LogicVein

User's Manual

Contents

Revision History

Edition	Revision Date	Contents
Rev.1	2/3/2019	First edition issued
Rev.2	8/4/2019	Revised explanations and images as functions
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
Rev.9	1/6/2025	Added new functions: HA

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 do the following:

- 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

Net LineDancer is an integrated and cloud ready solution that contains reporting, automation, and integration tools. Its Network Configuration and Change Management (NCCM) capabilities are suitable for large enterprise data centers.

1.2.1 NetLD Enterprise features:

NetLD Enterprise contains the following features:

- **Discovery Monitoring**
  - Configuration backup
  - Generational management
  - Compare
  - Export
- **Configuration Change**
  - Configuration backup
  - Generational management
  - Compare
  - Export
- **Terminal Proxy / Auto Login**
  - Telnet/SSH connection

  - Operation History Change
- **Job**
- **Compliance**
- **Report**
- **Zero-touch (optional)**
- **HA (Active/Standby) (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:

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

*Both thin and thick HDD provisioning types are supported.

1.4 List of ports used

The ports that 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.

Feature	**Port**	Protocol	UDP/TCP	Communication Direction
Zero-Touch	**67**	DHCP	UDP	NetLD ← Destination
	68	DHCP	UDP	NetLD → Destination
	80	HTTP	TCP	NetLD ← Destination
	69	TFTP	UDP	NetLD ← Destination
	-	ICMP	-	NetLD ← Destination
Automatic Discovery	**22, 23**	SSH, Telnet	TCP	NetLD → Destination
	161	SNMP	UDP	NetLD → Destination
	-	ICMP	-	NetLD → Destination
Send Settings (Restore Configuration)	**22, 23**	SSH, Telnet	TCP	NetLD → Destination
	69	TFTP	UDP	NetLD ← Destination
	20, 21	FTP	TCP	NetLD ← Destination
Settings Using Modification Tools	**22, 23**	SSH, Telnet	TCP	NetLD → Destination
Trap Sending	**162**	SNMP	UDP	NetLD → Destination
SNMP Monitoring	**161**	SNMP	UDP	NetLD → Destination
Trap Reception	**162**	SNMP	UDP	NetLD ← Destination
Real-time change detection	**514**	Syslog	UDP	NetLD ← Destination
Backup*	**22, 23**	SSH, Telnet	TCP	NetLD → Destination
	161	SNMP	UDP	NetLD → Destination
	69	TFTP	UDP	NetLD ← Destination
	20, 21	FTP	TCP	NetLD ← Destination
Terminal proxy	**2222, 443**	SSH or HTTPS	TCP	NetLD ← Client PC
	22, 23	SSH, Telnet	TCP	NetLD → Destination
Web Terminal	**443**	HTTPS	TCP	NetLD ← Client (GUI)
	22, 23	SSH, Telnet	TCP	NetLD → Destination

Feature	**Port**	Protocol	UDP/TCP	Communication Direction
Client	**443**	HTTPS	TCP	NetLD ← Client (GUI)
External authentication function	**389**	LDAP	TCP	NetLD → Authentication server
	1812	RADIUS	UDP	NetLD → Authentication server

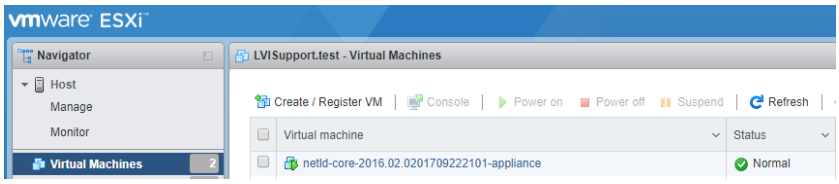
*The appropriate settings for the protocol you use will depend on the type of device you are using. For example, for IOS devices, “CLI (Telnet, SSH) only or both CLI and TFTP”

2 Installation

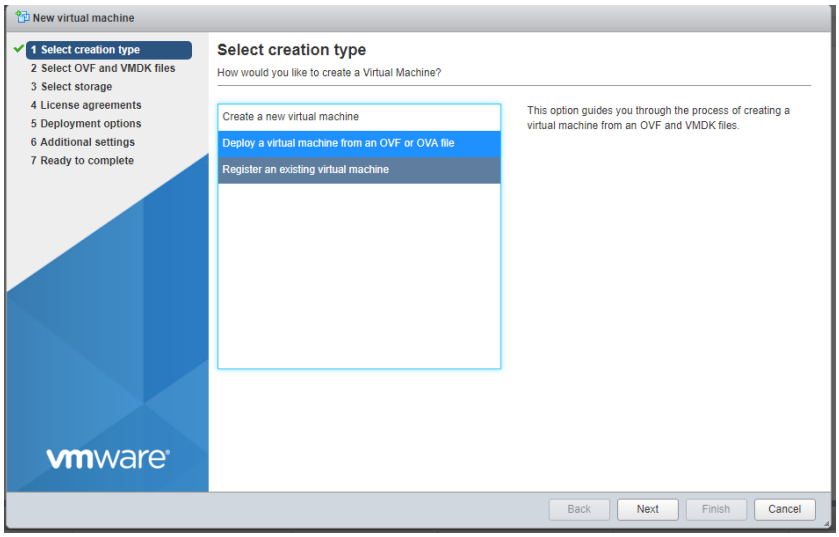
2.1 Deployment to VMware ESXi

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

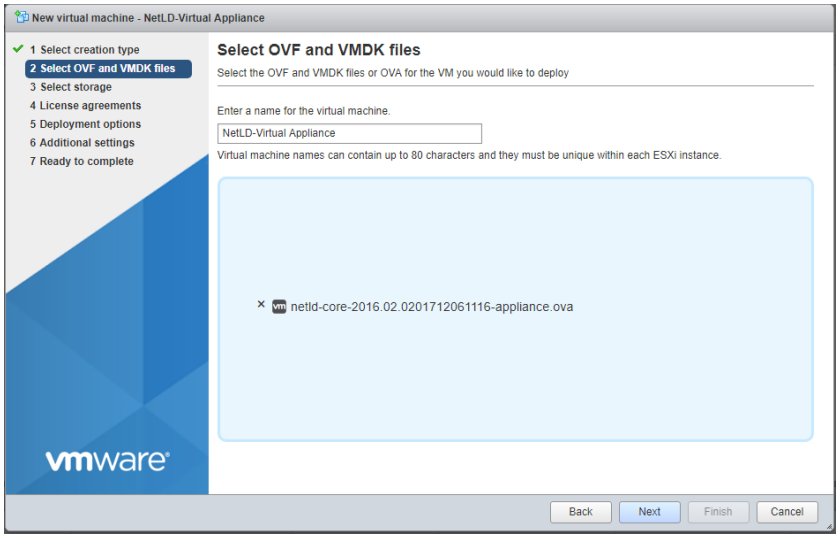
1. Log in to the Web UI and click [Create/Register Virtual Machine] from the virtual machine.



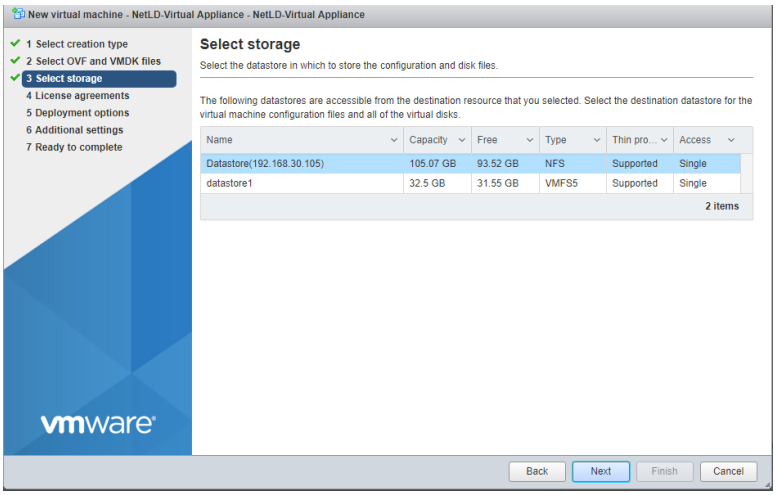
2. Select “Deploy a virtual machine from an OVF or OVA file” and click [Next].



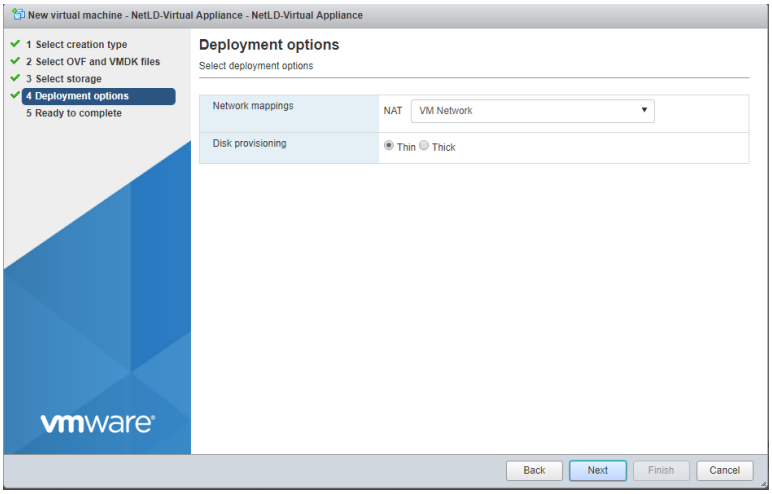
3. After entering the desired virtual machine name, drag and drop the OVA file “lvi-core-****-appliance.ova” and click [Next].



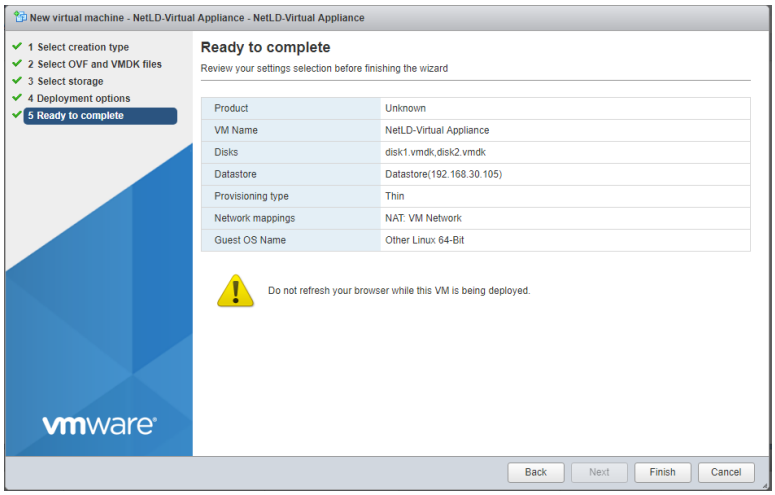
4. Select your storage and click [Next].



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



6. Click [Finish].



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

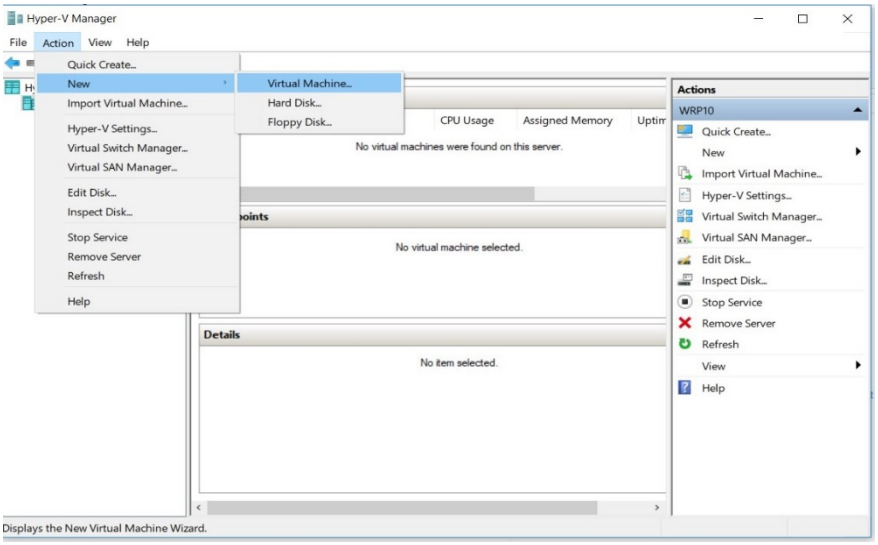
2.2 Deployment to Windows Hyper-V

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

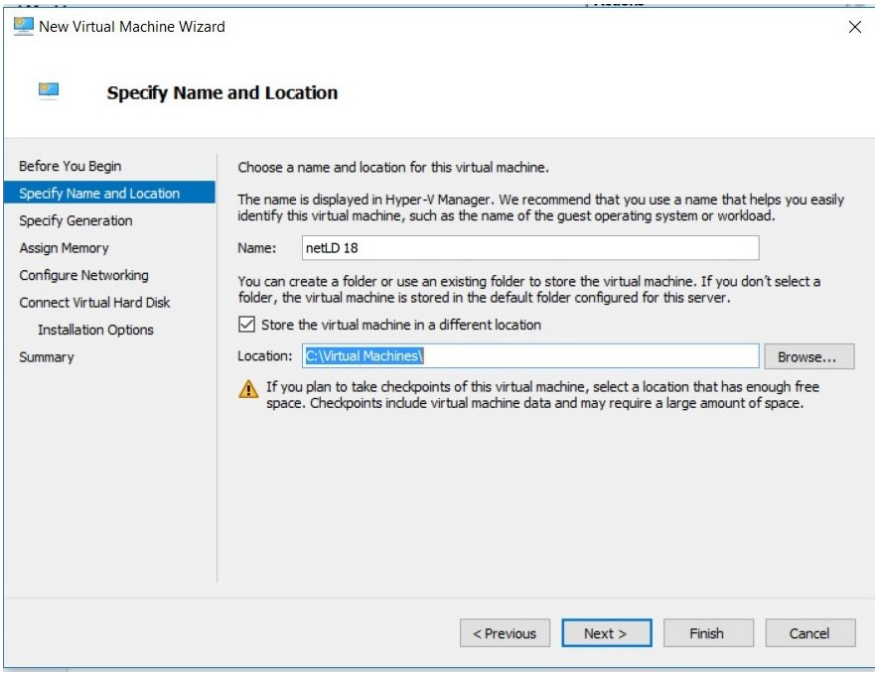
Prerequisites

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

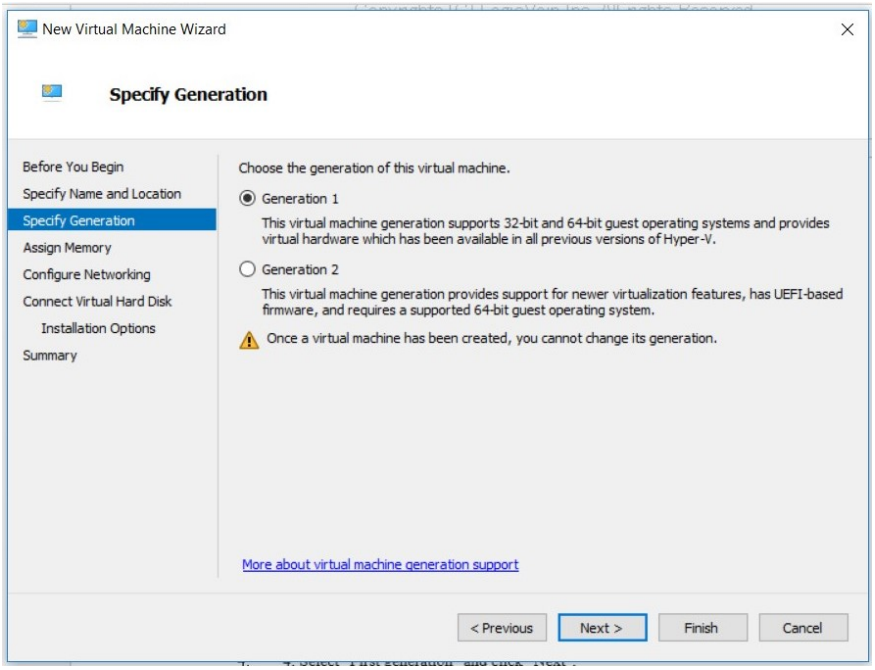
1. Start Hyper-V Manager and click [New] > [Virtual Machine].



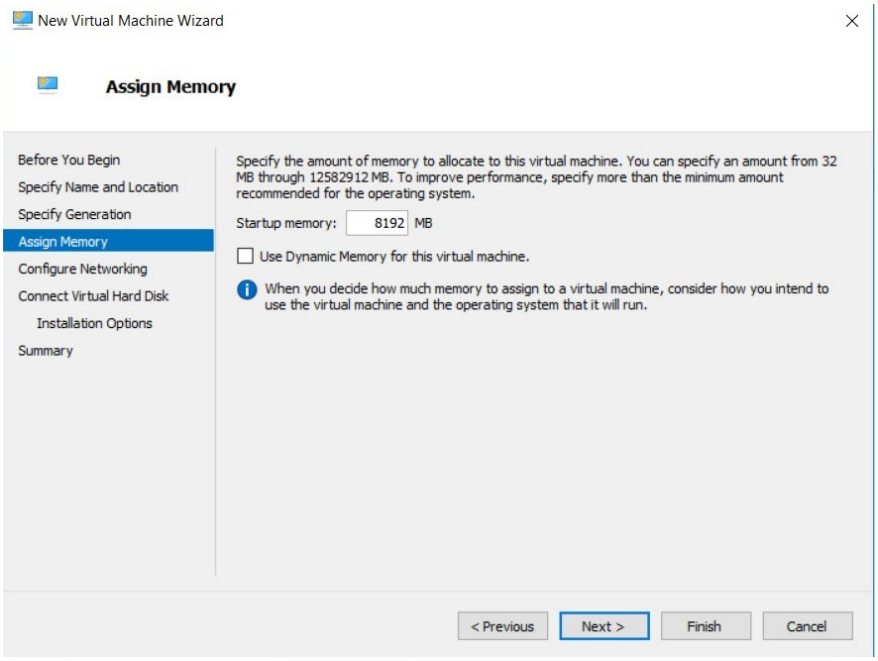
2. Enter a name for your virtual machine and click [Next].



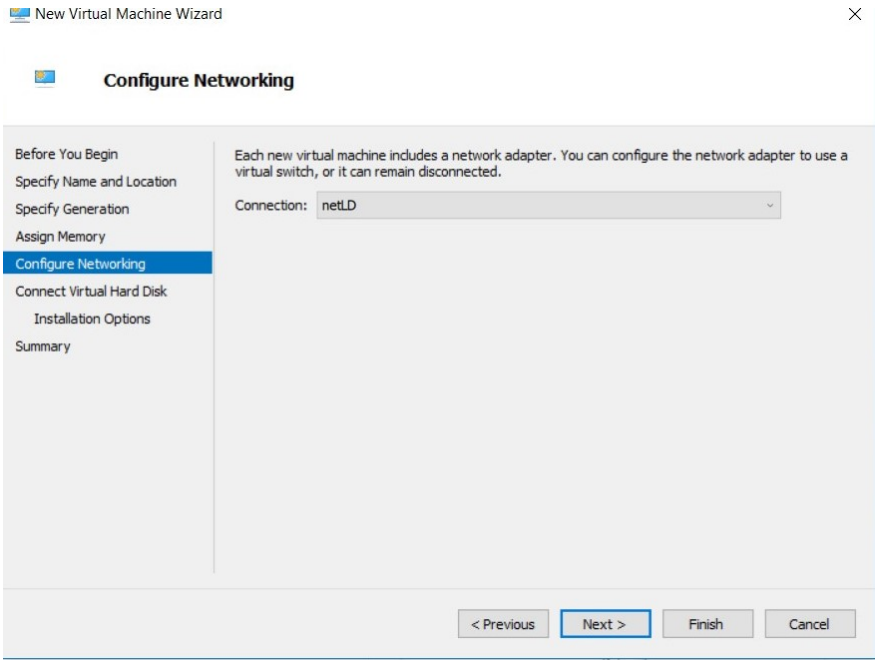
3. Select “Generation 1” and click [Next].



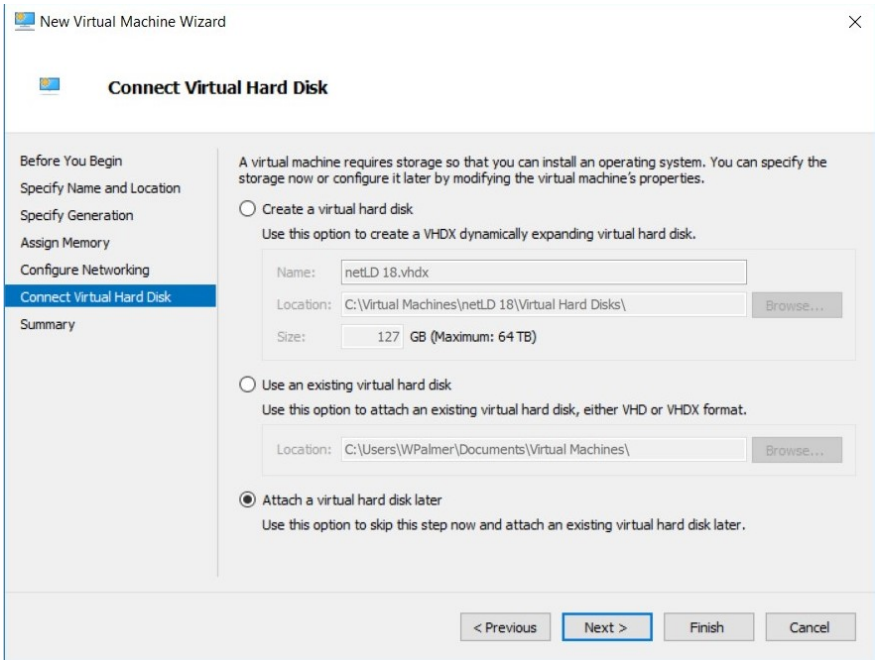
4. Set the startup memory and click [Next].



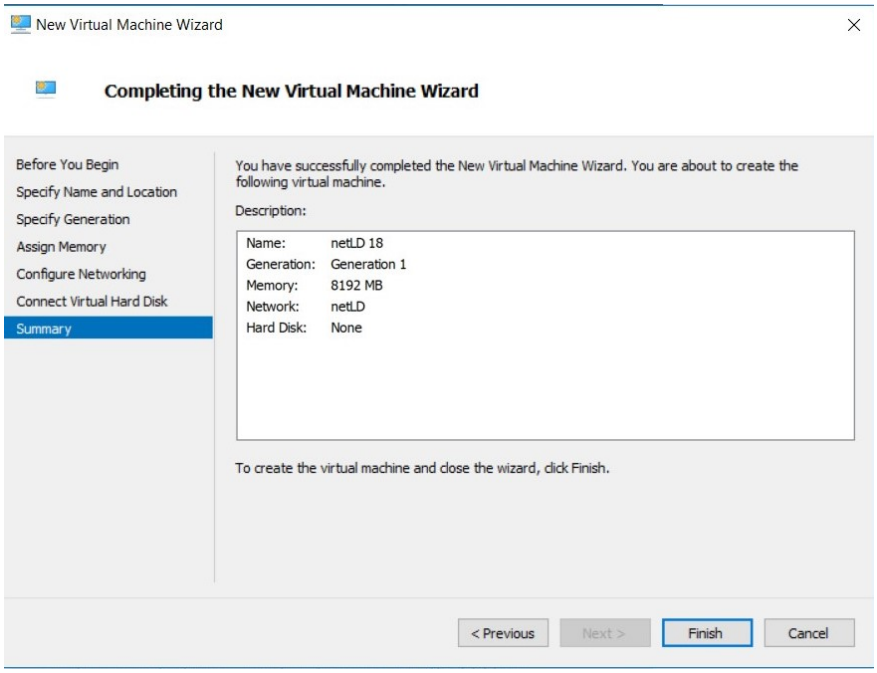
5. Select the virtual switch you want to connect to and click [Next].



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



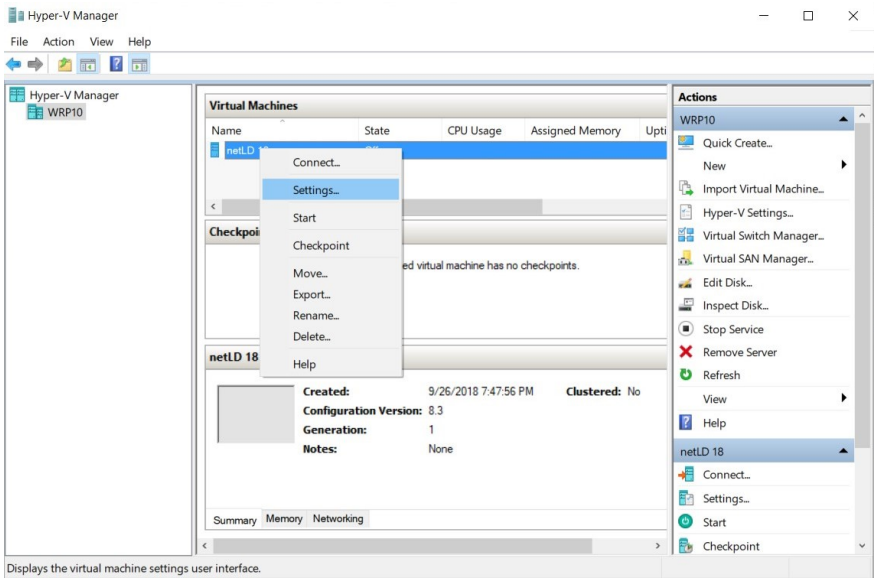
7. Click [Finish].



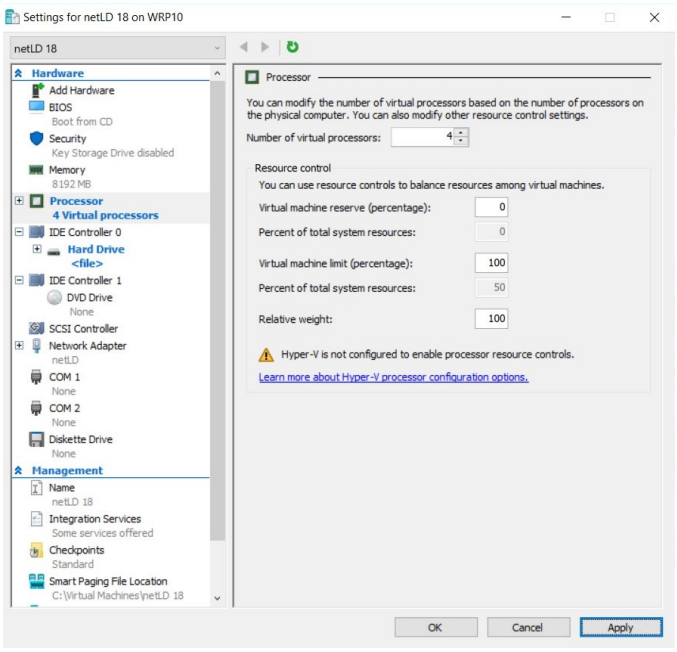
The virtual machine will now be created.

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

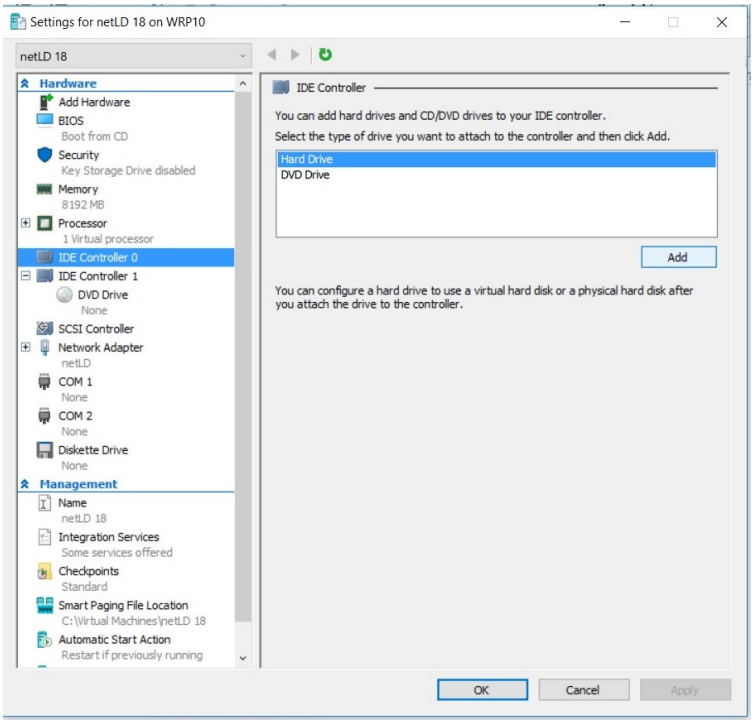
8. Right-click the virtual machine you created and click Settings.



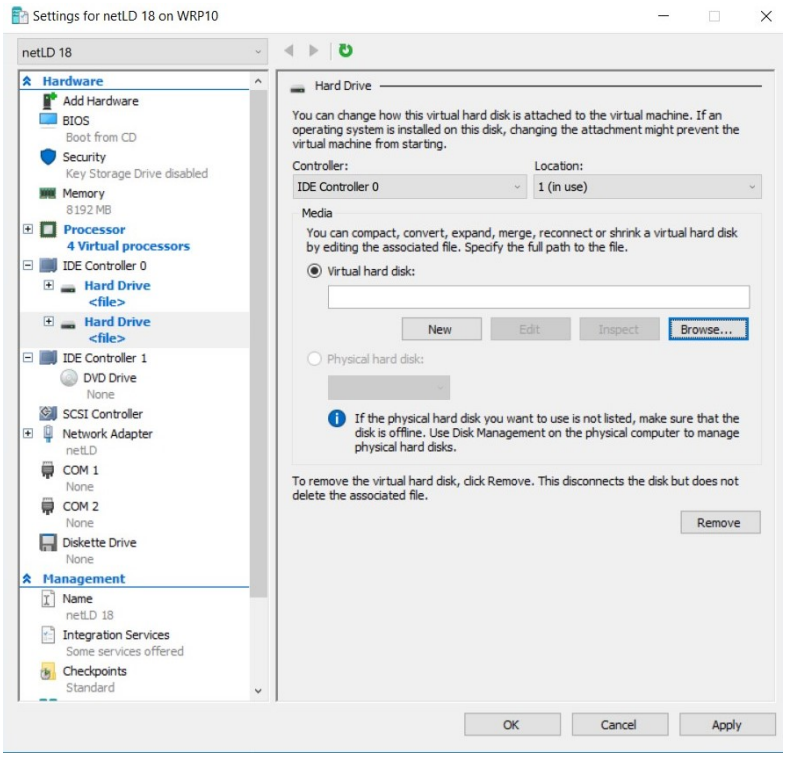
9. Select “Processor” and change [Number of virtual processors].



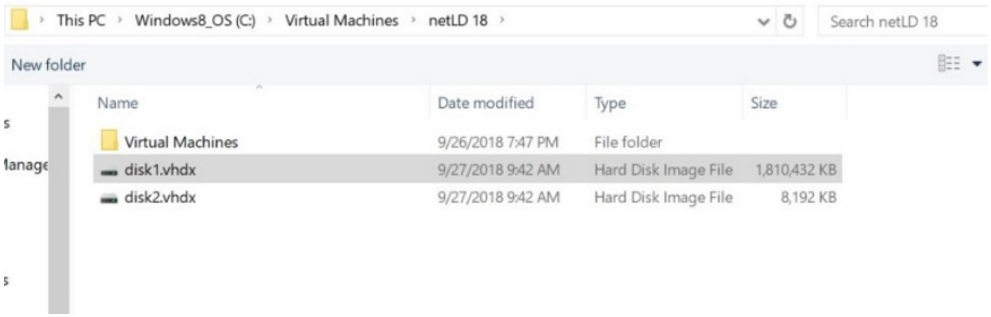
10. Select “IDE Controller 0” and click [Add].



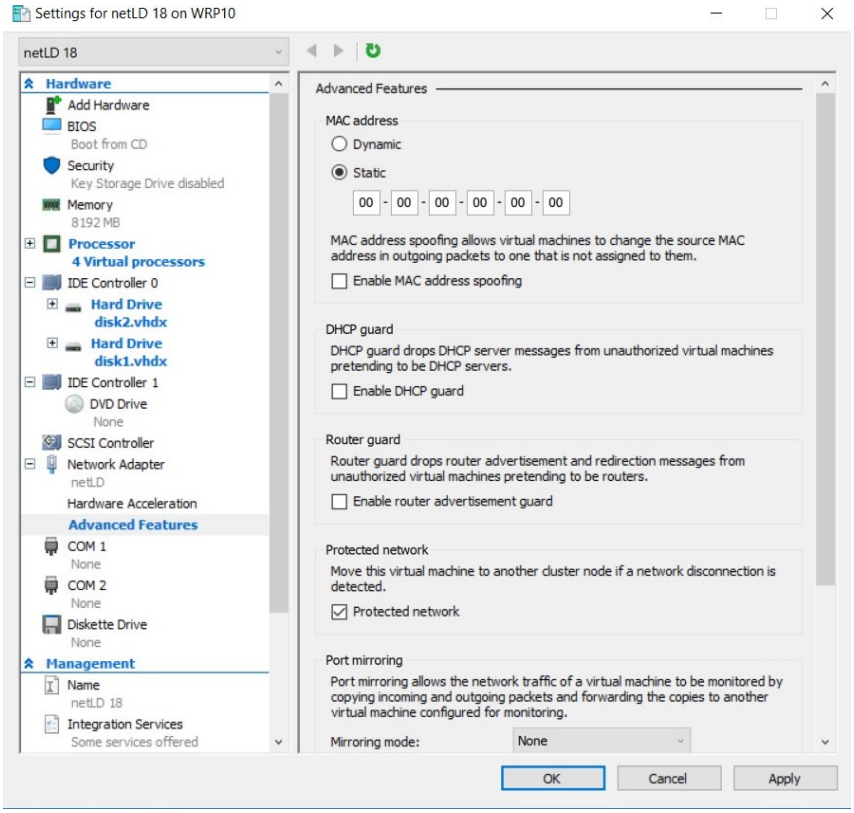
11. Click [Browse].



12. Add “disk1” and click [OK].



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



This completes the Windows Hyper-V deployment.

2.3 Deploying to Linux KVM

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

This completes the KVM deployment

2.4 Deploying to Nutanix AHV+

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

This completes the Nutanix deployment.

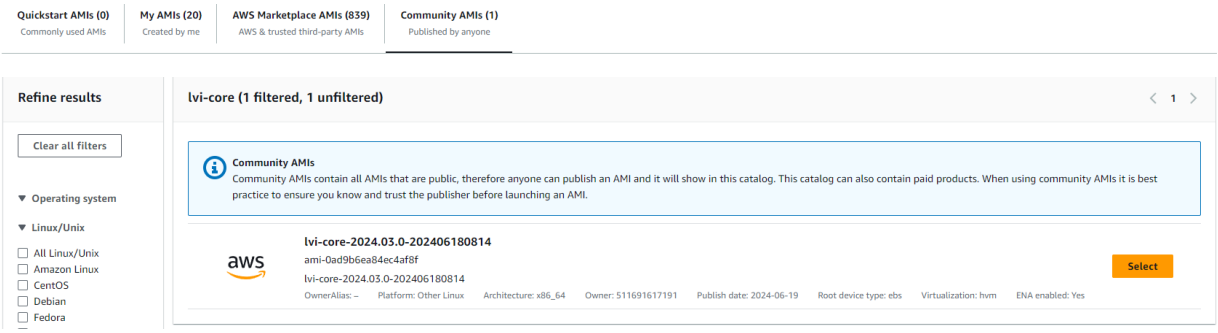
2.5 Deploy to Microsoft Azure

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

This completes the deployment on Azure.

2.6 Deploying to AWS

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



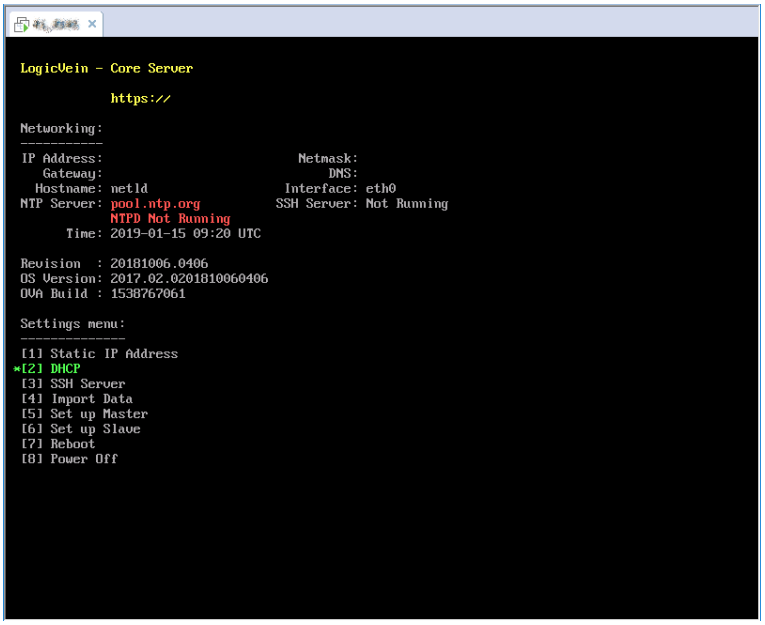
5. Select an instance type based on the sizing guidelines.
6. After creating a key pair in Key Pair (login), click [download key pair].
7. In the network settings, assign a group. You can choose an existing security group or create one. You can add a new security group.
8. [Under Configure Storage],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

2.7 Configuring Network Settings

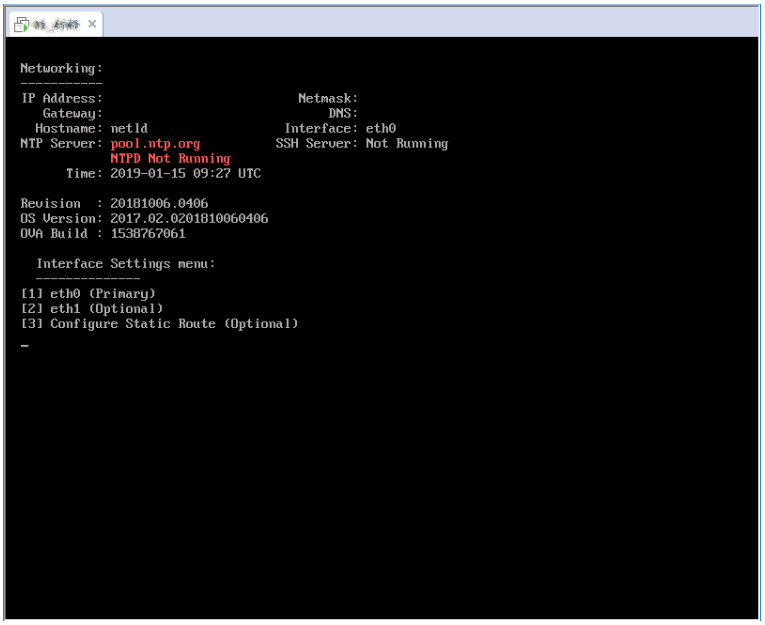
In the network settings, configure the host name and IP address to be given to NetLD. By default, the IP address etc. will be obtained from DHCP. In an environment without a DHCP server, perform various settings using the following steps.

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

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



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

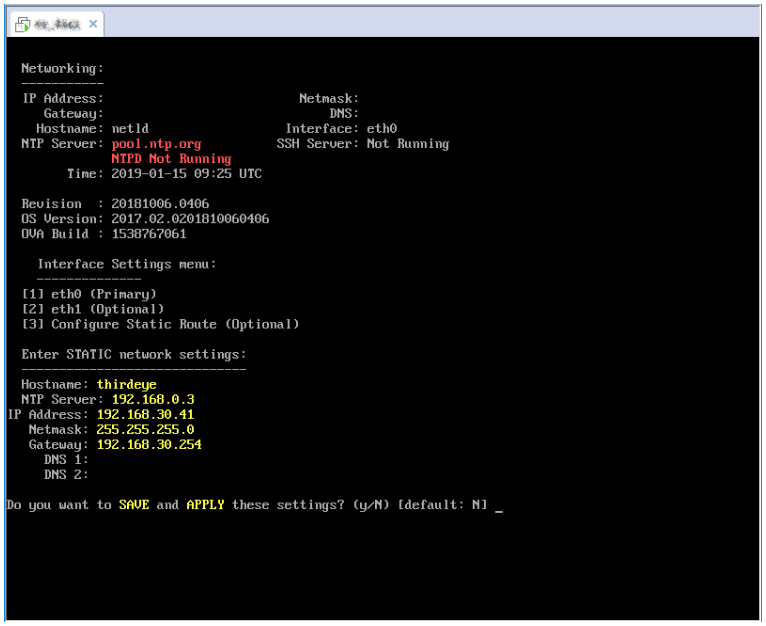


3. The following network setting items will be displayed in order.

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

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

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



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

2.8 Apply the license

Apply your license and activate your product.

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

`https://<Address>/`

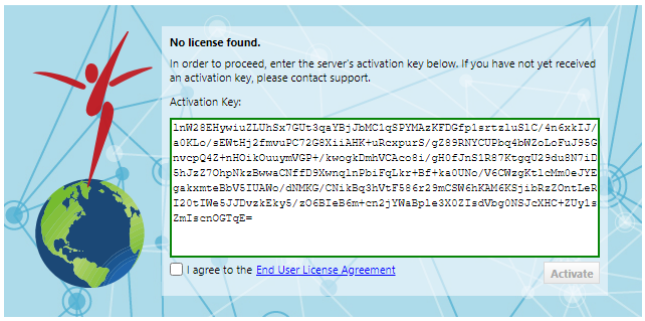
For `<Address>`, Specify the IP address or FQDN (Fully Qualified Domain Name).

The license authentication screen will be displayed.

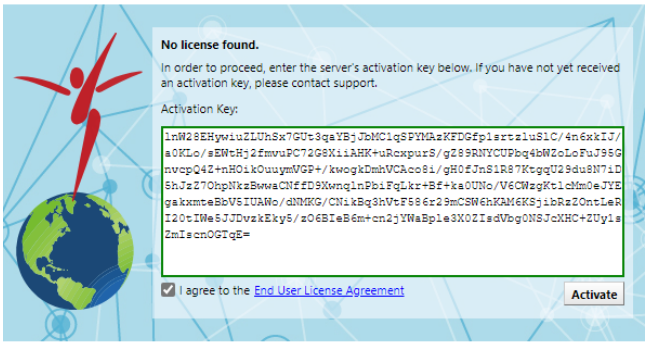
2. Copy and paste **Serial number** or **Activation key**.

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

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



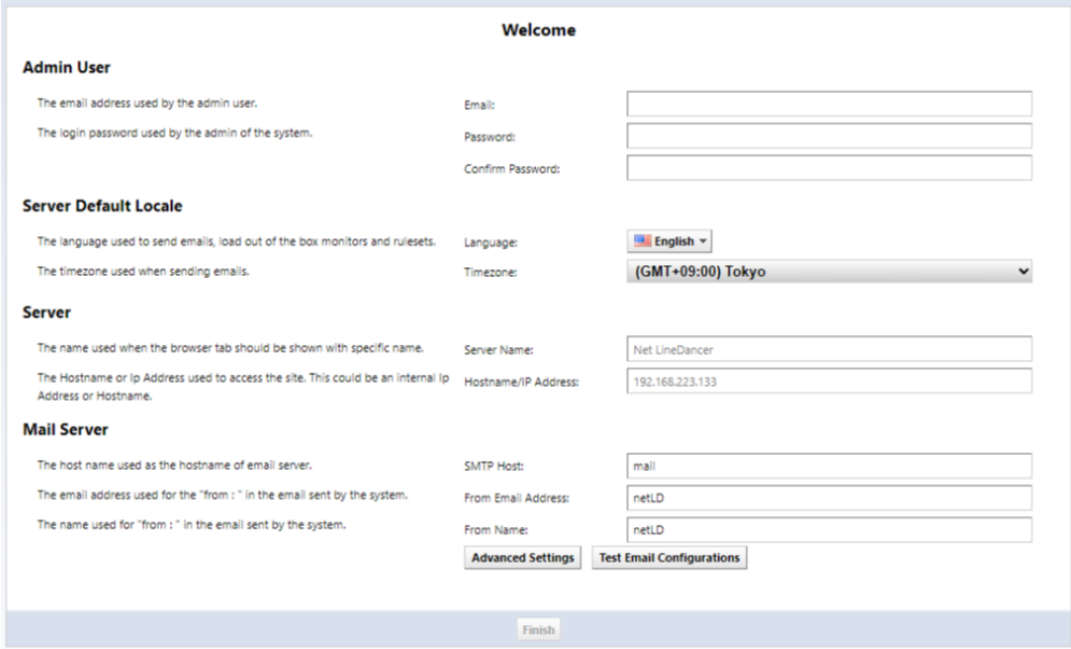
3. Check "I agree to the End User License Agreement", and click [Activate].



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

2.9 Initial settings (detailed settings)

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



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

Note

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

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

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

3 Login/Logout

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

3.1 Log in

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

https://`Address`/

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

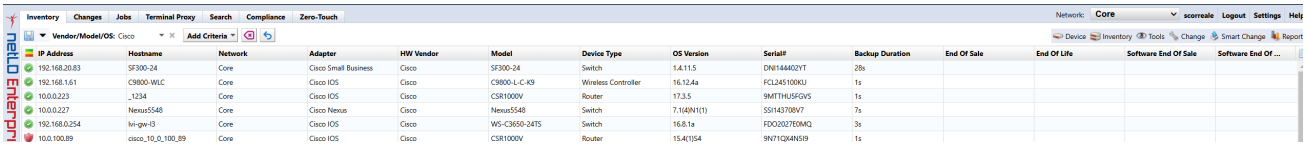
2. On the login screen, enter your username and password to log in.

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

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

3.2 Log out

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



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

4 Global Menu

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

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

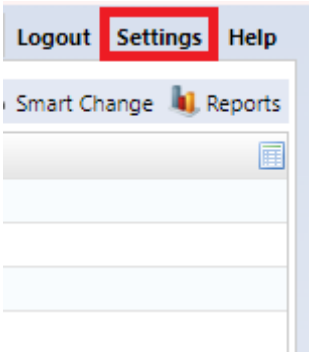
5 Manage Users

5.1 Create User Account

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.

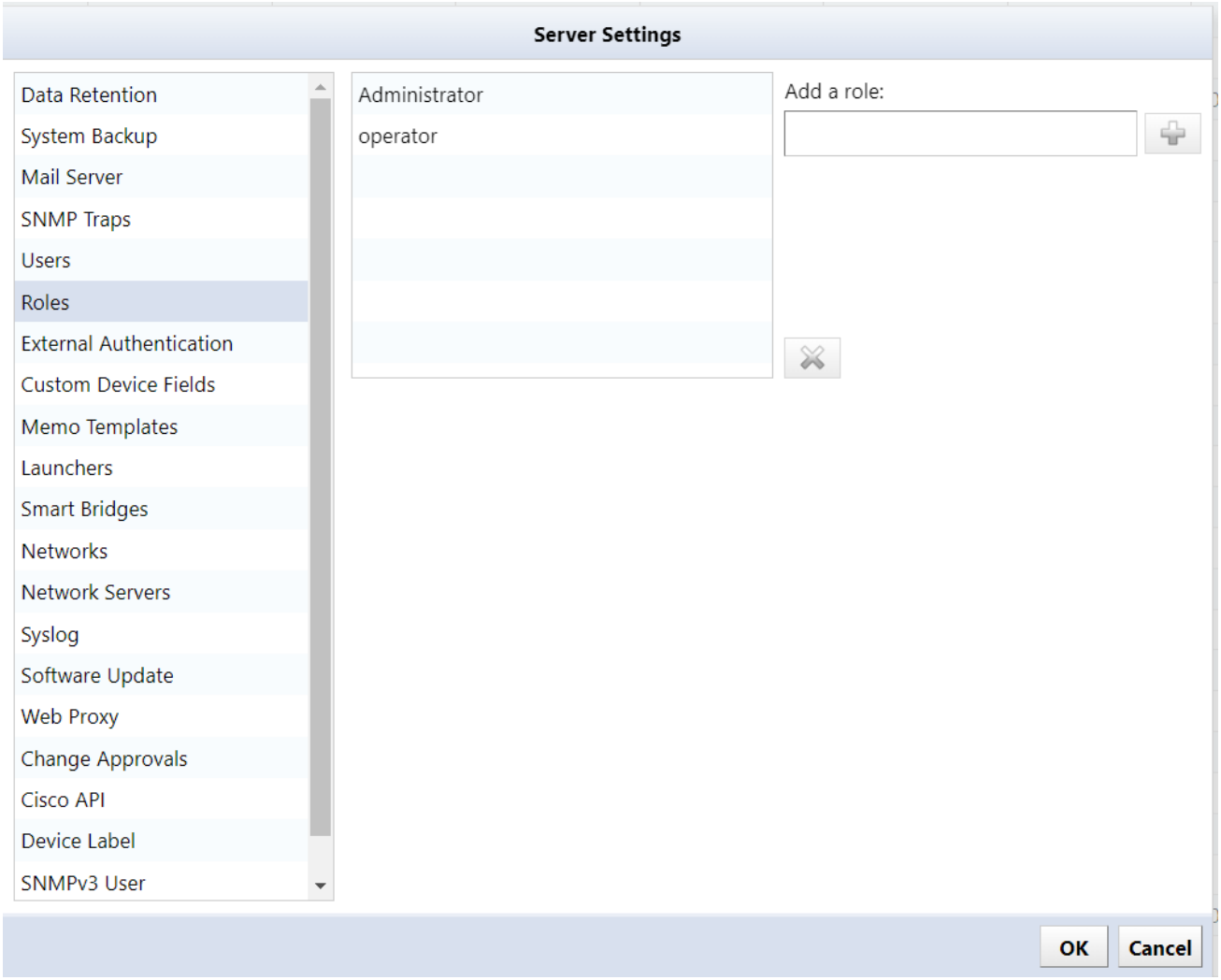
User and permission settings can be configured from Settings in the Global Menu.



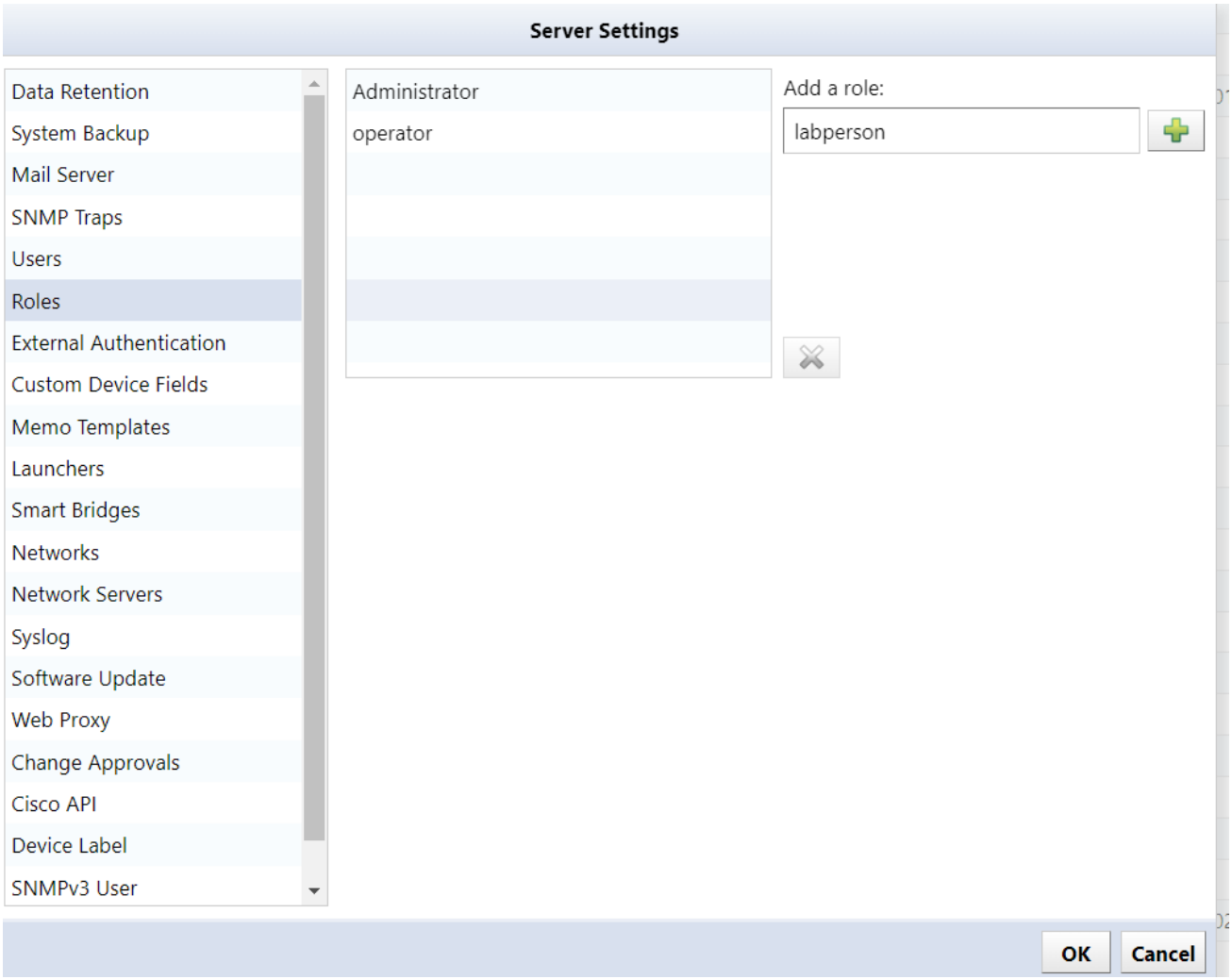
5.2 Add permissions

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

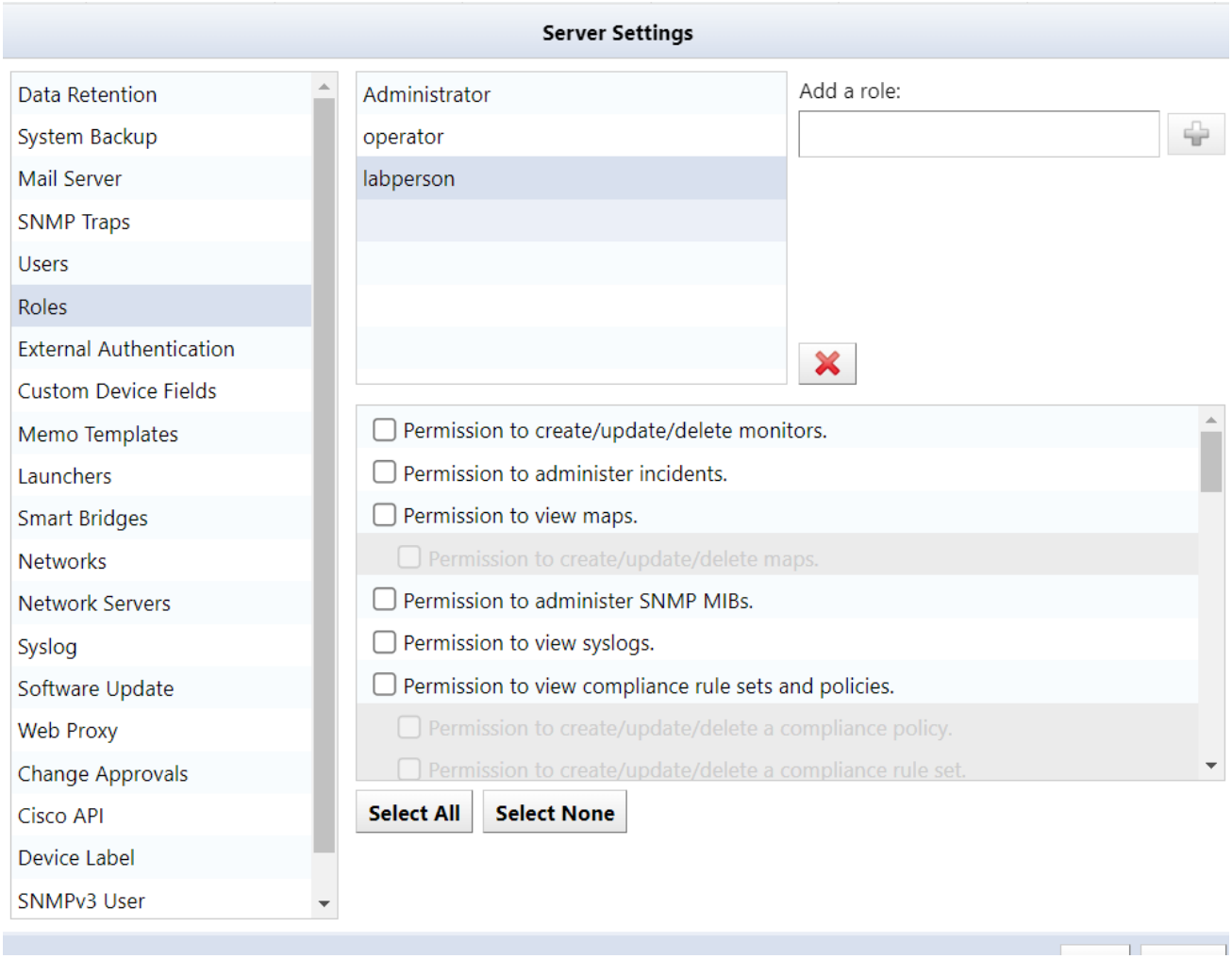
1. Click [Roles] in the left sidebar.



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



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



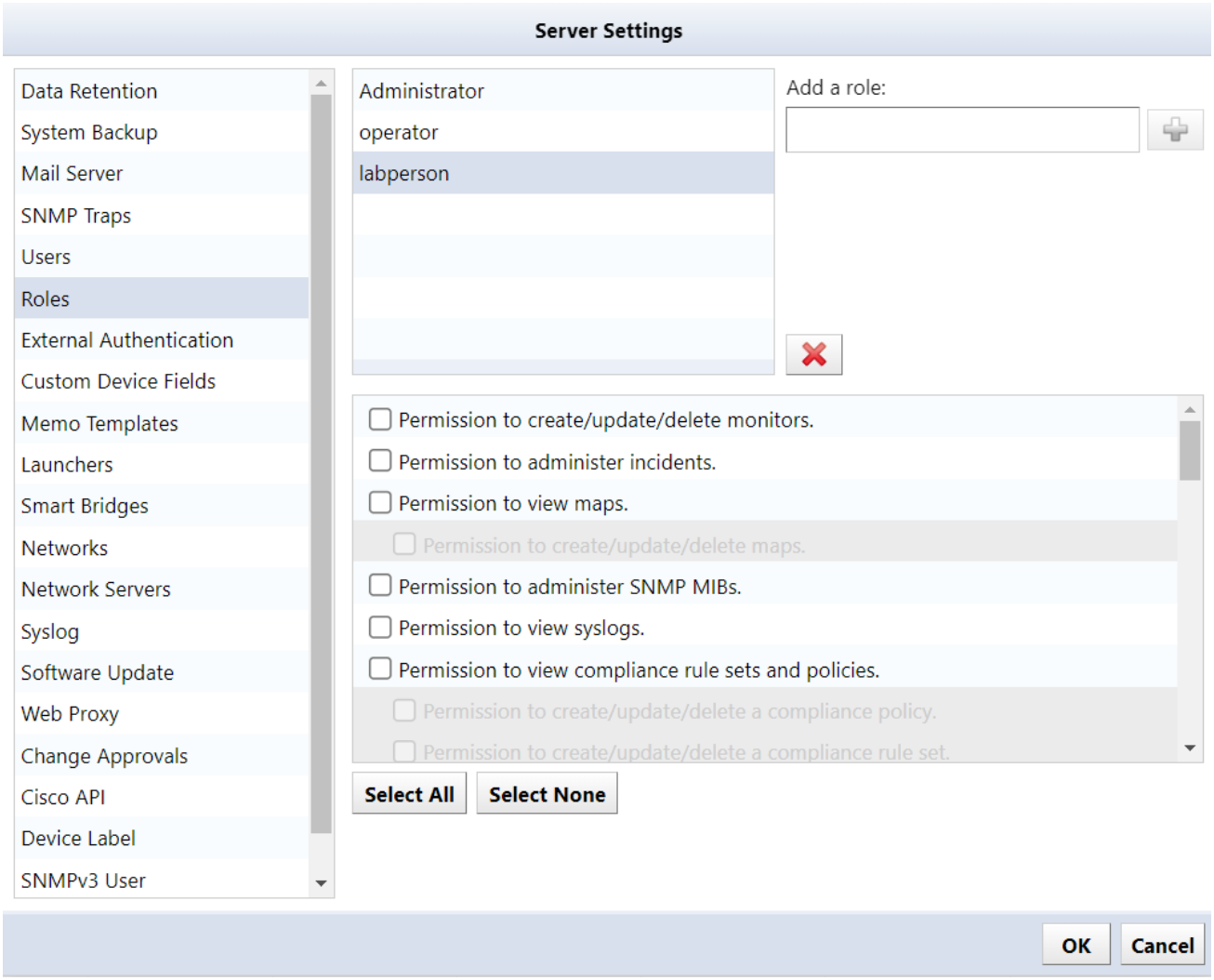
Permission Item	Explanation
Allow viewing of compliance Rule Sets and policies	You can view the Compliance tab.
Allow creation/update/delete of compliance policies	You can create/update/delete compliance policies. (Permissions associated with "Allow viewing of compliance Rule Sets and policies.")
Allow 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.

Permission Item	Explanation
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.”)
Allow smart change jobs to run	You can run smart change jobs.(Permissions associated with “Allow tool execution.”)

Permission Item	Explanation
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.

Permission Item	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.”)

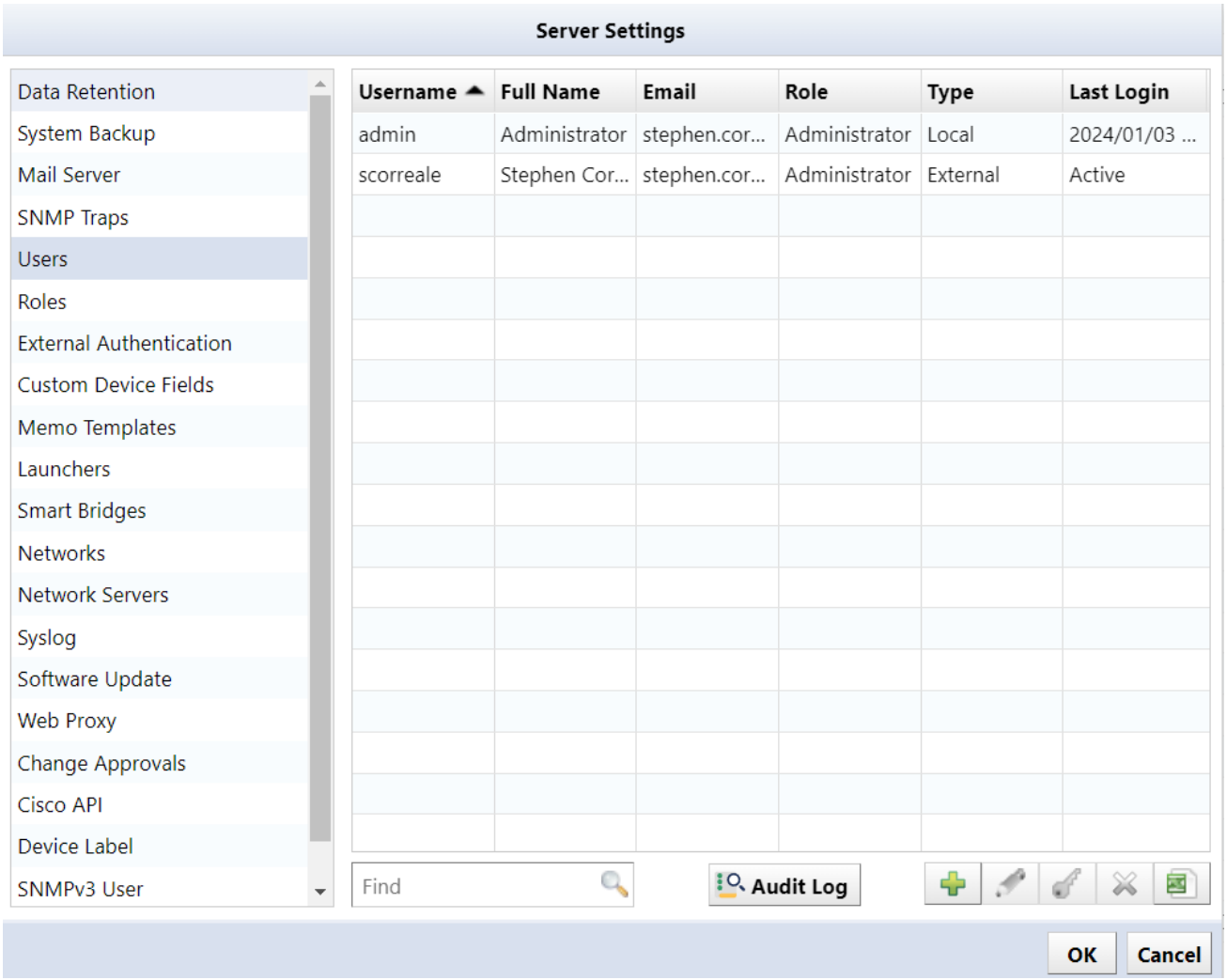
4. Click [OK].



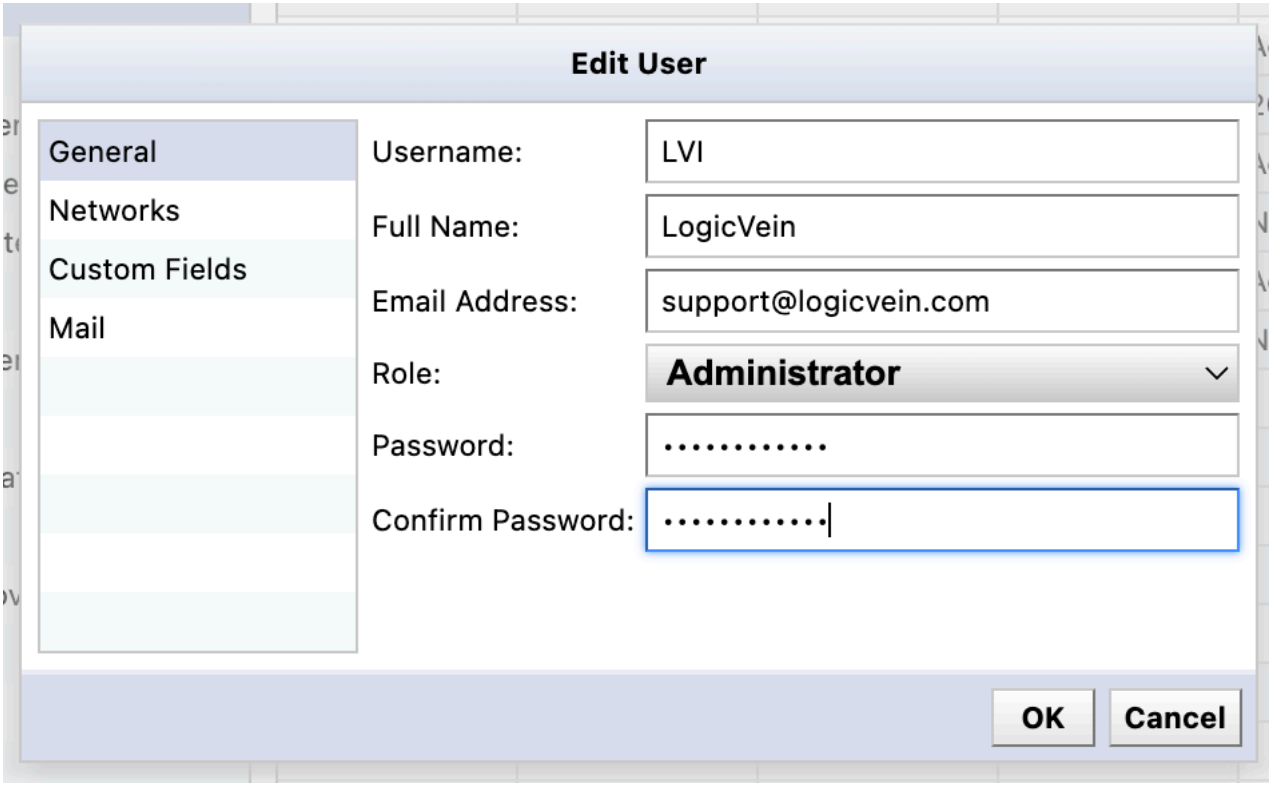
5.3 Add user

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

1. Click the buton.



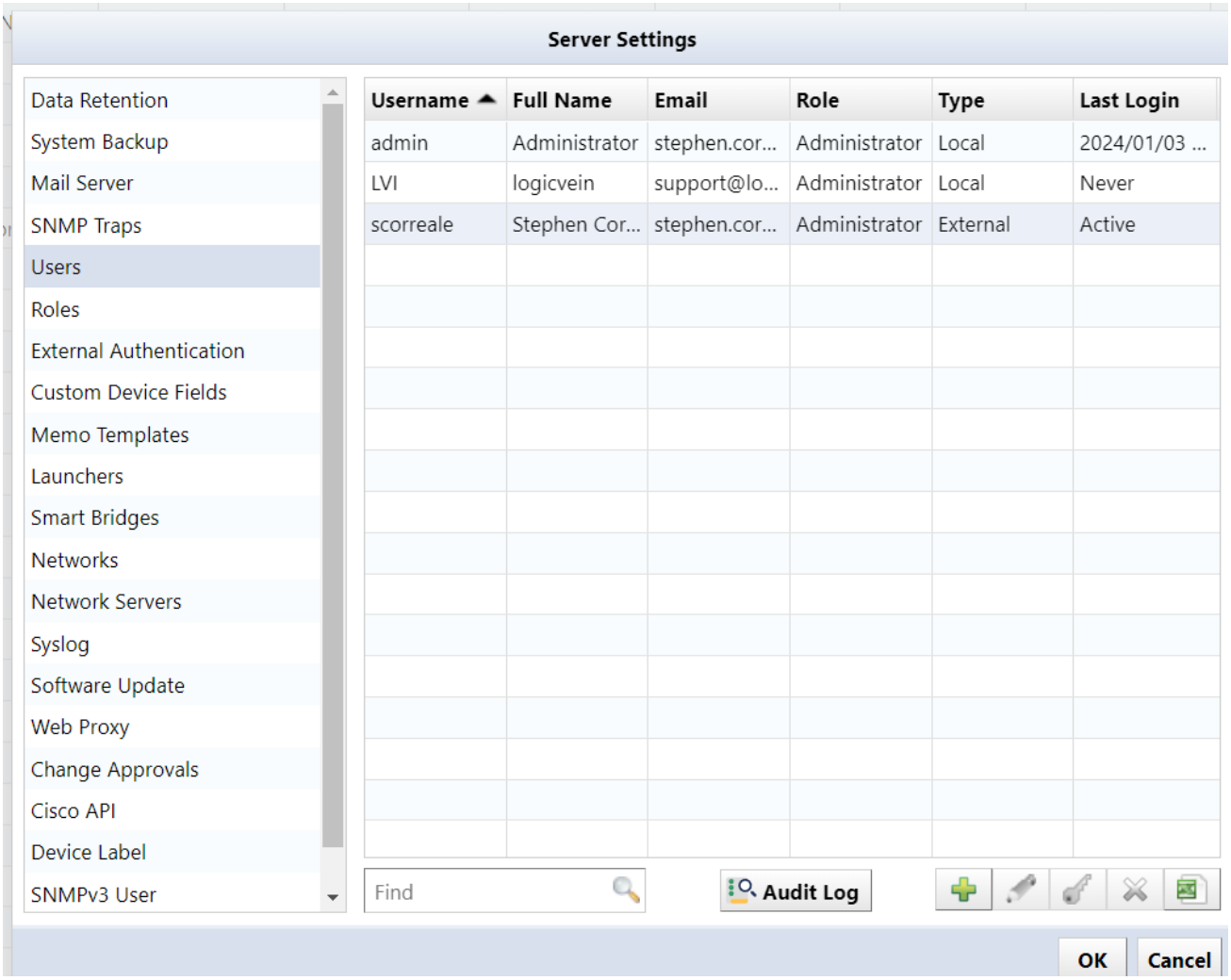
2. The user addition screen will be displayed. Enter the items and click [OK].



Item	Subitem	Explanation	Requirements
General	**Username**	Enter your username.	required
	Full name	Enter the user's full name.	—
	Email address	Enter the user's email address.	—
	Role	Select the user's permissions. You can select the permissions set in the **Add permissions** section from the pull-down menu.	required
	Password	Set the user's password.To set a password, the following conditions must be met. - Must be at least 8 characters - Must not be a character string that is easy to guess (person's name, proper noun, dictionary word, commonly used password)	

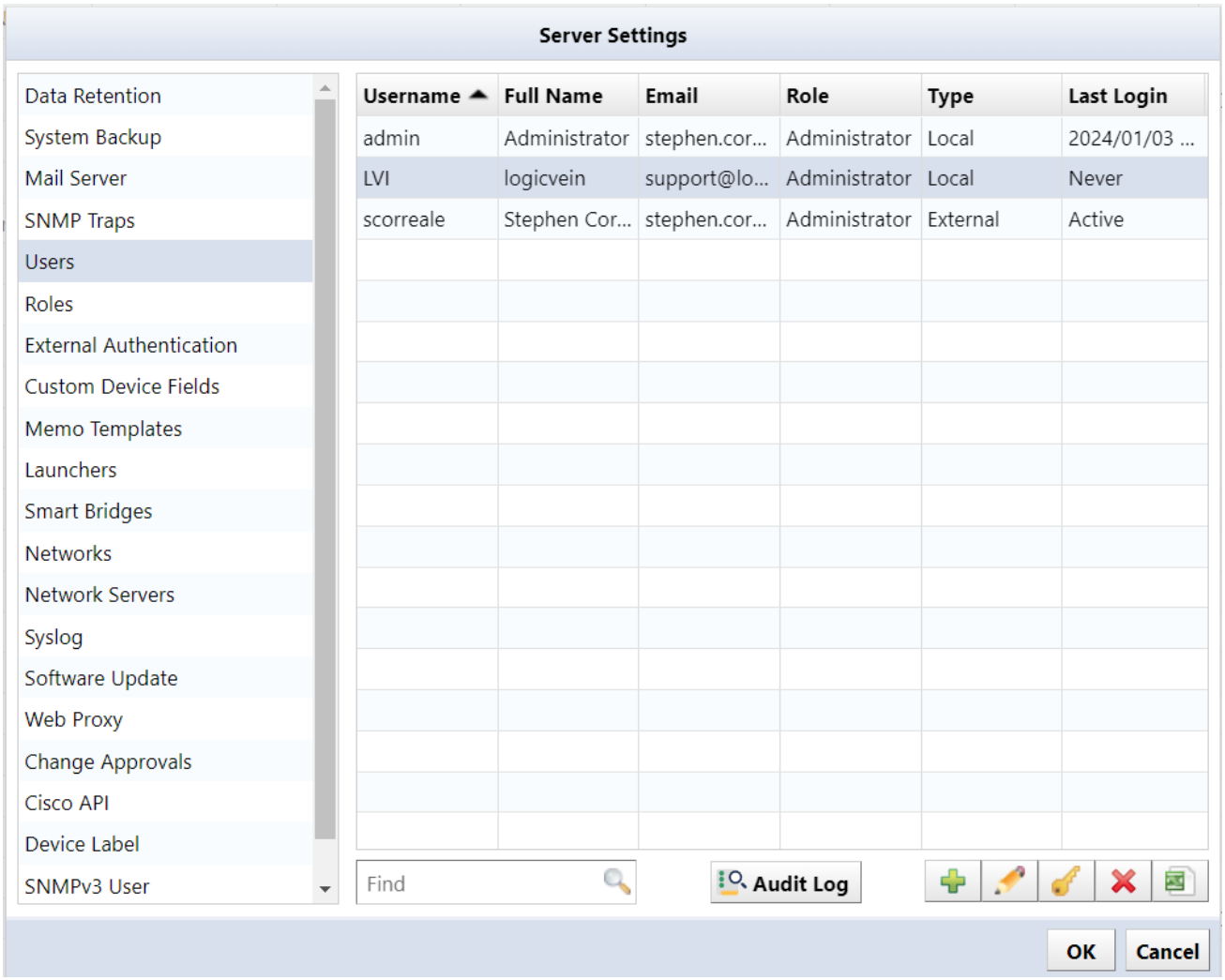
Item	Subitem	Explanation	Requirements
		- Character strings that do not repeat the same characters or are arranged in an easy-to-understand manner	required
Custom field	**Custom 1-5**	Select the custom device fields that users can view. Displayed item names will change based on the settings in the Add columns/change column names for custom device fields".	—

3. Click [OK].

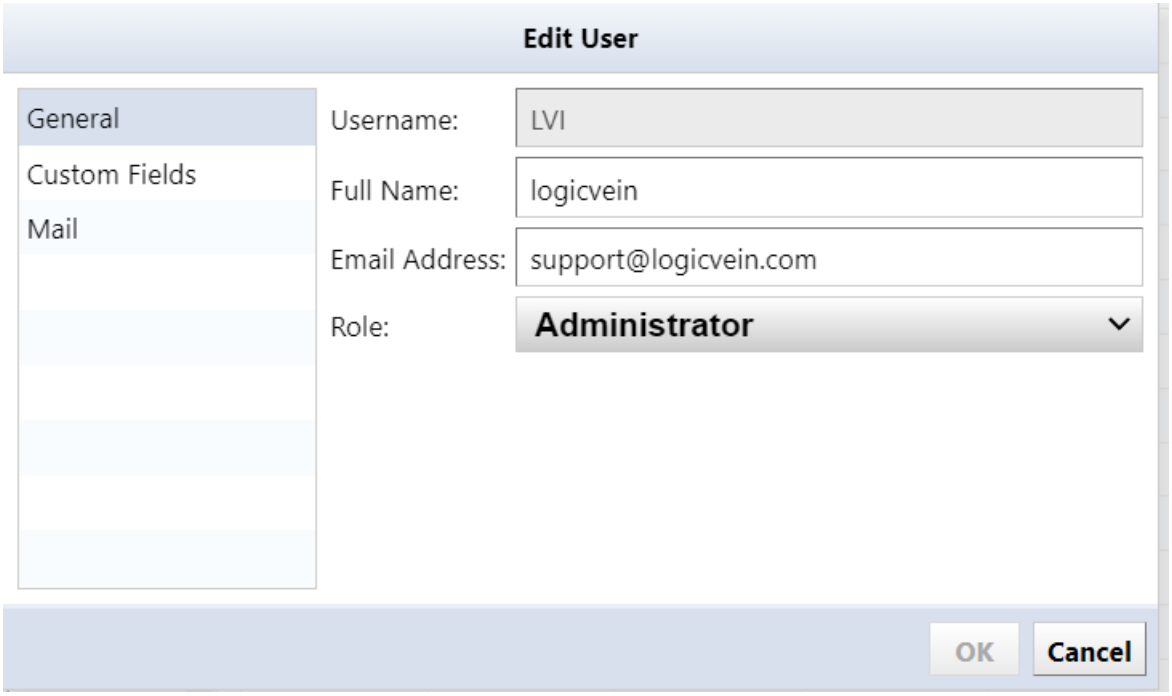


5.4 Change user information

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



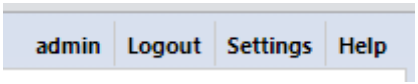
2. The user edit screen will be displayed. After editing, click [OK]. The Username cannot be changed. If you want to change your password, refer to the Change-password section below.



5.5 Change password

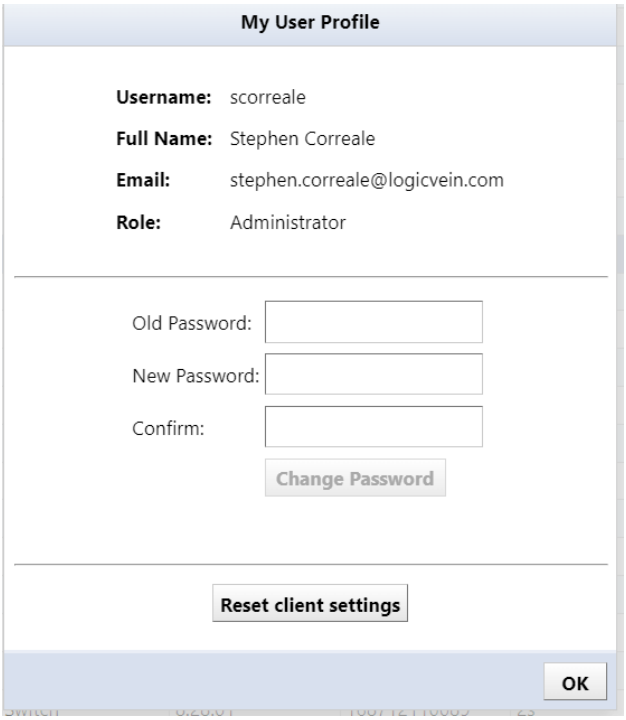
You can change your password from the login username in the Global Menu.

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



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

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



Note

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

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

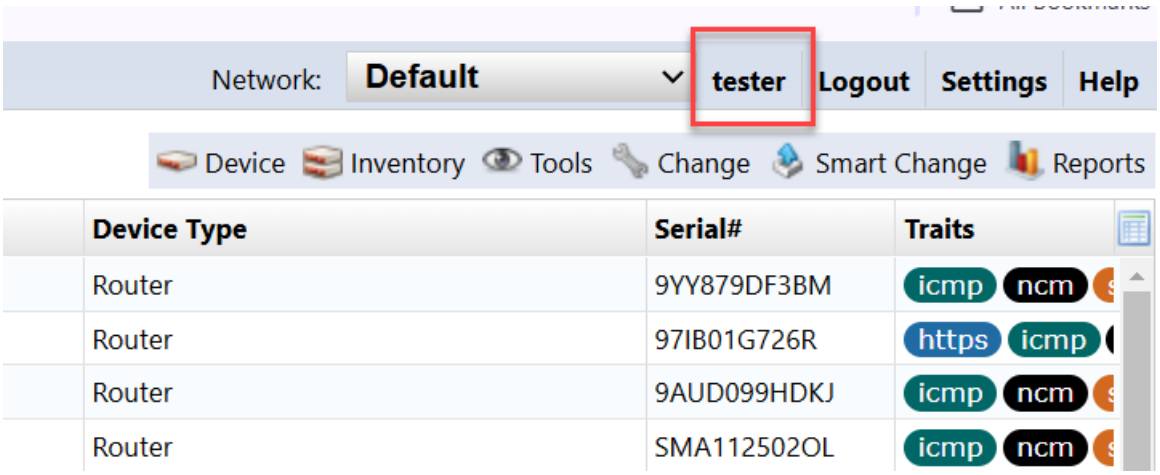
5.6 Setup two-factor authentication (2FA)

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

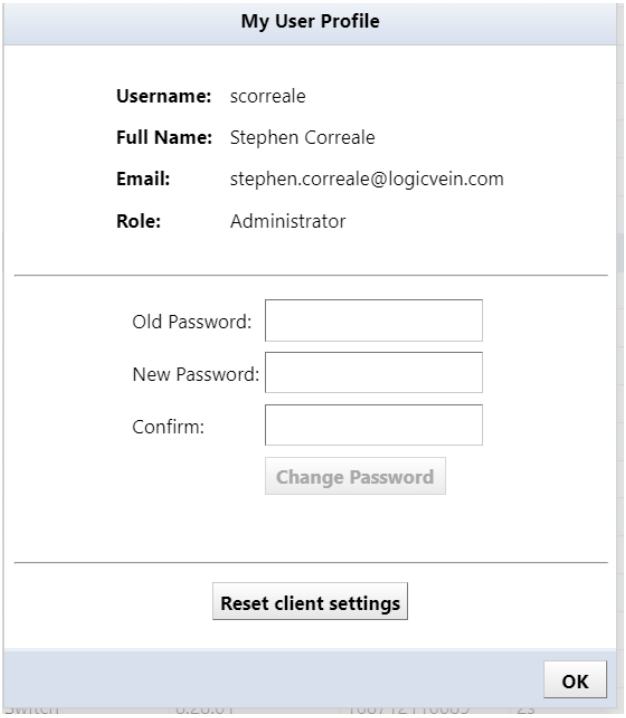
5.6.1 Enable two-factor authentication

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

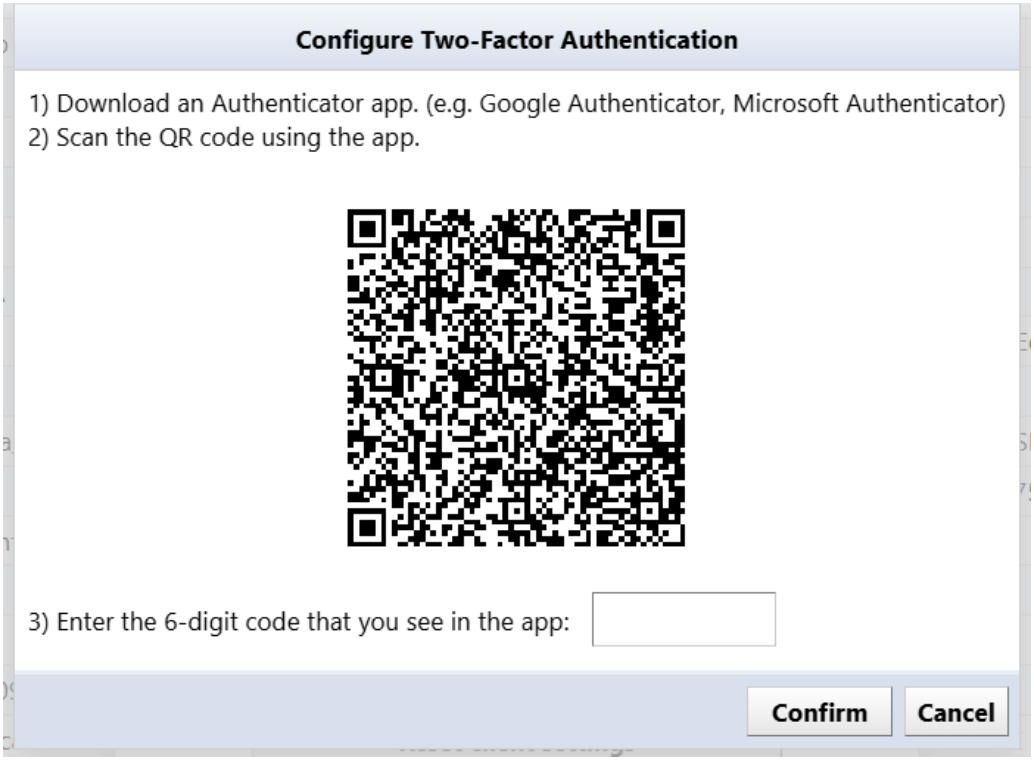
1. Click the username to open the User Profile dialog.



