D-Link D-View 8

D-View 8

Network Management System

User Manual

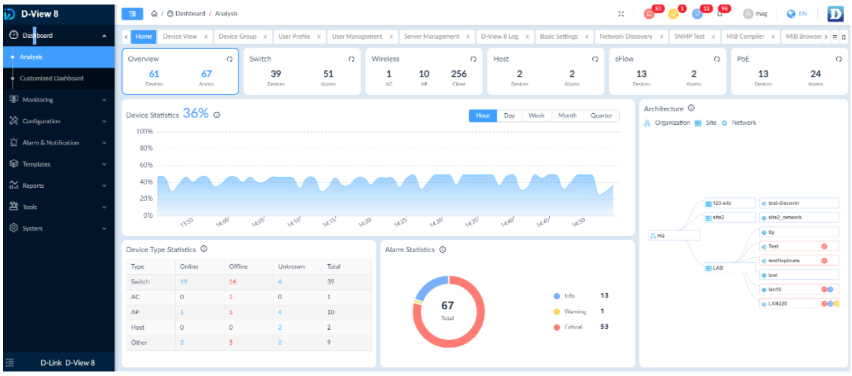
V2.01

Table of Contents

1 Introduction

1.1. D-Link D-View 8 Network Management Software

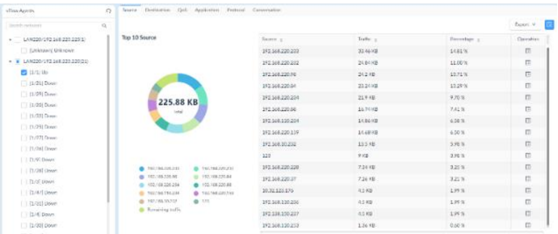
D-View 8 is a comprehensive management tool for both Ethernet and wireless Ethernet designed with the server and probe architecture, supporting troubleshooting, configuration, performance monitoring, and security of your network. It provides end-to-end operational management of IT structure, scalability of the system architecture, and accommodation of new technology that complements the management of D-Link and third-party devices.

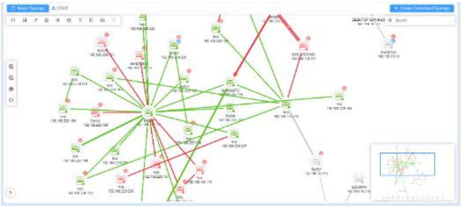


Device Type Statistics

Type	Online	Offline	Unknown	Total
Switch	19	16	4	39
AC	0	1	0	1
AP	1	5	4	10
Host	0	0	2	2
Other	2	5	2	9

D-View 8's offering of standard and enterprise licensing options is sufficient for different network requirements ranging from SMB to Enterprise deployment. Both Standard and Enterprise licenses can manage up to 5000 nodes, and the Enterprise Edition has richer features and supports multiple server probes either locally or remotely across multiple sites and networks.





Real-Time Network Analytics

sFlow Analyzer

Role-Based Administration

Intuitive Dashboard

Centralized Reporting

Highly Flexible and Scalable Deployment

Rich Resource Management

Inventory Management

Batch Configuration

Firmware Management

Service Monitoring

1.2. D-View 8 Features

The D-View 8 is a standards-based management tool designed for the centralized management of networks to achieve device availability, reliability, and resilience.

This manual is intended for network administrators. The D-View 8 supports the following features:

D-View 8 Features		
	Real-Time Network Analytics	Real-time network analysis provides insight into network operation. With instant visibility, you can obtain information on device statistics, such as critical alarm events, memory utilization statistics and analysis, response time statistics and analysis, and CPU utilization statistics as well as bandwidth utilization.
	sFlow Analyzer*	Configure sFlow analyzer to detect network anomalies in your organization, especially when the network is large and complex. It helps collect the sFlow data from devices and generate related statistics.
	Role-Based Administration	Allows easy integration of user management with a common authentication system such as Windows AD or RADIUS. User privileges are assigned by role and the access to each network can be individually granted with read or write or both.
	Intuitive Dashboard	The user-friendly dashboard can be customized to your needs for network device overview, device statistics, alarm statistics, CPU/memory utilization, response time, temperature, and much more.
	Centralized Reporting	Provides a wide variety of performance information with templates for resource reporting, including top N resource utilization with respective optional indicators, network device and connection status, traps, and traffic. It also provides options for automatic reports or saving as My Reports.
	Highly Flexible and Scalable Deployment	No matter the scale of your network environment, D-View 8 provides you with a whole suite of network management capabilities and deployment options.
	Rich Resource Management	Provides the exploration and topology of the network, including comprehensive network inventory. Views include both Layer 2 and Layer 3, as well as VLAN topology which can all be customized.
	Inventory Management	Provides holistic management in one place for multi-vendor devices. Monitor key indicators of a network by accessing the device page, which shows real-time data of performance information, connected clients, and more.
	Batch Configuration	Configures multiple devices at the same time by creating tasks with schedules to allow for automatic configuration and rapid deployment.
	Firmware Management	Conveniently upgrades firmware for multiple devices from a centralized location.
	Service Monitoring	Monitors the availability and responsiveness of common network services via probes. The probes reside on local and remote D-View 8 software agents to check the connectivity of servers and devices.
* This feature is only supported on Enterprise Edition.		

NOTE: For the purposes of this manual, the D-View 8 application is referred to as the application. The device on which the application is installed is referred to as the D-View 8 server.

NOTE: For further information about the latest D-View 8 release, see the D-View 8 application information on the D-View 8 website (https://dview.dlink.com/).

NOTE: For the latest software updates with new features and bug fixes, visit the D-View 8 website (https://dview.dlink.com/). Some devices require regular downloads and update of new software and can do so only through manual update.

1.3. D-View 8 Licenses

License Types	
Standard (DV-800S)	Product license determines the edition of the D-View 8 application. Target Customer: SMB 1. Nodes: < 5000 (applicable to D-View 8 Version 2.0.0 and later) 2. D-View 8 server and probe: • Single server, no support for redundancy. • Single probe 3. Supports local probe only 4. The Org-Site-Network architecture: • Single Organization • Multiple Sites • Multiple Networks 5. Supports limited features 6. Free maintenance & product support for one year (365 days). Annual renewal will be required to operate with complete functionality without the limitation of 30 nodes and to keep the support contract valid.
Standard Maintenance (DV-800MS)	The maintenance license determines the length of time maintenance service is valid and the support service stops when it reaches the expiration date; however, the D-View 8 application will still be operational with a reduction of manageable nodes. DV-800MS-Y1-LIC DV-800MS-Y2-LIC DV-800MS-Y3-LIC DV-800MS-Y4-LIC DV-800MS-Y5-LIC (Y1=365 days, Y2=730 days, Y3=1095 days, Y4=1460 days, Y5=1825 days) The above annual maintenance licenses can only be activated on the Standard Software edition.
Enterprise (DV-800E)	Product license determines the edition of the D-View 8 application. Target Customer: Enterprise. 1．Nodes: <5000 2. D-View 8 server and probe: • Supports 2 servers and HA (high availability) • Multiple probes (up to 20) 3. Supports both local and remote probes. 4. The Org-Site-Network architecture: • Single Organization • Multiple Sites • Multiple Networks 5. Supports all features including advanced development and

	management tools: • REST API (full graphic user interface) • sFlow Analyzer • HA (MongoDB cluster, NLB/Keepalived) • MIB Browser and Compiler 6. Free maintenance & product support for one year (365 days). Annual renewal will be required to operate with complete functionality without the limitation of 30 nodes and to keep the support contract valid.
Enterprise Maintenance (DV-800ME)	The maintenance license determines the length of time maintenance service is valid and the support service stops when it reaches the expiration date; however, the D-View 8 application will still be operational with a reduction of manageable nodes. DV-800ME-Y1-LIC DV-800ME-Y2-LIC DV-800ME-Y3-LIC DV-800ME-Y4-LIC DV-800ME-Y5-LIC (Y1=365 days, Y2=730 days, Y3=1095 days, Y4=1460 days, Y5=1825 days) The above annual maintenance licenses can only be activated on the Enterprise Software edition.

Notes:

1. Licensing only allows the upgrade from Standard to Enterprise but not the other way around.
2. When the maintenance license expires (free for the 1st year of product purchase), D-View 8 will be limited to 30 nodes without an annual maintenance license; functions such as Device View, Topology Map, Batch Configuration, Firmware Management, and Configuration Management will be restricted to only 30 nodes with full functionality. Refer to 14.3 Licenses for more information.
3. If you have remote probes in D-View 7, it is strongly recommended that you upgrade the system to D-View 8 Enterprise so that remote probes can be upgraded and maintained.

1.4. 90-Day Free Trial

Network administrators need advanced tools to help maintain and manage their network systems. D-Link stays at the competitive edge of innovation and is fully committed to continuous development of cutting-edge applications to match growing demands.

Download the D-View 8 application and test it free for a total of 90 days no matter the version of edition of the application. The current version of the application is available for download at https://dview.dlink.com/. After the trial period, you will be prompted to enter your activation information. Refer to **Chapter 2 Installation** for activation options and procedure.

1.5. D-View 8 Server System Requirements

Server Requirements	
CPU	Quad-core, 3.5 GHz or above
RAM	16 GB or above
Storage	200 GB or above
Supported OS (English version only)	• Windows Server 2012 64-bit (Standard Edition or above with the latest version) • Windows Server 2012 R2 64-bit (Standard Edition or above with the latest version) • Windows Server 2016 64-bit (Standard Edition or above with the latest version) • Windows Server 2019 64-bit (Standard Edition or above with the latest version) • Windows 10 64-bit (Professional Edition or above with the latest version) • Ubuntu 18.04 64-bit or above • Debian 10 64-bit or above
Database	MongoDB 4.0 or above
Web Browser	• Microsoft Edge • Firefox • Chrome • Safari

1.6. D-View 8 Remote Probe Requirements

Remote Probe Requirements	
CPU	Dual-core, 3.0 GHz or above
RAM	4 GB or above
Storage	200 GB or above
Supported OS (English version only)	• Windows Server 2012 64-bit (Standard Edition or above with the latest version) • Windows Server 2012 R2 64-bit (Standard Edition or above with the latest version) • Windows Server 2016 64-bit (Standard Edition or above with the latest version) • Windows Server 2019 64-bit (Standard Edition or above with the latest version) • Windows 10 64-bit (Professional Edition or above with the latest version) • Ubuntu 18.04 64-bit or above • Debian 10 64-bit or above
Management Capability	500 nodes

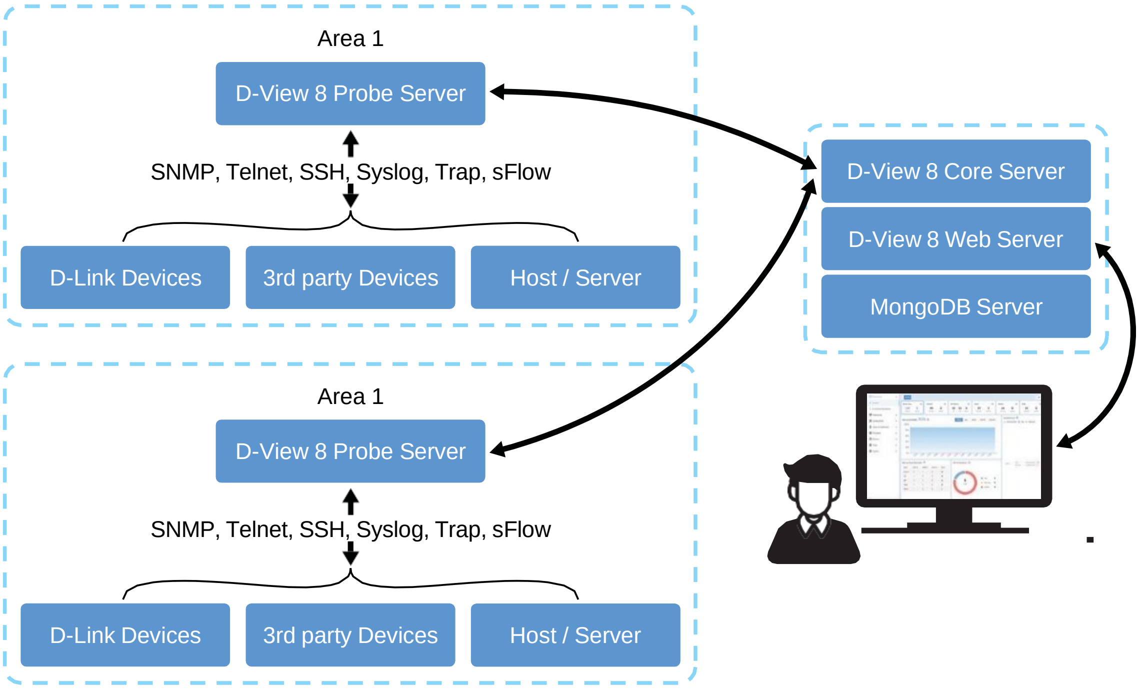
1.7. D-View 8 Client Requirements

Client System Requirements	
Web Browser	• Chrome • Firefox • Safari • Edge
CPU	Dual-core, 3.0 GHz or above
RAM	4 GB or above
Storage	100 GB or above

1.8. Network Environment Models

The application resides on the D-View 8 server with a static IP address on the local area network (LAN).

The D-View 8 application manages both D-Link and third-party devices on the network.



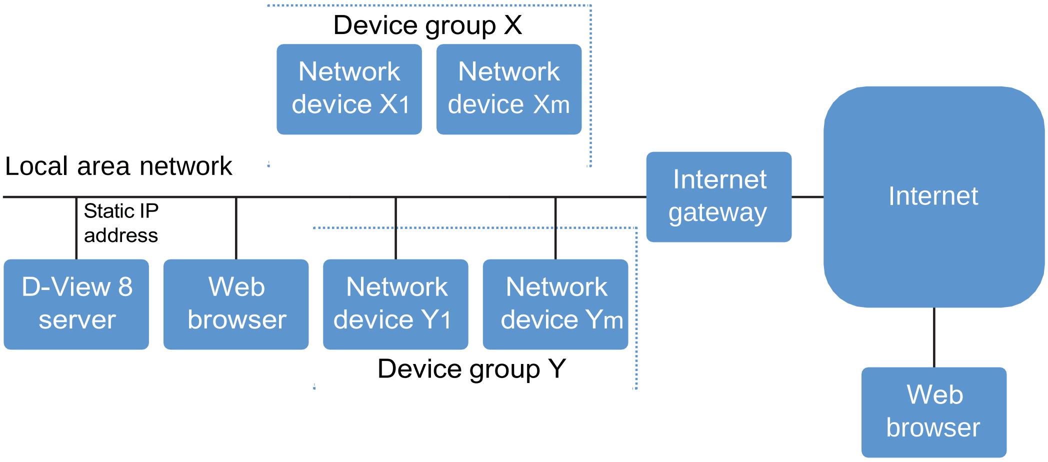
The D-View 8 application is accessed through a web browser. If the IP address cannot be accessed locally, access to the specific network must first be configured.

The application supports the following devices:

- D-Link devices support SNMP protocol. For further information about supported D-Link devices including model numbers, visit the D-View 8 website (https://dview.dlink.com/supportedModel).

1.9. Device Groups

Network management (e.g. firmware upgrade) is simplified with the use of the device group function of the D-View 8. Groups can be identified by site, network, location, device type or other device properties.



1.10. User Authentication Types

User authentication for the D-View 8 application can be accomplished in three methods. By associating an authentication profile to a user, privileges can be granted to users with restricted access to specific networks. The following are these types of authentication methods:

- Local: user account authenticated on a local system.
- RADIUS: user account authenticated by the Remote Authentication Dial-In User Service.
- Active Directory: user account authenticated by the Microsoft Management Console.

1.11. Prepare Network Devices for Discovery

Preparing a device on your network for management requires setup and configuration.

To prepare a device for network discovery:

1. Enable SNMP and configure the community’s name and associated read/write privilege.
2. Make sure that the device on the network has a valid IPv4 setting.

1.12. Start D-View 8

Please read **Chapter 2: Installation** and **Chapter 3: Overview and Basics** prior to using the D-View 8 system to understand the basic system configuration and device discovery procedure.

2 Installation

The D-View 8 software supports installation on a Linux or Windows operating system. The following sections provide guidance for software installation on both platforms.

To begin the installation process, download the D-View 8 setup application from the D-View 8 website (https://dview.dlink.com/). It provides setup assistance with wizard to guide you through the installation process.

2.1. Requirements

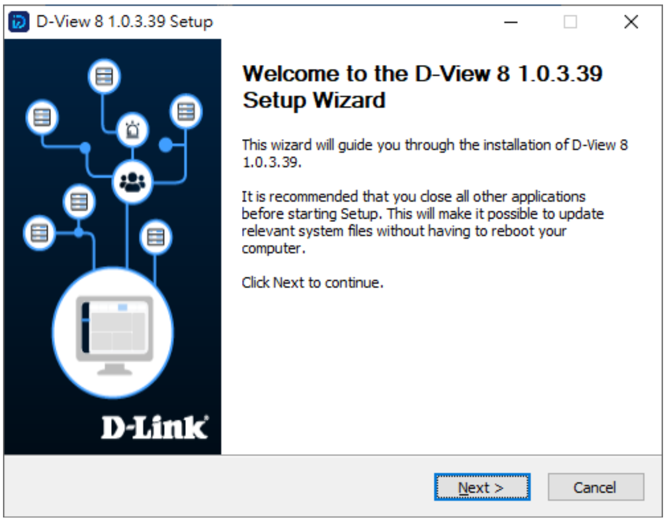
See 1.5 D-View 8 Server System Requirements for minimum hardware and software required to install and run the application on Windows and Linux.

2.2. Windows Installation

2.2.1. Standalone Edition Installation

To begin the installation process, download the software package.

1. Locate the software package and double-click it to start the installation wizard.
2. The Installation Wizard page displays. Click **Next** to continue the installation process.



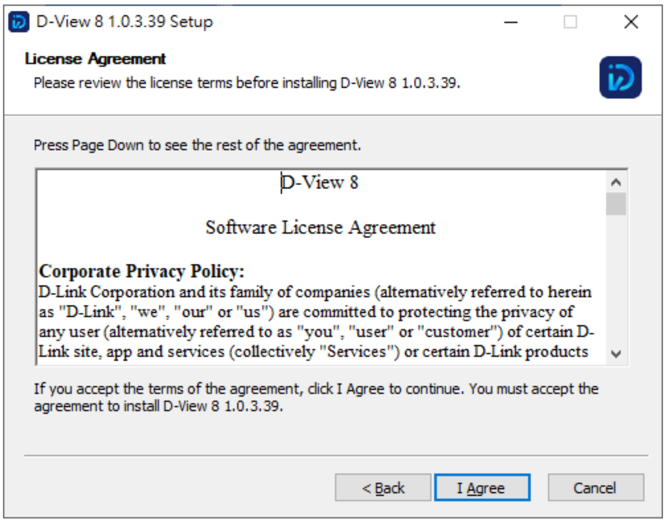
Welcome to the D-View 8 1.0.3.39 Setup Wizard

This wizard will guide you through the installation of D-View 8 1.0.3.39.

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

Click Next to continue.

3. The License Agreement page displays. Review the terms and click **I Agree** to continue. Otherwise, click **Back** or **Cancel** to restart the process.



License Agreement

Please review the license terms before installing D-View 8 1.0.3.39.

Press Page Down to see the rest of the agreement.

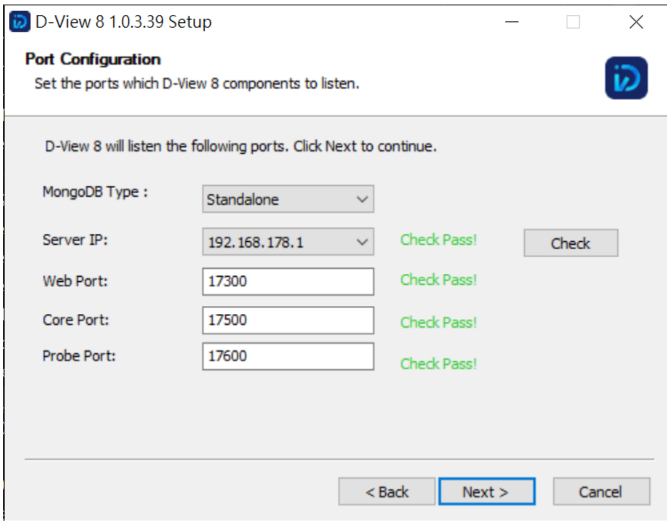
D-View 8

Software License Agreement

Corporate Privacy Policy:
D-Link Corporation and its family of companies (alternatively referred to herein as "D-Link", "we", "our" or "us") are committed to protecting the privacy of any user (alternatively referred to as "you", "user" or "customer") of certain D-Link site, app and services (collectively "Services") or certain D-Link products

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install D-View 8 1.0.3.39.

4. The Port Configuration page displays. In the **MongoDB Type** field, click the drop-down menu and select **Standalone**.
5. In the Server IP field, select the local IP address.
6. Click **Check** to test the service port availability. The green Check Pass! displays to indicate correct configuration.
7. Click **Next** to continue.



D-View 8 1.0.3.39 Setup

Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Standalone

Server IP: 192.168.178.1 Check Pass!

Web Port: 17300 Check Pass!

Core Port: 17500 Check Pass!

Probe Port: 17600 Check Pass!

D-View 8 requires a database such as MongoDB. You can select to install a new database or use an existing one as explained in the following options.

To install a new MongoDB database:

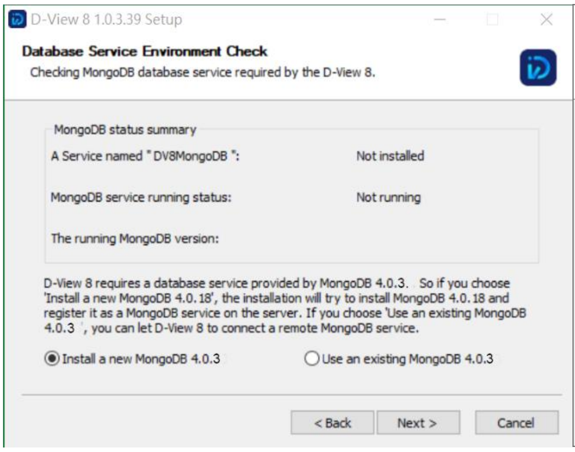
a. Select Install a new MongoDB.

b. Click **Next** to continue.

To access the database, a username and password must be assigned. In the MongoDB Port field, enter the designated port to access the database.

c. Enter the username and password for database authentication.

d. Click **Next** to continue the process.



D-View 8 1.0.3.39 Setup

Database Service Environment Check

Checking MongoDB database service required by the D-View 8.

MongoDB status summary

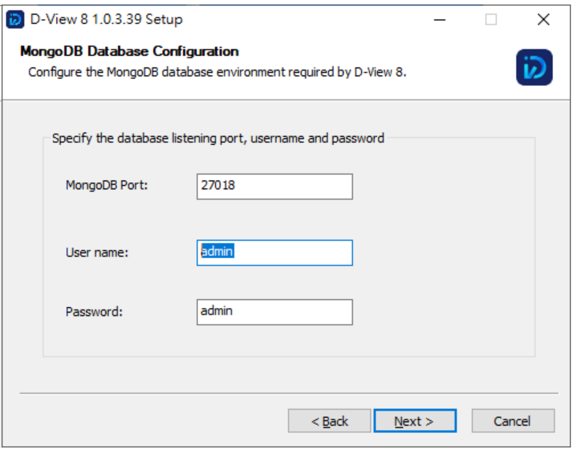
A Service named " DV8MongoDB ": Not installed

MongoDB service running status: Not running

The running MongoDB version:

D-View 8 requires a database service provided by MongoDB 4.0.3.   So if you choose 'Install a new MongoDB 4.0.18', the installation will try to install MongoDB 4.0.18 and register it as a MongoDB service on the server. If you choose 'Use an existing MongoDB 4.0.3 ', you can let D-View 8 to connect a remote MongoDB service.

● Install a new MongoDB 4.0.3 ○ Use an existing MongoDB 4.0.3



D-View 8 1.0.3.39 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

Specify the database listening port, username and password

MongoDB Port: 27018

User name: admin

Password: admin

To use an existing MongoDB database:

a. Select **Use an existing MongoDB**.

b. Click **Next** to continue.

Then provide the required settings to access the existing database.

c. In the MongoDB Address field, enter the IP address and port of the database.

d. Select Password Authentication if the database requires a username and password to access.

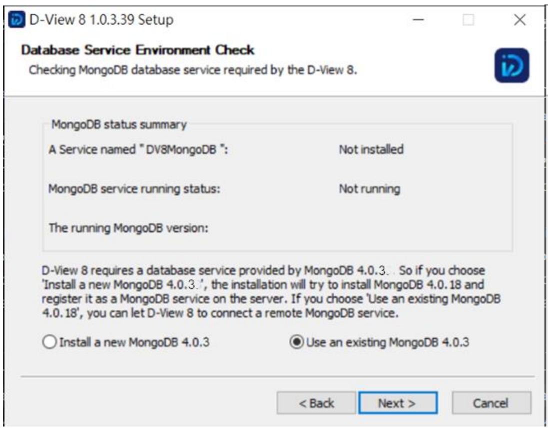
e. Enter the username and password of an account with authority to access the database.

f. Click **Check Connection** to test the settings.

If the settings are configured properly, the **Next** button is enabled.

If the connection fails, check the settings and enter the related information again.

g. Click **Next** to continue the process.



D-View 8 1.0.3.39 Setup

Database Service Environment Check

Checking MongoDB database service required by the D-View 8.

MongoDB status summary

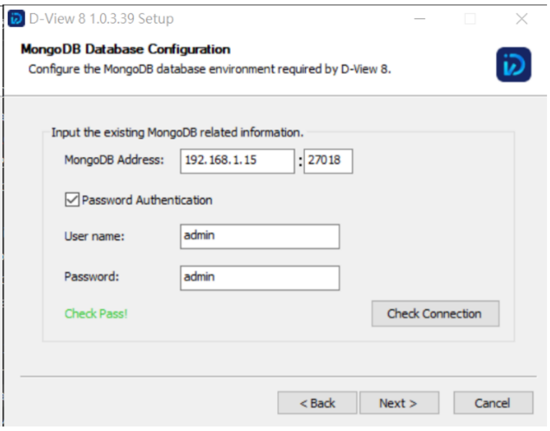
A Service named " DV8MongoDB ": Not installed

MongoDB service running status: Not running

The running MongoDB version:

D-View 8 requires a database service provided by MongoDB 4.0.3. So if you choose 'Install a new MongoDB 4.0.3', the installation will try to install MongoDB 4.0.18 and register it as a MongoDB service on the server. If you choose 'Use an existing MongoDB 4.0.18', you can let D-View 8 to connect a remote MongoDB service.

○ Install a new MongoDB 4.0.3 ● Use an existing MongoDB 4.0.3



D-View 8 1.0.3.39 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

Input the existing MongoDB related information.

MongoDB Address: 192.168.1.15 : 27018

☑ Password Authentication

User name: admin

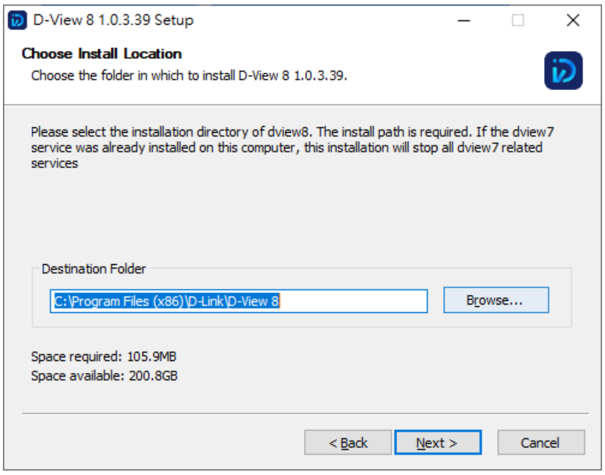
Password: admin

Check Pass!

The Choose Install Location page displays.

8. In the Destination Folder field, click **Browse** to select the destination folder, then click **Next** to continue.

9. Click **Install** to continue or **Back** to return to the previous page or **Cancel** to restart the process.



D-View 8 1.0.3.39 Setup

Choose Install Location

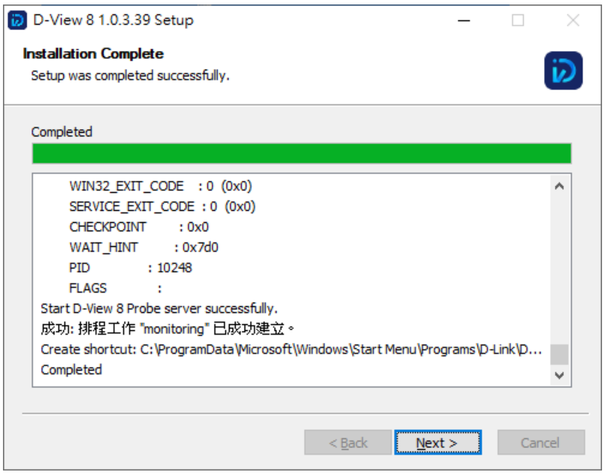
Choose the folder in which to install D-View 8 1.0.3.39.

Please select the installation directory of dview8. The install path is required. If the dview7 service was already installed on this computer, this installation will stop all dview7 related services

Destination Folder

C:\Program Files (x86)\D-Link\D-View 8

Space required: 105.9MB
Space available: 200.8GB



D-View 8 1.0.3.39 Setup

Installation Complete

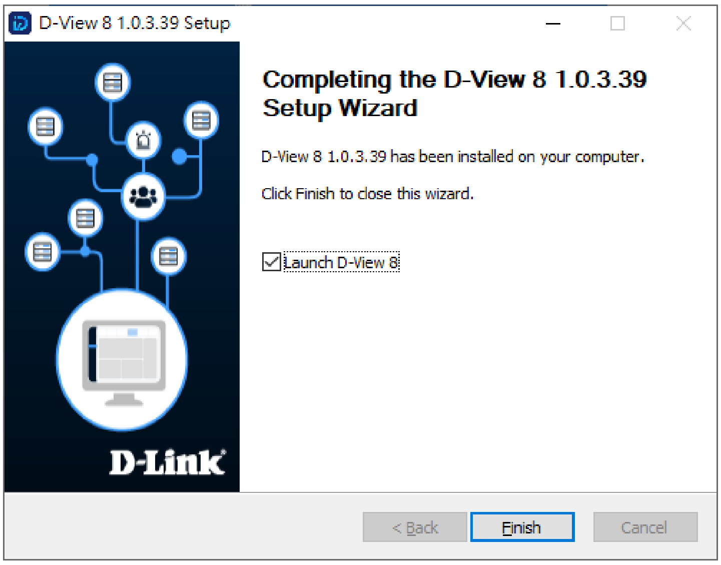
Setup was completed successfully.

Completed

```
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 10248
        FLAGS              :
Start D-View 8 Probe server successfully.
成功: 排程工作 "monitoring" 已成功建立。
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\D-Link\D...
Completed
```

Once the installation process is completed, the Setup Wizard page displays.

10. Select Launch D-View 8 and click **Finish** to open the application interface using the default browser.



D-View 8 1.0.3.39 Setup

Completing the D-View 8 1.0.3.39 Setup Wizard

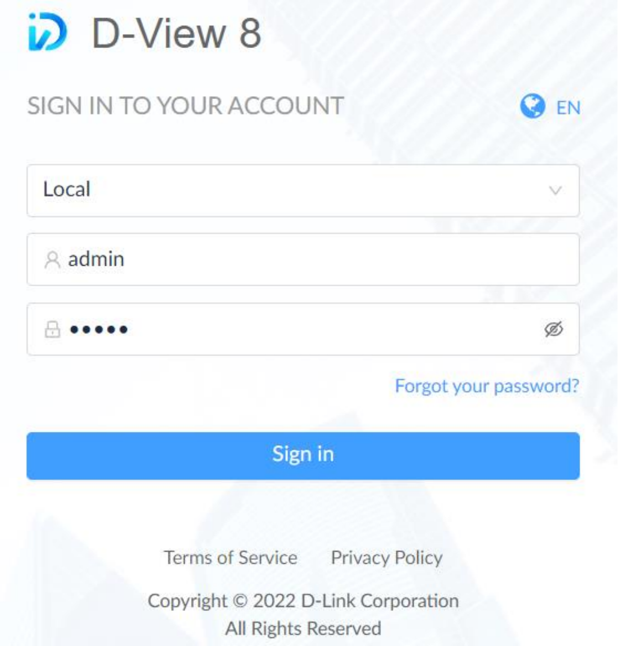
D-View 8 1.0.3.39 has been installed on your computer.

Click Finish to close this wizard.

☑ Launch D-View 8

If this is the first time that you open the application, more login details will be presented. You can opt to enter an activation code or use a trial account.

11. In the username and password fields, enter the following default values: admin (username), admin (password).



D-View 8

SIGN IN TO YOUR ACCOUNT

Local

admin

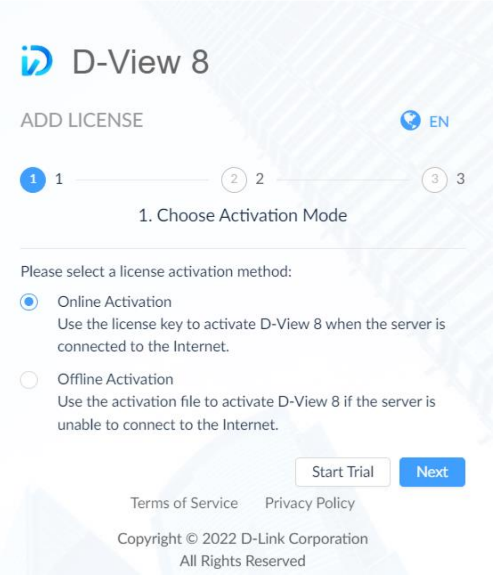
•••••

The Add License page displays. From this screen, you can set a preferred language (default: English).

For Activation, select a license type to activate, or click **Start Trial** to activate a trial license.

- Online Activation: enter the license key as provided to activate the application software. The server must be connected to the Internet for this function to authorize a license.
- Offline Activation: locate the activation file as provided to activate the application software. The function is available when the server is not connected to the Internet.
- Start Trial: try the application for 90 days. You can download the trial from the D-View 8 website (https://dview.dlink.com/.)

12. Click **Next** to continue.



D-View 8

ADD LICENSE

1. Choose Activation Mode

Please select a license activation method:

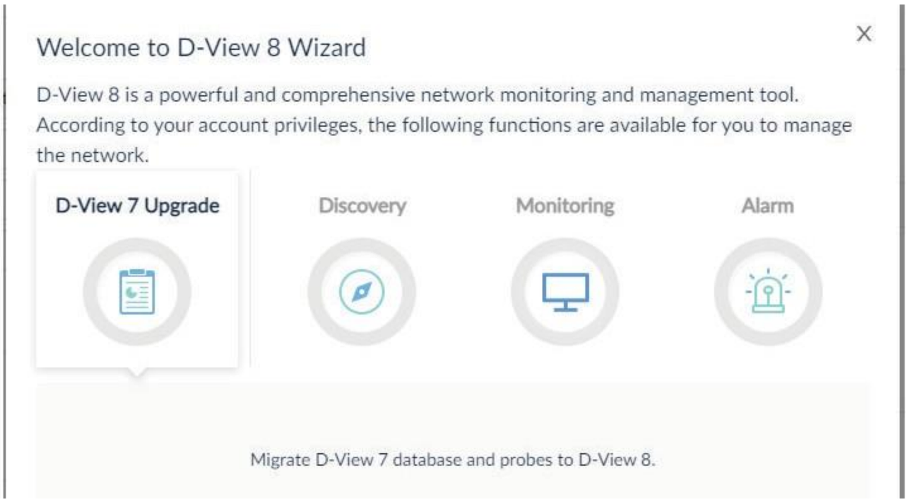
● Online Activation
Use the license key to activate D-View 8 when the server is connected to the Internet.

○ Offline Activation
Use the activation file to activate D-View 8 if the server is unable to connect to the Internet.

Copyright © 2022 D-Link Corporation
All Rights Reserved

The D-View 8 Wizard page displays. The available configuration options are based on the account privilege:

- D-View 7 Upgrade: Migrate the D-View 7 database and probes to the current application.
- Discovery: Discover available networks and connected devices.
- Monitoring: Create topologies, rack simulations, and dashboard to help monitor the network.
- Alarm: Configure notifications and alarms.



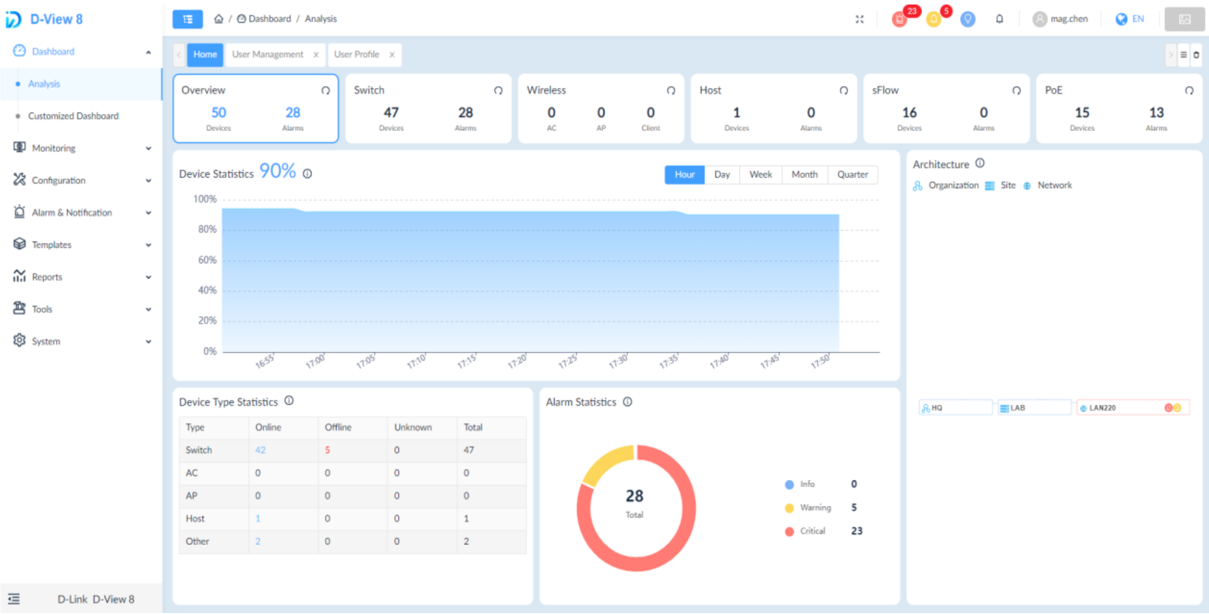
Welcome to D-View 8 Wizard

D-View 8 is a powerful and comprehensive network monitoring and management tool. According to your account privileges, the following functions are available for you to manage the network.

Migrate D-View 7 database and probes to D-View 8.

NOTE: Please follow the wizard’s guidance to set up an organization first. It is required for the subsequent Network Discovery to perform properly.

Once the installation is complete, the user Dashboard displays.



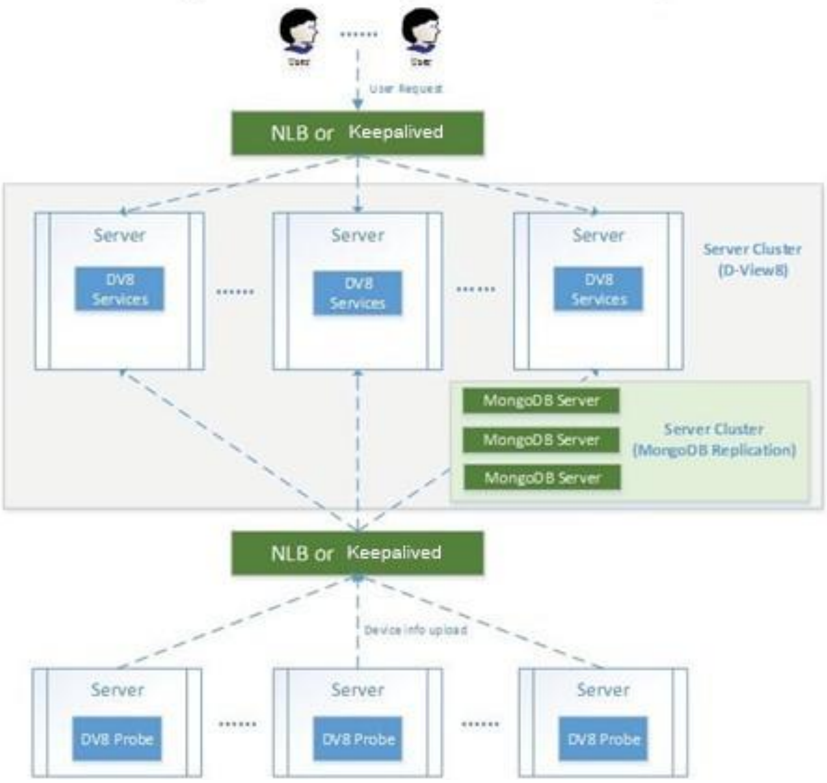
Device Type Statistics

Type	Online	Offline	Unknown	Total
Switch	42	5	0	47
AC	0	0	0	0
AP	0	0	0	0
Host	1	0	0	1
Other	2	0	0	2

2.2.2. Cluster Mode Installation (Only Available for Enterprise Edition)

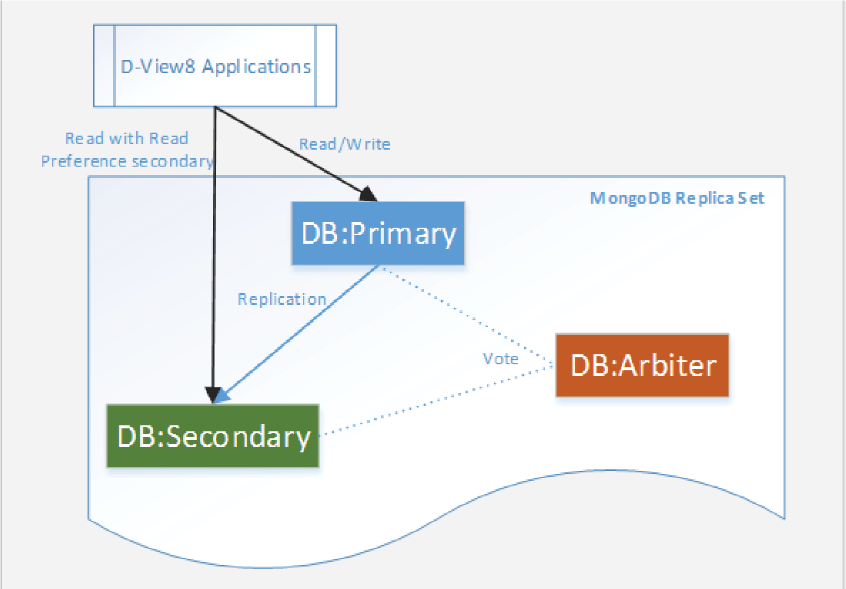
Cluster Architecture

The D-View 8 supports data redundancy and load balancing features. The following diagram depicts the cluster architecture.



The following shows the structure of D-View 8 application and MongoDB. The structure includes a primary, secondary, and an arbiter database. The application connects to both the primary and secondary database.

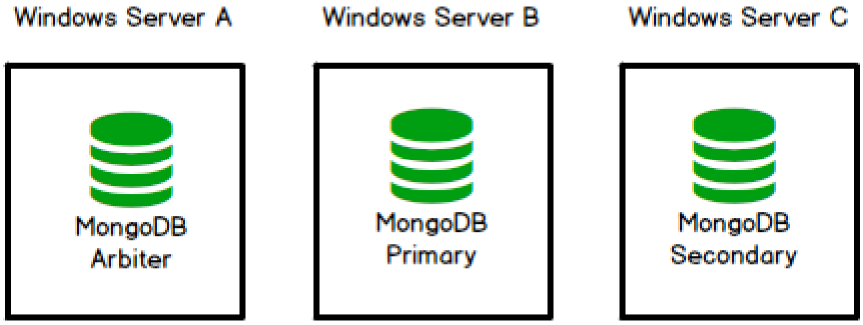
A primary database may be reassigned as the secondary while the secondary may also become the primary. By default, clients read from the primary database, but a read preference can be configured to allow read operations on the secondary database.



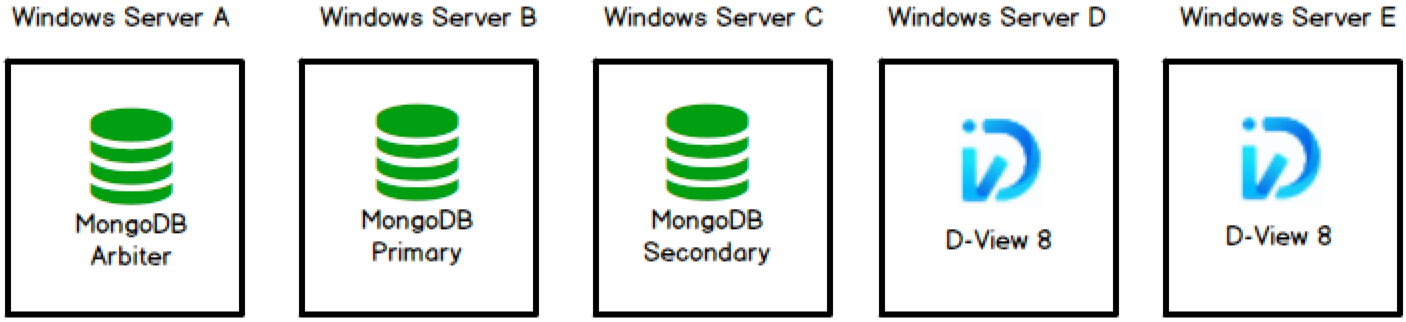
Building a Cluster

Clusters help support data redundancy and load balancing. Building clusters is outlined in this section.

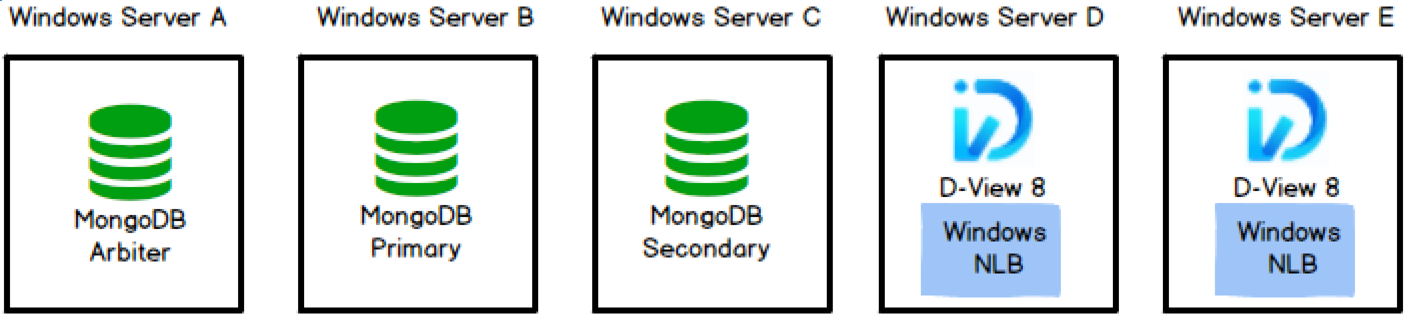
First, Install MongoDB on 3 Windows servers with the designated roles to support the above mentioned structure.



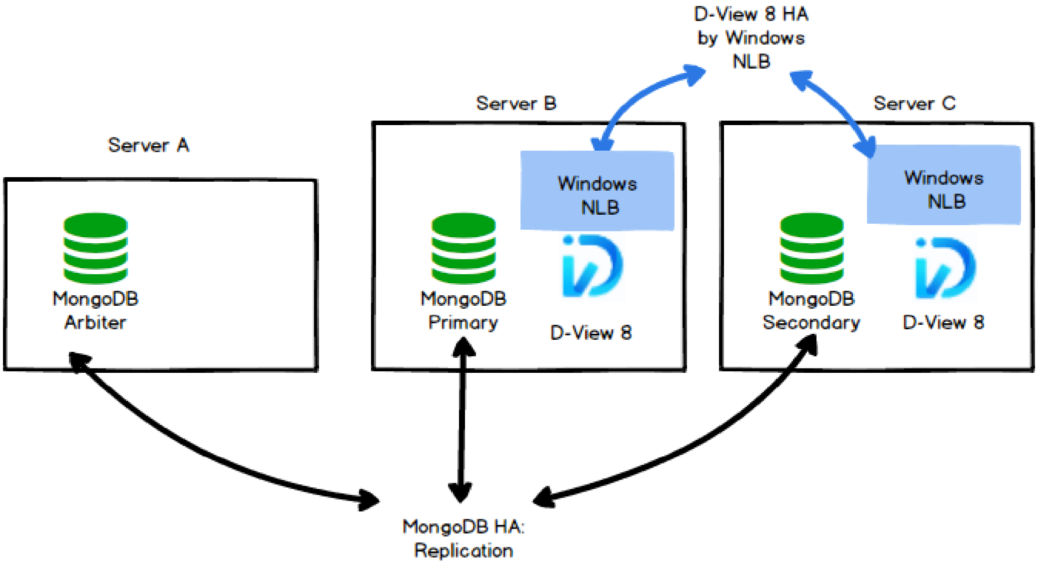
Deploy D-View 8 on additional servers and connect the D-View 8 application to the MongoDB cluster.



Then, enable NLB on Windows to support server load balancing:

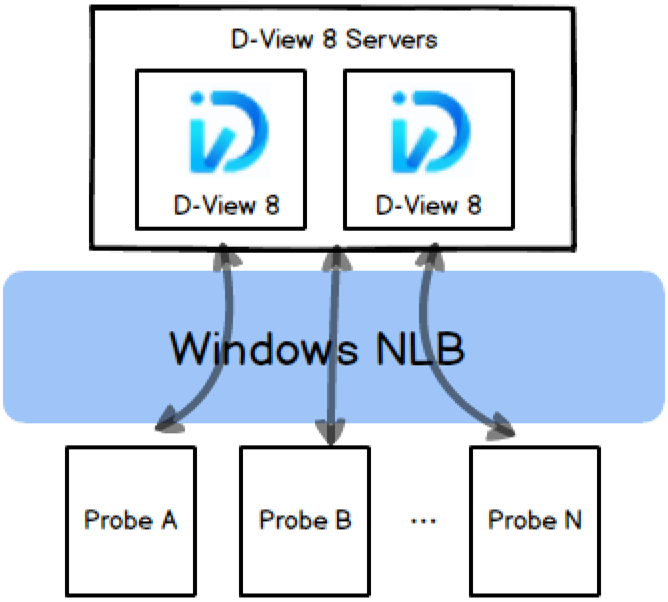


NOTE: You may opt to install D-View 8 on the primary and secondary database in lieu of additional servers. The following diagram depicts this three-server deployment topology:



To manage additional devices through Windows servers, you need to add probes in these servers to enable the connection to the D-View 8 servers with load-balancing managed by NLB.

s



NOTE: The following example demonstrates the deployment of three-server topology; for deployment example of five-server topology, refer to **Appendix A: Deployment with Five-server Topology**.

Preparation for Three-server Deployment

When planning for server cluster deployment, you must first set up 3 Windows servers with the following system configuration:

- SERVER A

  OS: Windows 10, Windows Server 2016/ Windows Server 2019

  MongoDB

  IP Address: 192.168.1.203

  Replica set role: arbiter

- SERVER B

  OS: Windows Server 2016/ Windows Server 2019

  MongoDB

  IP Address: 192.168.1.201

  Replica set Role: primary

  NLB enabled with virtual IP: 192.168.1.200

- SERVER C

  OS: Windows Server 2016/ Windows Server 2019

  MongoDB

  IP Address: 192.168.1.202

  Replica set Role: secondary

  NLB enabled with virtual IP: 192.168.1.200

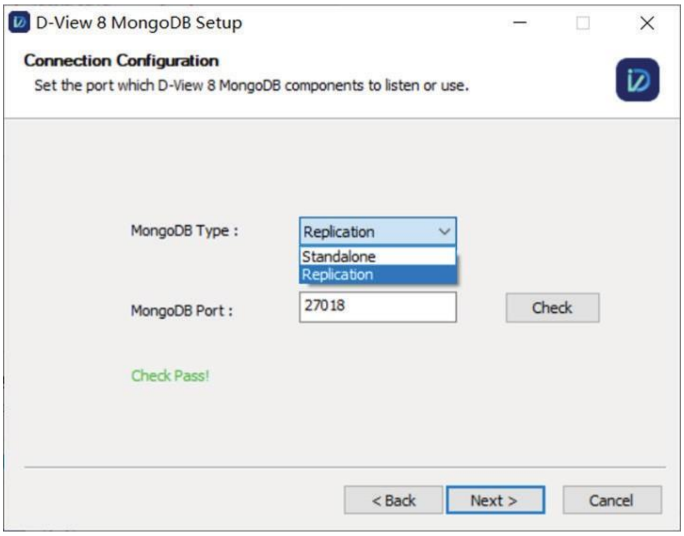
Data Redundancy Support on the MongoDB Server Cluster

This section details the steps to install the required MongoDB database and enable data redundancy in the database cluster.

MongoDB Cluster Installation

To install MongoDB in the database cluster:

1. Download the D-View 8 MongoDB installation package (e.g. D-View 8 MongoDB_2.0.0.26_Installation.exe) from the D-View 8 website.
2. Install the package on server, A, B, and C.
3. On the Connection Configuration page, select **Replication** in the MongoDB Type drop-down menu.
4. Enter the MongoDB port number for server communication.



D-View 8 MongoDB Setup

Connection Configuration

Set the port which D-View 8 MongoDB components to listen or use.

MongoDB Type : Replication

MongoDB Port : 27018

Check Pass!

5. Click **Check** to test the setting. If it is configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port setting and try again.
6. Click **Next** to continue and the installation should start.

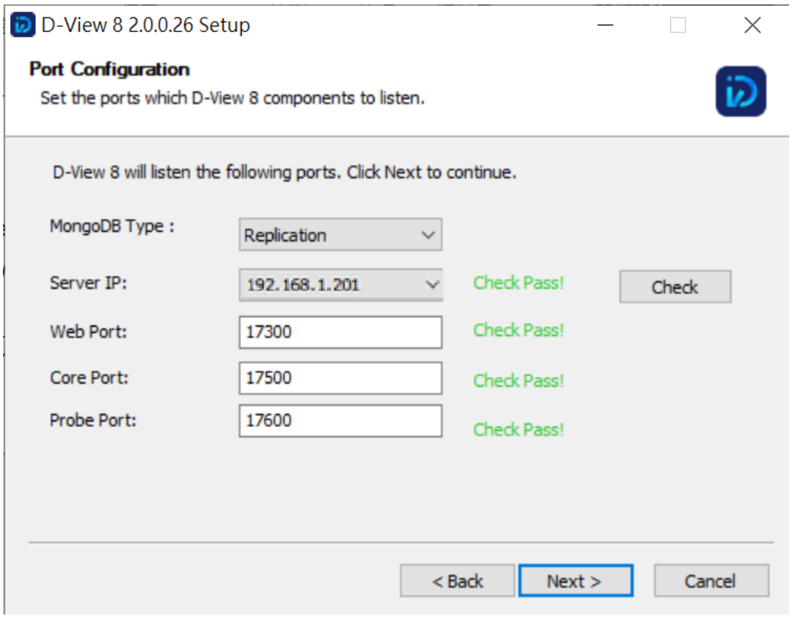
D-View 8 Installation

D-View 8 can be deployed in three-server or five-server topology as illustrated above.

Use the following procedure to install D-View 8 on multiple servers (e.g. server B & C) and connect them to the MongoDB cluster.

Installation on server B:

1. Download the D-View 8 Installation package (e.g. D-View 8_1.0.0.70_Installation.exe) from the D-View 8 website.
2. Install the package.
3. In the Port Configuration page, select **Replication** in the MongoDB Type menu.
4. In the Server IP field, enter the host server's IP address. As for our example, 192.168.1.201.
5. For port settings, enter the port number required for web access, core communication, and probe communication: 17300, 17500, and 17600.



D-View 8 2.0.0.26 Setup

Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Replication

Server IP: 192.168.1.201 Check Pass!

Web Port: 17300 Check Pass!

Core Port: 17500 Check Pass!

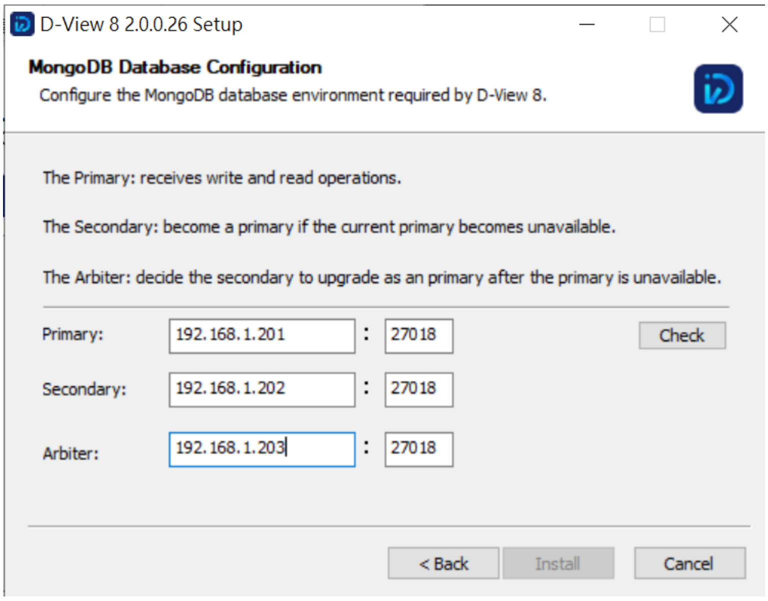
Probe Port: 17600 Check Pass!

6. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails,

verify the port settings and try again.

7. Click **Next** to continue.

8. The MongoDB Database Configuration page displays. Enter the IP address and port number for the primary, secondary and arbiter database.



D-View 8 2.0.0.26 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

The Primary: receives write and read operations.

The Secondary: become a primary if the current primary becomes unavailable.

The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.

Primary: 192.168.1.201 : 27018

Secondary: 192.168.1.202 : 27018

Arbiter: 192.168.1.203 : 27018

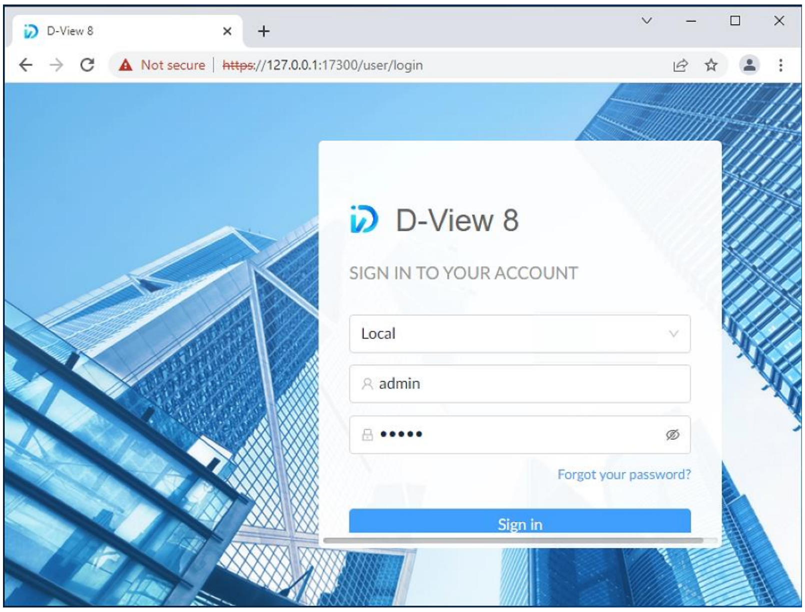
9. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails,

verify the settings and try again.

10. Click **Install** to continue.

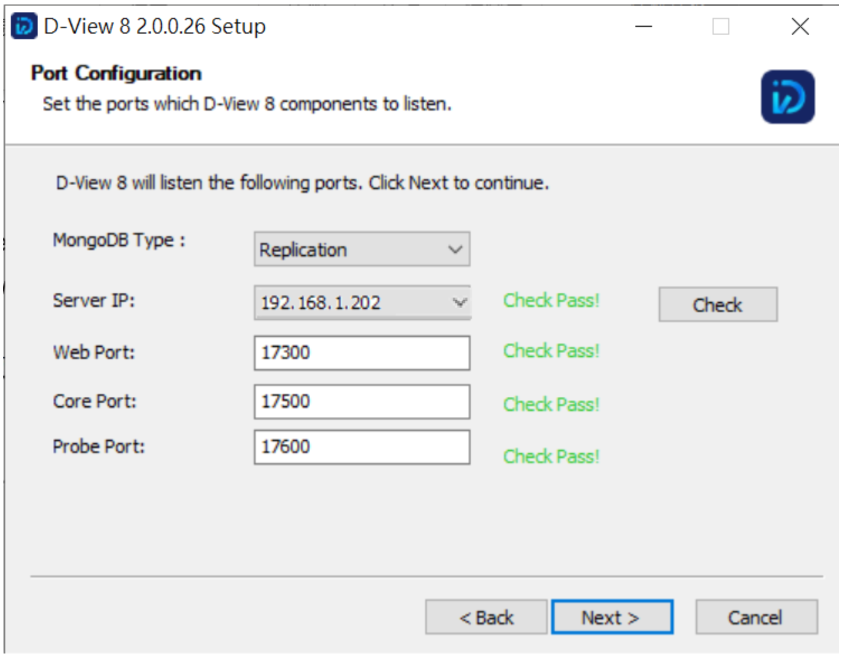
11. Once the installation completes, click **Finish** to close the Setup Wizard.

12. The D-View 8 Server can be accessed using a web browser on the server.



Installation on server C:

1. Download the D-View 8 Installation package (e.g. D-View 8_1.0.0.70_Installation.exe).
2. Install the package.
3. In the Port Configuration page, select **Replication** in the MongoDB Type menu.
4. In the Server IP field, enter the host server's IP address. As for our example, 192.168.1.202.
5. For port settings, enter the port number required for web access, core communication, and probe communication: 17300, 17500, and 17600.



D-View 8 2.0.0.26 Setup

Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Replication

Server IP: 192.168.1.202 Check Pass!

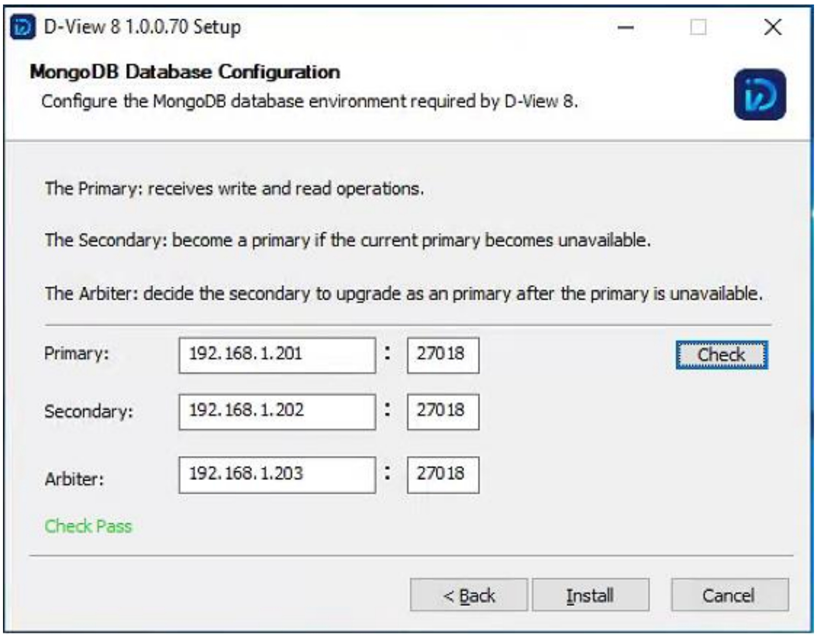
Web Port: 17300 Check Pass!

Core Port: 17500 Check Pass!

Probe Port: 17600 Check Pass!

6. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails,

   verify the port settings and try again.
7. Click **Next** to continue.
8. The MongoDB Database Configuration page displays. Enter the IP address and port number for the primary, secondary and arbiter database.



D-View 8 1.0.0.70 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

The Primary: receives write and read operations.

The Secondary: become a primary if the current primary becomes unavailable.

The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.

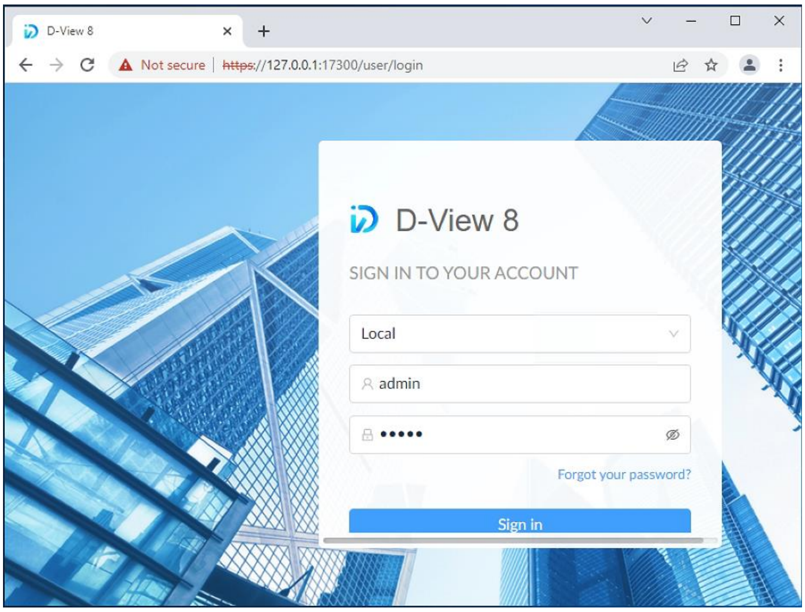
Primary: 192.168.1.201 : 27018

Secondary: 192.168.1.202 : 27018

Arbiter: 192.168.1.203 : 27018

Check Pass

9. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the settings and try again.
10. Click **Install** to continue.
11. Once the installation completes, click **Finish** to close the Setup Wizard.
12. The D-View 8 Server can be accessed using a web browser on the server.



D-View 8

Not secure | https://127.0.0.1:17300/user/login

D-View 8

SIGN IN TO YOUR ACCOUNT

Local

admin

•••••

Forgot your password?

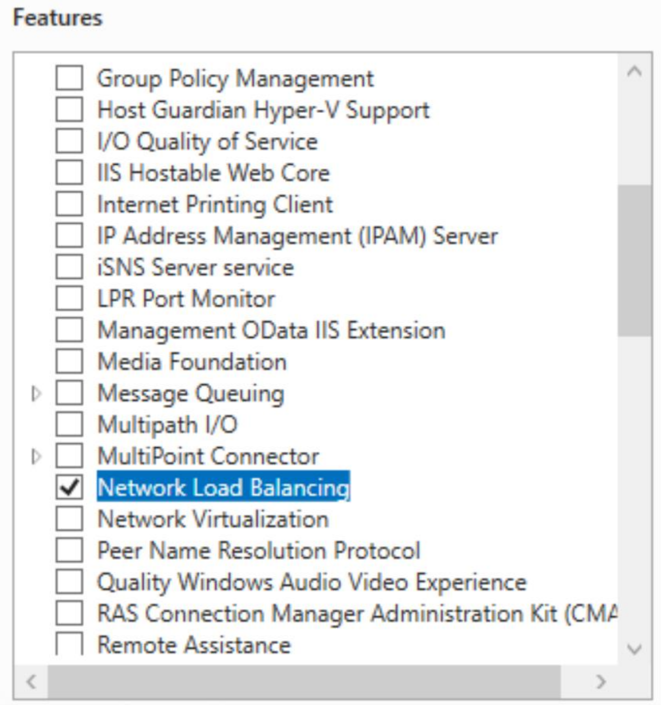
Sign in

Network Load Balancing Setup on D-View 8 Servers

Server load balancing is supported on D-View 8. At least two Windows servers on the same subnet will be required to configure load balancing. For our deployment demonstration of three-server topology, use the following procedure to set up NLB on D-View 8 servers.

To set up NLB on server B & C:

1. Install the Network Load Balancing service on both server B & C.



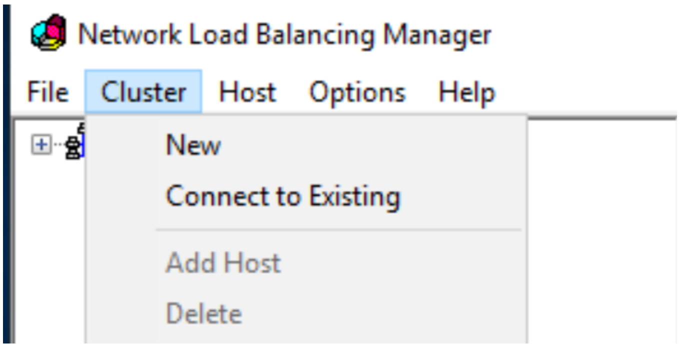
Features

- □ Group Policy Management
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor
- □ Management OData IIS Extension
- □ Media Foundation
- □ Message Queuing
- □ Multipath I/O
- □ MultiPoint Connector
- ☑ Network Load Balancing
- □ Network Virtualization
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ RAS Connection Manager Administration Kit (CMA
- □ Remote Assistance

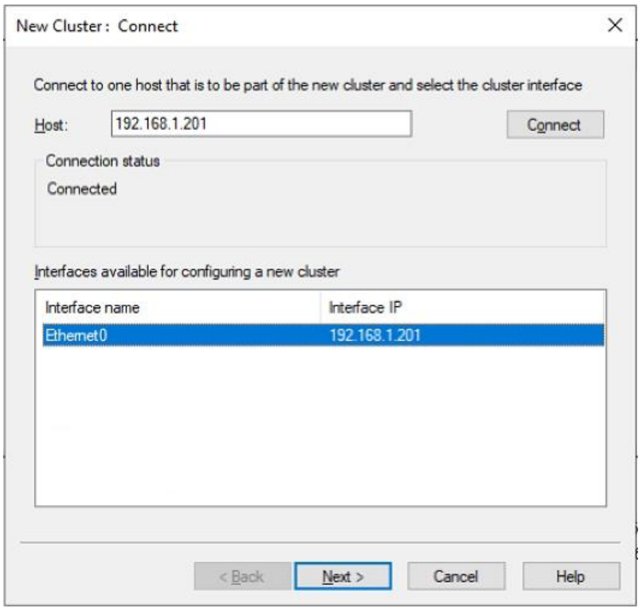
2. Start Network Load Balancing Manager on both servers. Then use the following procedure to configure them individually.

