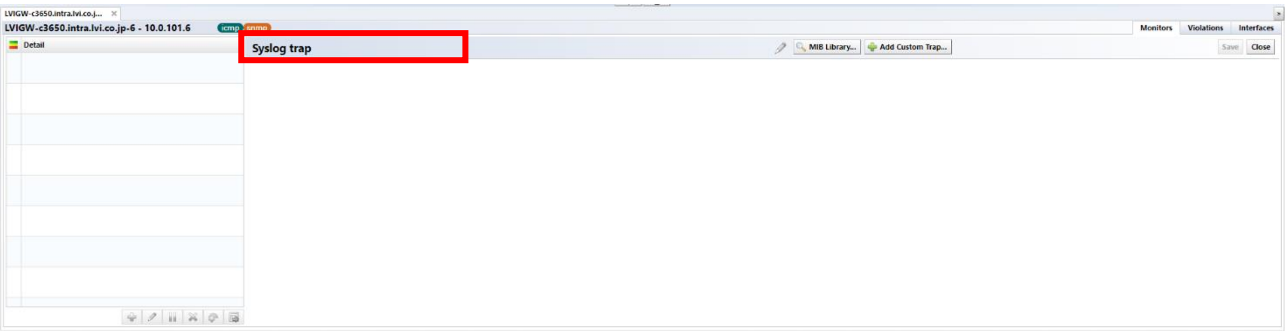
Monitored devices send various information in traps when sending traps. Depending on the content, you may not want to detect it as a failure. In ThirdEye, you can filter by specifying conditions.

In the following example, Syslog traps from Cisco equipment are used to filter the traps.

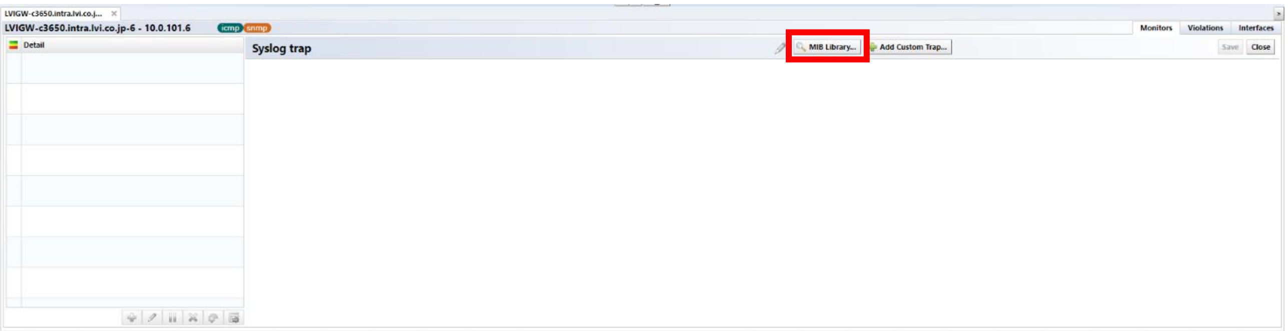
1. Monitored devices send various information in traps when sending traps. Depending on the content, you may not want to detect it as a failure. In ThirdEye, you can filter by specifying conditions.



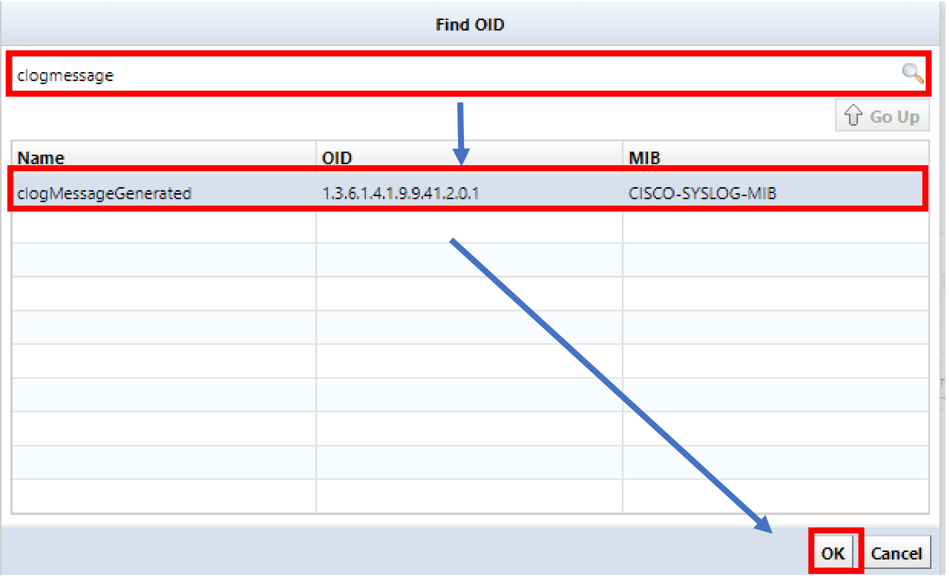
2. Display any monitor name.



3. Click [MIB Library].



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

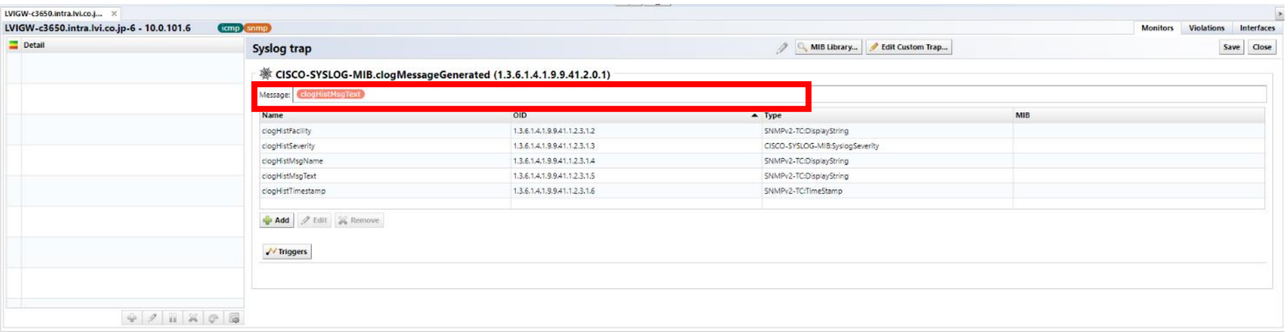


Find OID

clogmessage

Name	OID	MIB
clogMessageGenerated	1.3.6.1.4.1.9.9.41.2.0.1	CISCO-SYSLOG-MIB

5. Enter a message when a failure occurs.
   * Below, clogHitMsgText (message content) included in the trap is displayed.



LVIGW-c3650.intra.lvi.co.jp-6 - 10.0.101.6

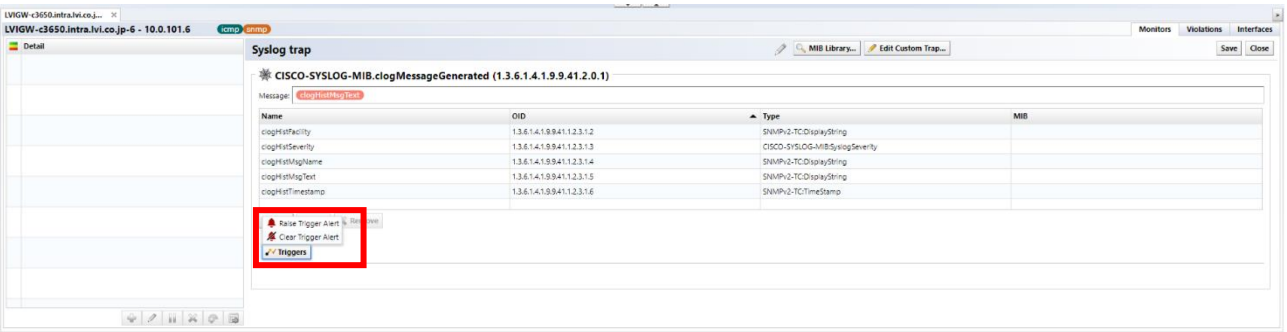
Syslog trap

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	

6. Click [Trigger], and then click [Rise Trigger Alert].



LVIGW-c3650.intra.lvi.co.jp-6 - 10.0.101.6

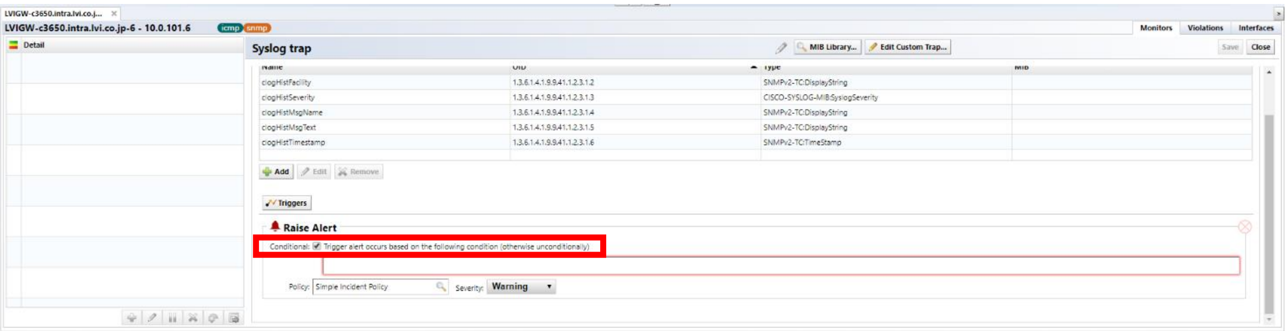
Syslog trap

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	

7. Check “Conditional”.



LVIGW-c3650.intra.lvi.co.jp-6 - 10.0.101.6

Syslog trap

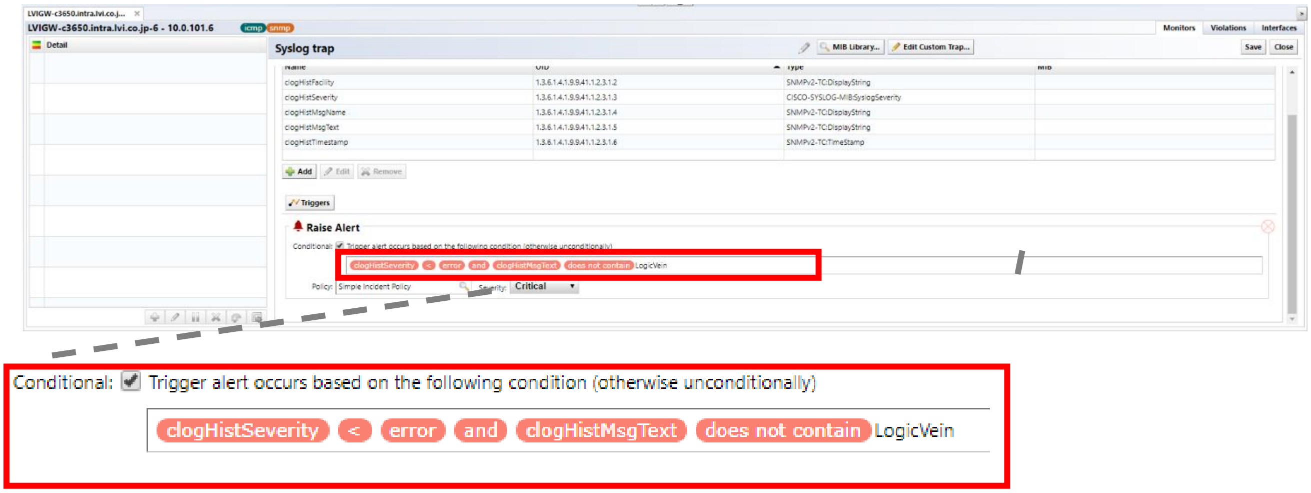
Name	OID	Type	MIB
clogHistFacility	1.3.6.1.4.1.9.9.41.1.2.3.1.2	SNMPv2-TC:DisplayString	
clogHistSeverity	1.3.6.1.4.1.9.9.41.1.2.3.1.3	CISCO-SYSLOG-MIB:SyslogSeverity	
clogHistMsgName	1.3.6.1.4.1.9.9.41.1.2.3.1.4	SNMPv2-TC:DisplayString	
clogHistMsgText	1.3.6.1.4.1.9.9.41.1.2.3.1.5	SNMPv2-TC:DisplayString	
clogHistTimestamp	1.3.6.1.4.1.9.9.41.1.2.3.1.6	SNMPv2-TC:TimeStamp	

Raise Alert

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

Policy: Simple Incident Policy Severity: Warning

8. Enter “Condition” in the red frame.



LVIGW-c3650.intra.lvi.co.jp-6 - 10.0.101.6

Syslog trap

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	

Raise Alert

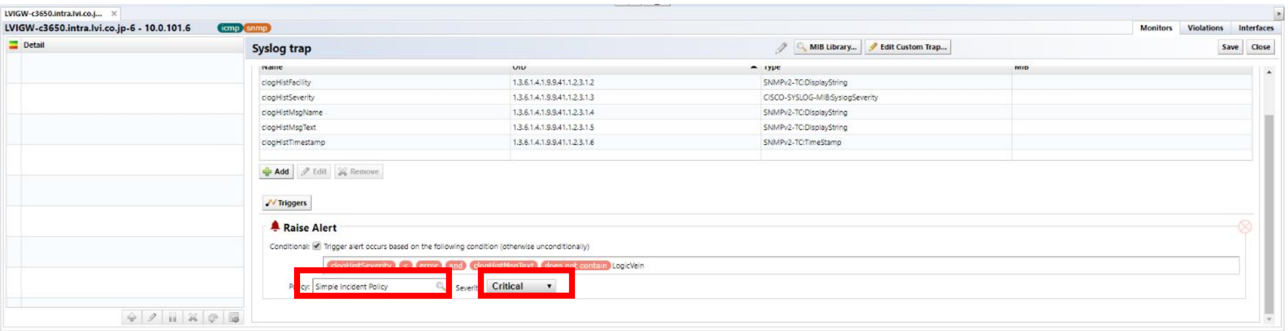
Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

clogHistSeverity < error and clogHistMsgText does not contain LogicVein

Policy: Simple Incident Policy Severity: Critical

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

9. Set the policy and severity.



LVIGW-c3650.intra.lvi.co.jp-6 - 10.0.101.6

Syslog trap

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	

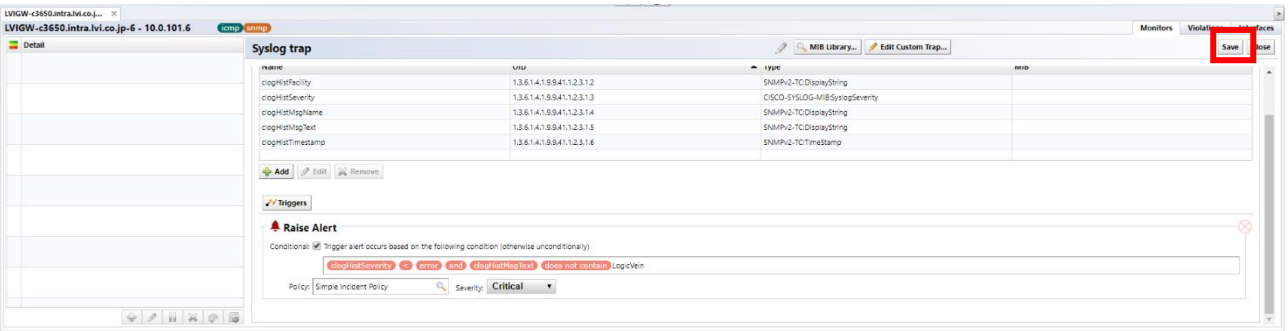
Raise Alert

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

clogHistSeverity < error and clogHistMsgText does not contain LogicVein

Policy: Simple Incident Policy Severity: Critical

10. Click [Save].



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	

Raise Alert

Conditional: ☑ Trigger alert occurs based on the following condition (otherwise unconditionally)

clogHistSeverity < error and clogHistMsgText does not contain LogicVein

Policy: Simple Incident Policy Severity: Critical

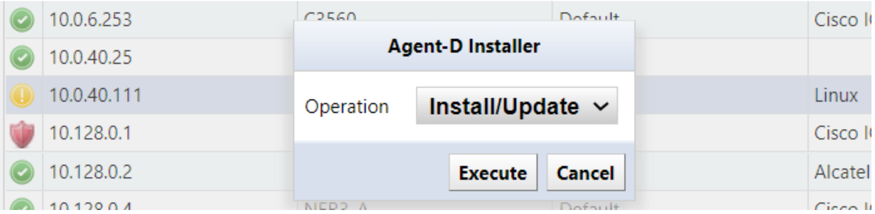
7.2 Agent-D

Agent-D is an agent installed on either Linux or Windows servers that runs in the background of the server. It can perform monitoring functions, collect metrics and send alerts/traps on the below functions.

- CPU
- Disk
- Memory
- Process
- Syslog monitoring

Agent-D can be installed two different ways

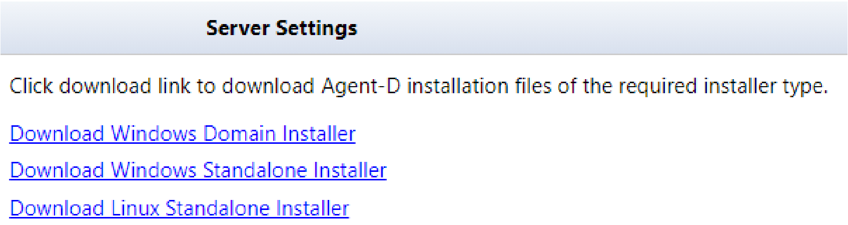
- From ThirdEye – right click on server, select Agent_D



Agent-D Installer

Operation: Install/Update

- Download from ThirdEye (settings/Agent-D) and install on server.

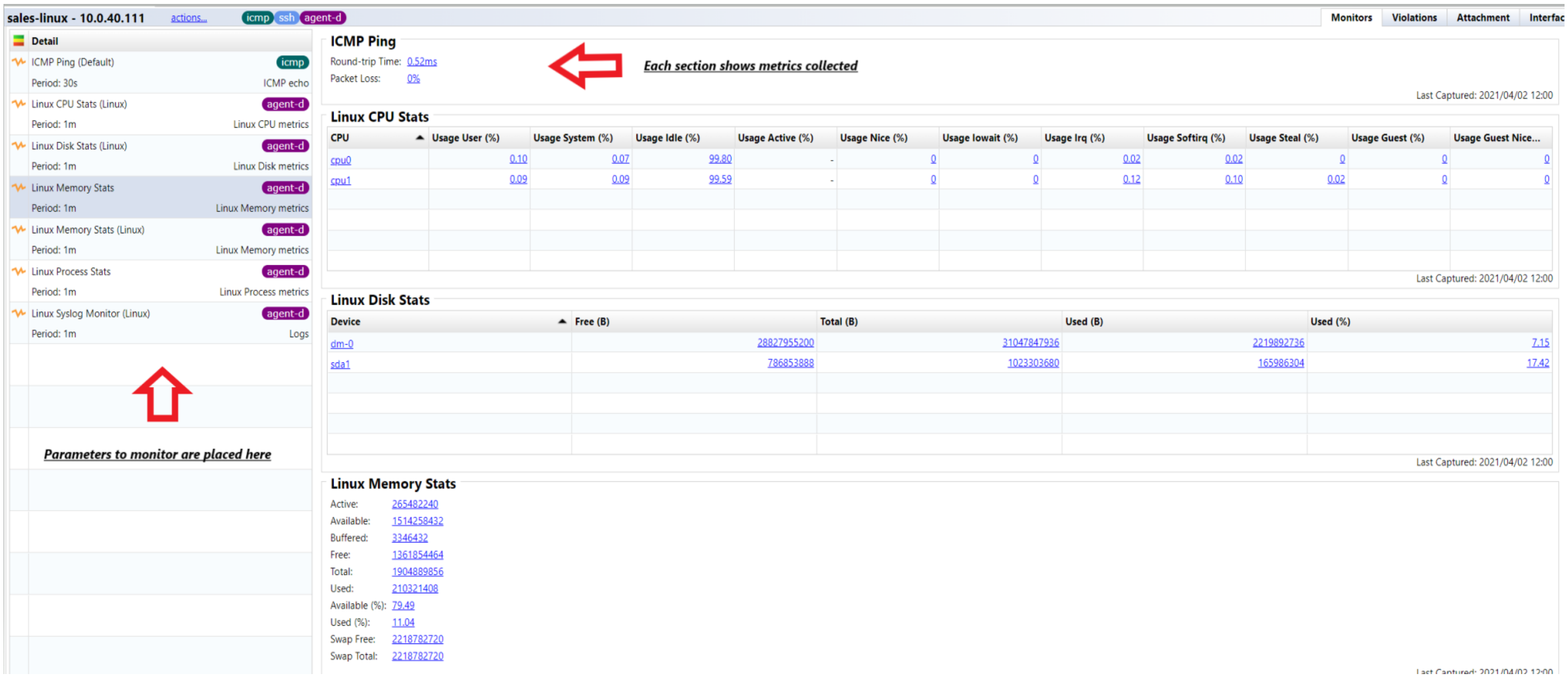


Server Settings

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

In the Device monitor section, you can visualize the parameters and settings.



sales-linux - 10.0.40.111 actions... icmp ssh agent-d

Detail	
ICMP Ping (Default)	icmp
Period: 30s	ICMP echo
Linux CPU Stats (Linux)	agent-d
Period: 1m	Linux CPU metrics
Linux Disk Stats (Linux)	agent-d
Period: 1m	Linux Disk metrics
Linux Memory Stats	agent-d
Period: 1m	Linux Memory metrics
Linux Memory Stats (Linux)	agent-d
Period: 1m	Linux Memory metrics
Linux Process Stats	agent-d
Period: 1m	Linux Process metrics
Linux Syslog Monitor (Linux)	agent-d
Period: 1m	Logs