2. Click [Set up two-factor authentication]



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



4. Click [OK].

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

5.6.2 Remove two-factor authentication

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

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

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

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

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

5.7 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.

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

5.7.1 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:

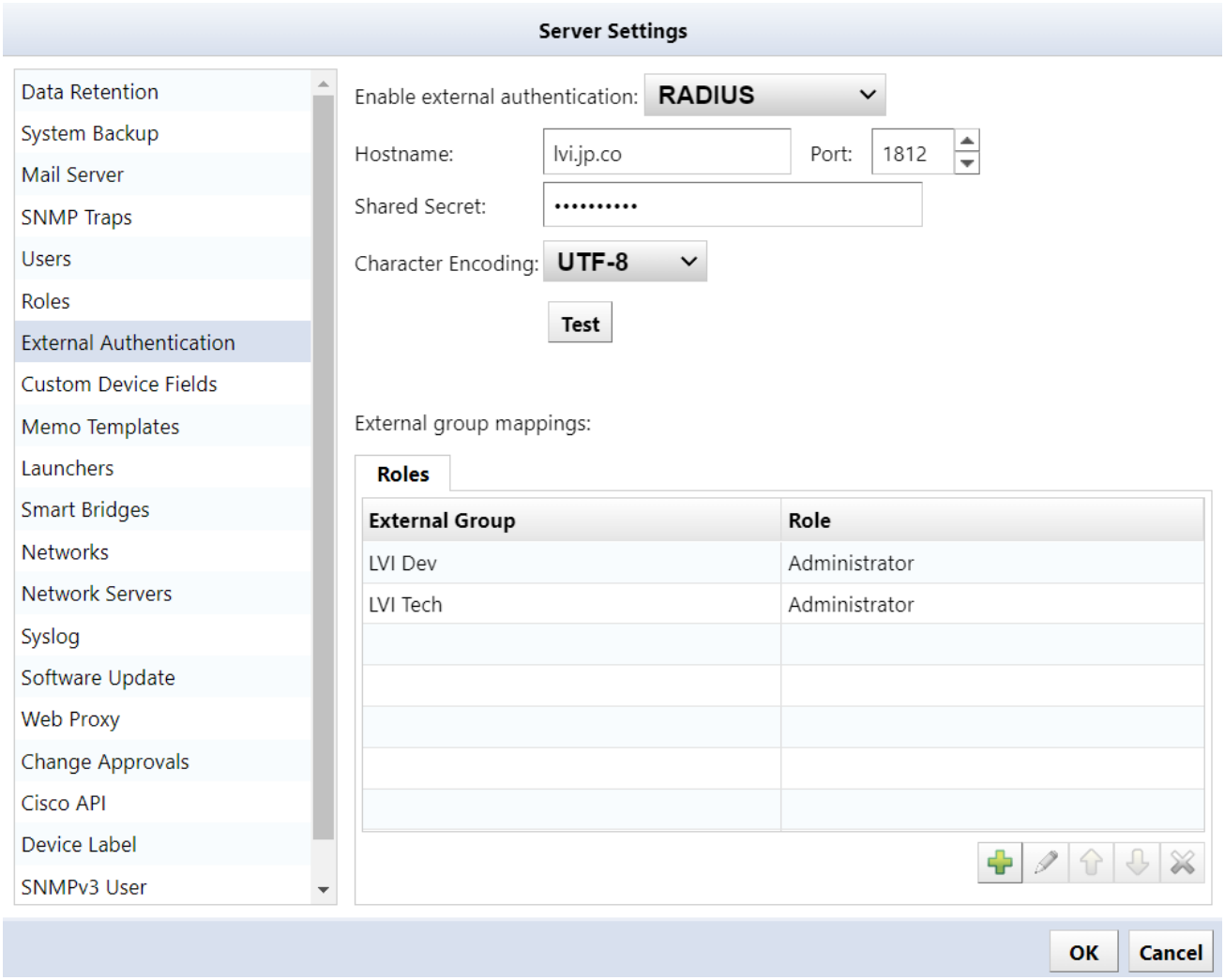
```
LogicVein Cleartext-Password: = "password"

Filter-Id += "GROUP"
```

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

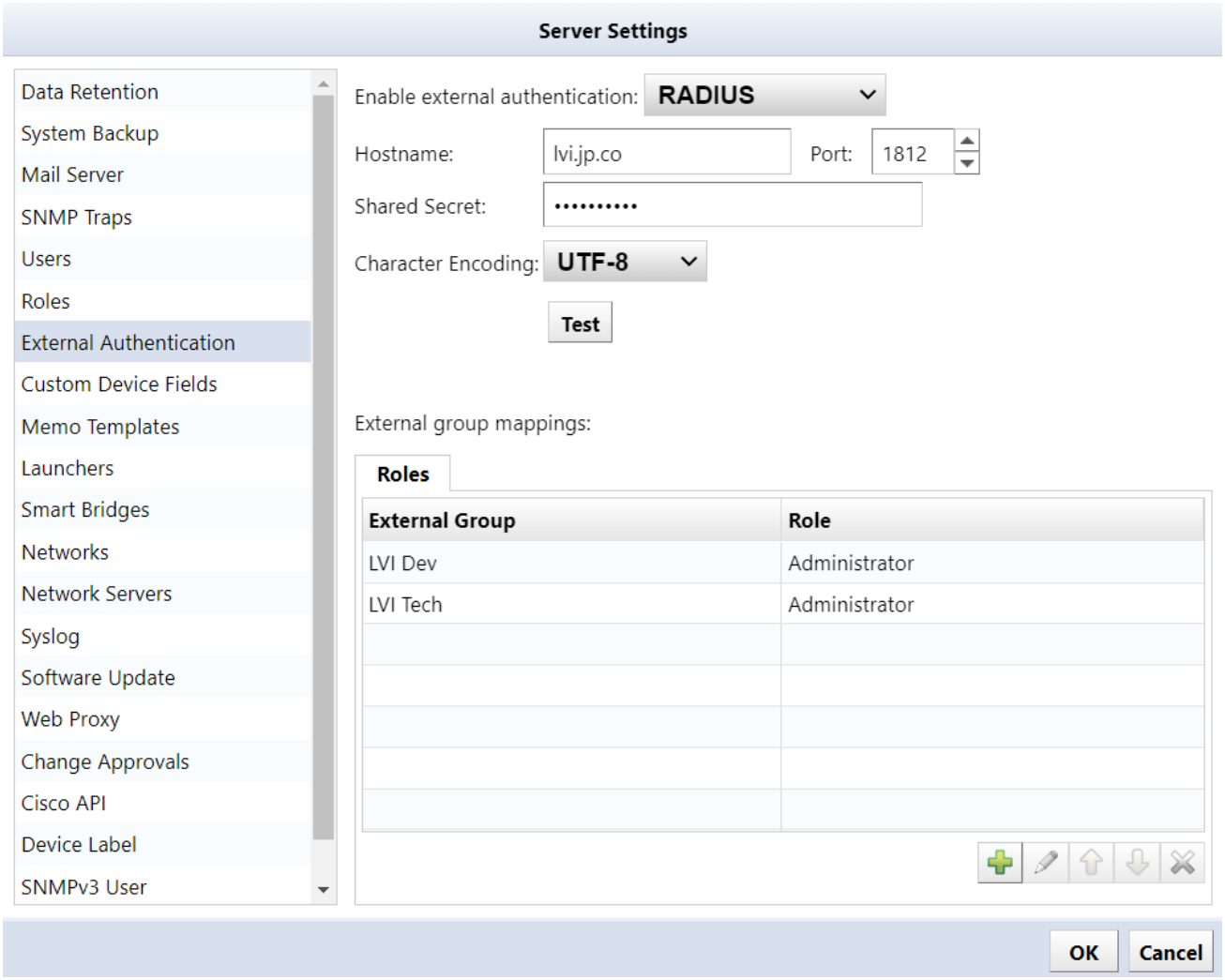
To configure external authentication:

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

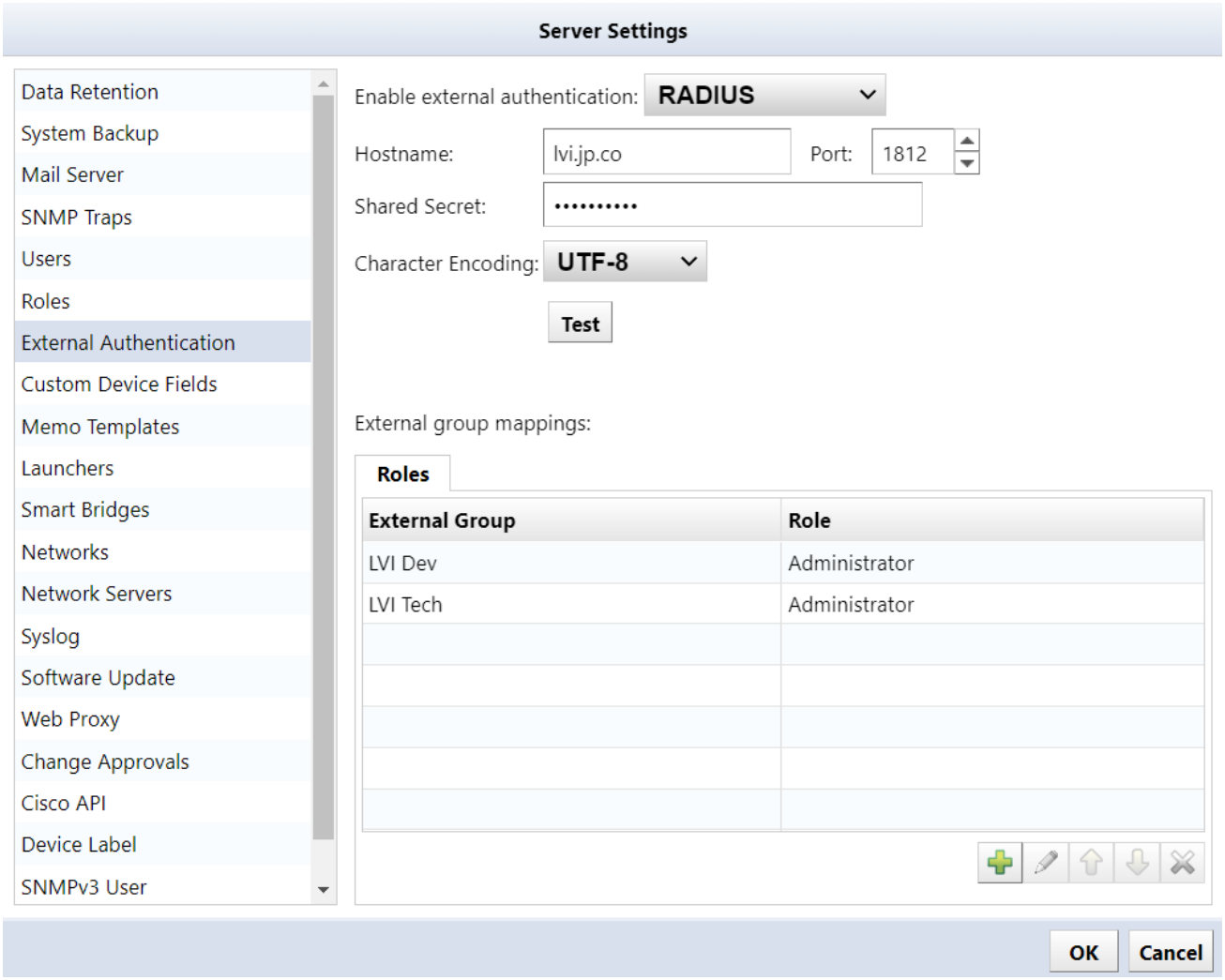
2. Change the [Enable external authentication] selection to “RADIUS”.



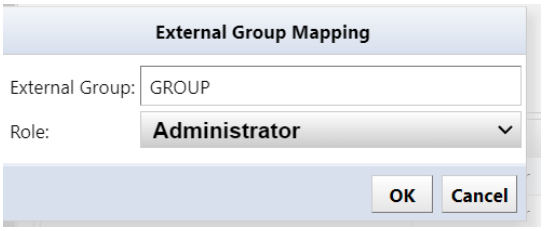
3. Set the RADIUS server's IP address (or hostname) and [Shared Secret].



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



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



The Active Directory RADIUS settings have now been successfully configured.

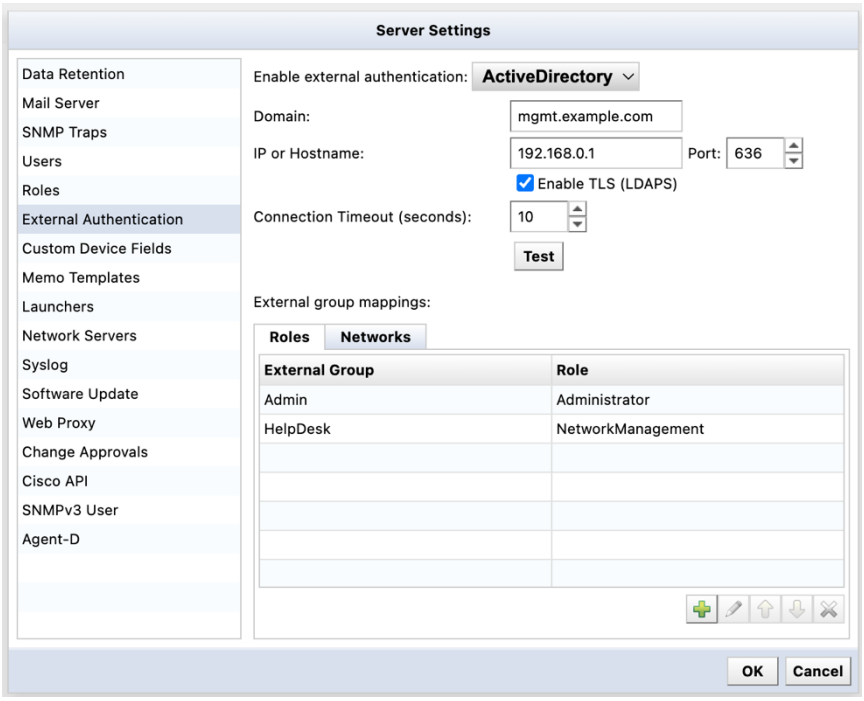
6. Click [OK] to save.
7. Click [Close] to exit the server settings.

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

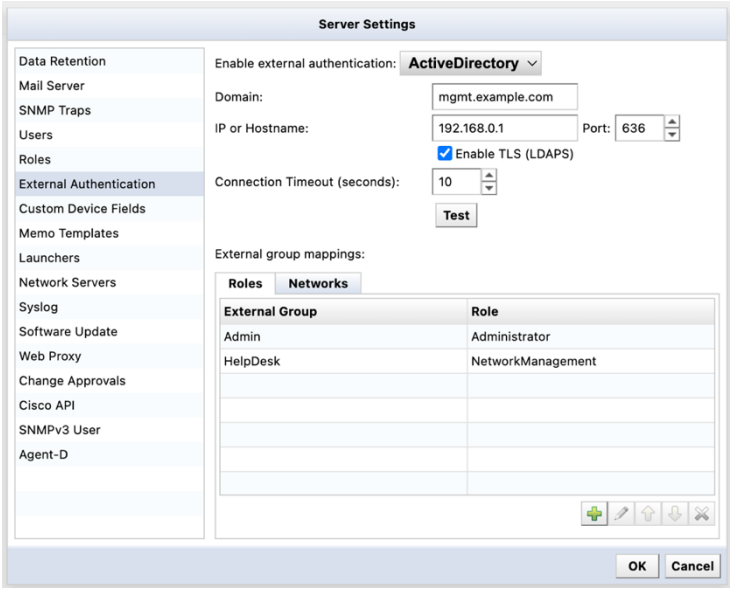
5.7.2 Active Directory

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

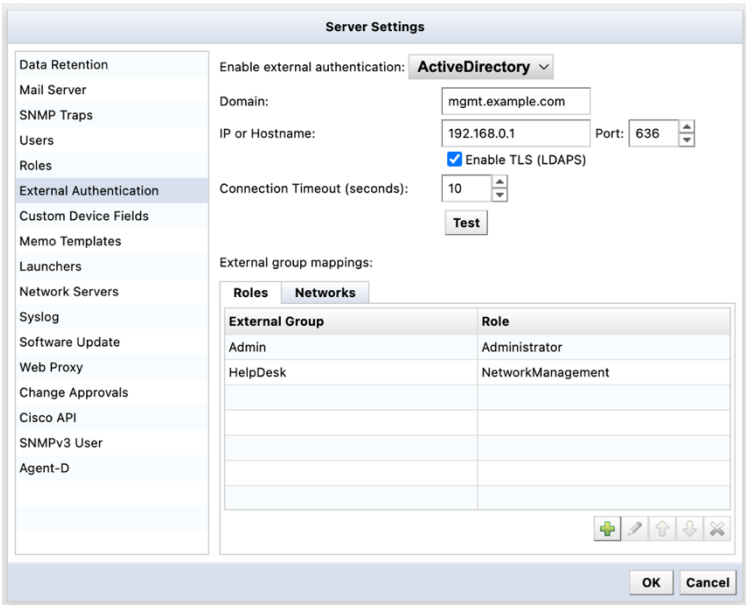
1. Navigate to the [Server Settings] window in NetLD and select [External Authentication].
2. Change [Enable external authentication] to Active Directory.



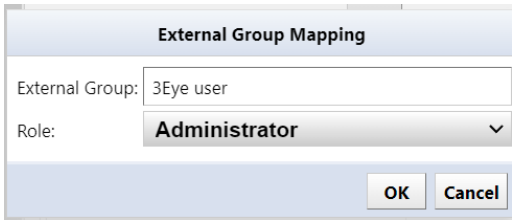
3. Set the domain name and the IP address (or host name) of the Active Directory server.



4. Add a new item using the button.



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



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

5.7.3 SAML

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

5.7.3.1 Microsoft Entra ID Integration Prerequisites

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

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

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

Procedure

Configure SAML 1. Log in to NetLD.

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

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

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

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

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

The downloaded file will be used in the next step.

Create a new application

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

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

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

Obtain IdP Metadata

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

Register the Application in NetLD

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

Note the object ID

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

Configure external group mapping

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

5.7.3.2 Okta Integration Prerequisites

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

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

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

Configure SAML

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:

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

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

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

8. Set the following items:

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

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

Item 1:

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

Item 2:

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

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

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

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

Assigning groups to use the application

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

Get IdP metadata

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

Register application with 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 {{ProuctName}}

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

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

5.7.3.3 Keycloak Integration Prerequisites

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

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

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

Configuaring SAML with Keycloak

Keycloak can be run with docker:

```
docker run -d --name keycloak    -p 8080:8080    -e KEYCLOAK_ADMIN=admin    -e KEYCLOAK_ADMIN_
```

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

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

```
docker logs -f keycloak
```

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

Client ID is: https:///auth

You can select any name (e.g. “NetLD”).

5. Click [Next] and add a callback URL

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SAML 2.0 Identity Provider Metadata file.

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

5.7.4 Use Local Authentication After Setting Up SAML Authentication

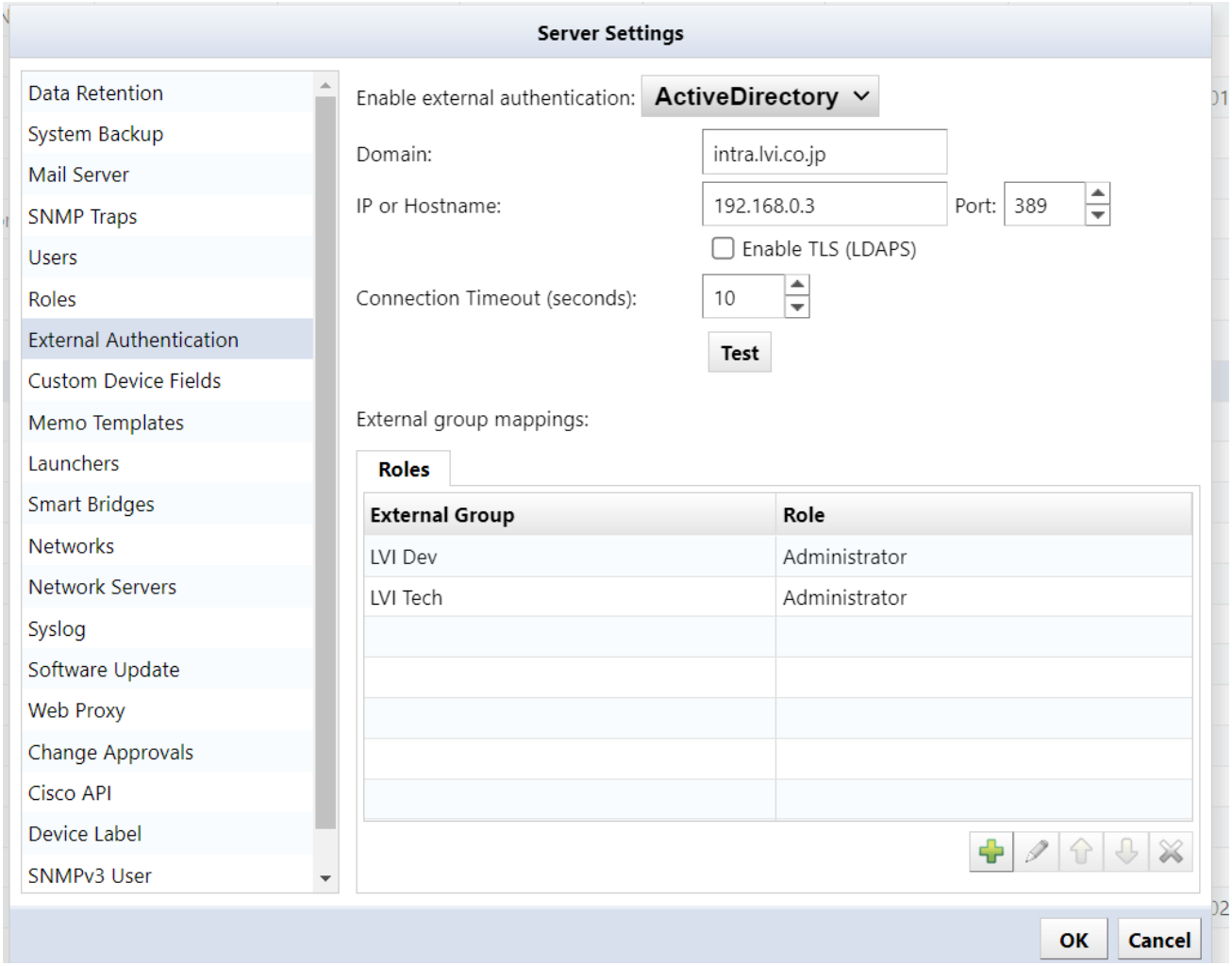
After completing the SAML authentication setup, when you access a NetLD product page, the linked sign-in page will be displayed. If you want to log in to the product using local authentication instead of SAML authentication, add the variable `"/?forceLoginPage=true"` to the end of the URL to access it:

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

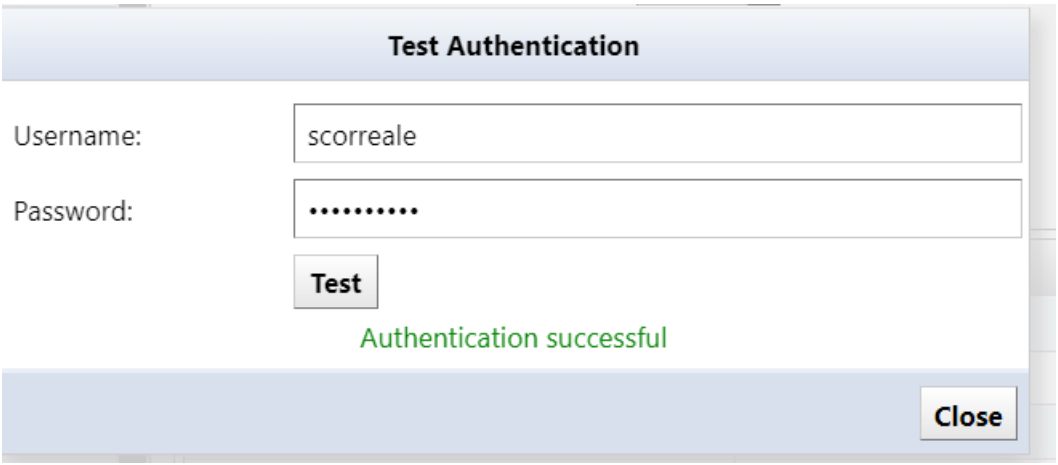
When you open the URL with the variable added, the product's login page will be displayed. You can log in with a local account such as admin.

5.7.5 Testing external authentication

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



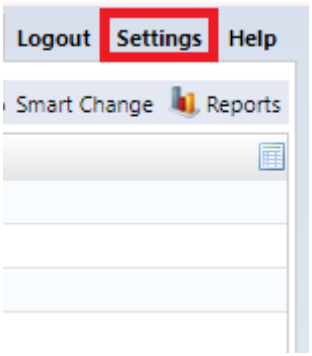
When the [Authentication Test] dialog appears, enter the [Username] and [Password] to test authentication, and click [Test]. If the authentication is successful, the message “Authentication was successful” will be displayed as shown below.



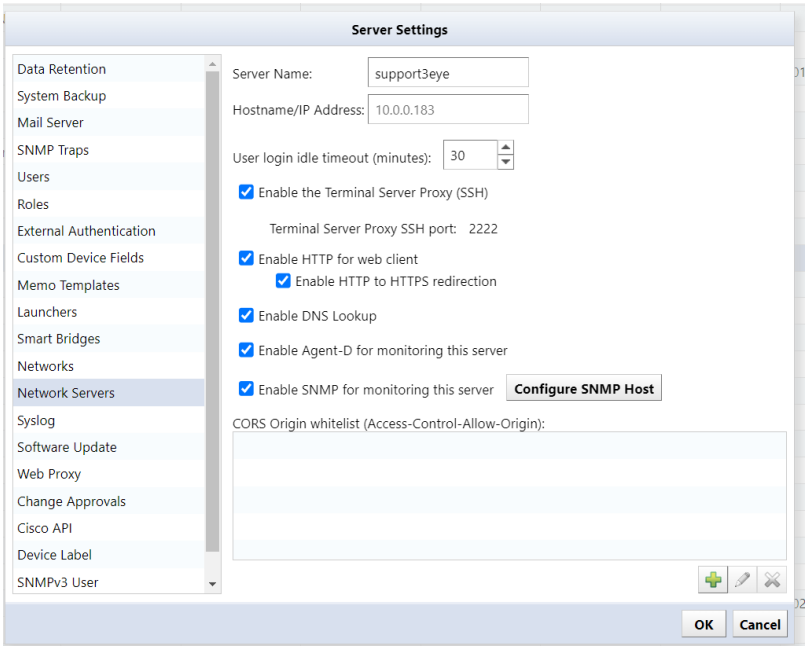
5.8 Set session timeout for users

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



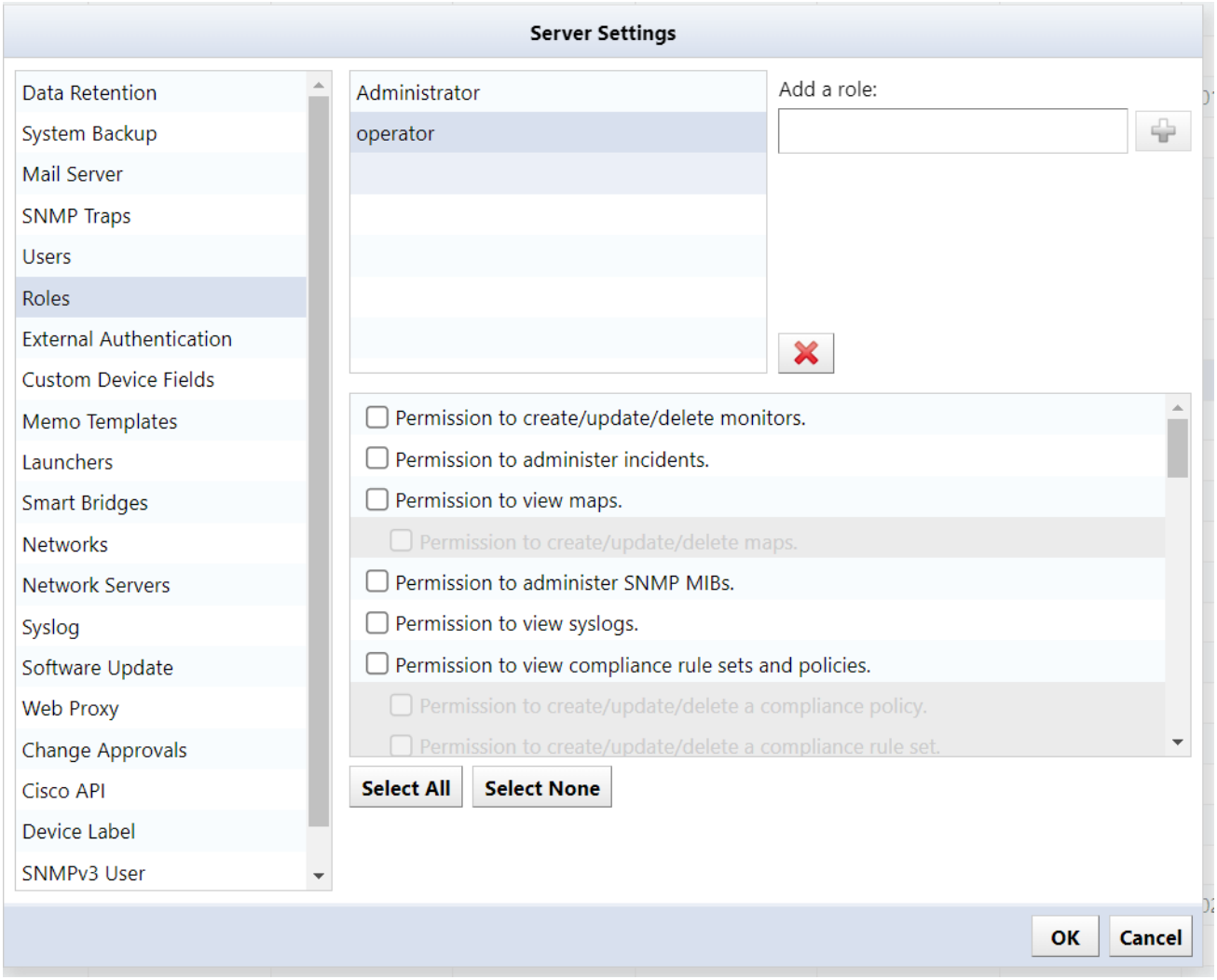
3. Click [OK].

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

4. Log out and log back in.

5.9 Remove permissions

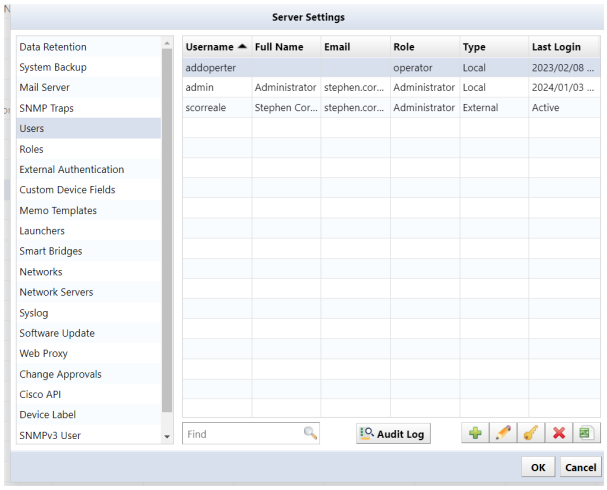
3. Select the authority name you want to delete and click  .



4. Click [OK] on the server settings.

5.10 Delete user

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



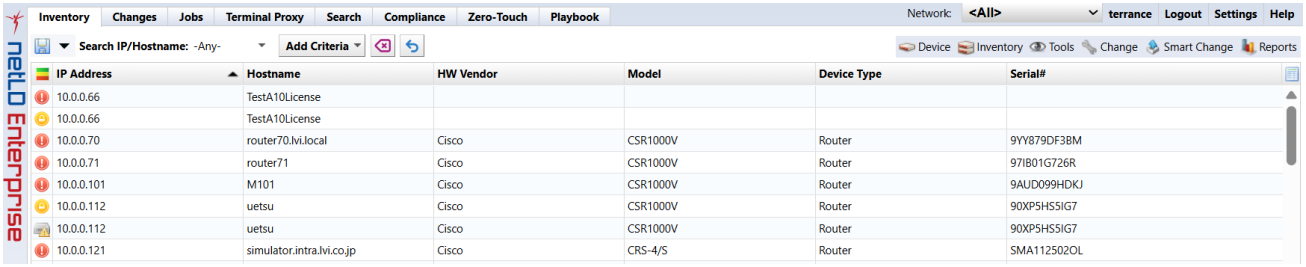
The user will be deleted.

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

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

6 Main tabs

The NetLD interface provides manages networks through 8 main tabs:



Item	Edition	Explanation
Inventory		Displays registered devices as an inventory (list).
Changes		View the configuration change history.
Jobs		Display a list of jobs.
Terminal Proxy		Displays a list of records when connecting to a device with a terminal.
Search		You can perform switch port searches, ARP searches, and interface searches.
Compliance		Configuring the device.
Zero-Touch		Display a list of incidents.
Playbook		Configure automation workflow settings for network operations.

6.1 Inventory

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

The [Inventory] tab contains 6 subtabs:

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

6.1.1 Inventory subtab

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

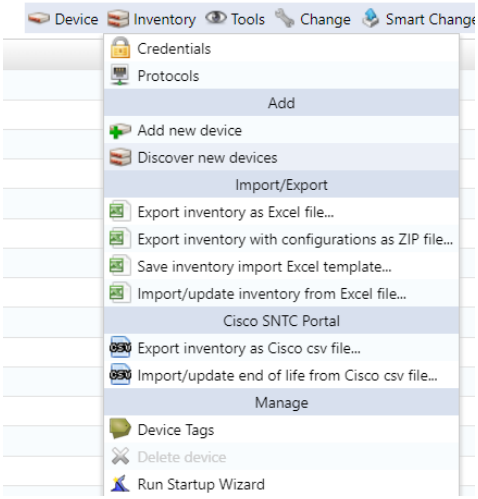
6.1.1.1 Credentials If you want to manage a device, you need to set the credentials (VTY user-name/password, SNMP community etc.) set on the managed device in NetLD.

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

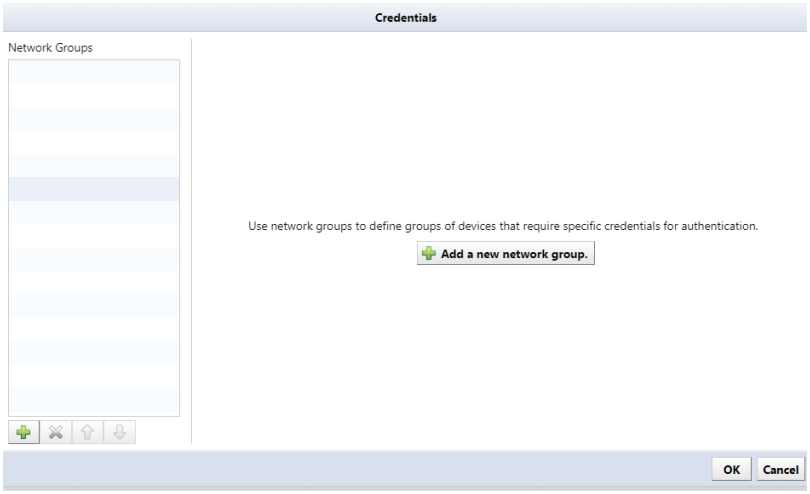
Credential Setting	Explanation
dynamic	Set common credentials for address ranges. This is useful when common credentials are set for monitored devices. Up to three credentials can be registered in one network group.
static	Set credentials for each IP address. Use this when different credentials are set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

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

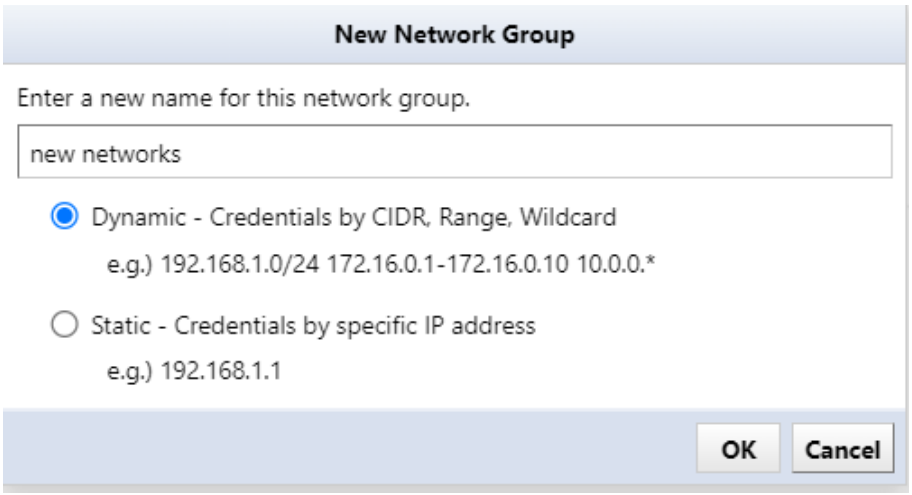
1. Click the [Inventory] main tab.
2. Click the [Inventory] subtab.
3. Click [Credentials].



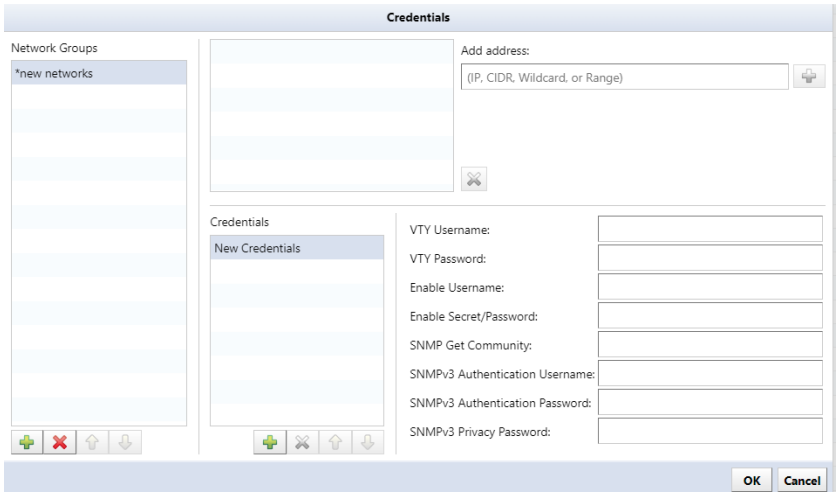
2. Click the button or [Add new network group].



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

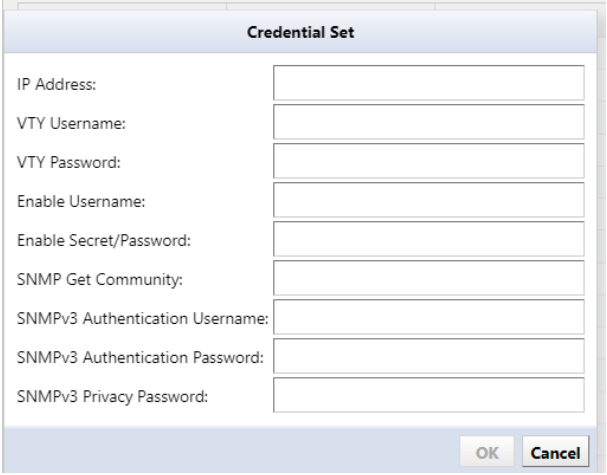


6. Enter the address range of the network group in the [Add Address] field, and click the button.



7. In the “Credentials” window, enter the IP address and set each item.

It is possible to omit items that are not required.

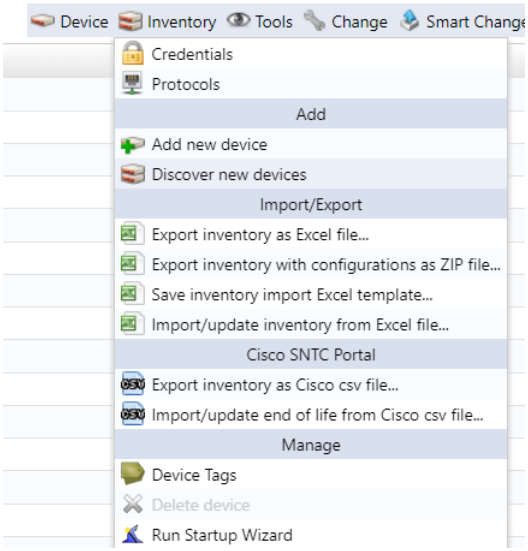


Item	Explanation
IP address	Enter the IP address of your network device.
VTY Username /VTY Password	Enter the username/password required to log in to the network device.
Enable Username /Enable Secret/Password	Enter the username/password to enter enable mode.
SNMP Get Community	Enter the SNMP community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

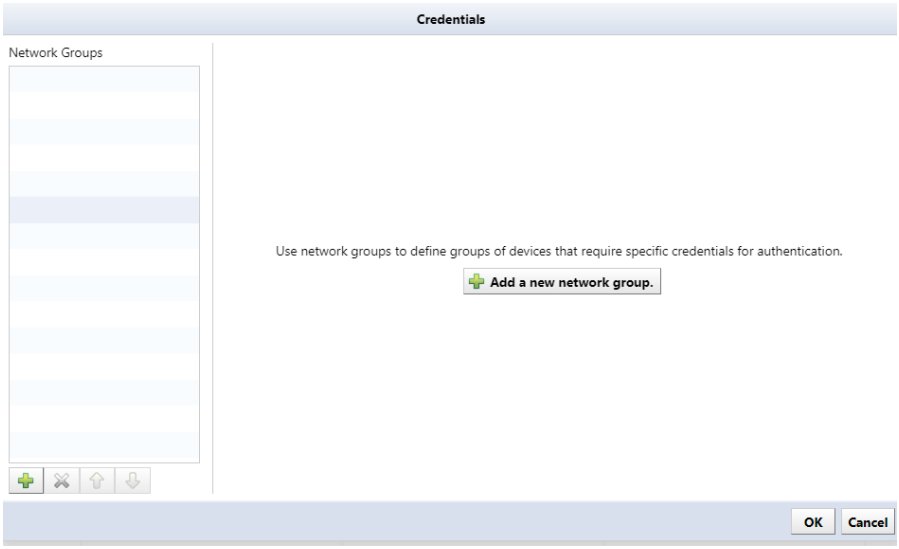
8. Click [OK] to save your settings.

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

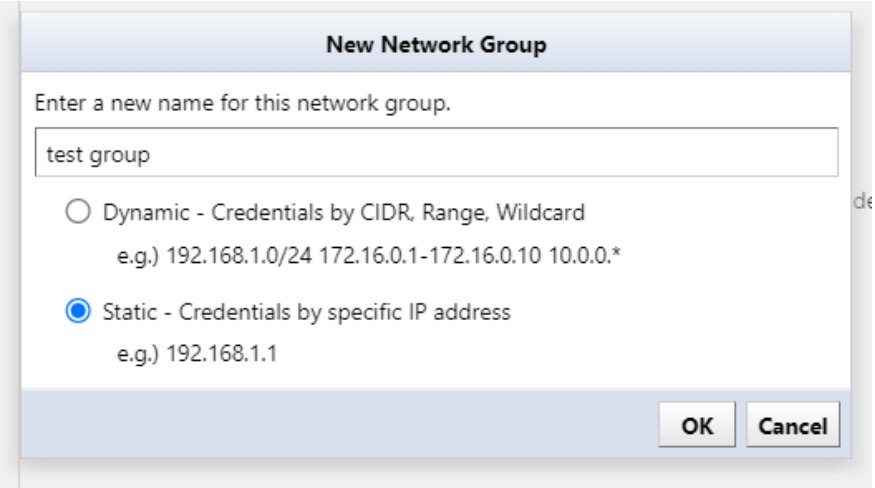
1. Click the [Inventory] main tab.
2. Click the [Inventory] subtab.
3. Click [Credentials].



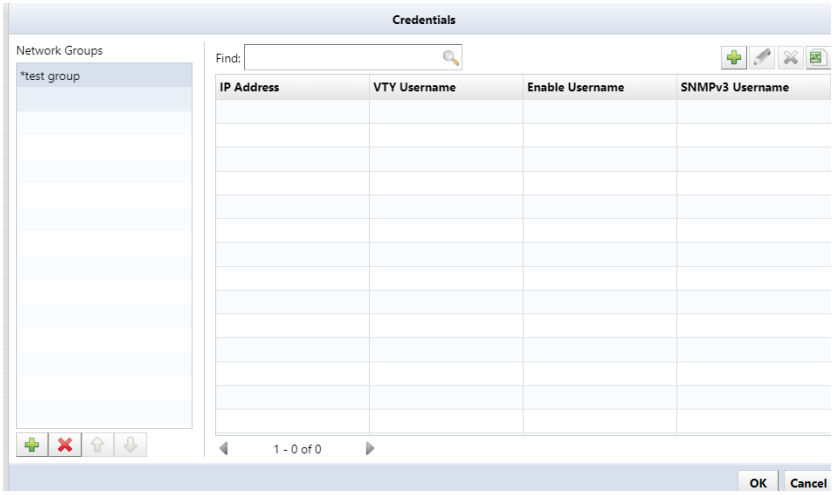
4. Click the button or the [Add new network group] button.



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

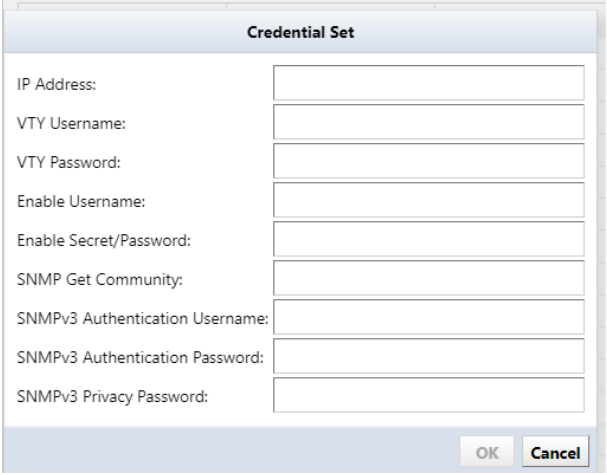


6. Click the  button.



7. In the “Credentials” window, enter the IP address and set each item.

It is possible to omit items that are not required.



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

8. Click [OK] to save your settings.

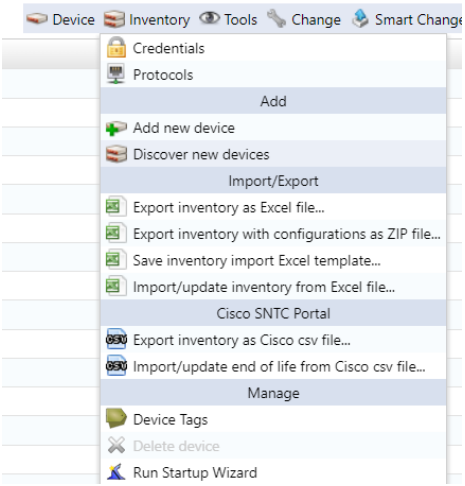
6.1.2 Add device

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

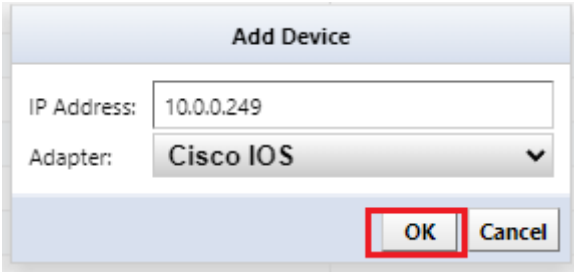
Method	Explanation
manual	Add a device by directly entering the device's IP address. Add one unit at a time.
discovery	Automatically discover and add devices within the specified IP address range.
import	This function reads device data from an XLSX file. Export the template file for import and enter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

6.1.2.1 Register one device

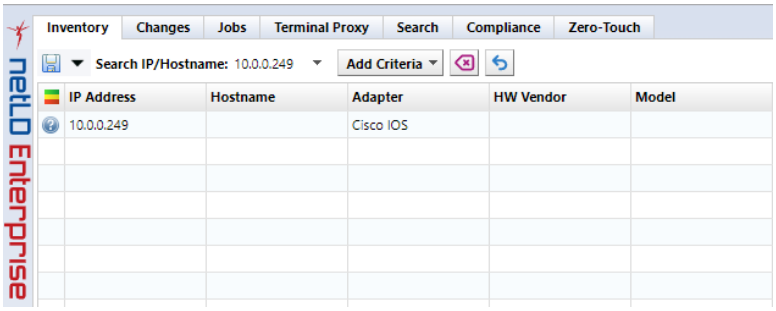
1. Click the Inventory > [Add new device] buttons.



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

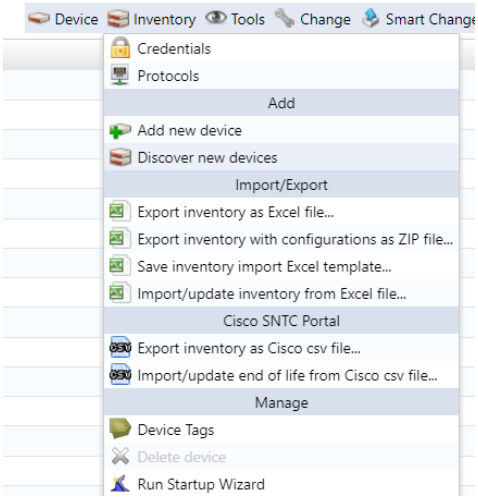


Once NetLD completes collecting information from the monitored devices, the added devices will be added to the device list in the Inventory tab. The device will be added even if it is not possible to communicate with the target IP address. However, the host name and interface information will not be obtained.

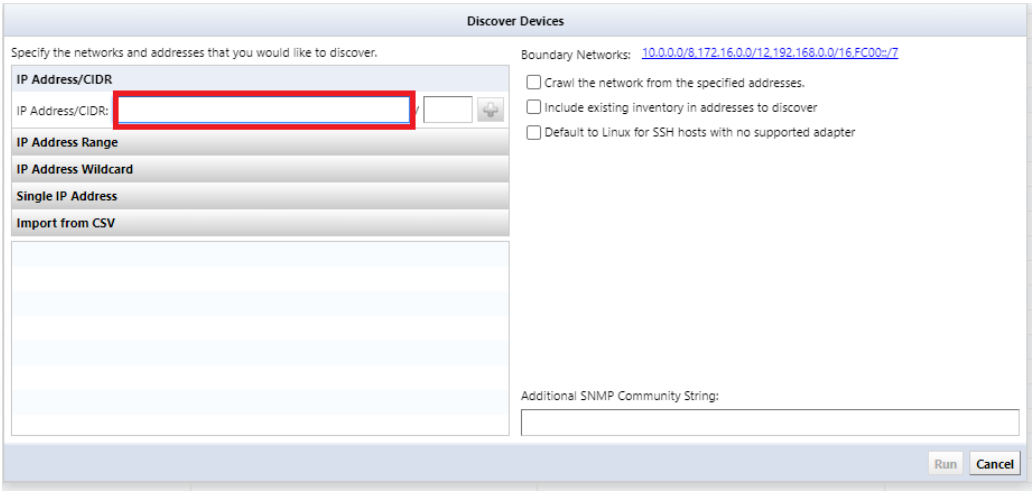


6.1.2.2 Discover devices on your network

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



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

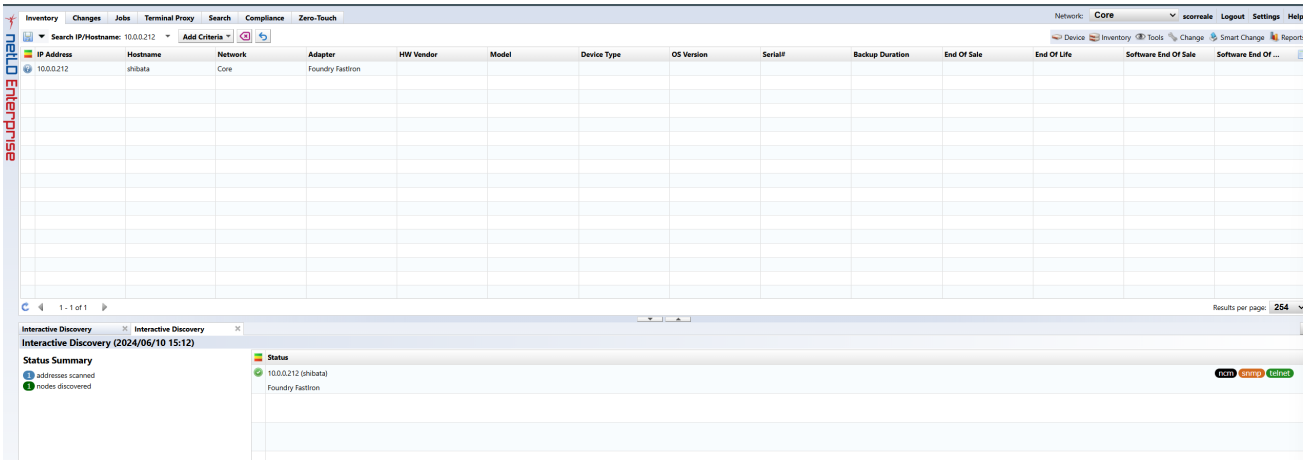


Item	Explanation
Refer to the device's routing table and add discovery targets	Add a discovery target network by referring to the discovered device's routing table.
Refer to the routing table of already registered devices and add discovery targets.	If there is already a registered device, add a discovery 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.

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

3. Click [Run].

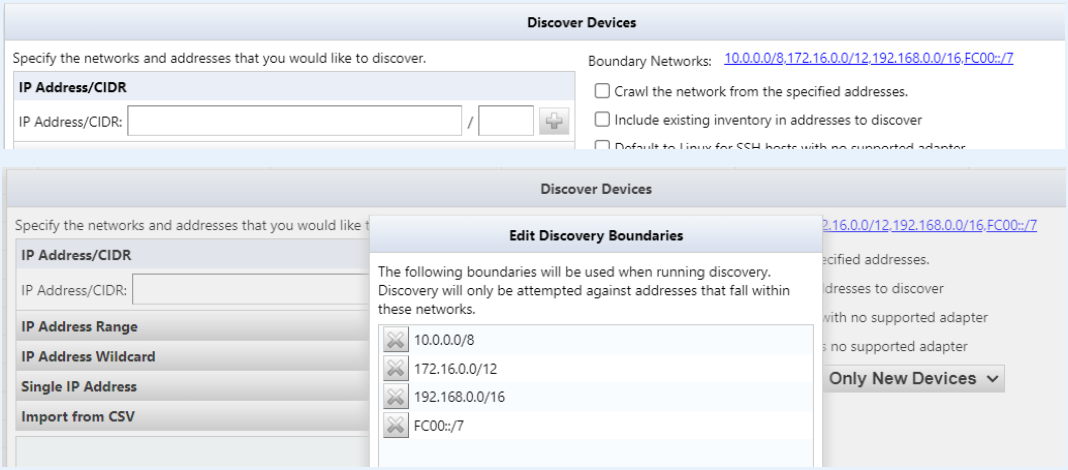
4. Discovery will start, and the discovery results will be displayed at the bottom of the screen.



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

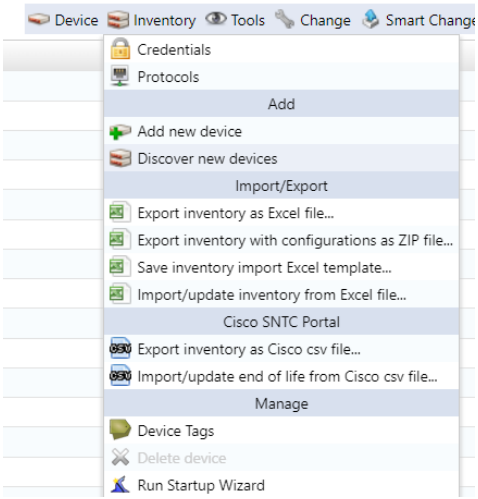
Note

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



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

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



The file opening screen will be displayed.

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

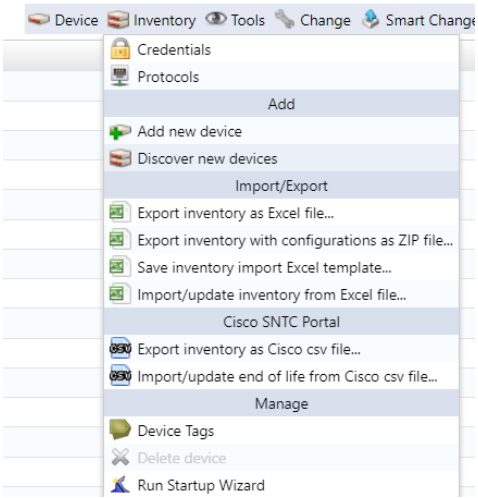
The file name will be “NetLD-inventory-template.xlsx” and will be saved in XLSX file format.

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																	

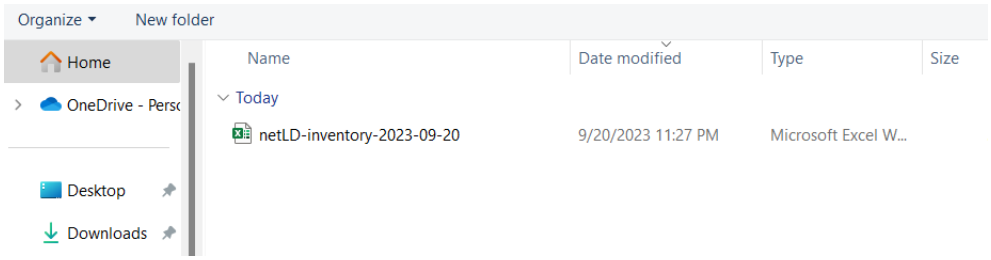
Item	Explanation	Requirements	Input example
IP Address	Enter the device's IP address.	required	192.168.1.10
Network	Select the network name to which you want to add the device.	required	Default
Adapter ID	Select your device's adapter. (In the current version, there is no need to specify this item.)	-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

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



A file selection dialog will be displayed.

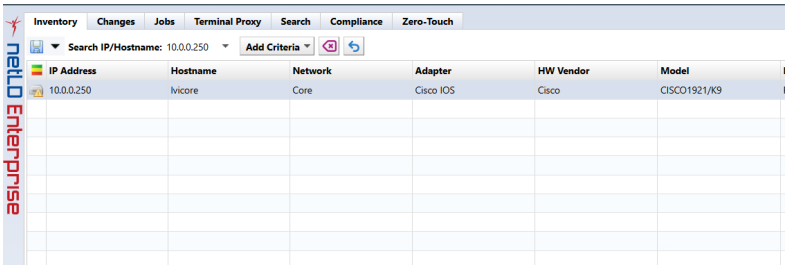
5. Select the edited file and click [Open].



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

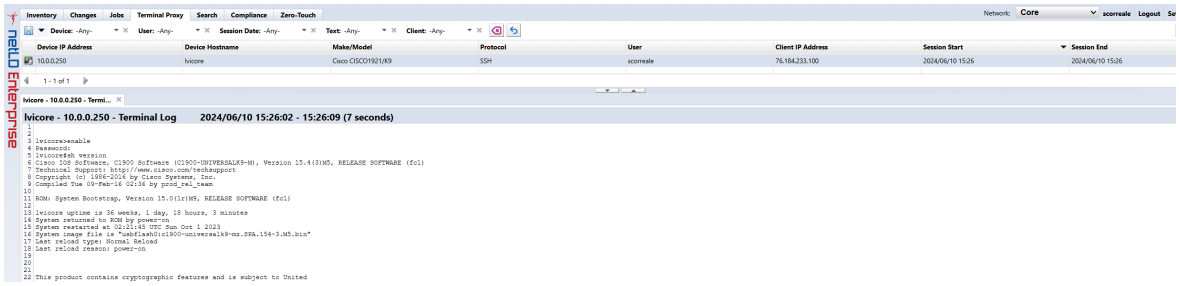
6.1.2.3.1 Check the operation log

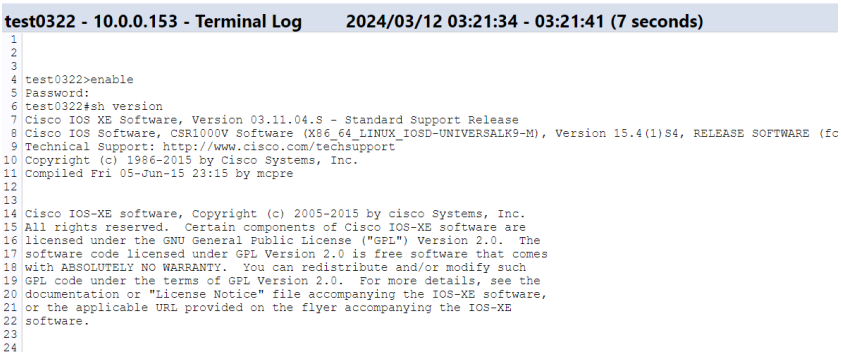
1. Select the Terminal Proxy tab.



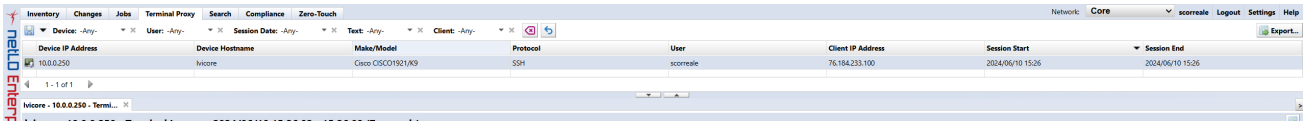
2. Doubleclick the log you want to view from the list.

You cannot check the session log while connected.





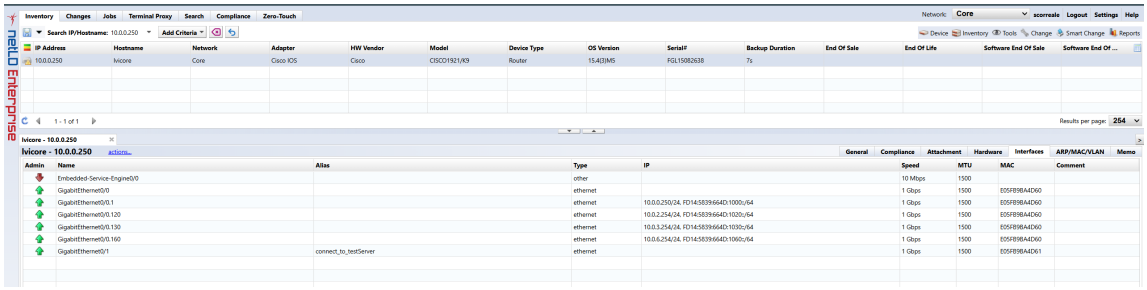
Click [Export] at the top right of the log screen to save session data as a text file. The file name is "`termlogs".*YYYY-MM-DD*.zip`" and is compiled in ZIP file format. "`*YYYY-MM-DD*`" indicates the date of saving.



6.1.3 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,doubleclick the device for which you want to check interfaces.



6.1.4 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.

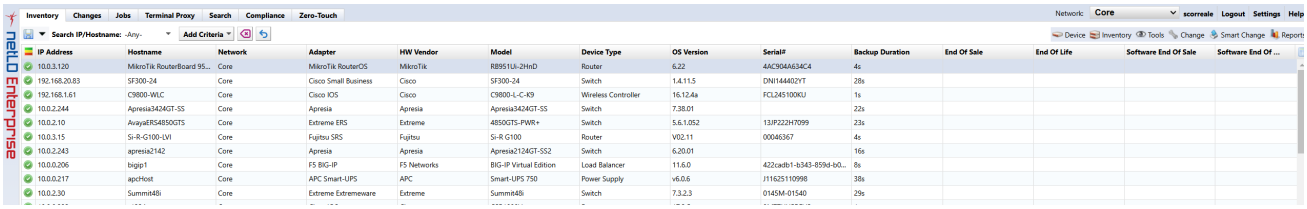
6.1.4.1 Prerequisites Before performing a configuration backup, ensure the following requirements are met:

- login username and password have been set. Refer to the **Set Credentials** sections to make sure the credentials are set.
- The model supports configuration backup by NetLD.

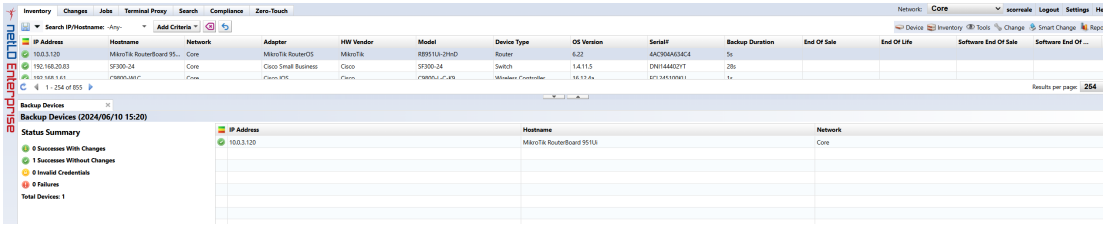
  For a list of supported devices, see the following web page:

  https://logicvein.com/supported-devices

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



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



The status summary list for backup execution is as follows:

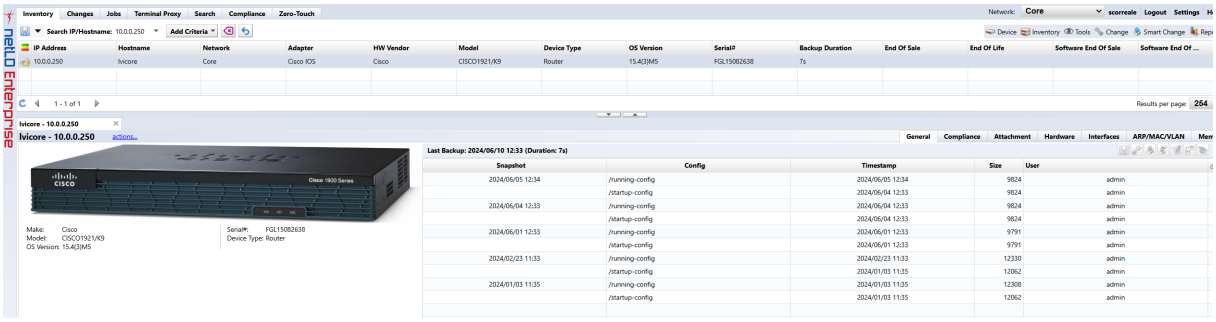
Icon	Explanation
	Backup successful, changes made. Displayed when a difference is detected between the last backup and the configuration on the device. It will also be displayed during the first backup.
	Backup successful, no changes. Displayed when the configuration data on the device is the same as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

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

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

6.1.4.4 Check the obtained configuration

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

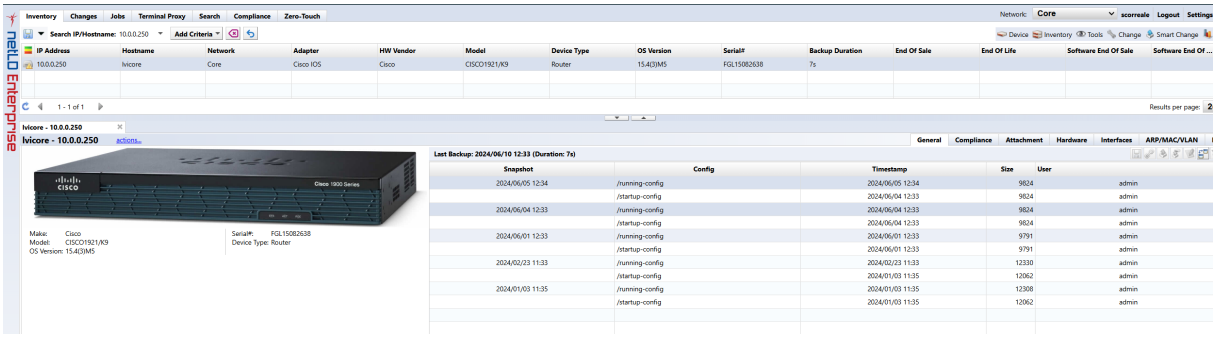


You can check the contents by doubleclicking on the [Config] button.

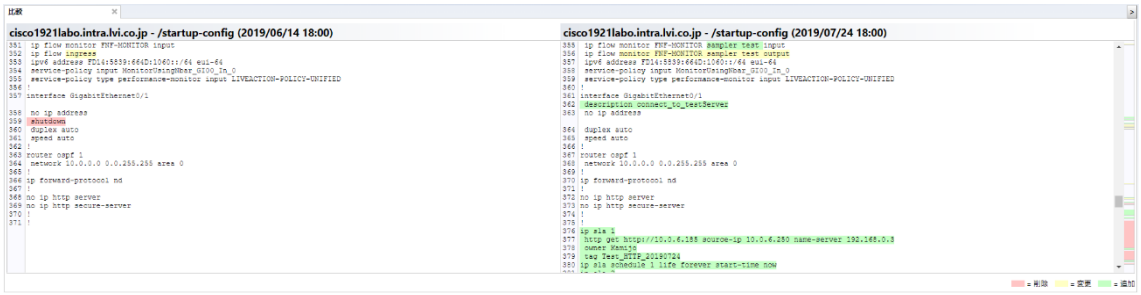
6.1.4.5 Configuration Comparison

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

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



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



6.1.5 Device Groups

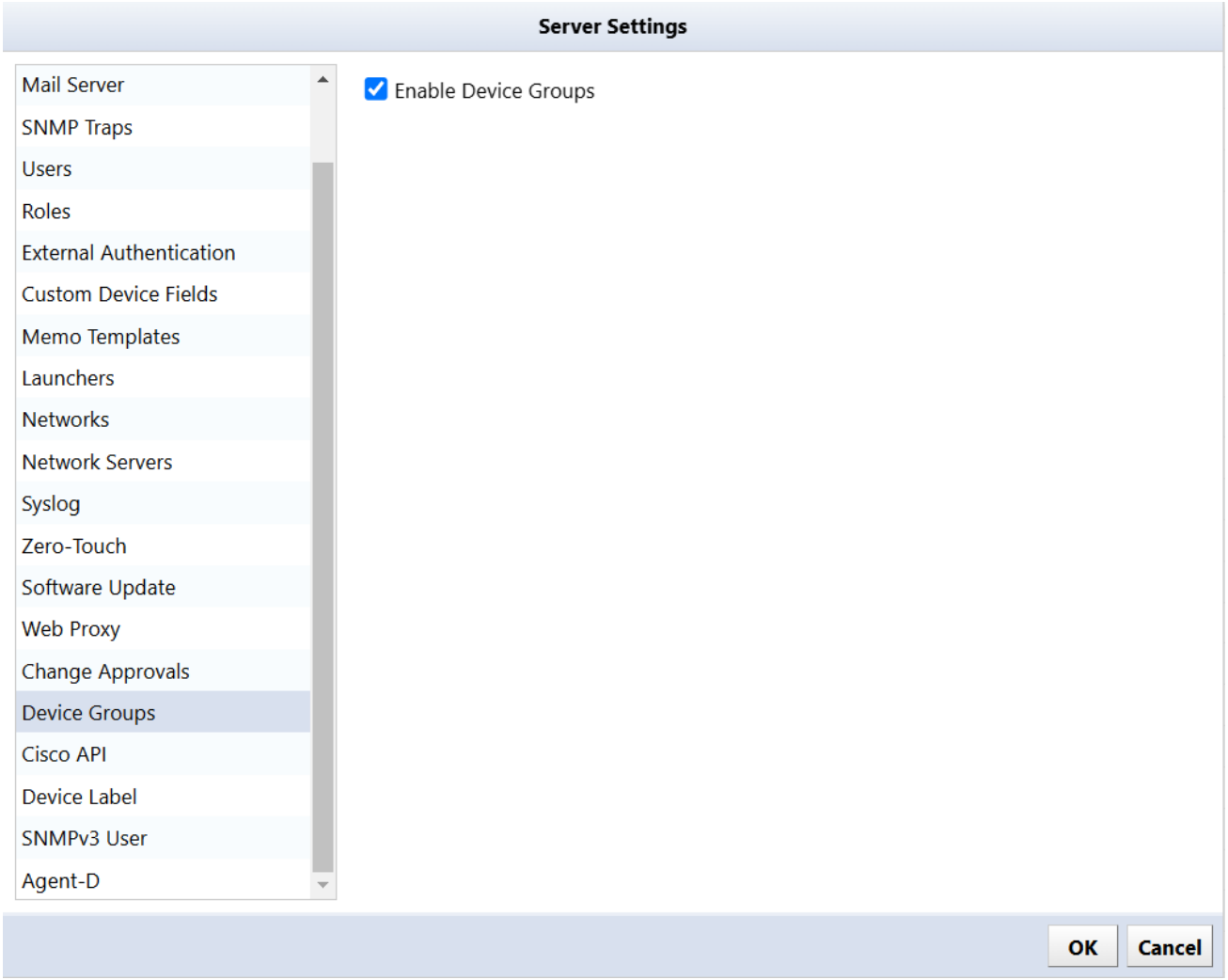
Device groups is a collection of devices grouprd together for easier administration and monitoring. Here are some key points:

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

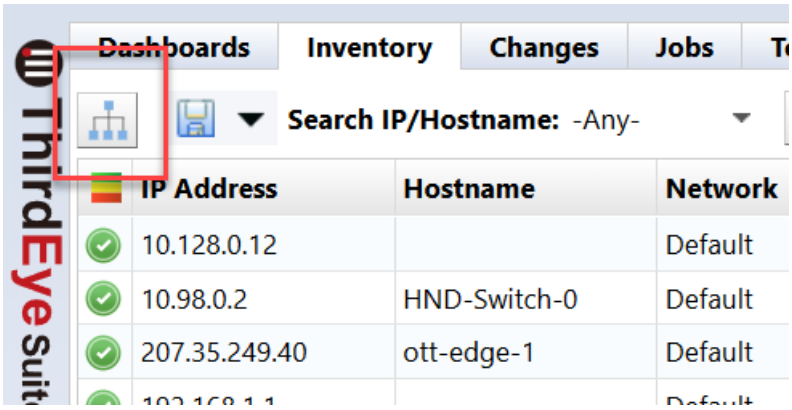
6.1.5.1 Setup and configuration

1. In the Global Menu, click Settings > [Server Settings], then clickDevice Groups in the left side-panel.

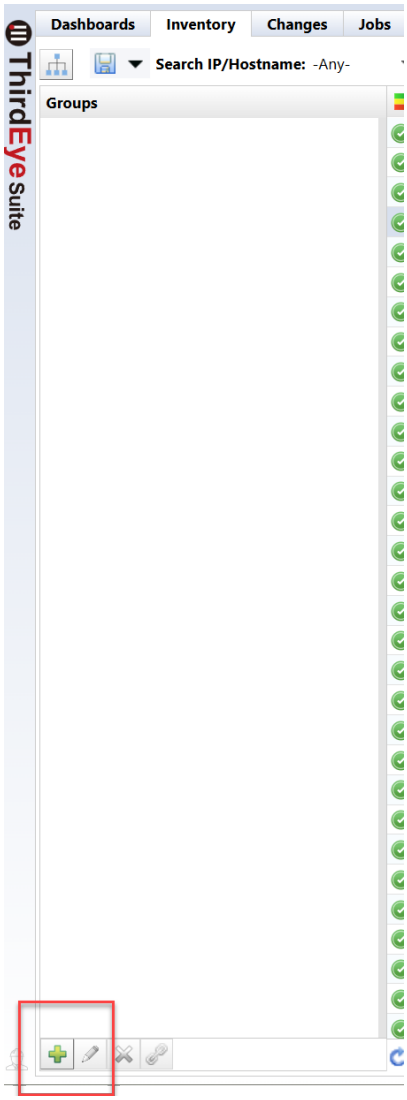
(Ensure “Enable Device Groups” is checked.)



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



4. Click the button in the bottom left corner.

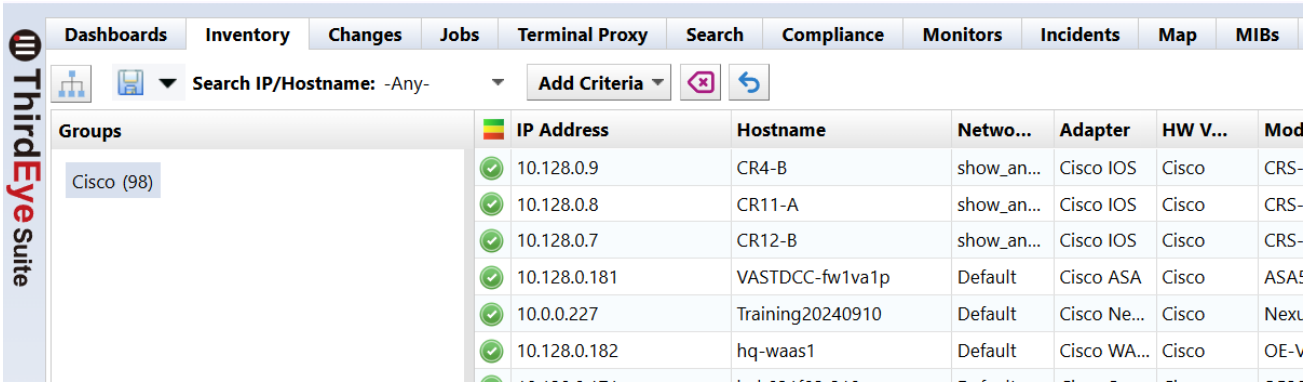


5. In the popup window, enter a name for the grouping (“Cisco” in the screenshot below).

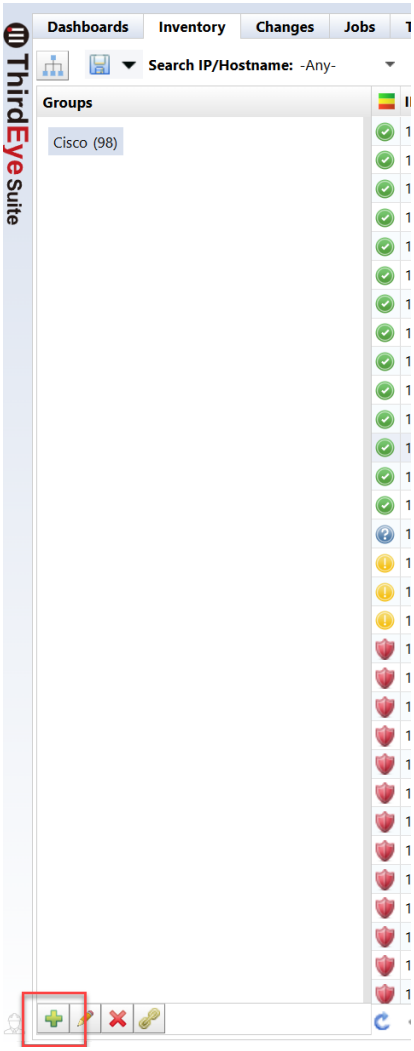
Sharing pulldown menu:

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

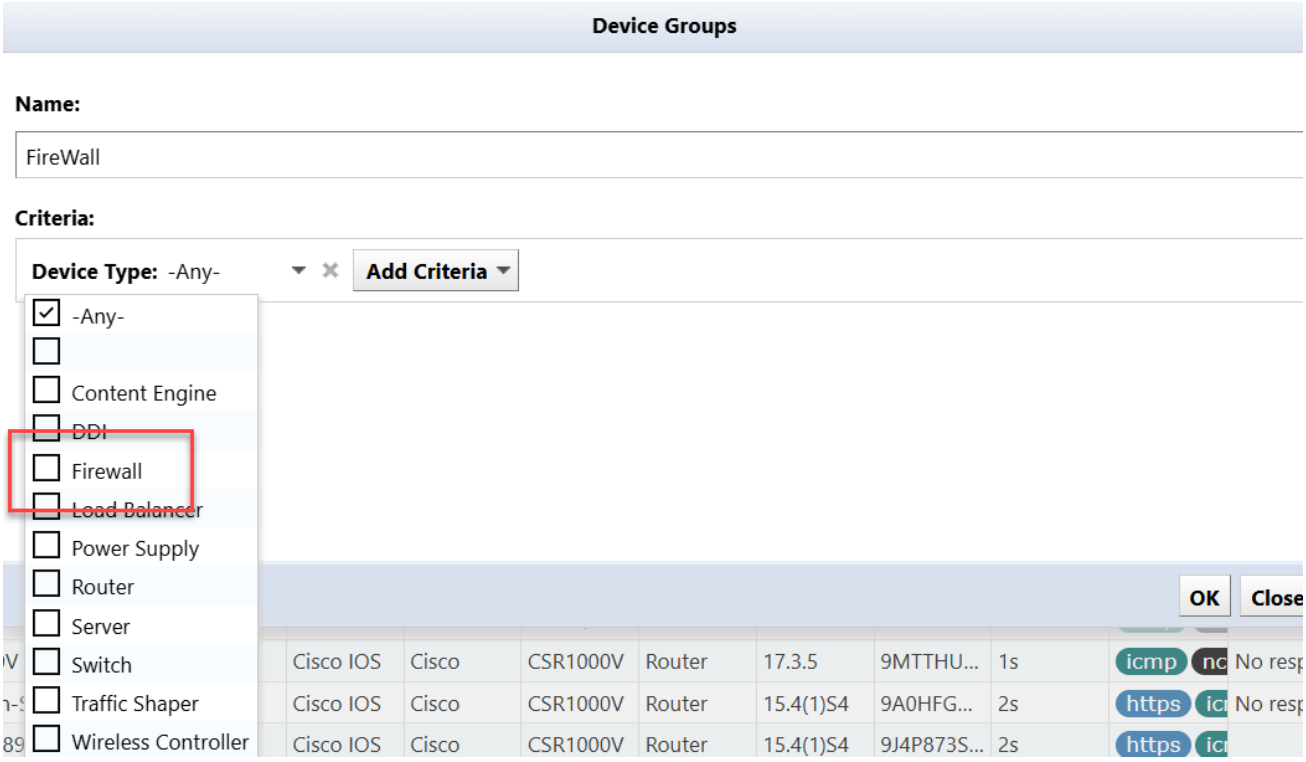
6. In the [Groups] sidebar, click on the vendor name, and those devices will appear in the Inventory tab.



