



# Net LineDancer

## User's Manual

### Table of Contents

User's Manual .....	1
1: Introduction.....	7
1.1 About NetLD .....	7
1.2 About NetLD edition .....	7
1.3 Environmental Settings.....	8
1.4 List of ports used.....	9
2: Installation.....	10
2.1 Deployment to VMware ESXi.....	10
2.2 Deployment to Windows Hyper-V.....	13
2.3 Deploying to Linux KVM.....	20
2.4 Deploying to Nutanix AHV+ .....	21
2.5 Deploy to Microsoft Azure .....	22
2.6 Deploying to AWS .....	23
2.7 Configuring Network Settings .....	24
2.8 Apply the license.....	26

2.9	Initial settings (detailed settings) .....	27
3:	Login/Logout .....	28
3.1	Log in .....	28
3.2	Log out .....	28
4:	Basic settings .....	29
4.1	Set credentials .....	29
4.1.1	Set common credentials .....	29
4.1.2	Set credentials for each device .....	32
4.2	Add device .....	35
4.2.1	Register one device at a time .....	35
4.2.2	Register devices on your network .....	36
4.2.3	Import registration from Excel file .....	38
5:	Use operations .....	40
5.1	Get Device Configuration .....	40
5.1.1	Prerequisites .....	40
5.1.2	Run a backup .....	40
5.1.3	About the status after backup .....	41
5.1.4	Check the obtained configuration .....	42
5.1.5	Comparison of configs .....	43
5.2	Make an SSH/Telnet connection to the device .....	44
5.2.1	Preparation before use .....	44
5.2.2	Start the terminal proxy .....	45
5.2.3	Check the operation log .....	46
5.3	Check the Up/Down status of the device interface .....	48
5.4	Jobs .....	49
5.4.1	Create a job .....	49
5.4.2	Job history .....	54
5.4.3	Job approval function .....	54
5.4.4	Check past job history .....	60
5.5	Remove device .....	61
5.5.1	Delete job .....	61
6:	Advanced Setting .....	62
6.1	Automatic configuration .....	63
6.1.1	Prerequisites .....	63
6.2	Compliance overview .....	66
6.2.1	Rule .....	66
6.2.2	Compliance policy .....	71
6.2.3	Automatic remediation function .....	75
6.3	Draft configuration .....	88
6.3.1	Creating a draft configuration .....	88
6.3.2	Import draft configuration from plain text .....	90

6.3.3	Export the draft .....	90
6.3.4	Delete draft .....	90
6.3.5	Comparison of drafts.....	91
6.3.6	Apply draft configuration to devices .....	91
6.4	Change Advisor.....	92
6.4.1	Execute commands using Change Advisor .....	93
6.5	Viewing tools .....	94
6.5.1	DNS lookup .....	94
6.5.2	IOS Show commands.....	94
6.5.3	IP routing table.....	95
6.5.4	Ping .....	95
6.5.5	SNMP system information.....	95
6.5.6	Interface overview .....	96
6.5.7	Traceroute .....	96
6.5.8	Port scan.....	96
6.5.9	Live ARP Table .....	96
6.6	Change Tools.....	97
6.6.1	MOTD banner settings.....	97
6.6.2	NTP server .....	97
6.6.3	SNMP community string .....	98
6.6.4	SNMP Trap Hosts .....	98
6.6.5	Syslog Hosts .....	98
6.6.6	Port VLAN Assignment .....	99
6.6.7	Enable or Disable Interfaces .....	99
6.6.8	Command Runner .....	100
6.6.9	AlliedTelesis OS software distribution .....	100
6.6.10	ASA OS software distribution .....	101
6.6.11	IOS software distribution .....	102
6.6.12	NEC WA software distribution .....	103
6.6.13	Manage OS image.....	103
6.6.14	Retrieve OS image file.....	104
6.6.15	Yamaha RT Firmware Distribution .....	104
6.6.16	Add Static Route .....	106
6.6.17	Delete Static Route .....	106
6.6.18	Change Enable Password .....	106
6.6.19	Change VTY Password .....	107
6.6.20	Delete User Account .....	107
6.6.21	Add User Account.....	107
6.6.22	Change Local User Password .....	108
6.7	Smart change overview .....	109
6.7.1	Create a smart change job .....	109

6.8	Register a user.....	113
6.8.1	Add permissions .....	113
6.8.2	Add user.....	118
6.8.3	Change user information.....	120
6.8.4	Change password .....	121
6.8.5	Configuring External Authentication .....	122
6.8.6	Set session timeout for users.....	132
6.8.7	Delete user .....	133
6.8.8	Remove permissions .....	133
6.9	Change data retention period .....	134
6.10	Set up your mail server.....	135
6.11	Configure SNMP trap sending.....	137
6.12	Add columns/change column names for custom device fields.....	139
6.13	Use sysName for hostname .....	140
6.14	Advanced Syslog file settings .....	141
6.14.1	Set Syslog file retention period/size.....	141
6.14.2	Set up Syslog rules.....	142
6.14.3	Save syslog files to external storage .....	145
6.15	Edit a memo template.....	146
6.16	Add specific URL to right-click menu .....	147
6.17	Update license .....	149
6.18	update online .....	150
6.19	Check revisions .....	151
6.20	Use a proxy server.....	152
6.21	Zero-Touch (optional) .....	153
6.21.1	Zero-Touch requirements.....	154
6.21.2	DHCP server .....	154
6.21.3	Use an external DHCP server .....	156
6.21.4	Distribution of configurations.....	156
6.21.5	Precautions when handling newly introduced devices.....	162
7:	System backup/restore .....	163
7.1	Perform system backup automatically .....	163
7.2	Perform a manual system backup .....	164
7.3	Change the number of system backups retained .....	165
7.4	Save to external storage .....	166
7.5	Restore system backup.....	169
8:	Reboot/Shutdown.....	172
9:	Uninstall.....	173
9.1	uninstall.....	173
10:	Inquiry.....	175
11:	Ending material.....	176



11.1	Smart Bridges (Optional) .....	176
11.1.1	SmartBridge Installation .....	178
11.1.2	Add SmartBridge to core server.....	178
11.1.3	SmartBridge Settings .....	180
11.1.4	Managing Devices via SmartBridge .....	181

## Revision history

Edition number	date of issue	Revised content
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
Rev.4	3/9/2020	Add config backups
Rev.5	2/2022	Updated documentation for remediation and EOL/EOS
Rev.6	09/2022	Modified EOL/EOS
Rev.7	05/2024	Changes due to added functionality

# 1: Introduction

This document is a manual for the network fault monitoring software "NetLD." This section explains various settings and operation methods for NetLD.

## 1.1 About NetLD

NetLD is a network configuration management tool that can be used in a wide range of environments, from small to large network environments. With NetLD, you can:

- Inventory management (customize display, sort, search)
- Trail management with terminal proxy
- Email notifications
- Configuration backup and generation management
- Change settings of network devices (router/switch/firewall, etc.)
- Syslog monitoring
- Command runner
- OS updates

## 1.2 About NetLD edition

Function		Enterprise
Discovery		○
Config management	config backup	○
	generational management	○
	Compare	○
	export	○
Config change	bulk change	○
	restoration	○
	change tools	○
	draft config	○
Terminal proxy	Telnet/SSH connection	○
	Saving operation history	○
Job		○
Compliance		○
Report		○
Zero-touch (optional)		○

## 1.3 Environmental Settings

NetLD is available as a virtual appliance and supports below platforms:

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

To use NetLD, you need the following environment:

project	Recommendation	Default	smallest
hard disk	HDD1: 2.5 GB HDD2: 50 GB or more	HDD1: 2.5 GB HDD2: 50 GB	HDD1: 2.5 GB HDD2: 50 GB
HDD provisioning	thin or chic	thin or chic	thin or chic
memory	8 GB or more	16 GB	8 GB
CPU	8 virtual CPUs (cores) or more	16 virtual CPUs (cores)	4 virtual CPUs (cores)

other noteworthy things

Both thin and thick HDD provisioning types are supported.

## 1.4 List of ports used

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

function	protocol	port	UDP /TCP	Communication direction
Zero-Touch	DHCP	67	UDP	NetLD (←) Destination
		68	UDP	NetLD (→) Destination
	HTTP	80	TCP	NetLD (←) Destination
	TFTP	69	UDP	NetLD (←) Destination
	ICMP	-	-	NetLD (←) Destination
automatic discovery	SSH, Telnet	22,23	TCP	NetLD (→) Destination
	SNMP	161	UDP	NetLD (→) Destination
	ICMP	-	-	NetLD (→) Destination
Send settings (restore configuration)	SSH, Telnet	22,23	TCP	NetLD (→) Destination
	TFTP	69	UDP	NetLD (←) Destination
	FTP	20,21	TCP	NetLD (←) Destination
Settings using modification tools	SSH, Telnet	22,23	TCP	NetLD (→) Destination
Trap sending	SNMP Trap	162	UDP	NetLD (→) Destination
SNMP monitoring	SNMP	161	UDP	NetLD (→) Destination
Trap reception	SNMP Trap	162	UDP	NetLD (←) Destination
Real-time change detection	Syslog	514	UDP	NetLD (←) Destination
backup*	SSH, Telnet	22, 23	TCP	NetLD (→) Destination
	SNMP	161	UDP	NetLD (→) Destination
	TFTP	69	UDP	NetLD (←) Destination
	FTP	20,21	TCP	NetLD (←) Destination
terminal proxy	SSH or HTTPS	2222,443	TCP	NetLD (←) Client PC
	SSH, Telnet	22, 23	TCP	NetLD (→) Destination
Web terminal	HTTPS	443	TCP	NetLD (←) Client (GUI)
	SSH, Telnet	22, 23	TCP	NetLD (→) Destination
client	HTTPS	443	TCP	NetLD (←) Client (GUI)
External authentication function	LDAP	389	TCP	NetLD (→) Authentication server
	RADIUS	1812	UDP	NetLD (→) Authentication server

\* The appropriate settings for the protocol you use will depend on the type of device you are using.

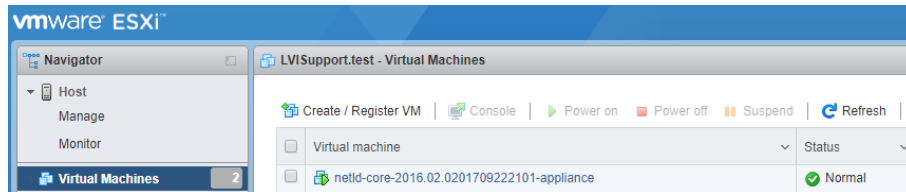
For example, for IOS devices, "CLI (Telnet, SSH) only or both CLI and TFTP"

## 2: Installation

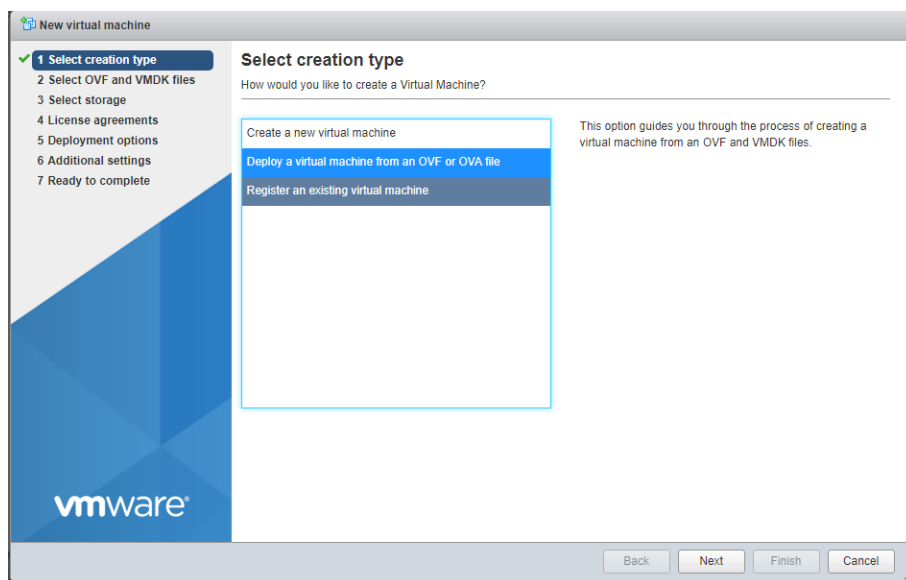
### 2.1 Deployment to VMware ESXi

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

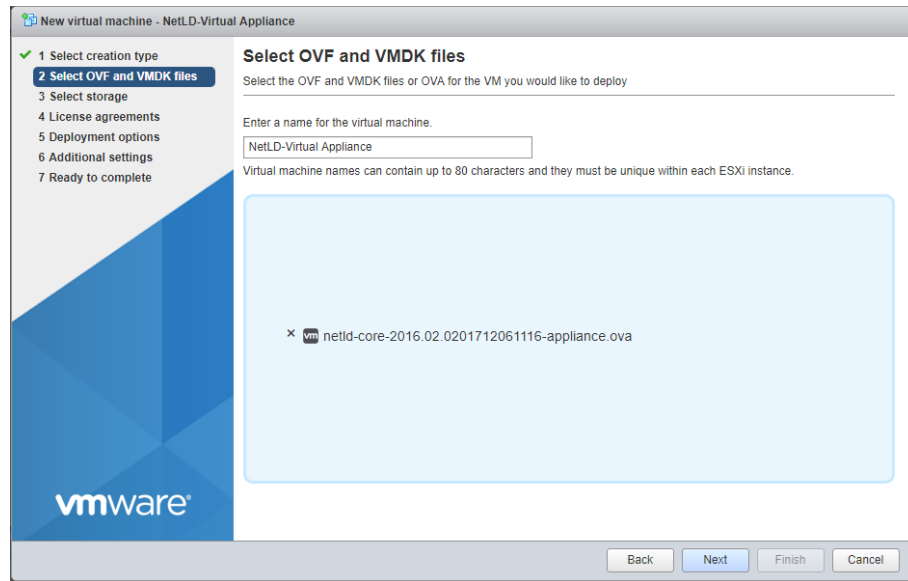
1. Log in to the Web UI and click "Create/Register Virtual Machine" from the virtual machine.



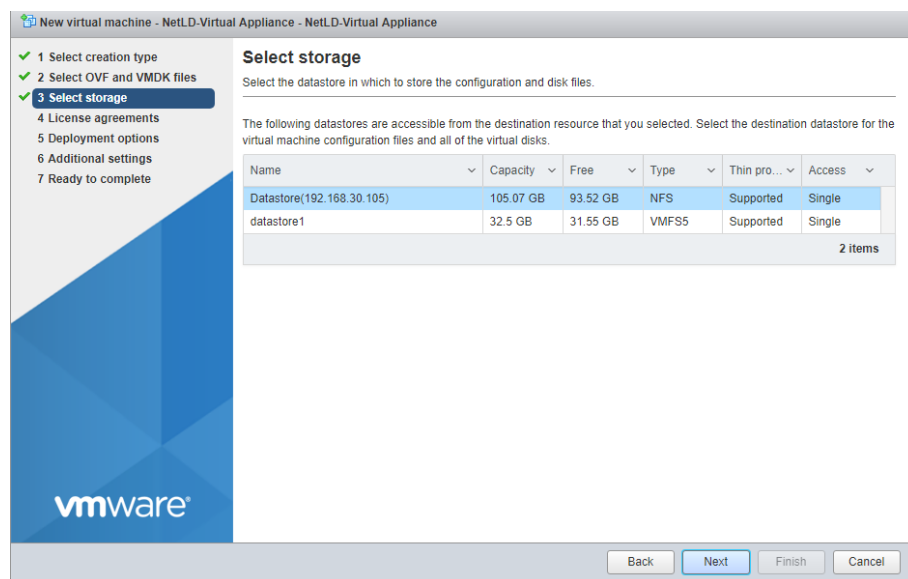
2. Select Deploy a virtual machine from an OVF or OVA file and click Next.



3. After entering the desired virtual machine name, drag and drop the OVA file "lvi-core-\*\*\*-appliance.ova" and click Next.



4. Select your storage and click Next.



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

The screenshot shows the 'New virtual machine' wizard for 'NetLD-Virtual Appliance'. The left sidebar indicates the progress: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options (highlighted), and 5 Ready to complete. The main area is titled 'Deployment options' and contains a table for 'Select deployment options'.

Select deployment options	
Network mappings	NAT VM Network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick

At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

6. Click Finish.

The screenshot shows the 'New virtual machine' wizard for 'NetLD-Virtual Appliance' at the 'Ready to complete' step. The left sidebar shows the progress: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options, and 5 Ready to complete (highlighted). The main area is titled 'Ready to complete' and contains a table for 'Review your settings selection before finishing the wizard'.

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

Below the table, there is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.'

At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

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



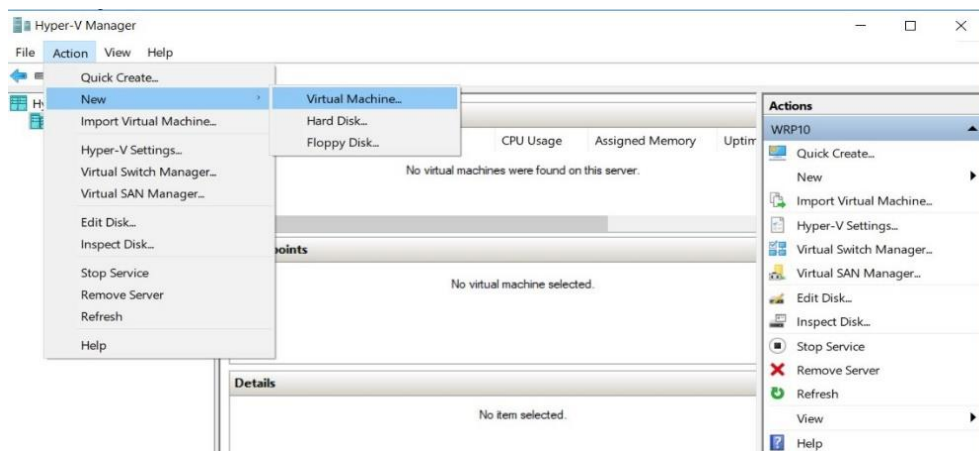
## 2.2 Deployment to Windows Hyper-V

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

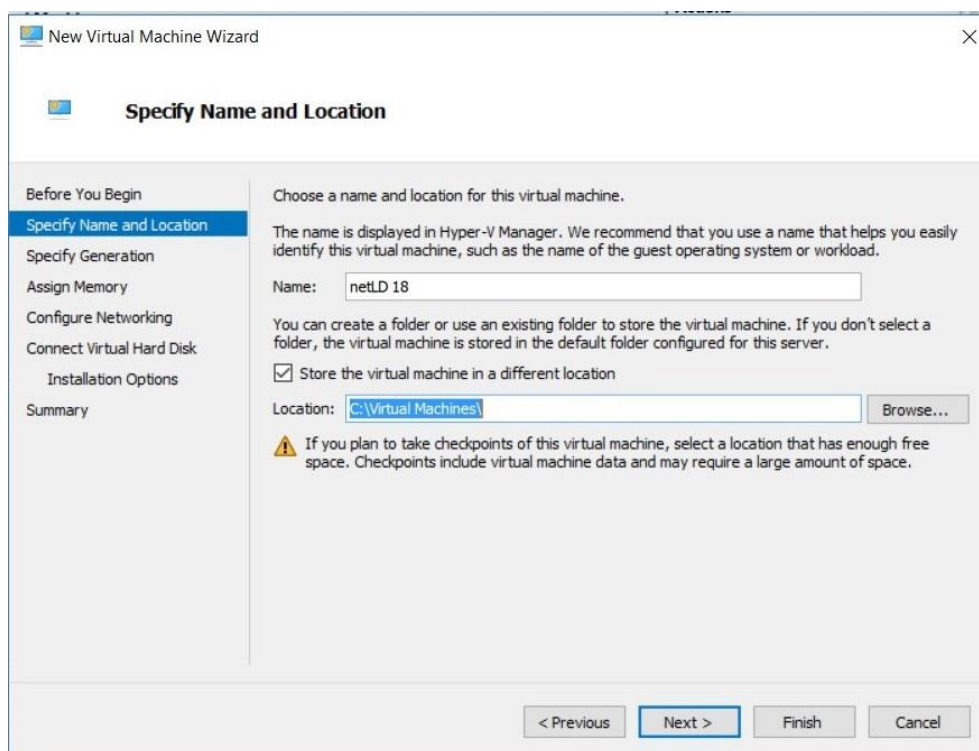
### [Prerequisites]

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

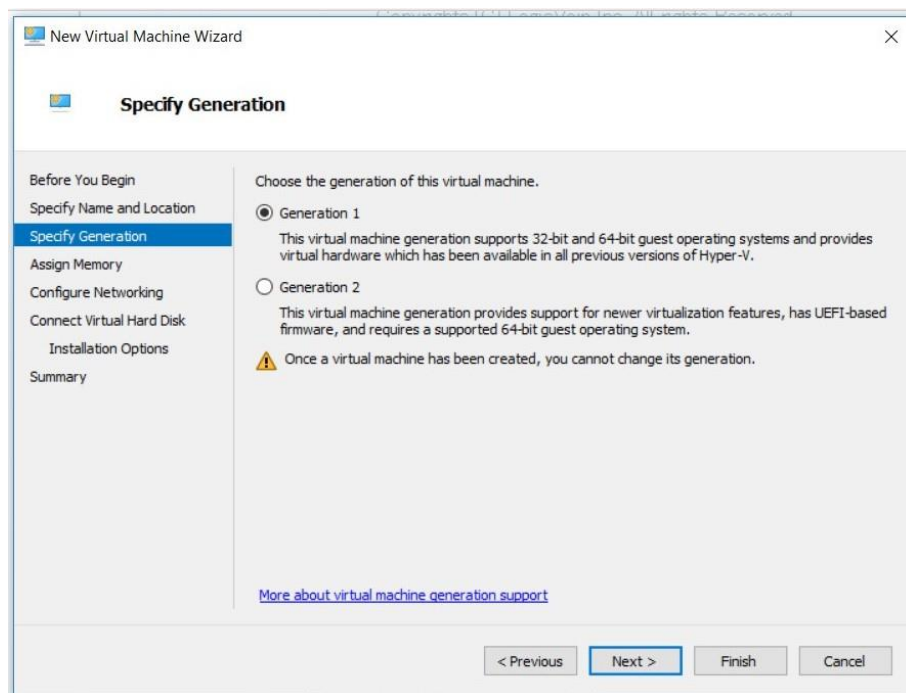
1. Start Hyper-V Manager and click New → Virtual Machine.



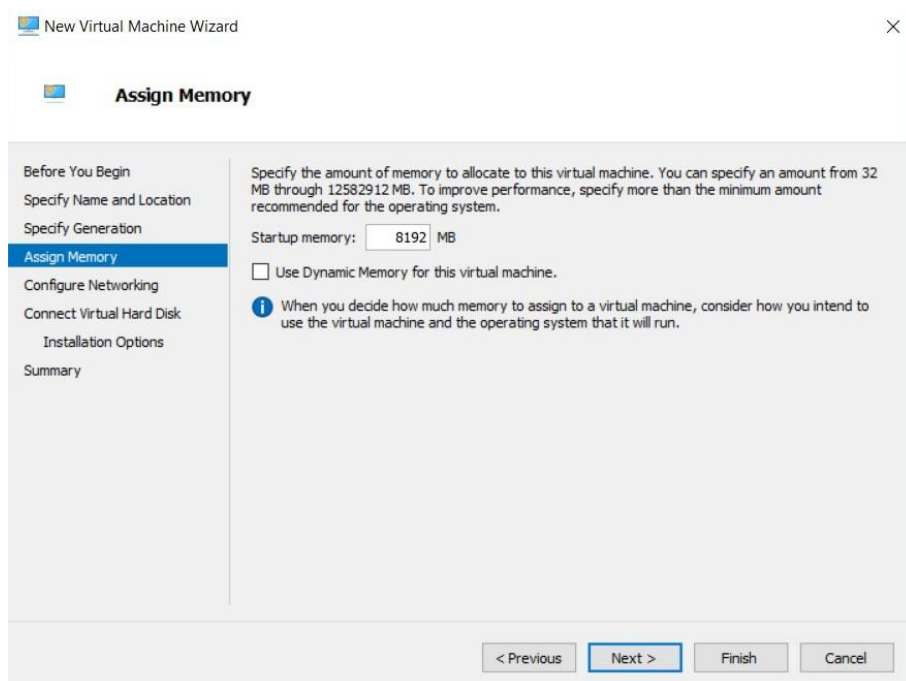
2. Enter a name for your virtual machine and click Next.



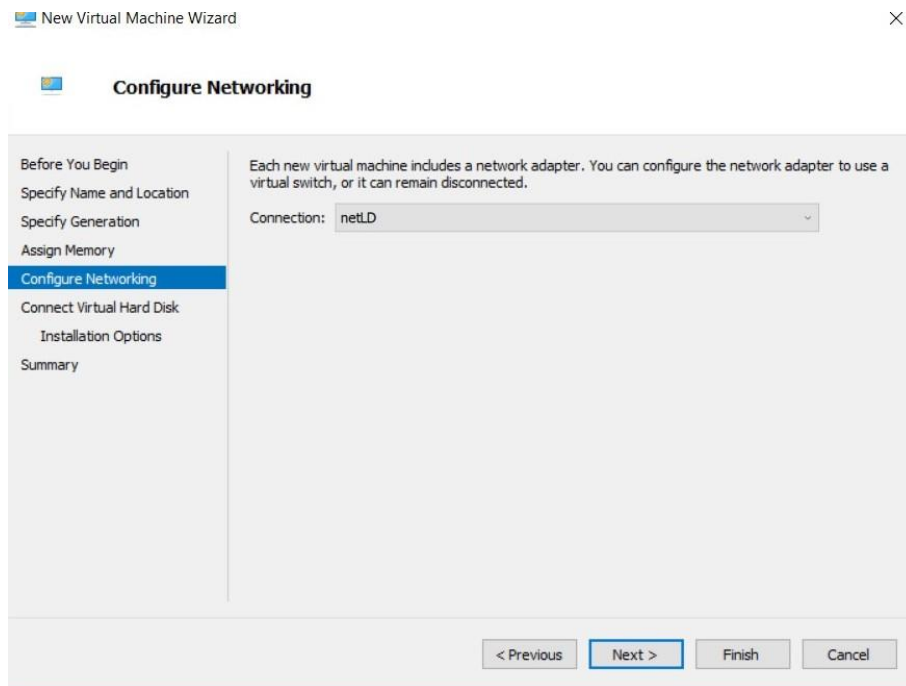
3. Select "1st generation" and click "Next".



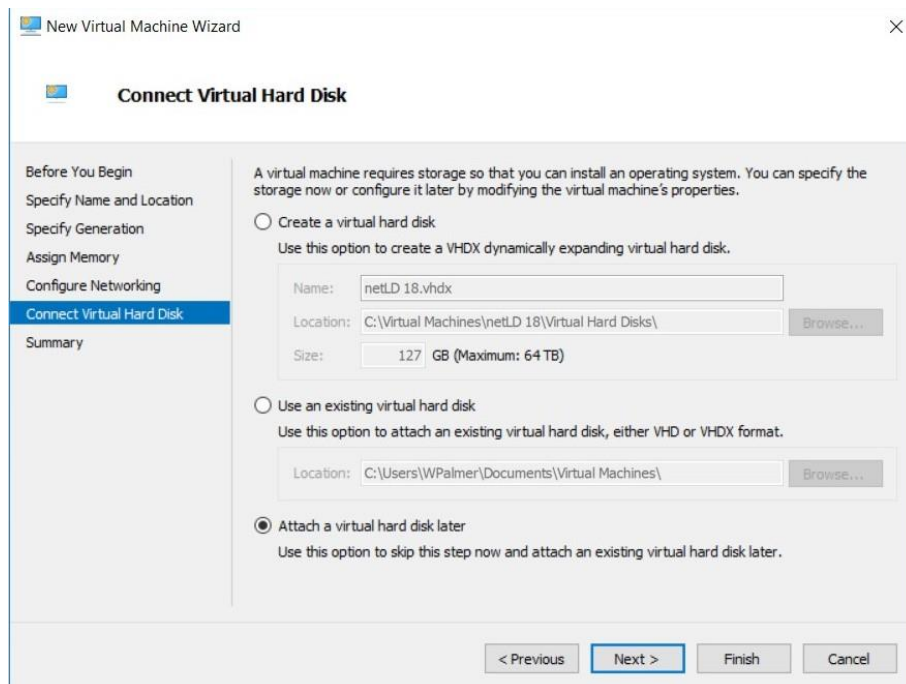
4. Set the startup memory and click Next.



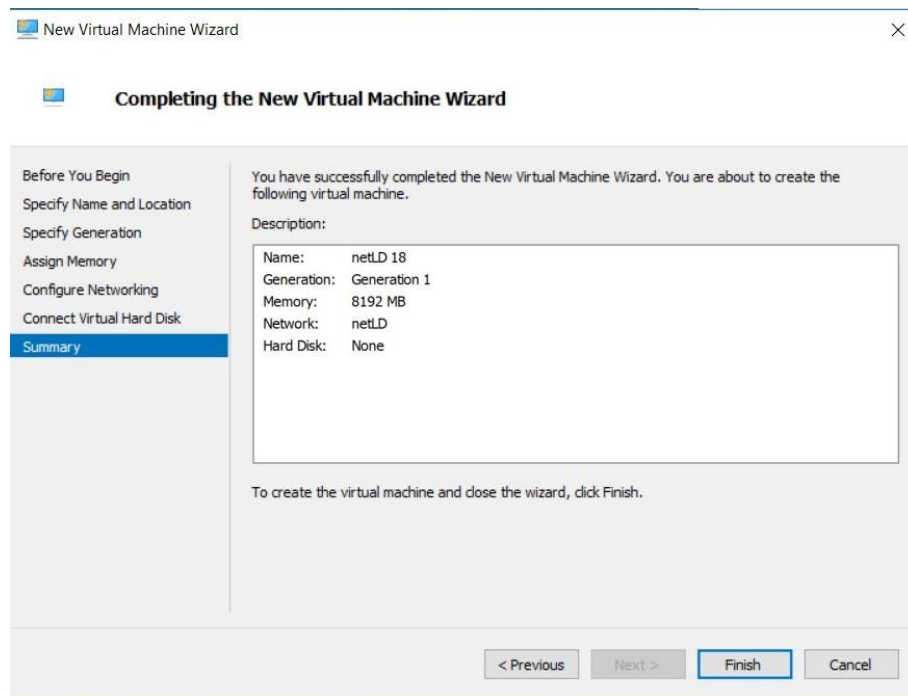
5. Select the virtual switch you want to connect to and click Next.



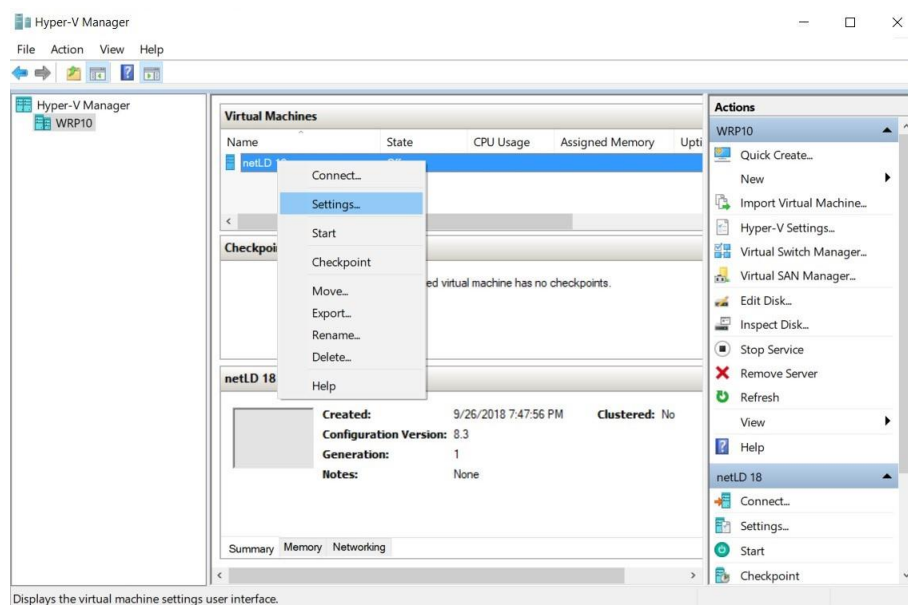
6. Select "Attach a virtual hard disk later" and click "Next".



7. Click Finish.

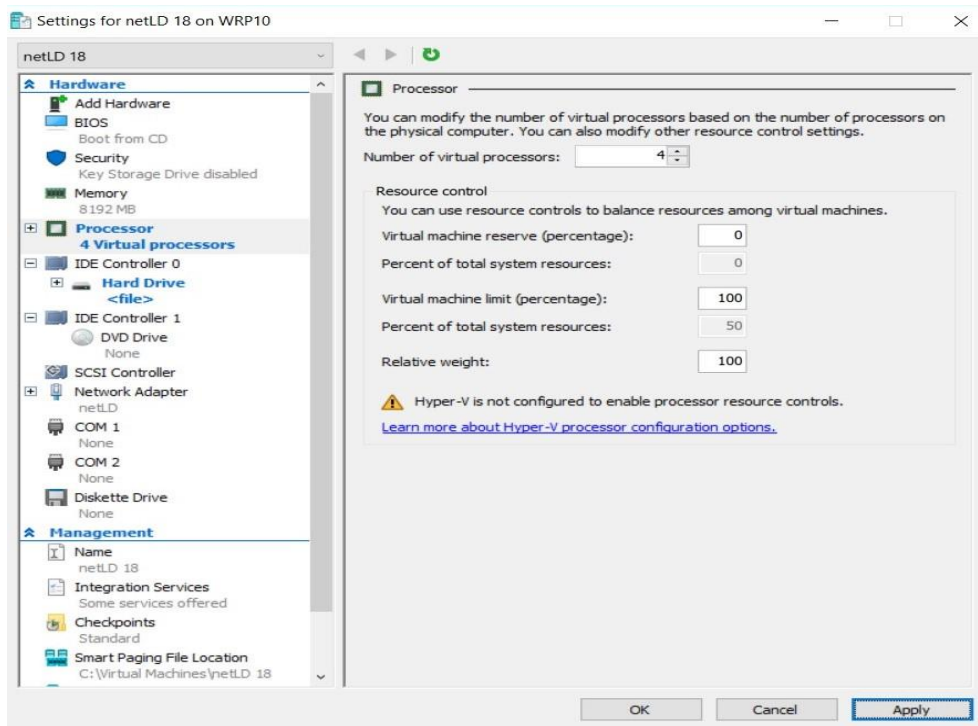


8. The virtual machine will now be created.
9. Next, assign the two VHDX files to the created virtual machine.
10. Right-click the virtual machine you created and click Settings.

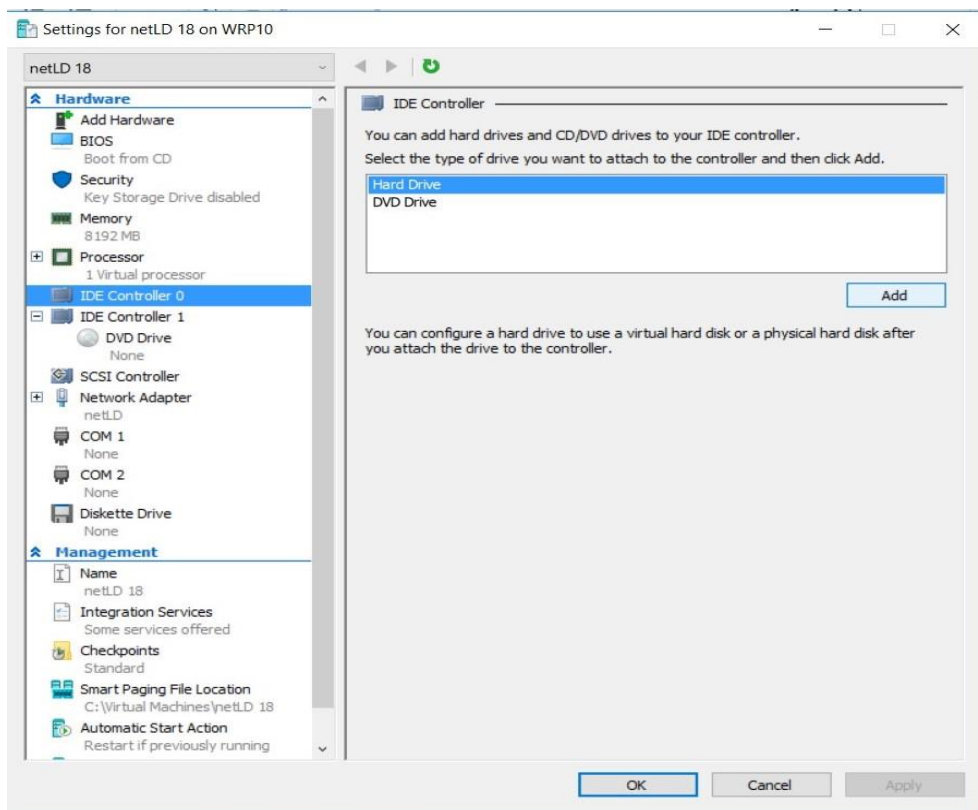


Displays the virtual machine settings user interface.

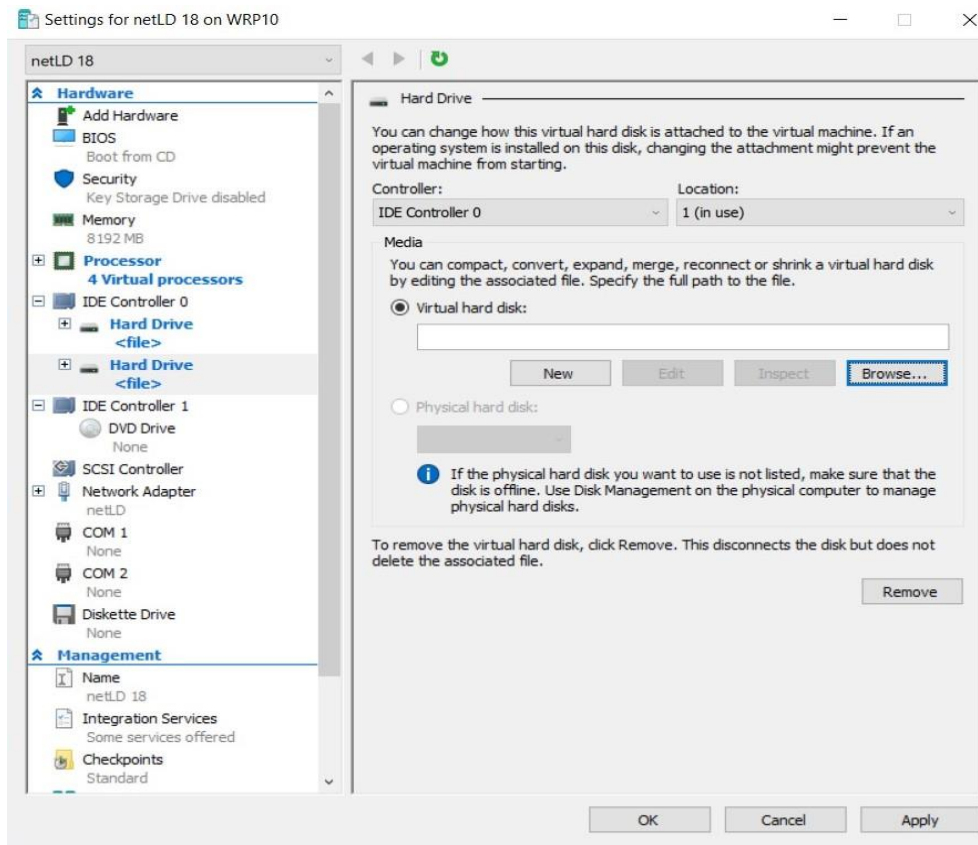
11. Select "Processor" and change "Number of virtual processors".



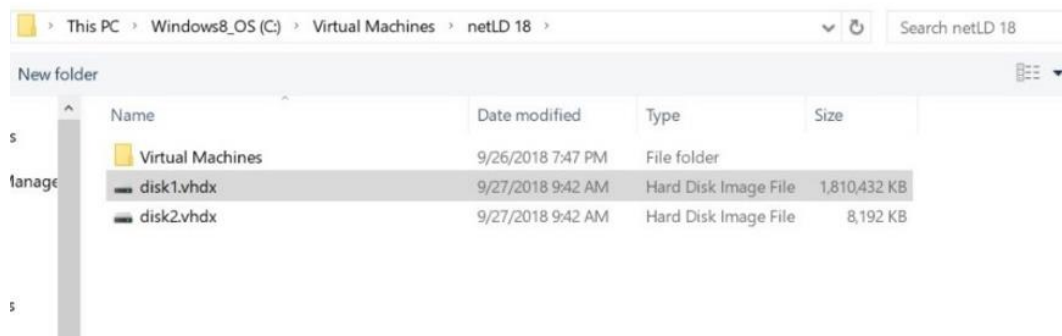
12. Select "IDE Controller 0" and click "Add".



