



Contents

1	Intr	oduction
	1.1	About NetLD
	1.2	About NetLD edition
		1.2.1 NetLD Enterprise features:
	1.3	Environmental Settings
	1.4	List of ports used
2	Inst	allation
	2.1	Deployment to VMware ESXi
	2.2	Deployment to Windows Hyper-V
	2.3	Deploying to Linux KVM
	2.4	Deploying to Nutanix AHV+
	2.5	Deploy to Microsoft Azure
	2.6	Deploying to AWS
	2.7	Configuring Network Settings
	2.8	Apply the license
	2.9	Initial settings (detailed settings)
3	Log	in/Logout
	3.1	Log in
	3.2	Log out
1	Glo	bal Menu
5	Мат	nage Users
3	5.1	Create User Account
	5.2	Add permissions
	5.2	Add user
	5.4	Change user information
	5.5	Change password
	5.6	Setup two-factor authentication (2FA)
	5.0	5.6.1 Enable two-factor authentication
		5.6.2 Remove two-factor authentication
	57	
	5.7	5 5
		5.7.2 Active Directory
		5.7.3 SAML
		5.7.4 Use Local Authentication After Setting Up SAML Authentication
		5.7.5 Testing external authentication

5.10 Delete user 5.10 Delete user 6 Main tabs 6.1 Inventory 6.1.1 Inventory subtab 6.1.2 Add device 6.1.2 Add device 6.1.3 Check the Up/Down status of the device interface 6.1.4 Get Device Configuration 6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs 6.3 Jobs	62
 6 Main tabs 6.1 Inventory. 6.1.1 Inventory subtab 6.1.2 Add device 6.1.3 Check the Up/Down status of the device interface 6.1.4 Get Device Configuration 6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs 	62
 6.1 Inventory 6.1.1 Inventory subtab 6.1.2 Add device 6.1.3 Check the Up/Down status of the device interface 6.1.4 Get Device Configuration 6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs 	64
6.1.1Inventory subtab6.1.2Add device6.1.3Check the Up/Down status of the device interface6.1.4Get Device Configuration6.1.5Device Groups6.1.6Remove device6.2Changes6.3Jobs	65
6.1.2 Add device 6.1.3 Check the Up/Down status of the device interface 6.1.4 Get Device Configuration 6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs	66
 6.1.3 Check the Up/Down status of the device interface	66
6.1.4 Get Device Configuration 6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs	73
6.1.5 Device Groups 6.1.6 Remove device 6.2 Changes 6.3 Jobs	81
6.1.6 Remove device 6.2 Changes 6.3 Jobs	82
6.1.6 Remove device 6.2 Changes 6.3 Jobs	88
6.3 Jobs	95
	96
6.3.1 Job management	96
	96
6.3.2 Delete job	13
6.4 Terminal Proxy	14
	15
6.5 Search	20
6.5.1 Search subtabs	20
	22
6.6.1 Compliance Policy subtab	22
	23
6.6.3 Rule Sets subtab	25
6.6.4 Automatic remediation function	37
	54
	54
	56
6.7.3 DHCP server	57
6.7.4 Use an external DHCP server	60
6.7.5 Creating a template	61
6.7.6 Zero-Touch self-recovery	.67
-	69
•	70
	71
-	71
5	72
	85
1	88
	89

6.9	Draft c	onfiguration	191
	6.9.1	Creating a draft configuration	191
	6.9.2	Import draft configuration from plain text	193
	6.9.3	Export a draft	193
	6.9.4	Delete a draft	193
	6.9.5	Compariing draft configurations	194
	6.9.6	Apply draft configuration to devices	194
	6.9.7	Configure SNMP trap sending	195
6.10	Viewin	g tools	199
	6.10.1	DNS lookup	199
	6.10.2	IOS Show commands	200
	6.10.3	IP Routing table	201
	6.10.4	Ping	201
	6.10.5	SNMP System Info	202
	6.10.6	Interface Brief	202
	6.10.7	Traceroute	202
	6.10.8	Port Scan	203
	6.10.9	Live ARP Table	203
6.11	Change	e tools	204
6.12	Change	e Tools	204
	6.12.1	Command Runner	206
	6.12.2	Enable or Disable Interfaces	207
	6.12.3	Login Banner (MOTD)	207
	6.12.4	Name Servers Manager	208
	6.12.5	NTP Servers	210
	6.12.6	Port VLAN Assignment	210
	6.12.7	SNMP community string	211
	6.12.8	SNMP Trap Hosts	211
	6.12.9	Syslog Hosts	211
	6.12.10	AlliedTelesis OS software distribution	212
	6.12.11	ASA OS software distribution	213
	6.12.12	2 IOS software distribution	214
	6.12.13	B Manage OS image	215
	6.12.14	NEC WA software distribution	216
	6.12.15	Retrieve OS image file	216
	6.12.16	Yamaha RT Firmware Distribution	217
	6.12.17	Add Static Route	219
	6.12.18	B Delete Static Route	219
	6.12.19	Add User Account	219
	6.12.20	Change Enable Password	220

		6.12.21 Changing Local User Password	220
		6.12.22 Change VTY Password	221
		6.12.23 Delete User Account	221
		6.12.24 Command Runner	222
		6.12.25 Enable or Disable Interfaces	223
		6.12.26 Login Banner (MOTD)	223
		6.12.27 Name Servers Manager	224
		6.12.28 NTP Servers	226
		6.12.29 Port VLAN Assignment	226
		6.12.30 SNMP Community Strings	227
		6.12.31 SNMP Trap Hosts	227
		6.12.32 Syslog Hosts	227
		6.12.33 AlliedTelesis OS software distribution	228
		6.12.34 ASA OS software distribution	229
		6.12.35 IOS software distribution	230
		6.12.36 Manage OS Images	231
		6.12.37 NEC WA software distribution	232
		6.12.38 Retrieve OS image files	232
		6.12.39 Yamaha RT Firmware Distribution	233
		6.12.40 Add Static Route	235
		6.12.41 Delete Static Route	235
		6.12.42 Add User Account	235
		6.12.43 Change Enable Password	235
		6.12.44 Changing Local User Password	236
		6.12.45 Change VTY Password	237
		6.12.46 Delete User Account	237
	6.13	Change advisor	238
		6.13.1 Change advisor setup	238
		6.13.2 Execute commands using change advisor	239
	6.14	Smart change	240
		6.14.1 Create a smart change job	240
	6.15	Device EOS/EOL management	246
	6.16	Change data retention period	247
7	U A 4	(Antivo/Standby)	248
/	н А (7.1	(Active/Standby) Prerequisites	248 248
	7.1	Restrictions	248 248
	7.2		248 249
	7.3 7.4	Settings	249 249
	7.4 7.5		249 257
	1.5	Confirm status	231

	7.6	Cases for Reconfiguration	260
7.7 Failover		Failover	260
		7.7.1 Manual failover	260
		7.7.2 Auto failover	263
	7.8	Automatic configuration	265
		7.8.1 Prerequisites	265
	7.9	Wireless Lan Controller Monitoring	269
		7.9.1 Setup and configuration	269
		7.9.2 Viewing clients on a Map	272
8	Syste	em backup/restore	273
	8.1	Perform system backup automatically	273
	8.2	Perform a manual system backup	275
	8.3	Change the number of system backups retained	277
	8.4	Save to external storage	278
	8.5	Create system backup zip file	283
	8.6	Restore system backup from zip file	283
9	Rebo	oot/Shutdown	287
	9.1	Restart procedure:	287
	9.1 9.2	Restart procedure:	
10		Shutdown procedure:	287
10	9.2 Unin	Shutdown procedure:	287 288
	9.2 Unin 10.1	Shutdown procedure:	287 288 289
	9.2 Unin 10.1 Sma	Shutdown procedure:	287 288 289 289 291
	9.2Unin10.1Sma11.1	Shutdown procedure: Install Uninstall	287 288 289 289
	9.2Unin10.1Sma11.1	Shutdown procedure: nstall Uninstall Uninstall art Bridges (Optional) Bridge-to-Server Server-to-Bridge	287 288 289 289 291 291
	 9.2 Unim 10.1 Sma 11.1 11.2 11.3 	Shutdown procedure: nstall Uninstall uninstall ort Bridges (Optional) Bridge-to-Server Server-to-Bridge Connection Token	287 288 289 289 291 291 292
	 9.2 Unin 10.1 Sma 11.1 11.2 11.3 11.4 	Shutdown procedure: Install Uninstall Int Bridges (Optional) Bridge-to-Server Server-to-Bridge Connection Token SmartBridge Installation	 287 288 289 289 291 292 293
	 9.2 Unin 10.1 Sma 11.1 11.2 11.3 11.4 	Shutdown procedure: nstall Uninstall Uninstall Server-to-Bridge Connection Token SmartBridge Installation Add SmartBridge to core server	287 288 289 289 291 291 292 293 293
	 9.2 Unin 10.1 Sma 11.1 11.2 11.3 11.4 11.5 11.6 	Shutdown procedure: nstall Uninstall Uninstall Server-to-Bridge Connection Token SmartBridge Installation Add SmartBridge to core server	287 288 289 289 291 291 292 293 293 293

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	$NetLD \leftarrow Destination$
	68	DHCP	UDP	$NetLD \rightarrow Destination$
	80	HTTP	ТСР	$NetLD \leftarrow Destination$
	69	TFTP	UDP	$NetLD \leftarrow Destination$
	-	ICMP	-	$NetLD \leftarrow Destination$
Automatic Discovery	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$
	161	SNMP	UDP	$NetLD \rightarrow Destination$
	-	ICMP	-	$NetLD \rightarrow Destination$
Send Settings (Restore Configuration)	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$
	69	TFTP	UDP	$NetLD \leftarrow Destination$
	20, 21	FTP	ТСР	$NetLD \leftarrow Destination$
Settings Using Modification Tools	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$
Trap Sending	162	SNMP	UDP	$NetLD \rightarrow Destination$
SNMP Monitoring	161	SNMP	UDP	$NetLD \rightarrow Destination$
Trap Reception	162	SNMP	UDP	$NetLD \leftarrow Destination$
Real-time change detection	514	Syslog	UDP	NetLD ← Destination
Backup*	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$
	161	SNMP	UDP	$NetLD \rightarrow Destination$
	69	TFTP	UDP	$NetLD \leftarrow Destination$
	20, 21	FTP	ТСР	$NetLD \leftarrow Destination$
Terminal proxy	2222, 443	SSH or HTTPS	ТСР	NetLD ← Client PC
	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$
Web Terminal	443	HTTPS	ТСР	$NetLD \leftarrow Client (GUI)$
	22, 23	SSH, Telnet	ТСР	$NetLD \rightarrow Destination$

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

vm ware [®] ESXi [®]			
Navigator		🔂 LVISupport.test - Virtual Machines	
✓ Host Manage		😭 Create / Register VM 📑 Console 🕨 Power on 🔳 Power off 💶 Sus	spend CRefresh
Monitor		Virtual machine	~ Status
📲 Virtual Machines	2	B netld-core-2016.02.0201709222101-appliance	Normal

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

🔁 New virtual machine		
 Select creation type Select OVF and VMDK files Select storage 	Select creation type How would you like to create a Virtual Machine?	
4 License agreements 5 Deployment options 6 Additional settings	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
7 Ready to complete	Register an existing virtual machine	
vm ware*		
		Back Next Finish Cancel

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

20 New virtual machine - NetLD-Virtual Appliance				
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy Enter a name for the virtual machine. NetLD-Virtual Appliance Virtual machine names can contain up to 80 characters and they must be unique within each ESXI instance.			
	× 🟧 netid-core-2016.02.0201712061116-appliance.ova			
vm ware				
	Back Next Finish Cancel			

4. Select your storage and click [Next].

Select creation type	Select storage						
Select OVF and VMDK files Select storage	Select the datastore in which to store the	configuration and dis	k files.				
License agreements Deployment options	The following datastores are accessible t virtual machine configuration files and all		esource that you	selected. Sele	ct the destinatio	n datastore	for t
Additional settings Ready to complete	Name	 Capacity 	Free ~	Туре ~	Thin pro ~	Access	~
Ready to complete	Datastore(192.168.30.105)	105.07 GB	93.52 GB	NFS	Supported	Single	
	datastore1	32.5 GB	31.55 GB	VMFS5	Supported	Single	
						2 ite	ems
vm ware [.]							

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

 1 Select creation type
 2 Select VGR and VMDK Tiles
 1 Select VGR and VMDK Tiles</p
- 5. Select the network and disk provisioning you want to deploy and click [Next].

6. Click [Finish].

/F and VMDK files Review your set	omplete	finishing the wizard		
orage ent options				
complete		Unknown		
VM Name		NetLD-Virtual Appliance		
Disks		disk1.vmdk,disk2.vmdk		
Datastore		Datastore(192.168.30.105)		
Provisioning	уре	Thin		
Network map	pings	NAT: VM Network		
Guest OS Na	me	Other Linux 64-Bit		
	to not refresh your bro	wwser while this VM is being depl	oyed.	

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].

Quid	:k Create							
New		>	Virtual Machine_				Actions	
	ort Virtual Machine er-V Settings		Hard Disk Floppy Disk	CPU Usage	Assigned Memory	Uptirr	WRP10	Create
Virtu	ual Switch Manager ual SAN Manager		No virtu	al machines were found on	this server.		New	t Virtual Machine
	Disk ect Disk	point	5		-	_		V Settings I Switch Manager
	o Service love Server			No virtual machine selecte	d.			il SAN Manager
Refr		-						ct Disk
		Details					F	ve Server
				No item selected.			View	
							Help	

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

New Virtual Machine Wiza	ard	×
Specify Name	ne and Location	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you ear identify this virtual machine, such as the name of the guest operating system or workload. Name: netLD 18 You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server. Store the virtual machine in a different location	sily
Summary	Location: C:Wrtual Machines Browse.	
	< Previous Next > Finish Cance	1

3. Select "Generation 1" and click [Next].

New Virtual Machine Wiz	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 Choose the generation of this virtual machine. Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V. Generation 2 This virtual machine generation provides support for newer virtualization features, has UEFI-based. More a virtual machine has been created, you cannot change its generation. More about virtual machine generation support
	More about virtual machine generation support < Previous

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

New Virtual Machine Wiza		×
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 8192 MB Use Dynamic Memory for this virtual machine. When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.	
	< Previous Next > Finish Cancel	

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

Configure N		×
Before You Begin Specify Name and Location Specify Generation	Each new virtual machine includes a network adapter. You can configure the network adapter to use virtual switch, or it can remain disconnected. Connection: netLD	e a
Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary		
	< Previous Next > Finish Cancel	

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

Before You Begin Specify Name and Location Specify Generation		requires storage so that you can install an operating system onfigure it later by modifying the virtual machine's properties ual hard disk	
Assign Memory Configure Networking		in to create a VHDX dynamically expanding virtual hard disk.	
Connect Virtual Hard Disk	Name: Location:	netLD 18.vhdx C:\Virtual Machines\netLD 18\Virtual Hard Disks\	Browse
Summary	Size:	127 GB (Maximum: 64 TB)	
	-	ng virtual hard disk In to attach an existing virtual hard disk, either VHD or VHDX	format.
	Location:	C:\Users\WPalmer\Documents\Virtual Machines\	Browse
	Attach a virtu	ual hard disk later	

7. Click [Finish].

New Virtual Machine Wiz	ard the New Virtual Machine Wizard	×
Completing Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Summary	the New Virtual Machine Wizard You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: netLD 18 Generation: Generation 1 Memory: 8192 MB Network: netLD Hard Disk: None	
	< Previous Next > Finish Cancel	

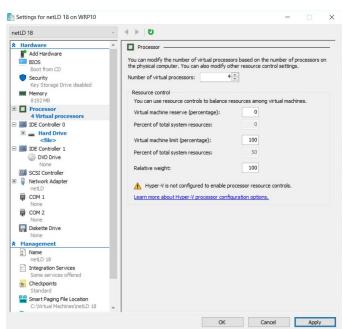
The virtual machine will now be created.

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

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

Hyper-V Manager	Machines			A	tions	
WRP10 Virtual Name	State	CPU Usage	Assigned Memory	Upti	RP10 Quick Create	•
	Connect				New	۲
	Settings			C	Import Virtual Machine	
Check	Start Checkpoint	-	_			
	Move Export Rename	ed virtual machine has no	checkpoints.	-	Edit Disk	
netLD	Delete	_		=		
	Created: Configuration Ver	9/26/2018 7:47:56	PM Clustered: N		Refresh View	•
	Generation: Notes:	1 None		2	Help	•
	notes			-		
					Settings	
Summ	ry Memory Networking				Start	
				>	Checkpoint	

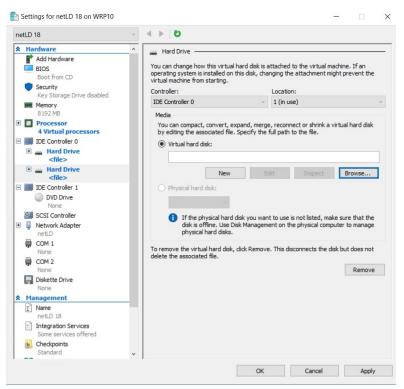
9. Select "Processor" and change [Number of virtual processors].



10. Select "IDE Controller 0" and click [Add].

netLD 18	5 4 ► ~	
hetLD 18 Add Hardware Add Hardware BIOS Boot from CD Scurity Key Storage Drive disabled Memory 8192 MB Processor 1 Virtual processor 0 DID Controller 1 0 DID Controller 1 0 DID Drive None	DE Controller You can add hard drives and CD/DVD drives to your IDE co Select the type of drive you want to attach to the controll Israd Drive DVD Drive You can configure a hard drive to use a virtual hard disk or	er and then dick Add.
None SCSI Controller Vetwork Adapter netLD COM 1 None COM 2 None Molecte Drive None Management Name netLD 18 Integration Services Some services offered Standard Standard Standard Standard	you attach the drive to the controller.	

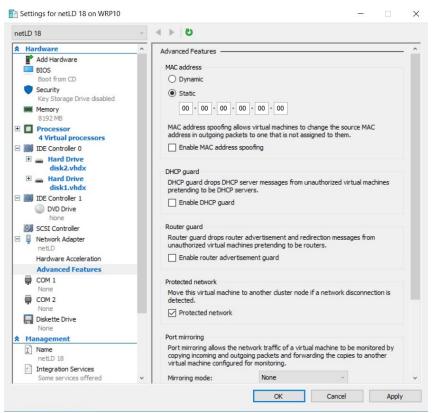
11. Click [Browse].



12. Add "disk1" and click [OK].

w folde	ir				8
^	Name	Date modified	Туре	Size	
	Virtual Machines	9/26/2018 7:47 PM	File folder		
g€	📥 disk1.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	1,810,432 KB	
	disk2.vhdx	9/27/2018 9:42 AM	Hard Disk Image File	8,192 KB	

- 13. Repeat steps 8 to 12 to add "disk2.vhdx".
- 14. Click [OK].



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

	AMIs (20) AWS Marketplace AMIs (839) Community AMIs (1) ted by me AWS & trusted third-party AMIs Published by anyone	
Refine results	lvi-core (1 filtered, 1 unfiltered)	(1 >
Clear all filters	Community AMIs Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.	t
Linux/Unix All Linux/Unix Amazon Linux CentOS Debian Fedora	Ivi-core-2024.03.0-202406180814 Select ami-God9b6ea84ec4af8f Vi-core-2024.03.0-202405180814 Select Vi-core-2024.03.0-202405180814 Owner: 511691617191 Publish date: 2024-06-19 Root device type: ebs Virtualization: hvm DNA enabled: Ves	t

- 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.

🗗 44, 4946 ×	
LogicVein - Core Server	
https://	
Networking:	
IP Address: Gateway: Hostname: netld NTP Server: pool.ntp.org NTPD Not Runni Time: 2019-01-15 09:	Netmask: DNS: Interface: eth0 SSH Server: Not Running ng 20 UTC
Revision : 20181006.0406 OS Version: 2017.02.020181 OVA Build : 1538767061	0060406
Settings menu:	
 Static IP Address II) Static IP Address II) SOFT Inport Data Isoport Data Set up Naster Set up Naster Set up Slave Reboot B) Power Off 	

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

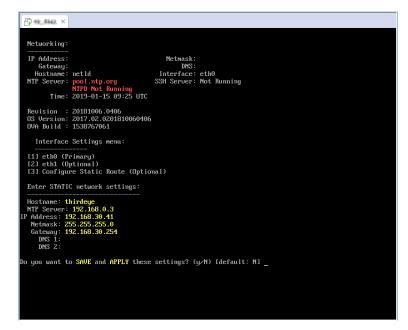
同執 約翰 ×	
Networking:	
IP Address: Netmask: Gateway: DNS:	
Gateway: DNS: Hostname: netld Interface: eth0	
NTP Server: pool.ntp.org SSH Server: Not Running	
NTPD Not Running Time: 2019-01-15 09:27 UTC	
11me: 2015-01-12 05-27 010	
Revision : 20181006.0406	
OS Version: 2017.02.0201810060406 OVA Build : 1538767061	
Interface Settings menu:	
[1] eth0 (Primary)	
[2] eth1 (Optional)	
[3] Configure Static Route (Optional)	
-	

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

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

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

Admin User			
The email address used by the admin user.	Email:		
The login password used by the admin of the system.	Password:		
	Confirm Password:		
erver Default Locale			
The language used to send emails, load out of the box monitors and rulesets.	Language:	🔜 English 👻	
The timezone used when sending emails.	Timezone:	(GMT+09:00) Tokyo	~
	Timezone.	(Gim1+03.00) Tokyo	
erver	THREE OFFE		
-	Server Name:	Net LineDancer	
ierver			
erver The name used when the browser tab should be shown with specific name. The Hostname or Ip Address used to access the site. This could be an internal Ip	Server Name:	Net LineDancer	
erver The name used when the browser tab should be shown with specific name. The Hostname or Ip Address used to access the site. This could be an internal Ip Address or Hostname.	Server Name:	Net LineDancer	
The name used when the browser tab should be shown with specific name. The Hostname or Ip Address used to access the site. This could be an internal Ip Address or Hostname.	Server Name: Hostname/IP Address:	Net LineDancer 192.168.223.133	
ierver The name used when the browser tab should be shown with specific name. The Hostname or Ip Address used to access the site. This could be an internal Ip Address or Hostname. Mail Server The host name used as the hostname of email server.	Server Name: Hostname/IP Address: SMTP Host:	Net LineDancer 192.168.223.133 mall	

Setting	Explanation	Requirements
Admin User	Admin user email address	_
Settings		
	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-tounderstand 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.

Inventory Changes			ce Zero-Touch								Network: C	core Y scorre	ale Logout Settings
🔛 🔻 Vendor/Model	OS: Cisco • × Add	l Criteria * 🔕 ち									🥯 Device 📚	Inventory 👁 Tools 🦠 Change	👶 Smart Change 🔰 F
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of
I92.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s				
I92.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	15				
10.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHUSEGVS	15				
10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	7s				
I92.168.0.254	lvi-gw-l3	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.8.1a	FDO2027E0MQ	3s				
10.0 100 PR	circo 10.0 100 89	Com	Cisco IOS	Cisco	CS81000V	Bouter	15.4(1)54	9N71OX4N5I9	15				

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:

	Network: <all></all>	✓ terrance Logout Settings Help
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 Logout		The current login user name is displayed. 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.

Logout	Settings	Help
Smart Ch	ange 툃	Reports

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.

	Server Settings	
Data Retention	Administrator	Add a role:
System Backup	operator	
Mail Server		
SNMP Traps		
Users		
Roles		
External Authentication		×
Custom Device Fields		~~
Memo Templates		
Launchers		
Smart Bridges		
Networks		
Network Servers		
Syslog		
Software Update		
Web Proxy		
Change Approvals		
Cisco API		
Device Label		
SNMPv3 User 🗸		
		OK Cancel

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

	Server	Settings	
Data Retention	Administrator	Add a role:	
System Backup	operator	labperson	+
Mail Server			
SNMP Traps			
Users			
Roles			
External Authentication		×	
Custom Device Fields		~~	
Memo Templates			
Launchers			
Smart Bridges			
Networks			
Network Servers			
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			
SNMPv3 User	•		
			OK Cancel

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

		Server Set	ttings
Data Retention		Administrator	Add a role:
System Backup		operator	
Mail Server		labperson	
SNMP Traps			
Users			
Roles			
External Authentication			×
Custom Device Fields			
Memo Templates		Permission to create/upda	ate/delete monitors.
Launchers		Permission to administer i	incidents.
Smart Bridges		Permission to view maps.	
Networks			
Network Servers		Permission to administer S	SNMP MIBs.
Syslog		Permission to view syslogs	IS.
Software Update		Permission to view compli	liance rule sets and policies.
Web Proxy			
Change Approvals		Permission to create/up	pdate/delete a compliance rule set.
Cisco API		Select All Select None	
Device Label			
SNMPv3 User	-		

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].

	Server Settings	
Data Retention	Administrator	Add a role:
System Backup	operator	
Mail Server	labperson	
SNMP Traps		
Users		
Roles		
External Authentication		×
Custom Device Fields		
Memo Templates	Permission to create/update/delete mon	itors.
Launchers	Permission to administer incidents.	
Smart Bridges	Permission to view maps.	
Networks	Permission to create/update/delete m	
Network Servers	Permission to administer SNMP MIBs.	
Syslog	Permission to view syslogs.	
Software Update	Permission to view compliance rule sets a	and policies.
Web Proxy	Permission to create/update/delete a	
Change Approvals	Permission to create/update/delete a	compliance rule set.
Cisco API	Select All Select None	
Device Label		
SNMPv3 User 🗸		
		OK Cancel

5.3 Add user

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

1. Click the 🕩 buton.

Data Retention		Username 📥	Full Name	Email	Role	Туре	Last Login
System Backup		admin	Administrator	stephen.cor	Administrator	Local	2024/01/03.
Mail Server		scorreale	Stephen Cor	stephen.cor	Administrator	External	Active
SNMP Traps							
Users							
Roles							
External Authentication							
Custom Device Fields							
Memo Templates							
Launchers							
Smart Bridges							
Networks							
Network Servers							
Syslog							
Software Update							
Web Proxy							
Change Approvals							
Cisco API							
Device Label							
SNMPv3 User	-	Find	0,	10. Au	udit Log	+ 1	8 💥 🗷

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

		Edit	User
er	General	Username:	LVI
e te	Networks	Full Name:	LogicVein
L	Custom Fields	Email Address:	support@logicvein.com
ЭI	Mail		
		Role:	Administrator ~
a.		Password:	•••••
		Confirm Password:	••••••
~			
			OK Cancel

Item	Subitem	Explanation	Requirements
General	Username Full name	Enter your username. Enter the user's full name.	required
	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].

Data Retention	🔶 Username 📥	Full Name	Email	Role	Туре	Last Login
System Backup	admin	Administrator	stephen.cor	Administrator	Local	2024/01/03
Mail Server	LVI	logicvein	support@lo	Administrator	Local	Never
NMP Traps	scorreale	Stephen Cor	stephen.cor	Administrator	External	Active
lsers						
oles						
xternal Authentication						
ustom Device Fields						
1emo Templates						
aunchers						
mart Bridges						
letworks						
letwork Servers						
yslog						
oftware Update						
/eb Proxy						
hange Approvals						
isco API						
evice Label						
NMPv3 User	Find	0	IQ Au	ıdit Log	+ 1	1 × E

5.4 Change user information

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

			Server Set	tings			
Data Retention		Username 📥	Full Name	Email	Role	Туре	Last Login
System Backup		admin	Administrator	stephen.cor	Administrator	Local	2024/01/03.
Mail Server		LVI	logicvein	support@lo	Administrator	Local	Never
SNMP Traps		scorreale	Stephen Cor	stephen.cor	Administrator	External	Active
Users							
Roles							
External Authentication							
Custom Device Fields							
Memo Templates							
Launchers							
Smart Bridges							
Networks							
Network Servers							
Syslog							
Software Update							
Web Proxy							
Change Approvals							
Cisco API							
Device Label							
SNMPv3 User	-	Find	0,	🤷 Au	ıdit Log	+ 🥖	6 🗙 🖻

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.

		Edit User		
General	Username:	LVI		
Custom Fields	Full Name:	logicvein		
Mail	Email Address:	support@logicvein.com		
	Role:	Administrator		~
			ОК	Cancel

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".

admin	Logout	Settings	Help
-------	--------	----------	------

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

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

	My User Profile		
Username:	scorreale		
Full Name:	Stephen Correale		
Email:	stephen.correale@logicvein.com		
Role:	Administrator		
Old Passwo	ord:		
New Password:			
Confirm:	Confirm:		
	Change Password		
	Reset client settings		
	ОК		

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-tounderstand 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.

Network:	Default	✓ te	ster	Logout	Settings	Help
🖘 Device 📚	Inventory 👁 Tool	s 🦠 Chang	e 🔌	Smart Ch	ange 鷱 F	Reports
Device Type		Serial#	ŧ	Tr	aits	
Router		9YY879	DF3BI	M	cmp ncn	D 🧲 🔶
Router		97IB01	G726R		nttps icm	קר (
Router		9AUD0	99HDI	KJ (i	cmp ncn	D 🧲
Router		SMA11	25020	DL (cmp ncn	D 🧯

2. Click [Set up two-factor authentication]

	My User Profile		
Username:	scorreale		
Full Name:	Stephen Correale		
Email:	stephen.correale@logicvein.com		
Role:	Administrator		
Old Passwo	ord:		
New Passw	New Password:		
Confirm:			
	Change Password		
F	Reset client settings		
	ОК		

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

)	Configure Two-Factor Authentication
	 Download an Authenticator app. (e.g. Google Authenticator, Microsoft Authenticator) Scan the QR code using the app.
a	3) Enter the 6-digit code that you see in the app:
	3) Enter the 6-digit code that you see in the app:
)9	Confirm Cancel

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".