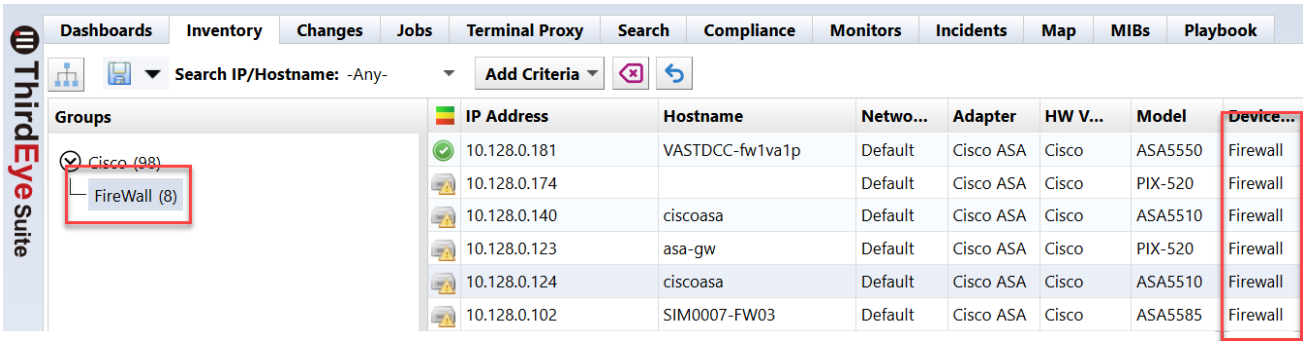
7. To make subgroups, click on the vendor name, and click on the  at the bottom of the page.



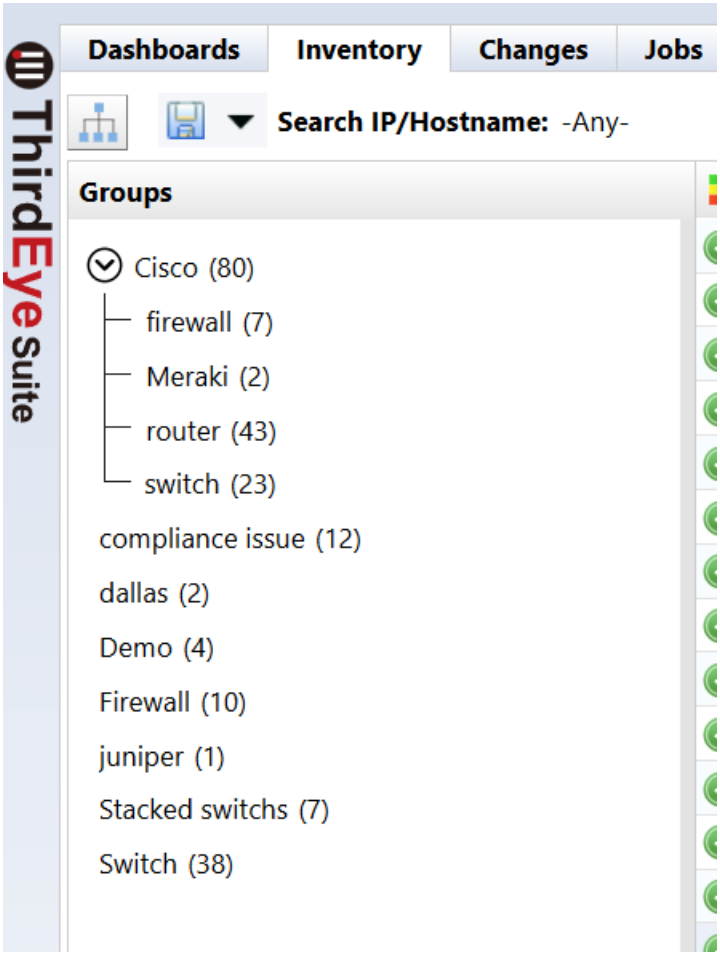
8. Enter a “Name” for the subgroup, (for example “FireWall” in the example below).
9. In the [Criteria] > [Device Type] left sidebar, select your new subgroup (“FireWall” in the example below).
10. Click [OK].



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

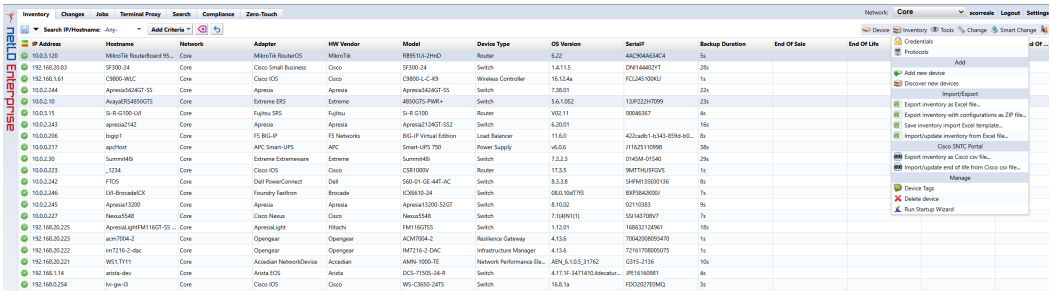


You can use Device Groups to isolate the devices you want to view, monitor, or run jobs against.



6.1.6 Remove device

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



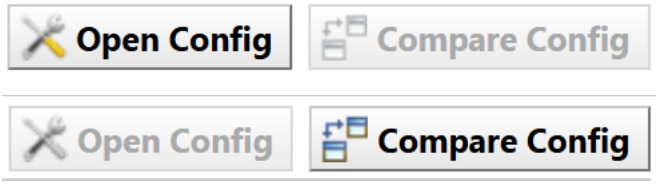
2. With the device selected, click Inventory > [Delete Device].

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

6.2 Changes

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

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



6.3 Jobs

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

The Jobs tab contains four main buttons that facilitate this:

- [Open Results]
- [Compare Results]
- [Cancel]
- [OJob Approvals Log]

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

6.3.1 Job management

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

The Job History subtab has the following buttons:

Button	Edition
Open Results	Opens the execution results of the selected job.
Compare Results	Compare the results of two selected jobs.
Cancel	Cancels the selected running job.

Button	Edition
Job Approvals Log	View the job approval log.

The Job Management subtab has the following buttons:

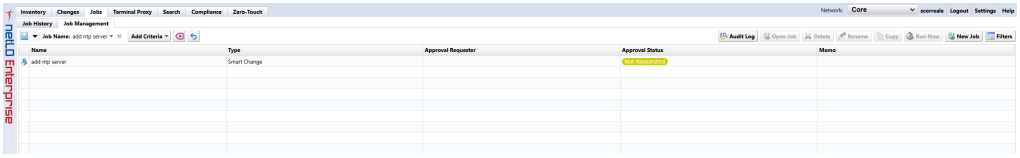
Button	Explanation
Audit Log	View audit log for changing job settings
Open Job	Open the properties of the selected job.
Delete	Delete the selected job.
Rename	Renames the selected job.
Copy	Copy an existing job and create it as new job.
Run Now	Run the selected job immediately.
New Job	Create a new job.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

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

Job creation procedure

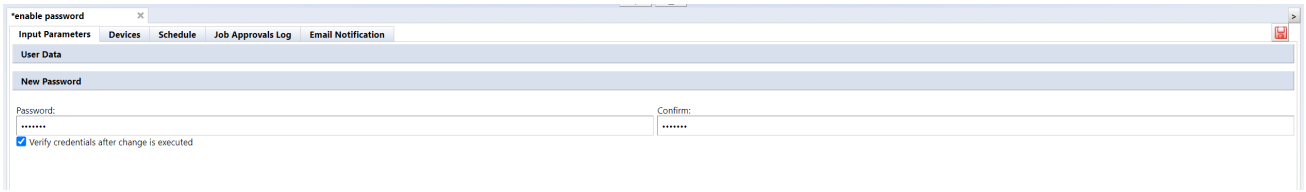
1. Decide on a job name and select the functions you want to use.
2. Enter the required parameters.
3. Select the target device.
4. Finally, enter the job trigger (execution frequency).

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



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

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

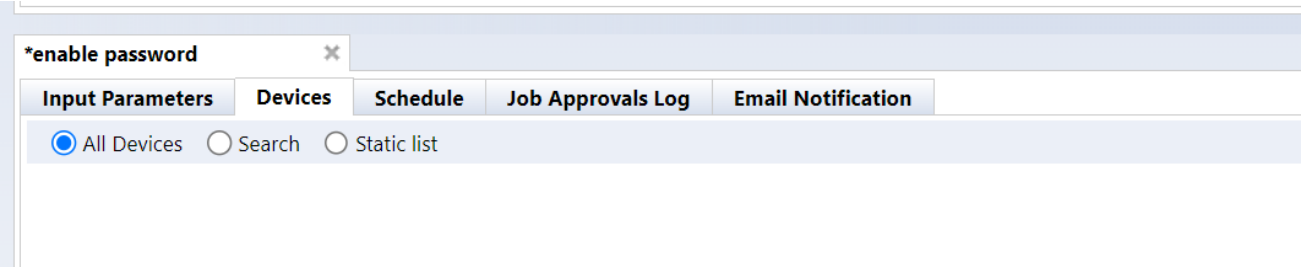


6.3.1.1.3 Select target device Select the device on which you want to run this job on the [Devices] subtab. There are three selection methods:

- All devices
- Search
- Static list

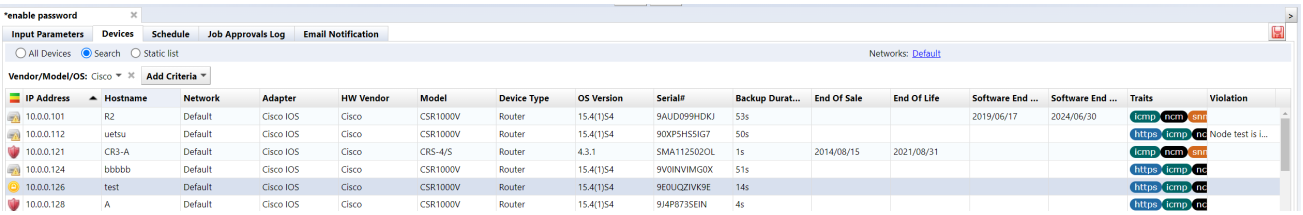
All devices

This applies to all registered devices.



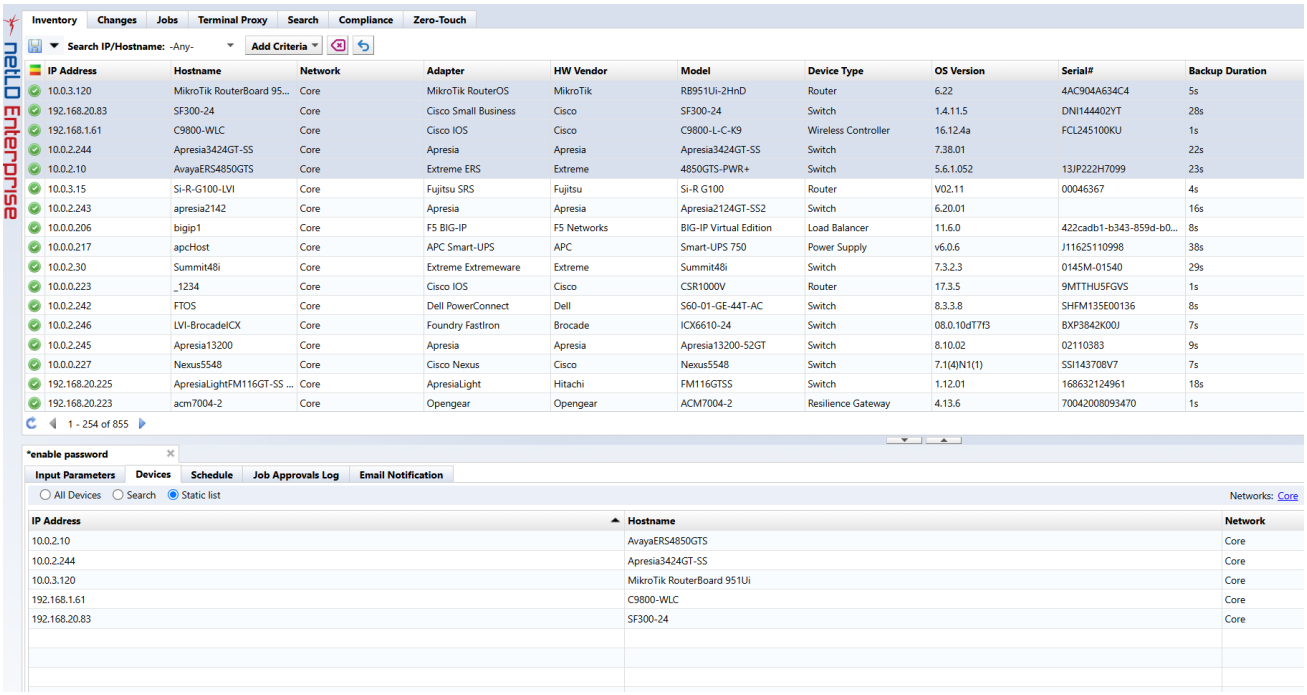
Search

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

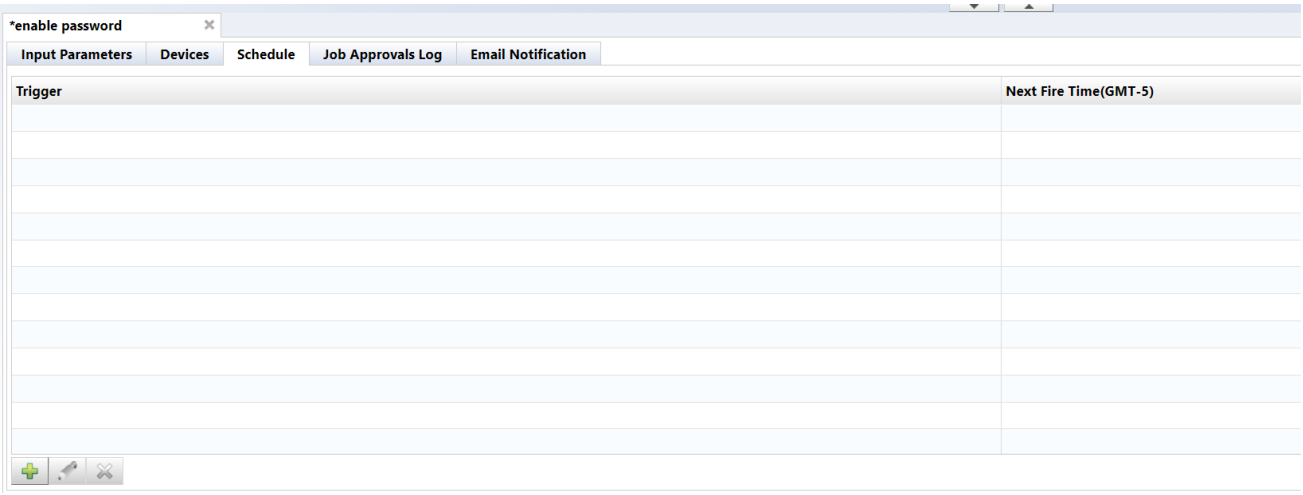


Static list

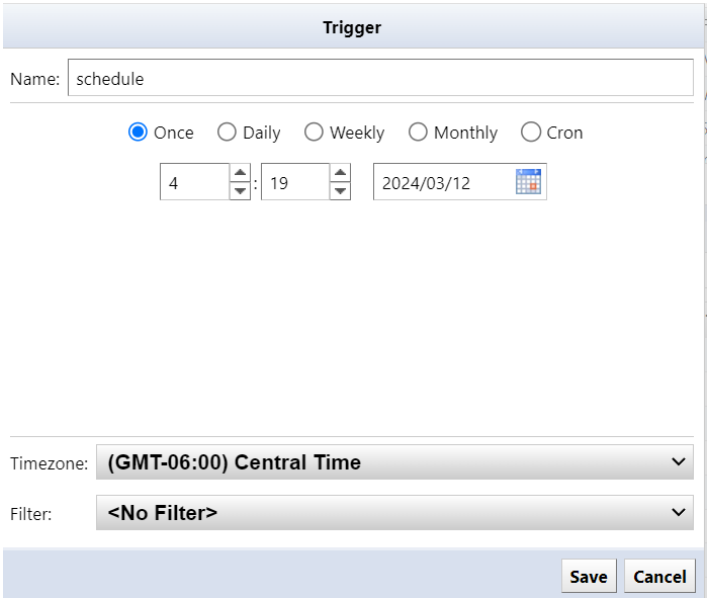
In the static list, you can add the devices selected in the [Devices] tab, and the added devices will be targeted.



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



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



Item	Explanation
name	Trigger name
time	Time and date to run the job
Schedule	Select from the following 5 types of execution schedules: - **Once**: Execute only once at the date and time set in the time. - **Daily**: Execute every n days (starting from the 1st of the month) - **Weekly**: Execute on a specific day of the week

Item	Explanation
	- **Monthly**: Execute every specified month - **Cron**: Run at the specified date and time in cron format
time zone	Time zone
filter	Select the registered schedule filter in “Filter Settings”. Timings that match this filter will be removed from the trigger.

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

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

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

6.3.1.3 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.

6.3.1.3.1 Set permissions for approval function

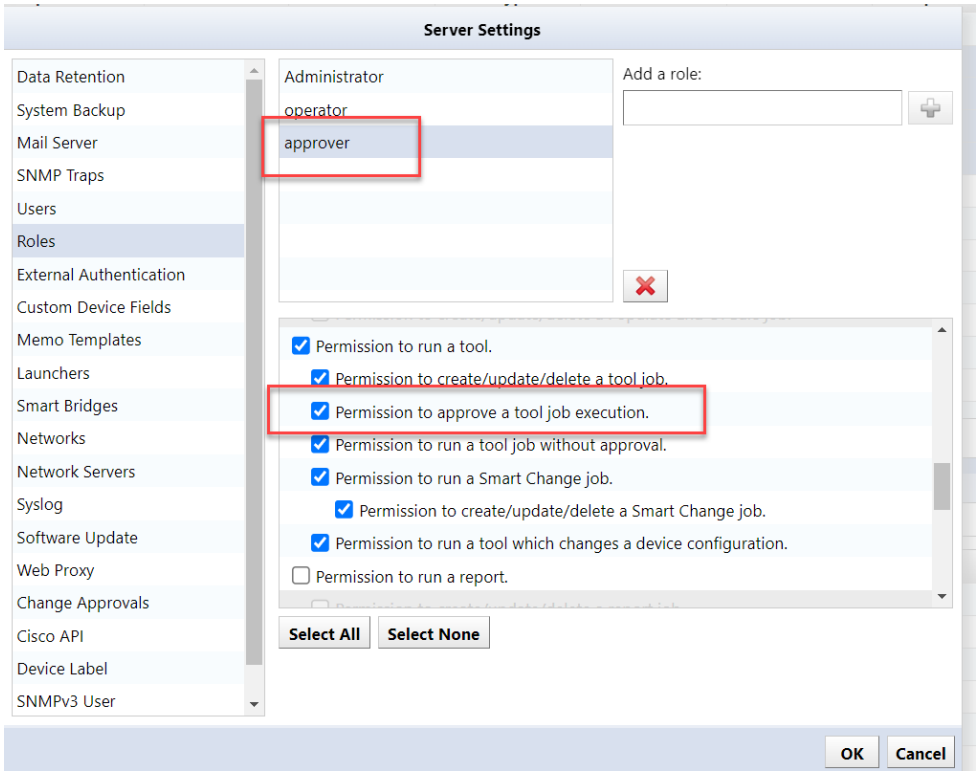
Set approvers for registered permissions. Users assigned the configured permissions can approve jobs.

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

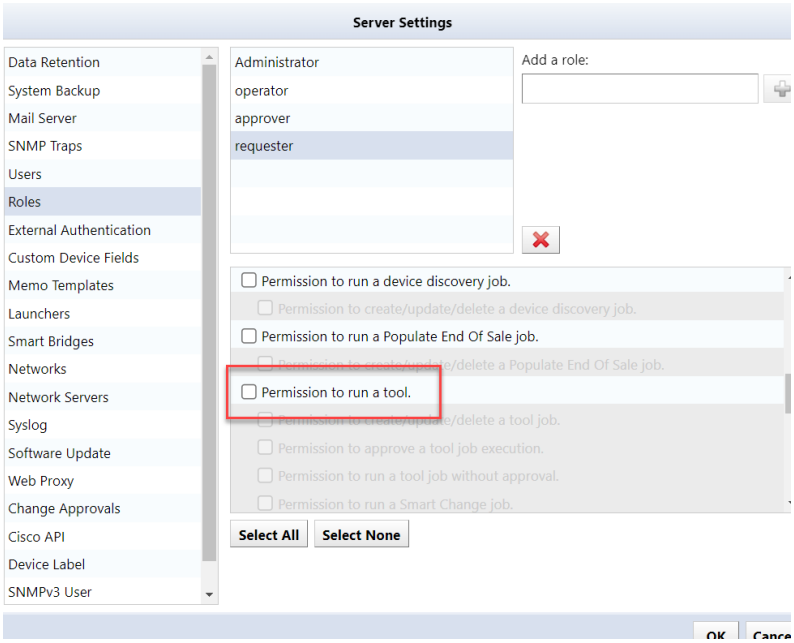
The authority related to the approval function consists of the following two authority contents.

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

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



When setting the applicant's authority, uncheck "Permission to run a tool".



6.3.1.3.2 Submit an approval request (submit a job)

Applicants can request approval when creating or editing a job.

Create/edit jobs.

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

Display example of the [Job approval status] column

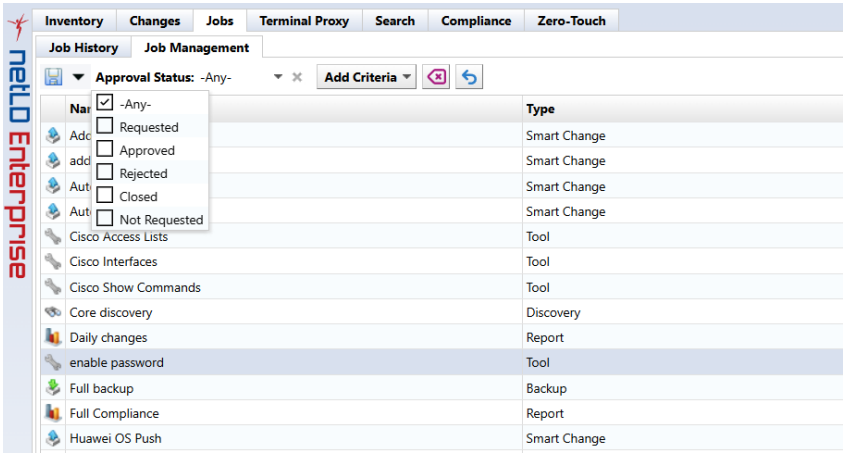
List of display contents in the [Job approval status] column

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

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

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

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



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

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

6.3.1.3.4 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.

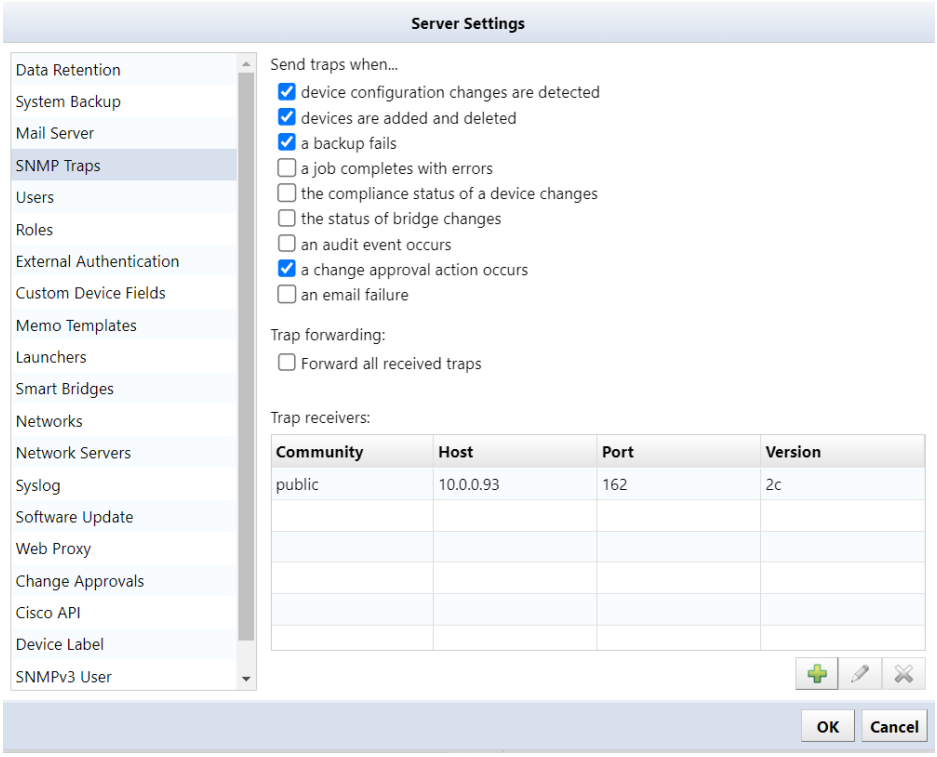
The [Job Approval Log] button is enabled only for jobs executed after approval.

6.3.1.3.5 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.

SNMP trap settings

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

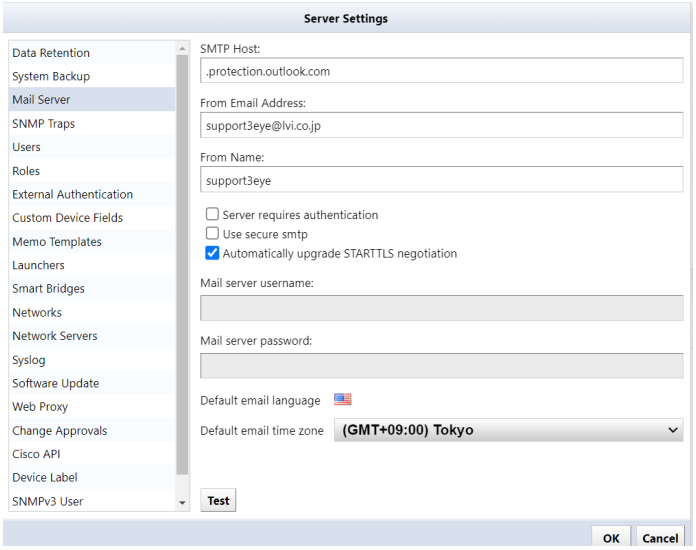
A trap is sent when a job is requested/executed/approved/rejected/closed.



Send e-mail

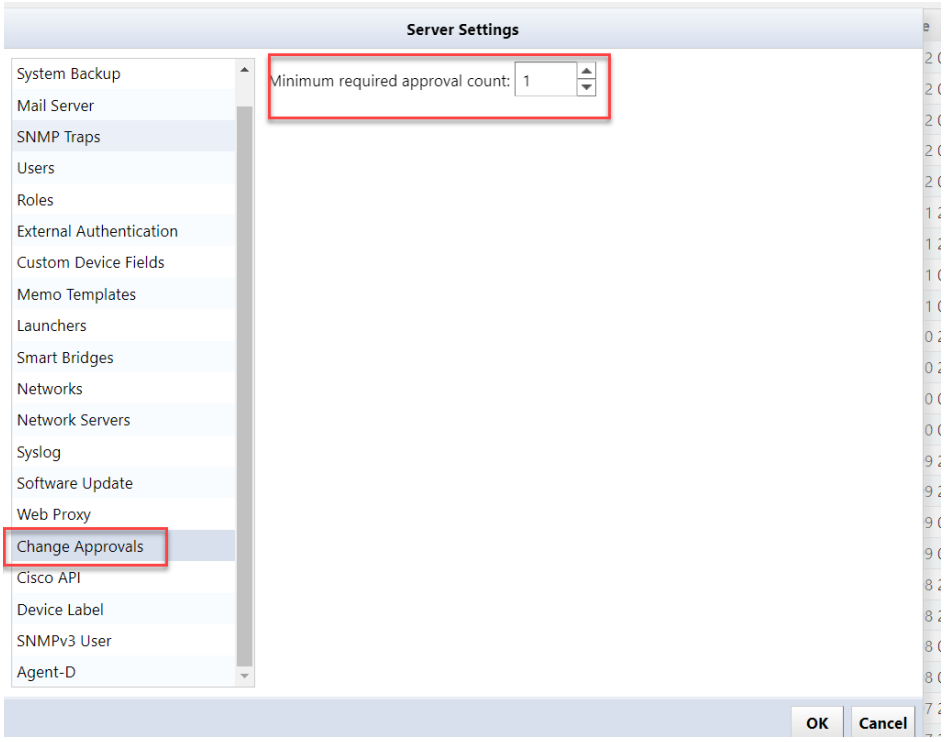
By setting the email address in the user edit on the server settings screen, you can send an email when an approval event occurs. An email will be sent when a job is requested/submitted/approved/rejected/closed.

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



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

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



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

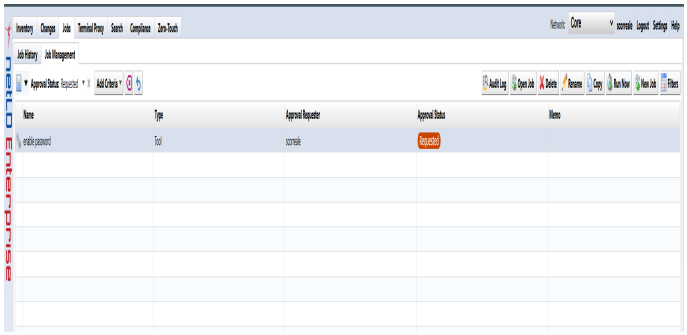
- Report
- Discover
- Neighbor
- Backup
- Agent-D
- Tool
- information such as “when”, “who”, and “what was done” is recorded

[Column list]

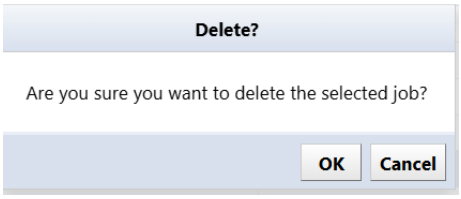
Item	Explanation
Name	Displays the name of the job.
Type	Displays the job type.
Start Time	Displays the start date and time when the job was executed.
End Time	Displays the completion date and time when the job was completed.
User	Displays the name of the user who executed the job.

6.3.2 Delete job

1. Click the Jobs > Job Management tabs.



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

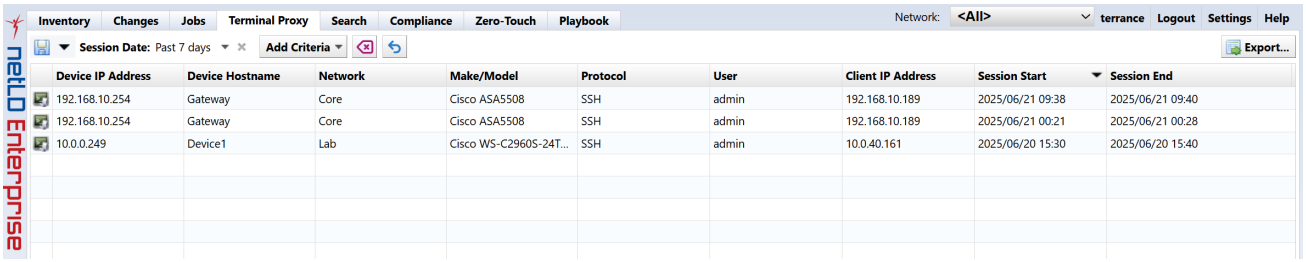


The selected job will be deleted from the job management list.

6.4 Terminal Proxy

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

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



The Terminal Proxy tab provides information about devices such as:

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

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

6.4.1 Make an SSH/Telnet connection to the device

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

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

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

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

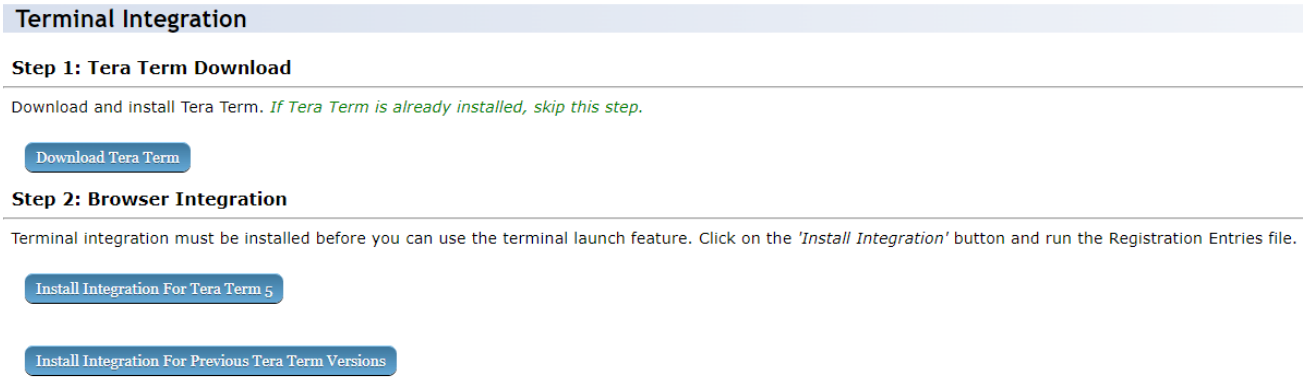
This preparation can be done from the screen that appears when you start the terminal proxy for the first time. The installation procedure for **Browser Integration**”** is described below.

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

1. Click [Install Integration] and download registration entries file.

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

2. Run the downloaded registration entries file.



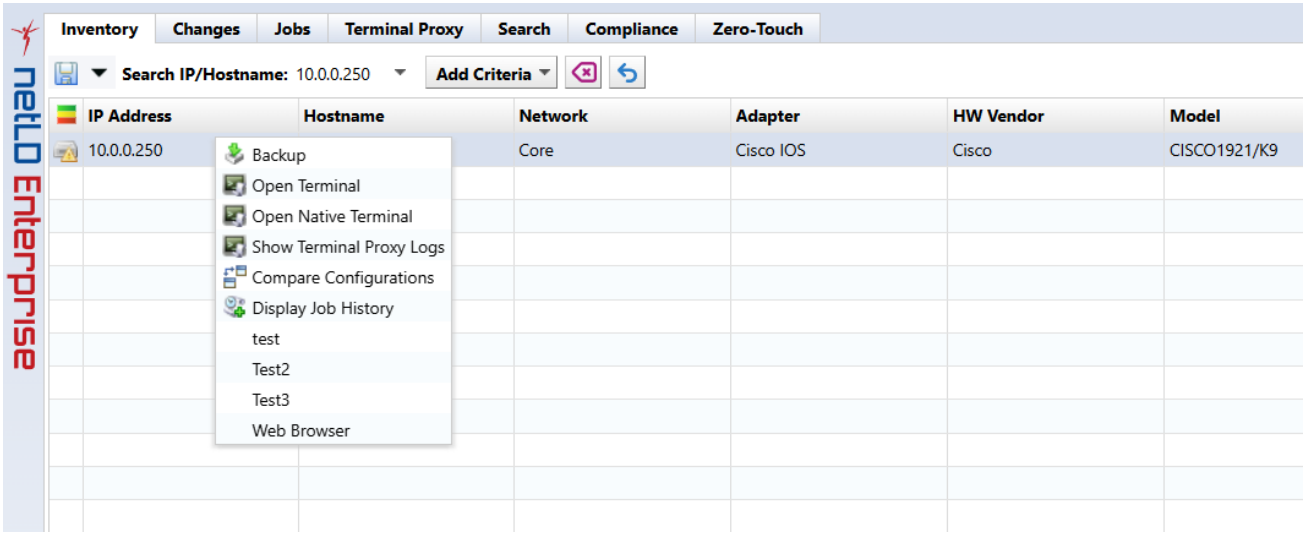
> **Note**
>
> Regarding “Browser Integration”, you may need to reconfigure if you clear your browser’s cache or update NetLD.

Setup is now complete.

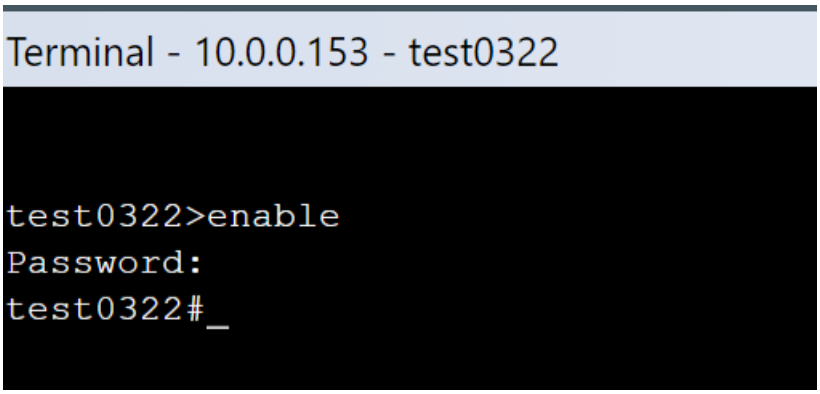
6.4.1.2 Start the terminal proxy If a device configuration backup has been obtained when you start the terminal proxy, you can skip selecting the protocol and entering the user name/password after starting the terminal proxy.

6.4.1.2.1 Use web browser

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

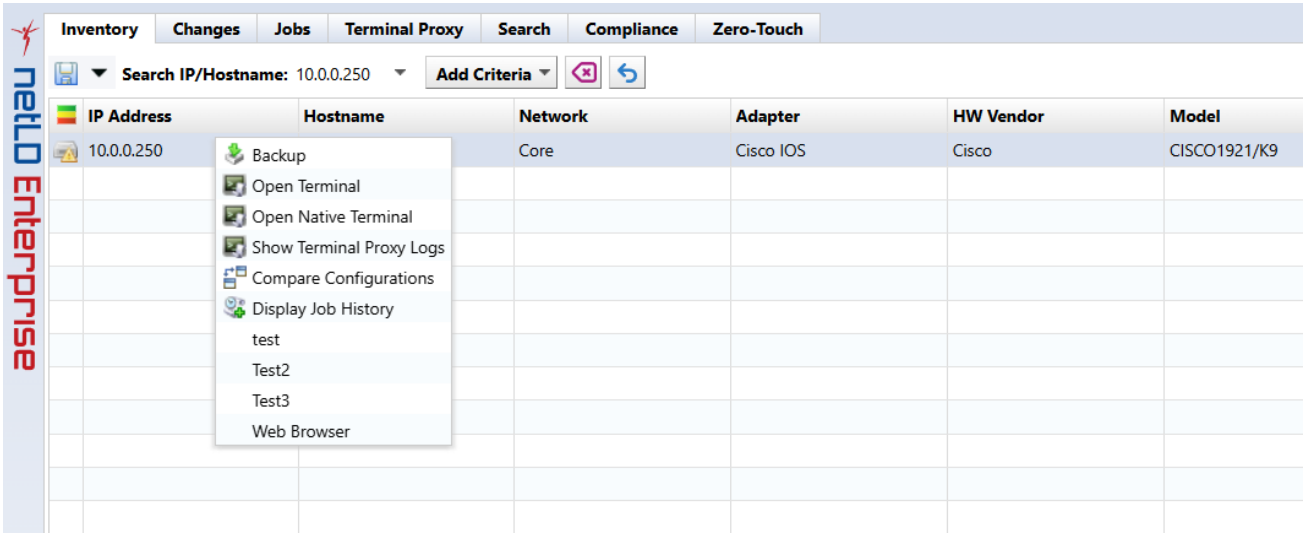


3. The terminal will open in a separate browser tab, and the device's login screen will be displayed. Enter your username and password to log into your device.

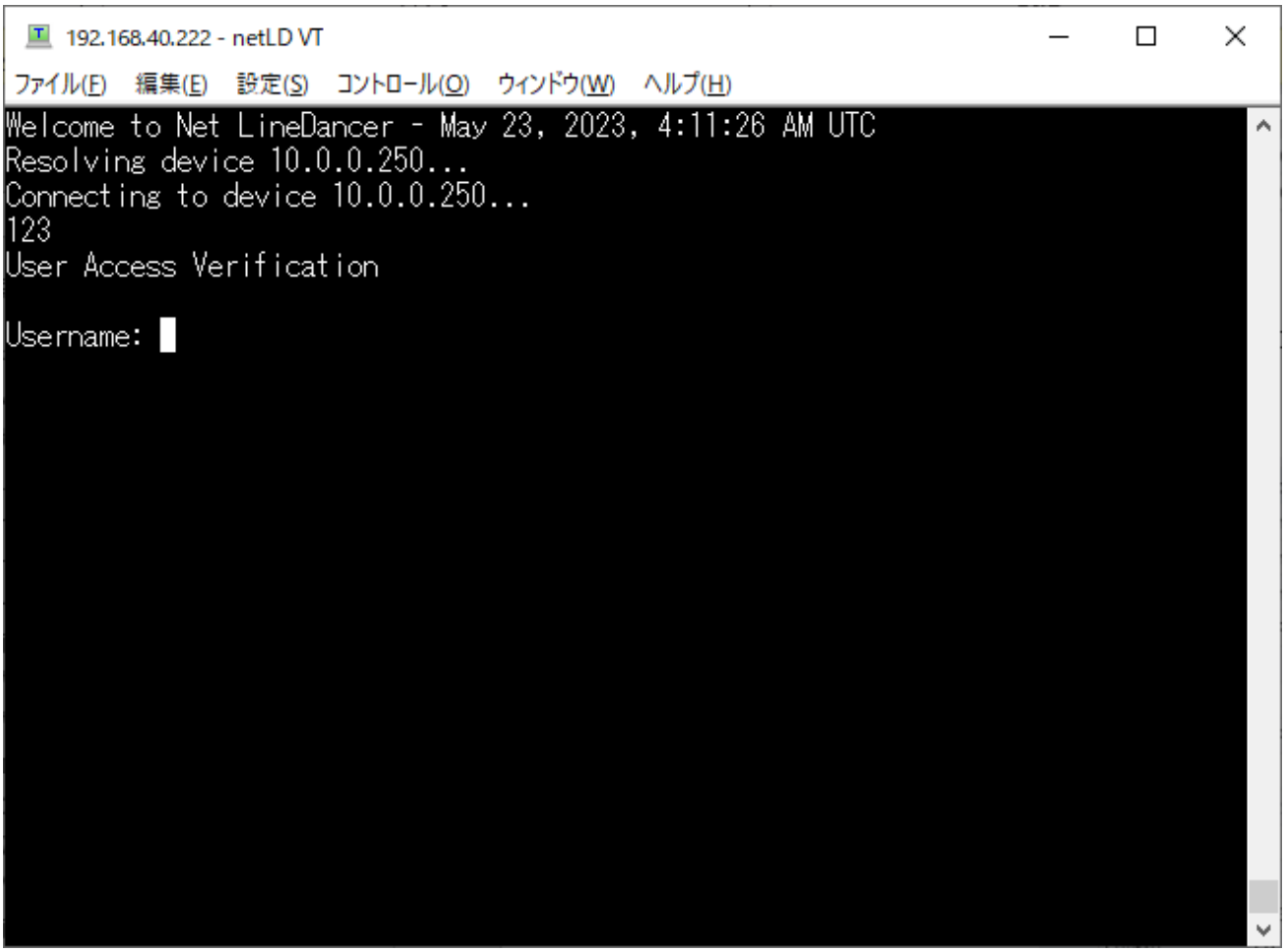


6.4.1.2.2 Use Tera Term

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



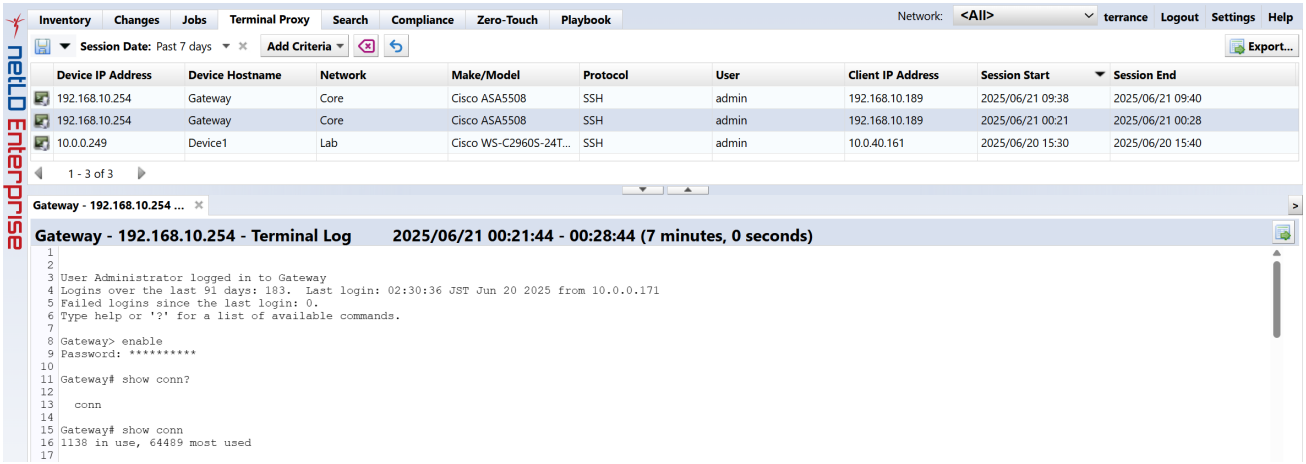
Tera Term will start and the device login screen will be displayed. Enter your username and password to log into your device.



6.4.1.3 Check the operation log

1. Select the Terminal Proxy tab.
2. Doubleclick the log you want to view from the list.

(You cannot check the session log while connected.)



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

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

6.5 Search

The Search main tab serves as a centralized investigation interface. In NetLD, it enables targeted device selection through dynamic filters (Search), full inventory access (All Devices), and predefined groups (Static List) when configuring network automation jobs.

6.5.1 Search subtabs

The Search main tab contains three subtabs:

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

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

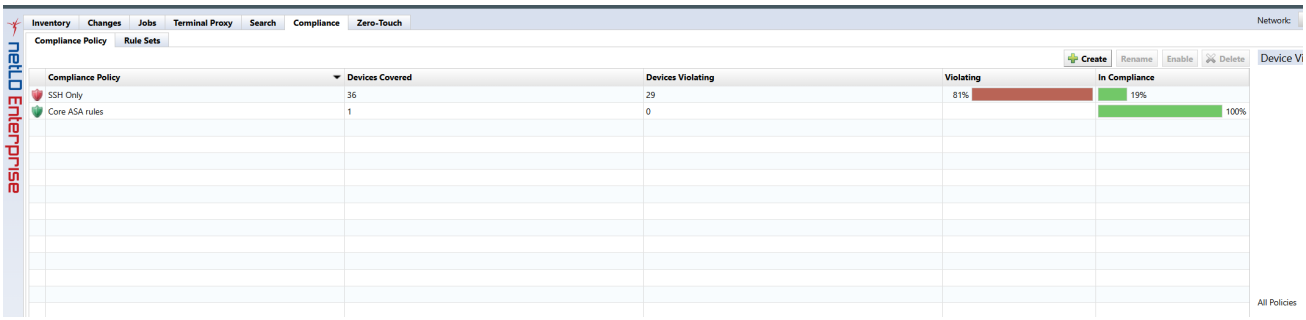
Device Information	Explanation
General	General information about the device (device name, make, model, OS version, serial number, device type, last backup/snapshot, config, timestamp, size, user).
Compliance	Information about compliance policies and associated messages, violations for Rule Sets.
Attachment	Information about any attachments associated with the device (name, size, MD5 hash)
Hardware	Description of device, and information about device type (chasis, card, memory, power, CPU, slots, model, serial number, version, port number, EOS, EOL)
Interfaces	Device name, alias, type, IP, Speed, MTU, MAC, and any related comments

Device Information	Explanation
ARP/MAC/VLAN	Information about device VLAN Member Port names and numbers, and option to collect a snapshot of MAC forwarding tables and ARP tables from the device by clicking the [Run Neighbor Collection Now] button.
Memo	Extra information about the device.

6.6 Compliance

The Compliance tab consists of the following subtabs:

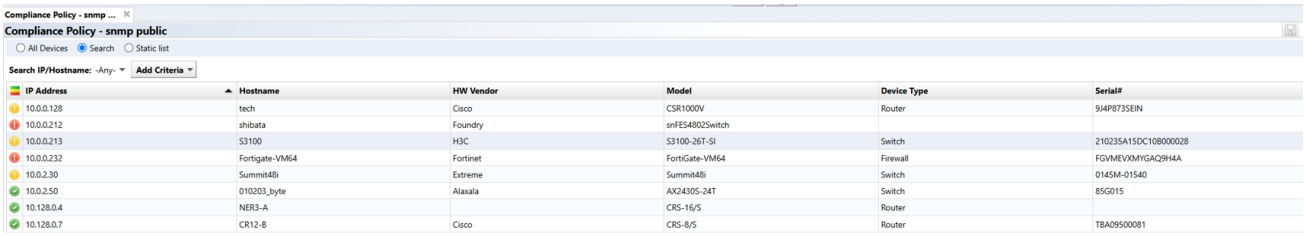
- **Compliance Policy** subtab
- **Rule Sets** subtab



6.6.1 Compliance Policy subtab

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

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



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

6.6.2 Compliance Policy

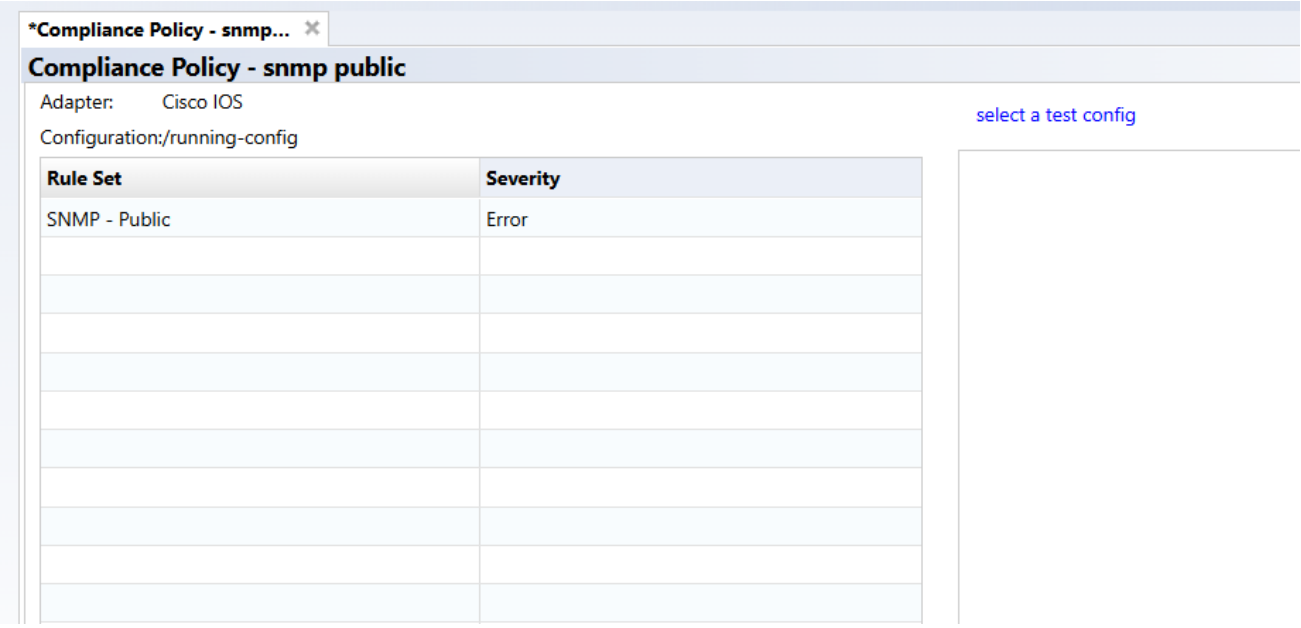
By setting a compliance policy, you can automatically ensure device configuration settings. For this automatic detection, you need to create a device compliance rule. A rule is constructed using the following four matching conditions.

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

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

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

Doubleclick a Compliance Policy to open the Compliance Policy window.

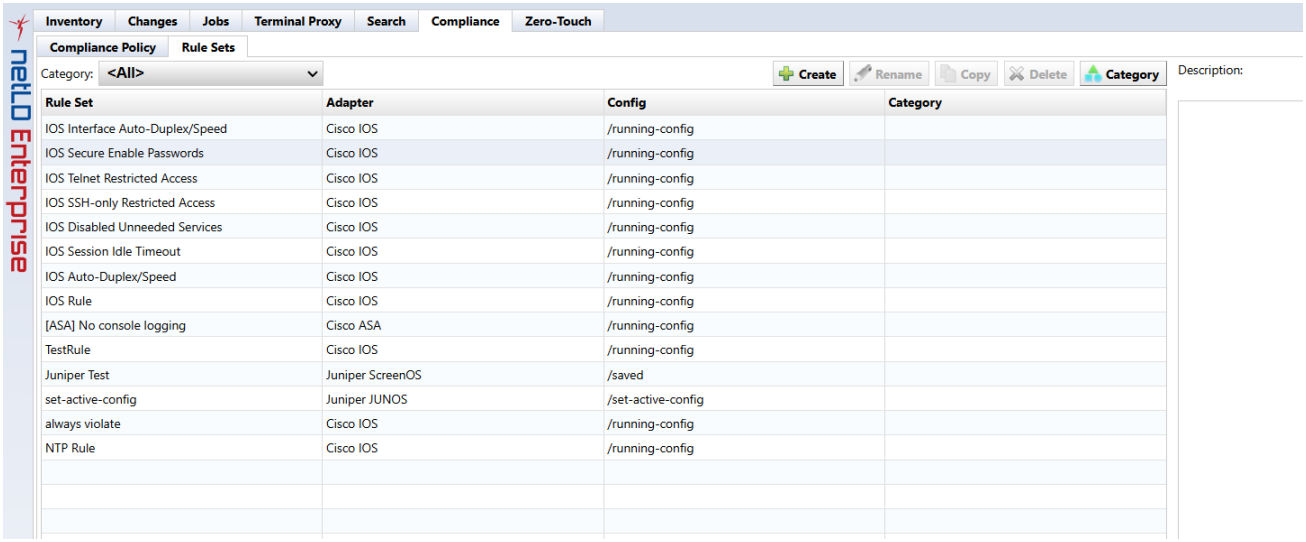


Item	Explanation
Adapter	Displaying adapters to which the policy applies.
Configuration	Displaying the configuration to which the policy is applied.
Rule Set	A rule added to a policy.

Severity	You can select the failure level from error or warning. The icon displayed when a policy is violated is different.

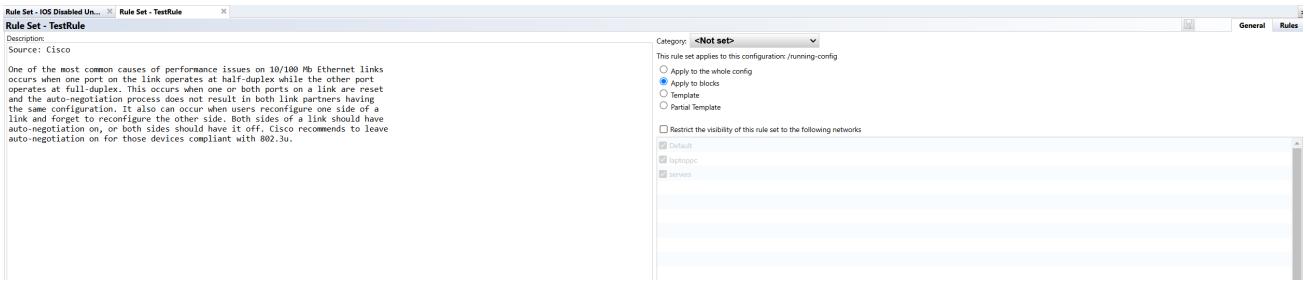
6.6.3 Rule Sets subtab

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



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

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



General Items	Explanation
Category	Select a category for the rule.
Description	Enter a description for the rule.
Apply to the whole config	Applies the rule to the entire configuration.
Apply to block	Divide the configuration into blocks and apply rules to each blog.
Template	The configuration is compared line by line from the template, and if there is a difference, it will be a violation.

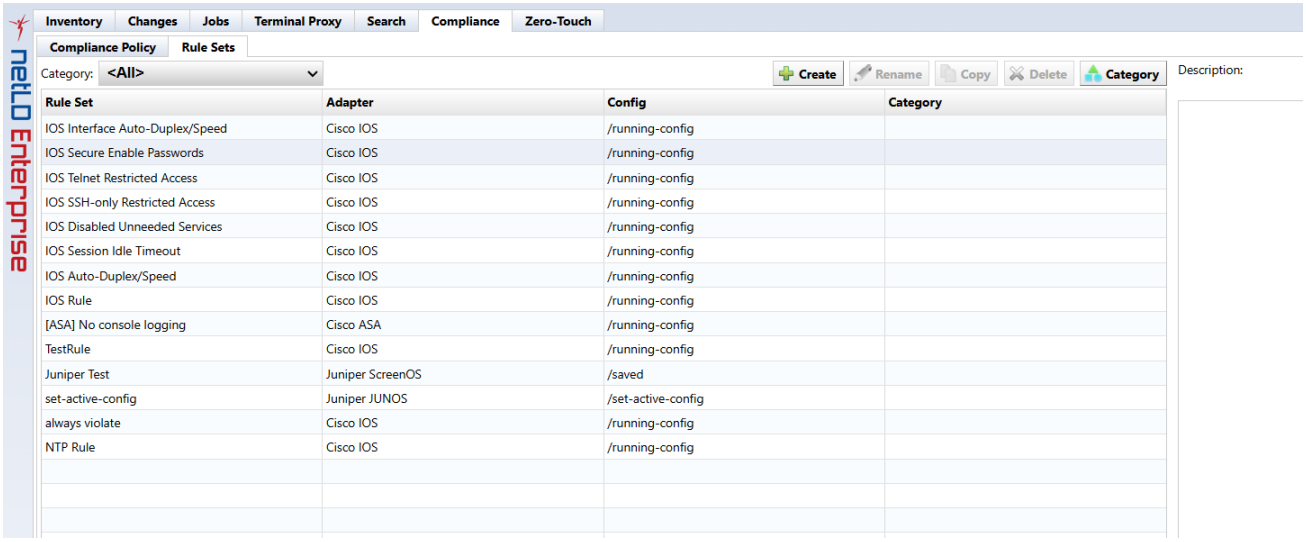
General Items	Explanation
Partial Template	The configuration is compared line by line against the template, but the comparison can be started from anywhere in the config text, not just from the first line.
Restrict the visibility of this Rule Set to the following networks	Enabling the check limits the networks to which the rule applies.

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

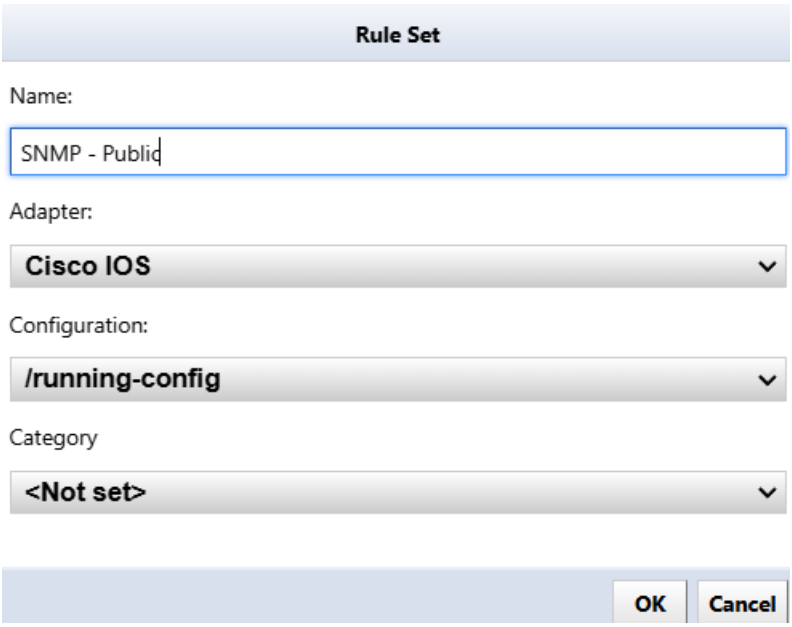
Rule Sets Item	Explanation
Violation message	Enter the message that will be displayed if the rule is violated.
Start/End	Specify the range to search for the string specified in the “Match” item. This field appears when Apply to Blocks is selected on the [General] subtab.
Match Expression	Specifies the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

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

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



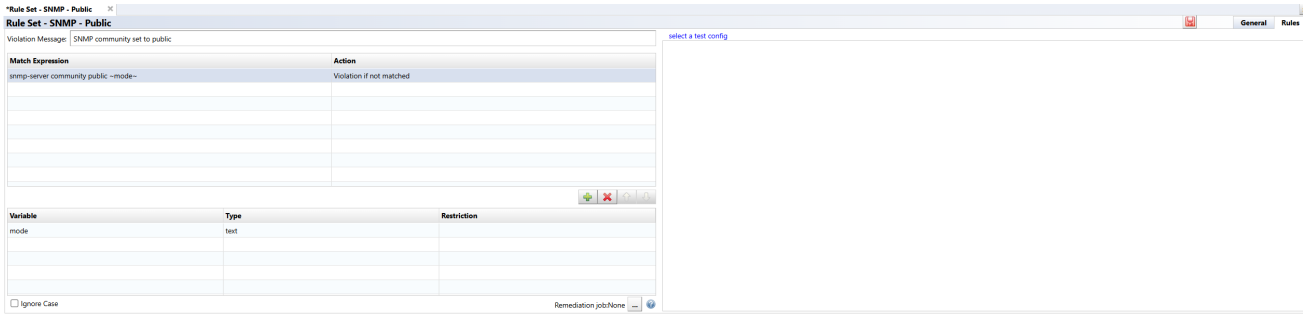
2. The name of the rule, the target adapter (model classification), and which configuration the rule applies to (running-config startup-config) and click the [OK] button.



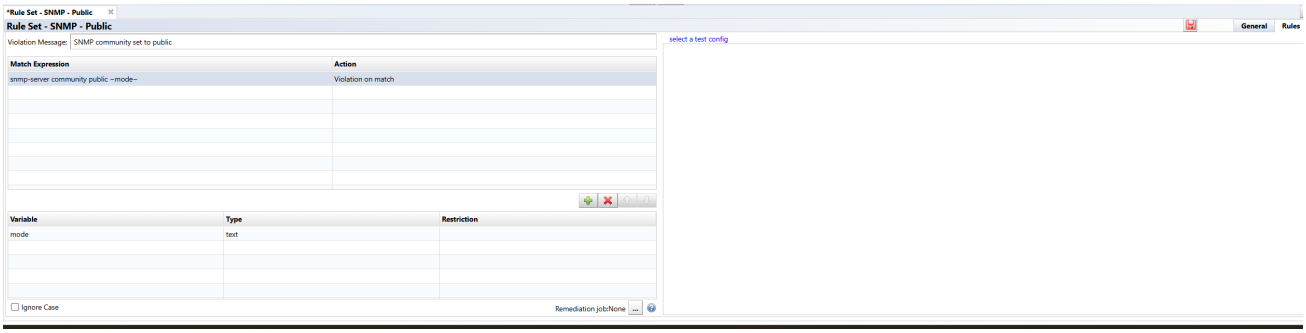
3. In the [Violation Message] field, enter the message that will be displayed when a violation is detected, and click the button.

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

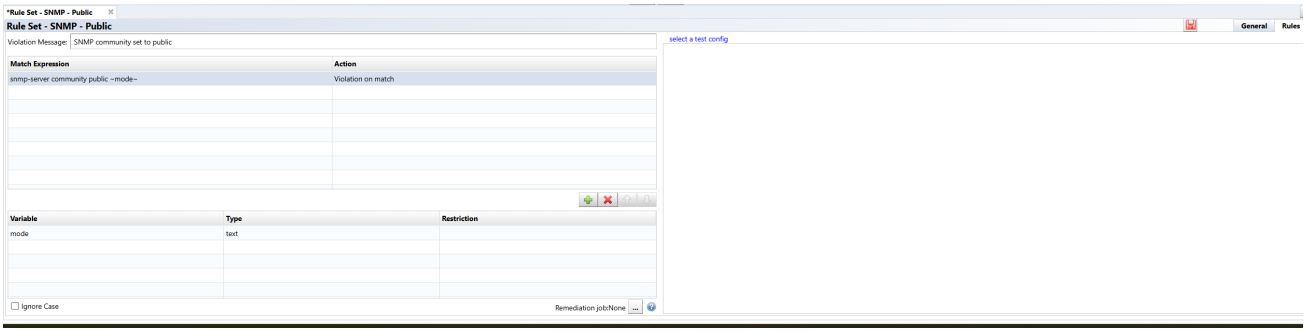
When finished, click the button.



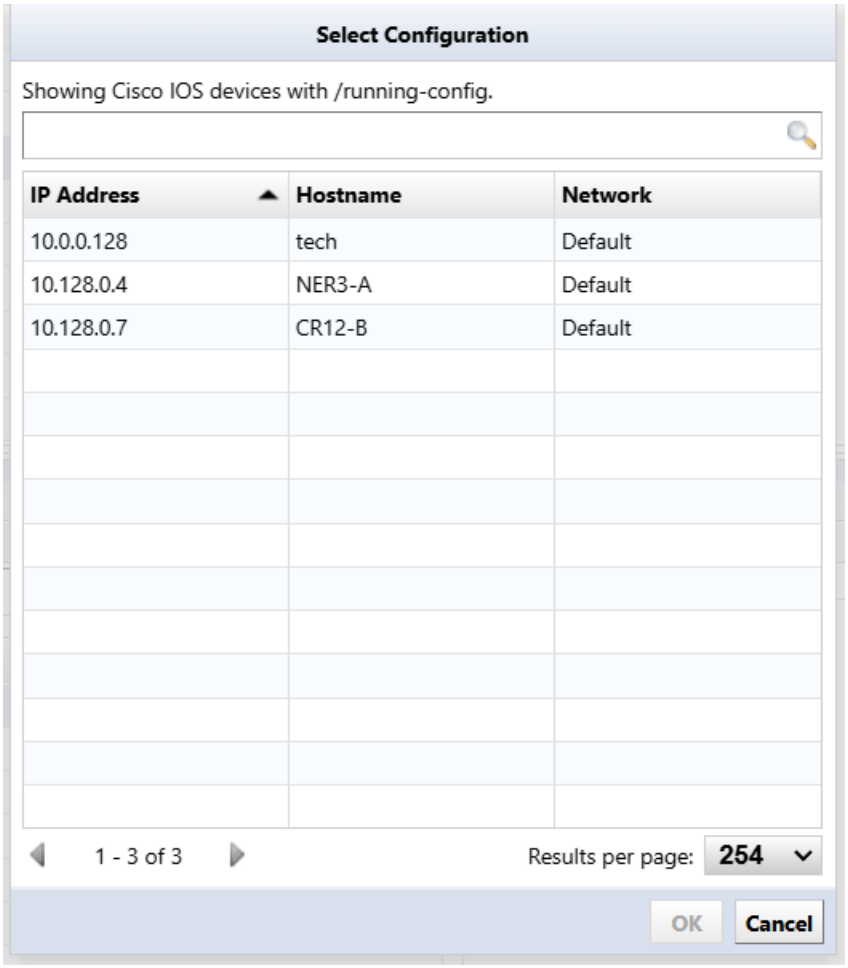
4. In the [Match Expression] column, enter the text that is a violation, and in [Action] column select [Violate on match].



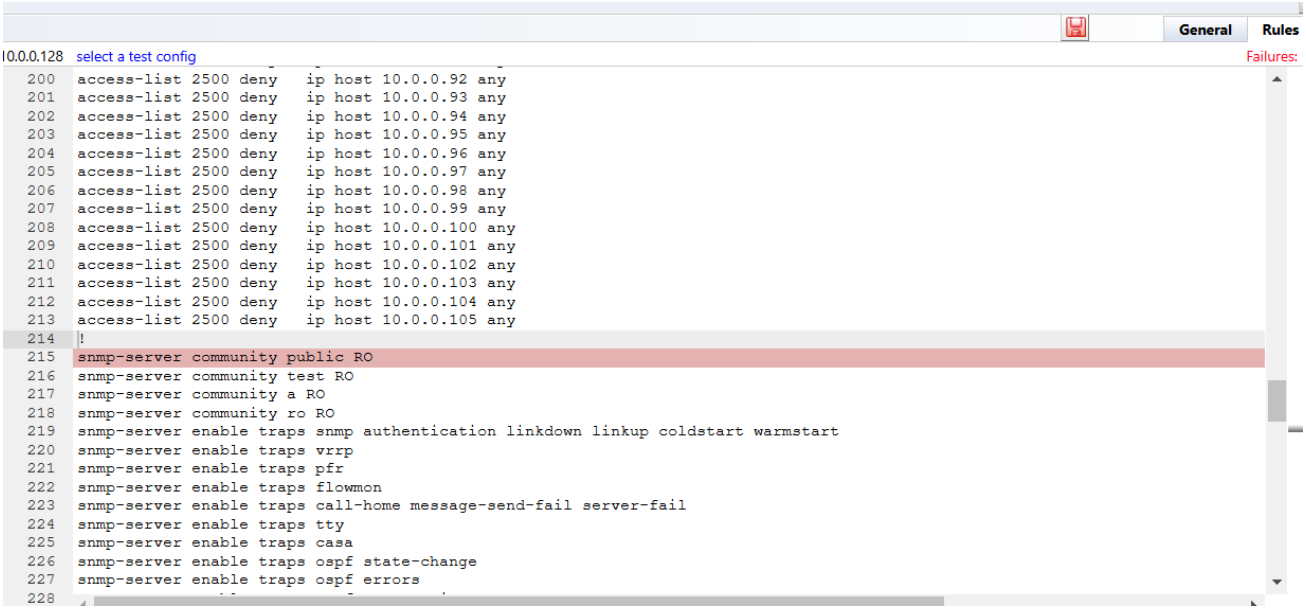
5. If you want to test the rule you created, click [Select a configuration] in the upper right to test and select a configuration from your inventory.



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

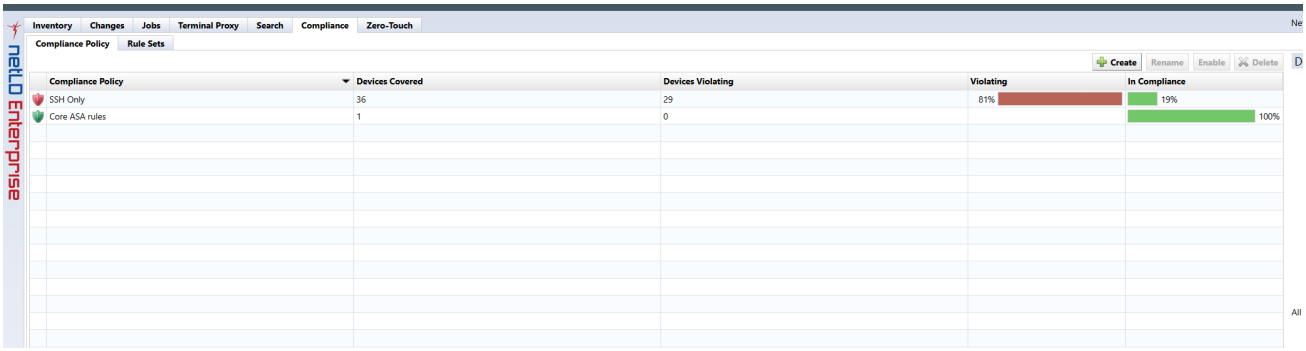


Violations will be searched for against this text rule, and if violations are found, they will be displayed in red. The following section will cover creating policies from this Rule Set.

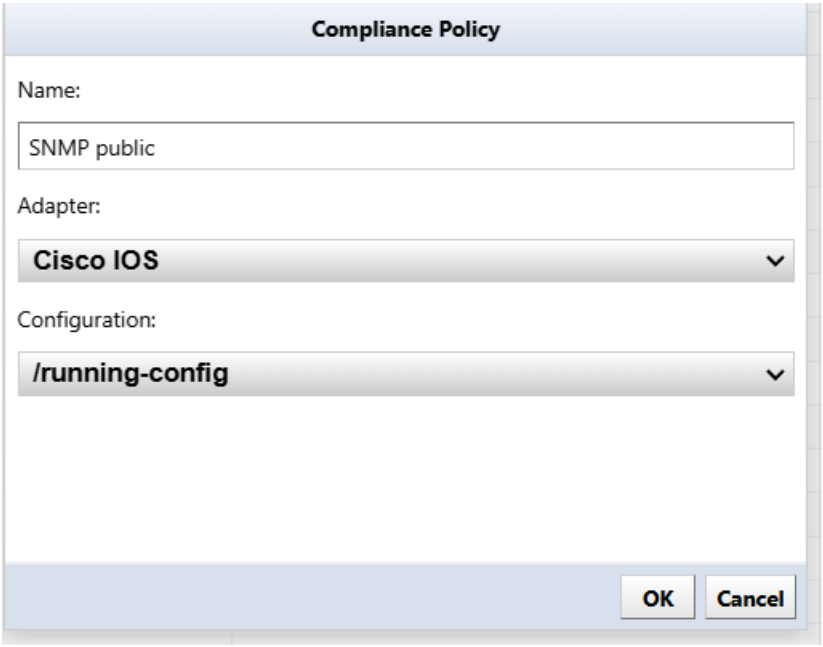


6.6.3.2 Creating a new policy This section will create a policy for a Cisco IOS device configuration using the Rule Set created in the previous section.

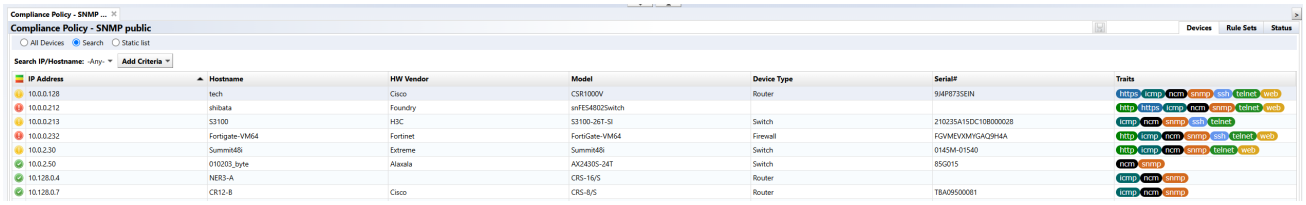
1. Click the Compliance > Compliance Policy tabs, then click the [Create] button.



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



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



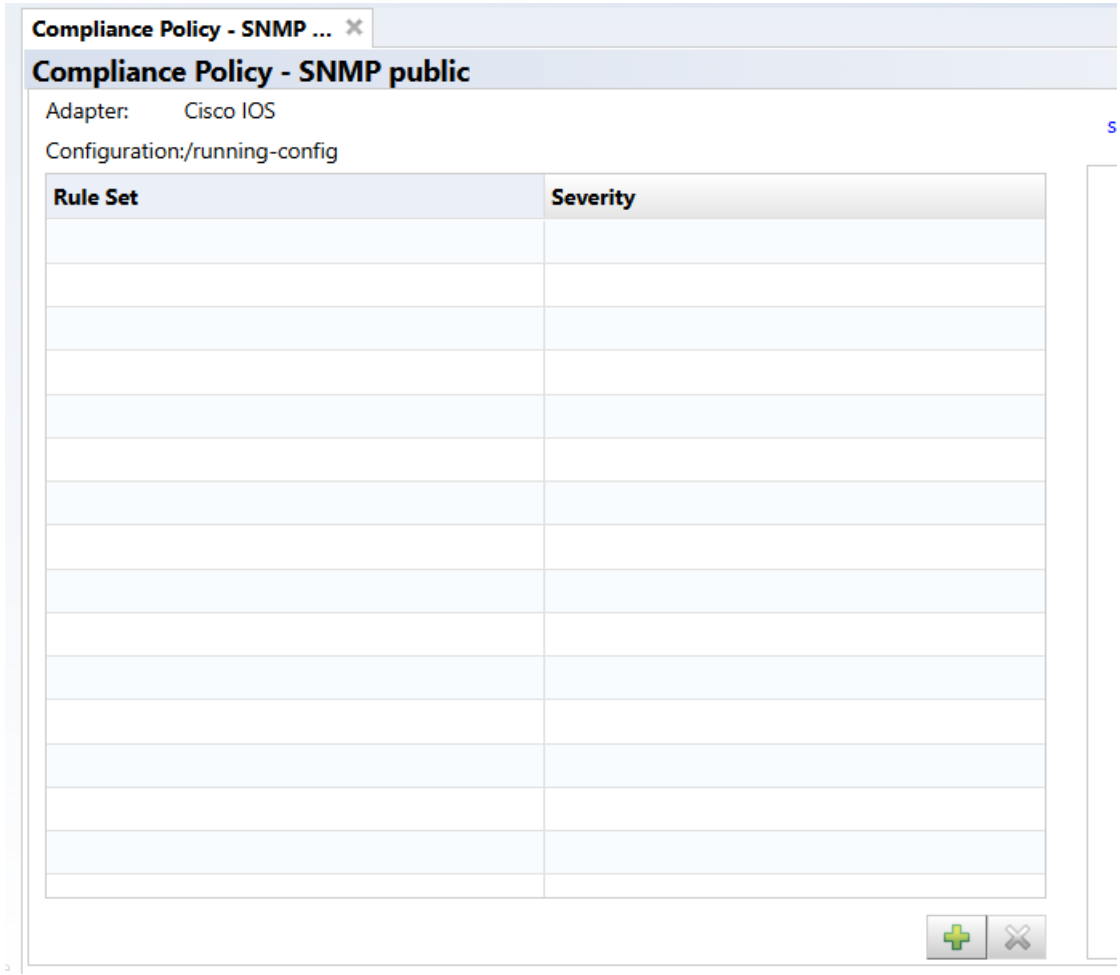
The setting behavior for Search and [Static list] in the [Device] subtab is same as the behavior setting behavior in Job Management.

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

Note

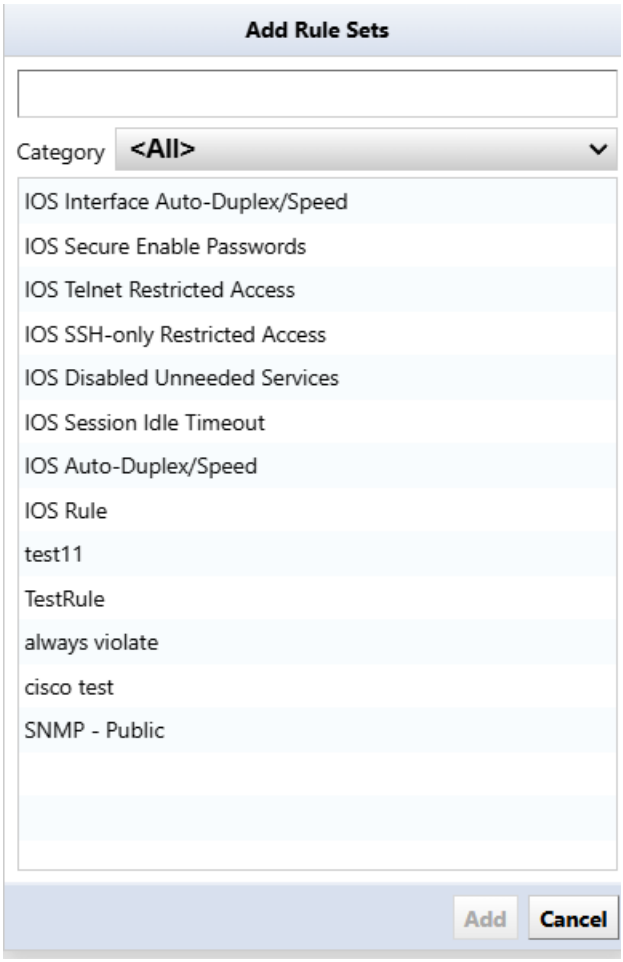
Search result is not saved when creating policy.

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



5. Select a Rule Set and click the button.

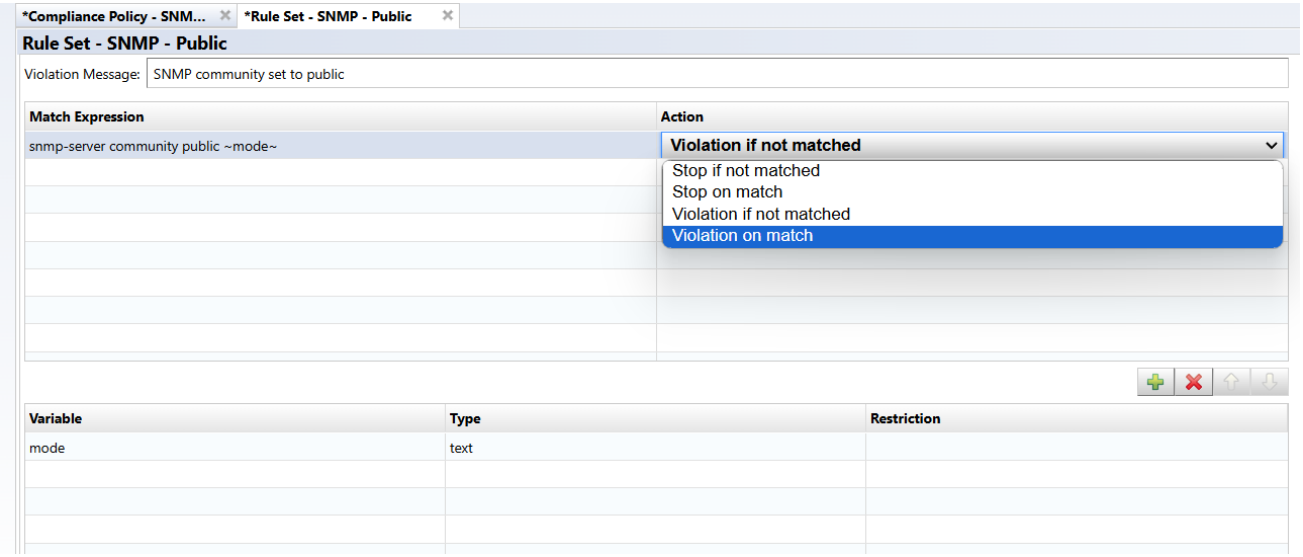
In this example, “IOS Secure Enable Password” Rule Set is selected.



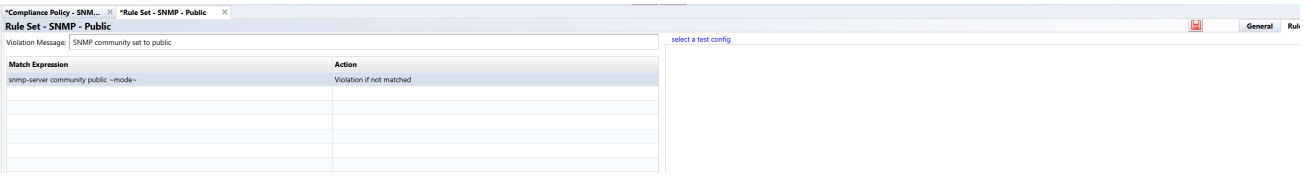
6. Select an Action for the rule. Different Actions can be set for each Rule Set.

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

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



7. Save the policy.



Note

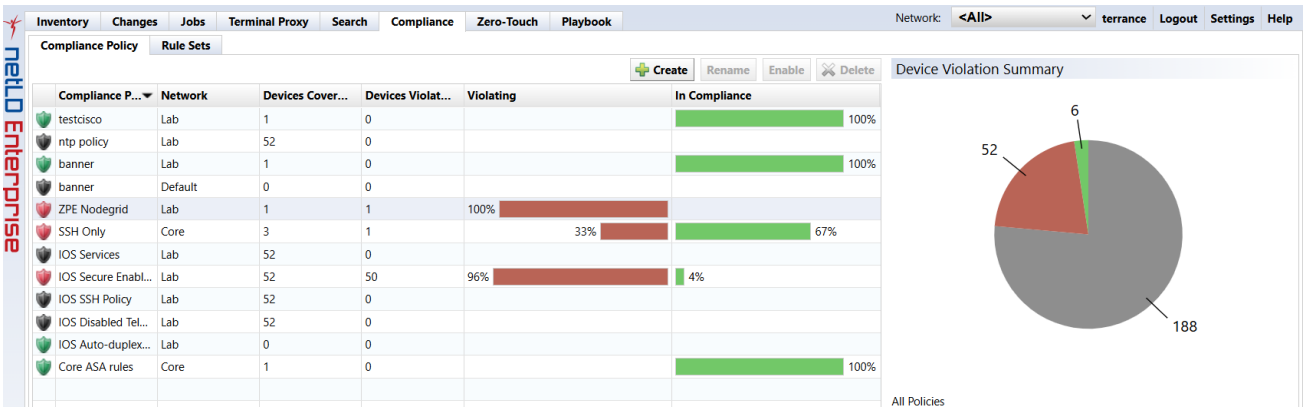
Activate the policy after saving. Simply creating a policy does not check for violations.