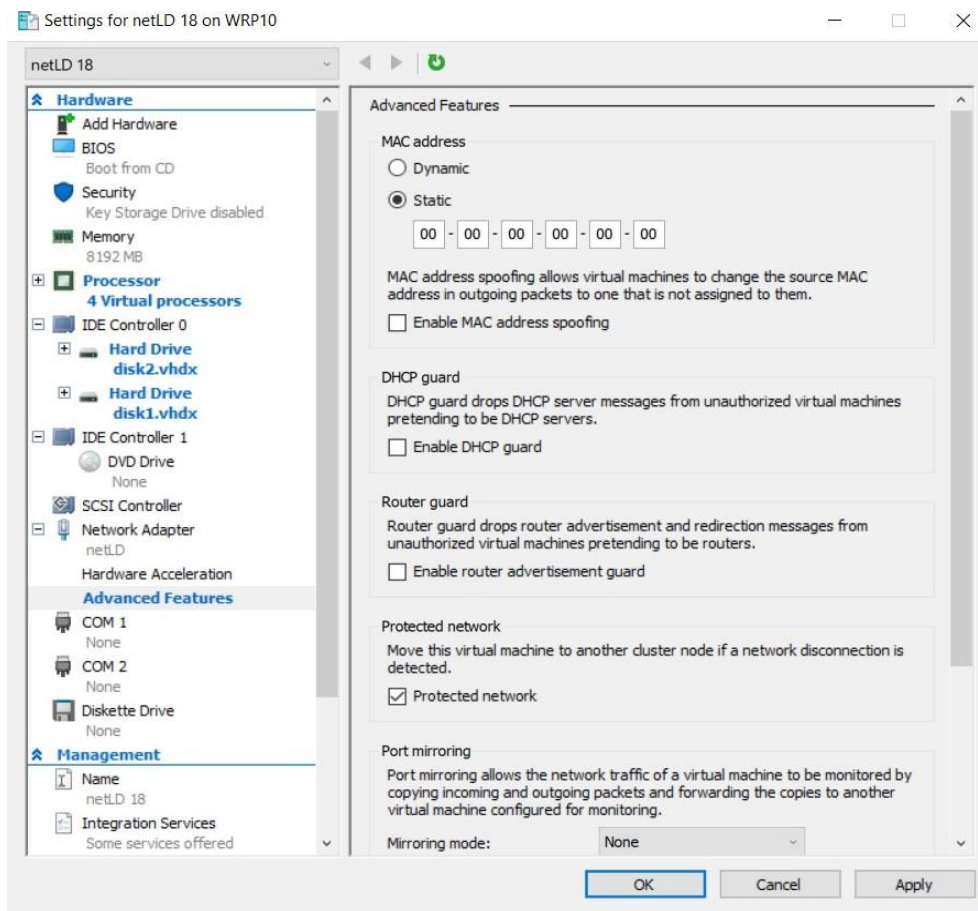
13. Click Browse.



14. Add "disk1" and click "OK".



15. Repeat steps 15 to 18 to add disk2.vhdx.
16. Click “OK”.



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

## 2.3 Deploying to Linux KVM

This section describes the deployment procedure to Linux KVM.

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

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



## 2.4 Deploying to Nutanix AHV+

This section describes the deployment procedure to Nutanix AHV.

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

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

## 2.5 Deploy to Microsoft Azure

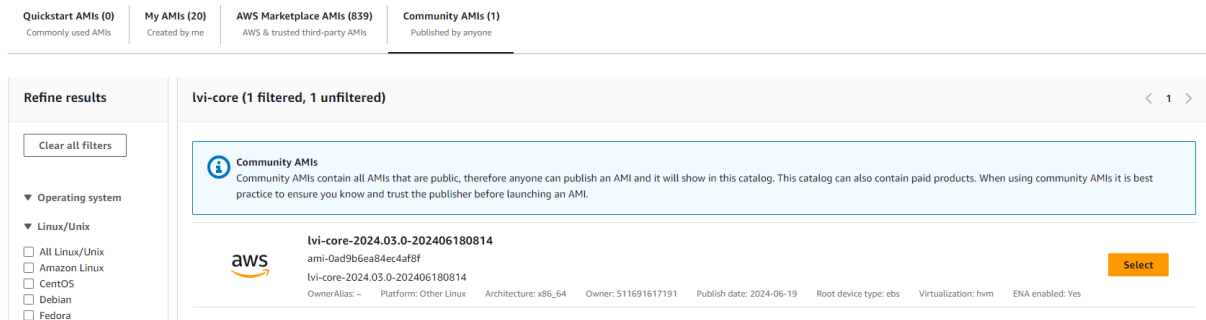
This section describes the deployment procedure to Microsoft Azure.

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

This completes the deployment on Azure.

## 2.6 Deploying to AWS

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



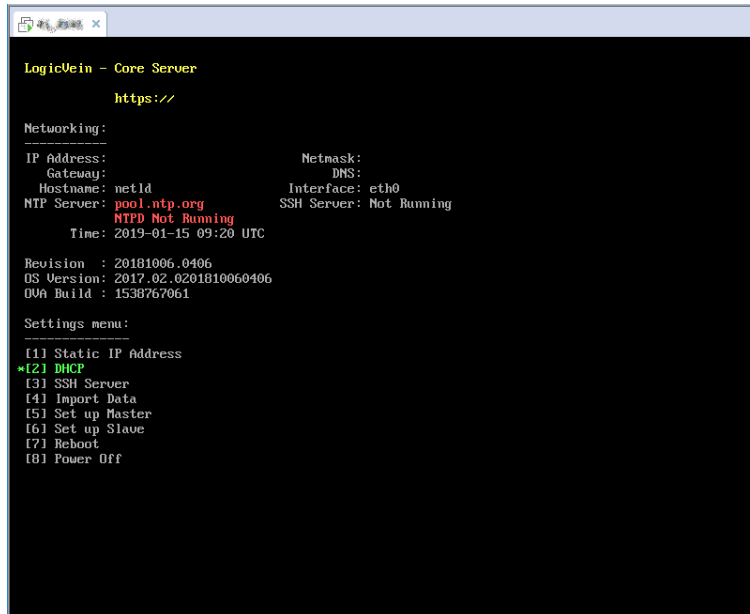
5. Select an instance type based on the sizing guidelines
6. After creating a key pair in Key Pair (login), click download key pair
7. In the network settings, assign a group. You can choose an existing security group or create one, you can add a new security group
8. Under Configure Storage, click add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

## 2.7 Configuring Network Settings

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

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

1. Press the “1” key on your keyboard [Static IP Address] and choose.



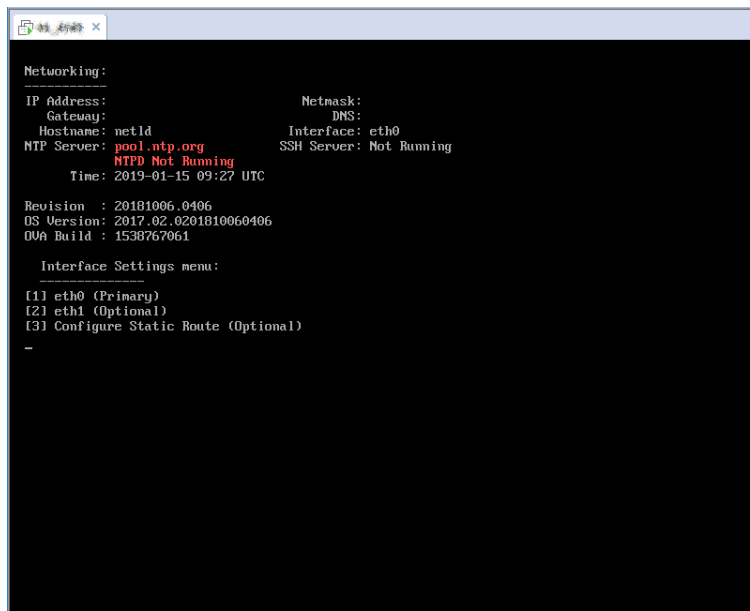
```
LogicVein - Core Server
https://

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

Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

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

2. Press the “1” key on your keyboard [eth0 (Primary)] and choose.



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

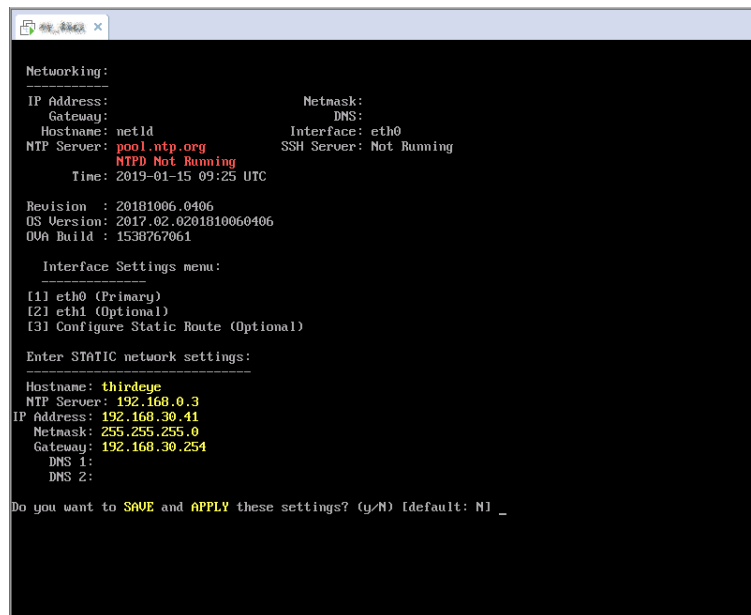
Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

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

- The following network setting items will be displayed in order. Enter the value using the keyboard and press the "Enter" key to proceed.

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

- A confirmation message will be displayed. Press the "Y" key on your keyboard to save the settings.



```

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

Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

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

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

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

```

That's all for the settings. After configuration, the service will restart automatically.

## 2.8 Apply the license

Apply your license and activate your product.

1. Access NetLD by entering its address in your web browser.

`https://<Address>/`

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

2. The license authentication screen will be displayed. Copy and paste **activation key** or **serial number**, enter it, and click [Activate].
- If you can't connect to the internet : **activation key**
  - If you can connect to the internet : **serial number** (Number consisting of 25 alphanumeric characters)

Update License

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

**Serial#:** 16710-4FE93-740EB-98948-AC197

Activation Key:

1nW28EHyw1vcKKWO1y+wb/PwBpGmUe2Uh+vg7wm0AX+TNwUYvAeG1spaWFFYoo0b  
EA6B3q4QTxd9S18ZFmMNBngie1/jQOqf1eQb5uywv3d2hu5eONbbLn5vgM1M3fq  
s0nGo/2KD4Eyo1BSbB7FDHqJkMzuFw3M81Xkb9QeSL7a97vUQuur5j5uEoqakjX6  
ZjJ1tvtHs1iH3hSn+pOsJUrWim871N20Sp72hnNtXAWPZOTScldAISOd9gxqdBp  
+ZzOU9gMHPV4UC/p4qcB3fcSYcnkQL1t2LTTyPzNg5gKGORhRJiZi7LvILMPGUXP  
R3NqIBx9V2UgmuvyBRzHekZKMeTSfpBg1W0VTjAAQg/cljtdSCKP/ZSMUBSKgoVg  
sK81zUDFOpGh25wLaRGxWEYav1Lo+bFwOTQkKPSzrVM=

ActivateCancel

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

## 2.9 Initial settings (detailed settings)

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

**Welcome**

**Admin User**

The email address used by the admin user. Email:

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

Confirm Password:

**Server Default Locale**

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

The timezone used when sending emails. Timezone:

**Server**

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

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

**Mail Server**

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

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

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

[Advanced Settings](#) [Test Email Configurations](#)

[Finish](#)

Items	Explanation	Required items
admin user settings	admin user email address	—
	admin user login password	must
Locale settings	Language when sending email	—
	Time zone when sending email	—
server settings	Browser tab display name	—
	Host name or IP address used for link addresses in emails, etc.	—
Email settings	SMTP server host name or IP address	—
	Email address when sending email	—
	Sender name when sending email	—

### Notice

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

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

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

## 3: Login/Logout

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

### 3.1 Log in

1. Access NetLD by entering its address in your web browser.

`https://<Address>/`

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

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



\*For a new installation, "2.4 Initial settings" to set the password for the admin user.

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

### 3.2 Log out

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

The image shows the NetLD top screen, which is a dashboard with various tabs and a large data table. The tabs include 'Inventory', 'Changes', 'Jobs', 'Terminal Proxy', 'Search', 'Compliance', and 'Zero-Touch'. The 'Inventory' tab is selected, showing a table of network devices. The table has columns for IP Address, Hostname, Network, Adapter, HW Vendor, Model, Device Type, OS Version, Serial#, Backup Duration, End Of Sale, End Of Life, Software End Of Sale, and Software End Of Life. The table contains several rows of data for different network devices.

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
192.168.20.81	SF300-24	Core	Class Small Business	Cisco	SF300-24	Switch	1.4.1.5	DN14440217	28h				
192.168.1.1	C8000-M4C	Core	Class IOS	Cisco	C8000-M4C-48	Wireless Controller	15.5.5a	FD24510000	1h				
10.0.0.223	_1234	Core	Class IOS	Cisco	C381000V	Router	17.3.5	9M7TH050005	1h				
10.0.0.227	Nexus548	Core	Class Nexus	Cisco	Nexus548	Switch	7.50(N11)	SD140370807	7h				
192.168.0.204	Netgear43	Core	Class IOS	Cisco	WS-C2960-24TS	Switch	16.8.1a	FD0000700042	3h				
168.100.89	inet_168_100_89	Core	Class IOS	Cisco	C381000V	Router	15.4(1)54	9W71QJ4R009	1h				

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



## 4: Basic settings

This section describes the basic settings for managing with NetLD.

### 4.1 Set credentials

If you want to manage device, you need to set the credentials (VTY username/password, SNMP community etc.) set on the managed device in NetLD. Set the credentials on the device tab under [Inventory] → [Credentials].

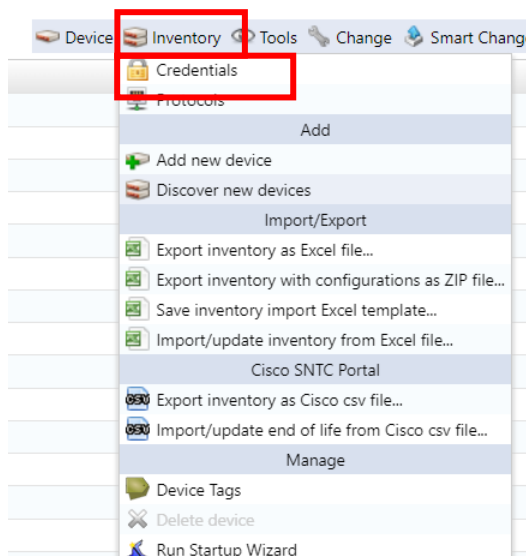
There are two ways to set credentials: "dynamic" and "static".

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

#### 4.1.1 Set common credentials

If you have set common credentials for monitored devices, use "Dynamic" to set them.

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



2. Click (Add) or Add new network group.

The screenshot shows the 'Credentials' window. On the left is a 'Network Groups' list with several empty rows. Below the list is a toolbar with a green plus icon (highlighted with a red box), a red X icon, an up arrow, and a down arrow. In the center, there is a message: 'Use network groups to define groups of devices that require specific credentials for authentication.' Below this message is a button labeled '+ Add a new network group.' (highlighted with a red box). At the bottom right are 'OK' and 'Cancel' buttons.

3. Enter the network group name, select Dynamic, and click OK.

The screenshot shows the 'New Network Group' dialog box. It has a title bar 'New Network Group'. Below the title bar is a text input field with the text 'new networks'. Below the input field are two radio button options: 'Dynamic - Credentials by CIDR, Range, Wildcard' (selected) and 'Static - Credentials by specific IP address'. Below the 'Dynamic' option is an example: 'e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.\*'. Below the 'Static' option is an example: 'e.g.) 192.168.1.1'. At the bottom right are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red box.

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

The screenshot shows the 'Credentials' window. On the left is a 'Network Groups' list with one entry: '\*new networks'. Below the list is a toolbar with a green plus icon, a red X icon, an up arrow, and a down arrow. In the center, there is a section titled 'Add address:' with a text input field containing '(IP, CIDR, Wildcard, or Range)' and a green plus icon (highlighted with a red box). Below this section is a 'Credentials' section with a 'New Credentials' list and a toolbar with a green plus icon, a red X icon, an up arrow, and a down arrow. To the right of the 'New Credentials' list are several input fields for 'VTY Username', 'VTY Password', 'Enable Username', 'Enable Secret/Password', 'SNMP Get Community', 'SNMPv3 Authentication Username', 'SNMPv3 Authentication Password', and 'SNMPv3 Privacy Password'. At the bottom right are 'OK' and 'Cancel' buttons.

5. Set each item.

The screenshot shows the 'Credentials' configuration window. On the left, there are two sections: 'Network Groups' with a list containing '\*new networks' and 'Credentials' with a list containing 'New Credentials'. The main area of the window is divided into two parts. The top part has an 'Add address:' label and a text input field with a placeholder '(IP, CIDR, Wildcard, or Range)' and a '+' button. The bottom part contains a table of credential fields. A red rectangle highlights the 'New Credentials' list and the credential input fields. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

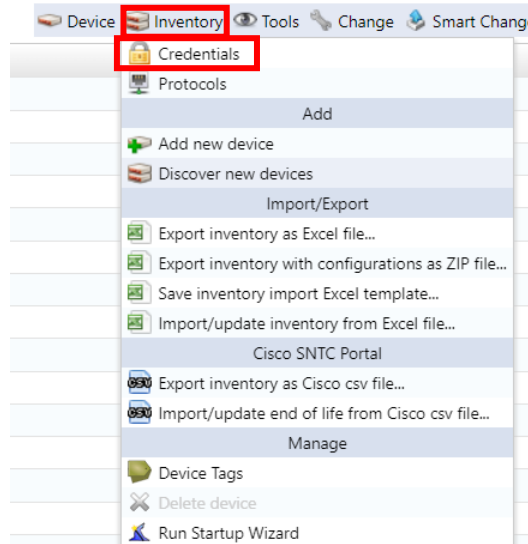
\*It is possible to omit inputting items that are not required.

6. Click OK to save your settings.

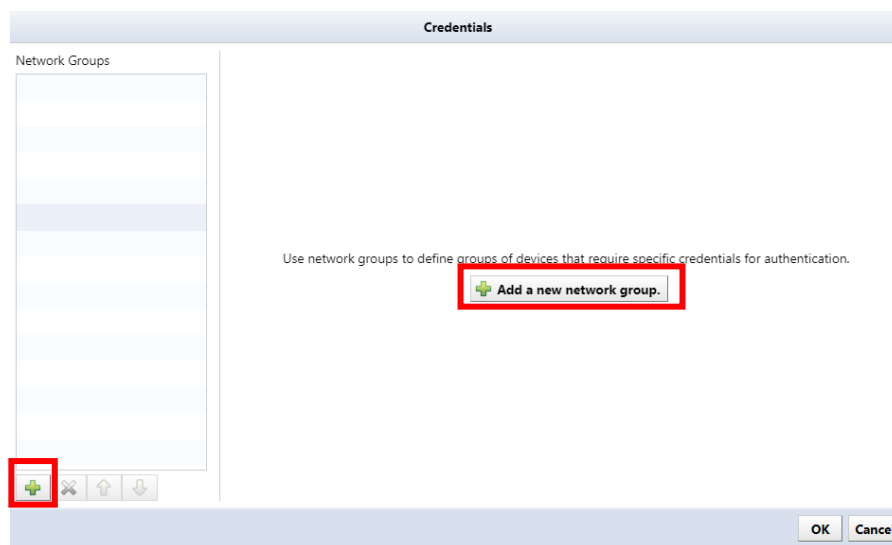
### 4.1.2 Set credentials for each device

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

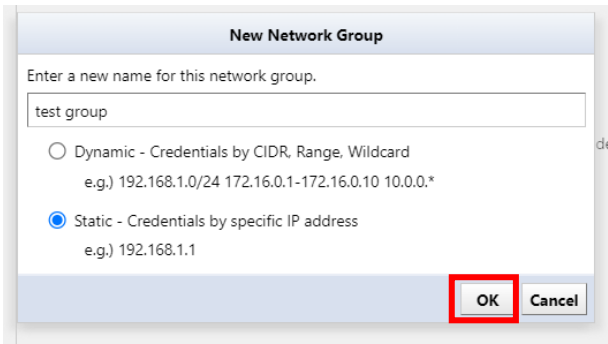
1. Select the Devices tab and click Inventory > Credentials.



2. Click + or Add a new network group.

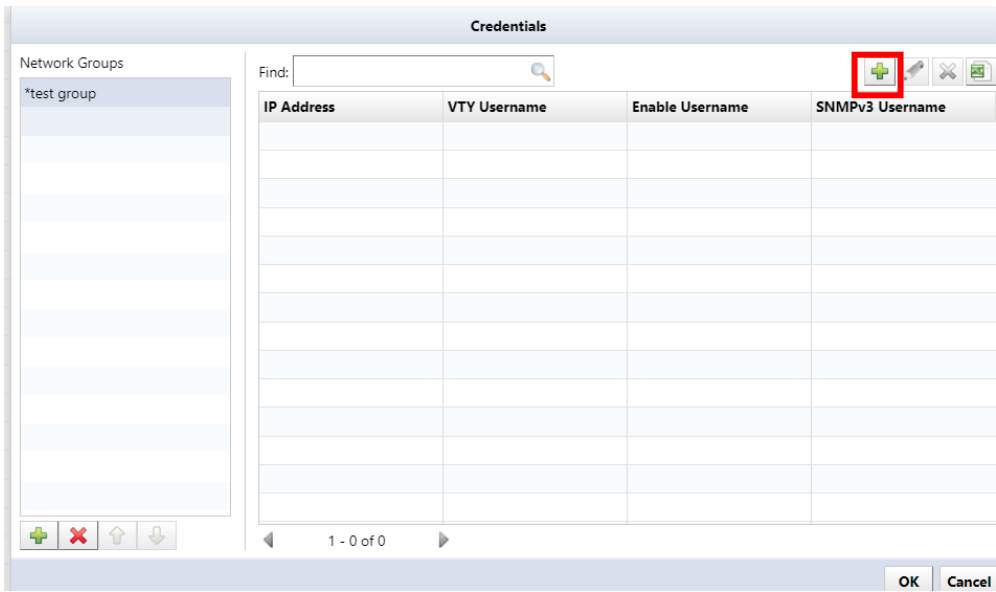


3. Enter the network group name, select Static, and click OK.



The 'New Network Group' dialog box is shown. It has a title bar 'New Network Group'. Below the title bar, it says 'Enter a new name for this network group.' There is a text input field containing 'test group'. Below the input field, there are two radio button options: 'Dynamic - Credentials by CIDR, Range, Wildcard' with the example 'e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.\*' and 'Static - Credentials by specific IP address' with the example 'e.g.) 192.168.1.1'. The 'Static' option is selected. At the bottom right, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red rectangle.

4. Click +.



The 'Credentials' window is shown. It has a title bar 'Credentials'. On the left, there is a 'Network Groups' list with '\*test group' selected. On the right, there is a table with columns: 'IP Address', 'VTY Username', 'Enable Username', and 'SNMPv3 Username'. The table is empty. Above the table, there is a 'Find:' search bar. To the right of the search bar, there is a '+' icon highlighted with a red rectangle. At the bottom right, there are 'OK' and 'Cancel' buttons.

5. Enter the IP address and set each item.



The 'Credential Set' dialog box is shown. It has a title bar 'Credential Set'. Inside, there are several input fields: 'IP Address:', 'VTY Username:', 'VTY Password:', 'Enable Username:', 'Enable Secret/Password:', 'SNMP Get Community:', 'SNMPv3 Authentication Username:', 'SNMPv3 Authentication Password:', and 'SNMPv3 Privacy Password:'. All these input fields are highlighted with a red rectangle. At the bottom right, there are 'OK' and 'Cancel' buttons.

Items	Explanation
IP address	Enter the IP address of your network device.

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

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

6. Click OK.
7. Click OK to save your settings.

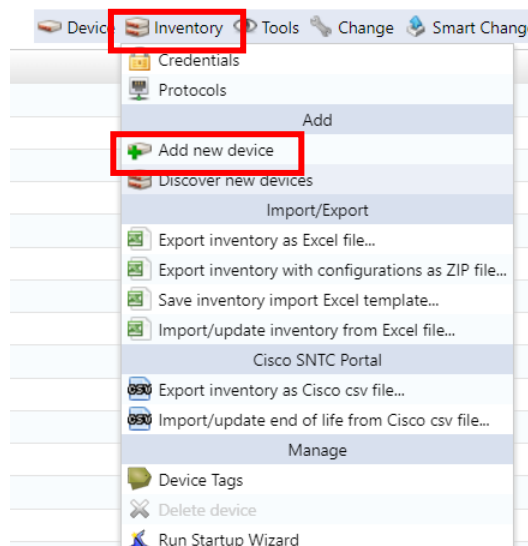
## 4.2 Add device

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

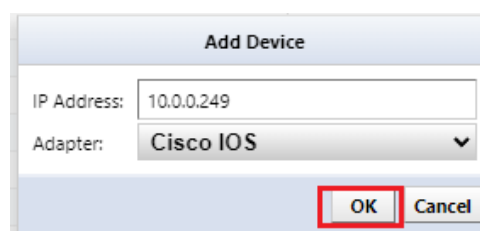
Items	Explanation
manual	Add a device by directly entering the device's IP address. Add one unit at a time.
discovery	Automatically discover and add devices within the specified IP address range.
import	This function reads device data from an XLSX file. Export the template file for import and enter information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

### 4.2.1 Register one device at a time

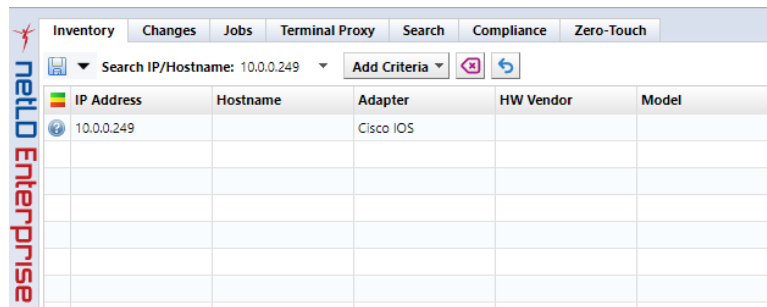
1. Select the Inventory button > Add new device.



2. Enter the IP address of the device you want to add and click OK.



Once NetLD completes collecting information from the monitored devices, the added devices will be added to the device list.

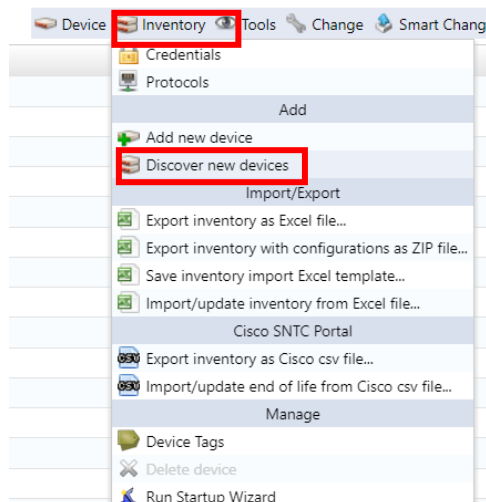


IP Address	Hostname	Adapter	HW Vendor	Model
10.0.0.249		Cisco IOS		


\*Even if it is not possible to communicate with the target IP address, the device will be added, but the host name and interface information will not be obtained.

## 4.2.2 Register devices on your network

1. Select the Inventory button and click Discover new device.



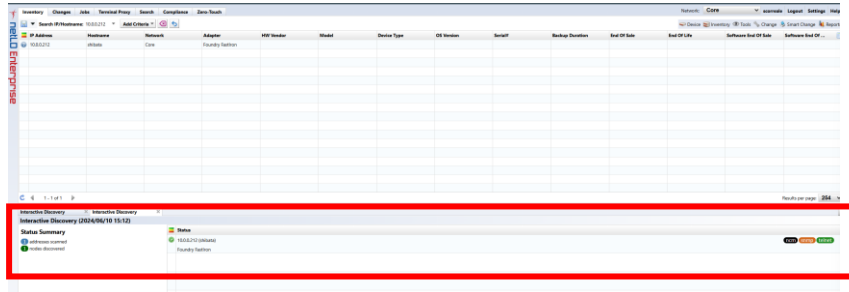
2. Specify the IP address range to discover, and click +.





Items	Explanation
Refer to the device's routing table and add discovery targets	Add a discovery target network by referring to the discovered device's routing table.
Refer to the routing table of already registered devices and add discovery targets.	If there is already a registered device, add a discovery target network by referring to the routing table of the registered device.
Assigning a Linux adapter to an SSH host that cannot identify the adapter	Assigns a Linux adapter when the adapter for configuration backup cannot be recognized.

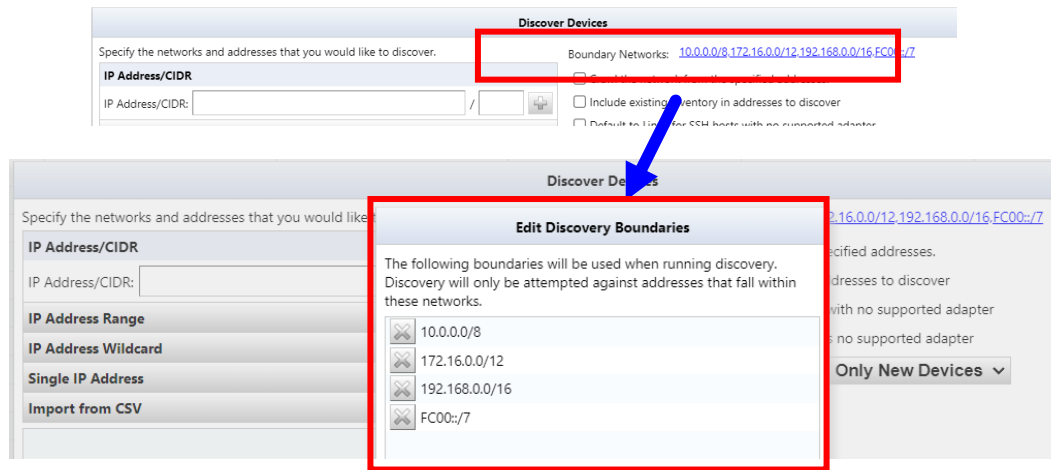
3. The input information will be added to the bottom left of the screen. Click Run.
4. Discovery will start and the discovery results will be displayed at the bottom of the screen.



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

## Supplement

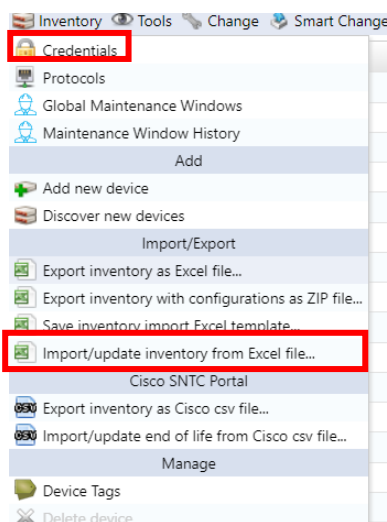
Discovery has a setting called "Perimeter Network", which allows you to limit the scope of discovery to the range specified in "Perimeter Network". Several ranges are specified for "Perimeter Network" by default, so edit "Perimeter Network" as necessary.



### 4.2.3 Import registration from Excel file

Information on monitored devices can be imported from an Excel file. A template for import is provided, so please export the template file in advance, fill in the information of the monitored device in that file, and then import it.

1. Select the Inventory button and click → [Save inventory import Excel Template].



2. The file opening screen will be displayed. Select "Save file" and click [OK].

\*The file name will be "NetLD-inventory-template.xlsx" and will be saved in XLSX file format.

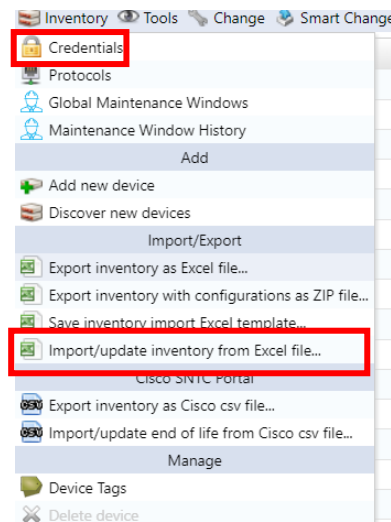
3. Edit the saved file, enter information in the following fields, and overwrite and save.

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

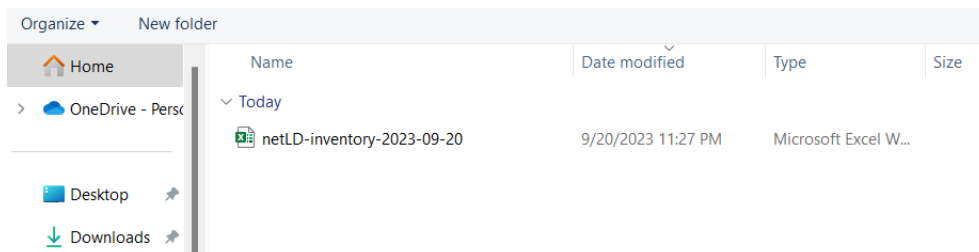
Items	Explanation	Required items	Input example
IP Address	Enter the device's IP address.	must	192.168.1.10
Network	Select the network name to which you want to add the device.	must	Default
Adapter ID	Select your device's adapter. *In the current version, there is no need to specify this item.	—	Cisco IOS

Hostname	Enter the device hostname.	—	
End Of Sale	Enter the sales end date in the format "yyyy/mm/dd".	—	2022/1/1
End Of Life	Enter the support end date in the format "yyyy/mm/dd".	—	2022/12/31
Custom 1～5	Enter the information for "Custom Device Field".	—	

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



5. A file selection dialog will be displayed. Select the edited file and click Open.



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



## 5: Use operations

This section describes operations used in daily operations.

### 5.1 Get Device Configuration

In NetLD, obtaining the device configuration is called a "Backup". To backup, NetLD connects to the device via SSH or Telnet and retrieves the configuration using show commands, tftp commands, etc.

#### 5.1.1 Prerequisites

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

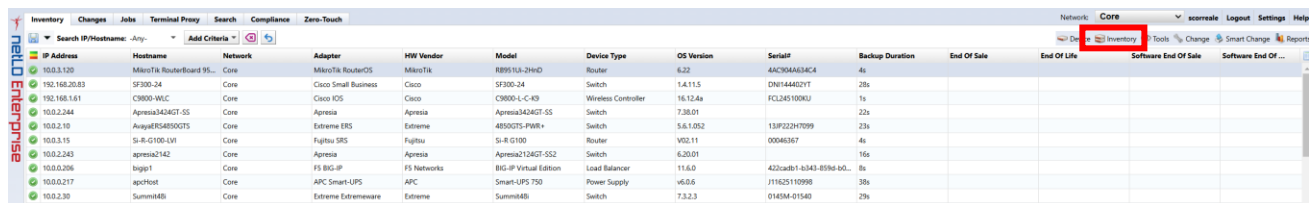
- The username and password for logging in to the device have been set.  
Refer to [4.1 Set credentials](#), and make sure that the credentials have been set.
- The model supports configuration backup by NetLD.

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

<https://logicvein.com/supported-devices>

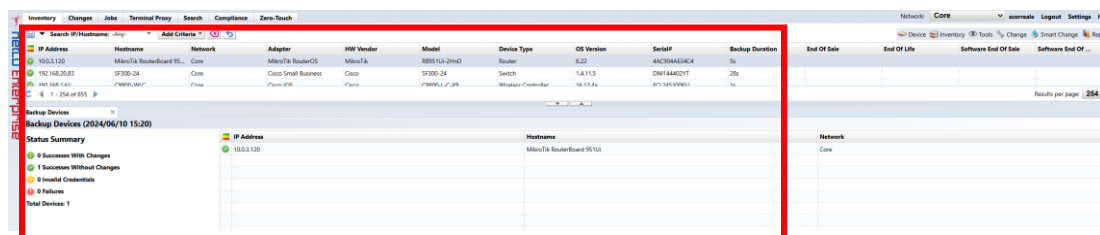
#### 5.1.2 Run a backup



To perform a backup, select the target device and click Backup from the device menu.





IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of ...
10.0.3.120	MicroTik RouterBoard 95...	Core	MicroTik RouterOS	MicroTik	RB951U-2HnD	Router	6.22	4AC70A6A34C4	4s				
192.168.20.83	SF300-24	Core	Cisco Smart Business	Cisco	SF300-24	Switch	1.4.11.5	DN144402YT	28s				
192.168.1.61	C9609-M4C	Core	Cisco IOS	Cisco	C9609-L-C-K9	Wireless Controller	16.12.4a	PCL245100KJ	1s				
192.0.2.244	Aprisa342G7-SS	Core	Aprisa	Aprisa	Aprisa342G7-SS	Switch	7.38.01		23s				
10.0.2.10	AvayaE854800TS	Core	Extreme ERS	Extreme	485025-PW8+	Switch	5.6.1.052	13P223H7099	23s				
10.0.3.15	Si-R-G100-LV1	Core	Fujitsu SRS	Fujitsu	Si-R-G100	Router	V03.11	00046367	4s				
10.0.2.243	aprisa2142	Core	Aprisa	Aprisa	Aprisa2142G7-SS2	Switch	6.20.01		16s				
10.0.0.206	bigip1	Core	F5 BIG-IP	F5 Networks	BIG-IP Virtual Edition	Load Balancer	11.6.0	422cad81-6343-859d-b0...	8s				
10.0.0.217	apcHost	Core	APC Smart-UPS	APC	Smart-UPS 750	Power Supply	v6.0.6	J11625110998	38s				
10.0.2.30	Summi48	Core	Extreme Extremesware	Extreme	Summi48	Switch	7.3.2.3	01405M-01540	29s				



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



Icon	Explanation
	Backup successful, changes made. Displayed when a difference is detected between the last backup and the configuration on the device. It will also be displayed during the first backup.
	Backup successful, no changes. Displayed when the configuration data on the device is the same as the last backup.








The status summary list for backup execution is as follows.

Icon	Explanation
	Backup successful, changes made. Displayed when a difference is detected between the last backup and the configuration on the device. It will also be displayed during the first backup.
	Backup successful, no changes. Displayed when the configuration data on the device is the same as the last backup.

Icon	Explanation
	Backup failed due to credentials mismatch. The registered credentials are incorrect. Click on the result shown on the right to see the credentials used for the backup. Please check the Inventory → Credential settings.
	Backup failed. Configuration could not be obtained. Double-click the icon to view details.

### 5.1.3 About the status after backup

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

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

## 5.1.4 Check the obtained configuration

You can check the acquired configuration from the device details screen.

The screenshot shows the Cisco Enterprise Network Manager interface. The top navigation bar includes links for Inventory, Changes, Jobs, Terminal Proxy, Search, Compliance, and Zero-Touch. The search bar shows "1921" and "1921". The table below the search bar lists configuration snapshots for a Cisco 1921 router. The table has columns for Snapshot, Config, Timestamp, Size, and User. A red box highlights the configuration snapshots table.

Snapshot	Config	Timestamp	Size	User
2024/06/05 12:34	/running-config	2024/06/05 12:34	9824	admin
2024/06/04 12:33	/startup-config	2024/06/04 12:33	9824	admin
2024/06/04 12:33	/running-config	2024/06/04 12:33	9824	admin
2024/06/01 12:33	/startup-config	2024/06/01 12:33	9791	admin
2024/06/01 12:33	/running-config	2024/06/01 12:33	9791	admin
2024/06/02 11:33	/running-config	2024/06/02 11:33	12330	admin
2024/06/03 11:35	/startup-config	2024/06/03 11:35	12062	admin
2024/06/03 11:35	/running-config	2024/06/03 11:35	12062	admin

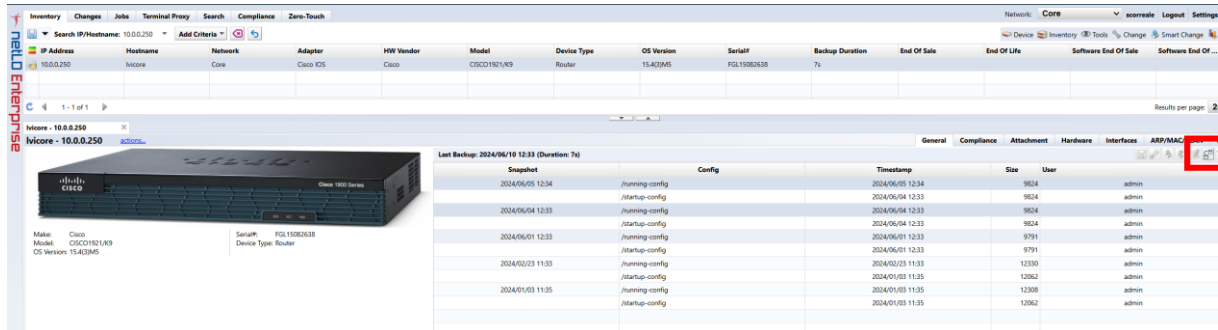
You can check the contents by double-clicking on the config.