Configuration on server B

1. In NLB Manager, click **Cluster > New** to create a new cluster.



2. In the Host field, enter the IP address of server B: 192.168.1.201 and click the **Connect** button.



Connect to one host that is to be part of the new cluster and select the cluster interface

Host: 192.168.1.201

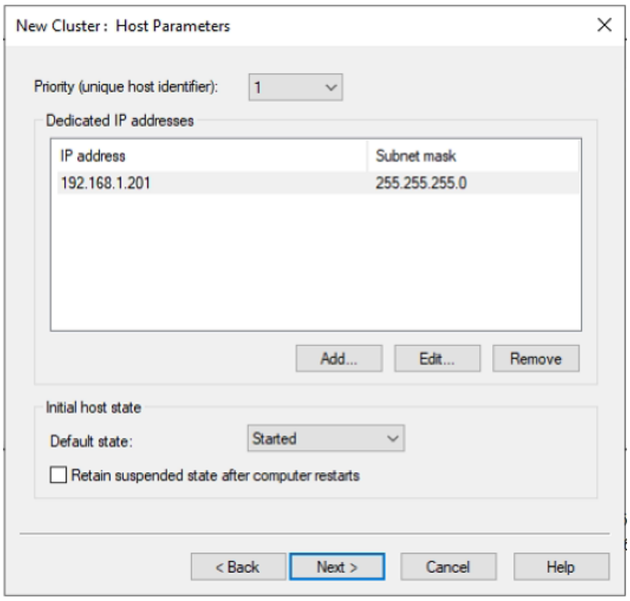
Connection status

Connected

Interfaces available for configuring a new cluster

Interface name	Interface IP
Ethernet0	192.168.1.201

3. Click **Next** to continue. The New Cluster: Host Parameters page displays.



Priority (unique host identifier): 1

Dedicated IP addresses

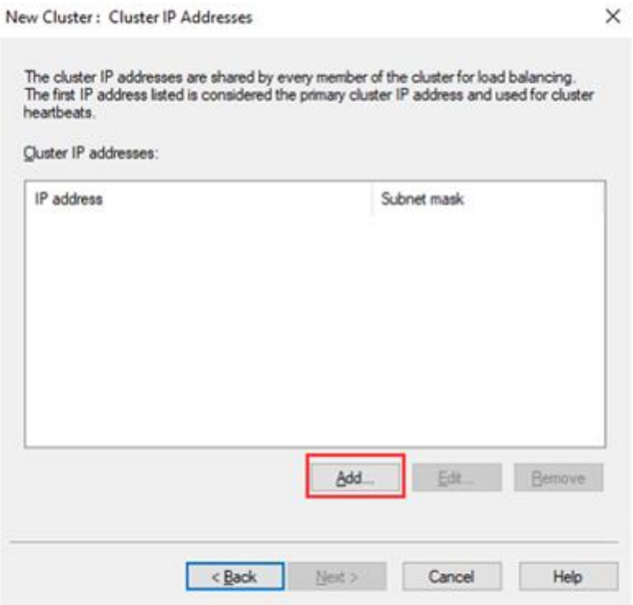
IP address	Subnet mask
192.168.1.201	255.255.255.0

Initial host state

Default state: Started

☐ Retain suspended state after computer restarts

4. Click **Next** to continue. The New Cluster: Cluster IP Addresses page displays.



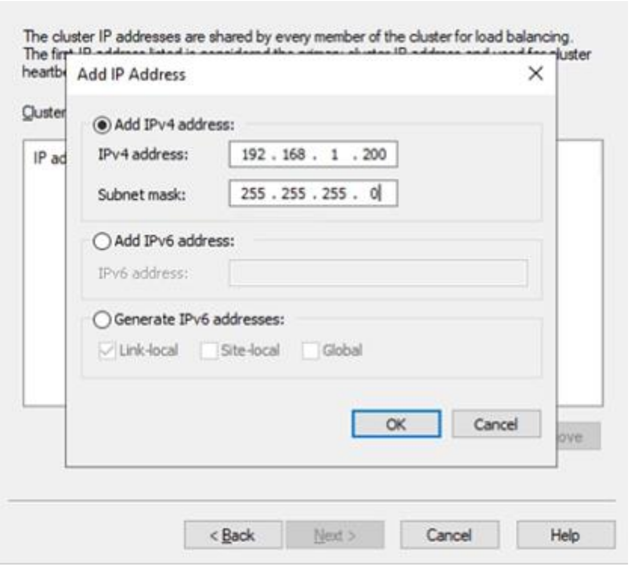
New Cluster : Cluster IP Addresses

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask

5. Click **Add** to enter a Virtual IP address and subnet mask that will be used as the cluster IP and netmask. Click **OK** to continue.



Add IP Address

● Add IPv4 address:

IPv4 address: 192 . 168 . 1 . 200

Subnet mask: 255 . 255 . 255 . 0

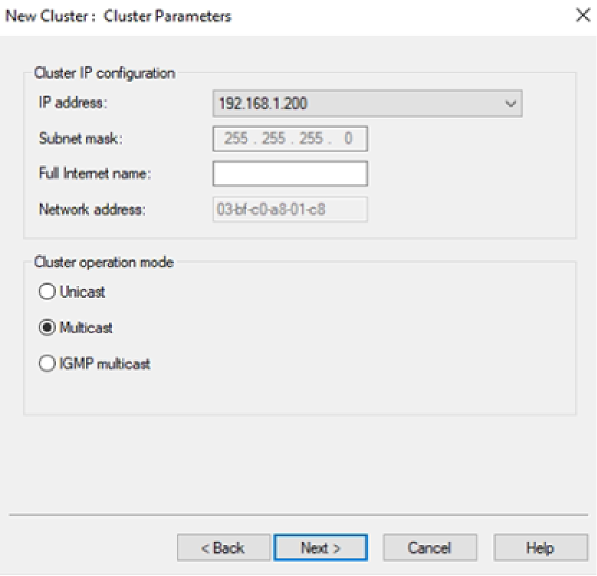
○ Add IPv6 address:

IPv6 address:

○ Generate IPv6 addresses:

☑ Link-local □ Site-local □ Global

6. Select **Multicast** for **Cluster Operation Mode** for optimal performance.



New Cluster : Cluster Parameters

Cluster IP configuration

IP address: 192.168.1.200

Subnet mask: 255 . 255 . 255 . 0

Full Internet name:

Network address: 03-bf-c0-a8-01-c8

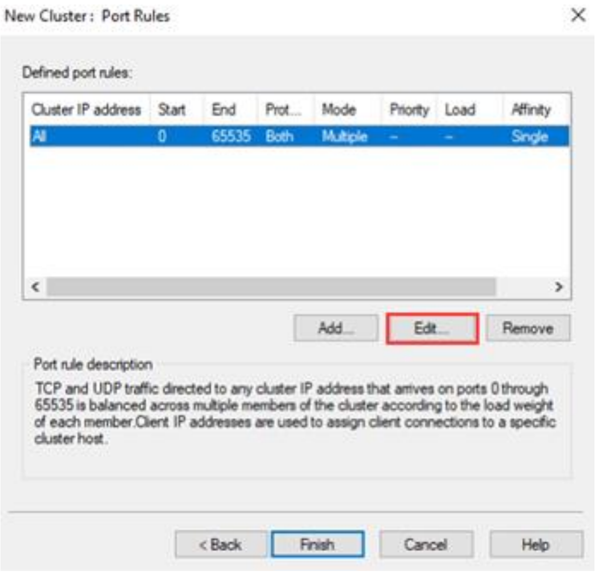
Cluster operation mode

○ Unicast

● Multicast

○ IGMP multicast

7. Click **Next** to continue to configure the port rules. The Port Rules page displays.



New Cluster : Port Rules

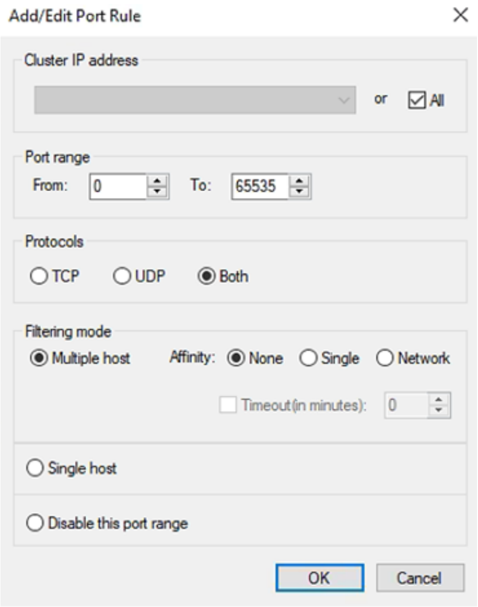
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	0	65535	Both	Multiple	-	-	Single

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced across multiple members of the cluster according to the load weight of each member.Client IP addresses are used to assign client connections to a specific cluster host.

8. Select the defined port rule and click **Edit**. The Add/Edit Port Rule page displays.



Add/Edit Port Rule

Cluster IP address

or ☑ All

Port range

From: 0 To: 65535

Protocols

○ TCP ○ UDP ● Both

Filtering mode

● Multiple host Affinity: ● None ○ Single ○ Network

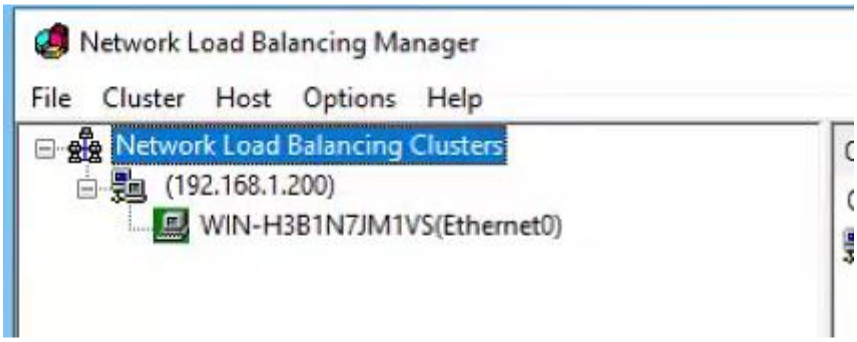
□ Timeout(in minutes): 0

○ Single host

○ Disable this port range

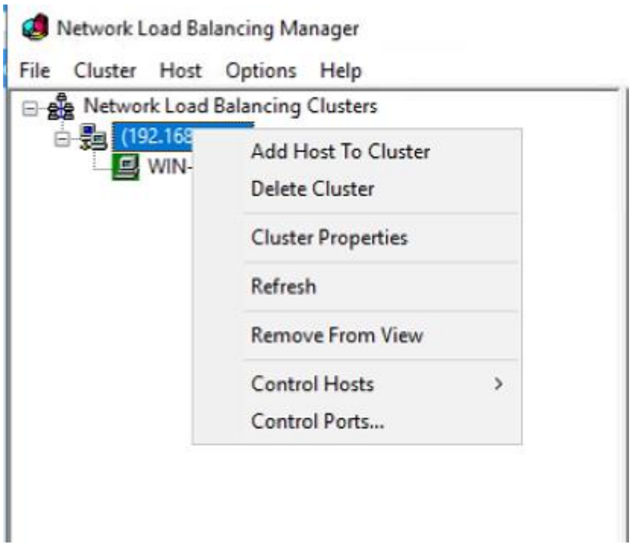
9. In the Filtering mode section, Select **Multiple host** for **Filtering mode** and **None** for **Affinity**. Click **OK** to continue.

10. An NLB cluster will be created as shown below.

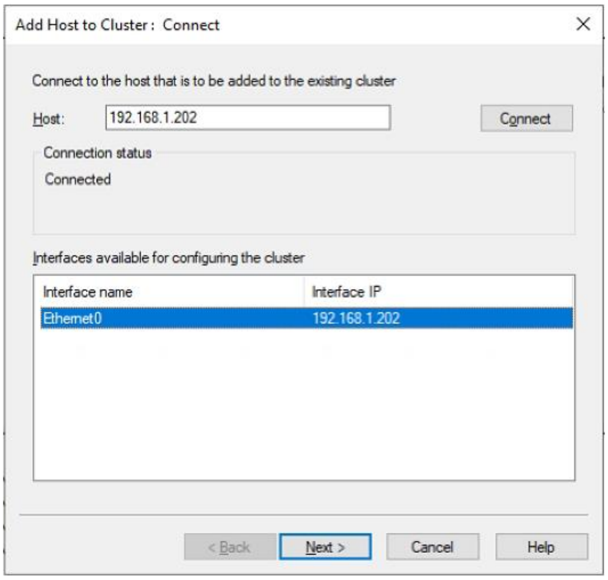


Network Load Balancing Manager
File
Cluster
Host
Options
Help
Network Load Balancing Clusters
(192.168.1.200)
WIN-H3B1N7JM1VS(Ethernet0)

11. Right click on the cluster node and click **Add Host To Cluster.**



12. Click **Next** to continue.
13. In the Host field, enter the server node 2's IP address.
14. Click **Connect** to establish the connection to the node. The interface will then appear in the Interface pane.



Add Host to Cluster : Connect

Connect to the host that is to be added to the existing cluster

Host: 192.168.1.202

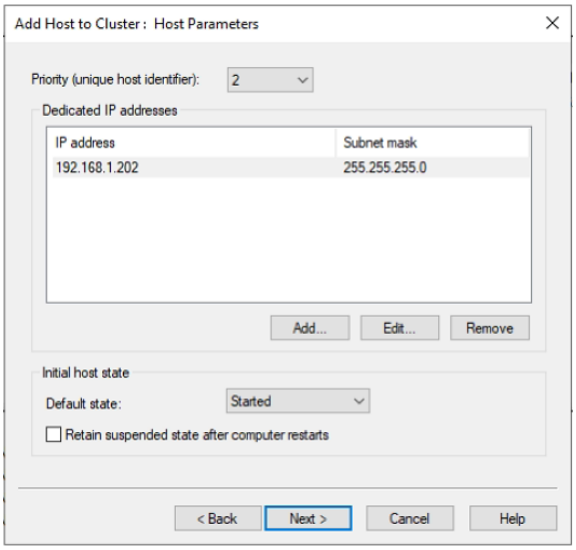
Connection status

Connected

Interfaces available for configuring the cluster

Interface name	Interface IP
Ethernet0	192.168.1.202

15. Click **Next** to continue.



Add Host to Cluster : Host Parameters

Priority (unique host identifier): 2

Dedicated IP addresses

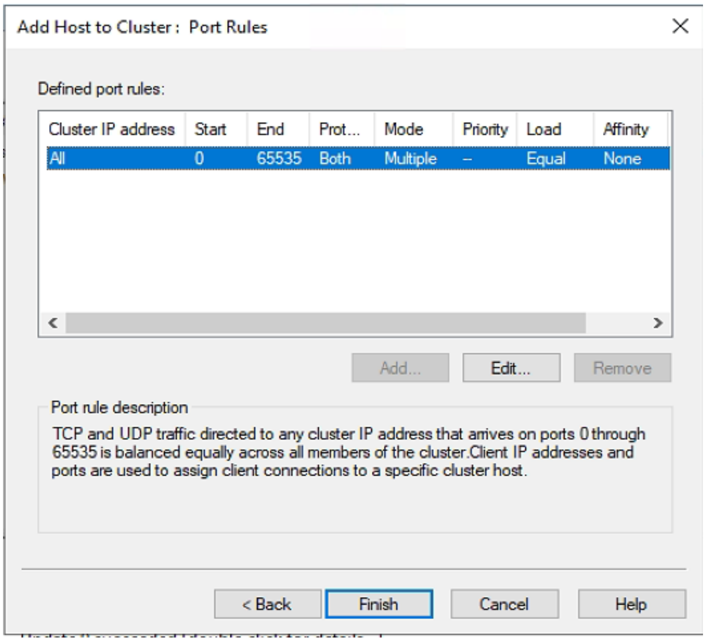
IP address	Subnet mask
192.168.1.202	255.255.255.0

Initial host state

Default state: Started

□ Retain suspended state after computer restarts

16. Click **Finish** to close the screen.



Add Host to Cluster : Port Rules

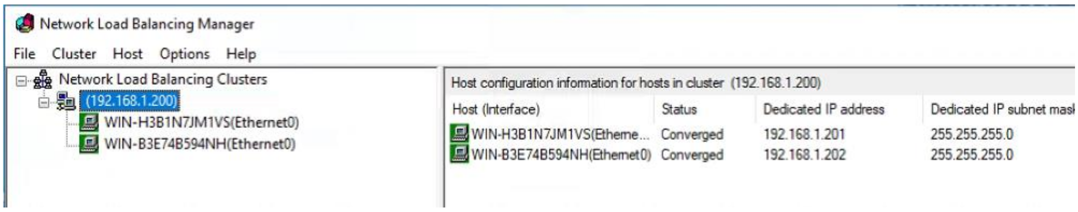
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	0	65535	Both	Multiple	–	Equal	None

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced equally across all members of the cluster.Client IP addresses and ports are used to assign client connections to a specific cluster host.

17. Open the Network Load Balancing Manager. Now a cluster containing both server B and C was created.

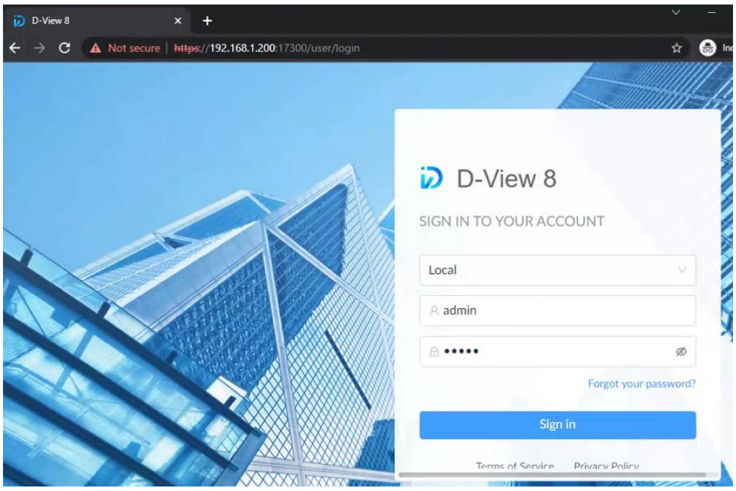


Network Load Balancing Manager
File
Cluster
Host
Options
Help
Network Load Balancing Clusters
(192.168.1.200)
WIN-H3B1N7JM1VS(Ethernet0)
WIN-B3E74B594NH(Ethernet0)

Host configuration information for hosts in cluster (192.168.1.200)

Host (Interface)	Status	Dedicated IP address	Dedicated IP subnet mask
WIN-H3B1N7JM1VS(Etherne...	Converged	192.168.1.201	255.255.255.0
WIN-B3E74B594NH(Ethernet0)	Converged	192.168.1.202	255.255.255.0

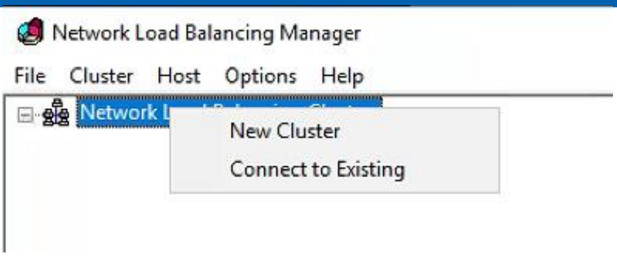
18. And the D-View 8 can be accessed with the Virtual IP.



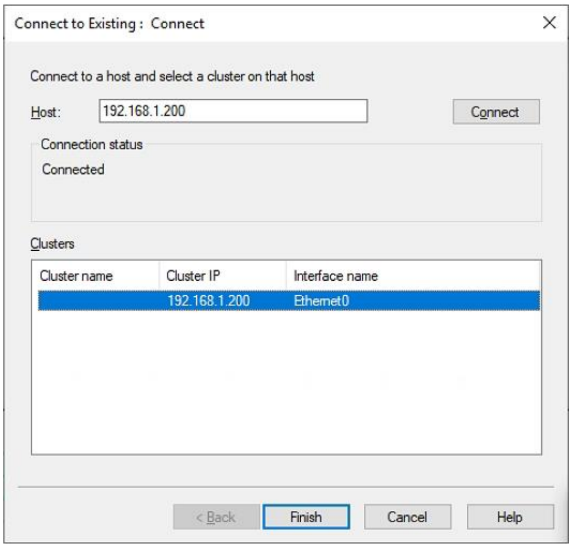
Configuration on Server C

You can also manage the NLB cluster on the other server (C) by configuring NLB with the Network Load Balancing Manager.

1. Go to **Cluster > Connect to Existing**.



2. Enter the NLB cluster IP: 192.168.1.200 and click **Connect**.


Connect to Existing : Connect

Connect to a host and select a cluster on that host

Host: 192.168.1.200

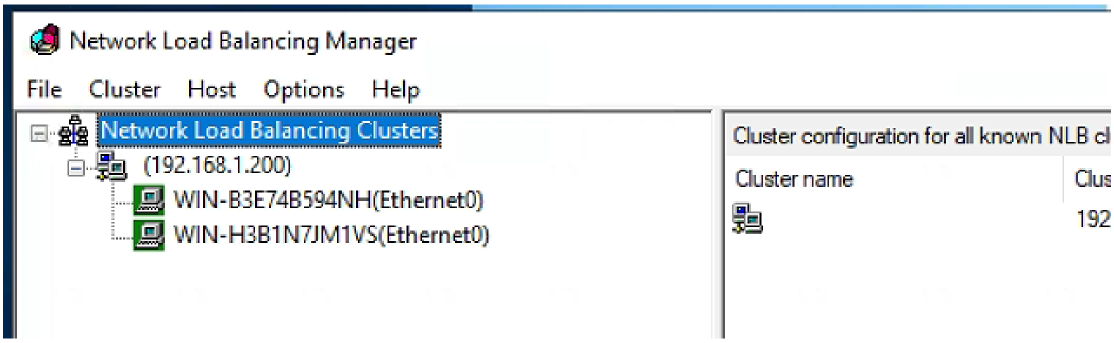
Connection status

Connected

Clusters

Cluster name	Cluster IP	Interface name
	192.168.1.200	Ethernet0

3. The NLB cluster will also be shown on the other server node (C) of the cluster.


Network Load Balancing Manager

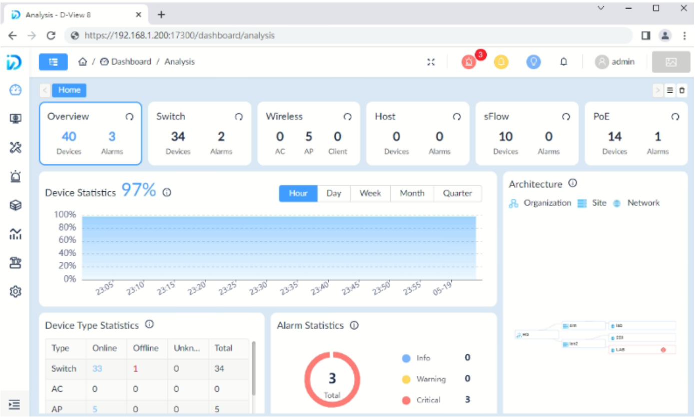
- Network Load Balancing Clusters
  - (192.168.1.200)
    - WIN-B3E74B594NH(Ethernet0)
    - WIN-H3B1N7JM1VS(Ethernet0)

Cluster configuration for all known NLB cl

Cluster name	Clus
	192

Verify the NLB

Disable the network adapter of one of the server node of the cluster (for example, 192.168.1.201). Then access the connectivity to the cluster by entering the Virtual IP as well as the IP address of the other server node into a browser. The Virtual IP (192.168.1.200) as well as the IP address of the other server node (192.168.1.202) should be accessible but the disconnected server (192.168.1.201) node will not be accessible.


Analysis - D-View 8

https://192.168.1.200:17300/dashboard/analysis

Dashboard / Analysis

Overview		Switch		Wireless			Host		sFlow		PoE	
40 Devices	3 Alarms	34 Devices	2 Alarms	0 AC	5 AP	0 Client	0 Devices	0 Alarms	10 Devices	0 Alarms	14 Devices	1 Alarms

Device Statistics 97%

Device Type Statistics

Type	Online	Offline	Unkn...	Total
Switch	33	1	0	34
AC	0	0	0	0
AP	5	0	0	5

Alarm Statistics

3 Total

Info	0
Warning	0
Critical	3

2.2.3. Probe Package Installation

Probes can be installed on a Windows PC. There are two types of Probes:

Local Probe: The Local Probe connects to the D-View 8 Core using the same IP address as the core. It is installed on the D-View 8 server via the D-View 8 Installation package by default.

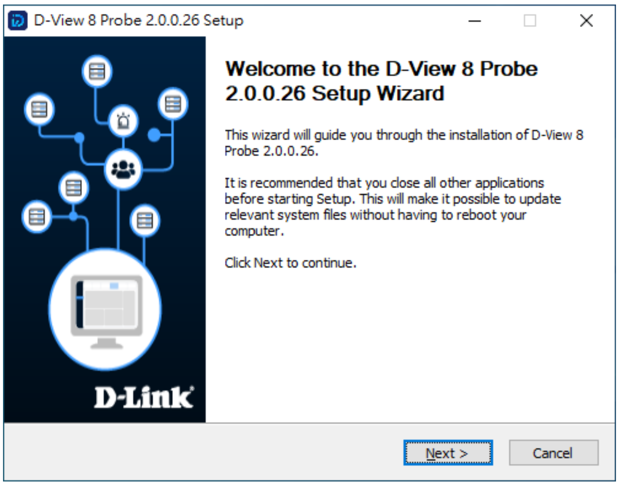
Remote Probe: The Remote Probe that connects to the D-View 8 Core has a different IP address. It can be installed using the Probe Installation Package.

Mode

Probes can operate with or without high-availability and load-balancing features offered by NLB. With high availability, a remote probe connects to the server cluster via a Virtual IP using port 17500, which is the default port for communicating with the D-View 8 server. Without high availability, a remote probe connects to the D-View 8 server directly using its physical IP address.

The D-View 8 probe installation can be accomplished through the setup wizard. Prior to starting the process, it is recommended that you close all applications to allow for the update of related system files without the need to reboot the system.

1. Download the D-View 8 Probe Setup package from the D-View 8 website and double-click it to start the wizard. The Probe Setup page displays.
2. Click **Next** to continue the installation process.



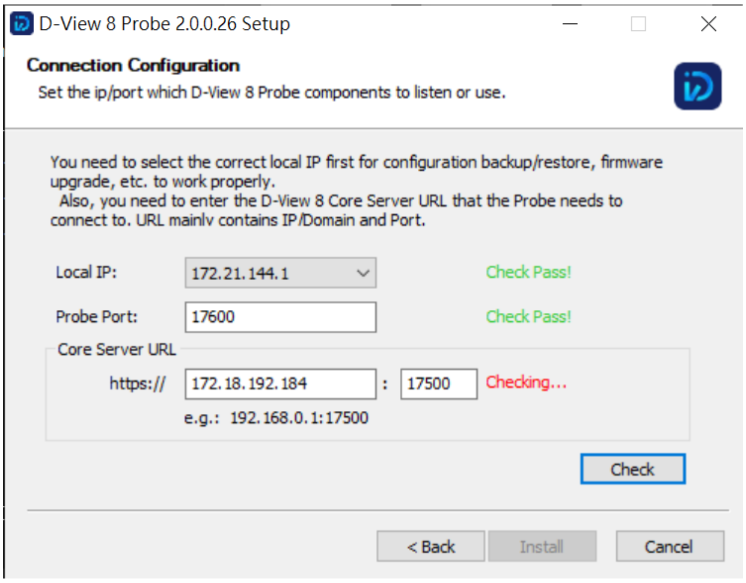
Welcome to the D-View 8 Probe 2.0.0.26 Setup Wizard

This wizard will guide you through the installation of D-View 8 Probe 2.0.0.26.

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

Click Next to continue.

3. The License Agreement page displays. Review the license terms prior to installation. Click **I Agree** to continue the process. Click **Back** to return to the previous menu or **Cancel** to stop the process.



Connection Configuration

Set the ip/port which D-View 8 Probe components to listen or use.

You need to select the correct local IP first for configuration backup/restore, firmware upgrade, etc. to work properly.
Also, you need to enter the D-View 8 Core Server URL that the Probe needs to connect to. URL mainly contains IP/Domain and Port.

Local IP: 172.21.144.1 Check Pass!

Probe Port: 17600 Check Pass!

Core Server URL

https:// 172.18.192.184 : 17500 Checking...

e.g.: 192.168.0.1:17500

4. The Connection Configuration page displays.
5. Click the Local IP drop-down menu to select the local IP address.
6. In the Probe Port field, enter the port with authorized access to allow probe communication.
7. Enter the Core Server IP of the core D-View 8 server along with the port number.
8. Click **Check** to validate the configuration. A **Check Pass!** message displays if the IP addresses and ports are configured correctly.Otherwise, restart the configuration process.

9. Click **Next** to continue the installation process. The Choose Install Location page displays. Click **Browse** to select the destination folder.

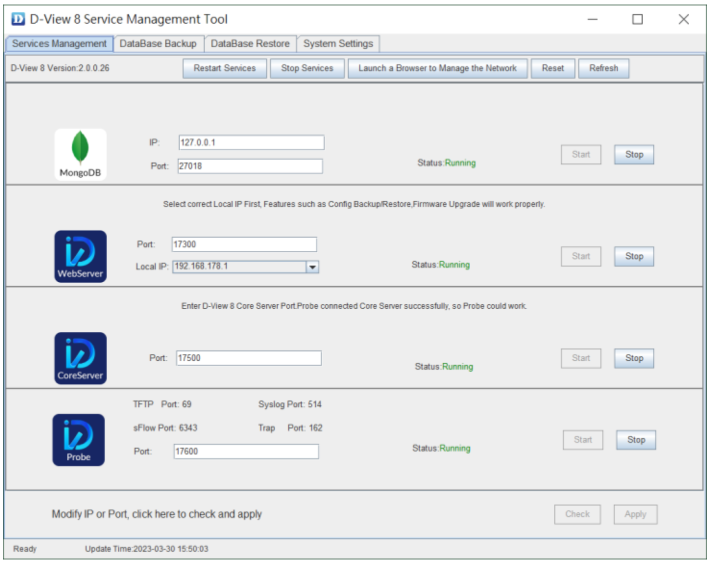
10. Then click **Install** to begin the process.
11. Click **Finish** to end the process when the Completing Setup Wizard page displays.

9. Then click **Install** to begin the process.
10. Click **Finish** to end the process when the Completing Setup Wizard page displays.

The Probe Setup process is completed and a shortcut is generated on the desktop containing the following

D-View 8 probe tools:

- D-View 8 Service Management Tool
- Uninstall



D-View 8 Version:2.0.0.26

IP: 127.0.0.1
Port: 27018
Status:Running

Select correct Local IP First, Features such as Config Backup/Restore,Firmware Upgrade will work properly.

Port: 17300
Local IP: 192.168.178.1
Status:Running

Enter D-View 8 Core Server Port.Probe connected Core Server successfully, so Probe could work.

Port: 17500
Status:Running

TFTP Port: 69
Syslog Port: 514
sFlow Port: 6343
Trap Port: 162
Port: 17600
Status:Running

Modify IP or Port, click here to check and apply

Ready
Update Time:2023-03-30 15:50:03

The Service Management Tool allows for management of the probe:

The Probe Setup is completed.

2.3. Linux Installation

2.3.1. Standalone Edition Installation

To begin the installation process, download the installation package.

1. Download the package:

```
DVIEW8_2.0.0.26.deb
```

2. In the root menu enter the following command to select the downloaded package:

```
dpkg -i DVIEW8_2.0.0.26.deb
```

3. At the prompt enter the local IP address:

> **NOTE:** This IP address is for reference only. Please enter the local IP address of the server.

```
Input the local IP: 172.18.192.256
```

The D-View 8 application requires a database service (MongoDB) to function. If this is the first time it is being installed, a new database instance must be created.

4. At the prompt, enter 1 to select the standalone MongoDB installation type.

```
You intend to use: 1.standalone MongoDB; 2.MongoDB cluster [1/2]
```

To install a new database instance:

a. At the prompt, enter y to install a new database instance:

```
If you need to install a new MongoDB. [y/n]
```

Once the installation is initialized, the administrator account for the database must be created. This will continue the process and initialize the built-in data for the D-View 8 instance.

b. At the username prompt, enter the username for the administrator account:

```
Username: [admin]
```

c. At the password prompt, enter the admin password. Enter it again for Confirm Password.

```
Password: [admin]

Confirm Password: [admin]
```

The installation process continues to install the web, core, and probe services. Once the process is completed, the services will be activated.

To use an existing database:

a. At the prompt, enter n to detect any existing database instances:

```
If you need to install a new MongoDB. [y/n]
```

b. At the prompt, enter y to configure an existing instance:

```
The system detects that you have MongoDB installed, do you want to use it? [y/n]
```

c. Enter the IP address and port of the MongoDB instance.

```
Input the existing mongodb IP: 172.18.192.201
```

d. At the prompt, enter the port of the database instance:

```
Input the existing mongodb port: 27018
```

NOTE: The IP address and port information is for reference only. Enter the information for your database configuration.

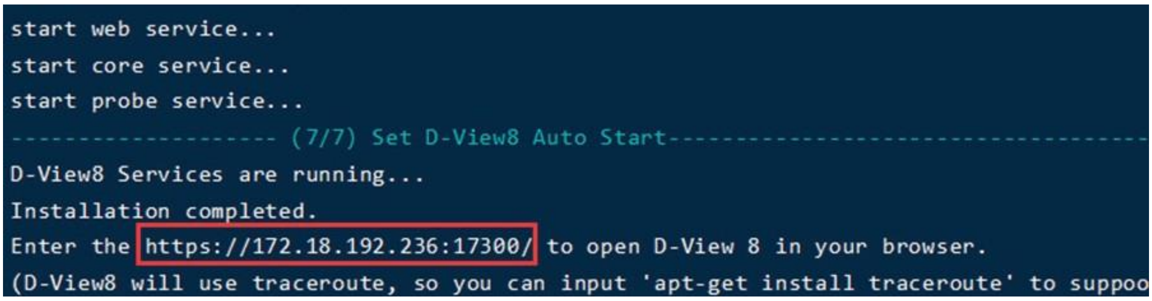
e. For database authentication, enter y if access is required:

```
Do MongoDB access require authentication? [y/n]
```

f. When prompted, enter the username and password to access the database instance.

```
Username: root

Password: root
```

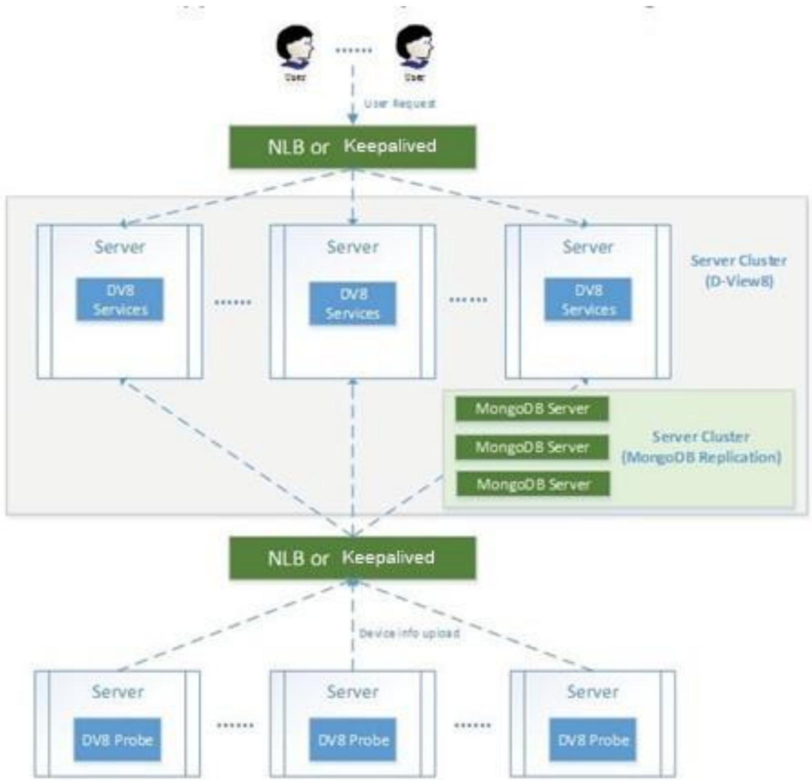
5. Once the instance is created or connected, start the application using a web browser.
6. Open a web browser and enter the IP address of the D-View 8 application in the address bar. In the following figure the IP address is shown for the created instance.



```
start web service...
start core service...
start probe service...
-------------------- (7/7) Set D-View8 Auto Start-----------------------------------
D-View8 Services are running...
Installation completed.
Enter the https://172.18.192.236:17300/ to open D-View 8 in your browser.
(D-View8 will use traceroute, so you can input 'apt-get install traceroute' to suppoo
```

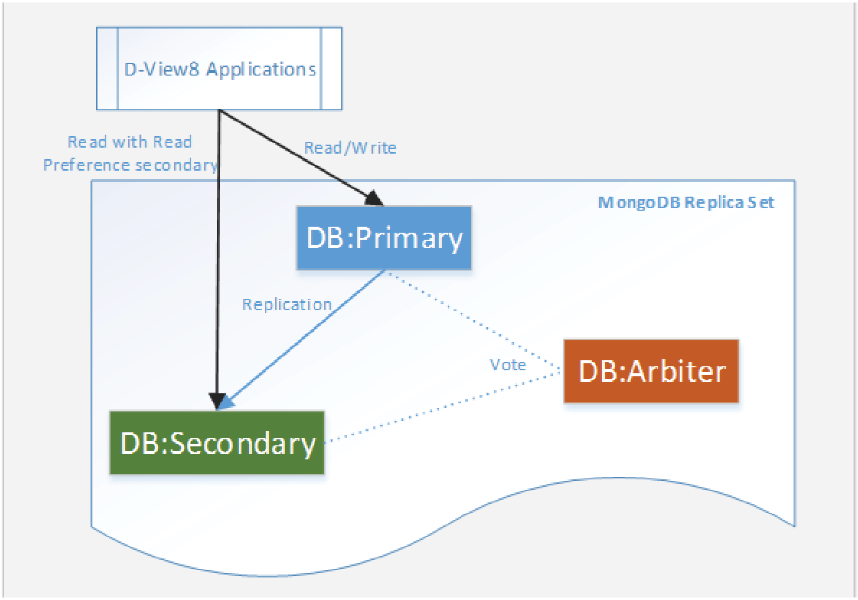
2.3.2. Cluster Mode Installation (Only Available for Enterprise Edition)

The D-View 8 supports redundancy and load balancing features. The following diagram depicts the cluster architecture.



Cluster Architecture

The following shows the structure of D-View 8 application and MongoDB. The structure includes a primary, secondary, and an arbiter database. In the foundational architecture, the application connects to both the primary and secondary databases.

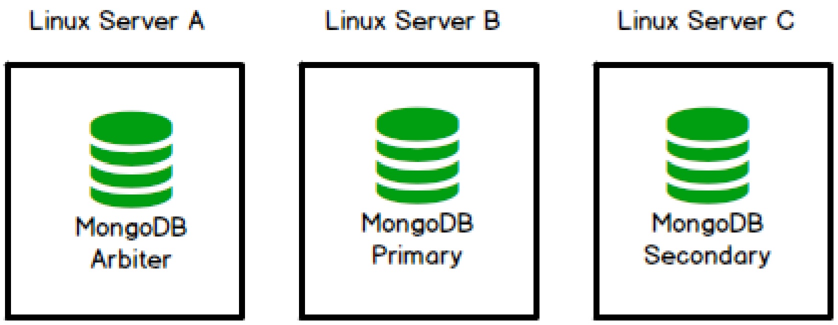


A primary database may become a secondary one, while the secondary may also be designated as the primary. By default, clients read from the primary, but a read preference can be configured to allow read operations on the secondary database.

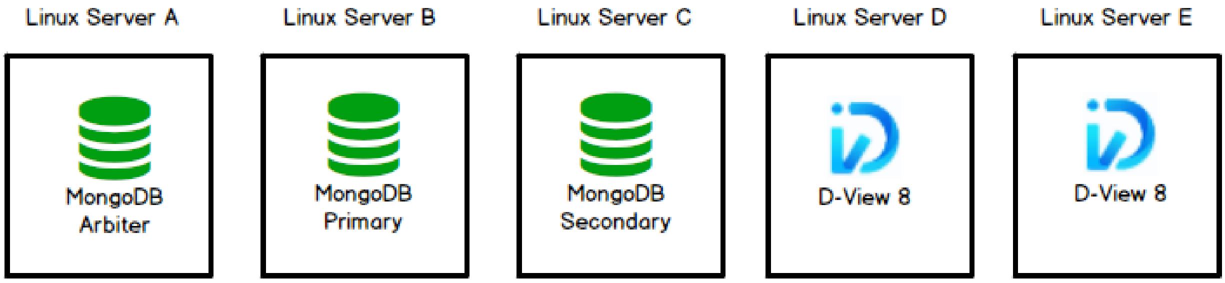
Build a Cluster

Clusters help support data redundancy and load balancing. Building clusters is outlined in this section.

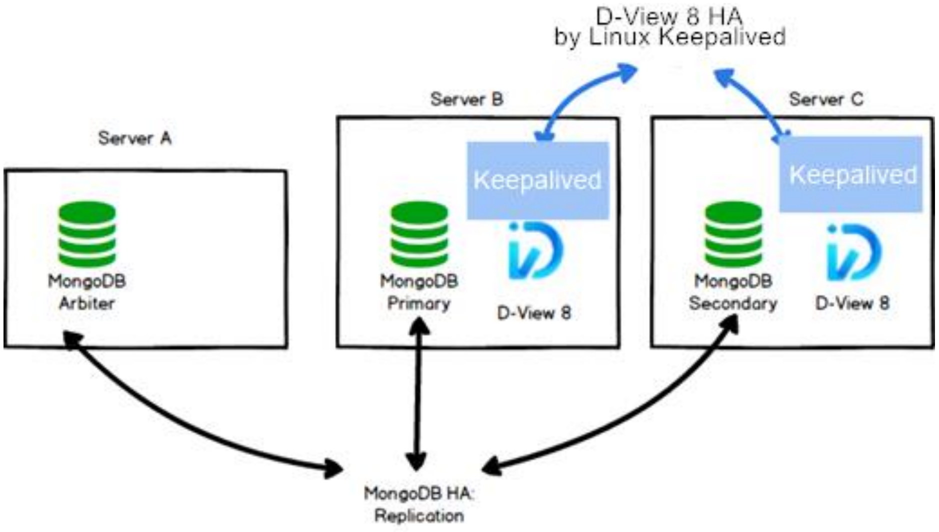
First, Install MongoDB on 3 Linux servers with the designated roles to support the above mentioned structure.



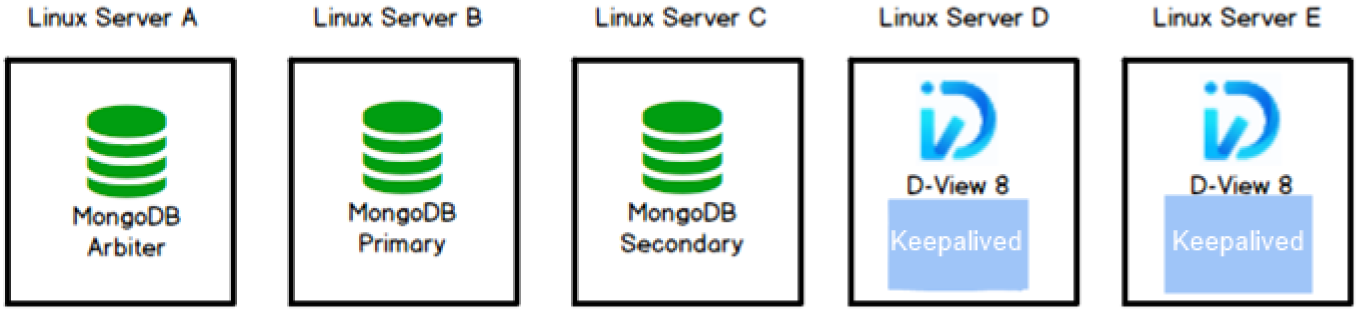
Install D-View 8 on additional servers and connect the D-View 8 application to the MongoDB cluster.



Or you may opt to install D-View 8 on the primary and secondary database servers in lieu of additional servers as the following diagram depicts:

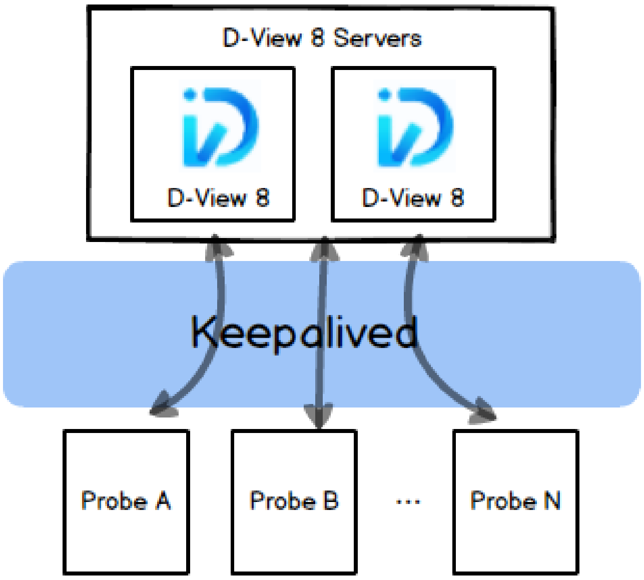


Then, install Keepalived on the D-View 8 servers to support load balancing:



Note: To support high availability and load balancing, please install the MongoDB servers, D-View 8 servers, and Keepalived in sequence as instructed. And the Keepalived must be enabled on the D-View 8 servers which can be a cluster of two servers depending on your network environment.

To manage additional devices through Linux servers, you need to add probes in these servers and connect them to the D-View 8 servers with high-availability clustering managed by Keepalived.



Preparation for Three-server Deployment

When planning for server cluster deployment, you must first set up 3 Linux servers with the following system configuration:

- SERVER A

  OS: Ubuntu 18.04 or above

  MongoDB

  IP Address: 10.32.123.130

  Replica set role: arbiter

- SERVER B

  OS: Ubuntu 18.04 or above

  MongoDB

  IP Address: 10.32.123.131

  Replica set Role: primary

  Keepalived with virtual IP: 10.32.123.133

- SERVER C

  OS: Ubuntu 18.04 above

  MongoDB

  IP Address: 10.32.123.132

  Replica set Role: secondary

  Keepalived with virtual IP: 10.32.123.133

A D-View 8 server includes 3 components: D-View 8 WebAPI, D-View 8 Core, and D-View 8 Probe. Both D-View-8 WebAPI and D-View 8 Core support load-balancing. We will only show load-balancing with D-View 8 WebAPI in our example. D-View 8 servers support load-balancing and failover features via the keepalived package in Linux. In our example, D-View 8 server B and C will be the load balancer and network traffic will be redirected to server B and C via a virtual IP. And users should be able to connect to the D-View 8 server with the virtual IP from a web browser.

Data Redundancy on the MongoDB Server Cluster

This section details the steps to install the required MongoDB database and enable data redundancy in the database cluster.

MongoDB Cluster Installation

Install MongoDB with the MongoDB PSA structure:

Note: MongoDB cluster can still work when either the primary or secondary database is malfunctioned. But when the arbiter is malfunctioned, MongoDB PSA will fail.

Perform MongoDB installation on 3 servers (server A, B, C) for the replica set.

To install a MongoDB Server on server A:

1. Obtain the D-View 8 - MongoDB Installation Package (e.g. dview8-mongodb-linux-*version*.tgz) from your sales representative.
2. Log in to the system as a root user.
3. Change the current directory to the D-View 8 directory, for example, /home/dview8
4. Enter the following to extract the package: tar -zxvf dview8-mongodb-linux-1.0.2.8.tgz.
5. Change the current directory to the extracted path. Then execute the init_mongo.sh shell script: `./init_mongo.sh`
6. You will need to import the built-in data by entering y in the following question:

```
Whether you first start MongoDB, first start will import D-View 8 built-in data. [y/n]
```

Choose to use cluster MongoDB by starting the instance in replication mode:

```
Are you going to use Cluster MongoDB and start MongoDB in replication mode. [y/n]
```

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# ./init_mongo.sh

.


---- check MongoDB port ----

MongoDB port : 27018 is free

 Whether you first start MongoDB, first start will import D-View 8 built-in data.[y/n]

y

mongodb is not running!

stop mongodb......

about to fork child process, waiting until server is ready for connections.

forked process: 385940

child process started successfully, parent exiting

Creating built-in data for D-View8 database...

Creating built-in data system.js.

Creating built-in data DView8_ConfigurationCategory.

Creating built-in data DView8_ConfigurationTemplate.

Creating built-in data DView8_Credit.

Creating built-in data DView8_DeviceCategory.

...

...

Creating built-in data DView8_SyslogKeyWords.

D-View8 database built-in data created.

 Are you going to use Cluster MongoDB and start MongoDB in replication mode.[y/n]
```

```
y

mongodb is running!

stop mongodb......

2022-08-20T06:04:11.324+0000 W CONTROL  [main] enableMajorityReadConcern startup

parameter was supplied, but its value was ignored; majority read concern cannot

be disabled.

about to fork child process, waiting until server is ready for connections.

forked process: 386317

child process started successfully, parent exiting

------ all completed ------

root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0#
```

The database server is ready for connections and will use TCP port 27018 for communication.

Perform the above installation procedure on server B and C as well.

D-View 8 Installation

Note: You can opt to install D-View 8 on the primary and secondary database (server B &C) to reduce the total number of servers as illustrated in the above three-server topology. Another option is to install D-View 8 on two additional servers.

To install D-View 8 on multiple servers and connect them to the MongoDB cluster:

1. Log in as a root user.
2. Download the package from the D-View 8 website:

   D-View_8_*version*_Installation.deb (e.g. dpkg -i D-View_8_2.0.0.26_Installation.deb)
3. Change the current directory to the D-View 8 directory, for example, /home/dview8
4. Execute the dpkg command to start the installation process:

   ```
   dpkg -i D-View_8_2.0.0.26_Installation.deb
   ```
5. At the prompt enter the physical IP address for the local server:

   Input the local IP: `x.x.x.x` (10.32.123.131 for server B as in our example)

   The D-View 8 application requires a database service (MongoDB) to function.
6. At the prompt, enter 2 for MongoDB cluster installation.

   ```
   You intend to use: 1. standalone MongoDB; 2. MongoDB cluster [1/2]
   ```

7. At the prompt, enter the physical IP address and port of the primary, secondary, and arbiter database.

```
root@dview8:/home/dview8# dpkg -i D-View_8_2.0.0.26_Installation.deb

Selecting previously unselected package dview8.

(Reading database ... 108358 files and directories currently installed.)

Preparing to unpack D-View_8_2.0.0.26_Installation.deb ...

Before installation...
```

```
.

----

Unpacking dview8 (2.0.0.26) ...

Setting up dview8 (2.0.0.26) ...

Installing...

.

-----------------------------------------------------------------------------------------------------------------------------------


--------------------（1/7）check local file and directory environments---------------------------------------------

--------------------（2/7）check local port environments-------------------------------------------------------

---- check WebServer ----

WebServer_port is free

---- check CoreServer_port ----

CoreServer_port is free

---- check Probe_port ----

Probe_port is free

Now initial set the local IP for D-View 8 (input format similar to: 192.168.131.25),

Local IP address detected may be as follows, Select correct local IP First, Features such as Config Backup/Restore,

Firmware Upgrade, Send Activation Email will work properly.

10.32.123.131

172.18.0.1

--------------------

please confirm that the input IP is valid:

Input the local IP：10.32.123.131  #Input the physical IP addresses for the D-VIEW 8 server

input: 10.32.123.131

--------------------（3/7）Chmod installation files-------------------------------------------------------

--------------------（4/7）Install D-View8 MongoDB Services-------------------------------------------------------

D-View 8 requires a database service provided by MongoDB 4.0.3. So if you choose 'Install a new MongoDB 4.0.3',

the installation will try to install MongoDB 4.0.3. If you choose 'Use an existing MongoDB 4.0.3', you can

let D-View 8 to connect a remote MongoDB service.

You intend to use: 1.standalone MongoDB; 2.MongoDB cluster[1/2]

2

-------------------------------------------------------------------------------------------------------------------

MongoDB cluster contains Primary node, Secondary node and Arbiter node.

The Primary: receives write and read operations.

The Secondary: become a primary if the current primary becomes unavailable.
```

The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.

```
Input the existing the Primary IP：10.32.123.131

input: 10.32.123.131

Input the existing the Primary port：27018

input: 27018

Input the existing the Secondary IP：10.32.123.132

input: 10.32.123.132

Input the existing the Secondary port：27018

input: 27018

Input the existing the Arbiter IP：10.32.123.130

input: 10.32.123.130

Input the existing the Arbiter port：27018

input: 27018

Creating built-in data for D-View8 database...

Creating built-in data DView8_ConfigurationCategory.

Creating built-in data DView8_ConfigurationTemplate.

Creating built-in data DView8_Credit.

Creating built-in data DView8_DeviceCategory.

Creating built-in data DView8_DeviceTemplate.

Creating built-in data DView8_DeviceType.

Creating built-in data DView8_Email.

Creating built-in data DView8_MailServer.

Creating built-in data DView8_MonitorCategory.

Creating built-in data DView8_MonitorTemplate.

Creating built-in data DView8_NotificationSoundSetting.

Creating built-in data DView8_Organization.

Creating built-in data DView8_PanelTemplate.

Creating built-in data DView8_Role.

Creating built-in data DView8_TimeSetting.
Creating built-in data DView8_PortGlobalSetting.



Creating built-in data DView8_AlarmRuleDefine.

Creating built-in data DView8_User.

Creating built-in data DView8_VendorTemplate.
Creating built-in data sFlow_mapping_DSCP.


Creating built-in data template_config_view.

Creating built-in data DView8_TrapOID.

Creating built-in data snmp_mib_node.

Creating built-in data sFlow_NicVendorMapping.

Creating built-in data sFlow_mapping_application.

Creating built-in data DView8_SyslogKeyWords.

Creating built-in data DView8_MonitorBatchAlarmSetting.

Creating built-in data system.js.

D-View8 database built-in data created.

--------------------（5/7）Modify D-View8 Service files------------------------------------------------------

modify webserver files

modify coreserver files

modify probe files

--------------------（6/7）Install D-View8 Local Services------------------------------------------------------

start web service...

start core service...

start probe service...

--------------------（7/7）Set D-View8 Auto Start------------------------------------------------------

D-View8 Services are running...

Installation completed.

Enter the https://10.32.123.131:17300/ to open D-View 8 in your browser.

(D-View8 will use traceroute, so you can input 'apt-get install traceroute' to support)

root@dview8:/home/dview8#
```

8. Perform the installation procedure for D-View 8 server C but using a different local IP address. For the above Step 5, input the physical IP address for server C (10.32.123.132):

   After the installation, you can access the application’s dashboard by opening a web browser and entering the assigned IP address and port number (e.g. https://10.32.123.131:17300/ and https://10.32.123.132:17300 from the above example) in the browser’s address field.

Server Load Balancing on D-View 8 Servers

The Keepalived package needs to be installed on the D-View 8 servers to enable load balancing. Keepalived uses LVS and VRRP to be the load-balancer. VRRP defines two states, MASTER and BACKUP. We will set server B (10.32.123.131) as the MASTER and server C (10.32.123.132) as the BACKUP.

1. Log in to server B using SSH with a root account.

2. Install Keepalived:

```
root@dview8:~# apt install keepalived
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  keepalived
0 upgraded, 1 newly installed, 0 to remove and 71 not upgraded.
Need to get 361 kB of archives.
After this operation, 1,250 kB of additional disk space will be used.
Get:1 http://tw.archive.ubuntu.com/ubuntu focal-updates/main amd64 keepalived amd64 1:2.0.19-2ubuntu0.2 [361 kB]
Fetched 361 kB in 0s (1,129 kB/s)
Selecting previously unselected package keepalived.
(Reading database ... 108694 files and directories currently installed.)
Preparing to unpack .../keepalived_1%3a2.0.19-2ubuntu0.2_amd64.deb ...
Unpacking keepalived (1:2.0.19-2ubuntu0.2) ...
Setting up keepalived (1:2.0.19-2ubuntu0.2) ...
Processing triggers for man-db (2.9.1-1) ...

Processing triggers for dbus (1.12.16-2ubuntu2.2) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...

root@dview8:~#
```

3. Create the /etc/keepalived directory if it is not created.

```
root@dview8:~# mkdir /etc/keepalived
```

4. Copy keepalived.conf and vip_service.sh from

   /usr/local/dview8/keepalived to /etc/keepalived:

```
root@dview8:~# cp /usr/local/dview8/keepalived/* /etc/keepalived
```

5. Modify the configuration file keepalived.conf as follows:

Note: The DView-8 server uses ports 17300 and 17500 for D-View 8 WebAPI and D-View 8 Core respectively and the port number will be configured in this file.

etc/keepalived/keepalived.conf

```
! Configuration File for keepalived

global_defs {            #Global Configuration

    router_id LVS_36       #The router_id is the load-balancing identifier, which should be unique.
```

```
}


vrrp_instance VI_1 {        # Identify a VRRP instance definition block

    state MASTER            # Specify the instance state in standard use: MASTER or BACKUP, has to be capitalized.

    interface eth0          # Specify the network interface for the instance to run on

    virtual_router_id 51     # Specify to which VRRP router id the instance belongs

    priority 50              # Specify the instance priority for VRRP MASTER router (lower means higher priority), the main node has the
                                highest  priority than other nodes.

    advert_int 1            # Specify the advertisement interval in seconds

    authentication {        # Identify a VRRP authentication definition block

        auth_type PASS       # specify the authentication method: PASS|AH

        auth_pass 1111       #Specify the password for authentication

    }

    virtual_ipaddress {      # identify a VRRP VIP definition block

        10.32.123.133

    }

}


virtual_server 10.32.123.133 17300 {   #Assign service to use the Virtual IP, the D-View 8 WebAPI uses port 17300

    delay_loop 6      # Healthcheck time interval

    lb_algo rr

    lb_kind DR        #Use the LVSDR mode

    persistence_timeout 5

    protocol TCP      # specify the protocol kind: TCP|UDP


    real_server 10.32.123.131 17300 {

        weight 1     #Assign weight to service node

        TCP_CHECK {

            connect_timeout 3

            retry 1

            delay_before_retry 3

            connect_port 17300

        }

    }



    real_server 10.32.123.132 17300 {
```

```
    weight 1     #Assign weight to service node

        TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
        }
    }
}

virtual_server 10.32.123.133 17500 {   #Assign service to use the Virtual IP, the D-View 8 Core uses port 17500
    delay_loop 6       #Healthcheck time interval
    lb_algo rr
    lb_kind DR         # Use the LVSDR mode

    persistence_timeout 5
    protocol TCP       # specify the protocol kind: TCP|UDP

    real_server 10.32.123.131 17500 {
        weight 1      #Assign weight to service node
        TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
        }
    }

    real_server 10.32.123.132 17500 {
        weight 1     #Assign weight to service node
        TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
```

```
      }


    }

}
```

6. Start the Keepalived service and check its status by entering the following:

```
root@dview8:~# service keepalived start
root@dview8:~# service keepalived status
```

Make sure that active (running) is displayed:

```
● keepalived.service - Keepalive Daemon (LVS and VRRP)
 Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; vendor preset: enabled)
Active: active (running) since Sat 2022-08-20 11:20:45 UTC; 51min ago
Main PID: 198630 (keepalived)
Tasks: 3 (limit: 9434)
Memory: 3.1M
CGroup: /system.slice/keepalived.service
             ├──198630 /usr/sbin/keepalived --dont-fork
             ├──198651 /usr/sbin/keepalived --dont-fork
             └──198652 /usr/sbin/keepalived --dont-fork
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating healthchecker for service [10.32.123.131]:tcp:17500 for VS [10>
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating healthchecker for service [10.32.123.132]:tcp:17500 for VS [10>
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating BFD healthchecker
Aug 20 11:20:47 dview8 Keepalived_healthcheckers[198651]: TCP connection to [10.32.123.132]:tcp:17500 success.
Aug 20 11:20:49 dview8 Keepalived_vrrp[198652]: (VI_1) Entering MASTER STATE
Aug 20 11:20:49 dview8 Keepalived_healthcheckers[198651]: TCP connection to [10.32.123.132]:tcp:17300 success.
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: TCP_CHECK on service [10.32.123.131]:tcp:17300 failed.
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: Removing service [10.32.123.131]:tcp:17300 to VS [10.32.123.133]:tcp:17300
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: TCP_CHECK on service [10.32.123.131]:tcp:17500 failed.
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: Removing service [10.32.123.131]:tcp:17500 to VS [10.32.123.133]:tcp:17500
lines 1-21/21 (END)
```

7. Modify the vip_service.sh by entering the assigned Virtual IP address:

/etc/keepalived/vip_service.sh

```
#!/bin/bash

check_ptah=`which ifconfig |wc -l`

if [ $check_ptah -eq 0 ]

    then echo -e  "\033[31mPlease run the 'apt install net-tools' command\033[0m"

   exit 1


fi
SNS_VIP=10.32.123.133 #Enter the Virtual IP address

case "$1" in

start)

       ifconfig lo:0 $SNS_VIP netmask 255.255.255.255 broadcast $SNS_VIP
        /sbin/route add -host $SNS_VIP dev lo:0
       echo "1" >/proc/sys/net/ipv4/conf/lo/arp_ignore
       echo "2" >/proc/sys/net/ipv4/conf/lo/arp_announce
       echo "1" >/proc/sys/net/ipv4/conf/all/arp_ignore
       echo "2" >/proc/sys/net/ipv4/conf/all/arp_announce
       sysctl -p >/dev/null 2>&1
       echo "RealServer Start OK"
       ;;
stop)
       ifconfig lo:0 down
       route del $SNS_VIP >/dev/null 2>&1
       echo "0" >/proc/sys/net/ipv4/conf/lo/arp_ignore
       echo "0" >/proc/sys/net/ipv4/conf/lo/arp_announce
       echo "0" >/proc/sys/net/ipv4/conf/all/arp_ignore
       echo "0" >/proc/sys/net/ipv4/conf/all/arp_announce
       echo "RealServer Stoped"
       ;;
*)
       echo "Usage: $0 {start|stop}"
       exit 1
esac
exit 0
```

8. Verify that the Virtual IP service is configured with an extra loopback network interface lo:0

```
root@dview8:/etc/keepalived# ./vip_service.sh start

RealServer Start OK
```

```
root@dview8:/etc/keepalived# ip a


1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.32.123.133/32 brd 10.32.123.133 scope global lo:0 # The loopback network interface
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
   valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether ca:e1:88:d7:da:40 brd ff:ff:ff:ff:ff:ff
    inet 10.32.123.131/16 brd 10.32.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.32.123.133/32 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::c8e1:88ff:fed7:da40/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:8e:b9:f3:bd brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

9. To start or stop /etc/keepalived/vip_service.sh whenever keepalived starts or stops, modify /lib/systemd/system/keepalived.service:

   Add the following two lines to /lib/systemd/system/keepalived.service:

   ExecStartPre=bash /etc/keepalived/vip_service.sh start

   ExecStopPost=bash /etc/keepalived/vip_service.sh stop

/lib/systemd/system/keepalived.service

```
[Unit]
Description=Keepalive Daemon (LVS and VRRP)
After=network-online.target
Wants=network-online.target
# Only start if there is a configuration file
```

```
ConditionFileNotEmpty=/etc/keepalived/keepalived.conf


[Service]

Type=simple

# Read configuration variable file if it is present

EnvironmentFile=-/etc/default/keepalived

ExecStart=/usr/sbin/keepalived --dont-fork $DAEMON_ARGS




ExecStartPre=bash /etc/keepalived/vip_service.sh start  # Add this line and the following line

ExecStopPost=bash /etc/keepalived/vip_service.sh stop

ExecReload=/bin/kill -HUP $MAINPID


[Install]

WantedBy=multi-user.target
```

10. Reload keepalived by entering the following commands:

```
root@dview8:/lib/systemd/system# systemctl daemon-reload

root@dview8:/lib/systemd/system# service keepalived restart
```

Perform the above installation procedure on the designated VRRP backup server (server C). However, the /etc/keepalived/keepalived.conf should be modified accordingly as the following example file shows:

/etc/keepalived/keepalived.conf

```
! Configuration File for keepalived


global_defs {           #Global configuration

  router_id LVS_36      #router_id should be unique in the LAN

}


vrrp_instance VI_1 {        # identify a VRRP instance definition block

  state BACKUP              #Here identify the VRRP backup server, has to be capitalized

  interface eth0            # Specify the network interface for the instance to run on

  virtual_router_id 51      # specify to which VRRP router id the instance belongs

  priority 100              # specify the instance priority for the VRRP BACKUP router

  advert_int 1              # Specify the advertisement interval in seconds (set to 1)

  authentication {          # Identify a VRRP authentication definition block

    auth_type PASS          #Authentication method
```

```
        auth_pass 1111        #Authentication password

    }
    virtual_ipaddress {     #Identify a VRRP VIP definition block; it can contain multiple addresses without specifying subnetwork masks, but
it must
                                          align with the Virtual IP address in the LVS client setting.
        10.32.123.133
    }
}

virtual_server 10.32.123.133 17300 {   #Assign the service to use the Virtual IP, the D-View 8 WebAPI uses port 17300
    delay_loop 6       #Healthcheck time interval
    lb_algo rr
    lb_kind DR         # Use the LVSDR mode
    persistence_timeout 5
    protocol TCP       #specify the protocol kind: TCP|UDP

    real_server 10.32.123.131 17300 { # Service Node 1
        weight 1     #Assign weight to the service node
        TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
        }
    }

    real_server 10.32.123.132 17300 { #Service Node 2
    weight 1    #Assign weight to the service node
        TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
        }
    }
```

```
}


virtual_server 10.32.123.133 17500 {   # Assign the service to use the Virtual IP and port #17500, the D-View 8 Core uses port 17500


    delay_loop 6       # Healthcheck time interval

    lb_algo rr

    lb_algo rr

    lb_kind DR         # Use the LVSDR mode

    persistence_timeout 5

    protocol TCP      # specify the protocol kind: TCP|UDP


    real_server 10.32.123.131 17500 {

        weight 1      # Assign weight to the service node


        TCP_CHECK {


            connect_timeout 3

            retry 1

            delay_before_retry 3

            connect_port 17500

        }

    }


    real_server 10.32.123.132 17500 {


        weight 1     # Assign weight to the service node

        TCP_CHECK {

            connect_timeout 3

            retry 1

            delay_before_retry 3

            connect_port 17500

        }

    }

}
```

Also modify /etc/keepalived/vip_service.sh for the VRRP backup server as shown in the above Step 7 using the assigned Virtual IP address (e.g. 10.32.123.133 as shown in the above example). Perform Step 8 as for the master server to verify that the Virtual IP service is configured with an extra loopback network interface lo:0. And modify *keepalived.service* so that *vip_service.sh* can start or stop whenever whenever *keepalived* starts or stops as shown in the above Step 9.

The installation package also provides scripts for restarting and stopping database services as well as status checking:

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# ls -la *.sh

-rwxr-xr-x 1 root root  983 Aug 17 07:43 restart_mongo.sh

-rwxrwxrwx 1 root root  496 Aug 17 07:43 status_mongo.sh

-rwxrwxrwx 1 root root  686 Aug 17 07:43 stop_mongo.sh
```

To obtain the D-View 8 version:

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# cat dv8-version

2.0.0.26
```

You can now verify the D-View 8 installation by entering the Virtual IP address of the server cluster. The

D-View 8 web interface can be accessed with the port 17300 (https://10.32.123.133:17300). The D-View 8 web interface should be operational even one D-View 8 sever of the cluster is disconnected.

2.3.3 Probe Package Installation

Probes can be installed on a Linux PC. The Linux distribution we are using for demonstration is Ubuntu 20.04.3 LTS. There are two types of Probes:

Local Probe: The Local Probe connects to the D-View 8 Core using the same IP address as the core. It is installed on the D-View 8 server via the D-View 8 Installation package by default.

Remote Probe: The Remote Probe that connects to the D-View 8 Core has a different IP address. It can be installed using the Probe Installation Package.

Mode

Probes can operate with or without high-availability and load-balancing features offered by Keepalived. With high availability, a remote probe connects to the server cluster via a Virtual IP using port 17500, which is the default port for communicating with the D-View 8 server. Without high availability, a remote probe connects to the D-View 8 server directly using its physical IP address.

Installation

Download the D-View 8 Probe Installation package from the [D-View 8 website](). Its file name should be

D-View_8_Probe_*Version*_Installation.deb.

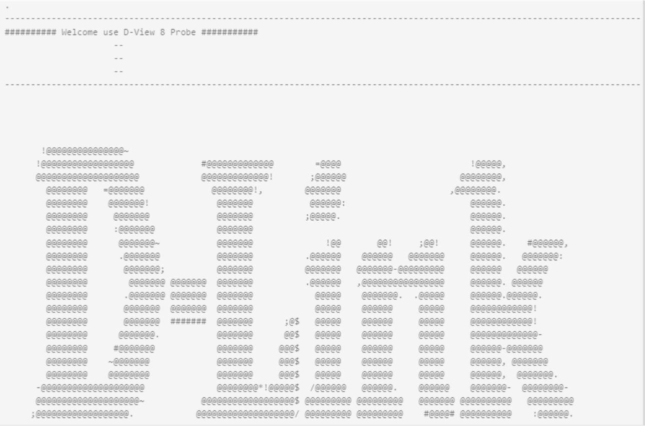
1. Log in to the system with a root user account.