	Server Sett	tings
Data Retention	Enable external authentication:	RADIUS ~
System Backup	Hostname: lvi.jp.co	Port: 1812
Mail Server		POIL 1012
SNMP Traps	Shared Secret: ••••••	
Users	Character Encoding: UTF-8	~
Roles		
External Authentication	Test	
Custom Device Fields		
Memo Templates	External group mappings:	
Launchers	Roles	
Smart Bridges	External Group	Role
Networks	LVI Dev	Administrator
Network Servers	LVI Tech	Administrator
Syslog		
Software Update		
Web Proxy		
Change Approvals		
Cisco API		
Device Label		₽ 2 1 9 ×
SNMPv3 User 🗸		
		OK Cancel

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

		Server Settings	
Data Retention	Enable external auth	entication: RADIUS	~
System Backup	Hostname:	lvi.jp.co	Port: 1812
Mail Server	Hostname.	IVI.Jp.co	
SNMP Traps	Shared Secret:	•••••	
Users	Character Encoding:	UTF-8 V	
Roles			
External Authentication		Test	
Custom Device Fields			
Memo Templates	External group map	pings:	
Launchers	Roles		
Smart Bridges	External Group		Role
Networks	LVI Dev		Administrator
Network Servers	LVI Tech		Administrator
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			+ 2 1 € 😣
SNMPv3 User 👻			
			OK Cancel

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

	5	Server Settings	
Data Retention	Enable external auth	entication: RADIUS	~
System Backup	Hostname:	lvi.jp.co	Port: 1812
Mail Server		111,19,000	
SNMP Traps	Shared Secret:	•••••	
Users	Character Encoding:	UTF-8 ~	
Roles			
External Authentication		Test	
Custom Device Fields			
Memo Templates	External group mapp	pings:	
Launchers	Roles		
Smart Bridges	External Group		Role
Networks	LVI Dev		Administrator
Network Servers	LVI Tech		Administrator
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			
SNMPv3 User 🗸			
			OK Cancel

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

	External Group Mapping	3
External Group:	GROUP	
Role:	Administrator	~
		OK Cancel

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.

Server Settings			
Data Retention	Enable external authentication: Activ	eDirectory ~	
Mail Server	Domain:	ngmt.example.com	
SNMP Traps			
Users	IP or Hostname: 1	92.168.0.1 Port: 636	
Roles		Enable TLS (LDAPS)	
External Authentication	Connection Timeout (seconds): 1	0	
Custom Device Fields		Test	
Memo Templates			
Launchers	External group mappings:		
Network Servers	Roles Networks		
Syslog	External Group	Role	
Software Update	Admin	Administrator	
Web Proxy	HelpDesk	NetworkManagement	
Change Approvals			
Cisco API			
SNMPv3 User			
Agent-D			
		OK Cancel	

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

	Server Settings
Data Retention	Enable external authentication: ActiveDirectory \checkmark
Mail Server	Domain: mgmt.example.com
SNMP Traps	
Users	IP or Hostname: 192.168.0.1 Port: 636
Roles	Enable TLS (LDAPS)
External Authentication	Connection Timeout (seconds): 10
Custom Device Fields	Test
Memo Templates	
Launchers	External group mappings:
Network Servers	Roles Networks
Syslog	External Group Role
Software Update	Admin Administrator
Web Proxy	HelpDesk NetworkManagement
Change Approvals	
Cisco API	
SNMPv3 User	
Agent-D	
	OK Cancel

4. Add a new item using the 🖻 button.

	Server Settings	3
Data Retention	Enable external authentication:	ActiveDirectory $ \smallsetminus $
Mail Server	Domain:	mgmt.example.com
SNMP Traps		
Users	IP or Hostname:	192.168.0.1 Port: 636
Roles		Enable TLS (LDAPS)
External Authentication	Connection Timeout (seconds):	10
Custom Device Fields		Test
Memo Templates		
Launchers	External group mappings:	
Network Servers	Roles Networks	
Syslog	External Group	Role
Software Update	Admin	Administrator
Web Proxy	HelpDesk	NetworkManagement
Change Approvals		
Cisco API		
SNMPv3 User		
Agent-D		
		OK Car

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

	External Group Mapping
External Group:	3Eye user
Role:	Administrator ~
	OK Cancel

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

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 \bowtie 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 -dname 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].

	Server Setti	ings	
Data Retention	Enable external authentication:	ActiveDirectory ~	
System Backup	Domain:	intra.lvi.co.jp	
Mail Server			
SNMP Traps	IP or Hostname:	192.168.0.3	Port: 389
Users		Enable TLS (LDAPS)	
Roles	Connection Timeout (seconds):	10	
External Authentication		Test	
Custom Device Fields			
Memo Templates	External group mappings:		
Launchers	Roles		
Smart Bridges	External Group	Role	
Networks	LVI Dev	Administrator	
Network Servers	LVI Tech	Administrator	
		Administrator	
Syslog		Administrator	
Syslog Software Update			
Syslog Software Update Web Proxy			
Syslog Software Update Web Proxy Change Approvals			
Syslog Software Update Web Proxy Change Approvals Cisco API Device Label			

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

Test Authentication		
Username:	scorreale	
Password:		
	Test	
	Authentication successful	
	Close	

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.

Logout	Settin	gs H	elp
Smart Ch	ange 🌡	🏮 Rep	orts

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

	Server Settings	
Data Retention	Server Name: support3eye	
System Backup	Hostname/IP Address: 10.0.0.183	
Mail Server	Hostname/IP Address: 10.0.0.183	
SNMP Traps	User login idle timeout (minutes): 30	
Users		
Roles	Enable the Terminal Server Proxy (SSH)	
External Authentication	Terminal Server Proxy SSH port: 2222	
Custom Device Fields	Enable HTTP for web client	
Memo Templates	Enable HTTP to HTTPS redirection	
Launchers	Enable DNS Lookup	
Smart Bridges	Enable Agent-D for monitoring this server	
Networks		
Network Servers	Enable SNMP for monitoring this server Configure SNMP Host	
Syslog	CORS Origin whitelist (Access-Control-Allow-Origin):	
Software Update		
Web Proxy		
Change Approvals		
Cisco API		
Device Label		
SNMPv3 User	•	🔶 🖉 💥
		OK Cancel

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 \bowtie .

	Server Sett	ings			
Data Retention	Administrator	Add a role:			
System Backup	operator		-		
Mail Server					
SNMP Traps					
Users					
Roles					
External Authentication		×			
Custom Device Fields					
Memo Templates	Permission to create/updat	e/delete monitors.	^		
Launchers	Permission to administer incidents.				
Smart Bridges	Permission to view maps.				
Networks	Permission to create/update/delete maps.				
Network Servers	Permission to administer SNMP MIBs.				
Syslog	Permission to view syslogs.				
Software Update	Permission to view compliance rule sets and policies.				
Web Proxy	Permission to create/up				
Change Approvals	Permission to create/up	date/delete a compliance rule set.	•		
Cisco API	Select All Select None				
Device Label					
SNMPv3 User	•				
		ОК	Cancel		

4. Click [OK] on the server settings.

5.10 Delete user

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

		Server Set	ttings			
Data Retention	Username ▲	Full Name	Email	Role	Туре	Last Login
System Backup	addoperter			operator	Local	2023/02/08
Mail Server	admin	Administrator	stephen.cor	Administrator	Local	2024/01/03
SNMP Traps	scorreale	Stephen Cor	stephen.cor	Administrator	External	Active
Users						
Roles						
External Authentication						
Custom Device Fields						
Memo Templates						
Launchers						
Smart Bridges						
Networks						
Network Servers						
Syslog						
Software Update						
Web Proxy						
Change Approvals						
Cisco API						
Device Label						
SNMPv3 User	✓ Find	0,	10 A	udit Log	🔶 🥖	🧹 🗙 🗟

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:

F Inventory Chang	jes Jobs Terminal Proxy Search	Compliance Zero-Touch P	laybook	Netwo	rk: <all> Yerrane</all>	ce Logout Settings Help
🔚 🔻 Search IP/Hostname: -Any- 🔹 Add Criteria 🛛 🔕 5						
IP Address	▲ Hostname	HW Vendor	Model	Device Type	Serial#	
10.0.0.66	TestA10License					A
n 😑 10.0.0.66	TestA10License					
10.0.0.70	router70.lvi.local	Cisco	CSR1000V	Router	9YY879DF3BM	
0 10.0.071	router71	Cisco	CSR1000V	Router	97IB01G726R	
10.0.0.101	M101	Cisco	CSR1000V	Router	9AUD099HDKJ	
0 10.0.0.112	uetsu	Cisco	CSR1000V	Router	90XP5HS5IG7	
10.0.0.112	uetsu	Cisco	CSR1000V	Router	90XP5HS5IG7	
0 10.0.0.121	simulator.intra.lvi.co.jp	Cisco	CRS-4/S	Router	SMA112502OL	

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.

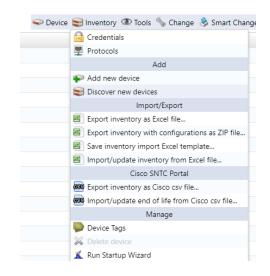
6.1.1.1 Credentials If you want to manage a device, you need to set the credentials (VTY user-name/password, SNMP community etc.) set on the managed device in NetLD.

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

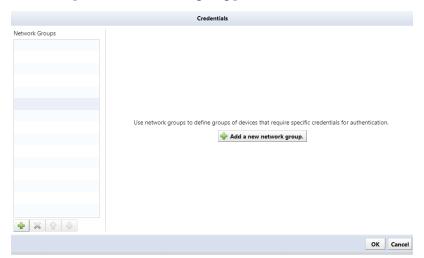
Credential Setting	Explanation	
dynamic	Set common credentials for address ranges. This is useful when common credentials are set for monitored devices.	
	Up to three credentials can be registered in one network group.	
static	Set credentials for each IP address.	
	Use this when different credentials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

New Network Group		
Enter a new name for this network group.		
new networks		
Oynamic - Credentials by CIDR, Range, Wildcard		
e.g.) 192.168.1.0/24 172.16.0.1-172.16.0.10 10.0.0.*		
Static - Credentials by specific IP address		
e.g.) 192.168.1.1		
	ОК	Cancel

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

	(Credentials	
Network Groups		Add address:	
*new networks		(IP, CIDR, Wildcard, or Range)	÷
		×	
	Credentials	VTY Username:	_
	New Credentials	VTY Password:	_
		Enable Username:	
		Enable Secret/Password:	
		SNMP Get Community:	
		SNMPv3 Authentication Username:	
		SNMPv3 Authentication Password:	
🕂 🗙 🗘 🦆	🔶 💥 🗘 🦆	SNMPv3 Privacy Password:	
		OK Ca	nce

In the "Credentials" window, enter the IP address and set each item.
 It is possible to omit items that are not required.

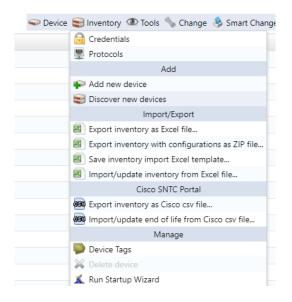
Cre	dential Set
IP Address:	
VTY Username:	
VTY Password:	
Enable Username:	
Enable Secret/Password:	
SNMP Get Community:	
SNMPv3 Authentication Username:	
SNMPv3 Authentication Password:	
SNMPv3 Privacy Password:	
	OK Cancel

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.		

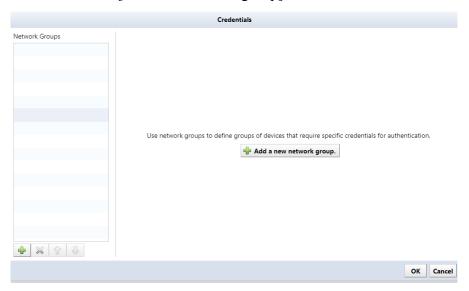
8. Click [OK] to save your settings.

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].

	Ċ
OK Cancel	
	OK Cancel

6. Click the 📥 button.

Vetwork Groups	Find:	۹,		🕂 🖋 😫
*test group	IP Address	VTY Username	Enable Username	SNMPv3 Username
💠 🗙 😚 😃		▶		

In the "Credentials" window, enter the IP address and set each item.
 It is possible to omit items that are not required.

Cre	dential Set
IP Address:	
VTY Username:	
VTY Password:	
Enable Username:	
Enable Secret/Password:	
SNMP Get Community:	
SNMPv3 Authentication Username:	
SNMPv3 Authentication Password:	
SNMPv3 Privacy Password:	
	OK Cancel

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.

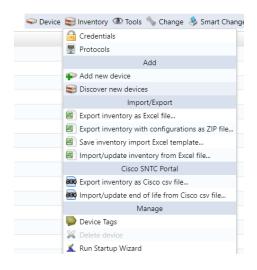
6.1.2 Add device

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.

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

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].

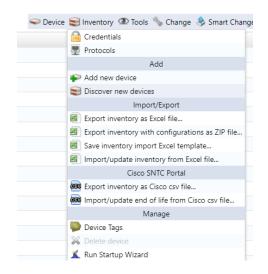
Add Device					
IP Address:	10.0.0.249				
Adapter:	Cisco IOS	~			
		OK Cancel			

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.

+	Inv	ventory Changes	Jobs Terminal F	Proxy Search Co	mpliance Zero-Tou	ıch
	Search IP/Hostname: 10.0.0.249 • Add Criteria • (3)					
Ē	=	IP Address	Hostname	Adapter	HW Vendor	Model
ь	0	10.0.0.249		Cisco IOS		
-P						
Ĕ.						
4						
Enterprise						
10						

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.

	Discove	er Devices
Specify the networks and addresses that you would like to discover.		Boundary Networks: 10.0.0.0/8.172.16.0.0/12.192.168.0.0/16.FC00::/7
IP Address/CIDR		Crawl the network from the specified addresses.
IP Address/CIDR:	4	Include existing inventory in addresses to discover
IP Address Range		Default to Linux for SSH hosts with no supported adapter
IP Address Wildcard		
Single IP Address		
Import from CSV		
		Additional SNMP Community String:
		Run Cancel

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.

	Hostname Netw									Cevice Conve	antory 👁 Tools 🦠 Change	Smart criange 👊 Kep
		vork Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of
3 10.0.0.212	shibata Core	Foundry FastIron										
4 1-1of1 🕨												Results per page: 254
teractive Discovery	Interactive Discovery	×				<u> </u>						
		Status										
		10.0.0.212 (shibata)										nom snmp (telne
addresses scanned												
tteractive Discovery		Status				• • • • •						

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

Note				
cover	overy has a setting called "Boury to the range specified in "B Networks" by default, so edit '	oundary Networl	ks". Several range	s are specified for "Bound-
		Discove	r Devices	
	Specify the networks and addresses that you would like to IP Address/CIDR IP Address/CIDR:	o discover.	Boundary Networks: 10.0.0.0/8.172 Crawl the network from the spe Include existing inventory in ad	dresses to discover
		Disco	ver Devices	
	Specify the networks and addresses that you would like IP Address/CIDR IP Address/CIDR: IP Address Range IP Address Wildcard Single IP Address Import from CSV	Edit Disco The following boundaries will be	very Boundaries e used when running discovery. d against addresses that fall within	2.16.0.0/12.192.168.0.0/16.FC00::/7 ⇒cified addresses. dresses to discover with no supported adapter s no supported adapter Only New Devices ∨

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.

- 🥪 Device 😂 Inventory 👁 Tools 🦠 Change 🔶 Smart Change 🔒 Credentials 🖳 Protocols Add ₽ Add new device Siscover new devices Import/Export Export inventory as Excel file... Export inventory with configurations as ZIP file... Save inventory import Excel template... Import/update inventory from Excel file... Cisco SNTC Portal छ Export inventory as Cisco csv file... 👼 Import/update end of life from Cisco csv file... Manage Device Tags 💥 Delete device 👗 Run Startup Wizard
- 1. Click the Inventory > [Save inventory import Excel Template] buttons.

The file opening screen will be displayed.

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

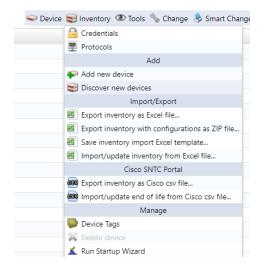
The file name will be "NetLD-inventory-template.xlsx" and will be saved in XLSX file format.

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

Q	Р	0	Ν	М	L	K	J	I.	Н	G	F	E	D	С	В	А	
14 Custom 5	Custom 4	Custom 3	Custom 2	Custom 1	End Of Life	End Of Sale	Memo	Serial Number	OS Version	Model	Vendor	ie Type	r ID Hostname	Adapter ID	Network	IP Address	1
												1	Demo-01		Default	172.16.0.1	2
												2	Demo-02		Default	172.16.0.2	3
												3	Demo-03		Default	172.16.0.3	4
												4	Demo-04		Default	172.16.0.4	5
												5	Demo-05		Default	172.16.0.5	6
												3	Demo-06		Default	172.16.0.6	7
												7	Demo-07		Default	172.16.0.7	8
												8	Demo-08		Default	172.16.0.8	9
												9	Demo-09		Default	172.16.0.9	10
												2	Demo-10		Default	172.16.0.10	11
																	12
	<u> </u>												Demo-10		Detault	172.16.0.10	

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.	-	Cisco IOS
	(In the current version, there is no need to specify this item.)		
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].

Organize New fold	der			
A Home	Name	Date modified	Туре	Size
> 🔷 OneDrive - Perso	∨ Today			
	netLD-inventory-2023-09-20	9/20/2023 11:27 PM	Microsoft Excel W	
🔄 Desktop 🔹 🖈				

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

Device Import Results	
14 devices updated.	
	ОК

6.1.2.3.1 Check the operation log

1. Select the Terminal Proxy tab.

Search IP/Hostn	ame: 10.0.0.250 * Ac	ld Criteria 👻 😒 🕤			
IP Address	Hostname	Network	Adapter	HW Vendor	Model
10.0.250	lvicore	Core	Cisco IOS	Cisco	CISCO1921/K9

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.

🞸 Inventory Changes Jobs Terminal	Proxy Search Compliance Zero-To	uch				Network	Core v scorreale Logout Settings Help
🖌 🔛 🔻 Device: -Any- 🛛 👻 User: -A	ny- * X Session Date: -Any-	r ≍ Text: -Any- × ≍ Client: -An	y- •× 🗷 5				🔯 Export
Device IP Address	Device Hostname	Make/Model	Protocol	User	Client IP Address	Session Start	 Session End
I 10.0.0.250	lvicore	Cisco CISCO1921/K9	SSH	scorreale	76.184.233.100	2024/06/10 15:26	2024/06/10 15:26
¶ 4 1-1of1 ≱							
lvicore - 10.0.0.250 - Termi ×				-			
4							

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.

	tname: 10.0.0.250 * A	dd Criteria 👻 🕙 😏									Devi	ce 😒 Inventory 🖪	🖓 Tools 🦄 Chang	e 👶 Smart Change	\rm Rep
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Soft	vare End Of Sale	Software End O	f
10.0.0.250	Micore	Core	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	75						
4 1-1of1															
4 1-1 of 1	Þ.													Results per page:	25
ore - 10.0.0.250	~						* <u>*</u>								
icore - 10.0.0.250	actions.									General C	ompliance Attac	hment Hardwar	e Interfaces	ARP/MAC/VLAN	M
idmin Name			AB	85			Туре	IP			Speed	мти	MAC	Comment	
Embedded	Service-Engine0/0						other				10 Mbps	1500			
GioabitEthe	met0/0						ethernet				1 Gbps	1500	E05F898A4D60		
	rnet0/0.1						ethernet	10.0.0.250/24, FD14:5839:664	D:1000:/64		1 Gbps	1500	E05FB9BA4D60		
	rnet0/0.120						ethernet	10.0.2.254/24, FD14:5839:664	D:1020:/64		1 Gbps	1500	E05FB9BA4D60		
GigabitEthe							ethernet	10.0.3.254/24, FD14:5839:664	D:1030:/64		1 Gbps	1500	E05F898A4D60		
GigabitEthe	rnet0/0.130							10.0.6.254/24, FD14:5839:664				1500	E05F898A4D60		
GigabitEthe GigabitEthe	met0/0.130 met0/0.160						ethernet				1 Gbps				

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.

n	ventory Changes Jo	bs Terminal Proxy S	iearch Compliance 2	Zero-Touch								Network: Core	✓ scorreale	Logout Settings
-	 Search IP/Hostname: 	-Any- * Add Crib	eria * 🔇 5									🗢 Device 😂 Invento	rry 👁 Tools 🦠 Change 🤅	> Smart Change 👢 Re
	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of
,	10.0.3.120	MikroTik RouterBoard 95	Core	MikroTik RouterOS	MikroTik	R8951Ui-2HnD	Router	6.22	4AC904A634C4	4s				
5	192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s				
2	192.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	1s				
2	10.0.2.244	Apresia3424GT-SS	Core	Apresia	Apresia	Apresia3424GT-SS	Switch	7.38.01		22s				
2	10.0.2.10	AvayaERS4850GTS	Core	Extreme ERS	Extreme	4850GTS-PWR+	Switch	5.6.1.052	13JP222H7099	23s				
2	10.0.3.15	Si-R-G100-LVI	Core	Fujitsu SRS	Fujitsu	Si-R G100	Router	V02.11	00046367	45				
2	10.0.2.243	apresia2142	Core	Apresia	Apresia	Apresia2124GT-SS2	Switch	6.20.01		16s				
2	10.0.0.206	bigip1	Core	F5 BIG-IP	F5 Networks	BIG-IP Virtual Edition	Load Balancer	11.6.0	422cadb1-b343-859d-b0	86				
2	10.0.0.217	apcHost	Core	APC Smart-UPS	APC	Smart-UPS 750	Power Supply	v6.0.6	J11625110998	38s				
2	10.0.2.30	Summit48i	Core	Extreme Extremeware	Extreme	Summit48i	Switch	7.3.2.3	0145M-01540	29s				

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

Search IP/Hostnar	ne: -Any- * Add Crit	eria * 🗷 🕤									🤝 Device 😂	Inventory @ Tools % Change	💩 Smart Change 🔌
P Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of
10.0.3.120	MikroTik RouterBoard 95	Core	MikroTik RouterOS	MkroTik	R8951UI-2HnD	Router	6.22	4AC904A634C4	58				
192,168,20,83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	285				
R 102 168 1 61	CSR00-WIC	Com	Circo IOS	Cierco	C000001-C-10	Wiselan Controller	16.12.44	ECI 245100411	14				
🖞 🍕 1 - 254 of 855 🕨													Results per page:
ackup Devices ackup Devices (2024	× //06/10 15:20)									Network			
tatus Summary			P Address 10.0.3.120				Hostname MikroTik RouterBoard 951U						
0 Successes With Chan													
3 1 Successes Without Cl	langes												
0 Invalid Credentials													
🔒 0 Failures													

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.
Ø	Backup successful, no changes. Displayed when the configuration data on the device is the same as the last backup.
0	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.
Ŵ	Warning	This device violates a compliance policy with severity set to Warning.
W	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.

Inventory Changes	Jobs Terminal Proxy	Search Compliance	e Zero-Touch								Network: Co	scorres	ale Logout Settings
🔮 🔻 Search IP/Hostnar	me: 10.0.0.250 * Add	d Criteria * 🙁 🕤									🗢 Device 😂 k	nventory 👁 Tools 🦴 Change	🛞 Smart Change 🔌 F
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of
10.0.0.250	lvicore	Core	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	7s				
- 4 1-1of1 ≱													Results per page: 2
icore - 10.0.0.250	×						¥						
icore - 10.0.0.250	actions.									General Compli	ance Attachment	Hardware Interfaces	ARP/MAC/VLAN
			6 A		ast Backup: 2024/06/10 12:33	(Duration: 7s)							23588
	a state of the state of the				Snapsho			onfia		mestamp	Size Use		
										mestamp	Size Usi	er	
-iluilu cisco			Cisco 1900 Series		2024/06/05		/running-config			mestamp 4/06/05 12:34	9824	admin	
cisco			Cisco 1900 Series		2024/06/05			and a second	202				
cisco			Cisco 1900 Series		2024/06/05	12:34	/running-config		202	4/06/05 12:34	9624	admin	
cisco	$\langle \rangle \langle \rangle \langle$		Circo 1900 Series			12:34	/running-config /startup-config	- may	202 202 202	4/06/05 12:34 4/06/04 12:33	9824 9824	admin admin	
Cisco		Serial#:	FGL15082638			12:34	/running-config /startup-config /running-config		202 202 202 202 202	4/06/05 12:34 4/06/04 12:33 4/06/04 12:33	9624 9624 9824	admin admin admin	
Visco Make: Cisco Modet: CISCO1921/KS			FGL15082638		2024/06/04	12:34	/running-config /startup-config /running-config /startup-config	anna g	202 202 203 203 203 203 203	4/06/05 12:34 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33	9824 9824 9824 9824	admin admin admin admin	
Make: Cisco Model: Cisco		Serial#:	FGL15082638		2024/06/04	12:34 12:33 12:33	/running-config /startup-config /running-config /startup-config /running-config		202 202 203 203 203 203 203 203 203	4/06/05 12:34 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33 4/06/01 12:33	9824 9824 9824 9824 9824 9791	admin admin admin admin admin admin	
Make: Cisco Model: CisCO1921/KS		Serial#:	FGL15082638		2024/06/04	12:34 12:33 12:33	/running-config /startup-config /running-config /startup-config /startup-config /startup-config		202 202 202 202 202 202 202 202 202 202	4/06/05 12:34 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33 4/06/01 12:33	9824 9824 9824 9824 9791 9791	admin admin admin admin admin admin admin	
Make: Cisco		Serial#:	FGL15082638		2024/06/04	12:34 12:33 12:33 11:33	/running-config /startup-config /running-config /startup-config /startup-config /startup-config /running-config		202 202 202 202 202 202 202 202 202 202	4/06/05 12:34 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33 4/06/04 12:33 4/06/01 12:33 4/06/01 12:33 4/02/23 11:33	9624 9624 9624 9624 9791 9791 9791 12330	admin admin admin admin admin admin admin	

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

2019/	12/12 23:14	枝索	Q. 🔶	1
1	version 15.4			under
2	service timestamps debug datetime msec			
3	service timestamps log datetime msec			
4	no service password-encryption			
5	1			
6	hostname Ciscol921			
7	1			
8	boot-start-marker			
9	boot-end-marker			
10	1			
11				
12	enable secret 5 #1#x1Th#bfnrSP8pJzxWVtOhFF9AN/			
13				
14	aaa new-model			
15	1			
16				
17	1			
18				
19	1			
20				
21	1			
22	aaa session-id common			
23				
24	1			
25				
26	1			

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.

Inventory Changes	Jobs Terminal Proc		e Zero-Touch								100	etwork: Cor		correale Logout Settin
🔛 🔻 Search IP/Hostnar	ne: 10.0.0.250 🔻 🗛	id Criteria 👻 🙁 🕤									-	Device 😂 Inv	ventory 👁 Tools 🦠 C	hange 👶 Smart Change
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of L	ife	Software End Of	ale Software End Of
10.0.0.250	lvicore	Core	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	75					
4 1-1of1 ⊮														Results per page:
a renorm p							¥							resons per page.
vicore - 10.0.0.250	×													
vicore - 10.0.0.250	actions									General	Compliance i	Attachment	Hardware Interfa	
	and the second second		1	1	ast Backup: 2024/06/10 12:33	(Duration: 7s)								88388
	and the second				Snapsho	rt .	c	onfig	Tir	mestamp	Si	ze User		
-11-11-1			Cisco 1900 Seri	• 10 a 28	2024/06/05	12:34	/running-config		2024	1/06/05 12:34		9824	a	dmin
11 1 1				1.1			/startup-config		2024	1/06/04 12:33		9824	a	dmin
1. 1.					2024/06/04	12:33	/running-config		2024	1/06/04 12:33		9824		imin
				1 A A			/startup-config		202	1/06/04 12:33		9824		dmin
Make: Cisco Model: CISCO1921/KS		Serial#: Device Type:	FGL15082638 Router		2024/06/01	12:33	/running-config		2024	1/06/01 12:33		9791	a	dmin
OS Version: 15.4(3)M5		berke type.					/startup-config		2024	1/06/01 12:33		9791	а	dmin
					2024/02/23	11:33	/running-config		2024	1/02/23 11:33		12330		imin
							/startup-config			1/01/03 11:35		12062		dmin
					2024/01/05	11:35	/running-config			1/01/03 11:35		12308		dmin
							/startup-config		202	1/01/03 11:35		12062		dmin

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.

比較 ×		2
cisco1921labo.intra.lvi.co.jp - /startup-config (2019/06/14 18:00)	cisco1921labo.intra.lvi.co.jp - /startup-config (2019/07/24 18:00)	
<pre>38 ig file monitor MFF-MULTOR input 39 ig file monitor MFF-MULTOR input 39 ig file monitor for a set of the set of t</pre>	<pre>135 is investign FFF-United Regist End (put) 135 is investign FFF United FFF United</pre>	
		🚃 = 削除 👥 = 変更 📰 = 這加

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 sidepanel.

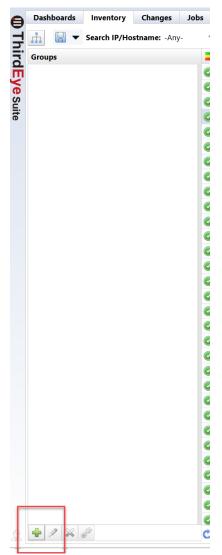
(Ensure "Enable Device Groups" is checked.)