6.6.3.3 Applying the created policy

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

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

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



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

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

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

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

6.6.4 Automatic remediation function

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

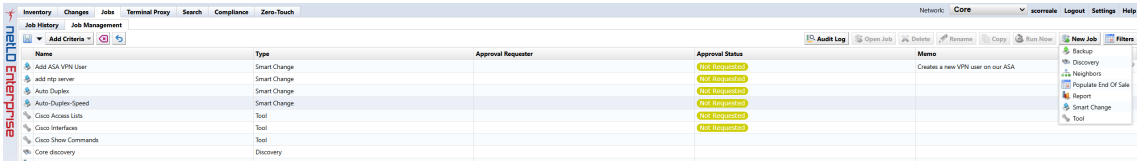
Setting Process

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

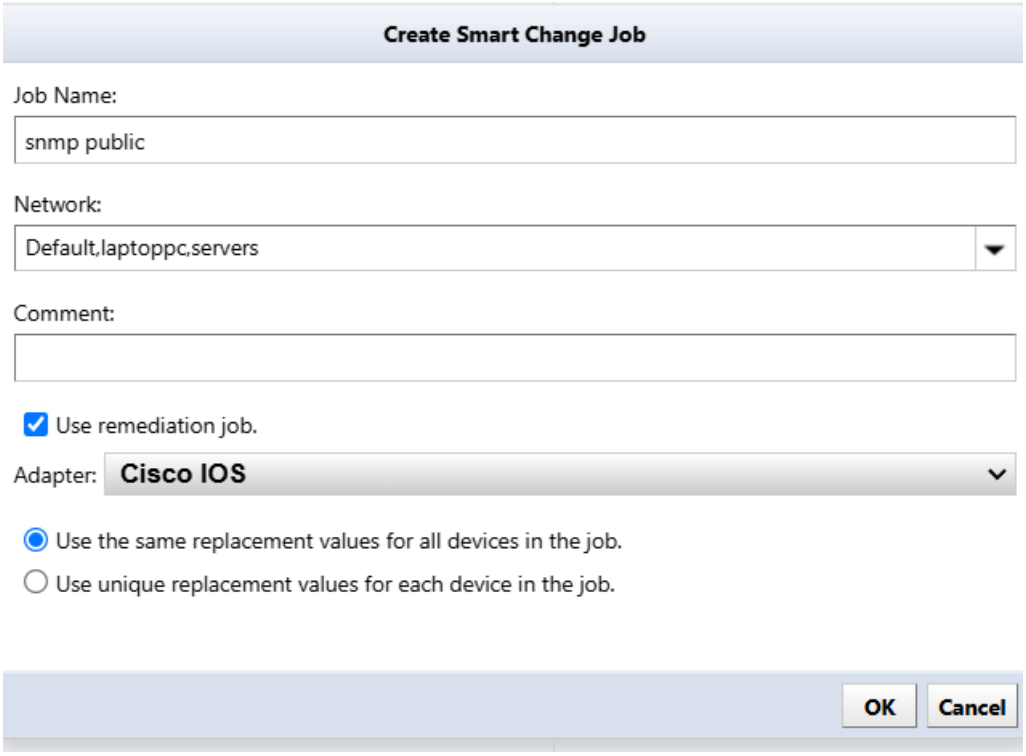
The following explains how to set it up using a setting example.

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

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

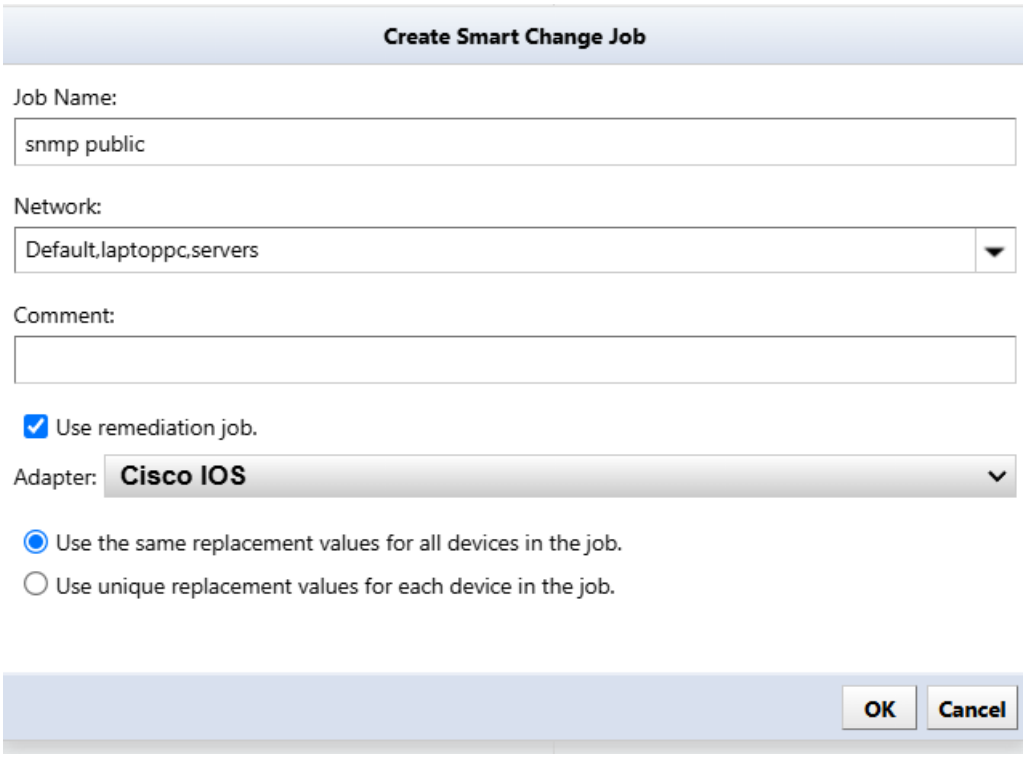


2. Enter the job name and comment (optional).



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

This is used for linking with Rule Sets.

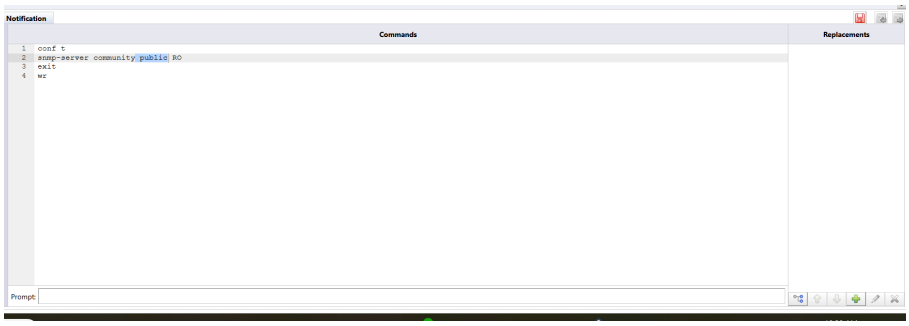


4. Enter the command you want the template to run.

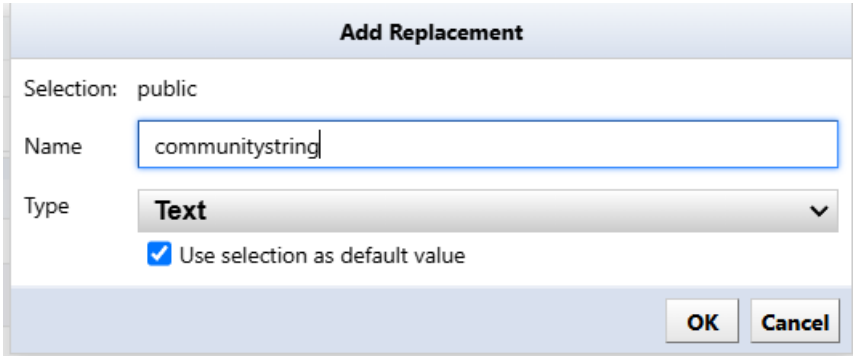
5. Select the part you want to convert into a variable and click the the  button.

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

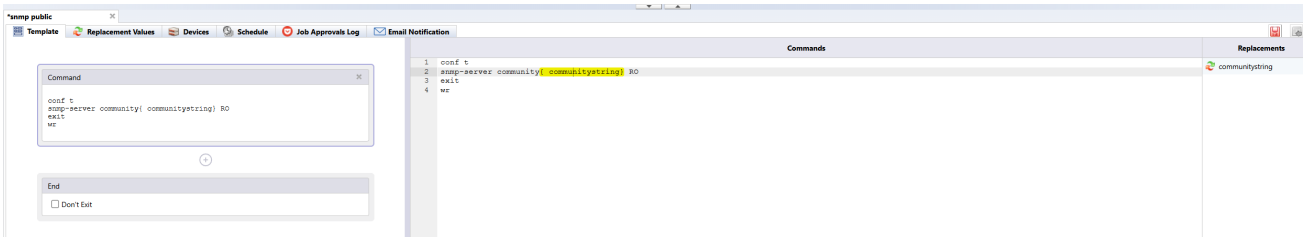
In this case, the community name will be obtained from the config, so we will convert the community name part into a variable.



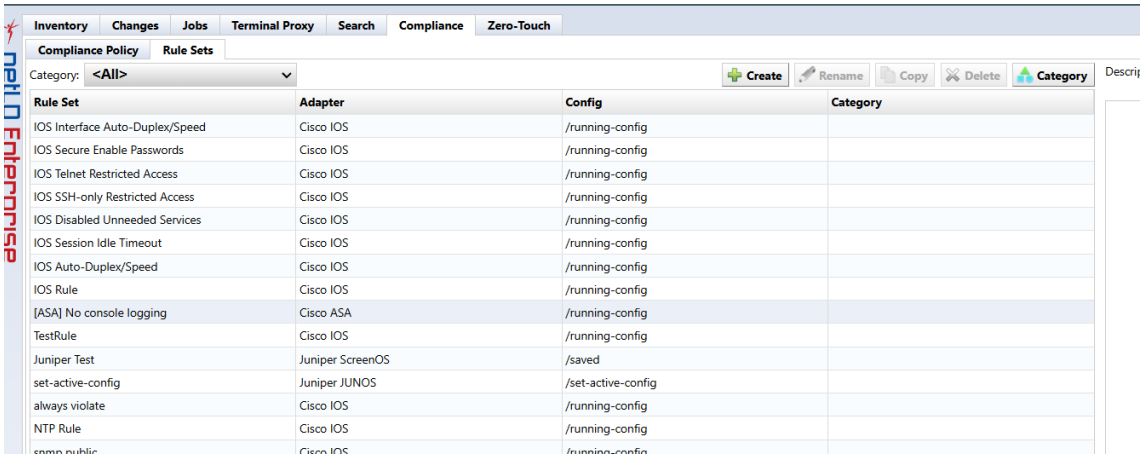
6. Enter the variable “Name” and click [OK].



7. Save the settings.



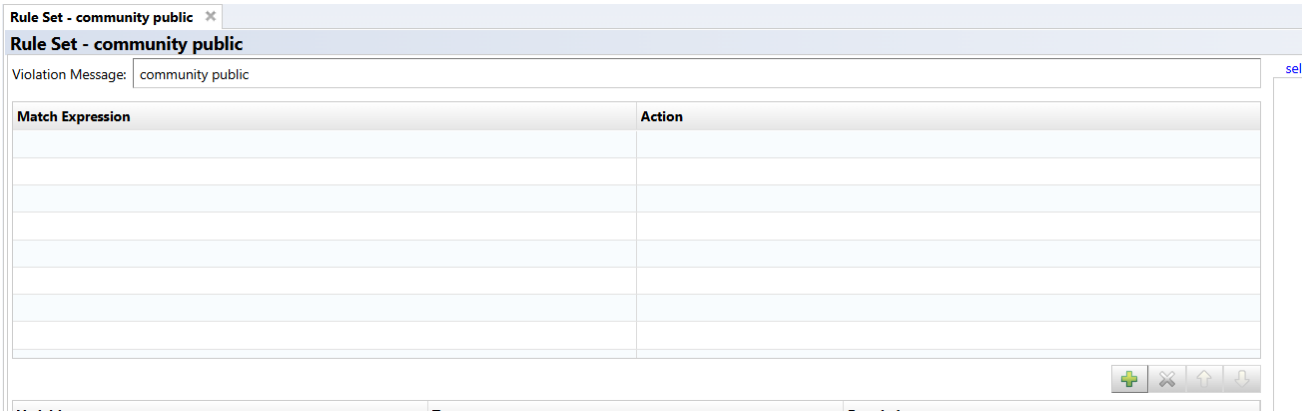
8. Go to Compliance > [Rule Sets] and click [Create].



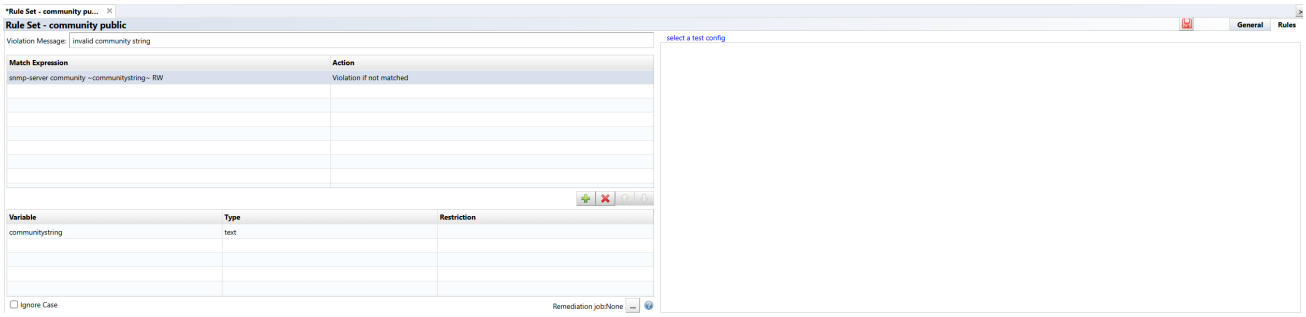
9. Enter the rule name, select the adapter, and click [OK].

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

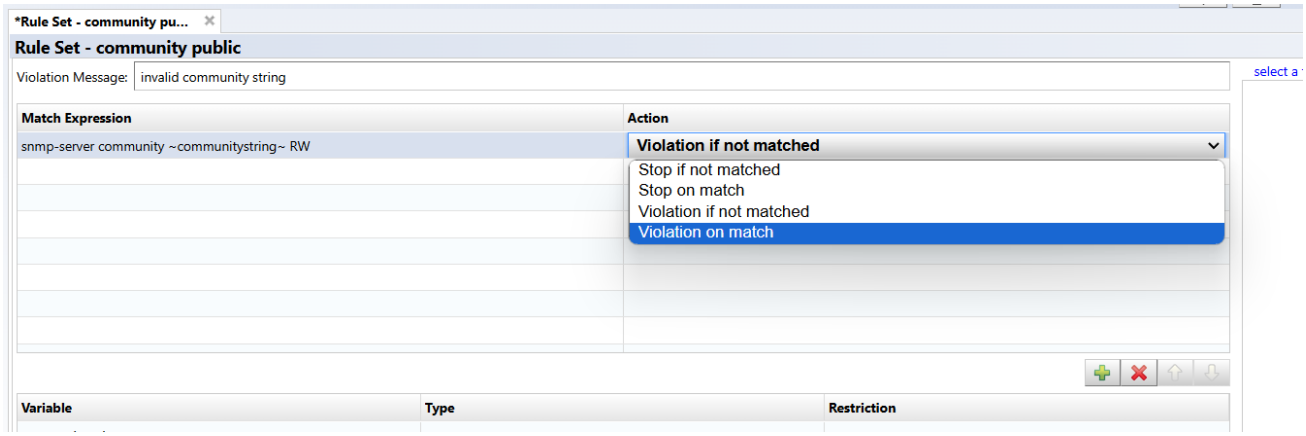
10. Click the button to add “Match Expression”.



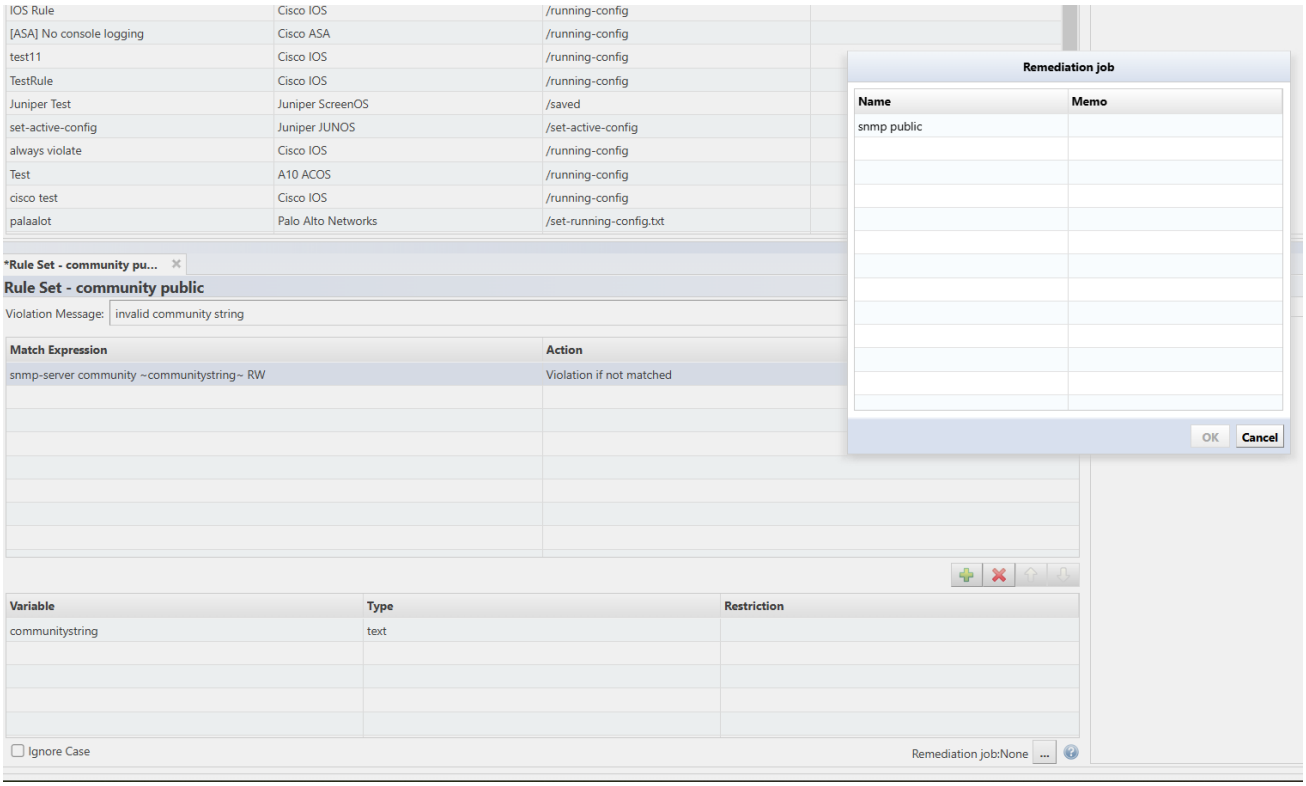
11. In the “Variable” section in the bottom half of the page, specify the community name as the smart change Variable.
12. In the “Match Expression” section in the top half of the page, add “~” before and after the variable name.



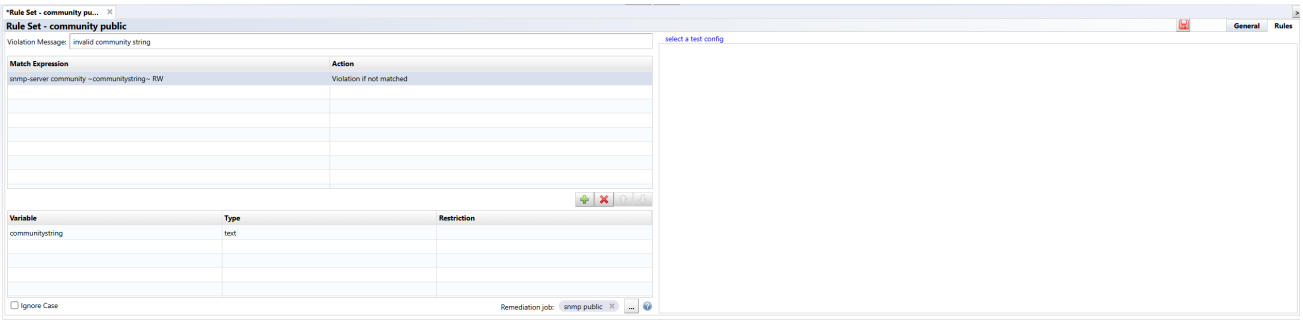
13. Set the Action to “Violation on match.”



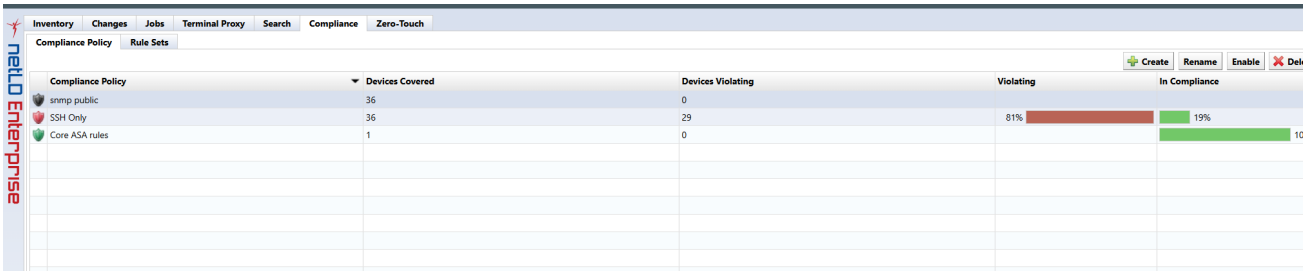
14. In the bottom right of the panel, click the […] button next to “Remediation job” to specify the smart change job to be executed in the event of a violation. Only one job can be specified.



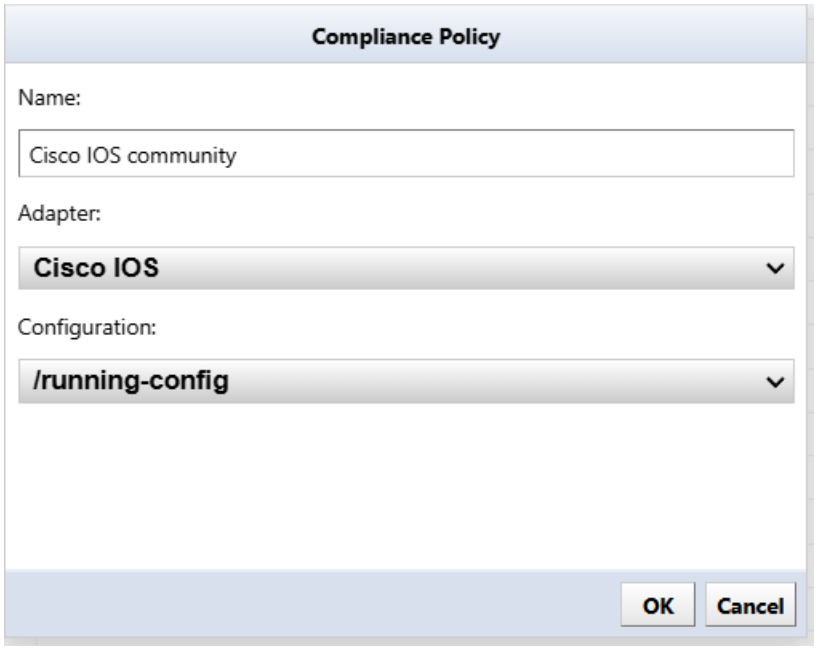
15. Save your settings.



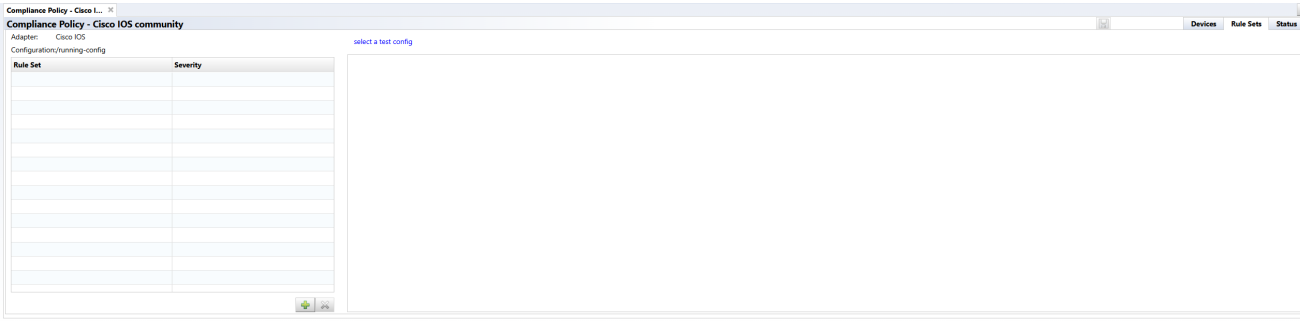
16. Go to Compliance > Compliance Policy and click [Create].



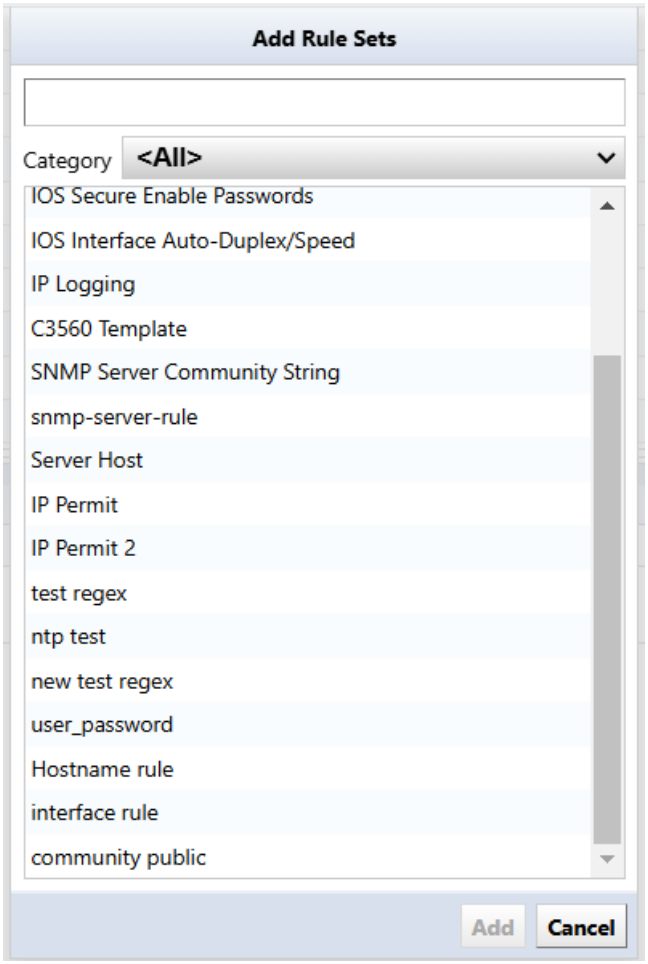
17. After entering the “Name”, select the adapter and target configuration file, and click [OK].



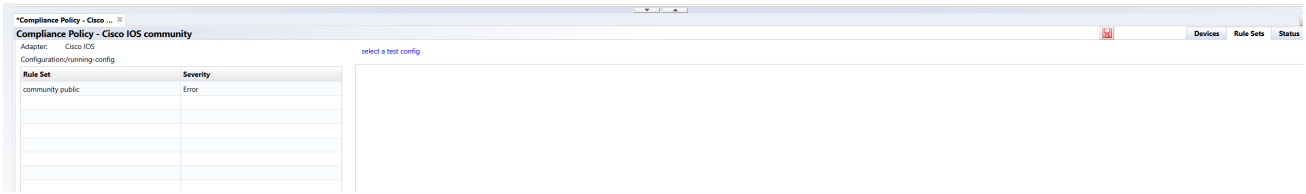
18. Click the ➕ button.



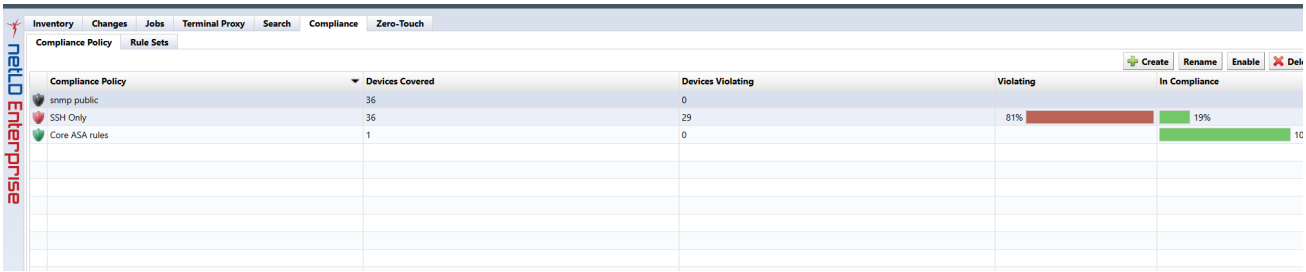
19. Select [Rule Sets] and click [Add].



20. Click [Save].

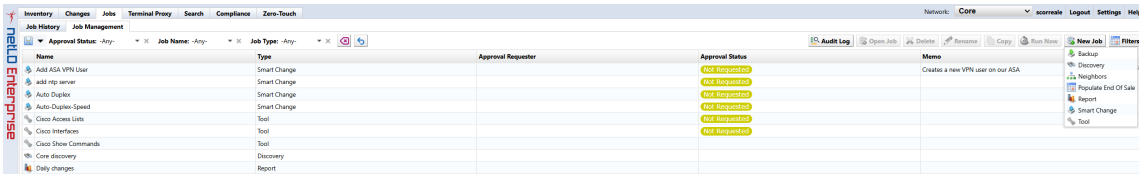


21. Select the compliance policy you created and click [Enable].

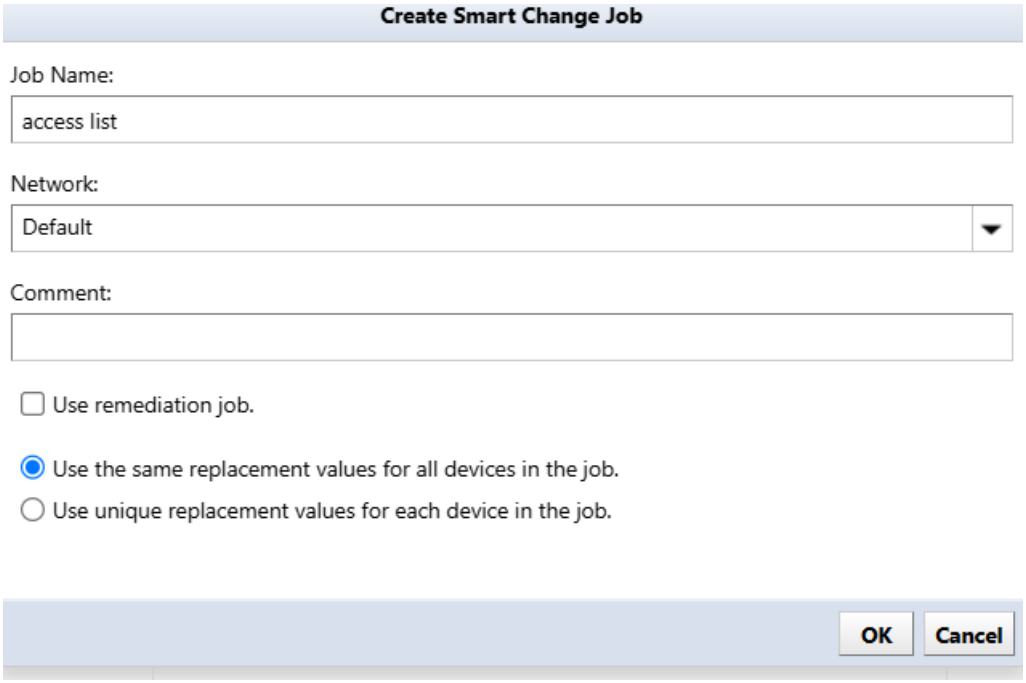


6.6.4.2 Case 2: No access list added to the interface

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



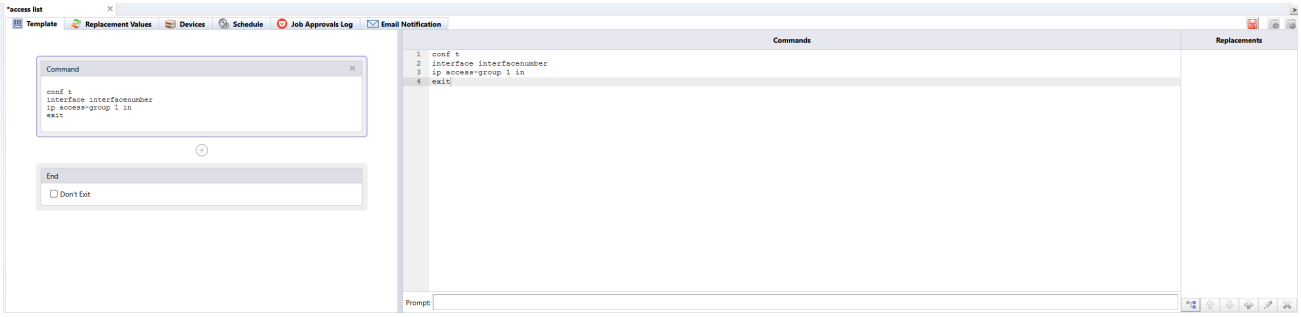
2. Enter the job name and comment (optional).



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

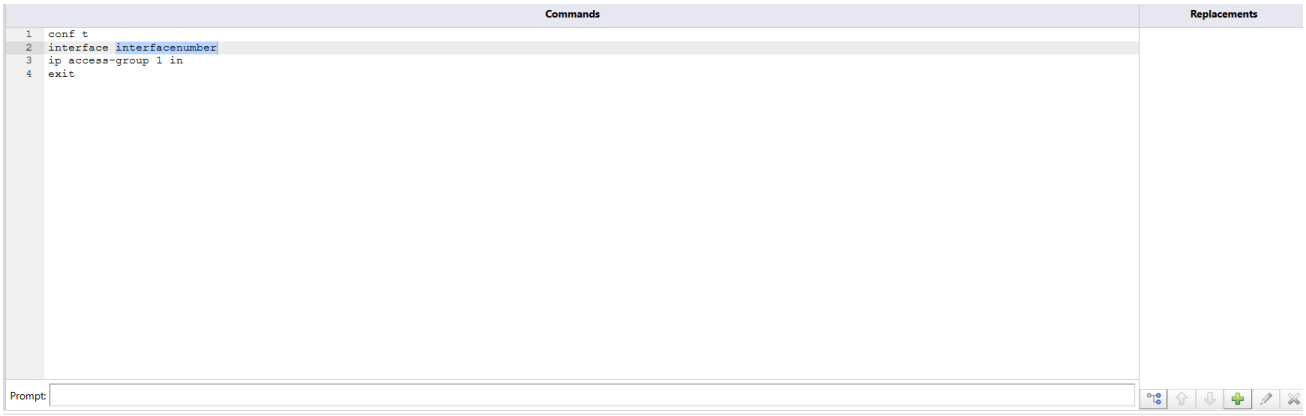
This is used for linking with Rule Sets.

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

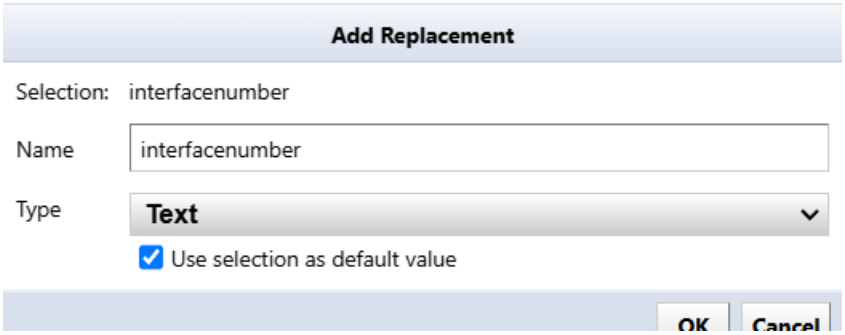


5. Select the part you want to convert into a variable and click the button.

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

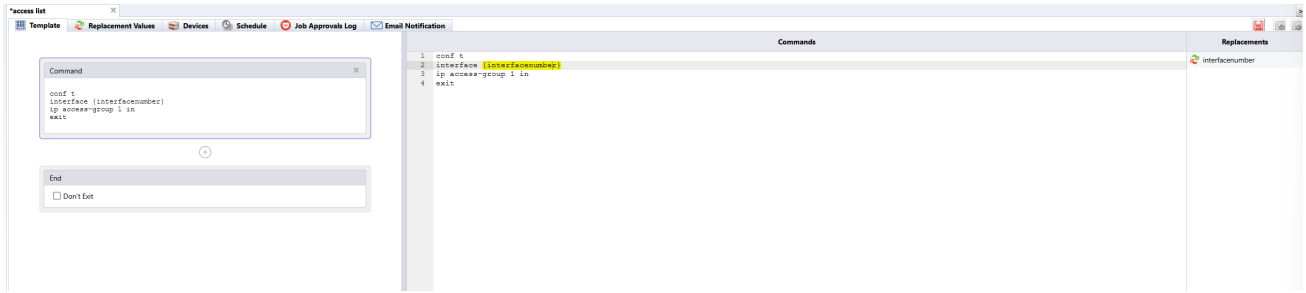


6. Enter the variable name and click [OK].

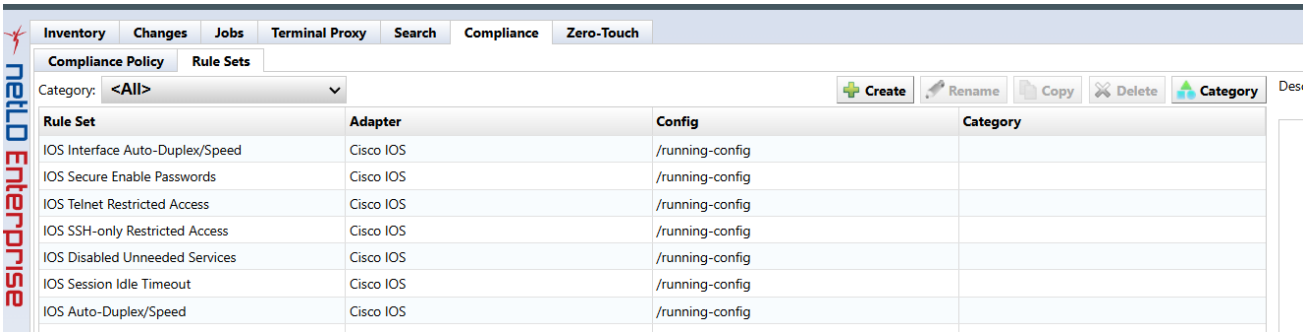


{n .center}

7. Click [Save].

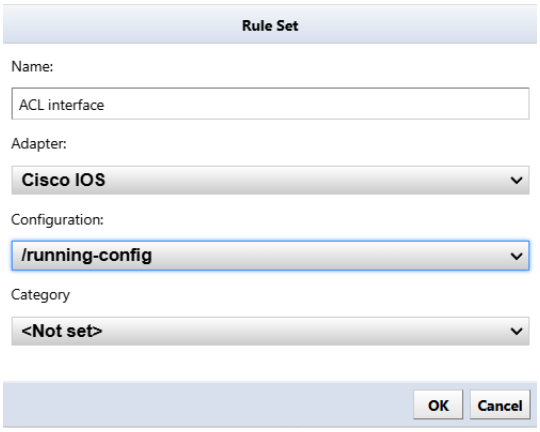


8. Go to Compliance > [Rule Sets] and click [Create].

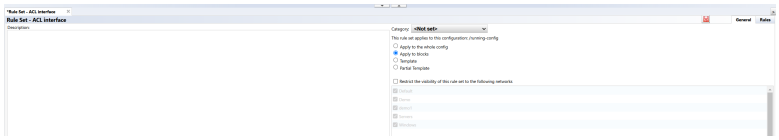


9. After entering the rule name, select the adapter and click [OK].

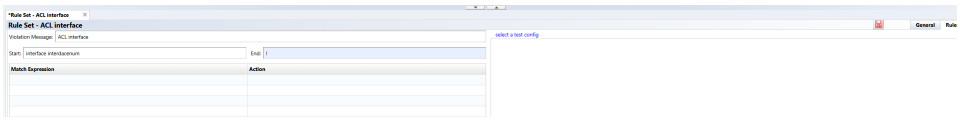
Please select the adapter you selected when creating the smart change.



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

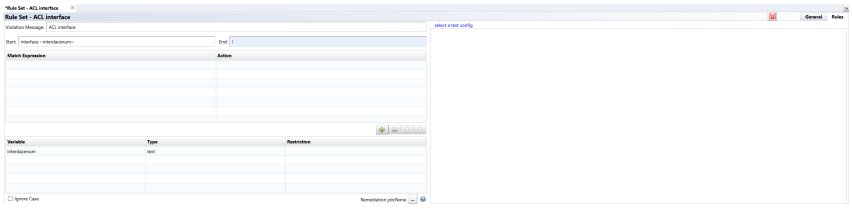


11. Specify the block to which the rule applies using “Start” and “End”.



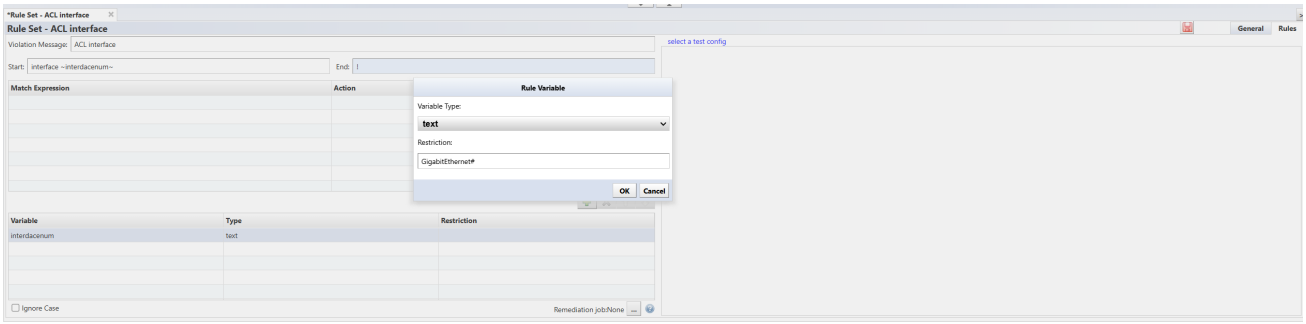
12. In the “Variable” section in the bottom half of the page, specify the interface number as the smart change Variable.

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

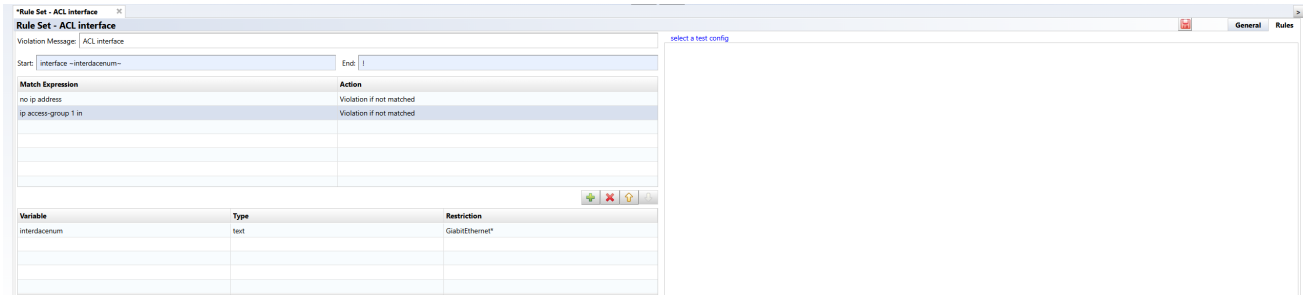


13. Doubleclick the added variable and add a text filter.

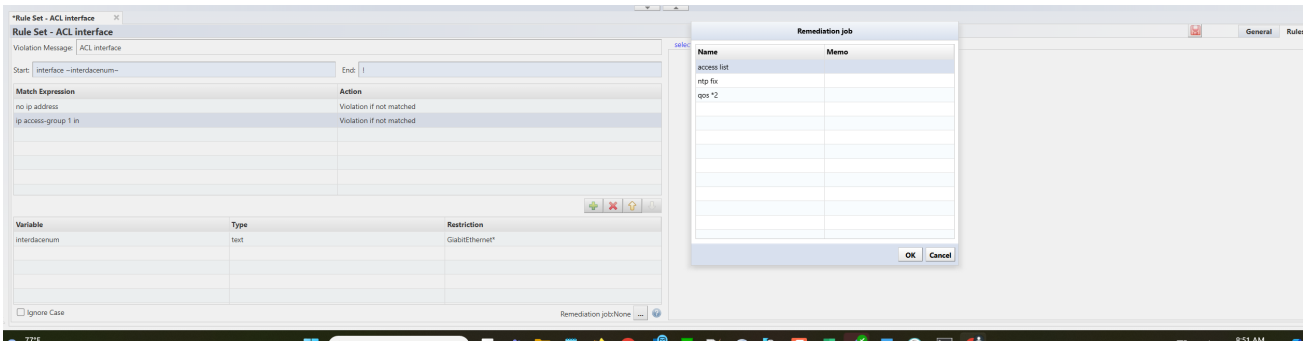
In this example, the GigabitEthernet interface is targeted, so “Gigabit Ethernet” is specified.



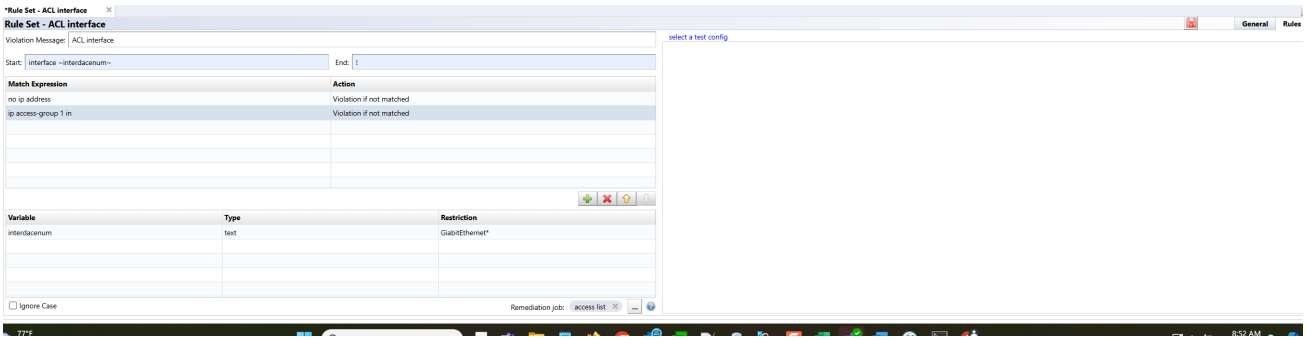
14. Click the button to add matching conditions.



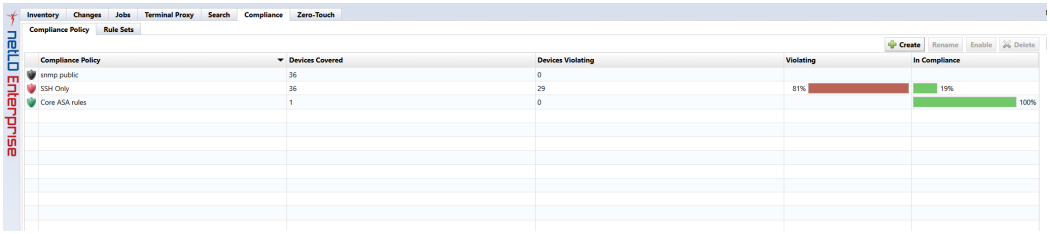
15. In the bottom right of the panel, click the […] button next to the “Remediation job”, and specify the smart change job to be executed in the event of a violation. Only one job can be specified.



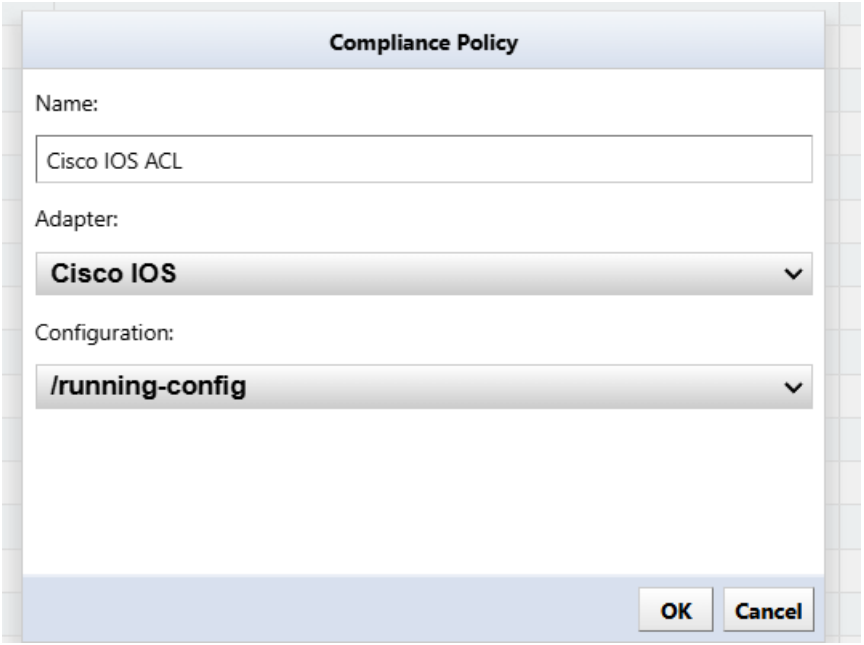
16. Save your settings.



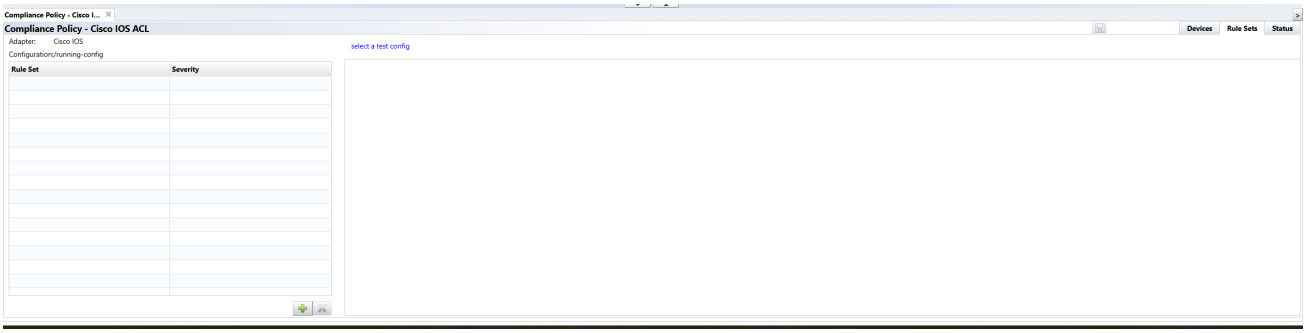
17. Go to Compliance > Compliance Policy and click [Create].



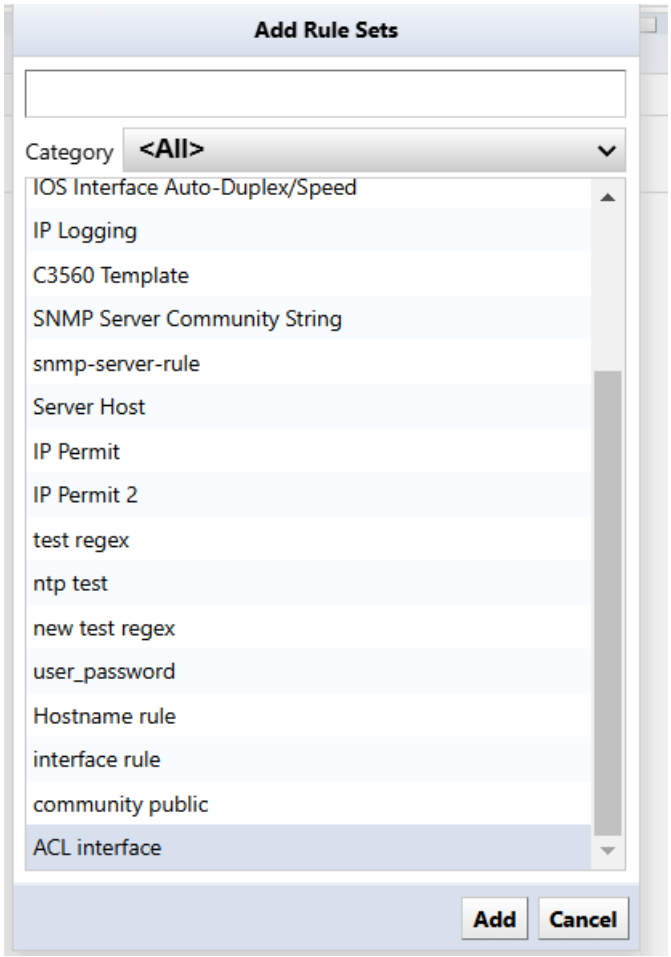
18. After entering the “Name”, select the “Adapter” and “Configuration” target file, and click [OK].



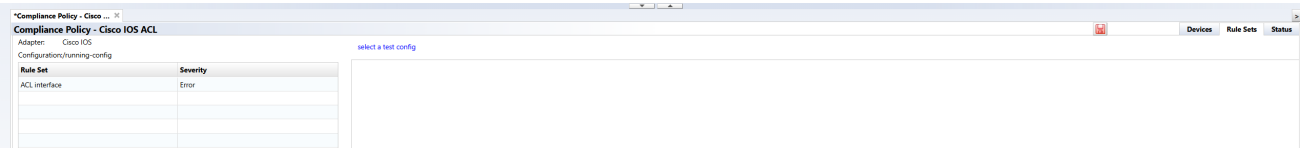
19. Click the ➕ button.



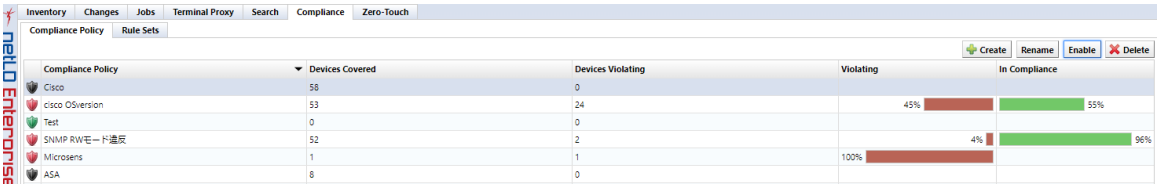
20. Add a Rule Set.



21. Click [Save].



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



6.7 Zero-Touch (optional)

The [Zero-Touch] tab 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.

6.7.1 Zero-Touch formats

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

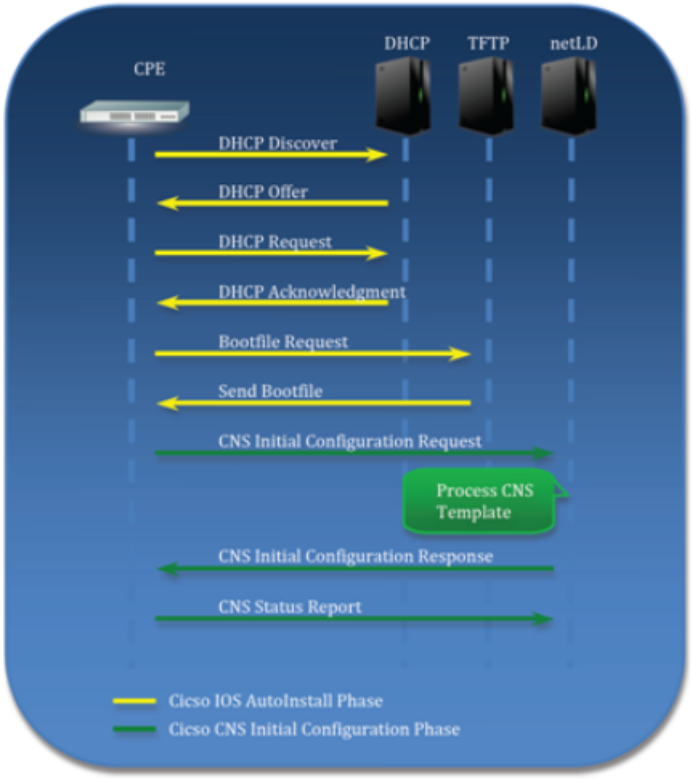
-**Template**: Distribute configurations based on templates. Used when introducing a new device to the network at a remote office.

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

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

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

The figure below shows the flow of processing performed by Plug and Play using PnP. To make the diagram easier to read, the DHCP and 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.

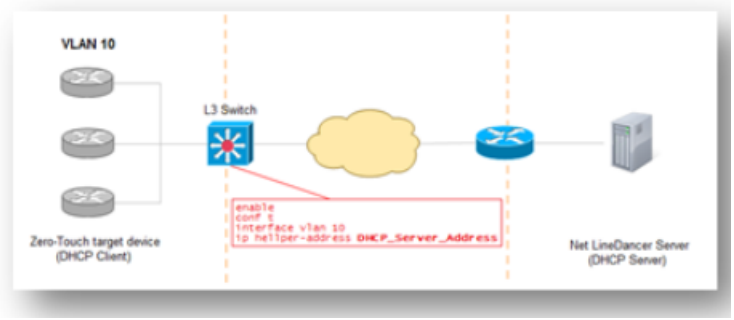


6.7.2 Zero-Touch requirements

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

- The IOS version of the target device must be IOS 15.2(2) or later for PnP.
- Devices must not have a startup-config.
- DHCP Server - If you want 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.

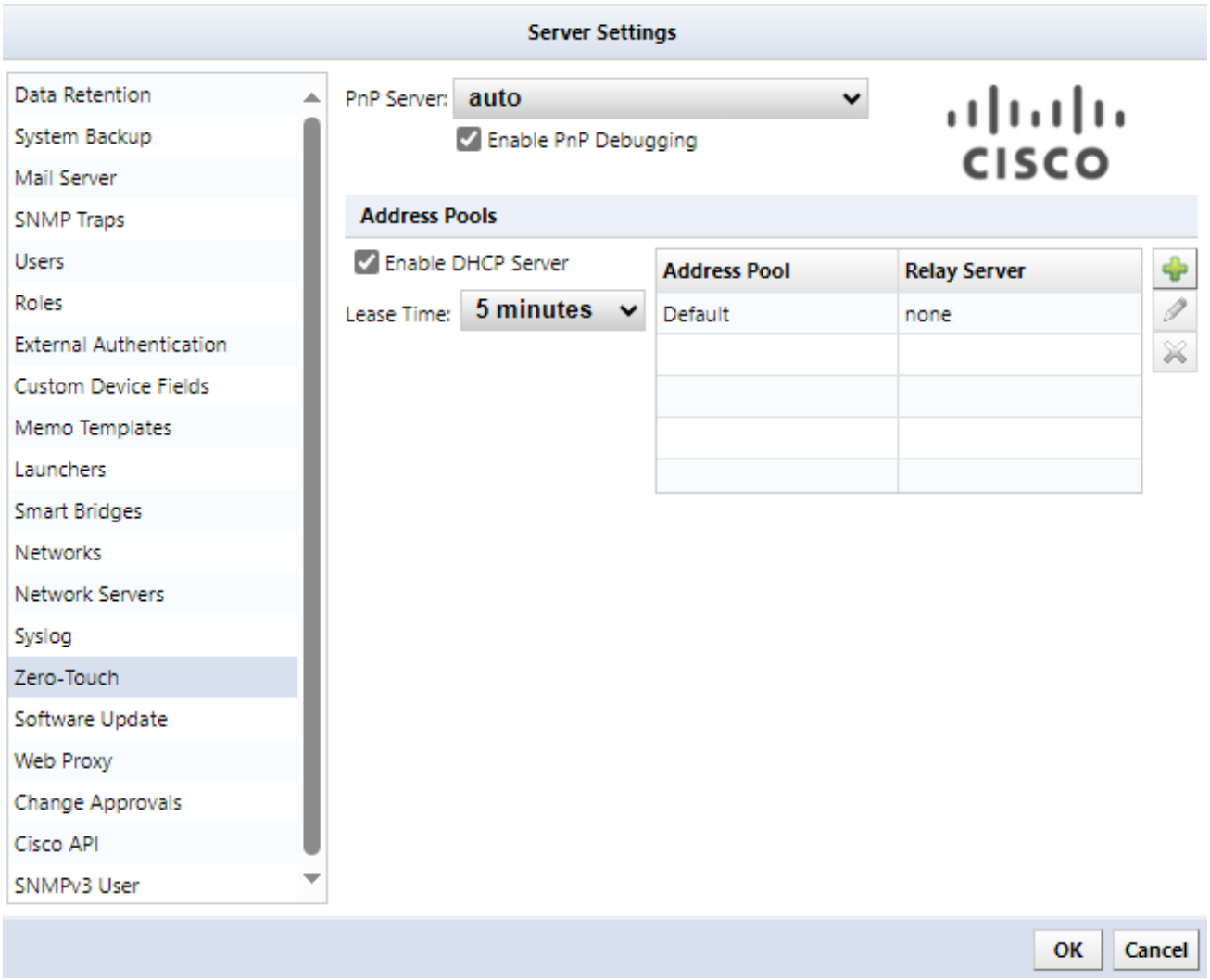
DHCP relay example:



6.7.3 DHCP server

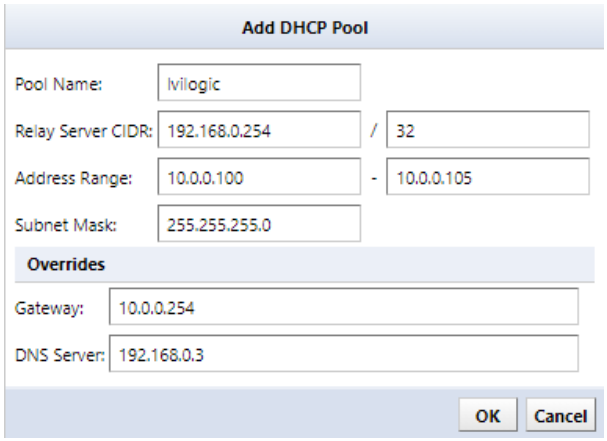
To set up a DHCP server:

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



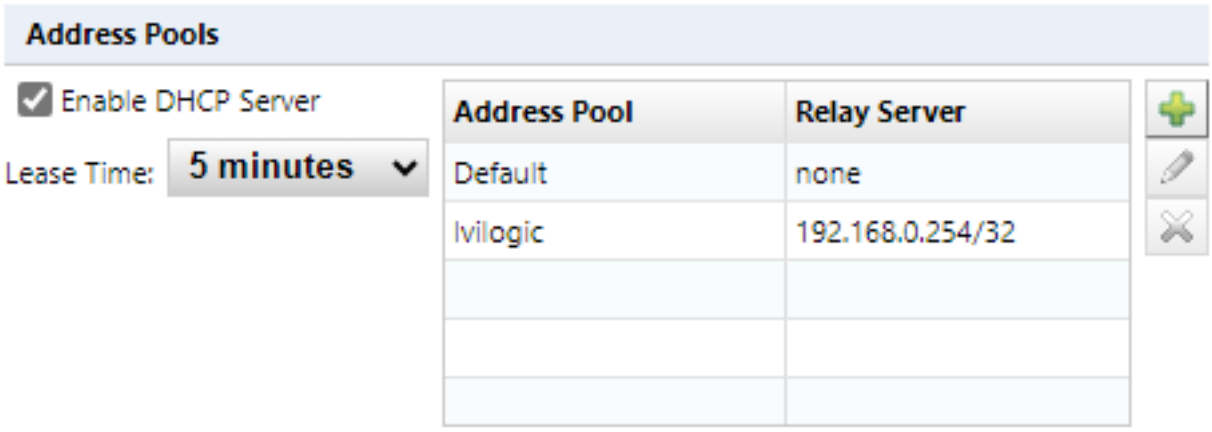
Item	Explanation
Enable DHCP server	Check this box if you want to use NetLD's DHCP server.
lease time	Set the DHCP lease time.

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



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

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

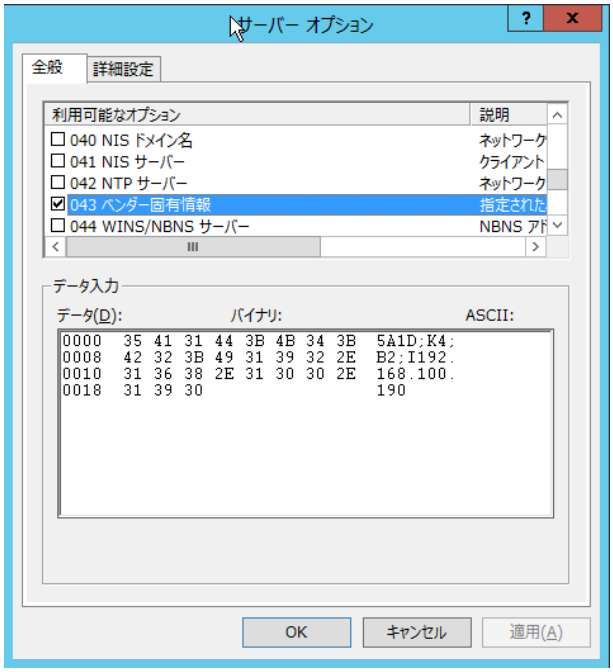


6.7.4 Use an external DHCP server

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

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

Enter the information in the ASCII field, using "`;`" to separate.

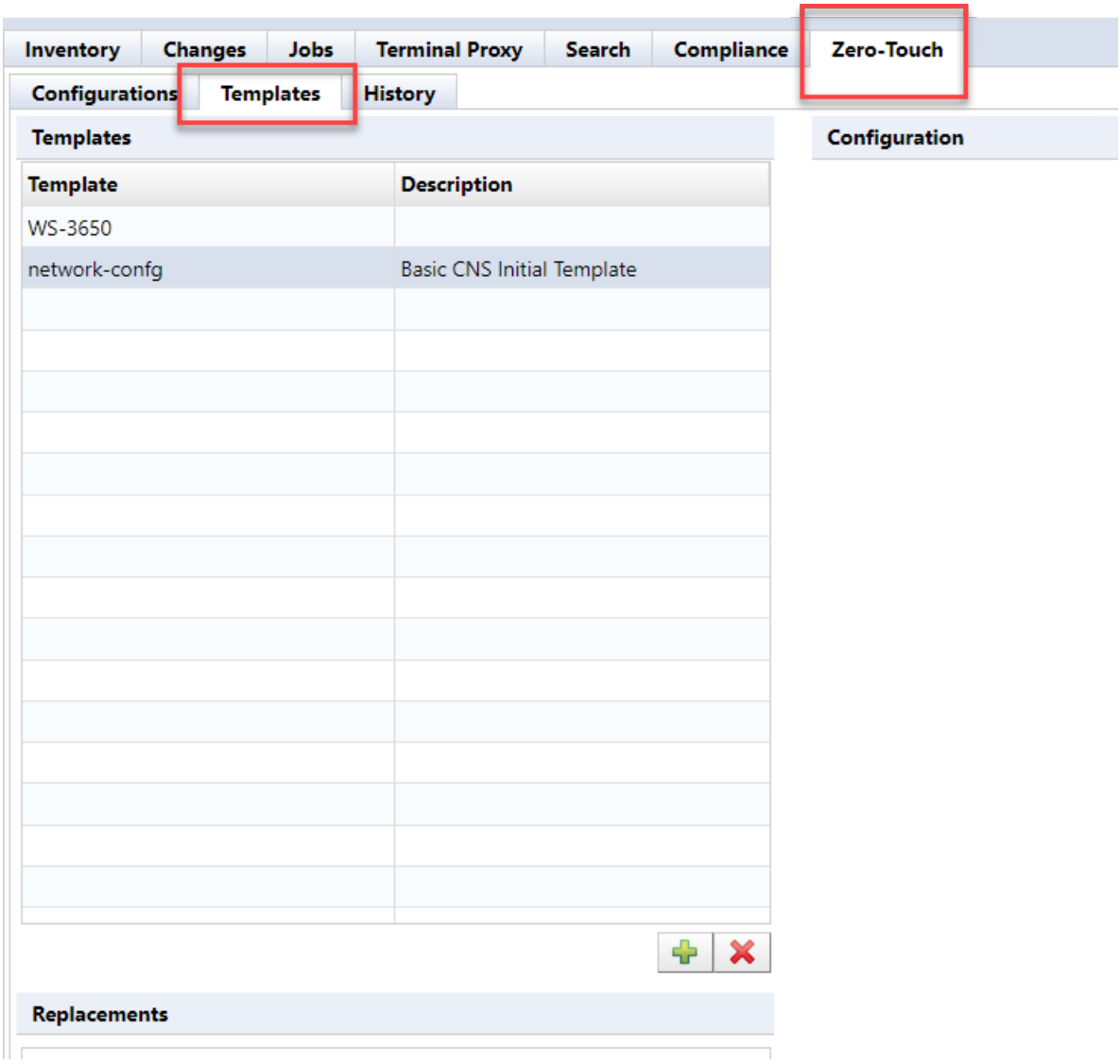


6.7.5 Creating a template

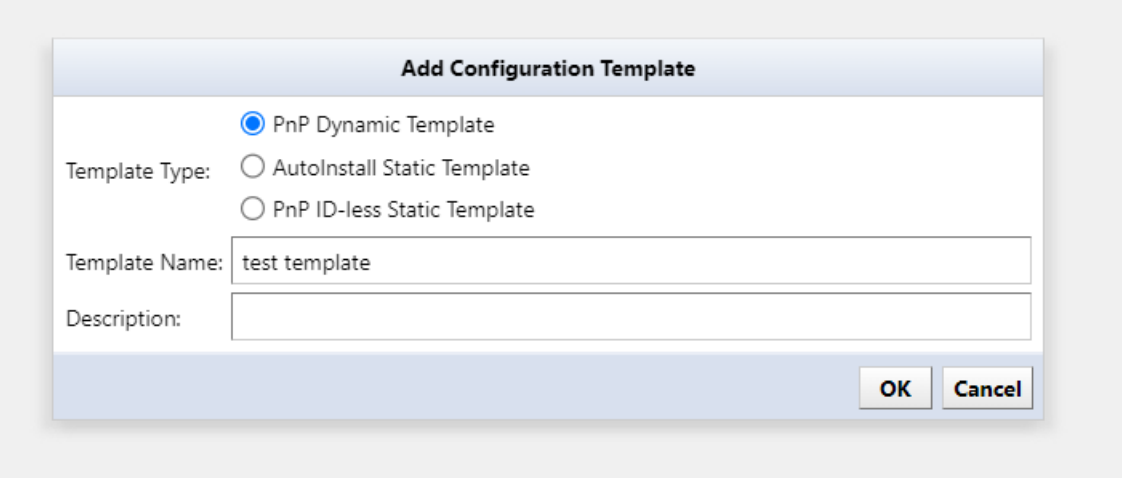
In large networks, there may be multiple devices with similar configurations, but differeng IP addresses, hostnames, DNSs, and syslog server addresses, Smart Change utilizes templates to send similar commands tailored for each device. Zero-Touch can utilize the same template for commands *and* device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

Follow the steps below to create a template:

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



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



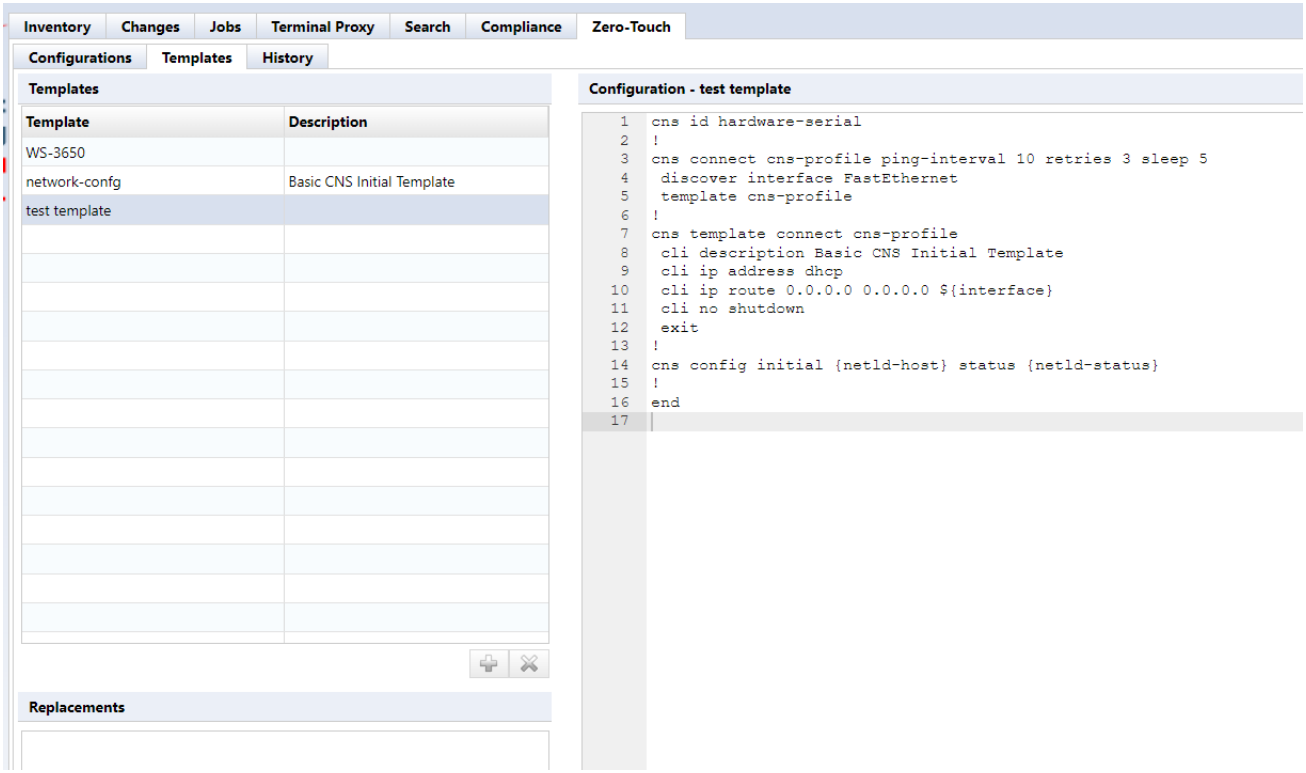
A large “Configuration” text area called the will open on the right side of the screen.

7. Enter the original configuration in this area.

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

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

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

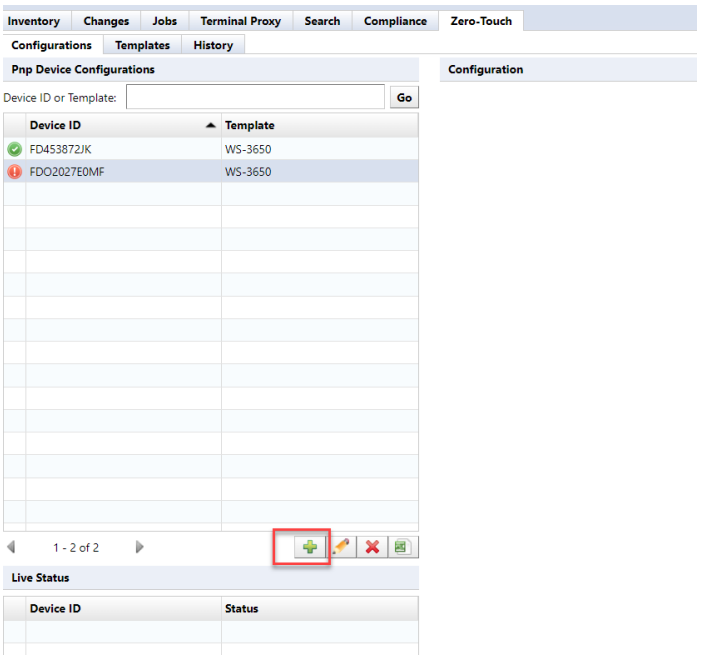


If you do not want to save the deployed configuration on the device, add a no-persist option at the end of cns "`config initial...`" when deploying the configuration.

Device registration

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

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



Importing values from outside into template variables

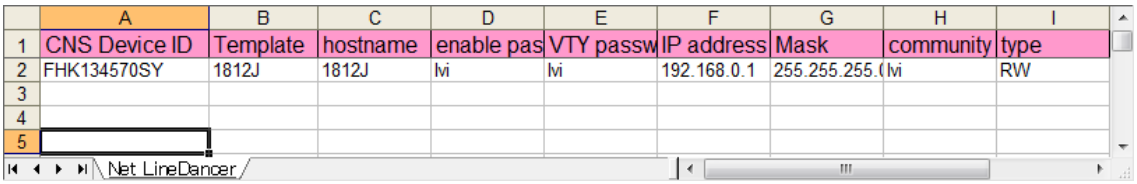
Tables written externally in can be used as template values.

Follow the steps below to import Excel files:

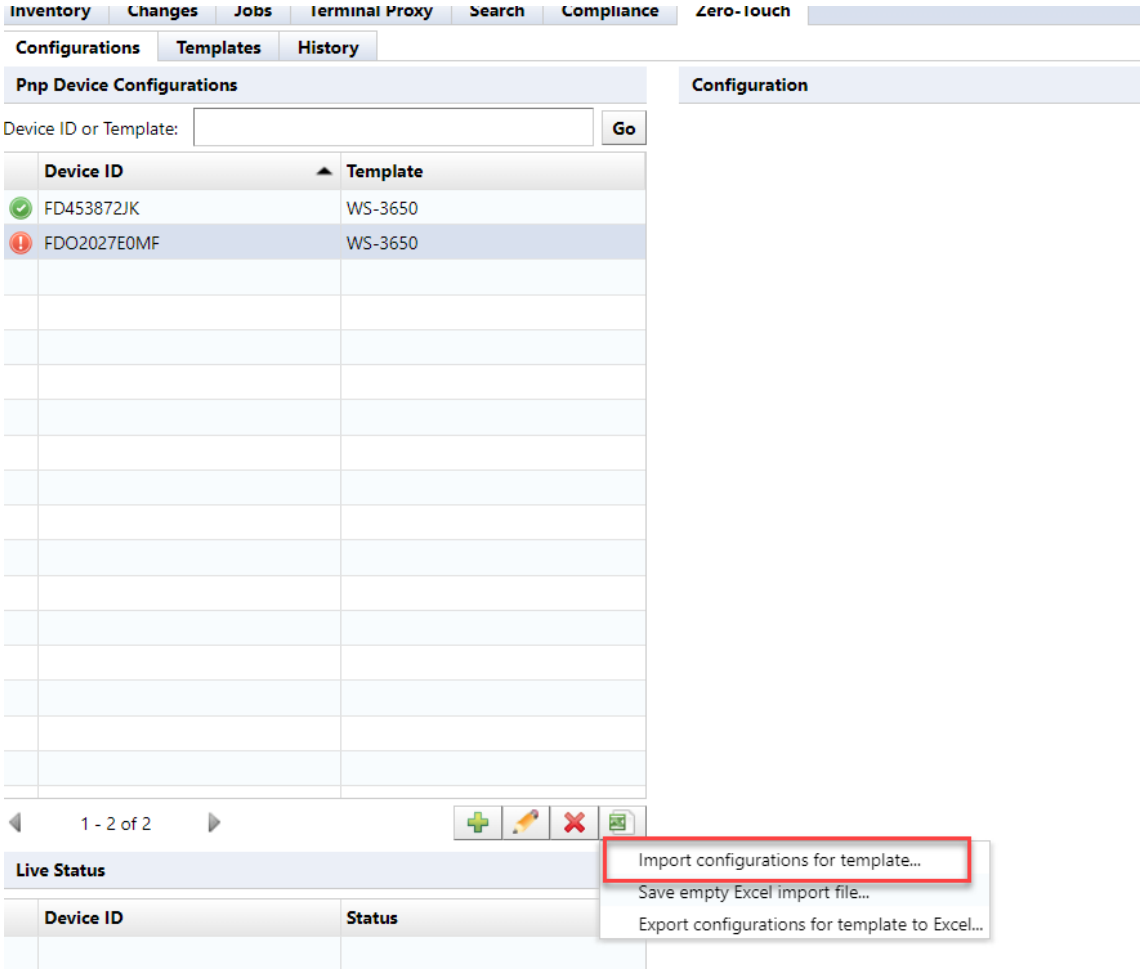
1. In the [Zero-Touch] tab, click the [Close] button if editing device data.
2. Click the [Import] button to display the submenu.
3. Select [Export import file] or [Export template] from the menu that appears.

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

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



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

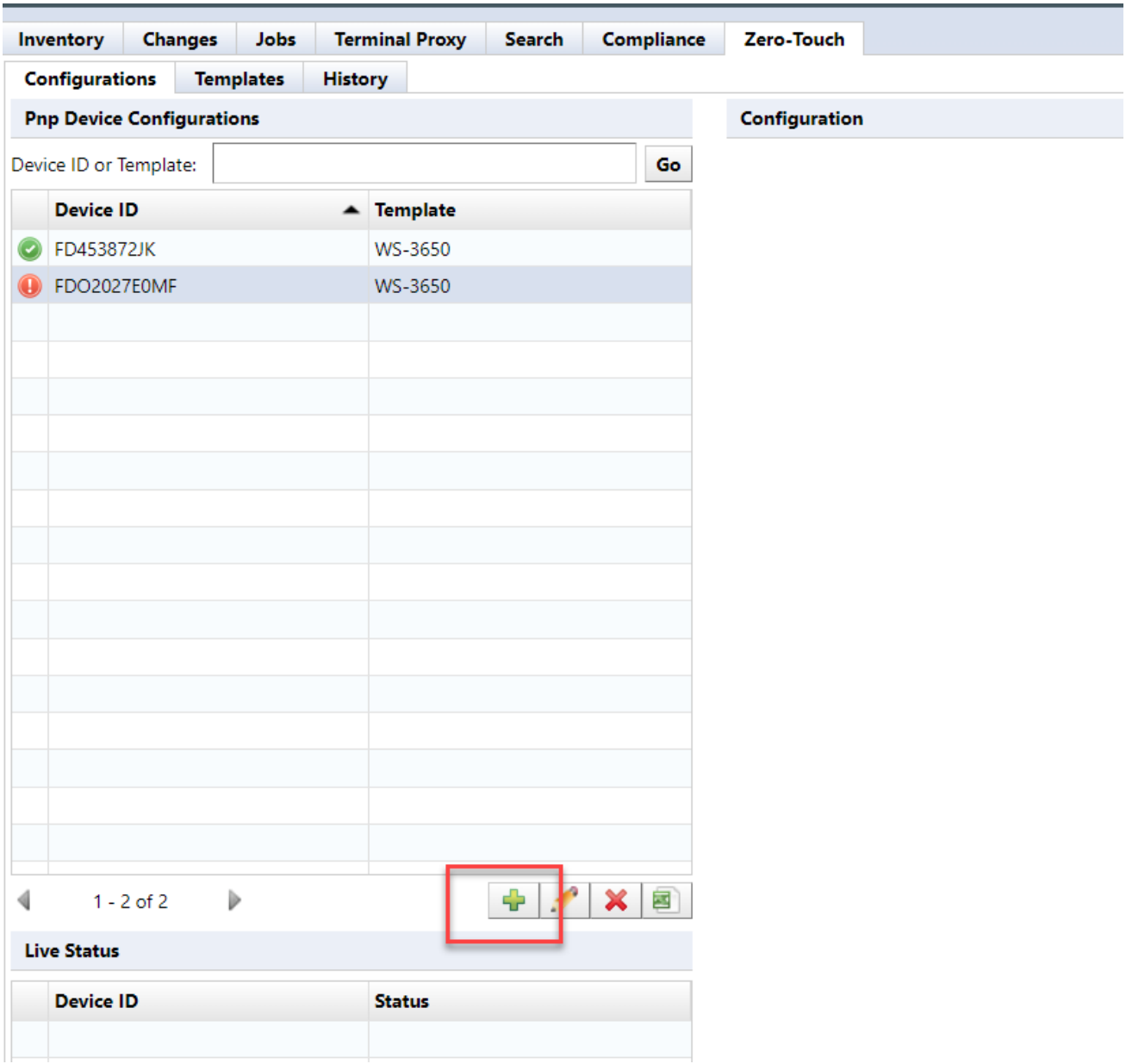


6.7.6 Zero-Touch self-recovery

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 steps are similar to other Zero-Touch template steps:

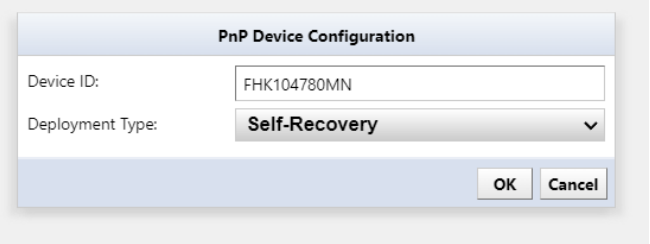
1. Click the [Zero-Touch] > [Configuration] tabs.
2. Click the button on the [Configuration] tabs.