Parameters to monitor are placed here

ICMP Ping

Round-trip Time: 0.52ms
Packet Loss: 0%

Each section shows metrics collected

Last Captured: 2021/04/02 12:00

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 Nice...
cpu0	0.10	0.07	99.80	-	0	0	0.02	0.02	0	0	0
cpu1	0.09	0.09	99.59	-	0	0	0.12	0.10	0.02	0	0

Last Captured: 2021/04/02 12:00

Linux Disk Stats

Device	Free (B)	Total (B)	Used (B)	Used (%)
dm-0	28827955200	31047847936	2219892736	7.15
sda1	786853888	1023303680	165986304	17.42

Last Captured: 2021/04/02 12:00

Linux Memory Stats

Active:	265482240
Available:	1514258432
Buffered:	3346432
Free:	1361854464
Total:	1904889856
Used:	210321408
Available (%):	79.49
Used (%):	11.04
Swap Free:	2218782720
Swap Total:	2218782720

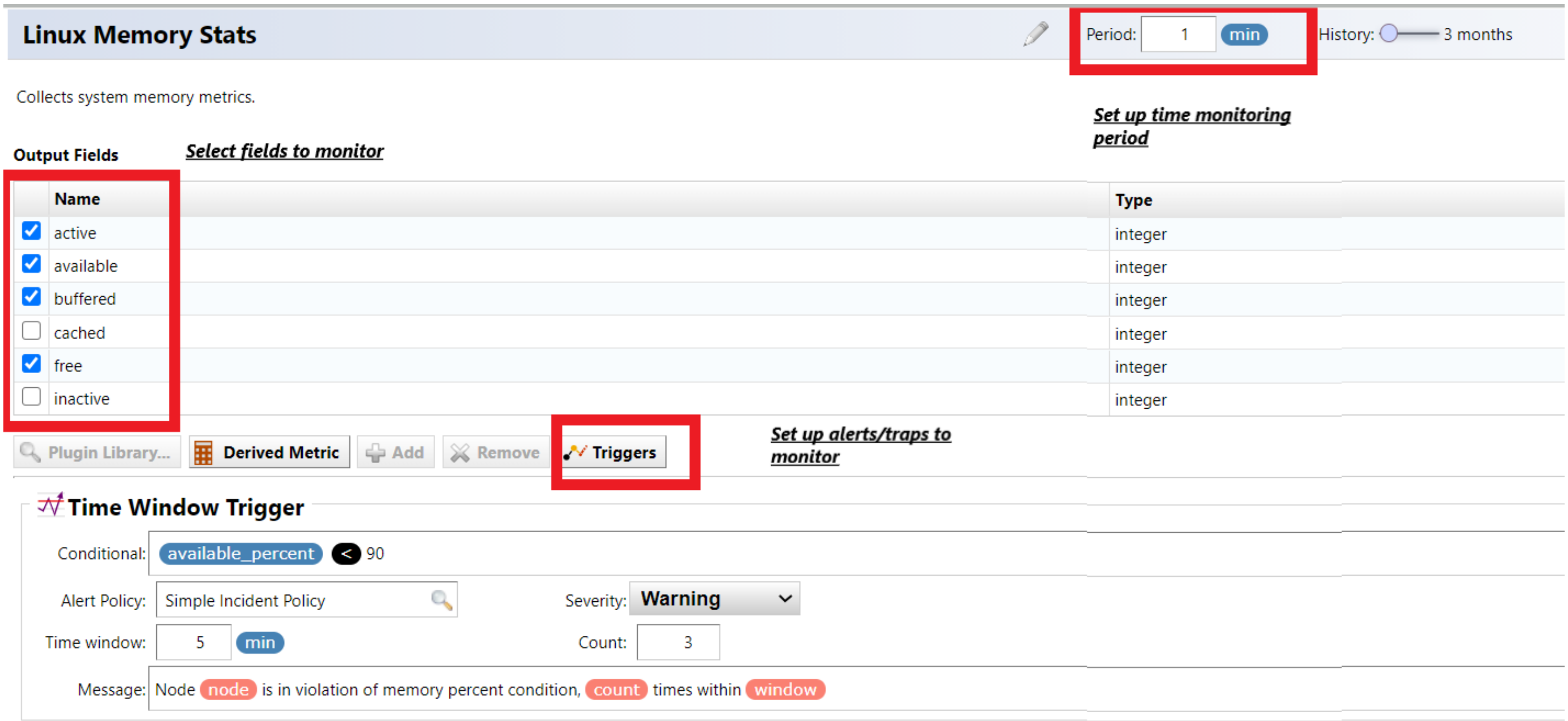
Last Captured: 2021/04/02 12:00

- ➢ Add the appropriate templates to the device from the template library
- ➢ Configure what you want to monitor

How often to pull data

Fields/metrics to monitor

Setup any alerts/traps to notify when there are issues



Linux Memory Stats

Period: 1 min History: 3 months

Collects system memory metrics.

Set up time monitoring period

Output Fields ***Select fields to monitor***

	Name	Type
☑	active	integer
☑	available	integer
☑	buffered	integer
□	cached	integer
☑	free	integer
□	inactive	integer

Set up alerts/traps to monitor

Time Window Trigger

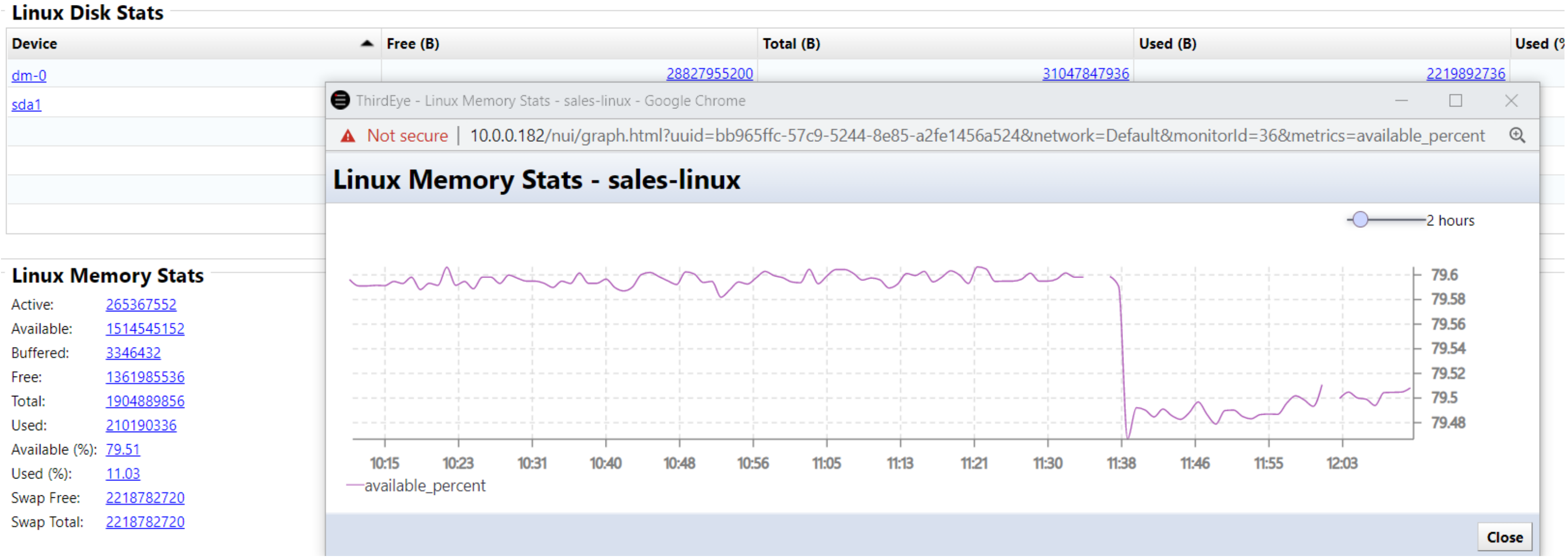
Conditional: available_percent < 90

Alert Policy: Simple Incident Policy Severity: Warning

Time window: 5 min Count: 3

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

- ➢ Clicking on any of the values, in any section, will popup a display that will graph that value. Display is configurable to show time from 1 hour up to 2 years



Linux Disk Stats

Device	Free (B)	Total (B)	Used (B)	Used (
dm-0	28827955200	31047847936	2219892736	
sda1				

Linux Memory Stats

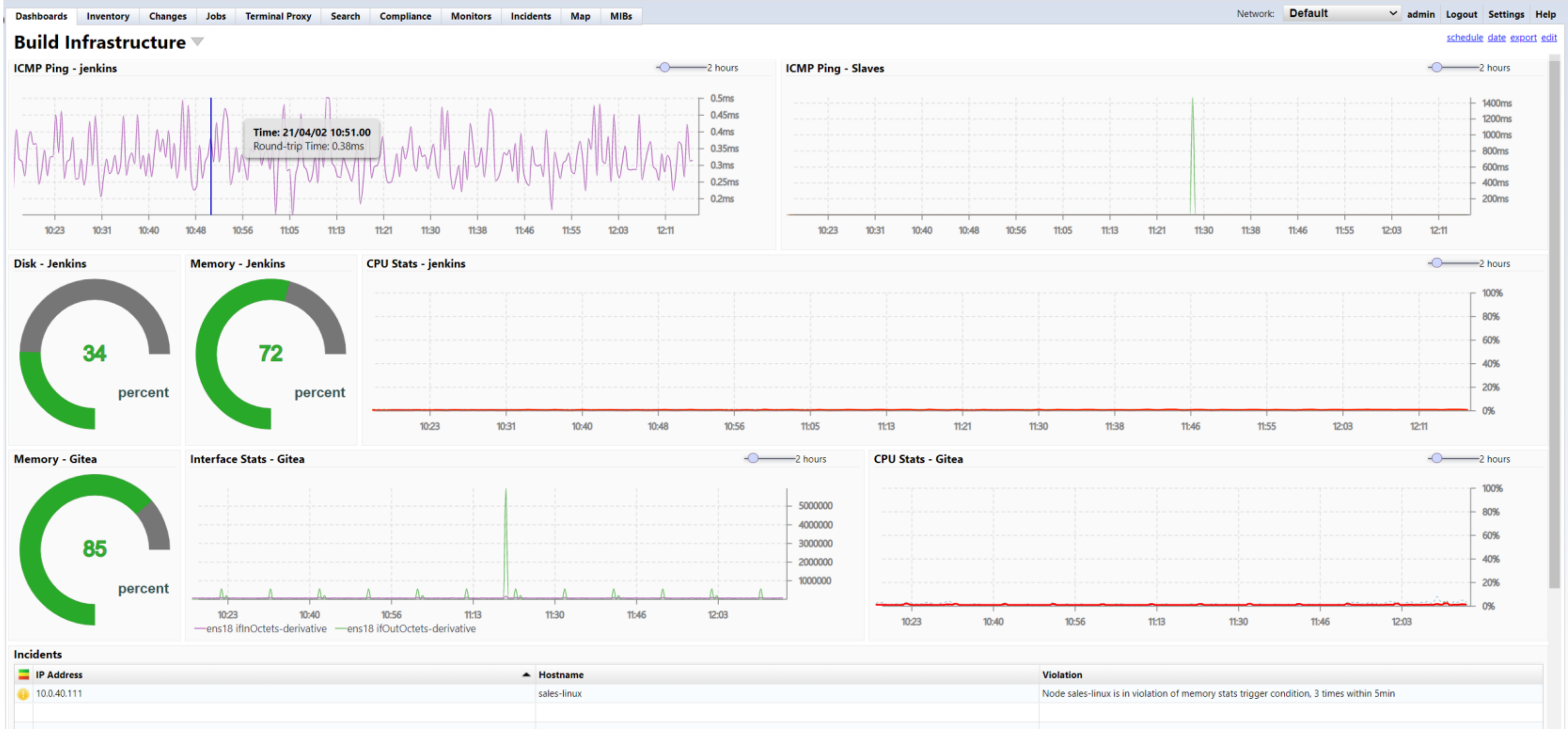
Active:	265367552
Available:	1514545152
Buffered:	3346432
Free:	1361985536
Total:	1904889856
Used:	210190336
Available (%):	79.51
Used (%):	11.03
Swap Free:	2218782720
Swap Total:	2218782720

ThirdEye - Linux Memory Stats - sales-linux - Google Chrome

Not secure | 10.0.0.182/nui/graph.html?uuid=bb965ffc-57c9-5244-8e85-a2fe1456a524&network=Default&monitorId=36&metrics=available_percent

Linux Memory Stats - sales-linux

- ➢ Agent-D results can be displayed in the Dashboard, exported to a file, or downloaded via API.
- ➢ Additionally, any alerts/traps can also be displayed for monitoring purposes.



Incidents

IP Address	Hostname	Violation
10.0.40.111	sales-linux	Node sales-linux is in violation of memory stats trigger condition, 3 times within 5min

METRICS:

CPU STATS
time_active
time_guest
time_guest_nice
time_idle
time_iowait
time_irq
time_nice
time_softirq
time_steal
time_system
time_user
usage_active
usage_guest
usage_guest_nice
usage_idle
usage_iowait
usage_irq
usage_nice
usage_softirq
usage_steal
usage_system
usage_user

DISK STATS
free
inodes_free
inodes_total
inodes_used
total
used
used_percent

MEMORY STATS	
active	mapped
available	page_tables
available_percent	shared
buffered	slab
cached	sreclaimable
commit_limit	sunreclaim
committed_as	swap_cached
dirty	swap_free
free	swap_total
high_free	total
high_total	used
huge_page_size	used_percent
huge_pages_free	vmalloc_chunk
huge_pages_total	vmalloc_total
inactive	vmalloc_used
low_free	wired
low_total	write_back
	write_back_tmp

PROCESS STATS	
child_major_faults	process_name
child_minor_faults	read_count
cpu_time	read_tytes
cpu_time_guest	realtime_priority
cpu_time_guest_nice	rlimit_cpu_time_hard
cpu_time_iowait	rlimit_cpu_time_soft
cpu_time_irq	rlimit_file_locks_soft
cpu_time_nice	rlimit_memory_data_hard
cpu_time_soft_irq	rlimit_memory_data_soft
cpu_time_steal	rlimit_memory_locked_hard
cpu_time_system	rlimit_memory_locked_soft
cpu_time_user	rlimit_memory_rss_hard
cpu_usage	rlimit_memory_rss_soft
cup_time_idle	rlimit_memory_stack_hard
involuntary_context_switches	rlimit_memory_stack_soft
major_faults	rlimit_memory_vms_hard
memory_data	rlimit_memory_vms_soft
memory_locked	rlimit_nice_prioity_soft
memory_rss	rlimit_nice_priority_hard
memory_stack	rlimit_num_fds_hard
memory_swap	rlimit_num_fds_soft
memory_usage	rlimit_realtime_priority_hard
memory_vms	rlimit_signals_pending_hard
minor_faults	rlimit_signals_pending_soft
nice_priority	signals_pending
num_fds	voluntary_context_switches
num_threads	write_bytes
	write_count

7.3 Remediation

The remediation function for non-compliance has been implemented. As a result, when a compliance violation is detected, the smart change job specified in advance can be automatically executed, and the compliance violation can be resolved immediately.

Setting flow

1. Create a smart change job

Create a smart change job to be executed when a compliance violation occurs.

2. Create a non-compliance rule

Create a violation rule and link the rule with the smart change job.

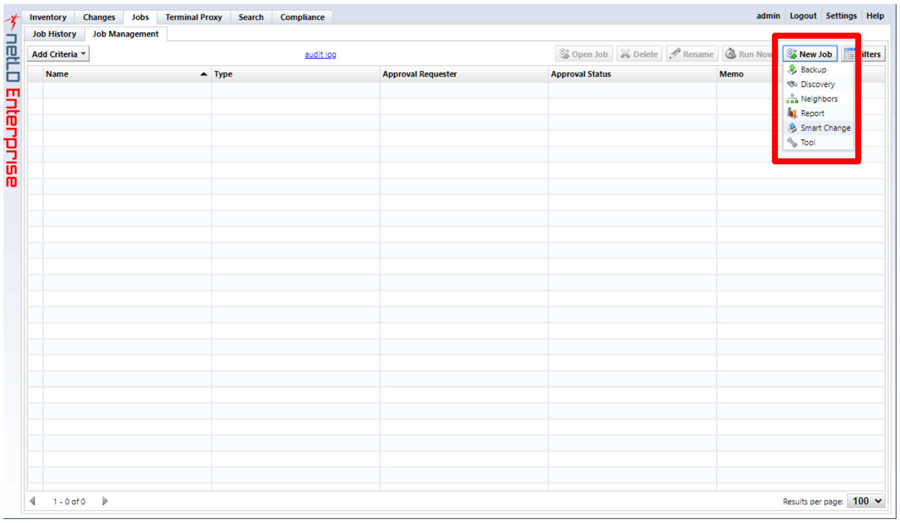
3. Creating a compliance policy

The compliance rule and the device are linked and set to be detected.

The following describes the setting method using a setting example.

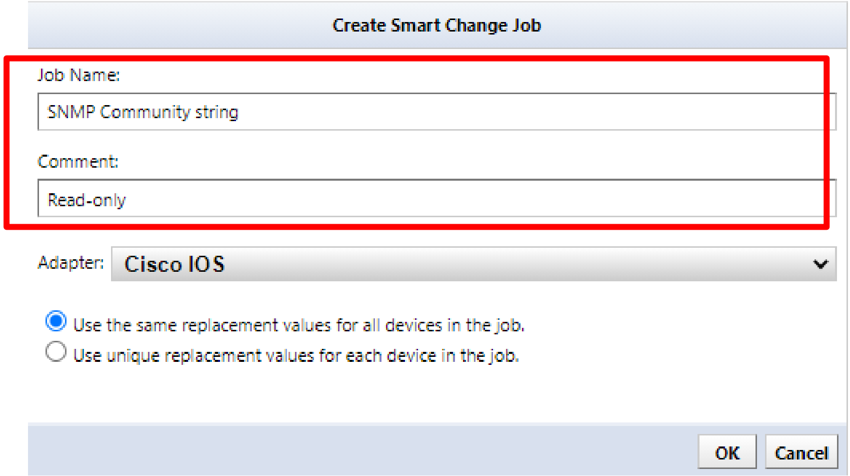
7.3.1 Create a Smart Change Job

1) Go to Job-> [Job Management] and select New Job-> [Smart change].



Name	Type	Approval Requester	Approval Status	Memo

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



Create Smart Change Job

Job Name: SNMP Community string

Comment: Read-only

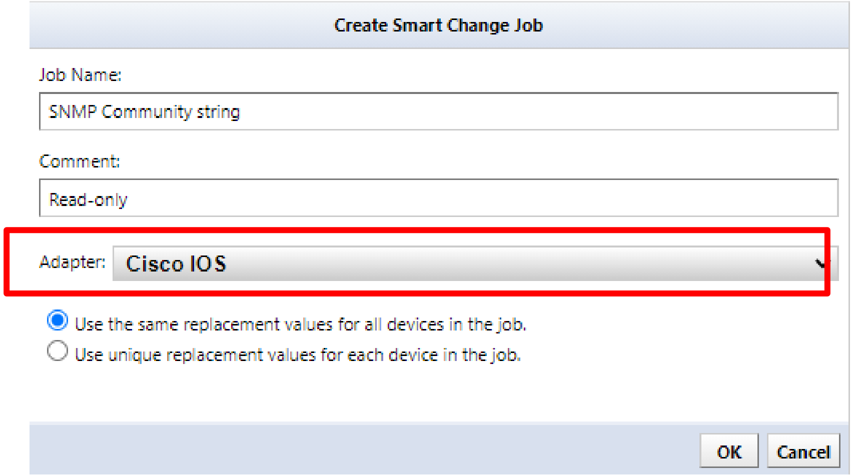
Adapter: Cisco IOS

● Use the same replacement values for all devices in the job.

○ Use unique replacement values for each device in the job.

3) Select the adapter for the device you want to apply and click OK.

※ Used for linking with the rule set.



Create Smart Change Job

Job Name: SNMP Community string

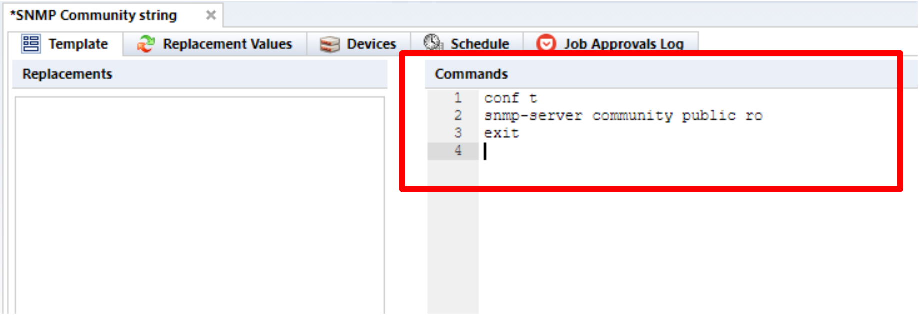
Comment: Read-only

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 to execute in the template.