2. Put the installation package to the D-View 8 home: /home/dview8

3. Change the directory to the D-View 8 home: /home/dview8

4. Install the package:

```
root@dview8:/home/dview8# dpkg -i D-View_8_Probe_1.0.2.8_Installation.deb

(Reading database ... 109264 files and directories currently installed.)

Preparing to unpack D-View_8_Probe_1.0.2.8_Installation.deb ...

Before installation...

.

Unpacking dview8probe (2.0.0.26) ...

Setting up dview8probe (2.0.0.26) ...

post installer......
```



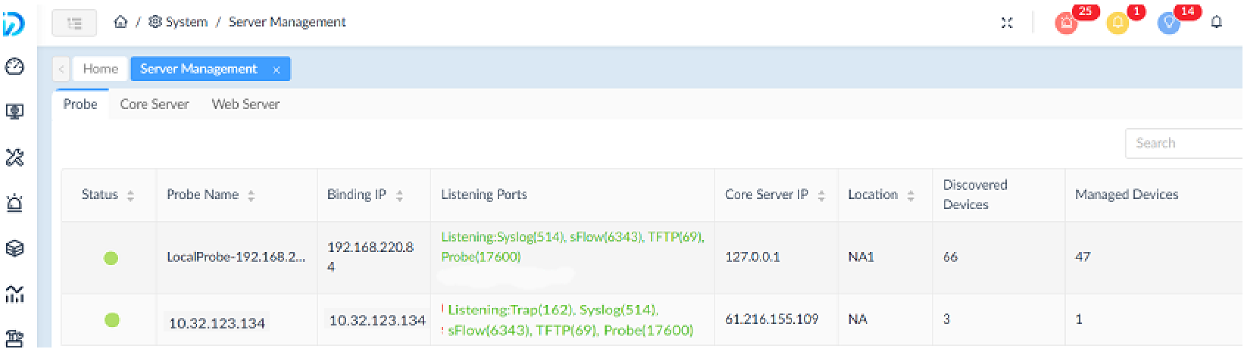
```
.
------------------------------------------------------------------------------------------------------------------------------
########## Welcome use D-View 8 Probe ###########
                     --
                     --
                     --
------------------------------------------------------------------------------------------------------------------------------
```

5. Input the physical IP address of the local server and the core server using the Virtual IP and the port number of the server cluster. For design without HA, enter the physical IP address of local server and the core server using the physical IP and the port number instead.

```
-------------------（1/7）check local file and directory environments---------------------------------------------

-------------------（2/7）check local port environments-----------------------------------------------------------

---- check probe_port ----

probe_port is free

-------------------（3/7）input local ip / coreserver url-------------------------------------------------------

---------- local IP address detected may be as follows ----------

-------------------

172.18.0.1

10.32.123.134

172.17.134.220

-------------------

Now initial set the local IP for D-View 8 Probe, features such as Config Backup/Restore,Firmware Upgrade will work properly.

please confirm that the input IP is valid:(input format similar to: 192.168.131.25)


input: 10.32.123.134

Now please enter D-View8 Core Server IP and Port. Probe connected Core Server successfully, So Probe could work.



please confirm that the input IP is valid:(input format similar to: 192.168.131.25)

Input the CoreServer IP：10.32.123.133   #Input the Virtual IP and port number of the server cluster for HA or a physical IP address of the server without HA

input: 10.32.123.133

Input the CoreServer Port：17500

input: 17500

-------------------

-------------------（4/7）Chmod installation files-------------------------------------------------------------

-------------------（5/7）Modify D-View8 Probe Service files---------------------------------------------------------

modify probe files

check file finished

-------------------（6/7）Install D-View8 Probe Local Services-----------------------------------------------------

start probe service

-------------------（7/7） Set D-View8 Probe Auto Start---------------------------------------------------------------

D-View8 Probe Service are running...
```

```
Installation completed.
```

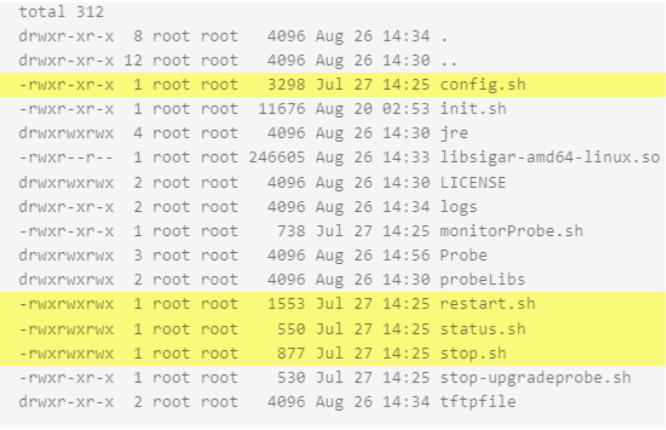
You can verify the installation of the remote probe by opening a web browser and entering the Virtual IP address (or the physical IP address if HA is not used) of the server cluster with the port: https://10.32.123.133:17300. Then go to **System > Server Management**. On the Probe tab, the remote probe should be listed in the table.



Status	Probe Name	Binding IP	Listening Ports	Core Server IP	Location	Discovered Devices	Managed Devices
●	LocalProbe-192.168.2...	192.168.220.84	Listening:Syslog(514), sFlow(6343), TFTP(69), Probe(17600)	127.0.0.1	NA1	66	47
●	10.32.123.134	10.32.123.134	Listening:Trap(162), Syslog(514), sFlow(6343), TFTP(69), Probe(17600)	61.216.155.109	NA	3	1

The installation package also provides scripts for restart and stop as well as status checking. You can also modify IP settings using the config.sh script.

```
dview8@dview8:~$ cd /usr/local/dview8_probe/

dview8@dview8:/usr/local/dview8_probe$ ls -la
```



```
total 312
drwxr-xr-x  8 root root   4096 Aug 26 14:34 .
drwxr-xr-x 12 root root   4096 Aug 26 14:30 ..
-rwxr-xr-x  1 root root   3298 Jul 27 14:25 config.sh
-rwxr-xr-x  1 root root  11676 Aug 20 02:53 init.sh
drwxrwxrwx  4 root root   4096 Aug 26 14:30 jre
-rwxr--r--  1 root root 246605 Aug 26 14:33 libsigar-amd64-linux.so
drwxrwxrwx  2 root root   4096 Aug 26 14:30 LICENSE
drwxr-xr-x  2 root root   4096 Aug 26 14:34 logs
-rwxr-xr-x  1 root root    738 Jul 27 14:25 monitorProbe.sh
drwxrwxrwx  3 root root   4096 Aug 26 14:56 Probe
drwxrwxrwx  2 root root   4096 Aug 26 14:30 probeLibs
-rwxrwxrwx  1 root root   1553 Jul 27 14:25 restart.sh
-rwxrwxrwx  1 root root    550 Jul 27 14:25 status.sh
-rwxrwxrwx  1 root root    877 Jul 27 14:25 stop.sh
-rwxr-xr-x  1 root root    530 Jul 27 14:25 stop-upgradeprobe.sh
drwxr-xr-x  2 root root   4096 Aug 26 14:34 tftpfile
```

Uninstallation

Uninstallation can be accomplished by removing the probe package dview8probe using the dpkg command with a parameter.

```
root@dview8:~# dpkg -P dview8probe
(Reading database ... 109422 files and directories currently installed.)
Removing dview8probe (2.0.0.26) ...
pre remove......
probe is running!
stop probe......
------ all completed ------
post remove......
Purging configuration files for dview8probe (2.0.0.26) ...
post remove......
dpkg: warning: while removing dview8probe, directory '/usr/local/dview8_probe/Probe' not empty so not removed
```

2.4 Software Upgrade

NOTE: Software upgrade is only supported after D-View 8 version 1.0.1.28. For D-View 8 version before 1.0.1.28, you can only install the new version after removing the old one.

2.4.1. On Windows

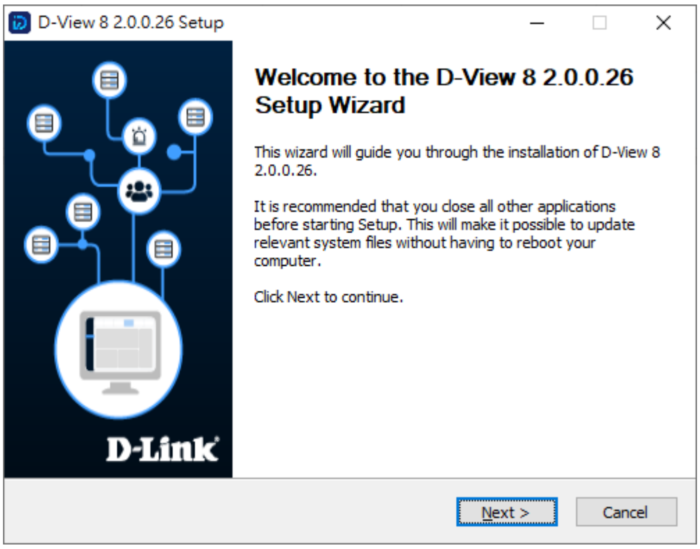
The D-View 8 application is upgraded from time to time to increase the performance and functionality of the software. Upgrading the software can be done by downloading a newer version of the full installation package.

To upgrade the software:

1. Download the latest D-View 8 installation package from the D-View 8 website.
2. Double-click the package file to start the installer.

The Installation Setup wizard displays.

3. Click **"Next"** to begin the installation process.



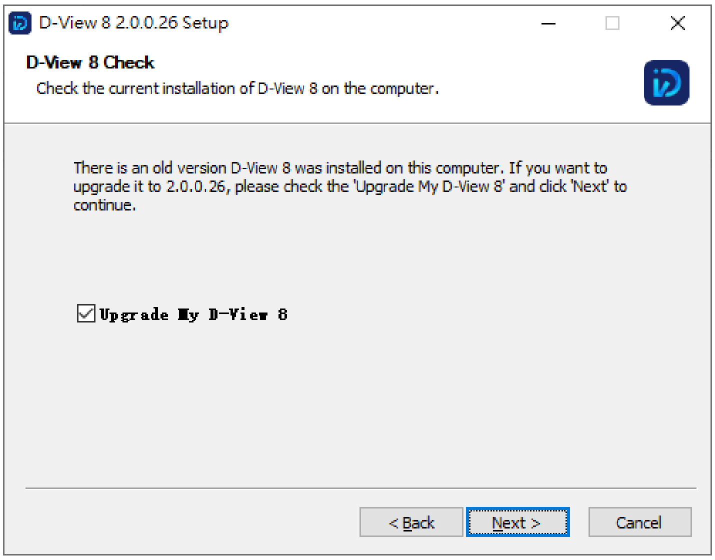
Welcome to the D-View 8 2.0.0.26 Setup Wizard

This wizard will guide you through the installation of D-View 8 2.0.0.26.

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

Click Next to continue.

4. Select "Upgrade My D-View 8" and click "Next" to continue.



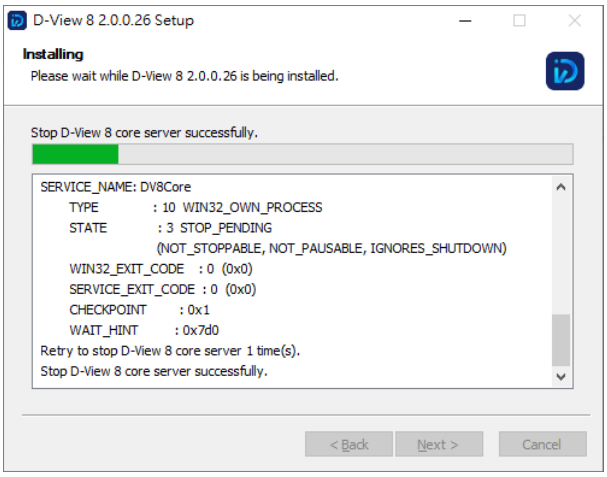
D-View 8 Check

Check the current installation of D-View 8 on the computer.

There is an old version D-View 8 was installed on this computer. If you want to upgrade it to 2.0.0.26, please check the 'Upgrade My D-View 8' and click 'Next' to continue.

☑ Upgrade My D-View 8

5. When the Installation Complete page displays, click **Next** to continue.



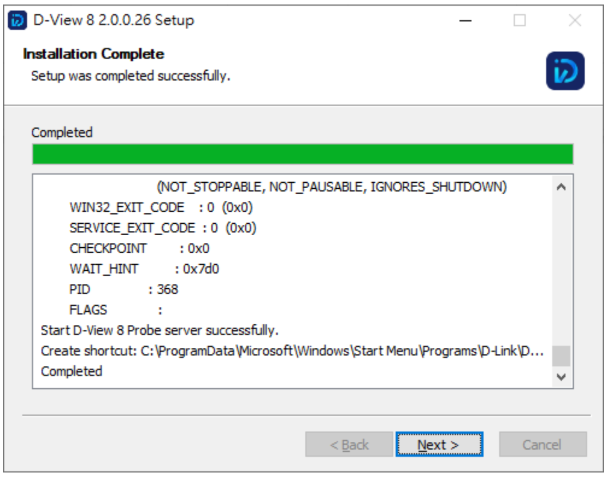
D-View 8 2.0.0.26 Setup

Installing

Please wait while D-View 8 2.0.0.26 is being installed.

Stop D-View 8 core server successfully.

```
SERVICE_NAME: DV8Core
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x7d0
Retry to stop D-View 8 core server 1 time(s).
Stop D-View 8 core server successfully.
```



D-View 8 2.0.0.26 Setup

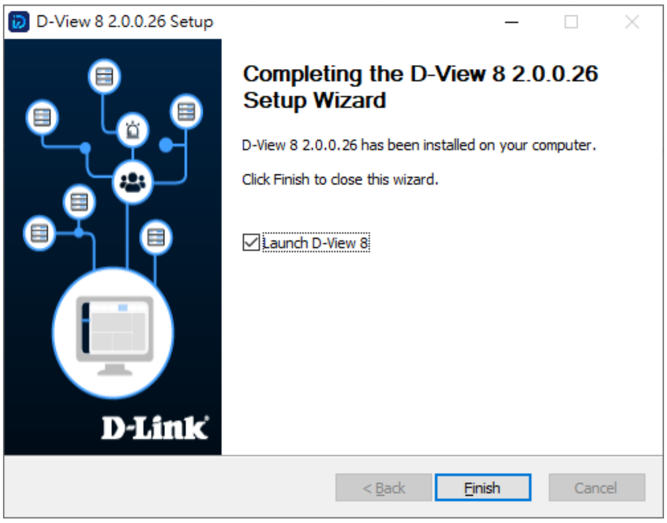
Installation Complete

Setup was completed successfully.

Completed

```
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 368
        FLAGS              :
Start D-View 8 Probe server successfully.
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\D-Link\D...
Completed
```

6. Click **Finish** to exit the wizard.



D-View 8 2.0.0.26 Setup

Completing the D-View 8 2.0.0.26 Setup Wizard

D-View 8 2.0.0.26 has been installed on your computer.

Click Finish to close this wizard.

☑ Launch D-View 8

7. To verify the current version of the application, open the application by logging in through a browser, see 3.2 Launch the D-View 8 Web GUI.

8. In the application interface, navigate to **System** > **About** to view the Software Version.

NOTE: Manual upgrade of remote probes will be required for software versions earlier than 2.0.0. Refer to 2.6.4 Upgrade Remote Probes for more information.

2.4.2. On Linux

The D-View 8 application is upgraded from time to time to enhance the performance and functionality of the software. Upgrading the software can be done by downloading a newer version of the full installation package.

The following shows how to upgrade the application through an installation package.

1. Log in with the `su` command to have root access.
2. Download the latest D-View 8 upgrade package from the D-View 8 website.
3. Go to the root directory.
4. Locate the package file and unpack it:

```
dpkg -i -G D-View_8_2.0.0.26_installation.deb
```

To continue with the update process, the application service must be stopped.

At the prompt, enter **y** to stop the service.

```
Choose whether to stop D-View 8 Services? [y/n]
```

5. Once the service is stopped, a prompt displays to confirm the input IP. Enter the local IP address.

For Standalone versions:

6. Select the type of MongoDB type, enter 1 to select standalone MongoDB.

```
You intend to use: 1. standalone MongoDB; 2 MongoDB cluster[1/2]
```

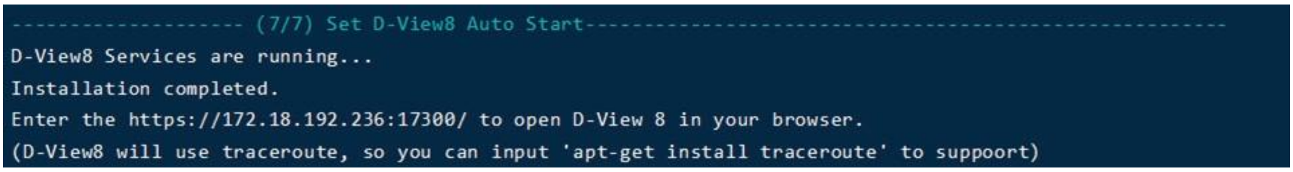
7. Select if a new MongoDB is required, enter n to skip a new installation:

```
If you need to install a new MongoDB. [y/n]
```

8. If a current MongoDB is installed, enter y to select the installed instance:

```
The system detects that you have MongoDB installed, do you want to use it? [y/n]
```

The update process continues and once complete, the application can be opened through a web browser. The application’s corresponding IP address is listed as seen in the following figure.



```
-------------------- (7/7) Set D-View8 Auto Start-------------------------------------------------------
D-View8 Services are running...
Installation completed.
Enter the https://172.18.192.236:17300/ to open D-View 8 in your browser.
(D-View8 will use traceroute, so you can input 'apt-get install traceroute' to suppoort)
```

For Cluster versions:

1. Select the MongoDB type, enter 2 to select MongoDB cluster.

```
You intend to use: 1. standalone MongoDB; 2 MongoDB cluster[1/2]
```

2. To view the current software version, enter the following in the command line:

```
dpkg -s dview8
```

3. Auto upgrade is supported through the remote probe.

2.5 Uninstallation

2.5.1. Uninstall under Windows

Before the application can be uninstalled, close the application before starting the uninstallation process.

NOTE: The screens and instructions may vary depending on the Windows operating system.

1. To uninstall, click **Windows**> **Start Menu**> **Programs** > **D-Link** > **D-View 8** and locate the Uninstall shortcut.
2. Click on the D-View 8 program shortcut to start the uninstallation process.
3. Follow the instructions as directed by the uninstallation wizard.

2.5.2. Uninstall under Linux

Before the application can be uninstalled, close the application before starting the uninstallation process.

1. Logon with the `su` command to obtain root access rights.
2. Enter the following command to stop the services: dpkg -P dview8.
3. The D-View 8 services must be stopped to continue, at the prompt enter y to stop the service and continue.

```
Choose whether to stop D-View 8 Services? [y/n]
```

4. The configuration files are purged from the application. A prompt to delete the database displays. At the prompt,

enter y to delete MongoDB:

```
Do you want to delete mongodb? [y/n]
```

The application is uninstalled.

2.6 Software Migration

Migrating your D-View 7 to D-View 8 version requires the completion of the following:

- Migrate the D-View 7 to D-View 8 database
- Upgrade the D-View 7 to D-View 8 probes

NOTE: The system does not support the migration from D-View 7 to D-View 8 2.0 and later versions. You need to upgrade your D-View 7 to D-View 8 Version 1.0.3.39 first.

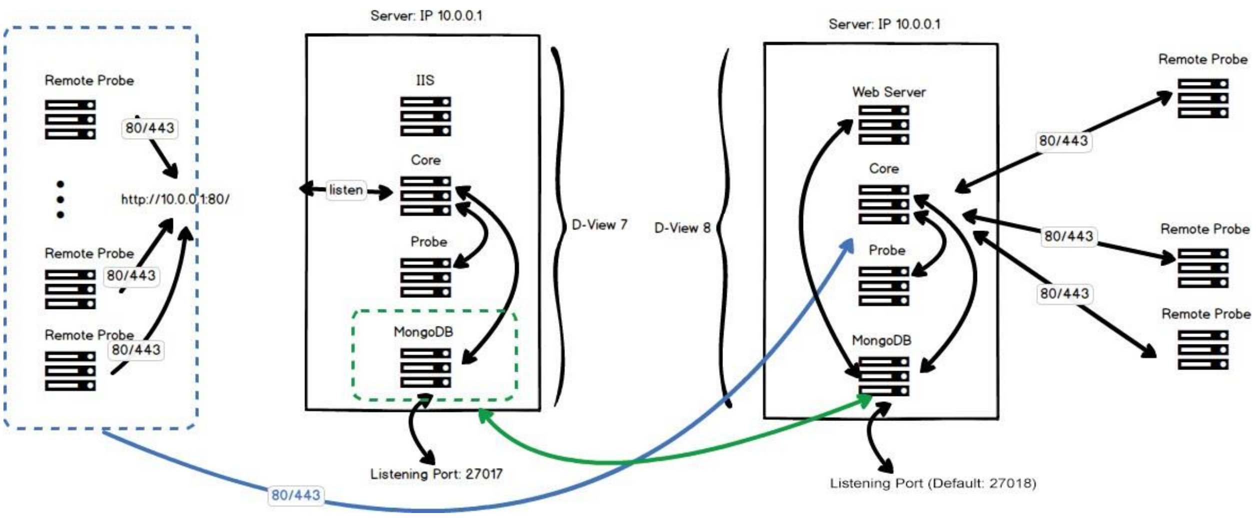
The entire migration process can be performed through the D-View 8 web interface, see **System > D-View 7 Upgrade** in the application interface menu.

Before you start, make sure your anti-virus software is disabled throughout the migration process.

NOTES: Migration to D-View 8 involves the following changes to the system:

1. The role and privilege will be converted to the D-View 8 structure (User Management).
2. Probe settings will be converted to D-View 8 configuration (Sites and Networks).
3. Sensor settings will be converted to D-View 8 configuration (Monitor & Alarm Settings).

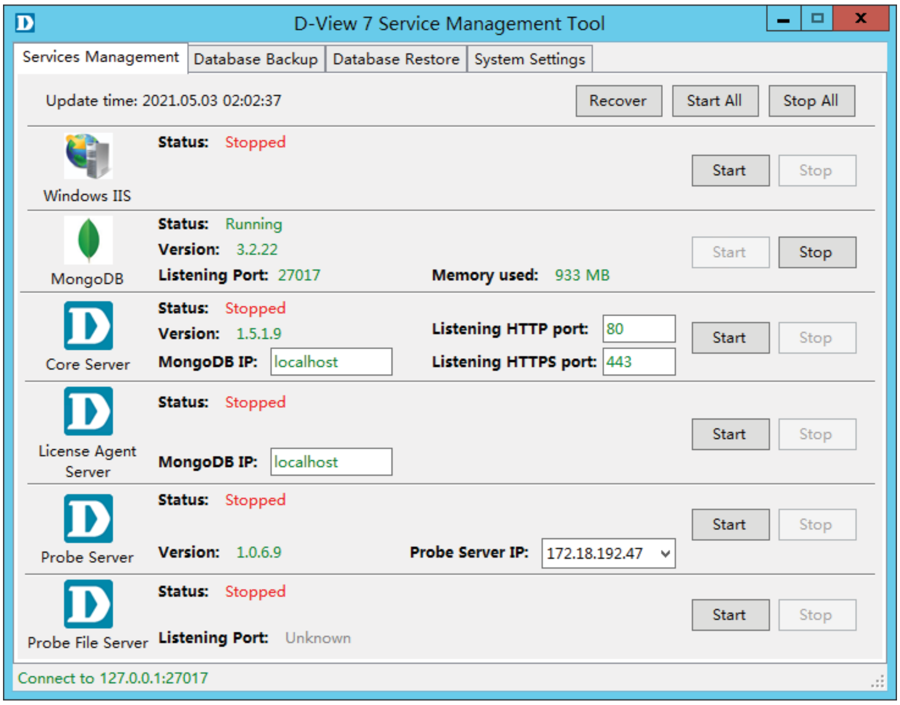
2.6.1. D-View 7 and D-View 8 Architecture



2.6.2. Install D-View 8 on a New Server

NOTE: The D-View 8 and D-View 7 can be installed on different servers. If you would like to install D-View 8 on a D-View 7 server, refer to Install D-View 8 on the Original D-View 7 Server.

1. Open the D-View 7 Service Management Tool.
2. In the Services Management tab, click **Stop** to stop the following D-View 7 services: Windows IIS, Core Server, License Agent Server, Probe Server, and Probe File Server. However, *do not* stop the MongoDB server.



D-View 7 Service Management Tool

Services Management | Database Backup | Database Restore | System Settings

Update time: 2021.05.03 02:02:37 — Recover | Start All | Stop All

Windows IIS — Status: Stopped — Start | Stop

MongoDB — Status: Running; Version: 3.2.22; Listening Port: 27017; Memory used: 933 MB — Start | Stop

Core Server — Status: Stopped; Version: 1.5.1.9; MongoDB IP: localhost; Listening HTTP port: 80; Listening HTTPS port: 443 — Start | Stop

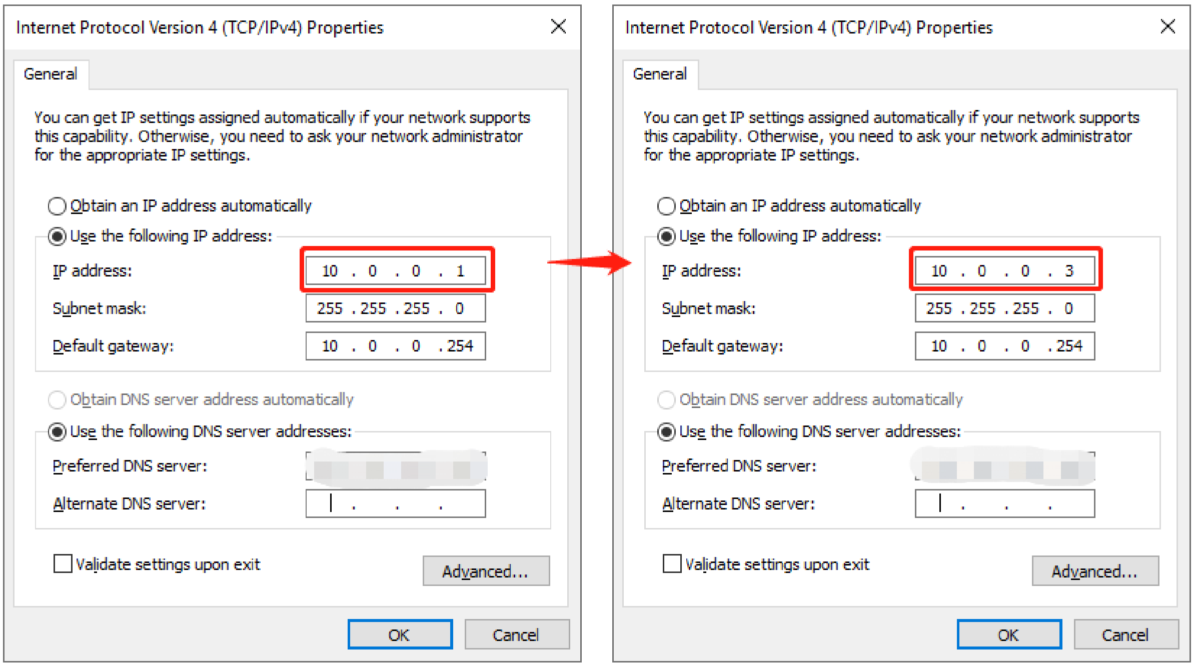
License Agent Server — Status: Stopped; MongoDB IP: localhost — Start | Stop

Probe Server — Status: Stopped; Version: 1.0.6.9; Probe Server IP: 172.18.192.47 — Start | Stop

Probe File Server — Status: Stopped; Listening Port: Unknown — Start | Stop

Connect to 127.0.0.1:27017

3. Change the D-View 7 server's IP address so as to use the current server IP address for the new D-View 8 server. For example, if the IP address is 10.0.0.1, change it to 10.0.0.X, where X is a value other than 1. We use the IP address 10.0.0.3 for demonstration on Windows:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: [redacted]

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK | Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 3

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: [redacted]

Alternate DNS server: . . .

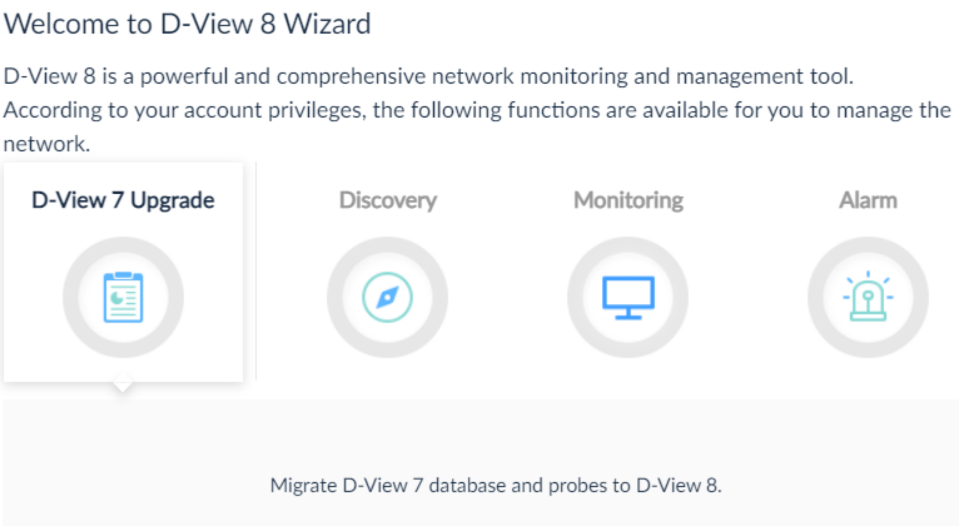
□ Validate settings upon exit

Advanced...

OK | Cancel

4. Download the D-View 8 package to your local directory.
5. Click on the installation package to begin installing the D-View 8 package. See Installation for more information.
6. The core listening port must be configured to use the D-View 7 port instead. (By default, the D-View 7 listening port is set to 80 while the D-View 8 port is set to 17500.) To do this, in the Port Configuration page, locate the Core Port field and change the value to 80.
7. Click **Check** to validate the configuration setup. If a connection can be established, the Check Pass! notification displays. Otherwise, check the settings and run the validation process.

8. Click **Next** to continue the process of installing the D-View 8 server.
9. Once the installation of the D-View 8 server is complete, log in to the application interface. See 3.1 Login and Basic Configurations.
10. The D-View 8 Wizard will be displayed as shown below after you log in.



Welcome to D-View 8 Wizard

D-View 8 is a powerful and comprehensive network monitoring and management tool.
According to your account privileges, the following functions are available for you to manage the network.

Migrate D-View 7 database and probes to D-View 8.

11. In the Wizard, click **D-View 7 Upgrade** to begin the process. This will migrate the D-View 7 database and probes to the D-View 8 server.

	NOTE: The wizard will start by asking you to enter your organization name, do *not* skip this step as subsequent Network Discovery requires this information being set.

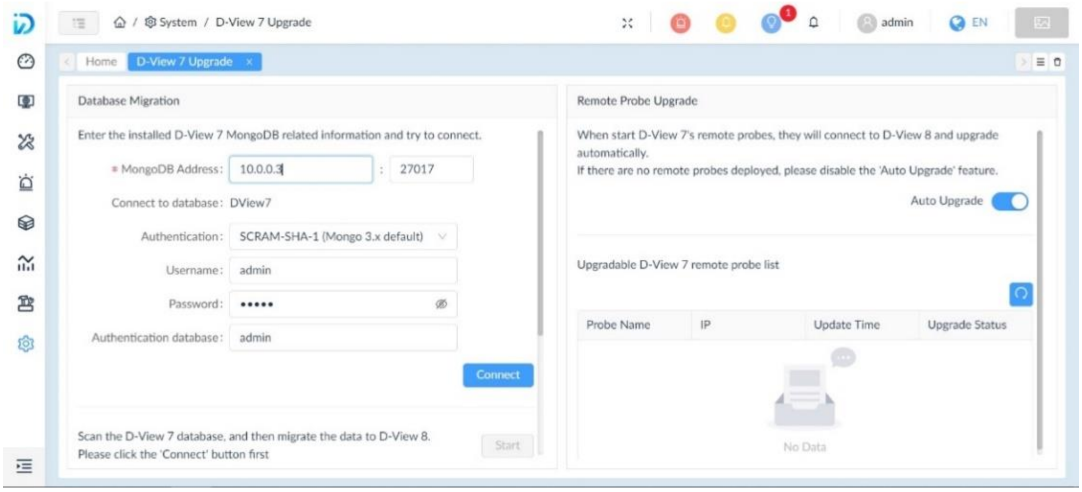
The Database Migration page displays.

The following settings are required to establish a connection to the D-View 7 MongoDB server:

- In the MongoDB Address field, enter the new IP address and port as previously configured, see previous steps: IP address: 10.0.0.3/ Port: 27017
- If the D-View 7 MongoDB server was installed using the D-View 7 installation wizard, click the Authentication drop-down menu and select SCRAM-SHA-1 (Mongo 3.x default). Otherwise, select **None**.
- In the Username field, enter the registered profile with administration access (admin).
- Enter the corresponding password for the registered admin profile.
- In the Authentication database field, enter admin.

	NOTE: If the Connection attempt fails, select None under Authentication and attempt to establish the connection once again.

12. Click **Connect** to initiate the connection with the D-View 7 MongoDB server.



Database Migration

Enter the installed D-View 7 MongoDB related information and try to connect.

* MongoDB Address: 10.0.0.3 : 27017

Connect to database: DView7

Authentication: SCRAM-SHA-1 (Mongo 3.x default)

Username: admin

Password: •••••

Authentication database: admin

Scan the D-View 7 database, and then migrate the data to D-View 8.
Please click the 'Connect' button first

Remote Probe Upgrade

When start D-View 7's remote probes, they will connect to D-View 8 and upgrade automatically.
If there are no remote probes deployed, please disable the 'Auto Upgrade' feature.

Auto Upgrade

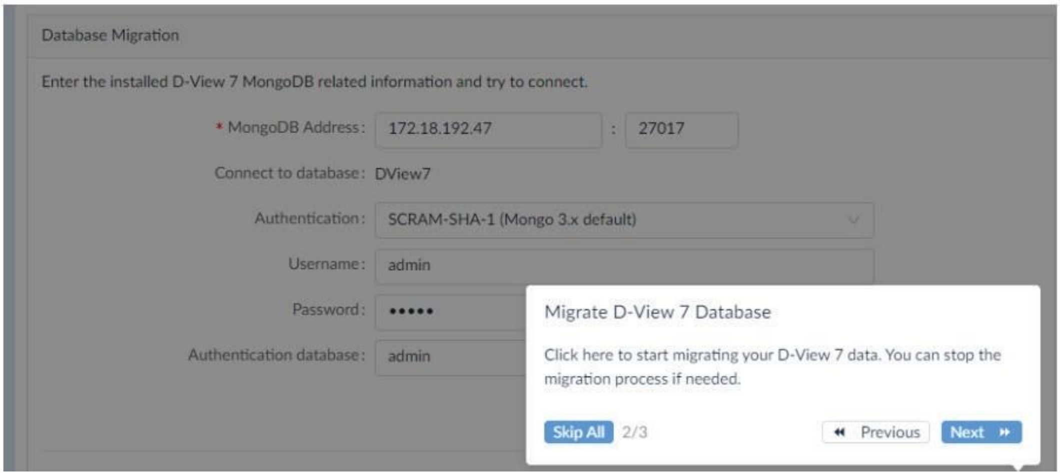
Upgradable D-View 7 remote probe list

Probe Name	IP	Update Time	Upgrade Status

13. The Migrate D-View 7 Database pop-up screen displays. Click **Start** to begin the migration. The wizard provides step-by-step guidance for the process.

14. Click **Next** to continue, **Previous** to return to the previous step, or **Skip All** to automate the process and compete it.

NOTE: If interruption occurs during the migration process, restart the process by clicking **System** > **D-View 7 Upgrade**.



Database Migration

Enter the installed D-View 7 MongoDB related information and try to connect.

* MongoDB Address: 172.18.192.47 : 27017

Connect to database: DView7

Authentication: SCRAM-SHA-1 (Mongo 3.x default)

Username: admin

Password: •••••

Authentication database: admin

Migrate D-View 7 Database

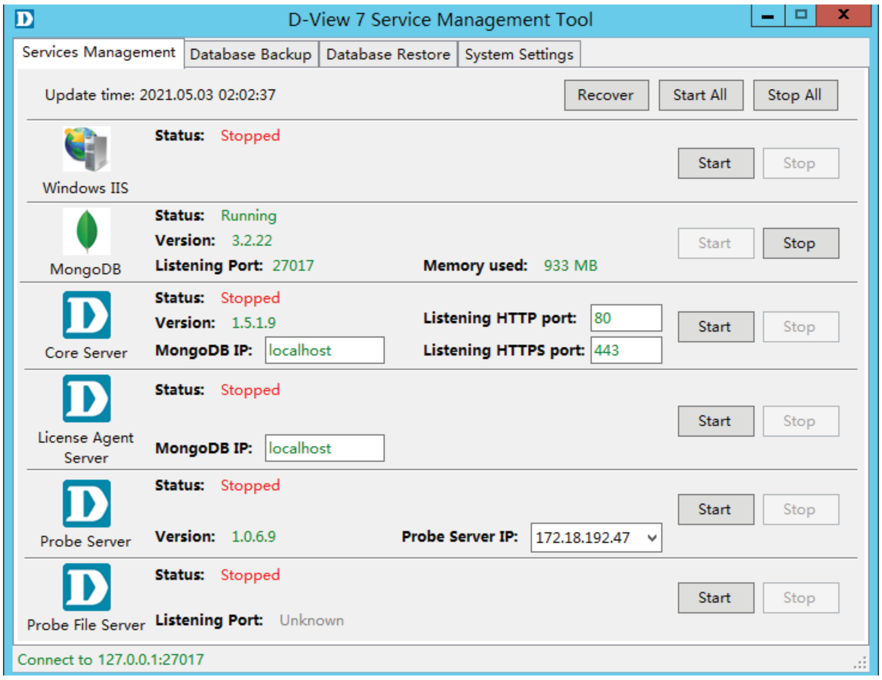
Click here to start migrating your D-View 7 data. You can stop the migration process if needed.

Once the process is completed, the D-View 7 local probes will be upgraded and replaced; however, you need to manually upgrade the remote probes (refer to 2.6.4 Upgrade Remote Probes.) Moreover, the data of the original D-View 7 MongoDB is retained and imported to the D-View 8 database.

2.6.3. Install D-View 8 on the Original D-View 7 Server

1. Open the D-View 7 Service Management Tool.

2. In the Services Management tab, click **Stop** to stop the following D-View 7 services: Windows IIS, Core Server, License Agent Server, Probe Server, and Probe File Server. However, *do not* stop the MongoDB server.



Update time: 2021.05.03 02:02:37

Windows IIS — Status: Stopped

MongoDB — Status: Running; Version: 3.2.22; Listening Port: 27017; Memory used: 933 MB

Core Server — Status: Stopped; Version: 1.5.1.9; MongoDB IP: localhost; Listening HTTP port: 80; Listening HTTPS port: 443

License Agent Server — Status: Stopped; MongoDB IP: localhost

Probe Server — Status: Stopped; Version: 1.0.6.9; Probe Server IP: 172.18.192.47

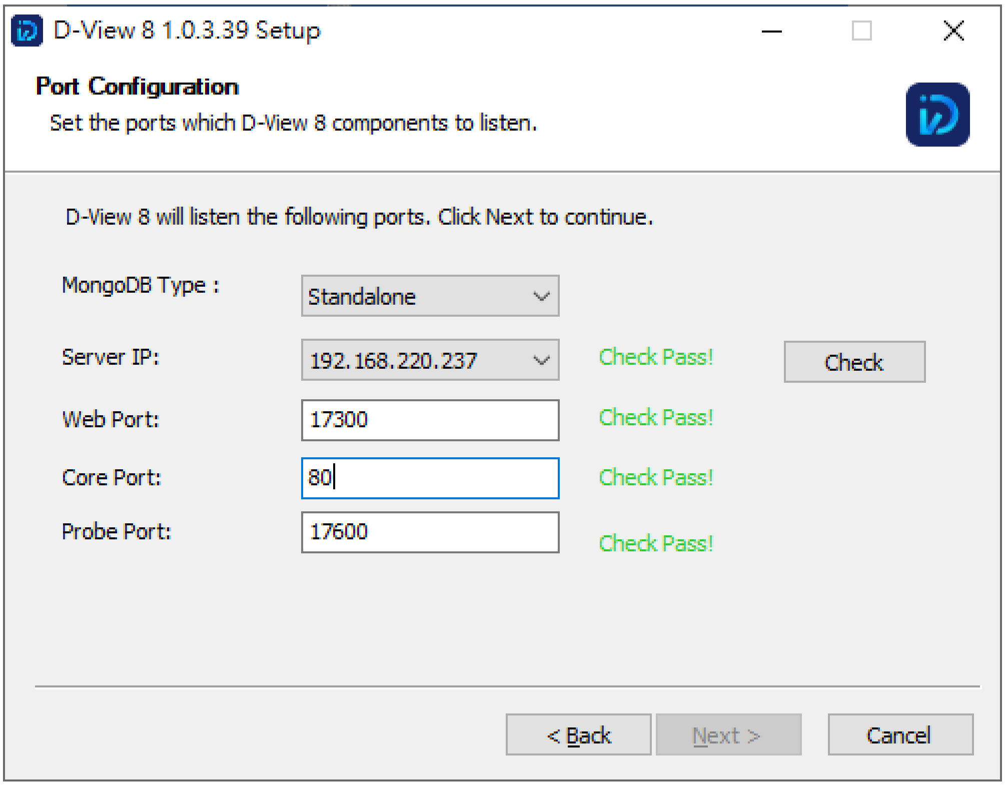
Probe File Server — Status: Stopped; Listening Port: Unknown

Connect to 127.0.0.1:27017

3. Download the D-View 8 package to a local directory.

4. Click on the installation package to begin the installation process. See **2 Installation** for further information.

5. The core listening port must be configured to use the D-View 7 port. (By default, the D-View 7 listening port is set to 80 while the D-View 8 port is set to 17500.) To do this, in the Port Configuration page, locate the Core Port field and change the value to 80.



Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Standalone

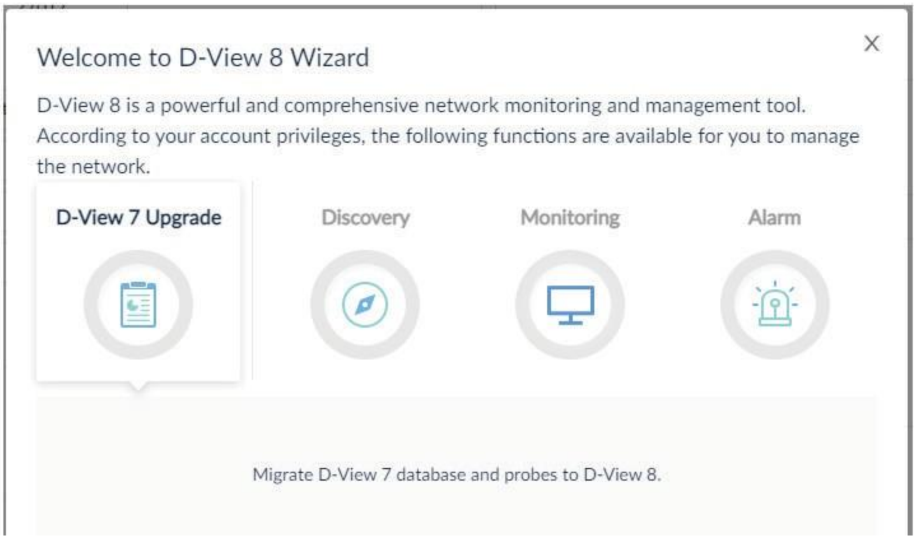
Server IP: 192.168.220.237 Check Pass!

Web Port: 17300 Check Pass!

Core Port: 80 Check Pass!

Probe Port: 17600 Check Pass!

6. Click **Check** to validate the configuration setup. If a connection can be established, the Check Pass! notification displays. Otherwise, check the settings and run the validation process.
7. Click **Next** to continue with the installation process and follow the installation wizard to completely setup thenew server.
8. Once the installation of the D-View 8 server is complete, log in to the application interface. See 3.1 Login and Basic Configurations.
9. The D-View 8 Wizard panel will be displayed as shown below after you log in.



Welcome to D-View 8 Wizard

D-View 8 is a powerful and comprehensive network monitoring and management tool. According to your account privileges, the following functions are available for you to manage the network.

Migrate D-View 7 database and probes to D-View 8.

10. In the Wizard panel, click **D-View 7 Upgrade** to begin the process. This will migrate the D-View 7 database and probes to the D-View 8 server.

The Database Migration page displays.

The following settings are required to establish a connection to the D-View 7 MongoDB server:

- In the MongoDB Address field, enter the IP address and port of the MongoDB server (the localhost):

  IP address: 127.0.0.1

  Port: 27017

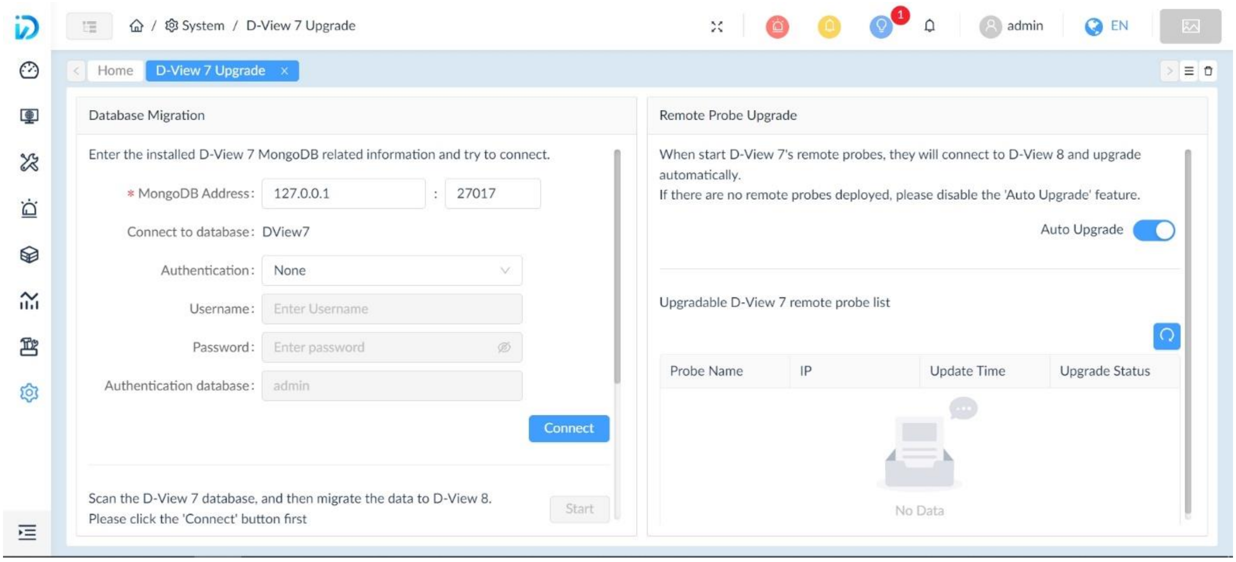
- If the D-View 7 MongoDB server was installed using the D-View 7 installation wizard, click the Authentication drop- down menu and select SCRAM-SHA-1 (Mongo 3.x default).

  Otherwise select **None**.

- In the Username field, enter the registered profile with administration access (admin).
- Enter the corresponding password for the registered admin profile.
- In the Authentication database field, enter admin.

NOTE: If the Connection attempt fails, select None under Authentication and attempt to establish the connection once again.

11. Click **Connect** to initiate the connection with the D-View 7 MongoDB server.



Database Migration

Enter the installed D-View 7 MongoDB related information and try to connect.

* MongoDB Address: 127.0.0.1 : 27017

Connect to database: DView7

Authentication: None

Username: Enter Username

Password: Enter password

Authentication database: admin

Connect

Scan the D-View 7 database, and then migrate the data to D-View 8.
Please click the 'Connect' button first

Start

Remote Probe Upgrade

When start D-View 7's remote probes, they will connect to D-View 8 and upgrade automatically.
If there are no remote probes deployed, please disable the 'Auto Upgrade' feature.

Auto Upgrade

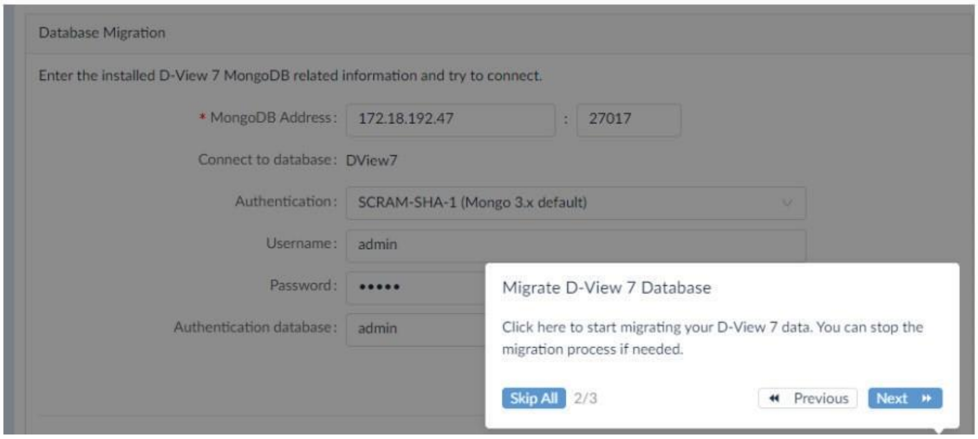
Upgradable D-View 7 remote probe list

Probe Name	IP	Update Time	Upgrade Status

No Data

12. The Migrate D-View 7 Database pop-up screen displays. Click Start to begin the migration. The wizard provides step-by-step guidance for the process.
13. Click **Next** to continue, **Previous** to return to the previous step, or **Skip All** to automate the process and complete it.

NOTE: In the event of an interruption in the migration process, restart the process by clicking **System** > **D-View 7 Upgrade**.


Database Migration

Enter the installed D-View 7 MongoDB related information and try to connect.

* MongoDB Address: 172.18.192.47 : 27017

Connect to database: DView7

Authentication: SCRAM-SHA-1 (Mongo 3.x default)

Username: admin

Password: •••••

Authentication database: admin

Migrate D-View 7 Database

Click here to start migrating your D-View 7 data. You can stop the migration process if needed.

Once the process is completed, the D-View 7 local probes will be upgraded and replaced; however, you need to manually upgrade the remote probes (refer to 2.6.4 Upgrade Remote Probes). Moreover, the data of the original D-View 7 MongoDB is retained and imported to the D-View 8 database.

NOTE: After successful migration, it is necessary that the corresponding ports used in D-View 7 being stopped while D-View 8 is running. Stop these services: World Wide Web Publishing Service (Windows built-in service), D-View7 CoreServer, D-View 7 License Agent Server, D-View 7 Probe File Server, and D-View7 Probe Server. To manage services on Windows, Select **Start**, and type **services**. Then click a service in the list and click an action button at the top to start, stop, pause, or resume it.

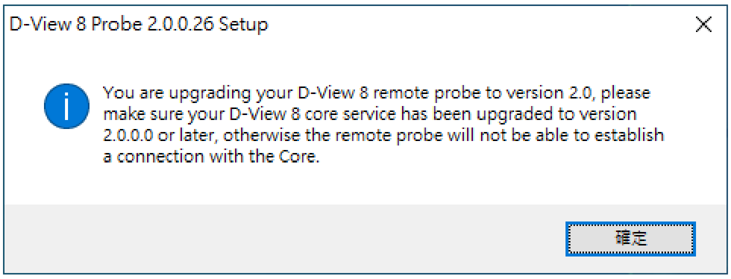
2.6.4. Upgrade Remote Probes

NOTE: Manual upgrade of remote probes will be required for software versions earlier than 2.0.0.

After the upgrade process is completed with the wizard of the web application, perform manual upgrade for all remote probes.

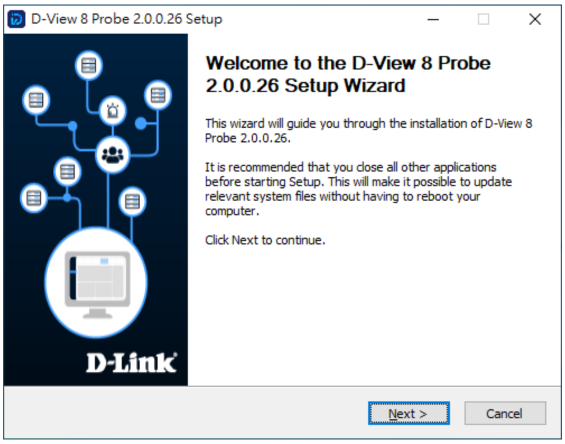
1. Check the connection status and the IP addresses of the remote probes: go to **System > Server Management** and select the **Probe** tab. The core server and remote probes information can be obtained from the probe list. Note that the remote probes are displayed in red color to indicate disconnection with the core server.

2. Install the probe package on the remote probes by double-clicking on the installation file. A warning message states that it is necessary that you have upgraded the core server to the intended version before upgrading your remote probes to this same version.



You are upgrading your D-View 8 remote probe to version 2.0, please make sure your D-View 8 core service has been upgraded to version 2.0.0.0 or later, otherwise the remote probe will not be able to establish a connection with the Core.

3. Click **Next** when the Welcome page displays.



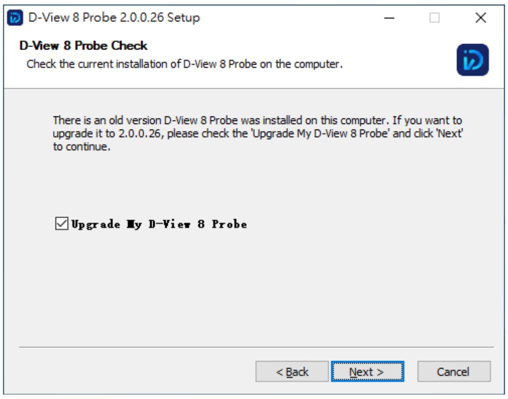
Welcome to the D-View 8 Probe 2.0.0.26 Setup Wizard

This wizard will guide you through the installation of D-View 8 Probe 2.0.0.26.

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

Click Next to continue.

4. The system automatically detects an older version of probe has been installed. Check **Upgrade My D-View 8 Probe** and click **Next** to continue.



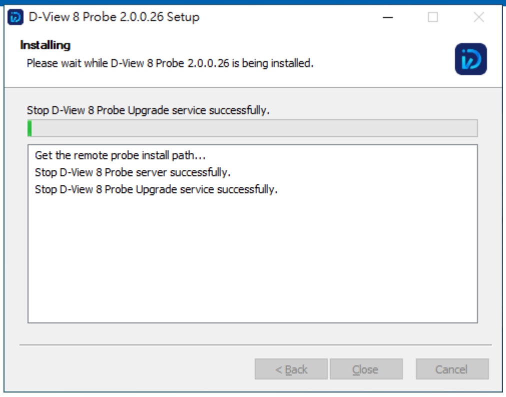
D-View 8 Probe Check

Check the current installation of D-View 8 Probe on the computer.

There is an old version D-View 8 Probe was installed on this computer. If you want to upgrade it to 2.0.0.26, please check the 'Upgrade My D-View 8 Probe' and click 'Next' to continue.

☑ Upgrade My D-View 8 Probe

The installation will progress and completes. The remote probe should be upgraded to the desired version.

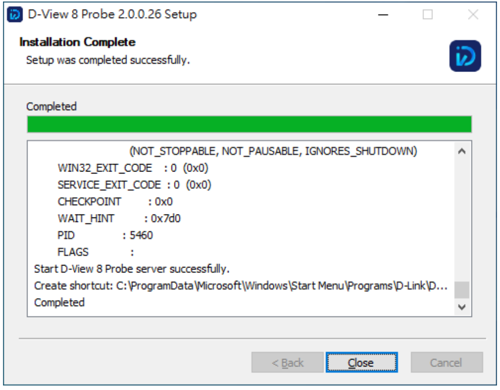


Installing

Please wait while D-View 8 Probe 2.0.0.26 is being installed.

Stop D-View 8 Probe Upgrade service successfully.

```
Get the remote probe install path...
Stop D-View 8 Probe server successfully.
Stop D-View 8 Probe Upgrade service successfully.
```



Installation Complete

Setup was completed successfully.

Completed

```
                  (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE    : 0  (0x0)
      SERVICE_EXIT_CODE  : 0  (0x0)
      CHECKPOINT         : 0x0
      WAIT_HINT          : 0x7d0
      PID                : 5460
      FLAGS              :
Start D-View 8 Probe server successfully.
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\D-Link\D...
Completed
```

You can now go back to the probe list and check the connection status of the remote probes (**System > Server Management** > **Probe**.)

3 Overview and Basics

Before connecting to the D-View 8 server, you need to install the required software package. Please refer to **Chapter 2 Installation** for instructions and procedure.

3.1. Login and Basic Configurations

After you log in to the application, it is highly recommended that you change your password and account information and configure the email settings for alert notifications. Refer to the following sections for more information:

- Launch the D-View 8 Web GUI
- Change User Password
- Configure Email Server for Notification

3.2. Launch the D-View 8 Web GUI

The application is accessible through a browser. Before logging in to the application, make sure that the D-View 8 application is installed on a server with a static IP address.

NOTE: The D-View 8 supports multiple concurrent users. Two users can make changes to the same page at the same time. To avoid management discrepancy, it is recommended that users coordinate management activities in advance.

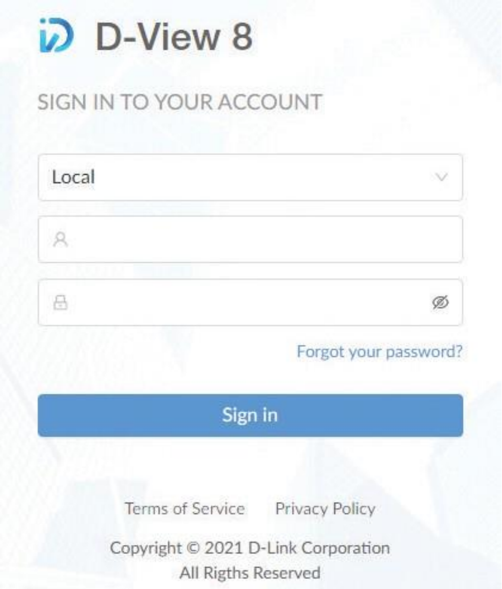
To log in to the application:

1. Open a browser and enter the assigned IP address of the D-View 8 server.

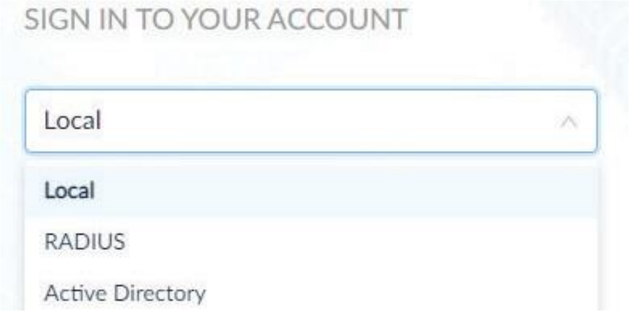
   - If connecting to the same D-View 8 server in which the application is installed, enter localhost and the default port 17300:

     https://localhost:17300.

   If connecting from a remote computer, enter the IP address of the D-View 8 server into the address field of the browser. Before connecting to the D-View 8 server, clear browser cache data. The Sign-in page appears.

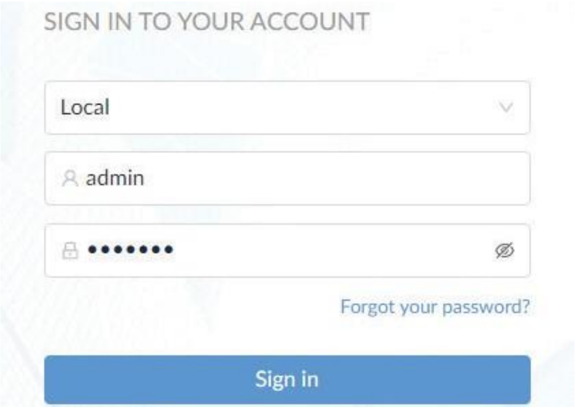


2. In the account type menu, select the account type of the user:
   - **Local:** user account authenticated on a local system.
   - **RADIUS:** user accounts authenticated by the Remote Authentication Dial-In User Service.
   - **Active Directory**: user accounts authenticated by Microsoft® Active Directory.



3. Enter an account name and a password.

By default, the administrator’s username is **admin** and the default password is also **admin**.

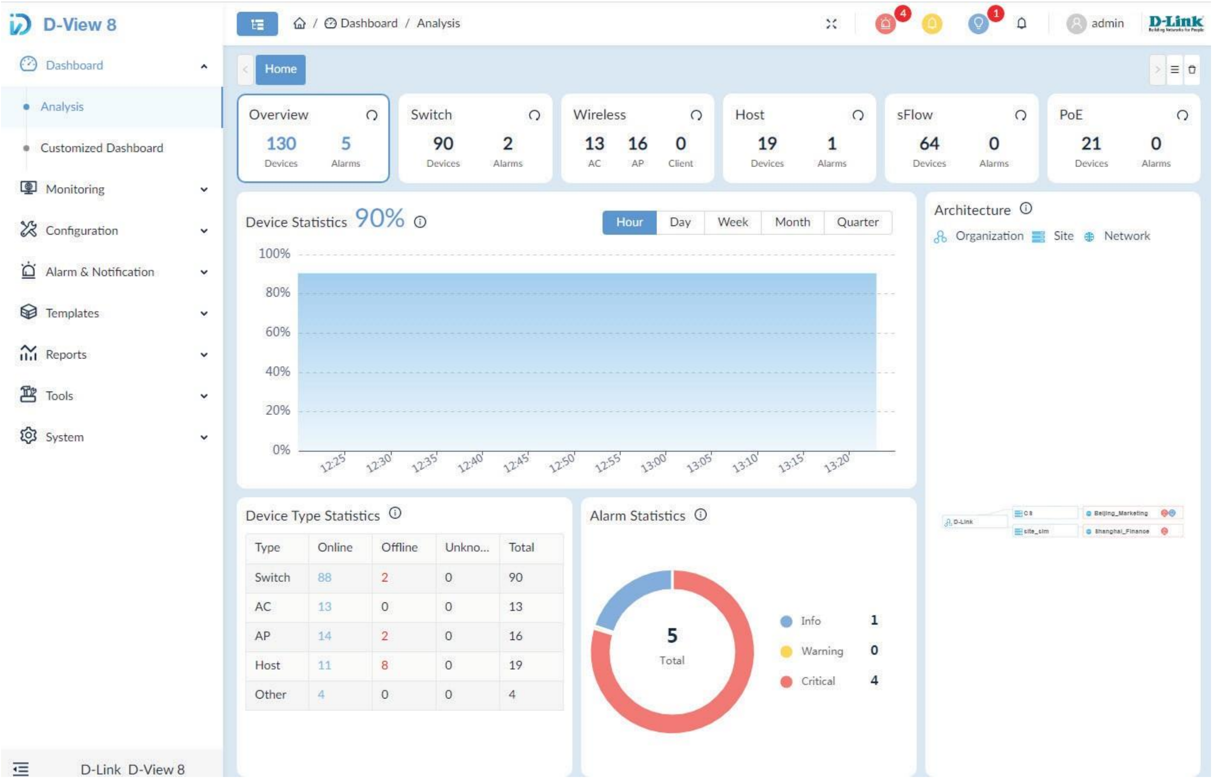

SIGN IN TO YOUR ACCOUNT

Local

admin

•••••••

4. Click the **Sign In** button to continue. The D-View 8 Dashboard displays.



Type	Online	Offline	Unkno...	Total
Switch	88	2	0	90
AC	13	0	0	13
AP	14	2	0	16
Host	11	8	0	19
Other	4	0	0	4

For more information on the **Dashboard**, refer to **3.3 Overview of the Web Dashboard** below.

First Time Login

When a Super Administrator logs into the application for the first time with the above username and password, a wizard will appear. Please select the **Discovery** tab to set up an organization and discover networks with the following guided steps:

1. Enter the fields required to fill in information for your organization.

2. Click **+ Add Network** to open the “Add Network” window.

3. Enter the following information to create a network:

   Network Name: Enter a name for the network.
   Site Name: Enter a name for the site.

4. Select the probes. A Primary probe will be required to discover and communicate with devices in the network.

5. Click **+ Add Discovery Range**. The discovery range can be specified with the following methods: IP, IP Range, Subnet, or Import CSV File. Refer to 4.1 Network Discovery for more information.

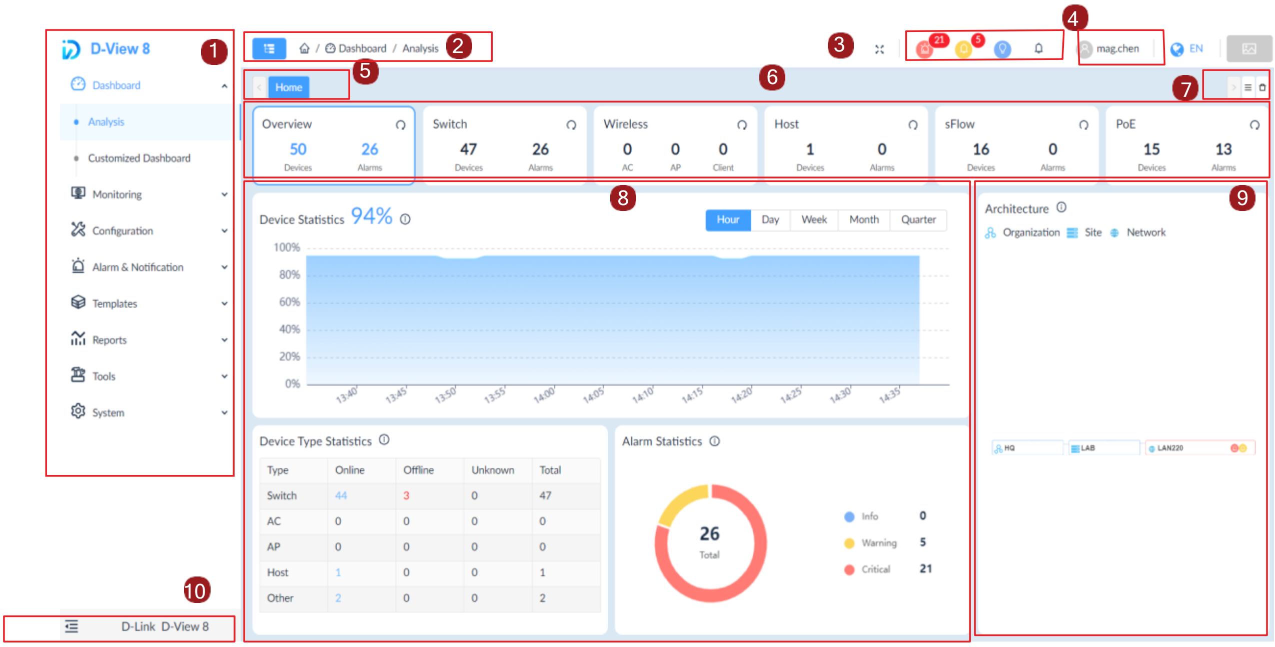
6. Click the SNMP field and select **Add SNMP Credential**. SNMP is the required protocol for device management.

7. Click Save to save the settings for network discovery.

Please wait while the system is discovering devices in the defined network.

3.3. Overview of the Web Dashboard

The D-View 8 Dashboard features and functionality can be accessed through the menus and toolbar of the web interface. The availability of the tools is determined by a user's role.



Device Type Statistics

Type	Online	Offline	Unknown	Total
Switch	44	3	0	47
AC	0	0	0	0
AP	0	0	0	0
Host	1	0	0	1
Other	2	0	0	2

Web Dashboard Annotations			
1.	Main menu	2.	Title bar
3.	Annunciators	4.	User Profile and Wizard
5.	Menu tab	6.	Widget menu
7.	Tab selector	8.	Widget information
9.	Architecture diagram	10.	Collapse/expand sidebar

3.3.1. Common Features

There are several features that are common on the D-View 8 dashboard regardless of the user privilege and license type.

- **Menus** are used to access tools and configurations.
  - Sort and Filter functions help you refine table data.
  - Configuration menus help you access features that are available on a configuration page, which can be accessed through toolbar buttons.
- **Help** menus can be opened by clicking ⓘ to obtain additional information relevant to the displayed page.
- **Toolbars** give quick access to the functions or pages of corresponding menu options.
- **Annunciators** offer visual notification of system state or alarms.

3.3.2. Menus and Toolbars

The following section describes the menu and toolbar options available through the D-View 8 dashboard. The menu items are listed along with the corresponding submenus and description.

NOTE: Menu and toolbar options vary depending on the user role, license type, and device type.