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

type] dropdown menu.

5. Click the [OK] button to save.



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

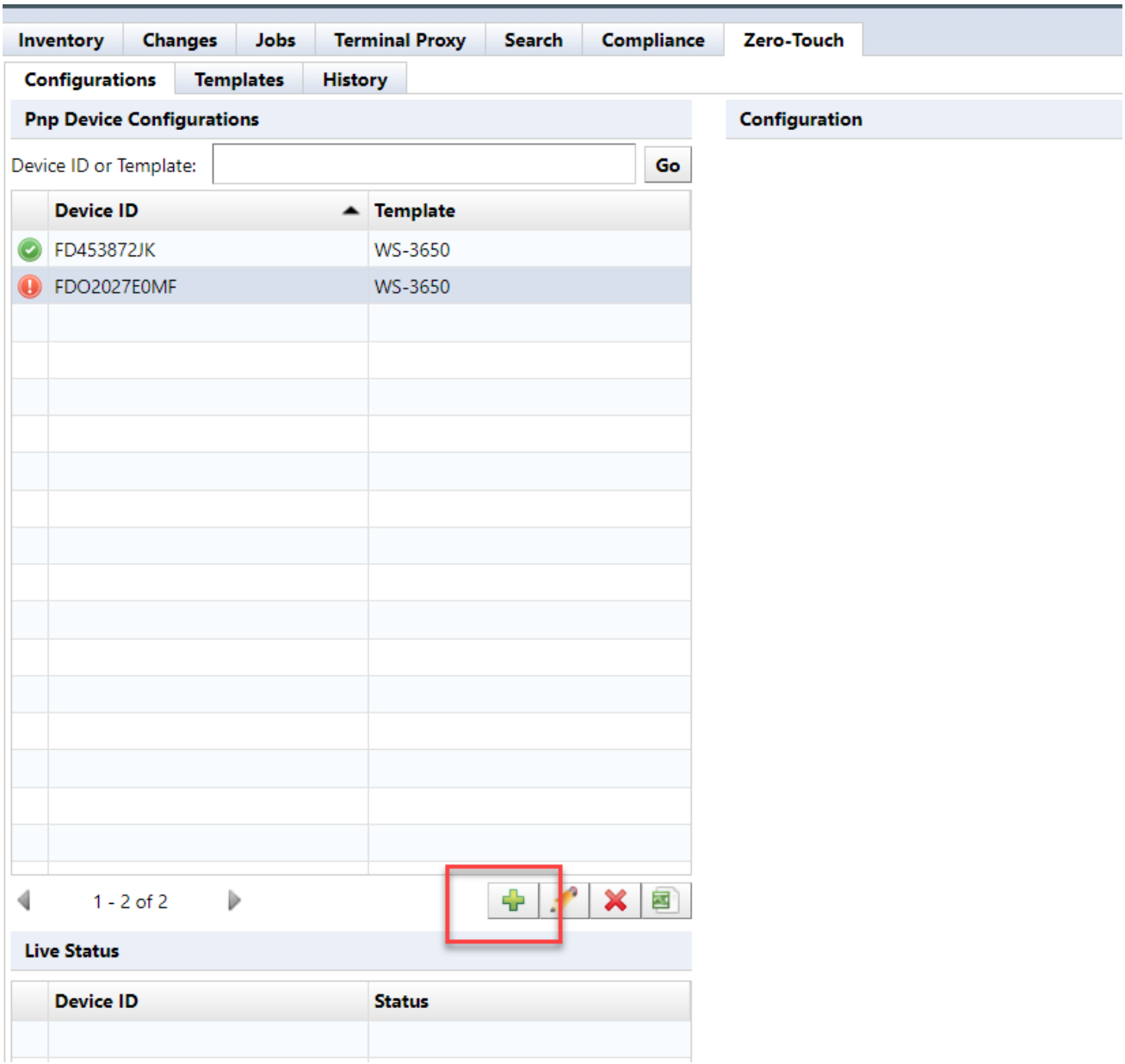
6.7.7 Zero-Touch Specific Device Restore

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

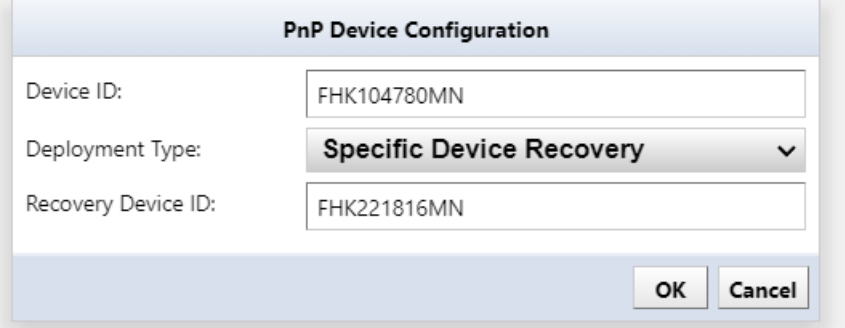
When you run Zero-Touch in this mode, you can connect a new device to the same location as the old device, write configuration from your old device to your new device, and restore your old device.

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

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



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



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

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

6.7.8 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.)

6.8 Playbook

The Playbook tab is a workflow automation interface designed to simplify and automate network management tasks using your custom scripts.

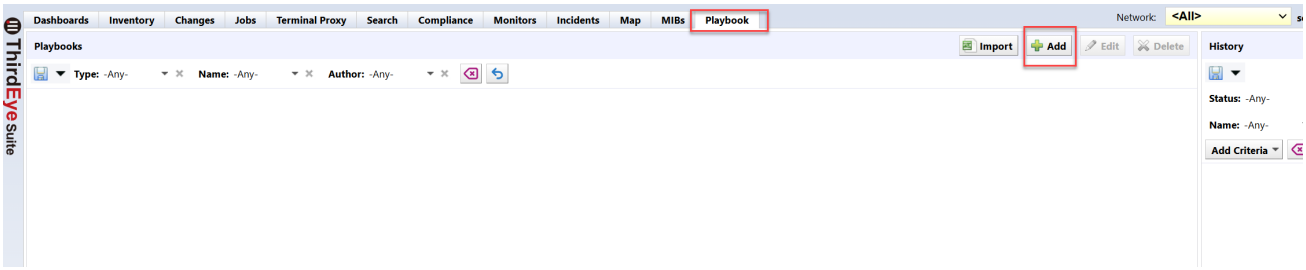
6.8.1 Playbook Features

- **Drag-and-Drop Interface** allows design and implement complex automation workflows.
- **Customizable Plays** allows the creation of individual plays for specific tasks can then be combined into larger “Playbooks” for more comprehensive automation.
- **Push-Button Execution** allows push-button execution of complex tasks.
- **Streamlined Workflow** allows the facilitates the automation of repetitive tasks.

Playbook example:

6.8.2 Setup and configuration

At the top of the page, click on the Playbook tab. Then click on the Add button.



In the [Add New Playbook] popup window, enter the "Name" of the job, and a corresponding "Description", then click [OK].

On the right side of the screen, is the [Node] panel. These are the different options to configure a job to run. These are the current nodes, more will be added in future releases:

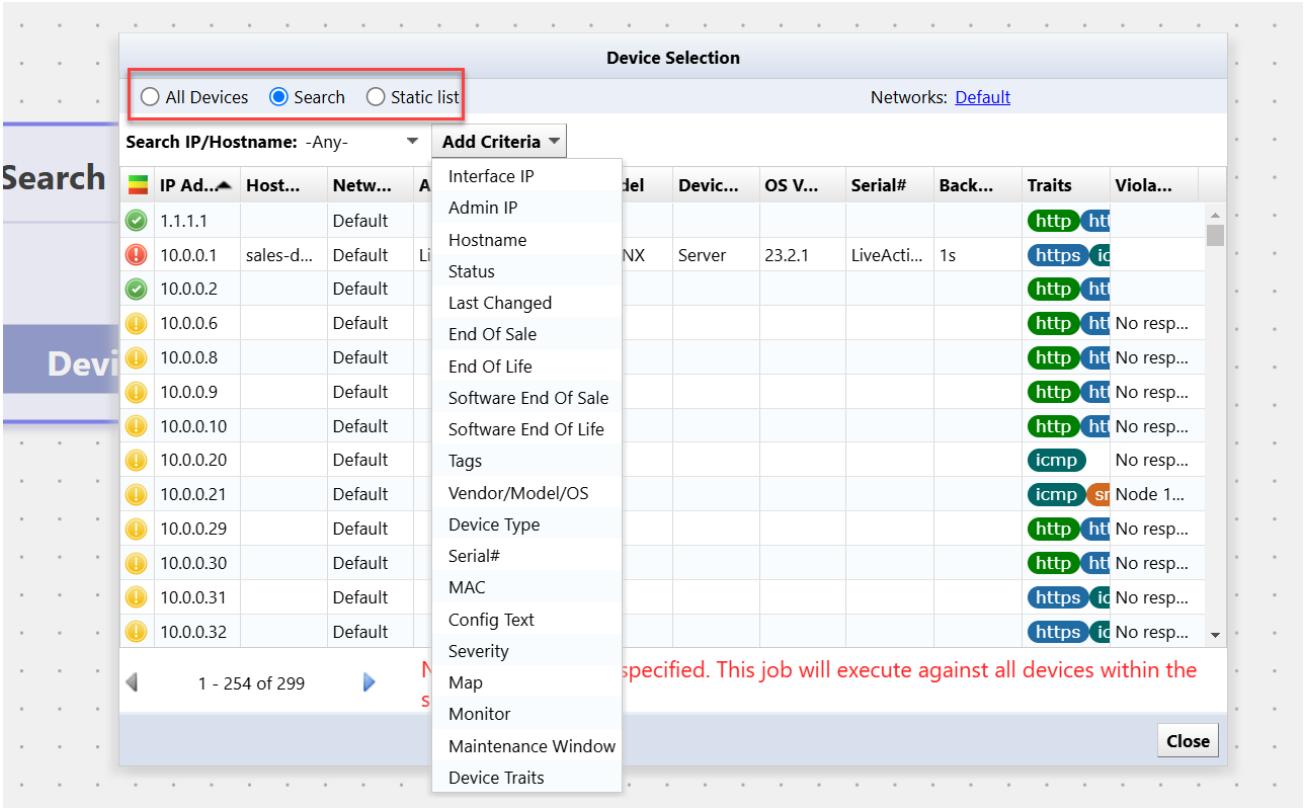
Node Option	Explanation
And	Only proceed after both inputs have received a signal
Backup Device	Run a device backup
Chat App	Webhook to send messages to either Teams/Slack/Mattermost/Webex
Compliance Violation	Get information from a Compliance Rule Set configured to run this playbook
Device Search	Search for devices in the inventory to be acted upon
Email	Send an email with tabular data
Incident	Get information from an alert policy configured to run this Playbook
Memo	Save a note
Regex Match	Execute a regular expression against the output of a node
Rule Set	Run a Rule Set against the output of a node

Node Option	Explanation
Run Code	Run a block of code on your devices
Run Code with Automatic Retry	Run a block of code on your devices a number of times or until it is successful
Schedule	Schedule this playbook to run automatically
Sleep	Delay for a number of milliseconds before forwarding input
Upload File	Send a file to your devices

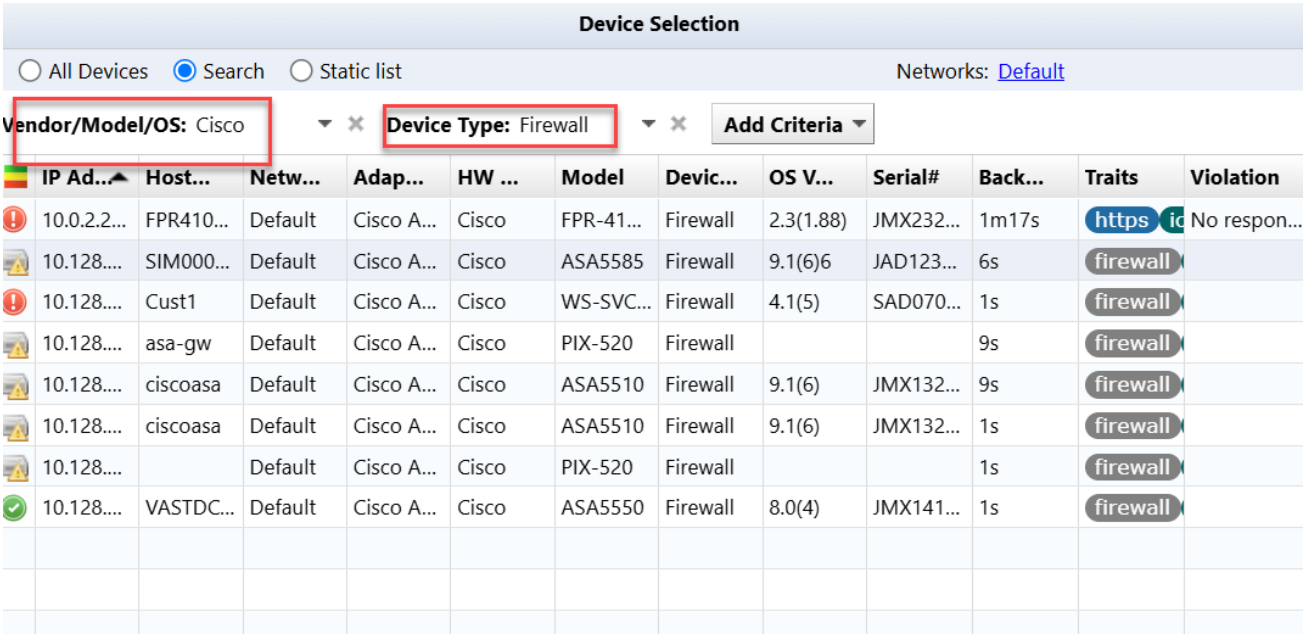
6.8.2.1 Create a playbook From the node panel, click and hold a node, and drag it to the playbook field. Once the node is in the play field, click the button in the top right corner of the node to give the node a description.

On the node, click on [Device Selection]. In this screen you have 3 options:

Option	Explanation
All Devices	Select all devices in the Inventory tab
Search	Select the [Add Criteria] and select options to select devices
Static List	Select devices from the Inventory tab and add to the selection



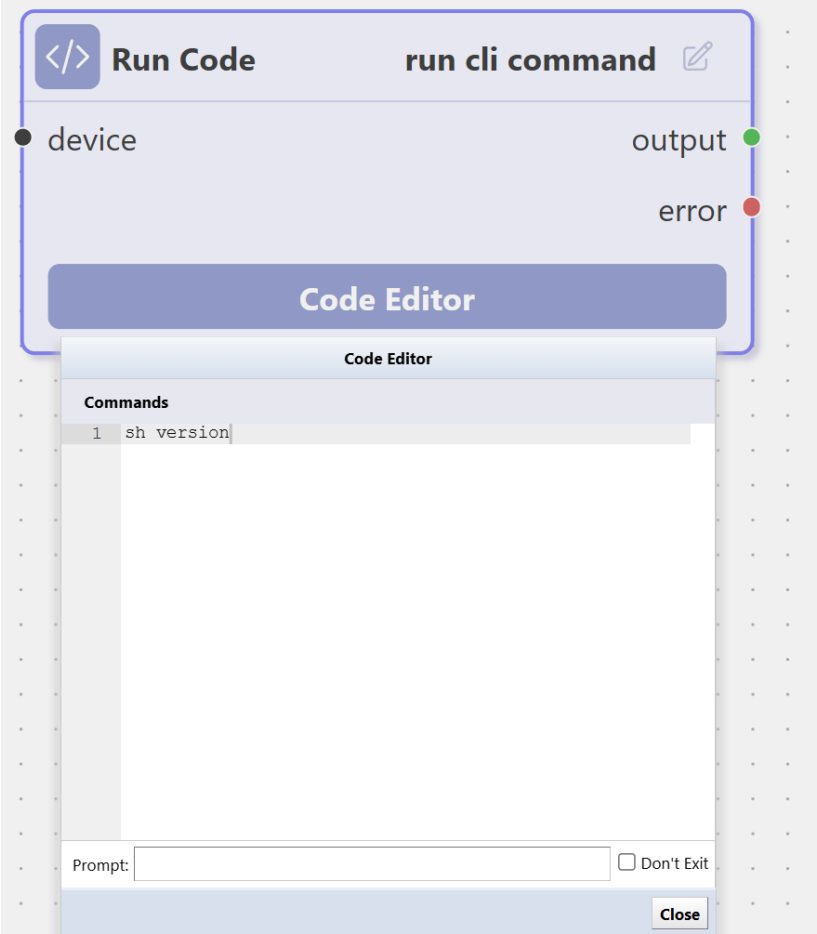
Enabling “Search” allows you to narrow your search using multiple criteria.



Add another node from the node table.

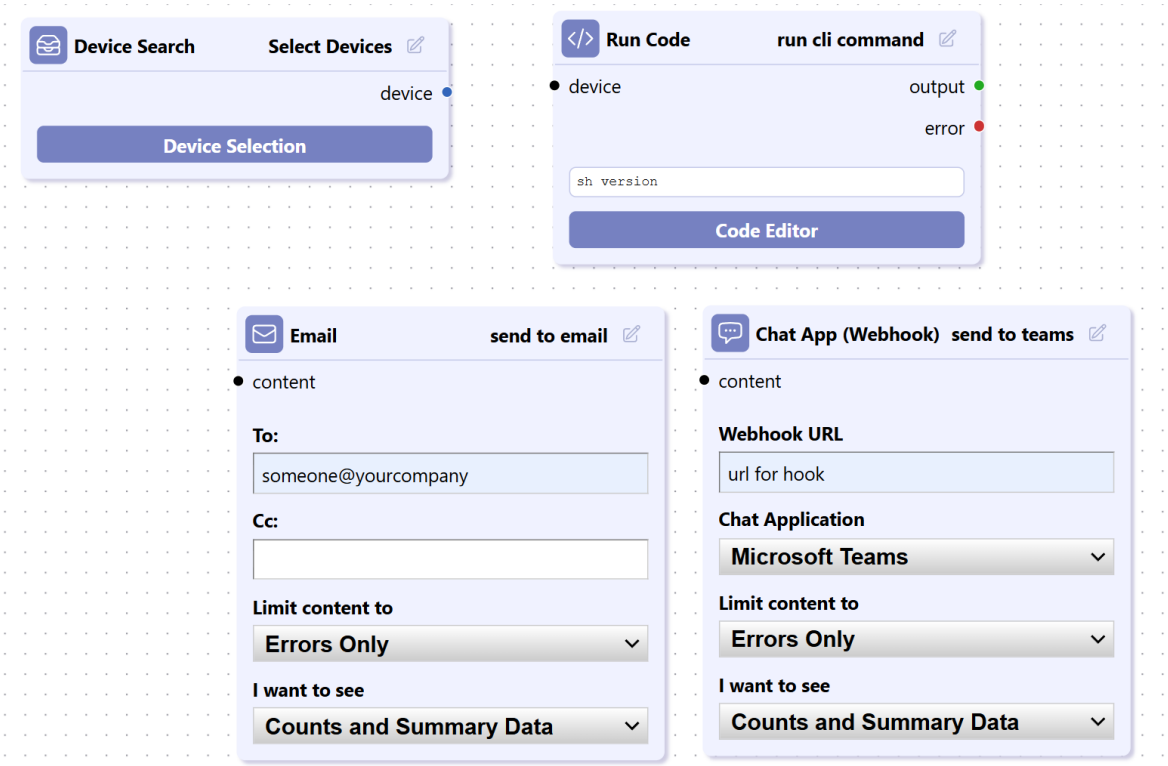
Select [Run Code] to change the description.

Click on [Code Editor] to enter any cli command for the devices you have selected.



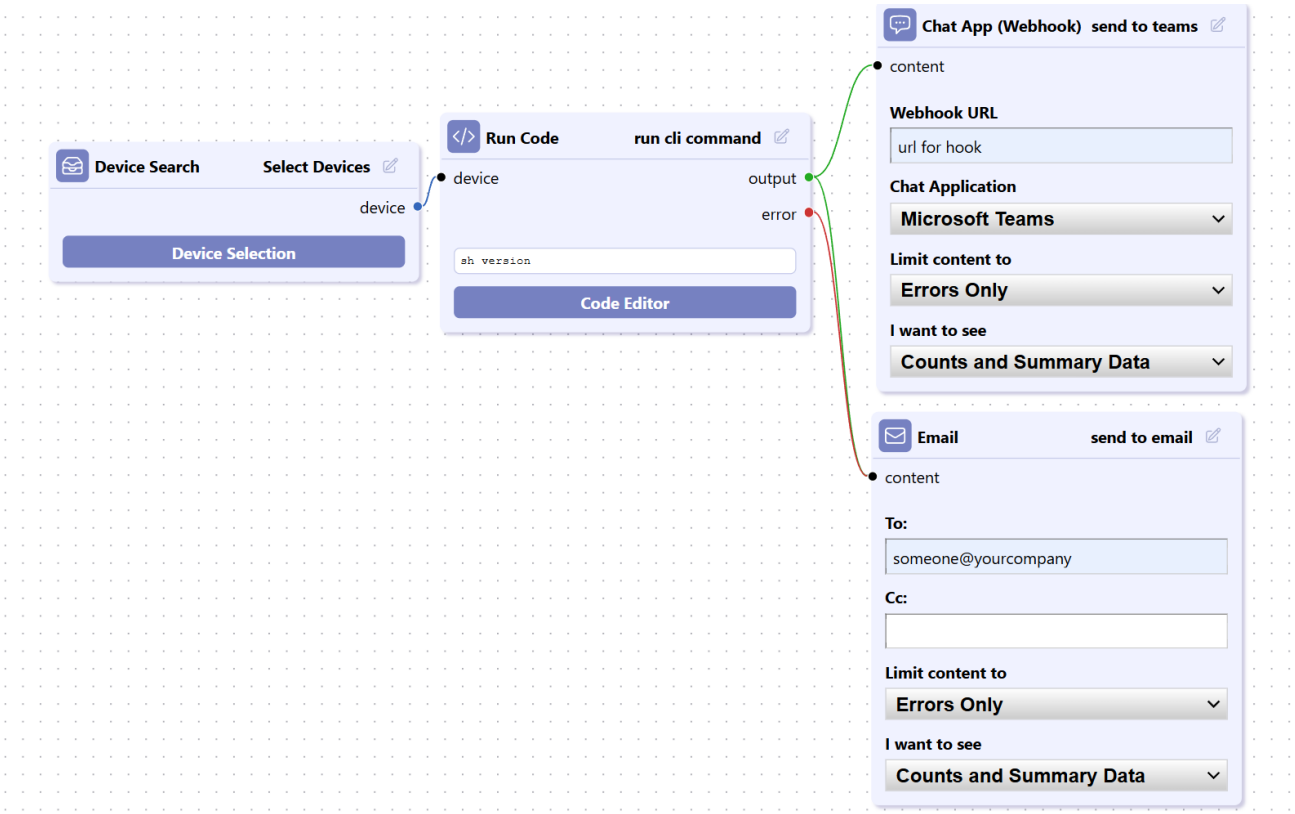
For Results you have three options:

Option	Explanation
Send email with results	Move email node to play field
Search	Send results with webhook to Teams/Slack/Mattermost/Webex/Line
Static List	Both email and webhook



In the “Email” and “Webhook” windows, you can click the pulldown menus to select reporting options.

Next, connect the nodes.

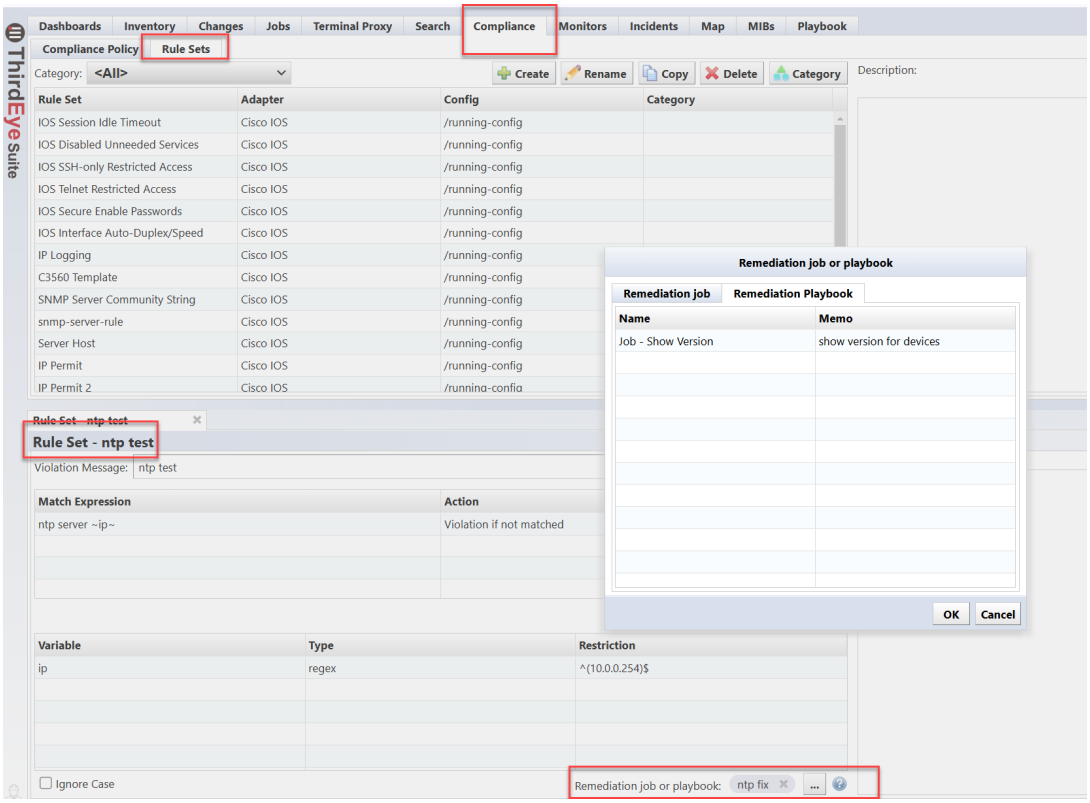


To remove a node, or a connection, select the desired item, and on your keyboard, click [Backspace].

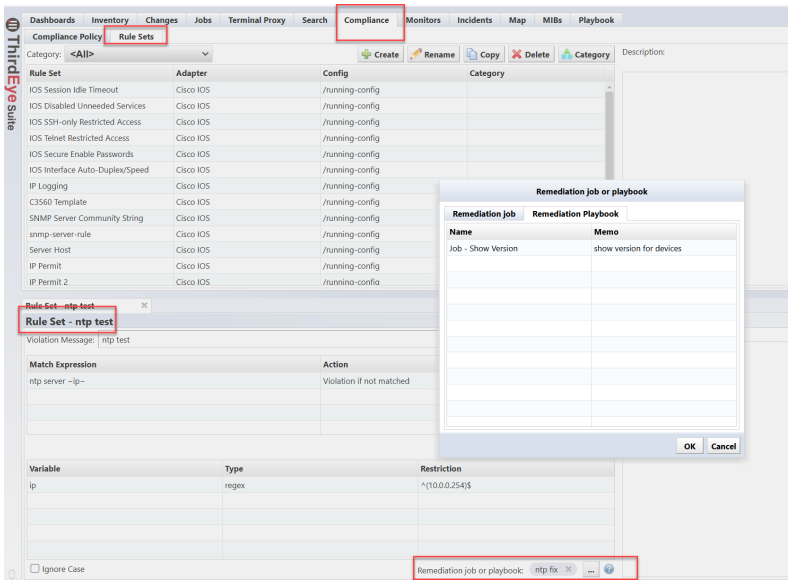
6.8.2.2 Compliance/Incident issues You can select a Playbook job to run remediation for both Incidents and Compliance issues.

Compliance Issues

1. Click the Compliance > [Rule Sets] tabs.
2. Select a Rule Set in the “Rule Set - ntp test”.
3. Click the [Remediation job or playbook] button in the lower right of the page.

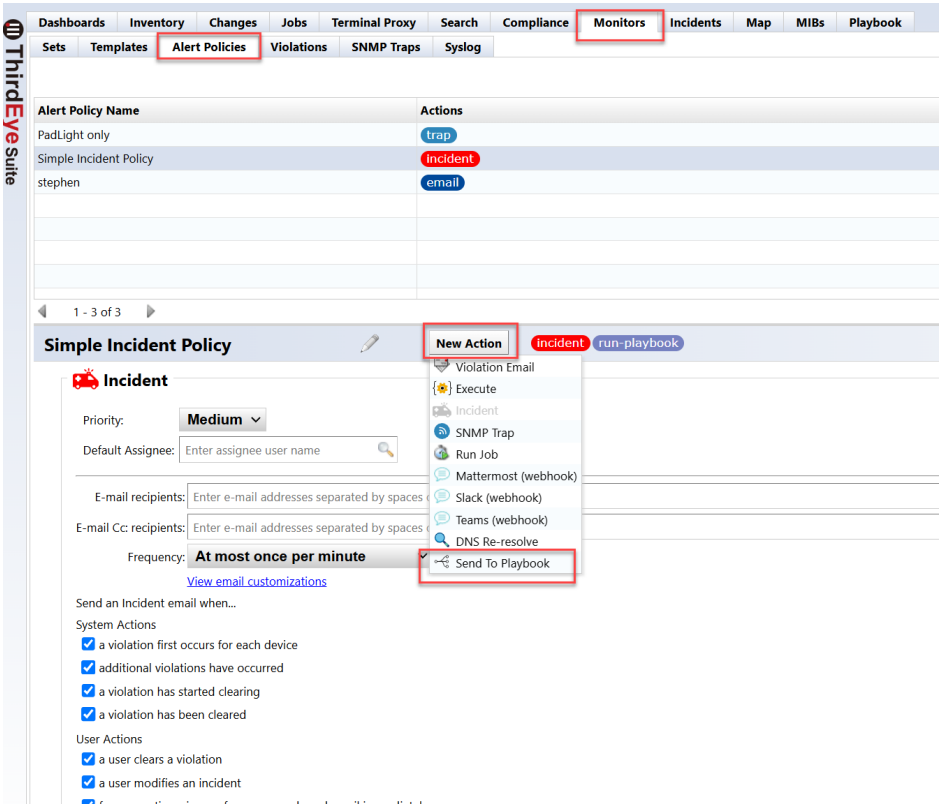


Compliance example:

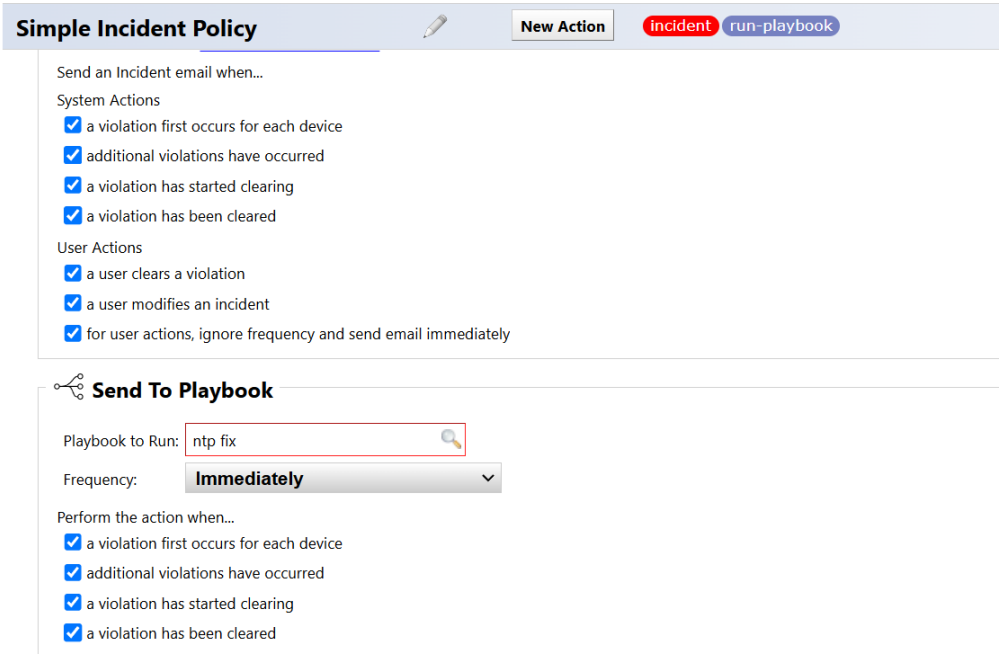


Incident Issues

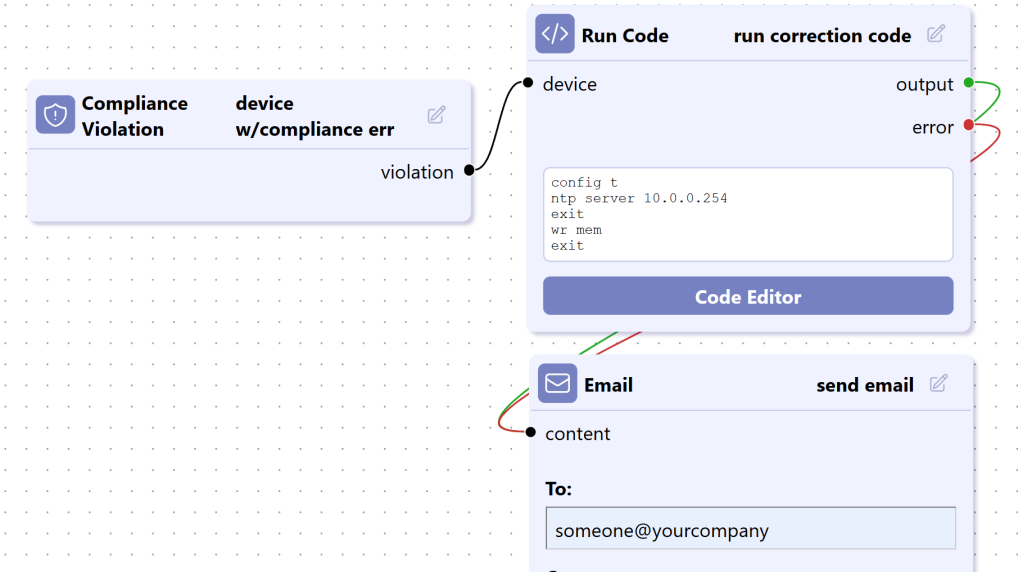
1. Click the [Monitors] > [Alert Policies] tabs.
2. Add a “Alert Policy Name”, or select an existing Alert Policy.
3. Click [New Action]. (You have the option to add [Send to Playbook]).



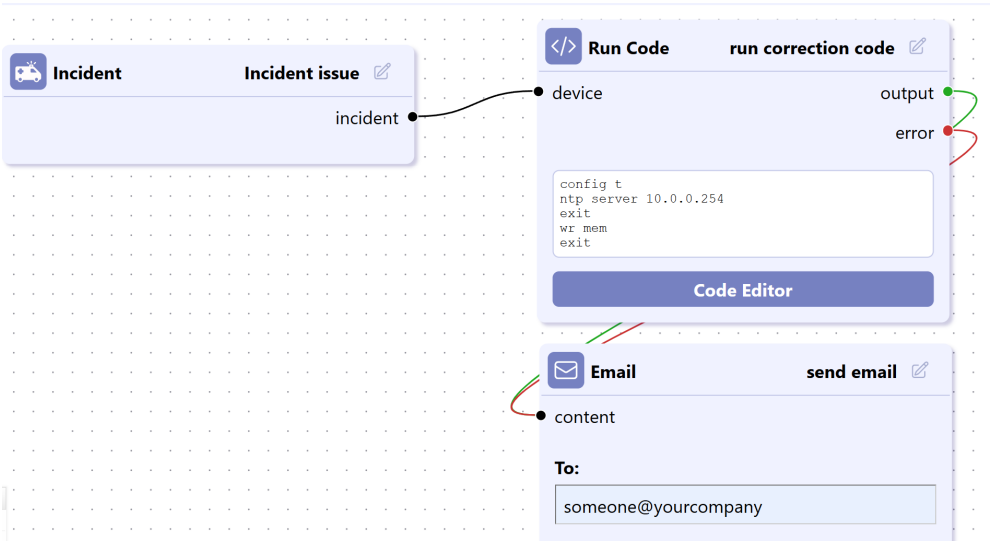
Once added, select the “Playbook to Run”, Frequency”, “Perform the action when…” options.



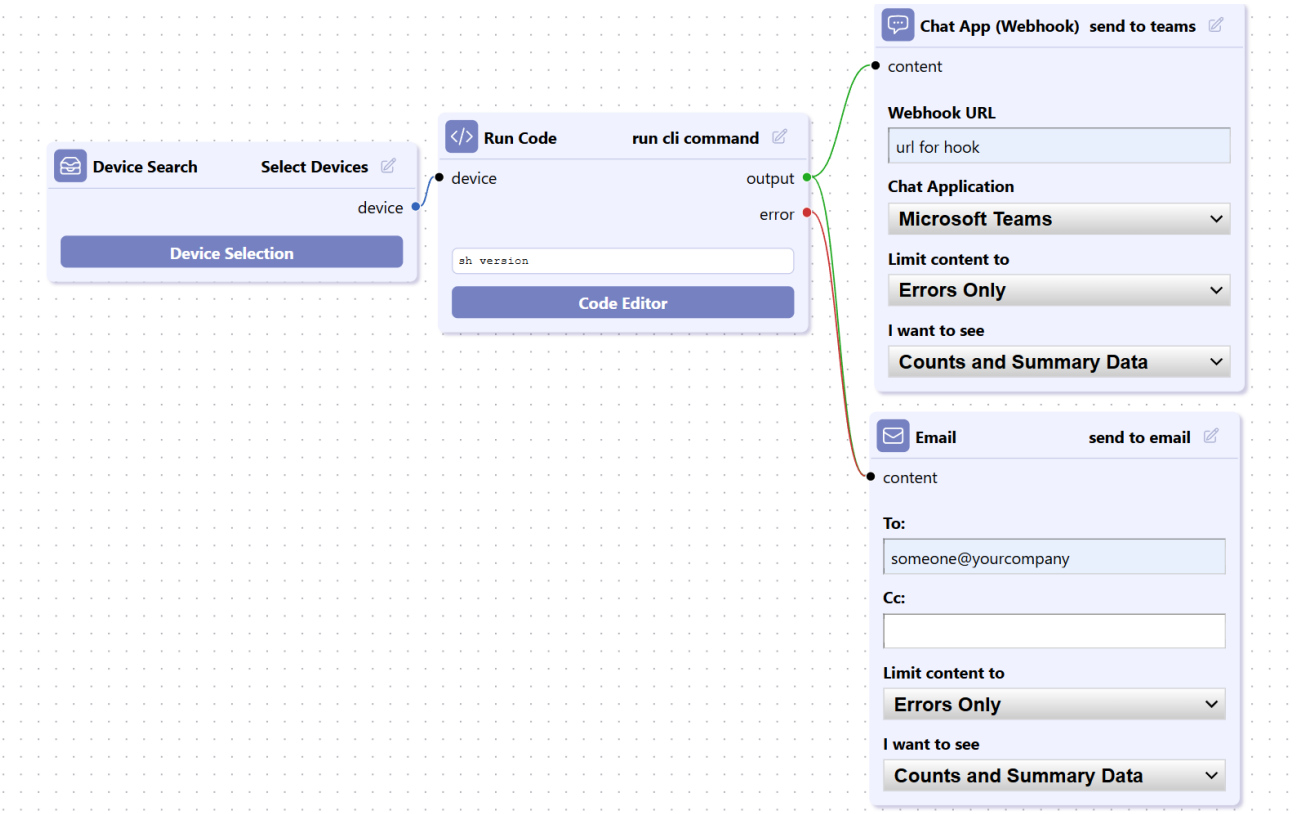
Compliance example:



Incident example:



Next, connect the nodes.



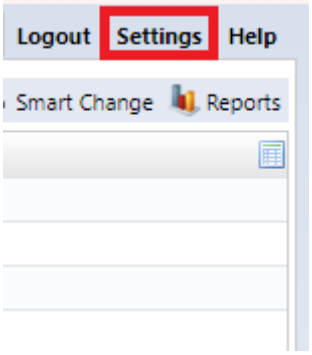
To remove a node, or a connection, select the desired item, and click on [Backspace] on your keyboard.

6.8.3 Set up mail server

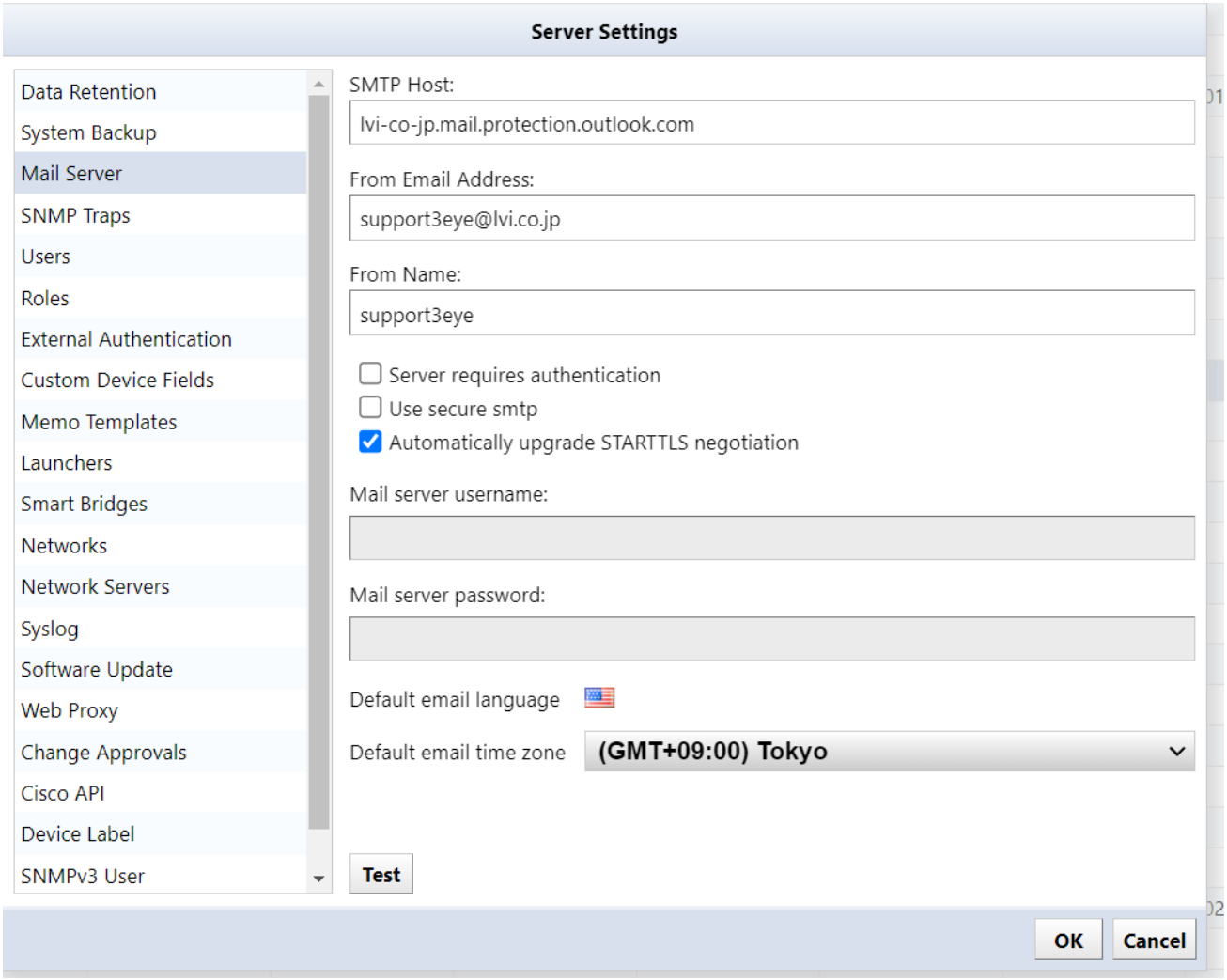
Enter the SMTP server information for Email Server notifications from NetLD.

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

1. Click Settings on the Global Menu.



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



Field	Explanation
SMTP Host	Specify the host name or IP address of the mail server. (Initial value: `mail`)
From Email Address	Specify the email address that will be displayed as the sender (sender) of the email. (Initial value: `netLD`)
From Name	Specify the name that will be displayed as the email sender's name (sender). (Initial value: `netLD`)
Server requires authentication	Configure mail server authentication. If SMTP authentication is required, check the box and configure the following items. (Initial value: `disabled`) Mail server username… Authentication ID

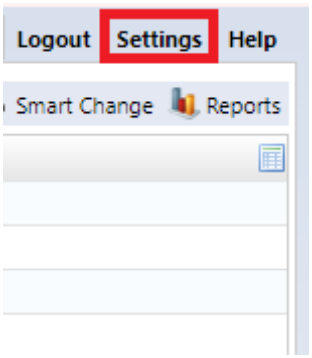
Field	Explanation
	Mail server password… Authentication password
Use secure smtp	Enable TLS.
Automatically upgrade STARTTLS negotiation	Automatically upgrade to secure connections using TLS or SSL.
Default email language	Set the email display language.
Default email time zone	Set the email time zone.
Root Certificate	Set the trusted CA certificate.

3. Click [OK].

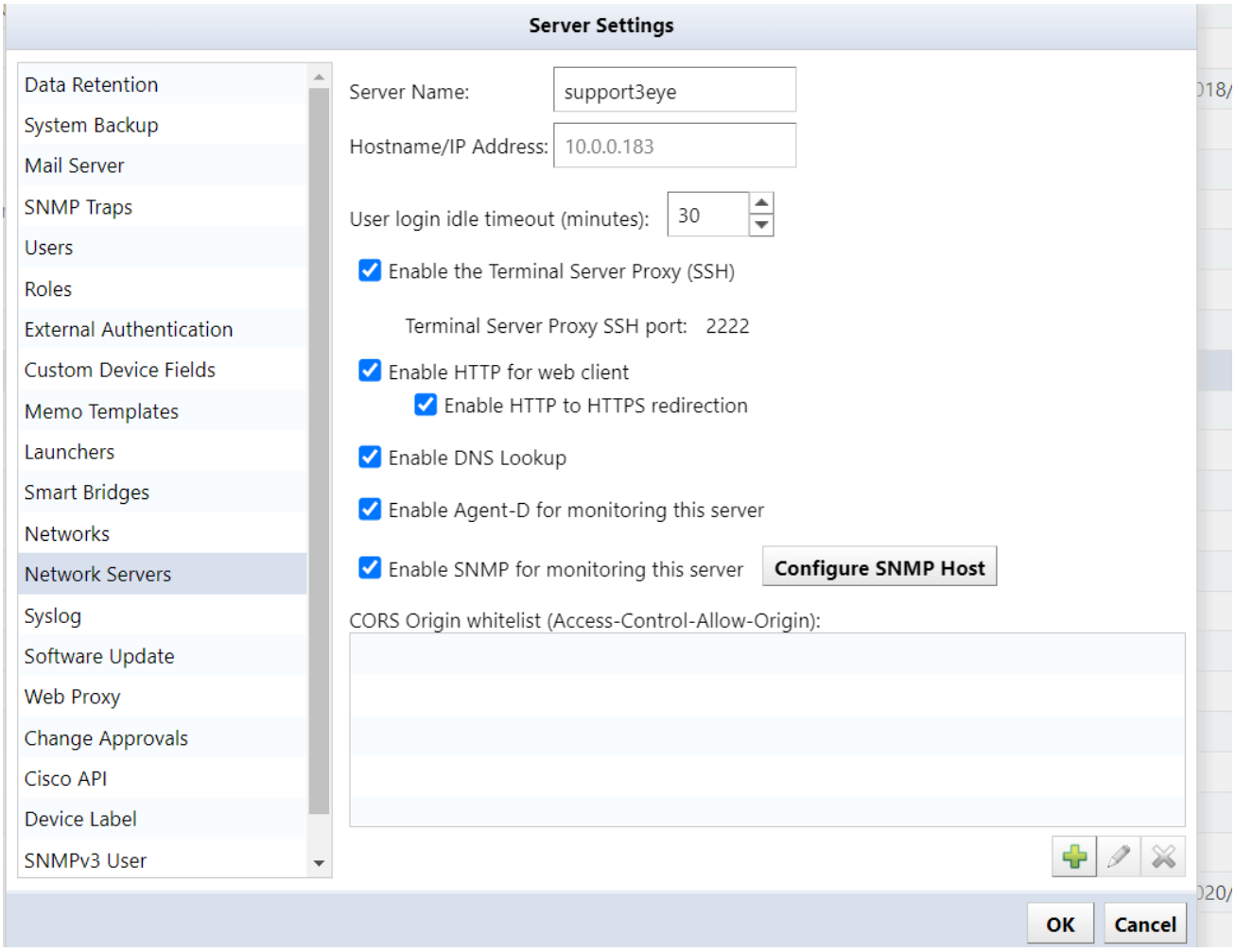
6.8.4 Use sysName for hostname

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

1. Click Settings on the Global Menu.



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

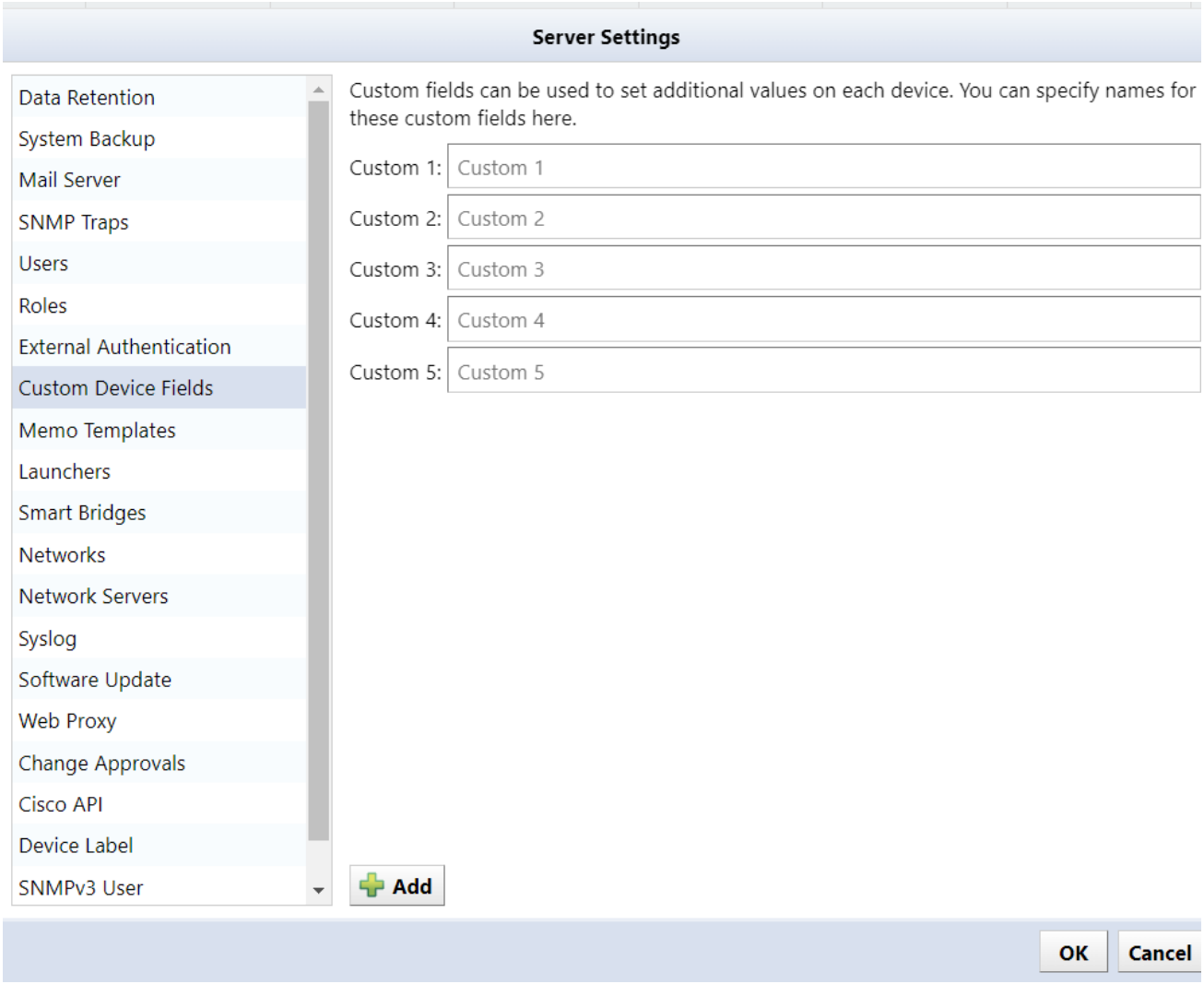


3. Click [OK].

6.8.5 Add columns/change column names for custom device fields

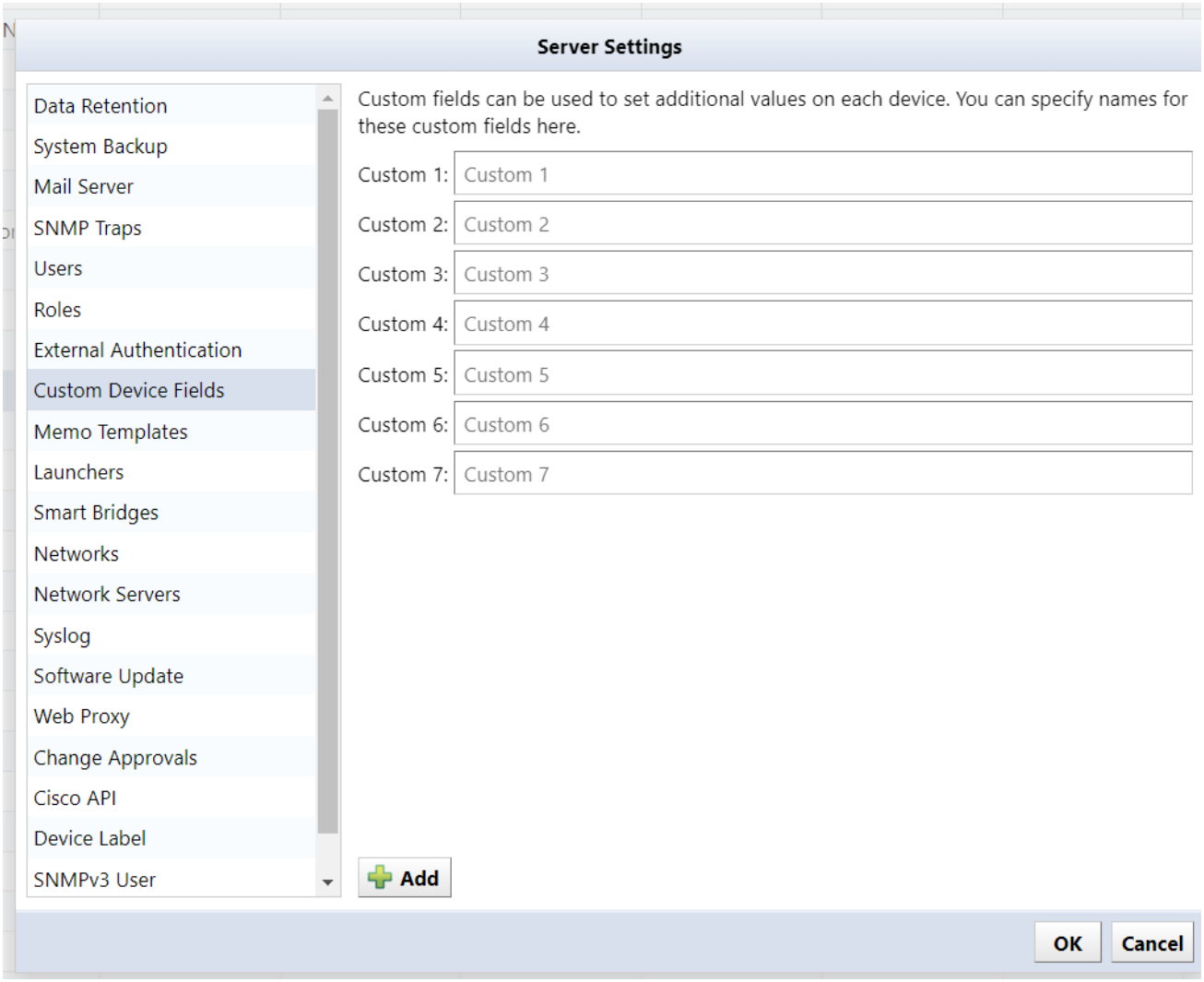
The custom device field allows you to set the name of a custom column to be used in device tabs and searches.

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



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

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



Note

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

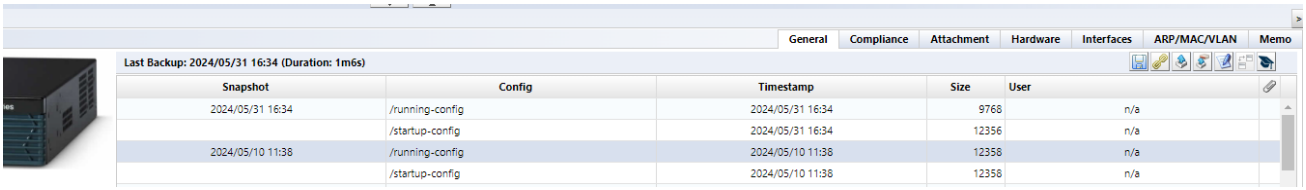
6.9 Draft configuration

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.

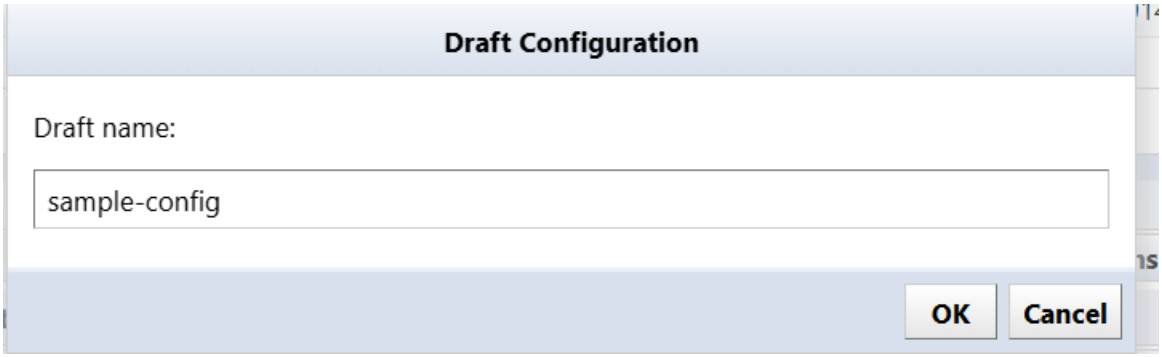
6.9.1 Creating a draft configuration

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

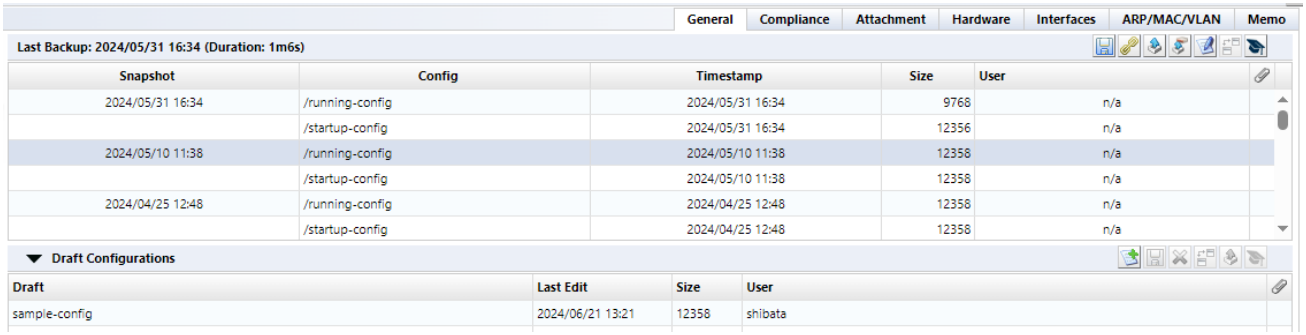
1. Doubleclick the target device to open the configuration history.
2. Select the one you want to base your draft configuration on and click the  button.



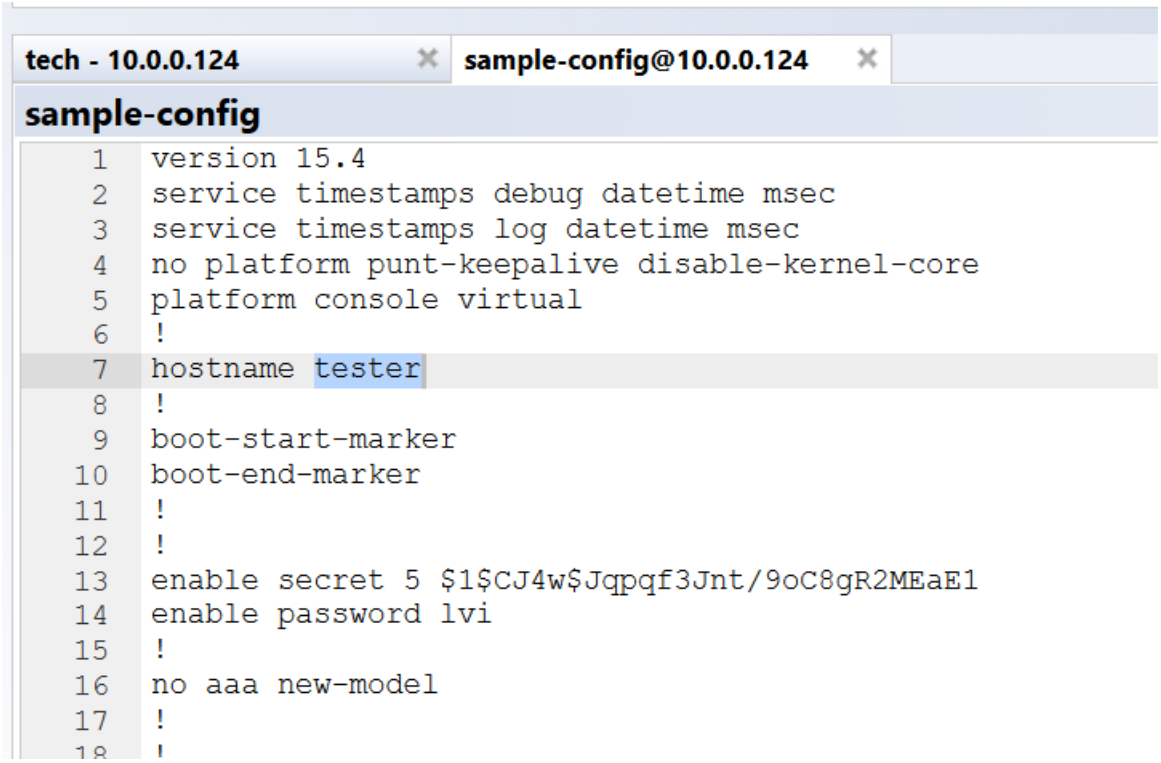
3. Enter a name for your draft configuration and click [OK].

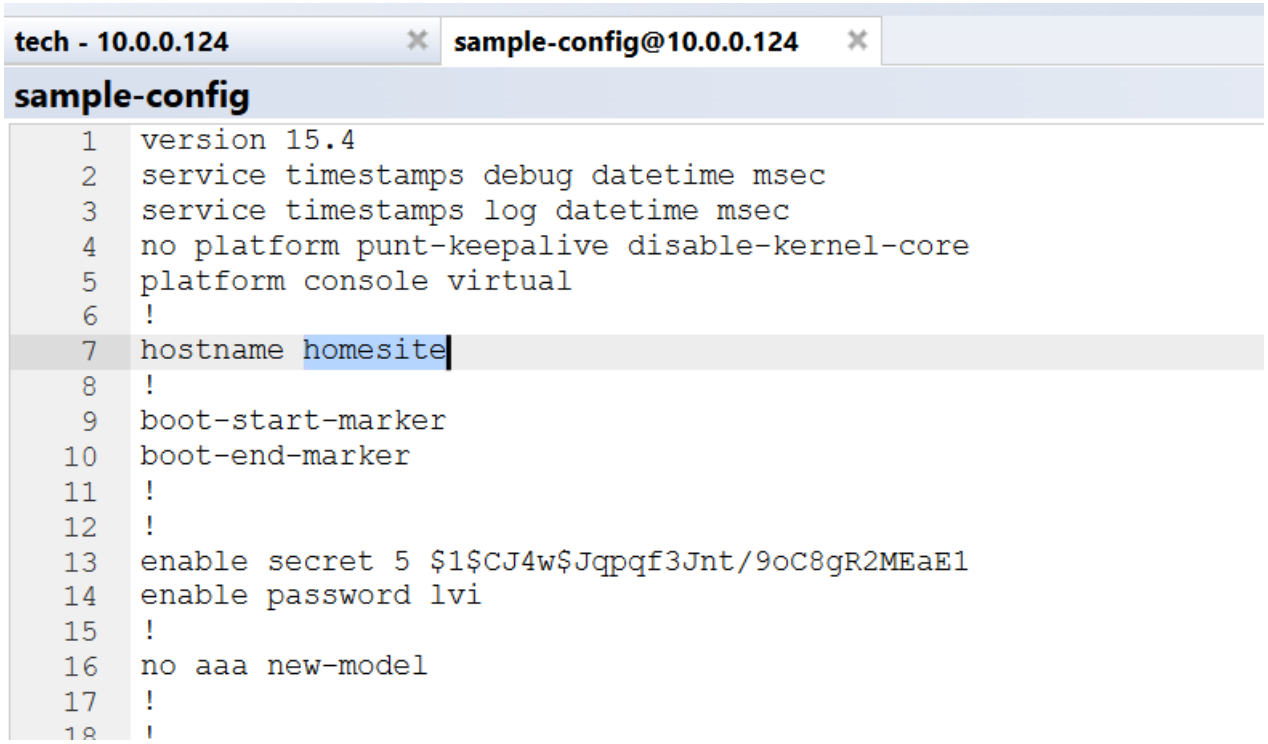


4. Doubleclick the created draft configuration.



5. Edit the configuration and click the button to save.

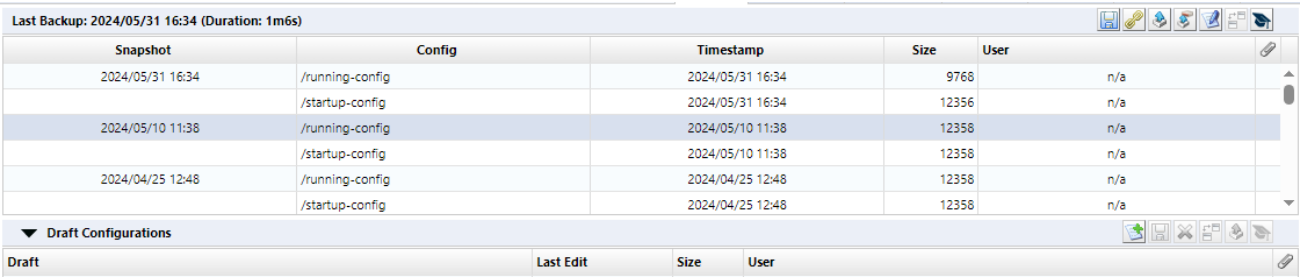




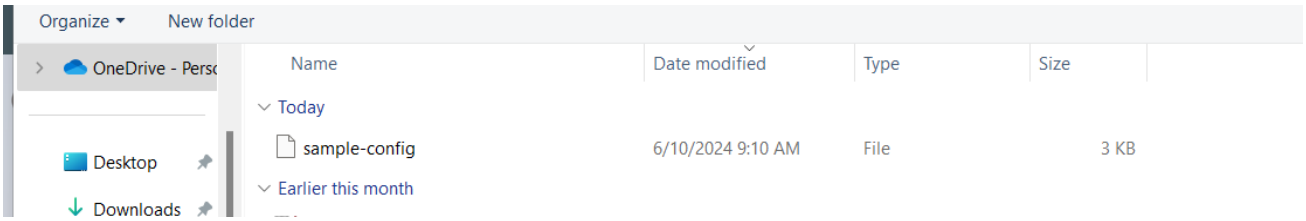
6.9.2 Import draft configuration from plain text

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

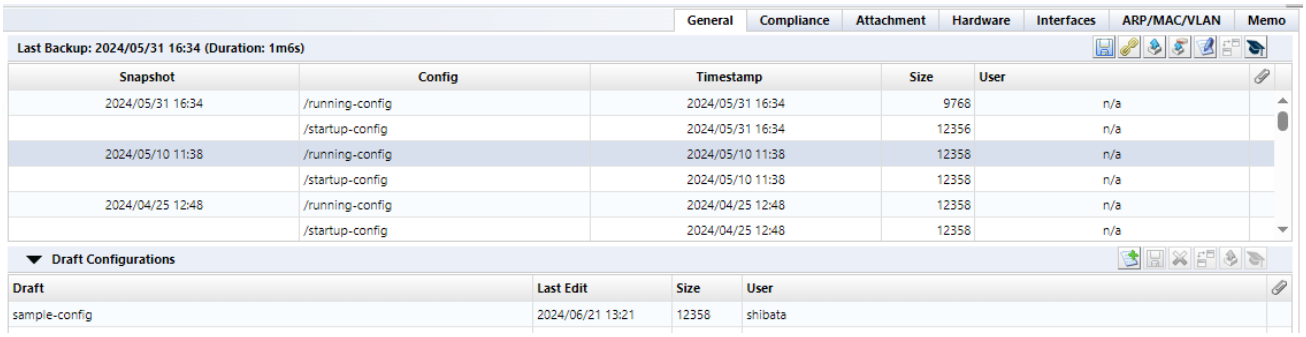
1. In the backup status panel, click the  button.



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



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



6.9.3 Export a draft

To export a draft configuration, click the  button.

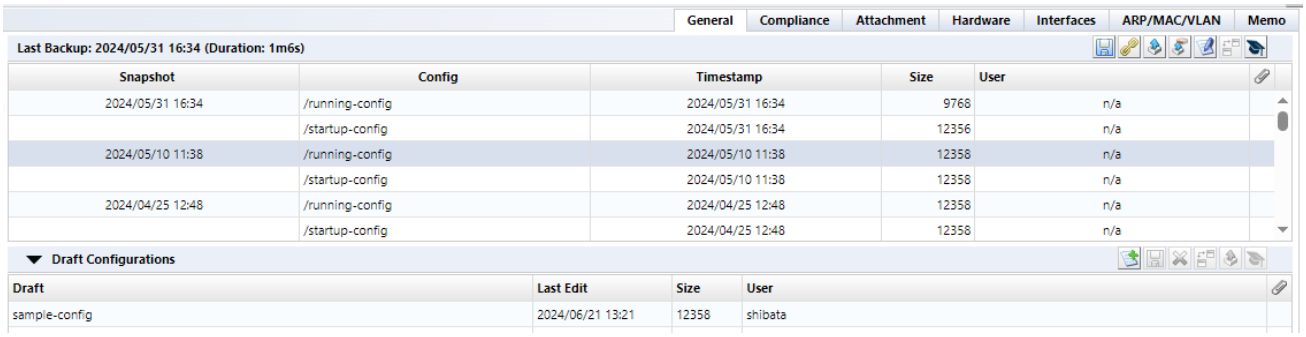
6.9.4 Delete a draft

To delete a draft configuration, click the the  button.

6.9.5 Compariing draft configurations

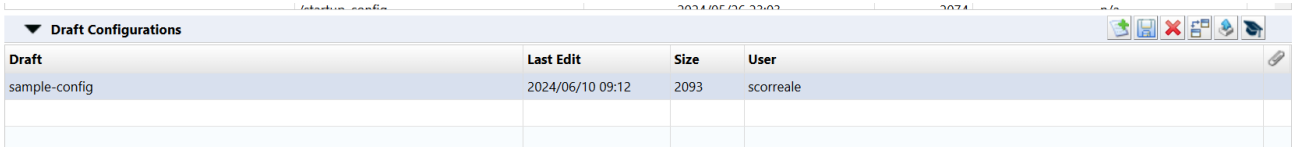
To compare draft configurations, click the button.

You can use the same comparison functions in draft configurations as in regular configurations.



6.9.6 Apply draft configuration to devices

Applying drafts can be done using the same procedure as applying (restoring) backup configurations. However, you must select the draft configuration to upload, then click the button.



Next, select which draft configuration you would like to upload to.

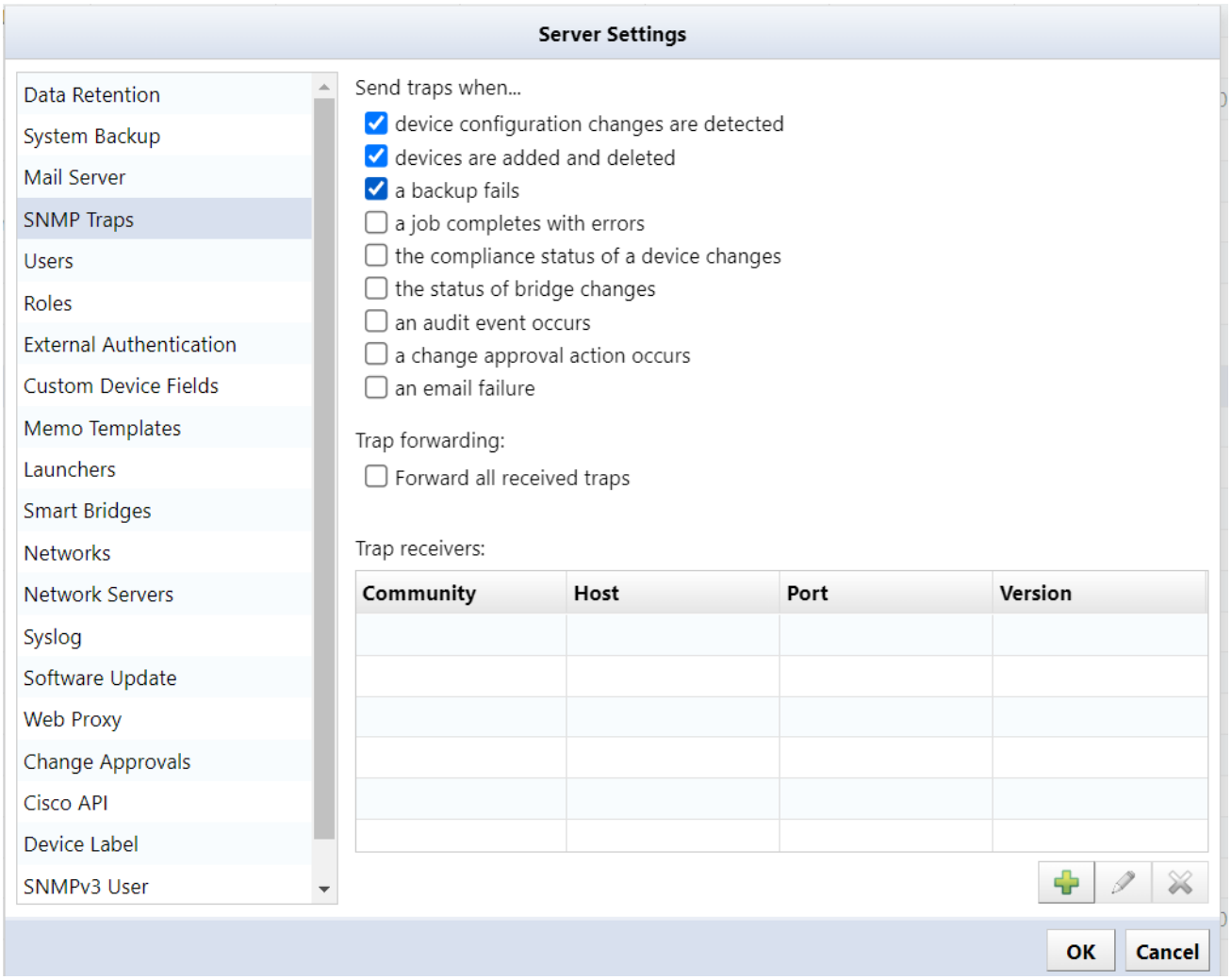
> **Note**
>
> This is different from history upload. When uploading history,running-config and startup-config will also be uploaded.

Click [OK] to start uploading.

6.9.7 Configure SNMP trap sending

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

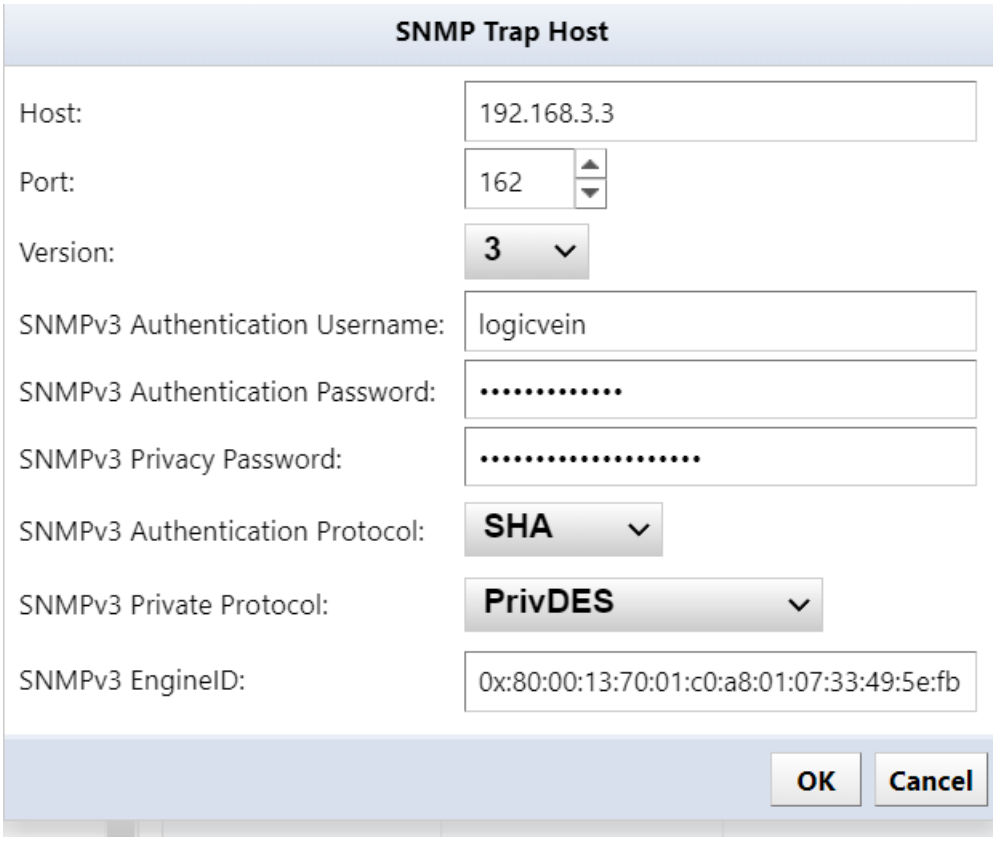
1. Click Settings on the Global Menu.
2. Click [SNMP Trap Settings] and select the events to be sent.



Event Trigger	SNMP Trap Action
Device configuration changes are detected	Sends an SNMP trap when it detects that the device configuration has changed since the last backup.
Devices are added and deleted	Sends SNMP traps when devices are added/removed.
A backup failure	Sends an SNMP trap if configuration backup fails.

Event Trigger	SNMP Trap Action
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 the  button.
4. Enter the trap destination information and click [OK].

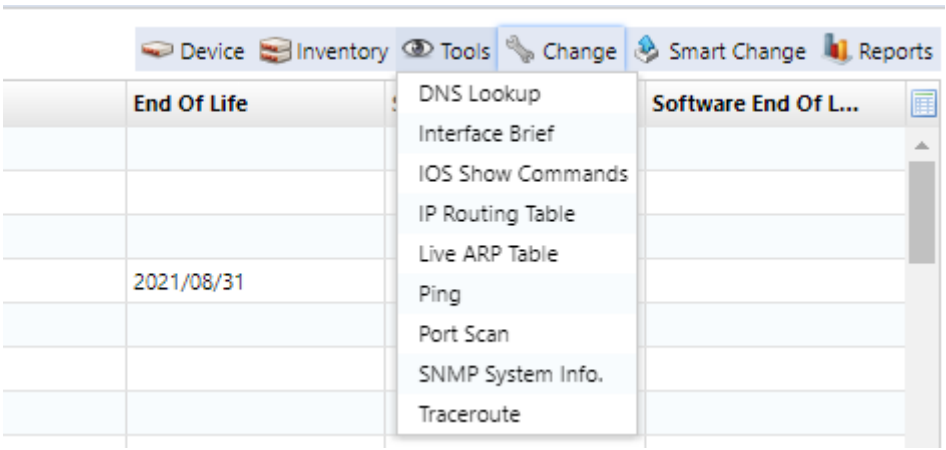


Items	Explanation
Host	Enter the IP address or host name of the trap destination.
Port	Specify the trap destination port. (Initial value: `162`)
Version	Specify the trap version from the following: `2c`, `3`
SNMP Community String	Enter the trap community name. (When selecting 1 or 2c at Version)
(SNMPv3) Authentication Username	Enter the username used for user authentication.
(SNMPv3) Privacy Password	Enter your encryption password.
(SNMPv3) Authentication Protocol	Specify the authentication protocol from the following: `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
(SNMPv3) Private Protocol	Specify the encryption protocol from the following:

Items	Explanation
	`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)

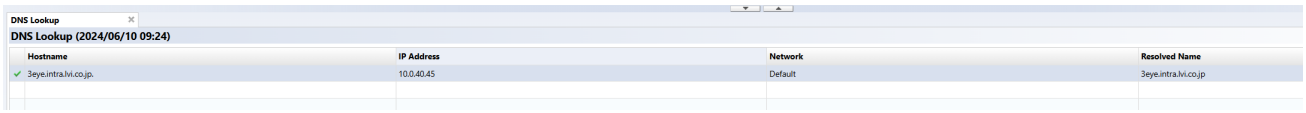
6.10 Viewing tools

The Viewing Tools menu allows you to determine the real-time status of the selected device. It is also possible to export all detected results as a CSV file. When using the viewing tool, a dedicated tab will be opened in the status panel, so exporting can be done using the button located in the top right corner.



6.10.1 DNS lookup

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

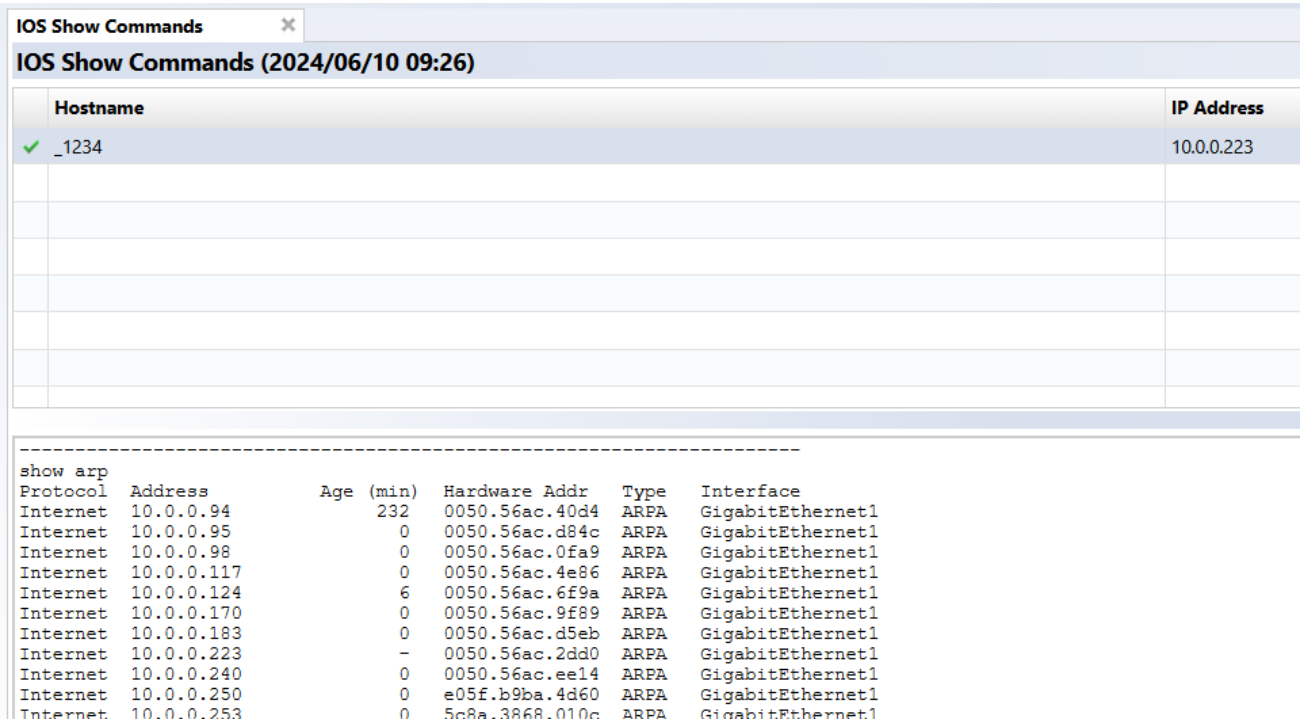


6.10.2 IOS Show commands

The IOS Show Commands window displays the results of the device's "IOS Show commands" request. Select the "show" command you want to run first from the list, and click [Execution] to issue the command.