		Server Settings
Mail Server		✓ Enable Device Groups
SNMP Traps		
Users	- 11	
Roles		
External Authentication		
Custom Device Fields		
Memo Templates		
Launchers		
Networks		
Network Servers		
Syslog		
Zero-Touch		
Software Update		
Web Proxy		
Change Approvals		
Device Groups		
Cisco API		
Device Label		
SNMPv3 User		
Agent-D	-	
		OK Cancel

3. Click the Inventory tab, then click the $f{m}$ button in the top left corner.

e	- Dashboards		Invent	ory	Changes	Jobs	Т			
Th	ф.		₽ -	Search I	Search IP/Hostname: -Any-					
ind	-	IP	Address		Host	tname	Netw	ork		
m	\bigcirc	10	.128.0.12				Defau	lt		
ye	\bigcirc	10	.98.0.2		HND	-Switch-0	Defau	lt		
Suit	\bigcirc	20	7.35.249.	40	ott-e	dge-1	Defau	lt		
it		10	0 1 0 0 1 1				Defau	14		

4. Click the 🔹 button in the bottom left corner.



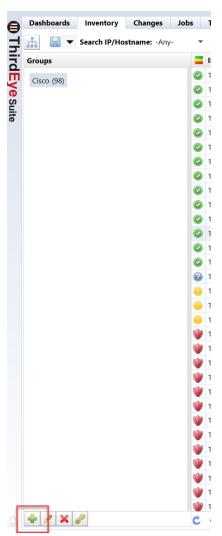
In the popup window, enter a name for the grouping ("Cisco" in the screenshot below).
 Sharing pulldown menu:

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.

0	Dashboards	Inventory	Changes	Jobs	Terminal Proxy	Search	Compliance	Monitors	Incidents	Мар	MIBs
)Th	<u>.</u>	Search IP/Ho	stname: -Any		Add Criteria 🔻	< ≤					
ird	Groups			=	IP Address	Ho	ostname	Netwo	Adapter	HW V	Mod
	Cisco (98)				10.128.0.9	CR	4-В	show_an	Cisco IOS	Cisco	CRS-
Eye	0.000 (00)				10.128.0.8	CR	811-A	show_an	Cisco IOS	Cisco	CRS-
Suite				Ø	10.128.0.7	CR	12-В	show_an	Cisco IOS	Cisco	CRS-
ite					10.128.0.181	VA	STDCC-fw1va1p	Default	Cisco ASA	Cisco	ASA
					10.0.0.227	Tra	aining20240910	Default	Cisco Ne	Cisco	Nexu
					10.128.0.182	hq	-waas1	Default	Cisco WA	Cisco	OE-V

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].

				Devi	ice Groups	;				
Na	me:									
Fi	reWall									
Cri	teria:									
D	Device Type: -Any-	→ × Ad	d Criteria	•						
Ē	Any-									
	Content Engine									
de la										
<u>[</u>	Firewall									
	Power Supply									
E	Router								ОК	Close
	Server									
V	Switch	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU	1s	icmp nc N	lo resp
n-5	Traffic Shaper	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9A0HFG	2s	https ici N	lo resp
89 C	Wireless Controller	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873S	2s	https ici	

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

0	Dashboards Inventory	Changes Jobs	s	Terminal Proxy	Search	Compliance	Monitors	Incidents	Мар	MIBs Play	/book
Thi	🚠 🔚 🔻 Search IP/Hos	stname: -Any-	-	Add Criteria 🔻	< ≤						
ird	Groups			IP Address	Ho	stname	Netwo	Adapter	HW V	Model	Device
Ē			\bigcirc	10.128.0.181	VA	STDCC-fw1va1p	Default	Cisco ASA	Cisco	ASA5550	Firewall
Уe	FireWall (8)			10.128.0.174			Default	Cisco ASA	Cisco	PIX-520	Firewall
Eye Suite				10.128.0.140	cis	coasa	Default	Cisco ASA	Cisco	ASA5510	Firewall
ite				10.128.0.123	asa	i-gw	Default	Cisco ASA	Cisco	PIX-520	Firewall
				10.128.0.124	cis	coasa	Default	Cisco ASA	Cisco	ASA5510	Firewall
				10.128.0.102	SIN	10007-FW03	Default	Cisco ASA	Cisco	ASA5585	Firewall

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

8	Dashboards	Inventory	Changes	Jobs
Ţ	<u>.</u>	Search IP/Hos	stname: -Any	-
ThirdEye Suite	Groups			
Ţ	🛇 Cisco (80)			
e	firewall (7)			
Suit	— Meraki (2)			
e	router (43)			
	switch (23)			
	compliance iss	ue (12)		
	dallas (2)			
	Demo (4)			
	Firewall (10)			
	juniper (1)			
	Stacked switch	s (7)		
	Switch (38)			

6.1.6 Remove device

+ 1	Inventory Changes	Jobs Terminal Praxy S	earch Complian	ce Zero-Touch								Network	Core v scorreale Logos	at 1
ģ i	🚽 🔻 Search IP/Hostr	ame: -Any- * Add Crib	eria = 🕢 🕤									Device	e 😂 Inventory 👁 Tools 🦠 Change 👶 Smart	Char
말 :	IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Generation Credentials	
Б.	10.03.120	MikroTik RouterBoard 95	Core	MikroTik RouterOS	MikroTik	R8951Ui-2HnD	Router	6.22	440904463404	56			Trotocola	
m e	9 192,168,20,83	SF300-24	Core	Cisco Small Business	Osco	SF300-24	Switch	14115	DNI144402YT	285			Add	
2	9 192,168,1,61	C9600-WLC	Core	Cisco IOS	Gico	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	14			P Add new device	
m a	002.244	Apresia3424GT-SS	Core	Accesia	Apresia	Apresia3428GT-SS	Switch	7.58.01		224			Discover new devices Import/Export	
	0.02.10	AvavaERS4850GTS	Core	Fatreme FRS	Futureme	4850GTS-PWR+	Switch	5.61.052	13/P222H7099	235			Emport/taport	
	0 1003.15	S-R-G100-LVI	Core	Fullow SRS	Fuilter	SI-R G100	Router	V02.11	00046367	41			 Export inventory as Excernic. Export inventory with configurations as ZP f 	o.,
ហ្គ 🖁	0.0.2.243	apresia2142	Core	Apresia	Aoresia	Apresia2124GT-SS2	Switch	6,20,01		165			Save inventory import Excel template	
	10.0.0206	bigip1	Core	FS BIG-IP	F5 Networka	BIG-IP Virtual Edition	Load Balancer	11.6.0	422radb1.b343.8594.b0				Manager August and August and August and August Aug	
	1000217	apchiast	Core	APC Smart-UPS	APC	Smart-UPS 750	Power Supply	16.0.6	/11625110998	354			Cisco SNTC Portal	
	0 10.0.2.30	Summitable	Core	Extreme Extremeware	Extreme	Summit48i	Switch	7323	0145M-01540	231			Report inventory as Cisco cav file	
	1000.223	1214	Core	Cisco IDS	Gsco	CSR1007V	Router	17.3.5	9MTTHUSEGVS	15			import/update end of life from Osco csv file	
	10.0.2.242	FIOS	Core	Dell PowerConnect	Del	SED.01.GE.MT.MC	Switch	8338	SHEM135E00136	85			Manage	
	10.0.2.246	LVI-BrocadelCX	Core	Foundry Fastiron	Brocade	ICX6610-24	Switch	08.0.10dT7/3	R(P3842000)	71			Device Tags	
	10.02.245	Apresia13200	Core	Apresia	Apresia	Apresia13200-52GT	Switch	8.10.02	02110383	95			X Delete device	
	1002245	Neon5548	Core	Cisco Necus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	79			K Run Startup Wizard	
	192.160.20.225	ApresiaLightFM116GT-SS -		ApresiaLight	Htachi	EMILIGITSS	Switch	1.12.01	160532124951	105				
	192.168.20.223	acm7004.2	Core	Opengear	Openpeer	ACM7004-2	Resilience Gateway	4.13.6	70042008093470	15				
	9 192.168.20.223	im7216-2-dac							72161708005075					
			Core	Opengear	Opengear	IM7216-2-DAC	Infrastructure Manager	4.13.6		16				
	9 192.168.20.221	WS1.TY11	Core	Accedian NetworkDevice	Accedian	AMN-1000-TE	Network Performance Ele		G315-2136	10s				
	9 192.168.1.14 9 192.168.0.254	arista-dev hi-gw-B	Core	Arista EOS	Arista	DCS-71505-24-R	Switch	4.17.1F-3471410.8decatur	JPE16160961	41				

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

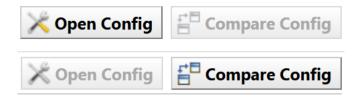
- 2. With the device selected, click Inventory > [Delete Device].
- 3. A confirmation message will be displayed. Click [Yes].



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.

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.

The Job History subtab has the following buttons:

ButtonEditionJob Approvals LogView 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.						
Сору	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].

*	ventory Changes Jobs Terminal Proxy Search Compliance	Zero-Touch			Network: Core v scorreale Logout Settings Help
4.2	ob History Job Management				
nett	🔻 Job Name: add ntp server * 🛛 Add Criteria * 💿 🕤			🔝 Audit Log 🛞 Open Job 😹	Delete 🥜 Rename 📄 Copy 🚳 Ran Now 📓 New Job 🛅 Filters
in .	Name	Туре	Approval Requester	Approval Status	Meno
m 4	add ntp server	Smart Change		Not Requested	
글					
۳.					
믹					
ត់					
m) add mg sener				

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.

Create Tool Job
lob Name:
enable password
Network:
Default 🗸
Comment:
Tool:
Change Enable Password V
OK Cancel

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.

*enable password	×					>
Input Parameters	Devices	Schedule	Job Approvals Log	Email Notification		
User Data						
New Password						
New Password						
Password:					Confirm:	
Verify credentials a	ifter change i	s executed				

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.

Input Parameters	Devices	Schedule	Job Approvals Log	Email Notification
O All Devices	Search 🔘	Static list		

Search

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

*enable password	×														
Input Parameters		chedule Job App	provals Log Em	ail Notification											Ū
			provais Log Em	all Notification											<u>La</u>
O All Devices	Search 🔾 Stat	ic list								N	etworks: Default				
Vendor/Model/OS:	Cisco 🕶 🗶 Ad	d Criteria 👻													
IP Address	 Hostname 	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Durat	End Of Sale	End Of Life	Software End	Software End	Traits	Violation
10.0.0.101	R2	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9AUD099HDKJ	53s			2019/06/17	2024/06/30	icmp ncm sn	6
10.0.0.112	uetsu	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7	50s					https icmp n	Node test is i
🥡 10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	1s	2014/08/15	2021/08/31			icmp ncm sn	6
10.0.0.124	bbbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	51s					https icmp n	5
10.0.0.126	test	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9E0UQZIVK9E	14s					https icmp n	9
10.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9J4P873SEIN	4s					https icmp n	5

Static list

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

IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration
10.0.3.120	MikroTik RouterBoard 95	Core	MikroTik RouterOS	MikroTik	RB951Ui-2HnD	Router	6.22	4AC904A634C4	5s
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s
192.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	1s
10.0.2.244	Apresia3424GT-SS	Core	Apresia	Apresia	Apresia3424GT-SS	Switch	7.38.01		22s
10.0.2.10	AvayaERS4850GTS	Core	Extreme ERS	Extreme	4850GTS-PWR+	Switch	5.6.1.052	13JP222H7099	23s
10.0.3.15	Si-R-G100-LVI	Core	Fujitsu SRS	Fujitsu	Si-R G100	Router	V02.11	00046367	4s
10.0.2.243	apresia2142	Core	Apresia	Apresia	Apresia2124GT-SS2	Switch	6.20.01		16s
10.0.0.206	bigip1	Core	F5 BIG-IP	F5 Networks	BIG-IP Virtual Edition	Load Balancer	11.6.0	422cadb1-b343-859d-b0	8s
10.0.0.217	apcHost	Core	APC Smart-UPS	APC	Smart-UPS 750	Power Supply	v6.0.6	J11625110998	38s
10.0.2.30	Summit48i	Core	Extreme Extremeware	Extreme	Summit48i	Switch	7.3.2.3	0145M-01540	29s
10.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	1s
10.0.2.242	FTOS	Core	Dell PowerConnect	Dell	S60-01-GE-44T-AC	Switch	8.3.3.8	SHFM135E00136	8s
10.0.2.246	LVI-BrocadeICX	Core	Foundry FastIron	Brocade	ICX6610-24	Switch	08.0.10dT7f3	BXP3842K00J	7s
10.0.2.245	Apresia13200	Core	Apresia	Apresia	Apresia13200-52GT	Switch	8.10.02	02110383	9s
10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	7s
192.168.20.225	ApresiaLightFM116GT-SS	Core	ApresiaLight	Hitachi	FM116GTSS	Switch	1.12.01	168632124961	18s
192.168.20.223	acm7004-2	Core	Opengear	Opengear	ACM7004-2	Resilience Gateway	4.13.6	70042008093470	1s
 1 - 254 of 855 able password nput Parameters 	× es Schedule Job Appr	rovals Log Email Notific	ation						
All Devices O Search	Static list								Networks:
Address				•	Hostname				Network
0.0.2.10					AvayaERS4850GTS				Core
0.0.2.244					Apresia3424GT-SS				Core
0.0.3.120					MikroTik RouterBoard 951Ui				Core
2.168.1.61					C9800-WLC				Core
2.168.20.83					SF300-24				Core

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

enable password	×				
Input Parameters	Devices	Schedule	Job Approvals Log	Email Notification	
Trigger					Next Fire Time(GMT-5)

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

	Trigger	
Name: scł	hedule	
	● Once ○ Daily ○ Weekly ○ Monthly ○ Cron	
	4	
Timezone:	(GMT-06:00) Central Time	~
Filter:	<no filter=""></no>	~
	Save Cano	

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
0	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."

	Server Settings
Data Retention	Administrator Add a role:
System Backup	operator
Mail Server	approver
SNMP Traps	
Users	
Roles	
External Authentication	×
Custom Device Fields	
Memo Templates	✓ Permission to run a tool.
Launchers	Permission to create/update/delete a tool job.
Smart Bridges	Permission to approve a tool job execution.
Networks	Permission to run a tool job without approval.
Network Servers	Permission to run a Smart Change job.
Syslog	Permission to create/update/delete a Smart Change job.
Software Update	Permission to run a tool which changes a device configuration.
Web Proxy	Permission to run a report.
Change Approvals	
Cisco API	Select All Select None
Device Label	
SNMPv3 User	•
	OK Cancel

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

	Server Setti	ings
Data Retention	Administrator	Add a role:
System Backup	operator	
Mail Server	approver	
SNMP Traps	requester	
Users		
Roles		
External Authentication		×
Custom Device Fields		~
Memo Templates	Permission to run a device	discovery job.
aunchers	Permission to create/upo	
Smart Bridges	Permission to run a Popula	te End Of Sale job.
Networks	Permission to create/upo	e/delete a Populate End Of Sale job.
Network Servers	Permission to run a tool.	
Syslog	Permission to create/upo	e/delete a tool job.
Software Update	Permission to approve a	
Web Proxy	Permission to run a tool	
Change Approvals	Permission to run a Sma	
Cisco API	Select All Select None	
Device Label		
SNMPv3 User	•	

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.

Inv	entory	Changes	Jobs	Terminal Proxy	Search	Compliance	Zero-Touch	
Jo	b History	Job Mar	nagement					
H		proval Status:	-Any-	▼ × Add (Criteria 🔻	🗷 🗲		
	Nar 🗹	-Any-					Туре	
۶	Adc	Requested					Smart Change	
٩	add	Approved					Smart Change	
٩	Autom	Rejected Closed					Smart Change	
٩		Not Requeste	d				Smart Change	
		cess Lists	u				Tool	
	Cisco Int	erfaces					Tool	
e de la composición de la comp	Cisco Show Commands					Tool		
\$	Core dis	Core discovery			Discovery			
h,	Daily cha	Daily changes			Report			
200	enable p	enable password				Tool		
\$	Full back	Full backup				Backup		
h,	Full Com	Full Compliance					Report	
٩	Huawei (OS Push					Smart Change	

- 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.

			Server Settings			
Data Retention		nd traps when				
System Backup		-	uration changes are	detected		
Mail Server	 ✓ devices are added and deleted ✓ a backup fails 					
SNMP Traps	a job completes with errors					
Users	the compliance status of a device changes					
Roles			bridge changes			
External Authentication		an audit even	nt occurs proval action occurs			
Custom Device Fields		an email failu				
Memo Templates	Tra	p forwarding:				
Launchers						
Smart Bridges		_				
Networks	Tra	p receivers:				
Network Servers	C	ommunity	Host	Port	Version	
Syslog	р	ublic	10.0.0.93	162	2c	
Software Update						
Web Proxy						
Change Approvals						
Cisco API						
Device Label						
SNMPv3 User	-				🕂 🖉 🖗	
					OK Cancel	

Send e-mail

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

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

	Server Settings					
Data Retention	SMTP Host:					
System Backup	.protection.outlook.com					
Mail Server	From Email Address:					
SNMP Traps	support3eye@lvi.co.jp					
Users	From Name:					
Roles	support3eye					
External Authentication	supportseye					
Custom Device Fields	Server requires authentication					
Memo Templates	Use secure smtp					
Launchers	Automatically upgrade STARTTLS negotiation					
Smart Bridges	Mail server username:					
Networks						
Network Servers	Mail server password:					
Syslog						
Software Update						
Web Proxy	Default email language 🔜					
Change Approvals	Default email time zone (GMT+09:00) Tokyo 🗸					
Cisco API						
Device Label						
SNMPv3 User	▼ Test					
	OK Cancel					

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.

	Server Settings		е
System Backup	▲ Minimum required approval count: 1		2
Mail Server			2
SNMP Traps			2
Users			2
Roles			2
External Authentication			1
Custom Device Fields			1
Memo Templates			1
Launchers			1
			0
Smart Bridges			0
Networks			0
Network Servers			0
Syslog			9
Software Update			9
Web Proxy			9
Change Approvals			9
Cisco API			8
Device Label			8
SNMPv3 User			8
Agent-D	×		8
			7
		ОК	Cancel

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.
Туре	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.

lob History Job Wanagement					
🔻 Approal Status Republic 🕫 X 🛛 Ado	dCriteria * 🕘 👆		🖗 Audit Lag 💈 Open Job 🗙 Décie 🦯 Rename	Capy 👌 han liber 💲 Hen Job 📑 A	
Nane	Type	Approval Requester	Approval Status	len	
erablepazavord	Tool	sonek	Requested		

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

Delete?
Are you sure you want to delete the selected job?
OK Cancel

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)

Inventory Changes	Jobs Terminal Pro	xy Search Co	mpliance Zero-Touch Pla	ybook		Network:	<ali></ali>	terrance Logout	Settings Hel
Session Date: Past 7 days * X Add Criteria * 🙁 5								📑 Export.	
Device IP Address	Device Hostname	Network	Make/Model	Protocol	User	Client IP Address	Session Start	 Session End 	
192.168.10.254	Gateway	Core	Cisco ASA5508	SSH	admin	192.168.10.189	2025/06/21 09:38	2025/06/21 09:40	
192.168.10.254	Gateway	Core	Cisco ASA5508	SSH	admin	192.168.10.189	2025/06/21 00:21	2025/06/21 00:28	
10.0.0.249	Device1	Lab	Cisco WS-C2960S-24T	SSH	admin	10.0.40.161	2025/06/20 15:30	2025/06/20 15:40	

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.

```
Terminal Integration
```

```
Step 1: Tera Term Download
```

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

Download Tera Term

Step 2: Browser Integration

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

Install Integration For Tera Term 5

Install Integration For Previous Tera Term Versions

Note

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

Setup is now complete.

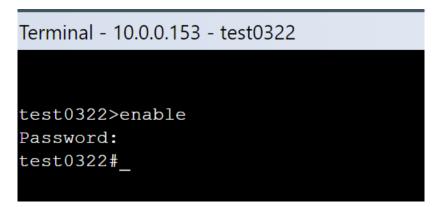
6.4.1.2 Start the terminal proxy If a device configuration backup has been obtained when you start the terminal proxy, you can skip selecting the protocol and entering the user name/password after starting the terminal proxy.

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].

$ \begin{array}{ c c c c c c } \hline \begin{tabular}{ c c c c } \hline \begin{tabular}{ c c c c c } \hline \begin{tabular}{ c c c c c c c } \hline \begin{tabular}{ c c c c c c c c c c c c c c c c c c c$	Search IP/H	lostname: 10.0.0.250 T Add	Criteria 🔻 🔇			
Image: Compare Configurations	IP Address	Hostname	Network	Adapter	HW Vendor	Model
Image: Compare Configurations	10.0.250	👶 Backup	Core	Cisco IOS	Cisco	CISCO1921/K
Image: Show Terminal Proxy Logs Image:		🔄 Open Terminal				
Compare Configurations Compare Compare Configurations Compare Compare Configurations Compare Compare Configurations Compare Compare Configurations Compare Compare Configurations Compare Compare Compar		🔄 Open Native Terminal				
Image: Spielay Job History Image: Spielay Job History Image: Spielay Job History		Show Terminal Proxy Logs				
test Test2 Test3		Compare Configurations				
Test2 Test3		💱 Display Job History				
Test3		test				
		Test2				
Web Browser		Test3				
		Web Browser				

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.

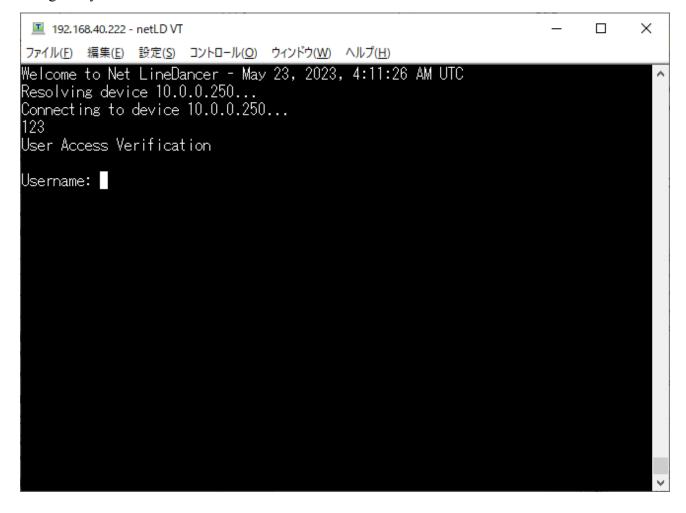


6.4.1.2.2 Use Tera Term

- 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].

F Inventory Chan		Search Compliand	ze Zero-Touch		
IP Address	Hostname	Network	Adapter	HW Vendor	Model
10.0.250	👶 Backup	Core	Cisco IOS	Cisco	CISCO1921/K9
п	🛐 Open Terminal				
Ţ	🔄 Open Native Terminal				
	Show Terminal Proxy Logs				
i l	Compare Configurations				
1	💱 Display Job History				
1	test				
J	Test2				
	Test3				
	Web Browser				

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.)

Session Date: Past	t 7 days 🔻 🗙 Add C	riteria 🔻 🔕 🕤							📑 Ехр
Device IP Address	Device Hostname	Network	Make/Model	Protocol	User	Client IP Address	Session Start	 Session End 	
192.168.10.254	Gateway	Core	Cisco ASA5508	SSH	admin	192.168.10.189	2025/06/21 09:38	2025/06/21 09:40	
192.168.10.254	Gateway	Core	Cisco ASA5508	SSH	admin	192.168.10.189	2025/06/21 00:21	2025/06/21 00:28	
10.0.0.249	Device1	Lab	Cisco WS-C2960S-24T	SSH	admin	10.0.40.161	2025/06/20 15:30	2025/06/20 15:40	
1-3 of 3									
Gateway - 192.168			25/06/21 00:21:44 - 0						

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

ompliance Policy Rule Sets	Search Compliance Zero-Touch			
				🕂 Create Rename Enable 😹 Delete 🛙
Compliance Policy	 Devices Covered 	Devices Violating	Violating	In Compliance
SSH Only	36	29	81%	19%
Core ASA rules	1	0		100%

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

Compliance Policy - snmp ×					
Compliance Policy - snmp publi	c				
O All Devices Search Static li	ist				
Search IP/Hostname: -Any- * Add Cr	riteria 👻				
IP Address	▲ Hostname	HW Vendor	Model	Device Type	Serial#
0 10.0.0.128	tech	Cisco	CSR1000V	Router	9J4P873SEIN
10.0.0.212	shibata	Foundry	snFES4802Switch		
0 10.0.213	S3100	H3C	S3100-26T-SI	Switch	210235A15DC10B000028
10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGVMEVXMYGAQ9H4A
0 10.0.2.30	Summit48i	Extreme	Summit48i	Switch	0145M-01540
2 10.0.2.50	010203_byte	Alaxala	AX24305-24T	Switch	85G015
2 10.128.0.4	NER3-A		CRS-16/S	Router	
I0.128.0.7	CR12-8	Cisco	CRS-8/S	Router	TBA09500081

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.

ompliance Policy - snmp 💥		
ompliance Policy - snmp p	oublic	
Adapter: Cisco IOS		select a test config
Configuration:/running-config		select a test comig
Rule Set	Severity	
SNMP - Public	Error	

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

Severity

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

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.

ategory: <aii></aii>	~	🕂 Create 🦪	Rename 📗 Copy 🔀 Delete 🔥 Category	Description
ule Set	Adapter	Config	Category	
DS Interface Auto-Duplex/Speed	Cisco IOS	/running-config		
DS Secure Enable Passwords	Cisco IOS	/running-config		
DS Telnet Restricted Access	Cisco IOS	/running-config		
DS SSH-only Restricted Access	Cisco IOS	/running-config		
OS Disabled Unneeded Services	Cisco IOS	/running-config		
DS Session Idle Timeout	Cisco IOS	/running-config		
DS Auto-Duplex/Speed	Cisco IOS	/running-config		
DS Rule	Cisco IOS	/running-config		
ASA] No console logging	Cisco ASA	/running-config		
estRule	Cisco IOS	/running-config		
uniper Test	Juniper ScreenOS	/saved		
et-active-config	Juniper JUNOS	/set-active-config		
lways violate	Cisco IOS	/running-config		
ITP Rule	Cisco IOS	/running-config		

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.

Rule Set - IOS Disabled Un × Rule Set - TestRule ×				2
Rule Set - TestRule		G	eneral	Rules
Description:	Category: <not set=""> V</not>			
Source: Cisco	This rule set applies to this configuration: /running-config			
One of the most common causes of performance issues on 10/100 Mb Ethernet links	O Apply to the whole config			
occurs when one port on the link operates at half-duplex while the other port operates at full-duplex. This occurs when one or both ports on a link are reset	Apply to blocks			
and the auto-negotiation process does not result in both link partners having	○ Template			
the same configuration. It also can occur when users reconfigure one side of a	O Partial Template			
link and forget to reconfigure the other side. Both sides of a link should have	-			2 Rules
auto-negotiation on, or both sides should have it off. Cisco recommends to leave auto-negotiation on for those devices compliant with 802.3u.	Restrict the visibility of this rule set to the following networks			
auto-negotiation on tor those devices compliant with 802.50.	Default			^
	Maptoppe			
	E servers			
				- 11
				_
				- 1
				- 1
				- 8
				- 8

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.

e Set - IOS Session	Idle Timeout				General	Ru
olation Message: Idle ses	sion timeout not configur	ed on VTY ~VTY~		select a test config		
art: line vty ~VTY~		End: !				
Natch Expression		Action				
xec-timeout ~timeout~		Violation if not m	atched			
ariable	Туре		Restriction			
ſΤΥ	text		*			
meout	text		*			

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.
Туре	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 screenshots. The examples below will generate a violation when the SNMP community setting is "public" in the Cisco IOS device configuration.

ategory: <aii></aii>	~		🕂 Create 🦪	Rename Copy	🖌 Delete 🔒 Category	Description:
Rule Set	Adapter	Config		Category		
OS Interface Auto-Duplex/Speed	Cisco IOS	/running-config				
OS Secure Enable Passwords	Cisco IOS	/running-config				
OS Telnet Restricted Access	Cisco IOS	/running-config				
OS SSH-only Restricted Access	Cisco IOS	/running-config				
OS Disabled Unneeded Services	Cisco IOS	/running-config				
OS Session Idle Timeout	Cisco IOS	/running-config				
OS Auto-Duplex/Speed	Cisco IOS	/running-config				
OS Rule	Cisco IOS	/running-config				
ASA] No console logging	Cisco ASA	/running-config				
FestRule	Cisco IOS	/running-config				
uniper Test	Juniper ScreenOS	/saved				
set-active-config	Juniper JUNOS	/set-active-config				
always violate	Cisco IOS	/running-config				
NTP Rule	Cisco IOS	/running-config				

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.

Rule Set		
Name:		
SNMP - Publid		
Adapter:		
Cisco IOS		~
Configuration:		
/running-config		~
Category		
<not set=""></not>		~
	ок	Cancel

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.

*Rule Set - SNMP - Public ×			
Rule Set - SNMP - Public			
Violation Message: SNMP community set to public			
Match Expression	Action		
snmp-server community public ~mode~	Violation if not mat	bed	
			🖕 🗶 😚 🕹
	Туре	Restriction	
mode	text		
Ignore Case			iation job:None 🔔 🤪

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

*Rule Set - SNMP - Public ×				
Rule Set - SNMP - Public				
Violation Message: SNMP community set to public				
Match Expression		Action		
snmp-server community public -mode-		Violation on match		
				🕂 🗙 🕆 🕹
Variable	Туре		Restriction	
mode	text			
Ignore Case			Pe	emediation job:None 📖 🔞
-,				

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.