System Configuration

Item	Description
Basic Settings	• Organization ▪ Configures the organization’s name, country, time zone, etc. ▪ Upload the organization logo in PNG or JPG file format (less than 2MB file size) • Mail Server Settings ▪ Configures mail server settings • Forward Trap ▪ Configures the trap receiver to send incoming device trap messages • Forward Syslog ▪ Configures the system log receiver to send device syslog messages • REST API ▪ Generating an API key which will be used by other applications to acquire a token from D-View 8 ▪ Third-party applications can use tokens to acquire needed information from D-View 8 • Credentials ▪ Configures the SNMP protocol types, community name and related parameters ▪ Configures Windows WMI (Windows Management Instrumentation) and SSH/Telnet communication credentials • sFlow Settings ▪ Configures sFlow parameter mapping for different traffic indicators • System Preferences ▪ Configures the table display settings and theme of D-View 8
User Management	• Users ▪ Lists user information: user’s email address, username, login time, authentication type, etc. ▪ Add, delete, remove users. • Role Privileges ▪ Lists the types of user role: Organization/ Site/ Network Administrator roles. ▪ Lists each role’s privileges. • AD Server ▪ Configures the Windows Active Directory Server’s information. • RADIUS Server ▪ Configures the RADIUS Server’s information. ▪ Supports Primary and Secondary RADIUS Server configuration

Item	Description
Scheduling	• Configures the "Recurrent Schedule" and "Time-range Schedule" • Recurrent Schedule List ▪ Allows users to configure recurrent schedules with customized frequency and duration • Time-range Schedule List ▪ Allows users to configure a specific range of time of a designated weekday or weekdays
Server Management	• Monitors the status of D-View Core Server, Web Server and Probe • Checks the real-time report of server's status, which includes the utilization of CPU, memory, hard drive, and the network traffic
D-View 8 Log	• D-View 8 features three types of logs: User Operation Log, System Log, and Device Maintenance Log • User Operation Log: ▪ Records user operational activity via web interface • System Log: ▪ Keeps the records of D-View 8's running status of servers and probes • Device Maintenance Log: ▪ Keeps configuration activity logs for devices
D-View 7 Upgrade	• Support for the following upgrade functions: • Database Migration • Remote Probe Upgrade
About Page	• The About page keeps the following information: • D-View 8's edition: Standard or Enterprise • Brief description for the purchased edition • Software version • The latest update time • The number of supported and used nodes • System uptime information • Product license information and activation link • Remaining days of the maintenance license and the license activation link

Dashboard

Item	Description
Analysis	• By default, there are six tabs representing major topics or device types in the analysis page: ▪ Overview ▪ Switch ▪ Wireless ▪ Host ▪ sFlow ▪ PoE • Provides an overview of alarm statistics, online/offline status of the devices, CPU/memory utilization, performance report, device health, etc. • The information varies according to device type
Customized Dashboard	• Customizable dashboard to display specific information

Monitoring

Item	Description
Network Discovery	• Configures network discovery parameters, which include: ▪ Basic Information: the name of the network and site to discover. ▪ Probe Mode: Choose the primary and secondary probe ▪ Discovery Range: Define the range that may include a single IPv4/v6 address, an IPv4/v6 address range, an IPv4/v6 subnet, or import of IP ranges from a file ▪ Schedule: Define the discovery schedule that may include one-time discovery or recurrent discovery • Displays discovery jobs' running status and related information
Device View	• Includes 5 categories: All, Managed, Unmanaged, Ignored and Conflicted • Displays a summary and detailed information of the devices • Detailed information can be accessed via the "System Name" link, which also allows login to a device using different protocols
Interface View	• List of devices' network connection properties, which includes: ▪ System/Model Name ▪ Device's IP address ▪ Interface and MAC address information ▪ VLAN information ▪ Update time information • Each of the above can be searched to find a specific device
Topology Map	• Displays connections between devices for the entire network, site or organization • Displays the online/offline status of devices • Displays link information of devices • PNG or JPG format files can be uploaded as the topology's background image • Supports Star, Tree, Circular and Grid topology layout • Zoom in and out the topology map • Supports customized topologies
Connection View	• List of the interface link information which includes: ▪ Link status ▪ Link name ▪ Name and IP address of the connected devices ▪ The connected interfaces of the devices ▪ The connected devices and interface information ▪ Traffic statistics of TX and RX ▪ Link utilization ▪ Link type (LACP or general) ▪ Link's related info such as update time ▪ Source of the detection, such as LLDP or FDB • Clicking the link interface name, more detailed information will be displayed, such as: ▪ Summary information of the selected link ▪ Monitor information of the selected link ▪ Alarm information of the selected link

Rack View	▪ Provides visualization of the device rack
sFlow Analyzer	• Collects the sFlow data from devices and generates related statistics reports • The statistics report information includes: ▪ Report based on the source or destination of packets ▪ Report based on QoS rules ▪ Report based on layer 4 applications ▪ Report based on protocols • Report based on conversation of two endpoints
Device Group	• Allows users to create device groups to simplify management tasks

Configuration

Item	Description
Batch Configuration	• Allows simultaneous configuration of multiple devices' parameters at the same time • Two sub-features: • Quick Configuration: a template for each function to apply the settings to multiple devices • Advanced Configuration: a profile for a specific type of device. The profile contains configurations of multiple features. Users can apply the profile to multiple devices of the same type/model.
Task Management	• Lists all created tasks to show the execution result with messages indicating a success or failure. It includes both Current and Historical Tasks. If a failure occurs, it will also state the reason of failure.
Firmware Management	• Management of devices' firmware centrally • Schedule-based updates of device firmware
Configuration Management	• Management of device configuration • Backup or restore of multiple device configuration files at the same time • Schedule-based backup or restore • Supports file baselining
File Management	• File comparison of configuration files to verify the differences • Upload of configuration or firmware files on D-View • Set the configuration file as the baselined file for easy comparison or version tracking

Alarms & Notifications

Item	Description
Alarms	• Displays all alarm information collected from network devices. The alarms include: • Active Alarms ▪ Lists all unacknowledged network alarms • Historical Alarms ▪ Lists all acknowledged network alarms
Trap & Syslog	• Displays the trap and system log receiving from devices. The trap log's information contains: ▪ Time received ▪ Device system name ▪ Device IP address ▪ SNMP version ▪ Generic type ▪ Trap description ▪ Original message of the trap • The syslog information contains: ▪ Time received ▪ System name of device generating the log ▪ Device IP address ▪ Syslog severity levels ▪ Syslog messages ▪ The associated alarm for the syslog ▪ The site and network of the device
Trap & Syslog Editor	Edits OID description for a specific trap OID Edits syslog description with matched keywords
Monitor & Alarm Settings	• Monitor Settings ▪ Configure the monitor status and interval for data collection • Alarm Settings ▪ Configure alarm rules to generate alarms with threshold values ▪ Configure the CLI commands for devices and D-View 8 servers to execute when the alarm is triggered ▪ Define the alarm properties for customized monitors and alarms
Notification Center	• Allows users to set the notification method when alarms are triggered: Web Scrolling Message, Email, and Execute script.

Templates

Item	Description
Device Template	• Add a device to be managed by D-View 8 if it’s not in the managed device list; a useful tool especially for managing third-party devices • Allows users to customize device’s information as the following: ▪ Model Name ▪ Device Type ▪ Vendor Name ▪ Device’s System OID (SOID) ▪ Panel Template • Allows advanced monitoring and configuration for different device models.
Device Support	• Create useful information to manage third-party vendors and devices, which includes: • Vendor ▪ Vendor name ▪ Vendor OID • Device Category ▪ Category name ▪ Photo of the category • Device Type ▪ Type name ▪ Device category ▪ Description
Panel Template	• Includes D-Link default device panel templates and customizable panels • Customizable panel details: ▪ Panel name ▪ Description ▪ Port type: 10G, 5G, 1G,100M, etc. • Customizable panel diagrams: ▪ Panel logo (PNG/JPG files less than 2 MB in size) ▪ Panel height and width • Port numbering scheme • Port layout design
Monitor Template	• Provides different monitoring templates for collection of device information • Multiple monitor templates can be associated with Device Template to monitor specified devices. • Customizable categories to identify specific monitoring data source. The following properties are available for each category: ▪ Category name ▪ Unit (-,°C,%, bits, bps, ms, pps, rpm) ▪ Protocol (WMI, SNMP/ HTTP(S)) ▪ Line chart (not supported, default/supported) ▪ Build type (system / user) ▪ Description ▪ Operation (User type: edit, delete; System type: view only) • Customizable Monitor Template to monitor and collect defined data source ▪ Template name ▪ Category ▪ Vendor name ▪ Monitoring Interval

	▪ Build type ▪ Description • Operation (User: edit, download, delete; System: download, view)
Configuration Template	• Configuration Template: Provides multiple configuration templates to configure devices • Multiple configuration templates can be associated with Device Template to configure devices. • Customizable Configuration Category to classify different configuration types ▪ Category name ▪ Configuration type: quick or advanced ▪ Template description • Customizable Configuration Template to configure specified devices with the following properties: ▪ Vendor name ▪ Template description ▪ Selected configuration template for engineering view ▪ Protocols (SSH/Telnet or SNMP) ▪ CLI commands list (if selected) • Programmable graphical objects to customize layout and control elements

Reports

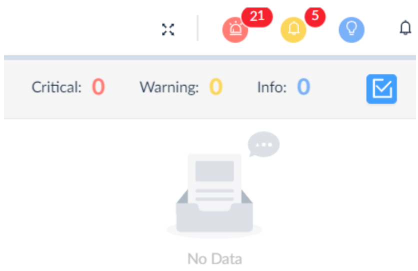
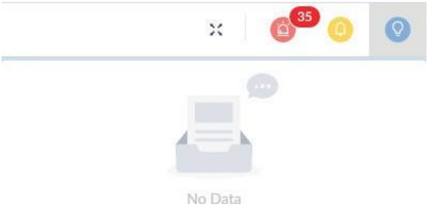
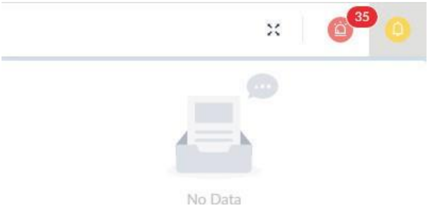
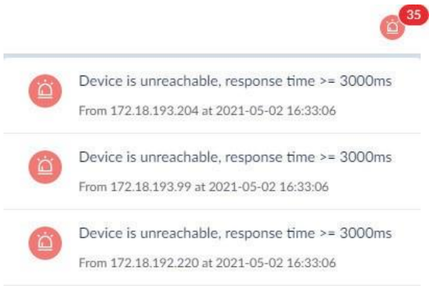
Item	Description
General Reports	Each report type has distinctive configurable parameters such as data source and data collection time interval. When reports are generated, they can be exported immediately, saved to My Report, or upgraded to Scheduled Report . The following types of reports are available: • Device Reports • Device Health • Trap • Syslog • Device Top N • Wired Interface Reports • Wired Traffic • Wired Throughput Top N • Wireless Reports • Wireless Client Count • Wireless Traffic • Advanced Reports • Inventory
Scheduled Reports	• Reports can be a one-time report or recurrent report.
My Reports	The My Reports category displays the saved list of reports categorized as My Reports from the general report category. Up to 500 report entries can be saved.

Tools

Item	Description
MIB Browser	• Retrieves and displays MIB data in readable format • Provides a graphical interface to read MIB information
MIB Compiler	• Compiles device MIB files into D-View 8. The MIB Compiler allows users to compile standard or proprietary MIBs but does not accept malformed MIBs. The compiled MIB file can then be loaded and managed only in the MIB browser.
ICMP Ping	• Checks device operation status and network performance
SNMP Test	• Checks device SNMP capabilities using SNMPv1, SNMPv2c or SNMPv3
Trace Route	• Checks the route and measures transmit delay of packets across the network • Terminal interface for users to connect with the device
Command Line Interface (CLI)	• Terminal interface for users to connect with the device
File Comparison	• Lets user check differences between two configuration files • Differences are highlighted in colors

3.3.3. Annunciator

The Annunciator is typically located at the top right of the application webpage to notify users of the system status. The following are the different types of alarms displayed via the annunciator:

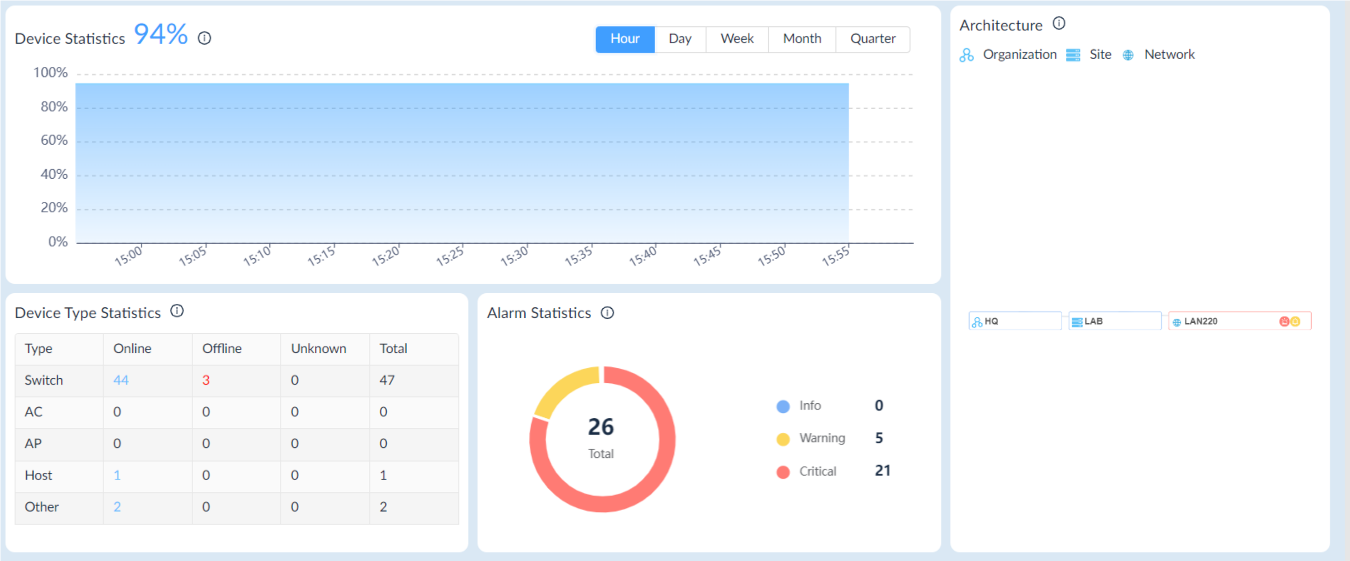
Item	Description	Icon
Notifications	Defined events to send notifications when an alarm is triggered	
Info Alarm	Information regarding system function requiring further attention to maintain proper system operation or to avoid unintended result.	
Warning Alarm	Information regarding system errors or faults that may affect system operation.	
Critical Alarm	Information regarding system errors or faults and requiring immediate attention and remediation to prevent further damage.	 Device is unreachable, response time >= 3000ms From 172.18.193.204 at 2021-05-02 16:33:06 Device is unreachable, response time >= 3000ms From 172.18.193.99 at 2021-05-02 16:33:06 Device is unreachable, response time >= 3000ms From 172.18.192.220 at 2021-05-02 16:33:06

User Menu

Item	Description
User Profile	Displays information about the current user
Wizard	• D-View 7 Upgrade: migrate D-View 7 database and probes to D-View 8 (only available to Super Administrator) • Discovery: discover the network and add devices to the network • Monitoring: create customized topologies, rack display, and customized dashboards • Alarm: customize related network alarms and notifications
Network Discovery Records	Displays the record of the discovered networks
Sign out	Sign out the current user from the application

3.3.4. Workspace Preferences

The D-View 8 workspace starts with a standard configuration displaying the available system and network information. Through the interface, you can quickly obtain the corresponding settings of the information displayed on the dashboard.



Type	Online	Offline	Unknown	Total
Switch	44	3	0	47
AC	0	0	0	0
AP	0	0	0	0
Host	1	0	0	1
Other	2	0	0	2

● Info	0
● Warning	5
● Critical	21

The workspace is designed for complete visibility and control of the entire network.

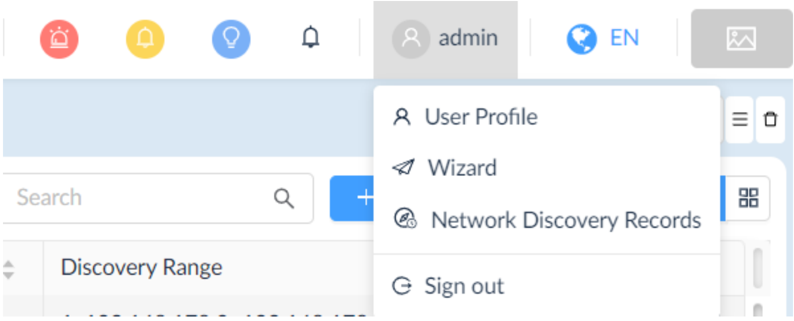
To view specific information, click on the link of the content.

3.4. Change User Password

It is highly recommended that you change your password for better security. An administrator can also create users within his administrative domain (i.e. a Super Admin can create users for an organization, a site, or a network while an Organization Admin can create users for only a site or a network.)

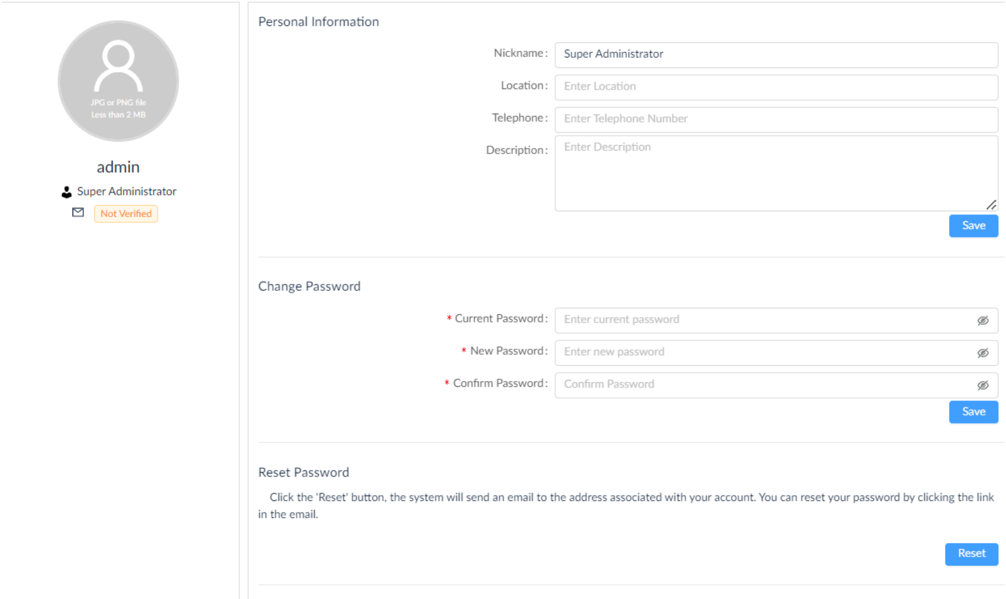
To change your password:

1. Log in to the Dashboard, see 3.2 Launch the D-View 8 Web GUI.
2. Locate the User Profile Menu under the account name.



3. Select **User Profile** to display the user's profile page.

The Personal Information page displays.



JPG or PNG file
Less than 2 MB

admin

Super Administrator

Not Verified

Personal Information

Nickname : Super Administrator

Location : Enter Location

Telephone : Enter Telephone Number

Description : Enter Description

Save

Change Password

* Current Password : Enter current password

* New Password : Enter new password

* Confirm Password : Confirm Password

Save

Reset Password

Click the 'Reset' button, the system will send an email to the address associated with your account. You can reset your password by clicking the link in the email.

Reset

4. Under the **Change Password** section, enter the Current Password.
5. Enter a New Password, then type the New Password again.
6. Click **Save** to save the new settings.The password will be updated.

you can also modify your account information such as name and email address as well as automatic sign-out time.

3.5. Configure Email Server for Notification

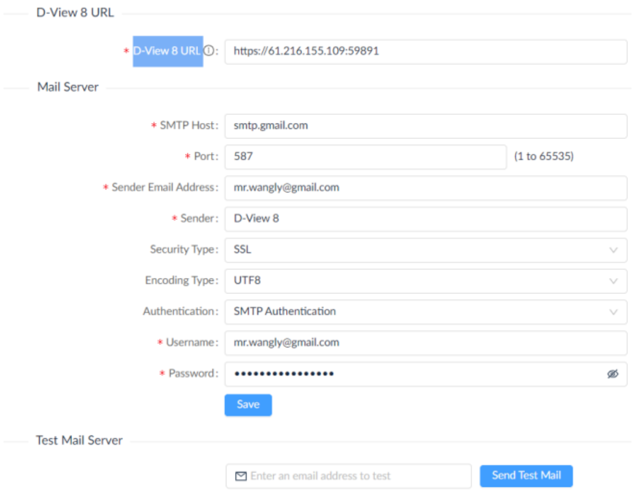
Prior to sending notifications, an Email server must be configured. Only an Organization-privileged Administrator or a Super Administrator can configure the email server settings.

NOTE: For information about generating notifications when an alarm is triggered, refer to the below 3.6 Configure the Notification Center.

To configure mail server settings:

1. Click the **System** ⚙ and select **Basic Settings**.

Select the **Mail Server Settings** tab. The **Mail Server Settings** page displays.



D-View 8 URL

* D-View 8 URL ⓘ : https://61.216.155.109:59891

Mail Server

* SMTP Host : smtp.gmail.com

* Port : 587 (1 to 65535)

* Sender Email Address : mr.wangly@gmail.com

* Sender : D-View 8

Security Type : SSL

Encoding Type : UTF8

Authentication : SMTP Authentication

* Username : mr.wangly@gmail.com

* Password : ••••••••••••••••

Save

Test Mail Server

Enter an email address to test

Send Test Mail

2. In the D-View 8 URL field, enter the URL with the correct port, for example, https://63.216.155.109:59800. This information will be used for email verification of user accounts and appear in password reset emails.
3. Under **Mail Server**, enter the following information:

Item	**Description**
SMTP Host	Enter the address of the SMTP server.
Port	Enter the SMTP port of the outgoing email server.
Sender Email Address	Enter the sender's email address.
Sender	Enter the sender's name for the outgoing email
Security Type	Select the encryption method used by the outgoing mail server (optional): None or SSL.
Encoding Type	Select the character encoding method which converts the sequence of bytes into characters:UTF8 or ASCII (optional).
Authentication	Enter the authentication method for use with the server: Anonymous or SMTP Authentication. If SMTP Authentication is selected, enter the following: • Username: Enter the authorized username to access the server. • Password: Enter the password.
Save	Click **Save** to save the Mail Server settings.

4. In the Test Mail Server field, enter a valid email to send a test email to verify the above mail server settings.

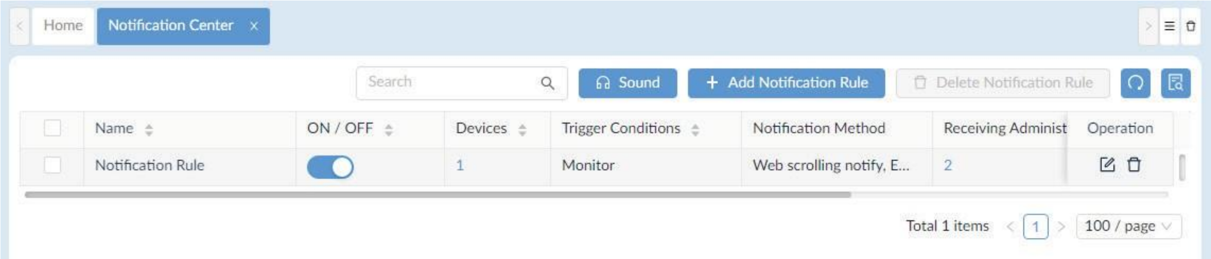
3.6. Configure the Notification Center

Notifications are messages that the system sends via emails or the notification display of the D-View 8 application. It provides you with timely information that requires your attention. The notifications can be easily accessed from the display at the top right of the D-View 8 web application. The Notification Rule is generated according to a monitoring condition with the triggered alarm level. Only an Organization-privileged Administrator or a Super Administrator can configure notification settings.

1. Log in to the Dashboard, refer to 3.2 Launch the D-View 8 Web GUI.
2. Click the **Alarm & Notification > Notification Cente**r.

The **Notification Center** page displays.

3. Click **+ Add Notification Rule**.



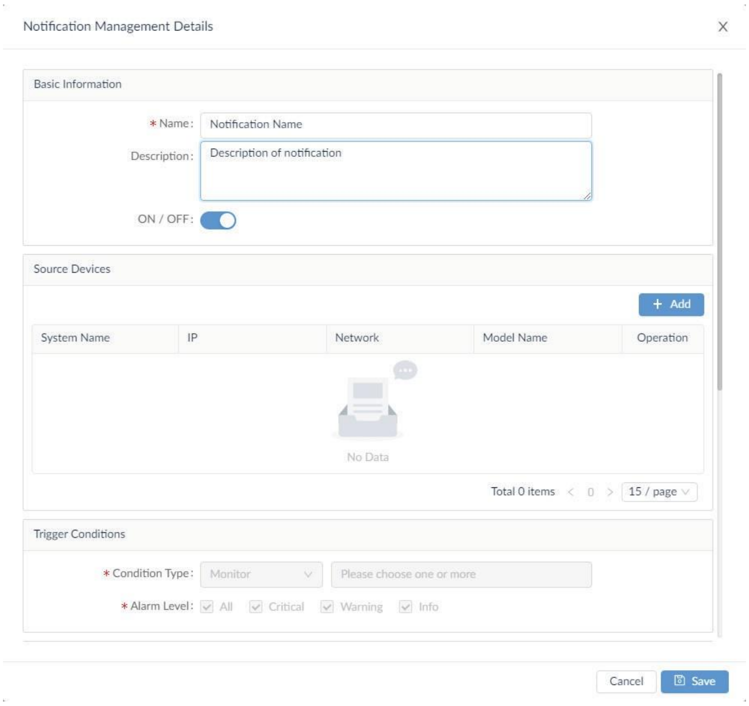
□	Name	ON / OFF	Devices	Trigger Conditions	Notification Method	Receiving Administ	Operation
□	Notification Rule	●	1	Monitor	Web scrolling notify, E...	2	

Total 1 items < 1 > 100 / page

The **Notification Management Details** page displays.

4. Fill in the Basic Information.

5. Click the **ON/OFF** button to enable or disable the rule.



Notification Management Details

Basic Information

* Name: Notification Name

Description: Description of notification

ON / OFF: ●

Source Devices

＋ Add

System Name	IP	Network	Model Name	Operation
No Data				

Total 0 items < 0 > 15 / page

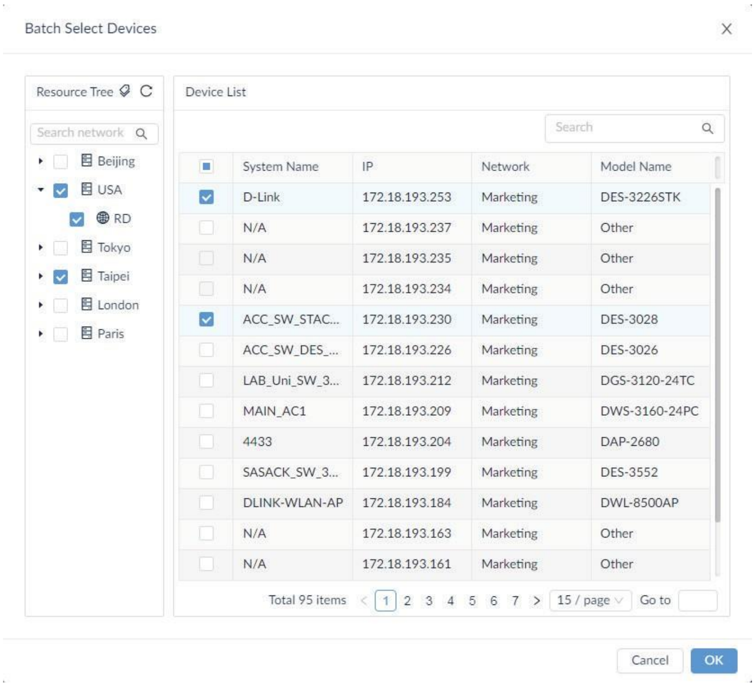
Trigger Conditions

* Condition Type: Monitor | Please choose one or more

* Alarm Level: ☑ All ☑ Critical ☑ Warning ☑ Info

Cancel | Save

6. In Source Devices, click **Add** to select target devices.The Batch Select Devices page displays.
7. From the Device List, select the device(s) to which the notification rule will be applied.



Batch Select Devices

Resource Tree

Search network

- □ Beijing
- ☑ USA
  - ☑ RD
- □ Tokyo
- ☑ Taipei
- □ London
- □ Paris

Device List

Search

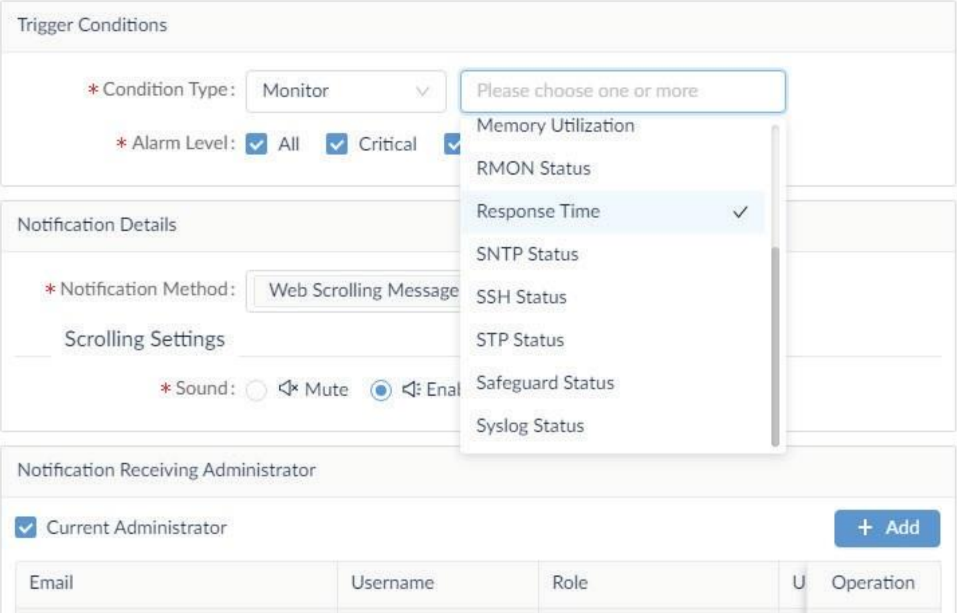
■	System Name	IP	Network	Model Name
☑	D-Link	172.18.193.253	Marketing	DES-3226STK
□	N/A	172.18.193.237	Marketing	Other
□	N/A	172.18.193.235	Marketing	Other
□	N/A	172.18.193.234	Marketing	Other
☑	ACC_SW_STAC...	172.18.193.230	Marketing	DES-3028
□	ACC_SW_DES_...	172.18.193.226	Marketing	DES-3026
□	LAB_Uni_SW_3...	172.18.193.212	Marketing	DGS-3120-24TC
□	MAIN_AC1	172.18.193.209	Marketing	DWS-3160-24PC
□	4433	172.18.193.204	Marketing	DAP-2680
□	SASACK_SW_3...	172.18.193.199	Marketing	DES-3552
□	DLINK-WLAN-AP	172.18.193.184	Marketing	DWL-8500AP
□	N/A	172.18.193.163	Marketing	Other
□	N/A	172.18.193.161	Marketing	Other

Total 95 items < 1 2 3 4 5 6 7 > 15 / page Go to

Cancel | OK

8. Click **OK** to accept the device selection and return to the previous menu.

9. Under **Trigger Conditions**, click the **Condition Type** drop-down menu to define a condition that generates notifications.



Trigger Conditions

* Condition Type: Monitor | Please choose one or more

* Alarm Level: ☑ All ☑ Critical ☑

- Memory Utilization
- RMON Status
- Response Time ✓
- SNTP Status
- SSH Status
- STP Status
- Safeguard Status
- Syslog Status

Notification Details

* Notification Method: Web Scrolling Message

Scrolling Settings

* Sound: ○ Mute ● Enal

Notification Receiving Administrator

☑ Current Administrator

+ Add

Email	Username	Role	U	Operation

The following table displays available options for trigger conditions:

Item	Description	
Condition Type		
Monitor	The availability of monitoring conditions varies depending on the selected device model.	
	• CPU Utilization • DHCP Server Status • Device Common Information • Fan • HTTP Status • LACP • LLDP • Memory Utilization • Private Port • RMON Status	• Response Time • SNTP Status • SSH Status • STP Status • Safeguard Status • Syslog Status • Telnet Status • Trap Status • Wireless Access Points • Wireless Error Packets
Trap	Select Trap as the condition type for notification so that alarms triggered by the trap alarm rules will also generate notifications. To configure trap alarm rules, go to **Alarm & Notification** > **Monitor & Alarm Settings** > **Alarm Settings**, from the Type pane, select the **Trap** category.	
Syslog	Select Syslog as the condition type for notification so that alarms triggered by the syslog alarm rules will also generate notifications. To configure syslog alarm rules, go to **Alarm & Notification** > **Monitor & Alarm Settings** > **Alarm Settings**, from the Type pane, select **Syslog**.	
Wired Traffic	Select Wired Traffic as the condition type for notification so that alarms triggered by wired traffic alarm rules will also generate notifications. To configure wired traffic alarm rules, go to **Alarm & Notification** > **Monitor & Alarm Settings** > **Alarm Settings**, from the Type pane, select **Monitor > Wired Traffic**.	

Alarm Level	Select the level of severity that will activate the notification: All: all severity levels will activate the notification. Or select one of the following alarm levels: Critical: error information indicating failure or malfunction. Warning: error information that may cause future problems Info: information-only alarm level Note that there must be an alarm rule with the corresponding severity level for the notification to take effect.

10. Under **Notification Details**, select the method to deliver the notification.

Item	**Description**
Notification Method	Configure the respective settings for each of the following notification methos.
Web Scrolling Message	Select whether to enable the sound: Mute or Enable Voice.
Email	• Click the Current Administrator to automatically select the current admin user. • Click **Add** to select another user to receive email notifications. You can select criteria (Email, Username, or Role) to search for a user. • Click **OK** to accept. Click **Cancel** to return to the previous screen.
Execute Script	• In the Command Line, enter a script to automate a task or modify device properties or status on the source devices (Itself) or devices other than the source devices (Other Devices) when a notification is generated. • For Other Devices, select the devices to run the script. To execute a script, you need to provide credentials to log in to the system remotely. • The **Acknowledge Alarm after Script Execution** parameter can be used to terminate the repetitive execution of the script. For each execution of the script, the alarm will be automatically acknowledged. Enter the total Number of Repetitions (1-100) and Cycle Time (5-1440) minutes. The automatic script execution will stop when the maximum number of repetitions has been reached in the defined cycle time.

11. Under the **Notification Suspension Period**, click **Add** to select a pre-defined schedule. Or click **Add Schedule** to add a new schedule. The schedule prohibits delivery of notifications at the specified time range of a designated weekday or weekdays for the effective duration of dates.
12. Click **Save** to accept the notification rule or **Cancel** to return to the previous screen. For more detailed instructions, refer to 7.6 Manage Notifications.

4 Organizations and Networks

Before you can manage your network, you must let the application find the devices on your network.

This chapter covers the following topics:

- Network Discovery
- Manage Wired and Wireless Devices on a Network
- Manage Device Groups
- SNMP Configuration
- Manage Multiple Networks with Batch Configuration

4.1. Network Discovery

D-View 8 is designed to utilize probes to connect network devices. Probes run as a background process, discovering devices, polling devices for statistics, and forwarding data to the D-View 8 server if devices are on other networks behind a firewall or in an NAT environment.

D-View 8 probes are not limited to D-Link products and will communicate with any network device that supports standard reporting protocols based on SNMP.

Deploying probes on servers for each network segment helps preserve bandwidth, as data is collected by the probe before being forwarded to the D-View 8 server to be compiled and analyzed. This reduces network overhead by reducing the number of open connections and the need to have all the devices communicating directly with the server. Separating network devices into groups also simplifies management.

Probes are also responsible for executing commands received from the application’s administrator on devices that are connected to the probe. Examples of this would be scheduling a reboot, managing event logs,or making changes to device configuration.

With network and device discovery, D-View 8 can discover wired devices and wireless devices such as access points and switches, no matter D-Link devices or third-party devices supporting standard SNMP MIBs.

Network Discovery allows an administrator to monitor and manage active networks configured with the D-View 8 server. Each network is displayed in the Architecture pane of the Dashboard. The number of managed devices is also displayed, along with device statistics, alarm statistics and an overview for all discovered devices.

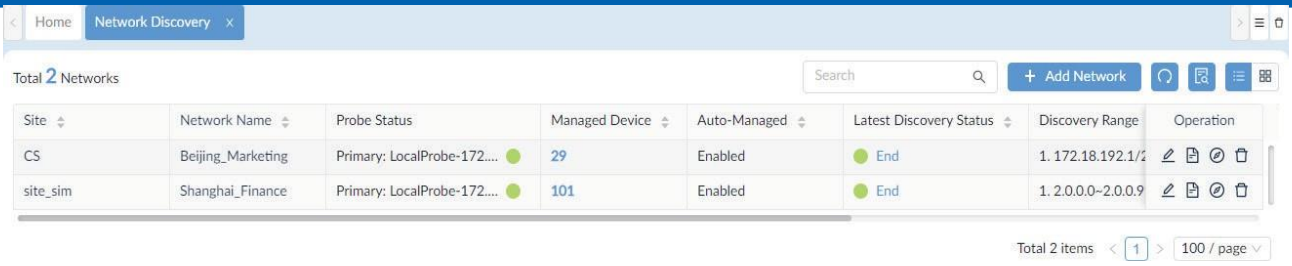
4.1.1. Add Network for Discovery

The application is accessible through a browser. Before logging in to the application, make sure that the D-View 8 application is installed on a server with a static IP address.

NOTE: When a Super Admin logs into the D-View 8 application for the first time with the default username/password, a wizard will appear, please select **Discovery** to be guided through the Network Discovery process, which requires you to set up an organization first.

To add a network:

1. Go to **Monitoring > Network Discovery**.
2. Click **+ Add Network**.

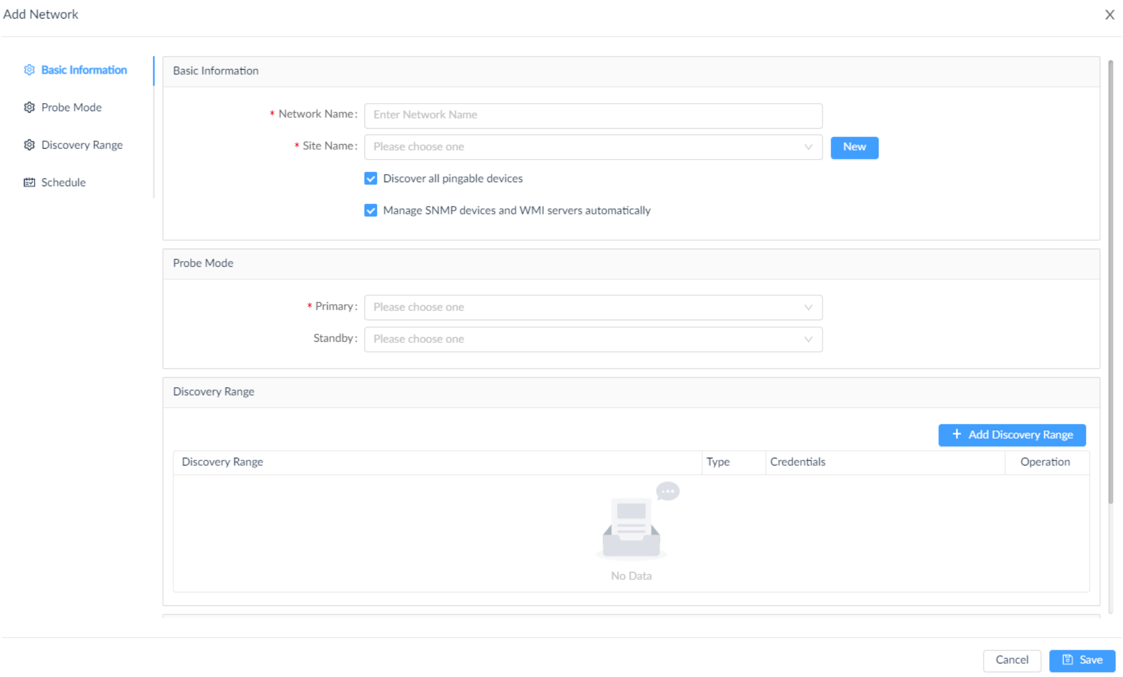


Total 2 Networks

Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest Discovery Status	Discovery Range	Operation
CS	Beijing_Marketing	Primary: LocalProbe-172.... ●	29	Enabled	● End	1. 172.18.192.1/2	
site_sim	Shanghai_Finance	Primary: LocalProbe-172.... ●	101	Enabled	● End	1. 2.0.0.0~2.0.0.9	

Total 2 items < 1 > 100 / page

The Add Network page displays.



Basic Information

* Network Name: Enter Network Name

* Site Name: Please choose one

☑ Discover all pingable devices

☑ Manage SNMP devices and WMI servers automatically

Probe Mode

* Primary: Please choose one

Standby: Please choose one

Discovery Range

Discovery Range	Type	Credentials	Operation

3. Enter the new network information for discovery:

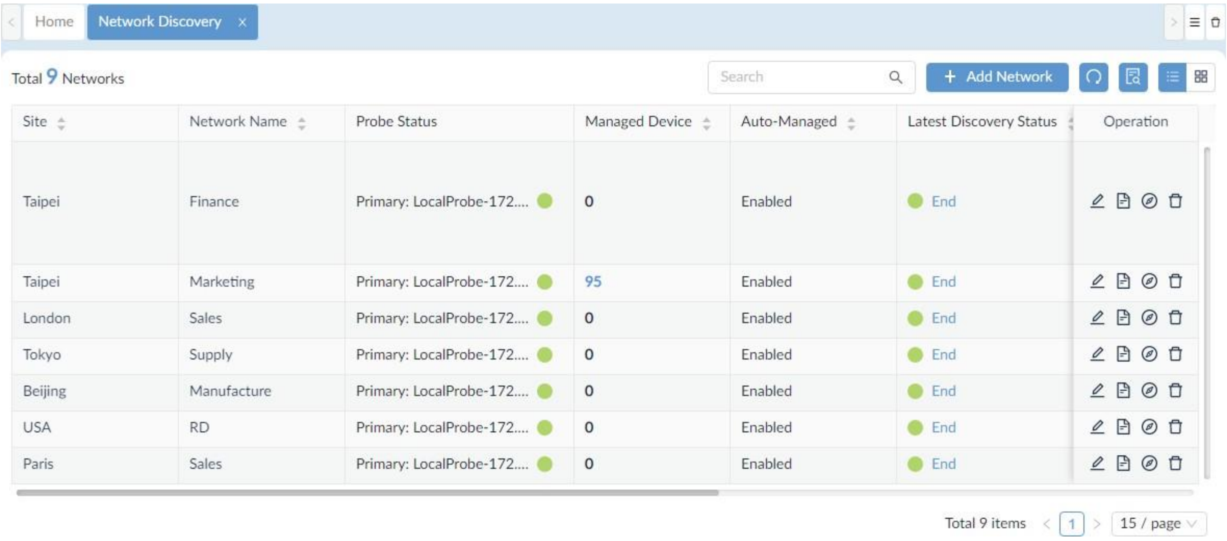
Item	Description
Basic Information	
Network Name	Enter a text string to name the new network.
Site Name	Click the drop-down menu to select an existing site or click **New** to name this site.
Discover all pingable devices	Enable or disable the function to discover alldevices that respond to the ping command automatically. The default is enabled.
Manage SNMP devices and WMI servers automatically	Enable or disable the automatic management of all SNMP or WMI devices. If it is not selected, all detected devices via SNMP will be placed under the **Unmanaged** category. The default is enabled.
Probe Mode	
Primary	Click the drop-down menu to select the primary probe. **NOTE:** If a probe is identified as primary, it cannot be designated as a standby probe.
Standby	Click the drop-down menu to select the standby probe. The Standby probe is a backup probe in case the primary probe fails.

Item	Description
Discovery Range	
Add Discovery Range	Click the **Add Discovery Range** button to define a range for network search.
Discovery Range	List of the configured range settings. See “**Add a Discovery Range**” below for further information.
SNMP Credentials	Click the SNMP field and select the credential version for discovery: **SNMP v3**, **SNMP v2c, SNMP v1,** or **Add SNMP Credential**. The available credentials are set via the Basic Settings menu (go to **System > Basic Settings** and click the **Credentials** tab; refer to **Set Up Credentials**.) If you would like to add a new SNMP credential, click **Add SNMP Credential**.
WMI Credentials	Click the WMI field and select the credential for discovery or click **Add WMI Credential**. The available credentials are set via the Basic Settings menu (go to **System > Basic Settings** and click the **Credentials** tab; refer **to Set Up Credentials**.) If you would like to add a new WMI credential, click **Add WMI Credential**.
Edit	Click the **Edit** button to modify the discovery range.
Delete	Click the **Delete** button to remove the discovery range.
Schedule Information	
Schedule Type	• **One Time**: Select this option to specify a date and time or immediately to initiate the network discovery. • **Recurrent**: Select this option to specify the frequency and effective time frame to initiate network discovery. Refer to 14.2 Scheduling for more information.
Cancel	Click **Cancel** to return to the previous page.
Save	Click **Save** to add the new network.

Add a Discovery Range

To add a discovery range:

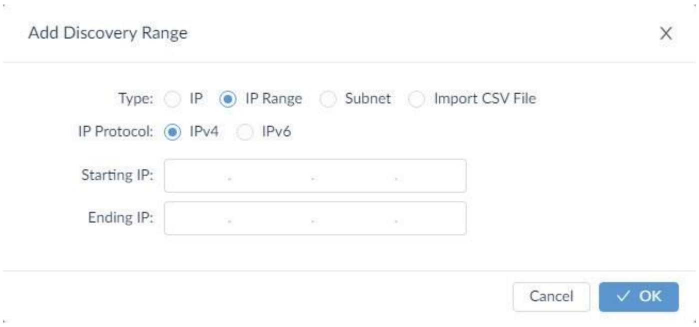
1. Go to **Monitoring** > **Network Discovery**.
2. The **Network Discovery** information displays.



Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest Discovery Status	Operation
Taipei	Finance	Primary: LocalProbe-172.... ●	0	Enabled	● End	
Taipei	Marketing	Primary: LocalProbe-172.... ●	95	Enabled	● End	
London	Sales	Primary: LocalProbe-172.... ●	0	Enabled	● End	
Tokyo	Supply	Primary: LocalProbe-172.... ●	0	Enabled	● End	
Beijing	Manufacture	Primary: LocalProbe-172.... ●	0	Enabled	● End	
USA	RD	Primary: LocalProbe-172.... ●	0	Enabled	● End	
Paris	Sales	Primary: LocalProbe-172.... ●	0	Enabled	● End	

3. Click + **Add Network** to add a new netowork. To add a discovery range under an exisiting network, select a network and click **Edit**.

4. Select **Probe Mode** and click **Add Discovery Range** or **Edit Discovery Range**.The Add Discovery Range or **Edit Discovery Range** screen displays.



Add Discovery Range

Type: ○ IP ● IP Range ○ Subnet ○ Import CSV File

IP Protocol: ● IPv4 ○ IPv6

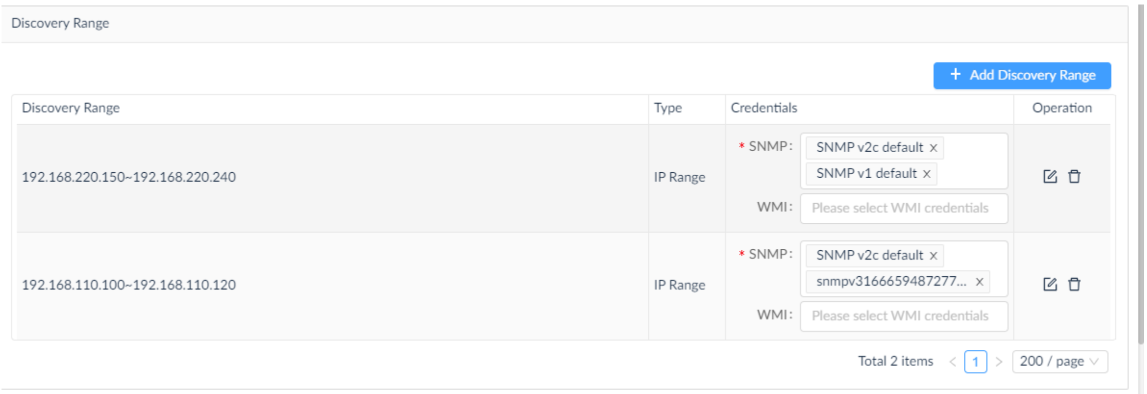
Starting IP:

Ending IP:

Item	**Description**
Type	Click to select the coverage range: IP, IP Range, Subnet, Import CSV File.
IP Protocol	Enter a single IP address as the discovery range. Select either IPv4 or IPv6 IP protocol.
IP Range	Enter the starting IP and ending IP addresses to define the range. • Use Starting IP to express the start of the discovery range. • Use Ending IP to express the end of the discovery range.
Subnet	Enter the subnet address in CIDR notation (e.g. 172.17.2.0/24 for IPv4 addressing or 2001:db8:abcd:0012::0/64 for IPv6 addressing) to define the discovery range. Select IPv4 or IPv6 to specify the IP protocol.
Import CSV File	Click **Select File** to select a pre-configured file. The following shows how the data should be recorded in the CSV file: 1. The import file extension must be “.csv”. 2. Each line must contain no more than one discovery rule. 3. Use a comma “,” to separate the parameters for each discovery rule: 4. The order of SNMP v2 parameters is: Discover IP, SNMP Version, Read-Only Community, RW Community. 5. The order of SNMP v3 parameters is: Discover IP, SNMP Version, Username, Mode, Auth Algorithm, Auth Password, Private Algorithm, Private Password. 6. Parameters can be set to the following values: ▪ Security Level: authNoPriv, noAuthNoPriv, Auth. ▪ Auth Protocol: MD5, SHA ▪ Privacy Protocol: AES, DES. 7. The “Discovery IP” can be a single IP, an IP range, or a subnet. 8. Use “Start IP - End IP” to express the IP range. The starting IP expression cannot be greater than the ending IP expression. 9. Use “IP/subnet mask” to express a subnet. 10.The “Import CSV File” method only supports discovery of SNMP V1/V2/V3 devices. The acceptable “SNMP Version” values are “V1, v1, V2, v2, V3, v3”. 11.The number of IP addresses defined in the CSV file must not exceed 5,000. 12.The file size must not exceed 1 MB. **Sample rules:** 192.168.1.10,v2,public,private 192.168.1.15-192.168.1.17,v2,public,private 192.168.2.0/24,v2,public,private 192.168.1.1,V3,user,noAuthNoPriv 192.168.1.1-192.168.1.17,V3,user,AuthNoPriv,SHA,password 192.168.1.0/24,v3,user,authPriv,MD5,password,AES,password
Cancel	Click **Cancel** to return to the previous page.
OK	Click **OK** to add the new range.

5. Under the **Discovery Range** section, select an existing range and click the **Credentials** field.

6. Click **Add SNMP Credential** or **Add WMI Credential** to define a new SNMP or WMI credential or select a pre-defined credential. Refer to **Set Up Credentials** in 14.1 Configure Global Settings for more information about WMI and SNMP credentials.

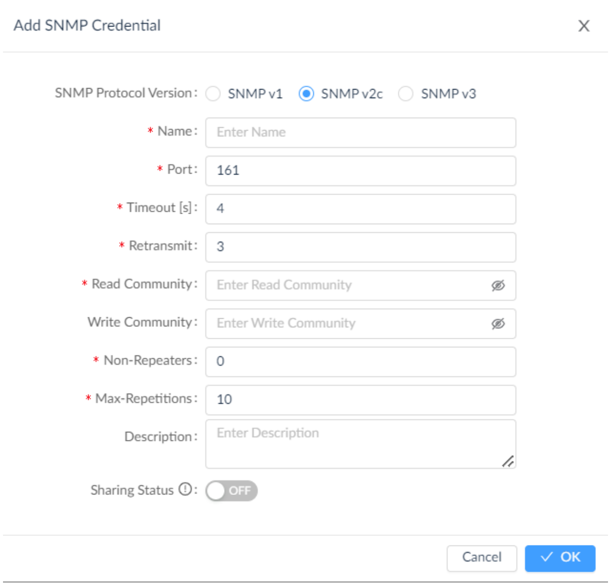


Discovery Range

Discovery Range	Type	Credentials	Operation
192.168.220.150~192.168.220.240	IP Range	* SNMP: SNMP v2c default × SNMP v1 default × WMI: Please select WMI credentials	
192.168.110.100~192.168.110.120	IP Range	* SNMP: SNMP v2c default × snmpv3166659487277... × WMI: Please select WMI credentials	

Total 2 items < 1 > 200 / page

If Add SNMP Credential is selected, the **Add SNMP Credential** page displays.



Add SNMP Credential X

SNMP Protocol Version: ○ SNMP v1 ● SNMP v2c ○ SNMP v3

* Name: Enter Name

* Port: 161

* Timeout [s]: 4

* Retransmit: 3

* Read Community: Enter Read Community

Write Community: Enter Write Community

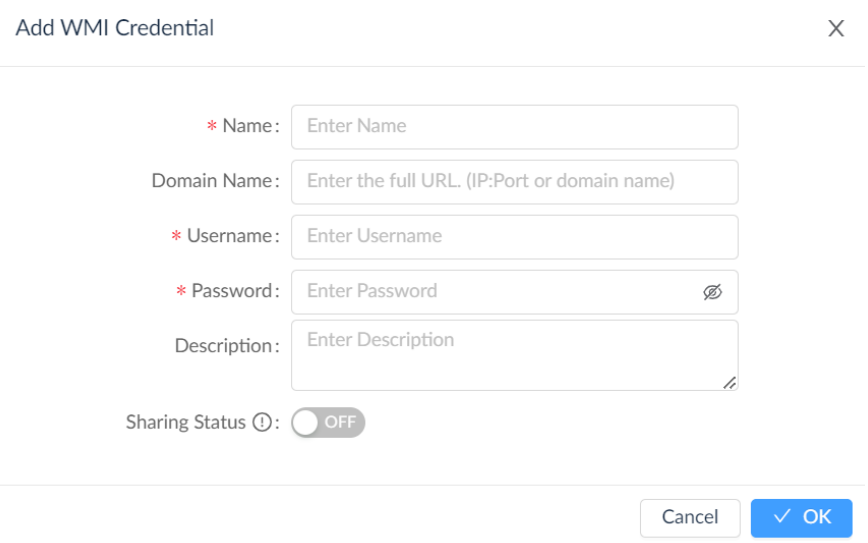
* Non-Repeaters: 0

* Max-Repetitions: 10

Description: Enter Description

Sharing Status ⓘ: OFF

If Add WMI Credential is selected, the **Add WMI Credential** page displays.



Add WMI Credential X

* Name: Enter Name

Domain Name: Enter the full URL. (IP:Port or domain name)

* Username: Enter Username

* Password: Enter Password

Description: Enter Description

Sharing Status ⓘ: OFF

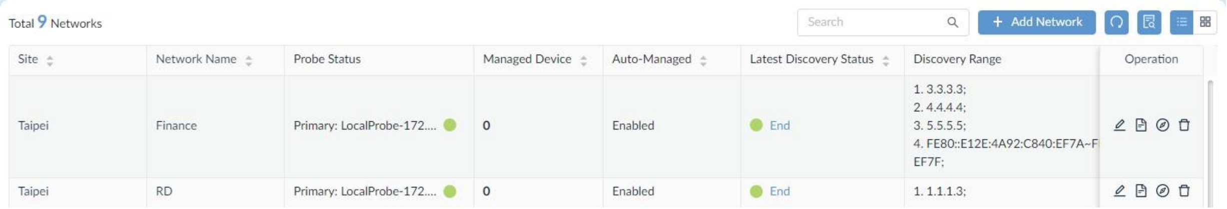
Note the added entry will be listed in the Credentials tab (go to **System > Basic Settings).**

4.1.2. Execute Network Discovery

The D-View 8 provides quick discovery of devices in a defined network.

To execute a discovery job:

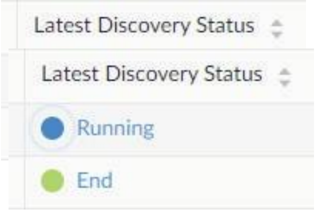
1. Go to **Monitoring > Network Discovery**.
2. Select an existing network profile and click **Discover** ⊘ to start detecting devices in the network.



Total 9 Networks

Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest Discovery Status	Discovery Range	Operation
Taipei	Finance	Primary: LocalProbe-172.... ●	0	Enabled	● End	1. 3.3.3.3; 2. 4.4.4.4; 3. 5.5.5.5; 4. FE80::E12E:4A92:C840:EF7A~F EF7F;	
Taipei	RD	Primary: LocalProbe-172.... ●	0	Enabled	● End	1. 1.1.1.3;	

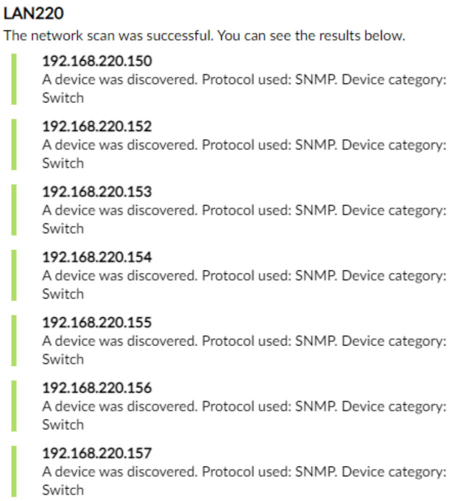
The Latest Discovery Status field displays the discovery result.



Latest Discovery Status
● Running
● End

For example, it displays Running when the discovery is in progress

The Discovery Results page displays. The list of discovered devices will be shown.



LAN220

The network scan was successful. You can see the results below.

192.168.220.150
A device was discovered. Protocol used: SNMP. Device category: Switch

192.168.220.152
A device was discovered. Protocol used: SNMP. Device category: Switch

192.168.220.153
A device was discovered. Protocol used: SNMP. Device category: Switch

192.168.220.154
A device was discovered. Protocol used: SNMP. Device category: Switch

192.168.220.155
A device was discovered. Protocol used: SNMP. Device category: Switch

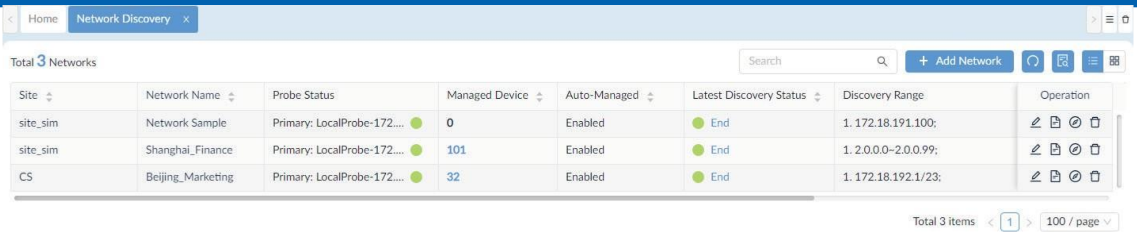
192.168.220.156
A device was discovered. Protocol used: SNMP. Device category: Switch

192.168.220.157
A device was discovered. Protocol used: SNMP. Device category: Switch

4.1.3. Modify or Delete a Network Discovery Profile

If you delete a network discovery profile from the network list, the system deletes the profile along with the device information.

1. Go to **Monitoring > Network Discovery**.The **Network Discovery** information displays.



Total 3 Networks

Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest Discovery Status	Discovery Range	Operation
site_sim	Network Sample	Primary: LocalProbe-172.... ●	0	Enabled	● End	1. 172.18.191.100;	
site_sim	Shanghai_Finance	Primary: LocalProbe-172.... ●	101	Enabled	● End	1. 2.0.0.0~2.0.0.99;	
CS	Beijing_Marketing	Primary: LocalProbe-172.... ●	32	Enabled	● End	1. 172.18.192.1/23;	

Total 3 items < 1 > 100 / page

2. You can obtain more information about the network discovery profile by clicking **Network Information** . It also provides detailed information about probes.

3. Select a network discovery profile and click **Delete** to delete the selected network or **Edit** to modify the network settings. A confirmation page displays for deletion; click **OK** to delete the profile or **Cancel** to return to the previous menu. To edit a discovered network, fill in the information on the **Edit Network** page. For detailed instruction, refer to the above 4.1.1 Add Network for Discovery.

4.2. Manage Wired & Wireless Network Devices

D-View 8 is designed to help you manage your fleet of devices centrally. This section covers the following tasks that you can perform on devices:

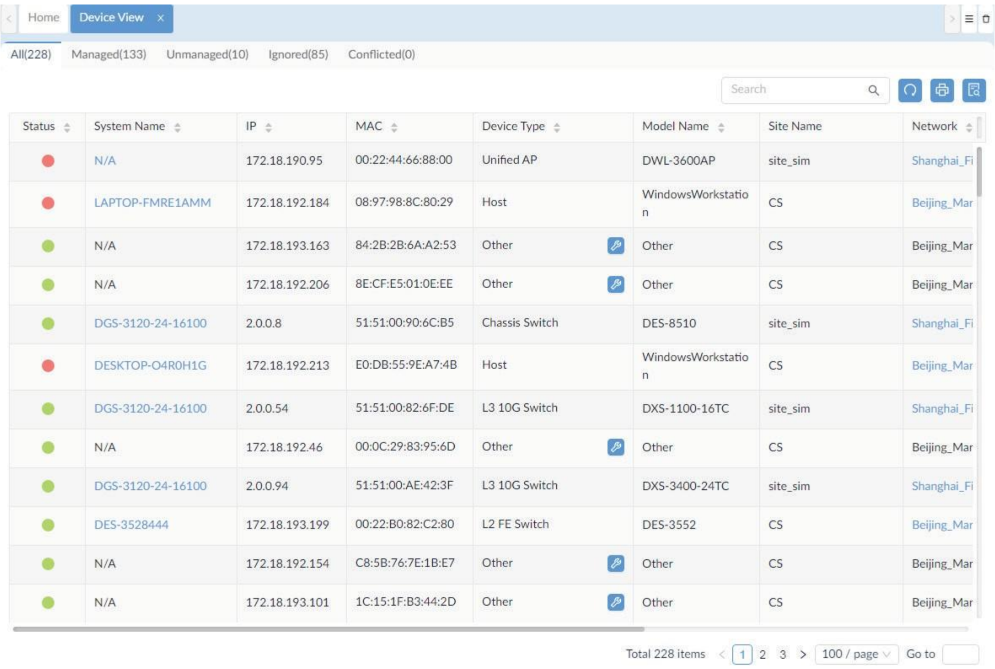
- View Device Information
- Modify Device Information
- Ping or Reboot Device
- View and Export Interface List
- View and Export Connection List

4.2.1. View Device Information

The **Device View** shows devices, which are categorized by managed/unmanaged, ignored, and conflicted. The default view is All. For each device category, device information such as status, system name, IP, and MAC address is displayed. For more detailed information, click on the system name link to display the device's detail page.

Note: When the license expires, the **Device View** page will alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

1. Go to **Monitoring** > **Device View**.The **Device View** information page displays.



Status	System Name	IP	MAC	Device Type	Model Name	Site Name	Network
●	N/A	172.18.190.95	00:22:44:66:88:00	Unified AP	DWL-3600AP	site_sim	Shanghai_Fi
●	LAPTOP-FMRE1AMM	172.18.192.184	08:97:98:8C:80:29	Host	WindowsWorkstation	CS	Beijing_Mar
●	N/A	172.18.193.163	84:2B:2B:6A:A2:53	Other	Other	CS	Beijing_Mar
●	N/A	172.18.192.206	8E:CF:E5:01:0E:EE	Other	Other	CS	Beijing_Mar
●	DGS-3120-24-16100	2.0.0.8	51:51:00:90:6C:B5	Chassis Switch	DES-8510	site_sim	Shanghai_Fi
●	DESKTOP-O4R0H1G	172.18.192.213	E0:DB:55:9E:A7:4B	Host	WindowsWorkstation	CS	Beijing_Mar
●	DGS-3120-24-16100	2.0.0.54	51:51:00:82:6F:DE	L3 10G Switch	DXS-1100-16TC	site_sim	Shanghai_Fi
●	N/A	172.18.192.46	00:0C:29:83:95:6D	Other	Other	CS	Beijing_Mar
●	DGS-3120-24-16100	2.0.0.94	51:51:00:AE:42:3F	L3 10G Switch	DXS-3400-24TC	site_sim	Shanghai_Fi
●	DES-3528444	172.18.193.199	00:22:B0:82:C2:80	L2 FE Switch	DES-3552	CS	Beijing_Mar
●	N/A	172.18.192.154	C8:5B:76:7E:1B:E7	Other	Other	CS	Beijing_Mar
●	N/A	172.18.193.101	1C:15:1F:B3:44:2D	Other	Other	CS	Beijing_Mar

Total 228 items < 1 2 3 > 100 / page Go to

The following table describes the properties of the devices:

Item	Description
Management Type	All, Managed, Unmanaged, Ignored, and Conflicted. Managed: Displays all devices managed by the D-View 8 server. Unmanaged: Displays all unmanaged devices. There are several reasons that a device is classified as Unmanaged: - Not being able to communicate with SNMP or WMI. - Lack of required system parameters such as SOID. - Exceeding the number of supported nodes. Ignored: Devices that are excluded from discovery. Conflicted: Devices that have an IP address conflict.

Status	Online (Green), Offline (Red), Unknown (Grey).
System Name	A unique name that identifies the device.
IP	The IP address of the device.
MAC	The MAC address of the device.
Device Type	The type of the device, e.g., L2/L3 switch, access point, or workstation.
Model Name	The device’s model name.
Site Name	The defined network site of the device.
Network	The defined network of the device.
Vendor	Displays the vendor name of the device.
Discovered Time	Displays the latest discovered time of the device.

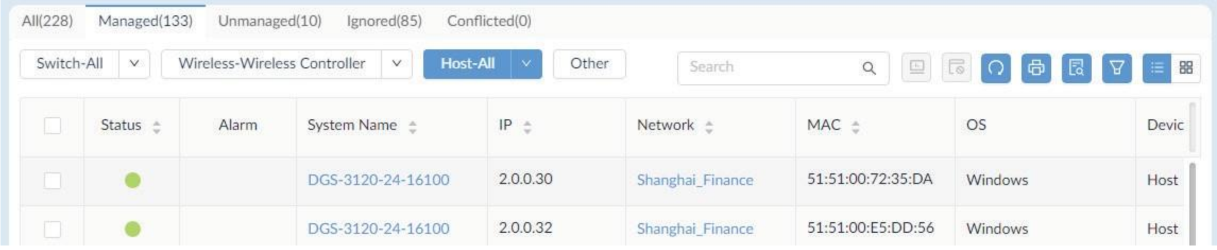
You can click on a column to sort the list by the column name; click it again to reverse the order. You can also configure the column headers with Column Selector .

View Managed Device Information

Managed devices are devices that can be communicated with the D-View 8 system and have the required SNMP parameters.

1. Go to **Monitoring > Device View**.
2. Select the **Managed** tab to view all the discovered devices that are managed by D-View 8.

The drop-down menu at the top of the table allows you to refine the list with device type, for example, wireless AP or controller.



□	Status	Alarm	System Name	IP	Network	MAC	OS	Devic
□	●		DGS-3120-24-16100	2.0.0.30	Shanghai_Finance	51:51:00:72:35:DA	Windows	Host
□	●		DGS-3120-24-16100	2.0.0.32	Shanghai_Finance	51:51:00:E5:DD:56	Windows	Host

Item	Description
All	Displays all detected devices.
Managed	Displays all devices managed by the D-View 8 server.
	Switch-All: click the drop-down menu to list All, sFlow, or PoE-capable switch devices.
	Wireless-Wireless Controller: click the drop-down menu to list the devices grouped by Wireless Controller, Access Point, SSID, or Wireless Client.
	Host-All: click the drop-down menu to list All, Process, or Software-hosting devices.
	Other: click to list devices that do not belong to any of the above device categories.
Toolbar Function	
Search	Enter a keyword and select the matching property for search .
Unmanage	Click to classify the selected device as unmanaged under the Managed category.
Manage	Click to classify the selected device as managed under the Unmanaged category.

Ignore	Click to classify the selected device as ignored. This device will be excluded from discovery. You can ignore a device under either Managed or Unmanaged category.
Refresh	Click to refresh the list information.
Export	Click to export the discovered device list to a CSV file. Up to 5000 entries can be included in a single export job.
Advanced query	Select the criteria to filter the list.
Columns Selector	Click to customize column headers. The available column properties vary depending on the device type. **Default:** Status, Alarm, System Name, Network, IP, MAC, Uptime, Vendor, CPU Utilization, Memory Utilization, Firmware Version, Hardware Version, Model Name, Temperature, Device Type, Serial Number, Discovered Time. **Other:** Device Category, Site Name, PoE Status, sFlow Status, Stack Info, Current Activated License, Activated / Total Licenses, Port Count, Latest Discovered Time, Trap Status, DHCP Status, Total Flash, Syslog Status, Attached on Probe, SNTP / NTP Status, SSH Status, Spanning Tree, LLDP Status, LACP Status, RMON Status, Safeguard Engine Status Click **All** to select or deselect all the categories.Click **Apply** to save the selection.
View List	Click to view the list either in a list format or a graphical representation.

3. To view the details of a device, click the device's **System Name** link.

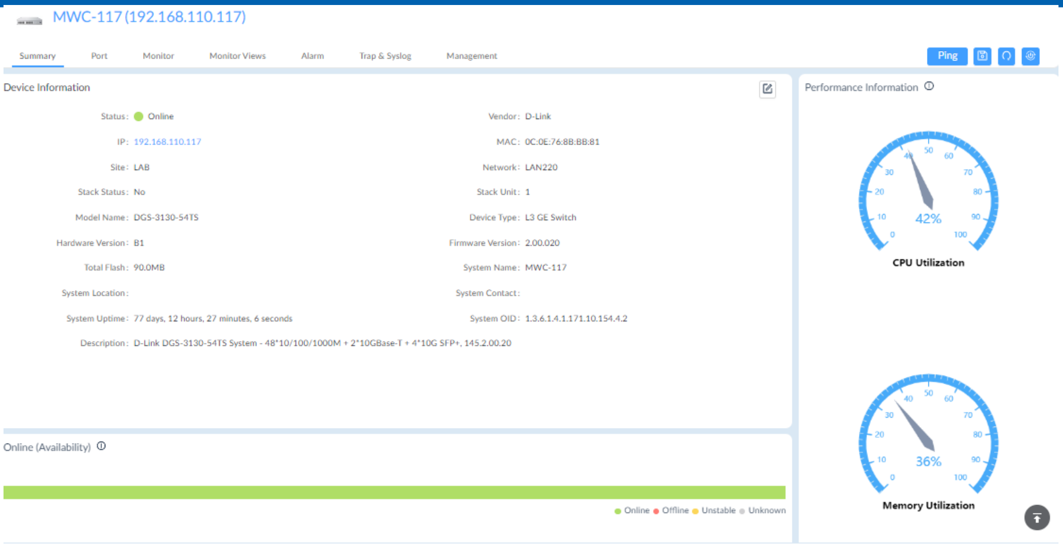
4.2.2. Modify Device Information

Device information can be modified for managed devices. You can modify device information such as system name, system location, system contact, and other properties depending on the device type.

To modify a device's information:

1. Log in to the Dashboard, see "3.2 Launch the D-View 8 Web GUI".
2. Click **Monitoring** and select **Device View**. The **Device View** information displays.
3. From the category menu select the **Managed** tab.
4. Select a device and click the **System Name**.

The device's detailed information page displays.



MWC-117 (192.168.110.117)

Device Information

Status: Online
IP: 192.168.110.117
Site: LAB
Stack Status: No
Model Name: DGS-3130-54TS
Hardware Version: B1
Total Flash: 90.0MB
System Location:
System Uptime: 77 days, 12 hours, 27 minutes, 6 seconds
Description: D-Link DGS-3130-54TS System - 48*10/100/1000M + 2*10GBase-T + 4*10G SFP+, 145.2.00.20

Vendor: D-Link
MAC: 0C:0E:76:8B:BB:81
Network: LAN220
Stack Unit: 1
Device Type: L3 GE Switch
Firmware Version: 2.00.020
System Name: MWC-117
System Contact:
System OID: 1.3.6.1.4.1.171.10.154.4.2

5. From the **Device Summary** page, click the edit button .
6. Click on a field to edit its property.
7. Click **Save** to update the device information.

Note: The device information also provides other tabs for additional information such as alarms and resource monitoring. The available information depends on the type of the managed device, for example, a wireless AP will have the **Wireless** tab showing the SSIDs and channel as well as authentication information.