```
2019/12/12 23:14
1 version 15.4
2 service timestamps debug datetime msec
3 service timestamps log datetime msec
4 no service password-encryption
5 !
6 hostname Cisco1921
7 !
8 boot-start-marker
9 boot-end-marker
10 !
11 !
12 enable secret 5 $1skx1h4bfnr5P8p7mdWV0hFF9AM/
13 !
14 aaa new-model
15 !
16 !
17 !
18 !
19 !
20 !
21 !
22 aaa session-id common
23 !
24 !
25 !
26 !
```

## 5.1.5 Comparison of configs

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

\*Multiple selections can be made by holding down the "Ctrl" key while selecting.



The screenshot shows the Cisco Enterprise Manager interface. On the left, there is a sidebar with 'Inventory', 'Changes', 'Jobs', 'Terminal Proxy', 'Search', 'Compliance', and 'Zero-Touch'. The main area displays a table of configurations for a Cisco 1921 router. The table has columns for 'IP Address', 'Hostname', 'Network', 'Adapter', 'HW Vendor', 'Model', 'Device Type', 'OS Version', 'Serial#', 'Backup Duration', 'End Of Sale', 'End Of Life', 'Software End Of Sale', and 'Software End Of ...'. A 'Compare' button is highlighted in the top right corner of the configuration list.

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



The screenshot shows a configuration comparison tool. It displays two startup configurations side-by-side. The left configuration is from 2019/06/14 18:00 and the right is from 2019/07/24 18:00. Differences are highlighted in red (deleted), yellow (changed), and green (added). The configurations are for a Cisco 1921 router. The left configuration includes lines for flow monitor, service-policy, and interface configuration. The right configuration includes similar lines but with some changes, such as the addition of a new service-policy and the deletion of an old one.

## 5.2 Make an SSH/Telnet connection to the device

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

### 5.2.1 Preparation before use

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

- Install Tera Term on the terminal to be operated  
The terminal proxy calls Tera Term on the PC you are operating.
- Installing browser integration  
It is necessary to link the browser connected to NetLD and Tera Term.

This preparation can be done from the screen that appears when you start the terminal proxy for the first time. The installation procedure for [Step 2] "Browser Integration" is described below. For information on installing Tera Term, please check the Tera Term manual.

1. Click Install Integration and download registration entries file.

**Terminal Integration**

**Step 1: Tera Term Download**

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

Download Tera Term

**Step 2: Browser Integration**

Terminal integration must be installed before you can use the terminal launch feature. Click on the 'Install Integration' button and run the Registration Entries file.

Install Integration For Tera Term

Install Integration For Previous Tera Term Versions

2. Run the downloaded registration entries file.

Preparation is now complete.

#### supplement

Regarding "Browser Integration" in [Step 2], you may need to reconfigure if you clear your browser's cache or update NetLD.

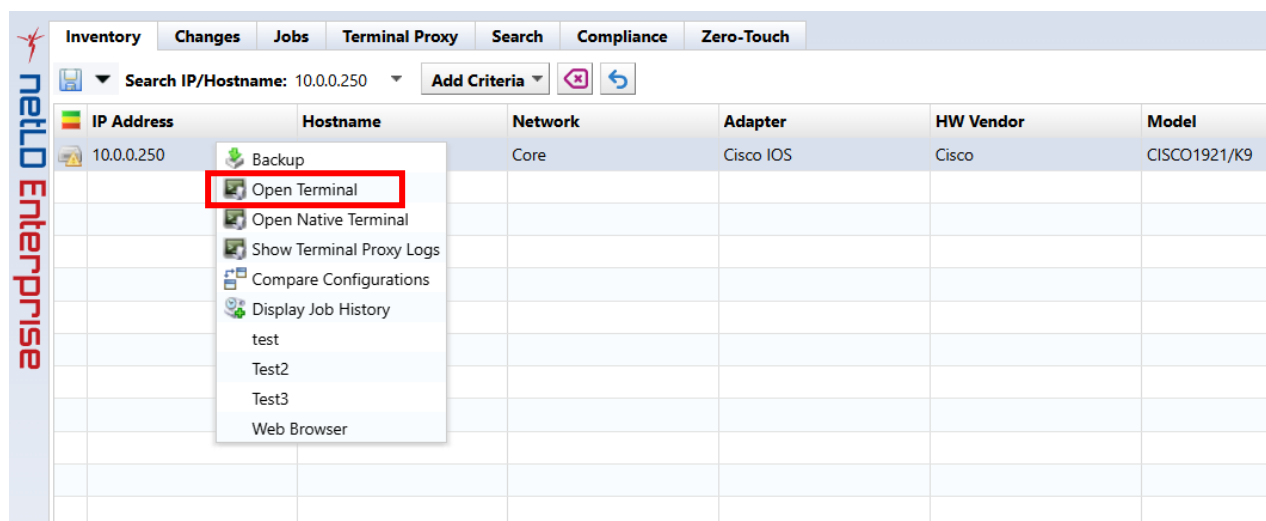


## 5.2.2 Start the terminal proxy

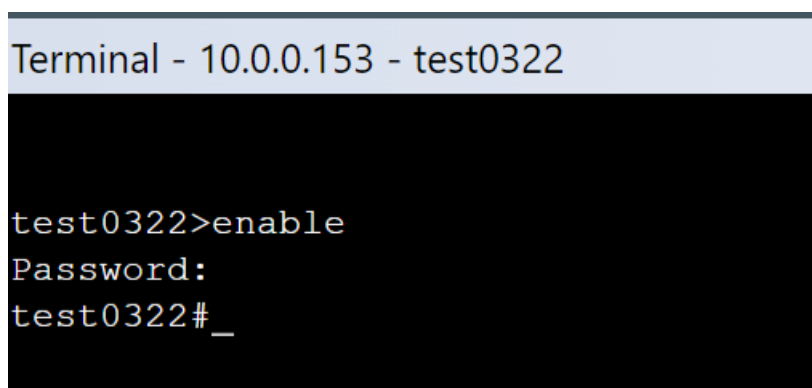
\*If a device configuration backup has been obtained when you start the terminal proxy, you can skip selecting the protocol and entering the user name/password after starting the terminal proxy.

### 5.2.2.1 Use web browser

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

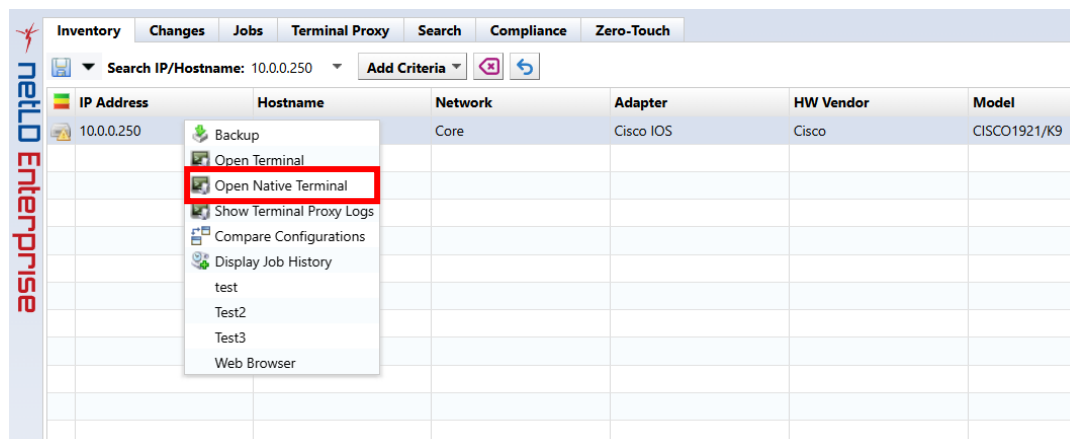


3. The terminal will open in a separate browser tab, and the device's login screen will be displayed. Enter your username and password to log into your device.

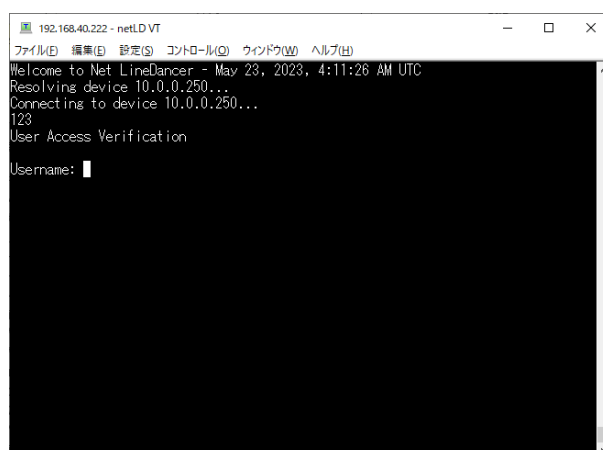


### 5.2.2.2 Use Tera Term

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

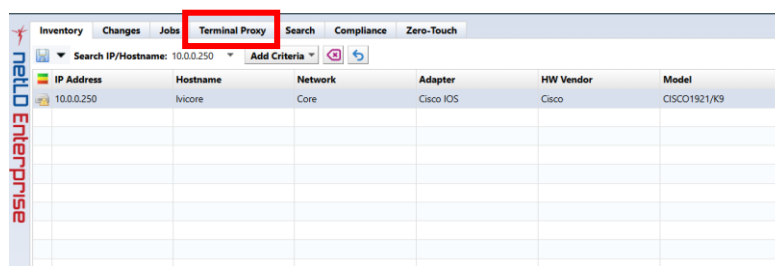


\*Tera Term will start and the device login screen will be displayed. Enter your username and password to log into your device.



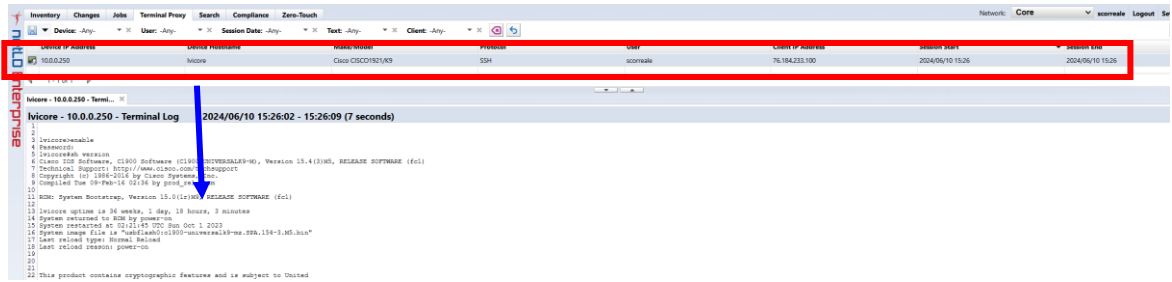
### 5.2.3 Check the operation log

1. Select the Terminal Proxy tab.



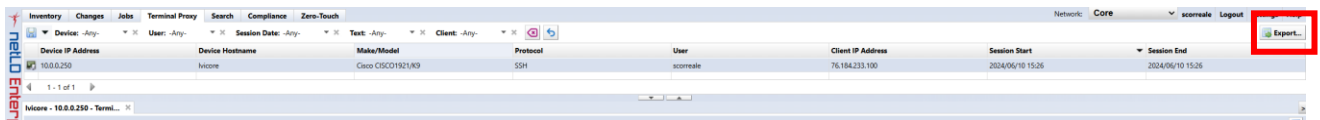
2. Double-click the log you want to view from the list.

\*You cannot check the session log while connected.