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

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



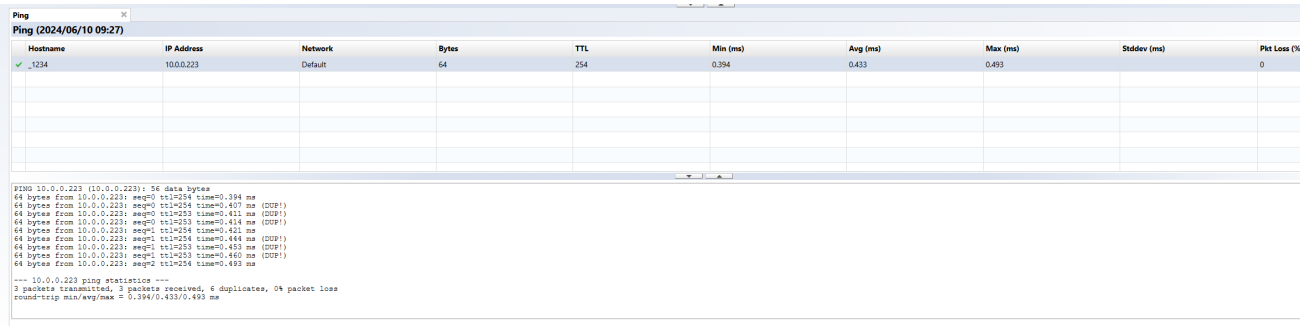
6.10.3 IP Routing table

The IP Routing table window displays the device's routing information.

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

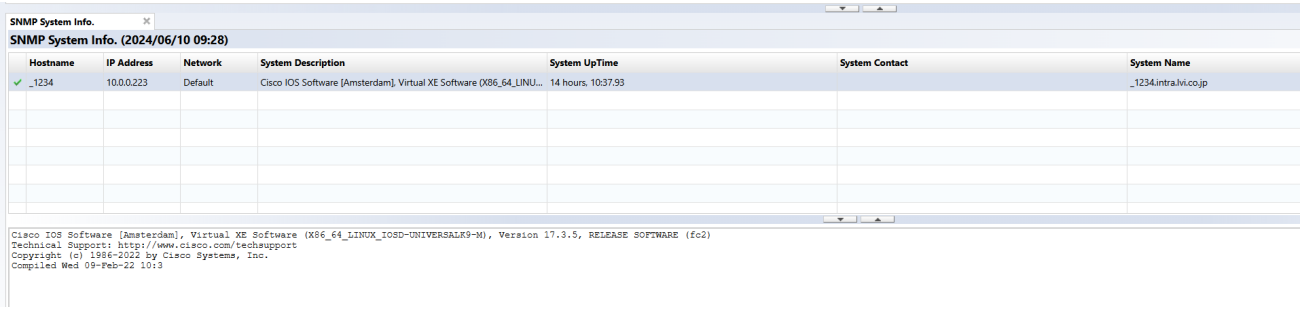
6.10.4 Ping

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



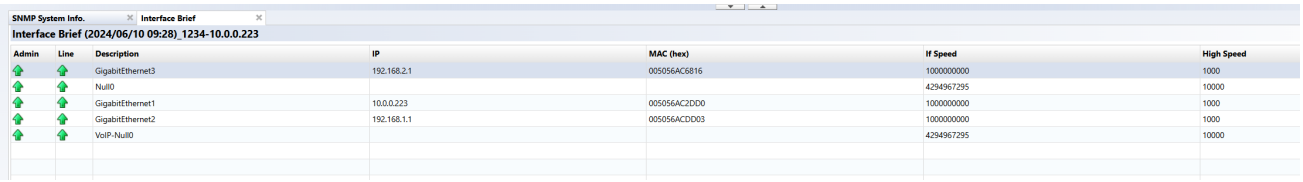
6.10.5 SNMP System Info

The SNMP System Info window displays the device's SNMP system information.



6.10.6 Interface Brief

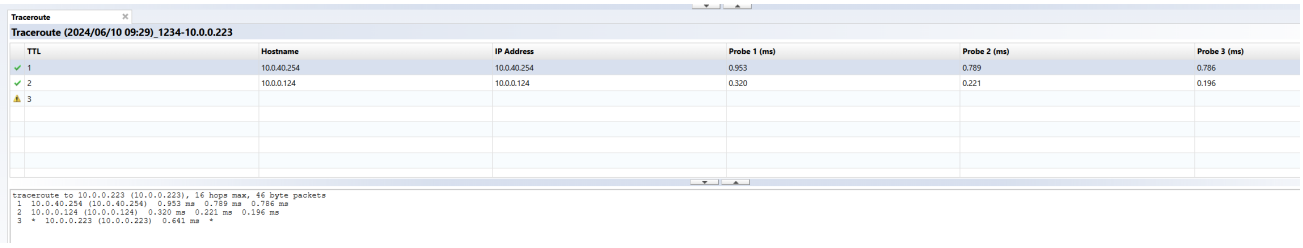
The Interface Brief window displays detailed information such as the open/close status of each interface of the device, device IP address, etc.



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

6.10.7 Traceroute

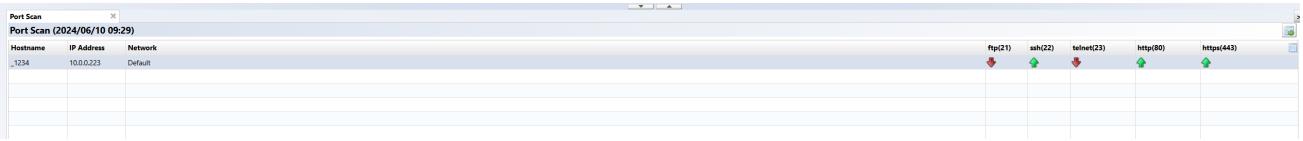
From the Traceroute window, you can perform a traceroute to the device and display the response.



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

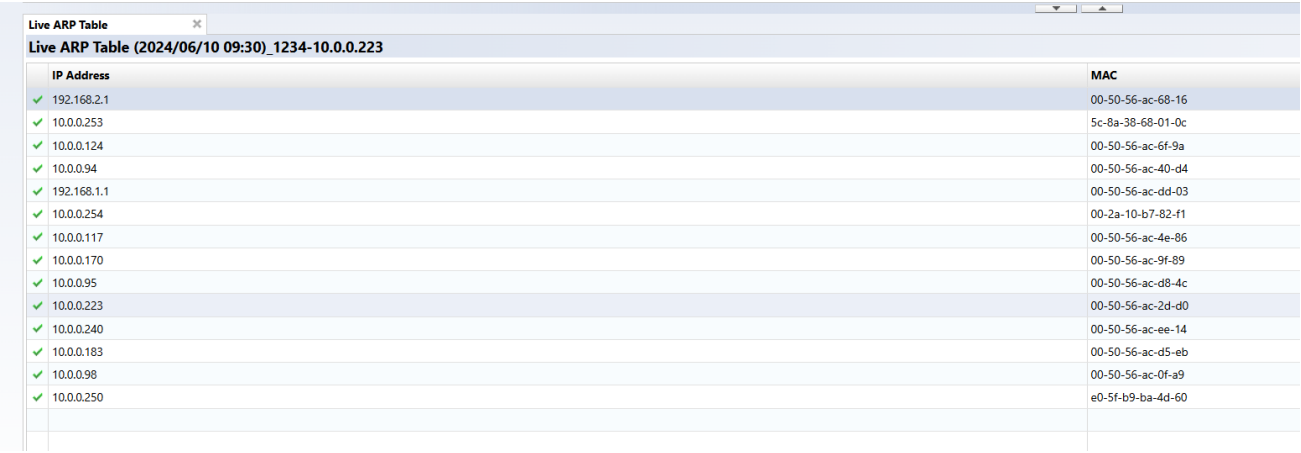
6.10.8 Port Scan

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



6.10.9 Live ARP Table

The Live ARP Table window displays the live status of the ARP table.



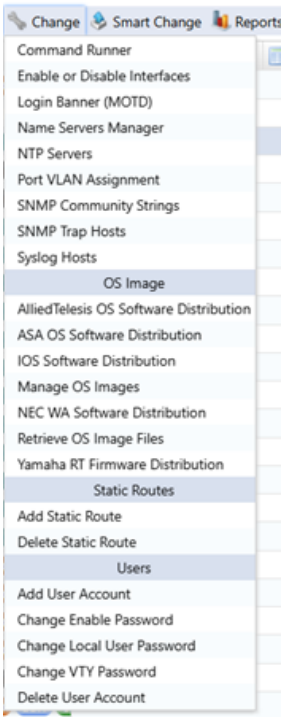
Note

This function cannot be executed when multiple devices are selected.

6.11 Change tools

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

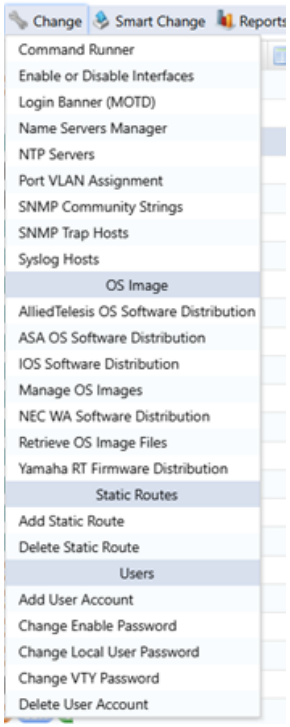
In this section, we will explain each function in the [Change] submenu.



6.12 Change Tools

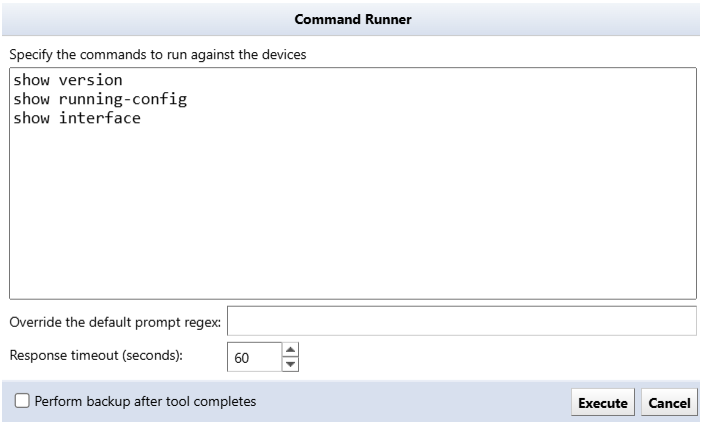
The [Change] submenu collects operations related to modifying the configuration of the selected device.

In this section, we will explain each function in the [Change] submenu.



6.12.1 Command Runner

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



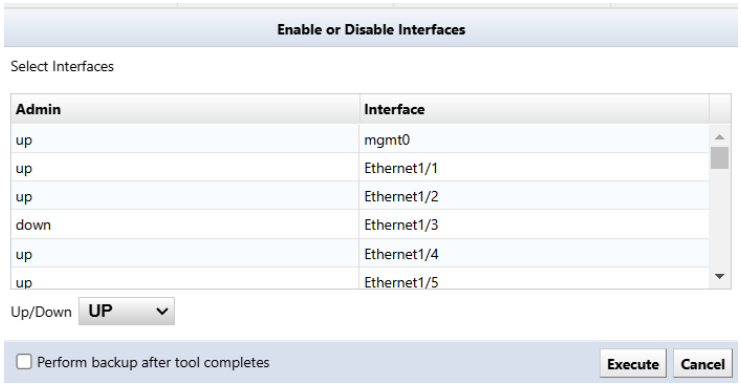
The [Override the default prompt regex] field specifies a regulars expression to match a particular type of prompt. The prompts to be matched are like PS1 variables in shell scripts. This field required if a command responds with an unusual prompt.

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

6.12.2 Enable or Disable Interfaces

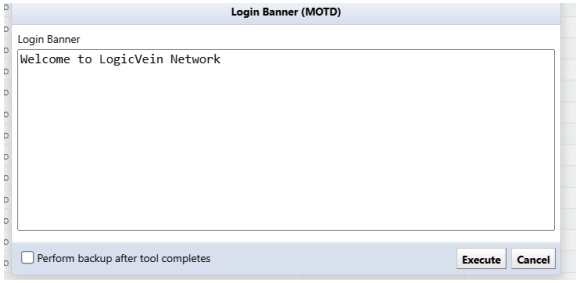
Change the Admin Status of the device interface. Please note that this function cannot be executed when multiple devices are selected.

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



6.12.3 Login Banner (MOTD)

Set the device login banner.

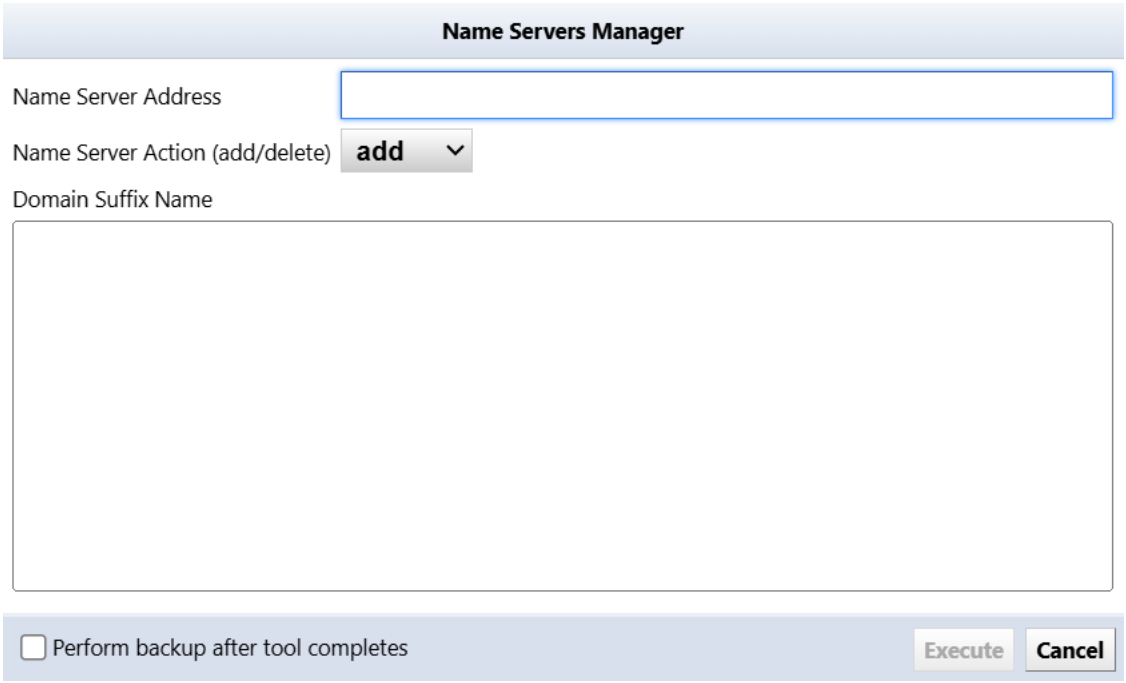


6.12.4 Name Servers Manager

Add or delete a “Name Server Address”.

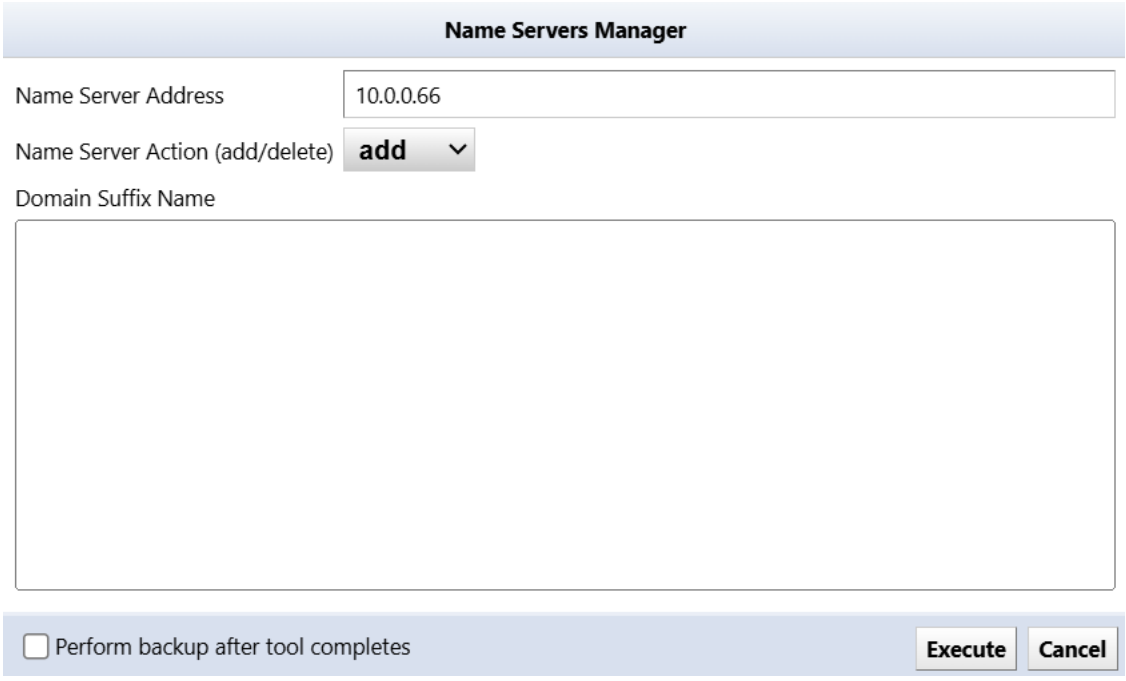
Add an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.



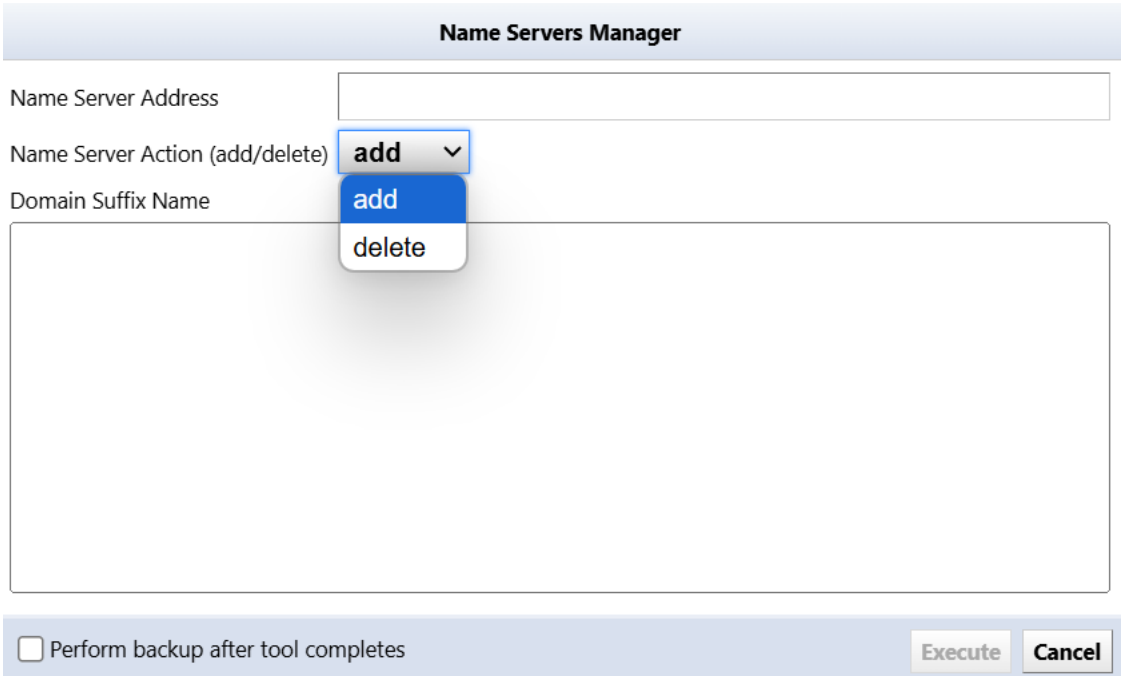
The [Execute] button, will become clickable.

3. Click [Execute].



Delete an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.
3. Change the “Name Server Action” to “delete”.

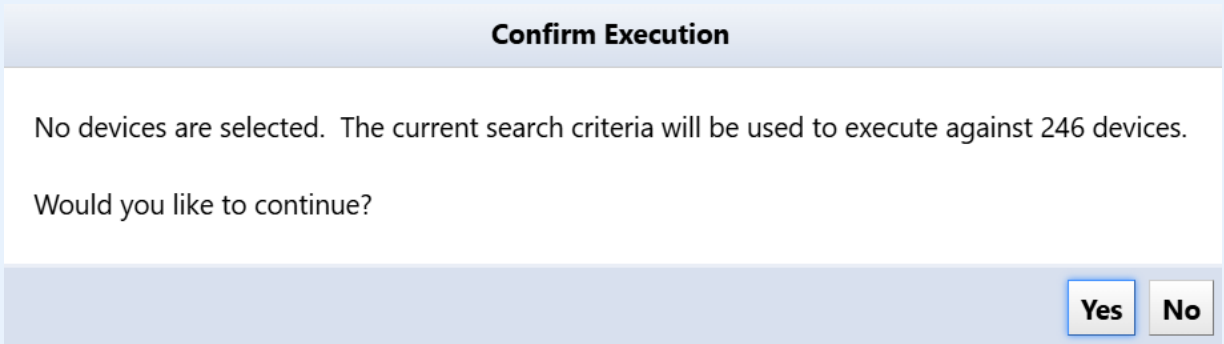


The [Execute] button, will become clickable.

4. Click [Execute].

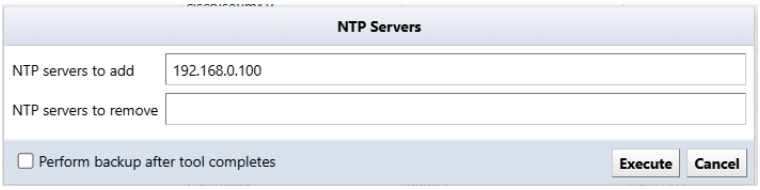
Note

If no IP Address is selected, clicking the [Name Server Manager] tool will act on all addresses in the Inventory window list.



6.12.5 NTP Servers

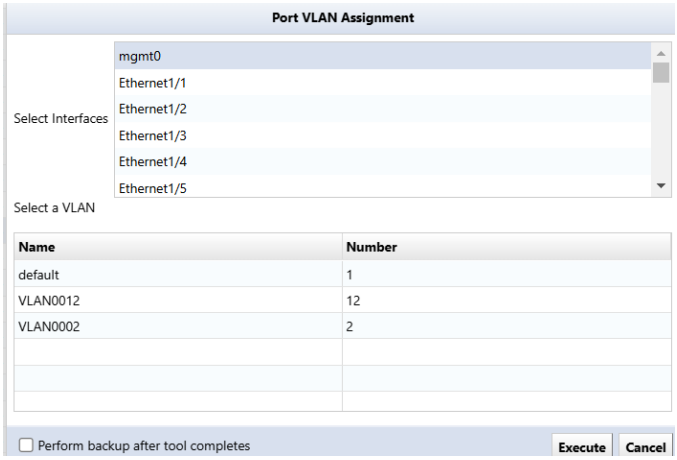
Add/remove NTP servers to your device.



6.12.6 Port VLAN Assignment

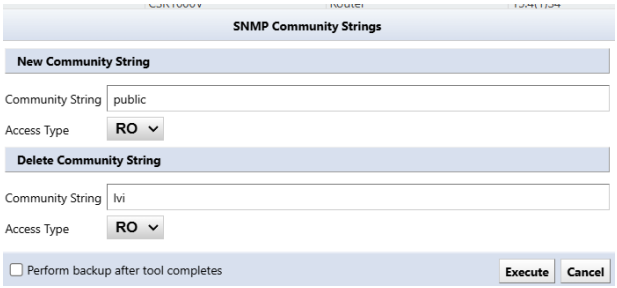
Perform VLAN port settings for the device's access port. Please note that this function cannot be executed when multiple devices are selected.

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.



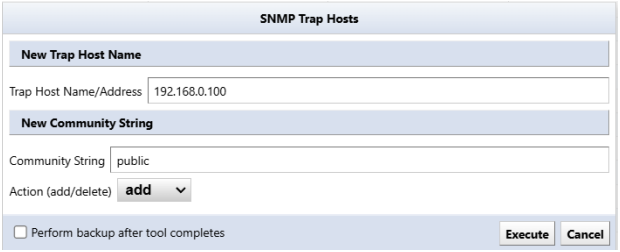
6.12.7 SNMP community string

Add/delete SNMP communities to/from devices.



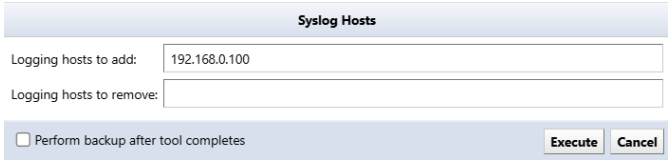
6.12.8 SNMP Trap Hosts

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



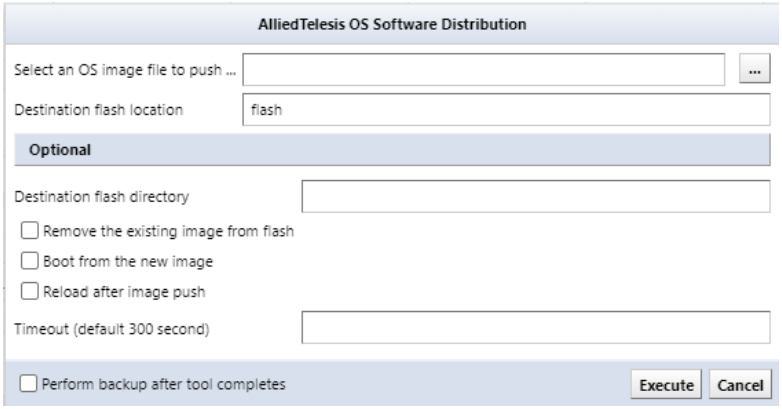
6.12.9 Syslog Hosts

Add/delete Syslog hosts to/from the device.



6.12.10 AlliedTelesis OS software distribution

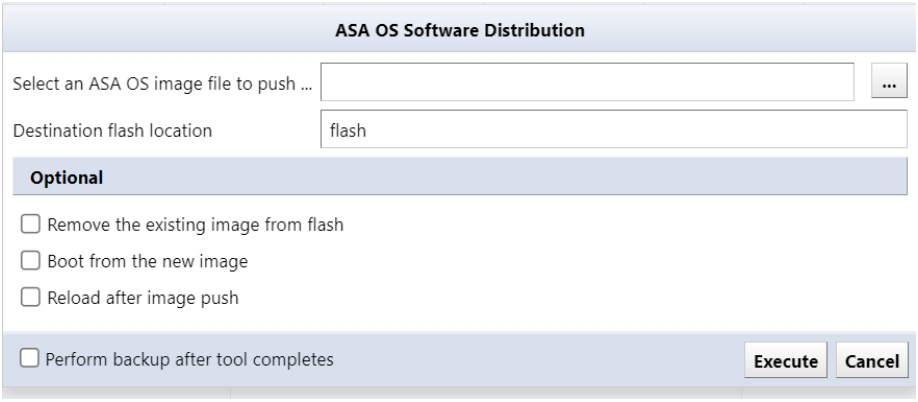
You can remotely distribute the OS to AlliedTelesis devices. To use this function, you must save the OS in advance.



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

6.12.11 ASA OS software distribution

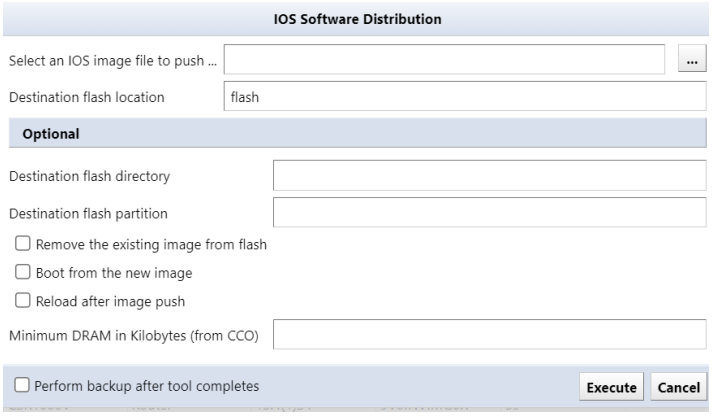
You can remotely distribute the OS to Cisco ASA devices. To use this function, you must save the OS in advance.



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

6.12.12 IOS software distribution

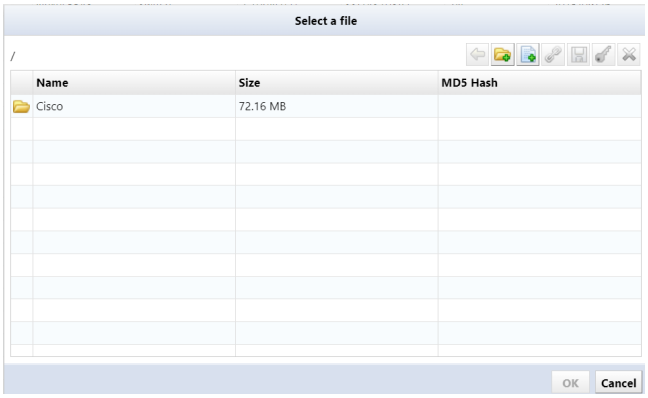
You can remotely distribute IOS to Cisco IOS devices. To use this feature, you must save the IOS in advance.



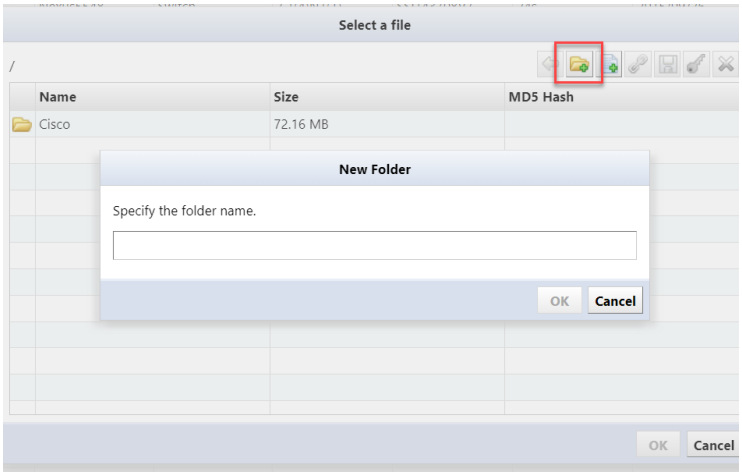
Setting	Explanation
Select an IOS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device. Depending on the model, flash/usbflash0/nvram - The content that can be specified differs.
Destination flash directory	A directory within the destination drive partition. If the directory does not exist, a directory with the specified name will be automatically created.
Destination flash partition	Partition of the destination drive. The command will fail if the specified partition does not exist.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time
Minimum DRAM in Kilobytes (from CCO)	Please check the DRAM capacity of the image to be submitted and enter it. Check if there is enough free space on the device before deploying the image

6.12.13 Manage OS image

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



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

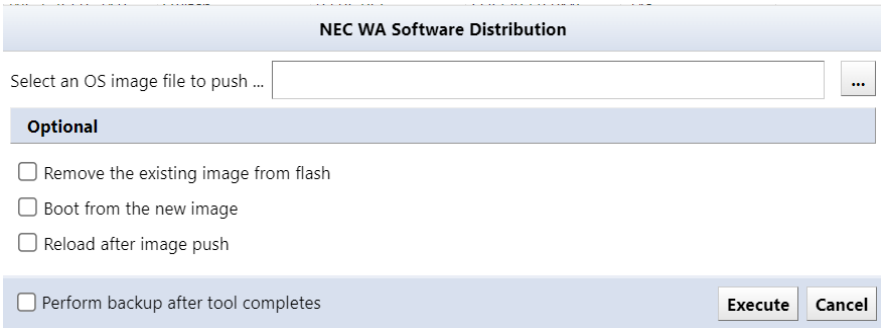


Once the OS image is added to the list, click the [OK] button.

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.

6.12.14 NEC WA software distribution

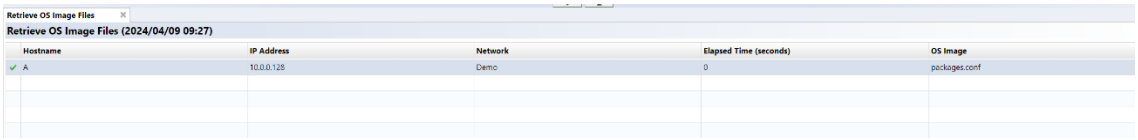
NEC WA software can be distributed remotely to the OS. To use this function, you must save the WA software in advance.



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

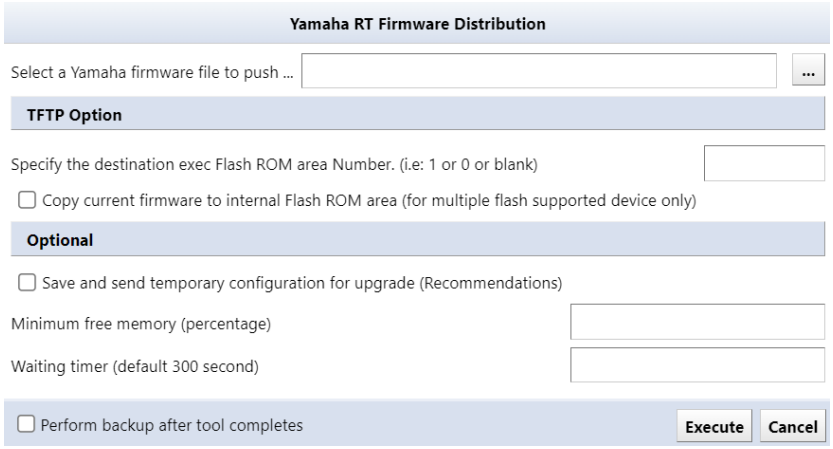
6.12.15 Retrieve OS image file

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



6.12.16 Yamaha RT Firmware Distribution

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



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

Note

*1 Since Rev.14.01.14, firmware will be backed up in these cases.

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

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

*2. The following command will be executed:

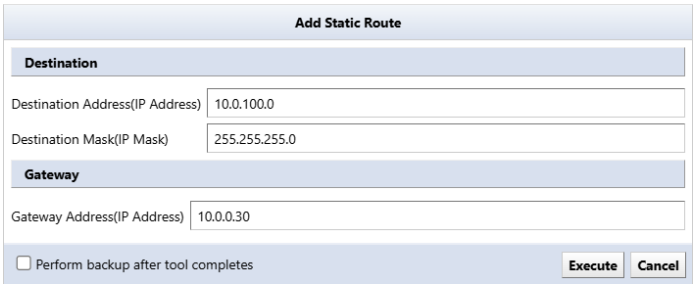
```
login timer [timer]
show config | grep "tftp host"
tftp host [NetLD IP]
```

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

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

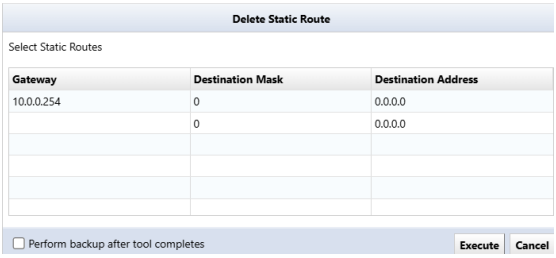
6.12.17 Add Static Route

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



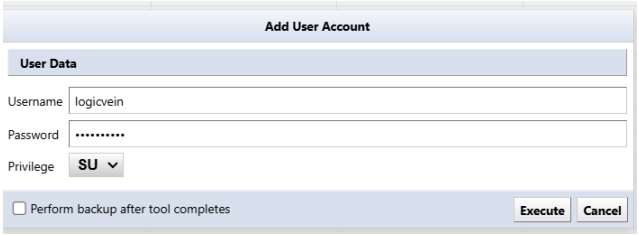
6.12.18 Delete Static Route

Select and delete an existing static route configuration.



6.12.19 Add User Account

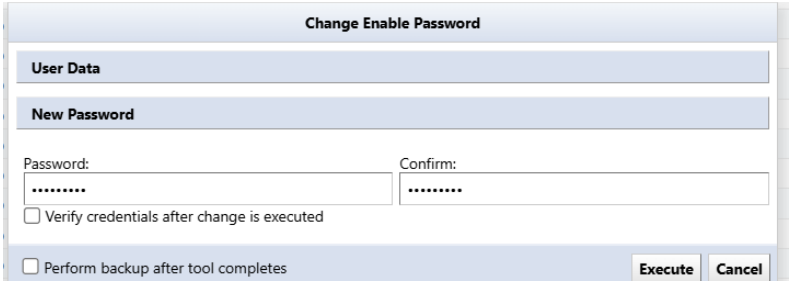
Add a new user account to your device. Please note that this function cannot be executed when multiple devices are selected.



6.12.20 Change Enable Password

Change the Enable Password or Enable Secret settings for your device:

- If Enable Password is set, Enable Password is changed.
- If Enable Secret is set, Enable Secret is changed.
- If both are set, Enable Secret will be changed.



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.

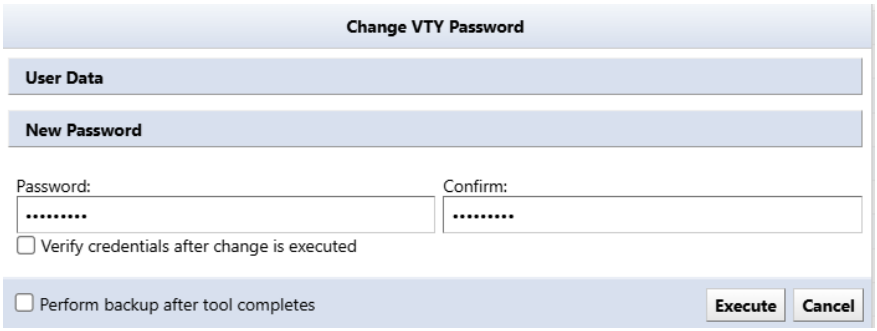
If static credentials are being used, by checking “Confirm credentials after change”, the credentials will be automatically changed, and you will be checked to see if you can log in with thempassword you set.

6.12.21 Changing Local User Password

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

6.12.22 Change VTY Password

Change the device's VTY Password settings.

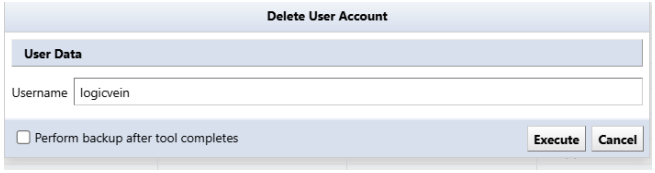


Just as with changing Enable Password by checking "Confirm credentials after change", the credentials will be automatically changed.

Test your new password after changing.

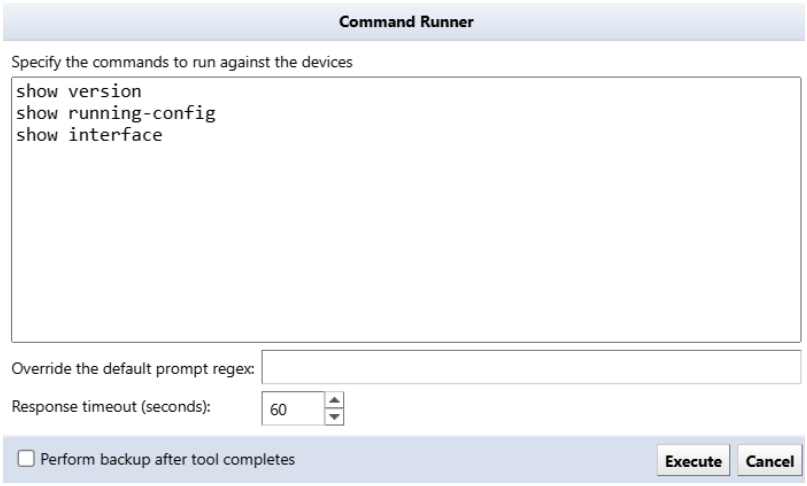
6.12.23 Delete User Account

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



6.12.24 Command Runner

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



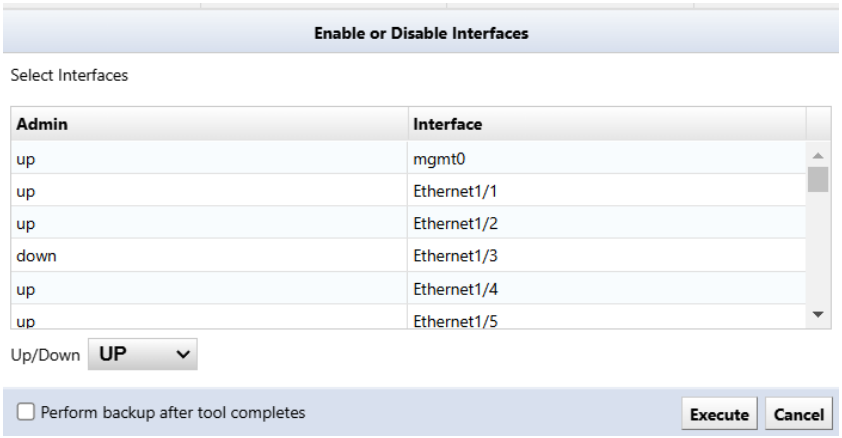
The [Override the default prompt regex] field specifies a regular expression to match a particular type of prompt. The prompts to be matched are like PS1 variables in shell scripts. This field required if a command responds with an unusual prompt.

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

6.12.25 Enable or Disable Interfaces

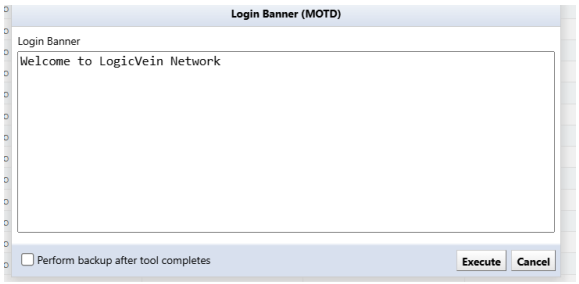
Change the Admin Status of the device interface. Please note that this function cannot be executed when multiple devices are selected.

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.



6.12.26 Login Banner (MOTD)

Set the device login banner.

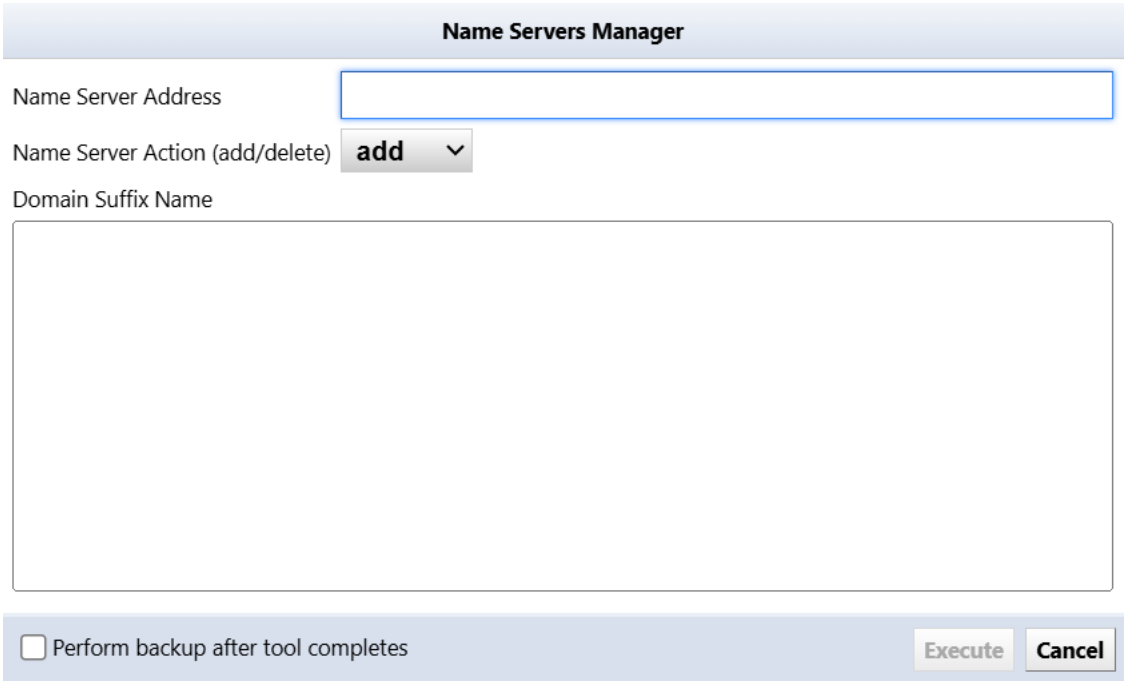


6.12.27 Name Servers Manager

Add or delete a “Name Server Address”.

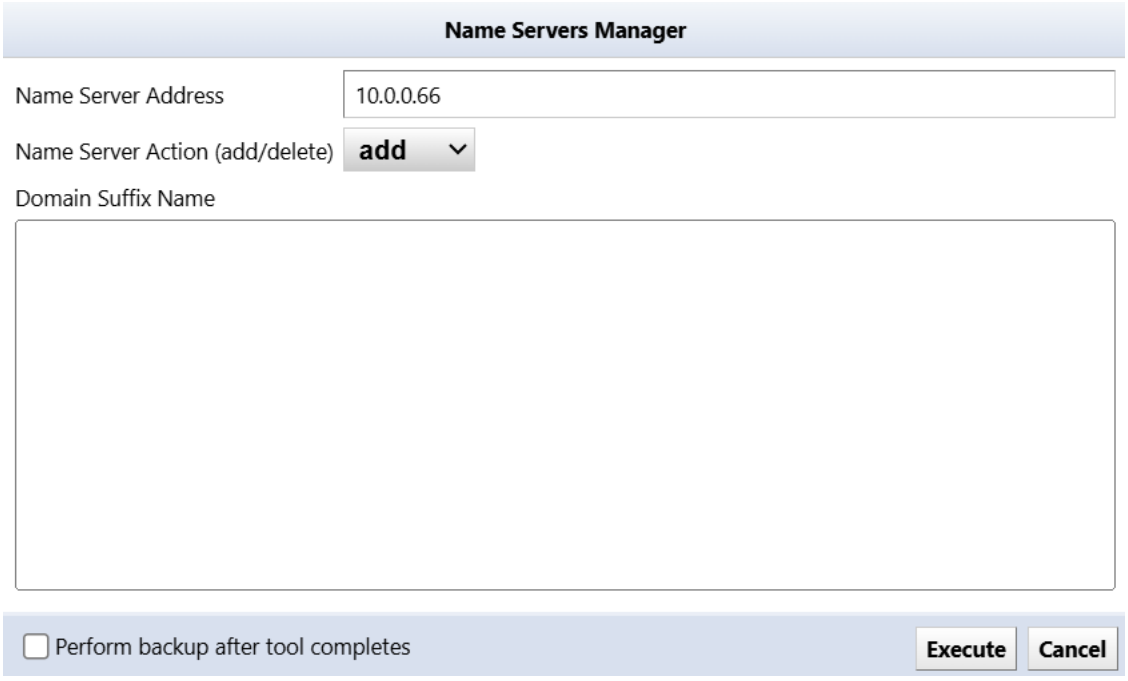
Add an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.



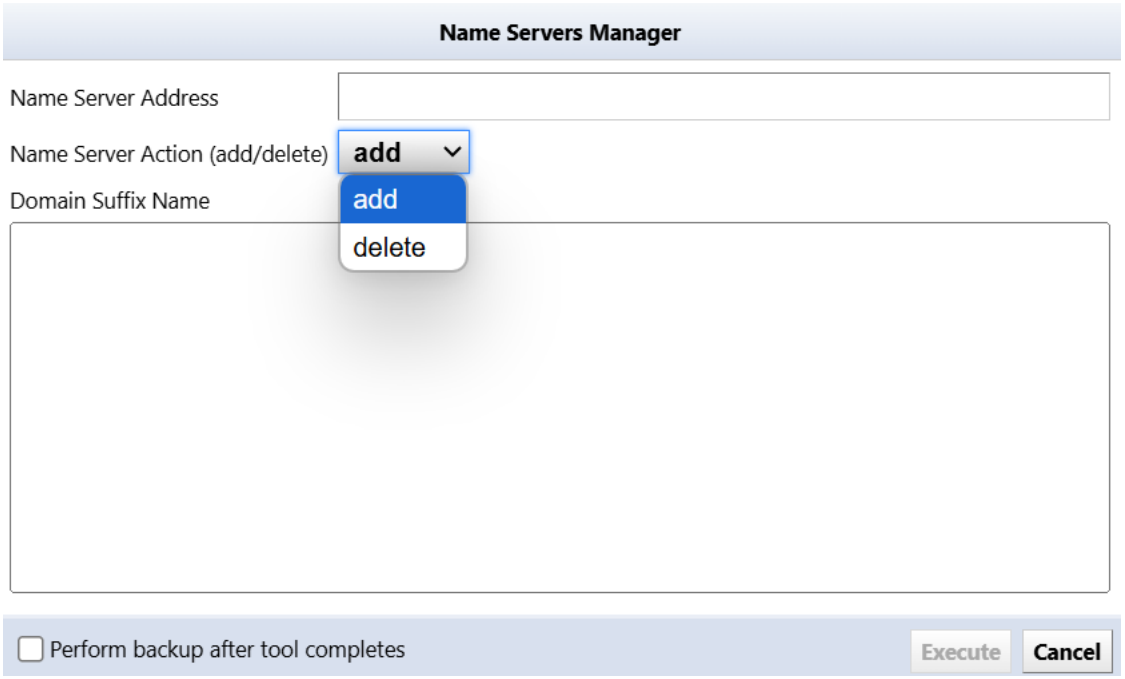
The [Execute] button, will become clickable.

3. Click [Execute].



Delete an address

1. Click [Change] > [Name Server Manager].
2. Enter the IP address in the “Name Server Address” field.
3. Change the “Name Server Action” to “delete”.

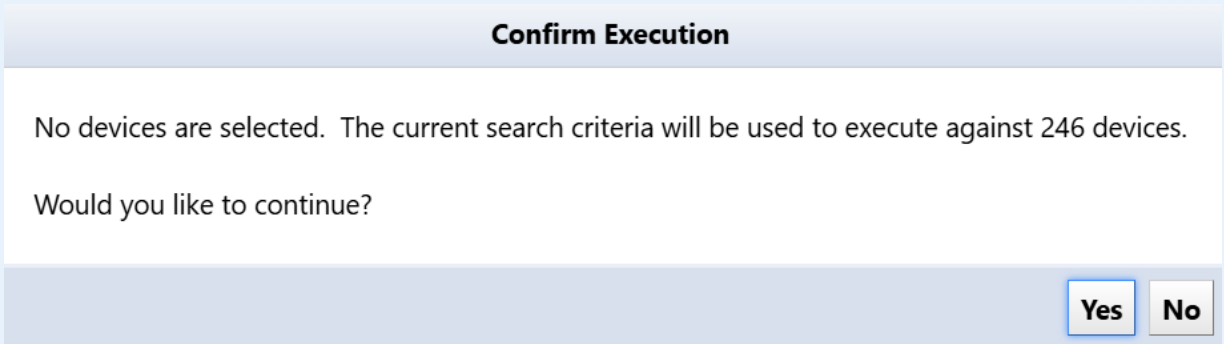


The [Execute] button, will become clickable.

4. Click [Execute].

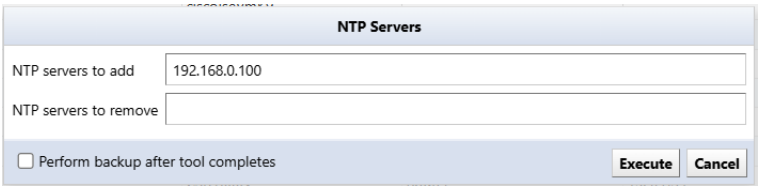
Note

If no IP Address is selected, clicking the [Name Server Manager] tool will act on all addresses in the Inventory window list.



6.12.28 NTP Servers

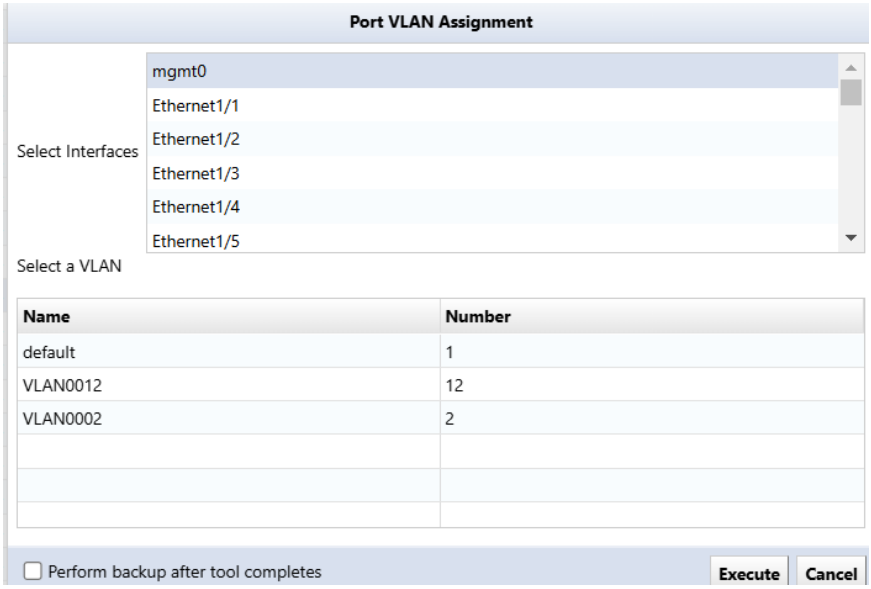
Add/remove NTP servers to your device.



6.12.29 Port VLAN Assignment

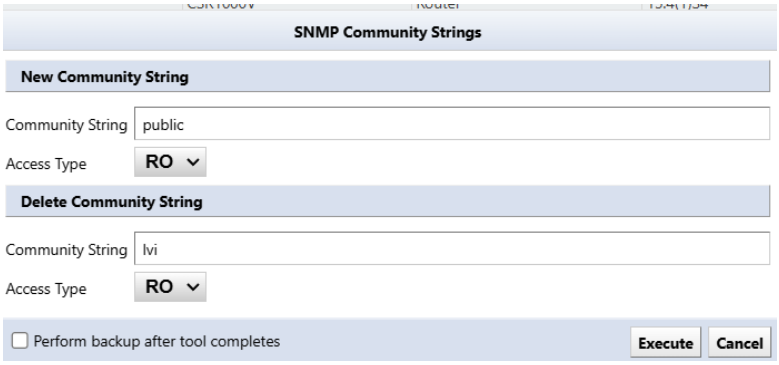
Perform VLAN port settings for the device's access port. Please note that this function cannot be executed when multiple devices are selected.

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.



6.12.30 SNMP Community Strings

Add/delete SNMP communities to/from devices.



6.12.31 SNMP Trap Hosts

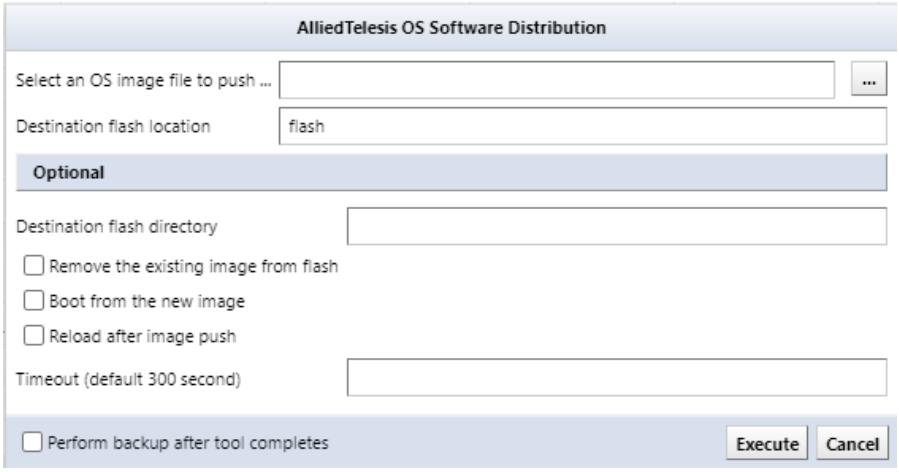
Add/delete SNMP trap host settings for devices. It is effective for batch setting of new NMS installations.

6.12.32 Syslog Hosts

Add/delete Syslog hosts to/from the device.

6.12.33 AlliedTelesis OS software distribution

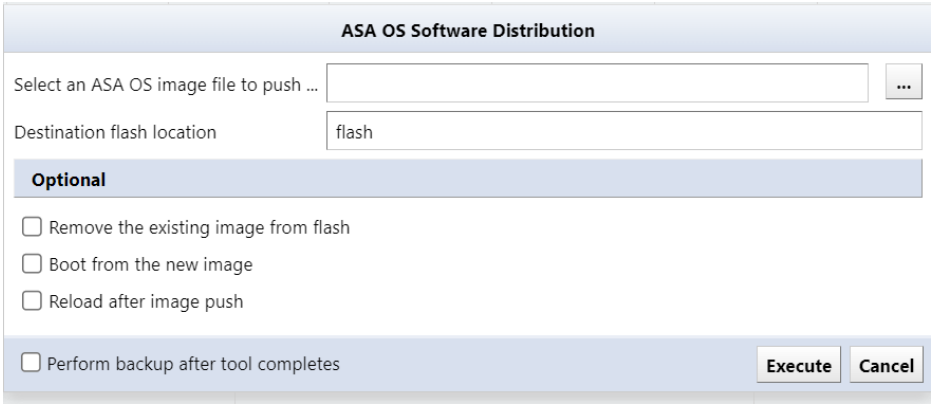
You can remotely distribute the OS to AlliedTelesis devices. To use this function, you must save the OS in advance.



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

6.12.34 ASA OS software distribution

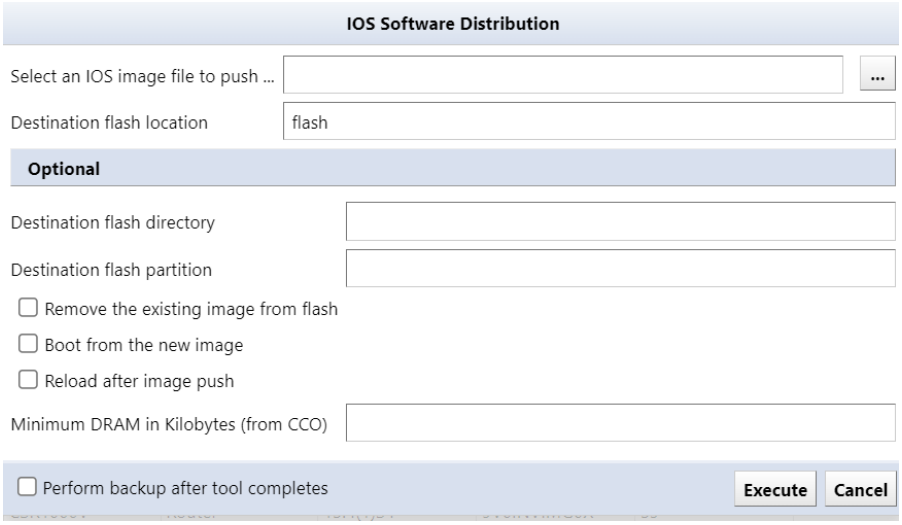
You can remotely distribute the OS to Cisco ASA devices. To use this function, you must save the OS in advance.



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

6.12.35 IOS software distribution

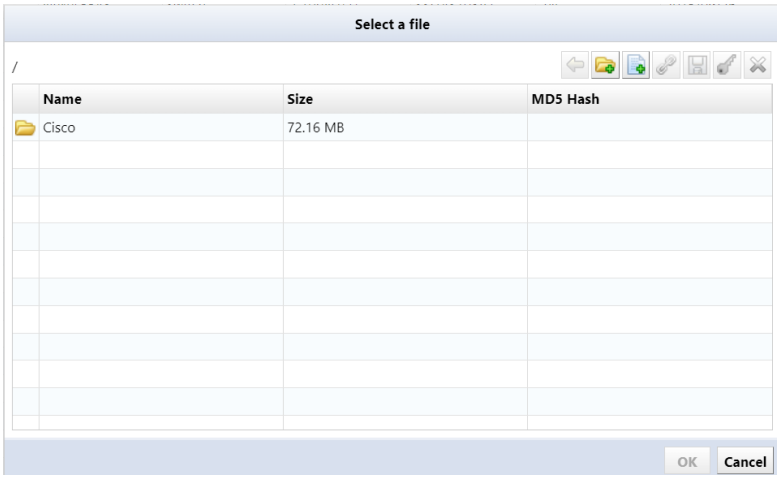
You can remotely distribute IOS to Cisco IOS devices. To use this feature, you must save the IOS in advance.



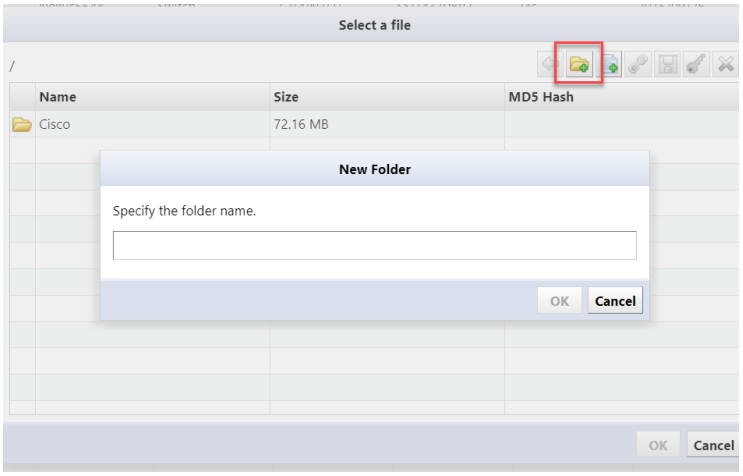
Setting	Explanation
Select an IOS image file to push	When you press the […] button on the right side, a window will appear where you can browse the registered OS images, so select the image you want to upload.
Destination flash location	Specifies the storage drive provided by the device. Depending on the model, flash/usbflash0/nvram - The content that can be specified differs.
Destination flash directory	A directory within the destination drive partition. If the directory does not exist, a directory with the specified name will be automatically created.
Destination flash partition	Partition of the destination drive. The command will fail if the specified partition does not exist.
Remove the existing images from flash	After image transfer, remove the existing image file.
Boot from the new image	After image transfer, reload the system.
Reload after image push	Timeout setting for setting transferring time
Minimum DRAM in Kilobytes (from CCO)	Please check the DRAM capacity of the image to be submitted and enter it. Check if there is enough free space on the device before deploying the image

6.12.36 Manage OS Images

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



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

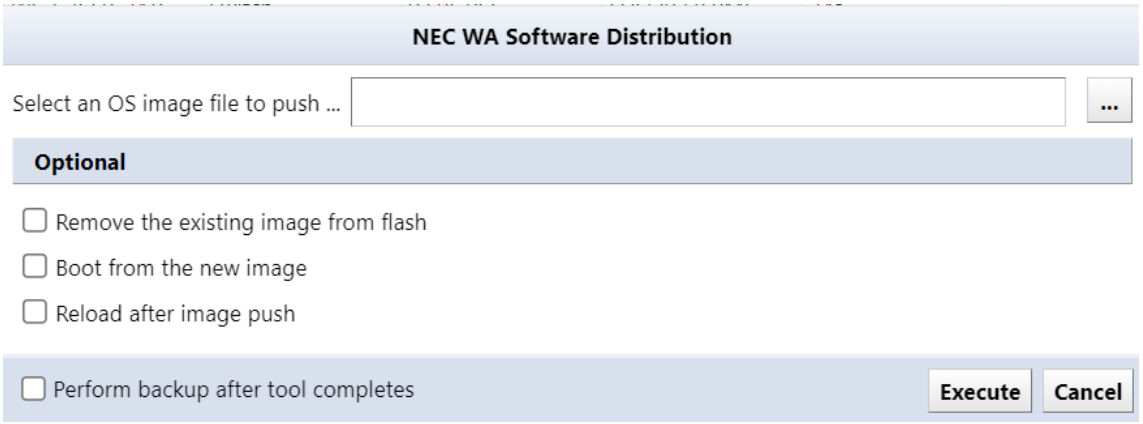


Once the OS image is added to the list, click the [OK] button.

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

6.12.37 NEC WA software distribution

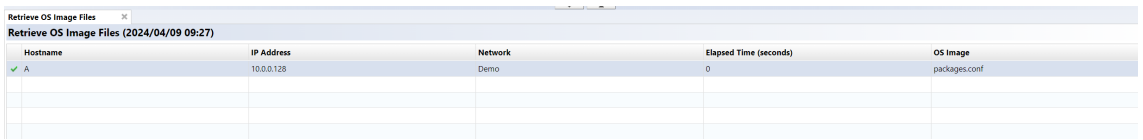
NEC WA software can be distributed remotely to the OS. To use this function, you must save the WA software in advance.



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

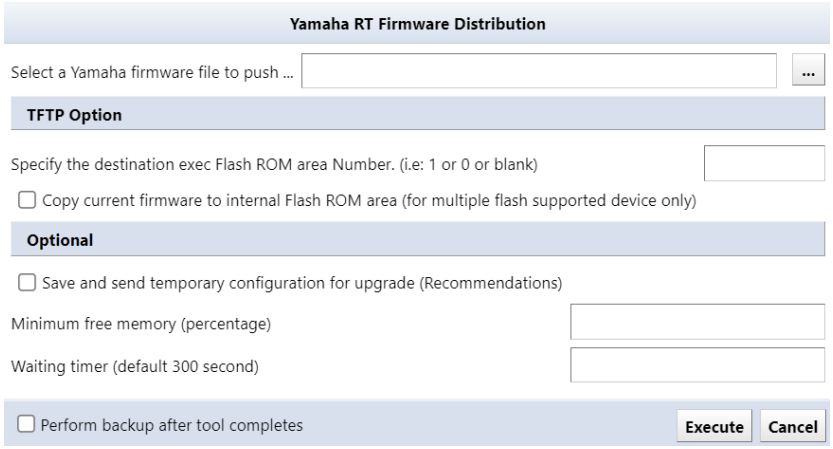
6.12.38 Retrieve OS image files

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



6.12.39 Yamaha RT Firmware Distribution

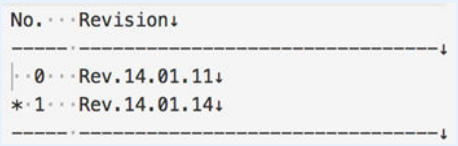
Yamaha RT software can be distributed remotely to the OS. To use this function, you must save the Yamaha RT software in advance.



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

Note

1. *Since Rev.14.01.14, firmware will be backed up in these cases.

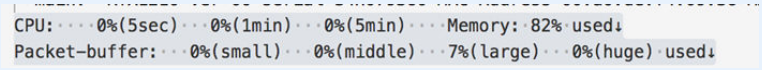


If this check is performed on a model that does not support multiple firmware, the firmware upgrade will be aborted. The upgrade will also be canceled if the ROM number of the revision destination and the ROM number of the running firmware are the same.

2. *The following command will be executed:

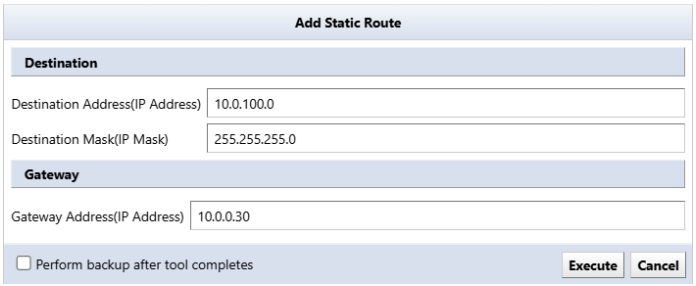
```
login timer [timer]
show config | grep "tftp host"
tftp host [NetLD IP]
```

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



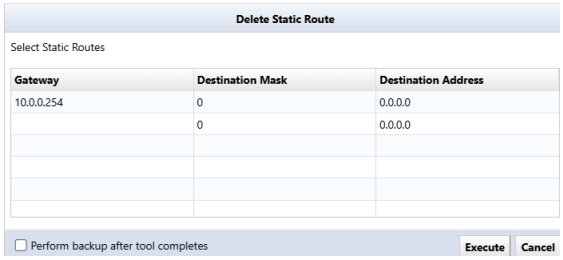
6.12.40 Add Static Route

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



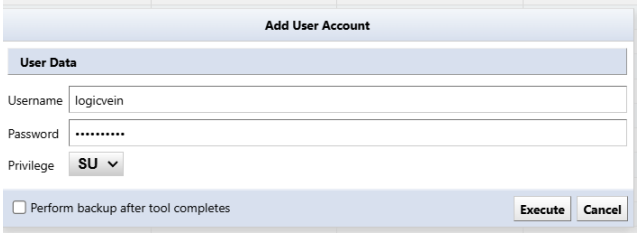
6.12.41 Delete Static Route

Select and delete an existing static route configuration.



6.12.42 Add User Account

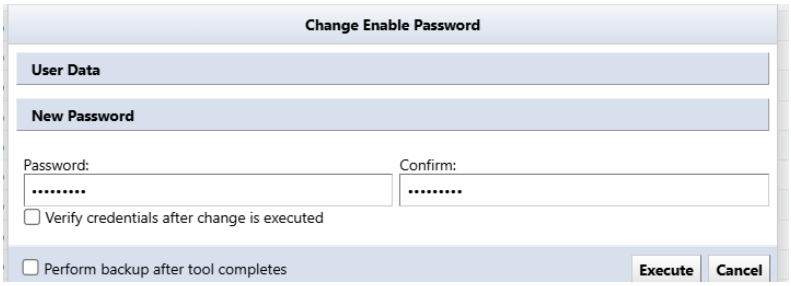
Add a new user account to your device. Please note that this function cannot be executed when multiple devices are selected.



6.12.43 Change Enable Password

Change the Enable Password or Enable Secret settings for your device:

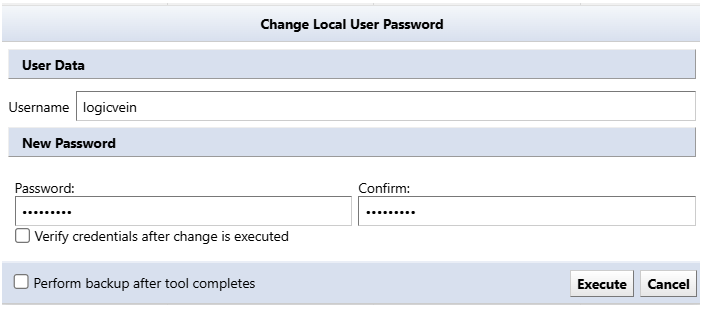
- If Enable Password is set, Enable Password is changed.
- If Enable Secret is set, Enable Secret is changed.
- If both are set, Enable Secret will be changed.



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

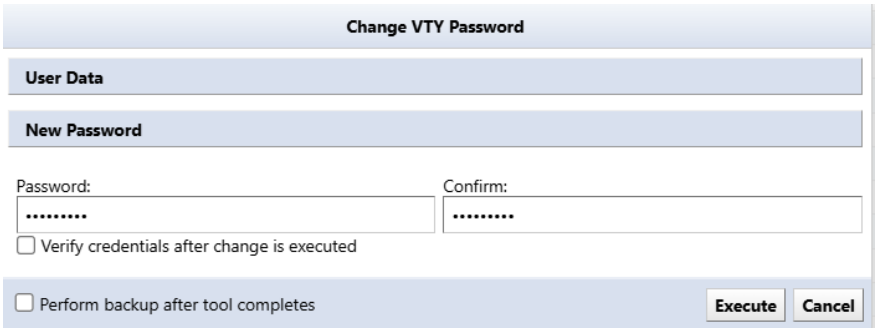
6.12.44 Changing Local User Password

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



6.12.45 Change VTY Password

Change the device's VTY Password settings.

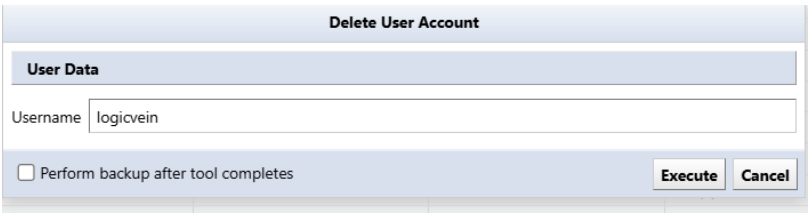


Just as with changing Enable Password by checking "Confirm credentials after change", the credentials will be automatically changed.

Test your new password after changing.

6.12.46 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.



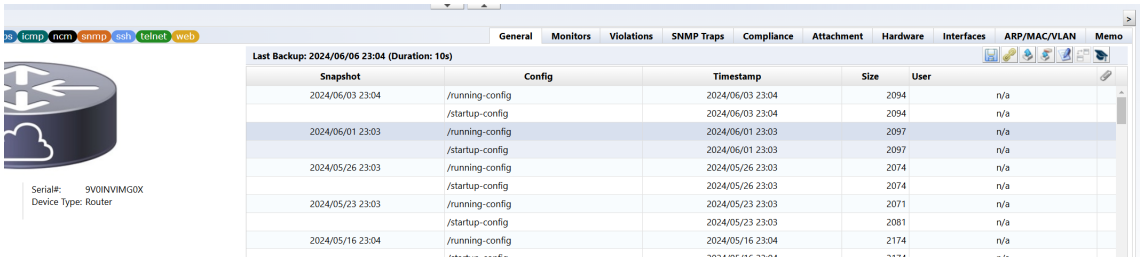
6.13 Change advisor

Change Advisor analyzes current/specified configurations and outputs any changes in configuration. It generates necessary CLI commands for configuration changes, allows command review/editing before execution, and logs execution results in job history.

Change Advisor is not available on some devices.

6.13.1 Change advisor setup

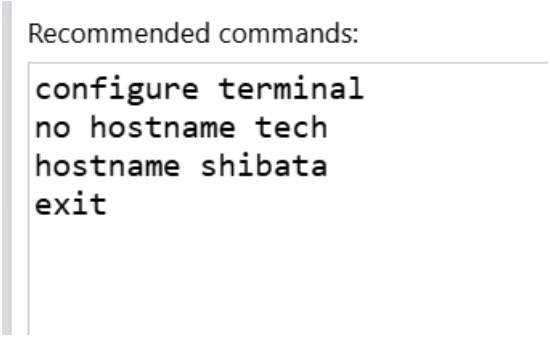
1. Doubleclick the device in the device view.
2. Select a configuration from configuration history or draft.
3. Click the  button.



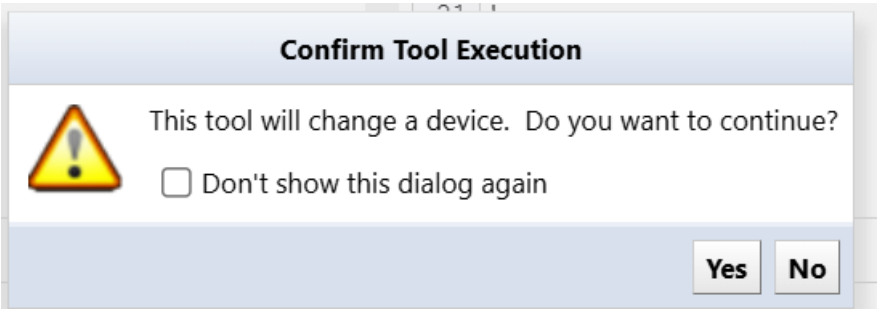
4. Change Advisor starts and presents commands in the lower panel.

6.13.2 Execute commands using change advisor

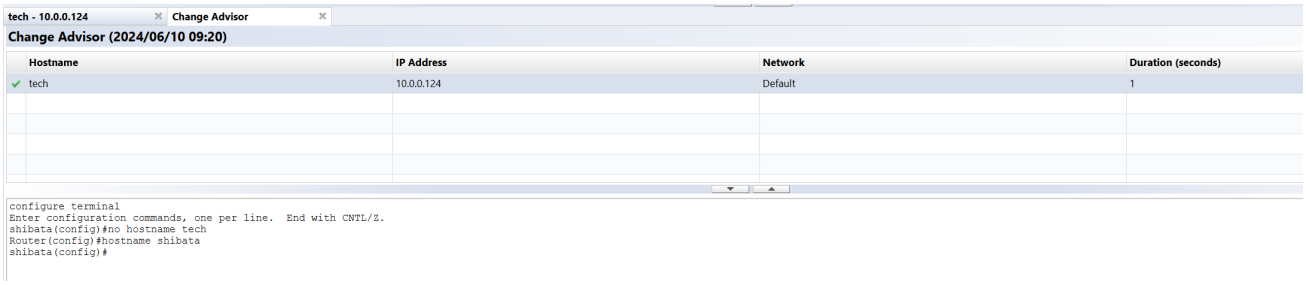
Commands output by Change Advisor can be executed on the device. Double check the command you want to run before executing the suggested command. If an incorrect command is antered, you can directly edit the output command.



To proceed, click [Run], then [Yes].



You can check the result after executing the command. Change Advisor execution results and history are also displayed in the job history.



Note

TFTP is the primary communication protocol for Configuration Restore and Draft Configuration upload. Therefore, restore and upload functionality is not available on devices that do not implement TFTP. However, the Change Advisor function can be used by most models as long as CLI login (telnet/SSH) is supported. Therefore, you can use the Change Advisor function as a substitute even in environments where uploading is not possible.

6.14 Smart change

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.

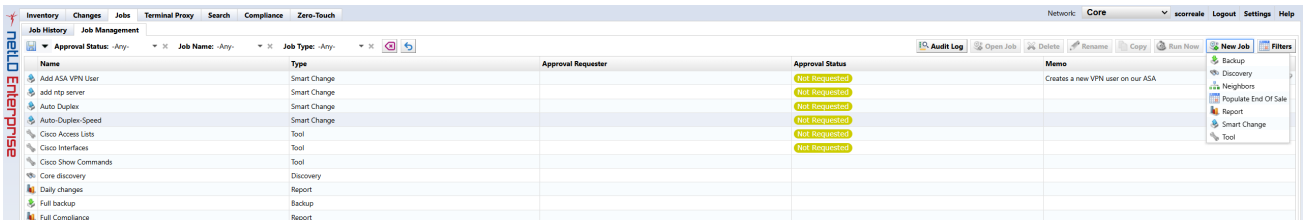
However, by using smart change, you can change passwords into variables and assign different values to each device, allowing you to set different passwords in one job.

6.14.1 Create a smart change job

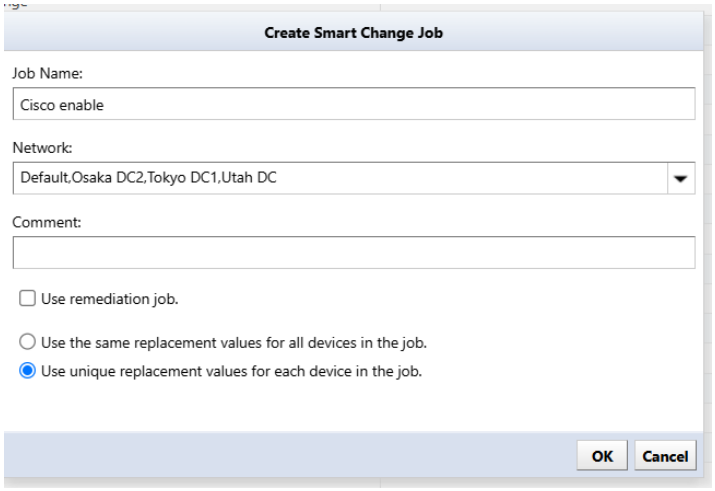
Smart change jobs can be created from the Jobs> Job Management tab. More information is available in the **Job management** section.

To create a job:

1. Click the [Job] > Job Management tabs, then click [New Job] > Smart Change.



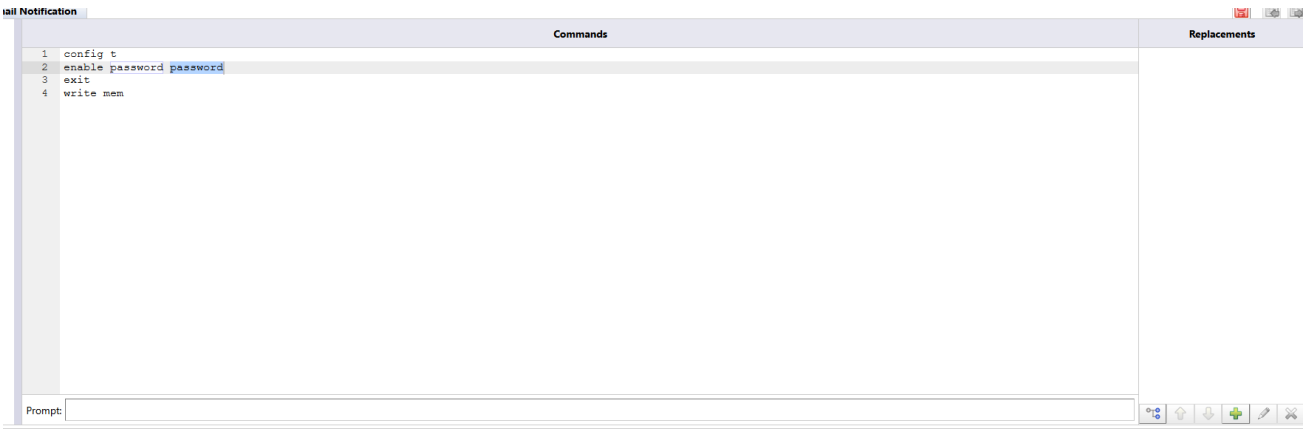
2. Enter the job name and comment, select the function, and click [OK].