The following table describes the information available through the **Device Information** page.

Item	Description
Summary	
Device Information	Displays an overview of the device information. You can click **Edit** to modify the following: System Name, System Location, and System Contact. Click **Save** to accept the updates or **Cancel** to continue without saving.
Performance Information	Displays charts for the device's CPU and memory usage.
Online (Availability)	Displays the online status of the equipment in the past 24 hours.
SNMP Protocol Credentials	Set the SNMP settings for the device. Refer to **Set Up SNMP Credentials** in System Settings. Click Reset to discard any setting updates. Click Test to test the settings to verify if they are correct. Click Save to accept the settings.
SSH/Telnet Credentials	Enter security settings for SSH or Telnet connection. Refer to Set Up SNMP Credentials in System Settings.
Additional Information	Click **Edit Additional Information** to include further device details: Purchase Date, Keeper, Warranty Expiration, Service Vendor, Service Contact, and Description.
LACP Working Status	Provides Link Aggregation Control Protocol (LACP) data if LACP is enabled.
Hardware Health	Provides a tabular view of the operational status of the device's fan, power supply, and temperature.
Port	Click to display the Port List overview page. The following information categories are available: Monitor, Comparison, and Alarm Settings. The Monitor and Alarm settings can be set on a per-port basis. You can enable or disable the monitoring status and configure alarm settings using the on/off switch. Or you can go to the **Alarm & Notification > Monitor & Alarm Settings** and select the **Wired Traffic** category on the **Monitor Settings** tab and the **Alarm Settings** tab. The **Monitor Settings** can be used to select

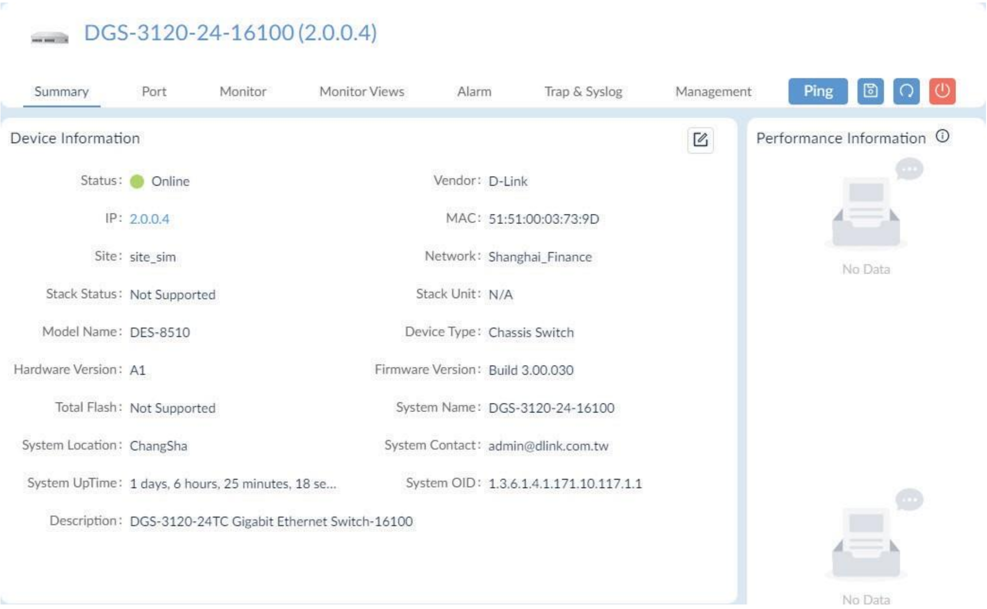
	the ports to be monitored whereas the **Alarm Settings** allows you to set alarm rules based on Rx/Tx traffic, error rate, discard rate and bandwidth utilization. The **Admin Status** switch allows you to enable or disable each port. **Note:** The connectivity information of the device is only available for managed devices which can send SNMP data to the D-View server with a unique and identifiable SOID.
Monitor	Click to view a graphical presentation of the CPU and memory utilization, response time, etc. The information can be shown by Hour, Day, Week, Month, or Quarter (3 months retention period). **Monitoring Settings**: click to enable/disable a specific measurement to monitor. The following categories are available: 802.1Q VLAN, BaseInfo, CPU Utilization, Device Common Information, DHCP Server Status, HTTP Status, LACP, LLDP, Memory Utilization, Power Status, Private Port, RMON Status, Response Time, SNTP Status, SSH Status, STP Status, Temperature, Syslog Status, Telnet Status, Trap Status, Safeguard Status, Syslog Status, and sFlow Profile. Note that the available monitor categories depend on the device's capability. Go to **Alarm & Notification > Monitor & Alarm Settings** for monitoring status control and **Templates > Monitor Template** for available monitor categories and templates. You can create customized monitoring functions for devices; for detailed instructions, refer to 11.1 Generate Device Template. Once you have added a customized monitoring function to the device, a **Customized Monitor** tab will appear next the default System Monitor tab.
Monitor Views	Click to view monitoring information in a topological format: Rack View and System as well as Customized topology. Click the topology name link or go to **Monitoring > Topology Map** to access the topology map view. (Refer to 8.1 View and Manage Network Topology for more information.)
Alarm	Click to view the active or historical (either automatically resolved by automatic script or manually resolved with admin acknowledgement) alarm events. Click **Alarm Settings** to turn on or off specific alarm rule listed by monitor category as in **Alarm & Notification > Monitor & Alarm Settings > Alarm Settings**. The **Trap** and **Syslog** tabs list alarms configured under the Trap and Syslog category.
Trap & Syslog	Click to view the trap messages and system logs. Go to **Alarm & Notification > Trap & Syslog** to access the Trap & Syslog page to view all trap events and system logs. (Refer to 7.2 View Traps and Syslog for more information.)
Management	Click to view and configure device service settings and manage firmware and configuration files. It also provides links to **Task Management** in **Configuration**. Note that the available configuration categories depend on the device's supported features. To view all supported configuration features, click the **More Settings** tab. Go to **Configuration > Batch Configuration > Quick Configuration** and **Advanced Configuration** to view available settings for both **Quick configuration** and **Advanced Configuration** categories. You can create customized configuration for devices using configuration templates; go to **Templates > Configuration Template**. For detailed instructions, refer to 11.5 Generate Configuration Templates and 11.1 Generate Device Templates. You can also create tasks to be executed immediately by clicking **"+ Create Task**" from this menu.
Ping	Click Ping at the upper right to display the ICMP ping menu.
Save	Click Save to Device at the upper right to save the updated settings to the device.
Refresh	Click Refresh from Device at the upper right to synchronize the device and panel information.
Reboot	Click Reboot at the upper right to reboot the device.
Note: You can view the Monitor and Management features supported for each model managed by D-View via Device Template (go to **Templates > Device Template** and search for a specific model to display all monitor and configuration templates configured for this model). However, some of the system-built templates that have been employed as system-defaults on managed devices are still undergoing the verification process and may not work correctly; please visit the D-View website (https://dview.dlink.com/supportedModel) to obtain the latest list of supported models.	

4.2.3. Ping or Reboot a Device

You can ping or reboot a network device. The device must be online to perform these tasks.

1. Go to **Monitoring** > **Device View**. The **Device View** information displays.

2. Select a device from the list and click its **System Name.**The **Device Information** page displays.



Status: Online
Vendor: D-Link
IP: 2.0.0.4
MAC: 51:51:00:03:73:9D
Site: site_sim
Network: Shanghai_Finance
Stack Status: Not Supported
Stack Unit: N/A
Model Name: DES-8510
Device Type: Chassis Switch
Hardware Version: A1
Firmware Version: Build 3.00.030
Total Flash: Not Supported
System Name: DGS-3120-24-16100
System Location: ChangSha
System Contact: admin@dlink.com.tw
System UpTime: 1 days, 6 hours, 25 minutes, 18 se...
System OID: 1.3.6.1.4.1.171.10.117.1.1
Description: DGS-3120-24TC Gigabit Ethernet Switch-16100

3. From the toolbar at the top right, perform one of the following actions:
   - **Ping** the device: click Ping to initiate a ping command on the device. For ping, you can specify the supported parameters such as the number of times and packet size to send the ping request.
   - **Save** to Devices: Click to save the updated information to the device.
   - **Refresh** the information: click Refresh to update the information with the device.
   - **Reboot** the device: click **Reboot** to restart the device.

4.2.4. View and Export an Interface List

You can view the interfaces (or ports) of device(s) managed by the application, and export the table to a tabular formatted (.csv) file. The export list only lists the information of managed devices.

1. Go to **Monitoring** > **Interface View**.The **Interface View** information page displays.

   The following device interface information is displayed:

Item	**Description**
System Name	The link redirects to the Device Information page.
Model Name	Device model name
IP	Device IP address
Network	The network of the device
Interface Index	The number of the port of the device.
Interface Name	The name of the port of the device.
Interface MAC	The MAC address of the port.
Connected MAC	The MAC address of connected port of the other device.
Connected Interface Name	The Interface Name of the connected port of the other device.
VLAN ID	The VLAN ID to which the port belongs.
VLAN Name	The VLAN name to which the port belongs.
VLAN Type	The configured VLAN type of the port.
VLAN Port Status	The status of the VLAN port: tagged or untagged.
Update Time	The last time that the information synced with the device.

2. Click **Export** to start the export job. The exported file will be saved in the default download folder of your

browser.

4.2.5. View and Export a Connection List

You can view the connected devices from the connection point of view with interface-level details. You can also export the data to a tabular file format file. The export list only lists the information of managed devices.

1. Go to **Monitoring** > **Connection View**.The **Connection View** information page displays.

   The following connected interface information is displayed:

Item	Description
Status	The connection status of the link
Alarm	Alarms on either of the connected devices of the link.
Link Name	The device IP addresses of the two ends of the link. You can click on it to obtain more information of the link such as the device performance information and online status of the ports
Device A	The device IP address of one end.
Interface A	The connected port of the Device A.
Device B	The device IP address of the other end.
Interface B	The connected port of the Device B.
RX/TX	The transport and receiving data.
Utilization	The bandwidth utilization in percentage.
Type	The connection type
Last Updated	The last time that the information synced with the device.
Detection Source	The detection protocol.

2. Click **Export** to start the export job. The exported file will be saved in the default download folder of your browser.

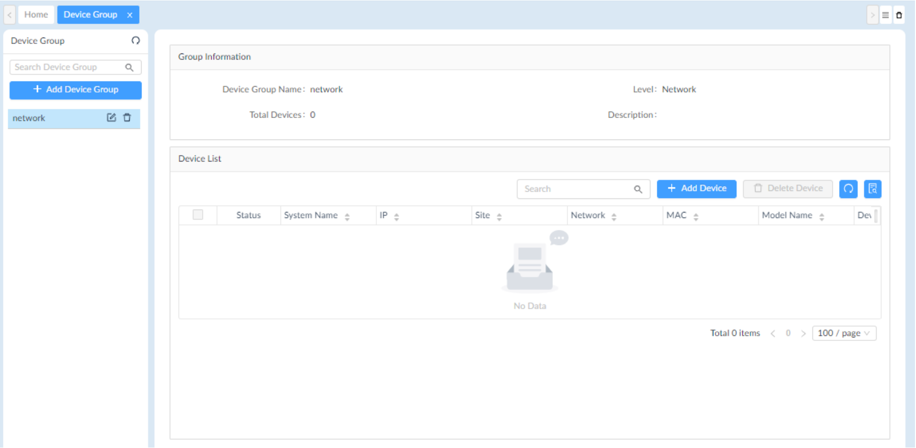
4.3. Manage Device Groups

Device groups are designed to simplify the organization of the network devices. It can be used for applying target devices in **Batch Configuration** and **Firmware Management**. Once a device is discovered, it can be added to a group. Groups can be created across sites or networks within an organization. After a device group is created, you can perform maintenance operation such as firmware upgrade on the devices of the group.

4.3.1. Add a Device Group

To add a device group:

1. Go to **Monitoring > Device Group** to open the device group page.



Group Information

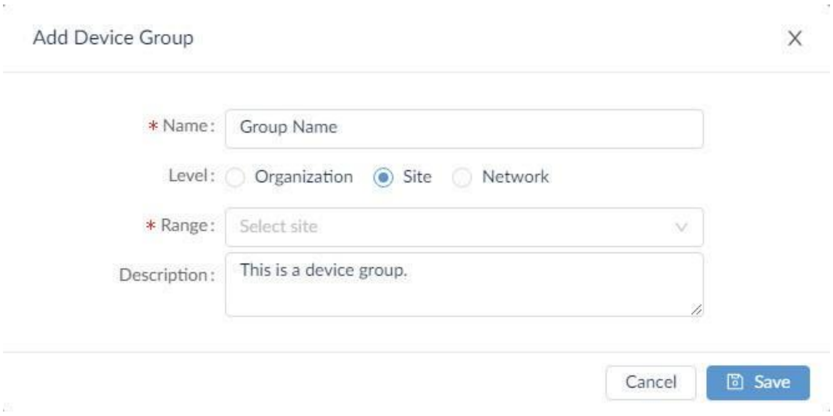
Device Group Name: network

Level: Network

Total Devices: 0

Description:

2. Click **+Add Device Group** from the left list pane.



Add Device Group

* Name: Group Name

Level: ○ Organization ● Site ○ Network

* Range: Select site

Description: This is a device group.

The **Add Device Group** page displays.

Enter the group information:

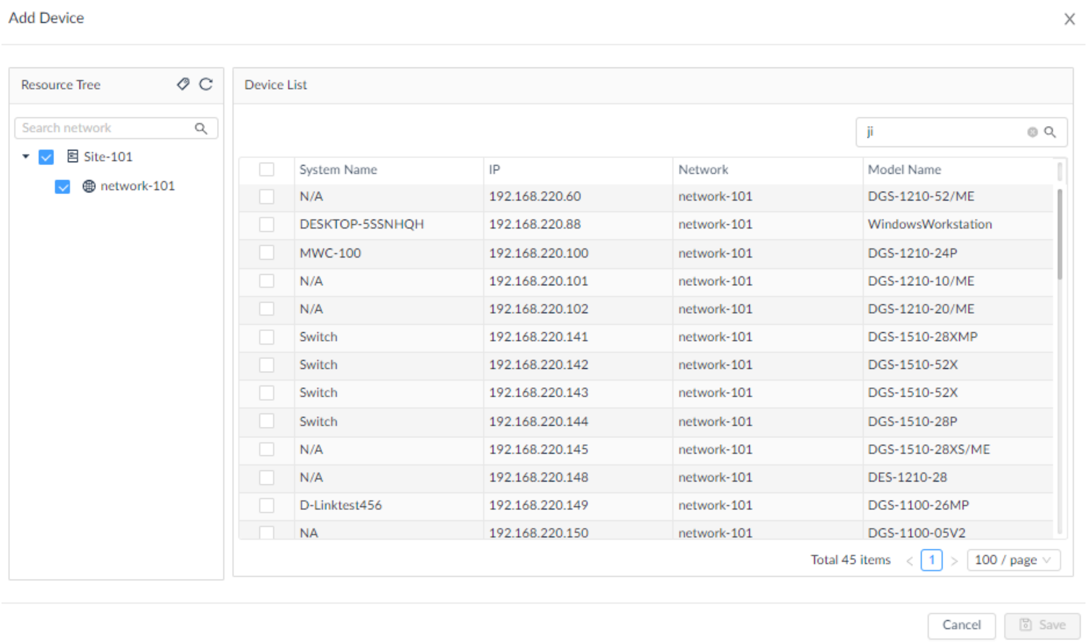
Item	Description
Name	Enter a name for the group.
Level	Click to select the group level (default: Organization). **Organization:** Select an organization to add all discovered devices in the organization. **Site:** Click the **Range** drop-down menu to select a site to add devices in the designated site. **Network:** Click the **Range** drop-down menu to select a network to add devices in the designated network.
Description	Enter a short description for easy identification.

3. Click **Save** to create the group.

The **Group Information** page will be shown on the right side.

4. Click **+ Add Device**. The **Add Device** page displays. From the **Resource Tree** pane, select the site and network to find the desired devices.

5. From the entries in the **Device List,** select a device to be included in the selected group. Or enter an IP address or a model name to find the desired devices.



Add Device

Resource Tree

Search network

☑ Site-101
☑ network-101

Device List

ji

□	System Name	IP	Network	Model Name
□	N/A	192.168.220.60	network-101	DGS-1210-52/ME
□	DESKTOP-5SSNHQH	192.168.220.88	network-101	WindowsWorkstation
□	MWC-100	192.168.220.100	network-101	DGS-1210-24P
□	N/A	192.168.220.101	network-101	DGS-1210-10/ME
□	N/A	192.168.220.102	network-101	DGS-1210-20/ME
□	Switch	192.168.220.141	network-101	DGS-1510-28XMP
□	Switch	192.168.220.142	network-101	DGS-1510-52X
□	Switch	192.168.220.143	network-101	DGS-1510-52X
□	Switch	192.168.220.144	network-101	DGS-1510-28P
□	N/A	192.168.220.145	network-101	DGS-1510-28XS/ME
□	N/A	192.168.220.148	network-101	DES-1210-28
□	D-Linktest456	192.168.220.149	network-101	DGS-1100-26MP
□	NA	192.168.220.150	network-101	DGS-1100-05V2

Total 45 items < 1 > 100 / page

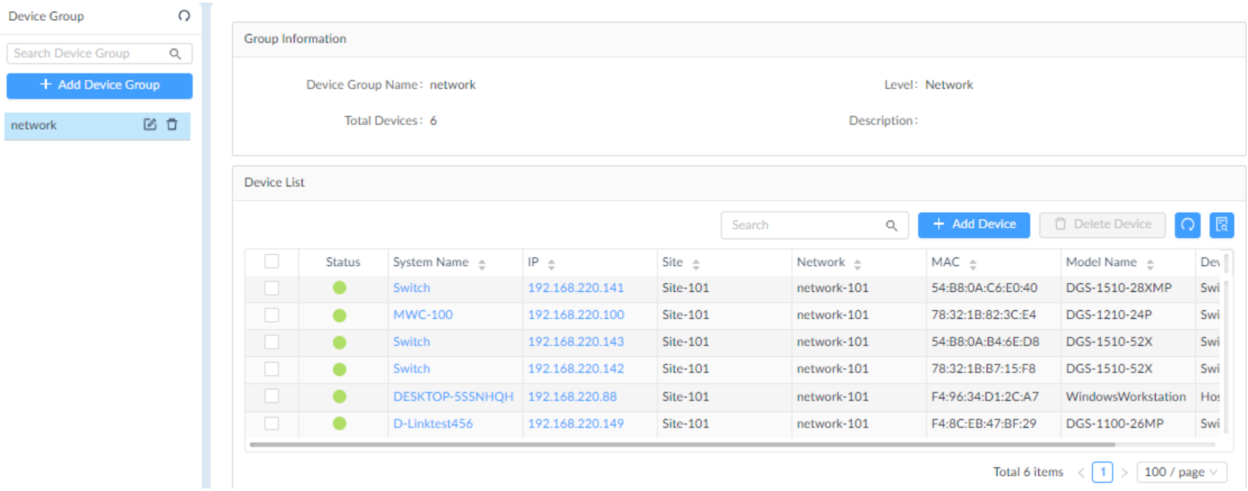
Cancel Save

6. Click **Save** to add the devices to the group.

4.3.2. Edit or Remove a Device Group

1. Go to **Monitoring > Device Group**.

2. The **Device Group** page displays.



Device Group

Search Device Group

+ Add Device Group

network

Group Information

Device Group Name: network

Level: Network

Total Devices: 6

Description:

Device List

Search

+ Add Device

Delete Device

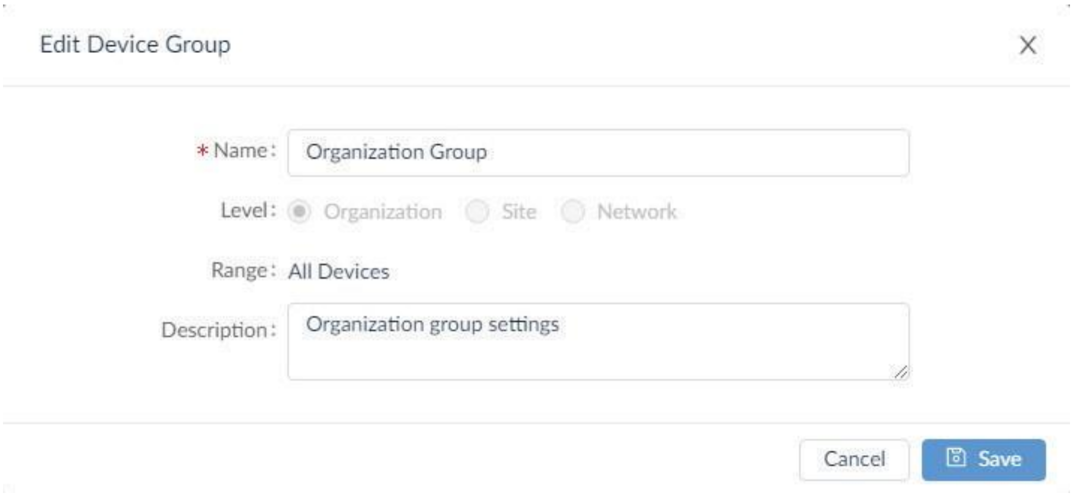
□	Status	System Name	IP	Site	Network	MAC	Model Name	Dev
□	●	Switch	192.168.220.141	Site-101	network-101	54:B8:0A:C6:E0:40	DGS-1510-28XMP	Swi
□	●	MWC-100	192.168.220.100	Site-101	network-101	78:32:1B:82:3C:E4	DGS-1210-24P	Swi
□	●	Switch	192.168.220.143	Site-101	network-101	54:B8:0A:B4:6E:D8	DGS-1510-52X	Swi
□	●	Switch	192.168.220.142	Site-101	network-101	78:32:1B:B7:15:F8	DGS-1510-52X	Swi
□	●	DESKTOP-5SSNHQH	192.168.220.88	Site-101	network-101	F4:96:34:D1:2C:A7	WindowsWorkstation	Ho:
□	●	D-Linktest456	192.168.220.149	Site-101	network-101	F4:8C:EB:47:BF:29	DGS-1100-26MP	Swi

Total 6 items < 1 > 100 / page

3. Select an existing device group and perform the following:

- **Edit:** click to edit the device group name and description.

- **Delete:** click to remove the device group.



Edit Device Group

* Name: Organization Group

Level: ● Organization ○ Site ○ Network

Range: All Devices

Description: Organization group settings

4.3.3. Remove a Device from a Group

1. Go to **Monitoring** > **Device Group**.The **Device Group** page displays.
2. Select a Group from the **Device Group** pane.

   The Device List page displays the devices in the group.
3. Select a device and click **Delete Device** to remove it.
4. A confirmation message appears. Click **Yes** to remove the device from the group or **No** to cancel the deletion.

4.4. SNMP Configuration

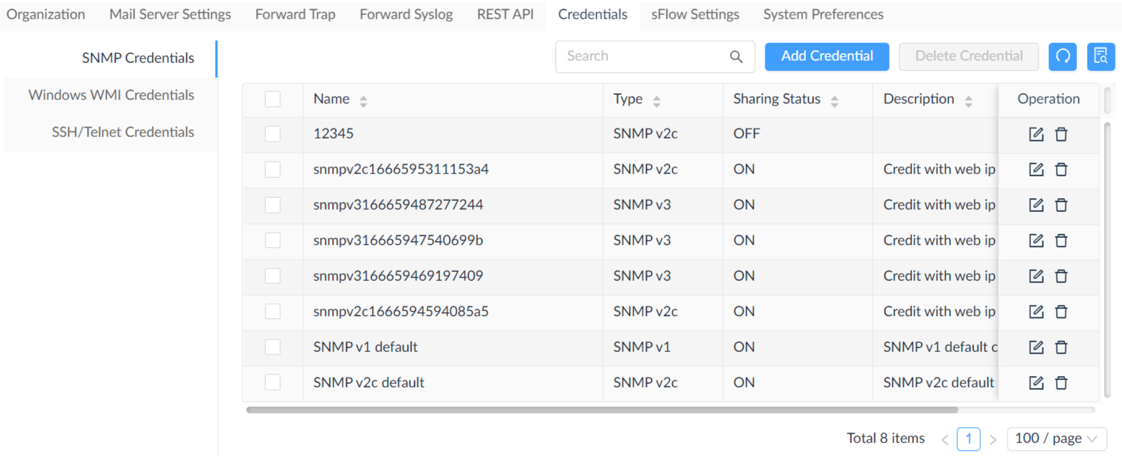
Network discovery and the device information is accomplished via Simple Network Management Protocol (SNMP). It allows D-View 8 application to monitor certain parameters of the devices. In addition, an alarm can be triggered when certain types of traps are sent from devices.

4.4.1 Configure SNMP Credentials

Devices can be polled individually for network discovery and monitoring. The required SNMP settings should be configured in SNMP credentials list.

To access the configuration page:

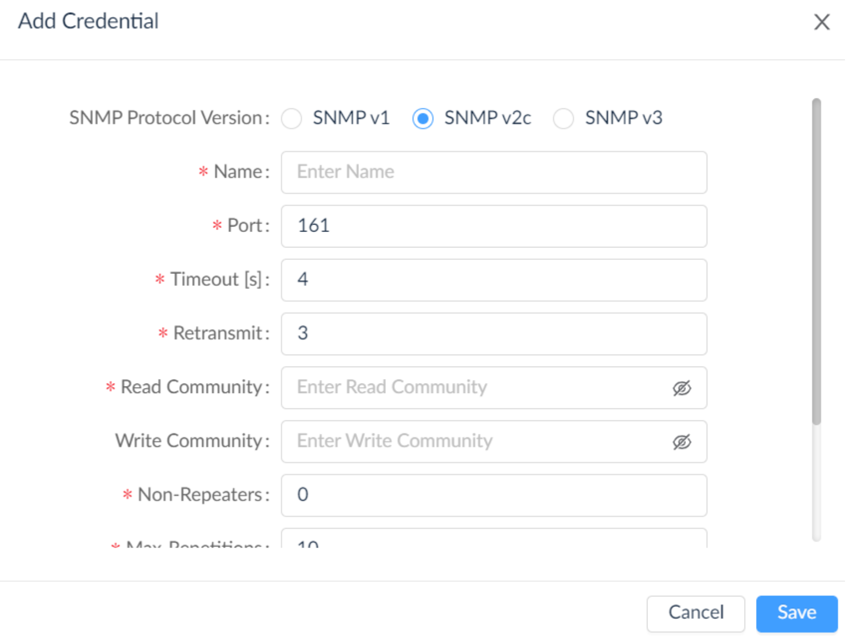
1. Go to **System > Basic Settings > Credentials**.
2. The SNMP Credentials page displays:



□	Name	Type	Sharing Status	Description	Operation
□	12345	SNMP v2c	OFF		
□	snmpv2c1666595311153a4	SNMP v2c	ON	Credit with web ip	
□	snmpv3166659487277244	SNMP v3	ON	Credit with web ip	
□	snmpv316665947540699b	SNMP v3	ON	Credit with web ip	
□	snmpv3166659469197409	SNMP v3	ON	Credit with web ip	
□	snmpv2c1666594594085a5	SNMP v2c	ON	Credit with web ip	
□	SNMP v1 default	SNMP v1	ON	SNMP v1 default c	
□	SNMP v2c default	SNMP v2c	ON	SNMP v2c default	

Total 8 items < 1 > 100 / page

3. Click **Add Credential** to add SNMP credentials for devices within the network:



Add Credential

SNMP Protocol Version: ○ SNMP v1 ● SNMP v2c ○ SNMP v3

* Name: Enter Name

* Port: 161

* Timeout [s]: 4

* Retransmit: 3

* Read Community: Enter Read Community

Write Community: Enter Write Community

* Non-Repeaters: 0

* Max Repetitions: 10

For detailed instructions, refer to **Set Up Credentials** in 14.1 Configure Global Settings

4.4.2 Test SNMP

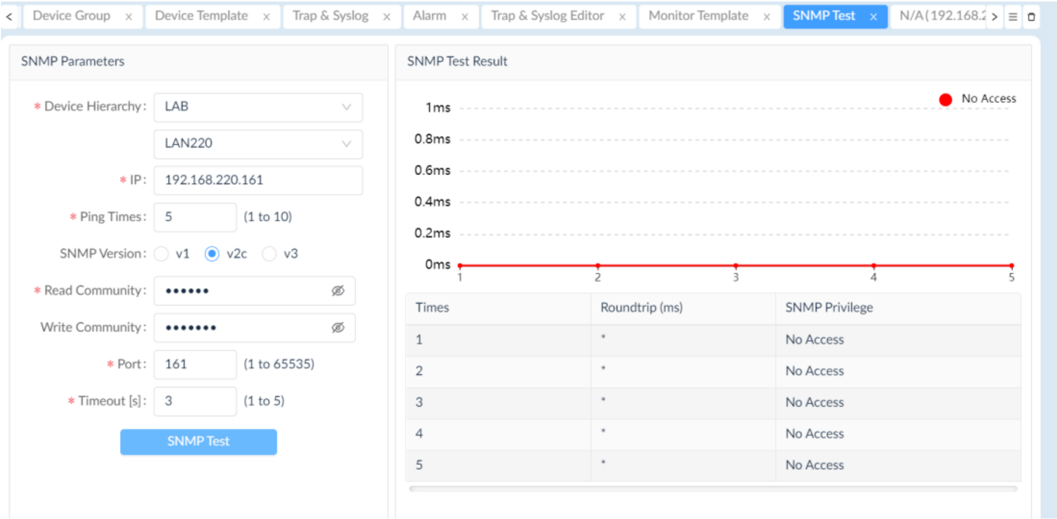
SNMP functionality can be tested on various platforms using compatible tools. The D-View 8 provides a convenient SNMP tool to test SNMP access to SNMP agents.

To use this tool:

1. Go to **Tools > SNMP Test**.

2. Enter the SNMP Parameters in the left pane to access the device agent. The verified SNMP parameters can be maintained in the above Credentials list.

3. The test result should be displayed in the right pane.



SNMP Parameters

* Device Hierarchy: LAB
LAN220
* IP: 192.168.220.161
* Ping Times: 5 (1 to 10)
SNMP Version: ○ v1 ● v2c ○ v3
* Read Community: ••••••
Write Community: •••••••
* Port: 161 (1 to 65535)
* Timeout [s]: 3 (1 to 5)

SNMP Test Result

Times	Roundtrip (ms)	SNMP Privilege
1	*	No Access
2	*	No Access
3	*	No Access
4	*	No Access
5	*	No Access

For detailed instructions, refer to 15.4 Perform an SNMP Test.

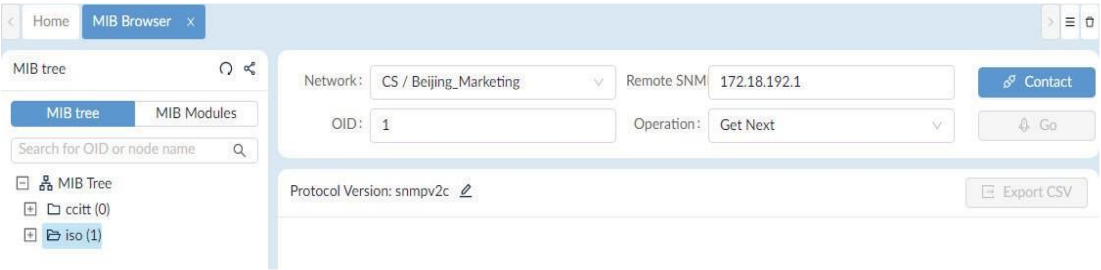
4.4.3. MIBs

Management Information Base (MIB) is an organized data that facilitates configuration and query of network devices. The D-View 8 provides a MIB browser to help extract data polled via SNMP. It supports all 3 versions of SNMP. MIB objects should be displayed after a successful connection.

To view MIBs with a MIB browser.

1. Go to **Tools > MIB Browser**.

2. Select the MIB file from the left pane to obtain information of each object or select the network and enter the SNMP agent IP address to contact with.



Network: CS / Beijing_Marketing
Remote SNM: 172.18.192.1
OID: 1
Operation: Get Next
Protocol Version: snmpv2c

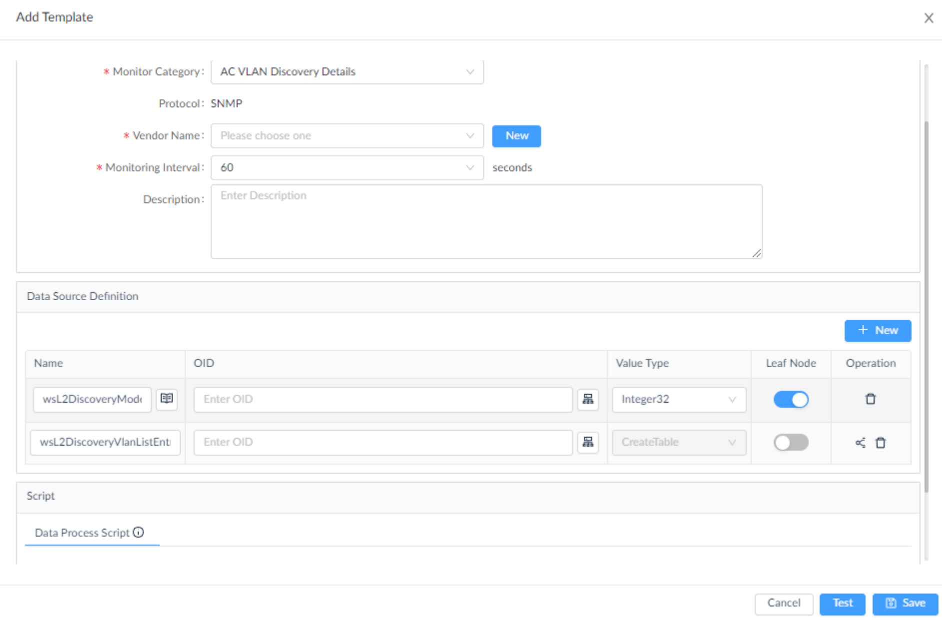
For detailed instructions, refer to 15.1 MIB Browser.

4.4.4. Monitor Devices with SNMP

SNMP can be used to monitor devices and the network by collecting data of packet transmission and associated errors and presenting them in a report.

To monitor devices with SNMP:

1. Go to **Templates > Monitor Template**. Create a monitor category defining the source data type. Then create a monitor template with specific OIDs according to the data type defined in the category.



* Monitor Category: AC VLAN Discovery Details

Protocol: SNMP

* Vendor Name: Please choose one

* Monitoring Interval: 60 seconds

Description: Enter Description

Data Source Definition

Name	OID	Value Type	Leaf Node	Operation
wsL2DiscoveryMod	Enter OID	Integer32	●	🗑
wsL2DiscoveryVlanListEnt	Enter OID	CreateTable	○	🗑

Script

Data Process Script ⓘ

2. Go to **Templates > Device Template**. Then associate a device model with the configured template.

For detailed instructions, refer to 11.1 Generate Device Template and 11.4 Generate Monitor Template.

4.4.5. View Traps and Generate Alarms for Traps

Traps can be viewed from the D-View 8 application and forwarded from the D-View 8 server to a configured destination. Alerts can also be triggered when a specific trap has been sent.

To enable traps on a device:

1. Go to **Monitoring > Device View**.

2. Select a device to open the **Device Information** page. Then click the **Management** tab and enable **Trap Status** to set the D-View as the trap server.

3. You can then obtain trap information on the **Trap& Syslog** tab of the **Device Information** page or by going to **Alarm & Notification > Trap & Syslog**.

To manage traps:

1. Go to **Alarm & Notification > Trap & Syslog** to view all trap events.

2. You can also define a trap OID by adding an OID description in the **Trap & Syslog Editor** menu below.

Refer to 7.2 View Traps and Syslog and 7.3 Trap Editor.

To set an alarm with a specific trap:

1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then click the **Alarm Settings** tab.

Scroll down to the Trap section for traps that are available for triggering an alarm. Then click **Add** to add an alarm rule to define a trigger condition with the specified trap OID or binding values for a variable.

For detailed instructions, refer to 7.5.1 Alarm Settings.

To forward traps:

1. Go to **System > Basic Settings**. Then click the **Forward Trap** tab.

2. Click **Add Destination Host** to add a destination to send the traps.

4.5. Manage Multiple Networks with Batch Configuration

The D-View 8 allows for batch configuration of devices across networks using a pre-configured schedule. To start, a configuration template must be created. There are pre-configured templates and customized templates. You also have the option of two different configuration types – quick configuration for a single configuration category or advanced configuration for multiple sets of configuration categories when setting batch configuration.

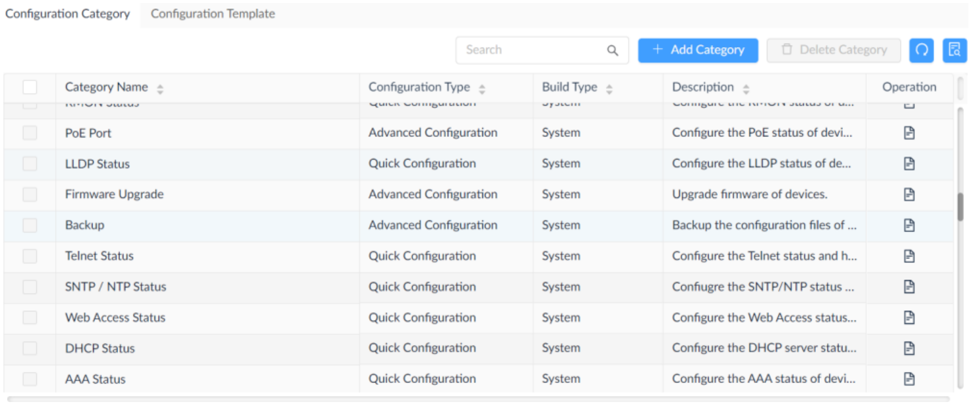
4.5.1 Create Configuration Templates

A configuration category which defines the components of the configuration items and their layout needs to be created first.

To create a configuration category:

1. Go to **Templates > Configuration Template**.

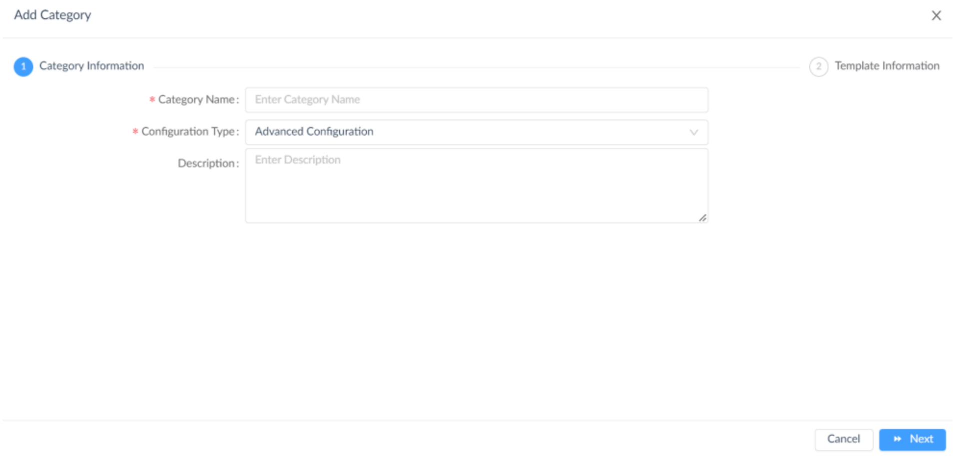
2. The Configuration Category displays:



	Category Name	Configuration Type	Build Type	Description	Operation
□	PoE Port	Advanced Configuration	System	Configure the PoE status of devi...	
□	LLDP Status	Quick Configuration	System	Configure the LLDP status of de...	
□	Firmware Upgrade	Advanced Configuration	System	Upgrade firmware of devices.	
□	Backup	Advanced Configuration	System	Backup the configuration files of ...	
□	Telnet Status	Quick Configuration	System	Configure the Telnet status and h...	
□	SNTP / NTP Status	Quick Configuration	System	Confiugre the SNTP/NTP status ...	
□	Web Access Status	Quick Configuration	System	Configure the Web Access status...	
□	DHCP Status	Quick Configuration	System	Configure the DHCP server statu...	
□	AAA Status	Quick Configuration	System	Configure the AAA status of devi...	

It lists two build types of configuration categories: System and User. The user type is created by users whereas system type is created by system and cannot be modified. It also gives a brief description of each configuration category.

3. Click **Add Category** to add a configuration category:



* Category Name: Enter Category Name
* Configuration Type: Advanced Configuration
Description: Enter Description

Enter the required information and click **Next** to continue. For **Configuration Type**, the **Quick Configuration** category will be available for Quick Configuration whereas the **Advanced Configuration** will be available for configuration profiles for Advanced Configuration in **Batch Configuration**.

In the design window, select the layout first with the following options: one-full column, two columns, three columns, or four columns. Then select the input controls and text fields to be displayed.

4. Click **Save** to create the category.

To create a configuration template:

1. Select the created category in the left pane, then click **Add Template** at the top right.

2. Enter a Name for the template, choose the Vendor from the drop-down menu, then enter a description for the template. Also choose the Protocol and CLI command to process the input values if SSH/Telnet has been selected as the communication protocol.

3. Modify or add more control or input elements to the design or configure the component settings of the preset configuration items.

4. Click **Save** to create the template.

You can choose to edit the template once it is created. Or you can preview the final layout of the template, delete it or download it as a JSON (JavaScript Object Notation) file.

To associate devices with a template

Once a template has been created, devices associated with this template can utilize its configuration as a base.

To associate devices with a template:

1. Go to **Templates > Device Template**.

2. Choose the device model from the **Device Type** pane.

3. Select **Configuration** at the bottom of the **Template Information** window. Then select **Associate Configuration Template** to choose the desired configuration template to associate with.

For more detailed instructions, refer to 11.1 Generate Device Template and 11.5 Generate Configuration Template.

4.5.2 Batch Configuration

Once a template has been associated with devices, batch configuration can be used to apply a configuration or a set of configurations to selected devices.

To apply batch configuration to devices:

1. Go to **Configuration > Batch Configuration**.

2. Select either **Quick Configuration** or **Advanced Configuration** tab according to the type of the configuration template.

For Advanced Configuration, click **Add Profile** at the top right.

1. Enter a name and description for the profile, select the device model in the **Device Hierarchy** field, then select configuration categories for the device model in the **Configuration Feature List**. Note that you can select multiple categories for a profile.

2. Click **Next** to continue configuring configuration items of selected categories.

3. Click **Save** to create the configuration profile.

For **Quick Configuration**, select a configuration category in the left pane. Then create a task to apply the configuration changes (see below 4.5.3 Create Tasks for Batch Configuration).

For more detailed instructions, refer to 6.1 Create Configuration and Profiles.

4.5.3. Create Tasks for Batch Configuration

For Quick Configuration, select a configuration category in the left pane, then click **Add Task** at the upper right.

Enter the following information:

Task Information	
Task Name	Enter the name for the task.
Task Description	Enter a brief description to identify the task.
Configuration Information	
Status/Input	Apply the configuration changes for the task. For custom category, the options depend on the design of the template and selected protocol.
Target Devices	
Add Devices	Click to add the device(s) for configuration. Note that only devices that support this function can be selected. For custom configuration categories, you need to associate the configuration template to the device template first (go to **Templates > Device Template**).
Schedule Information	
Schedule Type	• **One Time**: Select this option to specify a date and time or immediately to initiate the task. • **Recurrent**: Select this option to specify the frequency and effective time frame to initiate the task. Refer to 14.2 Scheduling for more information.

You can click **Task Management** to open the **Task Management** page.

For Advanced Configuration, select a profile in the list, then click **Create Task +** under **Operation**.

Enter the following information:

Task Information	
Task Name	Enter a name for the task.
Task Description	Enter a brief description to identify the task.
Target Devices	
Add Devices	Click to add the device(s) for configuration. The Batch Select Devices screen opens. Select the desired devices or use the Search function to find devices.
Schedule Information	
Schedule Type	• **One Time**: Select this option to specify a date and time or immediately to initiate the task. • **Recurrent**: Select this option to specify the frequency and effective time frame to initiate the task. Refer to 14.2 Scheduling for more information.

Click **Save** to create the new task and return to the previous menu.
You can click **Task Management** to open the **Task Management** page. Refer to 6.2.1 Current Tasks for details about tasks.

For more detailed instructions, refer to **Apply a Profile to Devices with Task** in 6.1 Create Configuration and Profiles.

5 Monitoring and Reporting

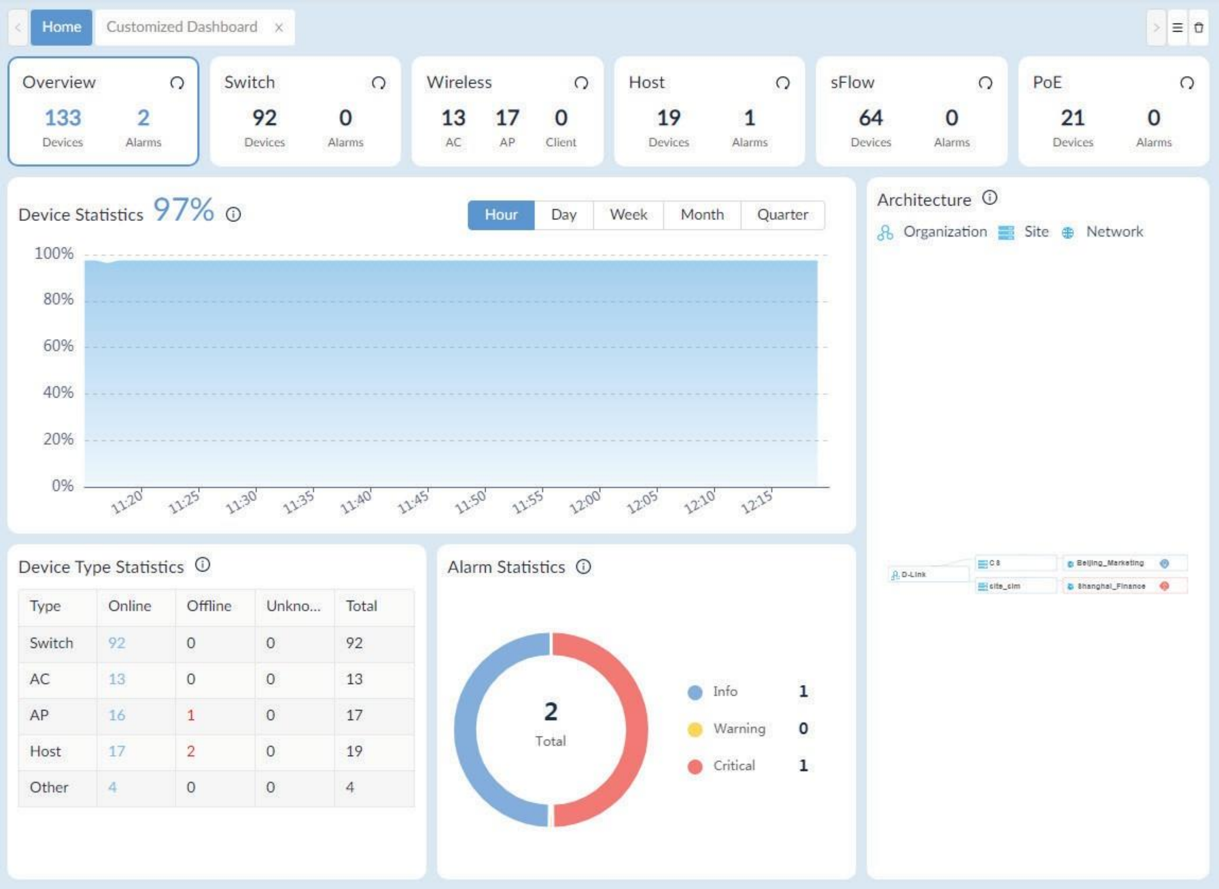
You can monitor your network through the Dashboard to obtain real-time statistics . The information to be displayed can be customized on the Customized Dashboard page.

5.1. View the Default Dashboard

The default dashboard provides information related to the distribution and management of the resources in the managed networks. The information can be used to assess, utilize, and centrally manage your networks.

Note: When the license expires, the **Dashboard** page will alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

To view the Overview dashboard, log in to the D-View 8 application. The Overview dashboard will be displayed.



Overview: 133 Devices, 2 Alarms
Switch: 92 Devices, 0 Alarms
Wireless: 13 AC, 17 AP, 0 Client
Host: 19 Devices, 1 Alarms
sFlow: 64 Devices, 0 Alarms
PoE: 21 Devices, 0 Alarms

Device Statistics 97%

Architecture

Device Type Statistics

Type	Online	Offline	Unkno...	Total
Switch	92	0	0	92
AC	13	0	0	13
AP	16	1	0	17
Host	17	2	0	19
Other	4	0	0	4

Alarm Statistics

2 Total

Info	1
Warning	0
Critical	1

By default, the overview displays the following widgets. To refresh data, click **Refresh** at the upper right.

Widget	Description
Device Statistics	The percentage of managed devices that are online.
Architecture	The D-View 8 network architecture diagram.
Device Type Statistics	The operating status of different types of managed devices.
Alarm Statistics	The distribution of alarm severity for managed devices.

You can click on any number or icon on the charts or graphs to be directed to the configuration page.

5.2. Switch Dashboard

From the Dashboard, click the Switch tab. The Switch Dashboard displays the following widgets. To refresh data, click **Refresh** ↻ at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity for managed switches.
Running Status	The online status of managed switches.
Temperature Statistics	The distribution of managed switches based on the specified temperature range: 40, 60, 80, or 90 °C.
Top 10 Wired Throughput (Rx / Tx)	The top 10 managed switches that currently send and receive the most traffic.
Top 10 Memory Utilization	The top 10 managed switches with the highest current memory utilization.
Top 10 CPU Utilization	The top 10 managed switches with the highest CPU utilization.
Top 10 Response Times	The top 10 managed switches with the longest response time according to a specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.

5.3. Wireless Dashboard

From the Dashboard, click the Wireless tab. The Wireless Dashboard displays the following widgets. To refresh data, click **Refresh** ↻ at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity for managed switches.
Running Status	The online status of wireless devices (AC/AP).
AP Summary	The distribution of AP device types.
Top 10 Wireless Throughput	The top 10 wireless devices that send and receive the most traffic in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Wireless Error Packets	The top 10 wireless devices with the most error packets in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Clients by 802.11 Protocol	The distribution of 802.11 protocol types used by the clients.
Clients by Authentication Type	The distribution of client authentication type.
Top 10 Devices by Critical Alarms	The top 10 wireless devices that generated the most critical alarms.
Top 10 SSIDs by Current Client	The top 10 SSIDs with the most clients currently connected.
Top 10 Response Times	The top 10 wireless devices with the longest response time in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 APs by Current Client	The top 10 APs with the most clients currently connected.

5.4. Host Dashboard

From the Dashboard, click the Host tab.The Host Dashboard displays the following widgets. To refresh data, click **Refresh** ↻ at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity for all hosts.
Running Status	The online status of host devices.
Top 10 CPU Utilization	Display the top 10 hosts with the highest CPU utilization.
Top 10 Memory Utilization	Displays the top 10 hosts with the highest memory utilization in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Most Installed Applications	Display the top 10 most installed applications on the hosts in the network.
Top 10 Volumes with Most Disk Usage	Display the top 10 volumes with the most disk usage in the network.
Top 10 Response Times	Display the top 10 hosts with the longest response time in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Volumes with Least Disk Usage	Display the top 10 volumes with the least disk usage in the network.

5.5. sFlow Dashboard

From the Dashboard, click the sFlow tab. The sFlow panel displays the following widgets. To refresh data, click **Refresh** ↻ at the upper right. Note that sFlow Dashboard is only supported in Enterprise version.

Widget	Description
Top 10 Endpoints	Display the top 10 most used endpoints.
Alarm Statistics	The distribution of alarm severity in the network.
Top 10 Applications	Display the top 10 applications with the most traffic in the specified time frame: last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 QoS	Display the top 10 QoS with the most traffic in the specified time frame: last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Protocols	Display the top 10 protocols with the most traffic in the specified time frame: last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Conversations	Display the top 10 conversations with the most traffic in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.

5.6. PoE Dashboard

From the Dashboard, click the PoE details panel. The PoE panel displays the following widgets. To refresh data, click **Refresh** ↻ at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity of the managed PoE devices.
Running Status	The online status of the managed PSE devices.
Top 10 PSEs by Current PD Count	The top 10 PSE devices with respect to the number of powered devices.
Top 10 Ports by Current Flow	The top 10 PoE device ports with the highest data flow.
Top 10 Ports by Power Output	The top 10 PoE ports with the highest power consumption.
Top 10 PSEs by Power Output	The top 10 PSE devices with the highest power output.
Top 10 Response Times	The top 10 PoE devices with the longest response time in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.

5.7. Customize the Dashboard

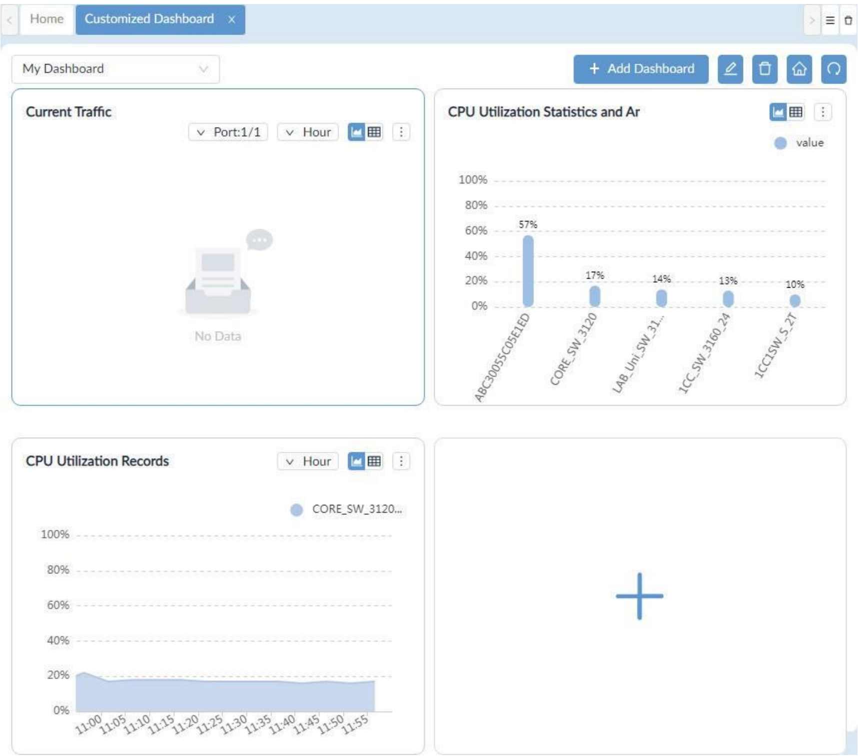
By default, the application displays the dashboard with standard information. You can customize the dashboard views by selecting the widgets.

5.7.1. Create a Customized Dashboard

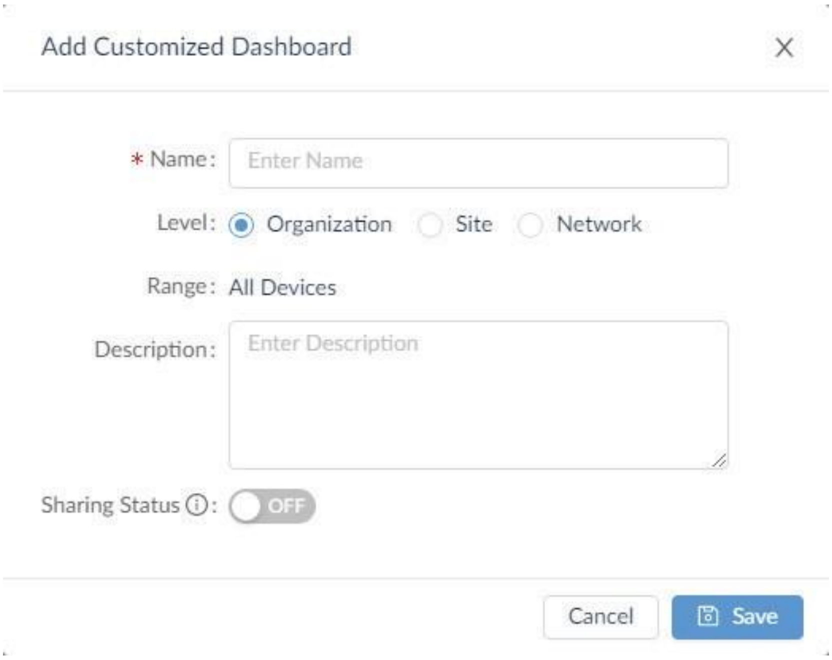
To create a customized dashboard:

1. Go to **Dashboard > Customized Dashboard**.

   The Customized Dashboard page displays.



2. Click **Add Dashboard**. The **Add Customized Dashboard** page displays.


Add Customized Dashboard

* Name: Enter Name

Level: ● Organization ○ Site ○ Network

Range: All Devices

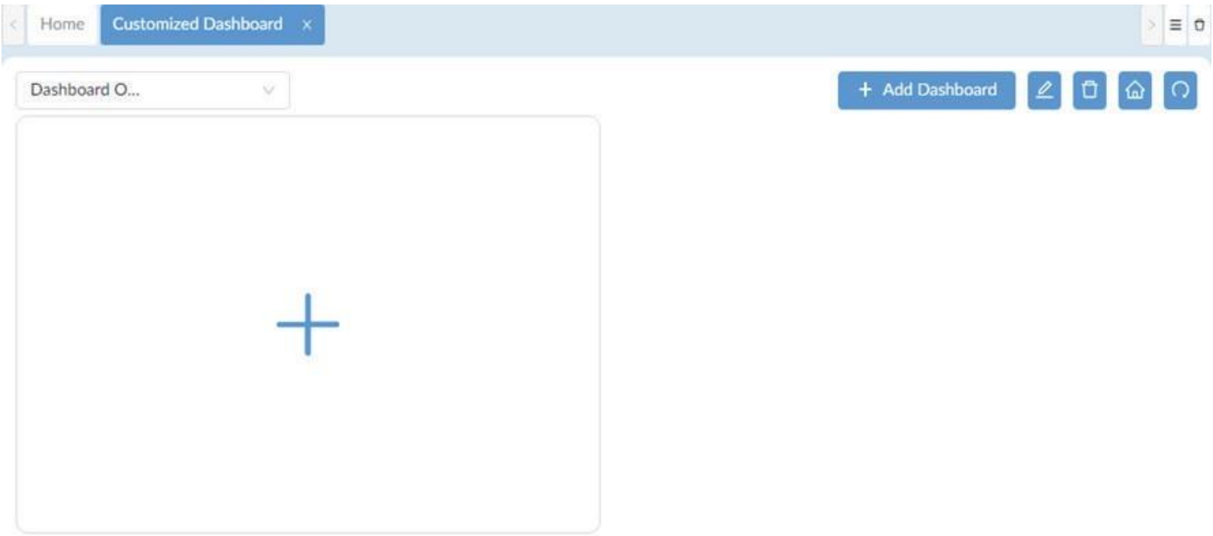
Description: Enter Description

Sharing Status ⓘ: OFF

Enter the following information:

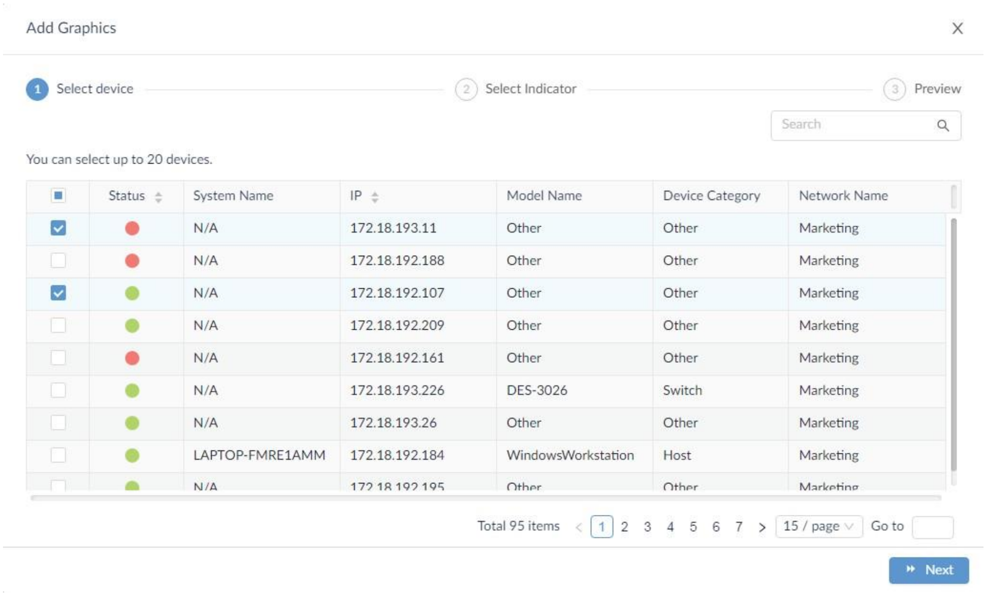
Item	Description
Name	Enter a name for the new dashboard.
Level	Click to select the network hierarchy level (default: Organization).
Organization	Add all discovered devices within the organization.
Site	Click the Range drop-down menu to select the devices within the desired site.
Network	Click the Range drop-down menu to select the devices within the desired network.
Description	Enter a short description to identify the group.
Sharing status	Slide the option to enable or disable (default) the sharing of the dashboard. After enabling the sharing status, other administrators with authorized role in your organization will be able to view or edit it.
Save	Click **Save** to create the dashboard.

The customized dashboard displays.



3. On the dashboard for the specified network level, click + (Add) to add a graphical presentation of network performance indicator to the dashboard.The **Add Graphics** page displays.
4. In the Select device step, select device(s) for the source data.

Or you can search devices by one of the following properties: System Name, IP, Model Name, Device Category, or Network Name. Then click **Next** to continue.



Add Graphics X

1 Select device — 2 Select Indicator — 3 Preview

Search

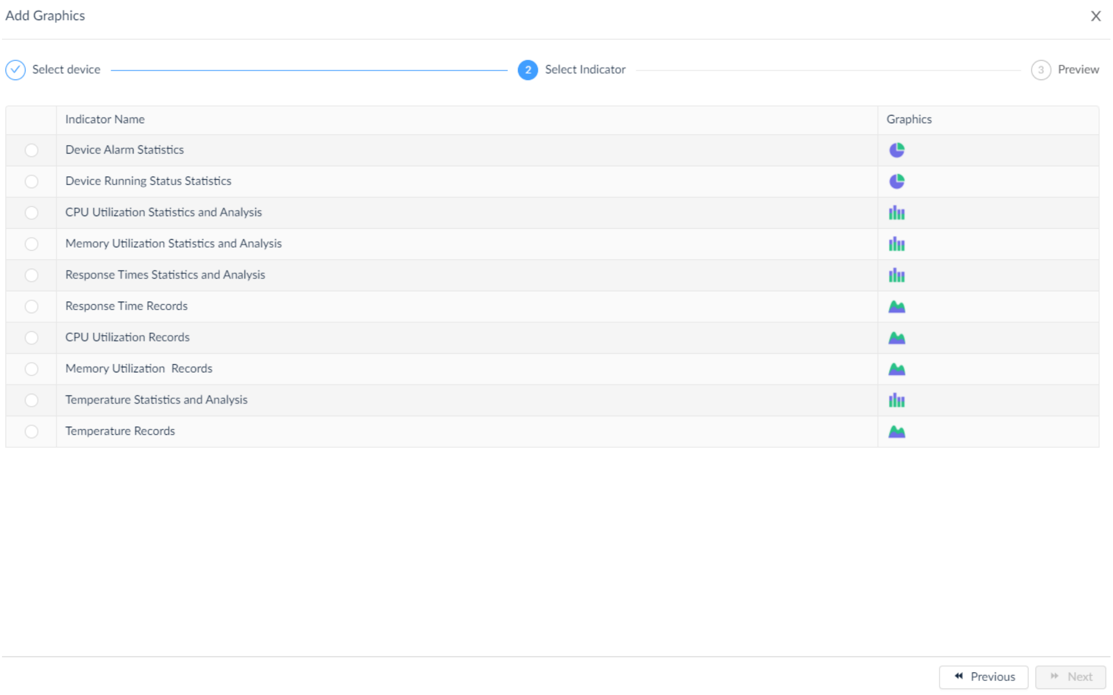
You can select up to 20 devices.

■	Status	System Name	IP	Model Name	Device Category	Network Name
☑	🔴	N/A	172.18.193.11	Other	Other	Marketing
□	🔴	N/A	172.18.192.188	Other	Other	Marketing
☑	🟢	N/A	172.18.192.107	Other	Other	Marketing
□	🟢	N/A	172.18.192.209	Other	Other	Marketing
□	🔴	N/A	172.18.192.161	Other	Other	Marketing
□	🟢	N/A	172.18.193.226	DES-3026	Switch	Marketing
□	🟢	N/A	172.18.193.26	Other	Other	Marketing
□	🟢	LAPTOP-FMRE1AMM	172.18.192.184	WindowsWorkstation	Host	Marketing
□	🟢	N/A	172.18.192.195	Other	Other	Marketing

Total 95 items < 1 2 3 4 5 6 7 > 15 / page Go to

Next

5. Click on an indicator to define the statistics. The availability of performance indicators depends on the supported device functions. Also, the report timing for some statistics depends on the polling interval of the respective monitoring function. To edit monitoring status or interval, go to **Alarm & Notification > Monitor & Alarm Settings > Monitor Settings**. You can also adjust monitoring status or interval by accessing the device information page (go to **Monitoring > Device View** and select the **System Name** link to open the device information page and click the **Monitor** tab.)



Add Graphics X

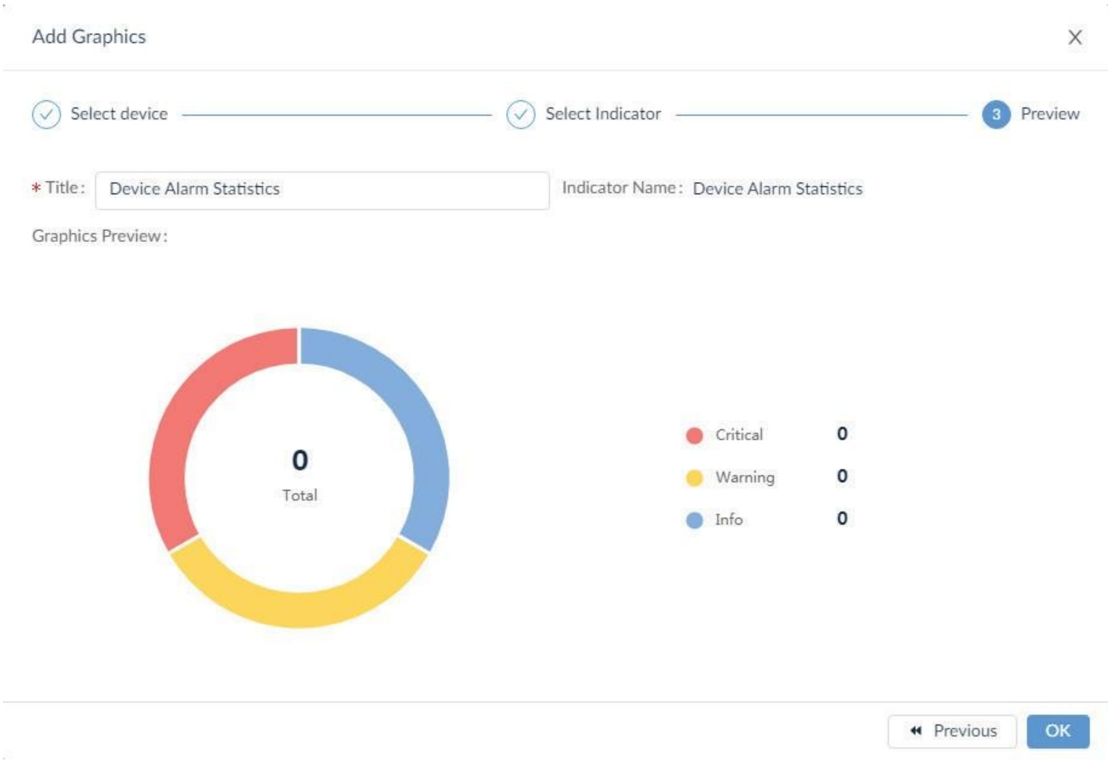
✓ Select device — 2 Select Indicator — 3 Preview

	Indicator Name	Graphics
○	Device Alarm Statistics	◔
○	Device Running Status Statistics	◔
○	CPU Utilization Statistics and Analysis	📊
○	Memory Utilization Statistics and Analysis	📊
○	Response Times Statistics and Analysis	📊
○	Response Time Records	📈
○	CPU Utilization Records	📈
○	Memory Utilization Records	📈
○	Temperature Statistics and Analysis	📊
○	Temperature Records	📈

Previous Next

- Device Alarm Statistics
- Device Running Status Statistics
- CPU Utilization Statistics and Analysis
- Memory Utilization Statistics and Analysis
- Response Times Statistics and Analysis
- Response Time Records
- CPU Utilization Records
- Memory Utilization Records
- Wireless Throughput (Bytes)
- Total Bytes Transmitted
- Total Packets Transmitted
- Current Traffic
- Packets Per Second
- Interface Utilization
- Total Errors and Discards
- Discard Rate
- Error Rate
- Wireless Throughput (Packets)
- Wireless Error Packets
- Wireless Clients by Protocol
- Wireless Clients by Authentication Type
- Wireless Clients by SSID
- Wireless Clients by AP
- SIM Traffic
- Temperature Statistics and Analysis
- Temperature Records

The Preview page displays.