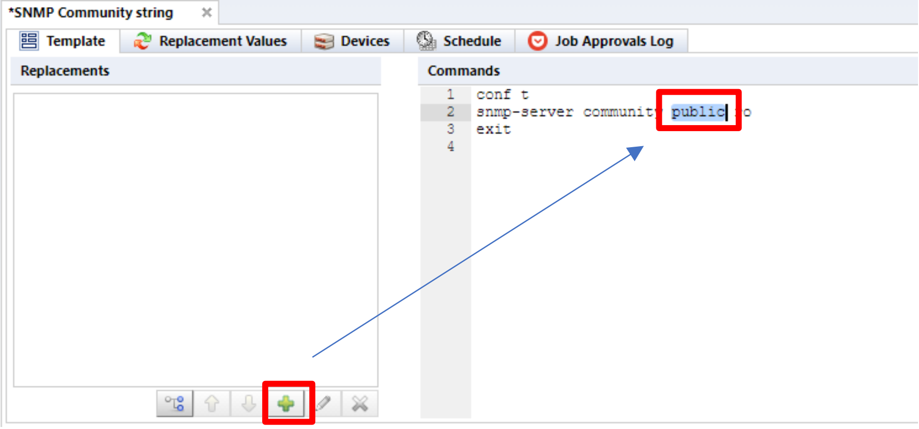


```
conf t
snmp-server community public ro
exit
```

5) Select the part you want to replace and click +.

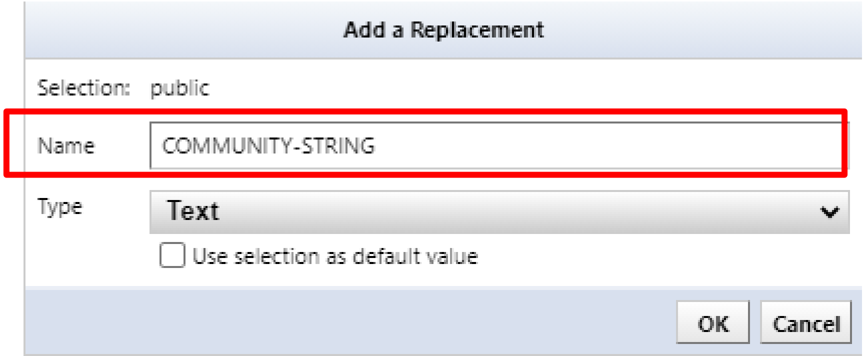
※ If you want to execute the command as it is without making it variable, skip this step.

※ In this case, the community name is obtained from the config, so the community name part is made variable.



```
conf t
snmp-server community public ro
exit
```

6) Enter the replacment name and click OK.



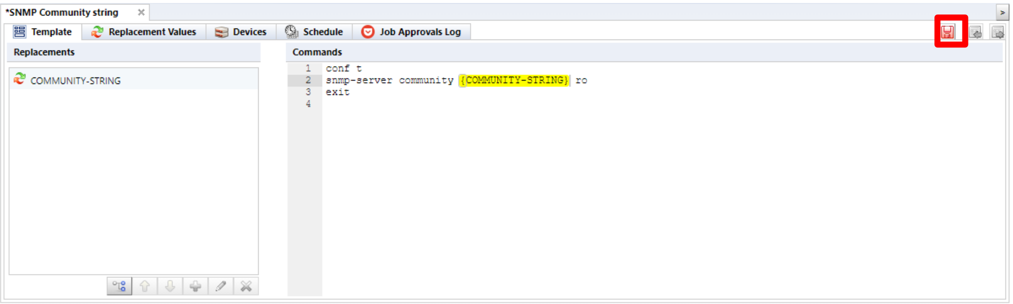
Selection: public

Name COMMUNITY-STRING

Type Text

□ Use selection as default value

7) Save.

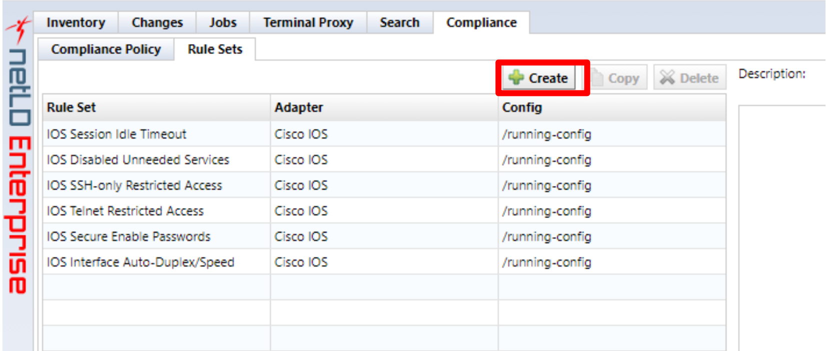


COMMUNITY-STRING

```
conf t
snmp-server community {COMMUNITY-STRING} ro
exit
```

7.3.2 Creating a RuleSet

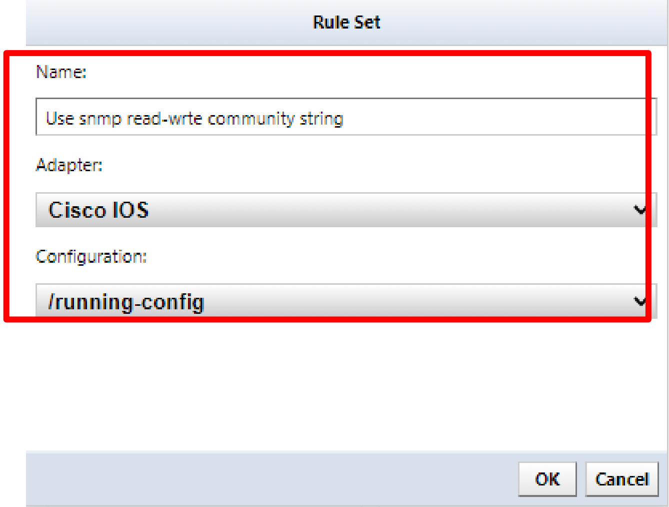
1) Go to Compliance-> [Rule sets] and click Create.



Rule Set	Adapter	Config
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

2) Enter the rule name, select the adapter, and click OK.

※ For the adapter, select the adapter selected when creating the smart change.

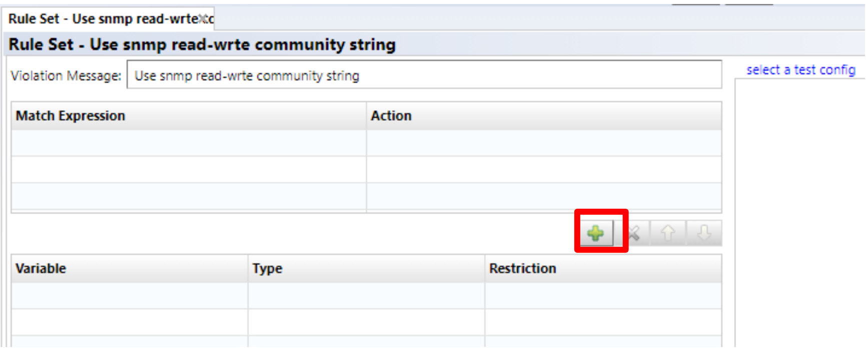


Name: Use snmp read-wrte community string

Adapter: Cisco IOS

Configuration: /running-config

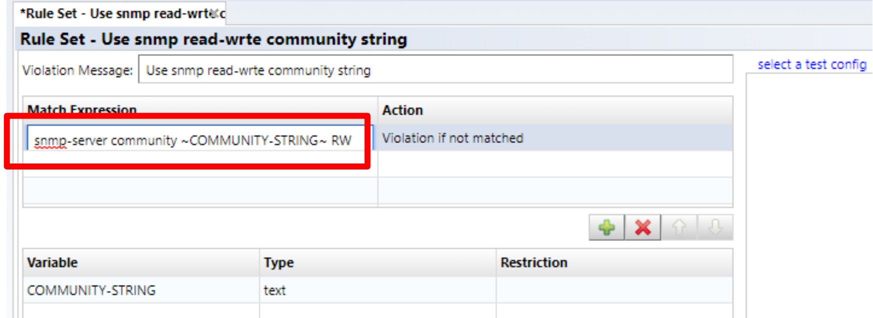
3) Click + to add a match condition.



Rule Set - Use snmp read-wrte community string

Violation Message: Use snmp read-wrte community string

4) Specify the community name part as the variable name of the smart change and put it between "~".



*Rule Set - Use snmp read-wrte c

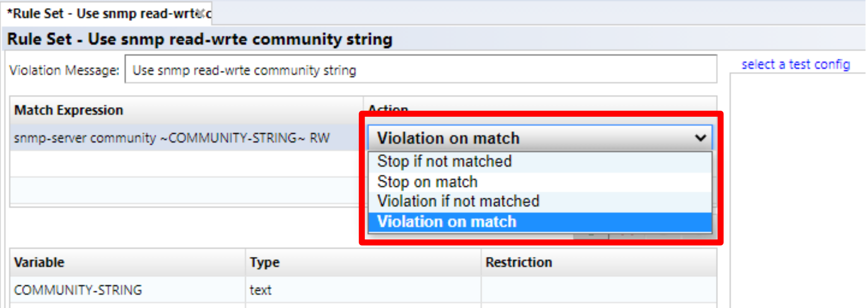
Rule Set - Use snmp read-wrte community string

Violation Message: Use snmp read-wrte community string

Match Expression	Action
snmp-server community ~COMMUNITY-STRING~ RW	Violation if not matched

Variable	Type	Restriction
COMMUNITY-STRING	text	

5) Set the action to Violation if matched.



*Rule Set - Use snmp read-wrte c

Rule Set - Use snmp read-wrte community string

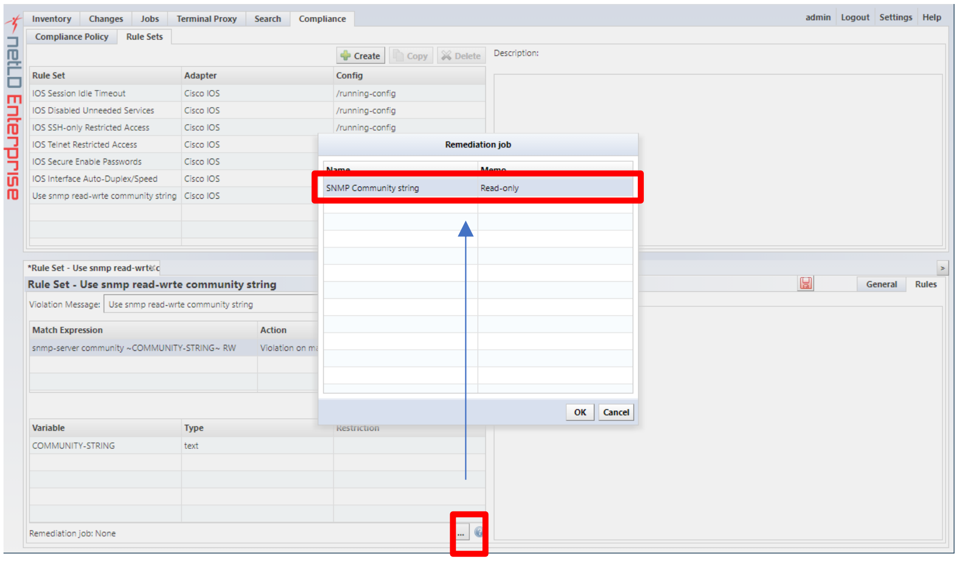
Violation Message: Use snmp read-wrte community string

Match Expression	Action
snmp-server community ~COMMUNITY-STRING~ RW	Violation on match

Variable	Type	Restriction
COMMUNITY-STRING	text	

6) Click the repair job "…" and specify the smart change job to run in the event of a violation.

※ Only one job can be specified.



Rule Set	Adapter	Config
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	
IOS Secure Enable Passwords	Cisco IOS	
IOS Interface Auto-Duplex/Speed	Cisco IOS	
Use snmp read-wrte community string	Cisco IOS	

Remediation job

Name	Memo
SNMP Community string	Read-only

*Rule Set - Use snmp read-wrte c

Rule Set - Use snmp read-wrte community string

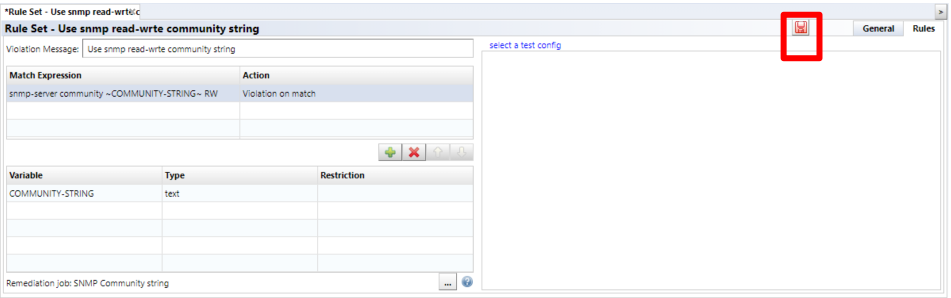
Violation Message: Use snmp read-wrte community string

Match Expression	Action
snmp-server community ~COMMUNITY-STRING~ RW	Violation on ma

Variable	Type	Restriction
COMMUNITY-STRING	text	

Remediation Job: None

7) Save your settings.



*Rule Set - Use snmp read-wrte c

Rule Set - Use snmp read-wrte community string

Violation Message: Use snmp read-wrte community string

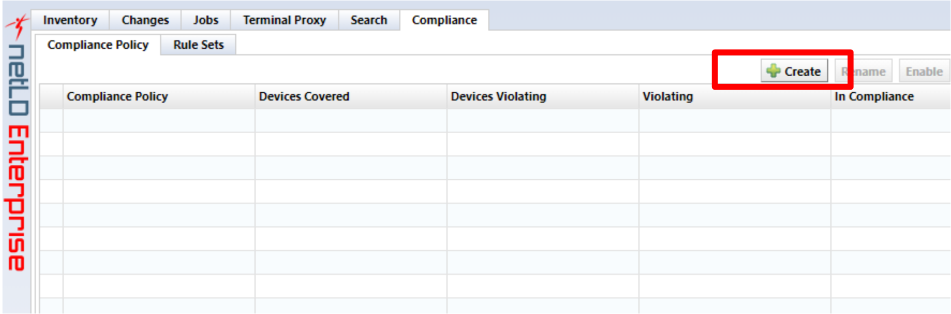
Match Expression	Action
snmp-server community ~COMMUNITY-STRING~ RW	Violation on match

Variable	Type	Restriction
COMMUNITY-STRING	text	

Remediation job: SNMP Community string

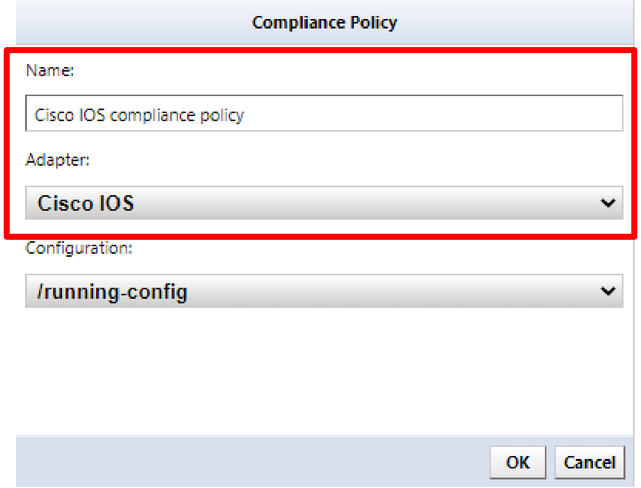
7.3.3 Creating a compliance policy

① Go to Compliance-> [Compliance Policy] and click Create.



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance

② After entering the name, select the adapter and target configuration file and click OK.



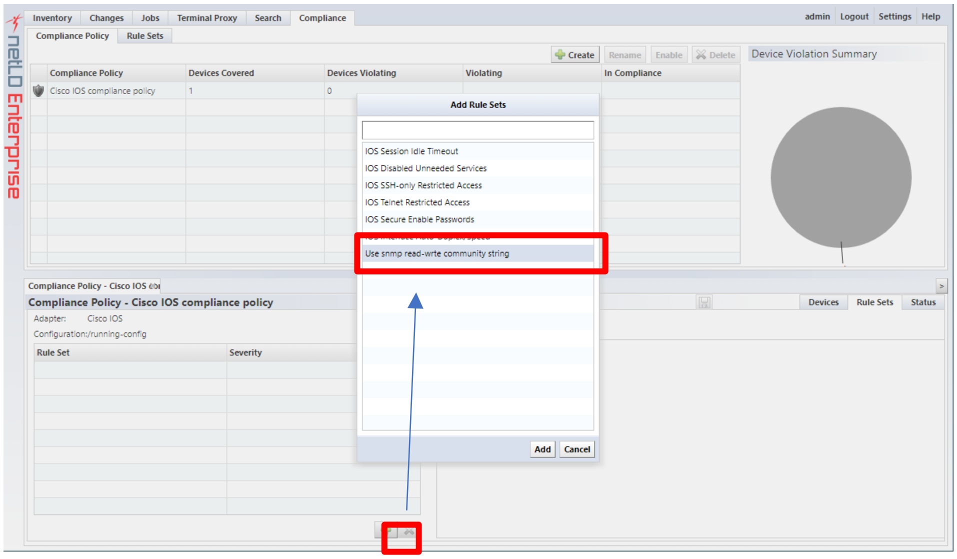
Compliance Policy

Name: Cisco IOS compliance policy

Adapter: Cisco IOS

Configuration: /running-config

③ Click + to add a ruleset.



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS compliance policy	1	0		

Add Rule Sets:

- IOS Session Idle Timeout
- IOS Disabled Unneeded Services
- IOS SSH-only Restricted Access
- IOS Telnet Restricted Access
- IOS Secure Enable Passwords
- Use snmp read-wrte community string

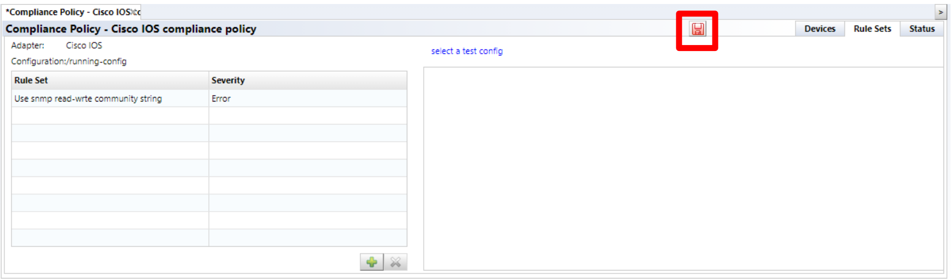
Compliance Policy - Cisco IOS compliance policy

Adapter: Cisco IOS

Configuration:/running-config

Rule Set	Severity

④ Click Save.



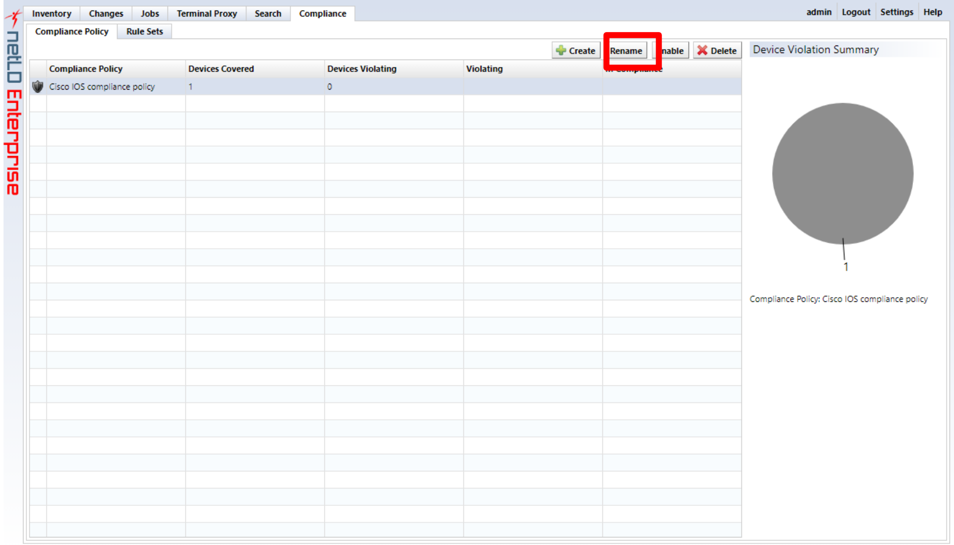
Compliance Policy - Cisco IOS compliance policy

Adapter: Cisco IOS

Configuration:/running-config

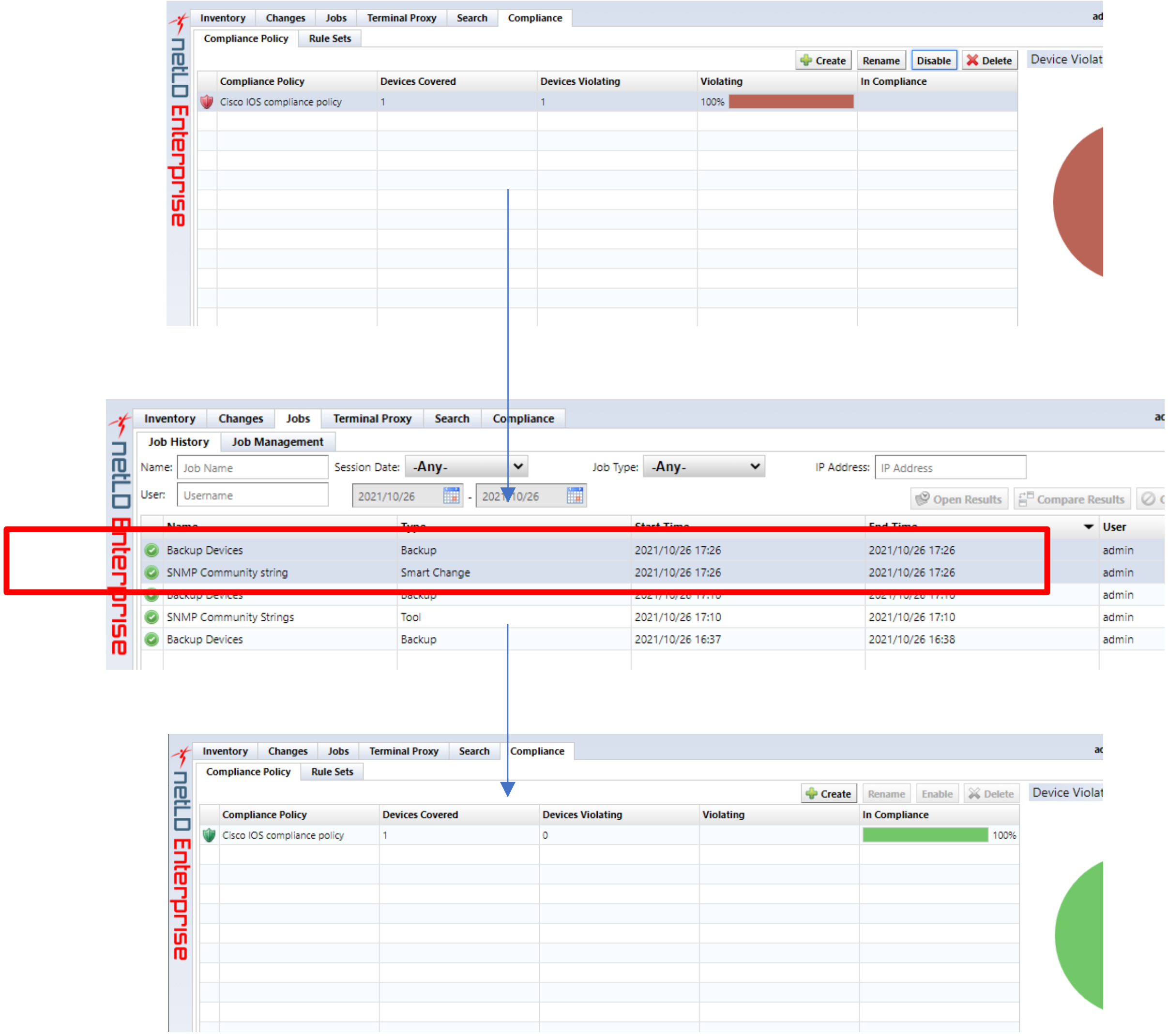
Rule Set	Severity
Use snmp read-wrte community string	Error

⑤ Select the compliance policy you created and click Enabled.