*Rule Set - SNMP - Public × Rule Set - SNMP - Public			
Match Expression			
snmp-server community public ~mode~	spe SIMP community set to public simular to publicIncode- Violation on match		
			🔶 🗶 🛧 🕹
Variable	Туре		Restriction
mode	text		
Ignore Case			Remediation job:None 🔐 😮

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.

 Hostname 	Network
tech	Default
NER3-A	Default
CR12-B	Default
	tech NER3-A

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.

	Gener	al Rules
10.0.0.128	select a test config	Failures:
200	access-list 2500 deny ip host 10.0.0.92 any	
201	access-list 2500 deny ip host 10.0.0.93 any	
202	access-list 2500 deny ip host 10.0.0.94 any	
203	access-list 2500 deny ip host 10.0.0.95 any	
204	access-list 2500 deny ip host 10.0.0.96 any	
205	access-list 2500 deny ip host 10.0.0.97 any	
206	access-list 2500 deny ip host 10.0.0.98 any	
207	access-list 2500 deny ip host 10.0.0.99 any	
	access-list 2500 deny ip host 10.0.0.100 any	
209	access-list 2500 deny ip host 10.0.0.101 any	
210	access-list 2500 deny ip host 10.0.0.102 any	
211	access-list 2500 deny ip host 10.0.0.103 any	
212	access-list 2500 deny ip host 10.0.0.104 any	
213	access-list 2500 deny ip host 10.0.0.105 any	
214		
215	snmp-server community public RO	
216	snmp-server community test RO	
217	snmp-server community a RO	
218	snmp-server community ro RO	
219	snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart	
220	snmp-server enable traps vrrp	
221	snmp-server enable traps pfr	
222	snmp-server enable traps flowmon	
223	snmp-server enable traps call-home message-send-fail server-fail	
224	snmp-server enable traps tty	
225	snmp-server enable traps casa	
226	snmp-server enable traps ospf state-change	
227	snmp-server enable traps ospf errors	-
228		

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.

				🕂 Create Rename Enable 💥 Dele
Compliance Policy	 Devices Covered 	Devices Violating	Violating	In Compliance
SSH Only	36	29	81%	19%
Core ASA rules	1	0		10

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

Compliance Policy		
Name:		
SNMP public		
Adapter:		
Cisco IOS		~
Configuration:		
/running-config		~
	ОК	Cancel

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

Compliance Policy - SNMP ×						
Compliance Policy - SNMP pu	ublic					Devices Rule Sets Status
🔿 All Devices (Search 🔿 Stat	tic list					
Search IP/Hostname: -Any- * Add	d Criteria 👻					
IP Address	 Hostname 	HW Vendor	Model	Device Type	Serial#	Traits
0 10.0.0.128	tech	Cisco	CSR1000V	Router	9J4P873SEIN	https icmp nom snmp ssh teinet web
10.0.0.212	shibata	Foundry	snFES4802Switch			(http://ttps.lonp.ncm.snmp.teinet.web)
0.0.0.213	\$3100	H3C	S3100-26T-SI	Switch	210235A15DC10B000028	(cmp ncm snmp ssh) teinet
10.0.0.232	Fortigate-VM64	Fortinet	FortiGate-VM64	Firewall	FGVMEVXMYGAQ9H4A	(http://cmpincmissnmpisshitelnet.web)
0 10.0.2.30	Summit48i	Extreme	Summit48i	Switch	0145M-01540	(http://cmpincmisnmpitelnet_web)
10.0.2.50 10.0.2.50	010203_byte	Alaxala	AX24305-24T	Switch	85G015	ncm snmp
10.128.0.4	NER3-A		CRS-16/S	Router		(icmp) (ncm) (snmp)
10.128.0.7	CR12-8	Cisco	CRS-8/S	Router	TBA09500081	(Icmp) nom (snmp)

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.

	1
Severity	
	Severity Sev

5. Select a Rule Set and click the 🕩 button.

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

	Add Rule Sets	
Category	<all></all>	~
IOS Inter	face Auto-Duplex/Speed	
IOS Secu	re Enable Passwords	
IOS Telne	t Restricted Access	
IOS SSH-	only Restricted Access	
IOS Disat	oled Unneeded Services	
IOS Sessi	on Idle Timeout	
IOS Auto	-Duplex/Speed	
IOS Rule		
test11		
TestRule		
always vi	olate	
cisco test		
SNMP - F	ublic	
		Add Cancel

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.

blic ×						
	Action					
	Violation if not matche	Violation if not matched Stop if not matched				
	Violation if not ma					
			♣ X ☆ ₽			
Туре		Restriction				
text						
	Туре	Action Violation if not me Stop if not matche Stop on match Violation on match Violation on match	Action Violation if not matched Stop if not matched Stop or match Violation if not matched Violation on match Type Restriction			

7. Save the policy.

ce Policy - SNM × *Rule Set - SNMP - Public ×			
Set - SNMP - Public			H
in Message: SNMP community set to public		select a test config	
latch Expression	Action		
mp-server community public ~mode~	Violation if not matched		

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.

Compliance Policy	Rule Sets											
						🔶 Create	Rename	Enable	🔀 Delete	Device Violation Summary		
Compliance P •	Network	Devices Cover	Devices Violat	Violating		In	Compliance				-	
🖤 testcisco	Lab	1	0						100%		6	
🖤 ntp policy	Lab	52	0							52		
🍿 banner	Lab	1	0						100%			
🖤 banner	Default	0	0									
💓 ZPE Nodegrid	Lab	1	1	100%								
😻 SSH Only	Core	3	1		33%				67%			
IOS Services	Lab	52	0									
iOS Secure Enabl	Lab	52	50	96%			4%					
1 IOS SSH Policy	Lab	52	0								×	
IOS Disabled Tel	Lab	52	0								188	
IOS Auto-duplex	Lab	0	0									
Core ASA rules	Core	1	0						100%			

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

(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.

Compliance Policy - SNMP public Devices Rule Sets Stat								
IP Address	Hostname	Rule Set	Message					
10.0.0.128	tech	SNMP - Public	SNMP community set to public					

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

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.

Inventory Changes Jobs Terminal Proxy Se Job History Job Management	earch Compliance Zero-Touch			Network Core v scorreals	e Logout Settings H
🔛 👻 Add Criteria 👻 🖪 🕤			19.	Audit Log 💲 Open Job 🙀 Delete 🖋 Rename 📄 Copy 🙆 Run Now	😵 New Job 📴 Filte
Name	Туре	Approval Requester	Approval Status	Memo	👶 Backup
🛞 Add ASA VPN User	Smart Change		Not Requested	Creates a new VPN user on our ASA	S Discovery
👶 add ntp server	Smart Change		Not Requested		Reighbors
👶 Auto Duplex	Smart Change		Not Requisted		Report
🛞 Auto-Duplex-Speed	Smart Change		Not Requested		Smart Change
% Cisco Access Lists	Tool		Not Requested		% Tool
No Cisco Interfaces	Tool		Not Requested		
% Cisco Show Commands	Tool				
18 Core decovery	Discreate				

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

Create Smart Change Job		
Job Name:		
snmp public		
Network:		
Default, laptoppc, servers		-
Comment:		
✓ Use remediation job.		
Adapter: Cisco IOS		~
Use the same replacement values for all devices in the job.		
\bigcirc Use unique replacement values for each device in the job.		
	ОК	Cancel

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

This is used for linking with Rule Sets.

Create Smart Change Job	
Job Name:	
snmp public	
Network:	
Default,laptoppc,servers	-
Comment:	
✓ Use remediation job.	
Adapter: Cisco IOS	~
Use the same replacement values for all devices in the job.	
\bigcirc Use unique replacement values for each device in the job.	
	OK Cancel

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

*snmp p	ublic	×							
🔠 Te	mplate 🧘	Replacement Values 🛛 😂	Devices	Schedule	😏 Job Approvals Lo	g 🛛 Em	ail Notif	ation	🔛 🖬
								Commands	Replacements
	Command					×	3	conft smmp-server community public RO exit	
	conf t snmp-serv exit wr	ver community public R	o				4	*e	
	End								
	Don't D	xit							

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.

Notificat	lon		4 4
	Commands	Replacements	
1 2 3 4	conft snmp-sever community public NO exit	Apparenteria	
Prompt		嘴 🕆 🌵 🧷	1 24

6. Enter the variable "Name" and click [OK].

	Add Replacement						
Selection:	public						
Name	communitystring]					
Туре	Text ~						
	✓ Use selection as default value						
	OK Cancel						

7. Save the settings.

ate 🥏 Replacement Values 😒 Devices 🕥 Schedule 🖸	Job Approvals Log 🛛 🖂 En	nail Notific		
			Commands	Replac
			f t p-server community <mark>(communitystring)</mark> RO	🥏 communitys
Command	×	3		
conf t smmp-server community{ communitystring} R0 wct				
End				
Don't Exit				

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

Compliance Policy Rule Sets			
Category: <aii></aii>	*		🕂 Create 🖋 Rename 📄 Copy 🔀 Delete 🔥 Category
Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Rule	Cisco IOS	/running-config	
[ASA] No console logging	Cisco ASA	/running-config	
TestRule	Cisco IOS	/running-config	
Juniper Test	Juniper ScreenOS	/saved	
set-active-config	Juniper JUNOS	/set-active-config	
always violate	Cisco IOS	/running-config	
NTP Rule	Cisco IOS	/running-config	
somo public	Cisco IOS	/rupping-config	

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

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

Rule Set		
Name:		
community public		
Adapter:		
Cisco IOS		~
Configuration:		
/running-config		~
Category		
<not set=""></not>		~
	ОК	Cancel

10. Click the 🕩 button to add "Match Expression".

Rule Set - community public 🙁		
Rule Set - community public		
Violation Message: community public		se
Match Expression	Action	
	♣ ※ ☆ 용	

- 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.

*Rule Set - community pu ×							
Rule Set - community public						General	General
Violation Message: invalid community string					select a test config		
Match Expression		Action					
snmp-server community ~communitystring~ RW		Violation if not matched					
			🕂 🗙 🕤	2			
Variable	Туре		Restriction				
communitystring	text						
Ignore Case			Remediation job:None	0			

13. Set the Action to "Violation on match."

*Rule Set - community pu × Rule Set - community public					
Violation Message: invalid community string					select a
Match Expression		Action			
snmp-server community ~communitystring~ RW		Violation if not matche	d	~	
		Stop if not matched Stop on match Violation if not matched Violation on match			
Variable	Туре		Restriction	🔶 🗙 🕆 8.	
variable	туре		Restriction		

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.

IOS Rule	Cisco IOS	/running-config					
[ASA] No console logging	Cisco ASA	/running-config					
test11	Cisco IOS	/running-config			Remediation job		
TestRule	Cisco IOS	/running-config			Remediation job		
Juniper Test	Juniper ScreenOS	/saved		Name	Memo		
set-active-config	Juniper JUNOS	/set-active-config		snmp public			
always violate	Cisco IOS	/running-config					
Test	A10 ACOS	/running-config					
cisco test	Cisco IOS	/running-config					
palaalot	Palo Alto Networks	/set-running-config.txt					
*Rule Set - community pu ×							
Rule Set - community public							
Violation Message: invalid community string							
Match Expression		Action					
snmp-server community ~communitystring~ R	W	Violation if not matched					
						ок	
						OK	Cancel
				+	X & &		
Variable	Туре	Restr	iction				
communitystring	text						
Ignore Case				Remediation jol	b:None 🕜		

15. Save your settings.

-				
*Rule Set - community pu ×				
Rule Set - community public				
Violation Message: invalid community string				
Match Expression		Action		
snmp-server community ~ communitystring~ RW		Violation if not matched		
anip-sever commany -commany.org - ww		Profession II nov mercines		
				🕂 🗶 🕜 🕹
Variable	Туре		Restriction	
communitystring	text			
Ignore Case			a	c snmp public X 🛄 🔞
C) give care			Remediation job	c samp public 🔬 🛄 🐠

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

Compliance Policy Rule Sets	oxy Search Compliance Zero-Touch			
interversion and a sets				🕂 Create Rename Enable
Compliance Policy	 Devices Covered 	Devices Violating	Violating	In Compliance
snmp public	36	0		
SSH Only	36	29	81%	19%
Core ASA rules	1	0		

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

Compliance Policy	
Name:	
Cisco IOS community	
Adapter:	
Cisco IOS	~
Configuration:	
/running-config	~
ок	Cancel

18. Click the া button.



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

		Add	Rule Set	ts		
Category	<all></all>					~
IOS Secu	re Enable	Password	ds			
IOS Inter	face Auto	-Duplex/	Speed			
IP Loggir	ng					
C3560 Te	mplate					
SNMP Se	erver Com	munity S	tring			
snmp-sei	rver-rule					
Server Ho	ost					
IP Permit						
IP Permit	2					
test rege	x					
ntp test						
new test	regex					
user_pass	sword					
Hostnam	e rule					
interface	rule					
commun	ity public					-
						Const
					Add	Cancel

20. Click [Save].

mpliance Policy - Cisco ×		
mpliance Policy - Cisco IO	community	
Adapter: Cisco IOS		select a test config
Configuration:/running-config		select a test coming
Rule Set	Severity	
community public	Error	

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

Compliance Policy Rule Sets				
				🕂 Create Rename Enable
Compliance Policy	 Devices Covered 	Devices Violating	Violating	In Compliance
snmp public	36	0		
SSH Only	36	29	81%	19%
Core ASA rules	1	0		

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.

Job History Job Management					
🔛 🔻 Approval Status: -Any- 👻 X Job Name: -Any-	* X Job Type: -Any- * X 🔕 🌜		10. Aue	Sk Log 🖏 Open Job 🙀 Delete 🥜 Rename 📄 Copy 🙆 Run Now	💲 New Job 📑 Filts
Name	Туре	Approval Requester	Approval Status	Memo	👶 Backup
 Add ASA VPN User add ntp server 	Smart Change		Not Requested	Creates a new VPN user on our ASA	S Discovery
🚸 add ntp server	Smart Change		Not Requested		Reighbors
🚸 Auto Duplex	Smart Change		Not Requested		Report
Auto-Duplex-Speed Gisco Access Lists Cisco Interfaces	Smart Change		Not Requested		Smart Change
No Cisco Access Lists	Tool		Not Requested		No Tool
% Cisco Interfaces	Tool		Not Requested		
% Cisco Show Commands	Tool				
1 Core discovery	Discovery				
L Daily changes	Report				

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

OK Cancel

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

This is used for linking with Rule Sets.

Creat	e Smart Change Job	
Job Name:		
access list		
Network:		
Default		•
Comment:		
✓ Use remediation job.		
Adapter: Cisco IOS		~
O Use the same replacement values for all	devices in the job.	
\bigcirc Use unique replacement values for each	device in the job.	
		OK Cancel

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

×			
late Replacement Values 📚 Devices 🔕 Schedule 📀 Job	Approvals Log 🖸 Email Notification	Commands	Replacements
Command	× conf t interface interfacenumber ip access-group 1 in	Comments	периосники
conf t interface interfacenumber jp access-group 1 in exit	4 exit		
\odot			
End			
Don't Exit			
	Prompt		** + +

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.

	Commands	Replacements
1	conf t	
2	interface interfacenumber	
3	ip access-group 1 in exit	
4	exit	
Promp	ε	😘 🕆 🤚 🖊 💥

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

	Add Replacement	
Selection:	interfacenumber	
Name	interfacenumber	
Туре	Text	~
	✓ Use selection as default value	
		OK Cancel

7. Click [Save].

*access li	t ×						>
🔠 Ten	nplate ĉ Replacement Values 🗧	Devices 🛛 🚱 Schedule	🕑 Job Approvals Log 🛛 Ema	I Notific	cation		ü
					Commands	Replacements	
				1	conft	2 interfacenumber	
	Command		×	3	ip access-group 1 in exit		
	<pre>conf t interface {interfacenumber} ip access-group 1 in exit</pre>			,	9812 		
	End						
	Don't Exit						

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

Inventory Changes Jobs Terminal Pr	roxy Search Compliance Zero-Touch		
Compliance Policy Rule Sets			
Category: <aii> ~</aii>		🕂 Create	🥙 Rename 📄 Copy 🔀 Delete 🔒 Category
Rule Set	Adapter	Config	Category
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config	
IOS Secure Enable Passwords	Cisco IOS	/running-config	
IOS Telnet Restricted Access	Cisco IOS	/running-config	
IOS SSH-only Restricted Access	Cisco IOS	/running-config	
IOS Disabled Unneeded Services	Cisco IOS	/running-config	
IOS Session Idle Timeout	Cisco IOS	/running-config	
IOS Auto-Duplex/Speed	Cisco IOS	/running-config	

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

Rule	Set
Name:	
ACL interface	
Adapter:	
Cisco IOS	· · · · · · · · · · · · · · · · · · ·
Configuration:	
/running-config	
Category	
<not set=""></not>	•
	OK Cance

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

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

*Bule Set - ACL Interface X			
Rule Set - ACL interface		🔛 Ger	neni Rales
Description	Company +Net set · · ·		
	This rule set applies to this configuration: /wwwing-config		
	Apply to the whole contig		
	 Apply to blocks 		
	C Tempters		
	O Partia Tempiano		
	Induits the validity of this rule set to the following networks.		
	El Colorit		
	E term		
	E cered		
	E laven		
	E Mindow		

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

*Rule Set - ACL Interface × Rule Set - ACL interface Violation Message: ACL interface				
Rule Set - ACL interface			Gener	ral Rule
Violation Message: ACL interface		select a test config		
Start interface interdacenum	End 1			
Match Expression	Action			

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.

"Rulo Set - ACL interface X				
Rule Set - ACL interface				
Valation Message: ACL interface				
Surt interface - interdacemen-		the I		
Match Expression		Action		
				A 10 0
Variable	Турн		Restriction	
interdacerson	tert			
Ignore Case				Remediation job/None 🔔 🔒

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

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

				-
*Rule Set - ACL interface ×				
Rule Set - ACL interface				
Violation Message: ACL interface				
Start: interface ~interdacenum ~		End: I		
Match Expression		Action	Rule Variable	
			Variable Type:	
			text	``
			Restriction:	
			GigabitEthernet#	
				_
			OK Can	lance
	Туре		Restriction	
interdacenum	text			
Ignore Case			Remediation job:None 🔔 🤫	0

14. Click the 🕩 button to add matching conditions.

*Rule Set - ACL interface ×				
Rule Set - ACL interface				
Violation Message: ACL interface				
Start: interfaceinterdacenum		End: I		
Match Expression		Action		
no ip address		Violation if not matched		
ip access-group 1 in		Violation if not matched	Violation if not matched	
				💠 🗶 😯 🐣
Variable	Туре		Restriction	
interdacenum	text		GiabitEthernet*	

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.

*Rule Set - ACL interface ×				¥							
Rule Set - ACL interface					Remediation job			General	R		
olation Message: ACL interface						Name		Memo			
Start: interface interdacenum-		End: I				access list					
Match Expression		Action				ntp fix qos *2					
no ip address		Violation if not matched				400 L					
ip access-group 1 in		Violation if not matched									
				🔶 🗶 😯 🕔							
Variable	Туре		Restriction								
interdacenum	text		GiabitEthemet*								
								OK Cancel			
Ignore Case				iation job:None 📖 🔞							
C) ignore case			Remed	iation job:None 🐨							

16. Save your settings.

*Rule Set - ACL interface ×				
Rule Set - ACL interface				
Violation Message: ACL interface				
Start interface ~interdacenum~		End: !		
Match Expression		Action		
no ip address		Violation if not matched		
ip access-group 1 in		Violation if not matched		
				💠 🗶 😚 🐥
Variable	Туре		Restriction	
interdacenum	text		GiabitEthernet*	
Ignore Case			Remediation j	ob: access list X 🔔 🥝
77°F		-		

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

				💠 Create Rename Enable 😹 De
Compliance Policy	 Devices Covered 	Devices Violating	Violating	In Compliance
snmp public	36	0		
SSH Only	36	29	81%	19%
Core ASA rules	1	0		

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

Compliance Policy	
Name:	
Cisco IOS ACL	
Adapter:	
Cisco IOS 🗸 🗸	
Configuration:	
/running-config v	
OK Cancel	

19. Click the 🕩 button.



20. Add a Rule Set.

Add Rule Sets							
Category	<ali></ali>				~		
IOS Inter	face Auto-D	uplex/Spe	ed				
IP Loggir	ıg						
C3560 Te	mplate						
SNMP Se	erver Comm	unity String)				
snmp-se	rver-rule						
Server He	ost						
IP Permit							
IP Permit	2						
test rege	x						
ntp test							
new test	regex						
user_pas	sword						
Hostnam	Hostname rule						
interface	interface rule						
commun	ity public						
ACL inter	face				-		
				Add	Cancel		

21. Click [Save].

*Compliance Policy - Cisco ×					>
Compliance Policy - Cisco IOS ACL			Devices R	ule Sets	Status
Adapter: Cisco IOS Configuration:/running-config		select a test config			
Configuration:/running-config					
Rule Set	Severity				
ACL interface	Error				

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

Y Inventory Changes Jobs Terminal Proxy Search	Compliance Zero-Touch			
Compliance Policy Rule Sets				
19			🔶 Cre	ate Rename Enable 🔀 Delete
	 Devices Covered 	Devices Violating	Violating	In Compliance
Cisco	58	0		
📜 🔰 cisco OSversion	53	24	45%	55%
🔟 🖤 Test	0	0		
SNMP RWモード違反	52	2	4%	96%
🗍 💗 Microsens	1	1	100%	
🖞 🖤 ASA	8	0		

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:

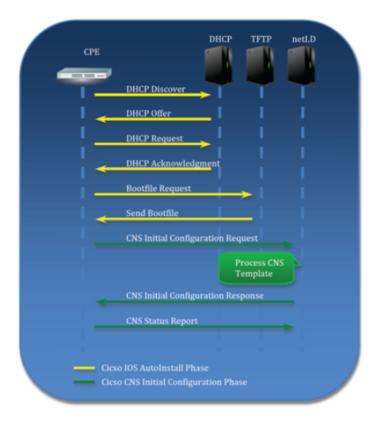
-**Template**: Distribute configurations based on templates. Used when introducing a new device to the network at a remote office.

-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.

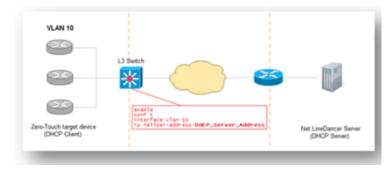


6.7.2 Zero-Touch requirements

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.

			Server S	ettin	gs		
Data Retention System Backup Mail Server	Î	PnP Server:	auto Enable PnP D	ebug	ging	ןיי כו	ı.ı ı. sco
SNMP Traps	н	Address P	ools				
Users		Enable D	HCP Server		Address Pool	Relay Serve	er 🧅
Roles	н	Lease Time:	5 minutes	~	Default	none	
External Authentication		cease mile.			Derdant	none	er 🔮
Custom Device Fields	н						
Memo Templates							
Launchers							
Smart Bridges							
Networks							
Network Servers							
Syslog							
Zero-Touch							
Software Update							
Web Proxy							
Change Approvals							
Cisco API							
SNMPv3 User	•						
							OK Cancel
Item	E	Explanation	1				
Enable DHCP server	C	Check this l	box if you wa	ant	to use NetLD's D	HCP server.	
lease time	S	Set the DH	CP lease time	e .			

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

Pool Name:		lvilogic				
Relay Server	CIDR:	192.168.0.254	/	32		
Address Ran	ge:	10.0.0.100	-	10.0.0	0.105	
Subnet Masl	с	255.255.255.0				
Overrides						
Gateway:	10.0.0	10.0.0.254				
DNS Server: 192.1		68.0.3				

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

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

Address Po	ools			
Enable D	HCP Server		Address Pool	Relay Server
Lease Time:	5 minutes	*	Default	none
			lvilogic	192.168.0.254/32

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.

マモプション	?	x
全般 詳細設定		
□ 040 NIS ドメイン名 ネ □ 041 NIS サーバー ク □ 042 NTP サーバー ネ ☑ 043 ペンダー固有情報 指	明 ットワーク ライアント ットワーク 定された BNS ア	
□ 044 WINS/NBNS 9-//- N < Ⅲ データ入力 データ(<u>D</u>): バイナリ: ASC	>	
0000 35 41 31 44 3B 4B 34 3B 5A1D;K4; 0008 42 32 3B 49 31 39 32 2E B2;1192. 0010 31 36 38 2E 31 30 30 2E 168.100. 0018 31 39 30 190		
OK キャンセル	適用	(A)

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.

nventory Changes Jobs	Terminal Proxy Search	Compliance	Zero-Touch
Configurations Templates	History		Configuration
Template	Description		
WS-3650			
network-confg	Basic CNS Initial Template		
		+ ×	
Replacements			

- 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.

	Add Configuration Template
	PnP Dynamic Template
Template Type:	O AutoInstall Static Template
	O PnP ID-less Static Template
Template Name:	test template
Description:	
	OK Cancel

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.

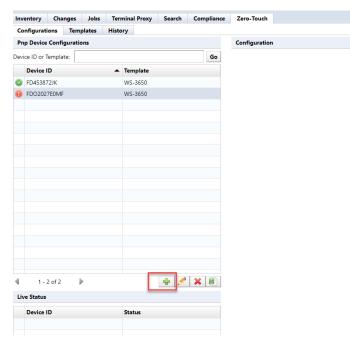
onfigurations Templates History	
emplates	Configuration - test template
Periphetes periphetes periphetes periphetes is-3650 etwork-confg Basic CNS Initial Template st template ist template	<pre>congutation test tempare 1 cns ich hardware-serial 2 l 3 cns connect ons-profile ping-interval 10 retries 3 sleep 5 4 discover interface FastEthernet 5 template connect cns-profile 6 l 7 cns template connect cns-profile 8 cli description Basic CNS Initial Template 9 clii ip address dhcp 10 cli ip route 0.0.0.0 0.0.0.0 \${interface} 11 cli no shutdown 12 exit 13 l 14 cns config initial {netld-host} status {netld-status} 15 l 16 end 17 </pre>
4	*
eplacements	

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.

	А	В	С	D	E	F	G	H		*
1	CNS Device ID	Template	hostname	enable pas	VTY passw	IP address	Mask	community	type	
2	FHK134570SY	1812J	1812J	lvi	lvi	192.168.0.1	255.255.255.0	lvi	RW	
3										
4										
5										-
I4 - 4	K ← ► N Net LineDancer /									

6. Return to NetLD, and click [Zero Touch] > [Configuration] again.

7.	Select	[Import]	Template	l from the	menu that	appears.
<i>.</i> .	~~~~~					

Inv	entory Char	nges Jobs	ler	minal Proxy	Search	Compliance	∠ero-louch
Co	onfigurations	Templates	Histo	ory			
Pn	p Device Config	gurations					Configuration
Dev	ice ID or Templat	te:				Go	
	Device ID		•	Template			
0	FD453872JK			WS-3650			
0	FDO2027E0MF			WS-3650			
4	1 - 2 of 2	▶			+ 🥖	×	
Liv	ve Status						port configurations for template
	Device ID			Status			ve empty Excel import file
	Device ID			Status		Exp	port configurations for template to Excel

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.

Inv	entory	Chan	ges	Jobs	Terr	mina	l Proxy	Search	Complia	nce Z	ero-Touch
Co	nfigurati	ons	Tem	plates	Histo	ory					
Pn	p Device	Config	urati	ons						C	onfiguratior
Devi	ce ID or Te	emplate	e:						Go	•	
	Device I	D			•	Tem	plate				
0	FD45387	2JK				WS-	3650				
0	FDO2027	7E0MF				WS-	3650				
										_	
										_	
4	1 - 2	2 of 2		Þ				+./	×		
Liv	e Status						_				
	Device I	D				Stat	us				

- 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.

	_	
Device ID:	FHK104780MN	
Deployment Type:	Self-Recovery	~
		OK Cancel

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

6.7.7 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.

Configurations Templates History Pnp Device Configurations Configuration Device ID or Template: Go Pevice ID Poblation Poblation Device ID Poblation Device ID Poblation Device ID Poblation Device ID Device ID Poblation Device ID Device ID Poblation Device ID Device ID Device ID Device ID Device ID Template WS-3650 WS-3650 WS-3650 Device ID WS-3650 WS-3650 WS-3650 WS-3650 WS-365
Device ID or Template: Go Device ID Template Image: Specific Product of the system of
Device ID Template Image: State of the state o
 FD453872JK WS-3650
Image: PDO2027E0MF WS-3650 Image: PDO2027E0MF Image: PDO2007E0MF Image: PD02027E0MF Image: PD020F Image: PD02027E0MF Image: PD0200F Image: PD02027E0MF Image: PD0200F Image: PD0200F Im
Image: section
Image: selection sel
Image: selection sel
Image: Section of the section of th
Image: Note of the sector of
Image: Constraint of the sector of the sec
Image: selection sel
Image: select
Image: Problem in the second secon
Image: Constraint of the second se
▲ 1 - 2 of 2 🕨 🕂 🗱
Live Status
Device ID Status

- 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.

PnP Device Configuration						
Device ID:	FHK104780MN					
Deployment Type:	Specific Device Recovery V					
Recovery Device ID:	FHK221816MN					
	OK Cancel					

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

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

6.7.8 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.)