```
test0322 - 10.0.0.153 - Terminal Log    2024/03/12 03:21:34 - 03:21:41 (7 seconds)
1
2
3
4 test0322>enable
5 Password:
6 test0322#sh version
7 Cisco IOS XE Software, Version 03.11.04.S - Standard Support Release
8 Cisco IOS Software, CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.4(1)S4, RELEASE SOFTWARE (fc
9 Technical Support: http://www.cisco.com/techsupport
10 Copyright (c) 1986-2015 by Cisco Systems, Inc.
11 Compiled Fri 05-Jun-15 23:15 by mcpre
12
13
14 Cisco IOS-XE software, Copyright (c) 2005-2015 by cisco Systems, Inc.
15 All rights reserved. Certain components of Cisco IOS-XE software are
16 licensed under the GNU General Public License ("GPL") Version 2.0. The
17 software code licensed under GPL Version 2.0 is free software that comes
18 with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
19 GPL code under the terms of GPL Version 2.0. For more details, see the
20 documentation or "License Notice" file accompanying the IOS-XE software,
21 or the applicable URL provided on the flyer accompanying the IOS-XE
22 software.
23
24
```

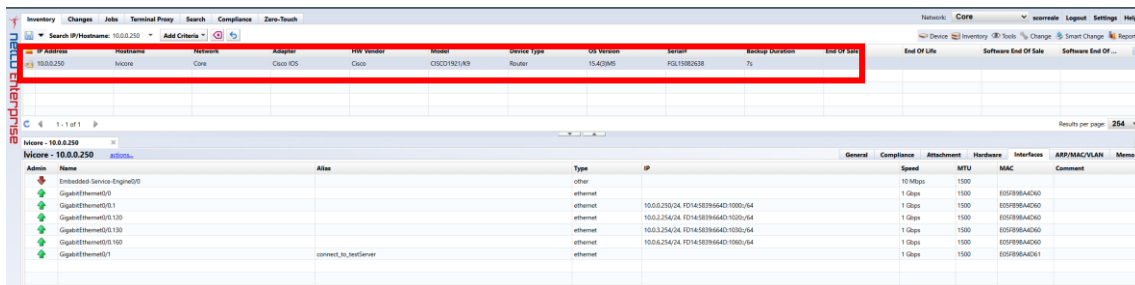
Click [ (Export)] at the top right of the log screen to save session data as a text file. The file name is “termlogs”.YYYY-MM-DD.zip” and are compiled in ZIP file format. "YYYY-MM-DD” indicates the date of saving.



## 5.3 Check the Up/Down status of the device interface

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

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



IP Address	Hostname	Network	Alias	File Vendor	Model	Device Type	OS Version	Serial	End of Sale
10.0.0.250	Netcore	Core	Cisco IOS	Cisco	CISCO1921-8B	Router	15.4(2)95	RL11582338	N

Admin	Name	Alias	Type	IP	Speed	MTU	MAC	Comment
	Embedded Service Engine0/0		other		10 Mbps	1500		
	GigabitEthernet0/0		ethernet		1 Gbps	1500	E05F96A0D0	
	GigabitEthernet0/0.1		ethernet	10.0.0.250/24	1 Gbps	1500	E05F96A0D0	
	GigabitEthernet0/0.130		ethernet	10.0.2.254/24	1 Gbps	1500	E05F96A0D0	
	GigabitEthernet0/0.130		ethernet	10.0.2.254/24	1 Gbps	1500	E05F96A0D0	
	GigabitEthernet0/0.160		ethernet	10.0.2.254/24	1 Gbps	1500	E05F96A0D0	
	GigabitEthernet0/1	connect_to_backend	ethernet		1 Gbps	1500	E05F96A0D1	

## 5.4 Jobs

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

**The Job History subtab has the following buttons:**

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

**The Job Management subtab has the following buttons:**

Items	Explanation
Audit Log	View audit log of the selected job.
Open Job	Open the properties of the selected job.
Delete	Delete the selected job.
Rename	Renames the selected job.
Copy	Copy the selected job.
Run Now	Run the selected job immediately.
New Job	Create a new job. You can add jobs for EOL/EOS, tools, discovery, neighbors, backups, bulk changes, and reports.
Filter	Register a cron-style filter.

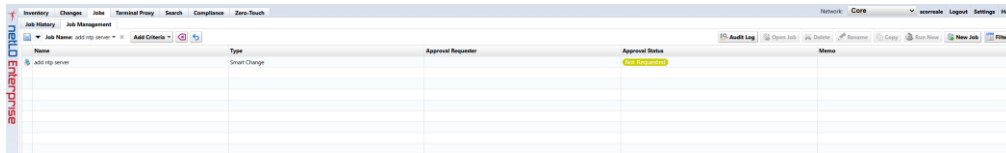
### 5.4.1 Create a job

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

#### [Flow of job creation procedure]

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

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



#### 5.4.1.1 Decide on a job name and choose a function

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

**Create Tool Job**

Job Name:

Network:  

Default
▼

Comment:

Tool:  

Change Enable Password
▼

#### 5.4.1.2 Enter the required parameters

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

**\*enable password**

Input Parameters
Devices
Schedule
Job Approvals Log
Email Notification

User Data

New Password

Password:

Confirm:

☒ Verify credentials after change is executed

#### 5.4.1.3 Select target device

Select the device on which you want to run this job on the Devices subtab. There are three selection methods: "All devices/Search/Static list".

##### 【All devices】

This applies to all registered devices.

\*enable password

Input Parameters

Devices

Schedule

Job Approvals Log

Email Notification

☒ All Devices
☐ Search
☐ Static list

## 【Search】

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

\*enable password

Input Parameters

Devices

Schedule

Job Approvals Log

Email Notification

☐ All Devices
☒ Search
☐ Static list

Add Criteria

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...	End Of Sale	End Of Life	Software End ...	Software End ...	Traits	Violation
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AUD099HDKJ	53s			2019/06/17	2024/06/30		
10.0.0.112	uefsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5H5HG7	50s						Node test is L...
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31				
10.0.0.124	bbbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVMIG0X	51s						
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UGZVVK9E	14s						
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9I4P8735EIN	4s						

## 【Static list】

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

Inventory

Changes

Jobs

Terminal Proxy

Search

Compliance

Zero-Touch

▼ Search IP/Hostname: -Any-

Add Criteria

↺

↻

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat...
10.0.3.120	MikroTik RouterBoard 95...	Core		MikroTik	RouterOS	Router	RB951Ui-2HnD		
192.168.20.83	SF300-24	Core		Cisco Small Business	Cisco	Switch	SF300-24		
192.168.1.61	C9800-WLC	Core		Cisco IOS	Cisco	Wireless Controller	C9800-L-C-K9		
10.0.2.244	Apresia3424GT-SS	Core		Apresia	Apresia3424GT-SS	Switch			
10.0.2.10	AvayaERS4850GTS	Core		Extreme ERS	Extreme	Switch	4850GTS-PWR+		
10.0.3.15	Si-R-G100-LVI	Core		Fujitsu SRS	Fujitsu	Router	Si-R G100		
10.0.2.243	apresia2142	Core		Apresia	Apresia2142GT-SS2	Switch			
10.0.0.206	bigip1	Core		F5 BIG-IP	F5 Networks	Load Balancer	BIG-IP Virtual Edition		
10.0.0.217	apchost	Core		APC Smart-UPS	APC	Power Supply	Smart-UPS 750		
10.0.2.30	Summit48i	Core		Extreme Extremeware	Extreme	Switch	Summit48i		
10.0.0.223	_1234	Core		Cisco IOS	Cisco	Router	CSR1000V		
10.0.2.242	FTOS	Core		Dell PowerConnect	Dell	Switch	S60-01-GE-44T-AC		
10.0.2.246	LVI-BrocadelCX	Core		Foundry Fasttron	Brocade	Switch	ICX6610-24		
10.0.2.245	Apresia13200	Core		Apresia	Apresia13200-S2GT	Switch			
10.0.0.227	Nexus5548	Core		Cisco Nexus	Cisco	Switch	Nexus5548		
192.168.20.225	ApresiaLightFM116GT-SS ...	Core		ApresiaLight	Hitachi	Switch	FM116GTS		
192.168.20.223	acm7004-2	Core		Opengear	Opengear	Resilience Gateway	ACM7004-2		

\*enable password

Input Parameters

Devices

Schedule

Job Approvals Log

Email Notification

☐ All Devices
☐ Search
☒ Static list

IP Address	Hostname	Network
10.0.2.10	AvayaERS4850GTS	Core
10.0.2.244	Apresia3424GT-SS	Core
10.0.3.120	MikroTik RouterBoard 951Ui	Core
192.168.1.61	C9800-WLC	Core
192.168.20.83	SF300-24	Core

### 5.4.1.4 Add a trigger

Finally, add the trigger. Click the Schedule subtab. You can add new triggers using the + button.

The screenshot shows a window titled 'enable password' with tabs for 'Input Parameters', 'Devices', 'Schedule', 'Job Approvals Log', and 'Email Notification'. The 'Schedule' tab is active, displaying a table with columns 'Trigger' and 'Next Fire Time(GMT-5)'. The table is currently empty. At the bottom left of the table, there is a red box highlighting a green '+' button, which is used to add new triggers.


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

The screenshot shows the 'Trigger' dialog box. The 'Name' field contains 'schedule'. Under the frequency options, the 'Once' radio button is selected. The time is set to 4:19 and the date is 2024/03/12. The timezone is set to '(GMT-06:00) Central Time' and the filter is set to '<No Filter>'. The 'Save' and 'Cancel' buttons are located at the bottom right of the dialog.

Items	Explanation
name	Trigger name
time	Time and date to run the job
Schedule unit	<p>Select from the following 5 types of execution schedules</p> <p>Once... Execute only once at the date and time set in the time.</p> <p>Daily: Execute every n days (starting point is the 1st of the current month)</p> <p>Weekly: Execute on a specific day of the week</p> <p>Monthly: Execute every specified month</p> <p>Cron: Run at the specified date and time in cron format</p>






Items	Explanation
time zone	Time zone
filter	Select the registered schedule filter in "Filter Settings". Timings that match this filter will be removed from the trigger.

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

### 5.4.2 Job history

The [Job] → [Job History] subtab displays a list of past job execution history. Past job execution status is recorded along with the status of whether the job was successful or failed.

The status icon is displayed on the left side of the job history list. The status icons and their meanings are as follows:

Icon	Explanation
	I was able to successfully connect to all devices.
	Processing failed on some devices.
	Processing failed on all devices.

### 5.4.3 Job approval function

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

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

#### Approval process

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

#### 5.4.3.1 Set permissions for approval function

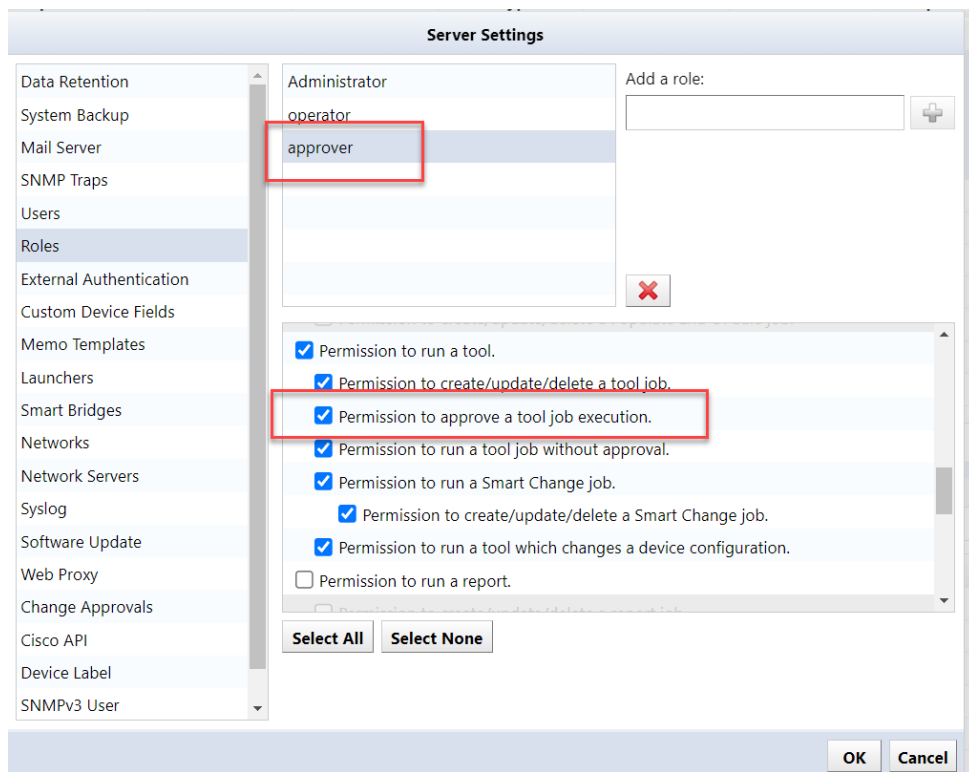
Set approvers for registered permissions. Users assigned the configured permissions can approve jobs.

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

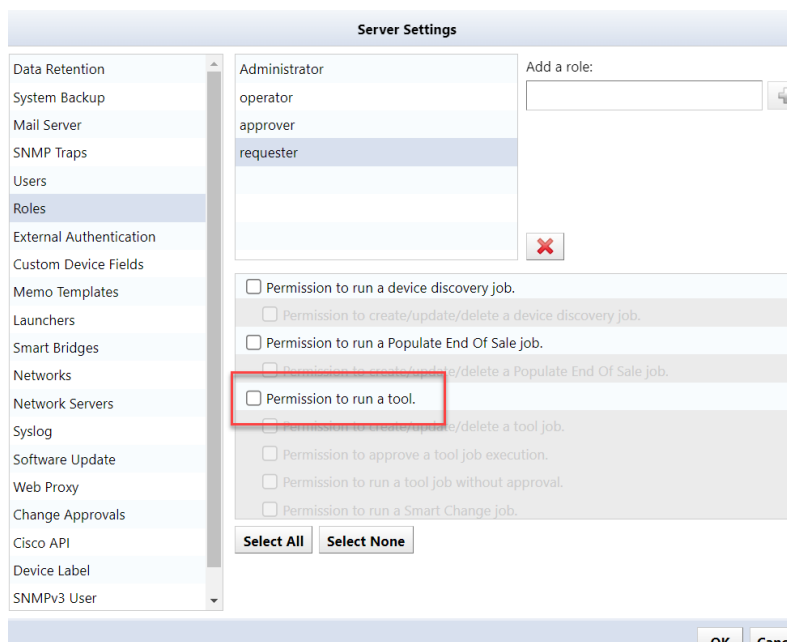
The authority related to the approval function consists of the following two authority contents.

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

- When setting the approver's permission, check "Permission to approve tool execution."



- When setting the requester's permission, uncheck "Permission to approve a tool job execution."



#### 5.4.3.2 Submit an approval request (submit a job)

Requester can request approval when creating or editing a job.

1. Create/edit jobs.
2. Open the [Job Approval Log] tab, enter a message in the message field, and click [Request Approval].

When the application is completed, "Request" is displayed in the [Job Approval Status] column.

- Display example of the [Job approval status] column
- List of display contents in the [Job approval status] column

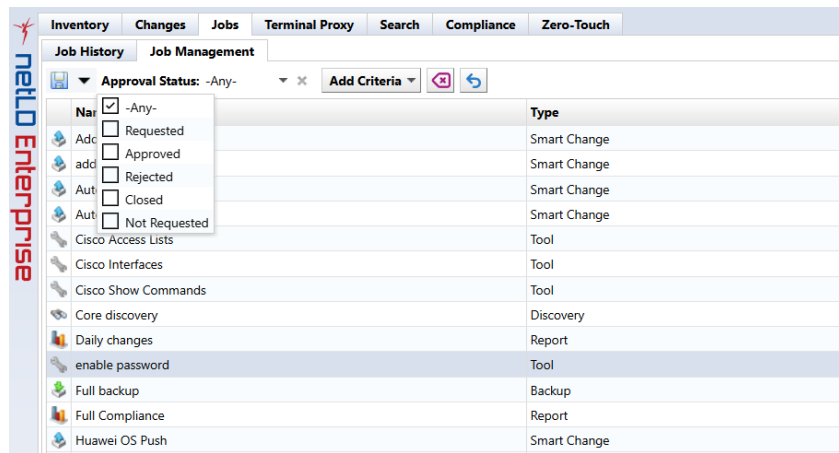
Job approval status	Explanation
No Requested	Job approval request is not set.
Requested	Job execution approval is requested.
Approved	Job execution is approved.
Rejected	Job approval request rejected.
Closed	Job is closed. This status is set when: Execute the job Closed by administrator/job requester *If you want to execute a closed job, you will need to request approval again.

#### 5.4.3.3 Approve an approval request (approve the job)

Approver can approve jobs (approval requests) applied by requester.

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

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



3. Check the job details and open the [Job Approval Log] tab.
  4. Enter your message in the message field and click Approve.
- If you have a problem, enter your message in the message field and click Reject or Comment.

#### 5.4.3.4 Check the record up to approval

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

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

#### 5.4.3.5 Notification of approval function

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

##### 5.4.3.5.1 SNMP trap settings

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

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

The screenshot shows the 'Server Settings' window with a sidebar on the left containing various settings categories. 'SNMP Traps' is selected and highlighted. The main area is titled 'Send traps when...' and contains a list of events with checkboxes. The checkbox for 'a change approval action occurs' is checked and highlighted with a red rectangle. Below this, there is a 'Trap forwarding:' section with a checkbox for 'Forward all received traps' which is unchecked. At the bottom, there is a 'Trap receivers:' section with a table. The table has four columns: 'Community', 'Host', 'Port', and 'Version'. The first row contains the values 'public', '10.0.0.93', '162', and '2c'. There are three empty rows below it. At the bottom right of the table are three icons: a green plus sign, a pencil, and a red X. At the very bottom of the window are 'OK' and 'Cancel' buttons.

Community	Host	Port	Version
public	10.0.0.93	162	2c

##### 5.4.3.5.2 send e-mail

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

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

**Server Settings**

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

SMTP Host:  
protection.outlook.com

From Email Address:  
support3eye@lvi.co.jp

From Name:  
support3eye

☐ Server requires authentication  
☐ Use secure smtp  
☒ Automatically upgrade STARTTLS negotiation

Mail server username:

Mail server password:

Default email language:

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

Test

OK Cancel

Additionally, if there is a job approval request, a banner will be displayed.

#### 5.4.3.6 Change the number of required approvals

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

**Server Settings**

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

Minimum required approval count: 1

OK Cancel

#### 5.4.4 Check past job history

You can check the job history from the [Job] tab → [Job History], and the jobs that have been executed so far are displayed. Job types include Report/Discovery/Neighbor/Backup/Tool, and information such as "when", "who", and "what was done" is recorded. You can also view the published report by double-clicking on the report job.

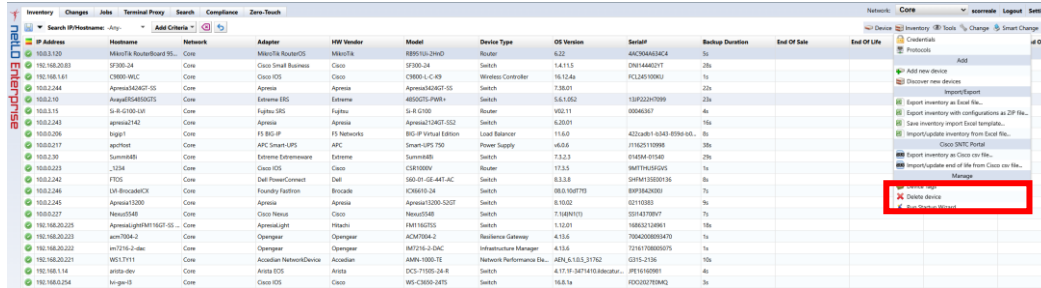
[Column list]

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



## 5.5 Remove device

1. Select the device you want to delete on the Inventory tab. \*Multiple selections possible



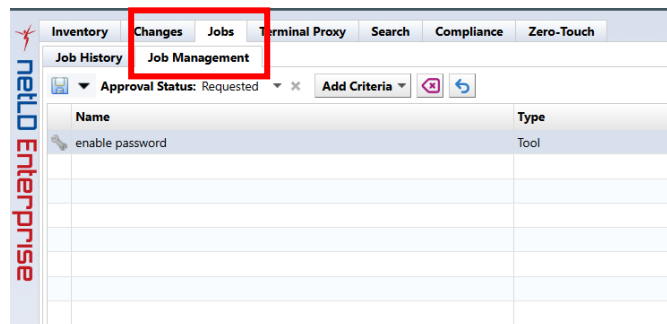
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Date	End Of Life
10.0.0.120	Mikrotik RouterBoard 95...	Core	Mikrotik RouterOS	Mikrotik	R8801u-2HnD	Router	6.22	AKC70A4434C4	5s		
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	CN1446231T	25s		
192.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-49	Wireless Controller	16.12.0a	PC1347108802	1s		
10.0.0.244	Agave4565627-OS	Core	Agave	Agave	Agave4565627-OS	Switch	7.3.0.1	7.3.0.1	25s		
10.0.0.10	Avaya4565627S	Core	Extrema	Extrema	4565627S-P888+	Switch	5.6.1.0.2	13P022207099	25s		
10.0.0.15	S-4-G100-L41	Core	Fujitsu IPS	Fujitsu	S-4-G100	Router	V02.11	00046267	4s		
10.0.0.243	apex4565627-42	Core	Agave	Agave	Apex4565627-022	Switch	6.20.01		15s		
10.0.0.206	big1-1	Core	F5 BIG-IP	F5 Networks	BIG-IP Virtual Edition	Load Balancer	11.6.0	4220a01-6343-8396a0...	5s		
10.0.0.217	apex4565627	Core	APC Smart-UPS	APC	Smart-UPS 750	Power Supply	v4.0.6	JT1025100908	30s		
10.0.0.20	Summit4565627	Core	Extrema	Extrema	Summit4565627	Switch	7.3.0.3	010204-01049	25s		
10.0.0.223	_1234	Core	Cisco IOS	Cisco	C3810B8N	Router	17.3.5	94074050505	1s		
10.0.0.242	F705	Core	Dell PowerConnect	Dell	S60-01-GE-48T-AC	Switch	8.3.3.8	SH4M13300136	5s		
10.0.0.246	UP-Brocade4565627	Core	Brocade	Brocade	KVM670-24	Switch	8.0.0.100709	84P2642002	7s		
10.0.0.245	Agave4565627-020	Core	Agave	Agave	Apex4565627-020	Switch	6.10.02	02101001	5s		
10.0.0.227	Neu4565627	Core	Cisco Nexus	Cisco	Nexus4565627	Switch	7.1.0.0.101	0314370007	7s		
192.168.20.225	Agave4565627-1001-OS	Core	Agave	Agave	1001-1001	Switch	1.1.0.01	1001-1001	10s		
192.168.20.223	am7004-2	Core	Openstack	Openstack	ACM7004-2	Resilience Gateway	4.1.0.6	7004000000470	1s		
192.168.20.221	im7116-2-dm	Core	Openstack	Openstack	im7116-2-dm	Infrastructure Manager	4.1.0.6	7116100000070	1s		
192.168.1.14	W017111	Core	Accedian NetworkDevice	Accedian	AMN-1000-TE	Network Performance Ma...	AMN_6.1.0.3_31762	0315-2136	10s		
192.168.1.14	avito-dm	Core	Avito OS	Avito	DCL-71000-24-8	Switch	4.17.19-10471410-Adm...	PE16-160001	4s		
192.168.20.204	Av-g01	Core	Cisco IOS	Cisco	WS-C3805-24TS	Switch	16.0.1a	WS0007000002	5s		

2. With the device selected, click Inventory > Delete Device.
3. A confirmation message will be displayed. Click Yes.



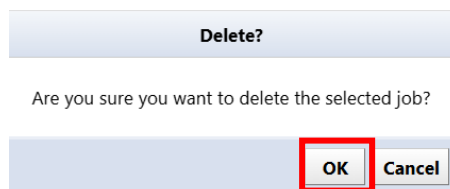
### 5.5.1 Delete job

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



Name	Type
enable password	Tool

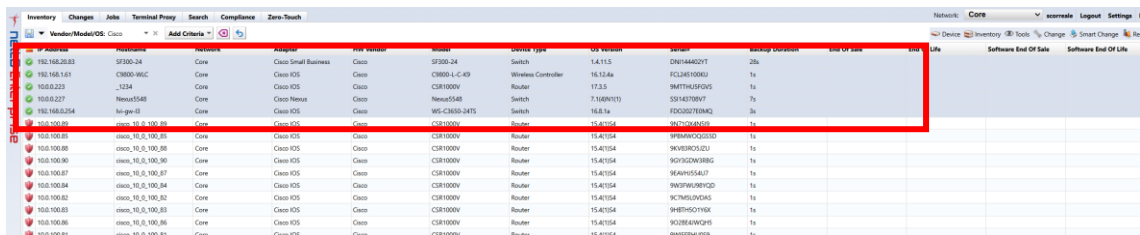
2. Select the job you want to delete and click [Delete].
3. Click Yes on the confirmation screen.



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

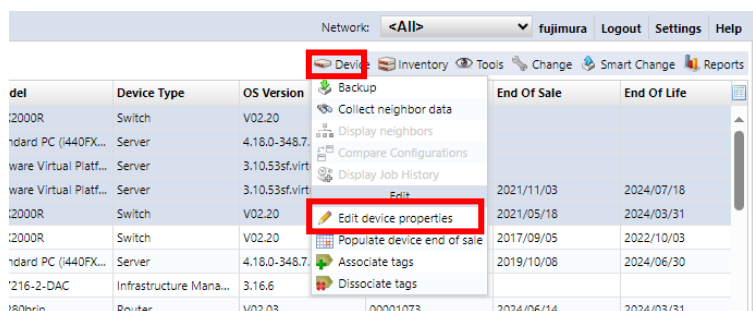
## 6: Advanced Setting

1. Select the device to obtain EOS/EOL.



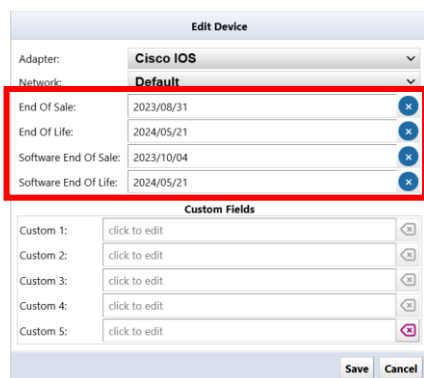
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DN144402YT	28s				
192.168.1.61	C3800-WLC	Core	Cisco IOS	Cisco	C3800-L-C-43	Wireless Controller	16.12.4a	FC1245100KJ	1s				
10.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTH4USGV5	1s				
10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1.60N(1T)	53143708V7	7s				
192.168.0.254	hr-gw-03	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.6.1a	FD0302708M2	3s				
10.0.100.89	cisco_10_0_100_89	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9N7020A0309	1s				
10.0.100.85	cisco_10_0_100_85	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9P8M9Q055SD	1s				
10.0.100.88	cisco_10_0_100_88	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9KVB3R05J2U	1s				
10.0.100.90	cisco_10_0_100_90	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9QY3GDN3R8G	1s				
10.0.100.87	cisco_10_0_100_87	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9EAPV554U7	1s				
10.0.100.84	cisco_10_0_100_84	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9W9P9W4RPFJ29	1s				
10.0.100.82	cisco_10_0_100_82	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9C7M6L6VND45	1s				
10.0.100.83	cisco_10_0_100_83	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9H8TH50Y10K	1s				
10.0.100.86	cisco_10_0_100_86	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9Q3B64WQ2H5	1s				
10.0.100.81	cisco 10 0 100 81	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9W9P9W4RPFJ29	1s				

2. Click Edit Device Properties from the device menu.



del	Device Type	OS Version	End Of Sale	End Of Life
2000R	Switch	V02.20	2021/11/03	2024/07/16
ard PC (i440FX...	Server	4.18.0-348.7	2021/05/18	2024/03/31
ware Virtual Plat...	Server	3.10.53sf.virt	2017/09/05	2022/10/03
ware Virtual Plat...	Server	3.10.53sf.virt	2019/10/08	2024/06/30
2000R	Switch	V02.20	2024/06/14	2024/03/31
2000R	Switch	V02.20		
ard PC (i440FX...	Server	4.18.0-348.7		
216-2-DAC	Infrastructure Mana...	3.1.6		
t80brin	Router	V02.03		

3. Select the product end of life and end of support dates and click Save.



Adapter: Cisco IOS

Network: Default

End Of Sale: 2023/08/31

End Of Life: 2024/05/21

Software End Of Sale: 2023/10/04

Software End Of Life: 2024/05/21

Custom Fields

Custom 1: click to edit

Custom 2: click to edit

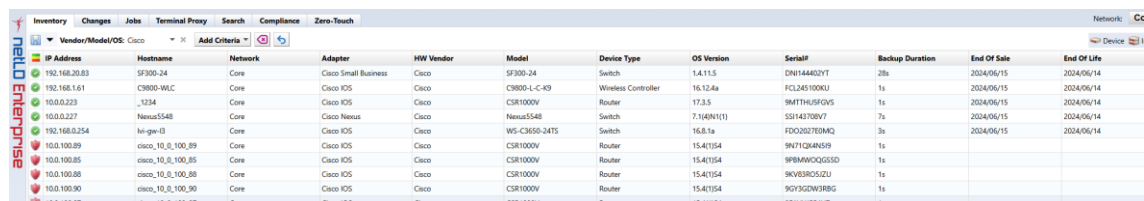
Custom 3: click to edit

Custom 4: click to edit

Custom 5: click to edit

Save Cancel

By following the above steps, the date set in the column will be displayed.



IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DN144402YT	28s	2024/06/15	2024/06/14		
192.168.1.61	C3800-WLC	Core	Cisco IOS	Cisco	C3800-L-C-43	Wireless Controller	16.12.4a	FC1245100KJ	1s	2024/06/15	2024/06/14		
10.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTH4USGV5	1s	2024/06/15	2024/06/14		
10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1.60N(1T)	53143708V7	7s	2024/06/15	2024/06/14		
192.168.0.254	hr-gw-03	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.6.1a	FD0302708M2	3s	2024/06/15	2024/06/14		
10.0.100.89	cisco_10_0_100_89	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9N7020A0309	1s				
10.0.100.88	cisco_10_0_100_88	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9KVB3R05J2U	1s				
10.0.100.90	cisco_10_0_100_90	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9QY3GDN3R8G	1s				
10.0.100.87	cisco 10 0 100 87	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9EAPV554U7	1s				

## 6.1 Automatic configuration

### 6.1.1 Prerequisites

The NetLD you are using must be able to connect to the Internet.

You must log in with your Cisco account and obtain an API key and secret code before accessing Cisco Smart Net Total Care.

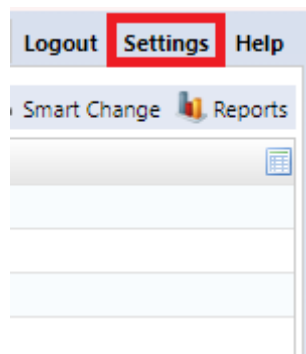
\*Valid Cisco Smart Net Total Care (SNTC) required.

\*Please see below for information on obtaining API.

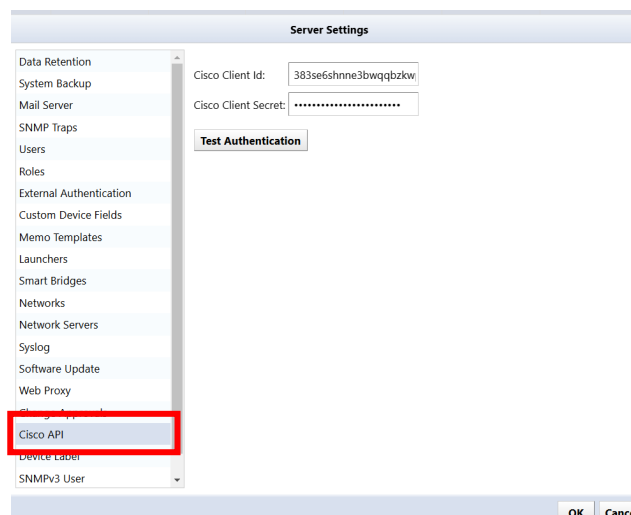
(<https://developer.cisco.com/docs/support-apis/#!user-onboarding-process>)

#### 6.1.1.1 Procedure (online environment)

1. Click Settings.



2. Click on Cisco API.



3. Enter your API key and secret code and click OK.

Server Settings

Data Retention

System Backup

Mail Server

SNMP Traps

Users

Roles

External Authentication

Custom Device Fields

Memo Templates

Launchers

Smart Bridges

Networks

Network Servers

Syslog

Software Update

Web Proxy

Change Approvals

Cisco API

Device Label

SNMPv3 User

Cisco Client Id: 383se6shnne3bwqgbzkw

Cisco Client Secret: .....

Test Authentication

OK Cancel

4. By clicking Test Authentication, you can check whether the ID and Secret code you entered can be used.
5. Select the device to obtain EOS/EOL.

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	SW Vendor	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
10.0.0.40	ASA-9122	Default	Cisco ASA	Cisco	ASA	Firewall	9.12(2)	8AAMCVBWS2H	Cisco				
10.0.0.70	router70	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9YV87DF3BM	Cisco				
10.0.0.101	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	8AUJ089HOKJ	Cisco				
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	5MA112502OL	Cisco	2014/08/15	2021/08/31		
10.0.0.126	R1	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	8E0UJ2VW9E	Cisco				
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	8MP8735EN	Cisco				
10.0.0.153	bbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	8A0HFGQVZF6	Cisco				

6. Click "Populate device end of sale" from the device menu.

Network: Default

fujimura Logout Settings Help

Device Inventory Tools Change Smart Change Reports

Backup

Collect neighbor data

Display neighbors

Compare Configurations

Display Job History

Edit

Edit device properties

Populate device end of sale

Associate tags

Dissociate tags

Device Type	OS Version	End Of Sale	End Of Life
Router	15.4(1)S4		
Firewall	9.12(2)		
Router	15.4(1)S4		
Router	15.4(1)S4		
Router	15.4(2)S		
Router	15.4(1)S4		
Router	17.3.5		
Router	15.4(2)S		
Router	15.4(1)S4	9YV87DF3BM	

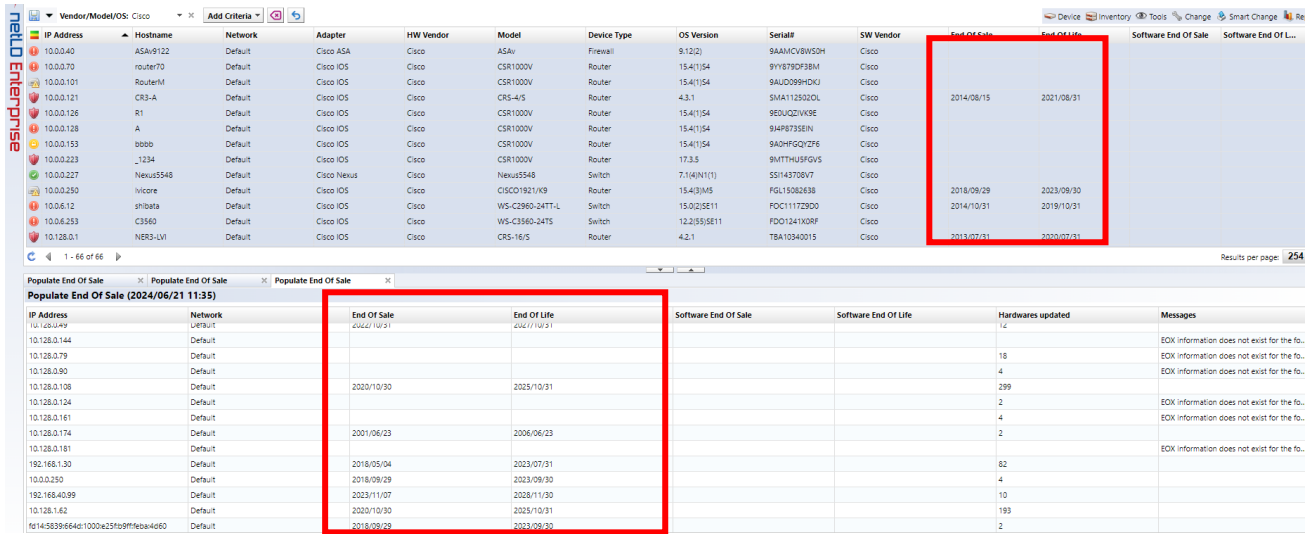
7. Click "Yes" on the screen below.

Populate End of Sales?

Are you sure you want to populate end of sales data for the selected devices?

Yes No

8. Using the above steps, EOS/EOL information will be automatically acquired and registered in the column.



The screenshot shows the NetLD Enterprise interface with a table of network devices. The table has columns for IP Address, Hostname, Network, Adapter, HW Vendor, Model, Device Type, OS Version, Serial#, SW Vendor, End Of Sale, End Of Life, Software End Of Sale, and Software End Of Life. A red box highlights the End Of Sale and End Of Life columns for several devices.

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	SW Vendor	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
10.0.0.40	ASA-9122	Default	Cisco ASA	Cisco	ASA5	Firewall	9.12(2)	SAAMCVBWS0H	Cisco				
10.0.0.70	router70	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9YH870P38M	Cisco				
10.0.0.101	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9AU099HDKJ	Cisco				
10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	Cisco	2014/08/15	2021/08/31		
10.0.0.126	R1	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9EDUQZVVK9E	Cisco				
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	94P8735EN	Cisco				
10.0.0.153	bbob	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFQZ2F6	Cisco				
10.0.0.223	_1234	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHUSFGV5	Cisco				
10.0.0.227	Nexus5548	Default	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SS143708V7	Cisco				
10.0.0.250	hvcare	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15062638	Cisco	2018/09/29	2023/09/30		
10.0.6.12	shibata	Default	Cisco IOS	Cisco	WS-C2960-24TT-L	Switch	15.0(2)SE11	FDC11172300	Cisco	2014/10/31	2019/10/31		
10.0.6.253	C3660	Default	Cisco IOS	Cisco	WS-C3660-24TS	Switch	12.2(55)SE11	FDC1241X0RF	Cisco				
10.128.0.1	NER3-LV1	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	Cisco	2013/07/31	2020/07/31		

Results per page: 254

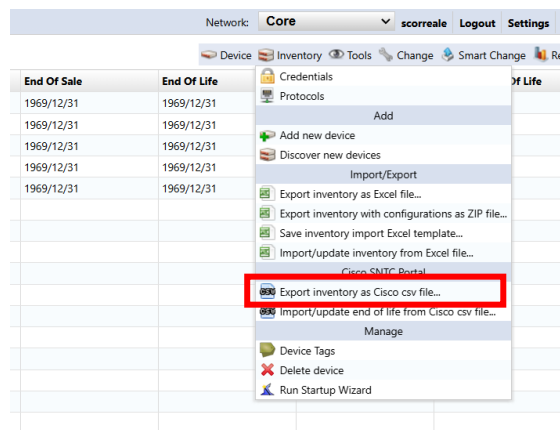
Populate End Of Sale (2024/06/21 11:35)

IP Address	Network	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life	Hardwares updated	Messages
10.128.0.99	Default	2062/10/31	2062/10/31			14	
10.128.0.144	Default					18	EOX information does not exist for the fo...
10.128.0.79	Default					4	EOX information does not exist for the fo...
10.128.0.90	Default					299	EOX information does not exist for the fo...
10.128.0.108	Default	2020/10/30	2025/10/31			2	
10.128.0.124	Default					4	EOX information does not exist for the fo...
10.128.0.161	Default					2	EOX information does not exist for the fo...
10.128.0.174	Default	2001/06/23	2006/06/23			2	
10.128.0.181	Default					62	EOX information does not exist for the fo...
192.168.1.30	Default	2018/05/04	2023/07/31			4	
10.0.0.250	Default	2018/09/29	2023/09/30			10	
192.168.0.99	Default	2023/11/07	2026/11/30			193	
10.128.1.62	Default	2020/10/30	2025/10/31			2	
10.14.5839.6640	Default	2018/09/29	2023/09/30				

### 6.1.1.2 Procedure (offline environment)

If NetLD cannot connect to the Internet, it will not be able to retrieve the end-of-sale date from the Cisco server. However, you can export your inventory as a csv file and use it for import into Cisco services. You can then export the csv file from your Cisco service and import it into NetLD to update the end of support date. Note that Cisco services do not include the end-of-sale date in the export file.

To export a csv file that can be used for import into Cisco services, select “Export Inventory as Cisco csv file” from the inventory menu.



## 6.2 Compliance overview

By setting a compliance policy, you can automatically ensure that unintended settings are set on a device's configuration. For automatic detection, you need to create a compliance rule. A rule is constructed using the following four matching conditions.

- If matched, excluded
- If it doesn't match, it's not applicable
- If matched, violation
- If it doesn't match, it's a violation.

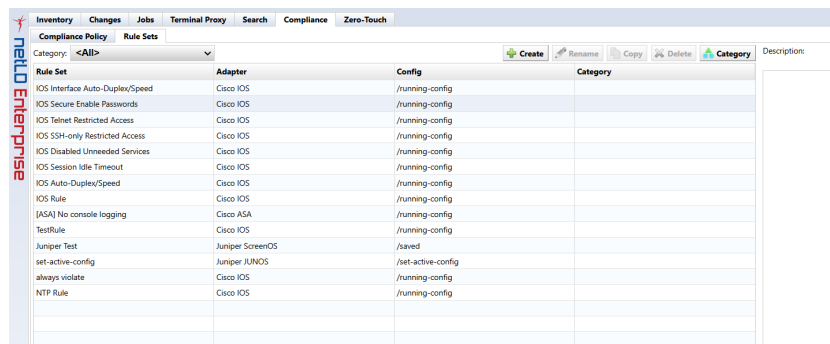
Each condition has a single search string and checks if the given configuration matches that string. A collection of compliance rules is called a ruleset. Rule sets can also be created freely.

In addition, policies are provided to manage compliance on a larger scale. A policy is created by combining multiple rule sets, but it also has information such as the list of devices to which it applies, the severity of violations (errors, warnings, or notifications), and the history of violations.