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS compliance policy	1	0		

When enabled, it will be checked immediately and if a violation is detected, it will be corrected automatically.



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS compliance policy	1	1	100%	

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

User: Username 2021/10/26 - 2021/10/26

Name	Type	Start Time	End Time	User
Backup Devices	Backup	2021/10/26 17:26	2021/10/26 17:26	admin
SNMP Community string	Smart Change	2021/10/26 17:26	2021/10/26 17:26	admin
Backup Devices	Backup	2021/10/26 17:10	2021/10/26 17:10	admin
SNMP Community Strings	Tool	2021/10/26 17:10	2021/10/26 17:10	admin
Backup Devices	Backup	2021/10/26 16:37	2021/10/26 16:38	admin

Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Cisco IOS compliance policy	1	0		100%

7.4 End of Sale/End of Life

You can update the system to show and report on devices where the software is, or when it will, expire, or show when a device is at end of life.

7.4.1 Cisco Support APIs onboarding

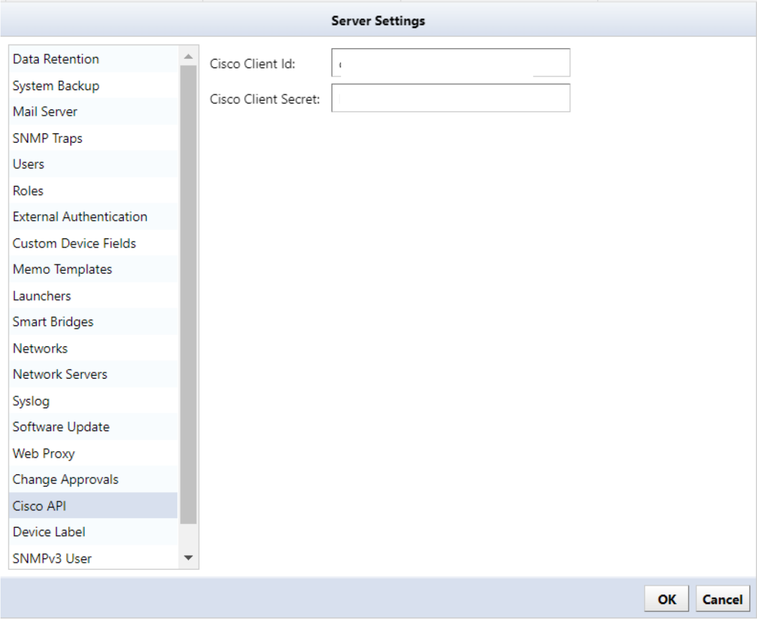
Every customer who wants to use a populating end of sale/end of life job for CISCO devices have to obtain api key and client secret from Cisco. Customers must have a valid Smart Net Total Care with Cisco to be able to obtain those keys.

7.4.2 Device's fields used for query

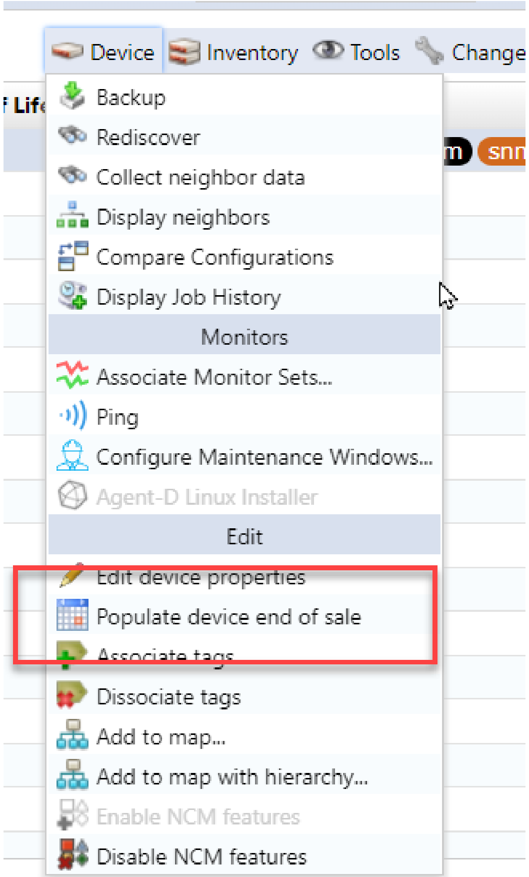
Device's HW vendor field is used to choose which manufacturer to fetch the data from.
For Cisco devices, Model and Serial number are used to query for the end of sale/end of life dates.

7.4.3 User Interface

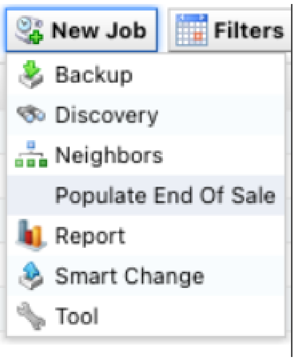
1. Cisco API keys settings – setup your Cisco client ID and secret. This can be found in settings under "Cisco API"



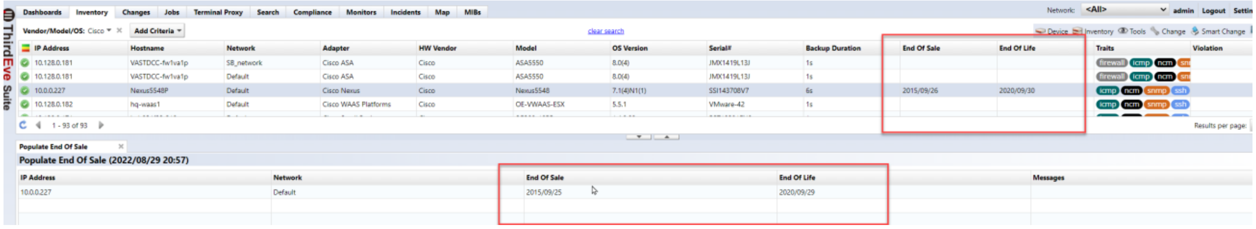
2. Ad-hoc population from Device menu



3. New Job – you can create a job that can be run to update the Cisco API for all, or specific, Cisco devices



4. Results from API call or job



IP Address	Hostname	Network	Adapter	HW Vendor	Model	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Traits	Violation
10.128.0.181	VASTDCC-fw1va1p	SB_network	Cisco ASA	Cisco	ASA5550	8.0(4)	JMX1419L13J	1s			firewall icmp ncm sn	
10.128.0.181	VASTDCC-fw1va1p	Default	Cisco ASA	Cisco	ASA5550	8.0(4)	JMX1419L13J	1s			firewall icmp ncm sn	
10.0.0.227	Nexus5548P	Default	Cisco Nexus	Cisco	Nexus5548	7.1(4)N1(1)	SSI143708V7	6s	2015/09/26	2020/09/30	icmp ncm snmp ssh	
10.128.0.182	hq-waas1	Default	Cisco WAAS Platforms	Cisco	OE-VWAAS-ESX	5.5.1	VMware-42	1s			icmp ncm snmp ssh	

Populate End Of Sale (2022/08/29 20:57)

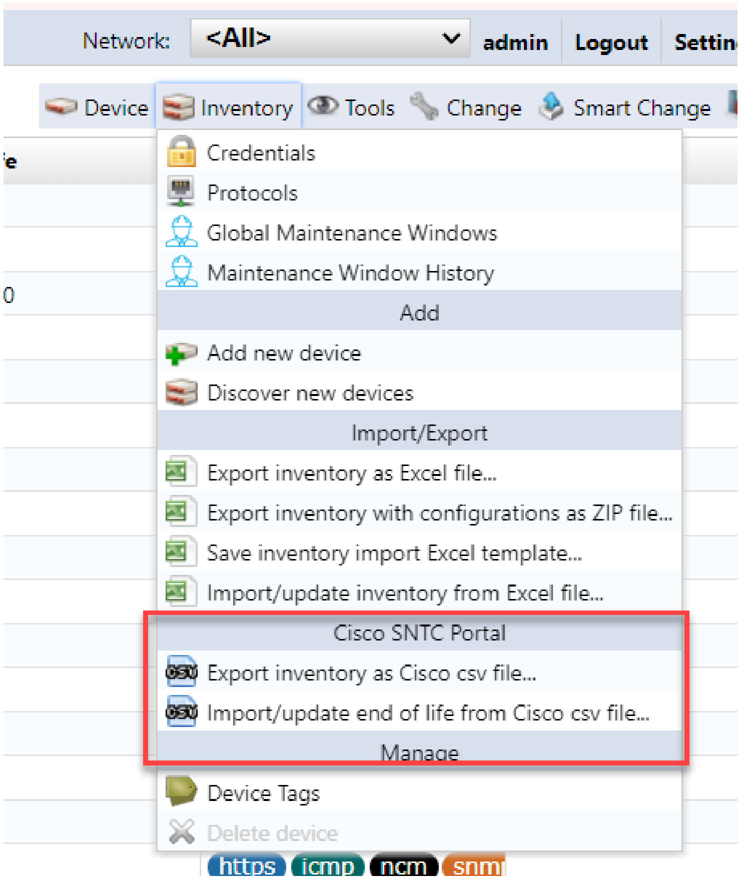
IP Address	Network	End Of Sale	End Of Life	Messages
10.0.0.227	Default	2015/09/25	2020/09/29	

7.4.4 Systems without Internet access

It's not possible to fetch end of sale dates from Cisco server without Internet access. However, users can export inventory as a csv file which can be used to import into Cisco Services. Then users can export a csv file from Cisco Services and import into the system to update end of life dates.

Please note that Cisco Services does not include end of sale dates in the export file.

To export a csv file that can be used to import into Cisco Services please select “Export inventory as Cisco csv file” from Inventory menu.


Network: <All>
admin
Logout
Settin
Device
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
https
icmp
ncm
snm

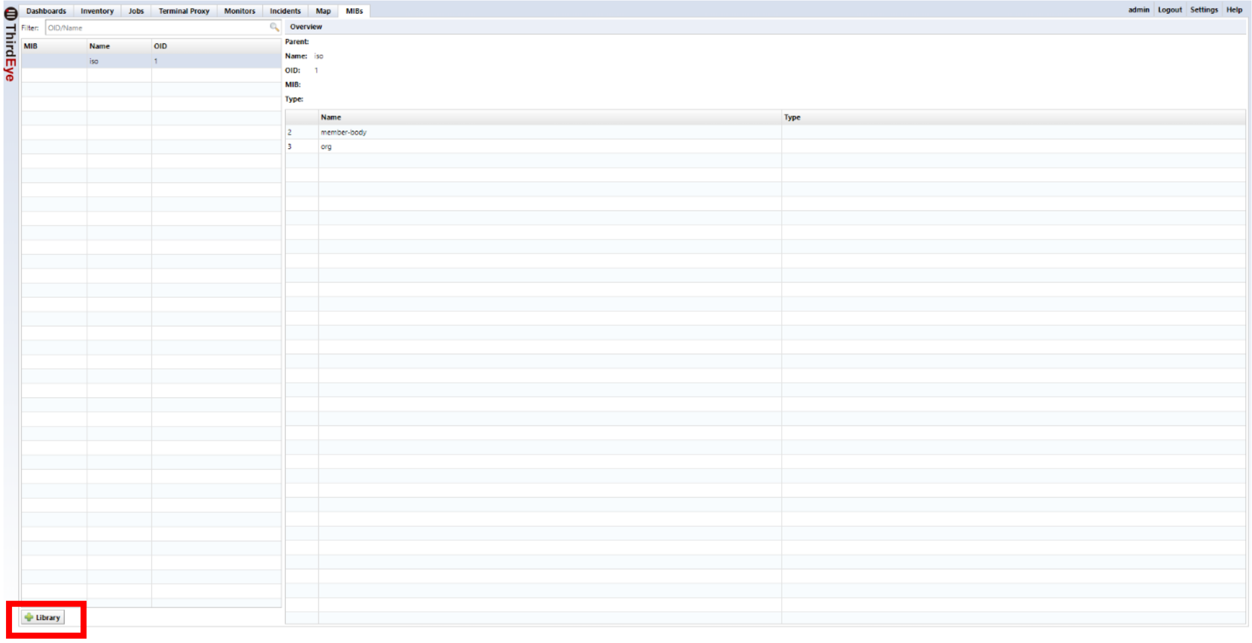
7.4.5 Reporting

In the Reporting section, there is a new report "End of Sale/End of Life" that can be run to generate a report showing any devices that have eos/eol tag. This report can also be setup to run as a job.

7.5 Compiling the MIB

You can add MIB files that have not been compiled to ThirdEye.

1. Click [Library] at the bottom left of the MIB screen.

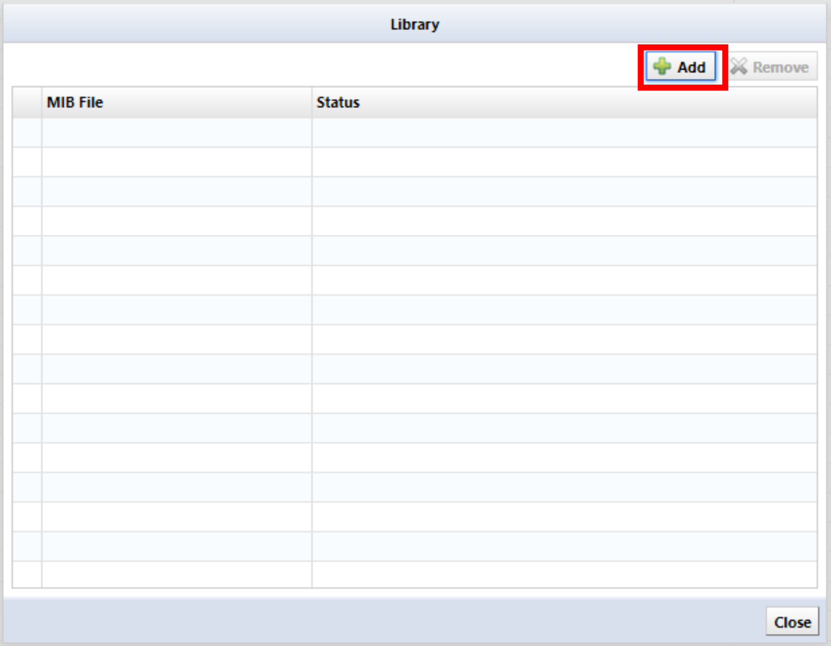


MIB	Name	OID
	iso	1

Parent:
Name: iso
OID: 1
MIB:
Type:

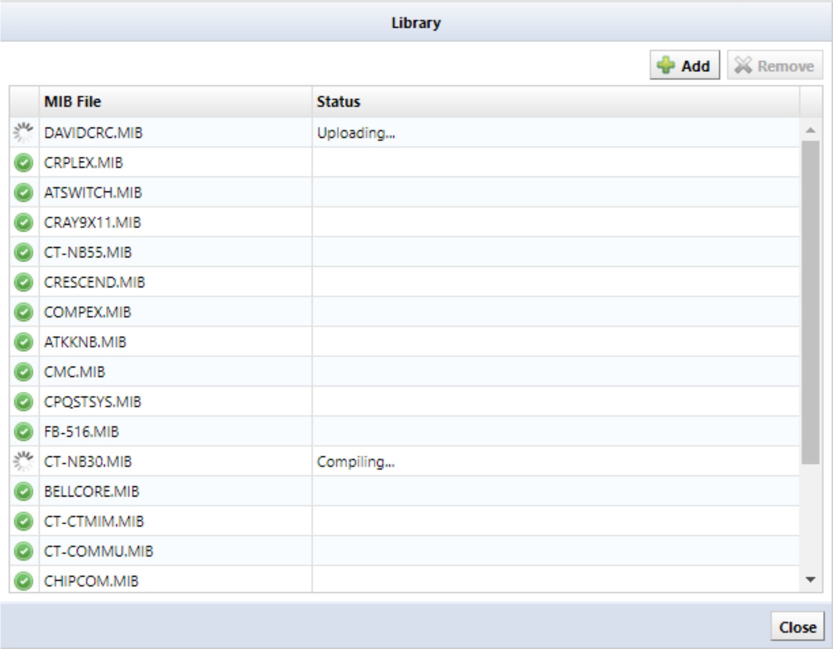
	Name	Type
2	member-body	
3	org	

2. The library screen is displayed. Click [Add].



Library
Add
Remove
MIB File
Status
Close

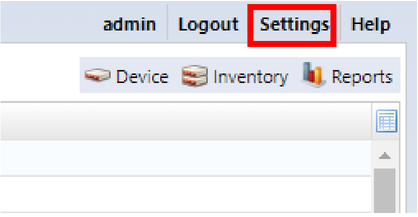
3. The file selection dialog is displayed. Select the MIB file to be compiled and click [Open]. The MIB file is displayed in the list. Compilation is complete when [✓ (green)] is displayed to the left of the MIB file.



	MIB File	Status
	DAVIDCRC.MIB	Uploading...
✓	CRPLEX.MIB	
✓	ATSWITCH.MIB	
✓	CRAY9X11.MIB	
✓	CT-NB55.MIB	
✓	CRESCEND.MIB	
✓	COMPEX.MIB	
✓	ATKKNB.MIB	
✓	CMC.MIB	
✓	CPQSTSYS.MIB	
✓	FB-516.MIB	
	CT-NB30.MIB	Compiling...
✓	BELLCORE.MIB	
✓	CT-CTMIM.MIB	
✓	CT-COMMU.MIB	
✓	CHIPCOM.MIB	

7.6 Registering users

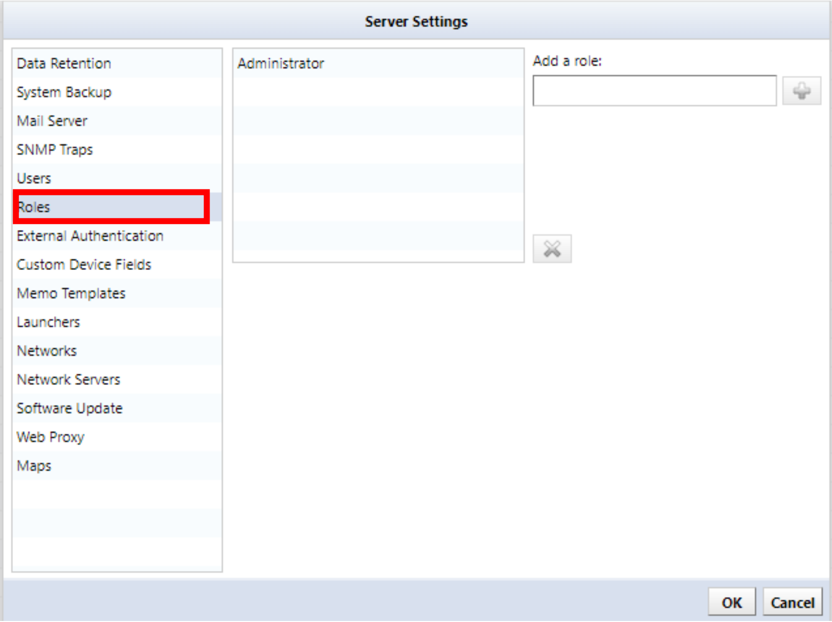
Create a user to log in to ThirdEye. By assigning permissions to users, you can limit the operations that users can perform. In ThirdEye, you can specify in detail by combining multiple permissions. Users and permissions can be set from [Settings] in the global menu.