Add Graphics

Select device — Select Indicator — 3 Preview

*Title: Device Alarm Statistics

Indicator Name: Device Alarm Statistics

Graphics Preview:

0 Total

● Critical 0

● Warning 0

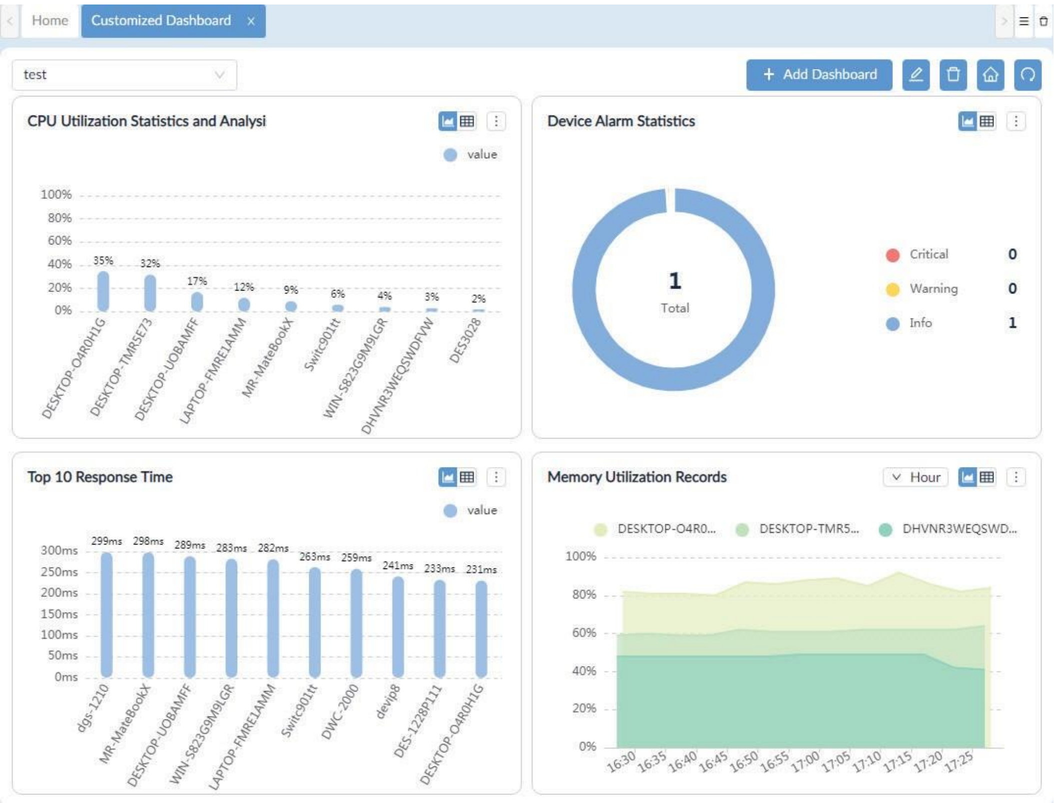
● Info 0

7. Click **OK** to create the new graphical presentation.

5.7.2. Modify a Customized Dashboard

To modify a customized dashboard:

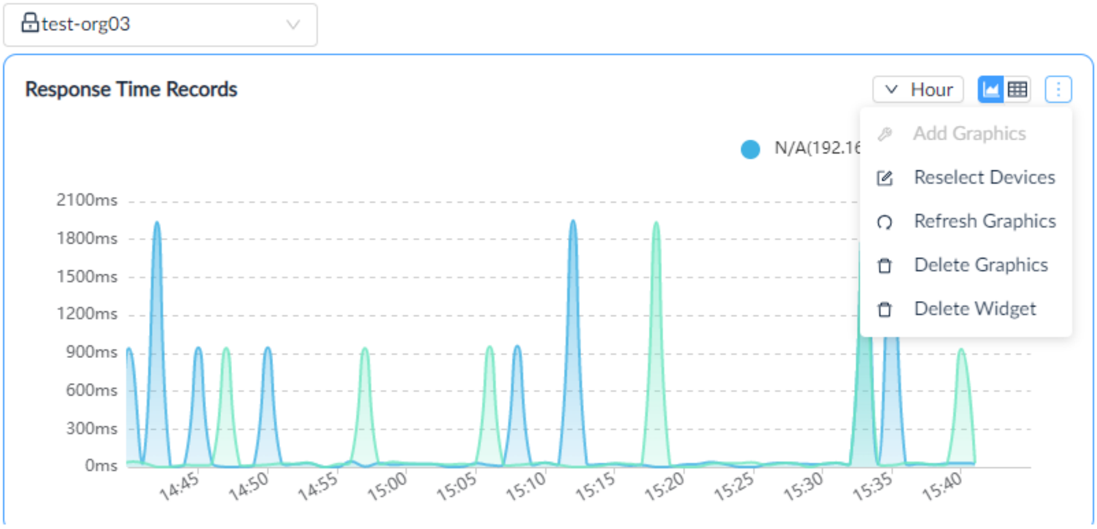
1. Go to **Dashboard > Customized Dashboard**.The **Customized Dashboard** page displays.



Click **Edit** at the upper right to modify the dashboard or **Delete** to delete the dashboard. You can also modify a widget of the dashboard.

The following example uses CPU Utilization Statistics and Analysis widget:

2. Click on the **More Settings** button. Available options depend on the widget function.



3. Click to perform an action:

Refresh Graphics: re-sync the function information.
Delete Graphics: remove the graphic from the widget frame.
Add Graphics: when the graphic is deleted, add a new performance indicator.
Delete Widget: remove the widget from the dashboard.
Reselect Devices: specify a different device(s).

The widget will be updated. The new dashboard can also be applied to the Home page to replace the default system dashboard. Click **Apply to homepage** ⌂ at the upper right.

5.8. View and Export Reports

The system provides a method to view information regarding the performance and resource utilization on the network.

The following reports are available:

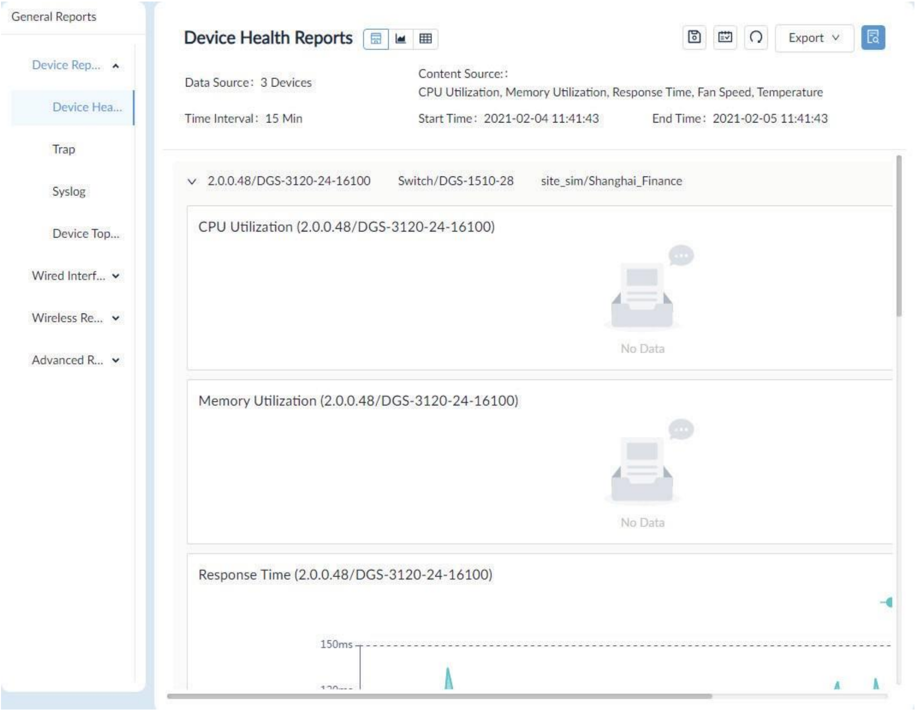
- General Reports
- Scheduled Reports
- My Reports

The period for statistics generation is based on the scheduled retention period. To view and export reports:

1. Go to **Reports > General Reports**.
2. Select the report type from the General Reports pane.

Report Category	Category	Event
General Reports	Device Reports	Device Health Reports
		Trap Reports
		Syslog Reports
		Device Top N Reports
	Wired Interface Reports	Wired Traffic Reports
		Wired Throughput Top N Reports
	Wireless Reports	Wireless Client Count Reports
		Wireless Traffic Reports
	Advanced Reports	Inventory Reports
Scheduled Reports	One Time	
	Recurrent	
My Reports	My Reports	

3. From Reports, click **General Reports**. The default Device Health Reports page displays.



Device Health Reports

Data Source: 3 Devices

Content Source::
CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature

Time Interval: 15 Min

Start Time: 2021-02-04 11:41:43

End Time: 2021-02-05 11:41:43

2.0.0.48/DGS-3120-24-16100 Switch/DGS-1510-28 site_sim/Shanghai_Finance

CPU Utilization (2.0.0.48/DGS-3120-24-16100)

Memory Utilization (2.0.0.48/DGS-3120-24-16100)

Response Time (2.0.0.48/DGS-3120-24-16100)

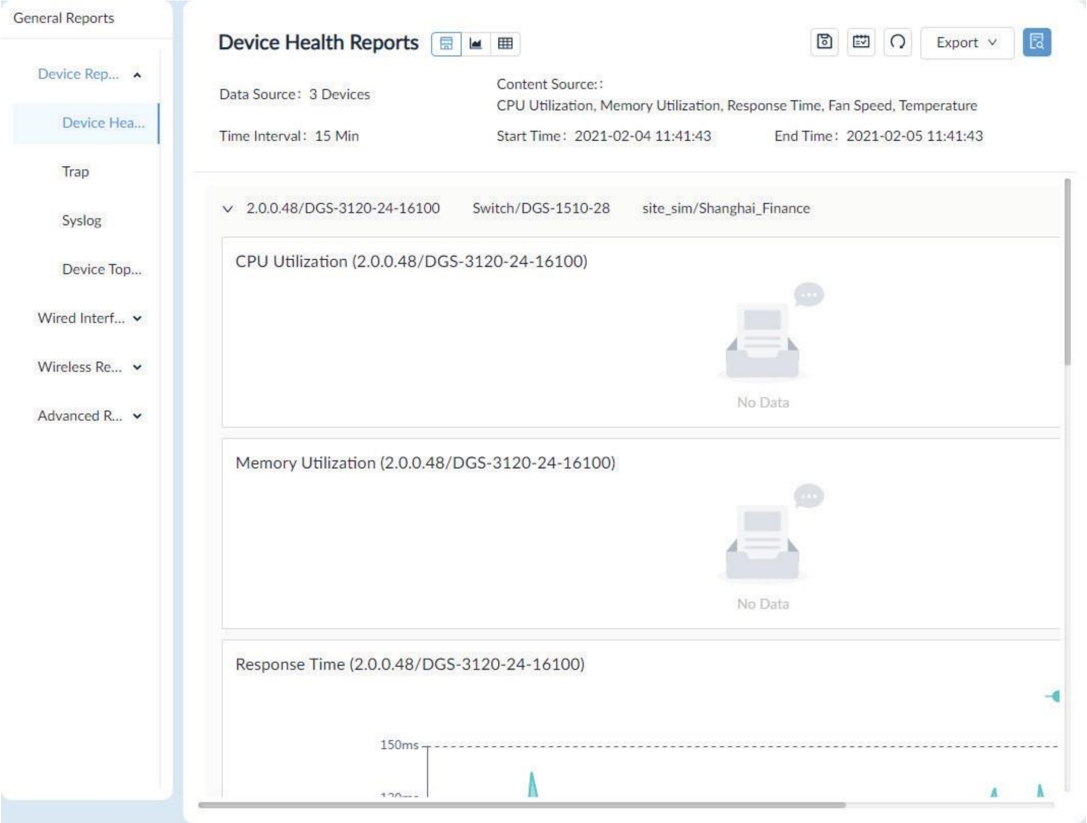
You will need to configure the settings if a report does not display any data. Refer to the below section for more information.

4. Click the **Export** drop-down menu at the top right and select the type of file format for download: PDF, Excel, or CSV.The report file is downloaded to the default download folder of your browser.

5.9. View Report Settings

1. From Reports, click **General Reports**.

   The default **Device Health Reports** page displays.



Device Health Reports

Data Source: 3 Devices

Content Source::
CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature

Time Interval: 15 Min

Start Time: 2021-02-04 11:41:43

End Time: 2021-02-05 11:41:43

2.0.0.48/DGS-3120-24-16100 Switch/DGS-1510-28 site_sim/Shanghai_Finance

CPU Utilization (2.0.0.48/DGS-3120-24-16100)

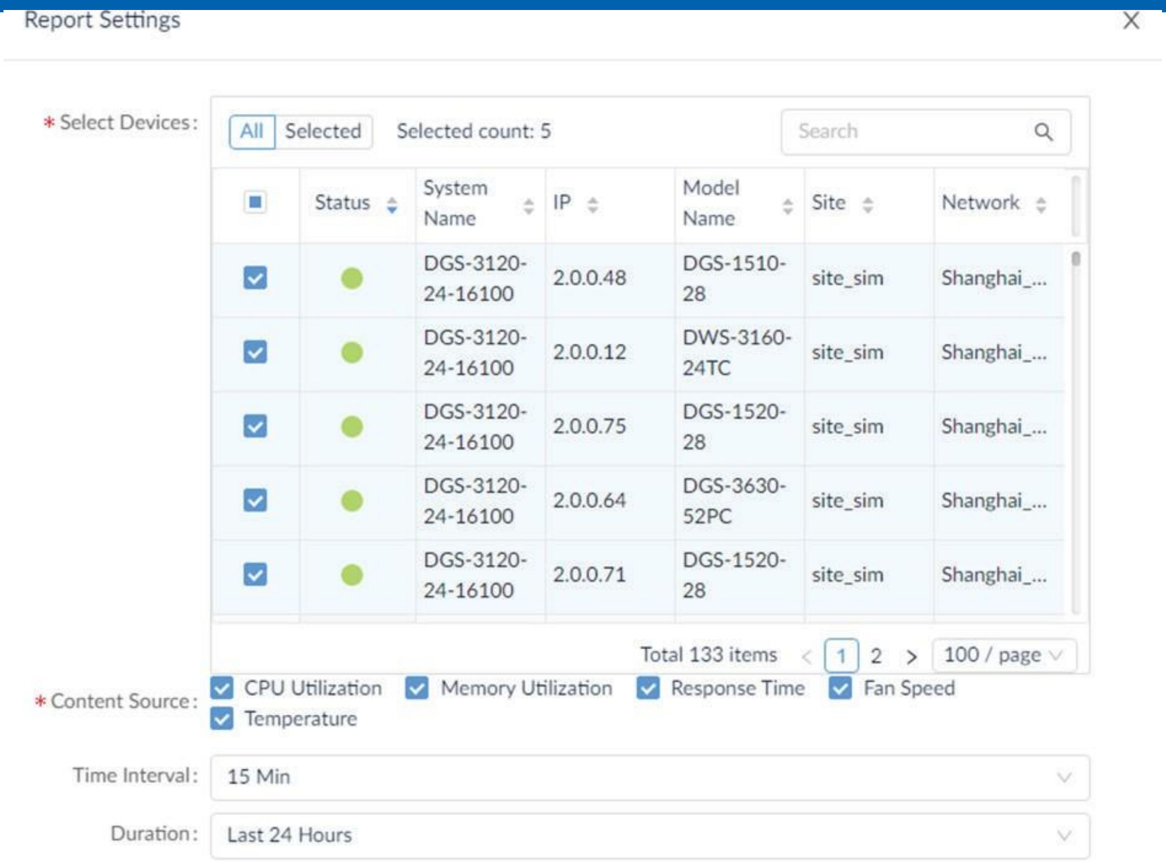
Memory Utilization (2.0.0.48/DGS-3120-24-16100)

Response Time (2.0.0.48/DGS-3120-24-16100)

The toolbar displays available functions:

Item	Description
Show All	Display all information.
Show Chart Only	Display available information in chart format.
Show Table Only	Display available information in tabular format.
Save to My Reports	Designate the current report as My Report.
Upgrade to Scheduled Reports	Designate the current report as Scheduled Report.
Refresh	Re-synchronize the report information.
Export Export ∨	Save the information to a file.
Report Settings	Configure the settings for the current report type.

2. Click **Report Settings** . The **Report Settings** page displays.



Report Settings

* Select Devices: All | Selected Selected count: 5 Search

☑	Status	System Name	IP	Model Name	Site	Network
☑	●	DGS-3120-24-16100	2.0.0.48	DGS-1510-28	site_sim	Shanghai_...
☑	●	DGS-3120-24-16100	2.0.0.12	DWS-3160-24TC	site_sim	Shanghai_...
☑	●	DGS-3120-24-16100	2.0.0.75	DGS-1520-28	site_sim	Shanghai_...
☑	●	DGS-3120-24-16100	2.0.0.64	DGS-3630-52PC	site_sim	Shanghai_...
☑	●	DGS-3120-24-16100	2.0.0.71	DGS-1520-28	site_sim	Shanghai_...

Total 133 items < 1 2 > 100 / page

* Content Source: ☑ CPU Utilization ☑ Memory Utilization ☑ Response Time ☑ Fan Speed ☑ Temperature

Time Interval: 15 Min

Duration: Last 24 Hours

Available report setting options:

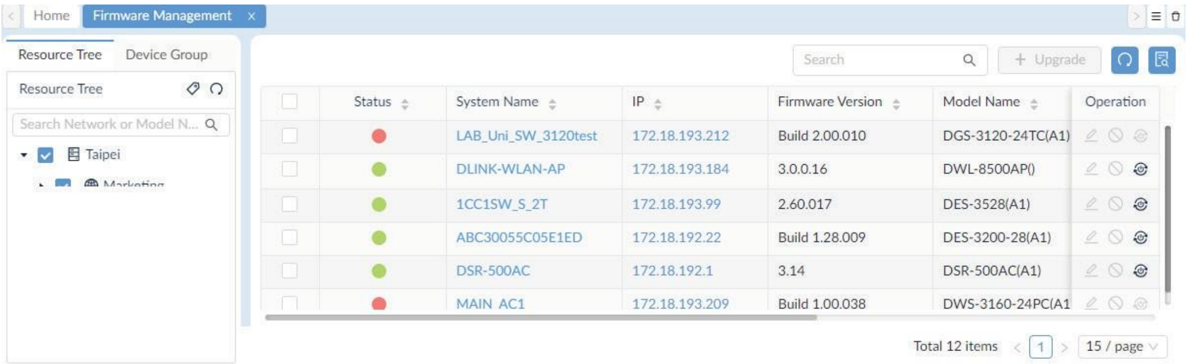
Item	**Description**
Select Devices	Click the slide bar to view All or only the Selected devices. To select a device, click a specific device.
Search	Enter a keyword to search for a device by System Name, IP, Model Name, Site, or Network.
Content Source	Click the report type: CPU Utilization, Memory Utilization, Response Time, Fan Speed, or Temperature.
Time Interval	Click to set the interval time to define the display interval for the report: Configured minimum interval, 15 min., 2 Hour, 8 Hour, 1 Day.
Duration	Click to select the duration for each report: Last 24 Hours, Today, Yesterday, Customized. If you select Customized, enter the Start and End Time.
Reset	Click to reset the report settings to the default settings.
Save	Click Save to create the report.
Note: The report settings vary depending on the report type.	

5.10. View Firmware Version

You can view the firmware version for all discovered D-Link devices.

To view the firmware version:

1. Go to **Configuration > Firmware Management**.
   The Firmware Management page displays.



	Status	System Name	IP	Firmware Version	Model Name	Operation
□	🟥	LAB_Uni_SW_3120test	172.18.193.212	Build 2.00.010	DGS-3120-24TC(A1)	
□	🟩	DLINK-WLAN-AP	172.18.193.184	3.0.0.16	DWL-8500AP()	
□	🟩	1CC1SW_S_2T	172.18.193.99	2.60.017	DES-3528(A1)	
□	🟩	ABC30055C05E1ED	172.18.192.22	Build 1.28.009	DES-3200-28(A1)	
□	🟩	DSR-500AC	172.18.192.1	3.14	DSR-500AC(A1)	
□	🟥	MAIN_AC1	172.18.193.209	Build 1.00.038	DWS-3160-24PC(A1	

Total 12 items < 1 > 15 / page

To upgrade firmware for devices”

2. Select devices for firmware upgrade.

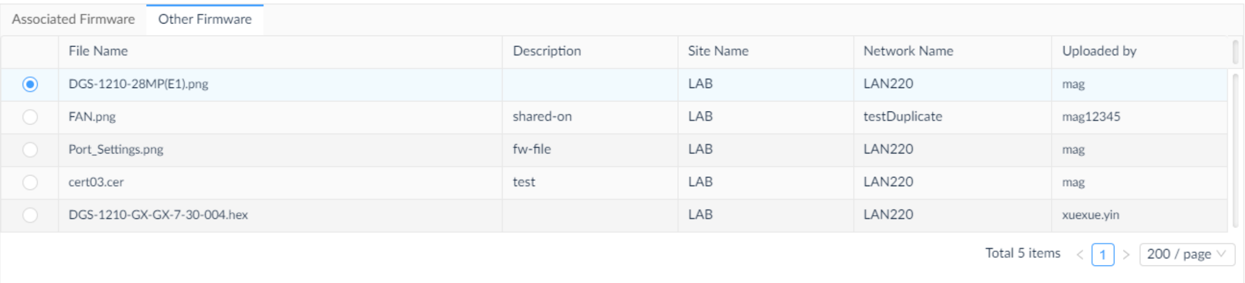
NOTE: If multiple devices are selected, make sure that correct firmware is selected for update for each model.

3. Click **Upgrade** to display Firmware Upgrade page.

4. Under **Firmware File**, click **Select Firmware File** to view available firmware sources.

NOTE: Make sure that you confirm the firmware version and its compatibility with the device before proceeding. Refer to **Configuration > File Management** for firmware files that have been uploaded to the D-View 8 server.

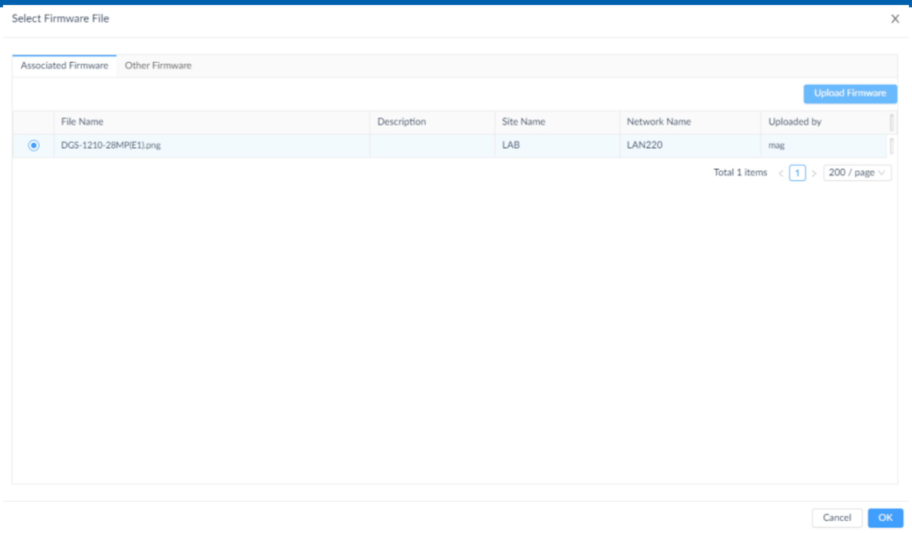
5. On the **Other Firmware** tab, select the appropriate file and click **OK** to continue. These firmware files have been uploaded to the D-View 8 server (refer to **Configuration > File Management**).



	File Name	Description	Site Name	Network Name	Uploaded by
●	DGS-1210-28MP(E1).png		LAB	LAN220	mag
○	FAN.png	shared-on	LAB	testDuplicate	mag12345
○	Port_Settings.png	fw-file	LAB	LAN220	mag
○	cert03.cer	test	LAB	LAN220	mag
○	DGS-1210-GX-GX-7-30-004.hex		LAB	LAN220	xuexue.yin

Total 5 items < 1 > 200 / page

6. Alternatively, select the **Associate Firmware** tab to view firmware that was uploaded specifically for this device model or to upload firmware from a local directory, then click **Upload Firmware.**



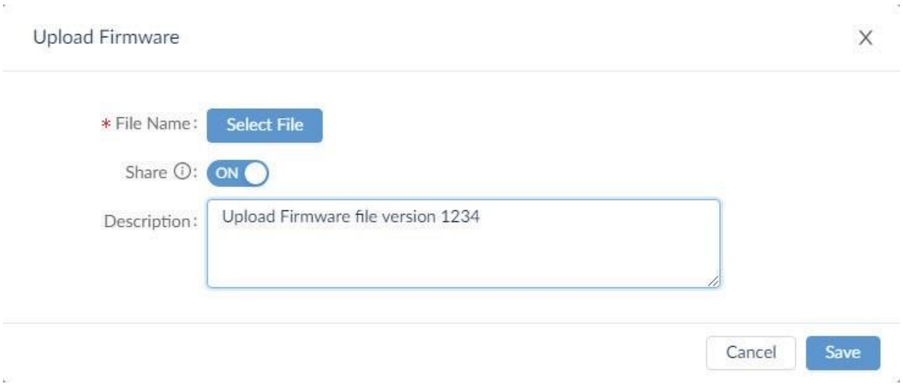
Select Firmware File

Associated Firmware | Other Firmware

	File Name	Description	Site Name	Network Name	Uploaded by
●	DGS-1210-28MP(E1).png		LAB	LAN220	mag

Total 1 items < 1 > 200 / page

7. The **Upload Firmware** page appears. The **Share** slide bar can be used to enable or disable sharing this firmware file with other networks besides the device's current network. After selecting the firmware, click **Save** to upload the file selection or **Cancel** to delete the upload.



Upload Firmware

* File Name: Select File

Share ⓘ: ON

Description: Upload Firmware file version 1234

8. From the Firmware Upgrade page, set the Schedule under Schedule Information:
   - Schedule Type: One Time
   - Execution Time:
     - Immediately: start the firmware updating once the upload file is saved.
     - Specify a Date: click the **Date** drop-down menu to select a date and time.

   Click **OK** to set the date.

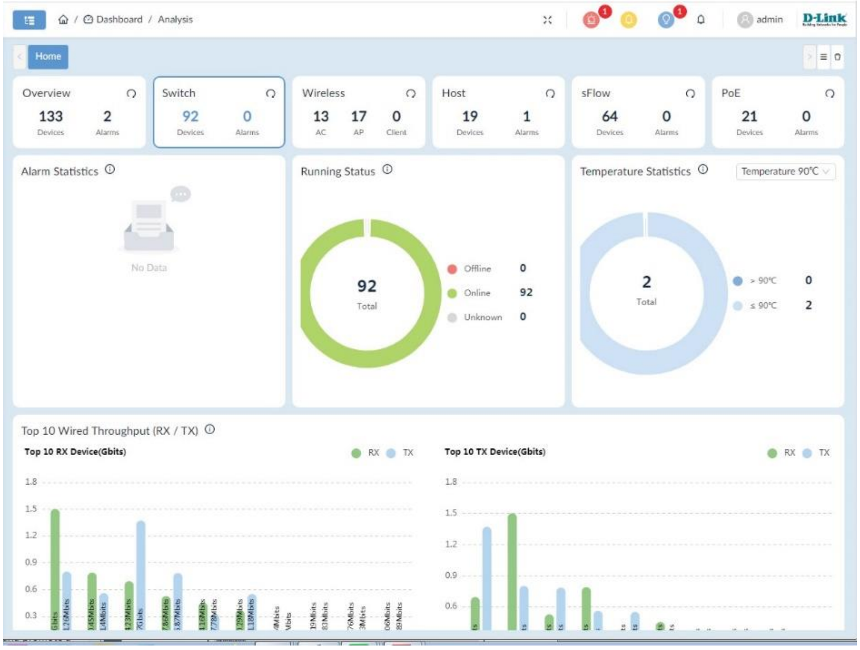
9. From Reboot Type, click **Reboot by D-View 8** to enable a restart of the device through the D-View 8 application. By default, the Reboot by D-View 8 option is disabled. A reboot is generally required for the new firmware to take effect.
10. Click **Save** to confirm the new upgrade job. Click **Cancel** to return to the previous menu.

5.11. View D-View 8 Notifications

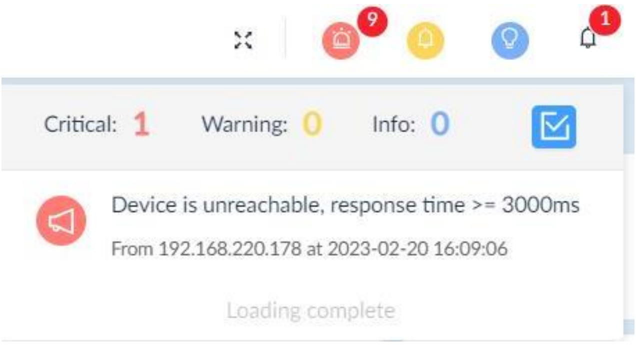
D-View 8 provides notifications via the D-View 8 web application and email. You can configure the notification rules for events that required immediate attention. For more information, refer to 3.6 Configure the Notification Center.

To view notifications:

1. Log in to the Dashboard, see "3.2. Launching D-View 8 Web GUI".



2. On the right side of the toolbar, click the Notification icon 🔔 .The Notification message page displays.



Critical: 1 Warning: 0 Info: 0 ☑

Device is unreachable, response time >= 3000ms

From 192.168.220.178 at 2023-02-20 16:09:06

Loading complete

To clear the list, click ☑. (Note that no historical records will be kept.). Click on a notification entry to open the Alarm Details page to obtain the alarms pertinent to this notification. You can view the notification rules from the Notification Center (go to **Alarm & Notification > Notification Center**).

5.12. Monitor Multiple Networks

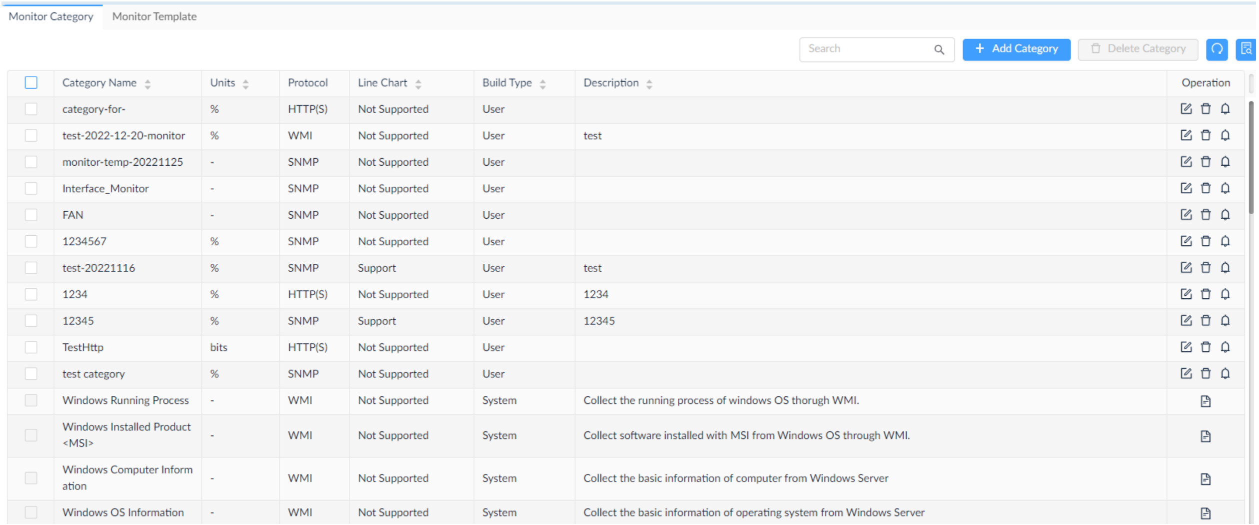
The D-View 8 allows for efficient monitoring of devices across networks with system default and customized monitor functions. To start, a monitor category and template must be created. There are system and user build monitor templates. You also have a choice among one of three communication protocols: SNMP, WMI or HTTP(s).

5.12.1 Create Monitor Templates

You need to create a monitor category first to define the communication protocol and measurement unit as well as data source definition for monitor templates. To create a monitor category:

1. Go to **Templates > Monitor Template.** Then select the **Monitor Category** tab.

2. The Monitor Category displays:



□	Category Name	Units	Protocol	Line Chart	Build Type	Description	Operation
□	category-for-	%	HTTP(S)	Not Supported	User		
□	test-2022-12-20-monitor	%	WMI	Not Supported	User	test	
□	monitor-temp-20221125	-	SNMP	Not Supported	User		
□	Interface_Monitor	-	SNMP	Not Supported	User		
□	FAN	-	SNMP	Not Supported	User		
□	1234567	%	SNMP	Not Supported	User		
□	test-20221116	%	SNMP	Support	User	test	
□	1234	%	HTTP(S)	Not Supported	User	1234	
□	12345	%	SNMP	Support	User	12345	
□	TestHttp	bits	HTTP(S)	Not Supported	User		
□	test category	%	SNMP	Not Supported	User		
□	Windows Running Process	-	WMI	Not Supported	System	Collect the running process of windows OS thorugh WMI.	
□	Windows Installed Product <MSI>	-	WMI	Not Supported	System	Collect software installed with MSI from Windows OS through WMI.	
□	Windows Computer Inform ation	-	WMI	Not Supported	System	Collect the basic information of computer from Windows Server	
□	Windows OS Information	-	WMI	Not Supported	System	Collect the basic information of operating system from Windows Server	

It lists two build types of templates: System and User. The User type is created by users whereas system type is created by system and cannot be modified.

To add a monitor category:

1. Go to **Templates > Monitor Template**. Then select the **Monitor Category** tab.

2. Click **Add Category** at the upper right.

3. Enter the following information:

Item	**Description**
Category Name	Enter a name for configuration.
Units	Select the measurement unit for configuration.
Protocol	Select the protocol for configuration: SNMP, HTTPs, or WMI.
Line Chart	Enable or disable the line chart function for graphical representation of the monitoring results. Open the **Device Information** page (go to **Monitoring > Device View** and click the **System Name** link of the selected device) and select **Monitor > Customized Monitor** to view the added monitoring results.
Description	Enter a brief description for the category.
Data Source Definition	Click Add to define a name with value type for each data type.

Click **Save** to create the monitor category.

To add a monitor template:

1. Go to **Templates > Monitor Template** and select the **Monitor Template** tab. Select the desired category from the Monitor Category pane in the left pane. Then Click **+ Add Monitor Template** at the upper right.

2. Enter the following information:

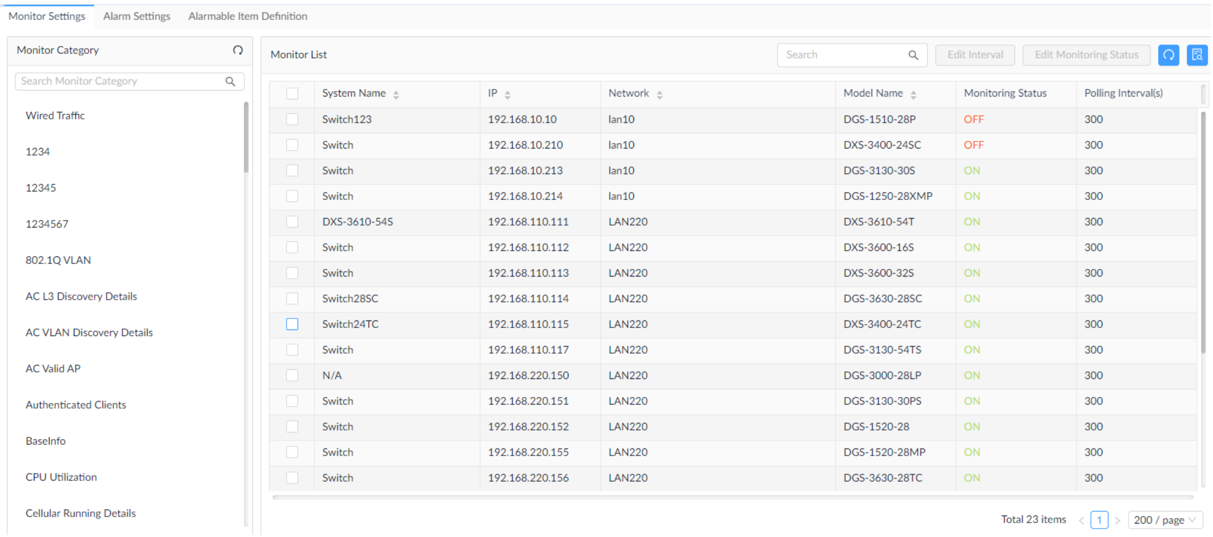
Item	**Description**
Template Name	Enter a name for the template.
Monitor Category	Select the desired category for configuration.
Vendor Name	Select the vendor with the vendor OID from the drop-down menu. Or click New at the right to add a new vendor. For more information about vendor, refer to **Templates > Device Support**.
Monitoring Interval	Select the polling interval for monitoring: 60, 300, 600, 1800, and 7200. The default is 60 seconds.
Description	Enter a brief description for this template.
Data Source Definition	Click Add to define a name with value type for the specific data object obtained from the monitored devices. The configuration options depend on the communication protocol used for device monitoring.
Script	Enter a script to process the value of the added data source in Groovy.

Click **Save** to create the monitor template. Once a template is created, you can associate it to a device model. It can then be configured for monitoring a device with the preset condition, refer to **Templates > Device Template.**

5.12.2 Configure Monitor Settings

You can configure monitoring settings such as monitoring status and polling interval.

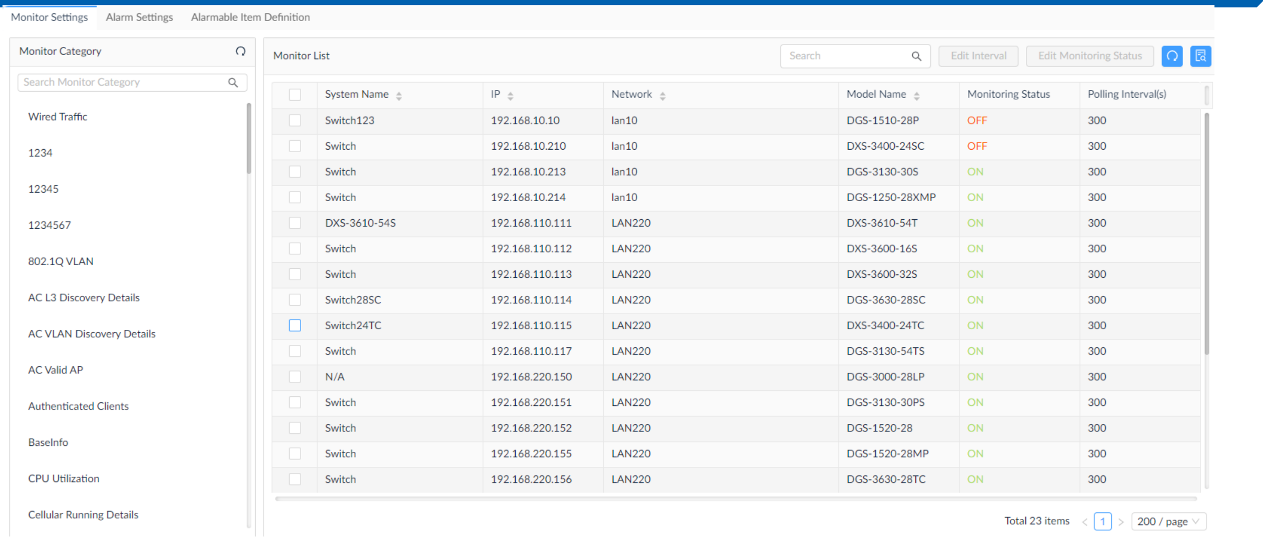
1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then Select the **Monitor Settings** tab.



□	System Name	IP	Network	Model Name	Monitoring Status	Polling Interval(s)
□	Switch123	192.168.10.10	lan10	DGS-1510-28P	OFF	300
□	Switch	192.168.10.210	lan10	DXS-3400-24SC	OFF	300
□	Switch	192.168.10.213	lan10	DGS-3130-30S	ON	300
□	Switch	192.168.10.214	lan10	DGS-1250-28XMP	ON	300
□	DXS-3610-54S	192.168.110.111	LAN220	DXS-3610-54T	ON	300
□	Switch	192.168.110.112	LAN220	DXS-3600-16S	ON	300
□	Switch	192.168.110.113	LAN220	DXS-3600-32S	ON	300
□	Switch28SC	192.168.110.114	LAN220	DGS-3630-28SC	ON	300
□	Switch24TC	192.168.110.115	LAN220	DXS-3400-24TC	ON	300
□	Switch	192.168.110.117	LAN220	DGS-3130-54TS	ON	300
□	N/A	192.168.220.150	LAN220	DGS-3000-28LP	ON	300
□	Switch	192.168.220.151	LAN220	DGS-3130-30PS	ON	300
□	Switch	192.168.220.152	LAN220	DGS-1520-28	ON	300
□	Switch	192.168.220.155	LAN220	DGS-1520-28MP	ON	300
□	Switch	192.168.220.156	LAN220	DGS-3630-28TC	ON	300

Total 23 items < 1 > 200 / page

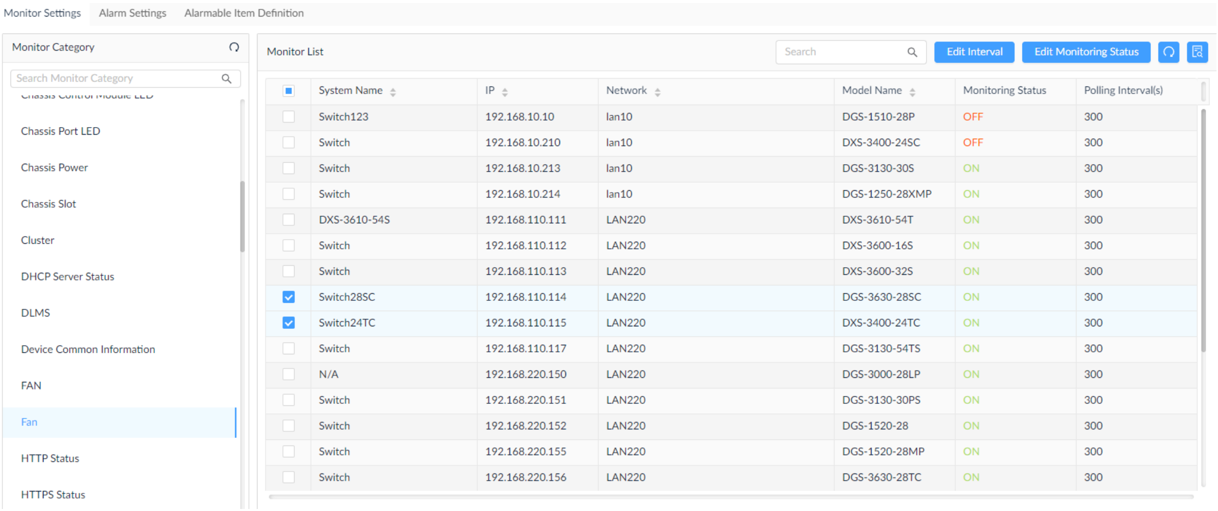
2. Select the monitor category from the left pane. The devices that have been associated with monitoring templates in this category will be displayed.



□	System Name	IP	Network	Model Name	Monitoring Status	Polling Interval(s)
□	Switch123	192.168.10.10	lan10	DGS-1510-28P	OFF	300
□	Switch	192.168.10.210	lan10	DXS-3400-24SC	OFF	300
□	Switch	192.168.10.213	lan10	DGS-3130-30S	ON	300
□	Switch	192.168.10.214	lan10	DGS-1250-28XMP	ON	300
□	DXS-3610-54S	192.168.110.111	LAN220	DXS-3610-54T	ON	300
□	Switch	192.168.110.112	LAN220	DXS-3600-16S	ON	300
□	Switch	192.168.110.113	LAN220	DXS-3600-32S	ON	300
□	Switch28SC	192.168.110.114	LAN220	DGS-3630-28SC	ON	300
□	Switch24TC	192.168.110.115	LAN220	DXS-3400-24TC	ON	300
□	Switch	192.168.110.117	LAN220	DGS-3130-54TS	ON	300
□	N/A	192.168.220.150	LAN220	DGS-3000-28LP	ON	300
□	Switch	192.168.220.151	LAN220	DGS-3130-30PS	ON	300
□	Switch	192.168.220.152	LAN220	DGS-1520-28	ON	300
□	Switch	192.168.220.155	LAN220	DGS-1520-28MP	ON	300
□	Switch	192.168.220.156	LAN220	DGS-3630-28TC	ON	300

Total 23 items < 1 > 200 / page

3. Select the devices for configuration and the **Edit Interval** and **Edit Monitoring Status** button will be activated.



■	System Name	IP	Network	Model Name	Monitoring Status	Polling Interval(s)
□	Switch123	192.168.10.10	lan10	DGS-1510-28P	OFF	300
□	Switch	192.168.10.210	lan10	DXS-3400-24SC	OFF	300
□	Switch	192.168.10.213	lan10	DGS-3130-30S	ON	300
□	Switch	192.168.10.214	lan10	DGS-1250-28XMP	ON	300
□	DXS-3610-54S	192.168.110.111	LAN220	DXS-3610-54T	ON	300
□	Switch	192.168.110.112	LAN220	DXS-3600-16S	ON	300
□	Switch	192.168.110.113	LAN220	DXS-3600-32S	ON	300
☑	Switch28SC	192.168.110.114	LAN220	DGS-3630-28SC	ON	300
☑	Switch24TC	192.168.110.115	LAN220	DXS-3400-24TC	ON	300
□	Switch	192.168.110.117	LAN220	DGS-3130-54TS	ON	300
□	N/A	192.168.220.150	LAN220	DGS-3000-28LP	ON	300
□	Switch	192.168.220.151	LAN220	DGS-3130-30PS	ON	300
□	Switch	192.168.220.152	LAN220	DGS-1520-28	ON	300
□	Switch	192.168.220.155	LAN220	DGS-1520-28MP	ON	300
□	Switch	192.168.220.156	LAN220	DGS-3630-28TC	ON	300

You can also enable or disable a monitor function on a per-device basis; go to the **Monitoring > Device View** and select the **Device Information** page by clicking the **System Name** link of the selected device. Then click the **Monitor** tab to access the **Monitoring Settings** button (refer to 4.2.2 Modify Device Information).

5.12.3 Create Alarm Rules

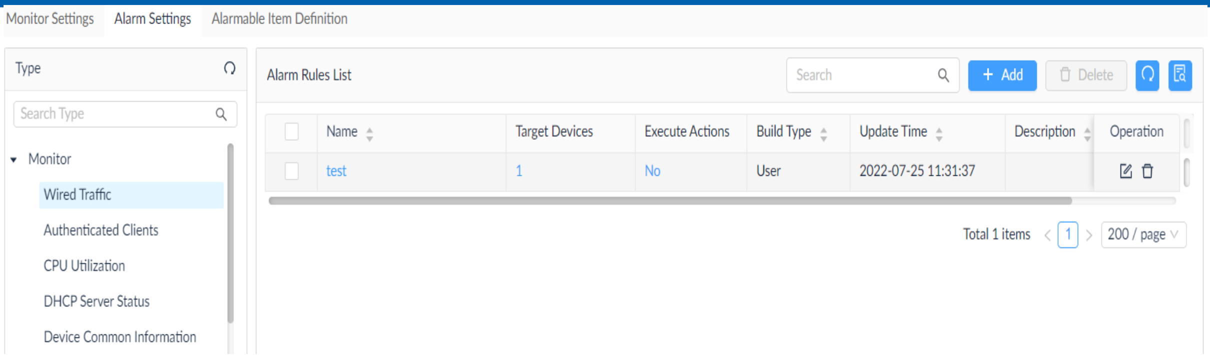
Alarms can be generated to be displayed in the Annunciator to notify users if a configured condition for alarms has been raised. Refer to 3.3.3 Annunciator.

To add an alarm rule:

1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then select the **Alarm Settings** tab.

2. From the left pane, select a monitoring condition for configuration.

3. Click +**Add** to configure a rule.



□	Name	Target Devices	Execute Actions	Build Type	Update Time	Description	Operation
□	test	1	No	User	2022-07-25 11:31:37		

The **Add Alarm Rule** page displays.

Different rules require different configurations. However, the following general settings are presented for all alarm rule types:

- Set profile information: enter a name and description for the alarm rule.
- Set alarm generation conditions: set the threshold value for different levels of severity of the alarm: Info, Warning, and Critical.
- Set alarm release conditions: set the threshold value for clearing the alarm.
- Add Inhibition Schedule Settings: select a pre-defined schedule. Or click **Add Schedule** to add a new schedule. The schedule prohibits delivery of alarms at the specified time range of a designated weekday or weekdays for the effective duration of dates.
- Select target devices: add devices for configuration.
- Set Action: execute a designated script. The script can be executed on designated device(s) other than the device configured as the alarm source or on selected D-View 8 servers. Click the respective Device Command or Server Command tab. For executing commands on device(s), configure the credentials and method for logging in to the devices.

4. Click **Next** or **OK** to continue the rule configuration.

5. Click **Save** to create the rule and exit the screen.

6 Configuration and Firmware

The D-View 8 makes it easy to save and restore device configurations. It also allows schedule-based firmware upgrade and configuration changes..

The following topics are covered:

- Create Configuration
- Manage Tasks
- Upgrade Firmware
- Back Up and Restore Device Configuration
- Import Configuration and Firmware Files

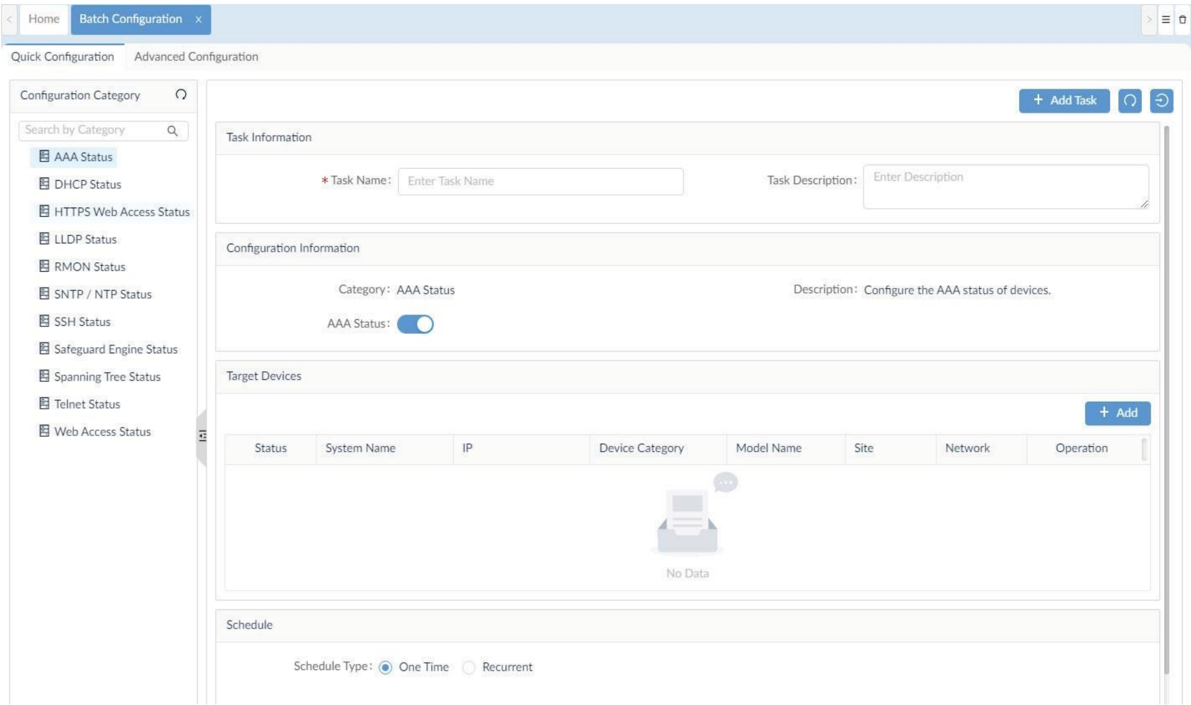
6.1. Create Configuration and Profiles

You can apply specific configurations to designated devices on the network with quick or advanced batch operations.

Note: When the license expires, the **Batch Configuration** page will alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

Add a Configuration Task

1. Go to **Configuration > Batch Configuration.** The Batch Configuration page displays.



*Task Name: Enter Task Name

Task Description: Enter Description

Category: AAA Status

Description: Configure the AAA status of devices.

AAA Status: ●

Schedule Type: ● One Time ○ Recurrent

2. From the Configuration Category, select a category or enter a keyword in the search field to search for a desired configuration category. The system default configuration categories are explained below:

AAA Status	Select to set the Authentication, Authorization, and Accounting status configuration task
DHCP Status	Select to set the DHCP Status configuration task
HTTPS Web Access Status	Select to set the HTTPS Web Access Status configuration task
LLDP Status	Select to set the Link Layer Discovery Protocol Status configuration task

SNTP/NTP	Select to set the SNTP (Simple Network Time Protocol) or NTP (Network Time Protocol) status configuration task.
RMON Status	Select to set the RMON alarm status configuration task
SSH Status	Select to set the SSH Status configuration task
Safeguard Engine Status	Select to set the Safeguard Engine Status configuration task
Spanning Tree Status	Select to set Spanning Tree Status configuration task
Telnet Status	Select to set the Telnet Status configuration task.
Web Access Status	Select to set the Web Access Status configuration task
Note: The above listed are system-built categories and it also displays customized categories of the Quick Configuration type. For user-defined categories, go to **Templates > Configuration Template** to add configuration categories and templates. Refer to 11.5 Generate Configuration Template.	

3. Complete the fields as explained below:

Task Information	
Task Name	Enter the name to define the task.
Task Description	Enter a brief description to identify the task.
Add Task	Click to create the defined task.
Refresh	Click to refresh the task.
Configuration Information	
Status/Input	Apply the configuration changes for the job. For customized category, the options depend on the design of the template and selected protocol.
Target Devices	
Add	Click to add the device(s) for configuration. Note that only devices that support this function can be selected. For customized configuration categories, you need to associate the configuration template to the device template first. Refer to **Templates > Device Template**.
Note: You can select multiple devices across different networks. To confine the configuration to only devices under the same network for better security, use the below **Configuration Profile** method.	
Schedule Information	
Schedule Type	• **One Time**: Select this option to specify a date and time or immediately to initiate the network discovery. • **Recurrent**: Select this option to specify the frequency and effective time frame to initiate network discovery. Refer to 14.2 Scheduling for more information.

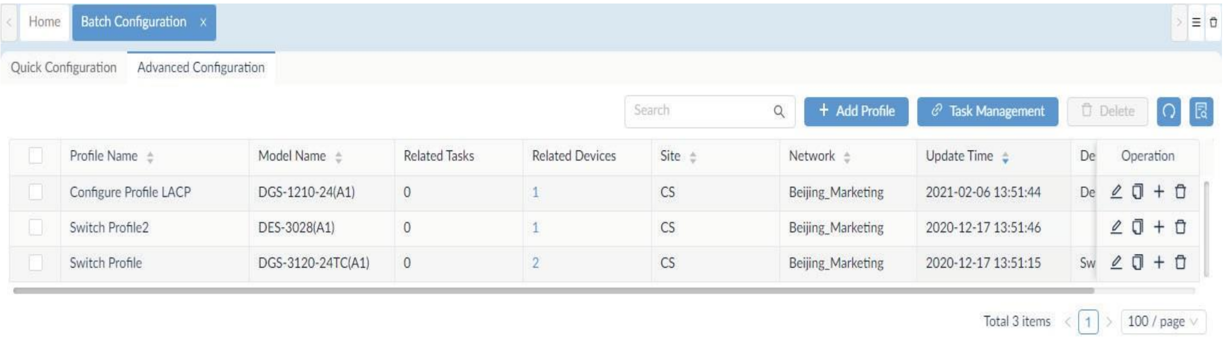
You can click **Task Management** to open the **Task Management** page or **Configuration Template** to open the template page. Refer to **6.2.1 Current Tasks** for details about tasks.

Add a Configuration Profile

Configuration profiles are designed to allow multiple configuration categories for rapid network deployment. Unlike the above quick configuration, it can accommodate categories of the **Advanced Configuration** type. Once a profile is defined, you can apply it to multiple devices in a network.

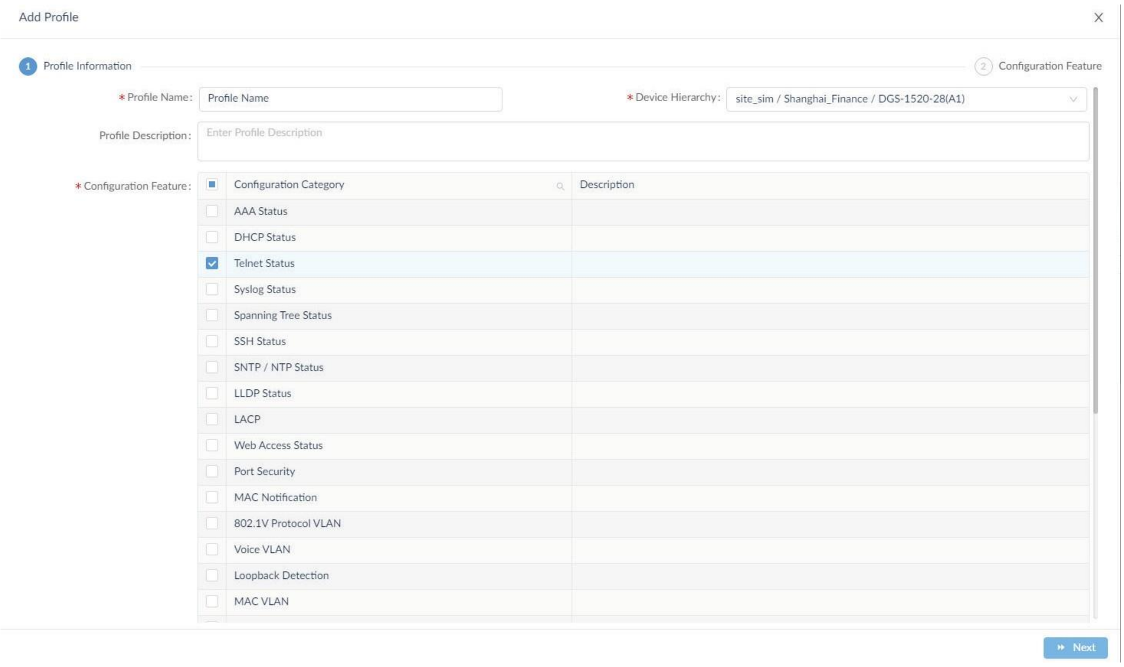
1. Go to **Configuration > Batch Configuration**.
2. Select the **Advanced Configuration** tab.

The Advanced Configuration page displays.



□	Profile Name	Model Name	Related Tasks	Related Devices	Site	Network	Update Time	De	Operation
□	Configure Profile LACP	DGS-1210-24(A1)	0	1	CS	Beijing_Marketing	2021-02-06 13:51:44	De	
□	Switch Profile2	DES-3028(A1)	0	1	CS	Beijing_Marketing	2020-12-17 13:51:46		
□	Switch Profile	DGS-3120-24TC(A1)	0	2	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	

3. Click **Add Profile** to display the **Add Profile** page.



* Profile Name: Profile Name

* Device Hierarchy: site_sim / Shanghai_Finance / DGS-1520-28(A1)

Profile Description: Enter Profile Description

* Configuration Feature:

■	Configuration Category	Description
□	AAA Status	
□	DHCP Status	
☑	Telnet Status	
□	Syslog Status	
□	Spanning Tree Status	
□	SSH Status	
□	SNTP / NTP Status	
□	LLDP Status	
□	LACP	
□	Web Access Status	
□	Port Security	
□	MAC Notification	
□	802.1V Protocol VLAN	
□	Voice VLAN	
□	Loopback Detection	
□	MAC VLAN	

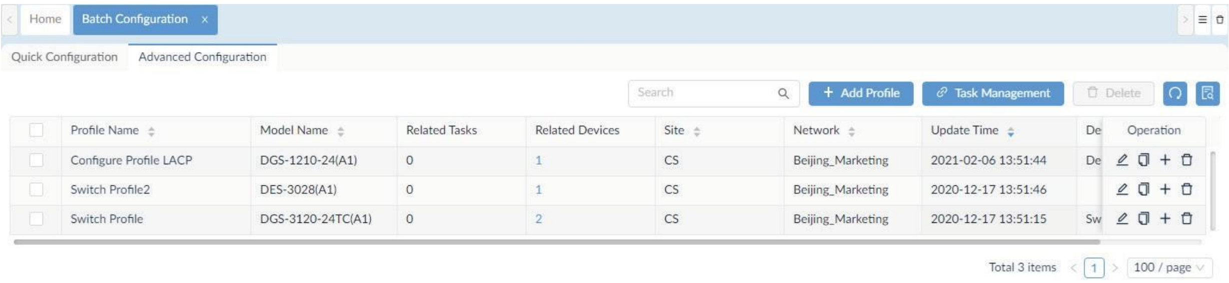
4. Enter the following information to define the profile:

Profile Name	Enter a name to define the profile.
Device Hierarchy	Click the drop-down menu to select a device. Note that here you only need to specify a model to apply the configuration to. You can select devices of the designated model when creating tasks. Refer to the below **Apply a Profile to Devices with Task**.
Profile Description	Enter a brief description to identify the profile.
Configuration Feature List	Select categories for the profile: • AAA Status • DHCP Status • HTTPS Web Access Status • LLDP Status • RMON Status • SNTP/NTP Status • SSH Status • Safeguard Engine Status • Spanning Tree Status • Telnet Status • Web Access Status
Note: The available configuration category depends on the features supported. Unlike the Quick Configuration page described above, it allows you to select categories of the **Advanced Configuration** type. For customized (or user-built) configuration categories, you need to associate the configuration template to the device template first (go to **Templates > Device Template**).	

5. Click **Next** to continue and configure the selected features.

6. Click **Save** after configuring the features for each category. Click **Previous** to return to the previous screen.

After a configuration profile is created, you can modify or delete it with the options under the Operation column.



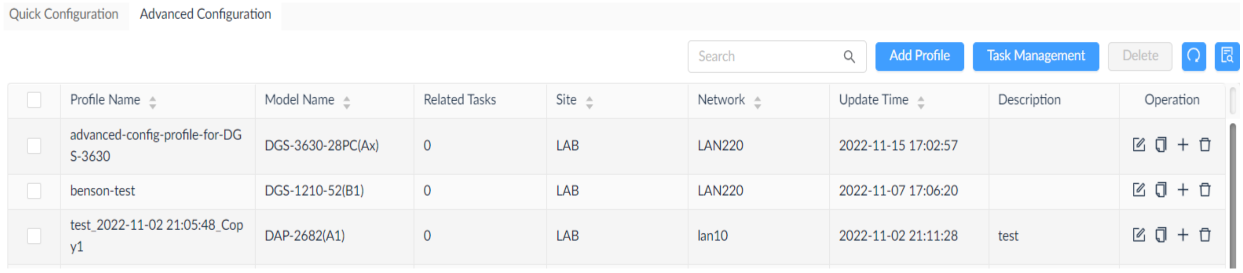
☐	Profile Name	Model Name	Related Tasks	Related Devices	Site	Network	Update Time	De	Operation
☐	Configure Profile LACP	DGS-1210-24(A1)	0	1	CS	Beijing_Marketing	2021-02-06 13:51:44	De	
☐	Switch Profile2	DES-3028(A1)	0	1	CS	Beijing_Marketing	2020-12-17 13:51:46		
☐	Switch Profile	DGS-3120-24TC(A1)	0	2	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	

Total 3 items < 1 > 100 / page

Item	Description
Edit	Modify the configuration profile settings.
Share	Copy the profile to configure devices of the same model on other networks.
Create Task	Create a task for the profile to perform the configuration on selected devices according to a set schedule. Refer to the following section for detailed instructions.
Delete	Remove the profile from the list.

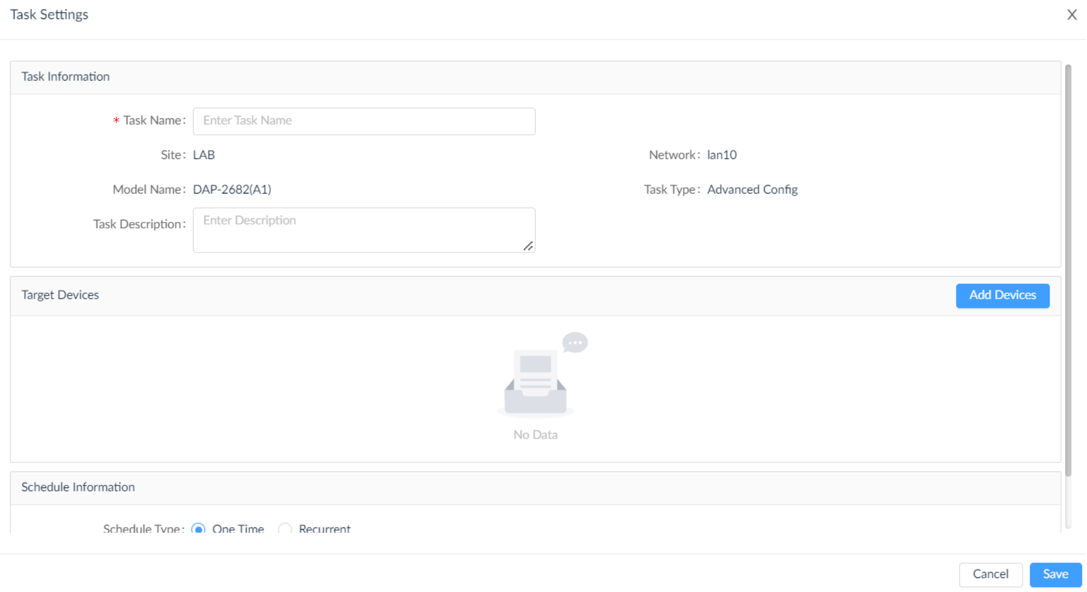
Apply a Profile to Devices with Task

1. Go to **Configuration > Batch Configuration.**
2. Select **Advanced Configuration**.
3. Select a profile, then click + (**Create Task)** from the Operation column on the right to apply the profile to devices by creating a task.



	Profile Name	Model Name	Related Tasks	Site	Network	Update Time	Description	Operation
□	advanced-config-profile-for-DGS-3630	DGS-3630-28PC(Ax)	0	LAB	LAN220	2022-11-15 17:02:57		+
□	benson-test	DGS-1210-52(B1)	0	LAB	LAN220	2022-11-07 17:06:20		+
□	test_2022-11-02 21:05:48_Copy1	DAP-2682(A1)	0	LAB	lan10	2022-11-02 21:11:28	test	+

The Task Settings page displays.



* Task Name: Enter Task Name

Site: LAB

Network: lan10

Model Name: DAP-2682(A1)

Task Type: Advanced Config

Task Description: Enter Description

Schedule Type: ● One Time ○ Recurrent

4. Enter the following information:

Task Information	
Task Name	Enter a name to define the task.
Task Description	Enter a brief description to identify the task.
Target Devices	
Add Devices	Click to add the device(s) for configuration. The Batch Select Devices screen displays. Select the desired devices or use the Search function to find devices.
Note: You can only select devices of the same model under the designated network. To apply the configuration profile to other networks, use the **Share** function under **Operation**. You can also create device groups with devices across networks in advance and select the desired group from the Device Group tab. (Refer to 4.3 Manage Device Groups.)	
Schedule Information	
Schedule Type	• **One Time**: Select this option to specify a date and time or immediately to execute the task. • **Recurrent**: Select this option to specify the frequency and effective duration to execute the task. Refer to 14.2 Scheduling for more information.

5. Click **Save** to create the new task and return to the previous menu.
You can click **Task Management** to open the **Task Management** page. Refer to **6.2.1 Current Tasks** for details about tasks.

6.2. Manage Tasks

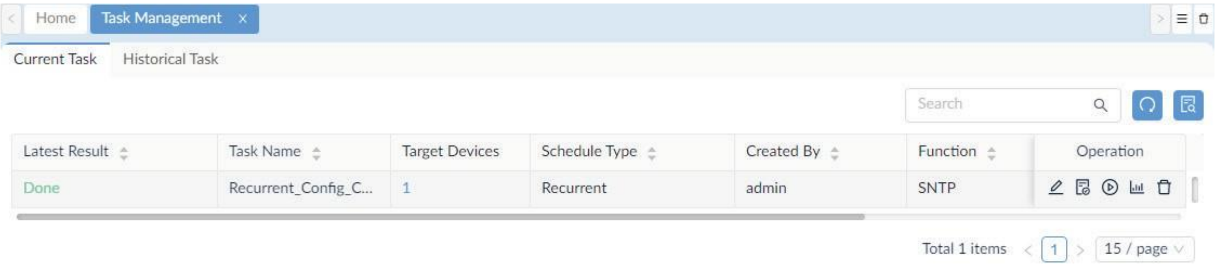
The Task Management function lets you manage current and previously performed tasks. Tasks initiated in the system can be edited, deleted, and restarted. You can also view the task execution record.

6.2.1. Current Tasks

Current tasks are tasks that are scheduled to be perform in the future.

To view current tasks:

1. Go to **Configuration > Task Management**. Then select the **Current Task** tab.



Latest Result	Task Name	Target Devices	Schedule Type	Created By	Function	Operation
Done	Recurrent_Config_C...	1	Recurrent	admin	SNTP	

The following table displays the properties of the tasks and the functions that you can perform on them:

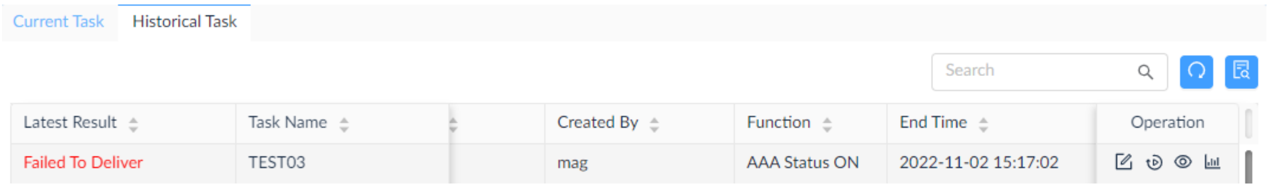
Item	**Description**
Task Name	Displays the defined name of the task.
Target Devices	Displays the number of devices that the task will be applied to.
Schedule Type	The configured schedule type: one-time or recurrent.
Created By	Displays the name of the task creator.
Function	Displays the featured functions or configuration profile name to be executed with the task.
Time Created	Displays the creation date of the task.
Next Execution Time	Displays the next scheduled start of the task.
Operation	
Edit Configuration	Click to edit the defined configuration.
Edit Task	Click to modify the task settings.
Restart/Pause Task	Click to activate/deactivate the task.
Show Task Record	Click to display the event timeline of the task, listed in chronological order.
Delete Task	Click to delete the task. You need to pause the task first for deletion.

6.2.2 Historical Tasks

Historical Tasks are tasks that have been performed in the past.

To view historical tasks:

Go to **Configuration > Task Management**. Then select the **Historical Task** tab.