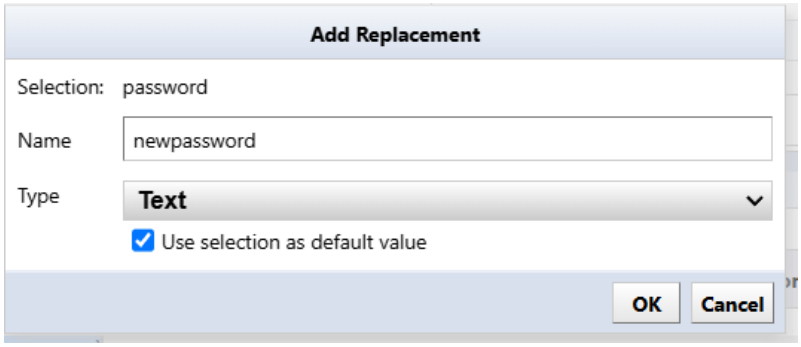
Item	Explanation
Job name	Enter the name of the smart change job.
Comment	Enter a comment (description) for the smart change job.
Use remediation job	Select whether to use smart change jobs as repair jobs. If selected, additionally select an adapter.
Use the same replacement values for all devices in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

3. In the template, enter the base command.

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

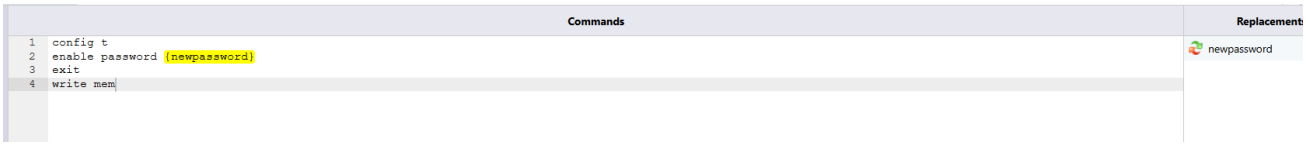


5. Enter a name for the alternative value and select a type.

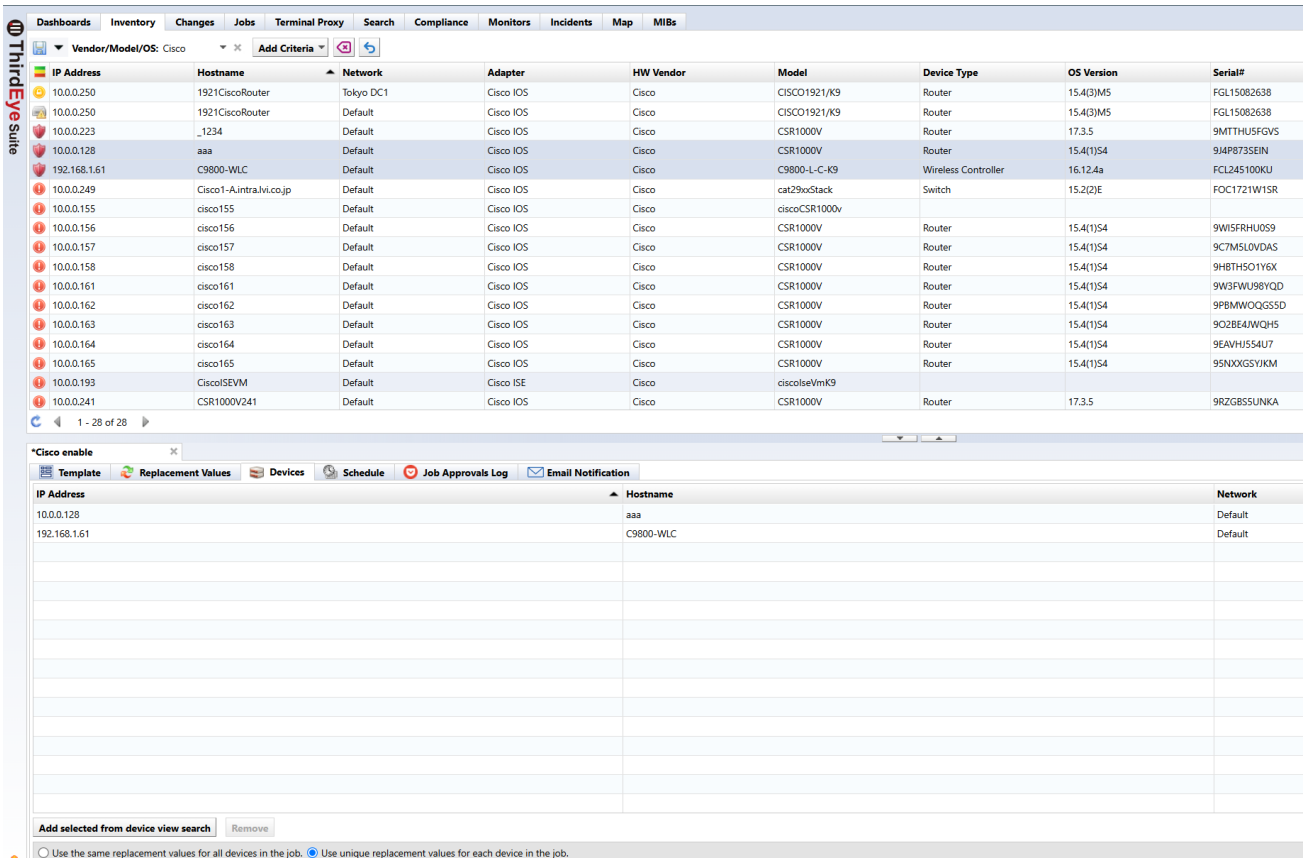


Item	Explanation
Text	Any text
IP address	IP address. If a value other than the correct IPv4 or IPv6 format is entered, an error will be reported.
Hostname	Hostname
IP address or hostname	IP address or host name
Choice	When entering an alternative value, you will be able to select it from a drop-down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

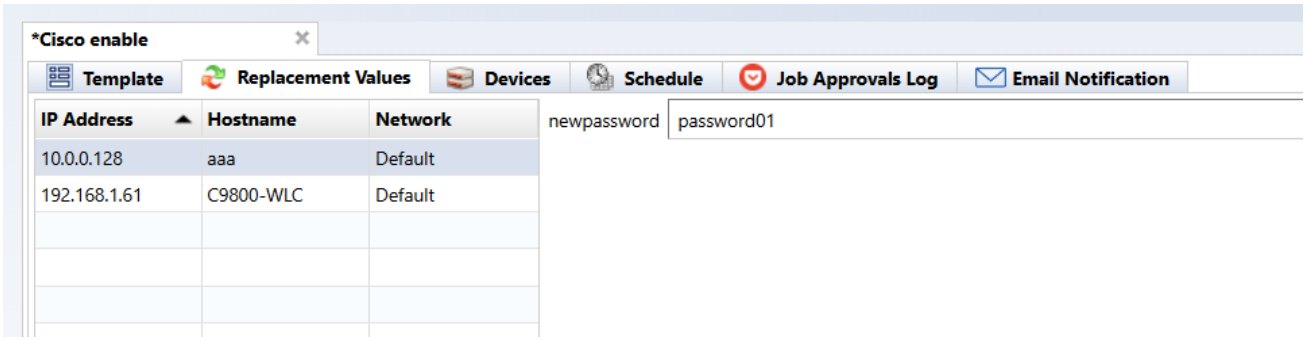
Variable parts are displayed in yellow.



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

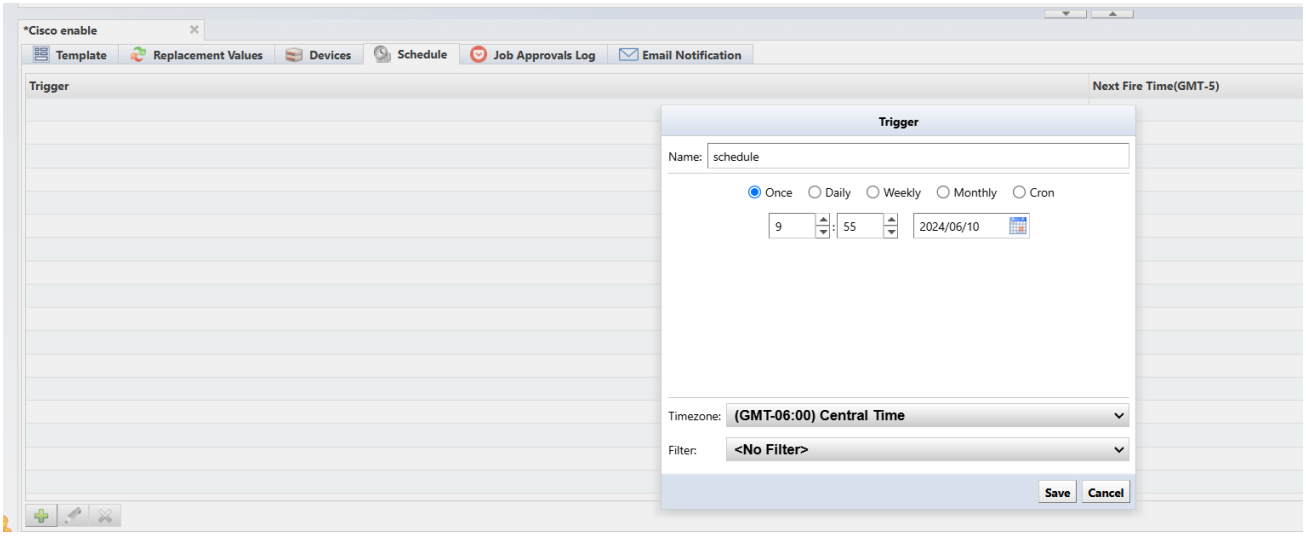


7. On the Replacement Values tab, enter the values.

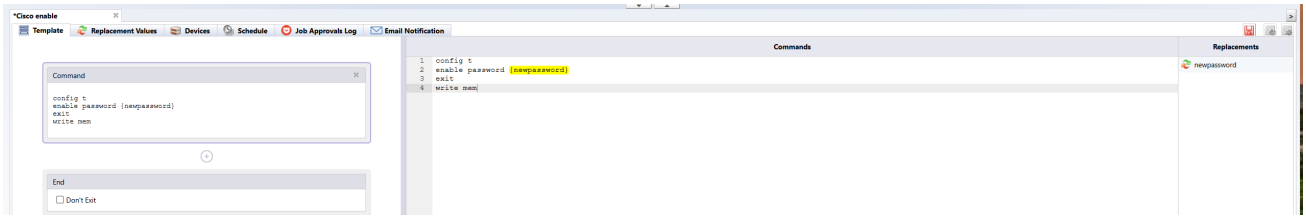


Alternative data can be can be imported/exported via Excel file using the (export) or (import) buttons.

8. Add triggers on the [Schedule] tab by clicking the the button in the lower lefthand corner of the window.

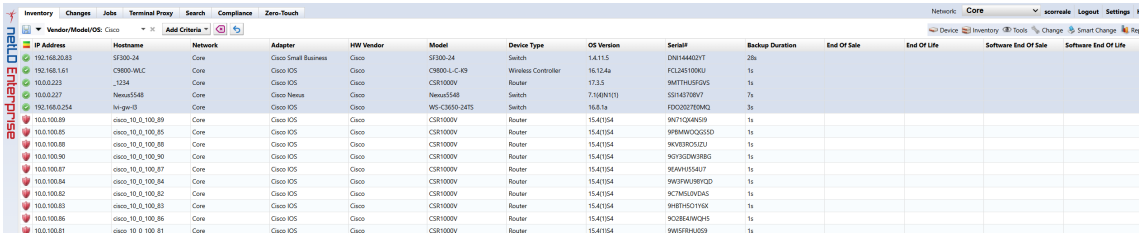


9. Click the button to save the job.

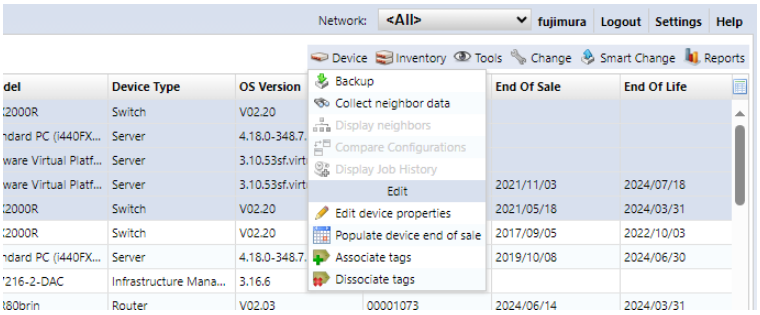


6.15 Device EOS/EOL management

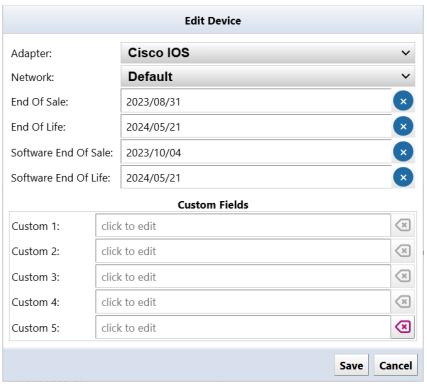
1. Select the device to obtain EOS/EOL.



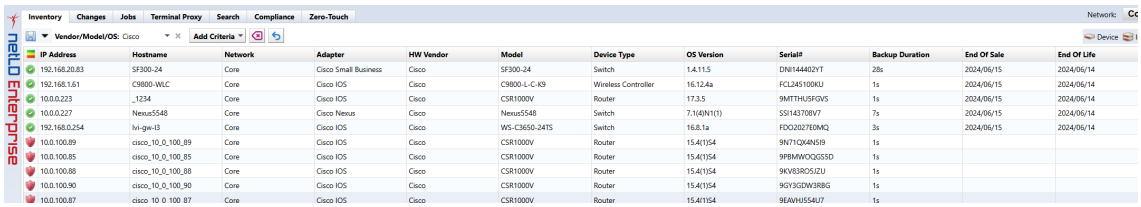
2. Click [Edit Device Properties] from the device menu.



3. Select the product “End of Sales” (support) and “End of Life” dates and click the [Save] button.

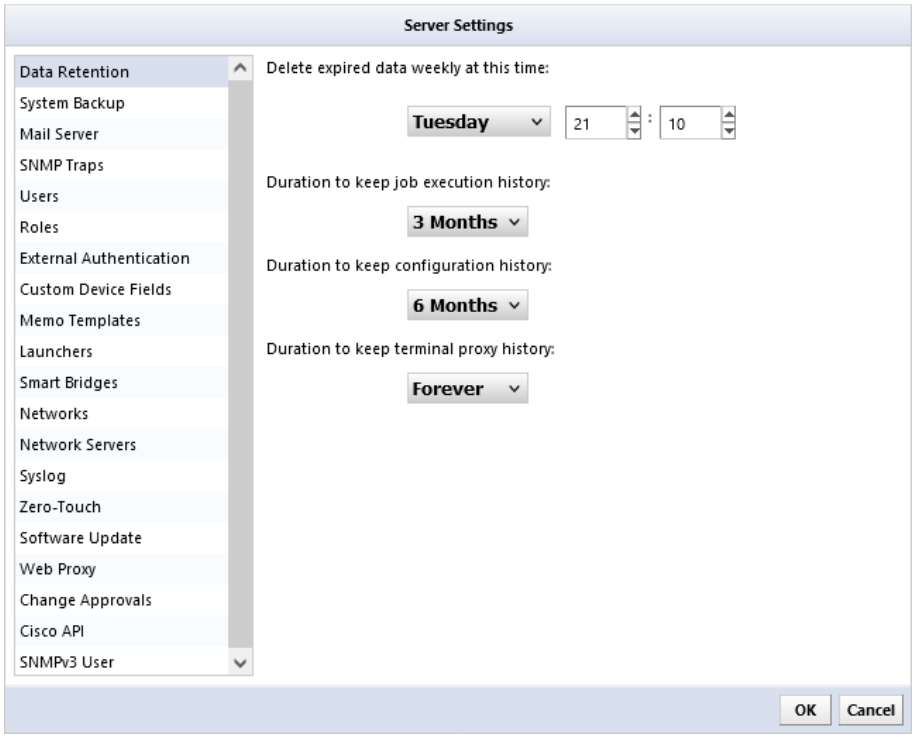


By following the above steps, the date set in the column will be displayed.



6.16 Change data retention period

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



Item	Explanation
Delete expired data weekly at this time	Data that has passed a certain period of time is automatically deleted every week on a specified day and time. (Initial value: Monday, 6:00) Specify the data retention period in the following items. (However, if you specify “No expiration date”, the data will not be deleted)
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”

7 HA (Active/Standby)

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

7.1 Prerequisites

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

7.2 Restrictions

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

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

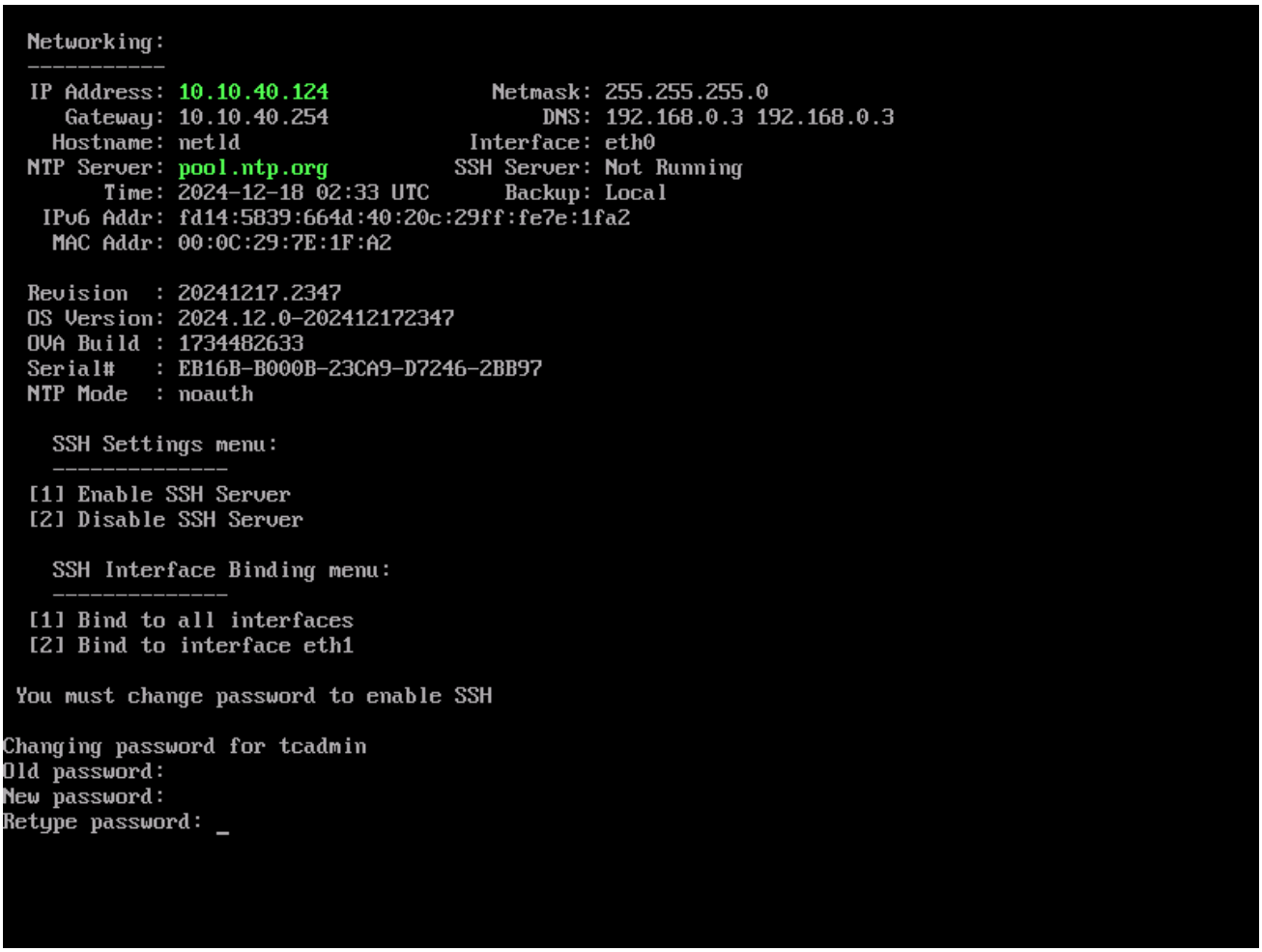
7.3 Settings

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

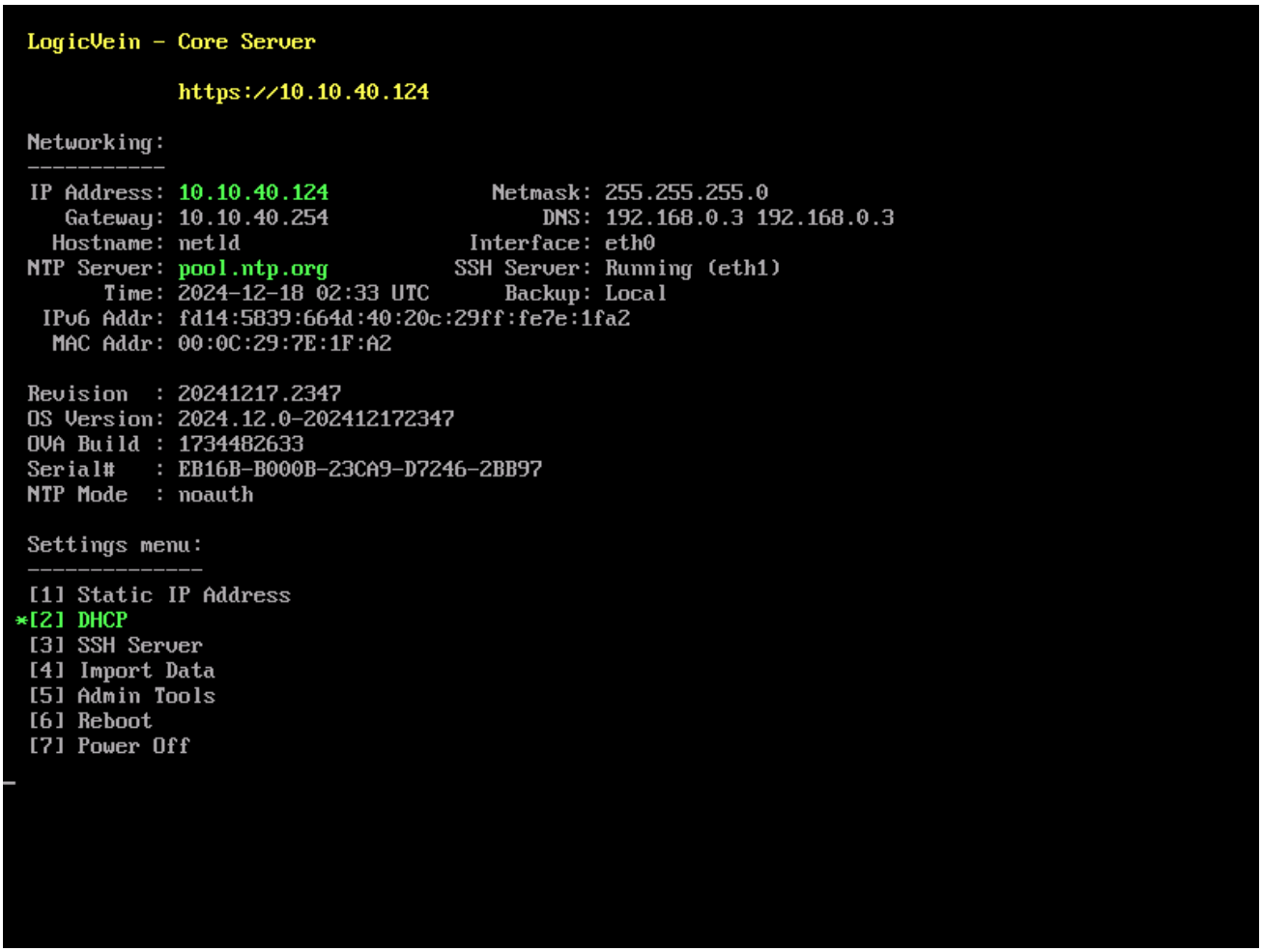
7.4 Procedure

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

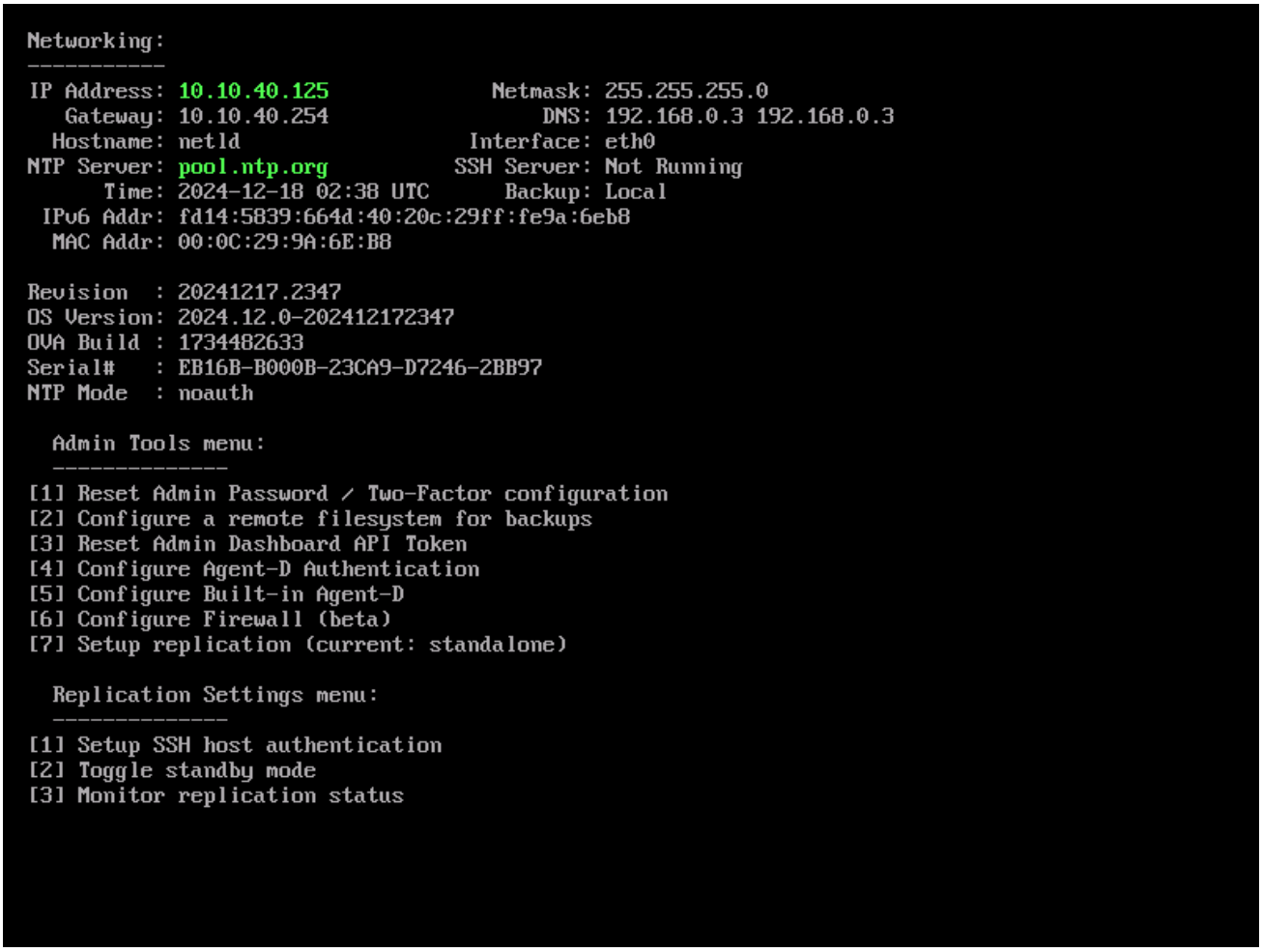
1. Connect to the OVA console on the primary server.
2. Enable SSH for eth1 by pressing [3] (SSH Server) > [1] (Enable SSH Server) > [2] (Bind to interface eth1) on the keyboard.



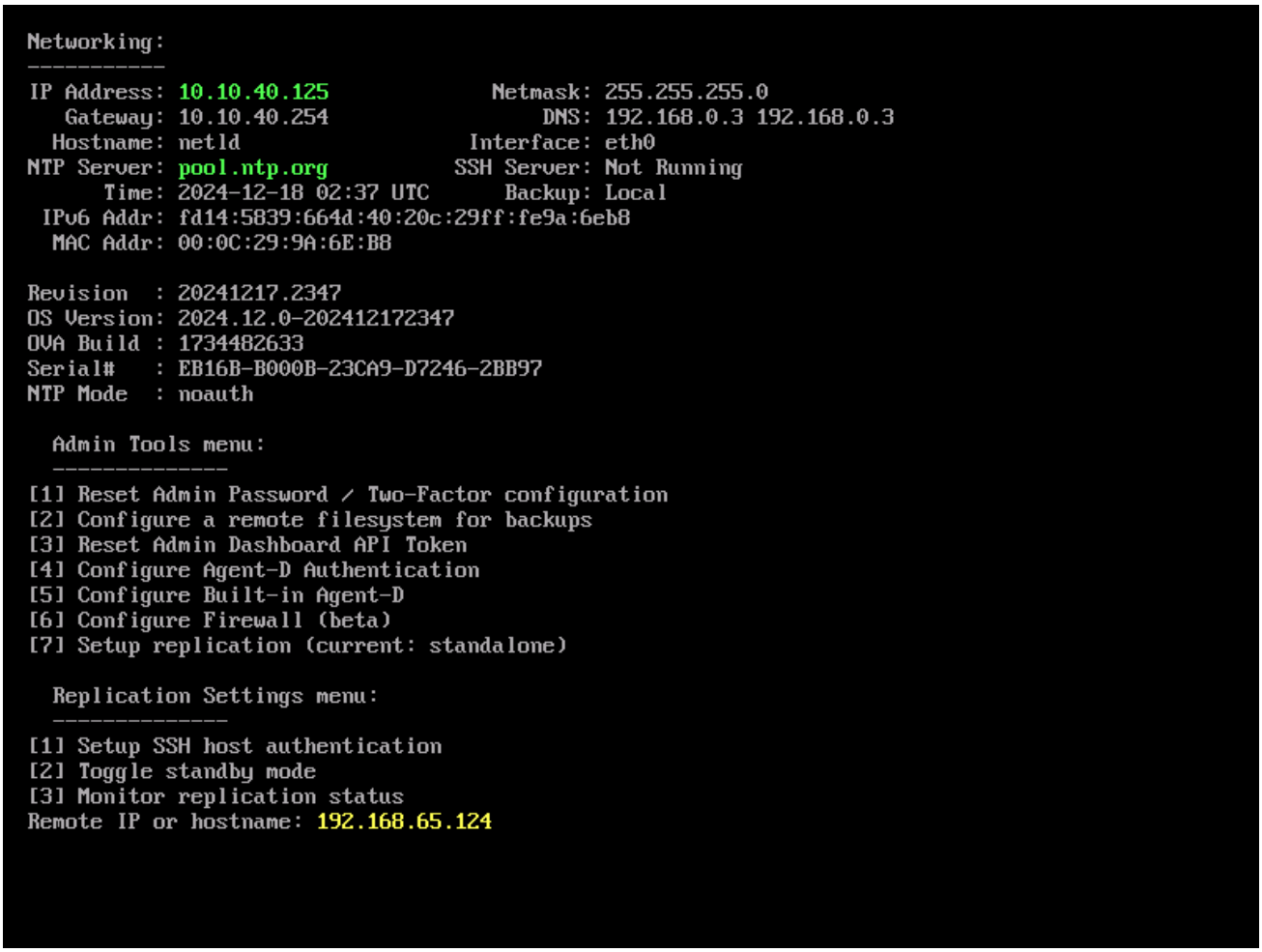
3. Confirm that the SSH Server is Running.



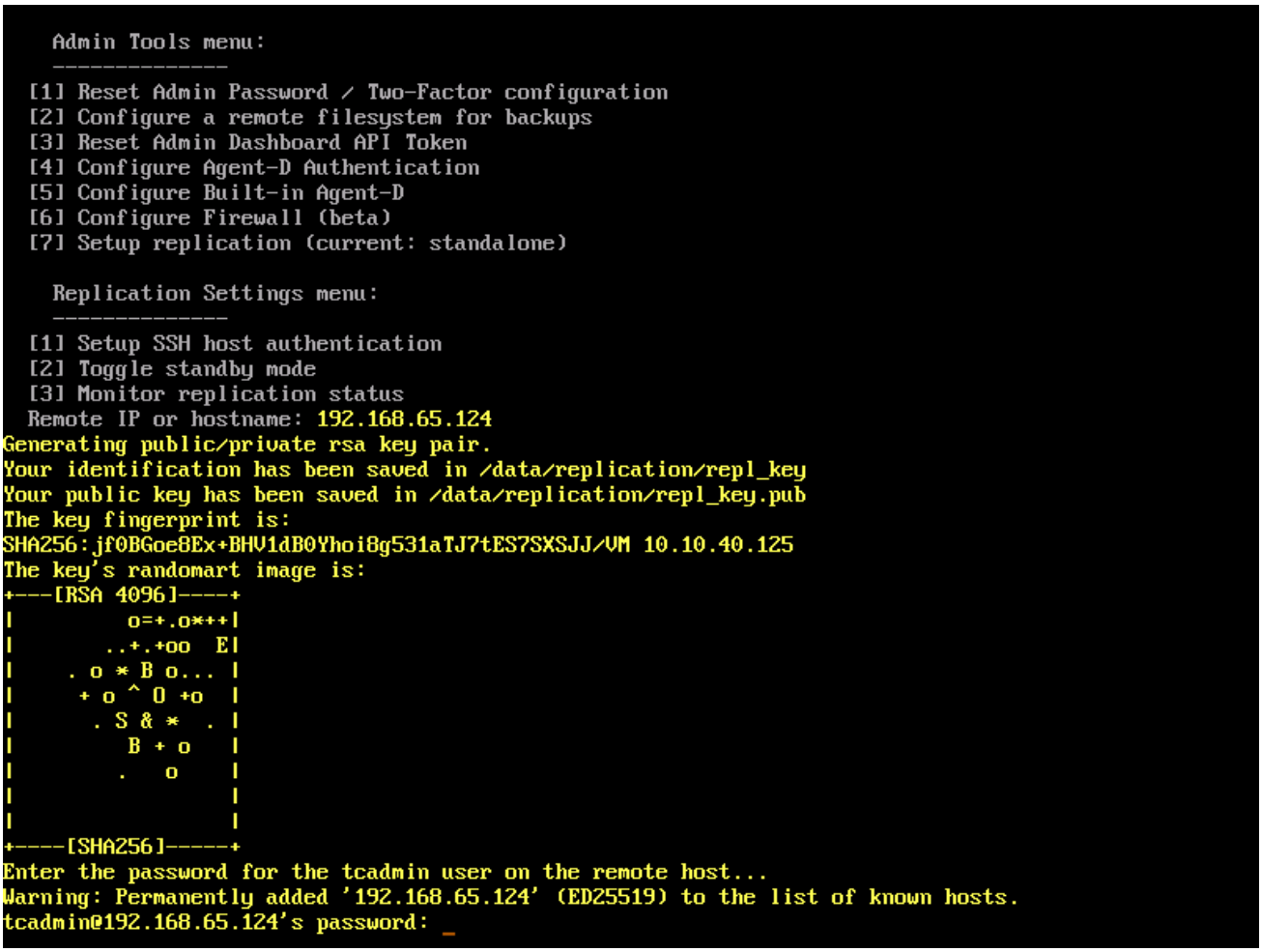
4. Connect to the OVA console of the standby server.
5. Press [5] (Admin Tools) > [7] (Setup replication) > [1] (Setup SSH host authentication) on the keyboard to configure SSH host authentication settings for the primary server.



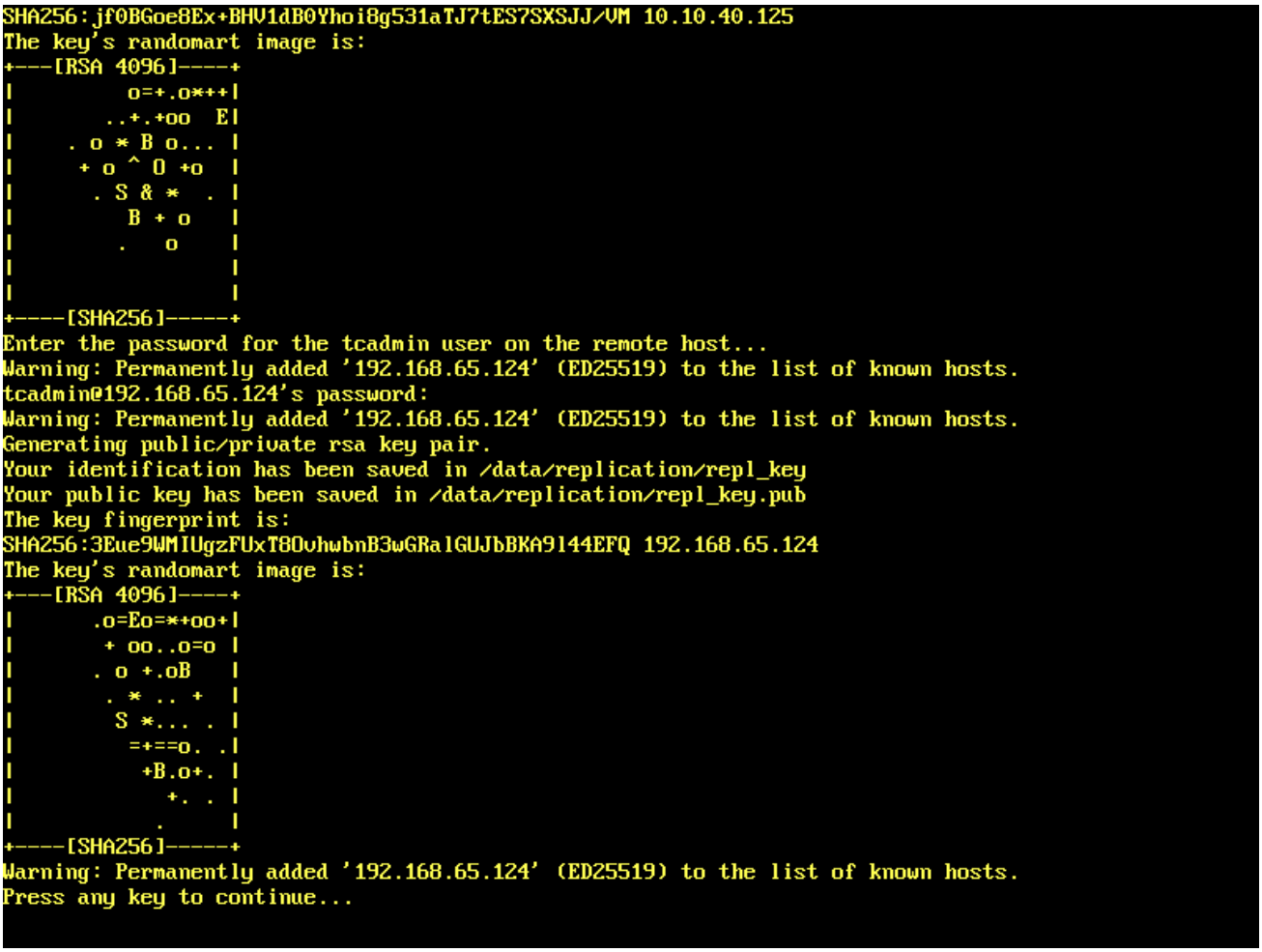
6. Enter the eth1 IP address of the primary server.



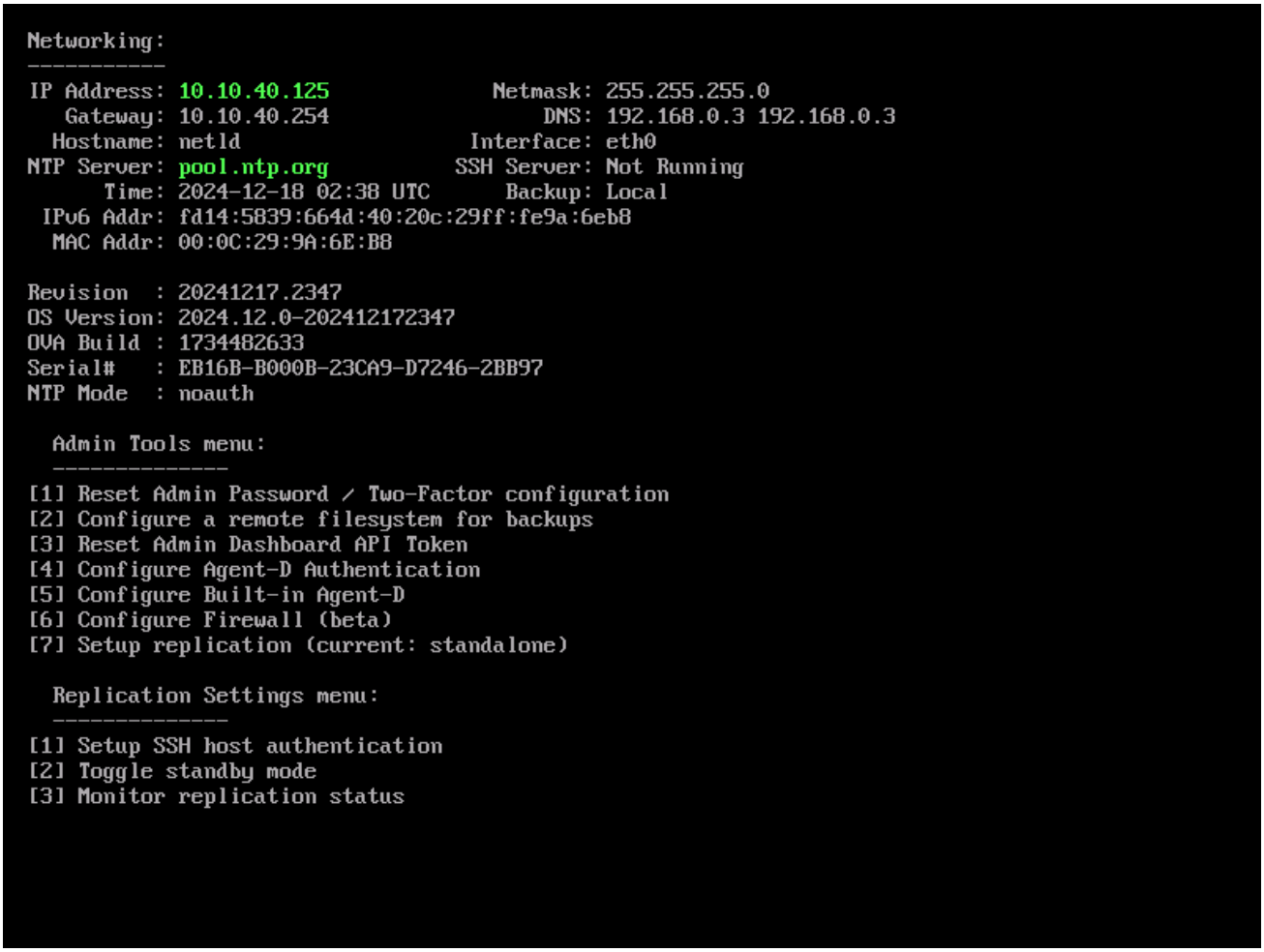
7. Enter the password for SSH to the primary server.



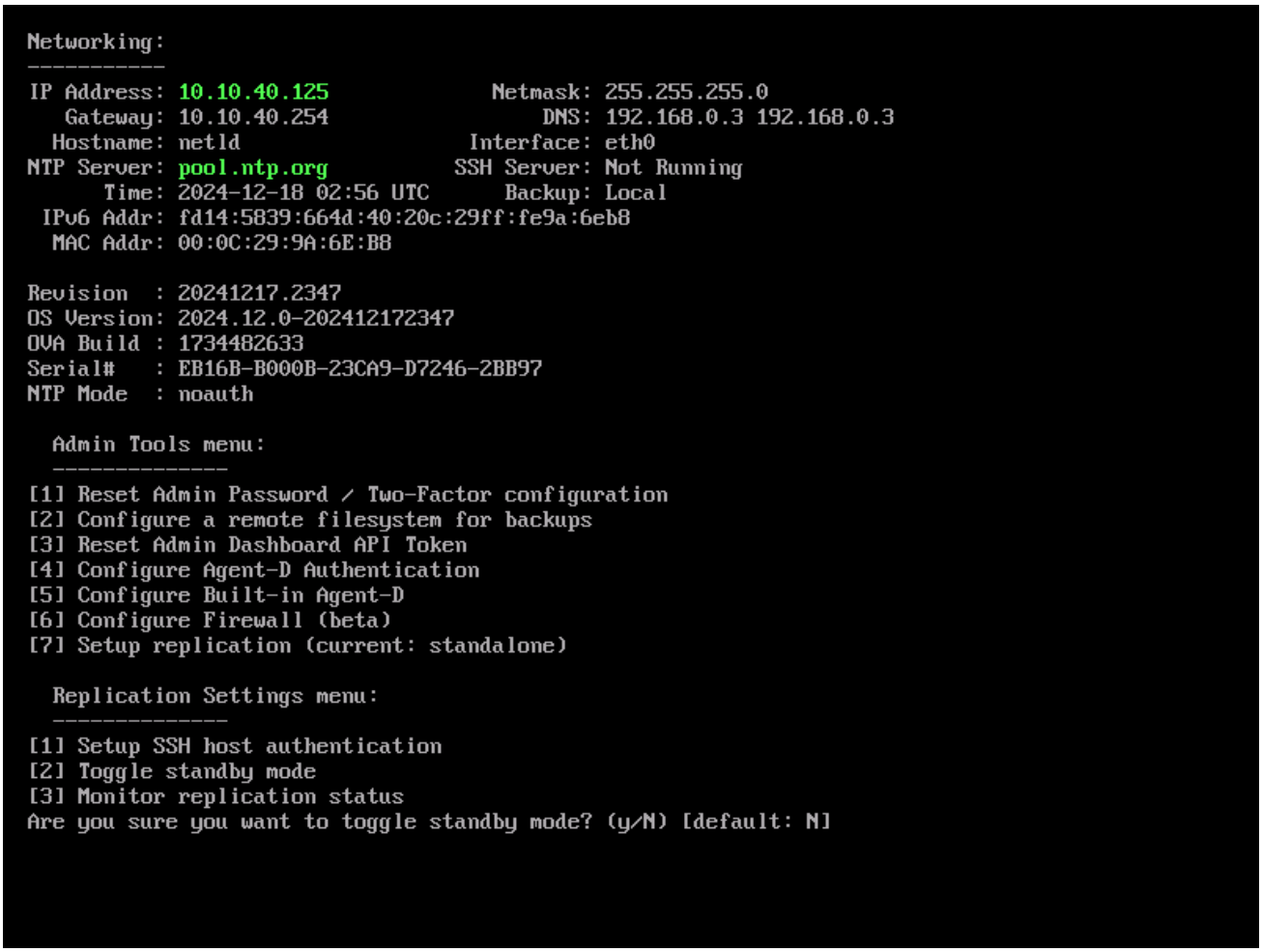
8. Press any key, such as the [Enter] key.



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



10. Press [Y].

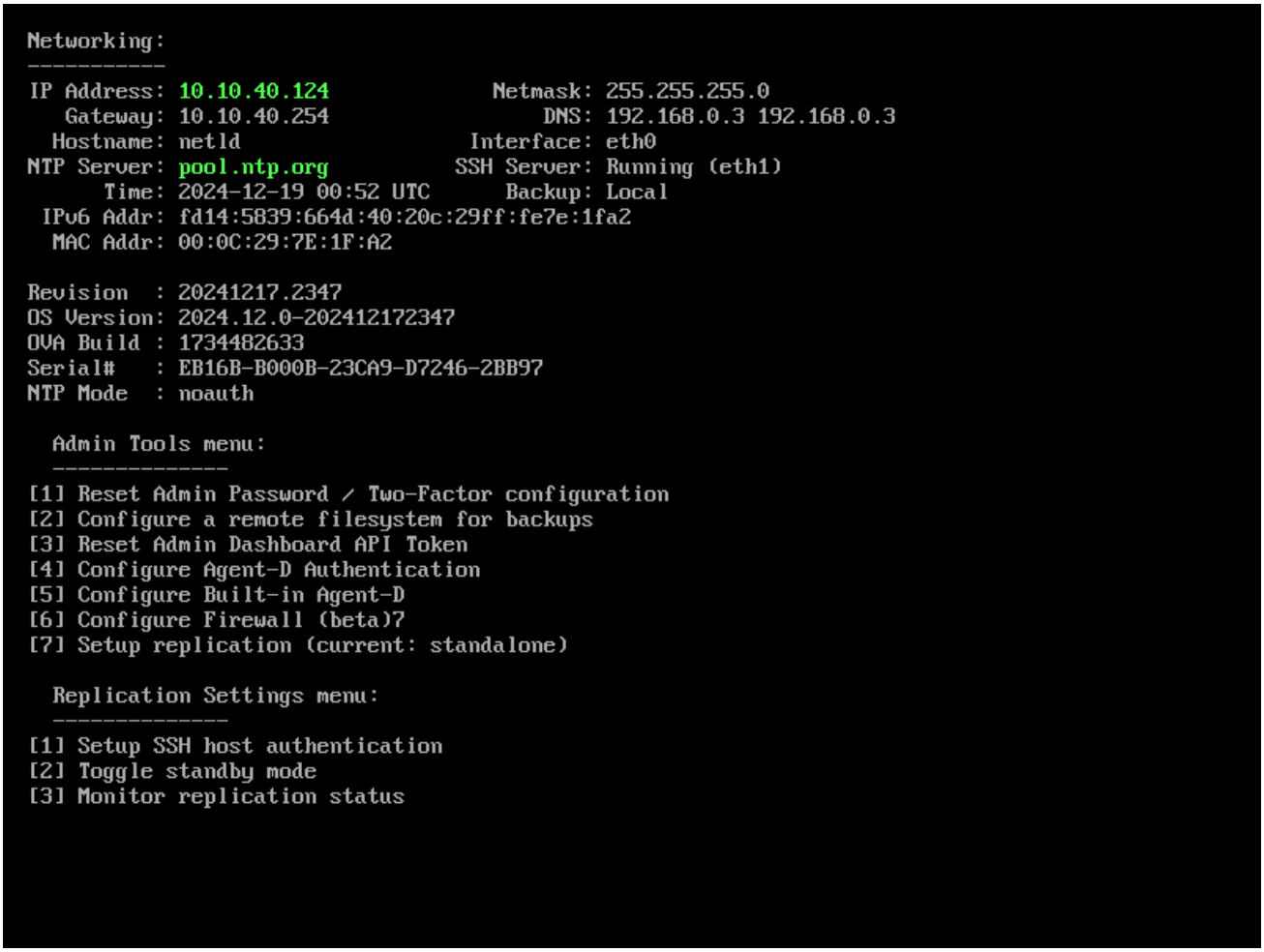


11. Press [Y] to automatically restart the standby server.

7.5 Confirm status

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

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

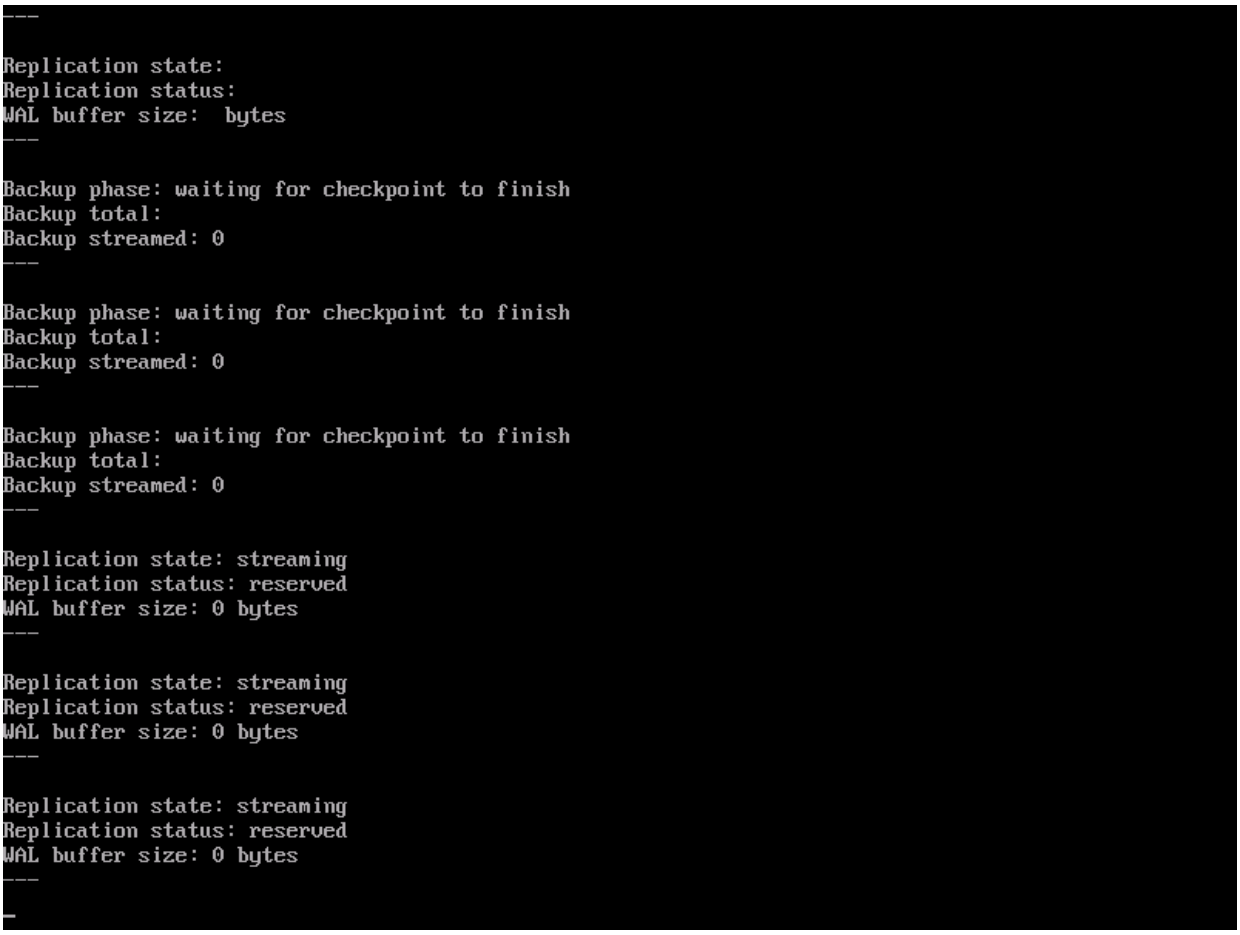


The status will be updated automatically when it is displayed. To close the status screen, press [Ctrl+C].