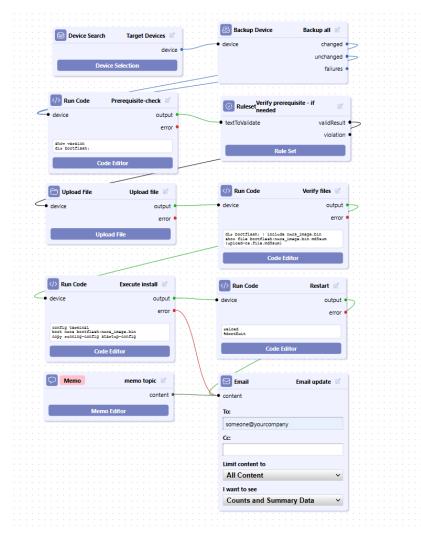
6.8 Playbook

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.

0	Dashboards	Inventory	Changes	Jobs	Terminal Proxy	Search	Compliance	Monitors	Incidents	Мар	MIBs	Playbook	Network: <aii< th=""><th>></th></aii<>	>
ThirdEye Suite	Playbooks												🗃 Import 🔮 Add 🖉 Edit 🔀 Delete	History
ird	🔛 🔻 Туре:	-Any-	+ × Name	: -Any-	→ × Autho	r: -Any-	- × ×	5						₩ -
Ē														Status: -Any-
Su														Name: -Any-
ite														Add Criteria 👻 🄇

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

Add New Playbook					
Name:					
Job - Show Version					
Description					
show version for devices					
	OK Close				

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 solution in the top right corner of the node to give the node a description.

Unsaved Job - Show Version 🖉	⊥	\triangleright	7	8	Nodes
					And Only proceed after both inputs have received a signal.
					Backup Device Run a device backup.
Device Search Humble_Glacier					Chat App (Webhook) Send basic results to a chat app via webhook.
device •					Compliance Violation Get information from a Compliance RuleSet configured to run this Playb
Device Selection					Device Search Search for a number devices in the inventory to be acted upon.
Enter new alias This alias will be used in the notifications					Email Send an email with tabular data to someone.
Select Devices					Get information from an alert policy configured to run this Playbook.
OK <u>Cancel</u>					Save a note.

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

	-				_		evice	Selection						
	0) All Device	es 🔘 Sea	arch 🔘 Si	atic	list				Networ	ks: <u>Default</u>	t		
	Sea	rch IP/Hos	stname: -A	Any-	•	Add Criteria 🔻								
earch		IP Ad	Host	Netw	A	Interface IP	lel	Devic	OS V	Serial#	Back	Traits	Viola	
	\bigcirc	1.1.1.1		Default		Admin IP						http ht		
		10.0.0.1	sales-d	Default	Li	Hostname Status	NX	Server	23.2.1	LiveActi	1s	https ic		
	\bigcirc	10.0.0.2		Default		Last Changed						http ht		
_		10.0.0.6		Default		End Of Sale						http ht	No resp	
Dev		10.0.0.8		Default		End Of Life						http ht	No resp	
		10.0.0.9		Default		Software End Of Sale						http ht	No resp	
		10.0.0.10		Default		Software End Of Life						http ht	No resp	
		10.0.0.20		Default		Tags						icmp	No resp	
		10.0.0.21		Default		Vendor/Model/OS						icmp sr	Node 1	
		10.0.0.29		Default		Device Type						http ht	No resp	
		10.0.0.30		Default		Serial#						http ht	No resp	
		10.0.0.31		Default		MAC						https ic	No resp	
		10.0.0.32		Default		Config Text						https ic	No resp	-
	4	1 - 25	54 of 299		Ν	Severity Map	spec	ified. This	s job will	execute a	gainst a	ll devices v	vithin the	
					S	Monitor								
						Maintenance Window							Clos	se
						Device Traits								

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

0	All Device	s 🔘 Sear	rch 🔾 St	atic list					Networ	ks: <u>Defaul</u> t	t	
end	or/Mode	I/OS: Cisco	· ·	× Device	Type: Fi	rewall 👻	× Ad	d Criteria	-			
I	P Ad	Host	Netw	Adap	нw	Model	Devic	os v	Serial#	Back	Traits	Violation
) 1	0.0.2.2	FPR410	Default	Cisco A	Cisco	FPR-41	Firewall	2.3(1.88)	JMX232	1m17s	https ic	No respon
1	0.128	SIM000	Default	Cisco A	Cisco	ASA5585	Firewall	9.1(6)6	JAD123	6s	firewall	1
) 1	0.128	Cust1	Default	Cisco A	Cisco	WS-SVC	Firewall	4.1(5)	SAD070	1s	firewall	
1	0.128	asa-gw	Default	Cisco A	Cisco	PIX-520	Firewall			9s	firewall	
1	0.128	ciscoasa	Default	Cisco A	Cisco	ASA5510	Firewall	9.1(6)	JMX132	9s	firewall	
1	0.128	ciscoasa	Default	Cisco A	Cisco	ASA5510	Firewall	9.1(6)	JMX132	1s	firewall	
1	0.128		Default	Cisco A	Cisco	PIX-520	Firewall			1s	firewall	
1	0.128	VASTDC	Default	Cisco A	Cisco	ASA5550	Firewall	8.0(4)	JMX141	1s	firewall	

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.

> Run Code	run cli command 🛛 🖉
device	output
	error
Co	ode Editor
-	Code Editor
Commands	
1 sh version	
Prompt:	Don't Exit
•	Close

For Results you have three options:

Option

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

Sta

Device Search	Select Devices 🖉	Run Code	e run cli command 🖉	
	device •	• device	output •	
Device S	Selection	· · · · · · · · · · · · · · · · · · ·	error • • • • •	· ·
		sh version		
· · · · · · · · · · ·	· · · · · · · · · · · · · ·		Code Editor	
	🖂 Email	send to email 🖉	Chat App (Webhook) send to teams	ß
	• content		• content	
	To:		Webhook URL	
· · · · · · · · · · ·	someone@yourcompan	y .	url for hook	
	Cc:		Chat Application	
			Microsoft Teams	~
	Limit content to		Limit content to	
	Errore Only	✓	Errors Only	~
	Errors Only	•		
	I want to see		I want to see	
	Counts and Summ	nary Data 🗸 🗸	Counts and Summary Data	~
	Couries and Summ		Sound Sund Sunnary Data	

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

Next, connect the nodes.

				Chat App (Webhook) send to teams 🖉
				✓● content
				Content
				Webhook URL
			run cli command 🖉 🗐	
 		> Run Code	run cii command	url for hook
 😂 Device Search	Select Devices 🖉			
	/	 device 	output 🜱	Chat Application
	device 🌙			
	device		error •	Microsoft Teams v
Device S	election	sh version		Limit content to
		C.	ode Editor	Errors Only ~
			Due Eultor	
				I want to see
				Counts and Summary Data V
				🛛 🖂 Email 🛛 🛛 send to email 🖉
				• content
				То:
				someone@yourcompany
				Cc:
				Limit content to
				Errors Only
				Errors Only ~
				I want to see
				Counto and Summony Data
 				Counts and Summary Data v

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.

	-				Description:
Category: <aii></aii>	~			Delete 🔒 Category	Description.
Rule Set	Adapter	Config	Category		
IOS Session Idle Timeout	Cisco IOS	/running-config		^	
IOS Disabled Unneeded Services	Cisco IOS	/running-config			
IOS SSH-only Restricted Access	Cisco IOS	/running-config			
IOS Telnet Restricted Access	Cisco IOS	/running-config			
IOS Secure Enable Passwords	Cisco IOS	/running-config			
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config			
IP Logging	Cisco IOS	/running-config		Remediation job or pl	avbook
C3560 Template	Cisco IOS	/running-config			
SNMP Server Community String	Cisco IOS	/running-config	Remediation job	Remediation Playbook	
snmp-server-rule	Cisco IOS	/running-config	Name	Memo	
Server Host	Cisco IOS	/running-config	Job - Show Version	show v	ersion for devices
IP Permit	Cisco IOS	/running-config			
IP Permit 2	Cisco IOS	/runnina-confia			
Rule Set - ntp test ×					
Rule Set - ntp test /iolation Message: ntp test					
Rule Set - ntp test		Action			
Rule Set - ntp test /iolation Message: ntp test Match Expression		Action Violation if not matched			
Rule Set - ntp test /iolation Message: ntp test Match Expression					
Rule Set - ntp test /iolation Message: ntp test Match Expression					
Rule Set - ntp test /iolation Message: ntp test					OK Cancel
Rule Set - ntp test /iolation Message: ntp test Match Expression	Туре	Violation if not matched	striction		OK Cancel
Rule Set - ntp test /iolation Message: htp test Match Expression ntp server ~ip~	Type regex	Violation if not matched	striction 10.0.2.54)\$		OK Cancel
Rule Set - ntp test /iolation Message: Intp test Match Expression ntp server ~ip~		Violation if not matched			OK Cancel
Rule Set - ntp test /iolation Message: Intp test Match Expression ntp server ~ip~		Violation if not matched			OK Cancel
Aule Set - ntp test /foldtion Message: Intp test Match Expression ntp server ~ip~		Violation if not matched			OK Cancel

Compliance example:

ategory: <all></all>	~	🔶 Create	📌 Rename	🗅 Copy 🛛 💢 D	elete 🔒 Catego	ry Description:
Rule Set	Adapter	Config		Category		
IOS Session Idle Timeout	Cisco IOS	/running-config				*
IOS Disabled Unneeded Services	Cisco IOS	/running-config				
IOS SSH-only Restricted Access	Cisco IOS	/running-config				
IOS Telnet Restricted Access	Cisco IOS	/running-config				
IOS Secure Enable Passwords	Cisco IOS	/running-config				
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config				
IP Logging	Cisco IOS	/running-config			Remediation job	or playbook
C3560 Template	Cisco IOS	/running-config				
SNMP Server Community String	Cisco IOS	/running-config	Ren	nediation job	Remediation Playb	look
snmp-server-rule	Cisco IOS	/running-config	Nam	e	M	emo
Server Host	Cisco IOS	/running-config	Job -	Show Version	sh	ow version for devices
IP Permit	Cisco IOS	/running-config				
IP Permit 2	Cisco IOS	/runnina-confia				
tule Set - ntp test		Action				
Match Expression						
ntp server –ip–		Violation if not matched				
						OK Cancel
Variable	Туре		Restriction			
ip	regex		^(10.0.0.254)	s		

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]).

Dashboards Inventory			Terminal Proxy	Search	Compliance	Monitors	Incidents	Мар	MIBs	Playbook
Sets Templates A	ert Policies	Violations	SNMP Traps	s Syslog			-			
lert Policy Name				Actions						
adLight only				trap						
imple Incident Policy				incident						
tephen				email						
1-3 of 3										
Simple Incident	Policy		Ì	New Actio		nt run-playb	ook			
📫 Incident				Violati						
				{* Execut						
Priority:	Medium 🗸			SNMP						
Default Assignee:	Enter assignee	user name	0	SNMP & Run Jo						
			-	_	most (webhook)				
E-mail recipients	Enter e-mail a	ddresses sep	arated by space	s 🤇 💭 Slack (webhook)					
E-mail Cc: recipients	Enter e-mail a	ddrossos son	arated by space	🗩 🗩 Teams	(webhook)					
			2.1	🔍 DNS R						
Frequency	At most or	-	inute	🎽 ኆ Send T	o Playbook					
Send an Incident em	View email cus	tomizations								
System Actions	all when									
a violation first	occurs for each	device								
dditional violat	ions have occur	red								
a violation has s	tarted clearing									
🗹 a violation has b	-									
User Actions										
🗹 a user clears a v	iolation									
a user modifies	1. S.									

Once added, select the "Playbook to Run", Frequency", "Perform the action when..." options.

pre incluent	t Policy		New Action	incident run-playbook	
Send an Incident e	mail when				
System Actions					
🗹 a violation firs	t occurs for each device				
🛃 additional viol	ations have occurred				
🗹 a violation has	started clearing				
🗹 a violation has	been cleared				
User Actions					
🗹 a user clears a	violation				
_					
🗹 a user modifie	s an incident				
_	s an incident is, ignore frequency and	send email immediate	ly		
_	is, ignore frequency and Playbook	send email immediate	ly		
for user action	is, ignore frequency and Playbook	send email immediate	ly		
✓ for user action ✓ Send To Playbook to Run:	Immediately	٩	ly		
✓ for user action ✓ Send To I Playbook to Run: Frequency: Perform the action	Immediately	٩	ly		
✓ for user action ✓ Send To I Playbook to Run: Frequency: Perform the action ✓ a violation first	Intp fix Immediately when	٩	ly		
✓ for user action ✓ Send To I Playbook to Run: Frequency: Perform the action ✓ a violation first	Interpretation of the second s	٩	ly		

Compliance example:

)	0	Co /ic	m ola	pl ti	iaı or	nce I	e		dev //	ce om	pl	lia	nc	e	erı	r		Ľ			./	(• device outp
															v	io	lat	io	n	•	/	•	config t ntp server 10.0.0.254 exit
•				:	1		1	1			•	•	•	:	•					:	:	:	wr mem exit
:				:	•							•	•	•						:		•	Code Editor
•				ł	ł	ł	-	-				•	•	•					-	2	1	÷	//
																			-				Email send email
											•		•								÷	/	Email send email
:				:	Ì	Ì	1	1				:	:							1	. (• content

Incident example:

, R	5	Inc	id	ent	t						Incident issue 🛛												•	•	Run Code run correction code	
	_														i	nc	ide	ent	•	•		· ·			(device output error
_																										
					•		•		•			•		•	•				•		•			-		config t
					Ċ	÷.	Ċ	1	Ċ	÷.	÷.	Ċ	÷	÷	÷		÷.		÷.	1	÷.	1	÷.			ntp server 10.0.0.254 exit
												Ċ						÷					÷			wr mem
																										exit
																										Code Editor
																										//
						-																				
																										🖉 Email 🛛 🛛 send email 🖉
																								۰,	/	
																			·					. (-	• content
							·		·					·					·		·		•			
																			·							_
									·		·			·					·		·		·			То:
																			·		·					
					•		•							·					·		·	•		•	-	someone@yourcompany

Next, connect the nodes.

														💬 Chat App (Webhook) send to teams 🖉
														Char App (Webnook) send to teams
													. (content
													1.	
													1.	Webhook URL
				21	Run Co				cli con		- 5/2	1.1	1	
					Kun Co	Je		run e	cii con	iman	a e			url for hook
6	Device Search	Select Device	ces 🖉 📋	• de										
_			(• de	vice						outpu	۲) .		Chat Application
			device 🍨								erro	r • •		
											eno	· .)		Microsoft Teams ~
	Device S	election												
	Device 5	election		sh	version							J ·		Limit content to
														Errors Only 🗸
						C	Code I	ditor					1 - I	Endis entry
													1.1	I want to see
													1.1	
													10.0	Counts and Summary Data V
														-
													1.	
													1.	🖂 Email 🛛 🛛 send to email 🖉
													[.	-
													. V	• content
														T
														То:
														someone@yourcompany
														someone@yourcompany
														(c
														Cc:
														1
														Limit content to
														Limit content to
														Errors Only V
														I want to see
														Counts and Summary Data V

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.

Logout Sett	ings Help
Smart Change	퇺 Reports

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

	Server Settings	
Data Retention	SMTP Host:	
System Backup	lvi-co-jp.mail.protection.outlook.com	
Mail Server	From Email Address:	
SNMP Traps	support3eye@lvi.co.jp	
Users	From Name:	
Roles	support3eye	
External Authentication	Supporteye	
Custom Device Fields	Server requires authentication	
Memo Templates	Use secure smtp	
Launchers	Automatically upgrade STARTTLS negotiation	
Smart Bridges	Mail server username:	
Networks		
Network Servers	Mail server password:	
Syslog		
Software Update		
Web Proxy	Default email language 🔤	
Change Approvals	Default email time zone (GMT+09:00) Tokyo	~
Cisco API		
Device Label		
SNMPv3 User	- Test	
	ок	Cancel

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.

Logout	Settings	Help
Smart Ch	ange 툃	Reports

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

	Server Settings
Data Retention	Server Name: support3eye
System Backup	
Mail Server	Hostname/IP Address: 10.0.0.183
SNMP Traps	User login idle timeout (minutes): 30
Users	
Roles	Enable the Terminal Server Proxy (SSH)
External Authentication	Terminal Server Proxy SSH port: 2222
Custom Device Fields	✓ Enable HTTP for web client
Memo Templates	Enable HTTP to HTTPS redirection
Launchers	✓ Enable DNS Lookup
Smart Bridges	Enable Agent-D for monitoring this server
Networks	
Network Servers	Configure SNMP for monitoring this server
Syslog	CORS Origin whitelist (Access-Control-Allow-Origin):
Software Update	
Web Proxy	
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
	OK Cancel

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].

			Server Settings
Data Retention	•		lds can be used to set additional values on each device. You can specify names for m fields here.
System Backup Mail Server		Custom 1:	Custom 1
SNMP Traps	T.	Custom 2:	Custom 2
Users		Custom 3:	Custom 3
Roles		Custom 4:	Custom 4
External Authentication		[
Custom Device Fields		Custom 5:	Custom 5
Memo Templates			
Launchers			
Smart Bridges			
Networks			
Network Servers			
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			
SNMPv3 User	•	🕂 Add	
			OK Cancel

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.

N		Server Settings
Data Retention		lds can be used to set additional values on each device. You can specify names for om fields here.
System Backup		
Mail Server	Custom 1:	Custom 1
SNMP Traps	Custom 2:	Custom 2
Users	Custom 3:	Custom 3
Roles	Custom 4:	Custom 4
External Authentication	Curtury F	Cartery F
Custom Device Fields	Custom 5:	Custom 5
Memo Templates	Custom 6:	Custom 6
Launchers	Custom 7:	Custom 7
Smart Bridges		
Networks		
Network Servers		
Syslog		
Software Update		
Web Proxy		
Change Approvals		
Cisco API		
Device Label		
SNMPv3 User	+ Add	
		OK Cancel

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 2 button.

				General	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
1	Last Backup: 2024/05/31 16:34 (Duration: 1m6s)								🥔 🔌 🌮 🛃 🗄	3
	Snapshot	Config	Time	estamp		Size	User			Ø
ios ing the	2024/05/31 16:34	/running-config	2024/0	5/31 16:34		9768		n/a		-
()		/startup-config	2024/0	5/31 16:34		12356		n/a		
	2024/05/10 11:38	/running-config	2024/0	5/10 11:38		12358		n/a		
		/startup-config	2024/0	5/10 11:38		12358		n/a		

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

Draft Configuration	112
Draft name:	
sample-config	
	าร
OK Ca	ncel

4. Doubleclick the created draft configuration.

			General	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
Last Backup: 2024/05/31 16:34 (Duration:					Ŀ] 🥜 🕭 🏂 🛃 🗄			
Snapshot	Config		Times	tamp	Size	User			Ø
2024/05/31 16:34	/running-config		2024/05	/31 16:34		9768	r	n/a	^
	/startup-config		2024/05	/31 16:34		12356	r	n/a	
2024/05/10 11:38	/running-config		2024/05	/10 11:38		12358	r	n/a	
	/startup-config		2024/05	/10 11:38		12358	r	ı/a	
2024/04/25 12:48	/running-config		2024/04	/25 12:48		12358	r	n/a	
	/startup-config		2024/04	/25 12:48		12358	r	ı/a	
Draft Configurations									
Draft		Last Edit	Size	User					9
sample-config		2024/06/21 13:21	12358	shibata					

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

tech - 10	.0.0.124 × sample-config@10.0.0.124 ×								
sample	e-config								
1	version 15.4								
2	service timestamps debug datetime msec								
3	service timestamps log datetime msec								
4	no platform punt-keepalive disable-kernel-core								
5	platform console virtual								
6	!								
7	hostname tester								
8	!								
9	boot-start-marker								
10	boot-end-marker								
11									
12	!								
13	enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8gR2MEaE1								
14	enable password lvi								
15	!								
16	no aaa new-model								
17	!								
1.8									

×

tech - 10.0.0.124 × sample-config@10.0.0.124

sample-config

```
version 15.4
 1
    service timestamps debug datetime msec
 2
    service timestamps log datetime msec
 3
    no platform punt-keepalive disable-kernel-core
 4
    platform console virtual
 5
 6
    1
 7 hostname homesite
 8
    1
    boot-start-marker
 9
    boot-end-marker
10
11
    1
12
    1
    enable secret 5 $1$CJ4w$Jqpqf3Jnt/9oC8qR2MEaE1
13
    enable password lvi
14
15
    1
16 no aaa new-model
17
   1.1
18
```

tech - 1	1.0.0.124 × sample-config@10.0.0.124 ×			
sampl	e-config	Find	Q 💠	🗟 🔛 🍉
2 3 4	version 15.4 service timestamps debug datetime msec service timestamps log datetime msec no platform punct-keepalive disable-kernel-core platform console virtual			
7				
	boot-start-marker boot-end-marker 1			

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.

Snapshot	Config		Timest	amp	Size	User	4
2024/05/31 16:34	/running-config		2024/05/	/31 16:34	9768	n/a	
	/startup-config		2024/05/	/31 16:34	12356	n/a	
2024/05/10 11:38	/running-config		2024/05/10 11:38		12358	n/a	
	/startup-config		2024/05/	/10 11:38	12358	n/a	
2024/04/25 12:48	/running-config		2024/04/25 12:48		12358	n/a	
	/startup-config		2024/04/	/25 12:48	12358	n/a	
raft Configurations						😒 🗔 🛛	× = 3 3
-		Last Edit	Size	User			

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

Organize 🔻 New fold	er			
> 🔷 OneDrive - Perso	Name	Date modified	Туре	Size
	∼ Today			
🔄 Desktop 🔹 🖈	sample-config	6/10/2024 9:10 AM	File	3 KB
↓ Downloads ★	 ✓ Earlier this month 			

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

			Genera	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
Last Backup: 2024/05/31 16:34 (Duratio					E] 🥜 🕭 🍠 🛃 🗄			
Snapshot	Config		Times	tamp	Size	User			Ð
2024/05/31 16:34	/running-config		2024/05	/31 16:34	9	768	r	n/a	
	/startup-config		2024/05	/31 16:34	12	356	r	n/a	
2024/05/10 11:38	/running-config		2024/05/10 11:38		12	358	r	n/a	
	/startup-config		2024/05/10 11:38		12	358	r	n/a	
2024/04/25 12:48	/running-config		2024/04/25 12:48		12	358	r	n/a	
	/startup-config		2024/04	/25 12:48	12	358	r	n/a	-
 Draft Configurations 								📑 🗶 🗐 将	
Draft		Last Edit	Size	User					Ø
sample-config		2024/06/21 13:21	12358	shibata					

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 \bowtie button.

6.9.5 Compariing draft configurations

To compare draft configurations, click the $\mathbf{E}^{\mathbf{T}}$ button.

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

			General	Compliance	Attachment	Hardw	are Interfaces ARP/MAC	/VLAN Memo
Last Backup: 2024/05/31 16:34 (Duration: 1m					🔚 🥔 🕭 🤞	1 📝 🖅 🍡		
Snapshot	Config		Timest	amp	Size	Us	ser	Ø
2024/05/31 16:34	/running-config		2024/05/	31 16:34		9768	n/a	
	/startup-config		2024/05/	31 16:34		12356	n/a	
2024/05/10 11:38	/running-config		2024/05/	10 11:38		12358	n/a	
	/startup-config		2024/05/	/10 11:38		12358	n/a	
2024/04/25 12:48	/running-config		2024/04/25 12:48			12358	n/a	
	/startup-config		2024/04/	25 12:48		12358	n/a	-
🔻 Draft Configurations								
Draft		Last Edit	Size	User				Ű
sample-config 2024/06/21 13:21			12358	shibata				

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 solution.

	latartur config		2024/05/2	c 12.02	2074	n /a	
 Draft Configurations 						😒 🔛 🗙 🖅 🤶	5
Draft		Last Edit	Size	User			Ð
sample-config		2024/06/10 09:12	2093	scorreale			

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

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



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.

			Server Settings				
Data Retention System Backup Mail Server SNMP Traps Users Users Roles External Authentication Custom Device Fields Memo Templates Launchers Smart Bridges Networks		 Send traps when device configuration changes are detected devices are added and deleted a backup fails a job completes with errors the compliance status of a device changes the status of bridge changes an audit event occurs a change approval action occurs an email failure Trap forwarding: Forward all received traps 					
Network Servers		Community	Host	Port	Version		
Syslog							
Software Update							
Web Proxy							
Change Approvals							
Cisco API							
Device Label							
SNMPv3 User	-				🔶 🖉 💥		
					OK Cancel		

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].

SNM	P Trap Host
Host:	192.168.3.3
Port:	162
Version:	3 ~
SNMPv3 Authentication Username:	logicvein
SNMPv3 Authentication Password:	•••••
SNMPv3 Privacy Password:	•••••
SNMPv3 Authentication Protocol:	SHA ~
SNMPv3 Private Protocol:	PrivDES ~
SNMPv3 EngineID:	0x:80:00:13:70:01:c0:a8:01:07:33:49:5e:fb
	OK Cancel

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

🗢 Device 😂 Inventory	👁 Tools 🌭 Change	🕸 Smart Change 🔳 Reports
End Of Life	DNS Lookup	Software End Of L
	Interface Brief	A
	IOS Show Commands	
	IP Routing Table	
	Live ARP Table	
2021/08/31	Ping	
	Port Scan	
	SNMP System Info.	
	Traceroute	

6.10.1 DNS lookup

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

		· · · · · · · · · · · · · · · · · · ·	
DNS Lookup ×			
DNS Lookup (2024/06/10 09:24)			
Hostname	IP Address	Network	Resolved Name
✓ 3eye.intra.lvi.co.jp.	10.0.40.45	Default	3eye.intra.lvi.co.jp

6.10.2 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.

IOS Show Commands	
show access-lists	
show arp	
show cdp	
show flash:	
show interfaces	
show spanning-tree	
show version	
show ip arp	
show ip bgp	
show ip eigrp neighbors	
show ip ospf	
show ip route	
show ip vrf	
	Execute Cancel
e	
s command can only be run on devices that are compatible with Cisco IG	OS.

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

	Commands	×					
IOS Shov	v Commands (2	2024/06/	/10 09	:26)			
Hostna	ime						IP Address
✓ _1234							10.0.0.223
·							
		-		tta u de sa sa Dadala	-		
		Age	(m n n)		Twpe	Interface	
Protocol		Age		Hardware Addr 0050.56ac.40d4			
Protocol Internet	Address 10.0.0.94 10.0.0.95	Age	(min) 232 0	0050.56ac.40d4	ARPA	Interface GigabitEthernet1 GigabitEthernet1	
Internet	10.0.0.94	Age	232	0050.56ac.40d4	ARPA ARPA	GigabitEthernet1	
Protocol Internet Internet Internet	10.0.0.94 10.0.0.95	Age	232 0	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9	ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.98	Age	232 0 0	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9	ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.98 10.0.0.117 10.0.0.124 10.0.0.170	Age	232 0 0 0	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9 0050.56ac.4e86	ARPA ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.98 10.0.0.117 10.0.0.124	Age	232 0 0 0 6	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9 0050.56ac.4e86 0050.56ac.6f9a	ARPA ARPA ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.95 10.0.0.117 10.0.0.124 10.0.0.170 10.0.0.183 10.0.0.223	Age	232 0 0 0 6 0	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9 0050.56ac.4e86 0050.56ac.6f9a 0050.56ac.9f89 0050.56ac.d5eb	ARPA ARPA ARPA ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.98 10.0.0.117 10.0.0.124 10.0.0.170 10.0.0.183 10.0.0.223 10.0.0.240	Age	232 0 0 6 0 0 -	0050.56ac.40d4 0050.56ac.d84c 0050.56ac.0fa9 0050.56ac.4e86 0050.56ac.4e86 0050.56ac.9f89 0050.56ac.45eb 0050.56ac.2dd0 0050.56ac.e14	ARPA ARPA ARPA ARPA ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	
Protocol Internet Internet Internet Internet Internet Internet Internet Internet	10.0.0.94 10.0.0.95 10.0.0.95 10.0.0.117 10.0.0.124 10.0.0.170 10.0.0.183 10.0.0.223	Age	232 0 0 6 0 0 -	0050.56ac.40d4 0050.56ac.dB4c 0050.56ac.0fa9 0050.56ac.4e86 0050.56ac.4e86 0050.56ac.9f89 0050.56ac.45eb 0050.56ac.2dd0 0050.56ac.ee14	ARPA ARPA ARPA ARPA ARPA ARPA ARPA ARPA	GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1 GigabitEthernet1	

6.10.3 IP Routing table

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

IP Routing Table ×					
IP Routing Table (2024/06/10 09:27)_1234-10.0.0.223					
Destination	Mask	Next Hop	Interface		
10.0.0	255.255.255.0	0.0.0.0	GigabitEthernet1		
10.0.0.223	255.255.255	0.0.0.0	GigabitEthernet1		
0.0.0.0	0.0.0.0	10.0.254			

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.

Hostname	IP Address	Network	Bytes	TTL	Min (ms)	Avg (ms)	Max (ms)	Stddev (ms)	Pkt Loss (
_1234	10.0.0.223	Default	64	254	0.394	0.433	0.493		0
i bytes from 10.0.0.2 i bytes from 10.0.0.2	0.223): 56 data bytes 231 seq0 til254 time0.394 m 231 seq0 til254 time0.401 m 231 seq0 til255 time0.411 m 231 seq1 til255 time0.414 m 231 seq1 til255 time0.442 m 231 seq1 til255 time0.443 m 231 seq2 til255 time0.453 m 231 seq2 til256 time0.	a (DUP!) 5 (DUP!) 6 (DUP!) 9 (DUP!) 9 (DUP!) 9							

6.10.5 SNMP System Info

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

						▼ ▲			
IM	System Info.	×							
SNMP System Info. (2024/06/10 09:28)									
H	lostname	IP Address	Network	System Description	System UpTime	System Contact	System Name		
-	1234	10.0.0.223	Default	Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINU	14 hours, 10:37.93		_1234.intra.lvi.co.jp		
ech	nical Suppor	are [Amsterdar rt: http://www 986-2022 by C: -Feb-22 10:3	cisco.com/ta	E Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version chaupport Inc.	17.3.5, RELEASE SOFTWARE (fc2)				

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.