### 6.2.1 Rule

#### 6.2.1.1 Ruleset tab

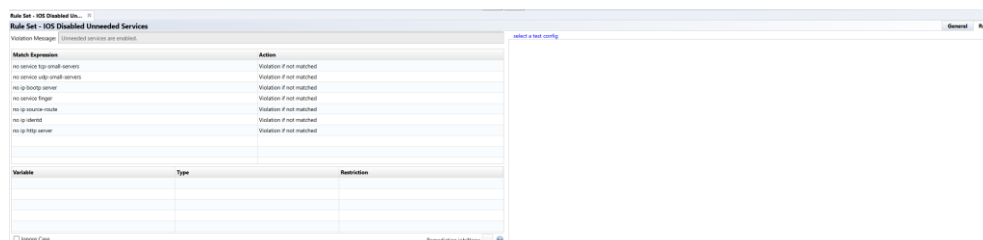
The Rulesets tab manages rulesets.



Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Rule	Cisco IOS	/running-config	
(ASA) No console logging	Cisco ASA	/running-config	
TestRule	Cisco IOS	/running-config	
Juniper Test	Juniper ScreenOS	/saved	
set-active-config	Juniper JUNOS	/set-active-config	
always violate	Cisco IOS	/running-config	
NTP Rule	Cisco IOS	/running-config	

#### Rules subtab

Double-clicking each ruleset in the Rulesets subtab displays its contents in a new tab in the status pane. The new tab has two subtabs, the General subtab and the Rules subtab.



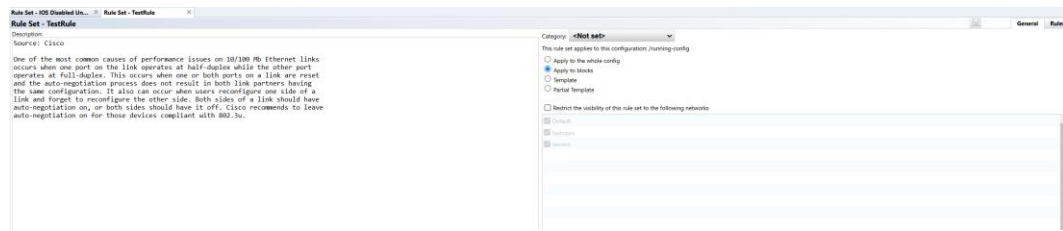
Match Expression	Action
no service tcp-small-servers	Violation if not matched
no service udp-small-servers	Violation if not matched
no ip bootp server	Violation if not matched
no service finger	Violation if not matched
no ip source route	Violation if not matched
no ip ident	Violation if not matched
no ip http server	Violation if not matched

Items	Explanation
Violation message	Enter the message that will be displayed if the rule is violated.
Start end	Specify the range to search for the string specified in the "Match" item. This field appears when Apply to Blocks is selected on the General subtab.
Consistent	Specifies the string to be searched for. You can convert a string into a variable by enclosing it between "~ (tilde)". Example: interface gigabitEthernet ~INT_NUM~
Action	Select matching conditions. <ul style="list-style-type: none"> <li>• If it doesn't match, it's not applicable</li> <li>• If matched, excluded</li> <li>• If it doesn't match, it's a violation.</li> <li>• If matched, violation</li> </ul>
Variable	Displays the value when a variable is used in the string specified in the "Match" item.
Type	Specify four possible types of matches. If it does not match the type, it will be excluded from the search conditions. <ul style="list-style-type: none"> <li>• Text: Matches all text.</li> <li>• IP address: Matches only strings representing IP addresses.</li> <li>• Hostname: Matches hostname.</li> <li>• Word: Matches words.</li> <li>• Regular expression: Search for matching strings using regular expressions.</li> </ul>
Filter	Enter the string or value to search for. If * is entered, it means "any value is fine"

### General subtab

The General subtab is a tab where you can set the rule description and scope of application. Writing explanations for rules is important for later maintenance. Consider what happens when your current administrator leaves your company. In order to properly manage compliance, successors must understand the written rules, but it is generally extremely difficult to infer the purpose of a rule just from its definition. That's it. In order to maintain stable maintenance no matter what happens, we add at least a minimum amount of explanation to the rules, and if possible, add an easy-to-understand explanation.

In addition to adding a description of the currently selected rule, you can also configure the rule itself.

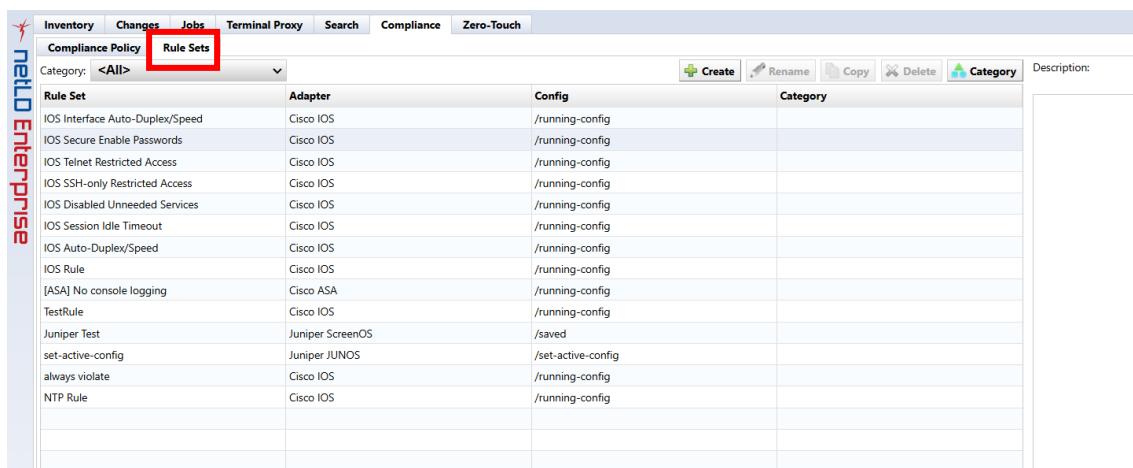


Items	Explanation
Category	
Description	Enter a description for the rule.
Applies to the whole config	Applies the rule to the entire configuration.
Apply to block	Divide the configuration into blocks and apply rules to each blog.
Template	The configuration is compared line by line from the template, and if there is a difference, it will be a violation.
Partial Template	
Restrict the visibility of this rule set to the following networks	Enabling the check limits the networks to which the rule applies.

### 6.2.1.2 Creating a new rule

Here, we will explain how to create a new rule with screenshots. As an example, let's generate a violation when the SNMP community setting is "public" in the Cisco IOS device configuration.

1. Click the button on the Compliance → Rulesets tab.





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

**Rule Set**

Name:

Adapter: Cisco IOS

Configuration: /running-config

Category: <Not set>

- In the Violation Message field, enter the message that will be displayed when a violation is detected. In this example, the message is "SNMP community set to 'public'" when finished, click the button.

**Rule Set - SNMP - Public**

Violation Message:

Match Expression:

Action: Violation if not matched

Variable	Type	Restriction
mode	text	

☐ Ignore Case Remediation job: None

- In Match, enter the text that is a violation, and in Action select ``Violate if matched."

**Rule Set - SNMP - Public**

Violation Message:

Match Expression:

Action: Violation on match

Variable	Type	Restriction
mode	text	

☐ Ignore Case Remediation job: None

- If you want to test the rule you created, click Select a configuration to test and select a configuration from your inventory.

**Rule Set - SNMP - Public**

Violation Message:

Match Expression:

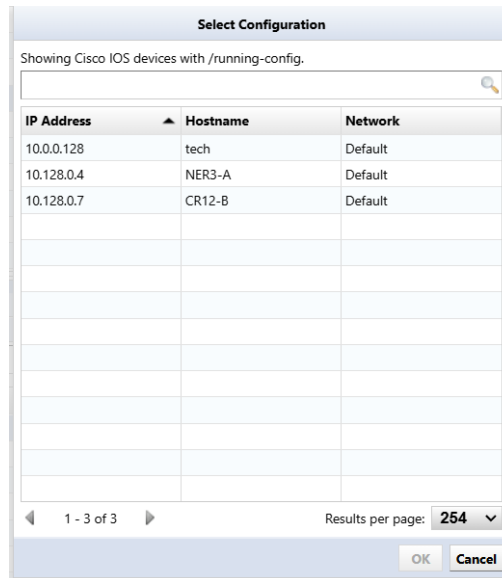
Action: Violation on match

Variable	Type	Restriction
mode	text	

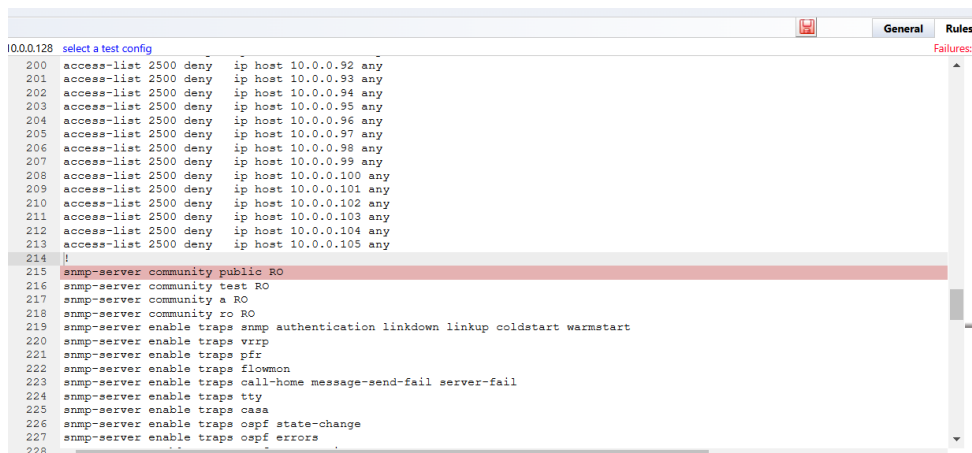
☐ Ignore Case Remediation job: None

- The configuration selection window displays a list of devices that apply to the adapter you selected when creating the rule.

This column only displays devices that match the IOS adapter you originally selected.



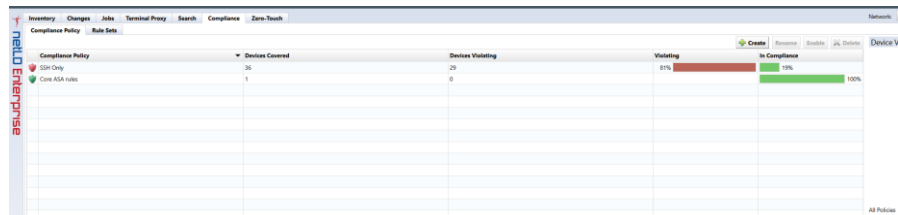
Violations will be searched for against this text rule, and if violations are found, they will be displayed in red. Once you're done, let's create a policy from this ruleset in the next chapter.



## 6.2.2 Compliance policy

### 6.2.2.1 Compliance policy tab

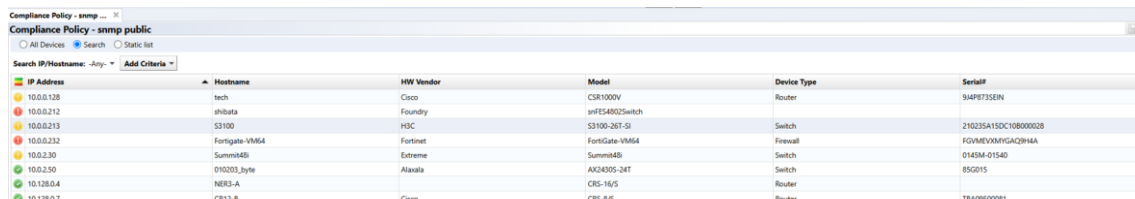
The Compliance Policy tab consists of the following subtabs:



Compliance Policy	Devices Covered	Devices Violating	Violating	In Compliance
Core ASA rules	35	29	81%	100%

#### Device subtab

This tab selects which devices the policy applies to. The input interface is the same as that of job management. Select devices using three methods: static list, search, and all devices, using tab switching techniques accordingly.



IP Address	Hostname	HW Vendor	Model	Device Type	SerialID
10.0.0.128	tech	Cisco	CSR1000V	Router	9IAP8735EN
10.0.0.212	shibata	Foundry	snFES4802Switch		
10.0.0.213	S3100	H3C	S3100-26T-SI	Switch	210235A15DC10B00002B
10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGVM64VM64GAC2P44A
10.0.2.30	Summit480	Extreme	Summit480	Switch	014304-01540
10.0.2.50	010203_byte	Alcatel	AX3400S-34T	Switch	850015
10.128.0.4	NER3-A		CRS-16/S	Router	
10.128.0.7	CR12-8	Cisco	CRS-4/S	Router	TBA09500001

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

Ruleset subtab

On this tab, register the created rule set to the policy.

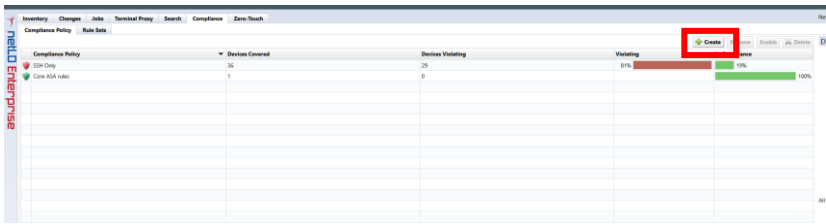


Items	Explanation
adapter	Displaying adapters to which the policy applies.
configuration	Displaying the configuration to which the policy is applied.
ruleset	A rule added to a policy.
Severity	You can select the failure level from error or warning. The icon displayed when a policy is violated is different.

6.2.2.2 Creating a new policy

Let's create a policy for Cisco IOS device configuration using the rule set we created earlier.

- Click the create button on the Compliance → Compliance Policy tab.



- Enter the policy name, target adapter, and configuration type, and click OK.

Compliance Policy

Name:

SNMP public

Adapter:

Cisco IOS

Configuration:

/running-config

OK

Cancel

- On the **Devices** subtab, select **Search** in this example.

Compliance Policy - SNMP public

☐ All Devices
 ☒ Search
 ☐ Static list

Search IP/Hostname:

IP Address	Hostname	HW Vendor	Model	Device Type	Serial#
10.0.0.128	tech	Cisco	CSR1000V	Router	914P8735EN
10.0.0.212	shibata	Foundry	snFE54802Switch		
10.0.0.213	SI100	H3C	S13100-26T-S	Switch	210235A15DC10B000028
10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGAM94XMPGACZPH4A
10.0.2.30	Summit08	Extreme	Summit08	Switch	0143M-0154G
10.0.2.50	010203_byte	Alcatel	AX24305-24T	Switch	85G015
10.128.0.4	NER3-A		CRS-16/S	Router	
10.128.0.7	KR12-8	Cisco	CRS-8/S	Router	TBA090500081

The setting behavior at search and static list at device sub tab is same as the behavior of Job Management.

Devices will be searched every time violation check is activated when using search rule and violation check will be performed toward these devices. Please note search result is not saved when creating policy.

- Click the button on the Ruleset subtab of the status pane.

[illegible]

5. Select a ruleset and click Add button. In this example, we selected the SNMP community 'public' & IOS Secure Enable Password rule.

Add Rule Sets

Category

<All>

IOS Interface Auto-Duplex/Speed

IOS Secure Enable Passwords

IOS Telnet Restricted Access

IOS SSH-only Restricted Access

IOS Disabled Unneeded Services

IOS Session Idle Timeout

IOS Auto-Duplex/Speed

IOS Rule

test11

TestRule

always violate

cisco test

SNMP - Public

Add

Cancel

6. The rules that appear in this window are whose adapter type matches the adapter type of the current policy associated to. If no rules are displayed, please review the policy or the adapter type of the rule. Select Action for the rule. Different action can be set per rule set.

**Rule Set - SNMP - Public**

Violation Message: SNMP community set to public

**Match Expression**

snmp-server community public ~mode~

**Action**

- Violation if not matched
- Stop if not matched
- Stop on match
- Violation if not matched
- Violation on match

Variable	Type	Restriction
mode	text	

Save it. After saving, let's activate the policy. Simply creating a policy does not check for violations.

**Rule Set - SNMP - Public**

Violation Message: SNMP community set to public

**Match Expression**

snmp-server community public ~mode~

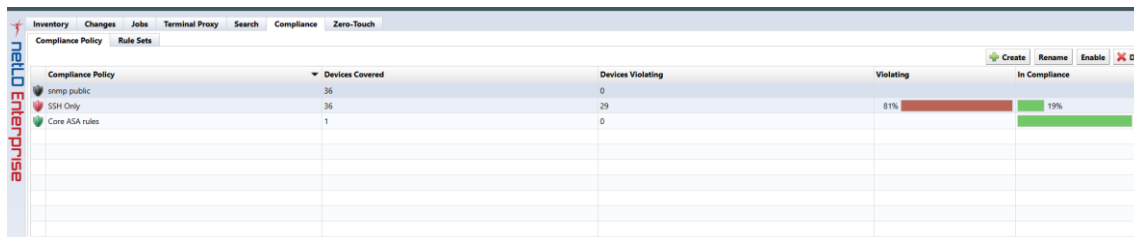
**Action**

Violation if not matched

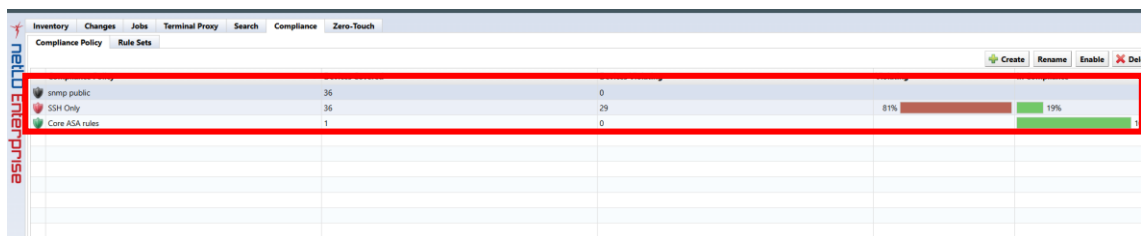
**General** | Rule

### 6.2.2.3 Applying the created policy

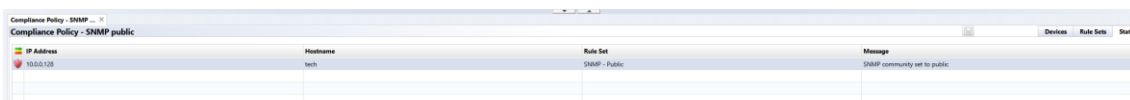
After you create a policy, you need to enable it. Make sure the subtab is open at Compliance → Compliance Policy. Click Enable button with policy selected. A pie chart is displayed, it allows you to check the violation status.



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



Double-click the changed icon. A subtab opens in the status pane. This subtab contains details of the violation.



The violation icon also appears in the device view. Double-click the icon to learn more about the violation.

### 6.2.3 Automatic remediation function

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

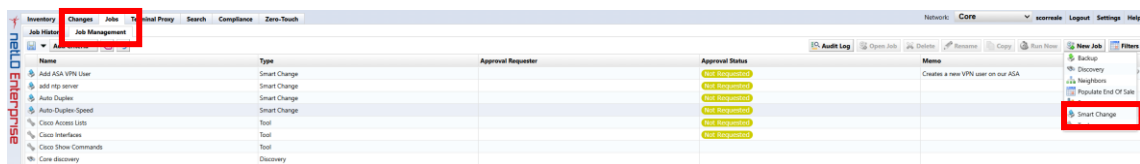
[Setting flow]

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

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

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

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



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

Create Smart Change Job

Job Name:  
snmp public

Network:  
Default.laptoppc.servers

Comment:

☒ Use remediation job.

Adapter: Cisco IOS

☒ Use the same replacement values for all devices in the job.  
☐ Use unique replacement values for each device in the job.

OK

Cancel

3. Check "Use remediation job", select the device adapter, and click OK.

\*Used for linking with rule sets.





**Create Smart Change Job**

Job Name:

Network:

Comment:

☒ Use remediation job.

Adapter:

☒ Use the same replacement values for all devices in the job.  
☐ Use unique replacement values for each device in the job.

- Enter the command you want the template to run.

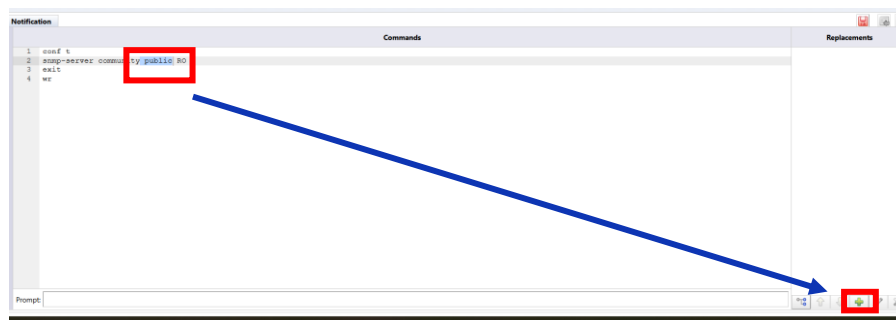


Template editor window showing the Commands tab. The Commands list is empty, and the Command input field is highlighted with a red box.

- Select the part you want to convert into a variable and click +.

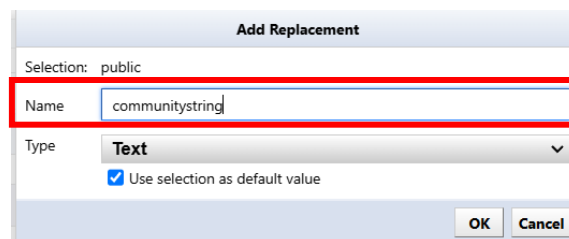
\*Skip this step if you want to execute the command as is without converting it to a variable.

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



Template editor window showing the conversion of 'public' to a variable. The command 'conf t' is selected, and the 'public' part is highlighted with a red box. A blue arrow points from the highlighted text to the '+' button in the bottom right corner of the Commands list.

- Enter the variable name and click OK.



**Add Replacement**

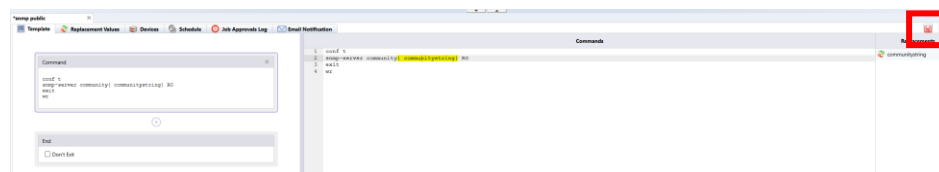
Selection: public

Name:

Type:

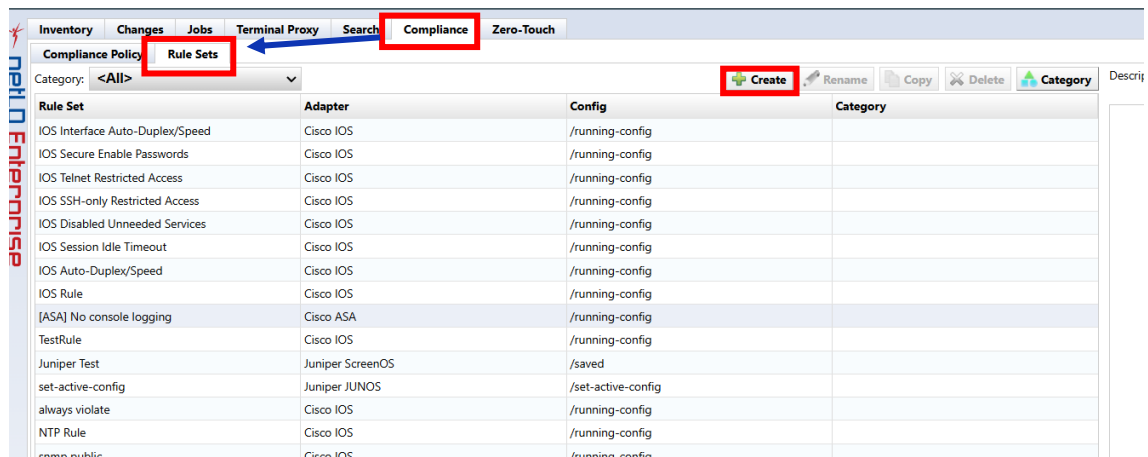
☒ Use selection as default value

- Save it.



Template editor window showing the final command. The command 'conf t' is selected, and the 'communitystring' part is highlighted with a red box. The '+' button in the bottom right corner of the Commands list is also highlighted with a red box.

8. Go to Compliance -> Rule Sets and click Create.

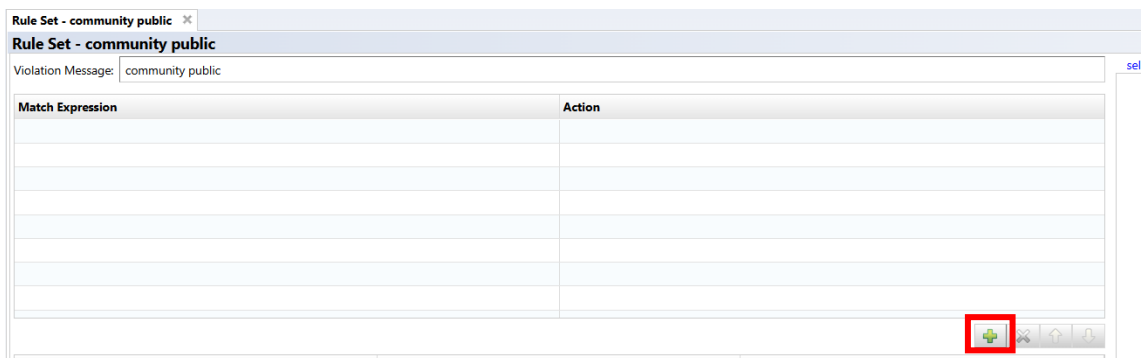


9. Enter the rule name, select the adapter, and click OK.

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

The 'Rule Set' dialog box is shown. The 'Name' field contains 'community public'. The 'Adapter' dropdown is set to 'Cisco IOS'. The 'Configuration' dropdown is set to '/running-config'. The 'Category' dropdown is set to '<Not set>'. The 'OK' button is highlighted.

10. Click + to add matching conditions.



11. Specify the community name part as the smart change variable name and surround the variables name with "~".

Rule Set - community public

Violation Message: invalid community string

Match Expression: snmp-server community ~communitystring~ RW

Action: Violation if not matched

Variable: communitystring, Type: text, Restriction:

12. Set the Action to "Violation if not matched."

Rule Set - community public

Violation Message: invalid community string

Match Expression: snmp-server community ~communitystring~ RW

Action: Violation if not matched

Variable: communitystring, Type: text, Restriction:

13. Click "..."/>next to the repair job and specify the smart change job to be executed in the event of a violation.

**\*Only one job can be specified.**

Rule Set - community public

Violation Message: invalid community string

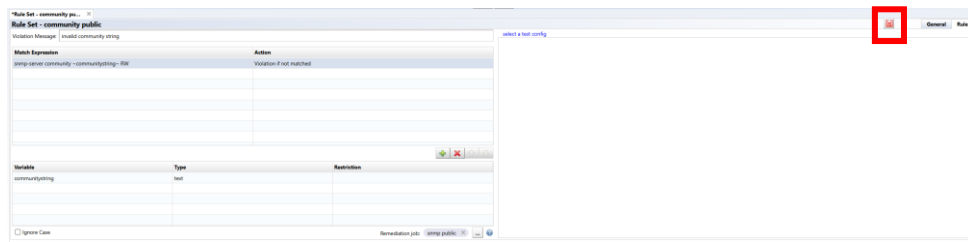
Match Expression: snmp-server community ~communitystring~ RW

Action: Violation if not matched

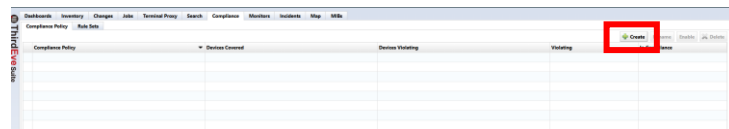
Remediation job: snmp public

Variable: communitystring, Type: text, Restriction:

14. Save your settings.



15. Go to Compliance -> Compliance Policy and click Create.



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

**Compliance Policy**

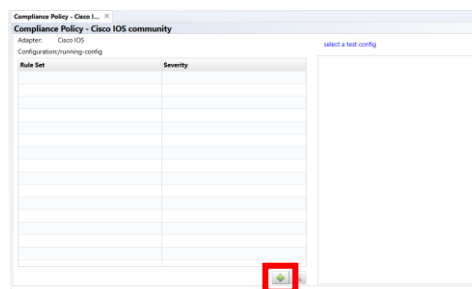
Name:  
Cisco IOS community

Adapter:  
Cisco IOS

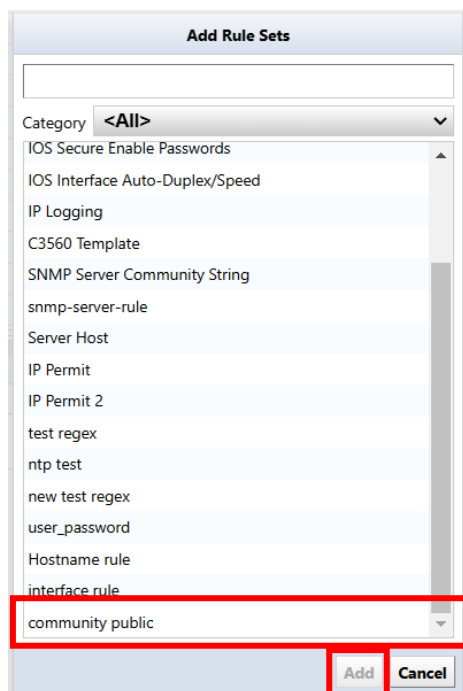
Configuration:  
/running-config

OK Cancel

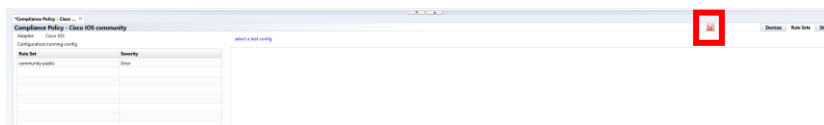
17. Click +.



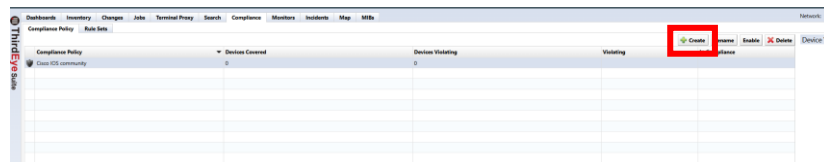
18. Select Ruleset and click Add.



19. Click Save.

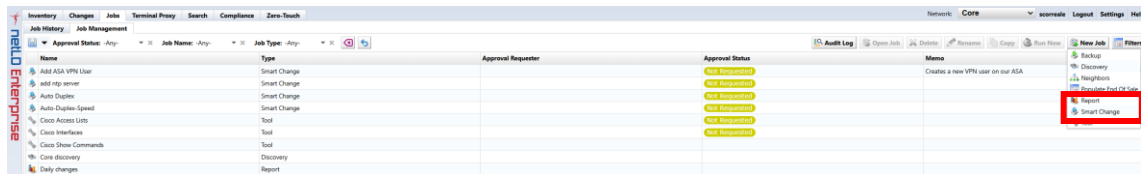


20. Select the compliance policy you created and click Enable.



### 6.2.3.2 Case 2: No access list added to the interface

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



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

A screenshot of the 'Create Smart Change Job' dialog box. The 'Job Name' field contains the text 'access list'. The 'Network' dropdown menu is set to 'Default'. The 'Comment' field is empty. Below the fields, there are three radio buttons: 'Use remediation job.' (which is selected), 'Use the same replacement values for all devices in the job.', and 'Use unique replacement values for each device in the job.'. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Check "Use remediation jobs", select the device adapter, and click OK.

\*Used for linking with rule sets.

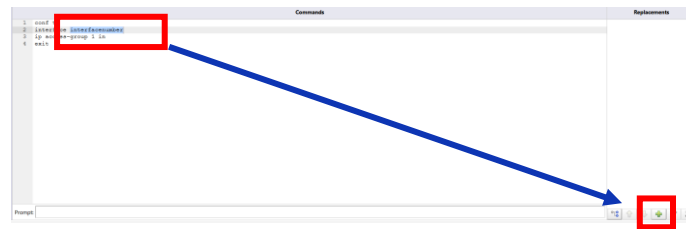
A screenshot of the 'Create Smart Change Job' dialog box, similar to the previous one. The 'Job Name' field contains 'access list'. The 'Network' dropdown is set to 'Default'. The 'Comment' field is empty. The 'Use remediation job.' radio button is selected. The 'Adapter' dropdown menu is set to 'Cisco IOS'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

A screenshot of the 'Template Set' dialog box. The 'Command' field contains the text 'conf t\ninterface ethernet/ethernet\nip address-group 1 10\nno\n'. The 'OK' and 'Cancel' buttons are at the bottom right.

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

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



6. Enter the variable name and click OK.

**Add Replacement**

Selection: interfacenumber

Name:

Type: **Text** ▼

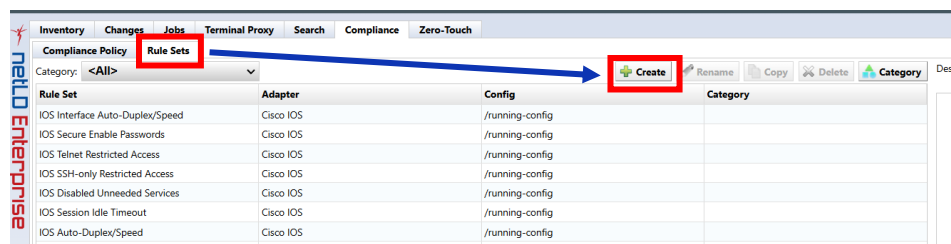
☒ Use selection as default value

OK Cancel

7. Save it.



8. Go to Compliance -> Rulesets and click Create.



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

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

**Rule Set**

Name:  
ACL interface

Adapter:  
**Cisco IOS**

Configuration:  
/running-config

Category  
<Not set>

OK Cancel

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

Rule Set - ACL interface

Rule Set - ACL interface

Violation Message: ACL interface

Start: interface interface-num

Match Expression

Action

Apply to the entire policy

Apply to blocks

Apply to interfaces

Apply to templates

Apply to the validity of the rule set for the following interfaces

OK Cancel

11. Specify the block to which the rule applies using "Start/End".

Rule Set - ACL interface

Rule Set - ACL interface

Violation Message: ACL interface

Start: interface interface-num

Match Expression

Action

Apply to the entire policy

Apply to blocks

Apply to interfaces

Apply to templates

Apply to the validity of the rule set for the following interfaces

OK Cancel

12. Specify the interface number part as the smart change variable name and surround the variable name by "~".

Rule Set - ACL interface

Rule Set - ACL interface

Violation Message: ACL interface

Start: interface interface-num

Match Expression

Action

Apply to the entire policy

Apply to blocks

Apply to interfaces

Apply to templates

Apply to the validity of the rule set for the following interfaces

OK Cancel

13. Double-click the added variable and add a text filter.

\*This time, we are targeting the GigabitEthernet interface, so specify "GigabitEthernet\*".

Rule Set - ACL interface

Rule Set - ACL interface

Violation Message: ACL interface

Start: interface interface-num

Match Expression

Action

Apply to the entire policy

Apply to blocks

Apply to interfaces

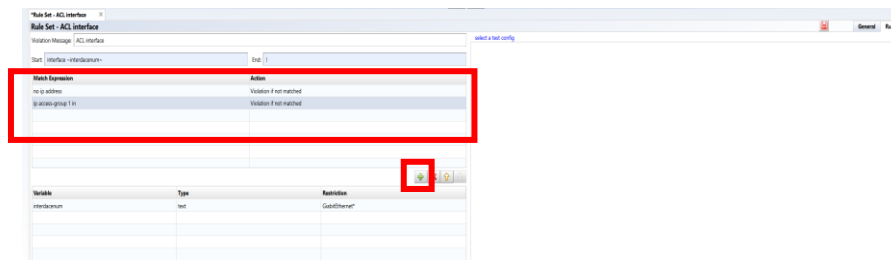
Apply to templates

Apply to the validity of the rule set for the following interfaces

OK Cancel

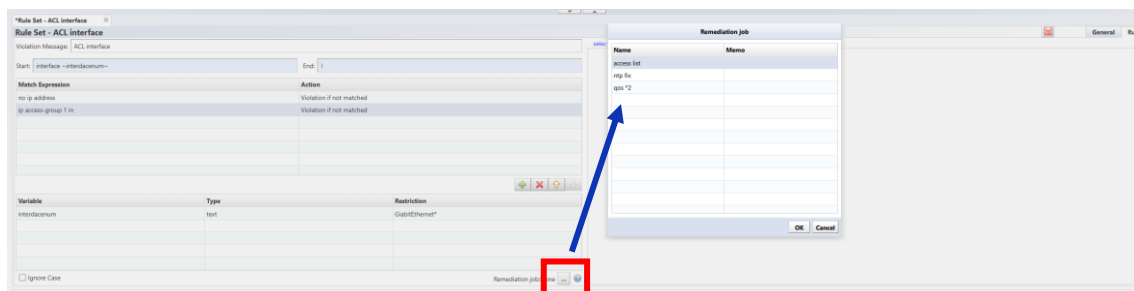


14. Click + to add matching conditions.

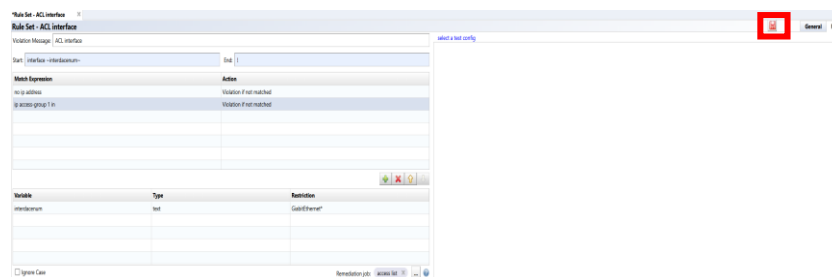


15. Click “...” next to the remediation job and specify the smart change job to be executed in the event of a violation.

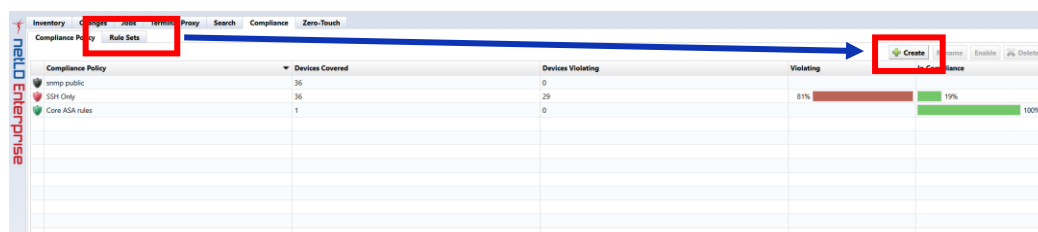
*\*Only one job can be specified.*



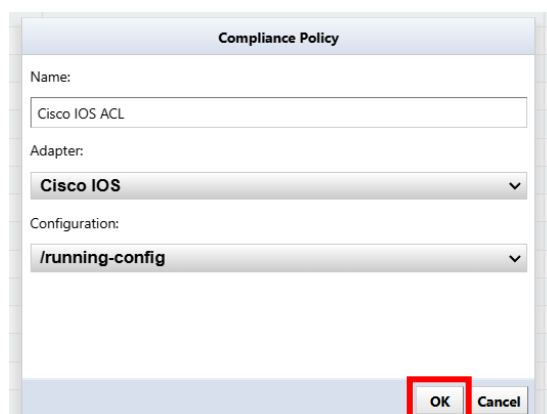
16. Save your settings.



17. Go to Compliance -> Compliance Policy and click Create.



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



Compliance Policy

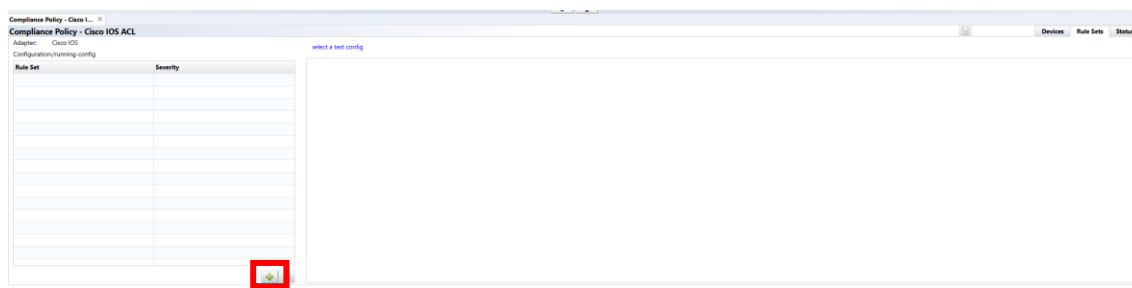
Name:  
Cisco IOS ACL

Adapter:  
Cisco IOS

Configuration:  
/running-config

OK Cancel

19. Click +.



Compliance Policy - Cisco IOS ACL

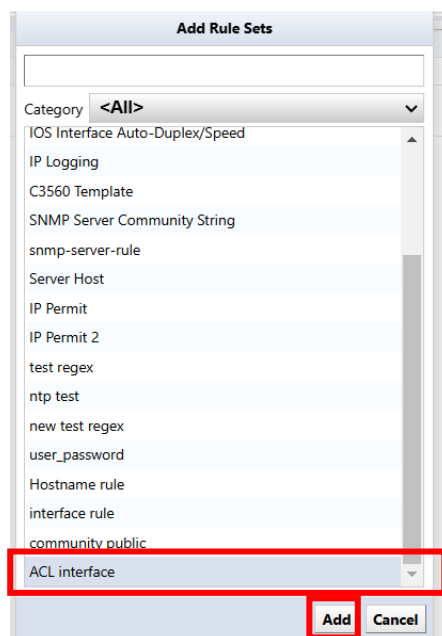
Adapter: Cisco IOS  
Configuration: running-config

Rule Set	Severity
----------	----------

select a test config

+

20. Add a ruleset.



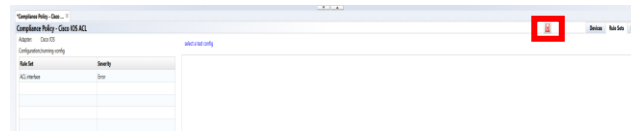
Add Rule Sets

Category: <All>

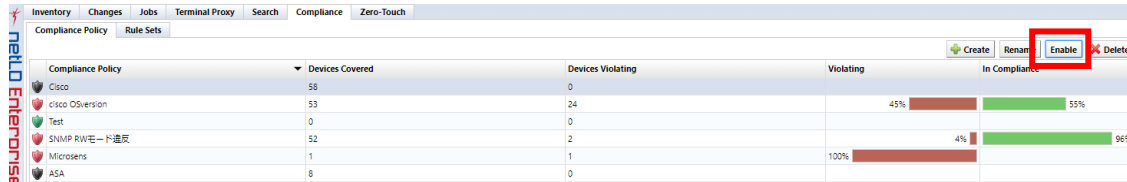
- IOS Interface Auto-Duplex/Speed
- IP Logging
- C3560 Template
- SNMP Server Community String
- snmp-server-rule
- Server Host
- IP Permit
- IP Permit 2
- test regex
- ntp test
- new test regex
- user\_password
- Hostname rule
- interface rule
- community public
- ACL interface

Add Cancel

21. Click Save.



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




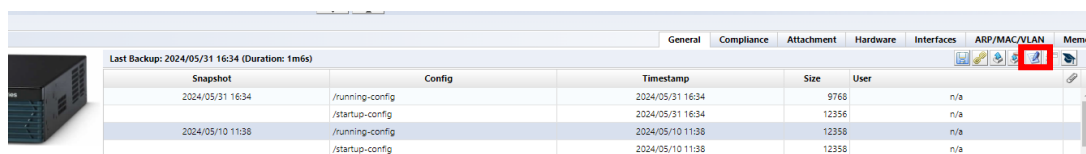
## 6.3 Draft configuration

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

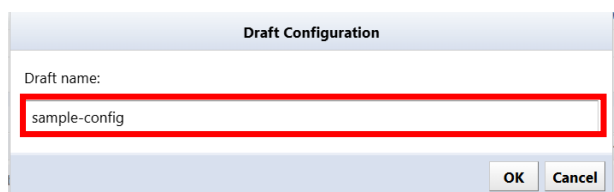
### 6.3.1 Creating a draft configuration

Draft configurations can be created by copying from an existing configuration history.













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



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



4. Double-click the created draft configuration.

					General	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
Last Backup: 2024/05/31 16:34 (Duration: 1m6s)											
Snapshot		Config	Timestamp		Size	User		    			
2024/05/31 16:34	/running-config		2024/05/31 16:34	9768	n/a						
	/startup-config		2024/05/31 16:34	12356	n/a						
2024/05/10 11:38	/running-config		2024/05/10 11:38	12358	n/a						
	/startup-config		2024/05/10 11:38	12358	n/a						
2024/04/25 12:48	/running-config		2024/04/25 12:48	12358	n/a						
	/startup-config		2024/04/25 12:48	12358	n/a						
▼ Draft Configurations											
Draft	Last Edit		Size	User		    					
sample-config	2024/06/21 13:21		12358	shibata							

5. Edit the configuration and click the save button.

tech - 10.0.0.124

sample-config@10.0.0.124

sample-config

1 version 15.4

2 service timestamps debug datetime msec

3 service timestamps log datetime msec

4 no platform punt-keepalive disable-kernel-core

5 platform console virtual

6 !

7 hostname **tester**

8 !

9 boot-start-marker

10 boot-end-marker

11 !

12 !

13 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8gR2MEaE1

14 enable password lvi

15 !

16 no aaa new-model

17 !

18 !

tech - 10.0.0.124

sample-config@10.0.0.124

sample-config

1 version 15.4

2 service timestamps debug datetime msec

3 service timestamps log datetime msec

4 no platform punt-keepalive disable-kernel-core

5 platform console virtual

6 !

7 hostname **homesite**

8 !

9 boot-start-marker

10 boot-end-marker

11 !

12 !

13 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8gR2MEaE1

14 enable password lvi

15 !

16 no aaa new-model

17 !

18 !

tech - 10.0.0.124

sample-config@10.0.0.124

sample-config

1 version 15.4

2 service timestamps debug datetime msec

3 service timestamps log datetime msec

4 no platform punt-keepalive disable-kernel-core

5 platform console virtual

6 !

7 hostname homesite

8 !


9 boot-start-marker

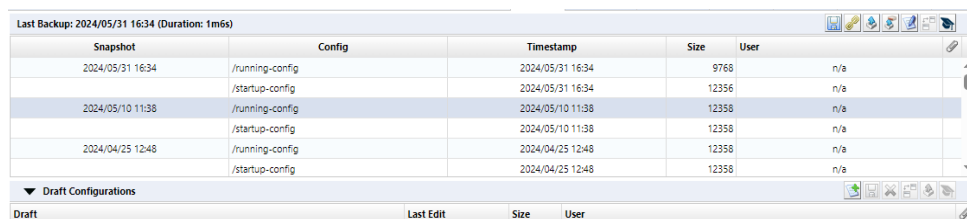
10 boot-end-marker

11 !

## 6.3.2 Import draft configuration from plain text

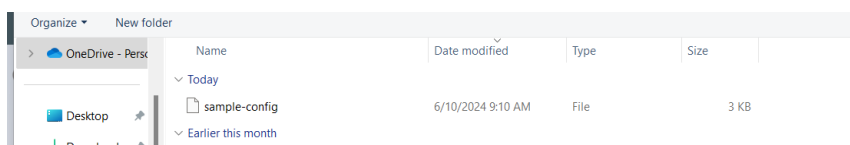
You can create a draft configuration by importing a configuration edited with a text editor, etc. First, double-click the target device in the device view to display the configuration history.

1. In the status pane click the  button.

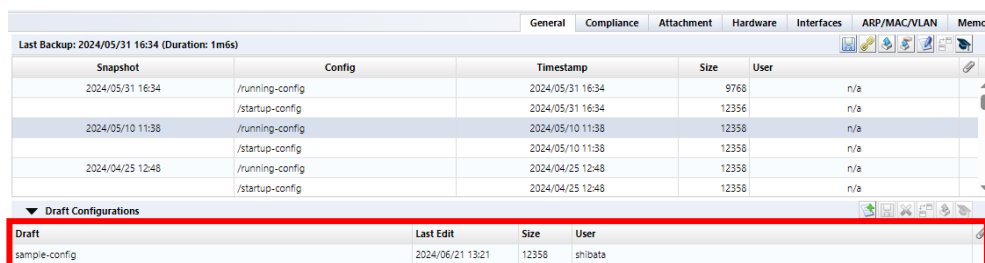


Last Backup: 2024/05/31 16:34 (Duration: 1m6s)				
Snapshot	Config	Timestamp	Size	User
2024/05/31 16:34	/running-config	2024/05/31 16:34	9766	n/a
	/startup-config	2024/05/31 16:34	12356	n/a
2024/05/10 11:38	/running-config	2024/05/10 11:38	12358	n/a
	/startup-config	2024/05/10 11:38	12358	n/a
2024/04/25 12:48	/running-config	2024/04/25 12:48	12358	n/a
	/startup-config	2024/04/25 12:48	12358	n/a
▼ Draft Configurations				
Draft	Last Edit	Size	User	

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




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




Last Backup: 2024/05/31 16:34 (Duration: 1m6s)				
Snapshot	Config	Timestamp	Size	User
2024/05/31 16:34	/running-config	2024/05/31 16:34	9766	n/a
	/startup-config	2024/05/31 16:34	12356	n/a
2024/05/10 11:38	/running-config	2024/05/10 11:38	12358	n/a
	/startup-config	2024/05/10 11:38	12358	n/a
2024/04/25 12:48	/running-config	2024/04/25 12:48	12358	n/a
	/startup-config	2024/04/25 12:48	12358	n/a
▼ Draft Configurations				
Draft	Last Edit	Size	User	
sample-config	2024/06/21 13:21	12358	shibata	


## 6.3.3 Export the draft















To export, click the  button.

## 6.3.4 Delete draft

To delete, click the  button.


### 6.3.5 Comparison of drafts

To compare configurations  click the button. You can use the same comparison functions in draft configurations as in regular configurations.

					General	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
Last Backup: 2024/05/31 16:34 (Duration: 1m6s)											
Snapshot		Config	Timestamp		Size	User		     			
2024/05/31 16:34	/running-config		2024/05/31 16:34	9768	n/a						
	/startup-config		2024/05/31 16:34	12358	n/a						
2024/05/10 11:38	/running-config		2024/05/10 11:38	12358	n/a						
	/startup-config		2024/05/10 11:38	12358	n/a						
2024/04/25 12:48	/running-config		2024/04/25 12:48	12358	n/a						
	/startup-config		2024/04/25 12:48	12358	n/a						
▼ Draft Configurations											
Draft			Last Edit	Size	User		    				
sample-config			2024/06/21 13:21	12358	shibata						

### 6.3.6 Apply draft configuration to devices

Similar to comparing drafts, applying drafts can be done using the same procedure as applying (restoring) backup configurations. However, there is one difference.

Select the draft configuration to upload, click the  button.

▼ Draft Configurations					
Draft	Last Edit	Size	User		
sample-config	2024/06/21 09:12	2093	scoreale		

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

**Push Draft**


Target Configuration: /running-config ▼

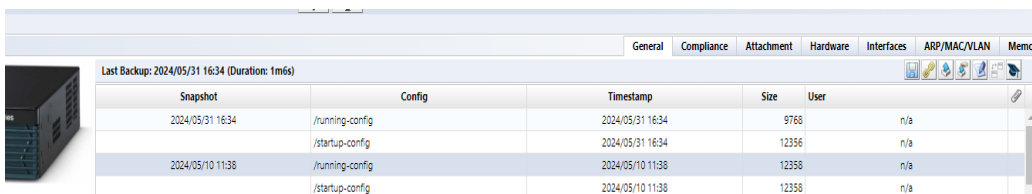
OK Cancel

Click OK to start uploading.

## 6.4 Change Advisor

Change Advisor is a function that reads the current configuration and the specified configuration and outputs the configuration change commands necessary to change the former to the latter. (This feature is not available on some devices.)

1. Double-click the device in the device view.
2. Select a configuration from configuration history or draft.
3. Click the  button.



The screenshot shows the Change Advisor interface with a table of configuration snapshots. The table has columns for Snapshot, Config, Timestamp, Size, and User. The data is as follows:

Snapshot	Config	Timestamp	Size	User
2024/05/31 16:34	/running-config	2024/05/31 16:34	9768	n/a
	/startup-config	2024/05/31 16:34	12356	n/a
2024/05/10 11:38	/running-config	2024/05/10 11:38	12358	n/a
	/startup-config	2024/05/10 11:38	12358	n/a

4. Change Advisor starts and presents commands in the lower pane.



The screenshot shows the Change Advisor interface with two panes displaying configuration differences. The left pane is titled "Current: /running-config (2024/06/03 23:04)" and the right pane is titled "/running-config (2024/06/01 23:03)". The configurations are compared line by line, with line numbers 1 through 27 shown on the left of each pane. The configurations are identical in the visible lines. Below the panes, a section titled "Recommended commands:" lists the following commands:

```
configure terminal
no hostname tech
hostname shibata
exit
```



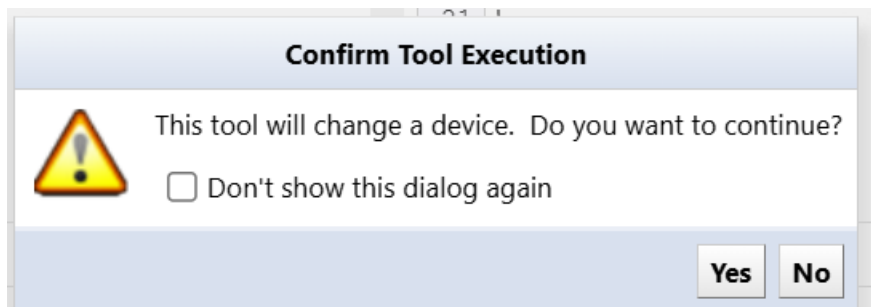
### 6.4.1 Execute commands using Change Advisor

Commands output by Change Advisor can be executed on the device. Please double check the command you want to run before executing the suggested command. If there is an inappropriate command, you can directly edit the output command.

Recommended commands:

```
configure terminal
no hostname tech
hostname shibata
exit
```

Then click Run, click Yes to proceed.




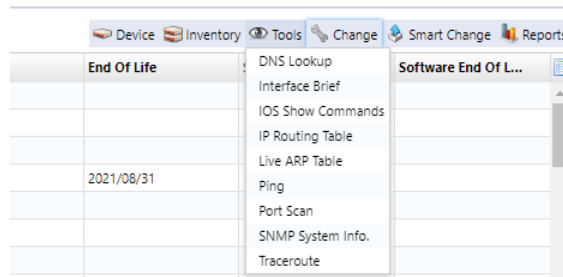
After executing the command, you can check the result. Change Advisor execution results and history are also displayed in the job history.

tech - 10.0.0.124			
Change Advisor			
Change Advisor (2024/06/10 09:20)			
Hostname	IP Address	Network	Duration (seconds)
✓ tech	10.0.0.124	Default	1
configure terminal			
Enter configuration commands, one per line. End with CTRL/Z.			
shibata(config)#no hostname tech			
Router(config)#hostname shibata			
shibata(config)#			

For configuration restore and draft configuration upload, the primary communication protocol is TFTP. Therefore, restore and upload functionality is not available on devices that do not implement TFTP. On the other hand, the change advisor function can be used as long as CLI login (telnet/SSH) is supported. CLI login is supported by most models, so even in environments where uploading is not possible, you can use the change advisor function as a substitute.

## 6.5 Viewing tools

The functions available from the viewing tools menu allow you to know the real-time status of the selected device. It is also possible to export all detected results as CSV. When using the viewing tool, a dedicated tab will be opened in the status pane, so exporting can be done using the  button that is always located in the top right corner.



### 6.5.1 DNS lookup

Display the device's DNS name resolution information.

DNS Lookup (2024/06/10 09:24)			
Hostname	IP Address	Network	Resolved Name
✓ 3sys-nttra-hl.ccs.jp	10.0.40.45	Default	3sys-nttra-hl.ccs.jp

### 6.5.2 IOS Show commands

Display the results of the device's IOS Show command. However, this command can only be run on devices that are compatible with Cisco IOS. Select the show command you want to run first from the list, click Execute to issue the command to the selected device using the IOS Show command.

IOS Show Commands

☐ show access-lists

☐ show arp

☐ show cdp

☐ show flash:

☐ show interfaces

☐ show spanning-tree

☐ show version

☐ show ip arp

☐ show ip bgp

☐ show ip eigrp neighbors

☐ show ip ospf

☐ show ip route

☐ show ip vrf

Execute

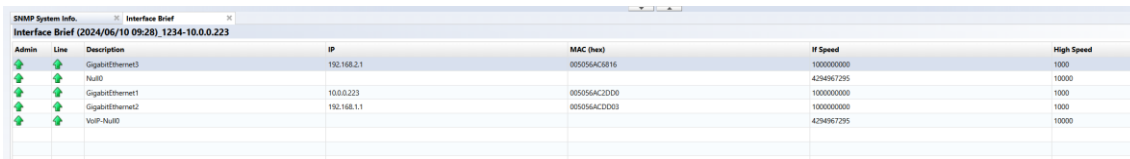
Cancel

show arp screen showing the results of executing the command will be displayed.



## 6.5.6 Interface overview

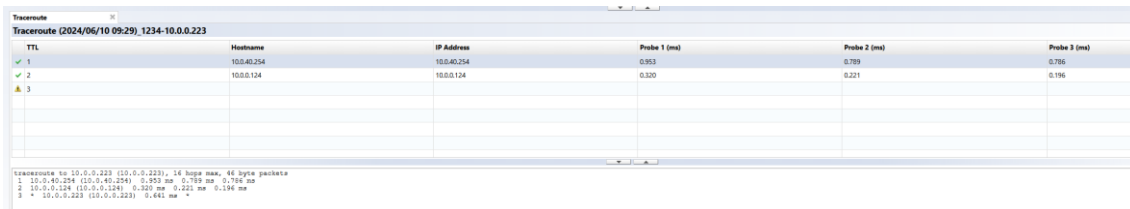
Display detailed information such as open/close status of each interface of the device, IP address, etc. Please note that this function cannot be executed when multiple devices are selected.



Admin	Line	Description	IP	MAC (hex)	IF Speed	High Speed
		GigabitEthernet3	192.168.2.1	95056ACB16	1000000000	1000
		NuID			4294967295	10000
		GigabitEthernet1	10.0.0.223	95056ACDD0	1000000000	1000
		GigabitEthernet2	192.168.1.1	95056ACDD3	1000000000	1000
		VoIP-NuID			4294967295	10000

## 6.5.7 Traceroute

Perform a traceroute to the device and display the response. Please note that this function cannot be executed when multiple devices are selected.

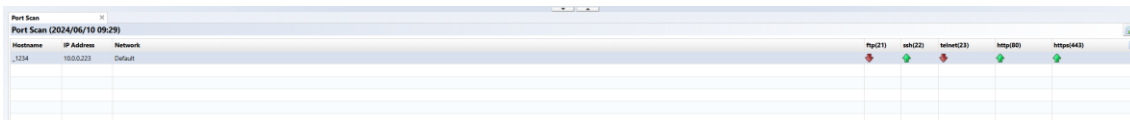


TTL	Hostname	IP Address	Probe 1 (ms)	Probe 2 (ms)	Probe 3 (ms)
✓ 1		10.0.40.254	0.953	0.789	0.786
✓ 2		10.0.0.124	0.320	0.221	0.196
▲ 3					

Traceroute to 10.0.0.223 (10.0.0.223), 14 hops max, 60 byte packets  
1 10.0.40.254 (10.0.40.254) 0.953 ms 0.789 ms 0.786 ms  
2 10.0.0.124 (10.0.0.124) 0.320 ms 0.221 ms 0.196 ms  
3 \* 10.0.0.223 (10.0.0.223) 0.641 ms \*

## 6.5.8 Port scan

Display device port opening/closing information.



Hostname	IP Address	Network	ftp(21)	ssh(22)	telnet(23)	http(80)	https(443)
1234	10.0.0.223	Default					

## 6.5.9 Live ARP Table

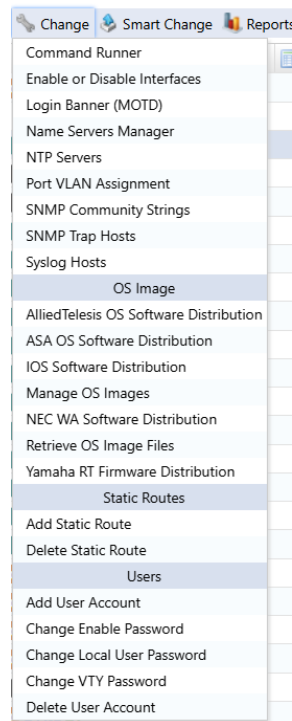
Display live status of ARP table. Please note that this function cannot be executed when multiple devices are selected.



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

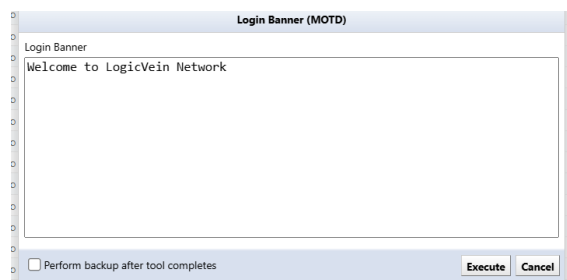
## 6.6 Change Tools

The Modify Tools menu collects operations related to modifying the configuration of the selected device. In this chapter, we will explain each function in this Modification Tools submenu in order from top to bottom.



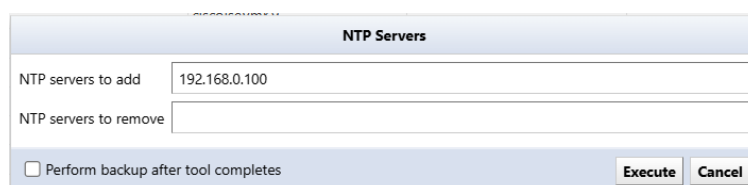
### 6.6.1 MOTD banner settings

Set the device login banner.



### 6.6.2 NTP server

Add/remove NTP servers to your device.



### 6.6.3 SNMP community string

Add/delete SNMP communities to/from devices.



The 'SNMP Community Strings' window contains two sections. The 'New Community String' section has a 'Community String' field with 'public' and an 'Access Type' dropdown set to 'RO'. The 'Delete Community String' section has a 'Community String' field with 'lvi' and an 'Access Type' dropdown set to 'RO'. At the bottom, there is a checkbox for 'Perform backup after tool completes' and 'Execute' and 'Cancel' buttons.

### 6.6.4 SNMP Trap Hosts

Add/delete SNMP trap host settings for devices. It is effective for batch setting of new NMS installations.



The 'SNMP Trap Hosts' window has two sections. The 'New Trap Host Name' section has a 'Trap Host Name/Address' field with '192.168.0.100'. The 'New Community String' section has a 'Community String' field with 'public' and an 'Action (add/delete)' dropdown set to 'add'. At the bottom, there is a checkbox for 'Perform backup after tool completes' and 'Execute' and 'Cancel' buttons.

### 6.6.5 Syslog Hosts

Add/delete Syslog hosts to/from the device.



The 'Syslog Hosts' window has two input fields: 'Logging hosts to add:' with '192.168.0.100' and 'Logging hosts to remove:'. At the bottom, there is a checkbox for 'Perform backup after tool completes' and 'Execute' and 'Cancel' buttons.

## 6.6.6 Port VLAN Assignment

Perform VLAN port settings for the device's access port. Please note that this function cannot be executed when multiple devices are selected.

Select the interface on the screen. Select the interface for VLAN settings (multiple selections are possible) and select the VLAN. Select the VLAN to be assigned from the field and click the Execute button.

The screenshot shows the 'Port VLAN Assignment' tool interface. It features a 'Select Interfaces' section with a list box containing 'mgmt0', 'Ethernet1/1', 'Ethernet1/2', 'Ethernet1/3', 'Ethernet1/4', and 'Ethernet1/5'. Below this is a 'Select a VLAN' section with a table listing available VLANs.

Name	Number
default	1
VLAN0012	12
VLAN0002	2

At the bottom, there is a checkbox labeled 'Perform backup after tool completes', and 'Execute' and 'Cancel' buttons.

## 6.6.7 Enable or Disable Interfaces

Change the Admin Status of the device interface. Please note that this function cannot be executed when multiple devices are selected.

From the "Select Interfaces" field, select the interface for which you want to change the Admin Status (multiple selections are possible), select Up/Down from the pull-down menu, and click the "Execute" button.

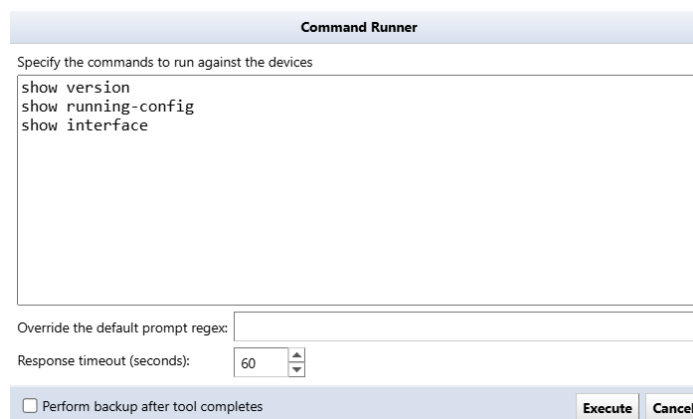
The screenshot shows the 'Enable or Disable Interfaces' tool interface. It features a 'Select Interfaces' section with a table listing interfaces and their current admin status.

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

Below the table is a 'Up/Down' section with a pull-down menu currently set to 'UP'. At the bottom, there is a checkbox labeled 'Perform backup after tool completes', and 'Execute' and 'Cancel' buttons.

## 6.6.8 Command Runner

Command Runner is a useful tool when performing the same operation repeatedly on multiple devices. For example, you can run commands of over 100 lines to many devices at once. Commands that can be performed include downloading and uploading configurations. After entering the required items, click Execute button.

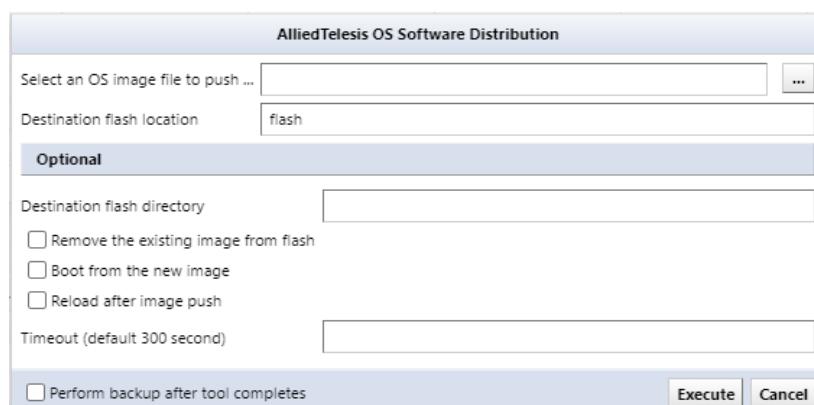


The screenshot shows the 'Command Runner' window. It has a title bar 'Command Runner'. Below it, a text area labeled 'Specify the commands to run against the devices' contains the text: 'show version', 'show running-config', and 'show interface'. Below the text area is a field labeled 'Override the default prompt regex:' which is empty. Below that is a field labeled 'Response timeout (seconds):' with a value of '60' and a spinner control. At the bottom, there is a checkbox labeled 'Perform backup after tool completes' which is unchecked. To the right of the checkbox are 'Execute' and 'Cancel' buttons.

The Override default regular expression field specifies a regular expression to match a particular type of prompt. The prompt to be matched is, in shell script terms, PS1 it's like a variable. This field is required if a command responds with an unusual prompt. For example, some interactive commands are typically <username>#” rather than the simpler prompt “<” may prompt you for the next input. In that case, use it as a regular expression ^< (at the beginning of the line<) must be specified. Otherwise, you will not be able to distinguish between the command output and the prompt.

## 6.6.9 AlliedTelesis OS software distribution

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



The screenshot shows the 'AlliedTelesis OS Software Distribution' window. It has a title bar 'AlliedTelesis OS Software Distribution'. Below it, there is a field labeled 'Select an OS image file to push ...' with a file selection button '...'. Below that is a field labeled 'Destination flash location' with the value 'flash'. Below that is a section titled 'Optional' with a light blue background. Inside this section, there is a field labeled 'Destination flash directory' which is empty. Below that are three checkboxes: 'Remove the existing image from flash', 'Boot from the new image', and 'Reload after image push', all of which are unchecked. Below the checkboxes is a field labeled 'Timeout (default 300 second)' which is empty. At the bottom, there is a checkbox labeled 'Perform backup after tool completes' which is unchecked. To the right of the checkbox are 'Execute' and 'Cancel' buttons.



Items	Explanation
Select an OS image file to push	When you press the [...] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, boot with new image
Reload after image push	After image transfer, reload the system.
Timeout (default 3000 seconds)	Timeout setting for setting transferring time

### 6.6.10 ASA OS software distribution

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

ASA OS Software Distribution

Select an ASA OS image file to push ...

...

Destination flash location

flash

Optional

☐ Remove the existing image from flash

☐ Boot from the new image

☐ Reload after image push

☐ Perform backup after tool completes

Execute

Cancel

Items	Explanation
Select an ASA OS image file to push	When you press the [...] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time

## 6.6.11 IOS software distribution

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

IOS Software Distribution

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

Destination flash location

Optional

Destination flash directory

Destination flash partition

☐ Remove the existing image from flash

☐ Boot from the new image

☐ Reload after image push

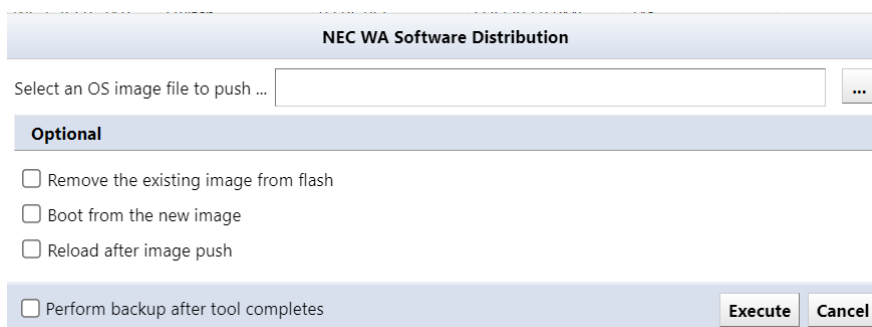
Minimum DRAM in Kilobytes (from CCO)

☐ Perform backup after tool completes

Items	Explanation
Select an IOS image file to push	When you press the [...] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
flash destination	Specifies the storage drive provided by the device. Depending on the model,flashusbflash0nvramThe content that can be specified differs.
Destination flash directory	A directory within the destination drive partition. If the directory does not exist, a directory with the specified name will be automatically created.
Destination flash partition	Partition of the destination drive. The command will fail if the specified partition does not exist.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time
Minimum DRAM in Kilobytes (from CCO)	<a href="http://cisco.com">http://cisco.com</a> Please check the DRAM capacity of the image to be submitted and enter it. Check if there is enough free space on the device before deploying the image

## 6.6.12 NEC WA software distribution


NEC WA software can be distributed remotely to the OS. To use this function, you must save the WA software in advance.

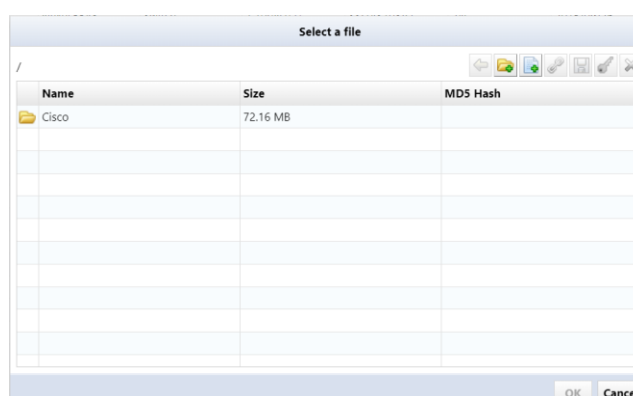


The dialog box is titled "NEC WA Software Distribution". It contains a text field labeled "Select an OS image file to push ..." with a browse button "...". Below this is an "Optional" section with three checkboxes: "Remove the existing image from flash", "Boot from the new image", and "Reload after image push". At the bottom, there is a checkbox "Perform backup after tool completes" and two buttons: "Execute" and "Cancel".


Items	Explanation
Select an OS image file to push	When you press the [...] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time

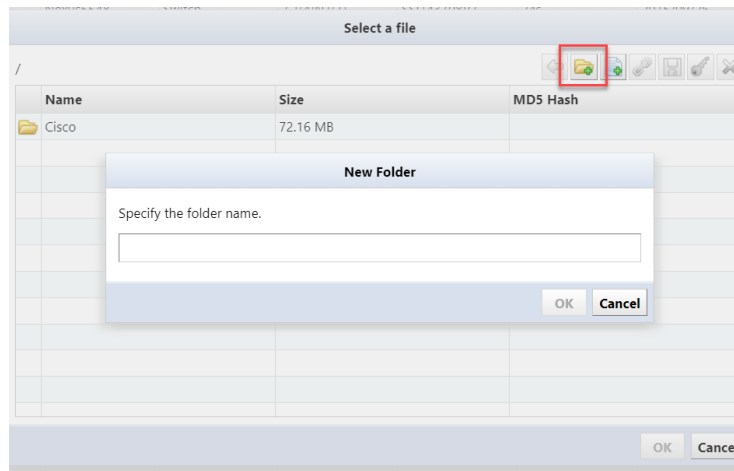
## 6.6.13 Manage OS image

Save the OS image used for software distribution on the server's file system.  Click the button and add the OS image file.



The dialog box is titled "Select a file". It shows a file list with columns "Name", "Size", and "MD5 Hash". The first entry is "Cisco" with a size of "72.16 MB". There are several empty rows below it. At the bottom right, there are "OK" and "Cancel" buttons.

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



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

Adding the OS image may take some time. If it takes too long or is not added, check the specified directory and try adding the file again.

#### 6.6.14 Retrieve OS image file

Downloads the OS image from the specified device and saves it to the database. Downloaded images can be uploaded again later.

Retrieve OS Image Files (2024/04/09 09:27)				
Hostname	IP Address	Network	Elapsed Time (seconds)	OS Image
✓ A	10.0.0.128	Demo	0	packages.conf

#### 6.6.15 Yamaha RT Firmware Distribution

Yamaha RT software can be distributed remotely to the OS. To use this function, you must save the Yamaha RT software in advance.

Yamaha RT Firmware Distribution

Select a Yamaha firmware file to push ...

TFTP Option

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

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

Optional

☐ Save and send temporary configuration for upgrade (Recommendations)

Minimum free memory (percentage)

Waiting timer (default 300 second)

☐ Perform backup after tool completes

Execute

Cancel

project	explanation
Select a Yamaha firmware file to push	Select target firmware file
Specify the destination exec Flash ROM area Number. (i.e: 1 or 0 or blank)	For models that support multiple firmware, you can select ROM area number (1,0). If not specified, the running firmware will be upgraded.
Copy currently firmware to internal Flash ROM area ( for multiple flash supported device only)	Back up the running firmware on models that support multiple firmware*1
Save and send temporary configuration for upgrade (Recommendations)	Save the settings and execute the command before uploading the firmware *2
Minimum free memory (percentage)	It is possible to cancel the firmware upgrade if the configured memory is exceeded*3
Waiting timer (default 300 seconds)	Specify standby time in environments with high network communication delays

\*1: In the following cases, since Rev.14.01.14 is running, this firmware will be backed up.

No.	Revision
0	Rev.14.01.11
*1	Rev.14.01.14

If this check is performed on a model that does not support multiple firmware, the firmware upgrade will be aborted. The upgrade will also be canceled if the ROM number of the revision destination and the ROM number of the running firmware are the same.

\*2: The following command will be executed.

login timer [timer]

show config | grep "tftp host"

tftp host [NetLD IP]

\*3: If the memory usage is below, firmware upgrade will be canceled by setting 80.

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

## 6.6.16 Add Static Route

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

**Add Static Route**

**Destination**

Destination Address(IP Address) 10.0.100.0

Destination Mask(IP Mask) 255.255.255.0

**Gateway**

Gateway Address(IP Address) 10.0.0.30

☐ Perform backup after tool completes

Execute Cancel

## 6.6.17 Delete Static Route

Select and delete an existing static route configuration.

**Delete Static Route**

Select Static Routes

Gateway	Destination Mask	Destination Address
10.0.0.254	0	0.0.0.0
	0	0.0.0.0

☐ Perform backup after tool completes

Execute Cancel

## 6.6.18 Change Enable Password

Change the Enable Password or Enable Secret settings for your device. If Enable Password is set, Enable Password is changed, and if Enable Secret is set, Enable Secret is changed. If both are set, Enable Secret will be changed.

**Change Enable Password**

**User Data**

**New Password**

Password: .....

Confirm: .....

☐ Verify credentials after change is executed

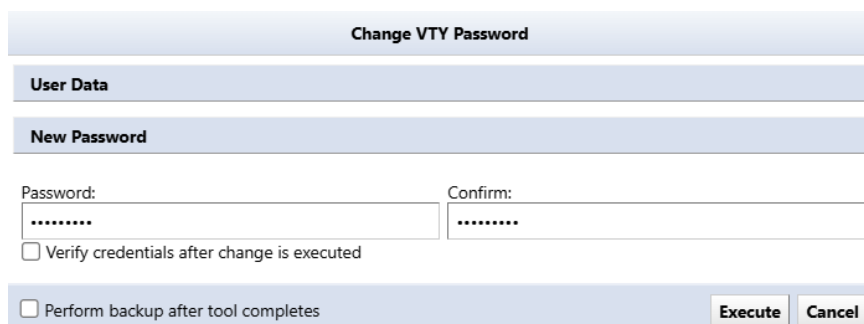
☐ Perform backup after tool completes

Execute Cancel

Also, if static credentials are being used, by checking "Confirm credentials after change", the credentials will be automatically changed, and you will be checked to see if you can log in with the password you set.

## 6.6.19 Change VTY Password

Change the device's VTY Password settings.

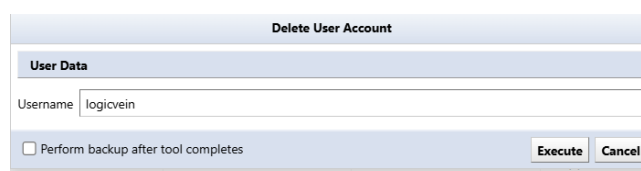


The 'Change VTY Password' dialog box features a title bar with the text 'Change VTY Password'. Below the title bar is a 'User Data' section. Underneath is a 'New Password' section containing two input fields: 'Password:' and 'Confirm:', both filled with seven dots. Below these fields is a checkbox labeled 'Verify credentials after change is executed'. At the bottom of the dialog is another checkbox labeled 'Perform backup after tool completes'. To the right of this checkbox are two buttons: 'Execute' and 'Cancel'.

Also, in the same way as changing Enable Password, by checking "Confirm credentials after change", the credentials will be automatically changed and you will be checked to see if you can log in with the password you set.

## 6.6.20 Delete User Account

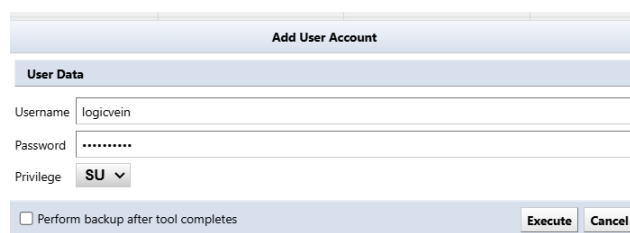
Delete an existing user account configured on the device. Please note that this function cannot be executed when multiple devices are selected.



The 'Delete User Account' dialog box has a title bar labeled 'Delete User Account'. It contains a 'User Data' section with a 'Username' input field containing the text 'logicvein'. Below the username field is a checkbox labeled 'Perform backup after tool completes'. At the bottom right are 'Execute' and 'Cancel' buttons.

## 6.6.21 Add User Account

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



The 'Add User Account' dialog box features a title bar labeled 'Add User Account'. It includes a 'User Data' section with three input fields: 'Username' (containing 'logicvein'), 'Password' (filled with seven dots), and 'Privilege' (a dropdown menu showing 'SU'). Below these fields is a checkbox labeled 'Perform backup after tool completes'. At the bottom right are 'Execute' and 'Cancel' buttons.

## 6.6.22 Change Local User Password

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

Change Local User Password	
<b>User Data</b>	
Username	logicvein
<b>New Password</b>	
Password:	Confirm:
*****	*****
<input type="checkbox"/> Verify credentials after change is executed	
<input type="checkbox"/> Perform backup after tool completes	
<div>ExecuteCancel</div>	



## 6.7 Smart change overview

The smart change feature is similar to the command runner, but with more flexibility. Instead of issuing one fixed command, you can create a template of the command and set template variables to change the value of the variable for each device.

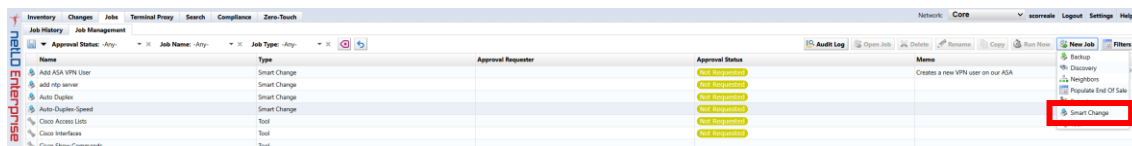
For example, if you want to change the password of a device, but you want to set a different password for each device, you will need to run a job for each device in the command runner.

However, by using smart change, you can change passwords into variables and assign different values to each device, allowing you to set different passwords in one job.

### 6.7.1 Create a smart change job

Smart change jobs can be created from "Job Management". How to create a job [6.10 Job management](#)

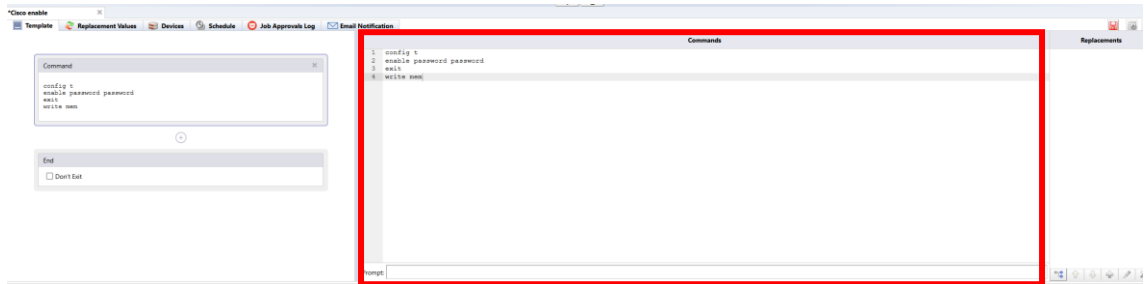
1. Click the [Job] tab → [Job Management], and then click [New Job] → [Smart Change].



Enter the job name and comment, select the function, and click [OK].

Items	Explanation
Job name	Enter the name of the smart change job.
Comment	Enter a comment (description) for the smart change job.
Use remediation job	Select whether to use smart change jobs as remediation jobs. If selected, additionally select an adapter.
Use the same replacement value for all devices in the job or Use unique replacement values for each device in the job	Choose one. When executing a command, you can choose whether to execute it with the same value in the variable or with a different value.

2. In the template, enter the base command.



3. Select the part you want to change as an alternative value, click the + button.



4. Enter a name for the alternative value and select a type.

**Add Replacement**

Selection: password

Name:

Type: **Text** (dropdown menu)

☒ Use selection as default value

Items	Explanation
Text	Any text
IP address	IP address. If a value other than the correct IPv4 or IPv6 format is entered, an error will be reported.
Hostname	Hostname
IP address or hostname	IP address or host name
Choice	When entering an alternative value, you will be able to select it from a drop-down list. It is safe because only the preset values will be entered.
Condition selection	Provide a checkbox to enable or disable it. For devices marked as disabled, the alternative value is an empty string.

Variable parts are displayed in yellow.



Commands			Replacement
1	config t		
2	enable password	newpassword	newpassword
3	exit		
4	write mem		

5. Add the device you want to run on the Devices tab.

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	Cisco	CISCO1921-K9	Router	15.4(3)M5	FL11582638
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	Cisco	CISCO1921-K9	Router	15.4(3)M5	FL11582638
10.0.0.223	_1234	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.3	WMT4U5FQV5
10.0.0.128	aaa	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	94P8T33EIN
192.168.1.61	C9800-WLC	Default	Cisco IOS	Cisco	C9800-4-C-K9	Wireless Controller	16.12.4a	FCJ245100KJ
10.0.0.249	Cisco-I-AuthServ	Default	Cisco IOS	Cisco	cat9k9508k	Switch	15.2(2)E	FOC1721W15R
10.0.0.155	cisco155	Default	Cisco IOS	Cisco	ciscoCSR1000v	Router	15.4(1)S4	9W5FRHJ039
10.0.0.156	cisco156	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.157	cisco157	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.158	cisco158	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.161	cisco161	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.162	cisco162	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.163	cisco163	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.164	cisco164	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.165	cisco165	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W5FRHJ039
10.0.0.195	CiscoS24M	Default	Cisco IOS	Cisco	ciscoS24M	Router	15.4(1)S4	9W5FRHJ039
10.0.0.241	CSR1000V241	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.3	9Z20SSUNKA

6. On the Replacement Values tab, enter the values.

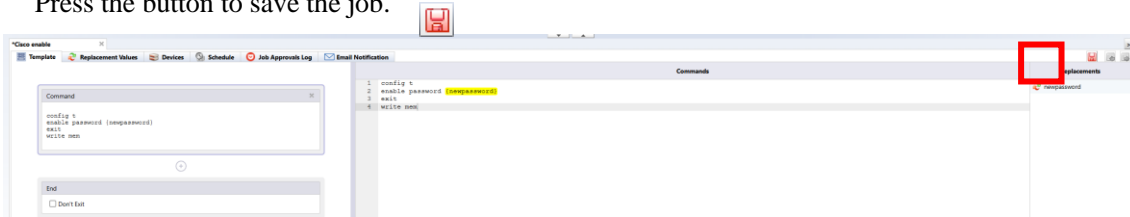
Template			Replacement Values	Devices	Schedule	Job Approvals Log	Email Notification
IP Address	Hostname	Network	newpassword	password01			
10.0.0.128	aaa	Default					
192.168.1.61	C9800-WLC	Default					

Alternative data can be imported/exported using Excel files. top right  (export) or  Please use (import).

7. Add triggers on the Schedule tab.

Template			Schedule	Job Approvals Log	Email Notification
Trigger					
<div> <div> Name: schedule </div> <div> <input checked="" type="radio"/> Once <input type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly <input type="radio"/> Cron </div> <div> 9:55 2024/06/10 </div> <div> Timezone: (GMT-06:00) Central Time </div> <div> Filter: &lt;No Filter&gt; </div> <div> Save Cancel </div> </div>					

8. Press the button to save the job.



## 6.8 Register a user

Create a user to log in to NetLD. By assigning privileges to users, you can restrict the operations that users can perform. NetLD allows you to specify detailed permissions by combining multiple permissions.

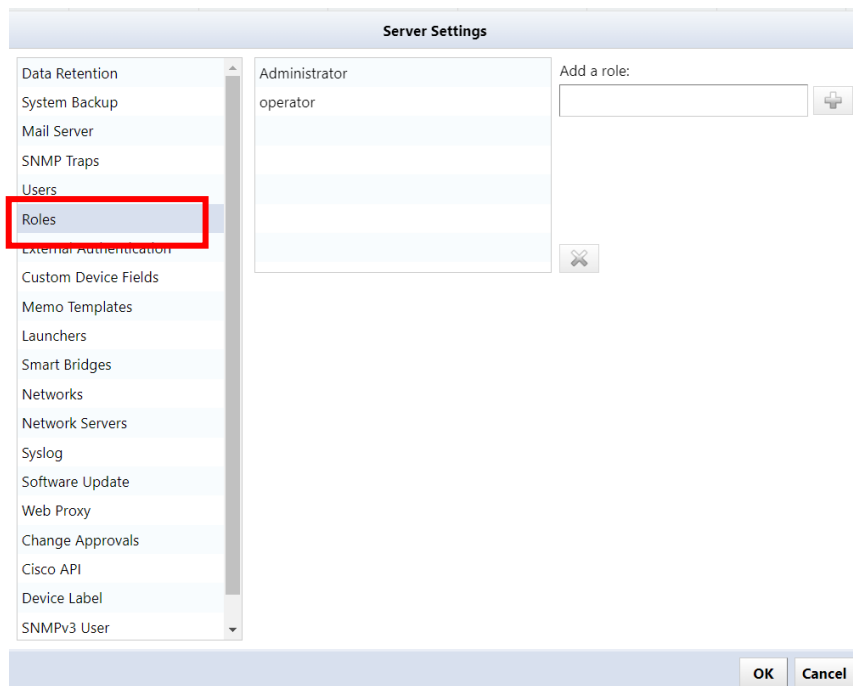
User and permission settings can be configured from [Settings] in the global menu.



### 6.8.1 Add permissions

\*"Administrator" who also has all execution privileges is registered. "Administrator" privilege cannot be removed.

1. Click Roles.



2. Enter the permission name in the [Add a role] field and click [(Add)].

The screenshot shows the 'Server Settings' dialog box with the 'Roles' tab selected. On the left is a list of settings categories, with 'Roles' highlighted. The main area contains a list of roles: 'Administrator', 'operator', and 'labperson'. The 'labperson' role is selected. To the right of the roles list is an 'Add a role:' text field containing 'labperson'. A green plus icon in a red box is located to the right of this field. Below the roles list is a small 'X' icon. At the bottom right are 'OK' and 'Cancel' buttons.

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

This screenshot shows the same 'Server Settings' dialog box, but now the 'labperson' role is selected in the roles list. A red box highlights the 'Authority' section at the bottom right. This section contains a list of permissions, each with a checkbox: 'Permission to create/update/delete monitors.', 'Permission to administer incidents.', 'Permission to view maps.', 'Permission to create/update/delete maps.', 'Permission to administer SNMP MIBs.', 'Permission to view syslogs.', 'Permission to view compliance rule sets and policies.', and 'Permission to create/update/delete a compliance policy.'. Below this list are 'Select All' and 'Select None' buttons. The 'Add a role:' field is now empty and has a plus icon to its right.

## [List of authority items]

Authority items	Explanation
Allow viewing of compliance rulesets and policies.	You can view the Compliance tab.
Allow creation/update/delete of compliance policies.	You can create/update/delete compliance policies. (*Permissions associated with "Allow viewing of compliance rule sets and policies.")
Allow creation/update/delete of compliance rule sets.	You can create/update/delete compliance rules. (*Permissions associated with "Allow viewing of compliance rule sets and policies.")
Allow configuration viewing.	You can view the configuration retrieved from the device.
Allow credentials and protocol settings.	You can configure credentials and protocols.
Allow creation/update/delete of device information in inventory.	You can create/update/delete device information in inventory.
Allow setting custom field names.	You can rename custom device fields.
Allows tags to be applied and removed from devices in inventory.	You can apply and remove tags to devices in your inventory.
Allow viewing of draft configurations.	You can view draft configurations.
Allow creation/update/delete of draft configurations.	Can create/update/delete draft configurations (*Authority associated with "Allow viewing of draft configuration.")
Allow schedule filter settings.	You can set filters for the schedule.
Allow backup jobs to run.	You can run backup jobs.
Allow creation/update/delete of backup jobs.	You can create/update/delete backup jobs. (*Permissions associated with "Allow execution of backup jobs.")
Allow discovery to run.	You can run discovery.
Allow creation/update/delete of discovery jobs.	You can create/update/delete discovery jobs. (*Authority associated with "Allow discovery to be executed.")
Allow the tool to run.	You can run the tool.
Allow creation/update/delete of tools.	You can create/update/delete tools. (*Permissions associated with "Allow tool execution.")
Permission to authorize tool execution.	You can approve jobs that require approval. (*Permissions associated with "Allow tool execution.")
Permission to run tools without authorization.	You can create and run jobs that do not require approval. (*Permissions associated with "Allow tool execution.")

Authority items	Explanation
Allow smart change jobs to run.	You can run smart change jobs. (*Permissions associated with "Allow tool execution.")
Allow creation/update/delete of smart change jobs.	You can create/update/delete smart change jobs. (*Authority associated with "Allow smart change job execution.")
Allow execution of device configuration change tools.	You can run the change tool. (*Permissions associated with "Allow tool execution.")
Allow reports to run.	You can run the report.
Allow to create/update/delete reports.	You can create/update/delete reports. (*Authority associated with "Allow report execution.")
Allow configuration restore jobs to run.	You can run configuration restore jobs.
Allow execution of neighbor information collection job.	You can run neighbor information collection jobs.
Allow creation/update/deletion of neighbor information collection jobs.	You can create/update/delete neighbor information collection jobs. (*Authority associated with "Allow execution of neighbor information collection job.")
Allow creation/update/delete of URL launchers.	You can create/update/delete URL launchers.
Allow creating/updating/deleting notes.	You can create/update/delete notes.
Allow creation/update/delete of management networks.	You can create/update/delete management networks.
Allow security settings.	You can set security.
Allow creation/update/delete of inventory tags.	You can create/update/delete inventory tags.
Allow login via terminal server proxy.	You can log in via a terminal server proxy.
Allow automatic login via terminal server proxy.	Automatic login via terminal server proxy is possible. (*Permissions associated with "Allow login via terminal server proxy.")
Allow automatic login directly to enable mode.	You can automatically log in directly to enable mode. (*Permissions associated with "Allow automatic login via terminal server proxy.")
Allow other users to view terminal access logs.	You can view other users' terminal access logs.



Authority items	Explanation
Allow deletion of terminal access log viewing.	You can delete terminal access logs. (*Permissions associated with "Allow viewing of other users' terminal access logs.")

4. Click OK.

**Server Settings**

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

Administrator  
operator  
labperson

Add a role:

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

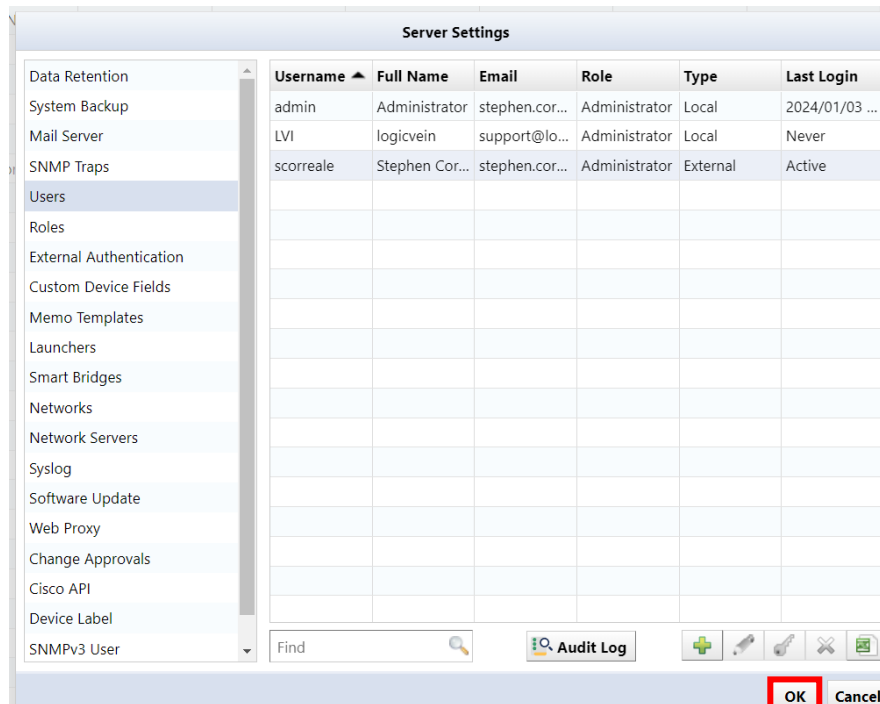
Select All Select None

**OK** Cancel



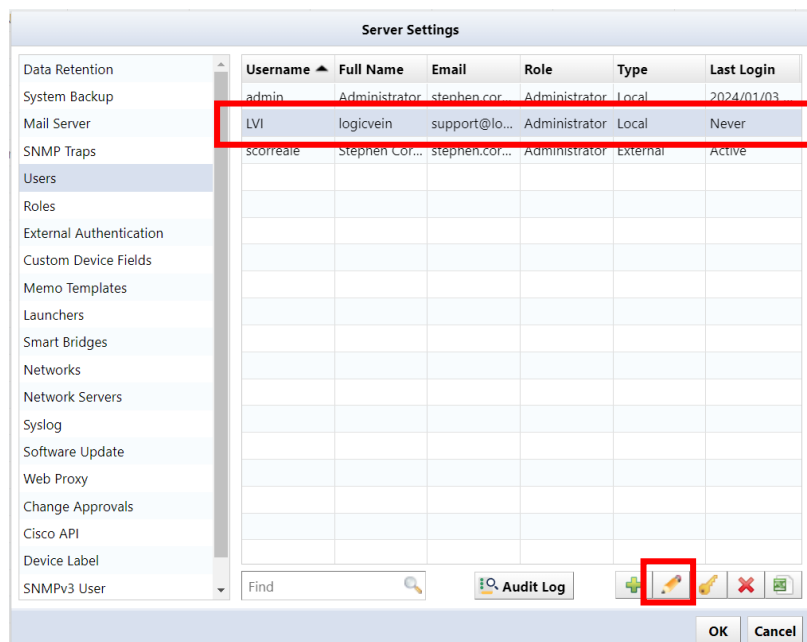
Category	Items	Explanation	must
	Role	Select the user's permissions. You can select the permissions set in "7.11.1 Add permissions" from the pull-down menu.	must
	Password	Set the user's password. *To set a password, the following conditions must be met. Must be at least 8 characters Must not be a character string that is easy to guess (person's name, proper noun, dictionary word, commonly used password) Character strings that do not repeat the same characters or are arranged in an easy-to-understand manner	must
Custom field	Custom 1-5	Select the custom device fields that users can view. *Displayed item names will change based on the settings in "6.12 Add columns/change column names for custom device fields".	—

3. Click OK.



### 6.8.3 Change user information

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



2. The user edit screen will be displayed. After editing, click OK.

\*Username cannot be changed.

\*If you want to change your password, set it from [ (Key)].

The screenshot shows the 'Edit User' window. On the left is a sidebar with tabs: 'General', 'Custom Fields', and 'Mail'. The 'General' tab is selected. The main area contains four fields: 'Username:' (LVI), 'Full Name:' (logicvein), 'Email Address:' (support@logicvein.com), and 'Role:' (Administrator). The 'Role' field is a dropdown menu. At the bottom right are 'OK' and 'Cancel' buttons.

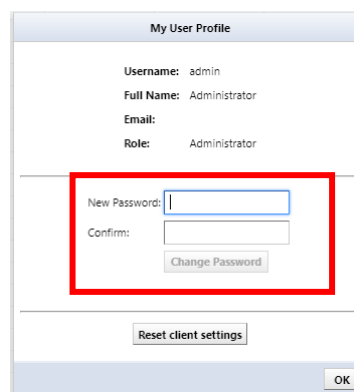
Field	Value
Username	LVI
Full Name	logicvein
Email Address	support@logicvein.com
Role	Administrator

## 6.8.4 Change password

You can change your password from the login user name in the global menu. Here, we are changing the password for the username "admin".



Enter your new password in [New Password] and [Retype Password]. Press the [Change password] button to register a new password. If the new password and the re-entered string are different, the [Change password] button will not be enabled.

A web form titled 'My User Profile'. It contains fields for 'Username: admin', 'Full Name: Administrator', 'Email:', and 'Role: Administrator'. Below these is a section for password change, which is highlighted with a red border. This section includes 'New Password:' and 'Confirm:' text labels, each followed by an input field. Below the input fields is a 'Change Password' button. At the bottom of the form is a 'Reset client settings' button and an 'OK' button in the bottom right corner.

### Notice

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

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

## 6.8.5 Configuring External Authentication

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

### 6.8.5.1 RADIUS

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

Below is a sample user configuration for FreeRADIUS:

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

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

1. Navigate to the Server Settings window in netLD and select External Authentication.
2. Change the 'Enable external authentication' selection to 'RADIUS'.

Server Settings

Enable external authentication: **RADIUS**

Hostname: lvijp.co Port: 1812

Shared Secret: .....

Character Encoding: UTF-8

Test

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

OK Cancel

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

Server Settings

Enable external authentication: **RADIUS**

Hostname: lvi.jp.co Port: 1812

Shared Secret: .....

Character Encoding: **UTF-8**

Test

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

OK Cancel

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

Server Settings

Enable external authentication: **RADIUS**

Hostname: lvi.jp.co Port: 1812

Shared Secret: .....

Character Encoding: **UTF-8**

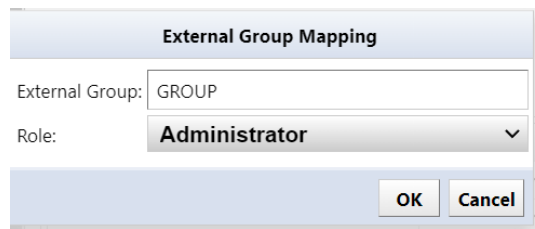
Test

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

OK Cancel

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



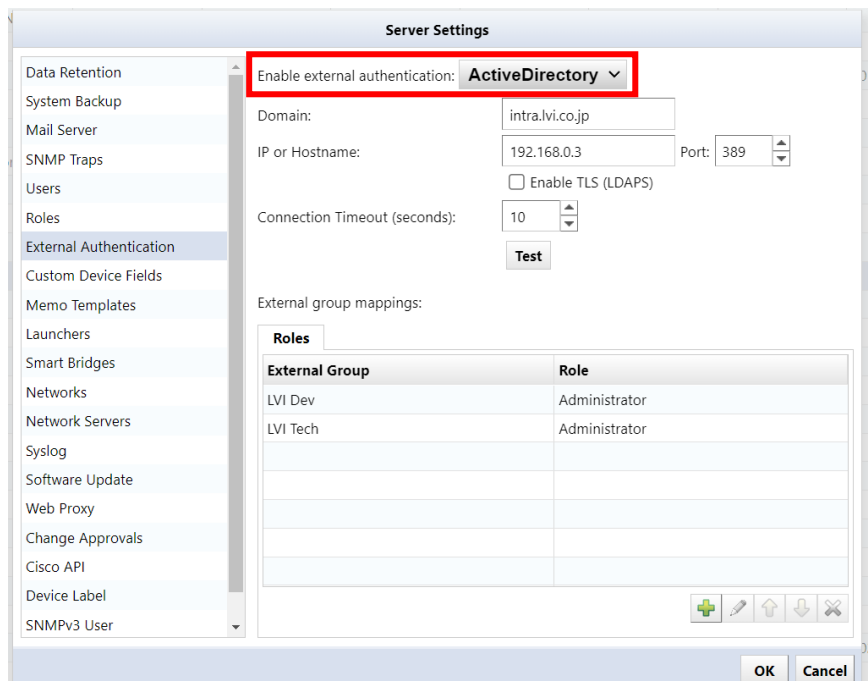
The dialog box is titled "External Group Mapping". It contains two fields: "External Group:" with the value "GROUP" and "Role:" with a dropdown menu showing "Administrator". At the bottom right are "OK" and "Cancel" buttons.

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

### 6.8.5.2 Active Directory linkage

When linking with an Active Directory server, permissions and networks are determined using the group to which the registered user belongs.

1. Change [Enable external authentication] to "Active Directory".



The "Server Settings" dialog box shows a sidebar on the left with various settings categories. The "External Authentication" category is selected. In the main area, the "Enable external authentication:" dropdown is set to "ActiveDirectory" and is highlighted with a red box. Other fields include "Domain:" (intra.lvi.co.jp), "IP or Hostname:" (192.168.0.3), "Port:" (389), and "Connection Timeout (seconds):" (10). There is a "Test" button. Below these fields is a table for "External group mappings:".

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

At the bottom right are "OK" and "Cancel" buttons.



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

Server Settings

Enable external authentication: **ActiveDirectory**

Domain: intra.lvi.co.jp

IP or Hostname: 192.168.0.3 Port: 389

☐ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

Test

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

OK Cancel

- Set permissions for external group mapping. Add a new item from [+ (Add)].

Server Settings

Enable external authentication: **ActiveDirectory**

Domain: intra.lvi.co.jp

IP or Hostname: 192.168.0.3 Port: 389

☐ Enable TLS (LDAPS)

Connection Timeout (seconds): 10

Test

External group mappings:

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

+ (Add) Edit Up Down Delete

OK Cancel

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

External Group Mapping

External Group: LVI Test

Role: Administrator

OK Cancel

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

### 6.8.5.3 SAML

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

#### 6.8.5.3.1 Microsoft Entra ID Integration

##### [Prerequisites]

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

- You can sign in to Microsoft Entra ID with administrator privileges
- The users and groups to be linked exist in Microsoft Entra ID
- You have the authority (\*) to configure settings in NetLD
  - (\*) Administrator privileges or the authority to "Allow security settings".

##### [Procedure]

##### Configure SAML with NetLD

1. Log in to NetLD.
2. Open [Settings] > [External Authentication].
3. Select "SAML" from [Enable external authentication].
4. Verify that [Callback URL] is the correct URL for the NetLD server.
  - \* Callback URL format: `https://[IP address or hostname]/auth`
  - \* By default, it refers to the value in [Network Servers] > [Hostname/IP Address].
5. Click the [Download LogicVein SAML Service Provider Metadata XML] link to download the Metadata XML file.
  - \* File name: `LogicVein-saml-sp-metadata.xml`
  - \* The downloaded file will be used in the next step.

## Create a new application

1. Sign in to the Microsoft Entra Admin Center.
2. Open [Identity] > [Applications] > [Enterprise applications].
3. Click the [New Application].
4. Click the [Create your own application].
5. Set a name for the app, select [Integrate any other application you don't find in the gallery (Non-gallery)], and click [Create].
6. Open [Manage] > [Single Sign-On].
7. On the Select a Single Sign-On Method page, click [SAML].
8. On Set up Single Sign-On with SAML, click [Upload metadata file], upload the logicVein-saml-sp-metadata.xml file downloaded in the previous step, and click [Add].
9. Make sure that the Callback URL configured in the NetLD server settings is entered in the Identifier, Response URL, and Logout URL fields.
10. Click [Save].
11. Click the [x] button to close the editing screen.
  - \* If a pop-up message appears saying Test Single Sign-On, click [No, I'll test it later].
12. Click [Edit] in the Attributes and Claims section.
13. On the Attributes and Claims page, select [Add a group claim].
14. Select the [Security Group] option and select "Group ID" in Source Attribute.
15. Click [Save].
16. Click the [x] button to close the Attributes and Claims page.

## Get IdP metadata

1. In the SAML Certificates section, for Federation Metadata XML, click [Download].
2. Download the IdP metadata XML file.
3. On the Set up single sign-on with SAML page, in the SAML Signing Certificate section, find Federation Metadata XML and select Download to download the certificate and save it on your computer.

## Register your application with NetLD

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

### Note the object ID

1. Return to the Microsoft Entra admin center and click [Manage] > [Users and Groups].
2. Click [Add user/group].
3. Click [None Selected] in the Users section.
4. From the users list, select the users who should be allowed to log in to NetLD.
5. Click [Select].
6. Click [Assign] to complete the user assignment.
7. In the left pane, navigate to [Identities] > [Groups] > [All Groups].
8. Note the Object ID of the group you want to allow to log in to NetLD.

### Configure external group mapping

1. Open [Settings] > [External Authentication].
2. Under [External Group Mapping], click [+] button.
3. In the [External Group] field, enter the "Object ID" noted in the previous step, specify the permissions you want to assign in [Permissions], and click [OK].
4. Click [OK] to save [Server Settings].
5. Click Logout of NetLD. You will be taken to the Microsoft login page.

## 6.8.5.3.2 Okta Integration

### [Prerequisites]

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

- You can sign in to the Okta dashboard with administrator privileges
  - The users and groups to be integrated exist in Okta
  - You have the permission to configure settings in NetLD (\*)
- (\*) Administrator privileges or the permission to "Allow security settings."

### [Procedure]

#### Configure SAML with NetLD

1. Log in to NetLD.
2. Open [Settings] > [External Authentication].
3. Select "SAML" from [Enable external authentication].
4. Make sure that [Callback URL] is the correct URL for your server.
  - \* By default, it refers to the value of [Network Servers] > [Hostname/IP Address].
5. Click the [Download LogicVein SAML Service Provider Certificate] link to download the certificate file.
  - \* File name: LogicVein-saml-sp-signing-certificate.crt
  - \* The downloaded file will be used in the next step.

## Create a new application

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

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

6. Click [Show Advanced Settings].
7. In [Signature Certificate], click [Browse files...] and select the SP certificate downloaded from NetLD in the previous step.  
\* File name: LogicVein-saml-sp-signing-certificate.crt

8. Set the following items.

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

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

- 1)

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

- 2)

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

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

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

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

### **Assigning groups to use the application**

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

### **Get IdP metadata**

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

### **Register application with NetLD**

1. Open NetLD Settings > External Authentication.
2. Click Upload IdP Metadata XML and select the XML file created in step "Get IdP Metadata".

### **Configure external group mapping**

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

### **Log in to NetLD**

Log in to NetLD as an Okta user.

After completing the settings described in [6.8.5.3.2 Okta Integration](#), when you access NetLD, the Okta sign-on screen will be displayed.

#### 6.8.5.4 Use Local Authentication After Setting Up SAML Authentication

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

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

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

#### 6.8.5.5 Testing external authentication

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

The screenshot shows the 'Server Settings' dialog box with the 'External Authentication' tab selected. The 'Enable external authentication' dropdown is set to 'ActiveDirectory'. The 'Domain' field contains 'intra.lvi.co.jp', 'IP or Hostname' is '192.168.0.3', and 'Port' is '389'. The 'Connection Timeout (seconds)' is set to '10'. A red box highlights the 'Test' button. Below, the 'External group mappings' table shows two entries: 'LVI Dev' mapped to 'Administrator' and 'LVI Tech' mapped to 'Administrator'.

External Group	Role
LVI Dev	Administrator
LVI Tech	Administrator

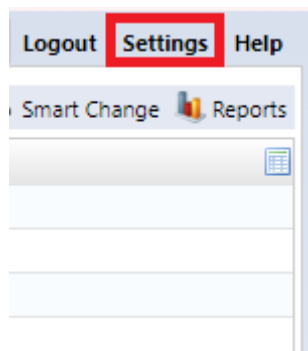
When the [Test Authentication] dialog appears, enter the [Username] and [Password] to test authentication, and click [Test]. If the authentication is successful, the message "Authentication was successful" will be displayed as shown below.

The screenshot shows the 'Test Authentication' dialog box. The 'Username' field contains 'scoreale' and the 'Password' field is masked with dots. A red box highlights the 'Test' button. Below the button, the text 'Authentication successful' is displayed in green. A 'Close' button is at the bottom right.

## 6.8.6 Set session timeout for users

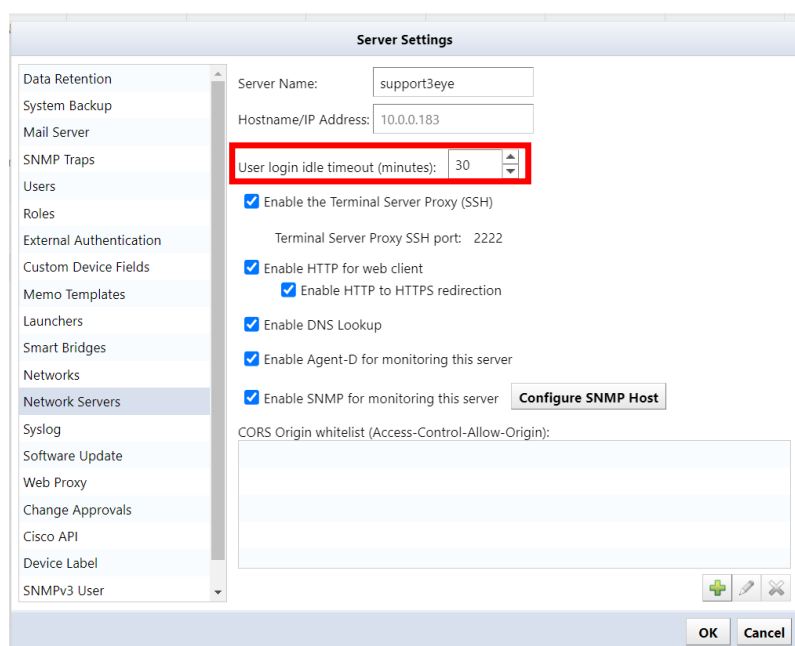
NetLD requires users to re-authenticate after 30 minutes of inactivity. To change this time, follow the steps below.

1. Click [Settings] on the global menu.



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

\*Settable range: 10 to 525600 (minutes)



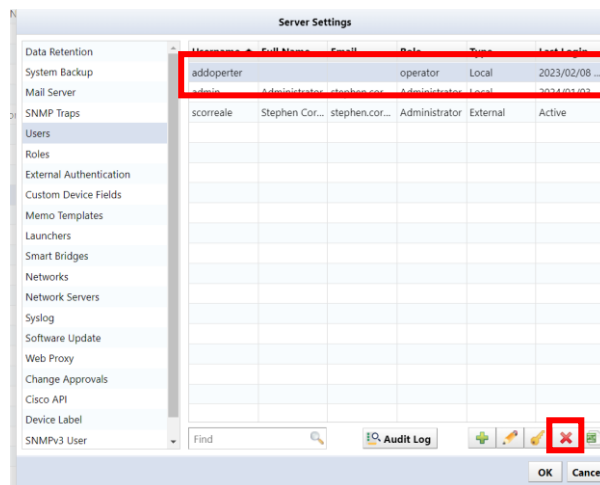
3. Click OK.
4. Log out and log back in.

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



## 6.8.7 Delete user

1. Select the user you want to delete and click [ (Delete)].

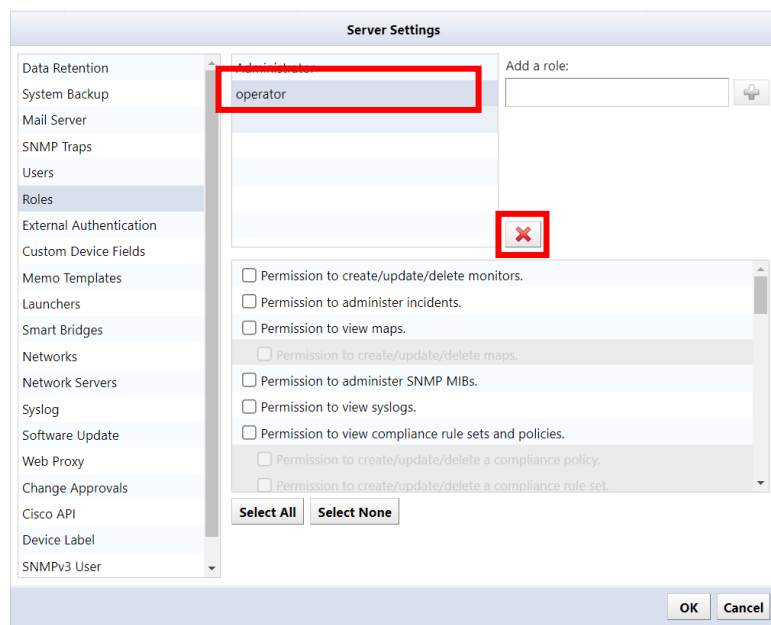


2. The user will be deleted. Click OK on the server settings.

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

## 6.8.8 Remove permissions

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



4. Click OK on the server settings.

## 6.9 Change data retention period

Data retention period sets the data retention period and automatic deletion timing.

The screenshot shows the 'Server Settings' window with the 'Data Retention' tab selected. The left sidebar lists various settings, including 'Data Retention', 'System Backup', 'Mail Server', 'SNMP Traps', 'Users', 'Roles', 'External Authentication', 'Custom Device Fields', 'Memo Templates', 'Launchers', 'Smart Bridges', 'Networks', 'Network Servers', 'Syslog', 'Zero-Touch', 'Software Update', 'Web Proxy', 'Change Approvals', 'Cisco API', and 'SNMPv3 User'. The main area contains four sections:

- Delete expired data weekly at this time:** A dropdown menu is set to 'Tuesday', and the time is set to 21:10.
- Duration to keep job execution history:** A dropdown menu is set to '3 Months'.
- Duration to keep configuration history:** A dropdown menu is set to '6 Months'.
- Duration to keep terminal proxy history:** A dropdown menu is set to 'Forever'.

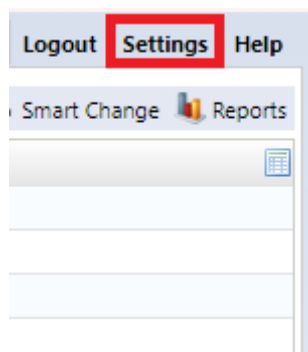
'OK' and 'Cancel' buttons are located at the bottom right of the window.

Items	Explanation
Delete expired data weekly at this time:	Data that has passed a certain period of time is automatically deleted every week on a specified day and time. (Initial value: Monday, 6:00) Specify the data retention period in the following items. (*However, if you specify "No expiration date", the data will not be deleted)
Duration to keep job execution history:	Specify the retention period for data on the [Job] → [Job History] tab from one of the following options. (Initial value: 3 months) " Forever", "3 months", "6 months", "9 months", "1 year"
Duration to keep configuration history:	Specify the configuration retention period for each monitored device from the following: (Initial value: Forever) "Forever", "6 months", "1 year", "2 years", "3 years", "4 years", "5 years", "6 years", "7 years"
Duration to keep terminal proxy history:	Specify the retention period for data on the Terminal Proxy tab from one of the following options. (Initial value: 3 months) " Forever ", "3 months", "6 months", "9 months", "1 year", "3 years"

## 6.10 Set up your mail server

For Email Server, enter the SMTP server information for email notifications from NetLD. If you want to send an email or a dashboard report in the event of a failure, you need to make settings in advance.

1. Click [Settings] on the global menu.



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

A screenshot of the 'Server Settings' dialog box. On the left, there is a list of settings categories: Data Retention, System Backup, Mail Server, SNMP Traps, Users, Roles, External Authentication, Custom Device Fields, Memo Templates, Launchers, Smart Bridges, Networks, Network Servers, Syslog, Software Update, Web Proxy, Change Approvals, Cisco API, Device Label, and SNMPv3 User. The 'Mail Server' category is selected and highlighted with a red box. The main area of the dialog shows the configuration for the mail server. It includes fields for 'SMTP Host' (lvi-co-jp.mail.protection.outlook.com), 'From Email Address' (support3eye@lvi.co.jp), and 'From Name' (support3eye). There are also checkboxes for 'Server requires authentication' (unchecked), 'Use secure smtp' (unchecked), and 'Automatically upgrade STARTTLS negotiation' (checked). Below these are fields for 'Mail server username' and 'Mail server password'. At the bottom, there are dropdown menus for 'Default email language' (set to English) and 'Default email time zone' (set to (GMT+09:00) Tokyo). A 'Test' button is located at the bottom left of the main area. At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons.

Items	explanation
SMTP Host	Specify the host name or IP address of the mail server. (Initial value: mail)
From Email Address	Specify the email address that will be displayed as the sender (sender) of the email. (Initial value: netLD)
From Name	Specify the name that will be displayed as the email sender's name (sender). (Initial value: netLD)

Items	explanation
Server requires authentication	Configure mail server authentication. If SMTP authentication is required, check the box and configure the following items. (Initial value: disabled) Mail server username... Authentication ID Mail server password ... Authentication password
Use secure smtp	Enable TLS.
Automatically upgrade STARTTLS negotiation	Automatically upgrade to secure connections using TLS or SSL.
Default email language	Set the email display language.
Default email time zone	Set the email time zone.
Root Certificate	Set the trusted CA certificate.

3. Click OK.

## 6.11 Configure SNMP trap sending

SNMP Trap Settings configures settings for sending SNMP traps from NetLD. Set the conditions for sending traps and the trap destination.

1. Click [Settings] on the global menu.
2. Click [SNMP Trap Settings] and insert a check mark on the events to be sent.

**Server Settings**

**Send traps when...**

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

**Trap forwarding:**

☐ Forward all received traps

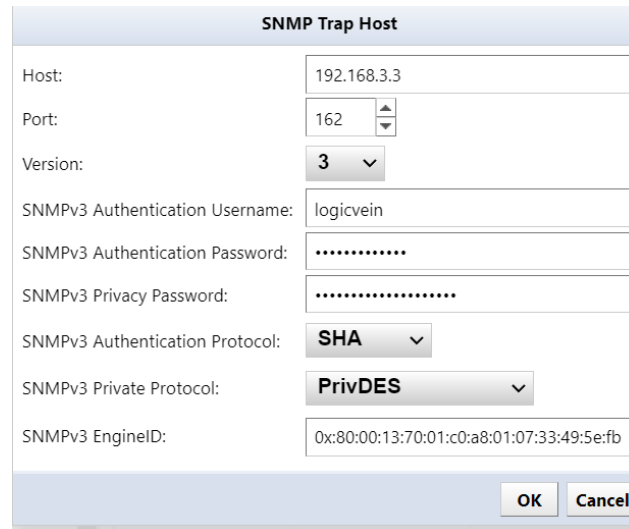
**Trap receivers:**

Community	Host	Port	Version

OK Cancel

Items	Explanation
device configuration changes are detected	Sends an SNMP trap when it detects that the device configuration has changed since the last backup.
devices are added and deleted	Sends SNMP traps when devices are added/removed.
a backup failure	Sends an SNMP trap if configuration backup fails.
a job completes with errors	Sends an SNMP trap if job execution fails.
the compliance status of a device changes	Sends SNMP traps when compliance status changes.
the status of bridge changes	Sends an SNMP trap when the connection status between the smart bridge and core server changes. (*Displayed only when the optional license is valid)
an audit event occurs	Sends an SNMP trap when a user logs in/logs out.
a change approval action occurs	Sends an SNMP trap when a job approval event occurs.
an email failure	If email sending fails, an SNMP trap will be sent.

3. Click [(Add)].
4. Enter the trap destination information and click OK.



The image shows a dialog box titled "SNMP Trap Host". It contains the following fields and controls:

- Host:** A text input field containing "192.168.3.3".
- Port:** A spin box with "162" selected.
- Version:** A dropdown menu with "3" selected.
- SNMPv3 Authentication Username:** A text input field containing "logicvein".
- SNMPv3 Authentication Password:** A password input field with masked characters ".....".
- SNMPv3 Privacy Password:** A password input field with masked characters ".....".
- SNMPv3 Authentication Protocol:** A dropdown menu with "SHA" selected.
- SNMPv3 Private Protocol:** A dropdown menu with "PrivDES" selected.
- SNMPv3 EngineID:** A text input field containing "0x:80:00:13:70:01:c0:a8:01:07:33:49:5e:fb".

At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Items	Explanation
Host	Enter the IP address or host name of the trap destination.
Port	Specify the trap destination port. (Initial value: 162)
Version	Specify the trap version from the following: 2c, 3
SNMP Community String	Enter the trap community name. (When selecting 1 or 2c at Version
(SNMPv3) Authentication Username	Enter the username used for user authentication.
(SNMPv3) Authentication Password	Enter the password of the user entered in Authentication Username.
(SNMPv3) Privacy Password	Enter your encryption password.
(SNMPv3) Authentication Protocol	Specify the authentication protocol from the following: SHA, SHA224, SHA256, SHA384, SHA512
(SNMPv3) Private Protocol	Specify the encryption protocol from the following: PrivDES, PrivAES128, PrivAES192, PrivAES256, Priv3DES, PrivAES256-3DES, PrivAES192-3DES
(SNMPv3) EngineID	Enter if you want to change the engine ID. (It will be filled in automatically)

## 6.12 Add columns/change column names for custom device fields

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

1. Click [Settings] on the global menu.
2. Click Custom Device Field.

Server Settings

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

Custom 1: Custom 1

Custom 2: Custom 2

Custom 3: Custom 3

Custom 4: Custom 4

Custom 5: Custom 5

+ Add

OK Cancel

3. If you want to change the column name, set the desired display name in the input field.
4. To add a column, click the Add button to add the column.

Server Settings

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

Custom 1: Custom 1

Custom 2: Custom 2

Custom 3: Custom 3

Custom 4: Custom 4

Custom 5: Custom 5

Custom 6: Custom 6

Custom 7: Custom 7

+ Add

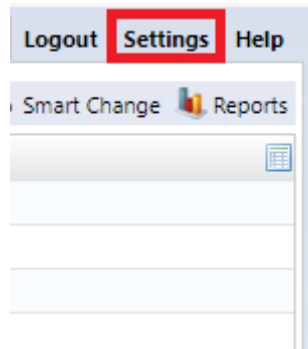
OK Cancel

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

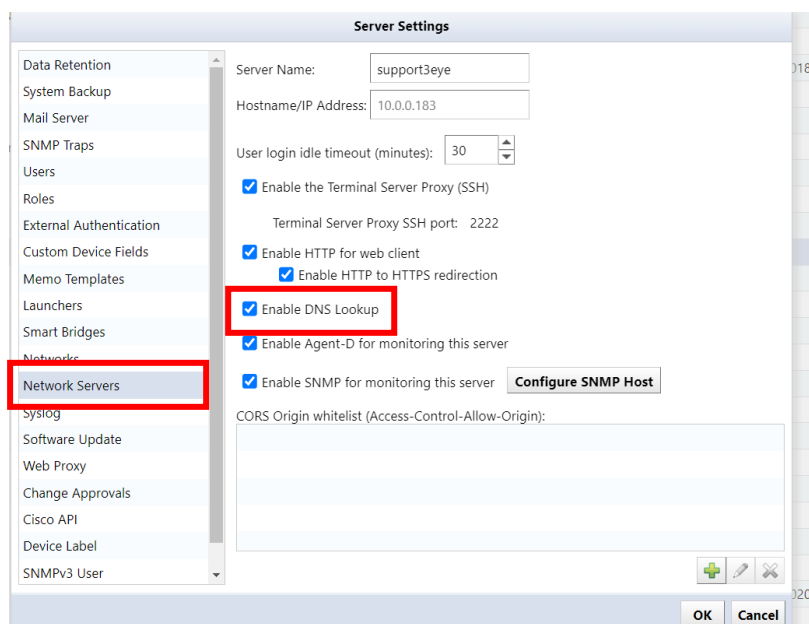
## 6.13 Use sysName for hostname

NetLD retrieves the hostname from your DNS server and displays it in the Devices tab. To use the host name (sysName) set on the device, make the following settings.

1. Click [Settings] on the global menu.



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



3. Click OK.



## 6.14 Advanced Syslog file settings

### 6.14.1 Set Syslog file retention period/size

Set the retention period for Syslog files.

1. Click [Settings] on the global menu.
2. Click [Syslog] and set each item.

**Server Settings**

**Syslog**

☒ Enable Syslog Server

☒ Enable realtime backup

Log size (MB)

Log count

Days to keep

Time Interval **None**

☐ DNS resolve the sender address

**Syslog Rules**

Filter	Action
Level : = Any	file : syslog.log

**OK** **Cancel**

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

3. Click OK.

## 6.14.2 Set up Syslog rules

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

To add a Syslog rule:

1. Click [Settings] on the global menu.
2. Click Syslog, then click + (Add) under Syslog rules.

The screenshot shows the 'Server Settings' window. On the left is a sidebar menu with various settings categories. 'Syslog' is highlighted with a red rectangle. The main area is divided into two sections. The top section, 'Server Settings', contains checkboxes for 'Enable Syslog Server' and 'Enable realtime backup', both of which are checked. Below these are input fields for 'Log size (MB)' (10), 'Log count' (2), 'Days to keep' (3), and a 'Time Interval' dropdown set to 'None'. There is also an unchecked checkbox for 'DNS resolve the sender address'. The bottom section, 'Syslog Rules', contains a table with two columns: 'Filter' and 'Action'. The first row has 'Level : = Any' in the Filter column and 'file : syslog.log' in the Action column. Below the table is a green plus icon in a red square, which is the 'Add' button, also highlighted with a red rectangle. At the bottom right are 'OK' and 'Cancel' buttons.

3. Configure Syslog Filter and Syslog Action.

The screenshot shows the 'Add Rule' window for configuring a Syslog Filter. The 'Syslog Filter' tab is selected. The 'Log Level' is set to 'Any' with a dropdown arrow. There is an unchecked checkbox for 'Include higher levels'. The 'IP Address' section has 'Single' selected with a radio button. Below this are input fields for 'Hostname' and 'Message'. The 'Time' section has 'From' and 'To' fields, each with hour and minute dropdowns. Below these are checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. At the bottom right are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Add Rule' window for configuring a Syslog Action. The 'Syslog Action' tab is selected. The 'Action' dropdown is set to 'Output to file'. Below this is a 'File Name' input field containing 'syslog', followed by '.log'. Below the file name is the text 'E.g. syslog.log'. The 'Split files by:' section has four radio button options: 'None' (selected), 'Log level', 'IP Address', and 'Time'. At the bottom right are 'OK' and 'Cancel' buttons.

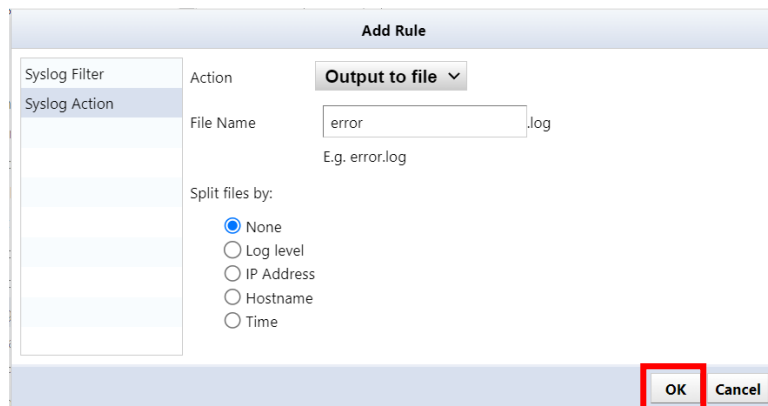
## Syslog filter

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

## Syslog action

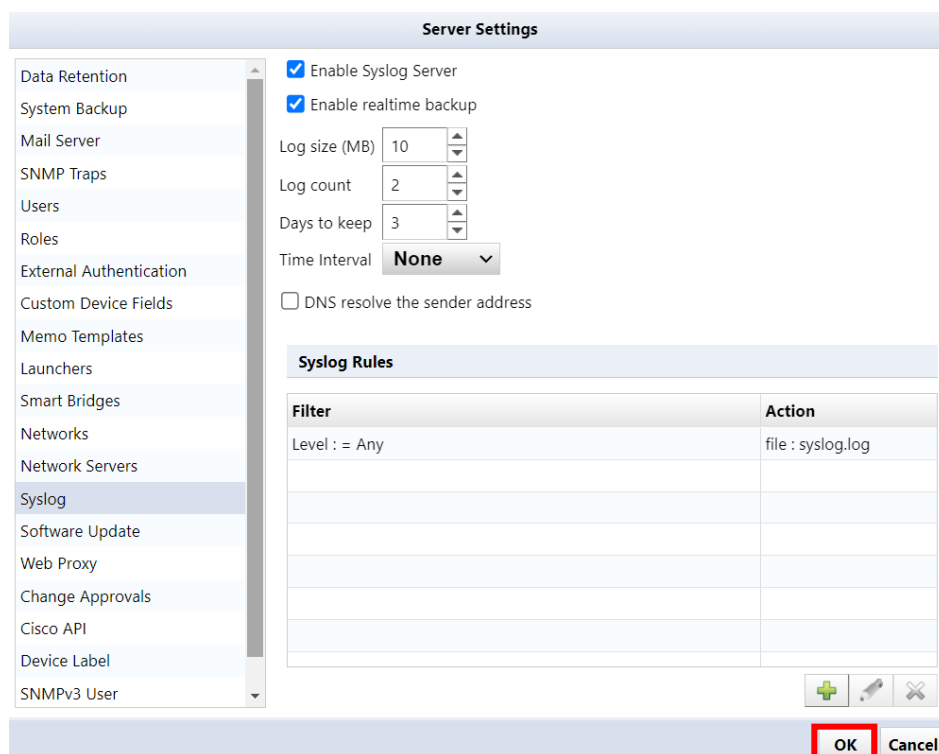
action	project	explanation
Output to file	File name	Specify the Syslog file name to output.
	Split files by	Divide the output Syslog file into specified units. None: Do not split Log Level: Divide by log level IP address: Divide by IP address or octet (1st, 2nd, 3rd) Hostname: Split by host name Time: Divide into selected time units
Forward	Transfer format	Select the transfer format from Syslog and SNMP.
	Target IP/Host name	Specify the forwarding destination.
	Port	Set the forwarding destination port number.
	Protocol	Select the transfer protocol from UDP or TCP. *Displayed when the transfer format is Syslog
	Spoofed source IP	*Displayed when the transfer format is Syslog
	Community	Specify the SNMP trap community. *Displayed when the transfer format is SNMP
Discard	—	Excludes the Syslog specified by the Syslog filter and will no longer log it to the Syslog file.

4. After setting, click [OK].



The 'Add Rule' dialog box is shown. It has a left sidebar with 'Syslog Filter' and 'Syslog Action'. The 'Action' dropdown is set to 'Output to file'. The 'File Name' field contains 'error' and '.log' is shown as a suffix. Below it, 'Split files by:' has radio buttons for 'None' (selected), 'Log level', 'IP Address', 'Hostname', and 'Time'. At the bottom right, 'OK' and 'Cancel' buttons are present, with 'OK' highlighted by a red box.

5. Click OK on the server settings screen.



The 'Server Settings' screen is shown. On the left is a sidebar with various settings categories, with 'Syslog' selected. The main area has checkboxes for 'Enable Syslog Server' and 'Enable realtime backup', both checked. Below these are input fields for 'Log size (MB)' (10), 'Log count' (2), and 'Days to keep' (3), along with a 'Time Interval' dropdown set to 'None'. There is also a checkbox for 'DNS resolve the sender address' which is unchecked. Below this is a 'Syslog Rules' section with a table:

Filter	Action
Level : = Any	file : syslog.log

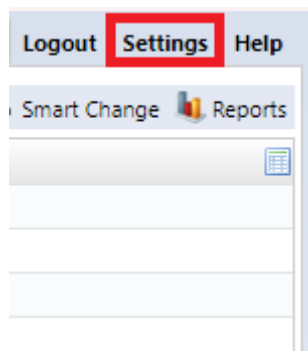
At the bottom right of the table are icons for adding, editing, and deleting rules. At the very bottom right of the screen, 'OK' and 'Cancel' buttons are present, with 'OK' highlighted by a red box.

### 6.14.3 Save syslog files to external storage

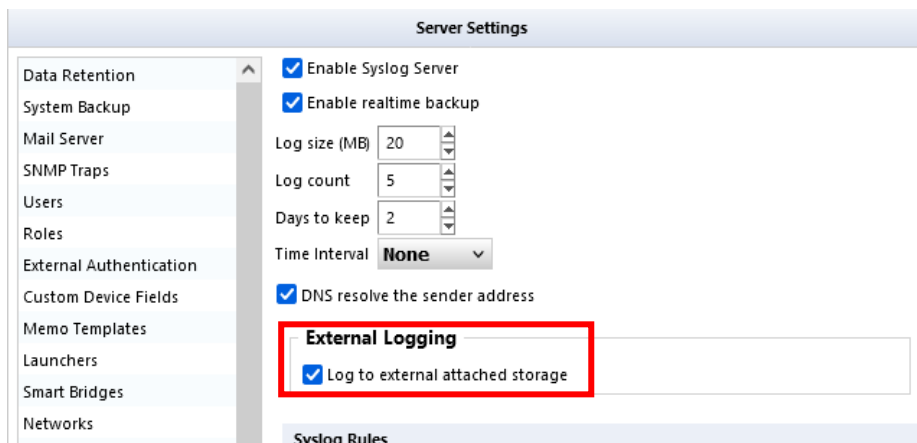
Normally, received Syslogs are saved to a local syslog.log file, but by linking with an NFS/SMB server, they can be saved to external storage.

**You must restart the NetLD appliance for this setting to take effect.**

1. Click [Settings] on the global menu.



2. Click [Syslog] and check "Logging to external storage".



**\*This "External logging" option is displayed when linked with an NFS/SMB server.**

3. Click OK.
4. Click OK on the reboot confirmation screen.

**\*NetLD must be restarted for the settings to take effect. Click OK and NetLD will automatically restart.**

#### Supplement

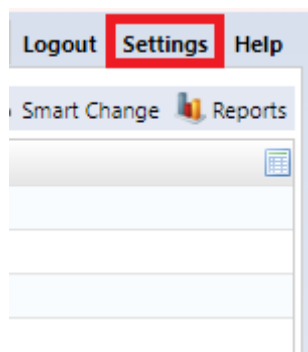
Changing the syslog.log file location from local to external storage copies the local file to external storage. On the other hand, changing the syslog.log file location from external storage to local does not copy the files on external storage locally.

This is not supported for security reasons.

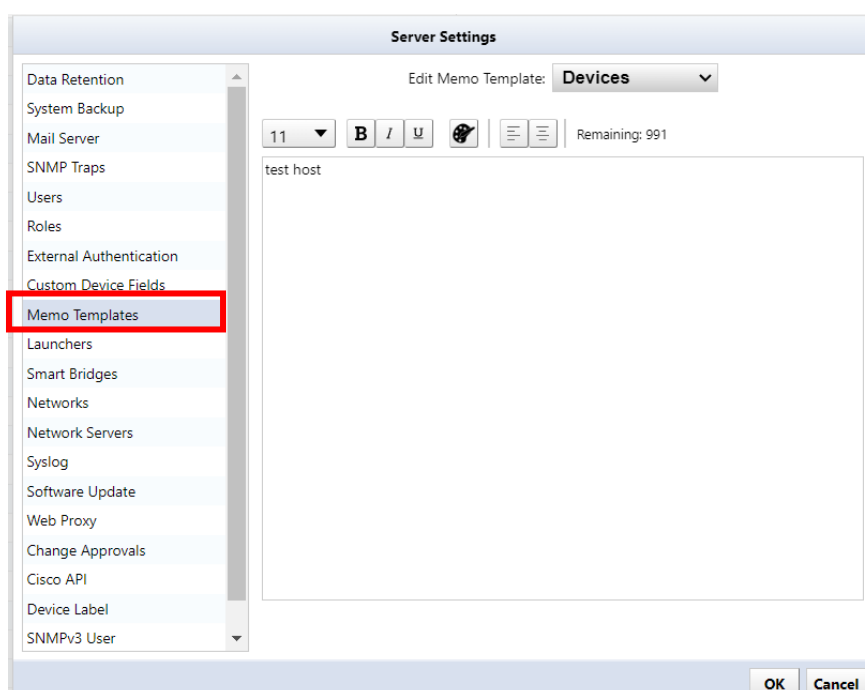
## 6.15 Edit a memo template

Memo template allows you to set a template that will be automatically inserted when creating a new device memo in the "Memo" column of the inventory.

1. Click [Settings] on the global menu.



2. Click [Memo Template]



Items	Explanation
Font size	Change font size.
Bold	Change the specified text to bold.
Italic	Change to italic.
Underline	Underline.
Text color	Change the font color.
Left alignment	Set the string alignment to left alignment.
Centered	Set text alignment to center.

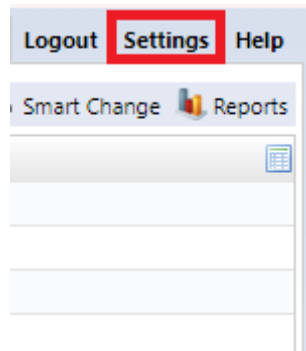
Items	Explanation
Number of input characters	Number of characters remaining that can be entered. *All characters are counted as one character, regardless of whether they are full-width or half-width.

3. Click OK.

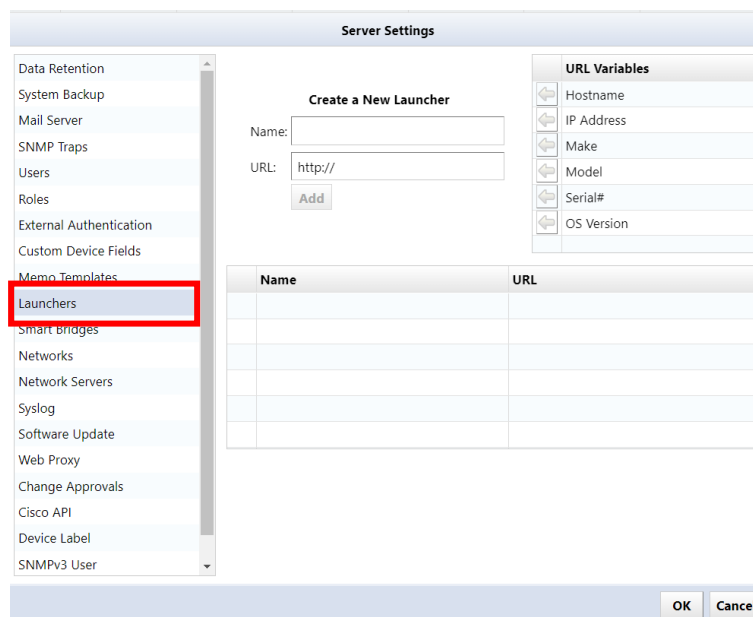
## 6.16 Add specific URL to right-click menu

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

1. Click [Settings] on the global menu.



2. Click [launcher]



3. Enter a name and specify the URL.

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

[URL variable explanation]

Items	Explanation	Example
Hostname	Quoting the device hostname.	If you select a device with host name=netLD.co.jp, the "{device.hostname}" part of the URL will be replaced with "netLD.co.jp" and executed. http://{device.hostname} ⇒ http://netLD.co.jp
IP address	Quote the device's IP address.	If you select a device with IP address = 192.168.0.1, the "{device.ipAddress}" part of the URL will be replaced with "192.168.0.1" and executed. http://{device.ipAddress} ⇒ http://192.168.0.1
Manufacturer	Quoting the manufacturer name obtained during configuration backup	http://{device.hardwareVendor}
Model	Quoting the model name obtained from the configuration backup	http://{device.model}
Serial number	Quoting the serial number obtained during configuration backup	http://{device.assetIdentity}
OS version	Quoting the software version obtained by config backup	http://{device.osVersion}

4. Click OK.

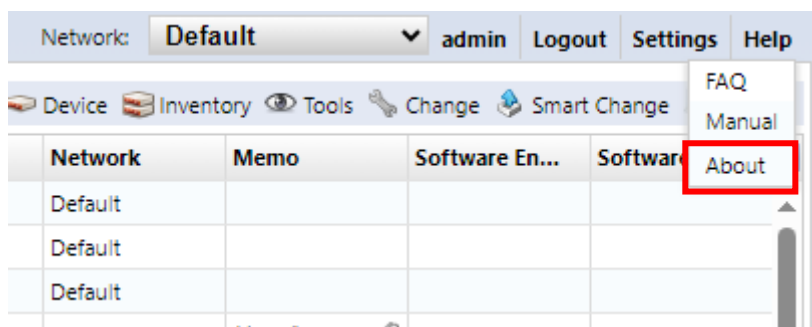


## 6.17 Update license

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

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

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



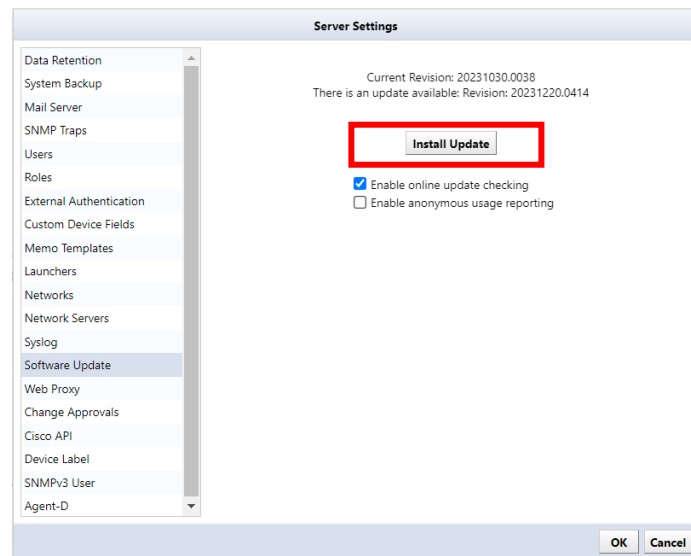
2. Click [Update License].



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

## 6.18 update online

NetLD 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.



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

## 6.19 Check revisions

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



You can also check from the virtual machine console.