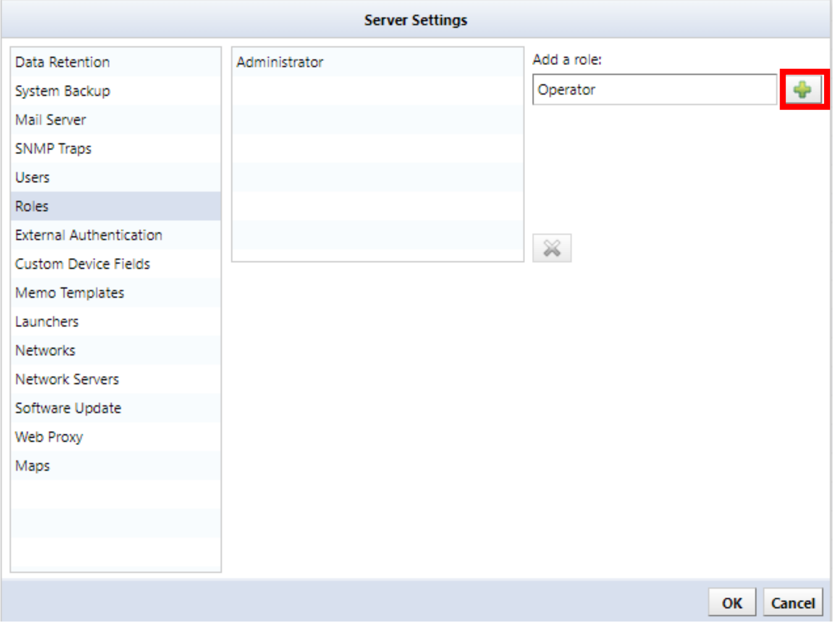
7.6.1 Adding permissions

* “Administrator” who has all execution rights is registered. This authority cannot be deleted.

1. Click [Roles].

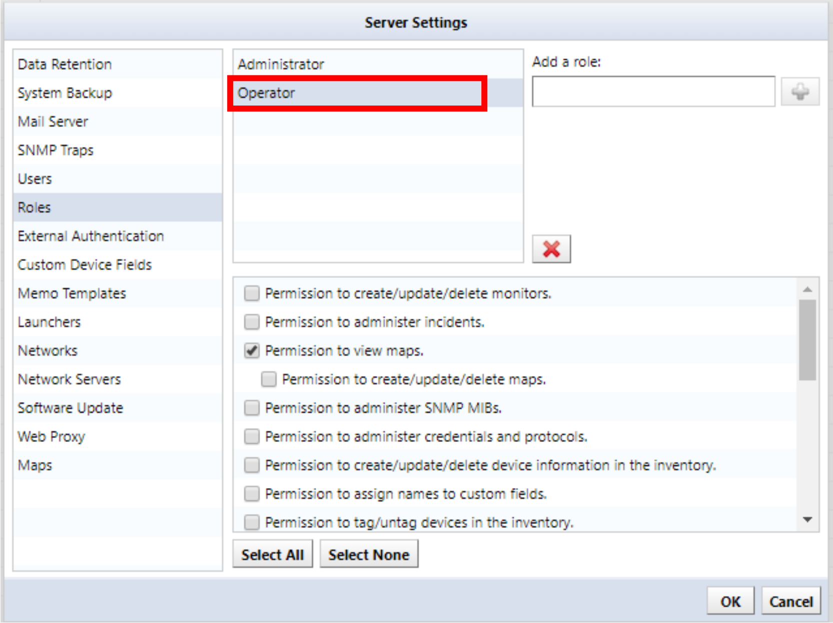


2. Enter the authority name in the [Add Authority] field and click [✚ (Add)].



Add a role: Operator

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



- □ 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 administer credentials and protocols.
- □ Permission to create/update/delete device information in the inventory.
- □ Permission to assign names to custom fields.
- □ Permission to tag/untag devices in the inventory.

No.	Description
1	Permission to create/update/delete monitors.
2	Permission to administer incidents.
3	Permission to view maps.

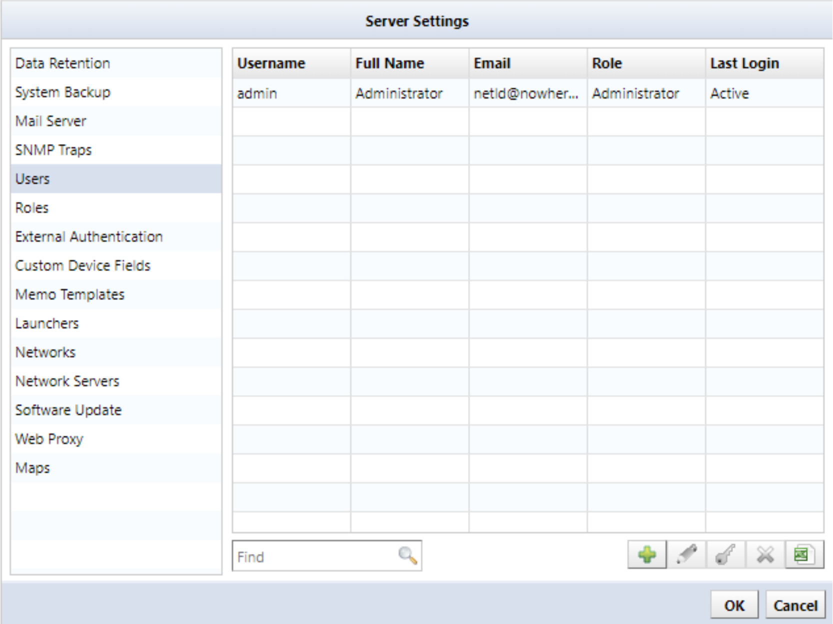
No.	Description
4	Permission to create/update/delete maps. (* No.3: Authority attached to "Permit map viewing")
5	Permission to administer SNMP MIBs.
6	Permission to administer credential and protocols.
7	Permission to create/update/delete device information in the inventory.
8	Permission to assign names to custom fields.
9	Permission to tag/untag devices in the inventory.
10	Permission to administer scheduler filters.
11	Permission to run a device discovery job.
12	Permission to create/update/delete a device discovery job. (* No. 11: Authority attached to "Permit discovery execution")
13	Permission to run a maintenance window job.
14	Permission to create/update/delete a maintenance window job. (* No.13: Authority attached to "Permit execution of unmonitored jobs")
15	Permission to run a report.
16	Permission to create/update/delete a report job. (* No.15: Authority attached to "Permit report execution")
17	Permission to create/update/delete URL launchers.
18	Permission to create/update/delete memos.
19	Permission to create/update/delete managed networks.
20	Permission to security settings.
21	Permission to create/update/delete inventory tags.
22	Permission to login using the terminal server proxy.
23	Permission to view other users' terminal proxy logs.

4. Click on [OK].

7.6.2 Adding users

* "Admin" user is registered. This user cannot be deleted.

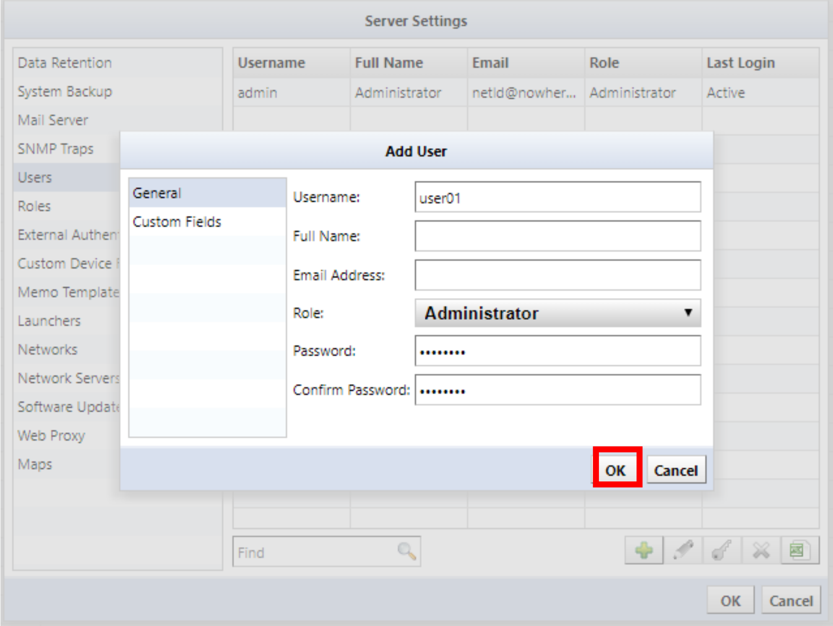
1. Click [✚ (Add)].



Server Settings

Username	Full Name	Email	Role	Last Login
admin	Administrator	netld@nowher...	Administrator	Active

2. The Add User screen is displayed. Enter the items and click [OK].



Add User

Username: user01

Full Name:

Email Address:

Role: Administrator

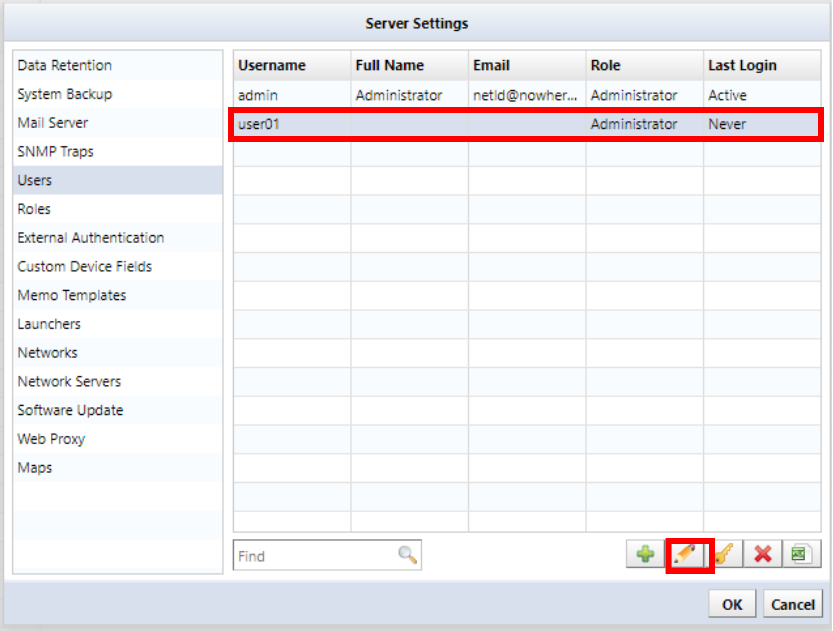
Password: ••••••••

Confirm Password: ••••••••

Category	Item	Explanation	Required
General	Username	Enter your username.	✓
	Full name	Enter the user's full name.	×
	Email Address	Enter the user's email address.	×
	Role	Select user permissions. The authority set in "7.3.1 Adding authority" can be selected from the pull-down menu.	✓
	Password	Set the user's password.	✓
Custom Fields	Custom 1～5	Select custom device fields that users can view. * The displayed item name changes based on the setting in "7.7 Change column name of custom device field".	×

7.6.3 Changing user information

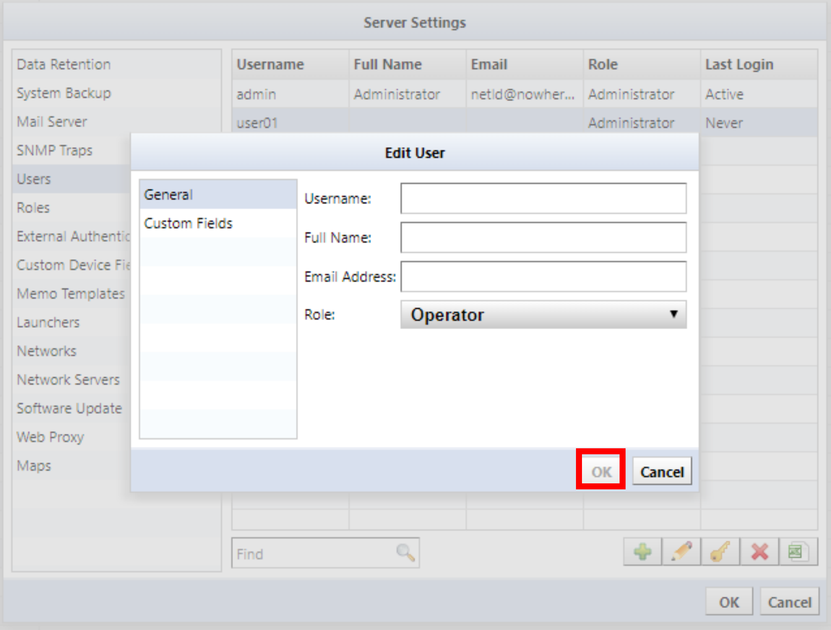
1. Select the user you want to edit and click [✏(Edit)].



Username	Full Name	Email	Role	Last Login
admin	Administrator	netld@nowher...	Administrator	Active
user01			Administrator	Never

2. The user edit screen is displayed. After editing, click [OK].

   * Username cannot be changed. If you want to change the password, set from [🔑(Key)].



Username	Full Name	Email	Role	Last Login
admin	Administrator	netid@nowher...	Administrator	Active
user01			Administrator	Never

Username:

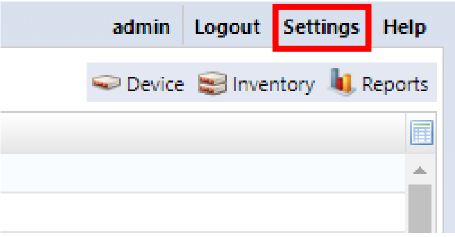
Full Name:

Email Address:

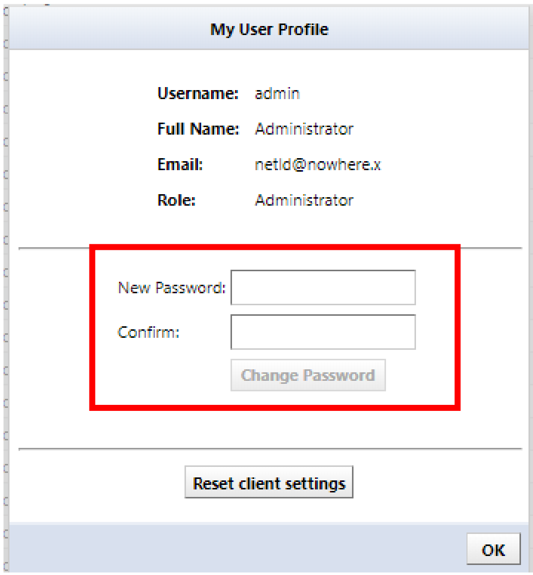
Role: Operator

7.6.4 Changing the password of the logged-in user

You can change the password from the login username in the global menu. Here, the password for the username “admin” is changed.



Fill in the new password and password re-entry fields. Press the password change button to register a new password. If the new password and the re-entered string are different, the password change button will not be enabled.



Username: admin

Full Name: Administrator

Email: netId@nowhere.x

Role: Administrator

New Password:

Confirm:

7.6.5 Linking with Active Directory or RADIUS server

With external authentication, you can log in to ThirdEye in cooperation with an authentication server that manages user information. This eliminates the need to register all users in advance in ThirdEye, reducing the work required during installation and organizational changes. External authentication can be set from [Settings] → [External Authentication] in the global menu.

i. RADIUS integration

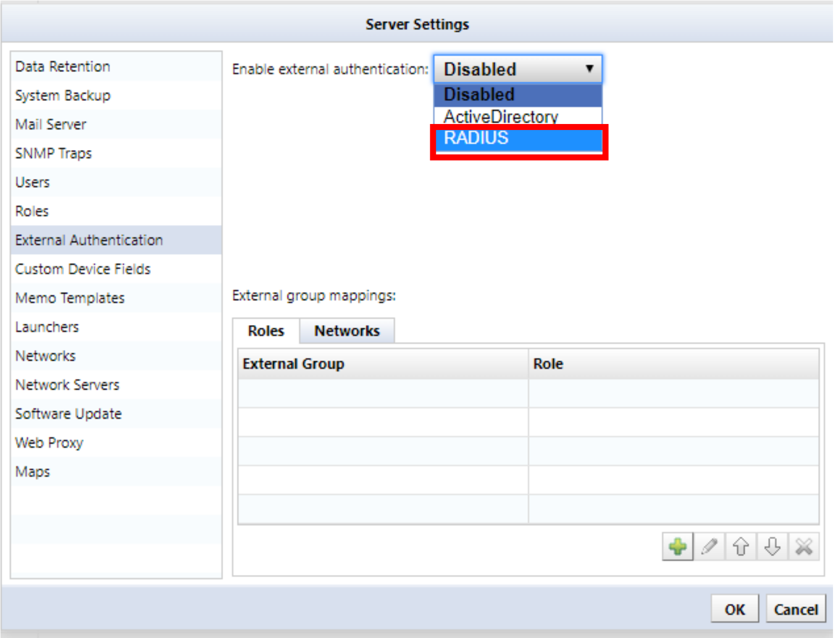
Sends an Access-Request to the RADIUS server for authentication. In order to cooperate with the RADIUS server, it is necessary to set to send Access-Accept with Filter-Id.

Below is a sample of FreeRADIUS user settings.

```
LogicVein     Cleartext-Password := "password"
  Filter-Id += "GROUP"
```

This setting sends **Access-Accept** with filter-id when you receive **the Access-Request** for "Username: LogicVein, Password:password".

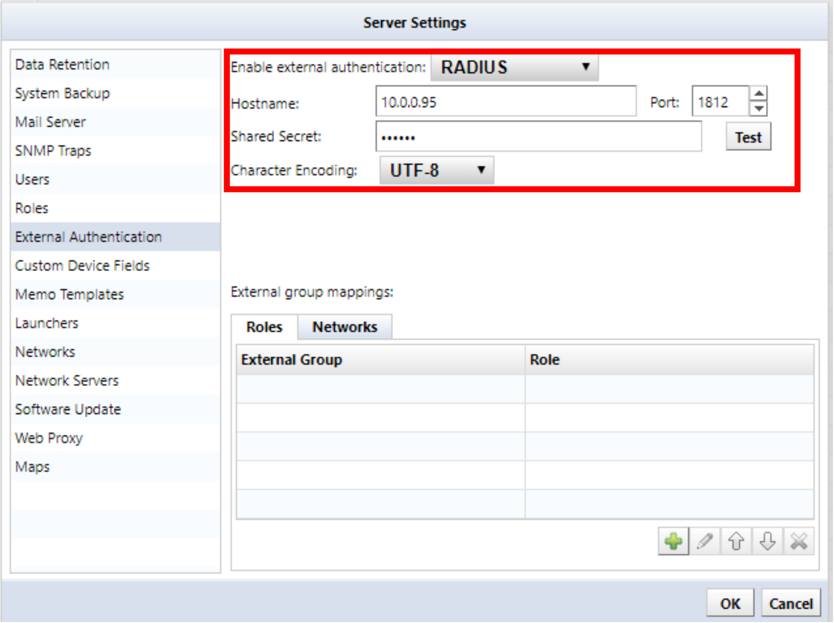
1. Change the external authentication server selection from disabled to "RADIUS".



Enable external authentication: Disabled

External group mappings:

2. Set the IP address (or host name) and shared secret of the RADIUS server.



Enable external authentication: RADIUS

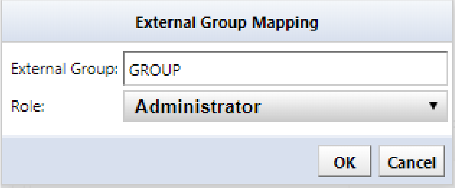
Hostname: 10.0.0.95 Port: 1812

Shared Secret: ••••••

Character Encoding: UTF-8

External group mappings:

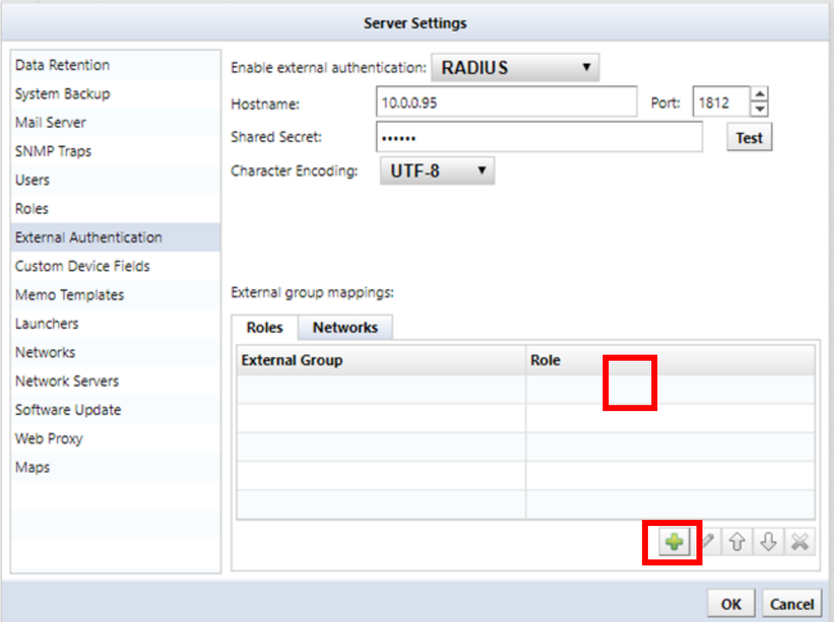
3. Set permissions for external group mapping. Add a new one from [➕ (Add)].