SNMP System Info. 🛛 🗙 Interface Brief 🛛 🗙								
Interfac	Interface Brief (2024/06/10 09:28)_1234-10.0.223							
Admin	Line	Description	IP	MAC (hex)	If Speed	High Speed		
	^	GigabitEthernet3	192.168.2.1	005056AC6816	100000000	1000		
	^	NullO			4294967295	10000		
	^	GigabitEthernet1	10.0.0.223	005056AC2DD0	100000000	1000		
^	^	GigabitEthernet2	192.168.1.1	005056ACDD03	100000000	1000		
	^	VoIP-Null0			4294967295	10000		

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.

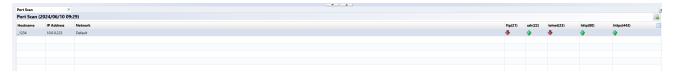
TTL	Hostname	IP Address	Probe 1 (ms)	Probe 2 (ms)	Probe 3 (ms)
1	10.0.40.254	10.0.40.254	0.953	0.789	0.786
2	10.0.0.124	10.0.0.124	0.320	0.221	0.196
3					

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.

Live ARP Table ×	
Live ARP Table (2024/06/10 09:30)_1234-10.0.0.223	
IP Address	МАС
✓ 192.168.2.1	00-50-56-ac-68-16
✓ 10.0.0.253	5c-8a-38-68-01-0c
✓ 10.0.0.124	00-50-56-ac-6f-9a
✓ 10.0.94	00-50-56-ac-40-d4
✓ 192.168.1.1	00-50-56-ac-dd-03
✓ 10.0.254	00-2a-10-b7-82-f1
✓ 10.0.0.117	00-50-56-ac-4e-86
✓ 10.0.0.170	00-50-56-ac-9f-89
✓ 10.0.095	00-50-56-ac-d8-4c
✓ 10.0.223	00-50-56-ac-2d-d0
✓ 10.0.240	00-50-56-ac-ee-14
✓ 10.0.0.183	00-50-56-ac-d5-eb
✓ 10.0.98	00-50-56-ac-0f-a9
✓ 10.0.250	e0-5f-b9-ba-4d-60

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.

🦴 Change 😣 Smart Change 嶋 Reports							
Command Runner							
Enable or Disable Interfaces							
Login Banner (MOTD)							
Name Servers Manager							
NTP Servers							
Port VLAN Assignment							
SNMP Community Strings							
SNMP Trap Hosts							
Syslog Hosts							
OS Image							
AlliedTelesis OS Software Distribution							
ASA OS Software Distribution							
IOS Software Distribution							
Manage OS Images							
NEC WA Software Distribution							
Retrieve OS Image Files							
Yamaha RT Firmware Distribution							
Static Routes							
Add Static Route							
Delete Static Route							
Users							
Add User Account							
Change Enable Password							
Change Local User Password							
Change VTY Password							
Delete User Account							

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.

Command Runner		
Specify the commands to run against the devices		
show version show running-config show interface		
Override the default prompt regex:		
Response timeout (seconds): 60		
Perform backup after tool completes	Execute	Cancel

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.

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

6.12.3 Login Banner (MOTD)

Set the device login banner.

D	Login Banner (MOTD)
	.ogin Banner
	Welcome to LogicVein Network
0	
0	
0	
0	
0	
0	
D	
D	
D	Perform backup after tool completes Execute Cancel

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.

	Na	me Servers Manager		
Name Server Address				
Name Server Action (add/delete)	add 🗸			
Domain Suffix Name				
Perform backup after tool cor	npletes		Execute	Cancel

The [Execute] button, will become clickable.

3. Click [Execute].

	Nai	me Servers Manager		
Name Server Address	10.0.0.66			
Name Server Action (add/delete)	add 🗸 🗸			
Domain Suffix Name				
		-		
Perform backup after tool con	npletes		Execute	Cancel

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".

	Nan	ne Servers Manager		
Name Server Address				
Name Server Action (add/delete)	add 🗸			
Domain Suffix Name	add			
	delete			
)
Perform backup after tool con	npletes		Execute	Cancel

The [Execute] button, will become clickable.

4. Click [Execute].

Note If no IP Address is selected, clicking the [Name Server Manager] tool will act on all addresses in the Inventory window list. Confirm Execution No devices are selected. The current search criteria will be used to execute against 246 devices. Would you like to continue? Yes No

6.12.5 NTP Servers

Add/remove NTP servers to your device.

NTP Servers		
NTP servers to add	192.168.0.100	
NTP servers to remove		
Perform backup afte	r tool completes	Execute Cance

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.

		Port VLAN Assignment	
	mgmt0		
	Ethernet1/1		
Select Interfaces	Ethernet1/2		
	Ethernet1/3		
	Ethernet1/4		
	Ethernet1/5		
Select a VLAN		Number	
		Number	
default			
delault		1	
VLAN0012		1 12	
VLAN0012		12	
VLAN0012		12	
VLAN0012		12	
VLAN0012 VLAN0002	up after tool completes	12 2	Execute Canco

6.12.7 SNMP community string

 Index
 Index
 Index

 SNMP Community Strings

 New Community String

 Community String

 Delete Community String

 Community String

 Community String

 Community String

 Community String

 Community String

 Perform backup after tool completes

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.

SNMP Trap Hosts		
New Trap Host Name		
Trap Host Name/Address 192.168.0.100		
New Community String		
Community String public		
Action (add/delete) add v		
Perform backup after tool completes	Execute	Cancel

6.12.9 Syslog Hosts

Add/delete Syslog hosts to/from the device.

	Syslog Hosts	
Logging hosts to add:	192.168.0.100	
Logging hosts to remove:		
Perform backup after	ool completes	Execute Cancel

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.

	AlliedTelesis OS Software Distribution
Select an OS image file to push	
Destination flash location	flash
Optional	
Destination flash directory	
Remove the existing image fro	m flash
Boot from the new image	
Reload after image push	
Timeout (default 300 second)	
Perform backup after tool com	pletes Execute Cancel

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.

	ASA OS Software Distribution	
Select an ASA OS image file to push		
Destination flash location	flash	
Optional		
Remove the existing image from f	ash	
 Boot from the new image Reload after image push 		
Perform backup after tool comple	es	Execute Cancel

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	After image transfer, remove the existing image file.
from flash	
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.

	IOS Software Distribution	
Select an IOS image file to push		
Destination flash location flash		
Optional		
Destination flash directory		
Destination flash partition		
Remove the existing image from flash		
Boot from the new image		
🗌 Reload after image push		
Minimum DRAM in Kilobytes (from CCO)		
Perform backup after tool completes	Execute	ncel

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.

	Select a file	
Name	Size	MD5 Hash
🚞 Cisco	72.16 MB	

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

		Select a file	
			 Image: Image: Im
Name		Size	MD5 Hash
) Cisco		72.16 MB	
		New Folder	
	Specify the fold	ler name.	
			OK Cancel

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.

NEC WA Software Distribution	
Select an OS image file to push	
Optional	
Remove the existing image from flash	
□ Boot from the new image	
Reload after image push	
Perform backup after tool completes	Execute Cancel

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.

Ref Re	Retrieve OS Image Files 🛛 🕺 👘 👘 👘				
	Hostname	IP Address	Network	Elapsed Time (seconds)	OS Image
~	A	10.0.0.128	Demo	0	packages.conf

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.

Yamaha RT Firmware Distribution	
Select a Yamaha firmware file to push	
TFTP Option	
Specify the destination exec Flash ROM area Number. (i.e: 1 or 0 or blank)	
Copy current firmware to internal Flash ROM area (for multiple flash supported device only)	
Optional	
Save and send temporary configuration for upgrade (Recommendations)	
Minimum free memory (percentage)	
Waiting timer (default 300 second)	
Perform backup after tool completes Execute	Cancel

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

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

Add Static Route			
Destination			
Destination Address(IP Address)	10.0.100.0		
Destination Mask(IP Mask)	255.255.255.0		
Gateway			
Gateway Address(IP Address)	0.0.0.30		
Perform backup after tool co	mpletes	Execute	Cancel

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

6.12.18 Delete Static Route

Select and delete an existing static route configuration.

Gateway	Destination Mask	Destination Address
10.0.0.254	0	0.0.0.0
	0	0.0.0.0

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.

Add User Account				
User Dat	a			
Username	logicvein			
Password				
Privilege	SU v			
Perform	n backup after tool completes			Execute Cancel

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.

Change Enable Password		
User Data		
New Password		
Password:	Confirm:	
Verify credentials after change is executed	I	
Perform backup after tool completes		Execute Cance

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.

Change Local User Password			
User Data			
Username logicvein			
New Password			
Password:	Confirm:		
Verify credentials after change is executed			
Perform backup after tool completes		Execute Cancel	

6.12.22 Change VTY Password

Change the device's VTY Password settings.

Change VTY Password		
User Data		
New Password		
Password:	Confirm:	
•••••••• Verify credentials after change is executed		
Perform backup after tool completes		Execute Cance

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.

Delete User Account			
User Dat	ta		
Username	logicvein		
Perform	n backup after tool completes	Execute Cancel	

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.

Command Runner				
Specify the commands to run against the devices				
show version show running-config show interface				
Override the default prompt regex:				
Response timeout (seconds):				
Perform backup after tool completes	Execute	Cancel		

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.

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

6.12.26 Login Banner (MOTD)

Set the device login banner.

Welcome t	to LogicVein	Network			

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.

	Na	me Servers Manager		
Name Server Address				
Name Server Action (add/delete)	add 🗸			
Domain Suffix Name				
·)
Perform backup after tool cor	npletes		Execute	Cancel

The [Execute] button, will become clickable.

3. Click [Execute].

	Na	me Servers Manager		
Name Server Address	10.0.0.66			
Name Server Action (add/delete)	add 🗸 🗸			
Domain Suffix Name				
		-		
Perform backup after tool con	npletes		Execute	Cancel

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".

	Nam	e Servers Manager		
Name Server Address				
Name Server Action (add/delete)	add ∽			
Domain Suffix Name	add			
	delete			
(
Perform backup after tool con	npletes		Execute	Cancel

The [Execute] button, will become clickable.

4. Click [Execute].

Note If no IP Address is selected, clicking the [Name Server Manager] tool will act on all addresses in the Inventory window list. Confirm Execution No devices are selected. The current search criteria will be used to execute against 246 devices. Would you like to continue?

6.12.28 NTP Servers

Add/remove NTP servers to your device.

	NTP Servers	
NTP servers to add	192.168.0.100	
NTP servers to remove		
Perform backup afte	r tool completes	Execute Cancel

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.

	Port VLAN	Assignment		
	mgmt0			^
	Ethernet1/1			
Select Interfaces	Ethernet1/2			
Select Interfaces	Ethernet1/3			
	Ethernet1/4			
	Ethernet1/5			-
Select a VLAN				
Name		Number		
default		1		
VLAN0012		12		
VLAN0002		2		
Perform back	sup after tool completes		Execute	Cancel

6.12.30 SNMP Community Strings

Add/delete SNMP communities to/from devices.

SNMP Community Strings						
New Communit	y String					
Community String	public					
Access Type	RO v					
Delete Commun	ity String					
Community String	lvi					
Access Type	RO v					
Perform backup	p after tool completes				Execute C	ancel

6.12.31 SNMP Trap Hosts

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

SNMP Trap Hosts						
New Trap Host Name						
Trap Host Name/Address 192.168.0.100						
New Community String						
Community String public						
Action (add/delete) add V						
Perform backup after tool completes	Execute Cancel					

6.12.32 Syslog Hosts

Add/delete Syslog hosts to/from the device.

Syslog Hosts				
Logging hosts to add:	192.168.0.100			
Logging hosts to remove:				
Perform backup after	ool completes	Execute Cancel		

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.	

	AlliedTelesis OS Software Distribution
Select an OS image file to push	
Destination flash location	flash
Optional	
Destination flash directory Remove the existing image fro Boot from the new image Reload after image push Timeout (default 300 second)	m flash
Perform backup after tool com	pletes Execute Cancel

Item	Explanation			
Select an OS image file to push	When you press the [] button on the right side, a window wi 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.

	ASA OS Software Distribution		
Select an ASA OS image file to push			
Destination flash location	flash		
Optional			
 Remove the existing image from fl Boot from the new image Reload after image push 	ash		
Perform backup after tool complet	es	Execute	Cancel

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.

	I	IOS Soft	ware Di	istributi	on				
Select an IOS image file to push [
Destination flash location	flash								
Optional									
Destination flash directory									
Destination flash partition									
□ Remove the existing image from	om flash								
Boot from the new image									
🗌 Reload after image push									
Minimum DRAM in Kilobytes (from	n CCO)								
Perform backup after tool comp	npletes						Execute	Can	cel
controoor incores	1.01			0.0					

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.

Select a file					
Name	Size	MD5 Hash			
🚞 Cisco	72.16 MB				

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

NIGHTER A		Select a file	- 148
/			< 🔁 🗟 🖉 🗄 💰 兴
Name	Siz	e	MD5 Hash
🚞 Cisco	72.	.16 MB	
		New Folder	
	Specify the folder name.		
			OK Cancel
			OK Cancel
			OK Cancel

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.

NEC WA Software Distribution			
Distribution			
Execute Cancel			
Explanation			
When you press the [] button on the rig			
side, a window will appear where you ca			
side, a window will appear where you ca browse the registered OS images, so sele the image you want to upload.			
side, a window will appear where you can browse the registered OS images, so selec the image you want to upload. After image transfer, remove the existing			

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.

	etrieve OS Image Files 🛛 🛪						
Retriev	Retrieve OS Image Files (2024/04/09 09:27)						
Host	tname	IP Address	Network	Elapsed Time (seconds)	OS Image		
🖌 A		10.0.0.128	Demo	0	packages.conf		

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.

Yamaha RT Firmware Distribution	
Select a Yamaha firmware file to push	
TFTP Option	
Specify the destination exec Flash ROM area Number. (i.e: 1 or 0 or blank)	
Copy current firmware to internal Flash ROM area (for multiple flash supported device only)	
Optional	
Save and send temporary configuration for upgrade (Recommendations)	
Minimum free memory (percentage)	
Waiting timer (default 300 second)	
Perform backup after tool completes Execute	Cancel

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

Note

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

```
No....Revision:
-----:
|.0...Rev.14.01.11:
*.1...Rev.14.01.14:
```

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

2. *The following command will be executed:

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

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

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

6.12.40 Add Static Route

	Add Static Route			
Destination				
Destination Address(IP Address)	10.0.100.0			
Destination Mask(IP Mask)	255.255.255.0			
Gateway				
Gateway Address(IP Address)	0.0.0.30			
Perform backup after tool co	ompletes	Execute	Cancel	

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

6.12.41 Delete Static Route

Select and delete an existing static route configuration.

Gateway	Destination Mask	Destination Address
10.0.0.254	0	0.0.0.0
	0	0.0.0.0

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.

Add User Account						
User Dat	a					
Username	logicvein					
Password						
Privilege	su ~					
Perform	n backup after tool completes	xecute Cancel				

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.

Change Enable Password						
User Data						
New Password						
Password:	Confirm:					
Verify credentials after change is executed						
Perform backup after tool completes		Execute Cancel				

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.

Change Local User Password					
User Data					
Username logicvein					
New Password					
Password:	Confirm:				
Verify credentials after change is executed					
Perform backup after tool completes	Execute Cancel				

6.12.45 Change VTY Password

Change the device's VTY Password settings.

Change VTY Password					
User Data					
New Password					
Password:	Confirm:				
••••••••• Uerify credentials after change is executed					
Perform backup after tool completes		Execute Cancel			

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.

Delete User Account	
User Data	
Username logicvein	
Perform backup after tool completes	Execute Cancel

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 Dutton.

np ncm snmp ssh telnet web			General	Monitors	Violations	SNMP Traps	Compliance	Attachment	Hardware	Interfaces	ARP/MAC/VLAN	Memo
	Last Backup: 2024/06/06 23:04 (Durati	on: 10s)] 🥜 🍣 🍣 🔮 🔒	- D
	Snapshot		Con	fig		Time	estamp	Si	ze User			Ø
	2024/06/03 23:04	/running-c	onfig			2024/	06/03 23:04		2094		n/a	
		/startup-co	/startup-config			2024/	06/03 23:04		2094		n/a	
	2024/06/01 23:03	/running-c	onfig			2024/	06/01 23:03		2097		n/a	
		/startup-co	onfig			2024/	06/01 23:03		2097		n/a	
	2024/05/26 23:03	/running-c	onfig			2024/	05/26 23:03		2074		n/a	
Serial#: 9V0INVIMG0X		/startup-co	onfig			2024/	05/26 23:03		2074		n/a	
e: Router	2024/05/23 23:03	/running-c	onfig			2024/	05/23 23:03		2071		n/a	
		/startup-co	onfig			2024/	05/23 23:03		2081		n/a	
	2024/05/16 23:04	/running-c	onfig			2024/	05/16 23:04		2174		n/a	
		(18) (1) (1)				20244	00.000.000		2274			

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

Current: /running-config (2024/06/03 23:04)	/running-config (2024/06/01 23:03)
11 1 12 1 13 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8gR2MEaE1 14 enable password lvi 15 1 16 no aaa new-model 17 1 18 1 19 1 19 1 20 1 21 1 22 1 23 1 24 2 25 2 26 1	<pre>version 15.4 2 service timestamps log datetime msec 3 service timestamps log datetime msec 4 no platform punt-keepalive disable-kernel-core 5 platform console virtual 6 ! 7 hostname shibata 8 ! 9 boot-start-marker 10 boot-end-marker 11 i 11 cl 12 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8qR2MEaE1 14 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8qR2MEaE1 14 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8qR2MEaE1 14 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8qR2MEaE1 15 enable secret 5 \$1\$CJ4w\$Jqpqf3Jnt/9oC8qR2MEaE1 16 no aaa new-model 17 ! 18 enable for the form of the form</pre>
Recommended commands:	

configure	terminal
no hostna	me tech
hostname	shibata
exit	

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.

Recommended commands:

configure terminal no hostname tech hostname shibata exit

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.

Change Advisor (2024/06/10 09:20)						
Hostname	IP Address	Network	Duration (seconds)			
/ tech	10.0.0.124	Default	1			

Enter configuration commands, one per line. End with CNT: shibata(config)#no hostname tech Router(config)#hostname shibata shibata(config)#

Note

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

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.

of Inventory Changes Jobs Terminal Proxy Search Complian	ce Zero-Touch			Network Core v scorreale	e Logout Settings Help
Job History Job Management					
👖 🔣 🔻 Approval Status: -Any- 🔹 🛪 Job Name: -Any- 🔹 🛪	Job Type: -Any- 👻 🗶 🥌		🖳 Audit Log 🛛 🛞 Open Job 😹 I	Delete 🥜 Rename 📄 Copy 🙆 Run Now	😵 New Job 📑 Filters
Name	Туре	Approval Requester	Approval Status	Memo	👶 Backup
📩 😣 Add ASA VPN User	Smart Change		Not Requested	Creates a new VPN user on our ASA	S Discovery
📮 🚸 add ntp server	Smart Change		Not Requested		Populate End Of Sale
🛄 👶 Auto Duplex	Smart Change		Not Requested		Report
🗂 🚸 Auto-Duplex-Speed	Smart Change		Not Requested		Smart Change
Cisco Access Lists	Tool		Not Requested		No Tool
Gisco Interfaces	Tool		Not Requested		
Sisco Show Commands	Tool				
S Core discovery	Discovery				
k Daily changes	Report				
👶 Full backup	Backup				
1. Full Compliance	Report				

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

Create Smart Change Job	
Job Name:	
Cisco enable	
Network:	
Default,Osaka DC2,Tokyo DC1,Utah DC	•
Comment:	
Use remediation job.	
O Use the same replacement values for all devices in the job.	
Use unique replacement values for each device in the job.	
	OK Cancel

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.

iail Notifi	cation	
	Commands	Replacements
1	config t	
2	enable password password	
3	exit	
4	write mem	
Prom		
Pron	the	啥 🕆 🤚 🖊 🕺

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

	Add Replacement	
Selection:	password	
Name	newpassword	
Туре	Text	~
	Use selection as default value	
		OK Cancel

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.

	Commands	Replacement
	config t	2 newpassword
1	enable password (newpassword)	- Hempassiona
1.1	exit	
1.00	write mem	

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

n	Changes Jobs Termina		liance Monitors Incide	nts Map MIBs				
Vendor/Model/OS:								
IP Address	Hostname	 Network 	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#
10.0.0.250	1921CiscoRouter	Tokyo DC1	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL150826
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL150826
10.0.0.223	_1234	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5F
10.0.0.128	aaa	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9J4P873SEI
192.168.1.61	C9800-WLC	Default	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100
10.0.0.249	Cisco1-A.intra.lvi.co.jp	Default	Cisco IOS	Cisco	cat29xxStack	Switch	15.2(2)E	FOC1721W
10.0.0.155	cisco155	Default	Cisco IOS	Cisco	ciscoCSR1000v			
10.0.0.156	cisco156	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9WI5FRHU
10.0.0.157	cisco157	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9C7M5L0VI
10.0.0.158	cisco158	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9HBTH5O1
10.0.0.161	cisco161	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W3FWU98
10.0.0.162	cisco162	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9PBMWOQ
10.0.0.163	cisco163	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9O2BE4JW
10.0.0.164	cisco164	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9EAVHJ554
10.0.0.165	cisco165	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	95NXXGSY.
			Cisco ISE	Cisco	ciscolseVmK9			
10.0.0.193	CiscolSEVM	Default	CISCO ISC	cisco				
10.0.241	CSR1000V241	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9RZGBS5U
10.0.0.241	CSR1000V241	Default		Cisco			17.3.5	9RZGBS5U
10.0.0.241	CSR1000V241	Default	Cisco IOS	Cisco			17.3.5	9RZGBS5UI Network
) 10.0.241 ↓ 1 - 28 of 28 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	CSR1000V241	Default	Cisco IOS	Cisco			17.3.5	
10.0.0.241 ↓ 1 - 28 of 28 ↓ Tisco enable Template	CSR1000V241	Default	Cisco IOS	Cisco Intification Hostname			17.3.5	Network
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			17.3.5	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			17.3.5	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			17.3.5	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			17.3.5	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			17.3.5	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default
 10.0.0.241 1 - 28 of 28 isco enable Template ₹ Repl. P Address 10.0.0.128 	CSR1000V241	Default	Cisco IOS	Cisco Iotification Hostname aaa			1735	Network Default

○ Use the same replacement values for all devices in the job. ● Use unique replacement values for each device in the job.

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

2 Replacement V	/alues 📄 Device	es 💧 Sche	dule 🛛 🖸 Job Approvals Log	Email Notification
Hostname	Network]		
aaa	Default			
C9800-WLC	Default			
	Hostname	Hostname Network aaa Default	Hostname Network newpassword aaa Default	Hostname Network newpassword password01 aaa Default

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.

📇 Template 🛛 🎅 Replacement Values 🛛 😒 Devices 🕼 Schedule 👩 Job Approvals Log	Email Notification	
Trigger		Next Fire Time(GMT-5)
	Trigger	
	Name: schedule	
	Once O Daily O Weekly O Monthly	⊖ Cron
	9 *: 55 * 2024/06/10	
	Timezone: (GMT-06:00) Central Time	~
	Filter: <no filter=""></no>	¥
		Save Cancel

9. Click the 📓 button to save the job.

*Cisco enab				>
🗮 Temp	late Replacement Values 🛛 😂 Devices 🕥 Schedule 🧿 Job Approvals Log 🚺	Email Notificatio		🔛 🐻 🗔
			Commands	Replacements
	Command	2 e 3 e	config v mable pasword <mark>(newpaseword)</mark> wit	2 newpassword
	config t emable paravord (newparavord) excite men	ur 3-	rrite men	
	\odot			
	End			
	Don't Exit			

6.15 Device EOS/EOL management

🔣 🔻 Vendor/Model	/OS: Cisco • × Add	i Criteria * 🗷 😏									Device	😂 Inventory 👁 Tools 🦴 Cha	nge 💩 Smart Change 🛓
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	Software End Of Sale	Software End Of Life
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s				
I92.168.1.61	C9800-WLC	Core	Cisco IOS	Gisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	15				
I0.0.0.223	_1234	Core	Cisco IOS	Gisco	CSR1000V	Router	17.3.5	9MTTHUSEGVS	15				
0 10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(d)N1(1)	SSI143706V7	78				
I92.168.0.254	M-gw-I3	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.8.1a	FDO202760MQ	35				
10.0.100.89	cisco_10_0_100_89	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)54	9N71QX4N5I9	1s				
10.0.100.85	cisco_10_0_100_85	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9PBMW0QGS5D	15				
10.0.100.88	cisco_10_0_100_88	Core	Cisco IOS	Gsco	CSR1000V	Router	15.4(1)54	9KV83R05JZU	15				
10.0.100.90	cisco_10_0_100_90	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)54	9GY3GDW3RBG	15				
10.0.100.87	cisco_10_0_100_87	Core	Cisco IOS	Osco	CSR1000V	Router	15.4(1)54	9EAVH0554U7	15				
10.0.100.84	cisco_10_0_100_84	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)54	9W3FWU96YQD	15				
10.0.100.82	cisco_10_0_100_82	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)S4	9C7MSLOVDAS	15				
10.0.100.83	cisco_10_0_100_83	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9HBTH5O1Y6X	1s				
10.0.100.86	cisco_10_0_100_86	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)54	9O28E4/WQH5	15				
10.0.100.81	cisco 10 0 100 81	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)54	9WISERHU059	11				

1. Select the device to obtain EOS/EOL.

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

			Network:	<all></all>	Y fujimura	Logout Settings	Help
			🥯 Device	😂 Inventory 👁 To	ols 🦴 Change 💩	Smart Change 💄	Reports
del	Device Type	OS Version	🕹 Backup	•	End Of Sale	End Of Life	
2000R	Switch	V02.20		neighbor data			
ndard PC (i440FX	Server	4.18.0-348.7	Display				
ware Virtual Platf	Server	3.10.53sf.virt		re Configurations Job History			
ware Virtual Platf	Server	3.10.53sf.virt		Edit	2021/11/03	2024/07/18	
2000R	Switch	V02.20	🥖 Edit de	vice properties	2021/05/18	2024/03/31	
2000R	Switch	V02.20	Popula	te device end of sale	2017/09/05	2022/10/03	
ndard PC (i440FX	Server	4.18.0-348.7	Associa	ate tags	2019/10/08	2024/06/30	
216-2-DAC	Infrastructure Mana	3.16.6	p Dissoci	ate tags			
t80brin	Router	V02.03	0	0001073	2024/06/14	2024/03/31	

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

Adapter:		Cisco IOS	~				
Network:		Default	~				
End Of Sale:		2023/08/31	×				
End Of Life:		2024/05/21	×				
Software End Of	Sale:	2023/10/04 2024/05/21					
Software End Of	Life:						
		Custom Fields					
Custom 1:	click	to edit	×				
Custom 2:	click	to edit	$\langle \times \rangle$				
Custom 3:	click	to edit	$\langle \times \rangle$				
Custom 4:	click	to edit	×				
Custom 5:	click	to edit	()				

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

Vendor/Model/0	S: Cisco • × Add	i Criteria 👻 🌜 🕤									🥯 C
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s	2024/06/15	2024/06/14
I92.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	15	2024/06/15	2024/06/14
I0.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	1s	2024/06/15	2024/05/14
10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	75	2024/06/15	2024/06/14
International and the second secon	Ivi-gw-I3	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.8.1a	FDO2027E0MQ	34	2024/06/15	2024/06/14
10.0.100.89	cisco_10_0_100_89	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9N71QX4N5I9	15		
10.0.100.85	cisco_10_0_100_85	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9PBMWOQGS5D	1s		
10.0.100.88	cisco_10_0_100_88	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9KV83RO5JZU	15		
10.0.100.90	cisco_10_0_100_90	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9GY3GDW3R8G	15		
10.0.100.87	cisco 10 0 100 87	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9EAVHJ554U7	15		

6.16 Change data retention period

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

		Server Settings
Data Retention	^	Delete expired data weekly at this time:
System Backup		
Mail Server		Tuesday ∨ 21 🛱 : 10 🛱
SNMP Traps		Duration to loss ich annution bistory
Users		Duration to keep job execution history:
Roles		3 Months v
External Authentication		Duration to keep configuration history:
Custom Device Fields		6 Months V
Memo Templates		6 Months *
Launchers		Duration to keep terminal proxy history:
Smart Bridges		Forever v
Networks		
Network Servers		
Syslog		
Zero-Touch		
Software Update		
Web Proxy		
Change Approvals		
Cisco API		
SNMPv3 User	~	

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.

```
Networking:
                                        Netmask: 255.255.255.0
  IP Address: 10.10.40.124
    Gateway: 10.10.40.254
                                            DNS: 192.168.0.3 192.168.0.3
   Hostname: netld
                                      Interface: eth0
 NTP Server: pool.ntp.org
Time: 2024-12-18 02:33 UTC
                                     SSH Server: Not Running
                                         Backup: Local
   IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe7e:1fa2
    MAC Addr: 00:0C:29:7E:1F:A2
  Revision : 20241217.2347
  OS Version: 2024.12.0-202412172347
  OVA Build : 1734482633
            : EB16B-B000B-23CA9-D7246-2BB97
  Serial#
 NTP Mode
           : noauth
   SSH Settings menu:
  [1] Enable SSH Server
  [2] Disable SSH Server
    SSH Interface Binding menu:
  [1] Bind to all interfaces
  [2] Bind to interface eth1
 You must change password to enable SSH
Changing password for tcadmin
Old password:
New password:
Retype password: _
```