```
LogicVein - Core Server
https://192.168.40.122

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

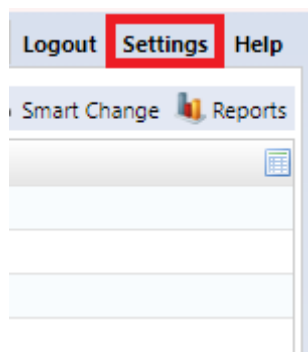
Revision : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

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

## 6.20 Use a proxy server

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

1. Click [Settings] on the global menu.



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

A screenshot of the 'Server Settings' dialog box. On the left is a list of settings categories, with 'Web Proxy' selected and highlighted in blue. The main area of the dialog is titled 'Web Proxy' and contains several input fields: 'Proxy type' (a dropdown menu set to 'Web Proxy'), 'Host' (text box with '192.168.40.200'), 'Port' (text box with '8080'), 'Realm' (text box with 'logicvein'), 'Username' (text box with 'thirdeye'), and 'Password' (text box with 'thirdeye'). At the bottom right of the dialog are 'OK' and 'Cancel' buttons. A red rectangular box highlights the 'Web Proxy' tab and its associated input fields.

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

## 6.21 Zero-Touch (optional)

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

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

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

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

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

NetLD Zero-Touch distributes configurations using the following protocols: Therefore, it is necessary to properly configure a firewall when using it.

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

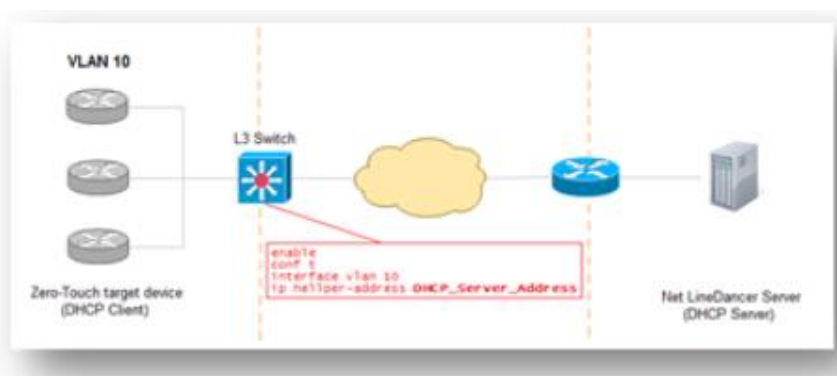


### 6.21.1 Zero-Touch requirements

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

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

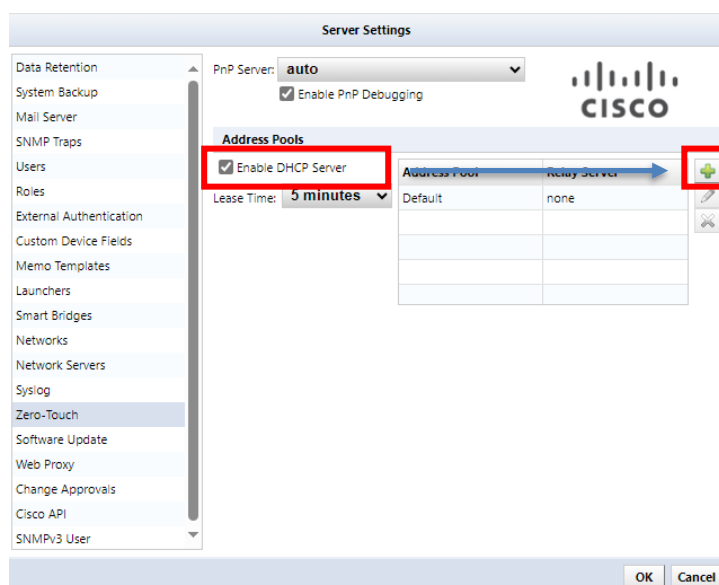
DHCP relay example



### 6.21.2 DHCP server

Open the settings window and enter the required information in the Zero-Touch section.

To set up a new DHCP pool Please press.



Items	Explanation
Enable DHCP server	Check this box if you want to use NetLD's DHCP server.
lease time	Set the DHCP lease time.

Please enter the necessary information and click OK button.