External Group: GROUP

Role: Administrator

4. Enter the group set in Filter-Id of the RADIUS server in the external group and select the authority to be assigned.



Enable external authentication: RADIUS

Hostname: 10.0.0.95 Port: 1812

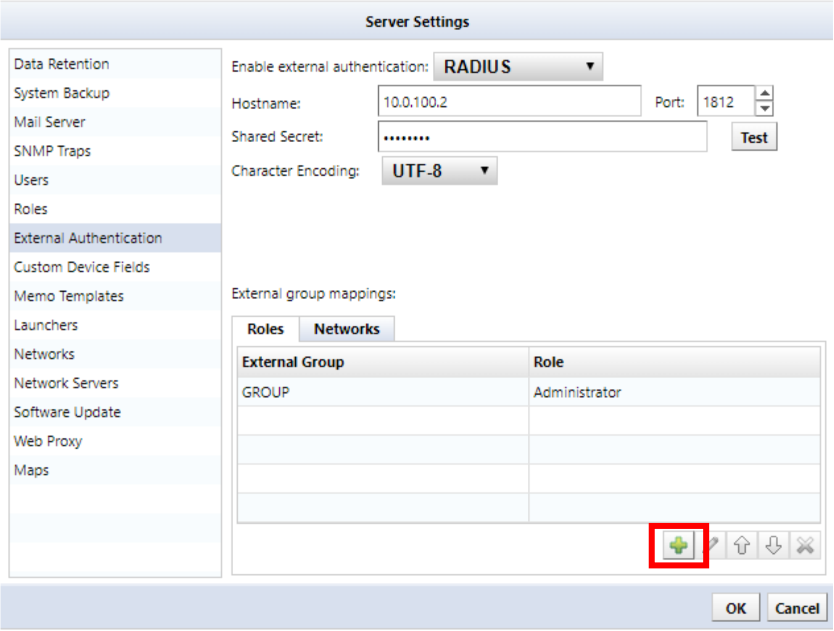
Shared Secret: ••••••

Character Encoding: UTF-8

External group mappings:

External Group	Role

5. Configure the network for external group mapping. Add a new one from [✚(Add)].



Enable external authentication: RADIUS

Hostname: 10.0.100.2 Port: 1812

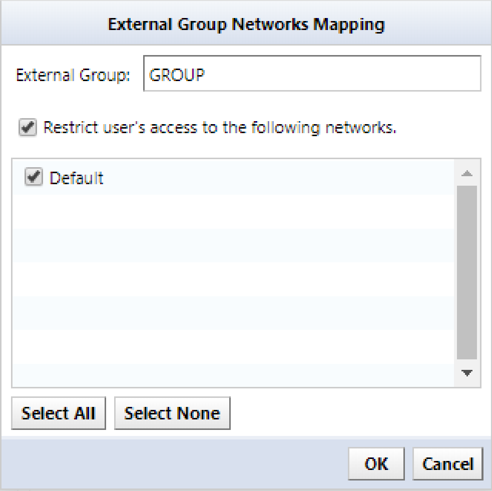
Shared Secret: ••••••••

Character Encoding: UTF-8

External group mappings:

External Group	Role
GROUP	Administrator

6. Select the network that can be browsed by entering the group set in the RADIUS server Filter-Id in the external group as well as the authority.



External Group Networks Mapping

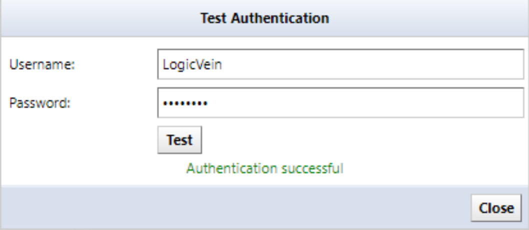
External Group: GROUP

☑ Restrict user's access to the following networks.

☑ Default

* You can browse networks with a check.

7. After setting, enter the username and password from the test, and click the test to check the cooperation with the RADIUS server. If there is no problem, “Authentication was successful” is displayed.



Test Authentication

Username: LogicVein

Password: ••••••••

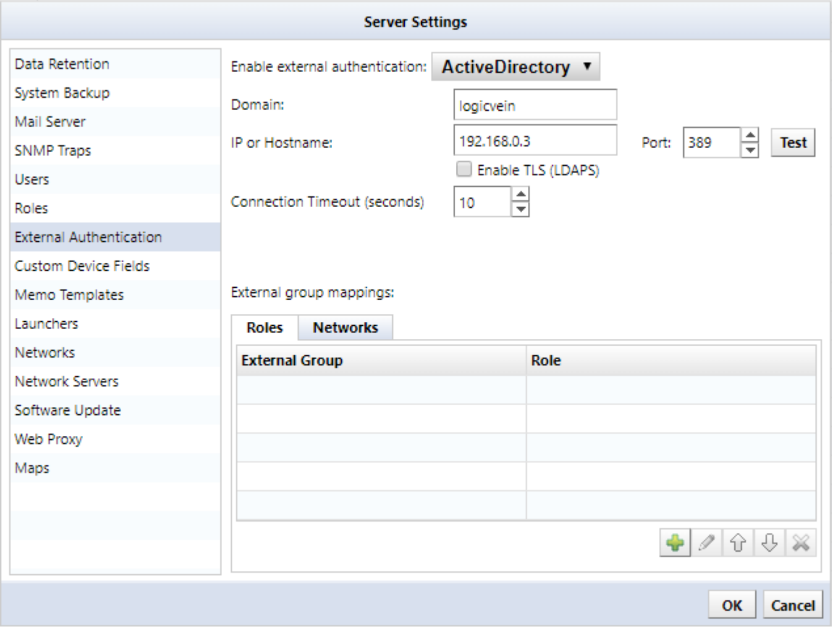
Authentication successful

The setting is now complete. Click [OK] to save the server settings, log out, and log in as the user set in the RADIUS server.

ii. Active Directory linkage

When linking with Active Directory server, authority and network are determined using the group to which the registered user belongs.

1. Change the external authentication server selection from disabled to "Active Directory".
2. Set the domain name and IP address (or host name) of the Active Directory server as follows. Set permissions for external group mapping. Add a new one from [✚ (Add)].



Server Settings

Enable external authentication: ActiveDirectory

Domain: logicvein

IP or Hostname: 192.168.0.3 Port: 389

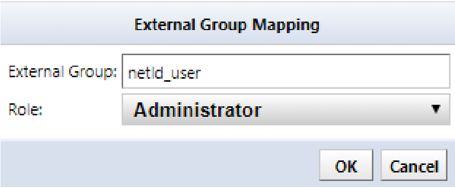
☐ Enable TLS (LDAPS)

Connection Timeout (seconds) 10

External group mappings:

External Group	Role

3. Enter the group to which the user belongs in the external group and select the right to assign.

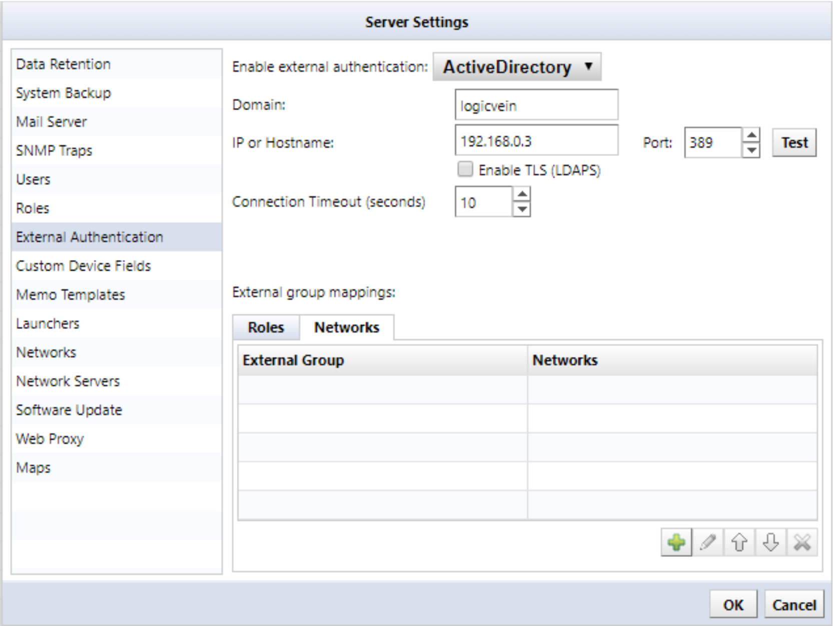


External Group Mapping

External Group: netld_user

Role: Administrator

4. Configure the network for external group mapping. Add a new one from [✚ (Add)].



Enable external authentication: ActiveDirectory

Domain: logicvein

IP or Hostname: 192.168.0.3 Port: 389

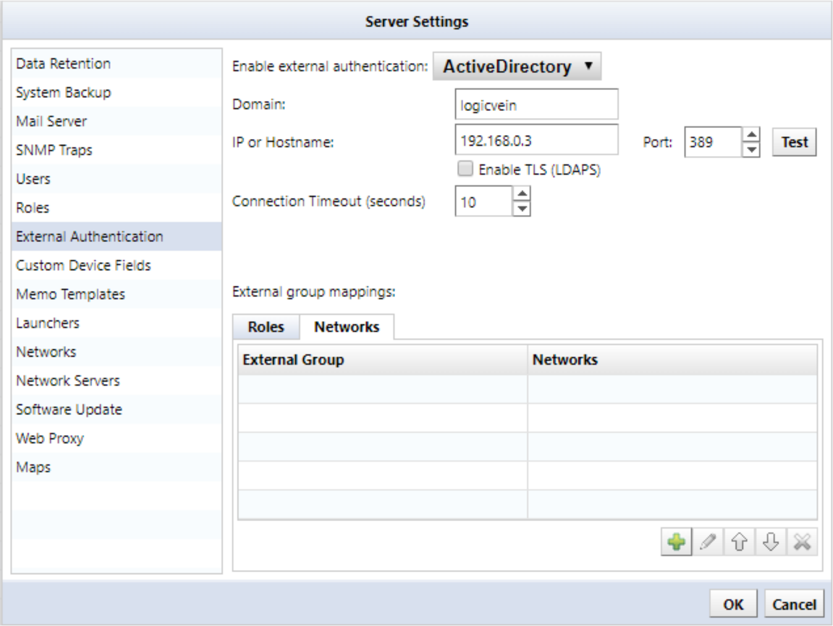
□ Enable TLS (LDAPS)

Connection Timeout (seconds) 10

External group mappings:

External Group	Networks

5. As with the authority, enter the group to which the user belongs in the external group and select the network that can be viewed.



Enable external authentication: ActiveDirectory

Domain: logicvein

IP or Hostname: 192.168.0.3 Port: 389

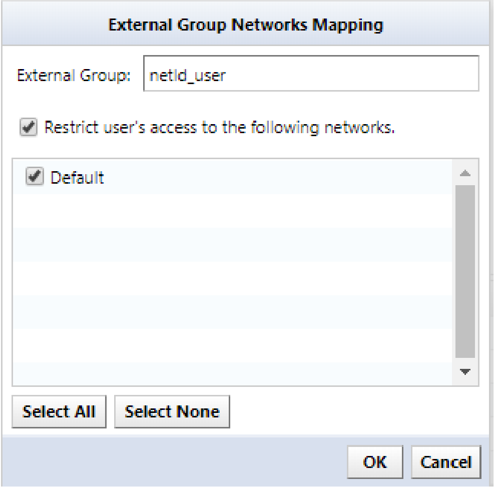
□ Enable TLS (LDAPS)

Connection Timeout (seconds) 10

External group mappings:

External Group	Networks

6. After setting, enter the username and password from the test, and click the test to check the linkage with the Active Directory server. If there is no problem, “Authentication was successful” is displayed.

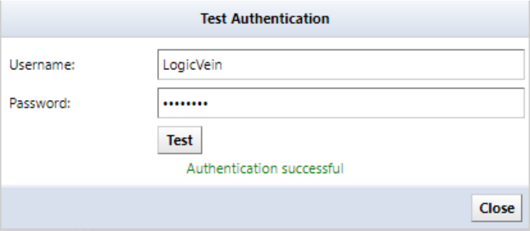


External Group: netId_user

☑ Restrict user's access to the following networks.

☑ Default

This completes the setting. Click [OK] to save the server settings, log out, and log in as a user set in the Active Directory server.



Username: LogicVein

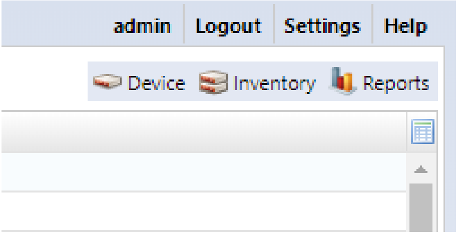
Password: ••••••••

Authentication successful

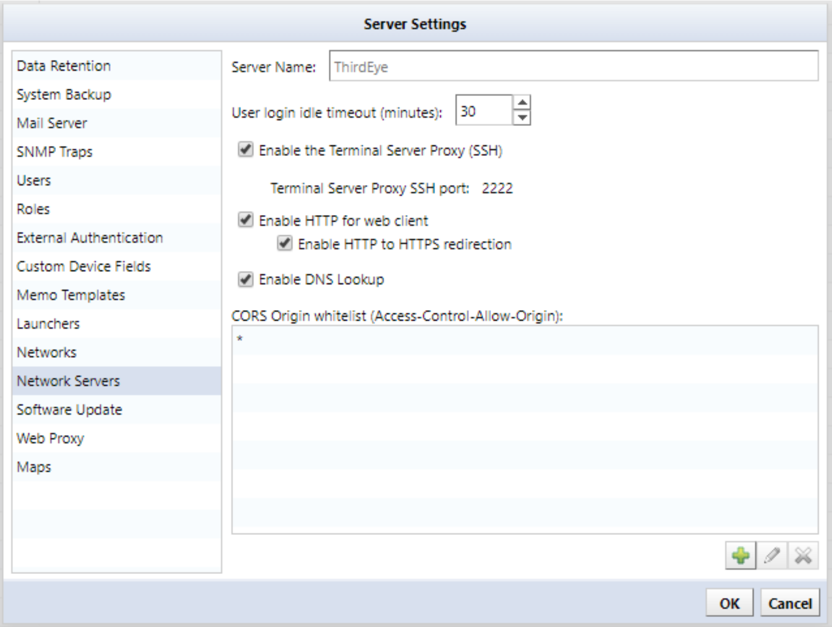
7.6.6 Setting user session timeout

With ThirdEye, users who have not operated for 30 minutes will need to authenticate again. To change this time, follow the procedure below.

1. Click [Settings] in the global menu.



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



Server Settings

Server Name: ThirdEye

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

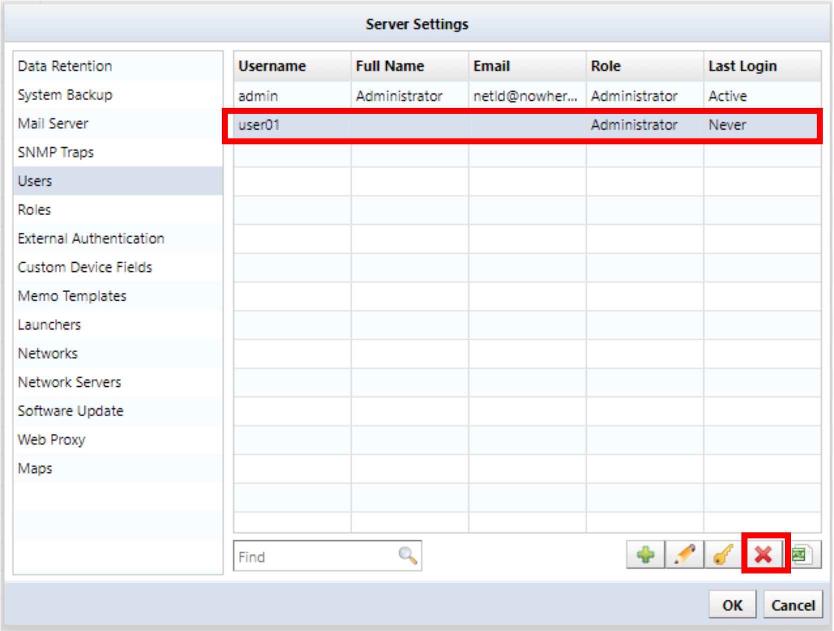
CORS Origin whitelist (Access-Control-Allow-Origin):

*

3. Click [OK].

7.6.7 Deleting a user

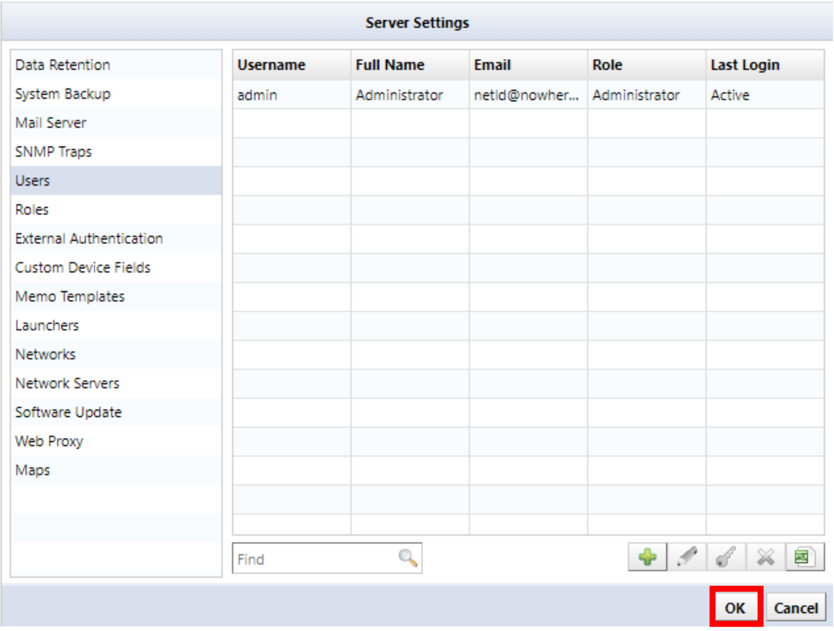
1. Select the authority name you want to delete and click [✖ (Delete)].



Username	Full Name	Email	Role	Last Login
admin	Administrator	netid@nowher...	Administrator	Active
user01			Administrator	Never

2. Click [OK] in the server settings.

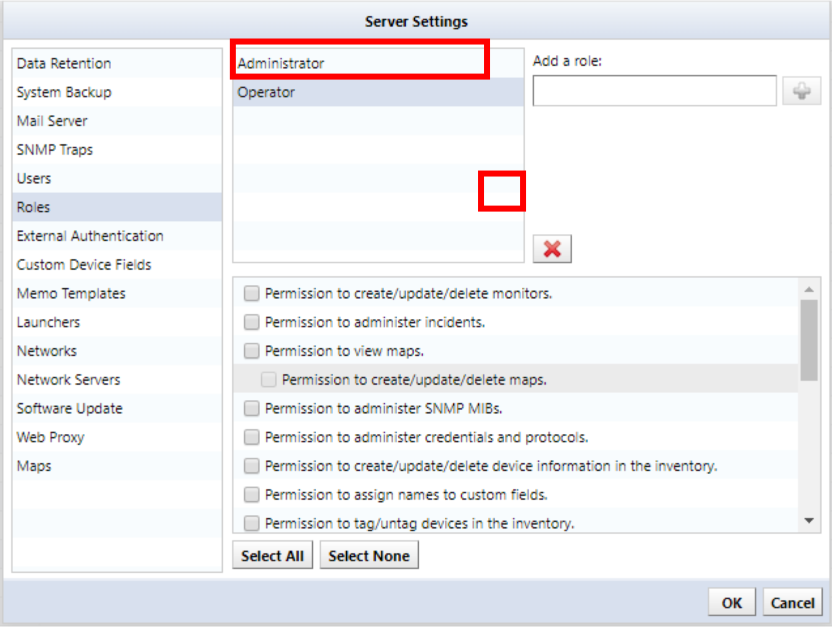
* If you have deleted the user by mistake, click [Cancel].



Username	Full Name	Email	Role	Last Login
admin	Administrator	netid@nowher...	Administrator	Active

7.6.8 Deleting permissions

1. Select the authority name you want to delete and click [✖ (Delete)].



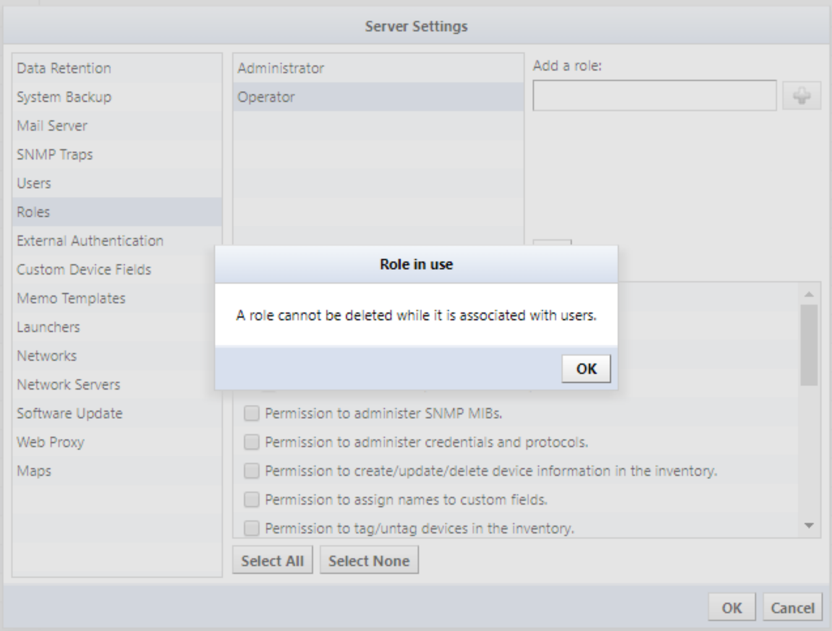
☐ Permission to create/update/delete monitors.
☐ Permission to administer incidents.
☐ Permission to view maps.
☐ Permission to create/update/delete maps.
☐ Permission to administer SNMP MIBs.
☐ Permission to administer credentials and protocols.
☐ Permission to create/update/delete device information in the inventory.
☐ Permission to assign names to custom fields.
☐ Permission to tag/untag devices in the inventory.