Latest Result	Task Name		Created By	Function	End Time	Operation
Failed To Deliver	TEST03		mag	AAA Status ON	2022-11-02 15:17:02	

The following table shows the properties of the tasks and the functions you can perform on them:

Item	**Description**
Latest Result	Displays the results of the task: Partially done, Done, or Failed. Click on the link to open the result details page.
Task Name	Displays the defined name of the task.
Target Devices	Displays the number of devices that the task will be applied to.
Schedule Type	The configured schedule information
Created By	Displays the name of the task creator.
Function	Displays the featured functions or configuration profiles to be executed with the task.
End Time	Displays the finishing time of the task.
Time Created	Displays the creation date of the task.
Operation	
Edit Configuration	Click to edit the corresponding configuration file.
Re-execute Task	Click to modify the task and reschedule the task to be performed again. It will appear in the above Current Task tab for future execution dates.
Review Task	Obtain task details including name and type, target devices and task scheduling.
Show Task Record	Click to display the event timeline of the task, listed in chronological order.

6.3. Schedule a Firmware Upgrade

Scheduling a firmware upgrade task requires uploading firmware files first in File Management (refer to **Configuration > File Management**).

Note: When the license expires, the **Firmware Management** page will alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

To configure a firmware upgrade task:

1. Go to **Configuration > Firmware Management**.

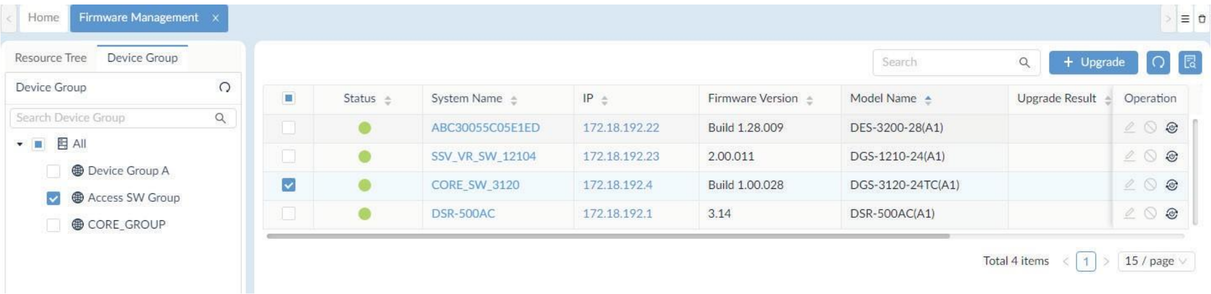
2. In the **Resource Tree** pane, select the desired device model under the designated site(s) and network(s) for the upgrade task. Or enter a keyword in the Search field to locate the target network or model name. You can select the **Device Group** tab if you have created device groups for designated devices.

3. From the discovered or listed devices, select device(s) for firmware upgrade.

   Device firmware information will be displayed:

Item	**Description**
Status	Displays the online/offline status of the device.
System Name	Displays the system name of the device.
IP	Displays the IP address of the device.
Firmware Version	Displays the device's firmware version.
Model Name	Displays the model name of the device.
Upgrade Result	Displays the result of the last firmware upgrade or the scheduled firmware upgrade.
Site/Network	Displays the site and network where the device resides.
Operation	
Edit	Click to modify the firmware upgrade task. You may need to stop the firmware upgrade task first to edit it.
Stop	Click to stop the task.
Reboot Device	Click to reboot the device after the firmware upgrade.

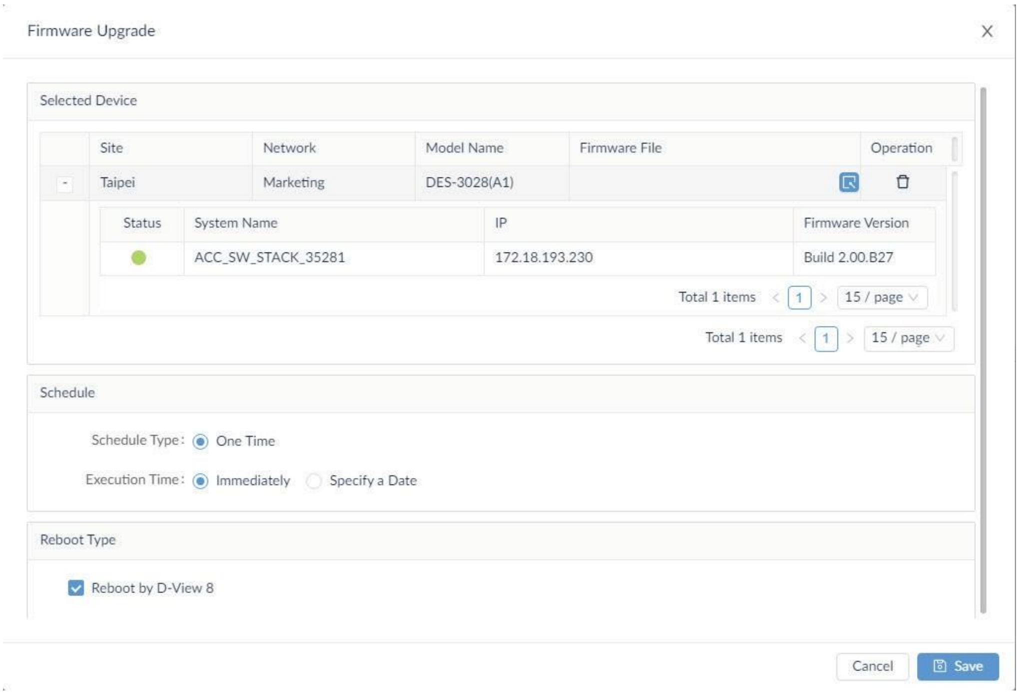
4. Click **Upgrade** in the upper right corner to configure the task.



	Status	System Name	IP	Firmware Version	Model Name	Upgrade Result	Operation
□	●	ABC30055C05E1ED	172.18.192.22	Build 1.28.009	DES-3200-28(A1)		
□	●	SSV_VR_SW_12104	172.18.192.23	2.00.011	DGS-1210-24(A1)		
☑	●	CORE_SW_3120	172.18.192.4	Build 1.00.028	DGS-3120-24TC(A1)		
□	●	DSR-500AC	172.18.192.1	3.14	DSR-500AC(A1)		

Total 4 items 1 15 / page

5. The **Firmware Upgrade** page displays.



Firmware Upgrade

Selected Device

	Site	Network	Model Name	Firmware File	Operation
-	Taipei	Marketing	DES-3028(A1)		

Status	System Name	IP	Firmware Version
●	ACC_SW_STACK_35281	172.18.193.230	Build 2.00.B27

Total 1 items < 1 > 15 / page

Total 1 items < 1 > 15 / page

Schedule

Schedule Type : ● One Time

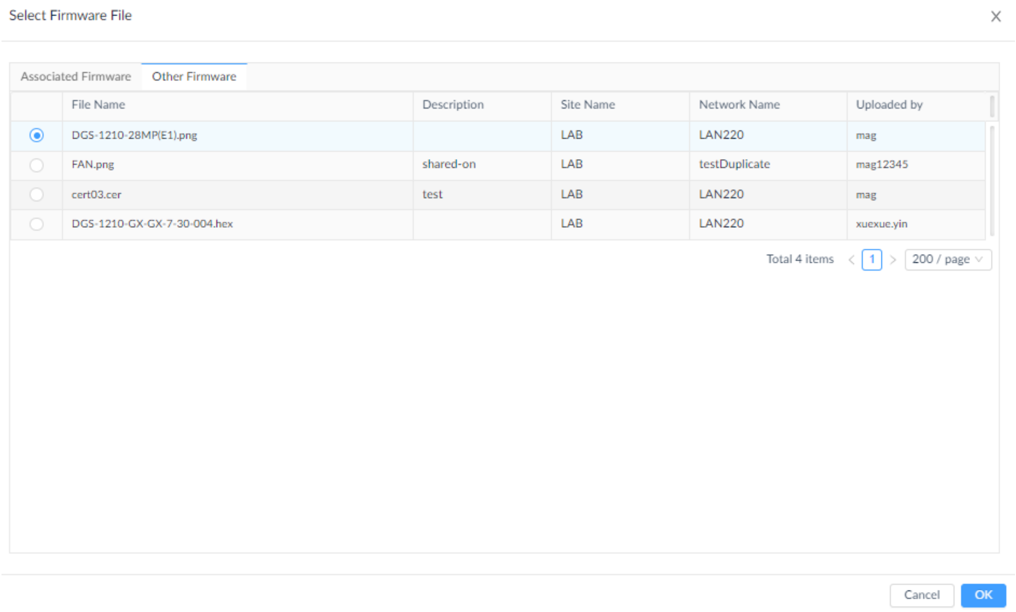
Execution Time : ● Immediately ○ Specify a Date

Reboot Type

☑ Reboot by D-View 8

6. Click **Select Firmware File** to select a firmware file for the specified devices.

7. The **Select Firmware File** page displays. Select the **Associated Firmware** tab to upload firmware from your local file system. Or select a firmware file stored in the server from the **Other Firmware** tab.



Select Firmware File

Associated Firmware | Other Firmware

	File Name	Description	Site Name	Network Name	Uploaded by
●	DGS-1210-28MP(E1).png		LAB	LAN220	mag
○	FAN.png	shared-on	LAB	testDuplicate	mag12345
○	cert03.cer	test	LAB	LAN220	mag
○	DGS-1210-GX-GX-7-30-004.hex		LAB	LAN220	xuexue.yin

Total 4 items < 1 > 200 / page

8. Configure the following:

Item	Description
Selected Device	Displays the device(s) selected for the task. You can click Delete to remove the selected devices.
Schedule Information	
Schedule Type	Firmware upgrade is a one-time event.
Execution Time	Define the execution time, immediately or a specific date and time.

Reboot Type	Click to enable or disable (default) device reboot after firmware upgrade. A reboot is typically required for the new firmware to take effect.

9. Click **Save** to create the firmware upgrade task. Click **Cancel** to return to the previous screen.

The **Upgrade Result** column will record the results of the firmware upgrade task.

6.4. Back Up and Restore Device Configuration

The D-View 8 provides backup function to maintain configuration files on the server.

6.4.1. Add or Modify a Backup Profile

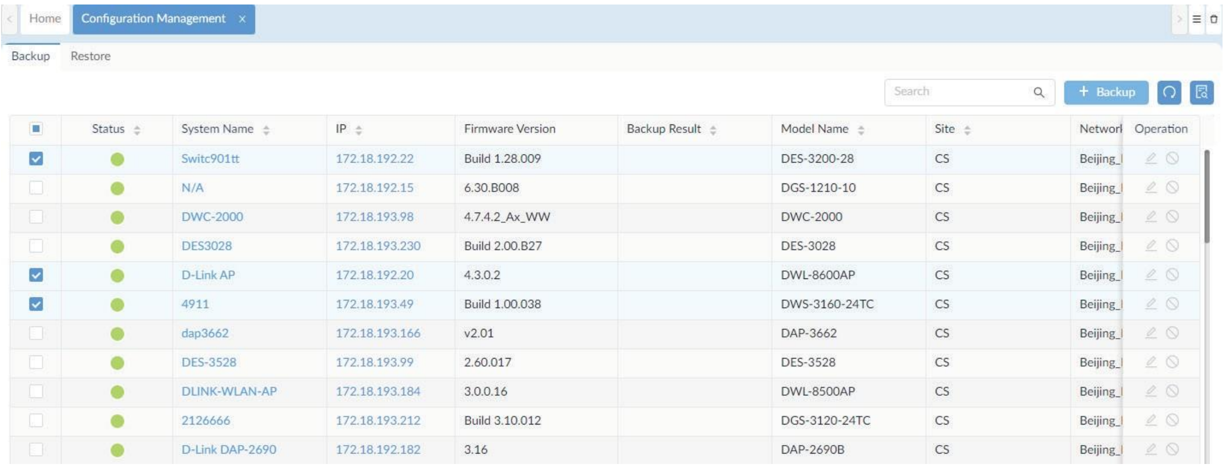
Regular system backup can be accomplished automatically through backup profiles.

Note: When the license expires, the **Configuration Management** page will alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

1. Go to **Configuration > Configuration Management**.
2. Select devices for backup.
   Available devices with device information are displayed:

Item	**Description**
Status	Displays the online/offline status of the device.
System Name	Displays the system name of the device.
IP	Displays the IP address of the device.
Firmware Version	Displays the device’s firmware version.
Model Name	Displays the model name of the device.
Backup Result	Displays the result of the last configuration backup or the scheduled backup.
Site/Network	Displays the site and network where the device resides.
Operation	
Edit	Click to modify the backup task. You may need to stop the backup task first to modify it.
Stop	Click to stop the task.

3. Click **Backup** to configure the task.



■	Status	System Name	IP	Firmware Version	Backup Result	Model Name	Site	Networl	Operation
☑	●	Switc901tt	172.18.192.22	Build 1.28.009		DES-3200-28	CS	Beijing_I	
□	●	N/A	172.18.192.15	6.30.B008		DGS-1210-10	CS	Beijing_I	
□	●	DWC-2000	172.18.193.98	4.7.4.2_Ax_WW		DWC-2000	CS	Beijing_I	
□	●	DES3028	172.18.193.230	Build 2.00.B27		DES-3028	CS	Beijing_I	
☑	●	D-Link AP	172.18.192.20	4.3.0.2		DWL-8600AP	CS	Beijing_I	
☑	●	4911	172.18.193.49	Build 1.00.038		DWS-3160-24TC	CS	Beijing_I	
□	●	dap3662	172.18.193.166	v2.01		DAP-3662	CS	Beijing_I	
□	●	DES-3528	172.18.193.99	2.60.017		DES-3528	CS	Beijing_I	
□	●	DLINK-WLAN-AP	172.18.193.184	3.0.0.16		DWL-8500AP	CS	Beijing_I	
□	●	2126666	172.18.193.212	Build 3.10.012		DGS-3120-24TC	CS	Beijing_I	
□	●	D-Link DAP-2690	172.18.192.182	3.16		DAP-2690B	CS	Beijing_I	

The **Backup** page displays.

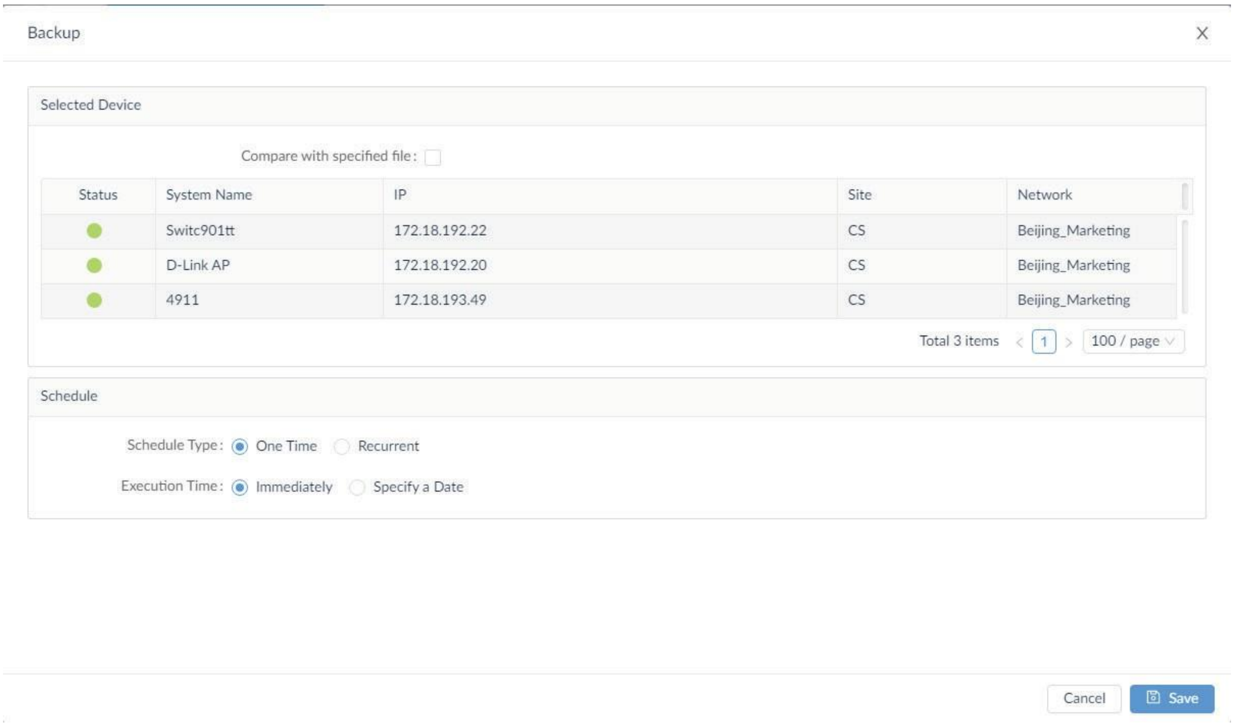
An existing configuration template or an uploaded new one can be used to compare the device’s configuration settings. If there is any difference between the selected template and the existing configuration settings, an alarm can be triggered.

To compare configuration settings:

1. Click **Compare with specified file** to enable the comparison function.
2. For **Actions when different**, select the severity level for an alarm: Critical, Warning, or Info.
3. Enable **Restore Configuration** to restore the device’s configuration with the specified file when the

device’s current settings show any difference. A configuration file for comparison and restoration must be selected.

4. For the selected devices, click **Upload File** in the **File** field to upload the configuration file for comparison.



Backup

Selected Device

Compare with specified file : □

Status	System Name	IP	Site	Network
●	Switc901tt	172.18.192.22	CS	Beijing_Marketing
●	D-Link AP	172.18.192.20	CS	Beijing_Marketing
●	4911	172.18.193.49	CS	Beijing_Marketing

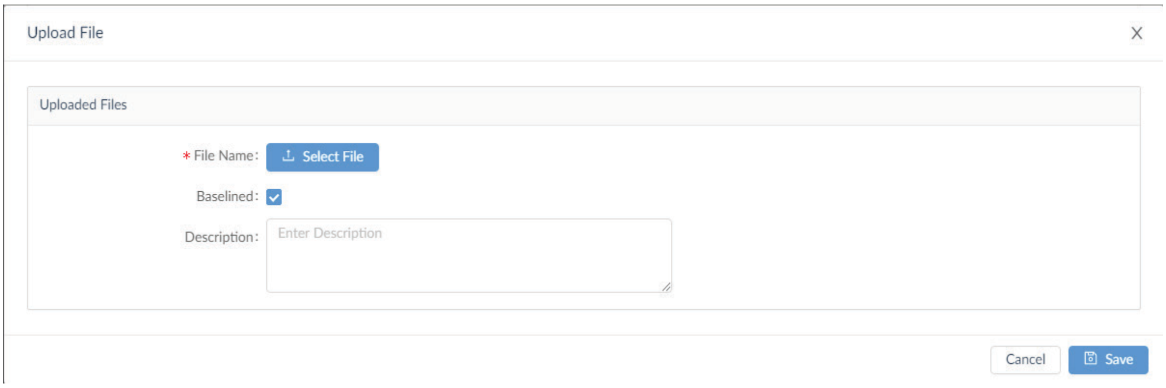
Total 3 items < 1 > 100 / page

Schedule

Schedule Type : ● One Time ○ Recurrent

Execution Time : ● Immediately ○ Specify a Date

5. The **Upload File** page displays. Click **Select File** to browse for a configuration file for comparison.
6. Click **Set as Baseline** if you would like to set this file as the baselined configuration for distinguishability or tracking between other configuration files.
7. Click **Save** to define the baseline file. Click **Cancel** to return to the previous screen. The uploaded files will be listed in **File Management** and will be available for configuration restoration.



Upload File

Uploaded Files

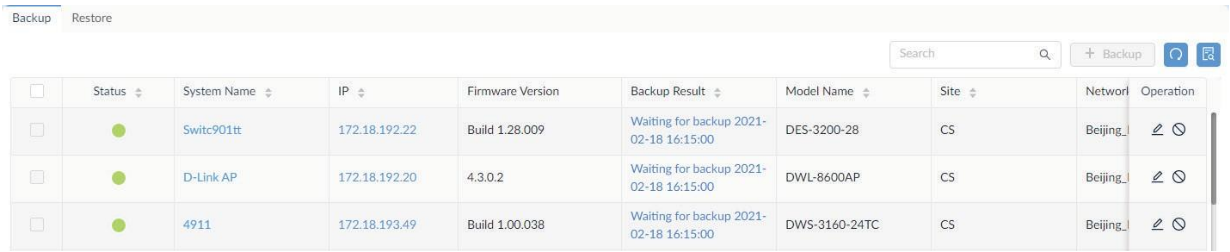
* File Name : Select File

Baselined : ☑

Description : Enter Description

8. Under Schedule, select the scheduling method to perform the task:
   - Schedule Type: Click to define the frequency of the task, a single event or recurring task. For a recurring task, specify a pre-defined schedule or add a new schedule by specifying the repetition frequency (daily, weekly, monthly, or discrete dates) and effective duration. Refer to 14.2 Scheduling for more information.
   - Execution Time: For a single event, define the execution time, immediately or a specific date and time.
9. Click **Save** to create the backup task. Click **Cancel** to return to the previous screen.The task is created and the backup task will be recorded in the **Backup Result** column.

10. You can also edit or stop a task. Under Operation, click the **Edit** or **Stop** on the right.



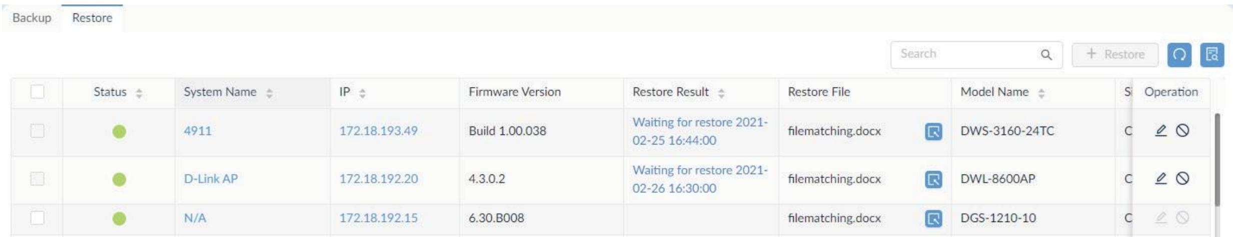
☐	Status	System Name	IP	Firmware Version	Backup Result	Model Name	Site	Networ	Operation
☐	●	Switc901tt	172.18.192.22	Build 1.28.009	Waiting for backup 2021-02-18 16:15:00	DES-3200-28	CS	Beijing_	✎ ⊘
☐	●	D-Link AP	172.18.192.20	4.3.0.2	Waiting for backup 2021-02-18 16:15:00	DWL-8600AP	CS	Beijing_	✎ ⊘
☐	●	4911	172.18.193.49	Build 1.00.038	Waiting for backup 2021-02-18 16:15:00	DWS-3160-24TC	CS	Beijing_	✎ ⊘

6.4.2. Restore Device Configurations

Device configuration settings can be restored through a defined backup task with an assigned configuration file.

To restore a device configuration:

1. Go to **Configuration > Configuration Management**.
2. Click the **Restore** tab to view the defined restore tasks.



☐	Status	System Name	IP	Firmware Version	Restore Result	Restore File	Model Name	S	Operation
☐	●	4911	172.18.193.49	Build 1.00.038	Waiting for restore 2021-02-25 16:44:00	filematching.docx	DWS-3160-24TC	C	✎ ⊘
☐	●	D-Link AP	172.18.192.20	4.3.0.2	Waiting for restore 2021-02-26 16:30:00	filematching.docx	DWL-8600AP	C	✎ ⊘
☐	●	N/A	172.18.192.15	6.30.B008		filematching.docx	DGS-1210-10	C	✎ ⊘

3. Select a device with a pre-defined baseline file or the most recent backup version and click **Restore** to configure the task.

NOTE: Files that will be used for restoration can be selected by clicking the Select button under the **Restore File** column. You can also upload additional configuration files and assign a baseline file on the **Select Restoration File** page.

In the Select Restoration File page, you can perform the following on restoration files:

- Upload file
- Download file
- Set as baseline configuration

3. On the **Restore** page, under Schedule Information, select the scheduling method to perform the task:
   - Schedule Type: Click to define the frequency of the task, a single event or recurring task. For a recurring task, specify a pre-defined schedule or add a new schedule by specifying the repetition frequency (daily, weekly, monthly, or discrete dates) and effective duration. Refer to 14.2 Scheduling for more information.
   - Execution Time: For a single event, define the execution, immediately or a specific date and time.
4. Click **Save** to create the restore task. Click **Cancel** to return to the previous

   screen.
5. You can also edit or stop a restore task. Under **Operation**, click **Edit** or **Stop** on the right.

The task is created and the restore task will be recorded in the **Restore Result** column along with other information such as system name, IP address, firmware version, and device model as well as device category.

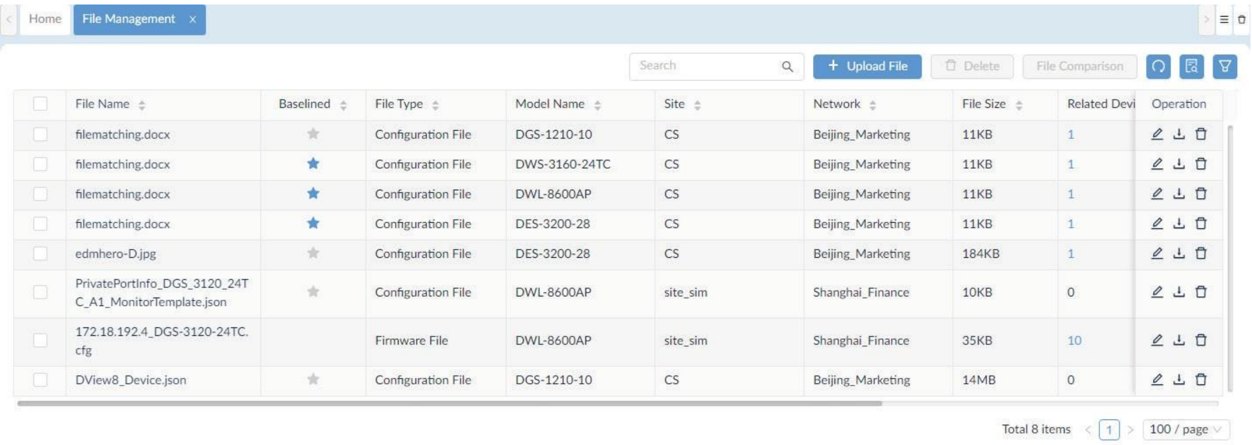
6.5. File Management

You can manage firmware and configuration files for different models through the File Management function in Configuration. This function allows uploading, deleting, file comparison, and searching to help organize and apply uploaded files to upgrade firmware or restore configuration. In this manner, templates for firmware and configuration settings can be utilized to streamline the maintenance process. With a firmware or configuration template, maintaining consistency across networks can be easily achieved.

The following section provides descriptions of the functions in File Management and the operations that you can perform in File Management.

To access File Management menu:

Go to **Configuration > File Management**.



□	File Name	Baselined	File Type	Model Name	Site	Network	File Size	Related Devi	Operation
□	filematching.docx	☆	Configuration File	DGS-1210-10	CS	Beijing_Marketing	11KB	1	✎ ⤓ 🗑
□	filematching.docx	★	Configuration File	DWS-3160-24TC	CS	Beijing_Marketing	11KB	1	✎ ⤓ 🗑
□	filematching.docx	★	Configuration File	DWL-8600AP	CS	Beijing_Marketing	11KB	1	✎ ⤓ 🗑
□	filematching.docx	★	Configuration File	DES-3200-28	CS	Beijing_Marketing	11KB	1	✎ ⤓ 🗑
□	edmhero-D.jpg	☆	Configuration File	DES-3200-28	CS	Beijing_Marketing	184KB	1	✎ ⤓ 🗑
□	PrivatePortInfo_DGS_3120_24TC_A1_MonitorTemplate.json	☆	Configuration File	DWL-8600AP	site_sim	Shanghai_Finance	10KB	0	✎ ⤓ 🗑
□	172.18.192.4_DGS-3120-24TC.cfg		Firmware File	DWL-8600AP	site_sim	Shanghai_Finance	35KB	10	✎ ⤓ 🗑
□	DView8_Device.json	☆	Configuration File	DGS-1210-10	CS	Beijing_Marketing	14MB	0	✎ ⤓ 🗑

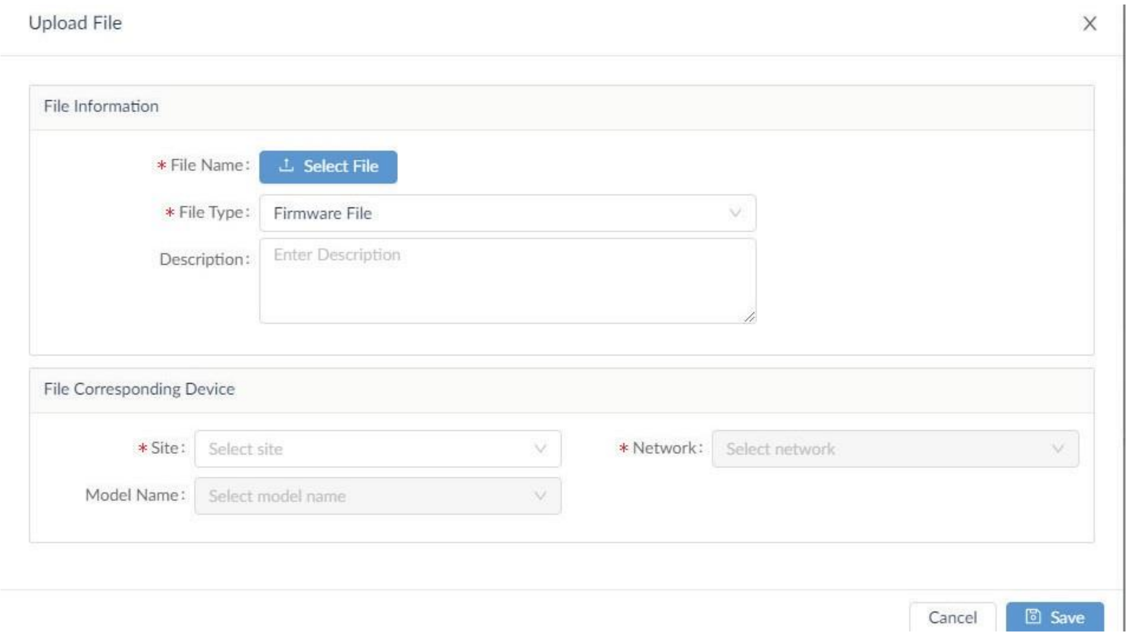
Total 8 items < 1 > 100 / page

The following table describes the functions in the File Management page.

Item	Description
Search	Enter a keyword to search for a file name, site, or network.
Delete	Select an entry and click Delete to remove it.
File Comparison	Select two configuration files to compare. Both files must be text based. You may also go to **Tools > File Comparison** to access this function.
Refresh	Refresh the table.
Advanced Query	Filter by File Name, File Type, Upload Time, Status, Site, Network, Uploaded by, or Model Name.
Column Selector	Click to add or remove columns from the File Management table. The following column properties are available: File Name, Baselined, File Type, Site, Fie Size, Status, Description, Model Name, Network, Related Devices, and Upload Time. Select All to enable all column options. Click **Apply** to confirm the new header selection.
Operation	
Edit	Click to edit the file listing.
Download	Click to export the file to a local system.
Delete	Click to remove the listing.

To upload a file to the server:

1. Click the **Upload File** at the top right.



Upload File

File Information

* File Name: Select File

* File Type: Firmware File

Description: Enter Description

File Corresponding Device

* Site: Select site

* Network: Select network

Model Name: Select model name

Cancel Save

2. Configure the following:

File Information	
Select File	Click to browse and define a configuration or firmware template.
File Type	Click the drop-down menu to select the type of file: Firmware File or Configuration File.
Description	Give a description of this file.
Set as Baseline	Designate the file as a baseline template. This is only available for the configuration file type.
Share	Enable this option to allow the uploaded file to be shared with other networks. This is only available for the firmware file type.
Description	Enter a short description to help identify this file.
Corresponding Device	
Site	Select a corresponding site.
Network	Select a network from the above selected site.
Model Name	Select the model name for file upload.
Device	Select the device for the file upload (only available for the configuration file type).
Cancel	Click **Cancel** to return to the previous menu.
Save	Click **Save** to add the defined file upload.

6.5.1. Firmware Management

Devices benefit from the latest firmware version, which may enhance the overall security and functionality. Check your device’s support or about page to obtain the latest firmware version.

Caution:

When updating firmware, make sure the firmware is correct for the selected device. Employing the right firmware to the selected devices is essential for successful upload. The wrong firmware may cause damage to devices.

This section covers the following topics:

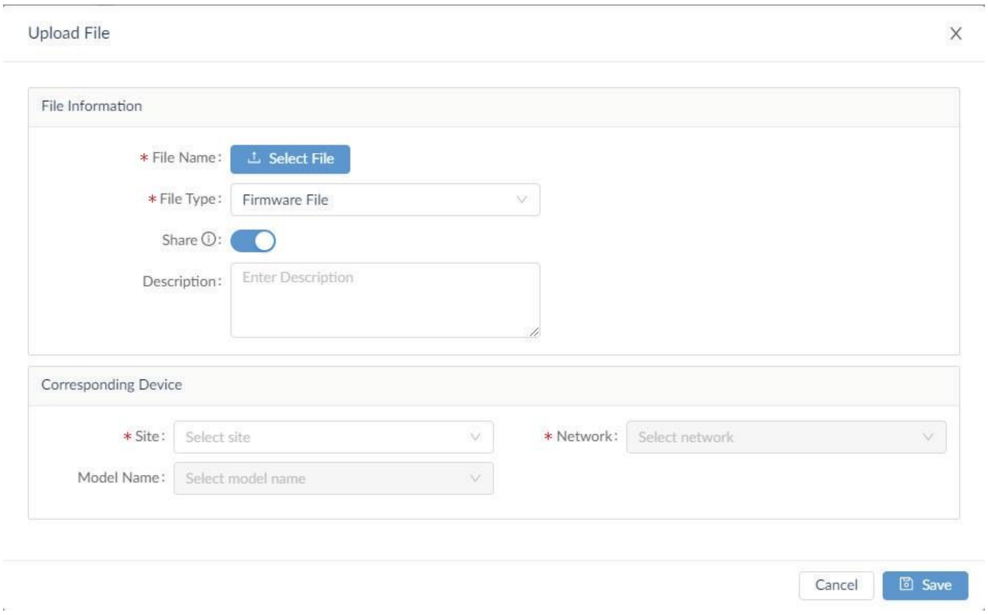
- Import a firmware file
- Modify a firmware file

- Export a firmware file
- Remove a firmware file

Import a Firmware File

To import a firmware file:

1. Go to **Configuration > File Management**.
2. Click **Upload File** at the right. The Upload File page appears.

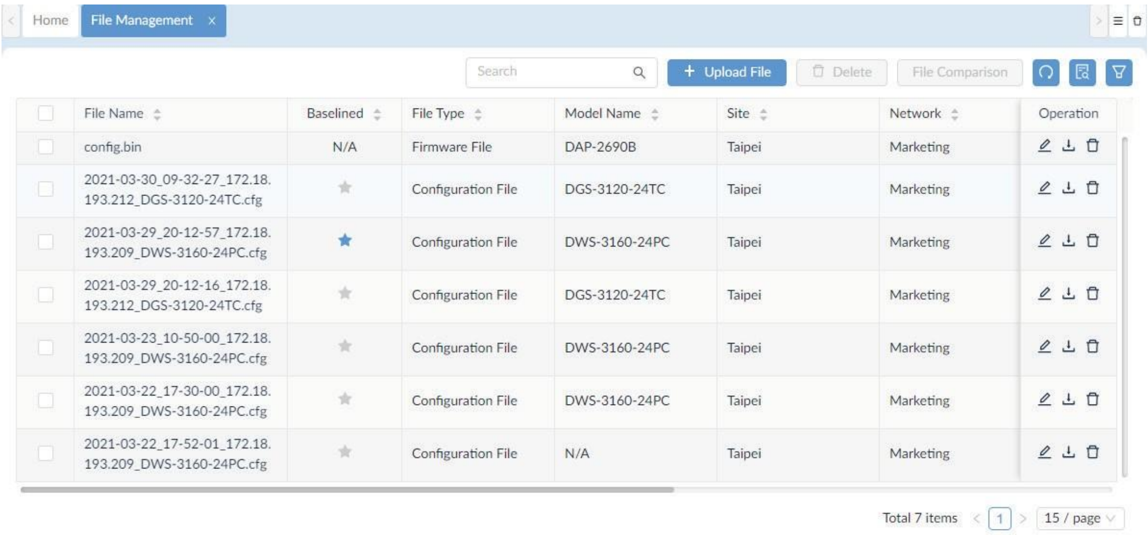


3. Click **Select File** to browse and select the target file for upload.
4. From **File Type**, select **Firmware File** for the uploaded file type.
5. Enable the **Share** option to share the uploaded firmware with other networks.
6. In the **Description** field, enter a brief description for the file.
7. Click the **Site** drop-down menu to select a site where the device model belongs to.
8. Click the **Network** drop-down menu to select a network under the selected site.
9. Click the **Model Name** drop-down menu to select a model to apply the firmware.
10. Click **Save** to create a firmware file entry or **Cancel** to return to the previous menu.

Modify a Firmware File Entry

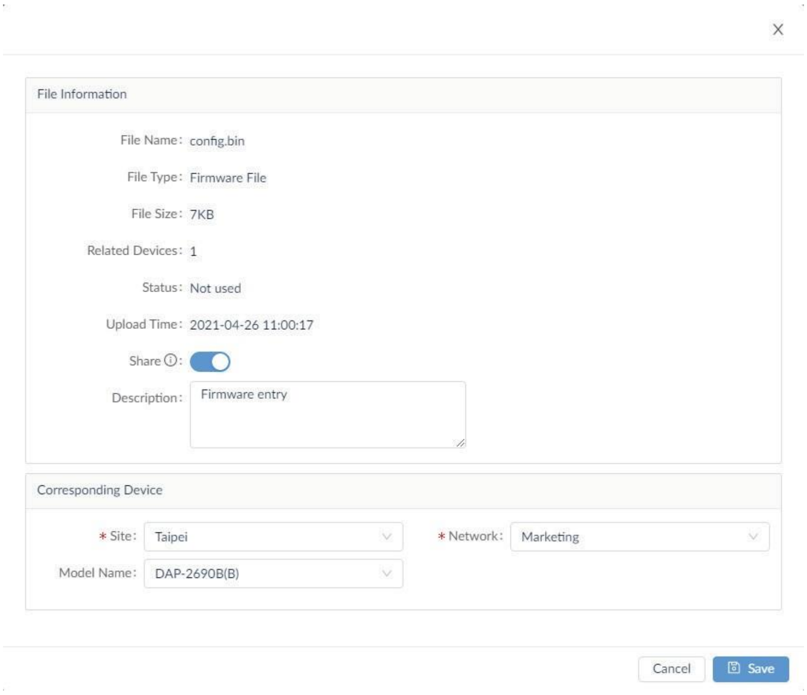
To modify an existing firmware file entry:

1. Go to **Configuration > File Management**.
2. From the File Management page, select an existing entry from the list, then click **Edit** under **Operation**.



□	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	
□	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	N/A	Taipei	Marketing	

3. The File Information page displays. From this page you can modify the file information.



File Information

File Name: config.bin

File Type: Firmware File

File Size: 7KB

Related Devices: 1

Status: Not used

Upload Time: 2021-04-26 11:00:17

Share ⓘ:

Description: Firmware entry

Corresponding Device

* Site: Taipei

* Network: Marketing

Model Name: DAP-2690B(B)

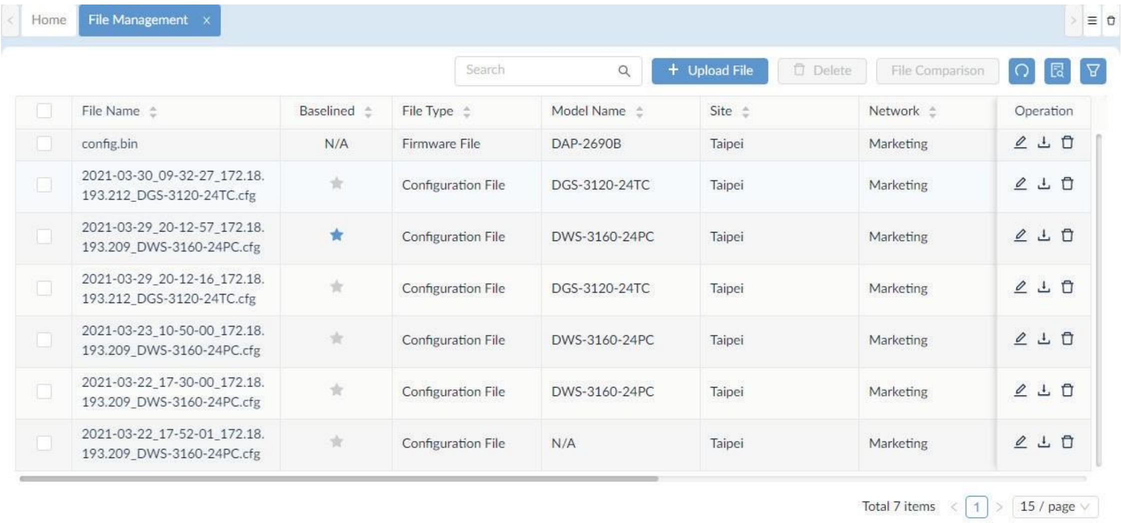
4. Enter a description to help identify the entry.
5. Modify the corresponding device information:
   - Site
   - Network
   - Model Name
6. Click **Save** to apply the changes or **Cancel** to return to the previous menu.

Export a Firmware File

To export an existing firmware file:

1. Go to **Configuration > File Management**.

2. From the File Management page, select an existing entry from the list, then click **Download**.



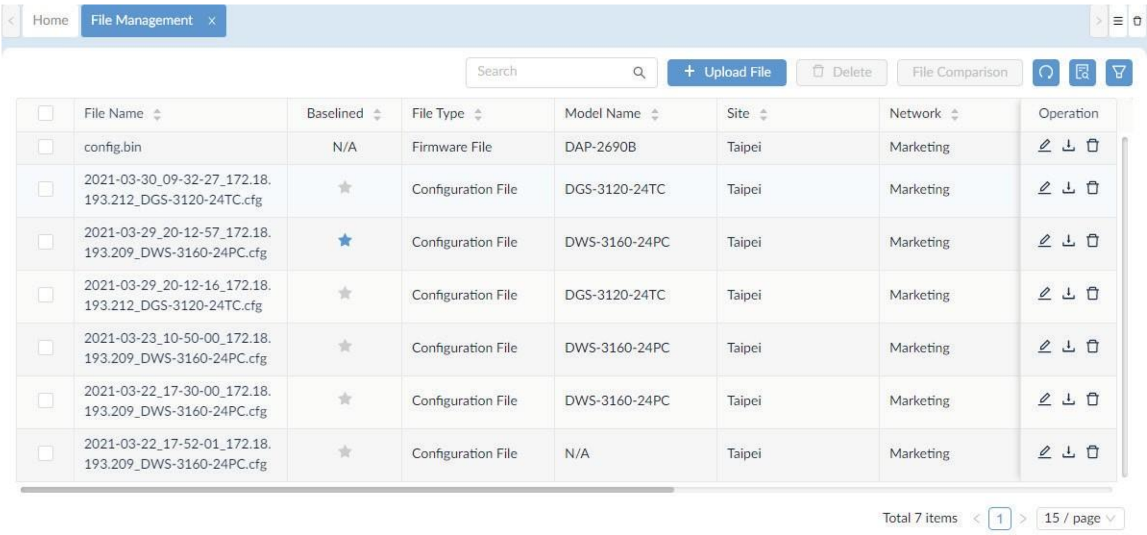
□	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	✎ ⤓ 🗑

The file will be downloaded to the default download folder of your browser. A successful download notification will be displayed once the file is exported to your local system.

Remove a Firmware File

To remove a firmware file:

1. Go to **Configuration > File Management.**
2. From the **File Management** page, select an existing entry from the list, then click **Delete File** under **Operation**.



□	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	✎ ⤓ 🗑

A confirmation prompt will be displayed. Click **Yes** to delete or **No** to cancel the operation.

6.5.2. Configuration Management

The Configuration Management allows you to back up and restore device configurations.

This section covers the following topics:

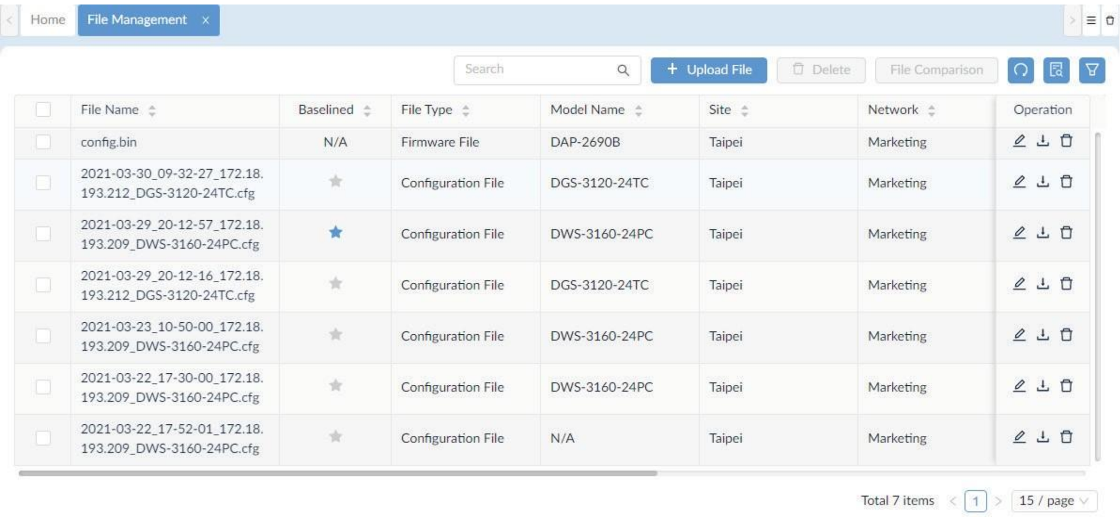
- Import a configuration file
- Modify a configuration file
- Export a configuration file
- Remove a configuration file

Import a Configuration File

You can restore the configuration of D-Link devices on your network. You can also schedule restoration tasks to be executed on a recurrent basis for batch operations.

To import a configuration file:

1. Go to **Configuration > File Management**.



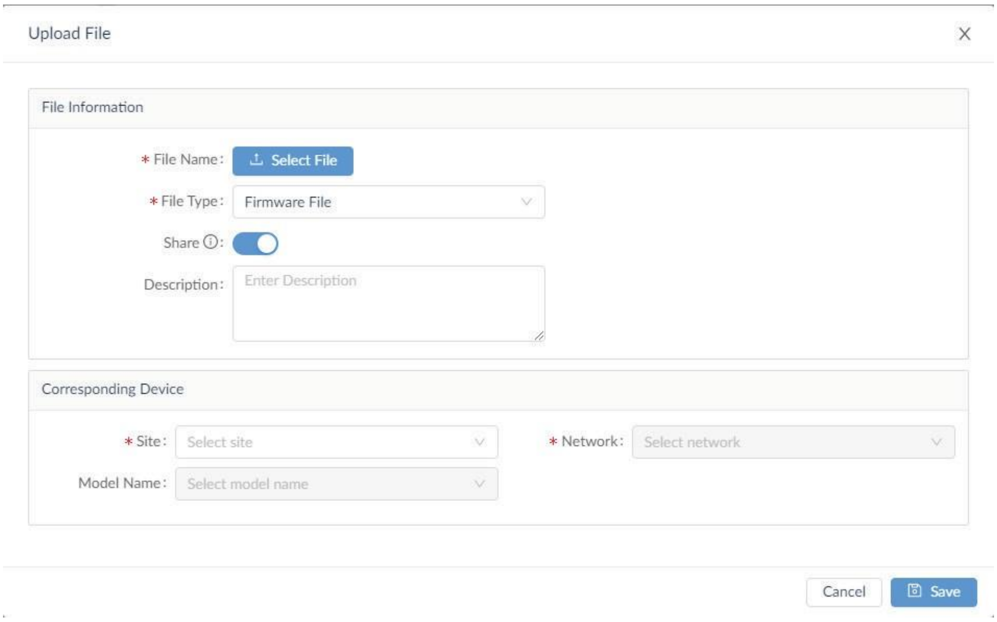
Home | File Management ×

Search | + Upload File | Delete | File Comparison

□	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	
□	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	

Total 7 items < 1 > 15 / page

2. Click **Upload File** to display the Upload File page.



Upload File ×

File Information

* File Name: Select File

* File Type: Firmware File

Share ⓘ: ●

Description: Enter Description

Corresponding Device

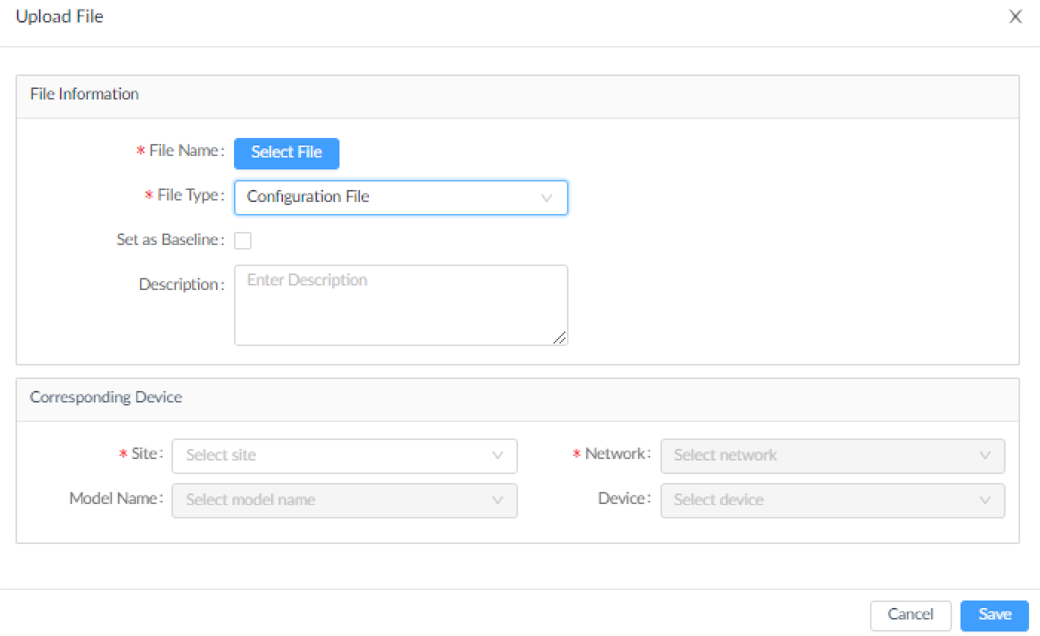
* Site: Select site

* Network: Select network

Model Name: Select model name

Cancel | Save

3. Click **Select File** to browse and select the file for upload.
4. From **File Type**, select Configuration File for the uploaded file type.
5. Click **Set as Baseline** to set the uploaded configuration as the baseline file for file comparison or default restore file.
6. In the **Description** field, enter a brief description for the file.
7. Click the **Site** drop-down menu to select a site for the devices.
8. Click the **Network** drop-down menu to select a network under the selected site.
9. Click the **Model Name** drop-down menu to select a model to apply the configuration.
10. Click the **Device** drop-down menu to select a device to apply the configuration.
11. Click **Save** to create a configuration file entry or **Cancel** to return to the previous menu.



Upload File

File Information

* File Name: Select File

* File Type: Configuration File

Set as Baseline: □

Description: Enter Description

Corresponding Device

* Site: Select site

* Network: Select network

Model Name: Select model name

Device: Select device

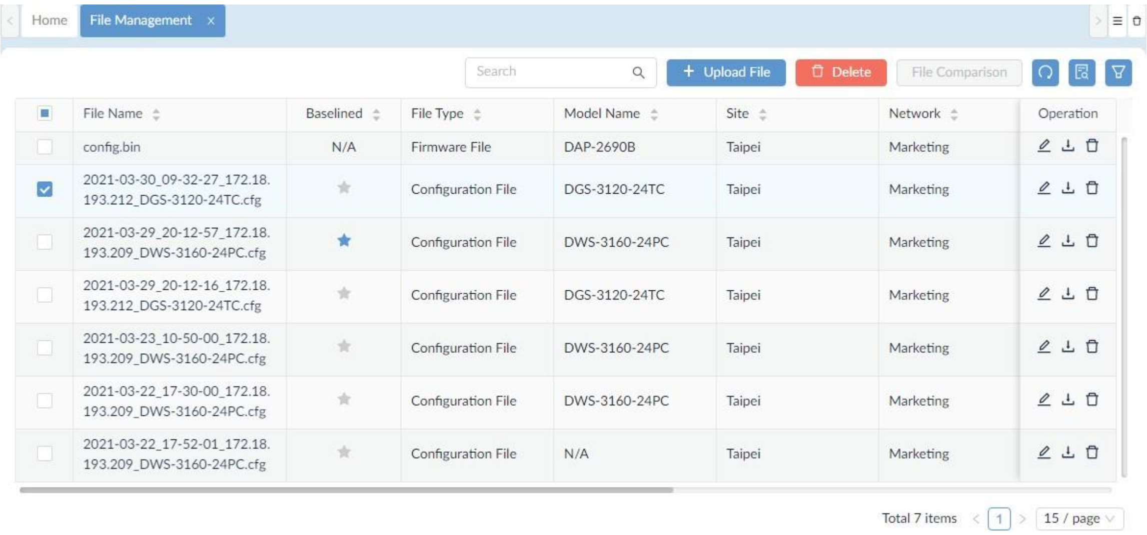
Modify a Configuration File Entry

A configuration file of a device can be used as a template to configure other devices on the network.The first step is to assign a configuration file to apply for the target device(s).

To modify settings of a configuration file:

1. Go to **Configuration > File Management**.

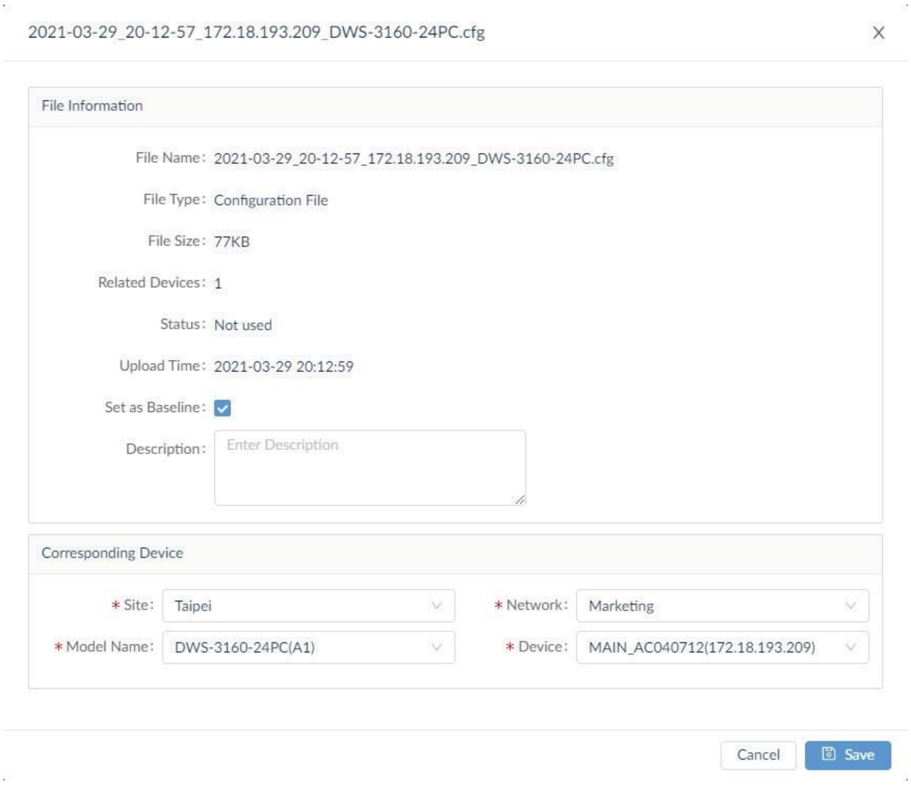
2. From the File Management page, select an existing entry from the list, then click **Edit**.



☐	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ⤓ 🗑
☑	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	✎ ⤓ 🗑

Total 7 items < 1 > 15 / page

3. The File Information page displays. From this page you can modify file information.



2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg

File Information

File Name: 2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg

File Type: Configuration File

File Size: 77KB

Related Devices: 1

Status: Not used

Upload Time: 2021-03-29 20:12:59

Set as Baseline: ☑

Description: Enter Description

Corresponding Device

* Site: Taipei

* Network: Marketing

* Model Name: DWS-3160-24PC(A1)

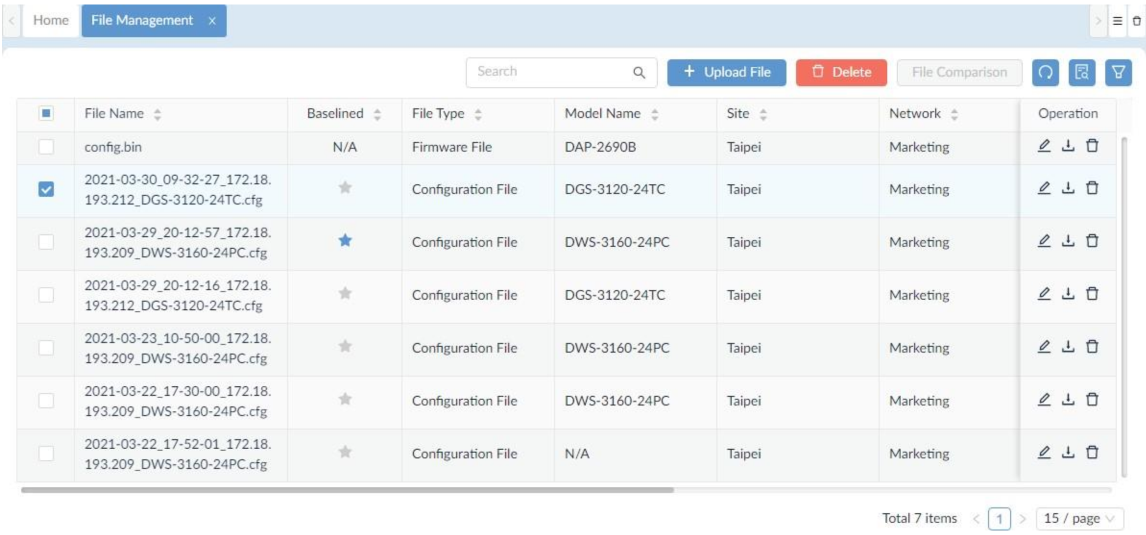
* Device: MAIN_AC040712(172.18.193.209)

4. Click **Set as Baseline** to designate this file as a baseline to be used as the default configuration for restoration.
5. Enter a description to identify the entry.
6. Modify the corresponding device information:
   - Site
   - Network
   - Model Name
   - Device
7. Click **Save** to apply the changes or **Cancel** to return to the previous menu.

Export a Configuration File

To export an existing configuration file:

1. Go to **Configuration > File Management**. The File Management page displays.



■	File Name	Baselined	File Type	Model Name	Site	Network	Operation
□	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ⤓ 🗑
☑	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ⤓ 🗑
□	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	✎ ⤓ 🗑

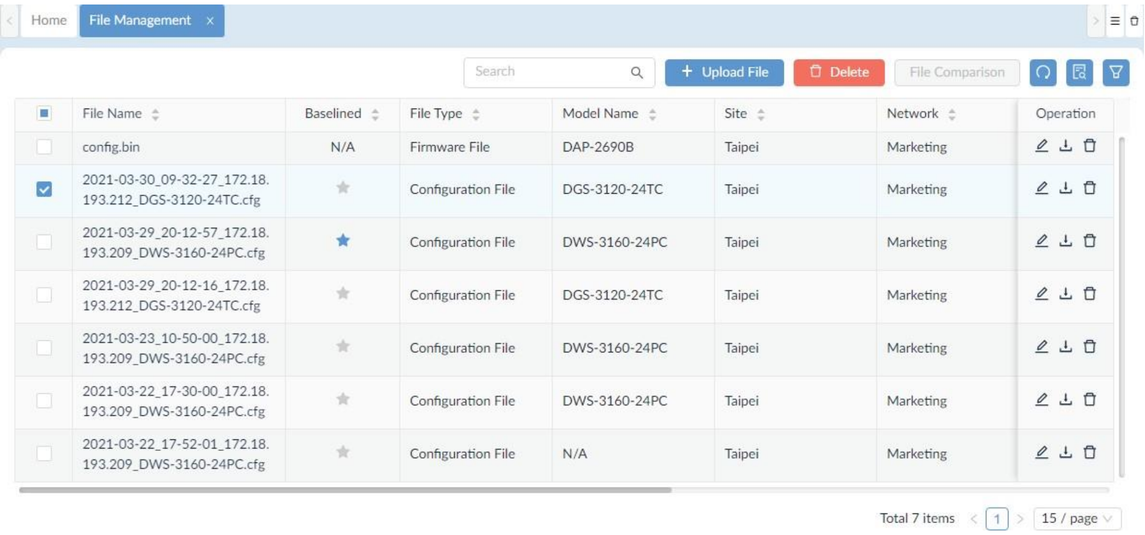
2. From the File Management page, select the desired entry from the list, then click **Download**.

The file will be downloaded to the default download folder of your browser. A successful download message will be displayed once the file is exported to the local system.

Remove a Configuration File

To remove a configuration file:

1. Go to **Configuration > File Management**.



☐	File Name	Baselined	File Type	Model Name	Site	Network	Operation
☐	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	
☑	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	
☐	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	
☐	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	☆	Configuration File	DGS-3120-24TC	Taipei	Marketing	
☐	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	
☐	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	DWS-3160-24PC	Taipei	Marketing	
☐	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	☆	Configuration File	N/A	Taipei	Marketing	

2. From the File Management page, select the desired entry with the configuration file type, then click **Delete File**.

3. A confirmation prompt will be displayed for the deletion. Click **Yes** to delete or **No** to cancel the operation.

7 Alarm and Notification

Alerts and notifications can be sent automatically when an upper or a lower threshold has been reached. If the threshold is exceeded, an alarm will be generated. You can set alarm notifications to be received by email, web scrolling notification, or as a script to be executed on selected devices.

The section covers the following topics:

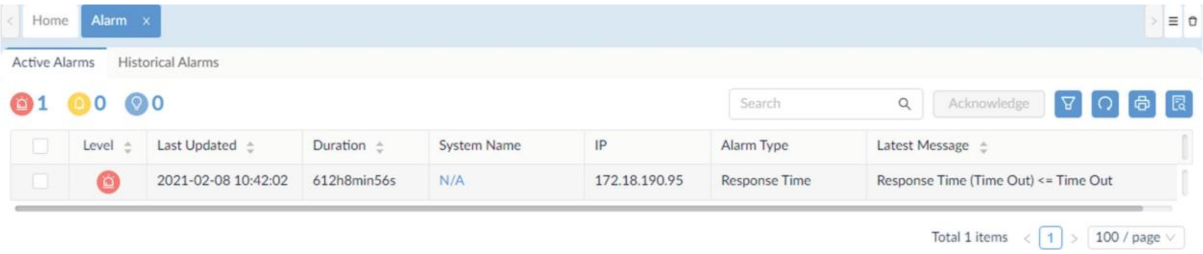
- View Alarms
- View Traps and Syslog
- Trap Editor
- Syslog Editor
- Monitor and Alarms
- View and Manage Notifications

7.1. View Alarms

Alarms for all devices can be viewed centrally from the D-View application interface.

1. Go to **Alarm & Notification > Alarm**.

2. You can view both active and historical alarms.



□	Level	Last Updated	Duration	System Name	IP	Alarm Type	Latest Message
□	●	2021-02-08 10:42:02	612h8min56s	N/A	172.18.190.95	Response Time	Response Time (Time Out) <= Time Out

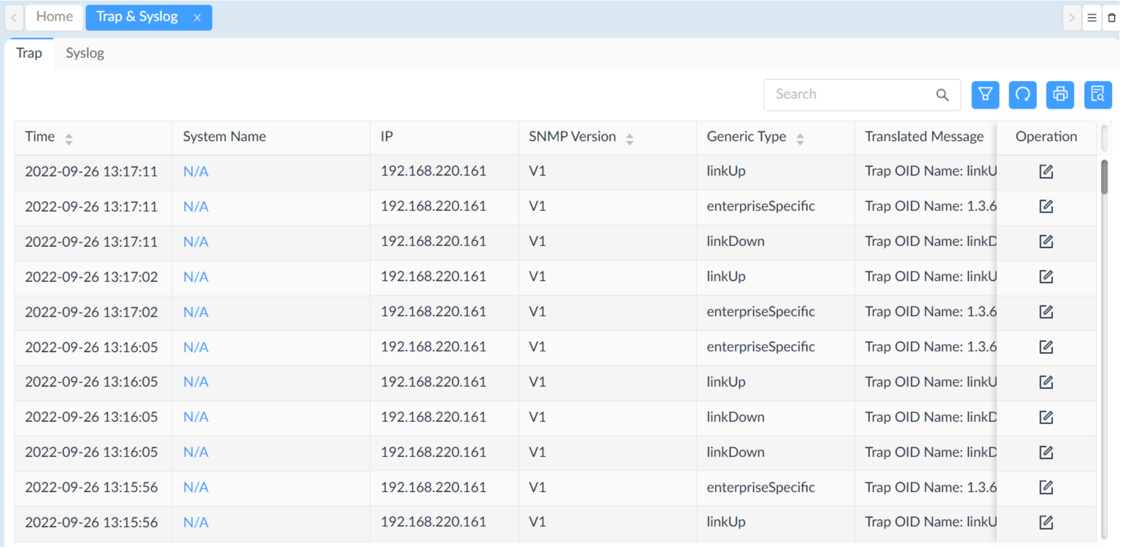
Item	Description
Active Alarms	Displays a list of the currently active alarm events.
Historical Alarms	Displays a list of alarm events already been acknowledged or been stopped.
Critical	Indicates a critical (highest) severity level for the alarm (red).
Warning	Indicates a warning (middle) severity level for the alarm (yellow).
Info	Indicates an informative (lowest) level for the alarm (blue).
Search	Enter a keyword to filter the list by System Name, IP, or Latest Message.
Acknowledge	Select an alarm event and click Acknowledge to move the alarm entry to Historical Alarms. Note that this will not disable the alarm setting.
Column Selector	Click to add or remove columns from the list. The following column properties are available: Level, Last Updated, Duration, System Name, IP, Alarm Type, and Latest Message.
Refresh	Click to refresh the table listing.
Export	Click to export the list as a CSV file. Up to 10,000 entries can be downloaded in one export job.
Advanced Query	Click to perform an advanced search job. Select the criteria to filter the table listing. Click Search to start the search.

7.2. View Traps and Syslog

The Trap & Syslog list displays the device trap events and syslog messages with the time. For trap events, the SNMP version, the original trap messages and the translated messages will be recorded. For syslog, messages will be assigned with a severity label. You can also send traps and logs to a remote logging server (go to **System > Basic Settings** > **Forward Trap** and **System > Basic Settings** > **Forward Syslog** to configure a remote trap and syslog server respectively). Both Trap and Syslog page allows you to refresh the list and export the records as a CSV file.

Note: You need to configure the D-View as Trap Server and Syslog Server for the managed devices so that logs and traps can be collected by the system (go to **Monitoring > Device View** and select the **System Name** link of a device to open its Device Information page. Then click the **Management** tab to find the Trap and Syslog status switch.) From the Device Information page, you can also view trap events and syslog messages generated from the selected device by clicking the Trap & Syslog tab.

To view device's logs, follow these steps:



Time	System Name	IP	SNMP Version	Generic Type	Translated Message	Operation
2022-09-26 13:17:11	N/A	192.168.220.161	V1	linkUp	Trap OID Name: linkU	✎
2022-09-26 13:17:11	N/A	192.168.220.161	V1	enterpriseSpecific	Trap OID Name: 1.3.6	✎
2022-09-26 13:17:11	N/A	192.168.220.161	V1	linkDown	Trap OID Name: linkD	✎
2022-09-26 13:17:02	N/A	192.168.220.161	V1	linkUp	Trap OID Name: linkU	✎
2022-09-26 13:17:02	N/A	192.168.220.161	V1	enterpriseSpecific	Trap OID Name: 1.3.6	✎
2022-09-26 13:16:05	N/A	192.168.220.161	V1	enterpriseSpecific	Trap OID Name: 1.3.6	✎
2022-09-26 13:16:05	N/A	192.168.220.161	V1	linkUp	Trap OID Name: linkU	✎
2022-09-26 13:16:05	N/A	192.168.220.161	V1	linkDown	Trap OID Name: linkD	✎
2022-09-26 13:16:05	N/A	192.168.220.161	V1	linkDown	Trap OID Name: linkD	✎
2022-09-26 13:15:56	N/A	192.168.220.161	V1	enterpriseSpecific	Trap OID Name: 1.3.6	✎
2022-09-26 13:15:56	N/A	192.168.220.161	V1	linkUp	Trap OID Name: linkU	✎

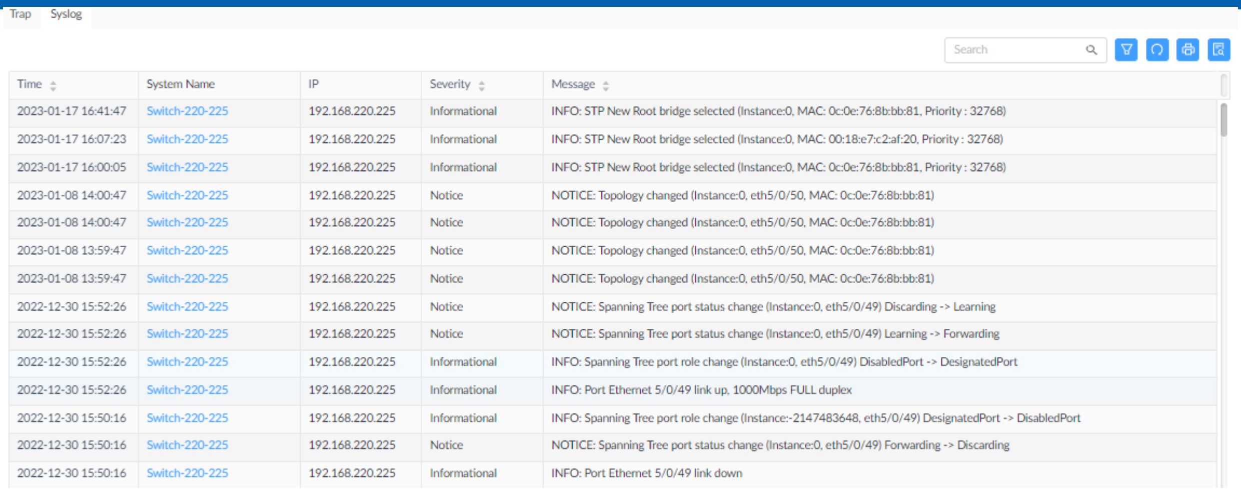
You can perform the following operations on the Trap or Syslog list:

Item	Description
Search	Enter a keyword to filter the Trap or Syslog Editor list.
Edit	For SNMP traps, you can modify their OID description as well as the value description of a binding variable (refer to the below Trap Editor section).
Advanced Query	Select the criteria to filter the events or logs.
Refresh	Click to refresh the table listing.
Export	Export the table in CSV file format.