3. Confirm that the SSH Server is Running.

LogicVein -	Core Server
	https://10.10.40.124
Networking	
Gateway: Hostname: NTP Server: Time: IPv6 Addr:	10.10.40.124 Netmask: 255.255.255.0 10.10.40.254 DNS: 192.168.0.3 192.168.0.3 net1d Interface: eth0 pool.ntp.org SSH Server: Running (eth1) 2024-12-18 02:33 UTC Backup: Local fd14:5839:664d:40:20c:29ff:fe7e:1fa2 00:0C:29:7E:1F:A2
OS Version OVA Build	
[1] Static *[2] DHCP [3] SSH Ser [4] Import [5] Admin 1 [6] Reboot [7] Power (IP Address ver Data Cools

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

```
Networking:
IP Address: 10.10.40.125
                                         Netmask: 255.255.255.0
   Gateway: 10.10.40.254
                                              DNS: 192.168.0.3 192.168.0.3
                                       Interface: eth0
  Hostname: netld
NTP Server: pool.ntp.org
Time: 2024-12-18 02:38 UTC
                                      SSH Server: Not Running
Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8
  MAC Addr: 00:0C:29:9A:6E:B8
Revision : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#
           : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode
          : noauth
  Admin Tools menu:
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone)
  Replication Settings menu:
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
```

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

Networking: IP Address: 10.10.40.125 Gateway: 10.10.40.254 Hostname: netld Netmask: 255.255.255.0 DNS: 192.168.0.3 192.168.0.3 Interface: eth0 NTP Server: pool.ntp.org Time: 2024-12-18 02:37 UTC SSH Server: Not Running Backup: Local IPu6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8 MAC Addr: 00:0C:29:9A:6E:B8 Revision : 20241217.2347 OS Version: 2024.12.0-202412172347 OVA Build : 1734482633 Serial# : EB16B-B000B-23CA9-D7246-2BB97 NTP Mode : noauth Admin Tools menu: [1] Reset Admin Password / Two-Factor configuration [2] Configure a remote filesystem for backups [3] Reset Admin Dashboard API Token [4] Configure Agent-D Authentication [5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone) Replication Settings menu: [1] Setup SSH host authentication [2] Toggle standby mode [3] Monitor replication status Remote IP or hostname: 192.168.65.124

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

Admin Tools menu:

```
[1] Reset Admin Password / Two-Factor configuration
  [2] Configure a remote filesystem for backups[3] Reset Admin Dashboard API Token
   [4] Configure Agent-D Authentication
   [5] Configure Built-in Agent-D
  [6] Configure Firewall (beta)[7] Setup replication (current: standalone)
      Replication Settings menu:
   [1] Setup SSH host authentication
   [2] Toggle standby mode
   [3] Monitor replication status
Remote IP or hostname: 192.168.65.124
Generating public/private rsa key pair.
Your identification has been saved in /data/replication/repl_key
Your public key has been saved in /data/replication/repl_key.pub
The key fingerprint is:
SHA256: jf0BGoe8Ex+BHV1dB0Yhoi8g531aTJ7tES7SXSJJ/VM 10.10.40.125
The key's randomart image is:
+---[RSA 4096]----+
| o=+.o*++|
            ..+.+00 El
        . o * B o... |
+ o ^ O +o |
. S & * . |
B + o |
                   0
       -[SHA256]-
Enter the password for the tcadmin user on the remote host...
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
tcadmin@192.168.65.124's password: _
```

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

```
SHA256:jf0BGoe8Ex+BHV1dB0Yhoi8g531aTJ7tES7SXSJJ/VM 10.10.40.125
The key's randomart image is:
+---[RSA 4096]----+
         0=+.0*++|
       ..+.+00 El
     . o * B o...
+ o ^ O +o
                 . S & * .
         B + o
         . 0
+ 00..0=0 |
       . o +.oB
                 S *... .
         =+==0. .
          +B.o+.
    -[SHA256]-
Warning: Permanently added '192.168.65.124' (ED25519) to the list of known hosts.
Press any key to continue...
```

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

Networking:

IP Address: 10.10.40.125 Netmask: 255.255.255.0 Gateway: 10.10.40.254 DNS: 192.168.0.3 192.168.0.3 Hostname: netld Interface: eth0 NTP Server: pool.ntp.org Time: 2024-12-18 02:38 UTC SSH Server: Not Running Backup: Local IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8 MAC Addr: 00:0C:29:9A:6E:B8 Revision : 20241217.2347 OS Version: 2024.12.0-202412172347 OVA Build : 1734482633 Serial# : EB16B-B000B-23CA9-D7246-2BB97 NTP Mode : noauth Admin Tools menu: [1] Reset Admin Password / Two-Factor configuration [2] Configure a remote filesystem for backups [3] Reset Admin Dashboard API Token [4] Configure Agent-D Authentication [5] Configure Built-in Agent-D [6] Configure Firewall (beta) [7] Setup replication (current: standalone) Replication Settings menu: [1] Setup SSH host authentication [2] Toggle standby mode [3] Monitor replication status

10. Press [Y].

Networking: IP Address: 10.10.40.125 Netmask: 255.255.255.0 Gateway: 10.10.40.254 Hostname: netld DNS: 192.168.0.3 192.168.0.3 Interface: eth0 NTP Server: pool.ntp.org SSH Server: Not Running Time: 2024-12-18 02:56 UTC Backup: Local IPu6 Addr: fd14:5839:664d:40:20c:29ff:fe9a:6eb8 MAC Addr: 00:0C:29:9A:6E:B8 Revision : 20241217.2347 OS Version: 2024.12.0-202412172347 OVA Build : 1734482633 Serial# : EB16B-B000B-23CA9-D7246-2BB97 NTP Mode : noauth Admin Tools menu: [1] Reset Admin Password / Two-Factor configuration [2] Configure a remote filesystem for backups [3] Reset Admin Dashboard API Token [4] Configure Agent-D Authentication [5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standalone) Replication Settings menu: [1] Setup SSH host authentication [2] Toggle standby mode [3] Monitor replication status Are you sure you want to toggle standby mode? (y/N) [default: N]

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

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.

```
Networking:
IP Address: 10.10.40.124
Gateway: 10.10.40.254
                                           Netmask: 255.255.255.0
                                                DNS: 192.168.0.3 192.168.0.3
  Hostname: netld
                                         Interface: eth0
NTP Server: pool.ntp.org
                                        SSH Server: Running (eth1)
       Time: 2024-12-19 00:52 UTC
                                            Backup: Local
 IPu6 Addr: fd14:5839:664d:40:20c:29ff:fe7e:1fa2
  MAC Addr: 00:0C:29:7E:1F:A2
Revision : 20241217.2347
OS Version: 2024.12.0-202412172347
OVA Build : 1734482633
Serial#
          : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode : noauth
  Admin Tools menu:
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)?
[7] Setup replication (current: standalone)
  Replication Settings menu:
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
```

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

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

```
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: streaming database files
Backup total: 106565120
Backup streamed: 89051136
Replication state: streaming
Replication status: reserved
WAL buffer size: 0 bytes
```

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

```
Replication state:
Replication status:
WAL buffer size: bytes
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Backup phase: waiting for checkpoint to finish
Backup total:
Backup streamed: 0
Replication state: streaming
Replication status: reserved
WAL buffer size: 0 bytes
Replication state: streaming
Replication status: reserved
WAL buffer size: 0 bytes
Replication state: streaming
Replication status: reserved
WAL buffer size: 0 bytes
```

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.

Networking: IP Address: 10.10.40.120 Netmask: 255.255.255.0 Gateway: 10.10.40.254 DNS: 192.168.0.3 192.168.0.3 Hostname: netld Interface: eth0 SSH Server: Not Running NTP Server: pool.ntp.org Time: 2024-12-18 07:05 UTC Backup: Local IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d MAC Addr: 00:0C:29:27:AF:1D Revision : 20241210.0635 OS Version: 2024.12.0-202412100635 OVA Build : 1733824919 Serial# : EB16B-B000B-23CA9-D7246-2BB97 NTP Mode : noauth Admin Tools menu: [1] Reset Admin Password / Two-Factor configuration[2] Configure a remote filesystem for backups [3] Reset Admin Dashboard API Token [4] Configure Agent-D Authentication [5] Configure Built-in Agent-D [6] Configure Firewall (beta) [7] Setup replication (current: standby, primary host: 192.168.65.121) Replication Settings menu: [1] Setup SSH host authentication [2] Toggle standby mode [3] Monitor replication status [4] Toggle auto failover (current: disabled)

Copyright © 2025 LogicVein, Inc.

3. Press [Y].

IP Address: 10.10.40.120 Gateway: 10.10.40.254 Netmask: 255.255.255.0 DNS: 192.168.0.3 192.168.0.3 Hostname: netld Interface: eth0
 NTP Server:
 pool.ntp.org
 SSH Server:
 No

 Time:
 2024-12-18
 07:20
 UTC
 Backup:
 Lo

 IPv6
 Addr:
 fd14:5839:664d:40:20c:29ff:fe27:af1d
 SSH Server: Not Running Backup: Local MAC Addr: 00:0C:29:27:AF:1D Revision : 20241210.0635 OS Version: 2024.12.0-202412100635 OVA Build : 1733824919 : EB16B-B000B-23CA9-D7246-2BB97 Serial# NTP Mode : noauth Admin Tools menu: [1] Reset Admin Password / Two-Factor configuration [2] Configure a remote filesystem for backups [3] Reset Admin Dashboard API Token [4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D [6] Configure Firewall (beta) [7] Setup replication (current: standby, primary host: 192.168.65.121) Replication Settings menu: [1] Setup SSH host authentication [2] Toggle standby mode [3] Monitor replication status [4] Toggle auto failover (current: disabled) Are you sure you want to toggle standby mode? (y/N) [default: N] y Switching to standalone mode...rebooting.Stopping PostgreSQL: OK 24-12-18 07:20:34,/3N Delete replication 24-12-18 07:20:34,%3N Removing the replication slot on master 24-12-18 07:20:34,%3N Delete replication dome

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.

```
Networking:
IP Address: 10.10.40.120
                                     Netmask: 255.255.255.0
   Gateway: 10.10.40.254
                                         DNS: 192.168.0.3 192.168.0.3
  Hostname: netld
                                   Interface: eth0
NTP Server: pool.ntp.org
                                  SSH Server: Not Running
      Time: 2024-12-18 07:05 UTC
                                      Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
  MAC Addr: 00:0C:29:27:AF:1D
Revision : 20241210.0635
OS Version: 2024.12.0-202412100635
OVA Build : 1733824919
Serial# : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode : noauth
  Admin Tools menu:
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standby, primary host: 192.168.65.121)
  Replication Settings menu:
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
[4] Toggle auto failover (current: disabled)
```

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

```
Networking:
IP Address: 10.10.40.120
                                      Netmask: 255.255.255.0
   Gateway: 10.10.40.254
                                          DNS: 192.168.0.3 192.168.0.3
  Hostname: netld
                                    Interface: eth0
NTP Server: pool.ntp.org
Time: 2024-12-18 07:04 UTC
                                   SSH Server: Not Running
                                       Backup: Local
 IPv6 Addr: fd14:5839:664d:40:20c:29ff:fe27:af1d
  MAC Addr: 00:0C:29:27:AF:1D
Revision : 20241210.0635
OS Version: 2024.12.0-202412100635
OVA Build : 1733824919
Serial#
          : EB16B-B000B-23CA9-D7246-2BB97
NTP Mode
         : noauth
  Admin Tools menu:
[1] Reset Admin Password / Two-Factor configuration
[2] Configure a remote filesystem for backups
[3] Reset Admin Dashboard API Token
[4] Configure Agent-D Authentication
[5] Configure Built-in Agent-D
[6] Configure Firewall (beta)
[7] Setup replication (current: standby, primary host: 192.168.65.121)
  Replication Settings menu:
[1] Setup SSH host authentication
[2] Toggle standby mode
[3] Monitor replication status
[4] Toggle auto failover (current: enabled)
```

7.8 Automatic configuration

7.8.1 Prerequisites

NetLD requires the following prerequisites:

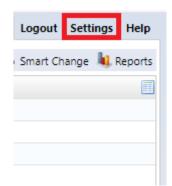
- The NetLD you are using must be able to connect to the Internet.
- You must log in with your Cisco account and obtain an API key and secret code before accessing Cisco Smart Net Total Care.
- Valid Cisco Smart Net Total Care (SNTC) is required.

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].

			Server Settings
Data Retention			
System Backup		Cisco Client Id:	383se6shnne3bwqqbzkw
Mail Server		Cisco Client Secret:	
SNMP Traps			
Users		Test Authentication	on
Roles			
External Authentication			
Custom Device Fields			
Memo Templates			
Launchers			
Smart Bridges			
Networks			
Network Servers			
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			
SNMPv3 User	*		

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

			Server Settings
Data Retention System Backup	Cisc	o Client Id:	383se6shnne3bwqqbzkw
Mail Server	Cisc	o Client Secret:	•••••
SNMP Traps			
Users	Te	st Authenticati	on
Roles			
External Authentication			
Custom Device Fields			
Memo Templates			
Launchers			
Smart Bridges			
Networks			
Network Servers			
Syslog			
Software Update			
Web Proxy			
Change Approvals			
Cisco API			
Device Label			
SNMPv3 User	-		

- 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.

Inventory Chang	jes Jobs Terminal I	Proxy Search Com	pliance Zero-Touch								Network: De	efault 💙 shiba	ta Logout Settings He
🔡 🔻 Vendor/Mod	lel/OS: Cisco 👻 🛪	Add Criteria 🔻 🙁	5								🗢 Device 😂 Im	ventory 👁 Tools 🦠 Change	💩 Smart Change 🔌 Repo
IP Address	▲ Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	SW Vendor	End Of Sale	End Of Life	Software End Of Sale	Software End Of L
0.0.0.40	ASAv9122	Default	Cisco ASA	Cisco	ASAv	Firewall	9.12(2)	9AAMCV8WS0H	Cisco				
0 10.0.0.70	router70	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9YY879DF3BM	Cisco				
 10.0.0.101 10.0.0.121 	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9AUD099HDKJ	Cisco				
🥡 10.0.0.121	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	Cisco	2014/08/15	2021/08/31		
9 10.0.0.126	R1	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9E0UQZ/VK9E	Cisco				
0.0.0.128	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9J4P873SEIN	Cisco				
0 10.0.0.153	bbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9A0HFGOYZF6	Cisco				

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

		Network: Default	Y fujimura L	ogout Settings Help
		🗢 Device 😂 Inventory 👁 T	ools 🦠 Change 💩 S	imart Change 塡 Reports
Device Type	OS Version	🕹 Backup	End Of Sale	End Of Life
Router	15.4(1)S4	Collect neighbor data		
Firewall	9.12(2)	Display neighbors		
Router	15.4(1)S4	Compare Configurations		
Router	15.4(1)S4	Edit		
Router	15.4(2)S	Edit device properties		
Router	15.4(1)S4	Populate device end of sale		
Router	17.3.5	Associate tags		
Router	15.4(2)S	Dissociate tags		
Router	15.4(1)S4	9YY879DF3BM		

7. Click [Yes] on the screen below.



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

IP Address 🔺 H	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	SW Vendor	End Of Sale	End Of Life	Software End Of Sale	Software End Of L
	ASAv9122	Default	Cisco ASA	Cisco	ASAv	Firewall	9.12(2)	9AAMCV8WS0H	Cisco	child of ball	child of the	Software End of Suic	Software End of En
	router70	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9YY879DF3BM	Cisco				
	RouterM	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9AUD099HDKJ	Cisco				
	CR3-A	Default	Cisco IOS	Cisco	CRS-4/S	Router	43.1	SMA112502OL	Cisco	2014/08/15	2021/08/31		
	R1	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	Cisco				
	A	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)\$4	9J4P873SEIN	Cisco				
 10.0.0.153 	bbbb	Default	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9A0HFGQYZF6	Cisco				
10.0.0.223	_1234	Default	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	Cisco				
10.0.0.227 N	Nexus5548	Default	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	Cisco				
n 10.0.0.250 N	lvicore	Default	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	Cisco	2018/09/29	2023/09/30		
10.0.6.12 st	shibata	Default	Cisco IOS	Cisco	WS-C2960-24TT-L	Switch	15.0(2)SE11	FOC1117Z9D0	Cisco	2014/10/31	2019/10/31		
10.0.6.253 C	C3560	Default	Cisco IOS	Cisco	WS-C3560-24TS	Switch	12.2(55)SE11	FDO1241X0RF	Cisco				
🔰 10.128.0.1 N	NER3-LVI	Default	Cisco IOS	Cisco	CRS-16/S	Router	4.2.1	TBA10340015	Cisco	2013/07/31	2020/07/31		
opulate End Of Sale	× Populate End Of 2024/06/21 11:35		ulate End Of Sale	×		_	¥ .						Results per page.
Populate End Of Sale	2024/06/21 11:35	5)			End Of Life	_		le	Software End Of Life	Harr	Iwares undated	Messages	Nesuls per page.
Populate End Of Sale Populate End Of Sale (20 IP Address		5) vork	Rulate End Of Sale End Of S 2022/10/	ale	End Of Life 2021/10/31	_	Software End Of Sa	le	Software End Of Life	Hard	dwares updated	Messages	results per page.
Populate End Of Sale Populate End Of Sale (20 Populate End Of Sale (20 P Address UL 128.0.49	2024/06/21 11:35 Netw	5) vork uit	End Of S	ale		-		le	Software End Of Life		dwares updated		
Populate End Of Sale Populate End Of Sale (20 Populate End Of Sale (20 IP Address 10.128.0.49 10.128.0.144	2024/06/21 11:35 Netw	5) vork uit	End Of S	ale		-		le	Software End Of Life		dwares updated	EOX information	n does not exist for the
Populate End Of Sale 20 Populate End Of Sale (20 IP Address 10.128.0.144 10.128.0.79	2024/06/21 11:35 Netw Defau Defau	5) vork ult ult ult	End Of S	ale		_		le	Software End Of Life	12	dwares updated	EOX information EOX information	n does not exist for the n does not exist for the
Populate End Of Sale 3 Populate End Of Sale (20 IP Address 10.1280.414 10.1280.79 10.1280.90	2024/06/21 11:35 Netw Defau Defau	5) vork uit uit uit uit	End Of S	ale 31		_		le	Software End Of Life	12	lwares updated	EOX information EOX information	n does not exist for the t
opulate End Of Sale 3 Opulate End Of Sale (20 P Address 10.128.0.49 10.128.0.79 10.128.0.90 10.128.0.108	2024/06/21 11:35 Netw Defau Defau Defau Defau	5) work uit uit uit uit uit	End Of 5 2022/10/	ale 31	2027/10/31	_		le	Software End Of Life	12	fwares updated	EOX information EOX information EOX information	n does not exist for the t does not exist for the t does not exist for the t
Populate End Of Sale 2 Populate End Of Sale (20) PAddress ID.128.0.144 10.128.0.79 IO.128.0.90 10.128.0.105 IO.128.0.105 10.128.0.124	2024/06/21 11:35 Netw Defau Defau Defau Defau Defau	5) vork uit uit uit uit uit uit	End Of 5 2022/10/	ale 31	2027/10/31			le	Software End Of Life	12 18 4 299	fwares updated	EOX information EOX information EOX information EOX information	h does not exist for the h does not exist for the h does not exist for the h does not exist for the
Populate End Of Sale 3 Populate End Of Sale (20 20 IP Address 10.128.0.49 10.128.0.79 10.128.0.79 10.128.0.108 10.128.0.108 10.128.0.108 10.128.0.101 10.128.0.108 10.128.0.108 10.128.0.108 10.128.0.108 10.128.0.101 10.128.0.101	2024/06/21 11:35 Netwo Defau Defau Defau Defau Defau Defau	5) vork uit uit uit uit uit uit	End Of 5 2022/10/	ale 31	2027/10/31	_		le	Software End Of Life	12 18 4 299 2	iwares updated	EOX information EOX information EOX information EOX information	h does not exist for the t does not exist for the t does not exist for the t does not exist for the t
Populate End Of Sale 37 Populate End Of Sale (20 Populate End Of Sale (20 Populate End Of Sale (20 Populate Sale (20 Pop	2024/06/21 11:35 Netw Defau Defau Defau Defau Defau Defau Defau	5) vork uit uit uit uit uit uit uit uit	End Of S 2022/10/ 2020/10/ 2020/10/	ale 51 30	2025/10/31	_		le	Software End Of Life	14 18 4 299 2 4 4 2	lwares updated	EOX information EOX information EOX information EOX information EOX information	s does not exist for the h does not exist for the h does not exist for the h does not exist for the h
opulate End Of Sale 2 PAddress 10.1280.0144 10.1280.019 10.1280.010 10.1280.108 10.1280.108 10.1280.108 10.1280.114 10.1280.11	2024/06/21 11:35 Netw Defau Defau Defau Defau Defau Defau Defau	5) vork uit uit uit uit uit uit uit uit	End Of S 2022/10/ 2020/10/	ale 51 30	2027/10/31	_		ie	Software End Of Life	12 18 299 2 4 2 2 82 82	awares updated	EOX information EOX information EOX information EOX information EOX information	s does not exist for the h does not exist for the h does not exist for the h does not exist for the h
Oppulate End Of Sale 3 Oppulate End Of Sale (20) P Address (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	2024/06/21 11:35 Netw Defau Defau Defau Defau Defau Defau Defau Defau Defau	5) vork uit uit uit uit uit uit uit uit uit uit	End Of 5 2022/10/ 2020/10/ 2020/10/ 2010/06/ 2018/05/ 2018/05/	ale 51 23 24 29	2027/10/31 2025/10/31 2006/06/23 2023/07/31 2023/07/31			ke en	Software End Of Life	12 18 299 2 4 2 4 82 82 82 4	Invares updated	EOX information EOX information EOX information EOX information EOX information	n does not exist for the f does not exist for the f
Populate End Of Sale 3 Populate End Of Sale (20 20 Populates End Of Sale (20 20 10/126/074 10 </td <td>2024/06/21 11:35 Netw Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau</td> <td>5) vork urt urt urt urt urt urt urt urt urt urt</td> <td>End OT 2 2022/10/ 2020/10/ 201/06/ 2016/05/ 2016/09/ 2023/11/</td> <td>30 30 23 04 29 07</td> <td>2027/10/31 2025/10/31 2006/06/23 2023/07/31 2023/07/31 2023/07/31</td> <td></td> <td></td> <td>ie and a second s</td> <td>Software End Of Life</td> <td>12 18 4 299 2 4 2 82 4 10</td> <td>awares updated</td> <td>EOX information EOX information EOX information EOX information EOX information</td> <td>Results per page 25 indoes not exist for the fi does not exist for the fi</td>	2024/06/21 11:35 Netw Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau	5) vork urt urt urt urt urt urt urt urt urt urt	End OT 2 2022/10/ 2020/10/ 201/06/ 2016/05/ 2016/09/ 2023/11/	30 30 23 04 29 07	2027/10/31 2025/10/31 2006/06/23 2023/07/31 2023/07/31 2023/07/31			ie and a second s	Software End Of Life	12 18 4 299 2 4 2 82 4 10	awares updated	EOX information EOX information EOX information EOX information EOX information	Results per page 25 indoes not exist for the fi does not exist for the fi
C Notes Notes Products End Of Sale 3 Products End Of Sale 3 In Labours 3 Notacan 1 Notacan	2024/06/21 11:35 Netw Uetau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau Defau	5) vork urt urt urt urt urt urt urt urt urt urt	End Of 5 2022/10/ 2020/10/ 2020/10/ 2010/06/ 2018/05/ 2018/05/	30 30 23 04 29 07	2027/10/31 2025/10/31 2006/06/23 2023/07/31 2023/07/31	-		ie 	Software End Of Life	12 18 299 2 4 2 4 82 82 82 4	wares updated	EOX information EOX information EOX information EOX information EOX information	s does not exist for the does not exist for the h does not exist for the n does not exist for the h does not exist for the

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.

🗑 🔻 Vendor/Model	OS: Cisco - X Add	Criteria 🔻 🗷 🕤									See Dev	vice 😂 Inventory 👁 Tools 🦠 Change 👶 Smart	Change 👪
IP Address	Hostname	Network	Adapter	HW Vendor	Model	Device Type	OS Version	Serial#	Backup Duration	End Of Sale	End Of Life	G Credentials)f Life
192.168.20.83	SF300-24	Core	Cisco Small Business	Cisco	SF300-24	Switch	1.4.11.5	DNI144402YT	28s	1969/12/31	1969/12/31	Protocols	
192.168.1.61	C9800-WLC	Core	Cisco IOS	Cisco	C9800-L-C-K9	Wireless Controller	16.12.4a	FCL245100KU	15	1969/12/31	1969/12/31	Add	
0 10.0.0.223	_1234	Core	Cisco IOS	Cisco	CSR1000V	Router	17.3.5	9MTTHU5FGVS	15	1969/12/31	1969/12/31	Add new device	
0 10.0.0.227	Nexus5548	Core	Cisco Nexus	Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	7s	1969/12/31	1969/12/31	Discover new devices	
192.168.0.254	hi-gw-B	Core	Cisco IOS	Cisco	WS-C3650-24TS	Switch	16.8.1a	FDO2027E0MQ	3s	1969/12/31	1969/12/31	Export inventory as Excel file	
10.0.100.89	cisco_10_0_100_89	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9N71QX4N5I9	15			Export inventory with configurations as ZIP	iir.
10.0.100.85	cisco_10_0_100_85	Core	Cisco IOS	Gisco	CSR1000V	Router	15.4(1)S4	9PBMWOQGS5D	15			Save inventory import Excel template	
10.0.100.88	cisco_10_0_100_88	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9KV83RO5JZU	15			Import/update inventory from Excel file	
10.0.100.90	cisco_10_0_100_90	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9GY3GDW3RBG	15			Cisco SNTC Portal	
10.0.100.87	cisco_10_0_100_87	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9EAVHJ554U7	15			Boo Export inventory as Cisco csv file	
10.0.100.84	cisco_10_0_100_84	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9W3FWU98YQD	15			import/update end of life from Cisco csv file	-
10.0.100.82	cisco_10_0_100_82	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9C7M5L0VDAS	15			Manage	
10.0.100.83	cisco_10_0_100_83	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9HBTH5O1Y6X	15			Device Tags	
10.0.100.86	cisco_10_0_100_86	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9O28E4JWQH5	15			X Delete device	
10.0.100.81	cisco_10_0_100_81	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9WI5FRHU059	15			Kun Startup Wizard	
10.0.0.128	888	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9J4P8735EIN	15				
10.0.0.101	RouterM	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	9AUD099HDKJ	15				
10.0.0.126	R1	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9E0UQZIVK9E	15				
9 192.168.1.10	hi-intra-sw	Core	Cisco IOS	Cisco	WS-C2960X-24TS-L	Switch	15.2(2)65	FOC1835S3PX	25				
10.0.0.250	hicore	Core	Cisco IOS	Cisco	CISCO1921/K9	Router	15.4(3)M5	FGL15082638	75				
10.0.0.124	shibata	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)S4	9V0INVIMG0X	15				
0 10.0.0.112	tech1121	Core	Cisco IOS	Cisco	CSR1000V	Router	15.4(1)54	90XP5HS5IG7	15				

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

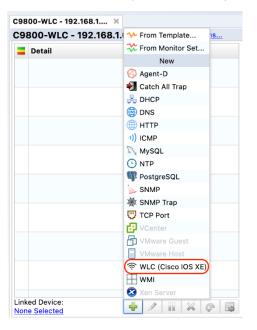
- 1. Add your Wireless Lan Controller, and its associated Access Points to the inventory.
- 2. Ensure that their hostnames are correct, and that their Device Adapters are set to Cisco IOS.

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:

wic		
Index	count	
C9120AXE-Q		<u>4</u>
C9120AXI-Q		<u>9</u>

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.

€	Das	shboards	Inventory	Chan	ges Jobs	Terminal Proxy	/ Search	Compliance	Monitors	Incidents	Мар	MIBs	Playbook	Wi-Fi Clients		admin	Logout	Settings	Help
-		▼ Name	: -Any-	×× La	ast Checked:	-Any- 👻 🛪	Last Seen: -	Any- 👻 🛪	Add Criter	ia 🔻 🙁 숙	>								ø
		SSID		•	Access Point	۱ I	Name		IP Address		IPv6 Ad	dress		MAC	Last Checked	Las	t Seen		
	\checkmark	🕼 logicy	ein_network		C9120AXI-Q				192.168.1.174		fe80::4	13:5435:0	:508:174e		25/02/18 10:43.02	25/0	02/18 10:4	3.02	
	С	∎G8 logicv	ein_network		C9120AXE-Q				192.168.1.126		fe80::8	3c:7eef:e3	36d:7694		25/02/18 10:43.02	25/0	02/06 13:1	3.40	
	С	≡Øð logicv	ein_network		C9120AXI-Q				192.168.1.172		fe80::8	Bbf:62ff:f	e6a:c294		25/02/18 10:43.02	25/0	02/06 13:1	3.40	
	С	≡Ø logicv	ein_network		C9120AXI-Q				192.168.1.129		fe80::8	a32:2efc:	af3b:bbd8		25/02/18 10:43.02	25/0	02/07 08:0	07.45	
	\checkmark	∎G8 logicv	ein_network		C9120AXI-Q				192.168.1.191		fe80::5	d37:e37a:	393c:9482		25/02/18 10:43.02	25/0	02/18 10:4	3.02	

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.