2. Click [OK] in the server settings.

* If you try to delete the authority being used, the following error will occur.

You cannot delete permissions that have been applied to users.

Please execute the deletion after reassigning the authority of the user being used.

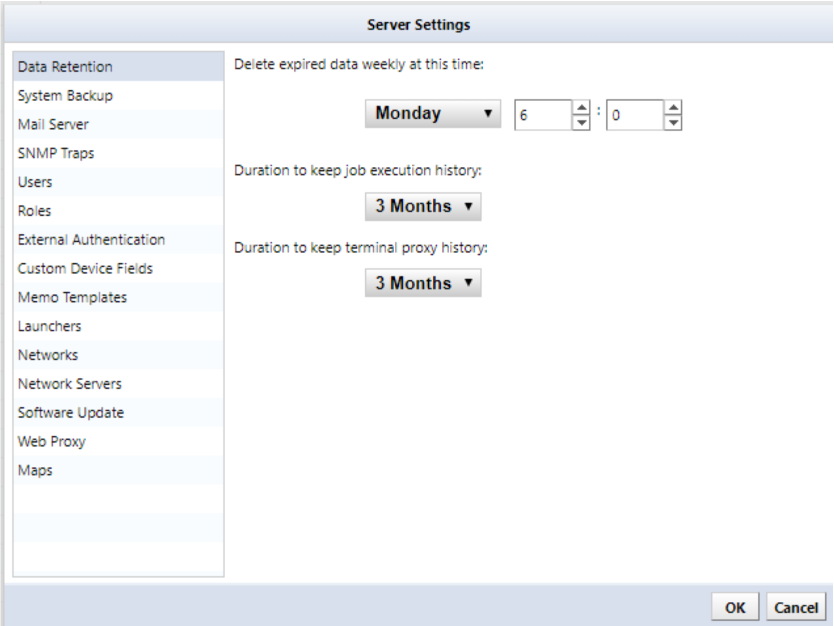


A role cannot be deleted while it is associated with users.

☐ Permission to administer SNMP MIBs.
☐ Permission to administer credentials and protocols.
☐ Permission to create/update/delete device information in the inventory.
☐ Permission to assign names to custom fields.
☐ Permission to tag/untag devices in the inventory.

7.7 Changing the data retention period

In the data retention period, set the data retention period and the automatic deletion timing.



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

Duration to keep job execution history: 3 Months

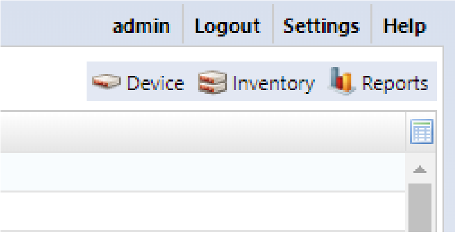
Duration to keep terminal proxy history: 3 Months

Description	Explanation
Delete expired date weekly this time	Data that has passed for a certain period is automatically deleted every week on the specified day of the week and time. (Initial value: Monday, 6:00) The data retention period is specified in the following items. (* If “No Expiration Date” is specified, data will not be deleted.)
Duration to keep job execution history	Specify the data retention period from [Jobs] → [Job History] from the following. (Initial value: 3 months) Unlimited", "3 months", "6 months", "9 months", "1 year"
Duration to keep terminal proxy history	Specify the data retention period on the [Terminal Proxy] tab from the following. (Initial value: 3 months) "Unlimited", "3 months", "6 months", "9 months", "1 year"

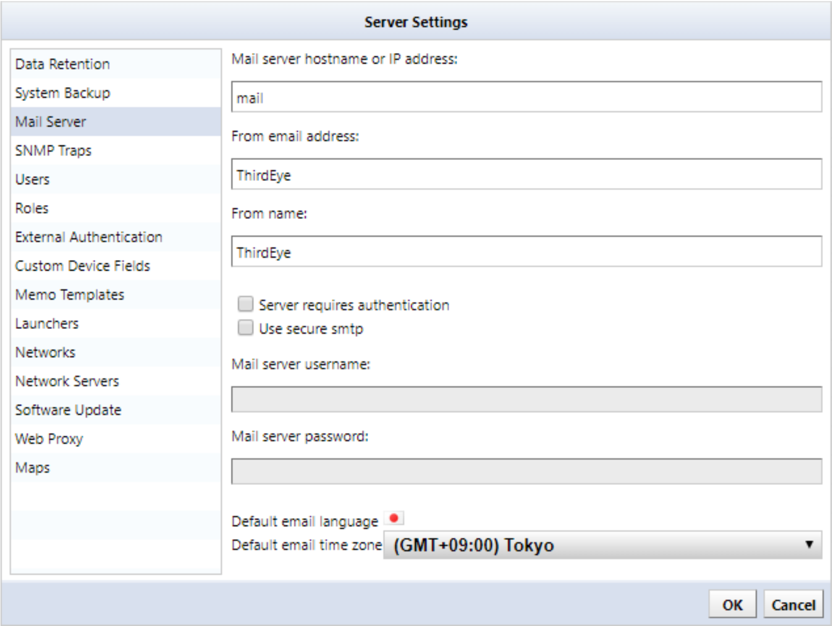
7.8 Setting up mail server

In the mail server, enter the SMTP server information for email notification from ThirdEye. If you want to send an e-mail or a dashboard report in the event of a failure, you need to set in advance.

1. Click [Settings] in the global menu.



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



Mail server hostname or IP address: mail

From email address: ThirdEye

From name: ThirdEye

□ Server requires authentication

□ Use secure smtp

Mail server username:

Mail server password:

Default email language

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

Description	Explanation
Hostname/IP address	Set the host name or IP address of the mail server. (Initial value: mail)
From email address	Specify the email address displayed as the sender (sender) of emails. (Initial value: ThirdEye)
From name	Specify the name to be displayed as the sender name (sender) of the mail. (Initial value: ThirdEye)
Server requires authentication	Set mail server authentication. If SMTP authentication is required, select the check box and set the following items. (Initial value: invalid)

Description	Explanation
	Mail server username… Authentication ID Mail server password… Authentication password
Use secure smtp	Enable TLS.
Email Language	Set the mail display language. (Initial value: Japanese)
Email time zone	Set the email time zone. (Initial value: (GMT + 09: 00) Tokyo)

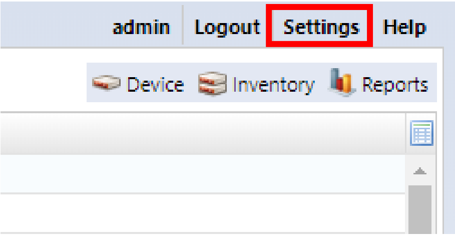
3. Click [OK].

7.9 SNMP trap notification of ThirdEye specific events

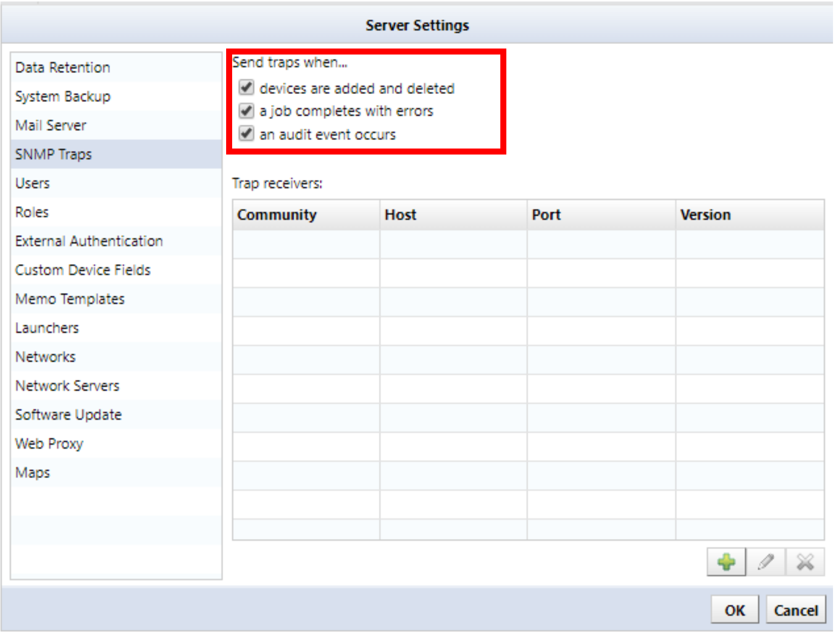
ThirdEye-specific events can be sent as traps. The following three events can be sent.

Description	Explanation
Devices add/delete	An SNMP trap is sent when a device is added / deleted.
Job fails	An SNMP trap is sent when a job fails.
Audit log	An SNMP trap is sent when a user logs in / out.

1. Click [Settings] in the global menu.



2. Click [SNMP Traps] and insert a check in the event to be sent.



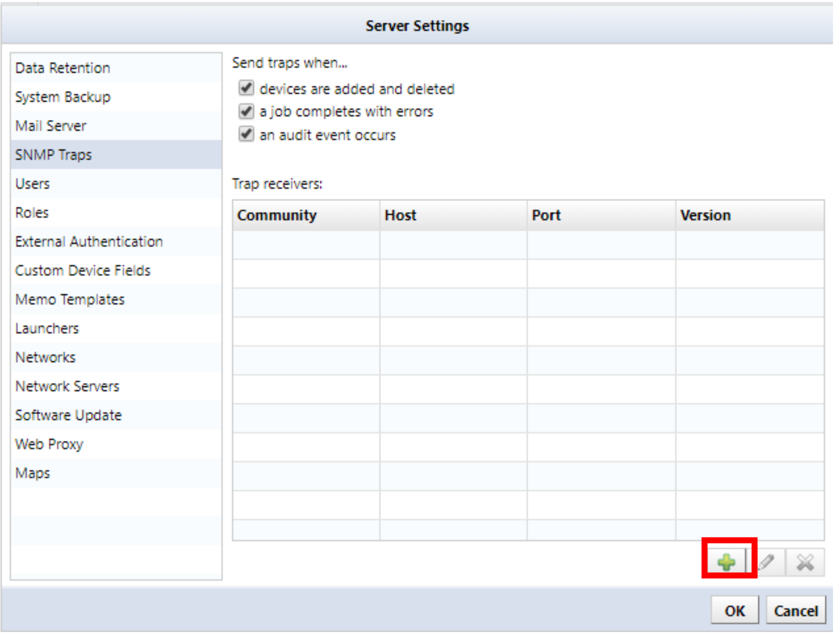
Send traps when...

☑ devices are added and deleted

☑ a job completes with errors

☑ an audit event occurs

3. Click [✚ (Add)]



Server Settings

- Data Retention
- System Backup
- Mail Server
- SNMP Traps
- Users
- Roles
- External Authentication
- Custom Device Fields
- Memo Templates
- Launchers
- Networks
- Network Servers
- Software Update
- Web Proxy
- Maps

Send traps when...

☑ devices are added and deleted

☑ a job completes with errors

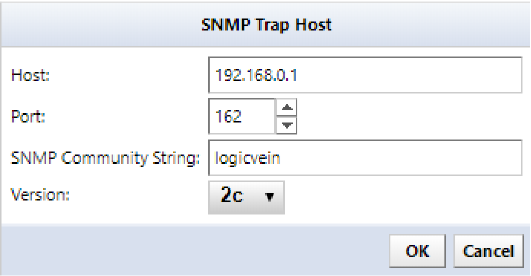
☑ an audit event occurs

Trap receivers:

Community	Host	Port	Version

OK Cancel

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



SNMP Trap Host

Host:	192.168.0.1
Port:	162
SNMP Community String:	logicvein
Version:	2c ▾

OK Cancel

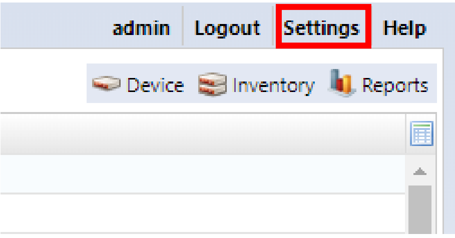
Description	Explanation
Host	Enter the IP address or host name of the trap destination.
Port	Specify the trap destination port. (Initial value: 162)
SNMP community string	Enter the trap community name.
Version	Select the trap version. ("2c" is recommended)

5. Click [OK].

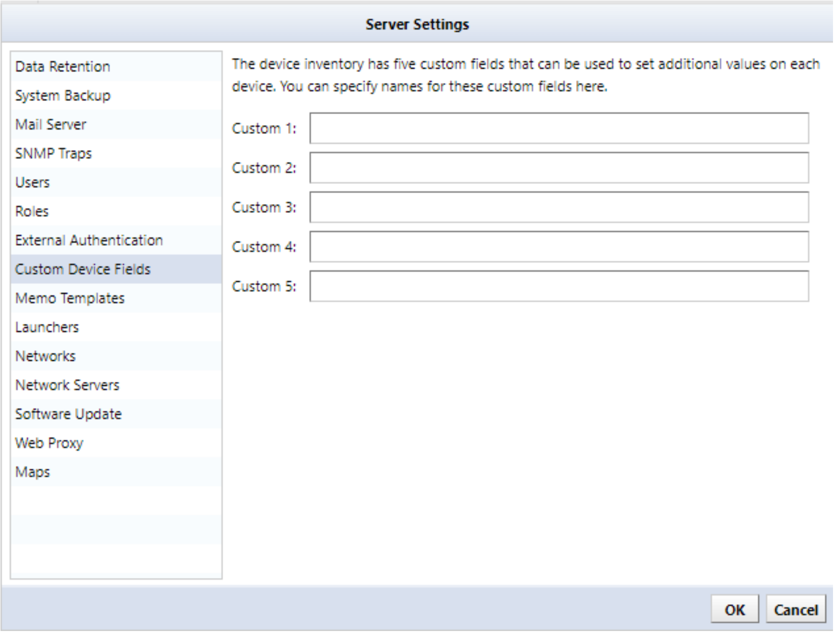
7.10 Changing column names in custom device fields

In the custom device field, you can set the name of the custom column used in the device tab or search.

1. Click [Settings] in the global menu.



2. Click [Custom Device Field].



Server Settings

The device inventory has five custom fields that can be used to set additional values on each device. You can specify names for these custom fields here.

Custom 1:

Custom 2:

Custom 3:

Custom 4:

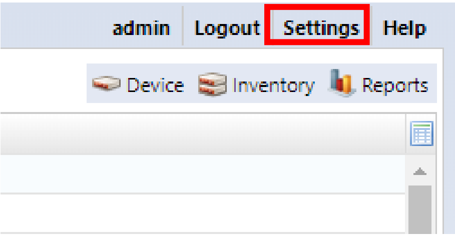
Custom 5:

3. Click [OK].

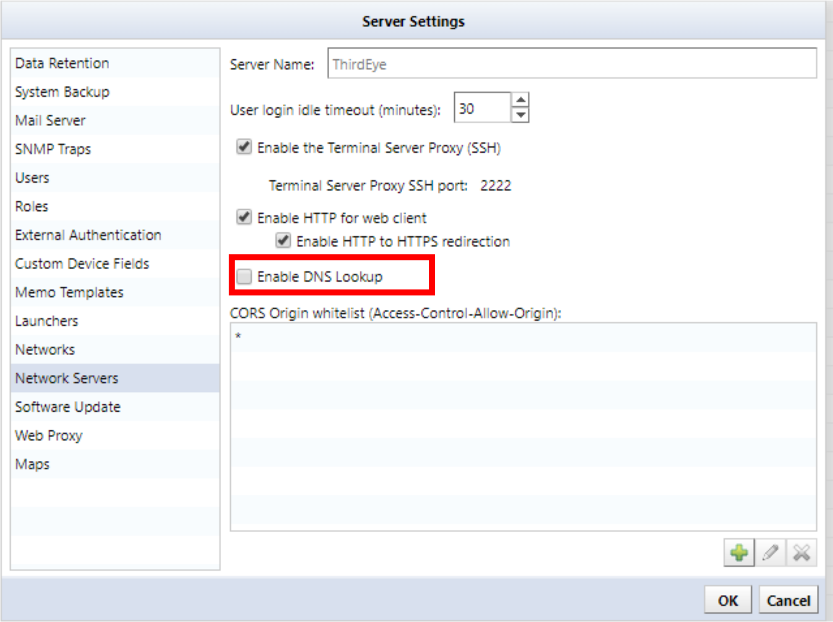
7.11 Use sysName as the host name

In ThirdEye, the host name displayed on the device tab is obtained from the DNS server and displayed. To use the host name (sysName) set for the device, make the following settings.

1. Click [Settings] in the global menu.



2. Click [Network Servers] and uncheck [Enable DNS Lookup].



Server Name: ThirdEye

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

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

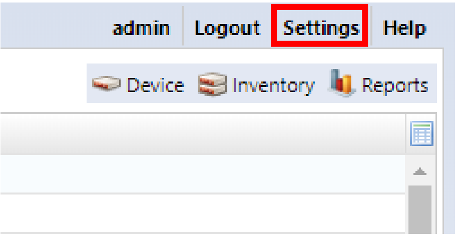
*

3. Click [OK].

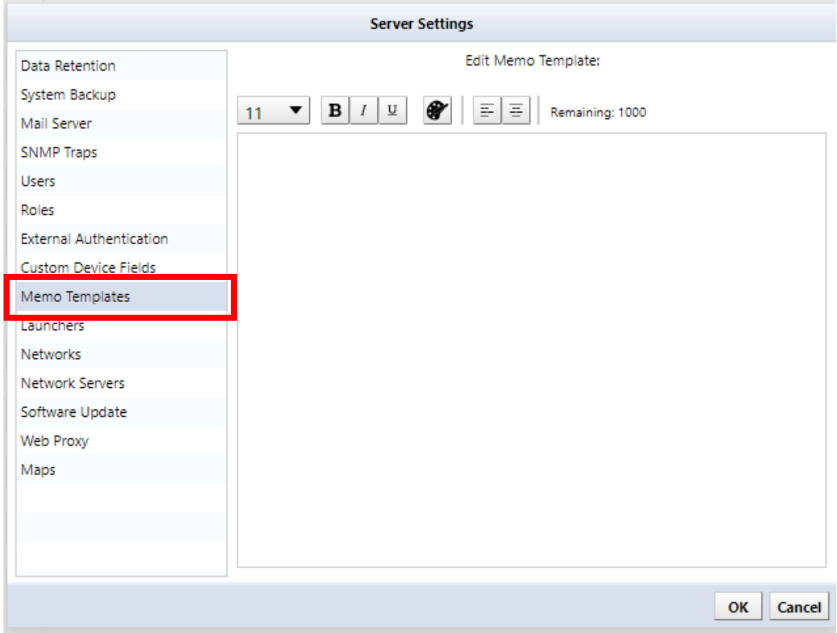
7.12 Editing a memo template

In the memo template, when you create a new device memo in the “memo” column of the inventory, you can set a template (template) that is automatically inserted.

1. Click [Settings] in the global menu.



2. Click [Memo Templates]



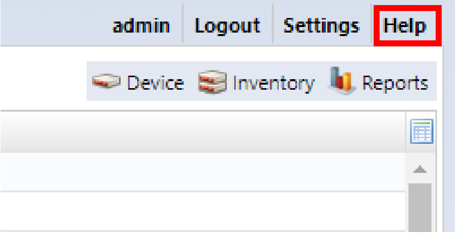
Description	Explanation
Font size	Change the font size.
Bold	Change the range specified characters to bold.
Italics	Change to italics.
Underline	Underline.
Text color	Change the text color.
Left-aligned	Set text alignment to left justification.
Centered	Set text alignment to center.
number of remaining characters	The number of remaining characters that can be entered.

	* Regardless of full width / half-width, all characters are counted as one character.

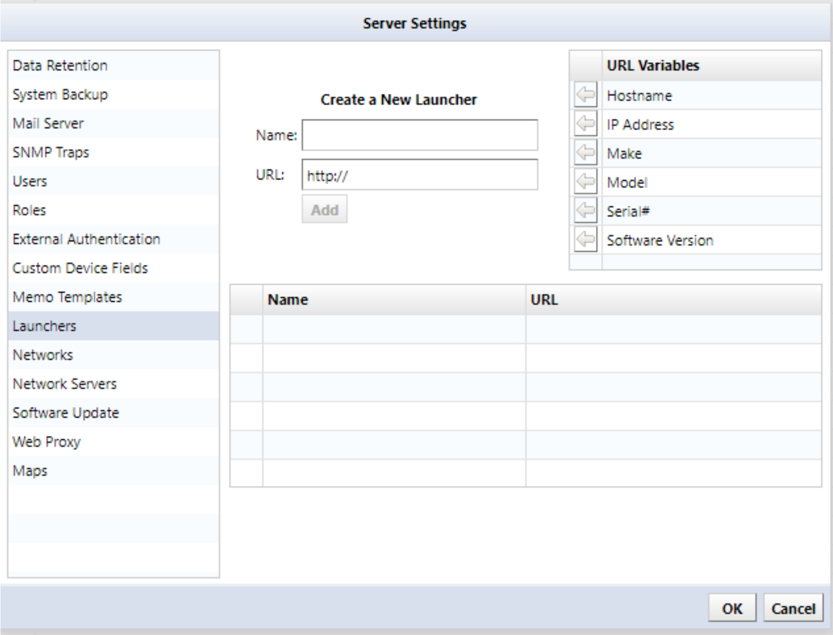
7.13 Adding a specific URL to the right-click menu

URL launcher is a shortcut function for easy access to a specific page. By registering the URL, you can access the page from the right-click menu.