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

```
---

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

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

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

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

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

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

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

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



7.6 Cases for Reconfiguration

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

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

7.7 Failover

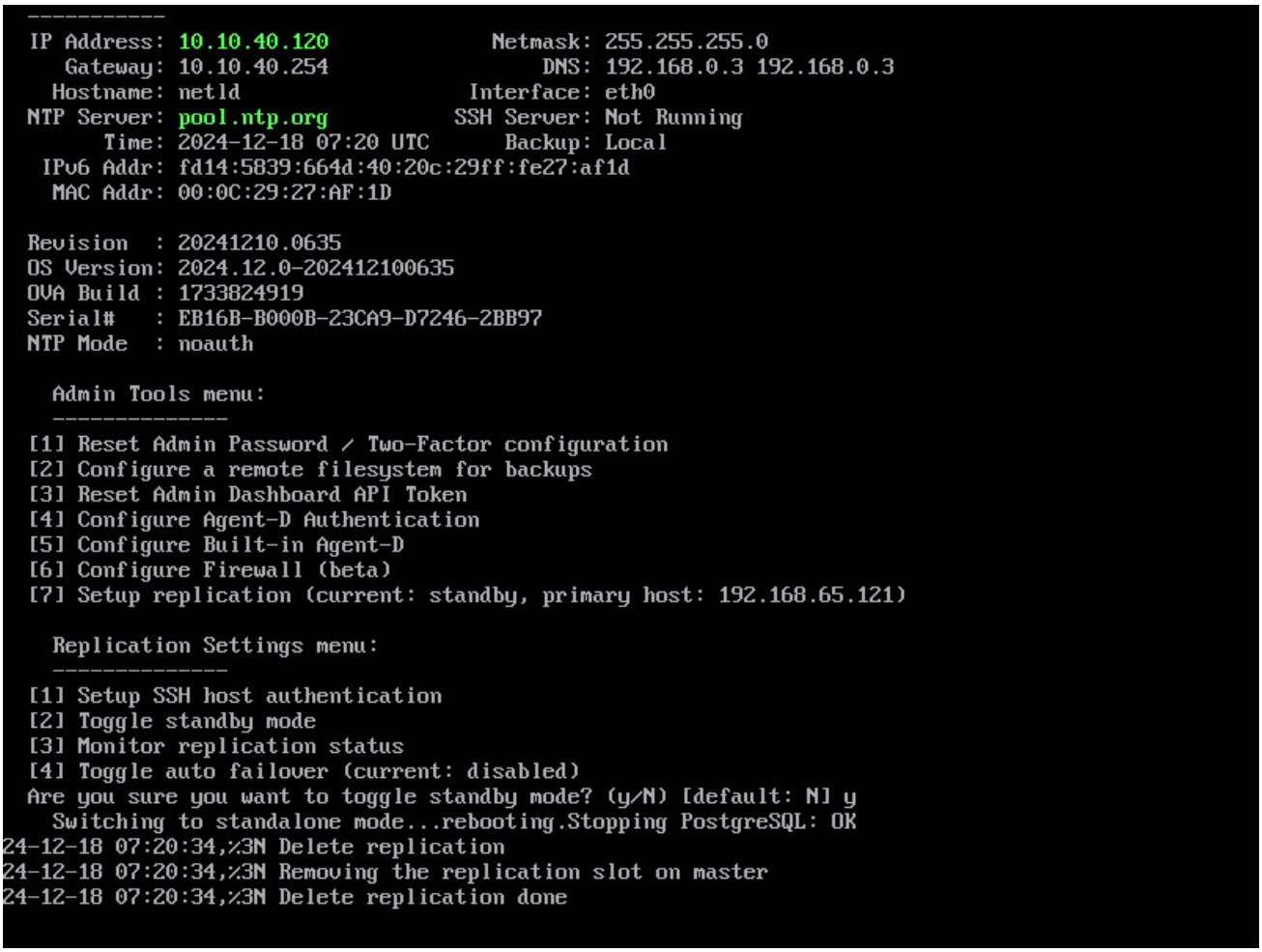
Failover refers to the process of automatically switching to a redundant or standby system when the primary system fails, ensuring minimal downtime and continuous operation.

7.7.1 Manual failover

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

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

3. Press [Y].



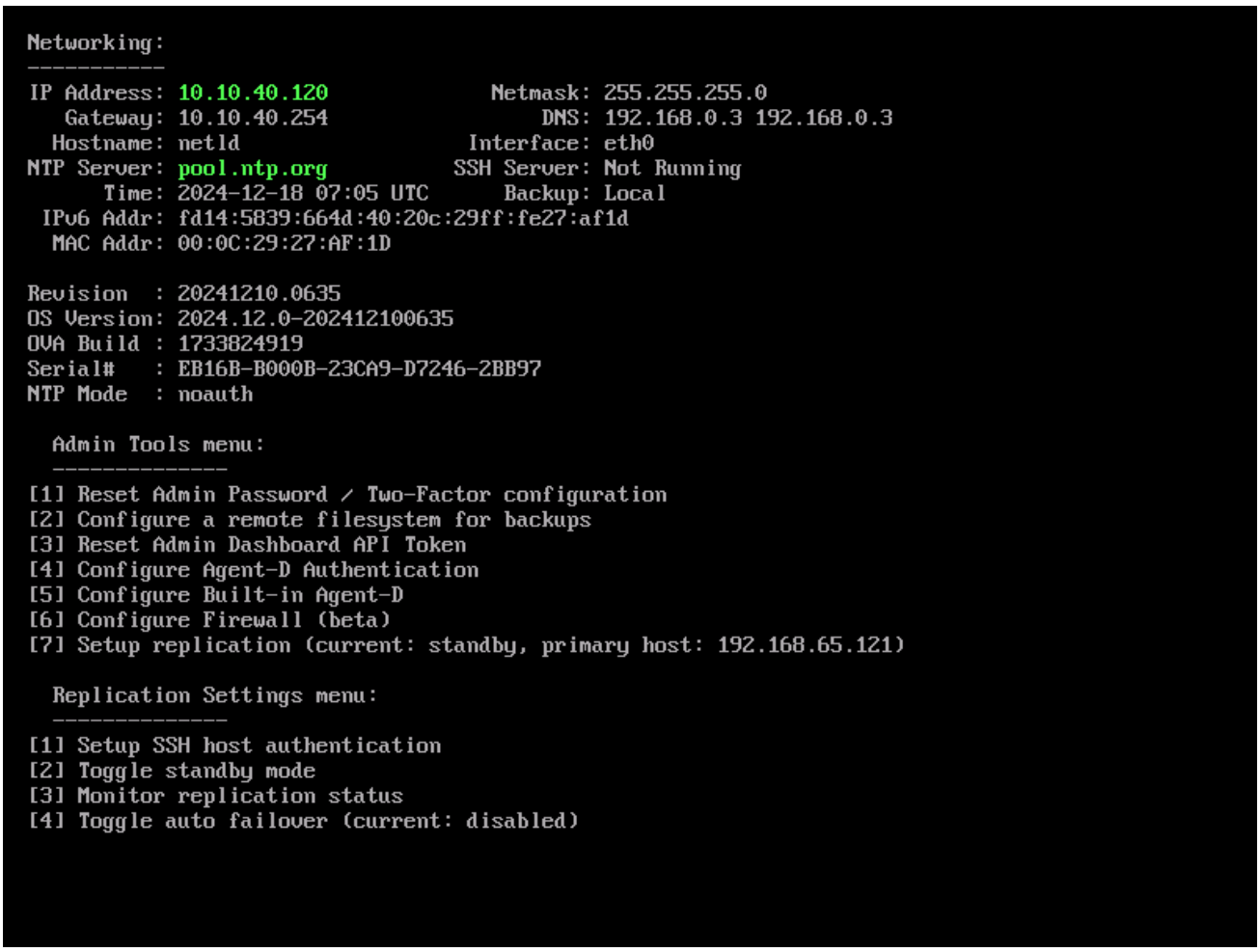
Press [Y] to automatically restart the standby server. After restarting, please log in from a web browser.

7.7.2 Auto failover

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

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

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



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

7.8 Automatic configuration

7.8.1 Prerequisites

NetLD requires the following prerequisites:

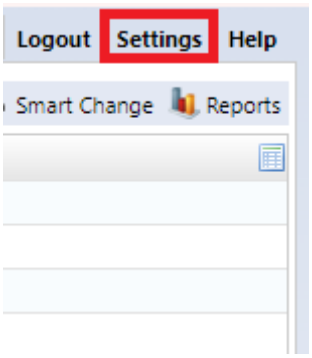
- The NetLD you are using must be able to connect to the Internet.
- You must log in with your Cisco account and obtain an API key and secret code before accessing Cisco Smart Net Total Care.
- Valid Cisco Smart Net Total Care (SNTC) is required.

Please see below for information on obtaining API:

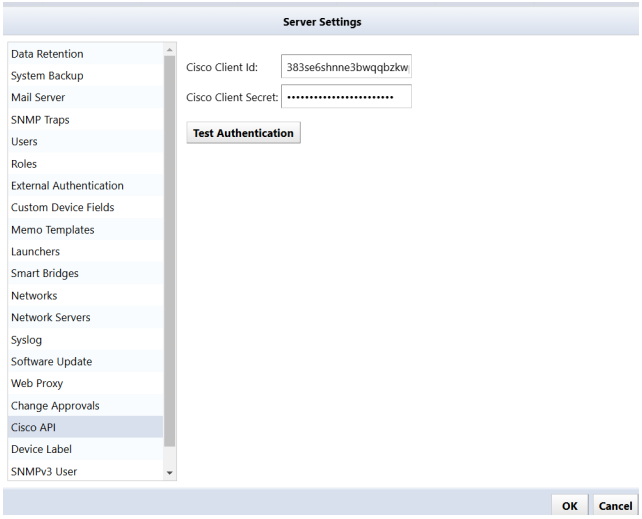
https://developer.cisco.com/docs/support-apis/#!user-onboarding-process

7.8.1.1 Procedure (online environment)

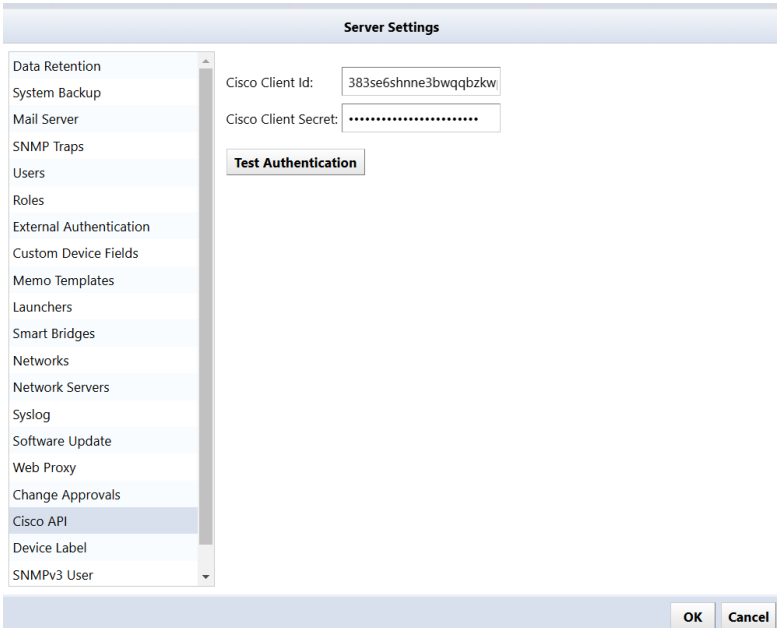
1. Click Settings .



2. Click [Cisco API].

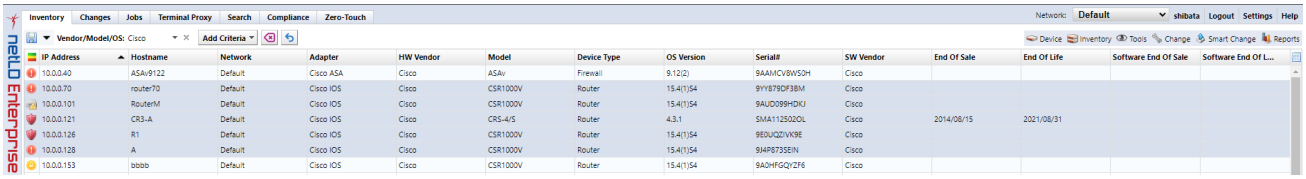


3. Enter your API key and secret code and click [OK].

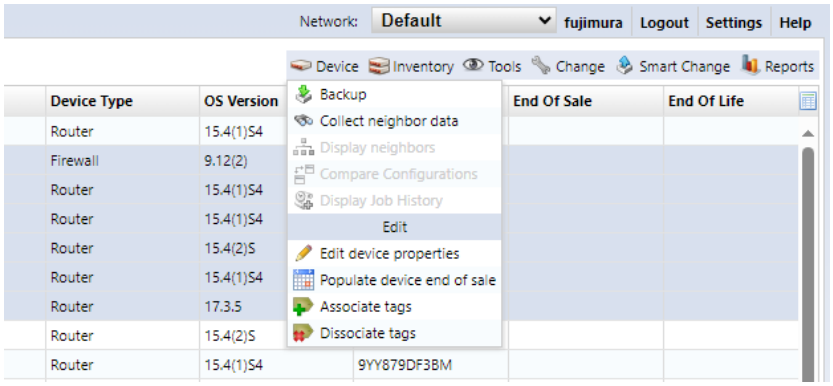


4. By clicking [Test Authentication], you can check whether the ID and Secret code you entered can be used.

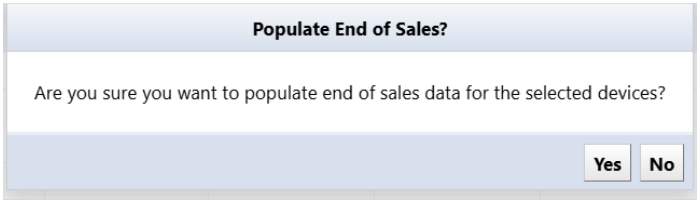
5. Select the device to obtain EOS/EOL.



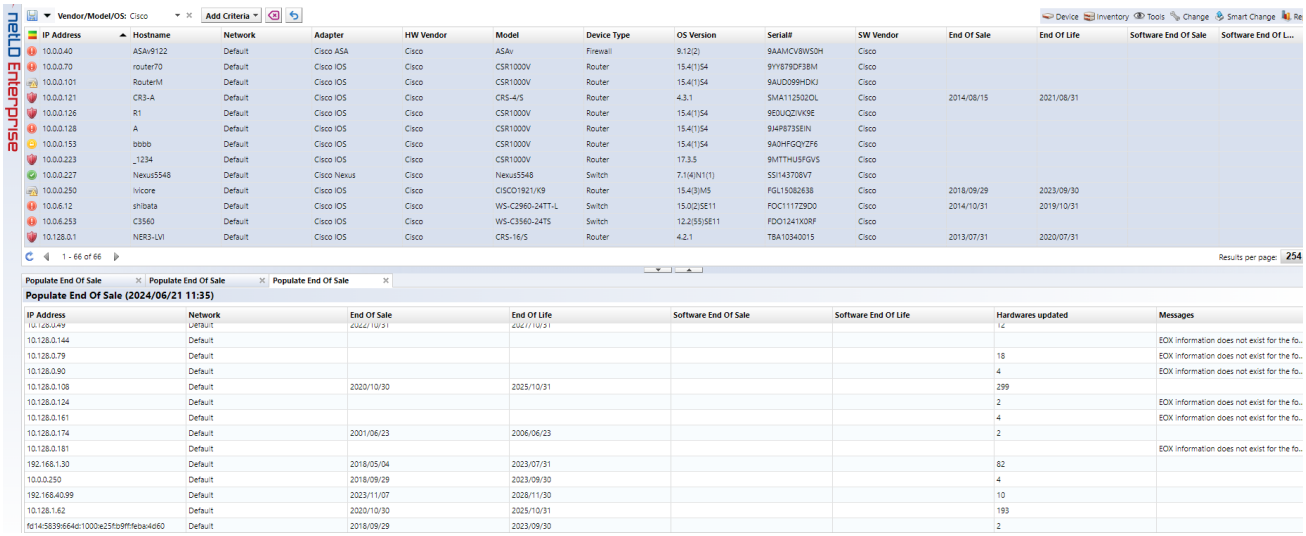
6. Click [Populate device end of sale] from the device menu.



7. Click [Yes] on the screen below.

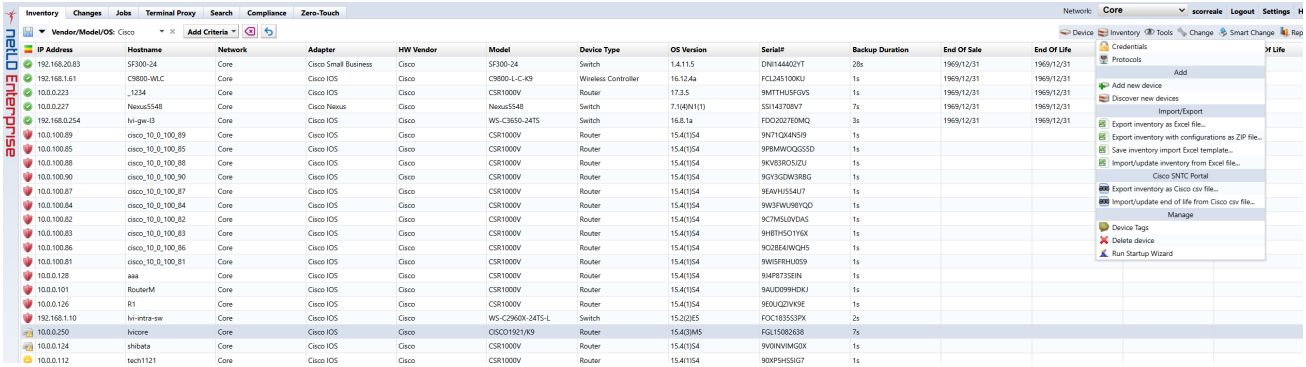


8. Using the above steps, EOS/EOL information will be automatically acquired and registered in the column.



7.8.1.2 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.



7.9 Wireless Lan Controller Monitoring

WLC monitors may now be added to Wireless Lan Controllers running the Cisco IOS XE Operating System. Monitored devices will be polled periodically via https for a set of connected clients as well as some associated information, such as which Access Point each client is connected to. This allows for the querying of clients based on data points such as MAC, IP Address, or when the client was last seen. It also allows for the display of clients on Maps under their associated Access Point.

7.9.1 Setup and configuration

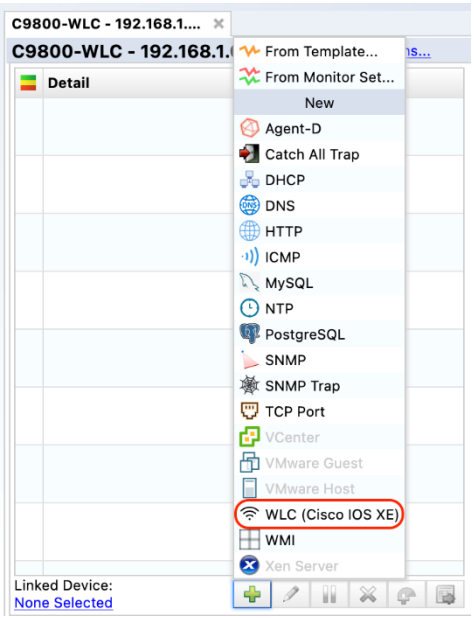
1. Add your Wireless Lan Controller, and its associated Access Points to the inventory.
2. Ensure that their hostnames are correct, and that their Device Adapters are set to Cisco IOS.

Access Points reported from the Wireless Lan Controller will automatically be given an AP tag. This identification is based on both the Managed Network and Hostname of the device in inventory. So please make sure that the APs are in the same Managed Network as the controller and that the hostnames in inventory match the hostnames configured in the Controller.

3. Make sure your Wireless Lan Controller has credentials configured for it in the Credential Manager.

Here "`VTY Username`" and "`VTY Password`" are used for authentication.

4. Add a WLC (Cisco IOS XE) Monitor to the Wireless Lan Controller.

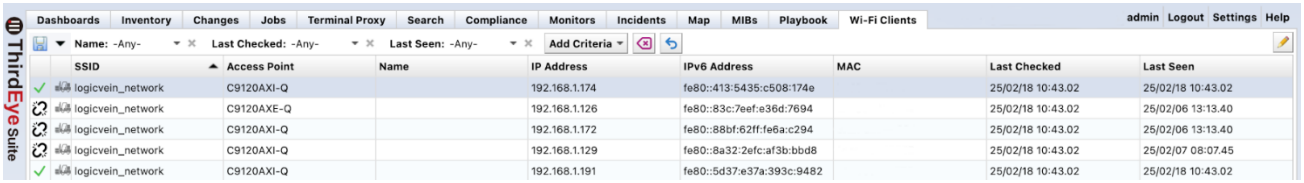


5. Set a name, polling period, retention history, and optionally some triggers, then hit save. In a few moments, a table displaying collected Access Point Names & the number of currently connected devices will appear:

wlc

Index	count
C9120AXE-Q	4
C9120AXI-Q	9

As the monitor starts polling, the access points will automatically receive the device tag "AP" ("Access Point"). Clients will also become visible under the new [Wi-Fi Clients] tab.



Here, the columns displayed will indicate in order:

1. The most recent connection status of the client:

✔: The Client was connected while the WLC was last polled for updates.

: The Client was not connected while the WLC was last polled for updates.

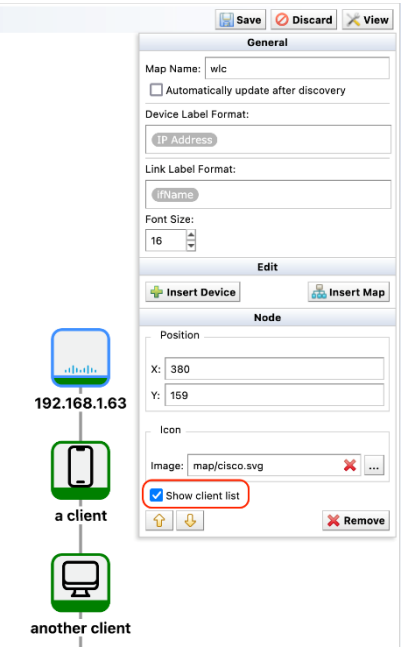
2. The customizable Icon for the Client.
3. The SSID the Client is, or was last, connected to.
4. The Access Point the Client is, or was last, connected to.
5. The customizable Name for the Client.
6. The current or last known IP Address of the Client.
7. The Client's MAC address.
8. The last time the WLC was polled.
9. The last time the Client was connected while the WLC was polled for updates.

Selecting a Client and clicking the pencil in the top right will also allow you to customize a Client's name and icon. These customizations are mapped to a client's MAC address, so even if they receive a new IP address, the customizations will continue to follow each client.

7.9.2 Viewing clients on a Map

Add your Access Points to a Map as Devices. Now that they have an AP tag, a new option will be available when editing each one.

Enable [Show client list] to display all clients under the Access Point.



The images and names of each client may also be customized in this view. When viewing clients on a Map, right click one and select [Edit Client].

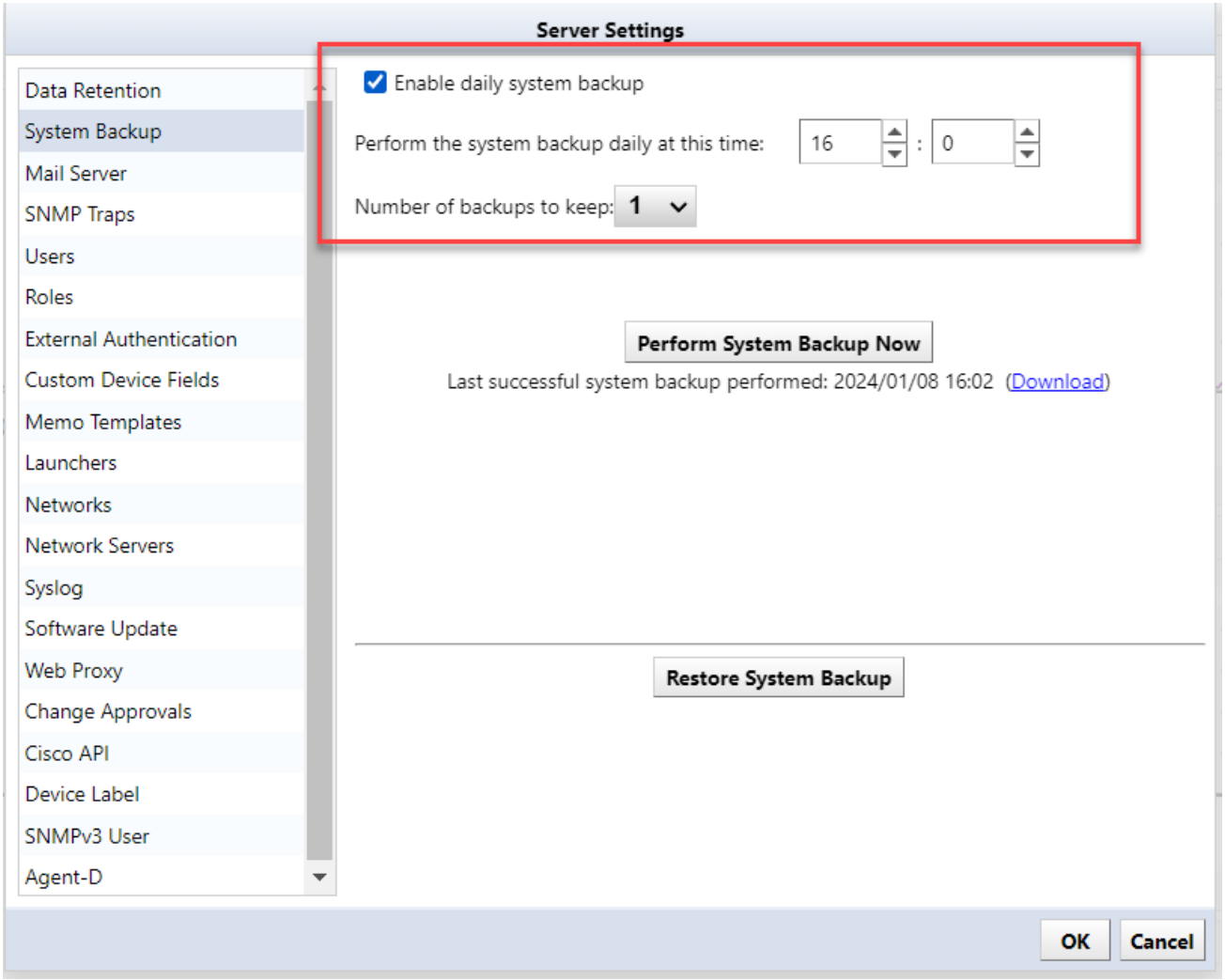
8 System backup/restore

A system backup is a backup of the entire NetLD. You can backup/restore various settings and monitor data (polling, SNMP traps, etc.).

To perform a system backup, click Settings > [System Backup] .

8.1 Perform system backup automatically

Automatica system backups are enabled by default. If you want to disable it or change the time for automatic nsystem backup, change the contents in the red frame below.

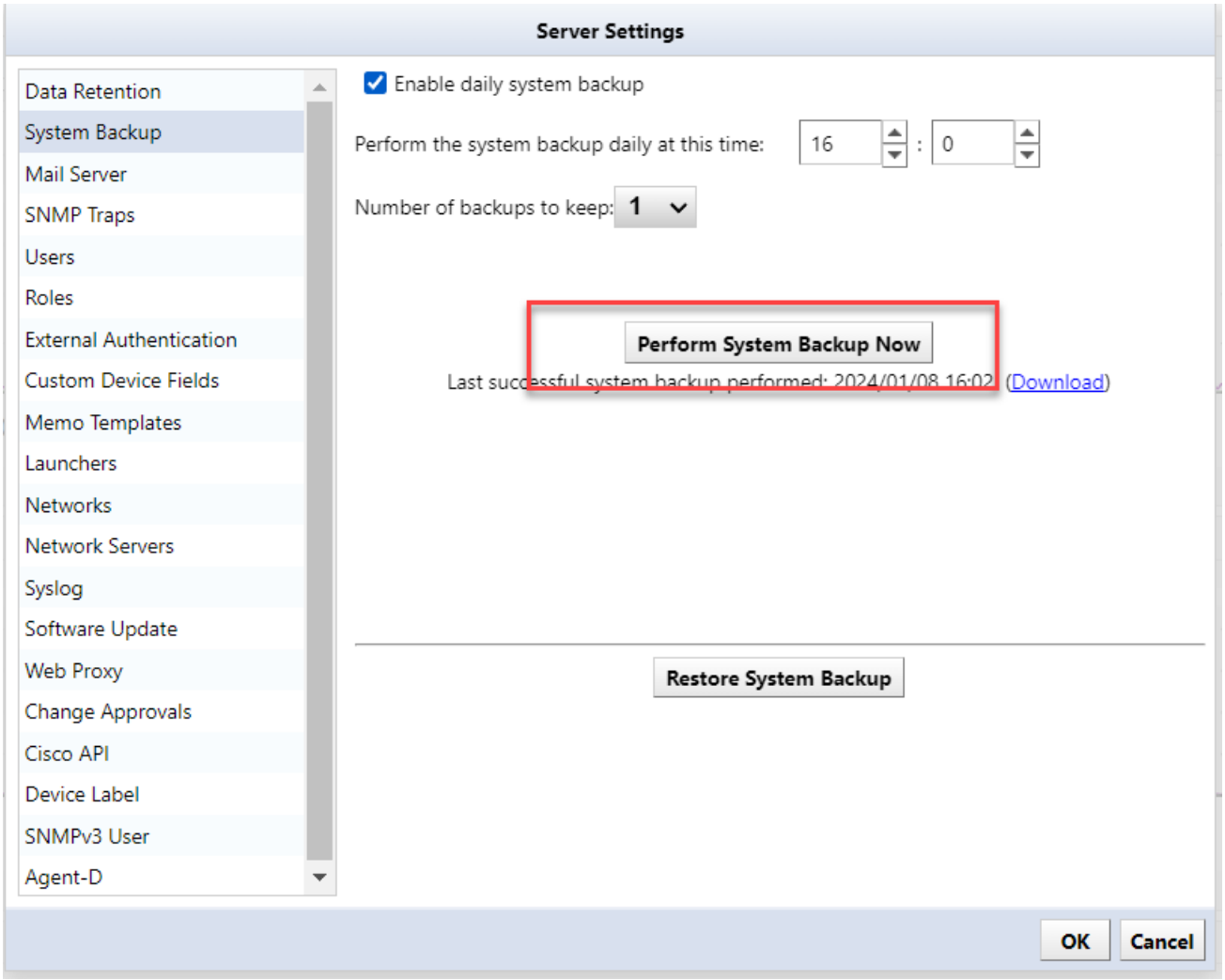


Item	Explanation
Enable daily system backups	Enable daily system backups. If this setting is enabled, a system backup will be performed at the specified time. (Initial value: `Enabled`)

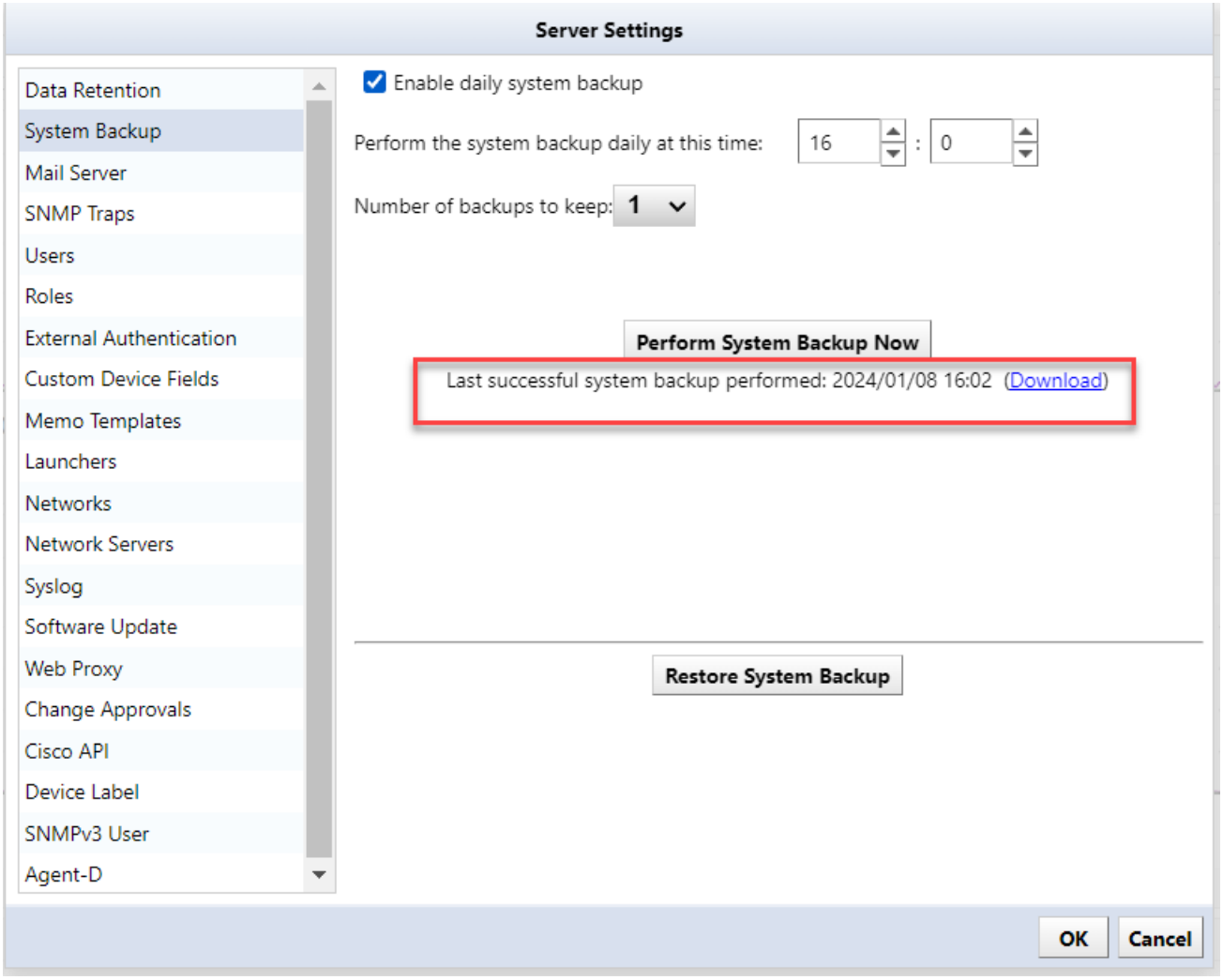
Item	Explanation
Perform the system backup daily at this time	Specify the execution time for daily system backups. (Initial value: `7:00`)

8.2 Perform a manual system backup

To perform a manual system backum, click [Server Settings] in the Global Menu, then click [Perform System Backup].



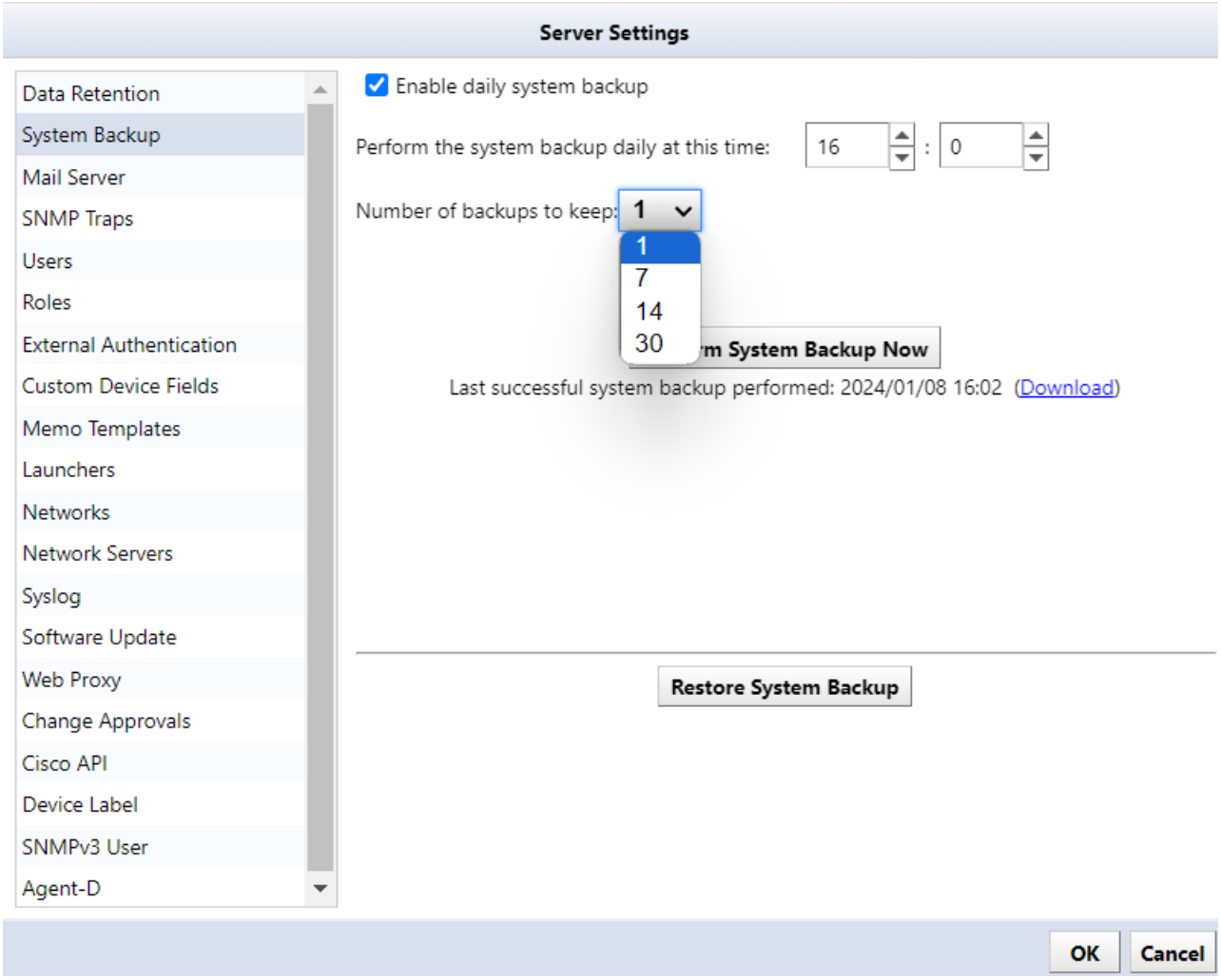
The button is grayed out while a backup is in progress. Once the button becomes clickable, the latest system backup date and time is updated, and the process is complete.



8.3 Change the number of system backups retained

You can select the number of system backups. The default value is 7. Any data that exceeds the selected number of backups is deleted.

Depending on the environment and length of operation period, the number of system backups can accumalate, and consume up disk space. Disk space usage can be reduced by reducing the number of system backups.

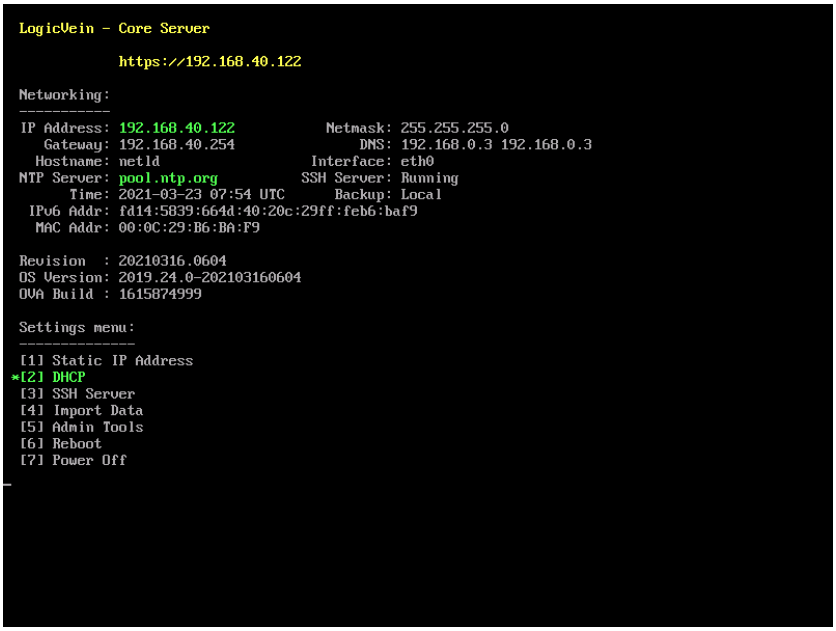


8.4 Save to external storage

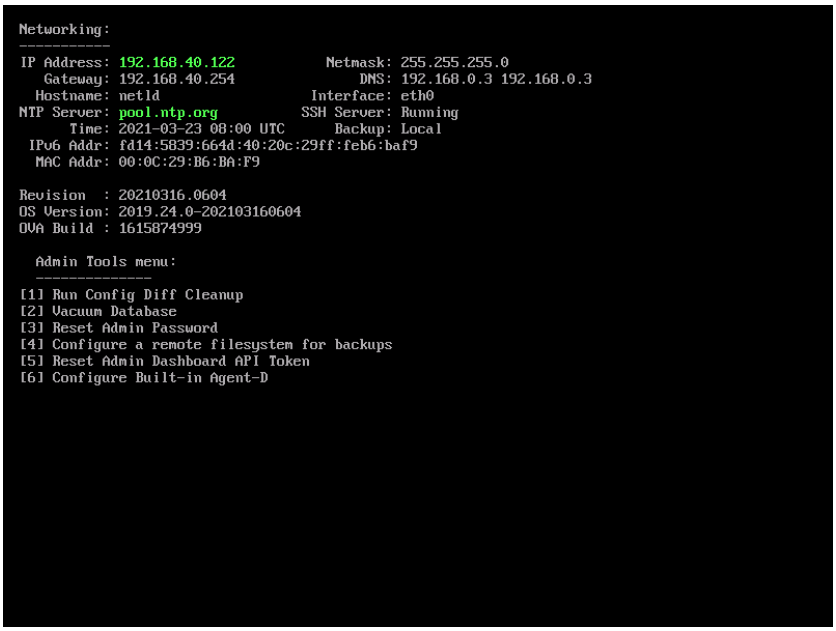
By default, system backup files are stored inside the virtual appliance. However, you can configure external storage to store them automatically outside the virtual appliance. Supported protocols are NFS/SMB.

To set up external storage:

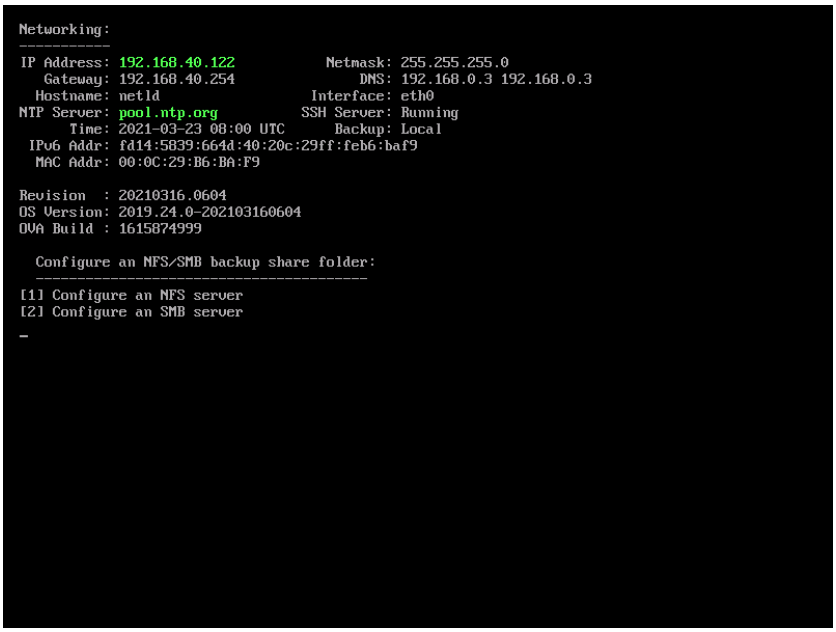
1. Click the [5] key on your keyboard, and select [Admin Tools].



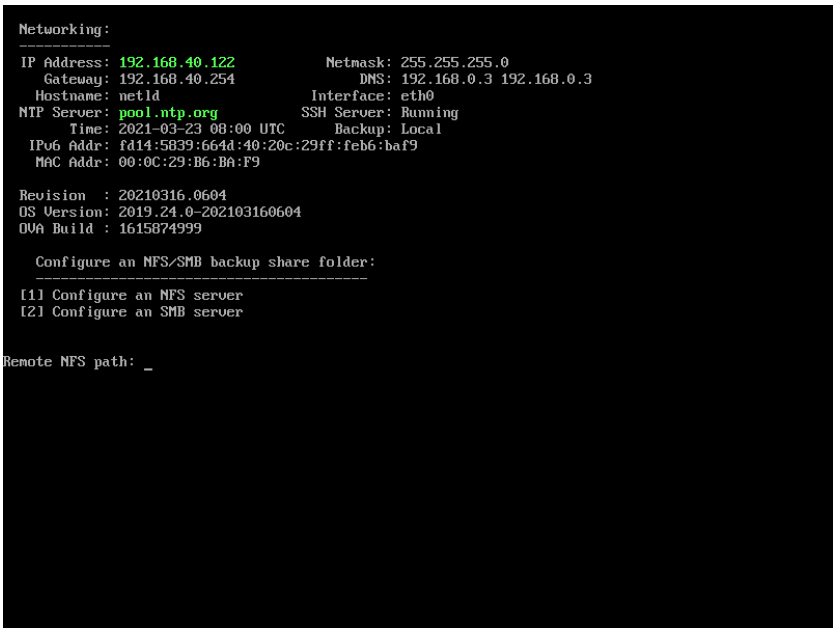
2. Click the [4] key on your keyboard, and select [Configure a remote filesystem for backups].



3. Select the server type.

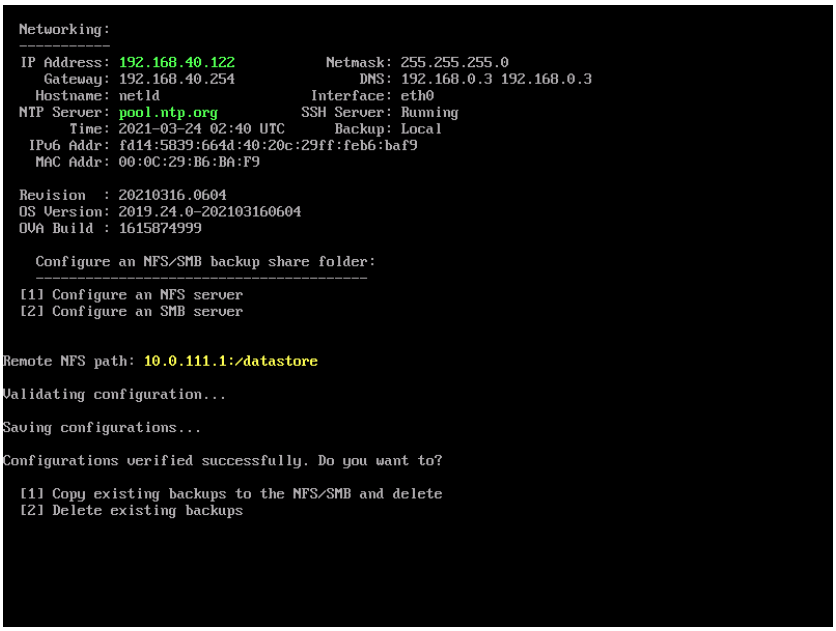


4. Enter the required information and press [Enter].



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

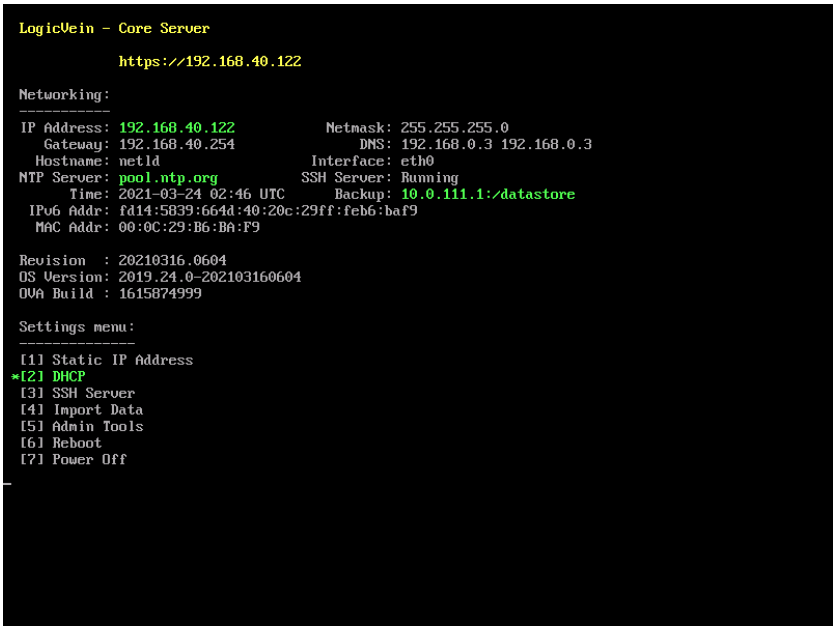
5. Select [1] or [2].



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

The console screen settings are now complete.

NetLD will restart automatically, and you can check the settings on the console screen.



8.5 Create system backup zip file

To create a backup zip file on external storage:

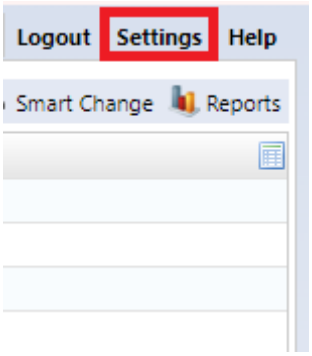
1. Open the backup folder. The folder name will be in the format "`(backup_YYYY\\MM\\DD)`".
2. Save the following three items to a zip file:
   - `pgsql` (folder)
   - `version.txt` (file)
   - `complete` (file)

8.6 Restore system backup from zip file

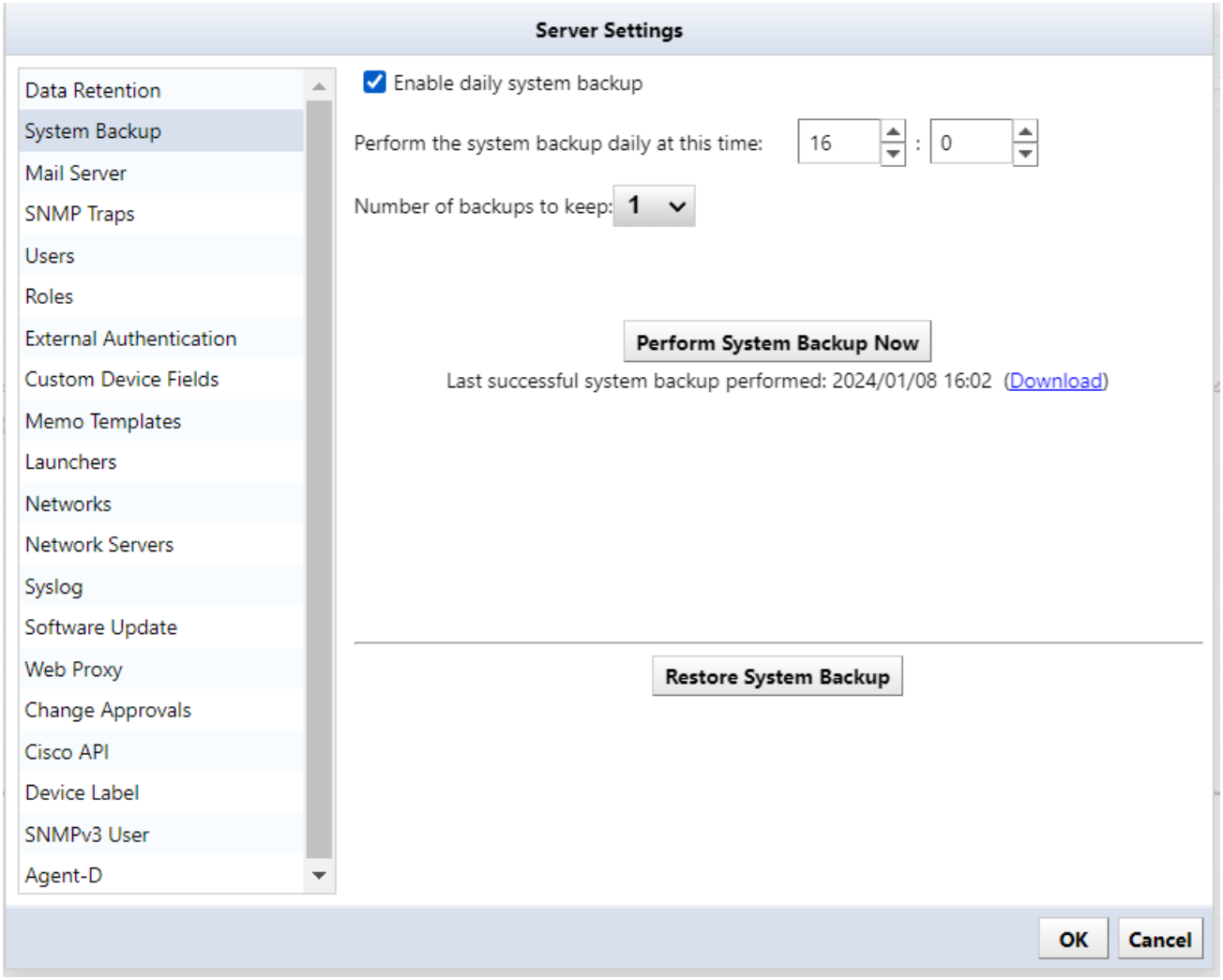
To restore system backup from a zip file, select the backup source and restore destination. It must be the same version (revision).

For information on how to check the version:

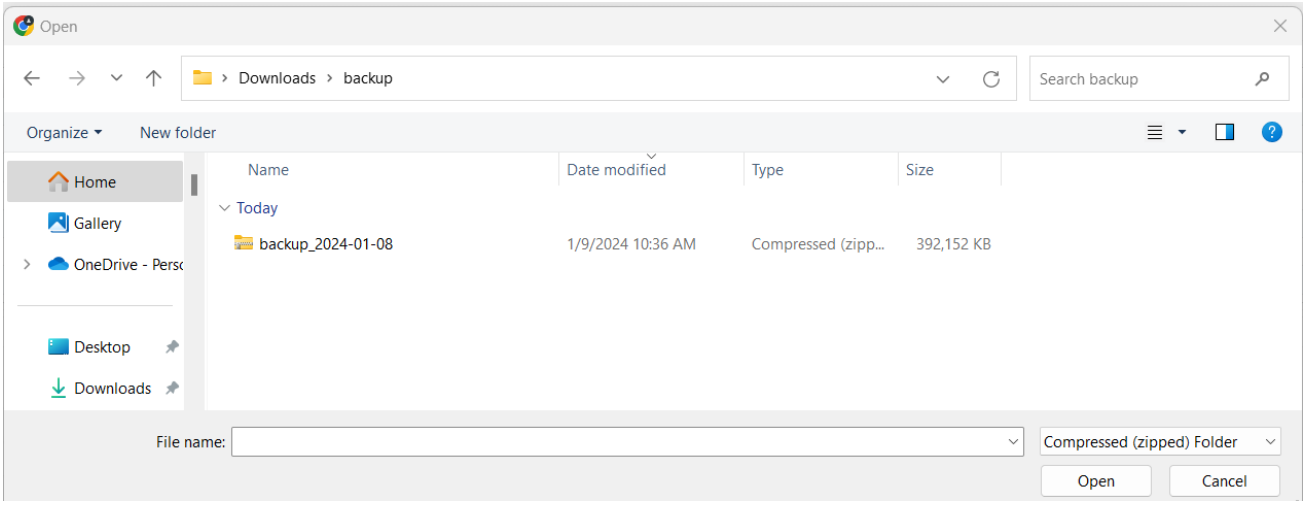
1. Log in as a user with administrator privileges.
2. Click Settings on the Global Menu.



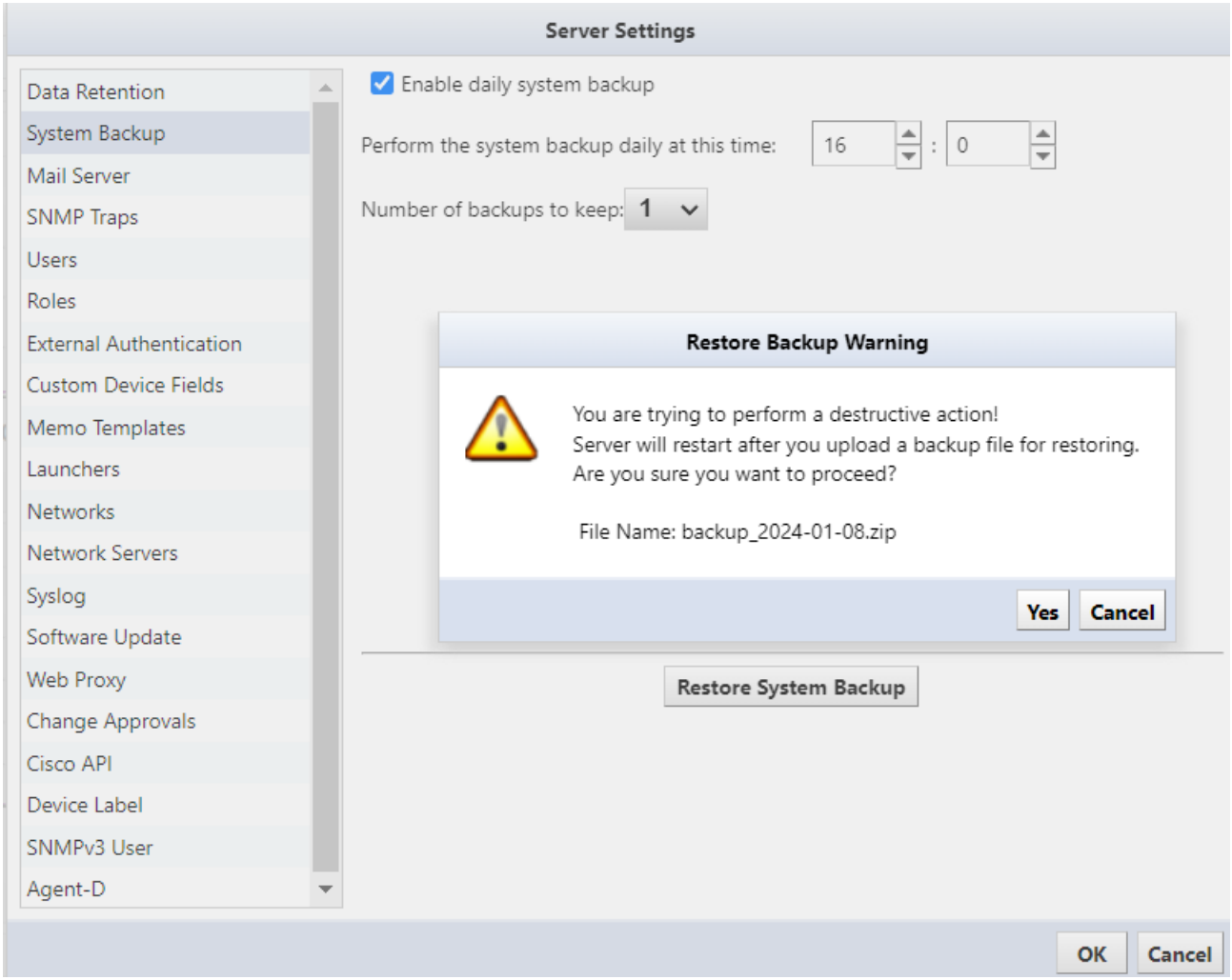
3. Click [System Backup] > [Restore System Backup].



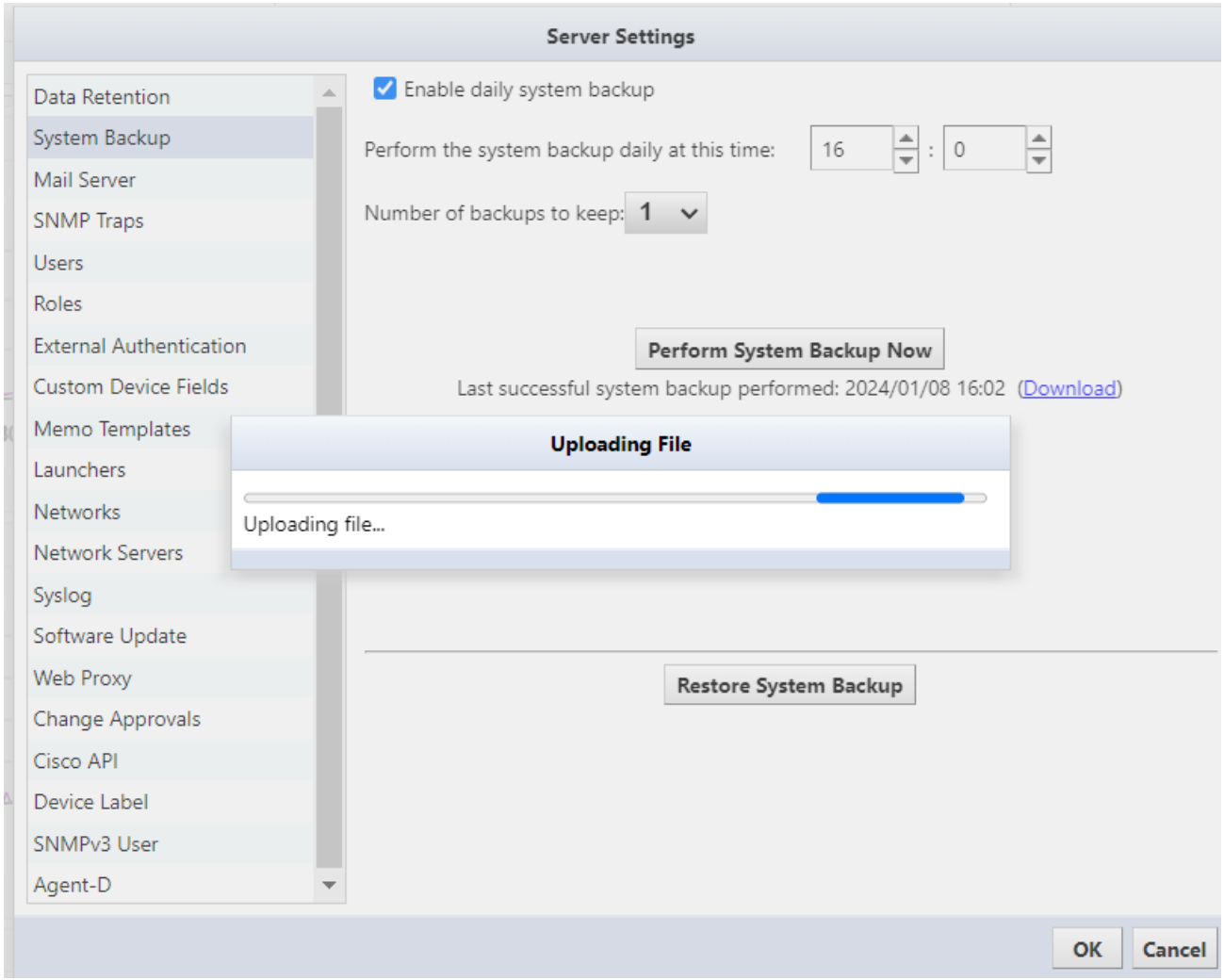
4. Select the file you want to restore, and click [Open].



5. Click [Yes] on the warning screen.



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

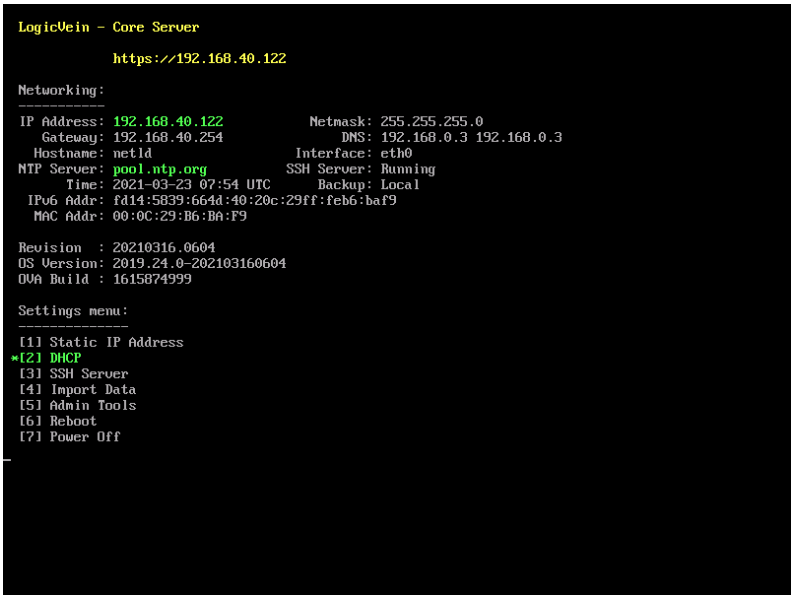


System backup/restore is now complete.

After uploading, the service will automatically restart and return to the login screen.

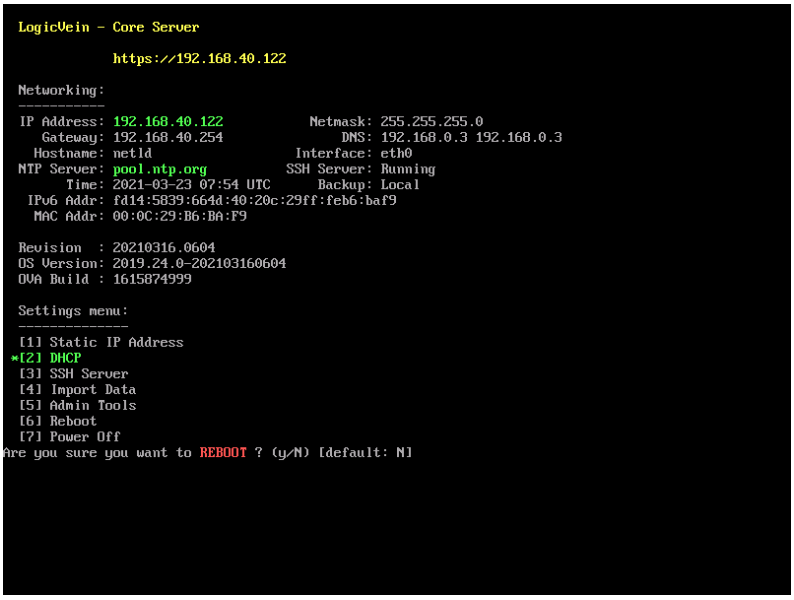
9 Reboot/Shutdown

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



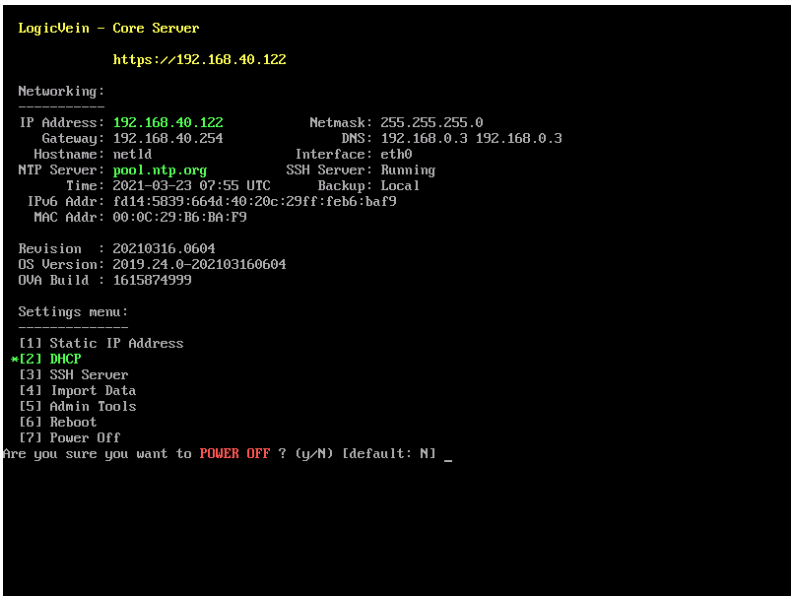
9.1 Restart procedure:

1. Click the [6] key on your keyboard.
2. Choose [Reboot].
3. Press the [Y] key on your keyboard to execute.



9.2 Shutdown procedure:

1. Click the [7] key on your keyboard.
2. Choose [Power Off].
3. Press the [Y] key on your keyboard to execute.

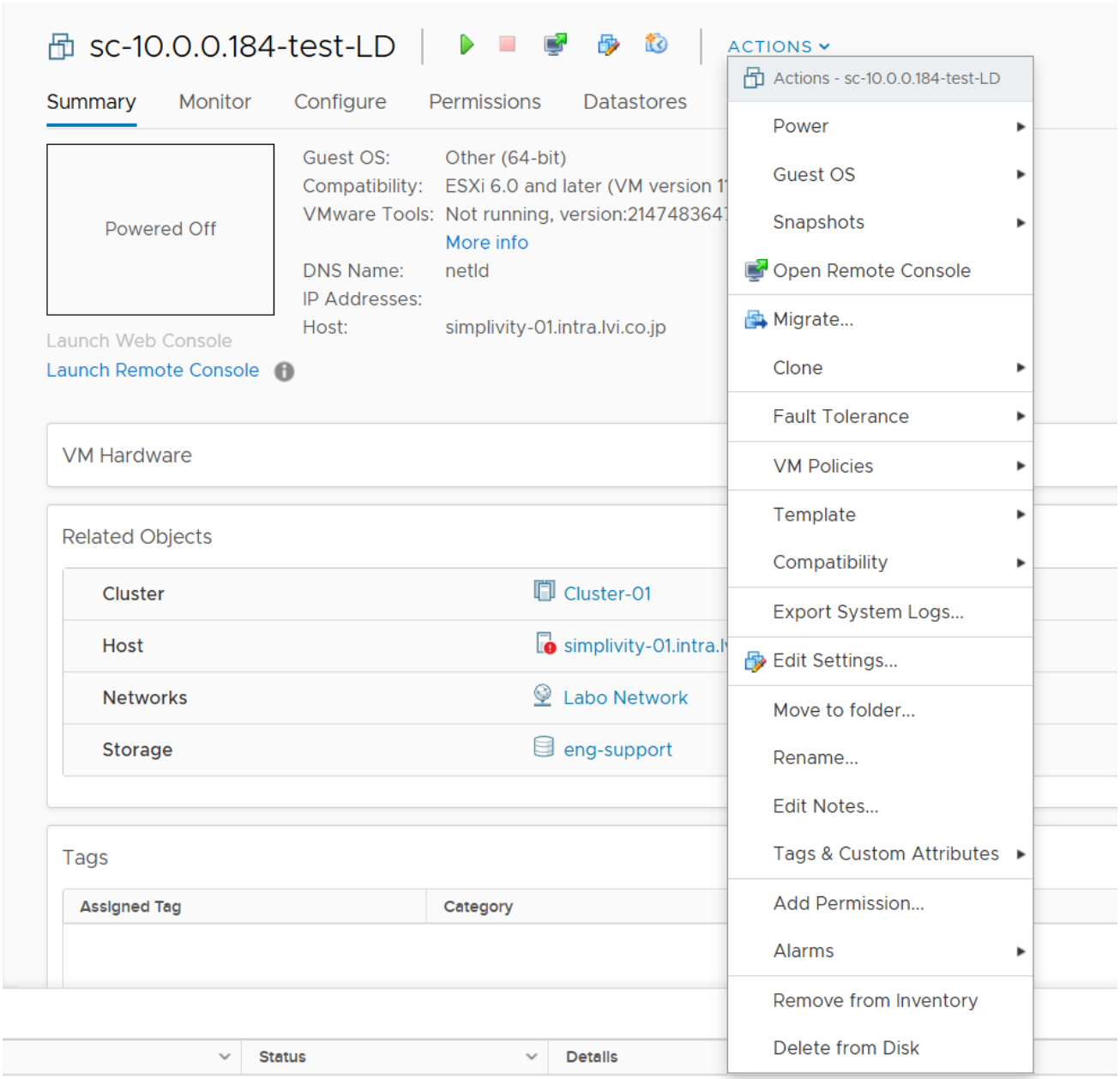


10 Uninstall

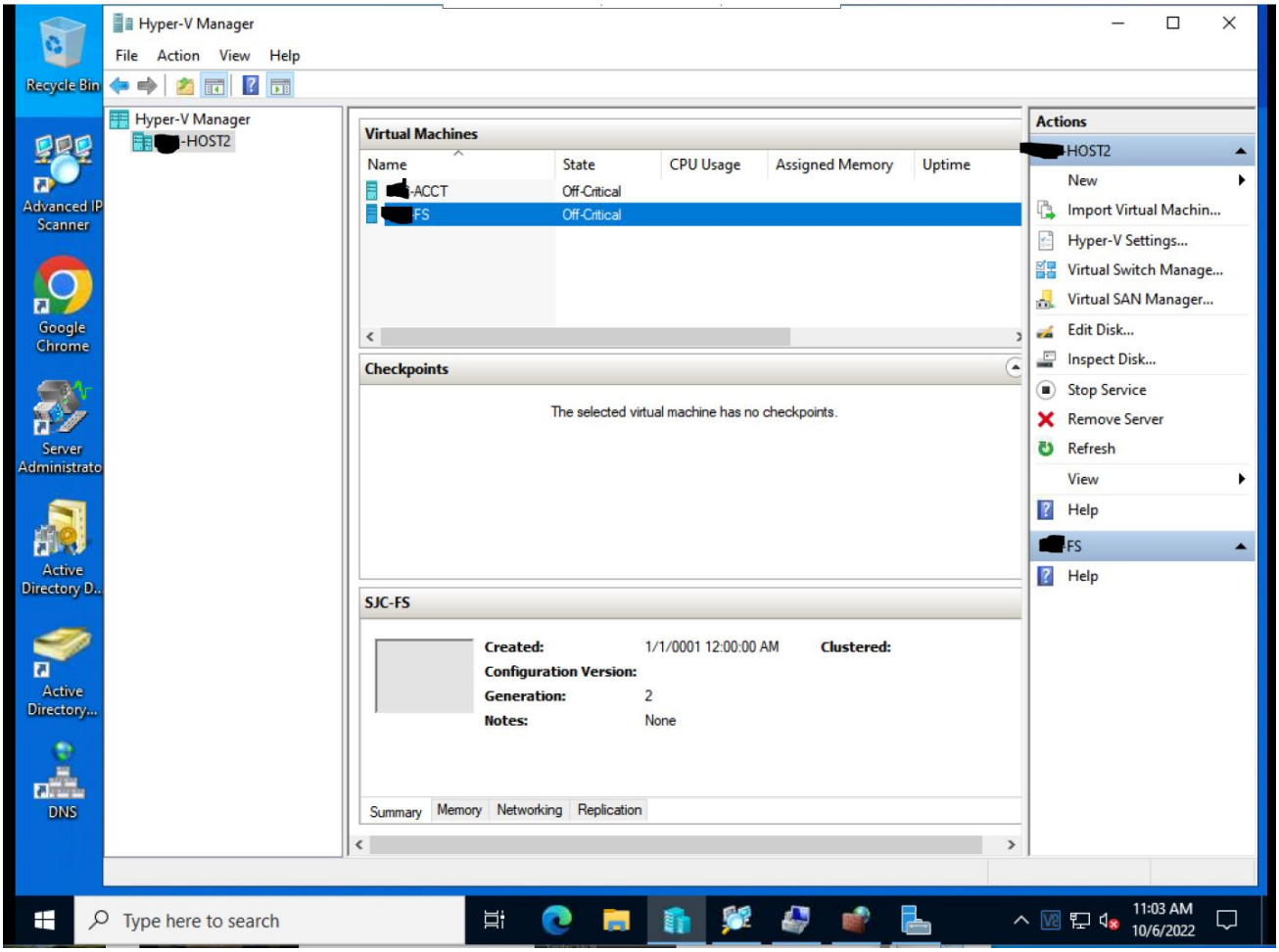
10.1 Uninstall

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

Example of deletion screen in VMware ESXi:



Example of deletion screen in Windows Hyper-V:



This completes the uninstallation of NetLD.

11 Smart Bridges (Optional)

NetLD supports two modes for the connection of Smart Bridges to the core server:

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

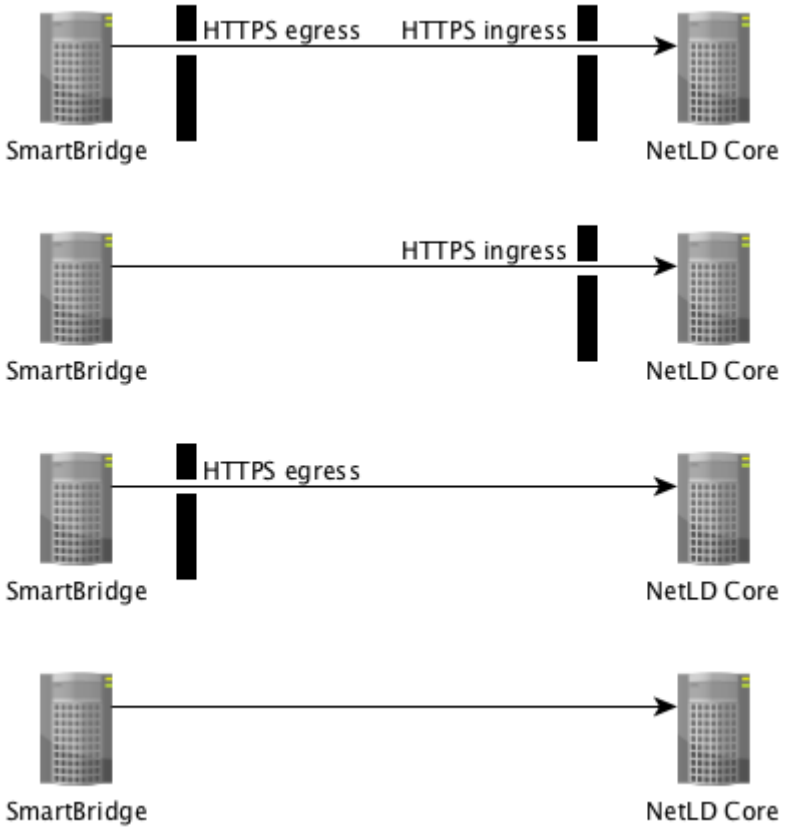
All connections are via HTTPS, so wire traffic is encrypted end-to-end.

11.1 Bridge-to-Server

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

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

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

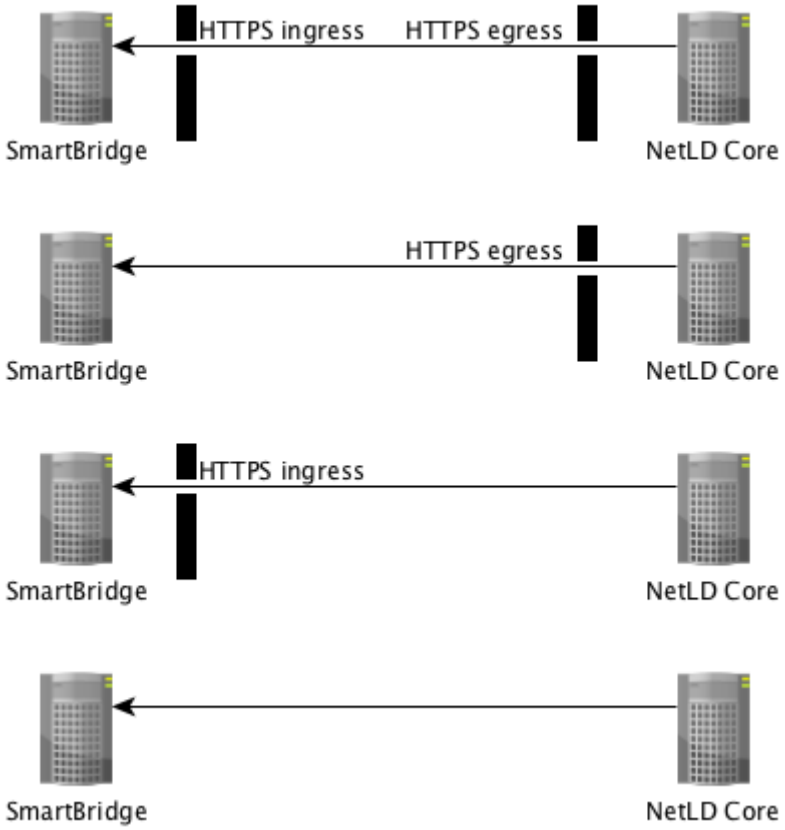


11.2 Server-to-Bridge

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

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

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



11.3 Connection Token

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

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

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

11.4 SmartBridge Installation

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

Example:

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

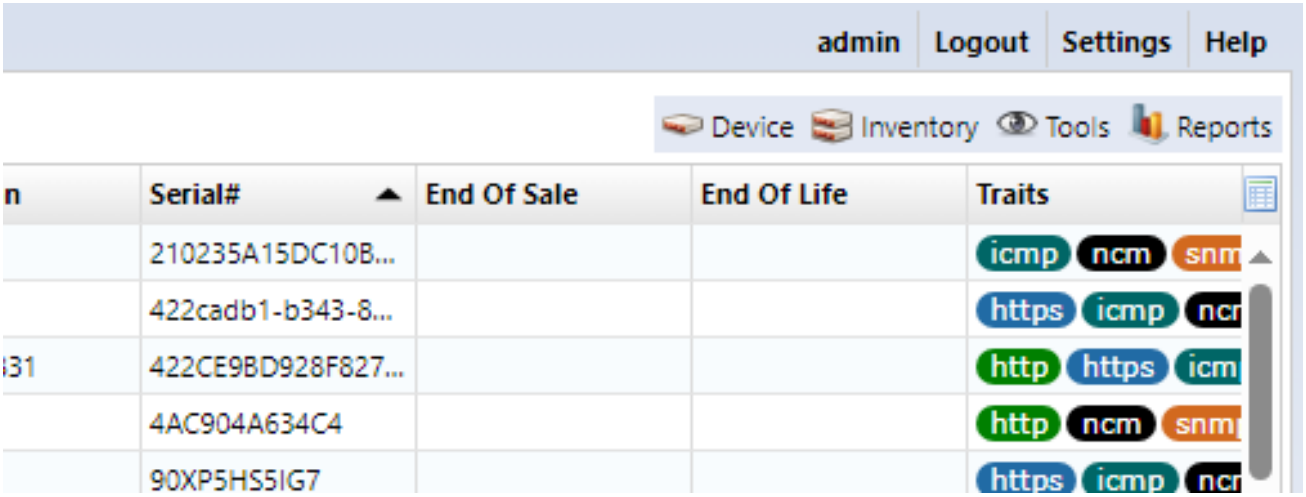
Smart bridge file name: `lvi-bridge-2024.03.0-202406180814-appliance.ova`

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

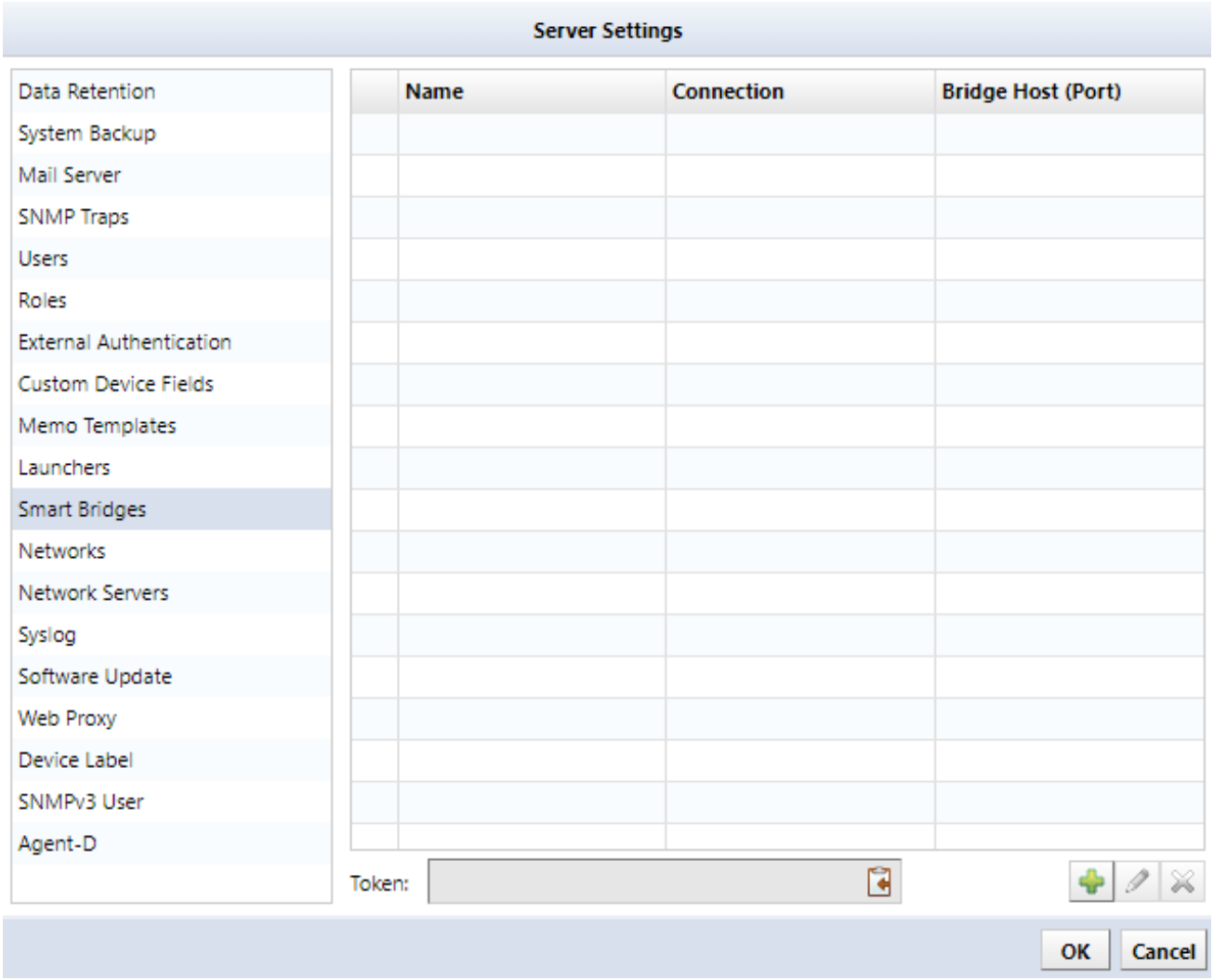
11.5 Add SmartBridge to core server

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

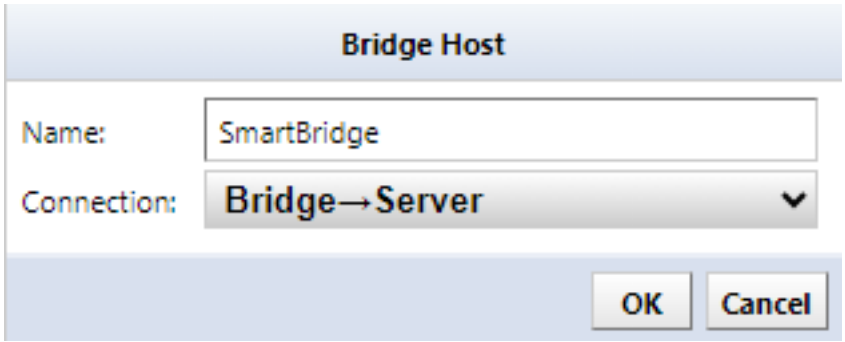
1. Login to the core server as an Administrator and click [Settings] in the Global Menu.



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

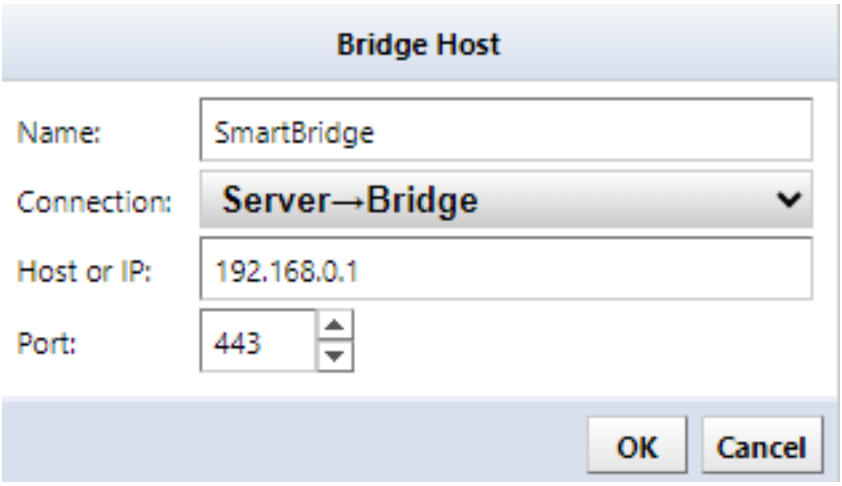


3. Enter the name for the Smart Bridge



4. Click [Connection].

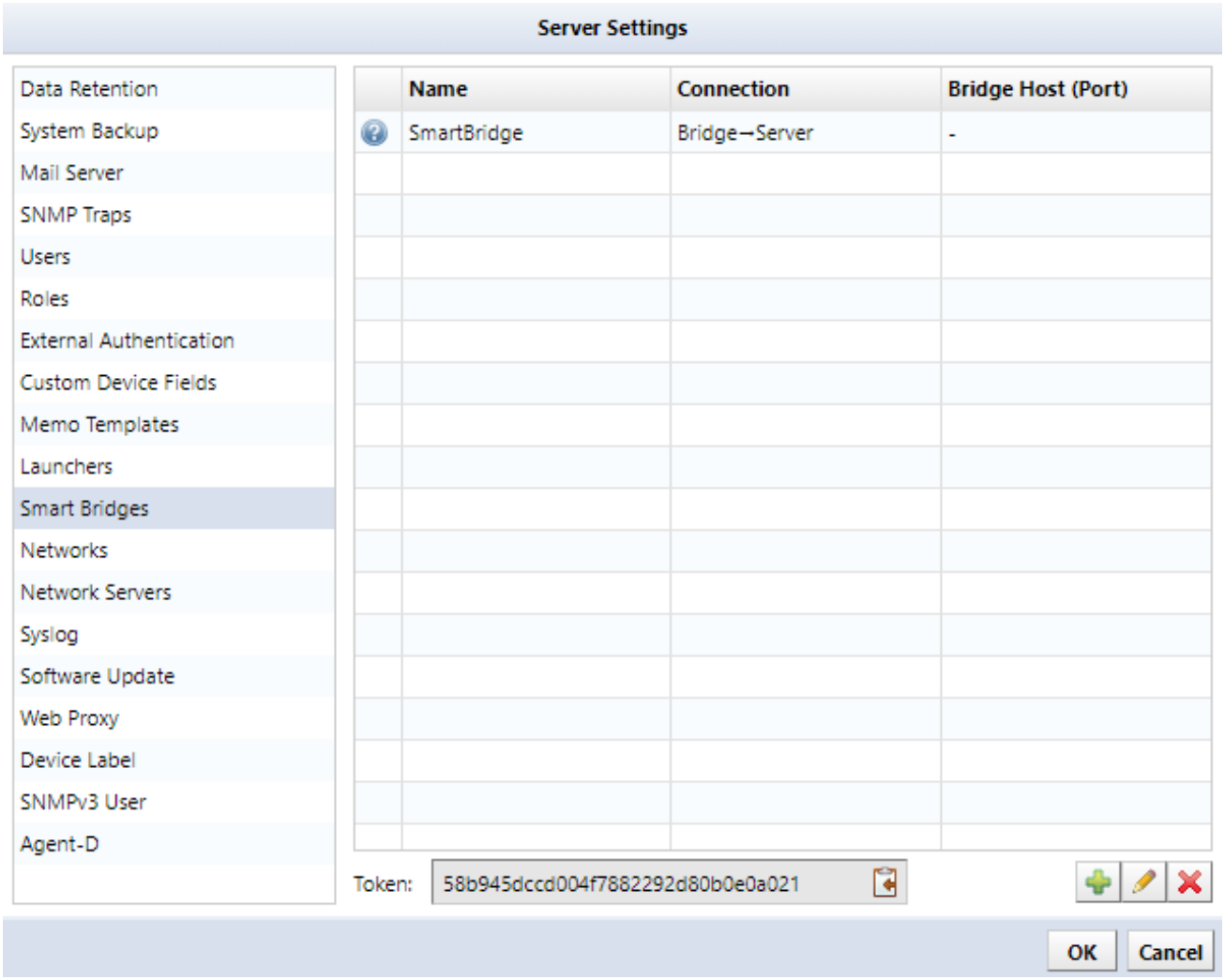
When you select [Server to Bridge], you have to enter a “Host or IP” address and “Port” for the bridge.



5. Click [OK].

6. Copy token.

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



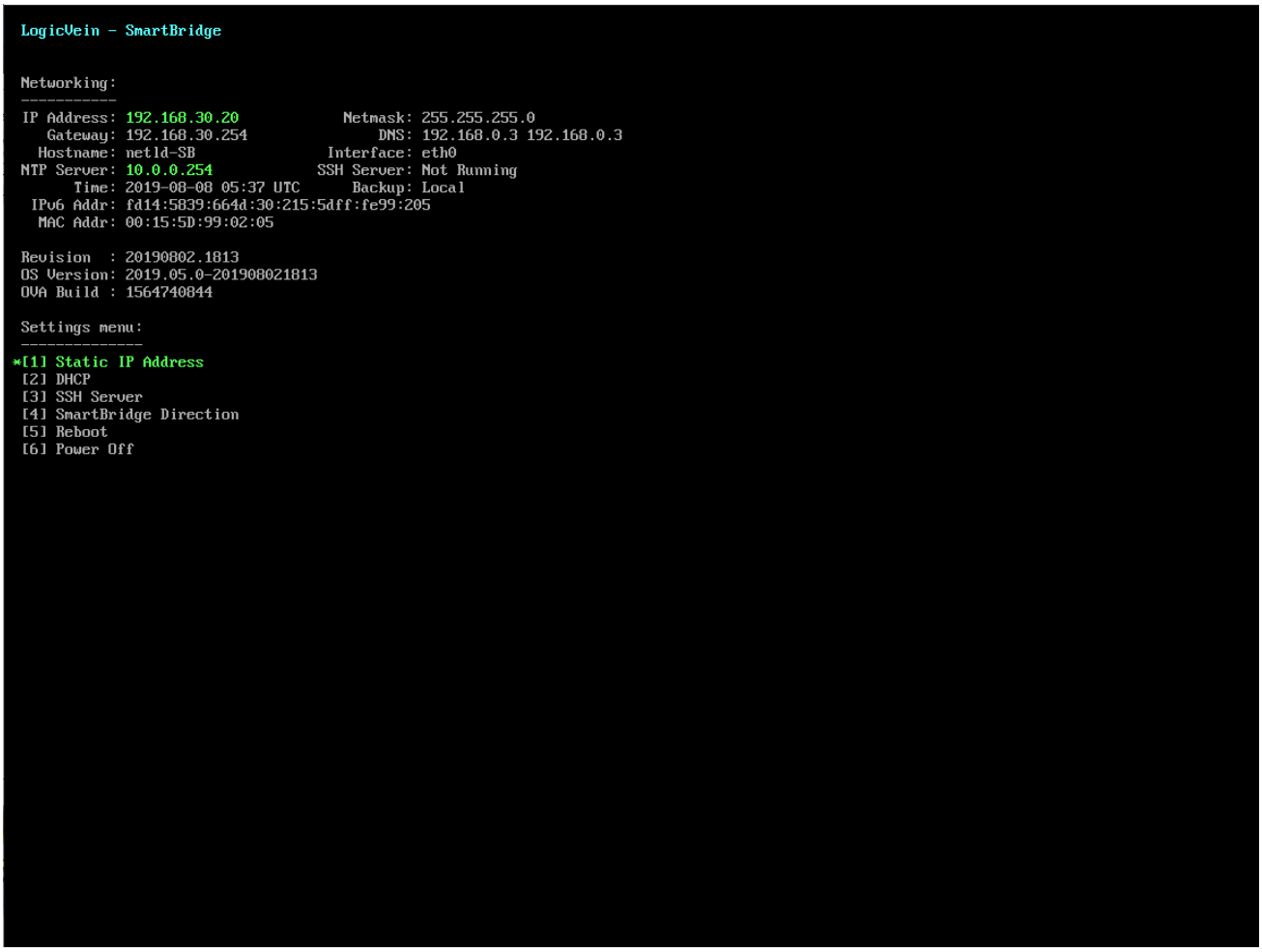
7. Click [OK].

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

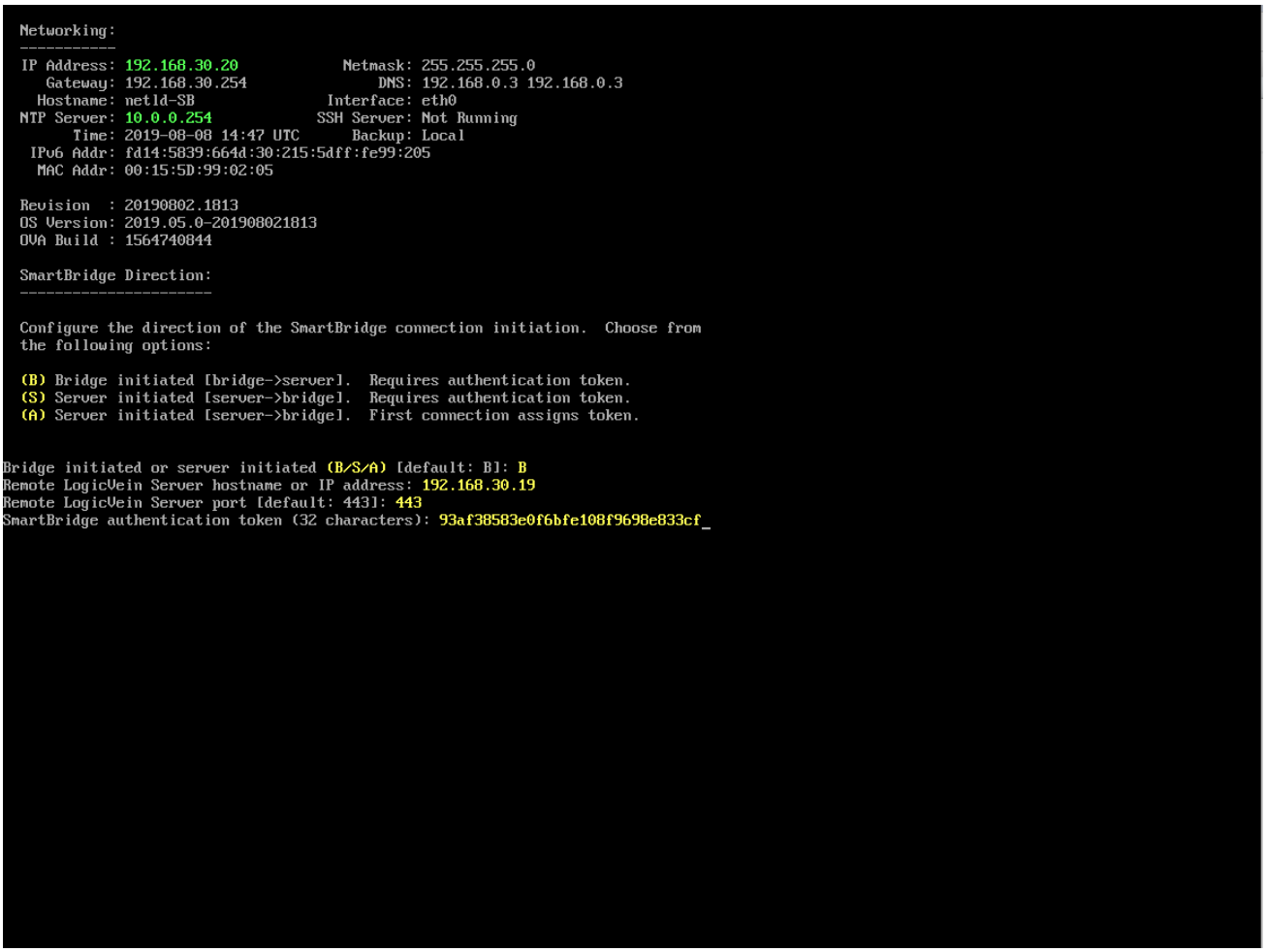
11.6 SmartBridge Settings

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

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



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



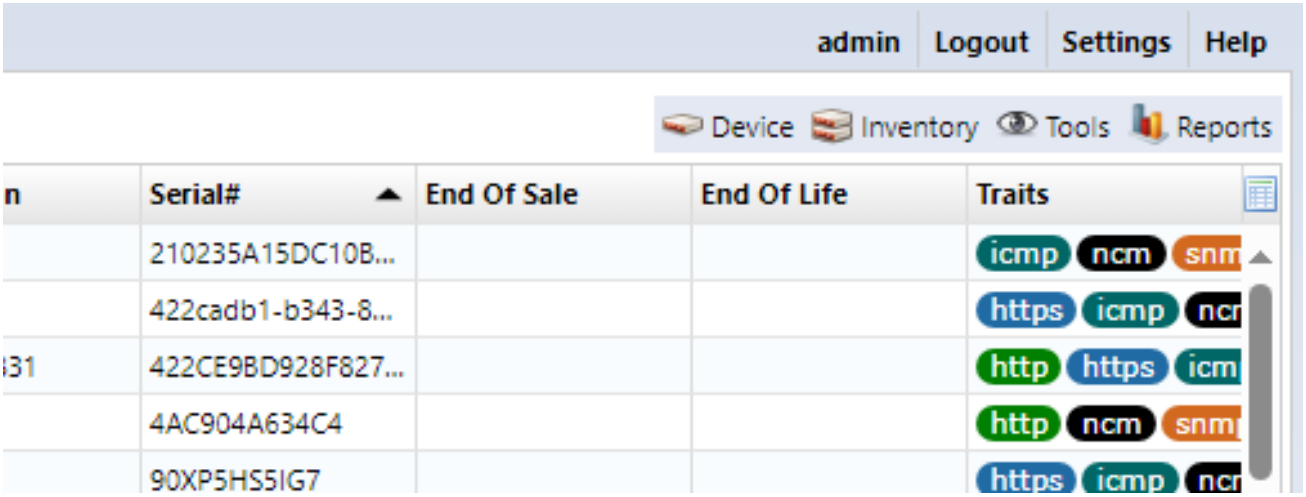
Project	Explanation	Keyboard Selction
Connection Initiation	Connection direction	
	Connect from Bridge to Server (with token)	[B]
	Connect from Server to Bridge (with token)	[S]
	Connect from Server to Bridge (without token)	[A]
Hostname or IP address	Core server (ThirdEye) IP address	`192.168.30.19`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

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

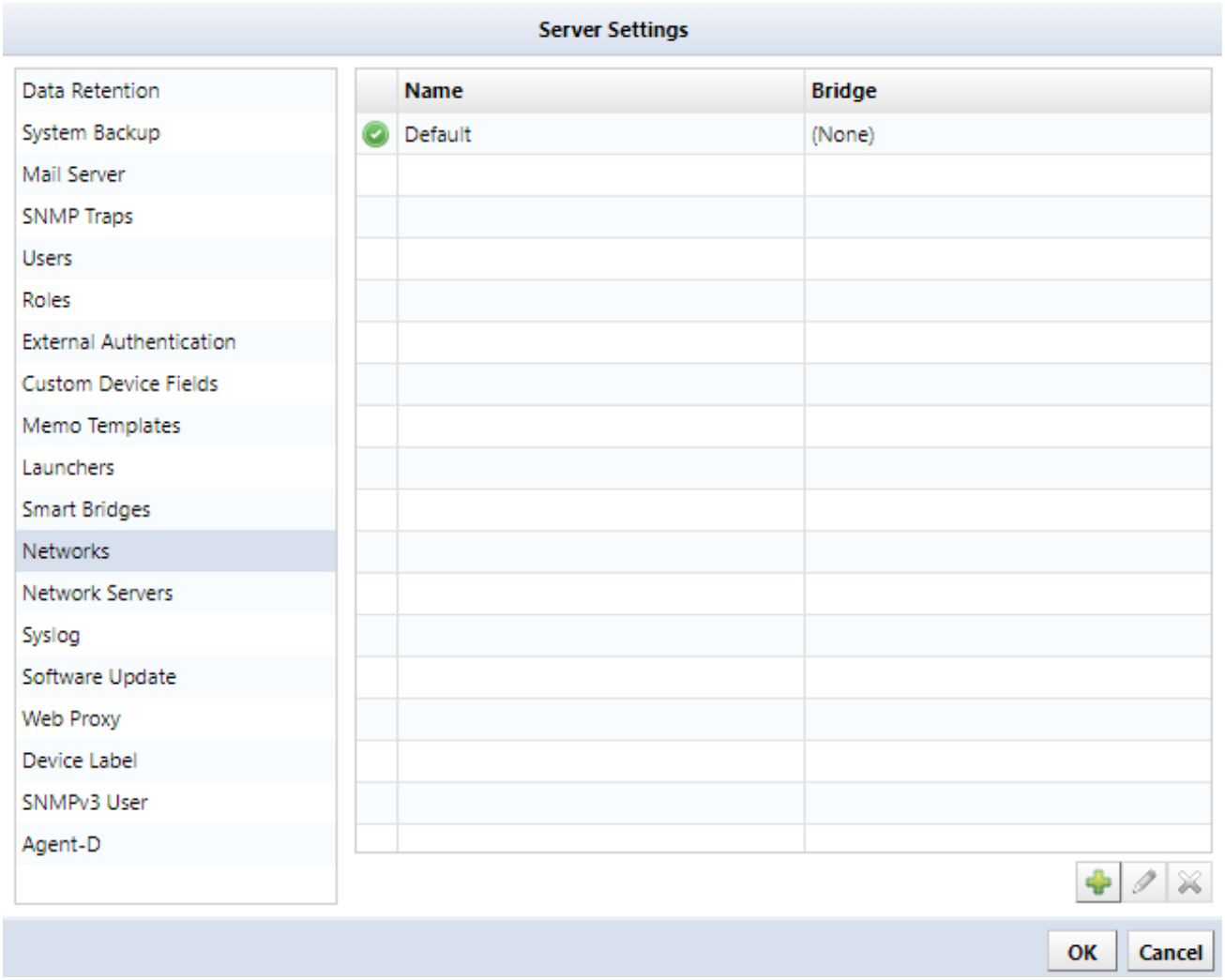
11.7 Managing Devices via SmartBridge

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

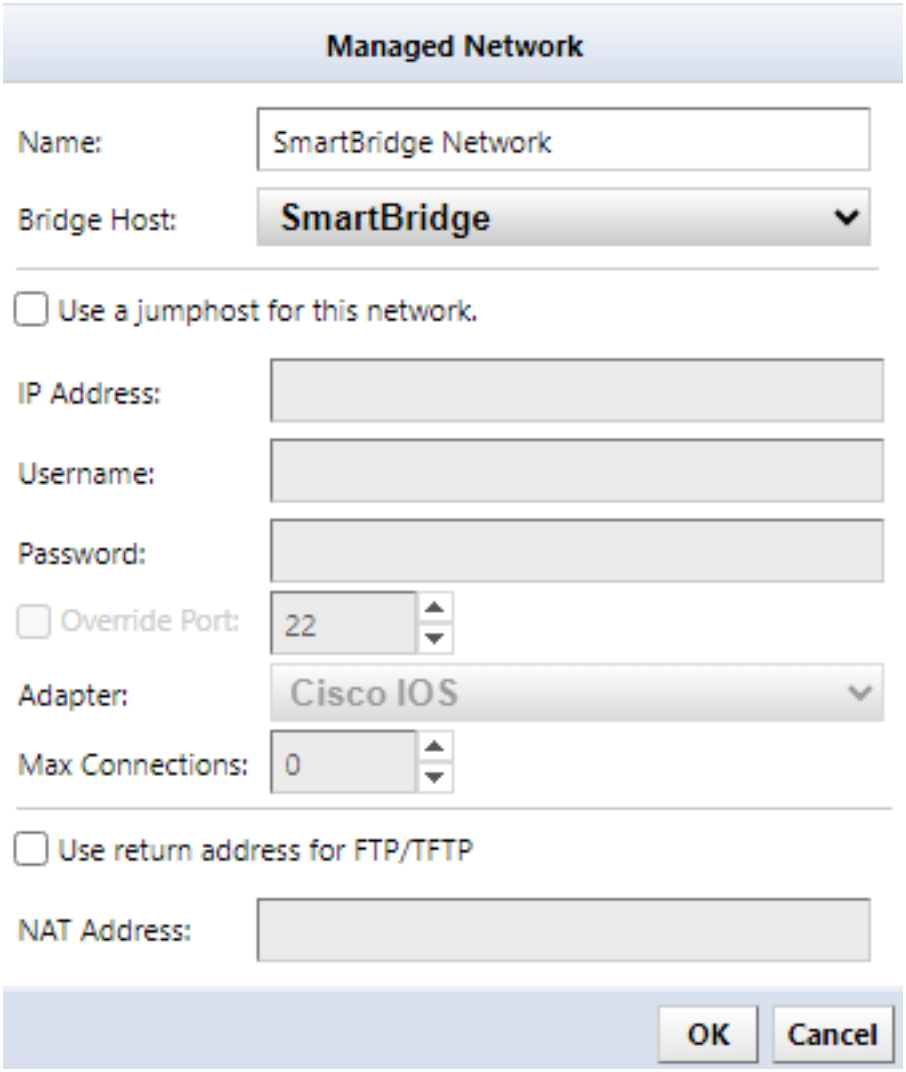
1. Click Settings.



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

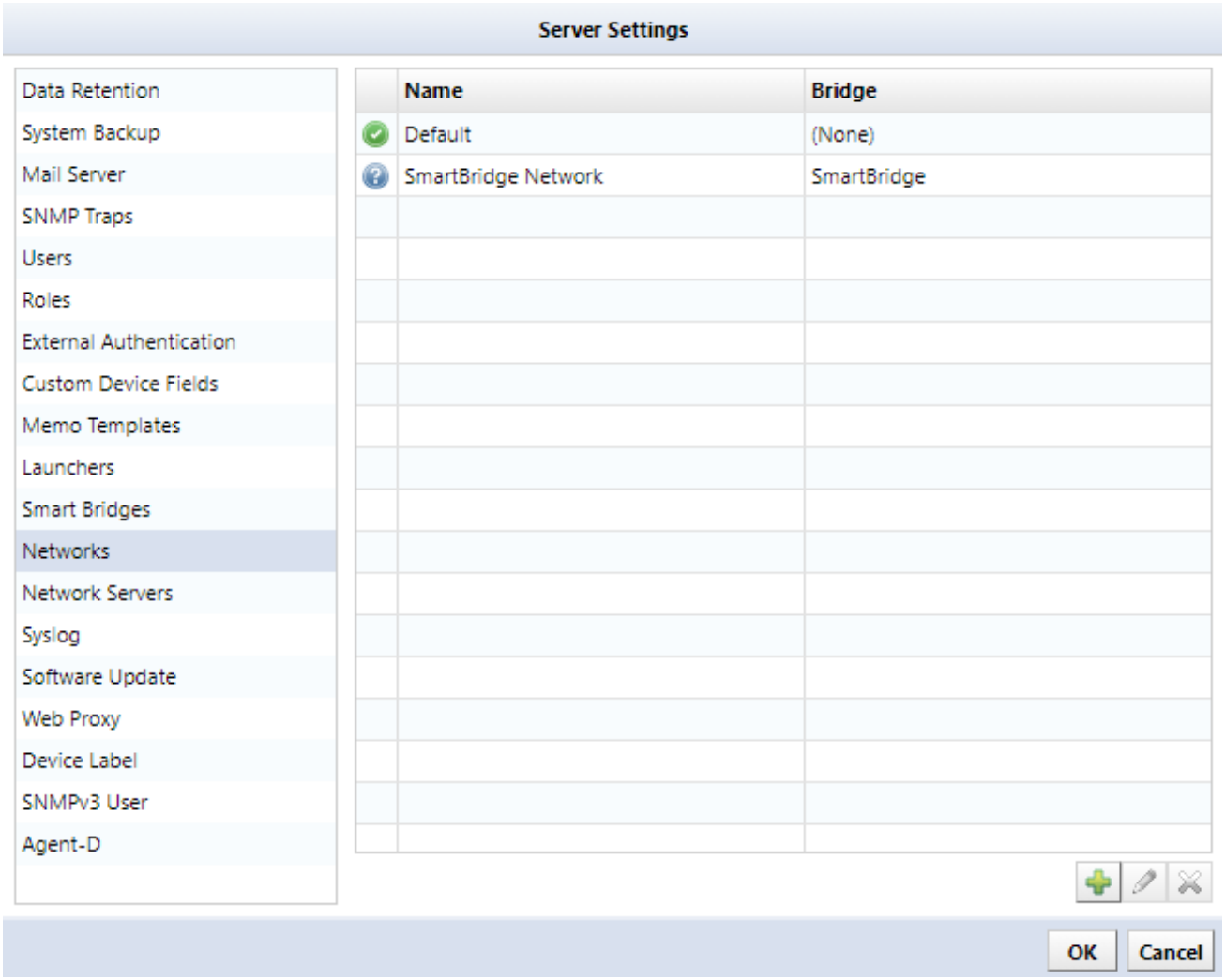


3. Enter a name for your network and select [Smart Bridge] in the “Bridge Host” field.

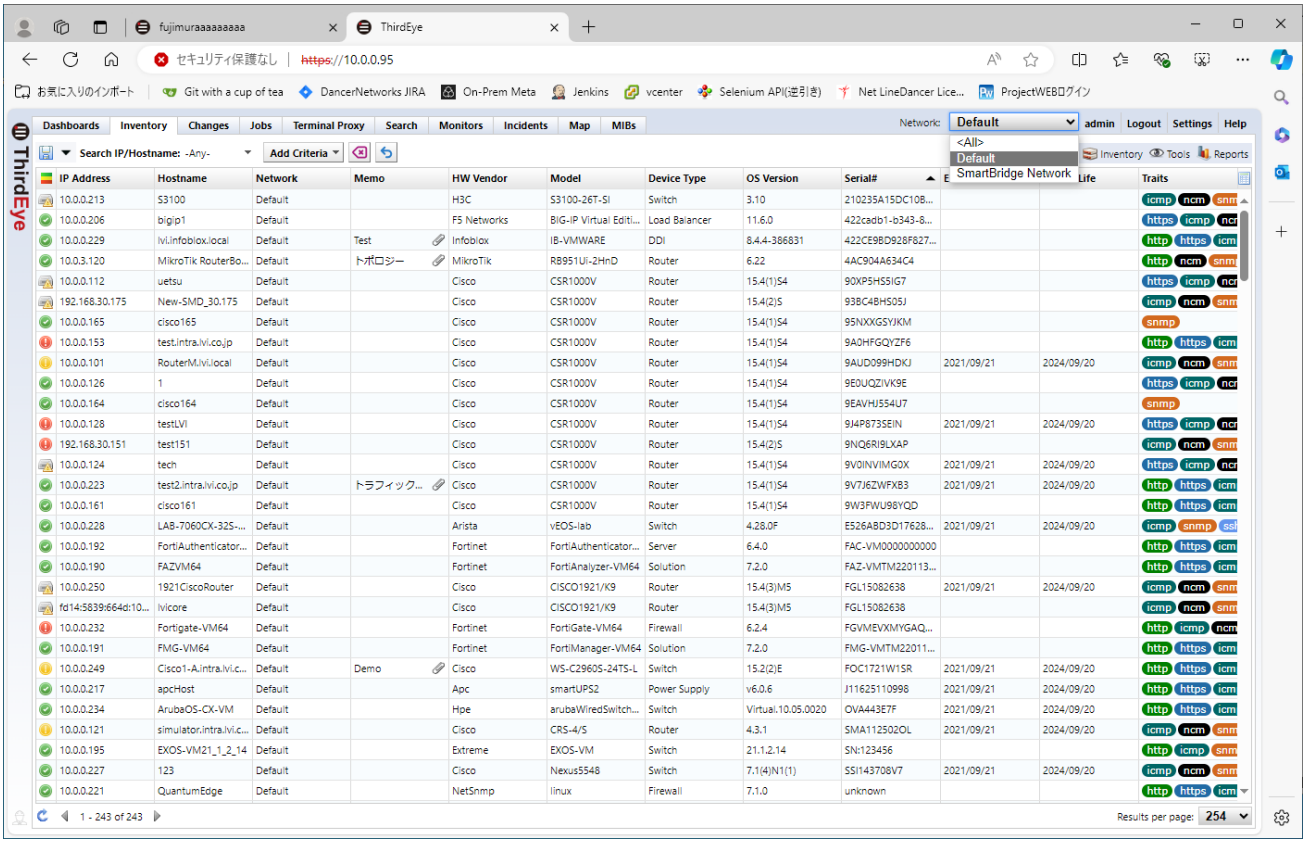


4. Click [OK]

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



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



12 Inquiries

If you have any problems or questions while using NetLD, please contact our support team:

LogicVein Support Desk Contact information: Email: support@logicvein.com

Before have the following information ready:

1. Product name
2. Product version information (including revisions)
3. Product serial number (NetLD license information)
4. Specific issue(s) and questions.
5. A screenshot of the issue (if possible).