Add DHCP Pool

Pool Name:

Ivilogic

Relay Server CIDR:

192.168.0.254

/

32

Address Range:

10.0.0.100

-

10.0.0.105

Subnet Mask:

255.255.255.0

Overrides

Gateway:

10.0.0.254

DNS Server:

192.168.0.3

OK

Cancel

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

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

Address Pools

☒ Enable DHCP Server

Lease Time:

5 minutes

▼

Address Pool	Relay Server
Default	none
Ivilogic	192.168.0.254/32

+

✎

✕

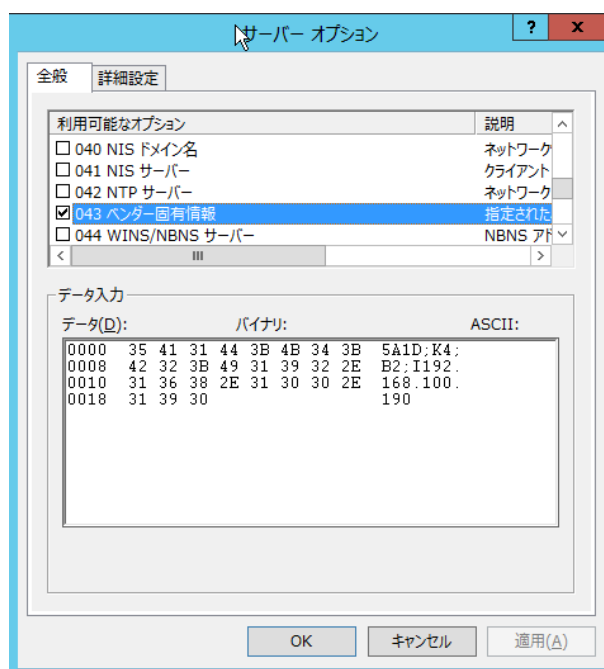
Click OK button.

### 6.21.3 Use an external DHCP server

If you use a DHCP server other than NetLD, you will need to add certain options in addition to the basic information to be able to communicate with NetLD. The options you add depend on the type of PnP.

Option 43 Option 43 allows you to add vendor-specific information.

The figure below is an example of a Windows DHCP server setting. Enter the information in the ASCII field, separating it with ";".



### 6.21.4 Distribution of configurations

#### 6.21.4.1 template

##### Creating a template

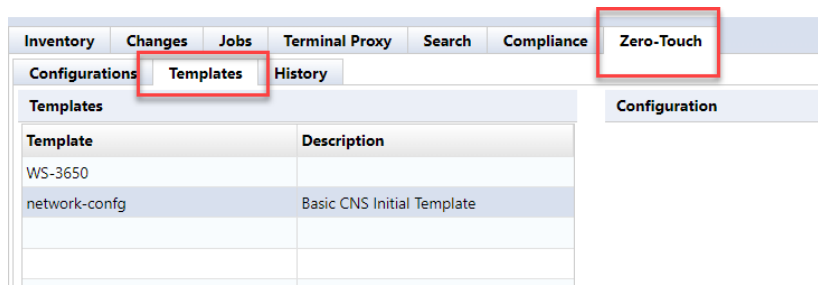
In large networks, there are often many devices with similar configurations. In other words, the only difference in the configuration is the IP address, host name, DNS, and syslog server address. In Smart Change, we used a template method to send similar commands by flexibly changing them to each device, but with Zero-Touch, the same template can be used not only for commands but also for configuration.

I've already explained how to use this template, so I won't go into details here. If you have not yet read that chapter, we strongly recommend that you do so to better understand the concept of templates.

Follow the steps below to create a template.

Go to Zero-Touch → Template tab, Press to create a template.



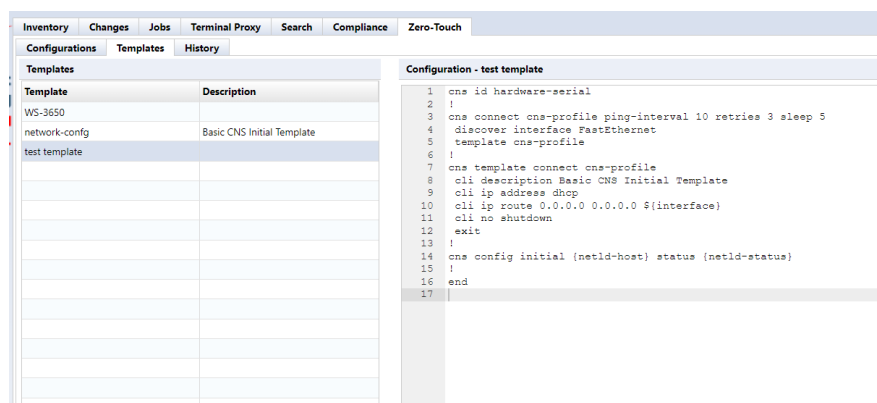


Select Dynamic Configuration as the template type and enter a name for the new template in the Template Name field. Optionally, you can write a description field. When finished, click the OK button.

A large text area will appear on the right side of the screen. Please enter the original configuration in this area. If you already have a device in your inventory of the same model as the one you plan to perform Zero-Touch on, you can change that device's configuration (e.g.start-up config) and paste it here.

The subsequent operations are as follows.[7.10 Bulk change overview.](#)

Once you have added all the required variables, you need to save your template. Click the button labeled Save at the top right of the text area to save the template you created.

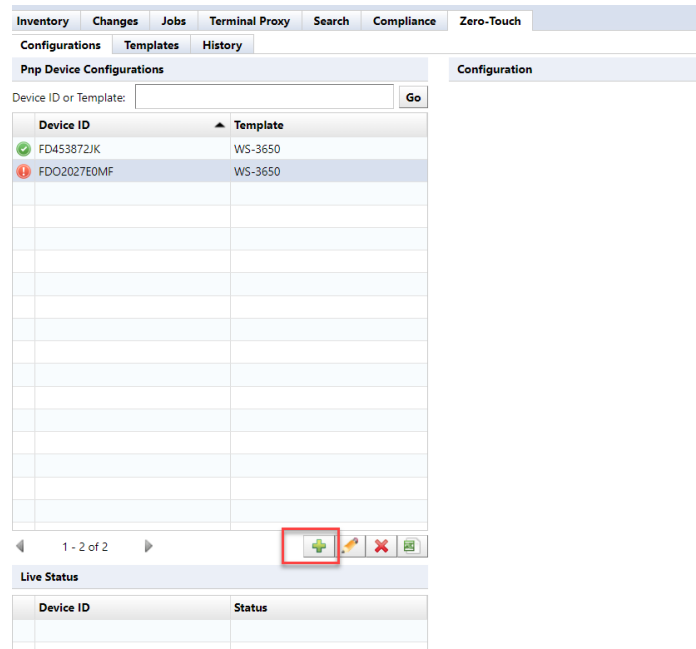


If you do not want to save the deployed configuration on the device, add no-persist option at the end of cns config initial... at deploying configuration.

## Device registration

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

First, move the main pane to the configuration subtab. Click + for Zero-Touch device configuration.



## Importing values from outside into template variables

Tables written externally in Excel files can be used as template values. To perform the import, please follow the steps below:

While working with Zero-Touch, click the Close button when entering alternative values for the device.

Click the import button to display the submenu.

Select Export import file or Export template from the menu that appears.

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

Edit the output file and input the values of the template variables in order. Don't forget to save after entering.

[illegible]

Return to NetLD, click again and select "Import Template" from the menu that appears.

[illegible]

### 6.21.4.2 Zero-Touch self-recovery

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

The required work is similar in many respects to Zero-Touch, which uses templates.

First, go to the Configuration subtab in the main pane. Then press + button.

Device ID	Template
FD453872JK	WS-3650
FDO2027E0MF	WS-3650

Enter the necessary information in the device configuration dialog. When finished, click OK button. However, in the distribution type section, select the self-recovery option.

PnP Device Configuration

Device ID: FHK104780MN

Deployment Type: Self-Recovery

OK Cancel

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

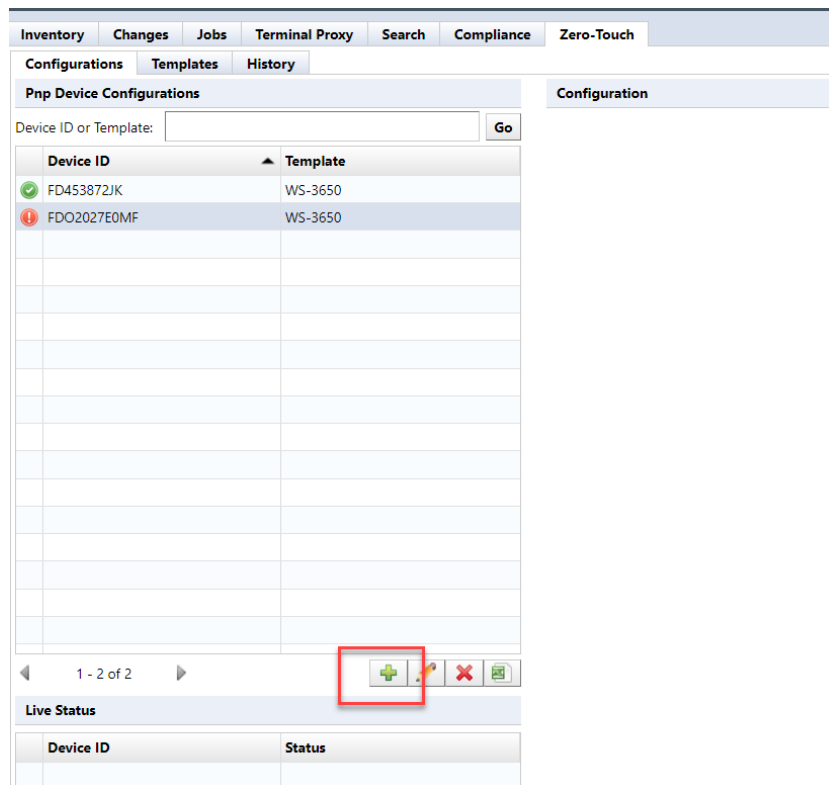
### 6.21.4.3 Zero-Touch Specific Device Restore

This feature is used when replacing an old device with a new device. Thanks to this feature, even if your device is broken and no longer works properly, you can connect a new device to the same location and restore it. When you run Zero-Touch in this mode, the configuration from your old device will be written to your new device.

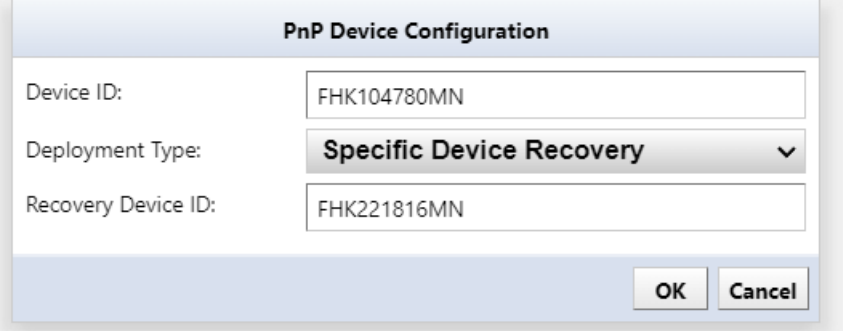
This feature is extremely useful when the device is located far away (e.g. in another data center) and there is no one on site to operate it directly. With Zero-Touch, all you have to do is tell someone at the local data center to plug in the cable over the phone, and the local person doesn't need any special skills. This is because subsequent operations such as device restoration are performed over the network rather than locally.

Similar to self-recovery, the specific device restore function can be performed in much the same way as the Zero-Touch template function.

First, open the configuration subtab on the main pane and click the + button displayed there.



Enter the required information within the Zero-Touch device configuration dialog. Select the specific device restore feature as the distribution type. After completion, click the OK button.

A screenshot of a 'PnP Device Configuration' dialog box. It has a light blue header with the title 'PnP Device Configuration'. Below the header, there are three input fields. The first is 'Device ID:' with the value 'FHK104780MN'. The second is 'Deployment Type:' with a dropdown menu showing 'Specific Device Recovery' and a downward arrow. The third is 'Recovery Device ID:' with the value 'FHK221816MN'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

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

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

#### 6.21.5 Precautions when handling newly introduced devices

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

## 7: System backup/restore

A system backup is a backup of the entire NetLD. You can backup/restore various settings. Perform a system backup from [Settings] → [System Backup].

### 7.1 Perform system backup automatically

The setting to automatically perform system backups is disabled by default. If you want to enable it or change the time for automatic system backup, change the contents in the red frame below.

Server Settings

☐ Enable daily system backup

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

Number of backups to keep: 1

[Perform System Backup Now](#)

Last successful system backup performed: 2024/05/14 18:16 ([Download](#))

[Restore System Backup](#)

OK Cancel

Items	Explanation
Enable daily system backups	Enable daily system backups. If this setting is enabled, a system backup will be performed at the specified time. (Initial value: Disabled)
Run daily system backups at	Specify the execution time for daily system backups. (Initial value: 7:00)

## 7.2 Perform a manual system backup

If you want to perform a system backup for changing settings, etc., click [Perform System Backup].

The screenshot shows the 'Server Settings' dialog box with the 'System Backup' tab selected. On the left is a vertical list of settings categories: Data Retention, System Backup, Mail Server, SNMP Traps, Users, Roles, External Authentication, Custom Device Fields, Memo Templates, Launchers, Networks, Network Servers, Syslog, Software Update, Web Proxy, Change Approvals, Cisco API, Device Label, SNMPv3 User, and Agent-D. The 'System Backup' section is active and contains the following elements: a checked checkbox for 'Enable daily system backup'; a time selection field set to '16 : 0'; a dropdown menu for 'Number of backups to keep' set to '1'; a red-bordered button labeled 'Perform System Backup Now'; and a text field showing 'Last successful system backup performed: 2024/01/08 16:02' with a blue '(Download)' link. Below this section is a 'Restore System Backup' button. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

The button is grayed out while a backup is in progress. Once the grayed out is removed and the latest system backup date and time is updated, the process is complete.

This screenshot is identical to the one above, but the 'Perform System Backup Now' button is no longer grayed out and is highlighted with a red border. The text 'Last successful system backup performed: 2024/01/08 16:02' and the '(Download)' link remain the same.



### 7.3 Change the number of system backups retained

Select the number of generations to keep system backups from the list. From the revision 20240131.0729, the number of system backup to keep has been changed to 1 in case of local storage setting. In the case of external storage setting, you can set, "1,7,14,30 generations" of system backups are retained as files, and old data that exceeds the number of generations is deleted.

Although it depends on the operating environment, it accumulates as the operation period becomes longer. As the data grows and the system backup itself up, sizes tend to increase. Therefore, if you keep a large number of system backups, system backups can take up disk space. Disk usage can be reduced by reducing the number of system backup generations to be retained.

The screenshot displays the 'Server Settings' window. On the left is a sidebar with a list of settings: Data Retention, System Backup (selected), Mail Server, SNMP Traps, Users, Roles, External Authentication, Custom Device Fields, Memo Templates, Launchers, Networks, Network Servers, Syslog, Software Update, Web Proxy, Change Approvals, Cisco API, Device Label, SNMPv3 User, and Agent-D. The main area shows the 'System Backup' configuration. It includes a checkbox 'Enable daily system backup' which is checked. Below it, a time picker is set to '16 : 0'. A dropdown menu 'Number of backups to keep' is open, showing a list with '1' selected, and other options '7', '14', and '30'. To the right of the dropdown is a button 'Run System Backup Now'. Below that, it says 'Last successful system backup performed: 2024/01/08 16:02' with a '(Download)' link. At the bottom center is a button 'Restore System Backup'. At the bottom right are 'OK' and 'Cancel' buttons.

## 7.4 Save to external storage

By default, system backup files are stored inside the virtual appliance, but you can configure external storage to automatically store them outside the virtual appliance. Supported protocols are NFS/SMB.

To set up external storage, do the following:

1. Press the 5 key on your keyboard and select Admin Tools.

```
LogicVein - Core Server

https://192.168.40.122

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

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

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

2. Press the "4" key on your keyboard and select "Configure a remote filesystem for backups".

```
Admin Tools menu:
-----
[1] Run Config Diff Cleanup
[2] Vacuum Database
[3] Reset Admin Password
[4] Configure a remote filesystem for backups
[5] Reset Admin Dashboard API Token
[6] Configure Built-in Agent-D
```

3. Select the server type.

```
Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server
-
```

4. Enter the required information and press Enter.

```
Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server

Remote NFS path: _
```

Item	Explanation
Remote NFS/SMB path	Network path/IP address
Username	Username set on the server *For SMB only
Password	Password set on the server *For SMB only

5. Select:

```
Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server

Remote NFS path: 10.0.111.1:/datastore

Validating configuration...

Saving configurations...

Configurations verified successfully. Do you want to?

[1] Copy existing backups to the NFS/SMB and delete
[2] Delete existing backups
```

Item	Explanation
[1] Copy existing backups to the NFS/SMB and delete	Copy existing backups to NFS/SMB and then delete them
[2] Delete existing backups	Delete existing backups

The console screen settings are now complete. After NetLD restarts automatically, you can check the settings on the console screen.

LogicVein - Core Server

https://192.168.40.122

Networking:

IP Address: 192.168.40.122 Netmask: 255.255.255.0  
Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3  
Hostname: netld Interface: eth0  
NTP Server: pool.ntp.org SSH Server: running  
Time: 2021-03-24 02:46 UTC Backup: 10.0.111.1:/datastore  
IPv6 Addr: fd14:5839:664d:40:20c:29f6:f6b6:baf9  
MAC Addr: 00:0C:29:B6:BA:F9

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

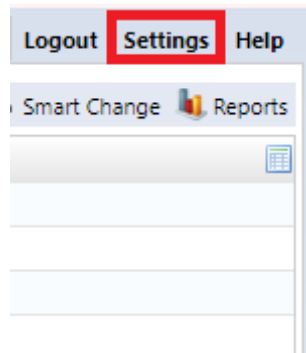
Settings menu:

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

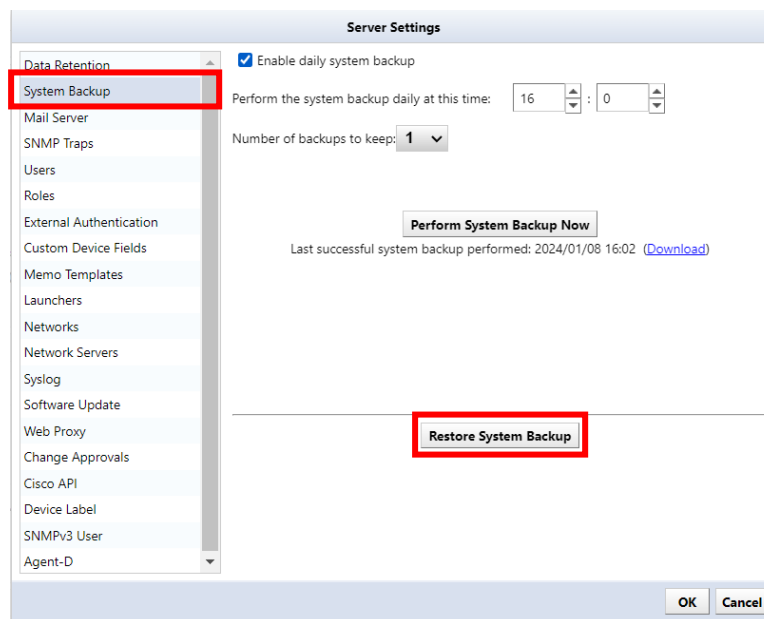
## 7.5 Restore system backup

To restore, select the backup source and restore destination. **Same version (revision)** Must be. For information on how to check the version.

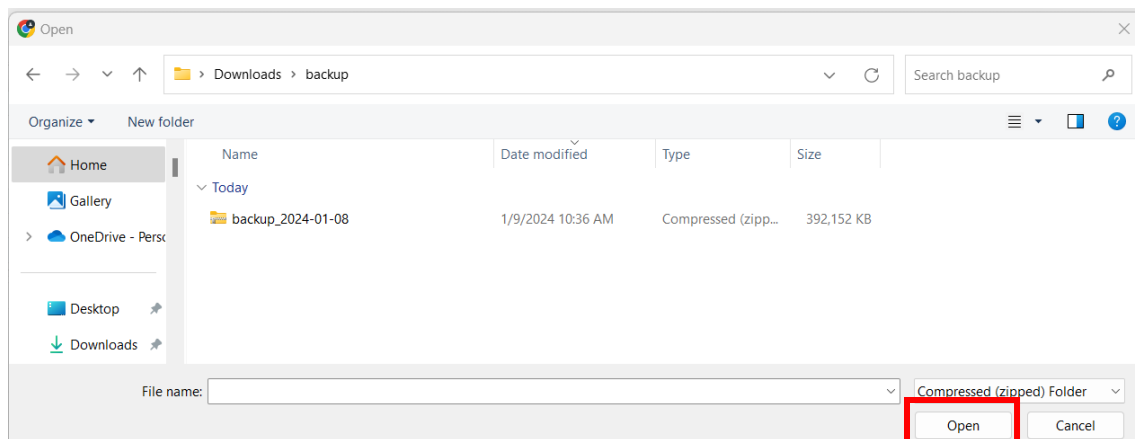
1. Log in as a user with administrator privileges.
2. Click Settings.



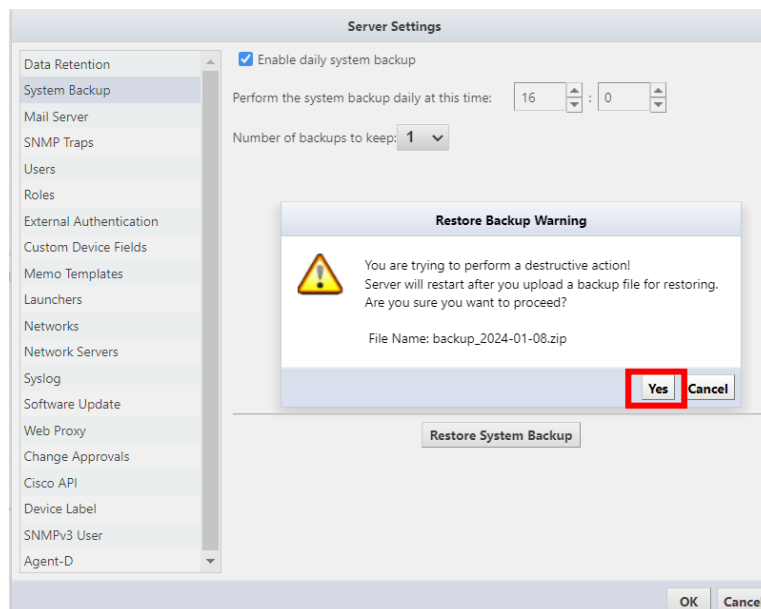
3. From System Backup, click Restore System Backup.



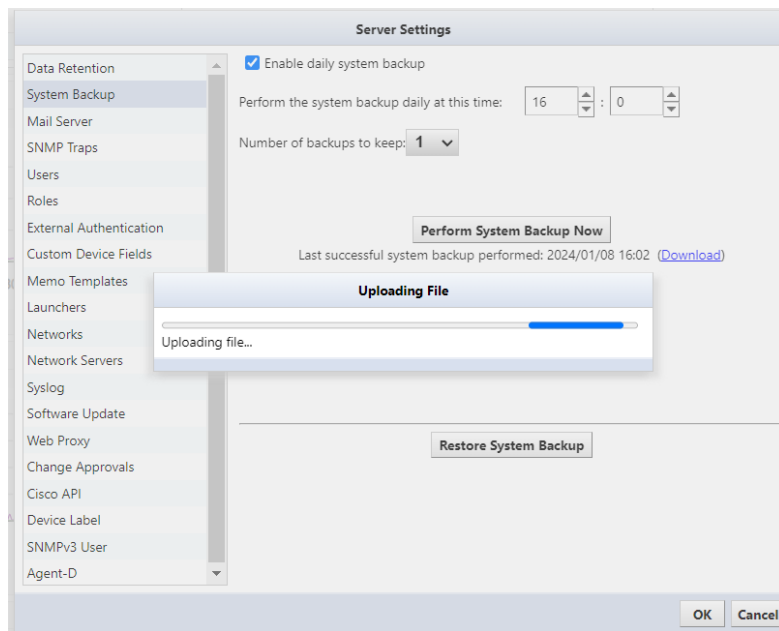
4. Select the file you want to restore and click Open.



5. Click [Yes] on the warning screen.



- The file will be uploaded, and the restoration will begin.



That's all for the operation. After uploading, the service will automatically restart and return to the login screen.

## 8: Reboot/Shutdown

Reboot and shutdown operations are performed using the keyboard on the virtual machine console.

```
LogicVein - Core Server
https://192.168.40.122

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

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

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

To restart, press the "6" key on your keyboard, choose **[Reboot]**.

To shut down, press the "7" key on your keyboard, choose **[Power Off]**.

After selecting the menu, a confirmation message will be displayed, so press the "Y" key on your keyboard to execute.

### 【Reboot】

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

### 【Power Off】

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

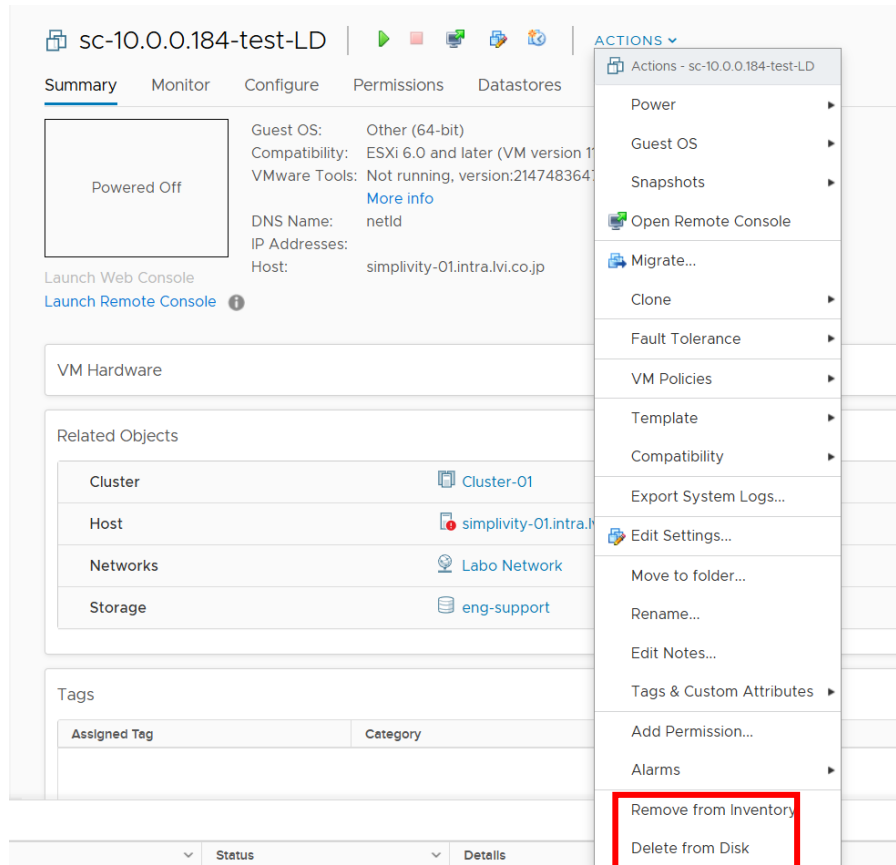


## 9: Uninstall

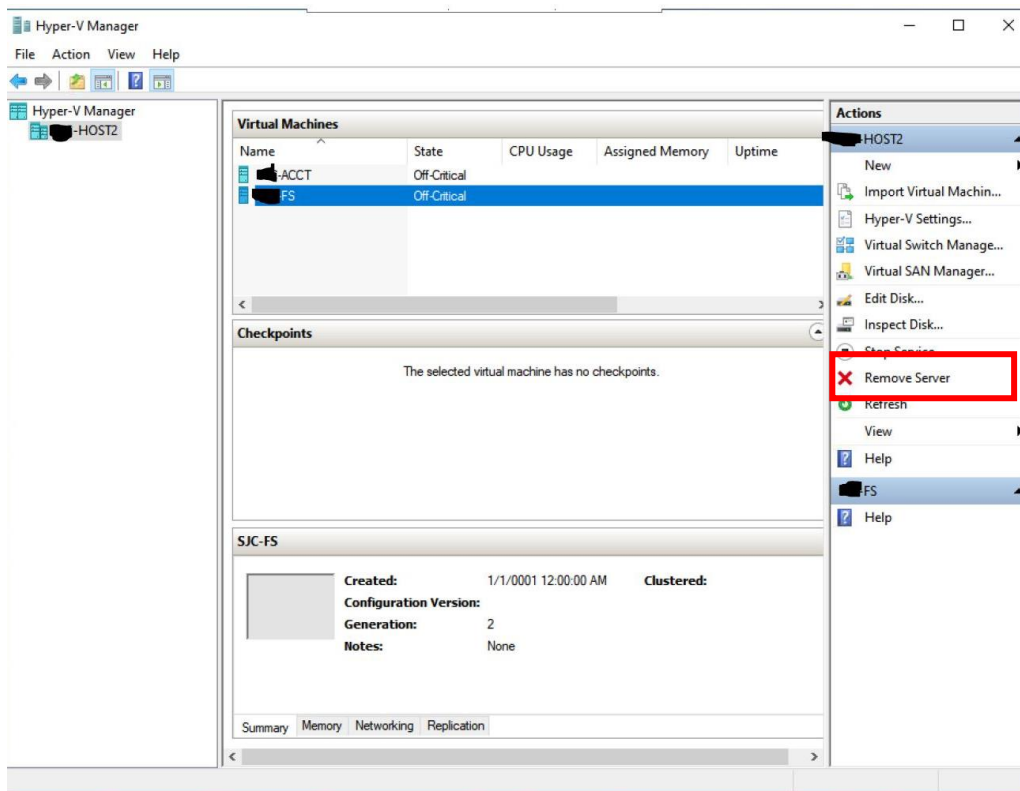
### 9.1 uninstall

1. Shut down NetLD.
2. After the shutdown is complete, delete the NetLD virtual machine from the virtual host OS.

Deletion screen in VMware ESXi (example)



Deletion screen in Windows Hyper-V (example)



This completes the uninstallation of NetLD.

## 10: Inquiry

If you have any problems or questions while using NetLD, please contact our support below.

Before contacting us, please check the following requirements.

### 【Required items】

1. Product name
2. Product revision information
3. Product serial number (NetLD license information)
4. Specific symptoms and questions (If you send us a screenshot, we can share information more smoothly and may be helpful in resolving the issue.)

Contact information

LogicVein Support Desk

Email: [support@logicvein.com](mailto:support@logicvein.com)

## 11: Ending material

### 11.1 Smart Bridges (Optional)

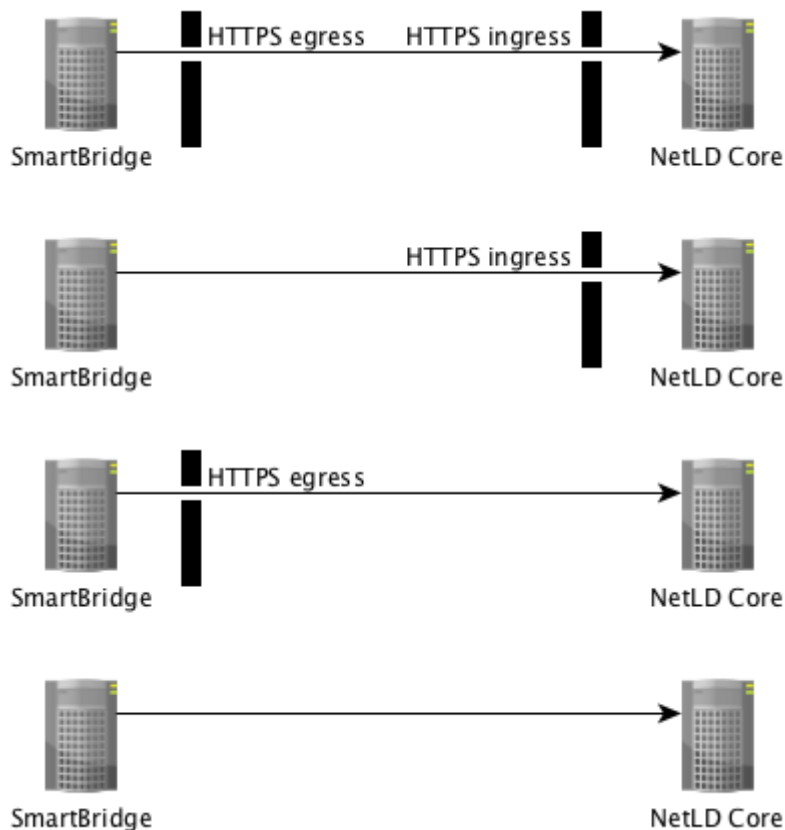
ThirdEye supports two modes for the connection of Smart Bridges to the core server: *Bridge-to-Server* and *Server-to-Bridge*. All connections are via HTTPS, so wire traffic is encrypted end-to-end.

#### Bridge-to-Server

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

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

The following diagram shows various scenarios in which firewalls are present in one network, in both networks, or not present.

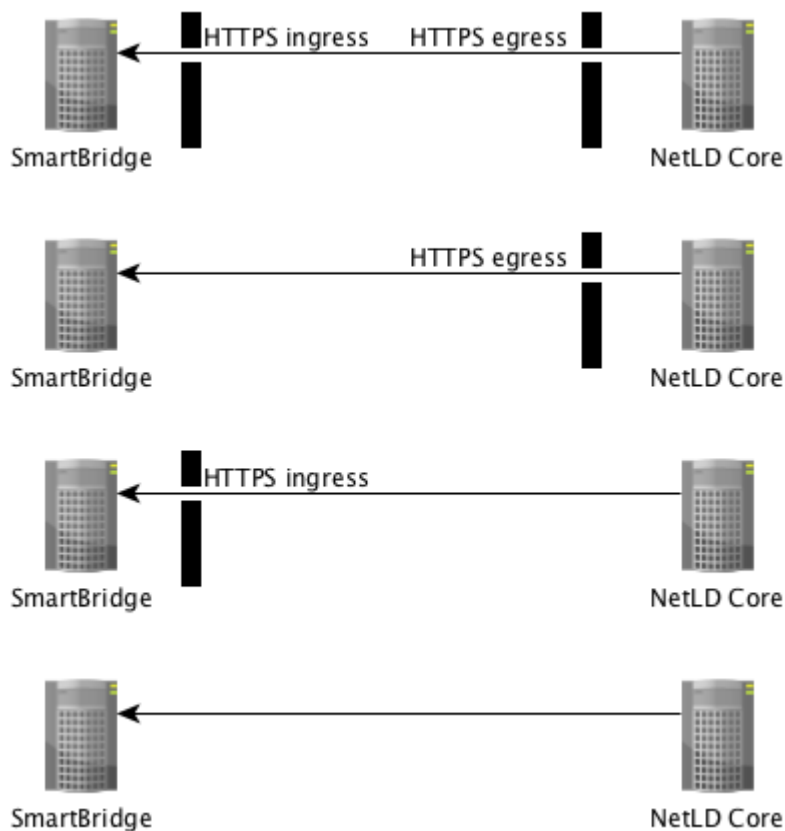


## Server-to-Bridge

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

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

The following diagram shows various scenarios in which firewalls are present in one network, in both networks, or not present.



## Connection Token

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

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

If SmartBridge is configured to use Server-to-Bridge mode, users can choose not to use Tokens. However, not using Tokens is not desirable for security reasons and we strongly recommend using it.

### 11.1.1 SmartBridge Installation

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

Example :

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

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

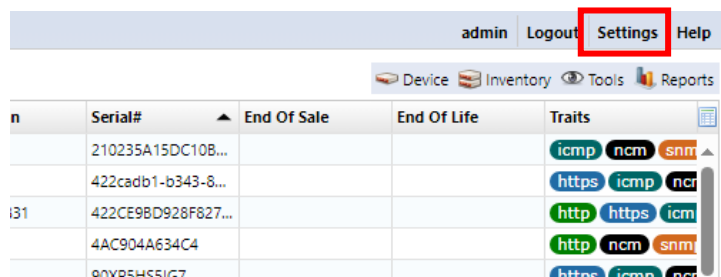
For installation instructions, see エラー! 参照元が見つかりません。 エラー! 参照元が見つかりません。 .

After installation, you can also configure the network by referring to エラー! 参照元が見つかりません。 エラー! 参照元が見つかりません。 .

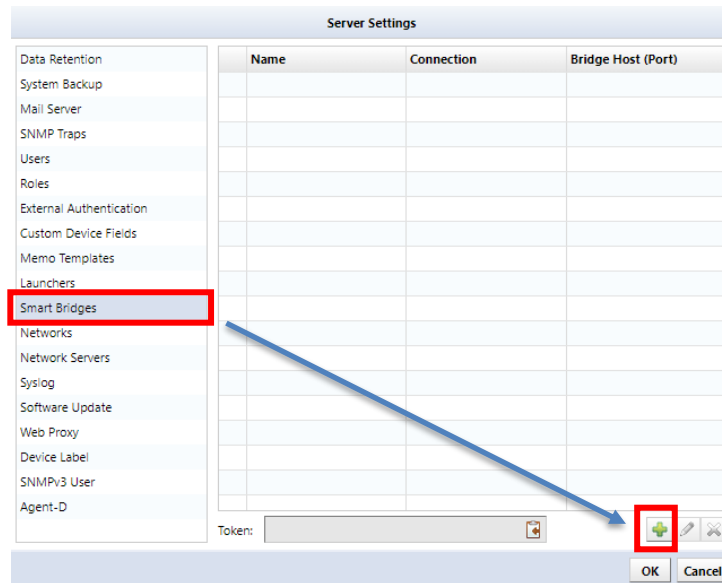
### 11.1.2 Add SmartBridge to core server

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

1. Login to the core server as an Administrator role use and click [Settings].



2. Select the Smart Bridges category on the left-hand side of the settings dialog and click [+] button to add a new Smart Bridge



3. Enter the name for the bridge

Bridge Host

Name:

Connection: **Bridge→Server**

OK Cancel

4. Select Connection. When you select “Server to Bridge”, you have to enter IP address and port of bridge.

Bridge Host

Name:

Connection: **Bridge→Server**

OK Cancel

Bridge Host

Name:

Connection: **Server→Bridge**

Host or IP:

Port:

OK Cancel

5. Click OK
6. Copy token.

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





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

```
SmartBridge Direction:
-----

Configure the direction of the SmartBridge connection initiation. Choose from
the following options:

(B) Bridge initiated [bridge->server]. Requires authentication token.
(S) Server initiated [server->bridge]. Requires authentication token.
(A) Server initiated [server->bridge]. First connection assigns token.

Bridge initiated or server initiated (B/S/A) [default: B]: B
Remote LogicVein Server hostname or IP address: 192.168.30.19
Remote LogicVein Server port [default: 443]: 443
SmartBridge authentication token (32 characters): 93af38583e0f6bfe108f9698e833cf_
```

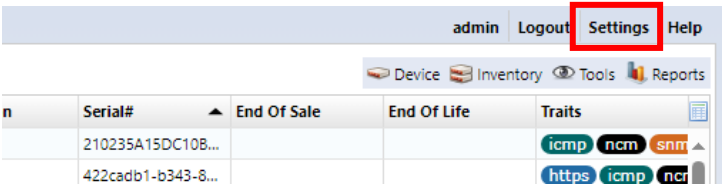
project	explanation	Input example
Connection initiation.	Connection direction	B
	B: Connect from Bridge to Server (with token)	S
	S: Connect from Server to Bridge (with token)	A
	A: Connect from Server to Bridge (without token)	
Hostname or IP address	Core server (ThirdEye) IP address	192.168.30.19
Port	Core server (ThirdEye) HTTPS port	443
Token	Token generated during SmartBridge registration	

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

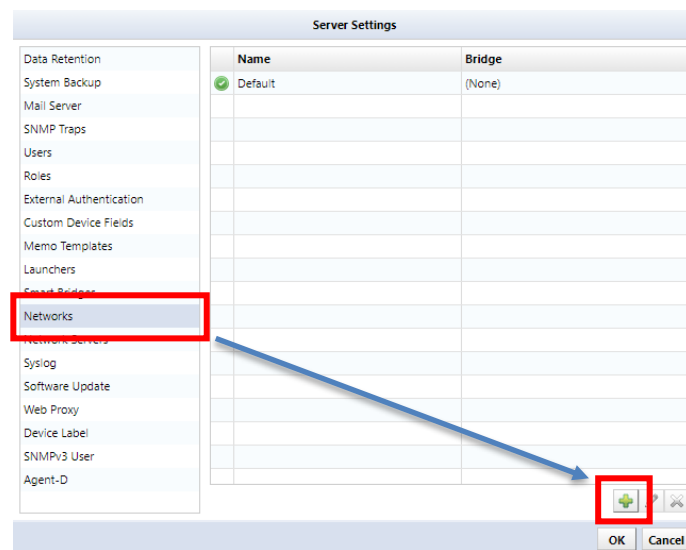
11.1.4 Managing Devices via SmartBridge

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

1. Click [Settings].



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



3. Enter a name for your network and select Smart Bridge in the Bridge Host.

The screenshot shows the 'Managed Network' dialog. The 'Name' field is set to 'SmartBridge Network' and the 'Bridge Host' dropdown is set to 'SmartBridge'. These two fields are highlighted with a red rectangle. Below them are several other fields: 'IP Address', 'Username', 'Password', 'Override Port' (checked), 'Adapter' (set to 'Cisco IOS'), 'Max Connections' (set to 0), 'Use return address for FTP/TFTP' (checked), and 'NAT Address'. At the bottom right are 'OK' and 'Cancel' buttons.

4. Click OK

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