1. Click [Settings] in the global menu.



2. Click [Launcher]



3. Enter a name and specify a URL.

* The name is displayed as the menu name of the right-click menu.

【Explanation of URL variable】

Description	Explanation	Example
Hostname	Quote the device hostname.	When a device with hostname = thirdeye.co.jp is selected, the "{device.hostname}" part of the URL is replaced with "thirdeye.co.jp". http://{device.hostname}

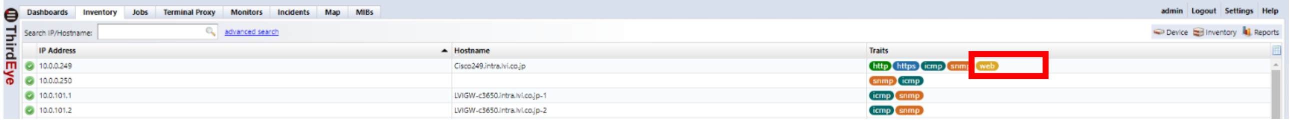
Description	Explanation	Example
		⇒ http://thirdeye.co.jp
IP address	Quote the device's IP address.	When the device with IP address = 192.168.0.1 is selected, the "{device.ipAddress}" part of the URL is replaced with "192.168.0.1". http://{device.ipAddress} ⇒ http://192.168.0.1
Vender	*Cannot use it.	http://{device.hardwareVendor}
Model	*Cannot use it.	http://{device.model}
Serial	*Cannot use it.	http://{device.assetIdentity}
Version	*Cannot use it.	http://{device.osVersion}

7.14 Update license

If the number of license nodes is increased or support is updated, the applied licenses must be.

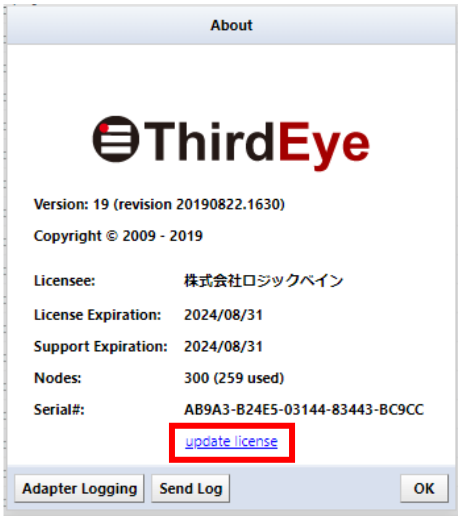
* This operation can only be performed by a user with ThirdEye Administrator privileges.

1. Click [Help] → [About] on the global menu.



IP Address	Hostname	Traits
10.0.0.249	Cisco249.intra.lvi.co.jp	http https icmp snmp web
10.0.0.250		snmp icmp
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp

2. Click [update license].



Version: 19 (revision 20190822.1630)

Copyright © 2009 - 2019

Licensee: 株式会社ロジックベイン

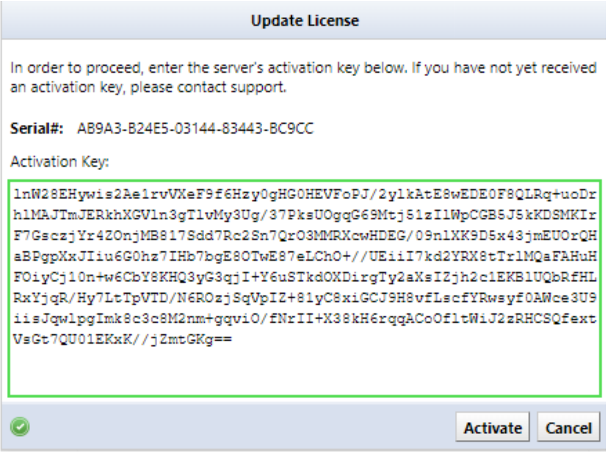
License Expiration: 2024/08/31

Support Expiration: 2024/08/31

Nodes: 300 (259 used)

Serial#: AB9A3-B24E5-03144-83443-BC9CC

In online environment, the license is automatically updated. In the offline environment, the screen for entering the activation key is displayed. Please update your activation key in advance.



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

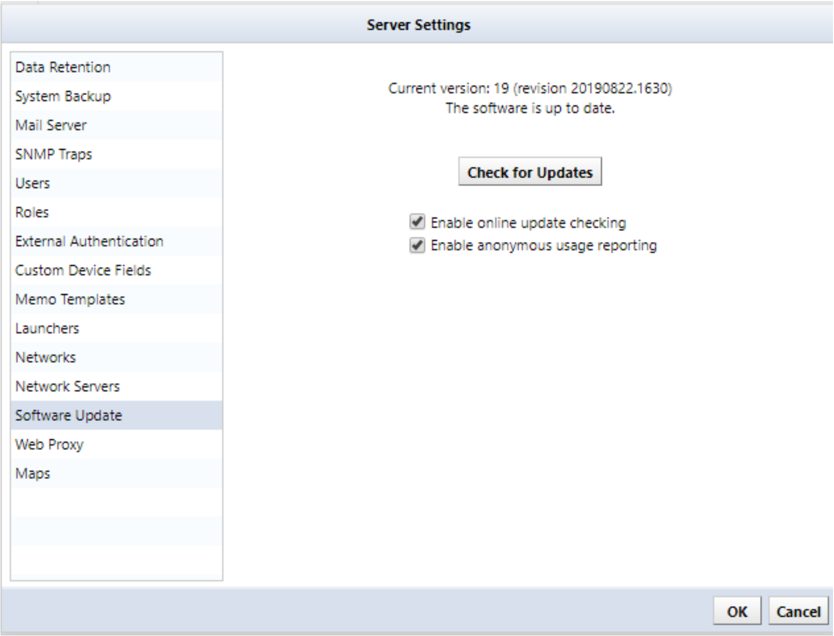
Serial#: AB9A3-B24E5-03144-83443-BC9CC

Activation Key:

```
lnW28EHywis2AelrvVXeF9f6Hzy0gHG0HEVFoPJ/2ylkAtE8wEDE0F8QLRq+uoDr
hlMAJTmJERkhXGVln3gTlvMy3Ug/37PksUOgqG69Mtj51zIlWpCGB5J5kKDSMKIr
F7GsczjYr4ZOnjMB817Sdd7Rc2Sn7QrO3MMRXcwHDEG/09nlXK9D5x43jmEUOrQH
aBPgpXxJIiu6G0hz7IHb7bgE8OTwE87eLChO+//UEiiI7kd2YRX8tTrlMQaFAHuH
FOiyCj10n+w6CbY8KHQ3yG3qjI+Y6uSTkdOXDirgTy2aXsIZjh2c1EKBlUQbRfHL
RxYjqR/Hy7LtTpVTD/N6ROzjSqVpIZ+81yC8xiGCJ9H8vfLscfYRwsyf0AWce3U9
iisJqwlpgImk8c3c8M2nm+gqviO/fNrII+X38kH6rqqACoOfltWiJ2zRHCSQfext
VsGt7QU01EKxK//jZmtGKg==
```

7.15 Updating online

ThirdEye can be updated via the Internet. Software update is a setting related to online update of software version. Software update settings only work in an environment where you can connect to the Internet.



Current version: 19 (revision 20190822.1630)
The software is up to date.

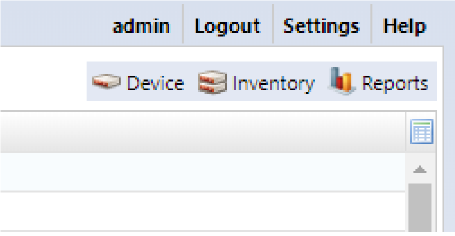
☑ Enable online update checking
☑ Enable anonymous usage reporting

Description	Explanation
Check for Updates	Click [Check for Updates] to check for updates online.
Enable Online Update Check	If [Enable Online Update Check] is checked, it will periodically check for updates. (Initial value: Enabled)
Enable anonymous usage reporting	If [Enable anonymous usage reporting] is checked, Send usage data anonymously. (Initial value: enabled)

7.16 Using a proxy server

When using software update or license update online via a proxy server, set the proxy server information.

1. Click [Settings] in the global menu.

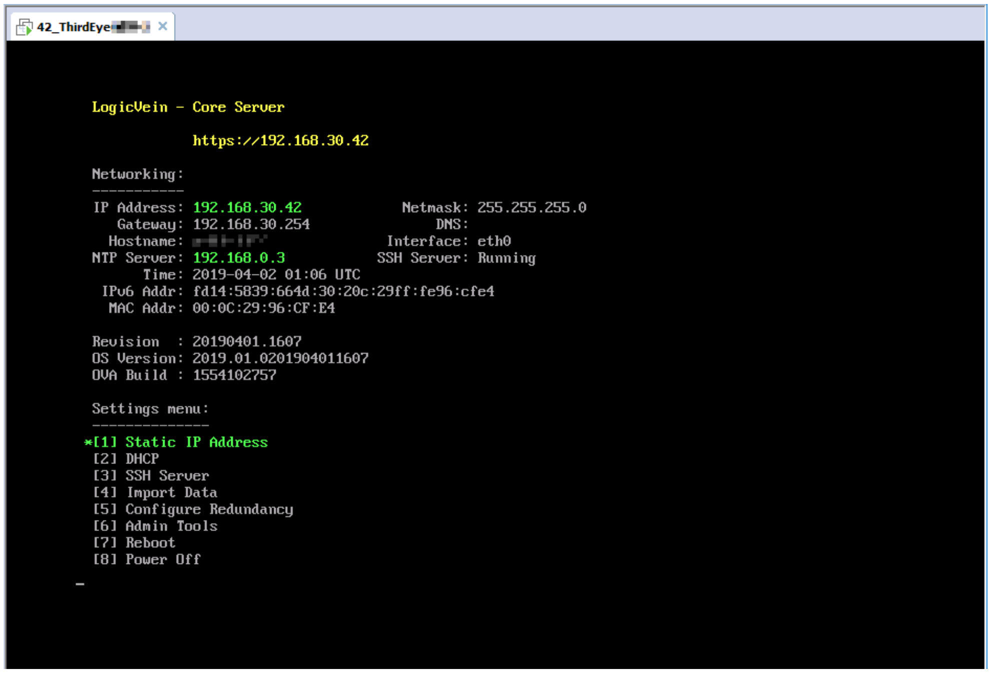


2. Click [Web Proxy] and enter the proxy server information.

Description	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 used as a proxy.
Port	Specify the port number on the proxy server. (Initial value: 8080)
Realm	Specifies the proxy authentication realm. If no realm is required, do not specify a value.
Username	Specify the username sent to the proxy server.
Password	Specify the password to send to the proxy server.

8. Reboot／Power Off

Restart and shut down by connecting to the virtual machine.



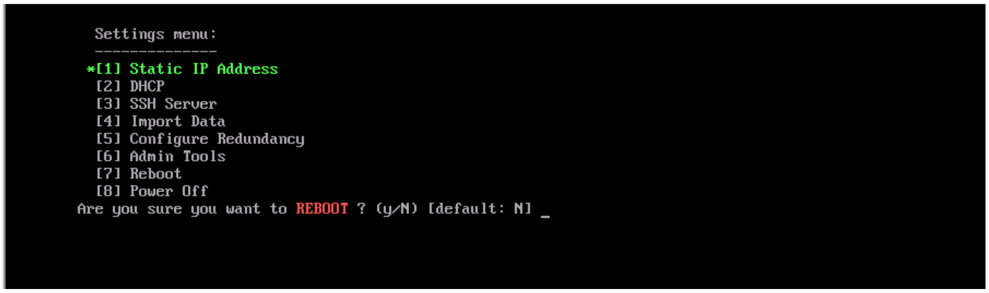
42_ThirdEye[redacted]

```
  LogicVein - Core Server

              https://192.168.30.42

  Networking:
  -----------
  IP Address: 192.168.30.42           Netmask: 255.255.255.0
     Gateway: 192.168.30.254              DNS:
    Hostname: [redacted]                Interface: eth0
  NTP Server: 192.168.0.3          SSH Server: Running
        Time: 2019-04-02 01:06 UTC
   IPv6 Addr: fd14:5839:664d:30:20c:29ff:fe96:cfe4
    MAC Addr: 00:0C:29:96:CF:E4

  Revision  : 20190401.1607
  OS Version: 2019.01.0201904011607
  OVA Build : 1554102757

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

Restart and shut down by connecting to the virtual machine.

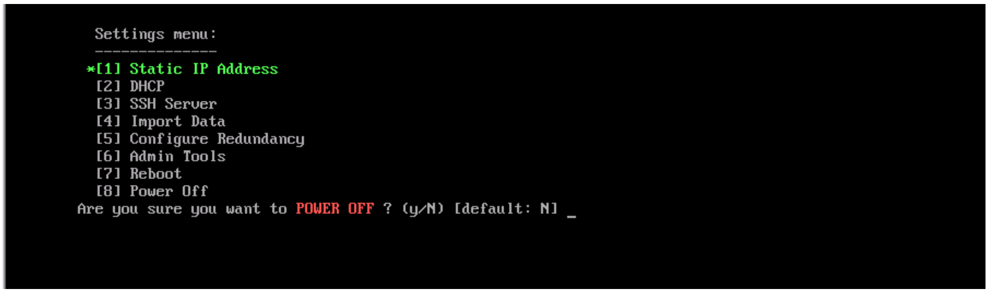
To restart, press the “7” key on the keyboard and select [Reboot].After selecting the menu, a confirmation message is displayed. Press the “Y” key on the keyboard to execute.

【REBOOT】



```
  Settings menu:
  --------------
 *[1] Static IP Address
  [2] DHCP
  [3] SSH Server
  [4] Import Data
  [5] Configure Redundancy
  [6] Admin Tools
  [7] Reboot
  [8] Power Off
Are you sure you want to REBOOT ? (y/N) [default: N] _
```

【POWER OFF】



```
  Settings menu:
  --------------
 *[1] Static IP Address
  [2] DHCP
  [3] SSH Server
  [4] Import Data
  [5] Configure Redundancy
  [6] Admin Tools
  [7] Reboot
  [8] Power Off
Are you sure you want to POWER OFF ? (y/N) [default: N] _
```

9. Contact

If you have any problems or questions during the operation of ThirdEye, please contact our support below.

Please confirm the necessary items below before making an inquiry.

[Required]

1. Product name
2. Product version information (including revision)
3. Product serial number (ThirdEye license information)
4. Specific symptoms and questions (Sending screenshots may facilitate information sharing and may help resolve issues)

■Contact information■

support@logicvein.com

10. Appendix

10.1 ICMP Algorithm

Different users have different requirements when performing ICMP polling, some of them complementary and some of them competing. The design of the algorithm tries to balance between the competing requirements, while still covering the broadest number of requirements.

Additionally, ThirdEye has a universal requirement to reduce the complexity and usability of any feature, including the ICMP monitor.

The requirements we have identified are:

- Accurately measuring roundtrip network transit time
- Quickly detecting and alerting host-down conditions
- Minimizing the volume of ICMP packets, while eventually detecting host-down conditions
- Detecting and alerting packet loss
- Minimizing false alerts while detecting host-down conditions

These goals will be addressed in the sections to follow.

10.1.1 Roundtrip Measurement Accuracy

The nature of ICMP roundtrip measurement is such that the responsibility for measuring the roundtrip time belongs to the host performing the measurement. In practical terms this means that delays introduced by the OS scheduler or CPU load cause the time measured to be longer than the actual network transit time. Thus, when viewing a graph of roundtrip times, occasional spikes can appear that do not reflect the true network transit time.

ThirdEye offers the option to send *two* ICMP packets per-poll, separated by several seconds, where the recorded measurement is the *lesser* of the two roundtrip times. This substantially reduces the number of outlier measurements by minimizing the effects of host CPU load and process scheduler jitter.

10.1.2 Packet Loss

The ICMP monitor stores two metrics: *roundTripTime* and *packetLossPercent*. In addition to setting an alert trigger based on "*no response*" or *roundTripTime*, the user can also configure an alert trigger based on the *packetLossPercent*. In some environments, this is at least as value to some customers as detecting host-down conditions.

If a single ICMP packet is used for monitoring, then a "no response" event will occur if that single packet has no response. If two ICMP packets are used, then a "no response" event will occur only if *both* packets have no response.

Regarding *packetLossPercent*, if we ignore automatic retry for now, then if a single ICMP packet is used for monitoring, then the *packetLossPercent* metric will be only one of two values: *0%* (no packet loss) or *100%*. If two ICMP packets are used for monitoring, then the *packetLossPercent* will be one of three values: *0%* (no packet loss), *50%* (one of the two packets lost), or *100%* (both packets lost).

The *packetLossPercent* calculation is also affected by the retry semantics described below.

10.1.3 Retry Semantics

To minimize false host-down alerts, the user can optionally enable ICMP retries. When ICMP retries are enabled, ThirdEye will send five (5) additional ICMP packets, with a *dynamic interval* in-between each packet based on the *polling interval* of the monitor.

If a *single* ICMP packet monitor is used, and there is no response to that packet, the retry algorithm is initiated. If a *double* ICMP packet monitor is used, and either of the two packets receives no response, the retry algorithm is initiated.

If a *single* ICMP packet monitor is used, and the retry path is entered, then a total of six (6) ICMP packets will be sent. Conversely, if a *double* ICMP packet monitor is used and the retry path is entered, then a total of seven (7) ICMP packets will be sent.

If *none* of the ICMP packets receive a response, then a "no response" alert is raised. But if any of the ICMP packets is acknowledged (i.e. a response is received), then a "no response" alert is <u>not</u> raised, but the *packetLossPercent* metric is calculated based on the responses.

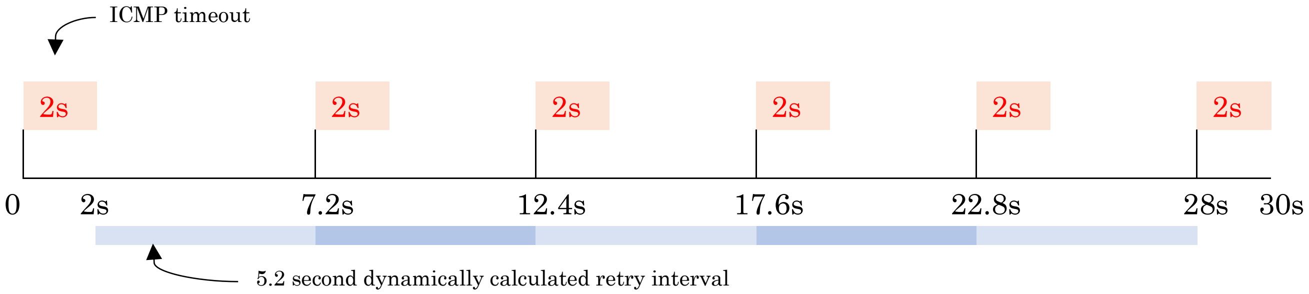
If a *single* ICMP packet monitor is used, and retries are enabled, the possible (approximate) values for the *packetLossPercent* metric are as follows: *0%, 16%, 33%, 50%, 66%, 83%, 100%.*

If a *double* ICMP packet monitor is used, and retries are enabled, the possible (approximate) values for the *packetLossPercent* metric are as follows: *0%, 14%, 28%, 42%, 57%, 71%, 85%, 100%.*

The *dynamic interval* varies between a minimum of a few seconds for an ICMP monitor with a 30 second polling interval, and a maximum of 25 seconds for ICMP monitors with a polling interval greater than 150 seconds.

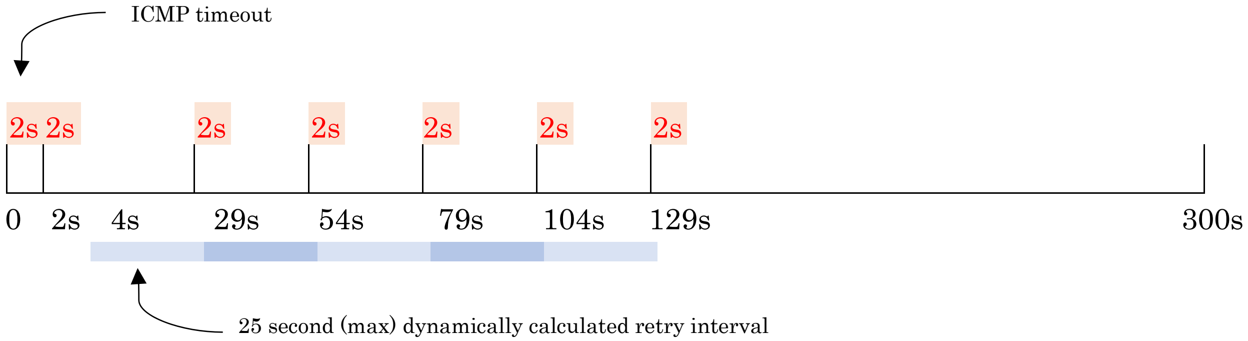
Visualization showing the polling and retry pattern for:

- *Single* ICMP monitor
- Retries enabled
- 30 second polling interval



Visualization showing the polling and retry pattern for:

- *Double* ICMP monitor
- Retries enabled
- 5-minute (300 second) polling interval


ICMP timeout
2s
2s
2s
2s
2s
2s
2s
0
2s
4s
29s
54s
79s
104s
129s
300s
25 second (max) dynamically calculated retry interval