S: 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.

		🔚 Save	🖉 Discard	🔀 View			
		Gen	eral				
	Map Name:	wlc					
	Automatically update after discovery						
	Device Label Format:						
	IP Address						
	Link Label Format:						
	ifName						
	Font Size:						
	🕂 Insert 🛙	Device		nsert Map			
		No	Node				
	Position						
ababa	X: 380						
192.168.1.63	Y: 159						
	Icon						
(m)							
	Image: ma	ap/cisco.svg		×			
	Show cl	ient list					
a client	∲ 🕹		3	Kemove			
E							
another client							

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].

System backup/restore 8

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.

	Server Settings
Data Retention	 Enable daily system backup
System Backup	Perform the system backup daily at this time: 16 🚔 : 0 🚔
Mail Server	Perform the system backup daily at this time: $16 = 0 =$
SNMP Traps	Number of backups to keep: 1 🗸
Users	
Roles	
External Authentication	Perform System Backup Now
Custom Device Fields	Last successful system backup performed: 2024/01/08 16:02 (Download)
Memo Templates	
Launchers	
Networks	
Network Servers	
Syslog	
Software Update	
Web Proxy	Restore System Backup
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
Agent-D	•
	OK Cancel
Item	Explanation

Enable daily system backups

planation

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].

	Server Settings
Data Retention	Enable daily system backup
System Backup	Perform the system backup daily at this time: 16 📥 : 0 📥
Mail Server	
SNMP Traps	Number of backups to keep: 1 🗸
Users	
Roles	
External Authentication	Perform System Backup Now
Custom Device Fields	Last successful system backup performed: 2024/01/08 16:02 (Download)
Memo Templates	
Launchers	
Networks	
Network Servers	
Syslog	
Software Update	
Web Proxy	Restore System Backup
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
Agent-D	•
	OK Cancel

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.

	Server Settings
Data Retention	Enable daily system backup
System Backup	Perform the system backup daily at this time: 16 📥 : 0
Mail Server	
SNMP Traps	Number of backups to keep: 1 🗸
Users	
Roles	
External Authentication	Perform System Backup Now
Custom Device Fields	Last successful system backup performed: 2024/01/08 16:02 (Download)
Memo Templates	
Launchers	
Networks	
Network Servers	
Syslog	
Software Update	
Web Proxy	Restore System Backup
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
Agent-D	~
	OK Cance

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.

	Server Settings
Data Retention	Enable daily system backup
System Backup	Perform the system backup daily at this time: 16 🚔 : 0
Mail Server	
SNMP Traps	Number of backups to keep: 1 🗸
Users	
Roles	14
External Authentication	30 m System Backup Now
Custom Device Fields	Last successful system backup performed: 2024/01/08 16:02 (Download)
Memo Templates	
Launchers	
Networks	
Network Servers	
Syslog	
Software Update	
Web Proxy	Restore System Backup
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
Agent-D	•
	OK Cancel

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].

LogicVein -	LogicVein - Core Server							
	https://192.168.40.122							
Networking:								
Gateway: Hostname: NTP Server: Time: IPu6 Addr: MAC Addr: Revision :	192.168.40.122 Netmask: 255.255.255.0 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 netld Interface: eth0 pool.ntp.org SSH Server: Ruming 2021-03-23 07:54 UTC Backup: Local fd14:5839:6644:40:20c:29ff:feb6:baf9 00:0c:29:B6:BaF9 20210316.0604 2019.24.0-202103160604							
OVA Build :	1615874999							
[1] Static *[2] DHCP [3] SSH Ser [4] Import 1 [5] Admin T [6] Reboot	[3] SSH Server [4] Inport Data [5] Admin Tools							

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

Networking:				
Gateway: Hostname: NTP Server: Time: IPv6 Addr:	192.168.40.122 192.168.40.254 netld pool.ntp.org 2021-03-23 08:00 UTC fd14:5539:6644:40:20c 00:0C:29:86:8A:F9	DMS: Interface: SSH Server: Backup:	Running Local	92.168.0.3
	20210316.0604 2019.24.0-202103160604 1615874999	1		
Admin Tool	ls menu:			
[2] Vacuum I [3] Reset Ad [4] Configur [5] Reset Ad	Tig Diff Cleanup Jatabase Amin Password re a remote filesystem Amin Dashboard API Toko re Built-in Agent-D			

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.

LogicVein - Core Server	
https://192.168.40.122	2
Networking:	
IP Address: 192.168.40.122 Gateway: 192.168.40.254 Hostname: metld NTP Server: pool.ntp.org Time: 2021-03-24 02:46 UTC IPVG Addr: Addr:5839:6644:40:20c: MAC Addr: 00:0C:29:86:BA:F9	Backup: 10.0.111.1:/datastore
Revision : 20210316.0604 OS Version: 2019.24.0-202103160604 OVA Build : 1615874999 Settings menu:	ł
[1] Static IP Address *12] DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Reboot [7] Power Off	
-	

8.5 Create system backup zip file

To create a backup zip file on external storage:

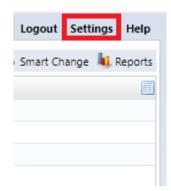
- 1. Open the backup folder. The folder name will be in the format "(backup_YYYY\\MM\\DD)".
- 2. Save the following three items to a zip file:
- pgsql (folder)
- version.txt (file)
- complete (file)

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].

		Server Settings
Data Retention		Enable daily system backup
System Backup		Perform the system backup daily at this time: 16 🔺 : 0
Mail Server		
SNMP Traps		Number of backups to keep: 1 🗸
Users		
Roles		
External Authentication		Perform System Backup Now
Custom Device Fields		Last successful system backup performed: 2024/01/08 16:02 (Download)
Memo Templates		
Launchers		
Networks		
Network Servers		
Syslog		
Software Update		
Web Proxy		Restore System Backup
Change Approvals		
Cisco API		
Device Label		
SNMPv3 User		
Agent-D	•	
		OK Cancel

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

😌 Open							>
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Dow	vnloads > backup			~ C	Search backup		ç
Organize • New folder					≣	•	?
A Home Na	ime	Date modified	Туре	Size			
→ Gallery → Toda	ay vackup_2024-01-08	1/9/2024 10:36 AM	Compressed (zipp	392,152 KB			
Esktop ★ ↓ Downloads ★							
File name:				~	Compressed (zip	ped) Folder Cancel	~

5. Click [Yes] on the warning screen.

	Server Settings
Data Retention	Enable daily system backup
System Backup	Perform the system backup daily at this time: 16
Mail Server	
SNMP Traps	Number of backups to keep: 1 🗸
Users	
Roles	
External Authentication	Restore Backup Warning
Custom Device Fields	
Memo Templates	You are trying to perform a destructive action! Server will restart after you upload a backup file for restoring.
Launchers	Are you sure you want to proceed?
Networks	File Name: backup_2024-01-08.zip
Network Servers	
Syslog	Yes Cancel
Software Update	
Web Proxy	Restore System Backup
Change Approvals	
Cisco API	
Device Label	
SNMPv3 User	
Agent-D 💌	
	OK Cancel

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

			Server Se	ttings			
	Data Retention		🗹 Enable daily system back	qu			
	System Backup		Perform the system backup da	Perform the system backup daily at this time: 16 $\frac{4}{\sqrt{2}}$: 0		A	
	Mail Server			-	· · · · · · · · · · · · · · · · · · ·	•	
	SNMP Traps		Number of backups to keep:	1 ~			
	Users						
	Roles						
	External Authenticatio	n		Perform System	n Backup Now		
-	Custom Device Fields		Last successful syste	em backup perfor	med: 2024/01/08 16:02	(Download)	
30	Memo Templates	_	Uploadin	a File			
	Launchers			.			
	Networks	Uploading f	ïle				
	Network Servers	, ,					
	Syslog						
	Software Update						
	Web Proxy			Restore Syst	em Backup		
	Change Approvals						
	Cisco API						
Δ.	Device Label						
	SNMPv3 User						
	Agent-D	-					
						ОК	Cancel

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.

https://192.168.40.122 Networking: If Address: 192.168.40.122 Netnask: 255.255.255.0 Gatoway: 192.168.40.254 District 20.0 Netstanae: metid Interface: etho Netstanae: metid Interface: etho Netstanae: metid Interface: etho Nets Addre: 2021-03-23 07:54 UTC Backup: Local Proceed: 2021-03-23 07:54 UTC Backup: Local Nets Addre: 00:0c:23:16:180:19 Revision: 20210316.0604 Os Version: 20210316.0604 Os Version: 2019.24.0-202103160604 Os Version: 2019.24.0-202103160604 Os Version: 2019.24.0-202103160604 Os Version: 2019.24.0-202103160604 Distription: 20210316.0604 Is Version: 2019.24.0-202103160604 Distription: 20210316.0604 Is Version: 2019.24.0-202103160604 Distription: 20210316.0604 Is Version: 2019.24.0-202103160604 Distription: 20210316.0604 Is Version: 20210316.0604 Distription: 202104 Distription: 202104 Distription: 202104 Distriptio	Networking: IP Address: 192.168.40.122 Netnask: 255.255.255.0 Gateway: 192.168.40.124 DNS: 192.168.0.3 192.168.0.3 Hostname: metld Interface: eth0 NTP Server: pool.ntp.org SSH Server: Running Time: 2021-03-23 07:54 UTC Backup: Local IPo6 Addr: 401:539:664:40:20:202:29ff:feb6:baf9 MAC Addr: 00:0C:29:B6:BA:F9 Revision : 20210316.0604 USV Bersion: 2019.24.0-202103160604 USV Backup: Local III Static IP Address *121 DMCP [13] Static IP Address *123 DMCP [13] Static IP Address *121 DMCP [13] Static IP Address *121 DMCP [13] Static IP Address *121 DMCP [14] Inport Data [15] Admin Tools [16] Reboot	LogicVein – Cor	re Server			
IP Address: 192.168.40.122 Netnask: 255.255.255.0 Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 HOStname: netld Interface: eth0 MTP Server: pointp.org SSH Server: Running Time: 2021-03-23 07:54 UTC Backup: Local IPo6 Addr: 100:0239:166.40.20 291f:feb6:baf9 MAC Addr: 00:02:29:186:188:F9 Revision: 20210316.0604 05 Version: 2019.24.0-202103160604 00 004 Build: 1615874999 Settings menu:	IP Adverses: 192.168.40.122 Netmask: 255.255.0 Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 HOStname: netId Interface: eth0 NTP Server: pool.htp.org SSH Server: Running Time: 2021-03-23 97:54 UTC Backup: Local IPo6 Addr: 601:020:29:166:184:90 Backup: Local USC MAC Addr: 00:0C:29:186:184:F9 Backup: Local USC USC	htt	tps://192.168.40.122			
Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 Hostname: netld Interface: eth0 NTP Server: pool.ntp.org SSH Server: Running Time: 2021-03-23 07:54 UTC Backup: Local IPv6 Addr: Add: 309:604.40:20c:29ff:feb6:baf9 MAC Addr: 00:00:29:B6:BA:F9 Revision : 20210316.0604 OS Version: 2019.24.0-202103160604 OVA Baild : 1615874399 Settings menu: 	Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 Hostname: netld Interface: eth0 NTP Server: pool.tp.org SSH Server: Running Time: 2021-03-23 07:54 UTC Backup: Local IPv6 Addr: f01:3039:6644:40:20c:29ff:feb6:baf9 MAC Addr: 00:00:29:B6:BA:F9 Revision : 20210316.0604 DS Version: 2019.24.0-202103160604 DV Baild : 1615874399 Settings menu: 	Networking :				
Settings menu: [1] Static IP Address *(2] DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Rebot	Settings menu: 	Gateway: 192 Hostname: nef NTP Server: poo Time: 202 IPu6 Addr: fd1 MAC Addr: 00: Revision : 202 OS Version: 201	2.168.40.254 E1d 1.ntp.org 21-03-23 07:54 UTC 14:5839:664d:40:20c: 06:29:86:8A:F9 210316.0604 19.24.0-202103160604	DNS: Interface: SSH Server: Backup: 29ff:feb6:ba	192.168.0.3 192.168.0 eth0 Running Local	.3
[1] Static IP Address #21 DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Beboot	[1] Static IP Address #21 DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Beboot	OVA Build : 161	15874999			
*IZI DHCP I31 SSH Server I41 Import Data I51 Admin Tools I61 Reboot	*IZI DHCP I31 SSH Server I41 Import Data I51 Admin Tools I61 Reboot	Settings menu:				
		*[2] DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Reboot	1			

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.

LogicVein -	Core Server
	https://192.168.40.122
Networking:	
Gateway: Hostname: NTP Server: Time: IPv6 Addr:	192.168.40.122 Netmask: 255.255.05 192.168.40.254 DNS: 192.168.0.3 netld Interface: etho pool.ntp.org S3H Server: Running 2021-03-23 07:54 UTC Backup: Local 1414:533':6644:40:20c:29:FF:Feb6:baf9 00:00:02:29:B6:BA:F9 00:00:20:20:20:20:20:20:20:20:20:20:20:2
	20210316.0604 2019.24.0-202103160604 1615874999
Settings men [1] Static [2] DHCP [3] SSH Serv [4] Import] [5] RAmin To [6] Reboot [7] Power 0 Are you sure g	Jer Paddress Joata Joals

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.

LogicVein - Core Server
https://192.168.40.122
Networking:
IP Address: 192.168.40.122 Netmask: 255.255.255.0 Gateway: 192.168.40.254 DNS: 192.168.0.3 192.168.0.3 Hostmane: netld Interface: eth0 NTP Server: pool.ntp.org SSH Server: Running Time: 2021-03-23 07:55 UTC Backup: Local IPv6 Addr: fd14:5833:6644:40:20e:29ff:feb6:baf9 MAC Addr: 00:00:223:B6:BA:F9
Revision : 20210316.0604 OS Version: 2019.24.0-202103160604 OVA Build : 1615874999
Settings menu:
[1] Static IP Address *[2] DHCP [3] SSH Server [4] Import Data [5] Admin Tools [6] Reboot [7] Power Off
Are you sure you want to POWER OFF ? (y/N) [default: N] _

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:

🔂 sc-10.0.0.184	-test-LD	P 🖗 🕼	ACTIONS V
Summary Monitor	Configure Permissions	Datastores	Actions - sc-10.0.0.184-test-LD
Powered Off aunch Web Console aunch Remote Console		d later (VM version 1	
VM Hardware			VM Policies
Related Objects			Template Compatibility
Cluster	li i	Cluster-01	Export System Logs
Host		simplivity-01.intra.h	🔂 Edit Settings
Networks	ŝ	Labo Network	Move to folder
Storage		eng-support	Rename
			Edit Notes
Tags			Tags & Custom Attributes 🕨
Assigned Tag	Category		Add Permission
			Alarms 🕨
			Remove from Inventory
× 51	tatus 🗸 🗸	Detalls	Delete from Disk

拱 Hyper-V Manager			Actions
dvanced IP Scanner Google Chrome Server ministrato	Virtual Machines Name State CPU Usage Assigned Memore ACCT Off-Critical FS Off-Critical Checkpoints The selected virtual machine has no checkpoints.		HOST2 New Import Virtual Machin Hyper-V Settings Virtual Switch Manage Virtual SAN Manager Edit Disk
Active rectory D Active irrectory	SJC-FS Created: 1/1/0001 12:00:00 AM Clustered Configuration Version: Generation: 2 Notes: None Summary Memory Networking Replication	:	Help

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

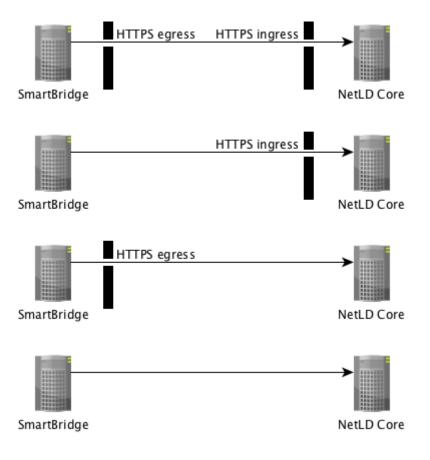
All connections are via HTTPS, so wire traffic is encrypted end-to-end.

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.

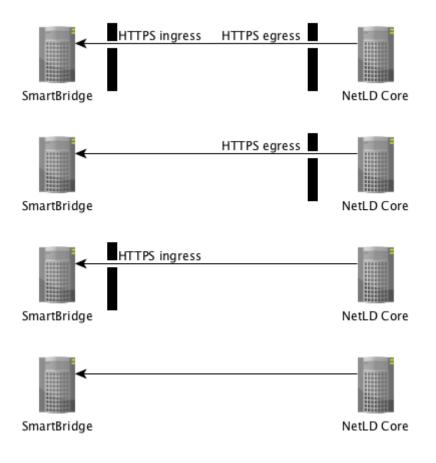


11.2 Server-to-Bridge

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 Smart-Bridge 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.

			admin	Logout Settings Help
			🗢 Device 😂 Invent	tory 👁 Tools 鷱 Reports
n	Serial#	End Of Sale	End Of Life	Traits
	210235A15DC10B			icmp ncm snm 🔺
	422cadb1-b343-8			https icmp ncr
31	422CE9BD928F827			http https icm
	4AC904A634C4			http ncm snm
	90XP5HS5IG7			https (icmp) ncr

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

Server Settings					
Data Retention	Name	Connection	Bridge Host (Port)		
System Backup					
Mail Server					
SNMP Traps					
Users					
Roles					
External Authentication					
Custom Device Fields					
Memo Templates					
Launchers					
Smart Bridges					
Networks					
Network Servers					
Syslog					
Software Update					
Web Proxy					
Device Label					
SNMPv3 User					
Agent-D					
	Token:		🔁 🧳 🖉 💥		
			OK Cance		

3. Enter the name for the Smart Bridge

	Bridge Host	
Name:	SmartBridge	
Connection:	Bridge→Server	~
		OK Cancel

4. Click [Connection].

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

	Bridge Host	
Name:	SmartBridge	
Connection:	Server→Bridge	~
Host or IP:	192.168.0.1	
Port:	443	
		OK Cancel

5. Click [OK].

6. Copy token.

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

		Server	Settings	
Data Retention		Name	Connection	Bridge Host (Port)
System Backup	0	SmartBridge	Bridge→Server	-
Mail Server				
SNMP Traps				
Users				
Roles				
External Authentication				
Custom Device Fields				
Memo Templates				
Launchers				
Smart Bridges				
Networks				
Network Servers				
Syslog				
Software Update				
Web Proxy				
Device Label				
SNMPv3 User				
Agent-D				
	Toker	58b945dccd004f	7882292d80b0e0a021	🖣 🧳 🥖
				OK Ca

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.

Networking:
IP Address: 192.168.30.20 Netmask: 255.255.0 Gateway: 192.168.30.254 DNS: 192.168.0.3
Hostname: netId-SB Interface: eth0 NTP Server: 10.0.0.254 SSH Server: Not Running Time: 2019-08-08 14:47 UTC Backup: Local
IPu6 Addr: fd14:5839:664d:30:215:5dff:fe99:205 MAC Addr: 00:15:5D:99:02:05
Revision : 20190802.1813 OS Version: 2019.05.0-201908021813 OVA Build : 1564740844
SmartBridge Direction:
Configure the direction of the SmartBridge connection initiation. Choose from the following options:
 (B) Bridge initiated [bridge->server]. Requires authentication token. (S) Server initiated [server->bridge]. Requires authentication token. (A) Server initiated [server->bridge]. First connection assigns token.
Bridge initiated or server initiated (B/S/A) [default: B]: B Remote LogicVein Server hostname or IP address: 192.168.30.19 Remote LogicVein Server port [default: 443]: 443
SmartBridge authentication token (32 characters): 93af38583e0f6bfe108f9698e833cf_

Project	Explanation	Keyboard Selction
Connection Initiation	Connection direction	
	Connect from Bridge to Server (with token)	[B]
	Connect from Server to Bridge (with token)	[S]
	Connect from Server to Bridge (without token)	[A]
Hostname or IP	Core server (ThirdEye) IP address	192.168.30.19
address		
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.

			admin	Logout Settings	Help
			🗢 Device 😂 Inver	ntory 👁 Tools 💐	Reports
n	Serial#	End Of Sale	End Of Life	Traits	Ē
	210235A15DC10B			icmp ncm	snm 🔺
	422cadb1-b343-8			https icmp	ncr
31	422CE9BD928F827			http https	icm
	4AC904A634C4			http ncm	snmj
	90XP5HS5IG7			https icmp	ncr

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

System Backup Default (None) Mail Server SMMP Traps I <lii< li=""> I I I</lii<>	Data Retention		Name	Bridge	
SNMP TrapsIImage: Constraint of the second of the se	System Backup	0	Default	(None)	
UsersIIIRolesIIIExternal AuthenticationIIICustom Device FieldsIIIMemo TemplatesIIILaunchersIIISmart BridgesIIINetworksIIINetworks ServersIIISyslogIIISoftware UpdateIIIWeb ProxyIIIDevice LabelIIISNMPv3 UserIII	Mail Server				
RolesImage: state of the state o	SNMP Traps				
External Authentication Image: Custom Device Fields Custom Device Fields Image: Custom Device Fields Memo Templates Image: Custom Device Fields Launchers Image: Custom Device Fields Smart Bridges Image: Custom Device Fields Networks Image: Custom Device Fields Networks Image: Custom Device Fields Networks Image: Custom Device Fields Network Servers Image: Custom Device Fields Syslog Image: Custom Device Fields Software Update Image: Custom Device Fields Web Proxy Image: Custom Device Fields Device Label Image: Custom Device Fields SNMPv3 User Image: Custom Device Fields	Users				
Custom Device Fields Image: Custom Device Fields Memo Templates Image: Custom Device Fields Launchers Image: Custom Device Fields Smart Bridges Image: Custom Device Fields Smart Bridges Image: Custom Device Fields Networks Image: Custom Device Fields Styling Image: Custom Device Fields Software Update Image: Custom Device Fields Web Proxy Image: Custom Device Fields Device Label Image: Custom Device Fields SNMPv3 User Image: Custom Device Fields	Roles				
Memo TemplatesImage: Constraint of the second s	External Authentication				
LaunchersImage: Constraint of the second	Custom Device Fields				
Smart Bridges Image: Constraint of the second of the s	Memo Templates				
NetworksImage: Servers serversImage: Servers servers serversImage: Servers	Launchers				
Network Servers Image: Constraint of the constraint of	Smart Bridges				
Syslog Image: Syslog Software Update Image: Syslog Web Proxy Image: Syslog Device Label Image: Syslog SNMPv3 User Image: Syslog	Networks				
Software Update Image: Constraint of the second of the s	Network Servers				
Web Proxy Image: Comparison of the second	Syslog				
Device Label SNMPv3 User	Software Update				
SNMPv3 User	Web Proxy				
	Device Label				
Agent-D	SNMPv3 User				
	Agent-D				

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

	Managed Network
Name:	SmartBridge Network
Bridge Host:	SmartBridge 🗸 🗸
Use a jumphost	for this network.
IP Address:	
Username:	
Password:	
Override Port:	22
Adapter:	Cisco IOS 🗸 🗸
Max Connections:	0
Use return addr	ress for FTP/TFTP
NAT Address:	
	OK Cancel

4. Click [OK]

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

		Server Settings		
Data Retention		Name	Bridge	
System Backup	0	Default	(None)	
Mail Server	0	SmartBridge Network	SmartBridge	
SNMP Traps				
Users				
Roles				
External Authentication				
Custom Device Fields				
Memo Templates				
Launchers				
Smart Bridges				
Networks				
Network Servers				
Syslog				
Software Update				
Web Proxy				
Device Label				
SNMPv3 User				
Agent-D				
				🔶 🖉 兴
				OK Cancel

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.

C 命 気に入りのインポート	 セキュリティ保証 Git with a cup 		//10.0.0.95 incerNetworks JIRA	🗿 On-Prem Met	a 🧕 Jenkins 💋	vcenter 🚸 S	elenium API(逆引き)	🌴 Net LineDancer		☆ CD Y ectWEBDグイン	⊱ % 00 …
Dashboards Invent	ory Changes	Jobs Terminal	Proxy Search N	Ionitors Incide	ents Map MIBs			Network	Default	✓ admin	Logout Settings Help
Search IP/Host		Add Criteria							<all></all>		entory 👁 Tools կ Reports
-	-								Default F SmartBridge		
IP Address	Hostname	Network	Memo	HW Vendor	Model	Device Type	OS Version		E	Life	Traits
10.0.0.213	\$3100	Default		H3C	S3100-26T-SI	Switch	3.10	210235A15DC10B			icmp ncm snm 🔺
10.0.0.206	bigip1	Default	- 0	F5 Networks	BIG-IP Virtual Editi	Load Balancer	11.6.0	422cadb1-b343-8			https icmp ncr
10.0.0.229	lvi.infoblox.local	Default	÷	Infoblox	IB-VMWARE	DDI	8.4.4-386831	422CE9BD928F827			http https icm
0.0.3.120	MikroTik RouterBo		トポロジー 🖉	MikroTik	RB951Ui-2HnD	Router	6.22	4AC904A634C4			http ncm snm
10.0.0.112	vetsu New-SMD 30.175	Default		Cisco	CSR1000V	Router	15.4(1)S4	90XP5HS5IG7			(https) (icmp) (ncr (icmp) (ncm) (snm
192.168.30.175 10.0.0.165	cisco165	Default Default		Cisco	CSR1000V CSR1000V	Router	15.4(2)5	93BC4BHS05J 95NXXGSYJKM			
10.0.0.153	test.intra.lvi.co.jp	Default		Cisco	CSR1000V CSR1000V	Router	15.4(1)S4 15.4(1)S4	95NXXGSYJKM 9A0HFGQYZF6			http https icm
10.0.0.101					CSR1000V CSR1000V				2021/09/21	2024/09/20	icmp ncm snm
10.0.0.126	RouterM.Ivi.local	Default Default		Cisco Cisco	CSR1000V CSR1000V	Router	15.4(1)S4 15.4(1)S4	9AUD099HDKJ 9E0UOZIVK9E	2021/09/21	2024/09/20	https icmp ncr
10.0.0.128	cisco164	Default		Cisco	CSR1000V CSR1000V	Router		9EAVHJ554U7			
10.0.0.128	testLVI	Default		Cisco	CSR1000V CSR1000V		15.4(1)54	9J4P8735EIN	2021/09/21	2024/09/20	(https) (cmp) ncr
192,168,30,151						Router	15.4(1)54		2021/09/21	2024/09/20	
	test151 tech	Default Default		Cisco	CSR1000V CSR1000V	Router	15.4(2)S	9NQ6RI9LXAP 9V0INVIMG0X	2021/09/21	2024/09/20	(icmp) ncm (snm (https) (icmp) ncr
10.0.0.124 10.0.0.223	tech test2.intra.lvi.co.ip	Default	1-7 (1) 0 0		CSR1000V CSR1000V	Router	15.4(1)54	9V7J6ZWFXB3	2021/09/21	2024/09/20	http https icm
10.0.0.161	cisco161	Default	トラフィック… 🖉	Cisco	CSR1000V CSR1000V	Router	15.4(1)54	9W3FWU98YOD	2021/09/21	2024/09/20	http https icm
							15.4(1)54		2021/00/21	2024/00/20	
10.0.0.228 10.0.0.192	LAB-7060CX-32S FortiAuthenticator	Default Default		Arista Fortinet	vEOS-lab FortiAuthenticator	Switch	4.28.0F 6.4.0	E526ABD3D17628 FAC-VM0000000000	2021/09/21	2024/09/20	(icmp snmp ssl (http https (icm
	FAZVM64					Server	7.2.0	FAZ-VM000000000			http https icm
	1921CiscoRouter	Default Default		Fortinet	FortiAnalyzer-VM64			FGL15082638	2021/09/21	2024/00/20	
10.0.0.250 fd14:5839:664d:10	1921CISCOROUTEr	Default		Cisco	CISCO1921/K9 CISCO1921/K9	Router	15.4(3)M5 15.4(3)M5	FGL15082638	2021/09/21	2024/09/20	(icmp) ncm (snm (icmp) ncm (snm
10.0.0.232							15.4(3)M5 6.2.4				http icmp ncm
	Fortigate-VM64 FMG-VM64	Default Default		Fortinet	FortiGate-VM64	Firewall	6.2.4 7.2.0	FGVMEVXMYGAQ FMG-VMTM22011			http icmp ncm
10.0.0.191 10.0.0.249		Default	Demo //	Cisco	FortiManager-VM64 WS-C2960S-24TS-L		7.2.0 15.2(2)E	FOC1721W1SR	2021/09/21	2024/09/20	http https icm
10.0.0.249	apcHost	Default	Demo	Apc	smartUPS2	Power Supply	v6.0.6	J11625110998	2021/09/21	2024/09/20	http https icm
10.0.0.217	apcHost ArubaOS-CX-VM	Default		Apc Hpe	arubaWiredSwitch		V6.0.6 Virtual.10.05.0020	OVA443E7F	2021/09/21	2024/09/20	
											http https icm
10.0.0.121	simulator.intra.lvi.c			Cisco	CRS-4/S	Router	4.3.1	SMA112502OL	2021/09/21	2024/09/20	icmp ncm snm
0.0.0.195	EXOS-VM21_1_2_14			Extreme	EXOS-VM	Switch	21.1.2.14	SN:123456	2024 (20 (24	2024/202720	http icmp snm
10.0.0.227 10.0.0.221	123 QuantumEdge	Default Default		Cisco	Nexus5548	Switch	7.1(4)N1(1)	SSI143708V7	2021/09/21	2024/09/20	(icmp) ncm (snm (http) (https) (icm -

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).