The translated message is based on the message from the original trap events. You can modify the translation between a trap OID and OID description as well as the translation between binding variable value and value description for OIDs with binding variables by clicking **Edit** ✎ under **Operation**. Note the modification here will also be saved on the **Trap Editor** page (go to **Alarm & Notification > Trap & Syslog Editor > Trap Editor**.)

You can also configure alarm rules based on selected trap event with matched trap OID or binding values. Refer to 7.5 Monitor and Alarms for more information.

Click the **Syslog** tab to view syslog list.



Time	System Name	IP	Severity	Message
2023-01-17 16:41:47	Switch-220-225	192.168.220.225	Informational	INFO: STP New Root bridge selected (Instance:0, MAC: 0c:0e:76:8b:bb:81, Priority : 32768)
2023-01-17 16:07:23	Switch-220-225	192.168.220.225	Informational	INFO: STP New Root bridge selected (Instance:0, MAC: 00:18:e7:c2:af:20, Priority : 32768)
2023-01-17 16:00:05	Switch-220-225	192.168.220.225	Informational	INFO: STP New Root bridge selected (Instance:0, MAC: 0c:0e:76:8b:bb:81, Priority : 32768)
2023-01-08 14:00:47	Switch-220-225	192.168.220.225	Notice	NOTICE: Topology changed (Instance:0, eth5/0/50, MAC: 0c:0e:76:8b:bb:81)
2023-01-08 14:00:47	Switch-220-225	192.168.220.225	Notice	NOTICE: Topology changed (Instance:0, eth5/0/50, MAC: 0c:0e:76:8b:bb:81)
2023-01-08 13:59:47	Switch-220-225	192.168.220.225	Notice	NOTICE: Topology changed (Instance:0, eth5/0/50, MAC: 0c:0e:76:8b:bb:81)
2023-01-08 13:59:47	Switch-220-225	192.168.220.225	Notice	NOTICE: Topology changed (Instance:0, eth5/0/50, MAC: 0c:0e:76:8b:bb:81)
2022-12-30 15:52:26	Switch-220-225	192.168.220.225	Notice	NOTICE: Spanning Tree port status change (Instance:0, eth5/0/49) Discarding -> Learning
2022-12-30 15:52:26	Switch-220-225	192.168.220.225	Notice	NOTICE: Spanning Tree port status change (Instance:0, eth5/0/49) Learning -> Forwarding
2022-12-30 15:52:26	Switch-220-225	192.168.220.225	Informational	INFO: Spanning Tree port role change (Instance:0, eth5/0/49) DisabledPort -> DesignatedPort
2022-12-30 15:52:26	Switch-220-225	192.168.220.225	Informational	INFO: Port Ethernet 5/0/49 link up, 1000Mbps FULL duplex
2022-12-30 15:50:16	Switch-220-225	192.168.220.225	Informational	INFO: Spanning Tree port role change (Instance:-2147483648, eth5/0/49) DesignatedPort -> DisabledPort
2022-12-30 15:50:16	Switch-220-225	192.168.220.225	Notice	NOTICE: Spanning Tree port status change (Instance:0, eth5/0/49) Forwarding -> Discarding
2022-12-30 15:50:16	Switch-220-225	192.168.220.225	Informational	INFO: Port Ethernet 5/0/49 link down

The syslog contains the following severity levels from the highest to the lowest.

Severity	Description
Emergency	Indicates that the device is failing to operate normally.
Alert	Indicates that immediate investigation is needed.
Critical	Indicates that the device is in critical condition.
Error	Indicates that an error has been found on the device.
Warning	Indicates a warning condition of the device’s operation.
Notice	Indicates a normal but significant condition that needs an operator’s attention.
Informational	Indicates a specific condition that is not erroneous but needs to be recorded for reference or troubleshooting purposes.
Debug	Indicates messages for debugging purposes.

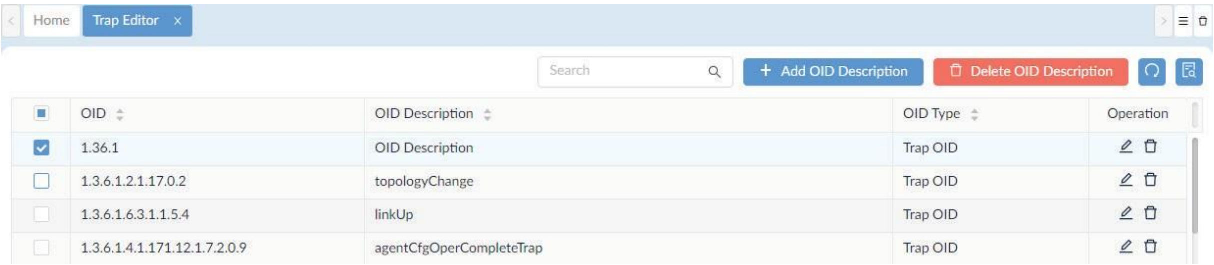
You can easily spot a particular log message when interpreting syslog reports by setting a syslog description with associated syslog keywords. Refer to the below **12 Reports** and 7.4 Syslog Editor for more information.

7.3. Trap Editor

Traps can alert you to possible errors of the managed devices while syslog records problems of device operation. You can define object identifiers (OIDs) of a trap to help determine the nature of a problem. To view trap messages of all managed devices, go to **Alarm & Notification >Trap & Syslog > Trap**.

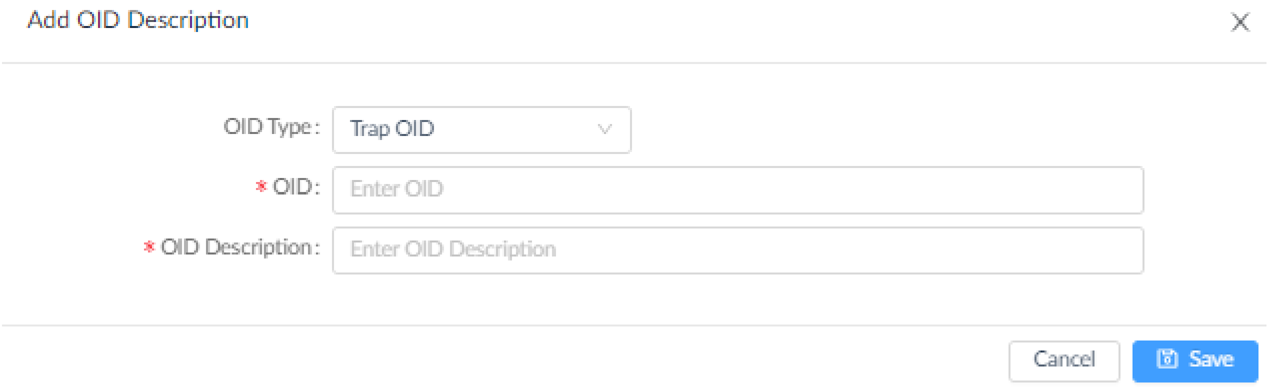
To add an OID description entry:

1. Go to **Alarm & Notification > Trap & Syslog Editor**.
2. Click the **Trap Editor** tab. You can add a trap OID or a binding variable OID type.



□	OID	OID Description	OID Type	Operation
☑	1.36.1	OID Description	Trap OID	✎ 🗑
□	1.3.6.1.2.1.17.0.2	topologyChange	Trap OID	✎ 🗑
□	1.3.6.1.6.3.1.1.5.4	linkUp	Trap OID	✎ 🗑
□	1.3.6.1.4.1.171.12.1.7.2.0.9	agentCfgOperCompleteTrap	Trap OID	✎ 🗑

To add a trap or binding variable OID, click **Add OID Description**. Then enter an OID with a description for both types of OID. For binding variable OIDs, enter variable values with matching descriptions. The entry determines how a trap should be interpreted.


Add OID Description

OID Type: Trap OID

* OID: Enter OID

* OID Description: Enter OID Description

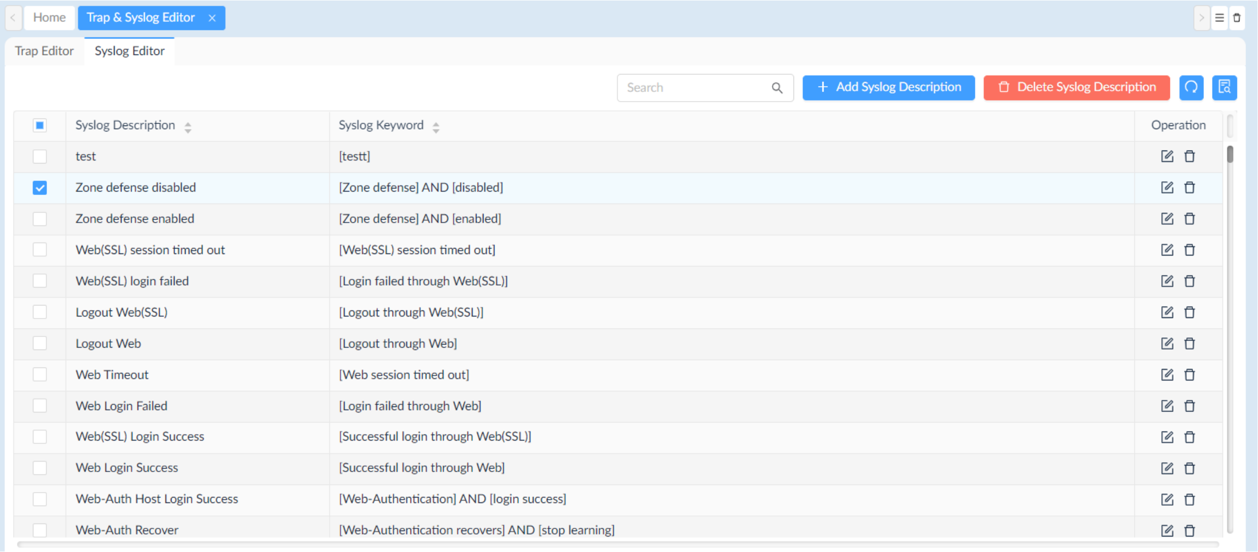
To edit an entry, select it and click Edit ✎. The translated message in the Trap list should reflect the changes. You can generate trap reports using the provided report template and the OID description will be the highlighted text to signify trap events. Refer to 12.2.1 Add a Report for more information.

7.4. Syslog Editor

The syslog is used to log device data. It allows you to analyze and help troubleshoot problems in time. Furthermore, you can add a syslog description to help you visualize particular log messages. To generate a Syslog report with the effect provided by Syslog Editor, go to **Reports > General Reports** and select the **Syslog** category under **Device Reports**. (Refer to 12.2 Manage Report Templates for more information.) To view logs of all managed devices, go to **Alarm & Notification >Trap & Syslog > Syslog**.

To obtain the types of syslog messages:

1. Go to **Alarm & Notification > Trap & Syslog Editor**.



■	Syslog Description	Syslog Keyword	Operation
□	test	[testt]	
☑	Zone defense disabled	[Zone defense] AND [disabled]	
□	Zone defense enabled	[Zone defense] AND [enabled]	
□	Web(SSL) session timed out	[Web(SSL) session timed out]	
□	Web(SSL) login failed	[Login failed through Web(SSL)]	
□	Logout Web(SSL)	[Logout through Web(SSL)]	
□	Logout Web	[Logout through Web]	
□	Web Timeout	[Web session timed out]	
□	Web Login Failed	[Login failed through Web]	
□	Web(SSL) Login Success	[Successful login through Web(SSL)]	
□	Web Login Success	[Successful login through Web]	
□	Web-Auth Host Login Success	[Web-Authentication] AND [login success]	
□	Web-Auth Recover	[Web-Authentication recovers] AND [stop learning]	

2. Click the **Syslog Editor** tab. You can perform the following operations on the list of Syslog Description:

Item	Description
Search	Enter a keyword to search for a log description entry using syslog description or syslog keyword.
Add Syslog Description	Add a syslog description representing selected log keywords to be displayed as highlight text to signify a condition or operation from log messages. Refer to 12.2.1 Add a Report for more information.
Delete Syslog Description	Click to delete a syslog description entry.
Refresh	Click to refresh the table listing.
Advanced Query	Click to perform advanced search. Enter the criteria to filter the table.
Edit	Click Edit to modify a syslog description.
Delete	Click to delete a syslog description.

You can also configure alarm rules based on the severity of Syslog. In addition, you can set the system to alert you that certain types of messages with matching content have been logged. Refer to 7.5 Monitor and Alarms for more information.

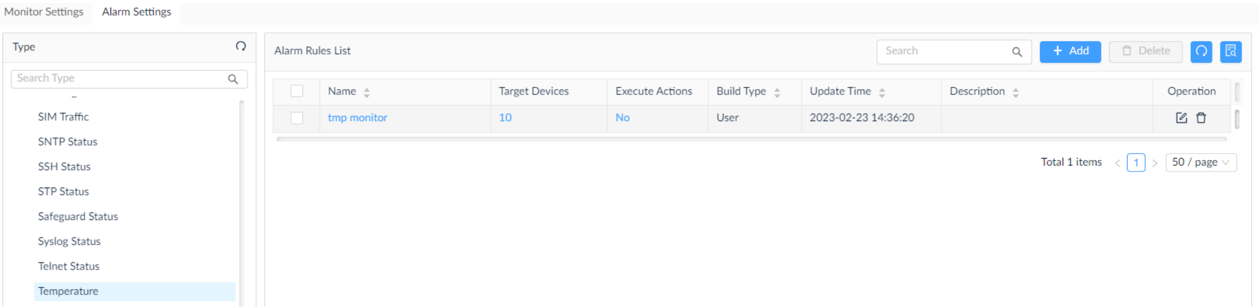
7.5. Monitor and Alarms

7.5.1 Alarm Settings

You can manage monitor and alarm settings and configure conditions to trigger alarms. Alarms can be triggered by CPU or memory utilization and a wide range of system metrics. They can be configured by users or by the system as the defaults.

To view all configured alarms:

1. Go to **Alarm & Notification > Monitor & Alarm Settings**.
2. Click the **Alarm Settings** tab.



□	Name	Target Devices	Execute Actions	Build Type	Update Time	Description	Operation
□	tmp monitor	10	No	User	2023-02-23 14:36:20		

Total 1 items < 1 > 50 / page

The following system-built categories of device status can be configured for an alarm:

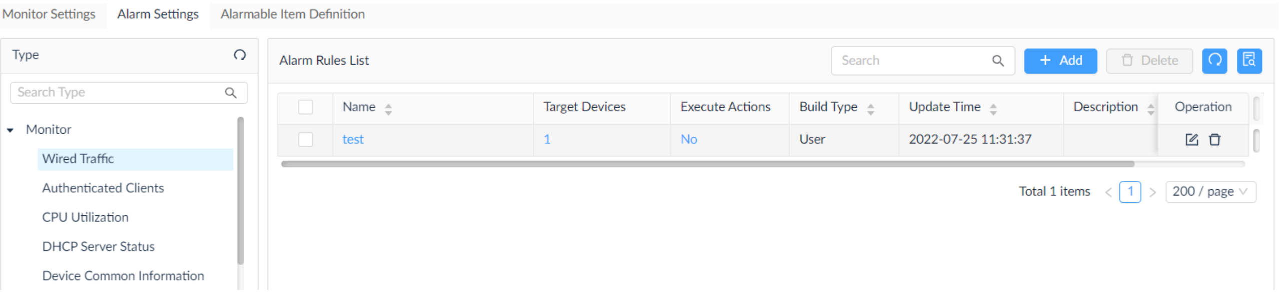
Category	Item	Description
Monitor	Wired Traffic	Alert based on Rx/Tx traffic, error rate, discard rate, and bandwidth utilization
	Authenticated Clients	Alert based on Rx/Tx speed of authenticated clientsand client number
	CPU Utilization	Alert based on CPU utilization
	DHCP Server Status	Alert based on DHCP status
	Device Common Information	Alert based on firmware version, hardware version, MAC address, serial number, or total flash capacity.
	Fan	Alert based on fan status or speed
	HTTP Status	Alert based on HTTP status or port number.
	HTTPS Status	Alert based on HTTPS status
	Installed Apps	Alert based on the number of installed apps.
	LACP	Alert based on LACP state
	LLDP	Alert based on LLDP status
	Managed AP WLAN Traffic (packet)	Alert based on WLAN Rx or Tx traffic
	Memory Utilization	Alert based on memory utilization

	Power Status	Alert based on power status
	Private Port	Alert based on the port details of D-Link switches using the private MIB.
	RMON Status	Alert based on RMON status
	Response Time	Alert based on response time (a system-default alarm)
	Running Software	Alert based on the software running on hosts
	SIM Traffic	Alert based on the upload and download traffic on the SIM card
	SNTP Status	Alert based on the SNTP status
	SSH Status	Alert based on the SSH version, status, maximum authentication failed attempts, session key rekeying times, maximum session, connection timeout, or port number
	STP Status	Alert based on STP status
	Safeguard Status	Alert based on Safeguard status
	Syslog Status	Alert based on Syslog status
	Telnet Status	Alert based on telnet status and port
	Temperature	Alert based on the temperature indicators and measurements
	Trap Status	Alert based on the trap status
	Wireless Access Points (number)	Alert based on the number of standalone AP, managed AP, total AP, or rogue AP
	Wireless Error Packets	Alert based on the number of Rx or Tx error packets transmitted wirelessly
	Wireless Traffic (bit)	Alert based on the Rx or Tx traffic (bps)
	Wireless Traffic (packet)	Alert based on the Rx or Tx traffic (pps)
Trap	Cold Start	Alert based on a device coldStart trap
	Warm Start	Alert based on a device warmStart trap
	Link Down	Alert based on a port linkDown trap
	Link Up	Alert based on a linkUp trap
	Authentication Failure	Alert based on an SNMP authentication failure trap
	EGP Neighbor Loss	Alert based on an EGP Neighbor Loss trap
	Enterprise Specific	Alert based on an enterprise-specific trap
Syslog	Syslog	Alert based on a syslog message with matching content
sFlow	sFlow traffic	Alert based on an sFlow traffic packet

From the Alarm Settings menu, you can set rules for different monitor categories or traffic and message types such as Trap, Syslog, and sFlow.

To add an alarm rule:

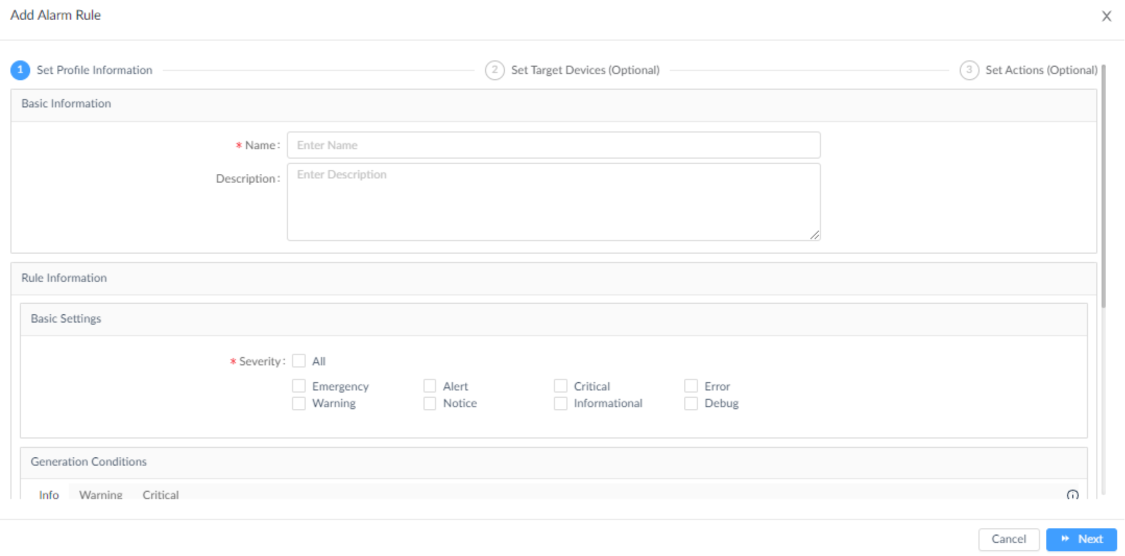
1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then select the **Alarm Settings** tab.
2. From the left pane, select a system-defined monitor category (or a customized monitor category) for configuration.
3. Click +**Add** to configure a rule.



	Name	Target Devices	Execute Actions	Build Type	Update Time	Description	Operation
□	test	1	No	User	2022-07-25 11:31:37		

Total 1 items < 1 > 200 / page

The **Add Alarm Rule** page displays.



* Name: Enter Name

Description: Enter Description

* Severity: □ All

□ Emergency □ Alert □ Critical □ Error

□ Warning □ Notice □ Informational □ Debug

Different rules require different configurations that may involve traffic rate or utilization percentage as well as traffic direction. The following general settings are presented for all alarm rule types:

- Set profile information: enter a name and description for the alarm rule.
- Set alarm generation conditions: set the threshold value for different levels of severity for the alarm: Info, Warning, and Critical. The parameters for settings the threshold value depend on the monitored condition types.
- Set alarm release conditions: set the threshold value for clearing the alarm.
- Set target device/source: set the devices and device interfaces (for the **Wired Traffic** monitoring condition) to be monitored.
- Set alarm criteria (only applicable to the sFlow alarm category): set criteria (e.g. application, DSCP value, IP address, or protocol) along with sFlow interfaces and direction to be monitored.
- Add Inhibition Schedule Settings: select a pre-defined schedule or click **Add Schedule** to add a new schedule. The Schedule prohibits delivery of alarms at the specified time range of a designated weekday or weekdays for the effective duration of dates.
- Set Actions (optional): execute a script. The script can be executed on designated device(s) other than the device configured as the alarm source or on the selected D-View 8 servers. Click **Add actions** at the upper right and click the respective Device or Server Command tab. To execute commands on device(s), configure the credentials and method for logging in to the devices.

Click **Next** or **OK** to continue the rule configuration. Then click **Save** to create the rule and exit the screen.

Note: After an alarm has been configured for the selected devices, you can activate the alarm on a per-device or per-port basis (for the **Wired Traffic** monitoring condition) . Go to **Monitoring > Device View** and click the

System Name link to go to the **Device Information** page. Then select the **Port** or **Alarm** tab to access the port list or alarm settings page. For Port list, you can turn on or off the Alarm Switch for each port. For Alarm settings, turn on or off a specific alarm type.

7.5.2 Monitor Settings

Network monitoring is performed through the Monitor and Alarm settings menu. You can select a specific monitor category to view available configuration settings.

To obtain monitoring conditions:
1. Go to **Alarm & Notification > Monitor & Alarm Settings**.
2. Click the **Monitor Settings** tab.
3. Click a monitor category to view all monitoring settings in that category.

To edit a monitoring condition:

Select a device or multiple devices and adjust the monitoring interval by clicking **Edit Interval**. Depending on the monitored condition, you may edit monitor status or port numbers if they are applicable.

To apply ports settings:

Select a device or multiple devices, click **Batch Select Port** and enter the port range (e.g. 1,3-8,10), and click **Apply**. Then click **Edit Monitoring Status** to enable or disable monitoring on the designated ports.

To stop monitoring:

Select a device or multiple devices and adjust the monitoring status by clicking **Edit Monitoring Status**. Then click ON or OFF to enable or disable monitoring.

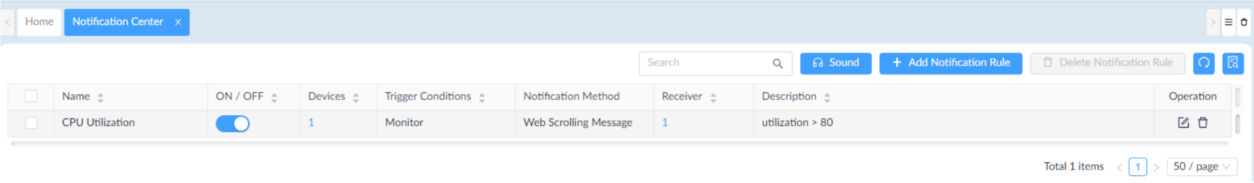
Note: Stopping a monitoring condition will cause the associated alarms to be disabled automatically.

7.6. Manage Notifications

The Notification Center displays the notification rules. It allows you to configure rules of trigger conditions and notification recipients and set schedules for notification activation.

To set a notification rule:

1. Go to **Alarm & Notification > Notification Center**.



Name	ON / OFF	Devices	Trigger Conditions	Notification Method	Receiver	Description	Operation
CPU Utilization	●	1	Monitor	Web Scrolling Message	1	utilization > 80	

Total 1 items 1 50 / page

The

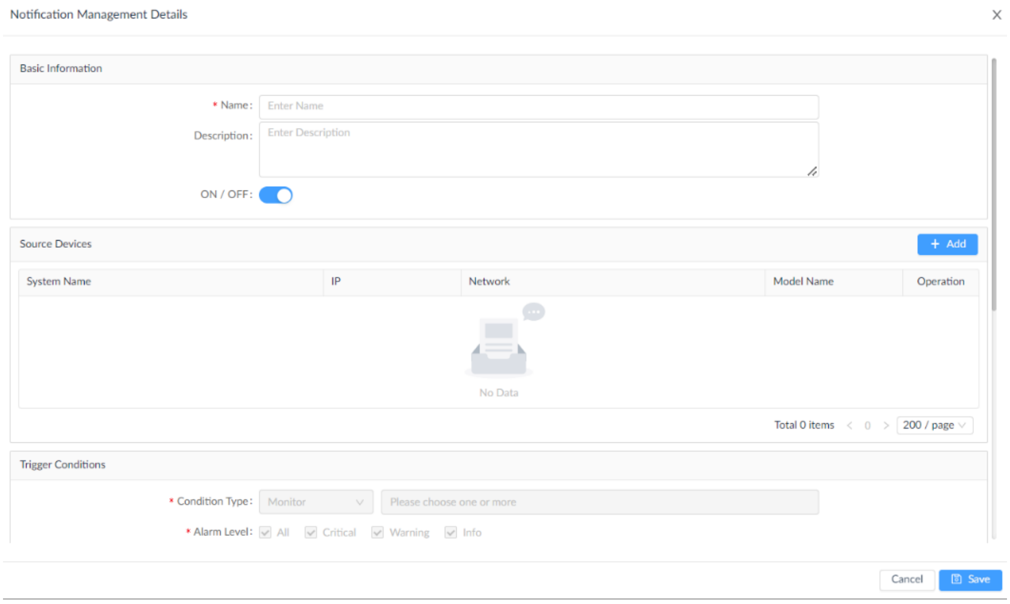
The Notification Center page displays.

The list contains the following information on rule and display control:

Item	**Description**
Search	Enter a keyword to search for a specific notification name.
Sound	Click to customize a ringtone to sound when a notification is triggered. Different alarm levels can be configure with different built-in ringtones.
Add Notification Rule	Click to define a notification rule.
Delete Notification Rule	Click to remove the notification rule.
Refresh	Click to refresh the table.
Advanced Query	Click to configure an advanced search job. Select the criteria to filter the list: Name, On/Off status, Trigger Conditions, or Notification Method.
Name	The name of the notification rule.
On/OFF	Enable or disable the notification.
Devices	The number of devices to which the rule applies.
Trigger Conditions	The monitored condition type (i.e. monitor, trap, syslog, or wired traffic) to trigger a notification.
Notification Method	The method of notification for the rule (i.e. web scrolling message, email, or execute script).
Receiver	The number of notification recipients. Click on it to display user profile as the recipient of the notification.
Description	A description of the rule.

1. Click **+ Add Notification Rule** to configure a new rule.

The **Notification Management Details** page displays.



Notification Management Details

Basic Information

* Name: Enter Name

Description: Enter Description

ON / OFF:

Source Devices

+ Add

System Name	IP	Network	Model Name	Operation

No Data

Total 0 items < 0 > 200 / page

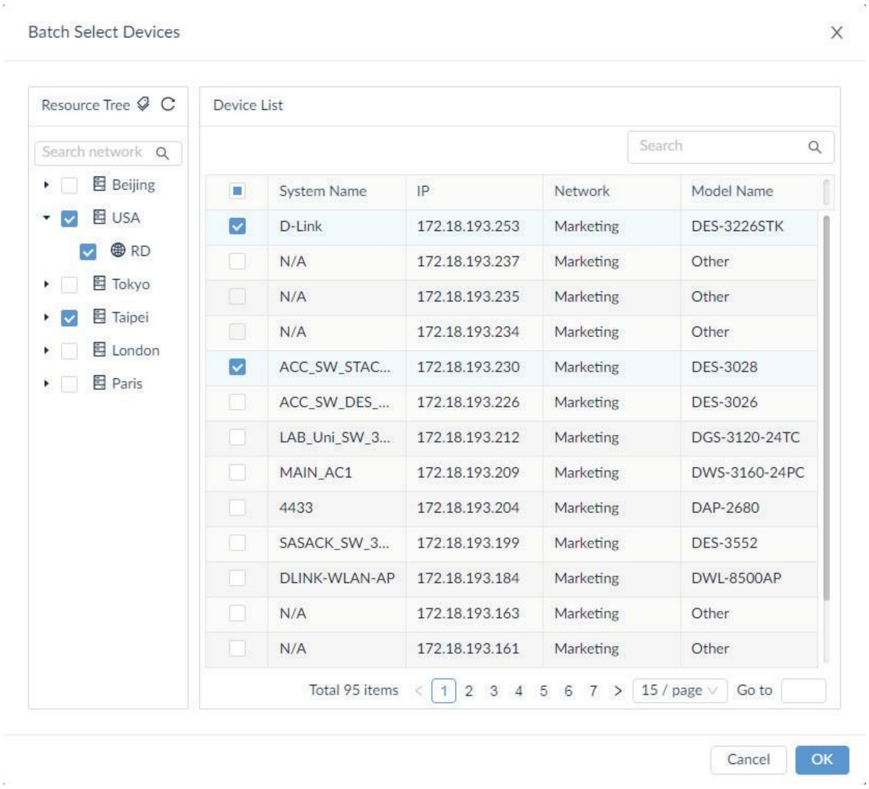
Trigger Conditions

* Condition Type: Monitor | Please choose one or more

* Alarm Level: ☑ All ☑ Critical ☑ Warning ☑ Info

Cancel | Save

2. Under **Basic Information**, enter a name and description to define the rule.
3. Click **ON/OFF** switch to enable or disable the rule.
4. In Source Devices, click **Add** to select target devices.The **Batch Select Devices** page displays.



Batch Select Devices

Resource Tree

Search network

- □ Beijing
- ☑ USA
  - ☑ RD
- □ Tokyo
- ☑ Taipei
- □ London
- □ Paris

Device List

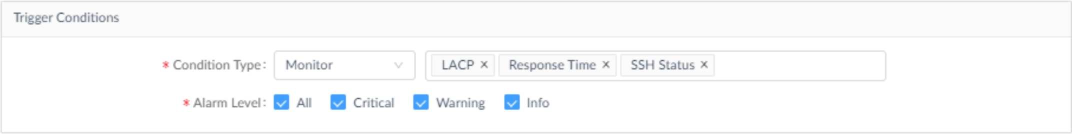
Search

■	System Name	IP	Network	Model Name
☑	D-Link	172.18.193.253	Marketing	DES-3226STK
□	N/A	172.18.193.237	Marketing	Other
□	N/A	172.18.193.235	Marketing	Other
□	N/A	172.18.193.234	Marketing	Other
☑	ACC_SW_STAC...	172.18.193.230	Marketing	DES-3028
□	ACC_SW_DES_...	172.18.193.226	Marketing	DES-3026
□	LAB_Uni_SW_3...	172.18.193.212	Marketing	DGS-3120-24TC
□	MAIN_AC1	172.18.193.209	Marketing	DWS-3160-24PC
□	4433	172.18.193.204	Marketing	DAP-2680
□	SASACK_SW_3...	172.18.193.199	Marketing	DES-3552
□	DLINK-WLAN-AP	172.18.193.184	Marketing	DWL-8500AP
□	N/A	172.18.193.163	Marketing	Other
□	N/A	172.18.193.161	Marketing	Other

Total 95 items < 1 2 3 4 5 6 7 > 15 / page Go to

Cancel | OK

5. Click **OK** to confirm the selection and return to the previous screen.
6. Under the Trigger Conditions, click the **Condition Type** drop-down menu to select a trigger condition type.



Trigger Conditions

* Condition Type: Monitor | LACP × | Response Time × | SSH Status ×

* Alarm Level: ☑ All ☑ Critical ☑ Warning ☑ Info

The following table describes the condition types.

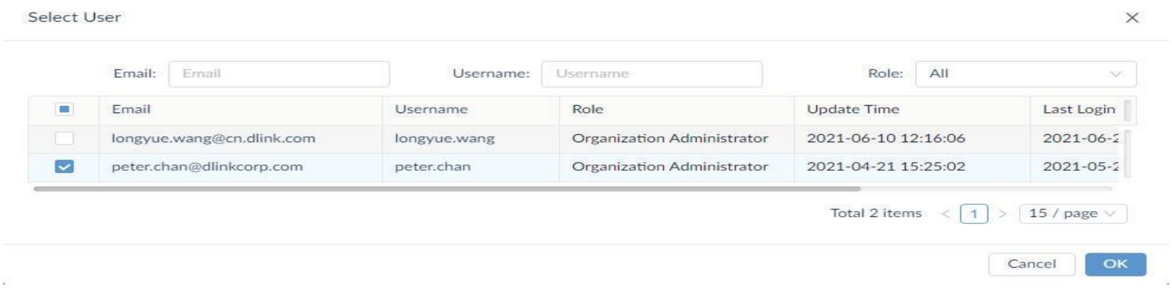
Item	Description
Condition Type	
Monitor	The monitor categories vary depending on the selected device model. • CPU Utilization • DHCP Server Status • Device Common Information • Fan • HTTP Status • LACP • LLDP • Memory Utilization • Power Status • Private Port • RMON Status • Response Time • SNTP Status • SSH Status • STP Status • Safeguard Status • Syslog Status • Telnet Status • Temperature • Trap Status • Authenticated Clients • Wireless Traffic • Wireless Error Packets
Trap	Select the corresponding severity level to generate a notification for the configured alarms based on Trap: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification.
Syslog	Select the corresponding severity level to generate a notification for configured alarms based on Syslog: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification.
Wired Traffic	Select the corresponding severity level to generate a notification for configured alarms based on Wired Traffic: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification. For Wired Traffic, select the ports that will be monitored for notification rules. Note that the monitored ports must also be the ports configured in the corresponding alarm rules for the notification to take effect. Note that there must be an alarm set with the corresponding severity level for the notification to take effect.

7. Under **Notification Details**, select the Notification Method.

Item	Description
Notification Method	
Web Scrolling Message	Notifications will appear as toast messages when you are logged in to the D-View 8 web application. Select the Screen Scrolling Setting for the alert: Mute sound or Enable Voice.
Email	Select this option to receive notifications by email. See below steps to add notification receiving administrators.
Execute script	In the Command Line, enter the script to execute. **Notes:** 1. Lines begin with a '#' will be considered as comments and will not be considered as commands. 2. Use '%' before and after the word to label it as a variable. Example: %IP%. 3. The variables' value can be set in the 'Device Attribute' table. 4. Each line must contain no more than one CLI command. 5. Avoid endless CLI commands to prevent deadlock operation. Example: ping 10.0.0.1. 6. Avoid CLI commands that may require special inputs to exit to prevent deadlock operation. Example: show ports. Sample script: config ssh authmode password enable config ssh server contimeout 120 enable SSH Sample script with variables: config fdb aging_time %TimeoutSeconds% Sample comments: # this is a comment You can choose to execute a script the source devices (Itself) or devices other than the source devices (Other Devices) when a notification is generated. To execute a script, config the username and password and protocol to log in to the selected devices to which the script will apply. • The **Acknowledge Alarm after Script Execution** parameter can be used to terminate the repetitive execution of the script. For each execution of the script, the alarm will be automatically acknowledged. Enter the total Number of Repetitions (1-100) and Cycle Time (5-1440) minutes. The automatic script execution will stop when the maximum number of repetitions has been reached in the defined cycle time.

8. Under the **Notification Receiving Administrator**, click **Add** to specify users who will receive notifications.

9. The **Select User** page displays. Select administrators to receive notifications from the list or enter criteria (email, username, or user role) to search for a user.



Select User

Email: Email　Username: Username　Role: All

■	Email	Username	Role	Update Time	Last Login
□	longyue.wang@cn.dlink.com	longyue.wang	Organization Administrator	2021-06-10 12:16:06	2021-06-2
☑	peter.chan@dlinkcorp.com	peter.chan	Organization Administrator	2021-04-21 15:25:02	2021-05-2

Total 2 items　< 1 >　15 / page

10. Click **OK** to add users to the rule or **Cancel** to return to the previous page.

11. Under **Notification Suspension Period**, click **Add Schedule** to add a new schedule or select a pre-defined schedule whereby notification rule will be inactive. You can add a schedule for a specified time range of a designated weekday or weekdays for the effective duration of dates.

12. Click **Save** to accept the notification rule. Click **Cancel** to return to the previous screen.

After a notification rule is created, you can edit or delete it with the edit and delete functions under **Operation**.

8 Network Architecture

You can view network architecture through hierarchical maps. The following topics are covered in this section:

- View and Manage Network Topology
- Create a Topology View

8.1. View and Manage Network Topology

Locating devices within the network can be accomplished through a hierarchical map. Additional information such as device information and status and related performance statistics can also be obtained from the map.

Note: When the license expires, the **Topology Map** page alert you that the system is running under a restriction on the number of nodes with full functionality and encourage you to renew your annual maintenance. To add maintenance licenses, refer to 14.3 Licenses.

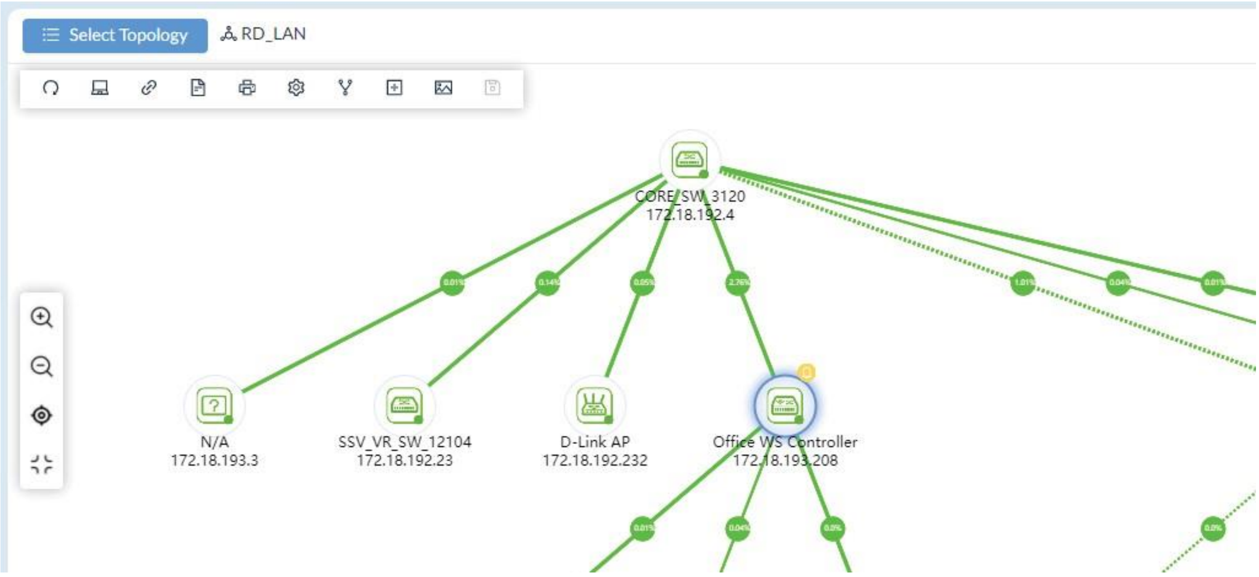
1. Go to **Monitoring > Topology Map.**
2. Click **Select Topology** to select the network diagram. The System Topology is built automatically whereas the Customized Topology is created by users.

The Topology Map page displays.

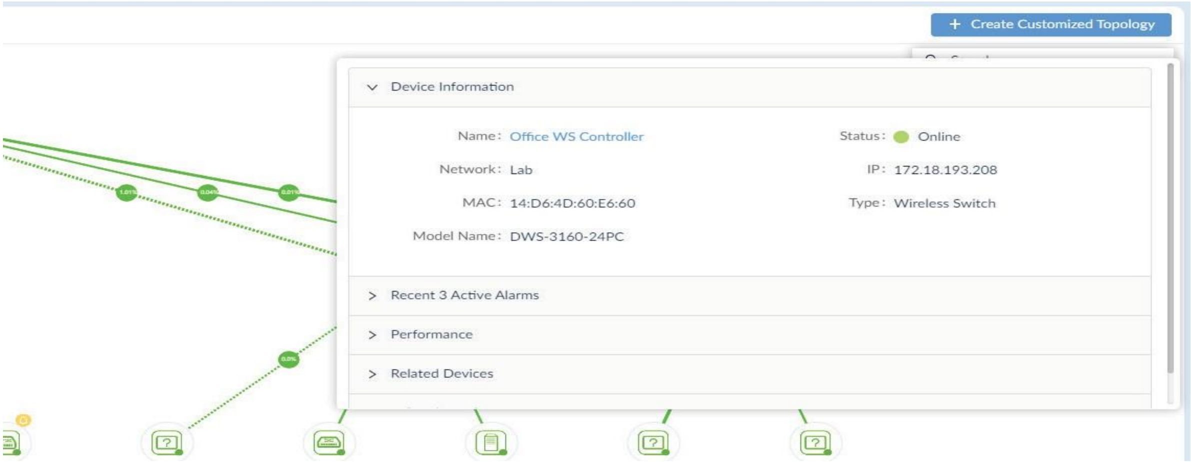
Item	**Description**
Select Topology	Click to open the System Topology or Customized Topology library. Or you can use the Search function to search available maps by entering a keyword.
Create Customized Topology	Create a customized diagram with respect to organization, site, or network.
Toolbar	**Refresh:** Refresh the screen display. **Device List:** Displays the Device View menu for the selected topology. **Link List:** Displays the Connection View page with the connecting interfaces. **Network Overview:** (1) Displays the distribution of the devices with respect to model, device type and status. (2) Displays the distribution of the devices with respect to bandwidth and status. **Export:** Save the map as a PNG file to your local drive. **Topology Settings:** Change the current topology’s information settings and layout style. Also select the information to be displayed alongside the devices. **Rediscover:** Scan the devices on the map to update the link information. **Display Settings/Current Topology Setting:** Control what should be displayed for the nodes and links on the map. Control the topology layout and central device. **Link Edit:** Enable or disable the link editing function. Enable this option and right-click on a link on the map to edit or delete it. Or you can right-click on a node to delete it. Disable this option to create link lines on the map. **Add Background:** Add a background image to the map. **Save:** Save the current topology map.
Search	Click to search specific devices.
Control Bar	The following is a description of the control bar icons from left to right. Zoom in Zoom out Focus on central node

	Zoom fit
Help	Help menu provides the following operation guidance: Topological Legend: the state/status, device type, and bandwidth representation explanation Link Operation: select a link to edit or delete Batch Select Nodes: select multiple nodes

3. From the Topology Map, select a device.When selected, the device will be highlighted.



4. Click on a device to display the device's information page in Link Edit mode (⑂).



Device Information

Name: Office WS Controller

Status: ● Online

Network: Lab

IP: 172.18.193.208

MAC: 14:D6:4D:60:E6:60

Type: Wireless Switch

Model Name: DWS-3160-24PC

> Recent 3 Active Alarms

> Performance

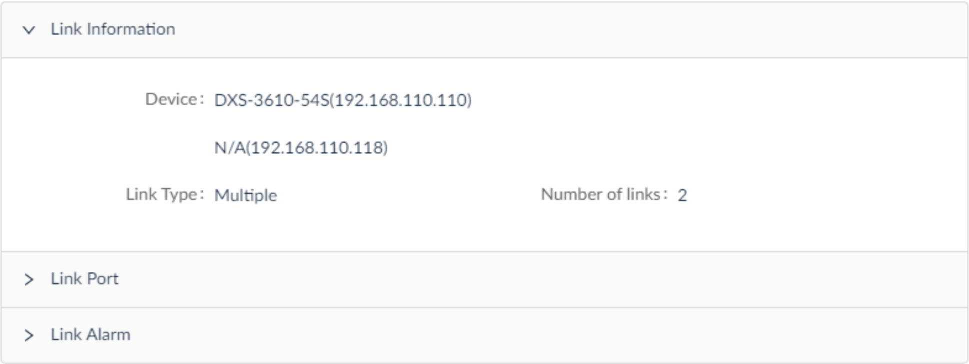
> Related Devices

`

5. The Information page provides the following information:

- Device Information: Name, Status, Network, IP Address, MAC Address, Type of the device, and Model Name.
- Recent 3 Active Alarms
- Performance: CPU utilization, availability, and memory utilization
- Related Devices: Connected devices' information
- Related Topology: Other topology from connected devices
- To modify device information, click the Device Name link to open the **Device Information** page.

6. To view details for a link, click on a link to display the Link Information page in Link Edit mode (⑂).



Link Information

Device: DXS-3610-54S(192.168.110.110)

N/A(192.168.110.118)

Link Type: Multiple

Number of links: 2

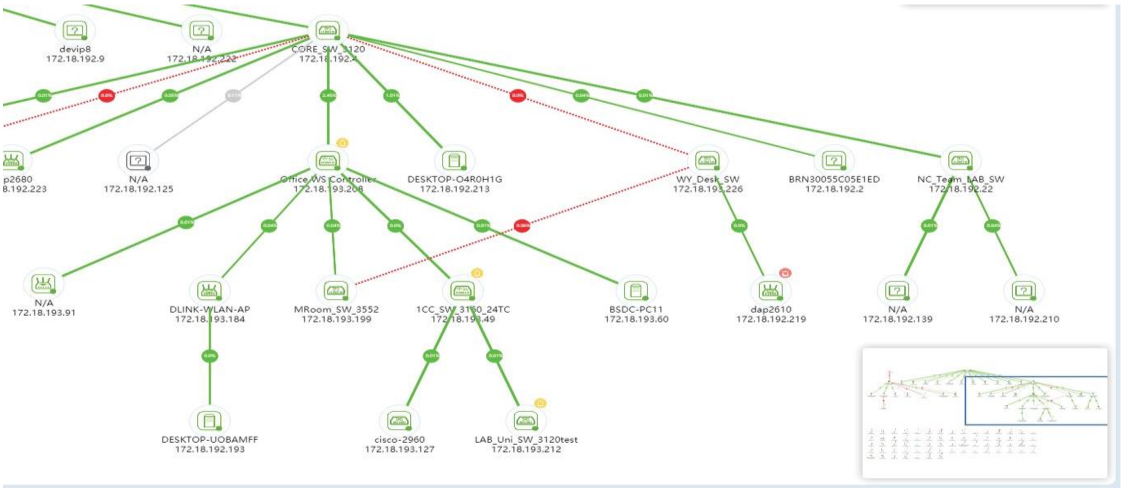
Link Port

Link Alarm

7. The Information page provides the following:

- Link Information: devices that establish the link with link type and number of links
- Link Port: linked ports of the device, bandwidth, utilization and Rx/Tx rate
- Link Alarm: alarms generated for this link activity
- To edit a link, right-click on a link and click **Edit Link**. You can modify the type of link (Normal, LACP, or logical) and the ports of the link. Normal link uses wires and cables for physical data flow whereas logical link shows data flow regardless of the physical connections among the devices in the network. For LACP link, check the Device Information page for LACP support and configuration.

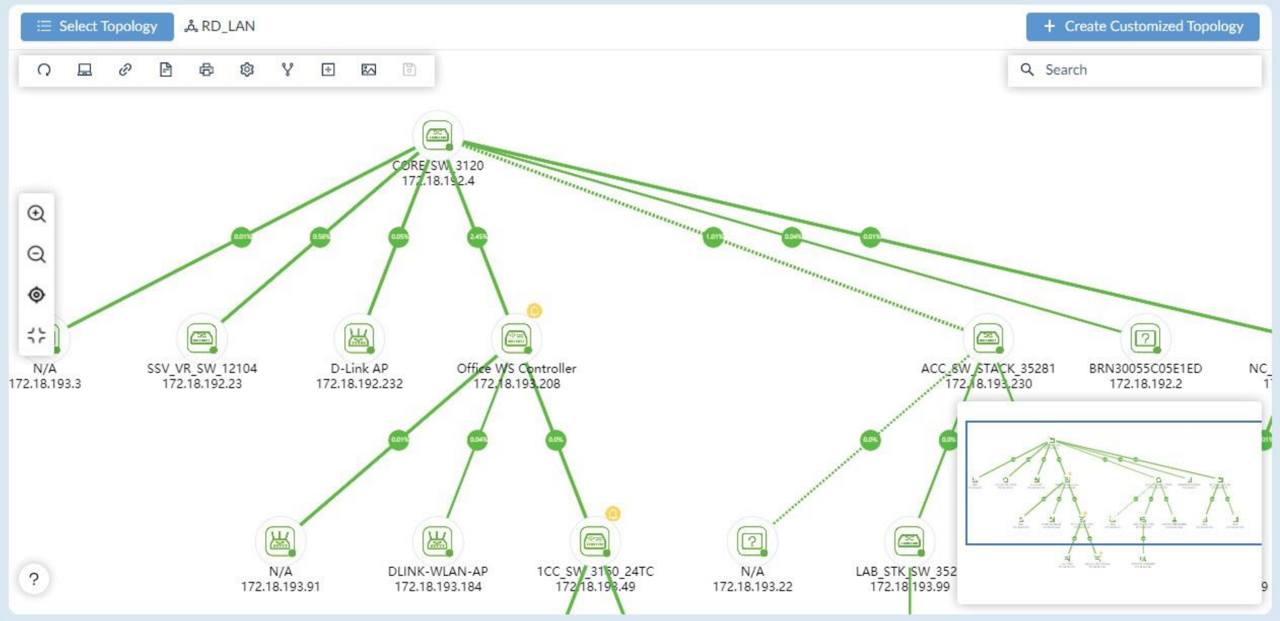
8. You can also use the navigation window at the lower right to focus an area on the map.



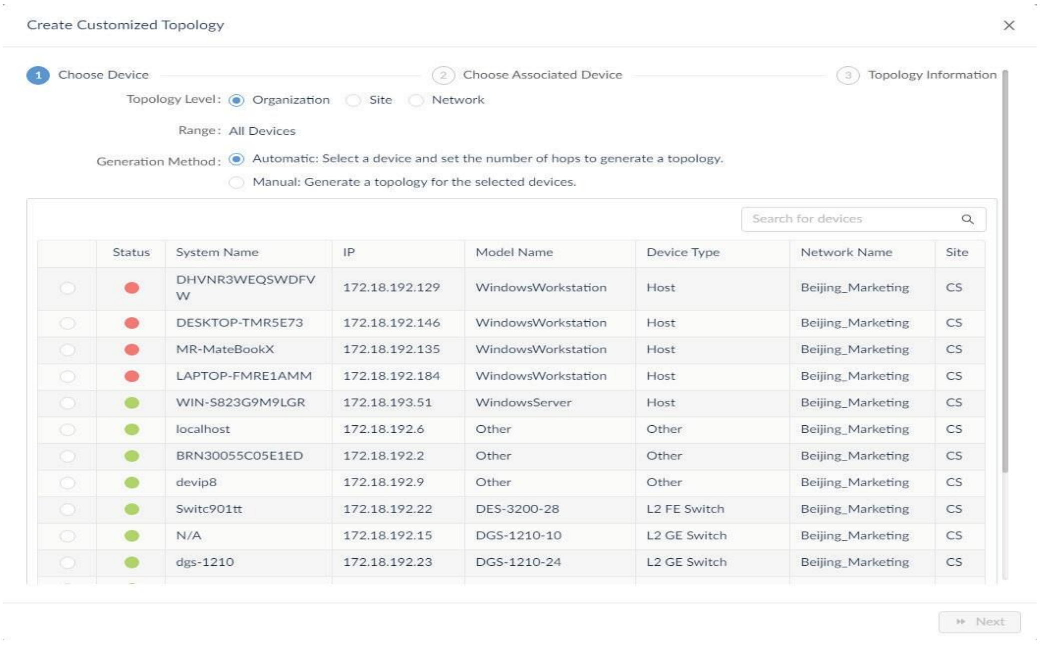
8.2. Create a Topology View

In addition to system-built topologies, you can create your own topology within a network hierarchy.

1. Go to **Monitoring > Topology Map**. The Topology Map page displays.



2. Click **Create Customized Topology** at the upper right. The Create Customized Topology page displays.



Create Customized Topology ×

1 Choose Device — 2 Choose Associated Device — 3 Topology Information

Topology Level: ● Organization ○ Site ○ Network

Range: All Devices

Generation Method: ● Automatic: Select a device and set the number of hops to generate a topology.
○ Manual: Generate a topology for the selected devices.

Search for devices

	Status	System Name	IP	Model Name	Device Type	Network Name	Site
○	🟥	DHVNR3WEQSWDFVW	172.18.192.129	WindowsWorkstation	Host	Beijing_Marketing	CS
○	🟥	DESKTOP-TMR5E73	172.18.192.146	WindowsWorkstation	Host	Beijing_Marketing	CS
○	🟥	MR-MateBookX	172.18.192.135	WindowsWorkstation	Host	Beijing_Marketing	CS
○	🟥	LAPTOP-FMRE1AMM	172.18.192.184	WindowsWorkstation	Host	Beijing_Marketing	CS
○	🟩	WIN-S823G9M9LGR	172.18.193.51	WindowsServer	Host	Beijing_Marketing	CS
○	🟩	localhost	172.18.192.6	Other	Other	Beijing_Marketing	CS
○	🟩	BRN30055C05E1ED	172.18.192.2	Other	Other	Beijing_Marketing	CS
○	🟩	devip8	172.18.192.9	Other	Other	Beijing_Marketing	CS
○	🟩	Switc901tt	172.18.192.22	DES-3200-28	L2 FE Switch	Beijing_Marketing	CS
○	🟩	N/A	172.18.192.15	DGS-1210-10	L2 GE Switch	Beijing_Marketing	CS
○	🟩	dgs-1210	172.18.192.23	DGS-1210-24	L2 GE Switch	Beijing_Marketing	CS

Next

3. Select the Topology Level to choose devices from: Organization, Site, or Network.

4. Select the method to generate the diagram.

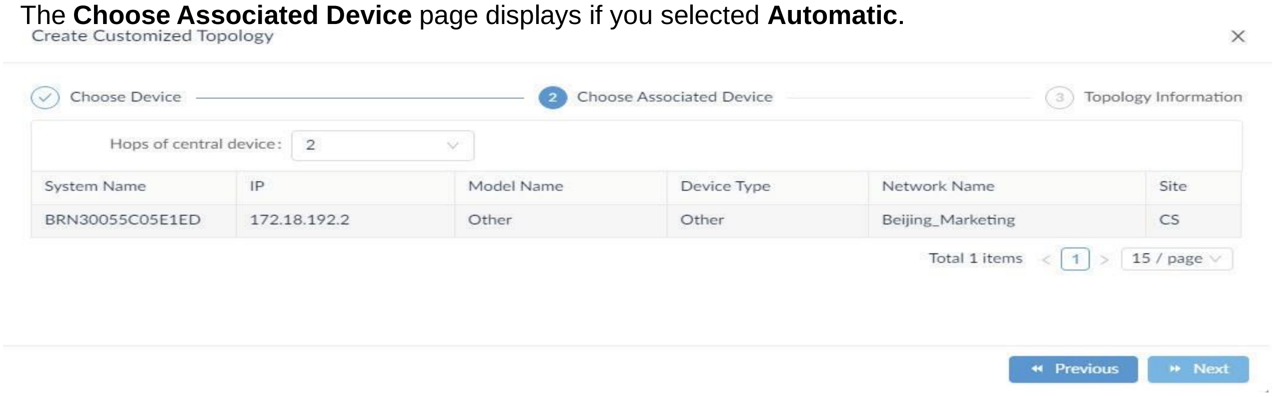
   Automatic (default): select a device and set the number of hops to generate the topology.

   Manual: generate a topology for the selected devices.

5. For manual, select device(s) to be included in the topology architecture. Or you can search for specific device(s) by entering a keyword in the search field.

6. Click **Next** to proceed.

The **Choose Associated Device** page displays if you selected **Automatic**.



Hops of central device: 2

System Name	IP	Model Name	Device Type	Network Name	Site
BRN30055C05E1ED	172.18.192.2	Other	Other	Beijing_Marketing	CS

7. Click the **Hops of central device** drop-down menu to define the number of hops or devices (2 to 10) of a single link from the central device down to add additional devices in the diagram. This is only available if the Automatic method is selected above.

8. Click **Nex**t to continue or click **Previous** to return to the previous menu.The **Topology Information** page displays.

9. In the Name field, enter a name for the topology map.

10. In the Description field, enter a description to identify the map.

11. In **Data source of links**, select either **Synchronization with system** or **User-defined** to specify whether the data will be dynamically updated with the system. The user-defined type will not update dynamically with the system when there is any topological change with the nodes and links in the system.

12. Select the type of layout for the map: Star, Tree, Circular, or Grid.

13. Enable or disable sharing of the topology with other administrators so they may also view or modify it.

14. Enable or disable the **Auto** button to control the selection mode of the central device for display as the central device in the topology. ON indicates the system will specify the central device automatically. (The system will select the device having the greatest number of links as the central device.) If OFF is selected, choose a central device manually.

15. Select a central device if you disable the above Auto option.

16. Click **Save** to create the topology map. Click **Previous** to return to the previous menu.

You can modify the information of a customized topology or delete a customized topology. Click **Select Topology** at the upper left, select **Customized Topology**, select the desired topology, then click **Edit** ✎ or **Delete** 🗑.

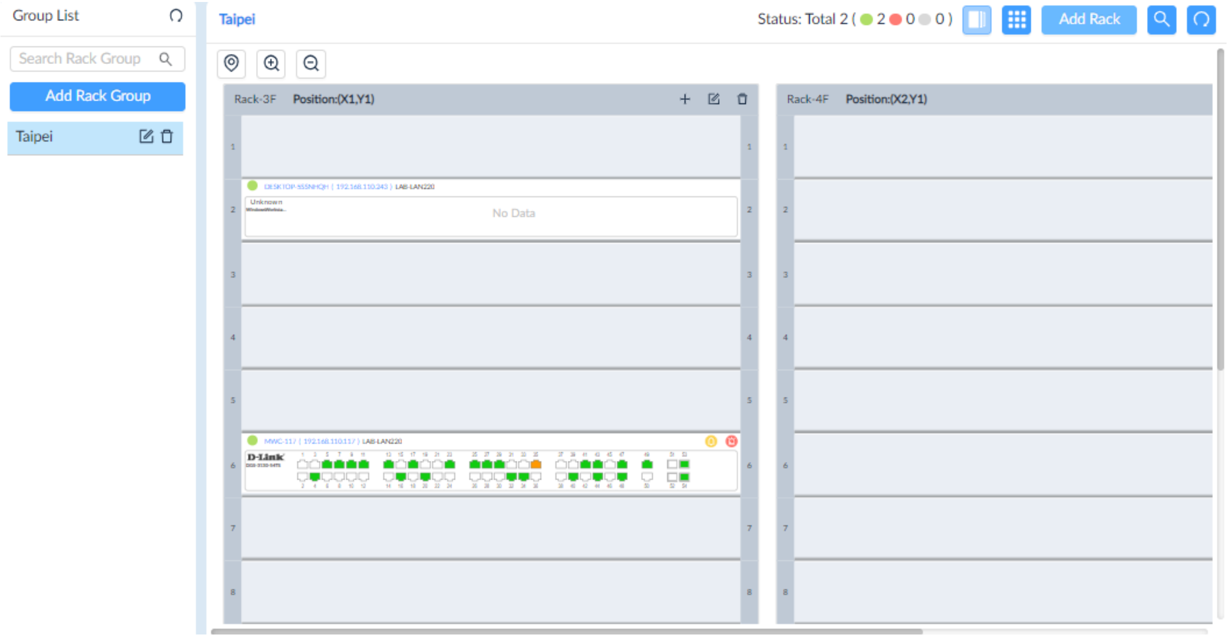
9 Rack Groups and Devices

In heterogeneous networks with lots of different types of devices, organizing device placement is essential and may take a lot of time. This Rack View function assists in viewing and managing such placement at the deployment site.

9.1. Add a Rack Group

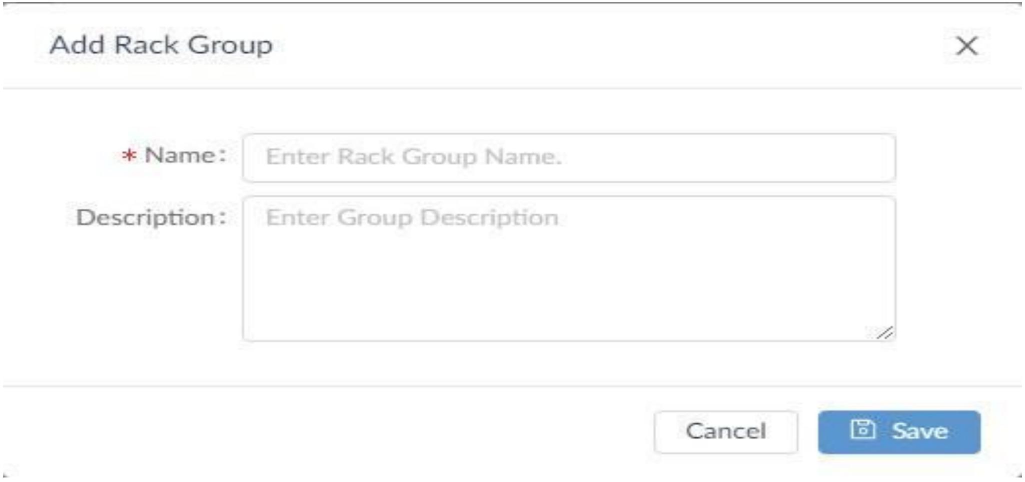
Racks are organized by groups. Creating a rack group is required for the subsequent rack and device management.

1. Go to **Monitoring > Rack View** to display the Group List page.

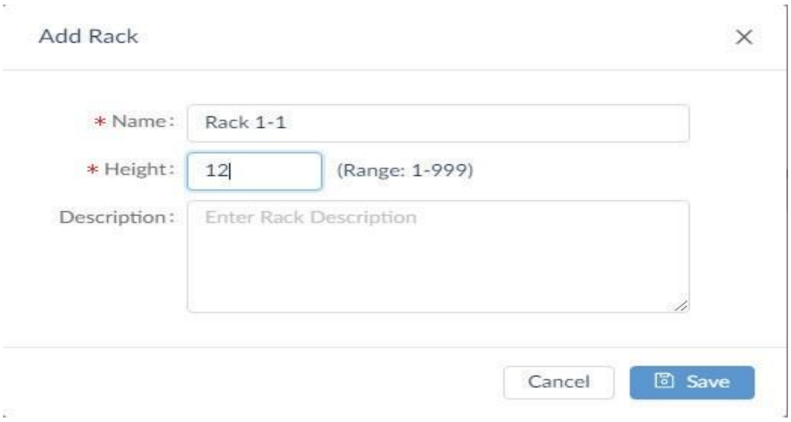


2. Click **Add Rack Group**.

   The Add Rack Group page displays.



3. Enter a name and description for the group.
4. Click **Save** to create the group. Or click **Cancel** to return to the previous screen.
5. The group rack page appears. Click **Add Rack** to add more racks to the group.The **Add Rack** page displays.



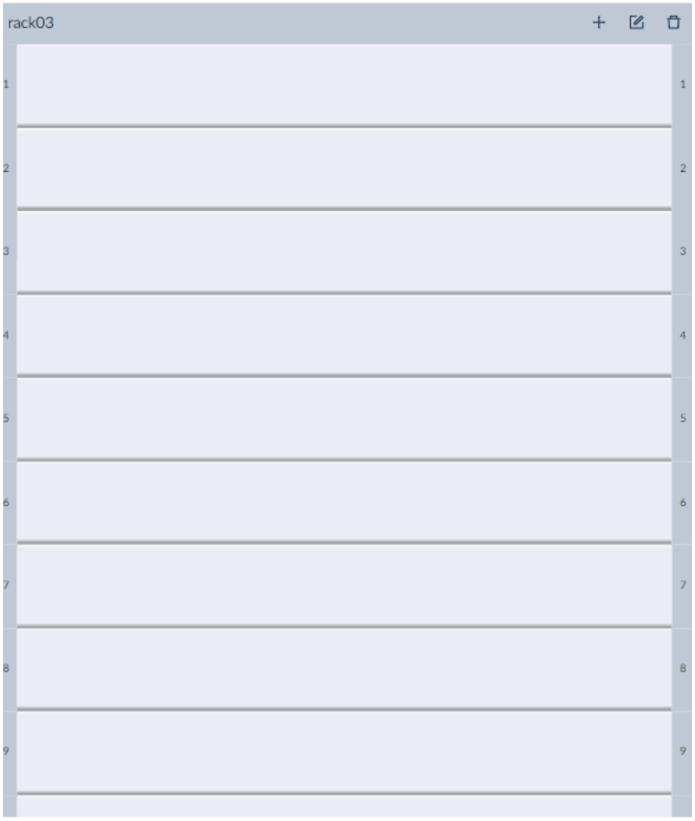
Add Rack

* Name: Rack 1-1

* Height: 12 (Range: 1-999)

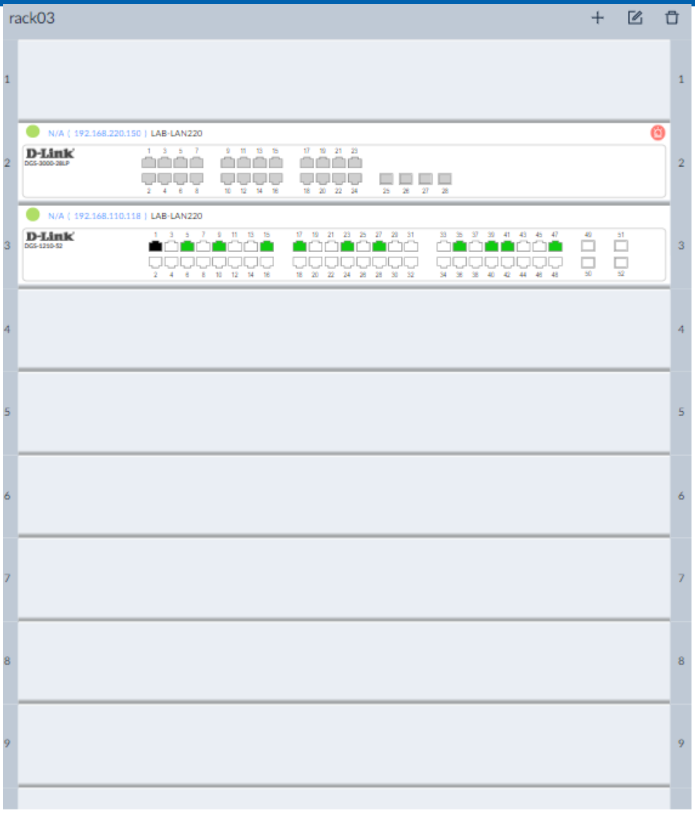
Description: Enter Rack Description

6. Enter a name to identify this new rack display.
7. Enter the units, a unit of 1 equals 1 device slot space (range: 1 to 999).
8. Enter a description to better identify the rack.
9. Click **Save** to create the rack or click **Cancel** to return to the previous menu.The **Create Rack** page displays.



10. Click on a slot to add a device.The Available Devices page displays.
11. Select a device to insert into the slot.
12. Click **Save**.

The selected device is now inserted into the rack location.


rack03
N/A (192.168.220.150 | LAB-LAN220
D-Link
DGS-3000-28LP
N/A (192.168.110.118 | LAB-LAN220
D-Link
DGS-1210-52
1
2
3
4
5
6
7
8
9

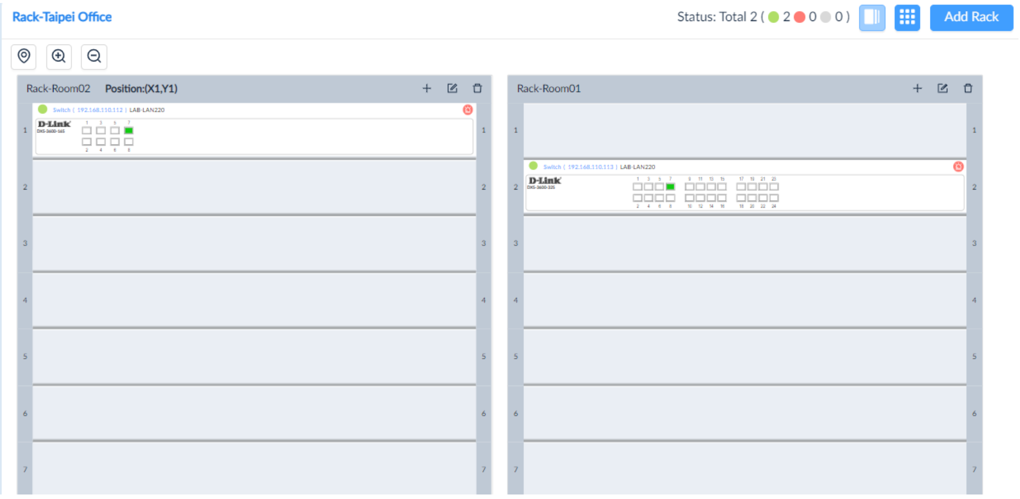
The Rack Group page also offers controls for different views of the rack display:

To adjust the level of the detail on the rack group page:

- Default: click to set the viewing ratio to default
- Zoom in: click to zoom in the viewing area
- Zoom out: click to zoom out the viewing area
- Arrange the racks of a rack group on the group page

To arrange the racks of a rack group on the group page:

Click and hold anywhere on a rack and drag it to a new location.

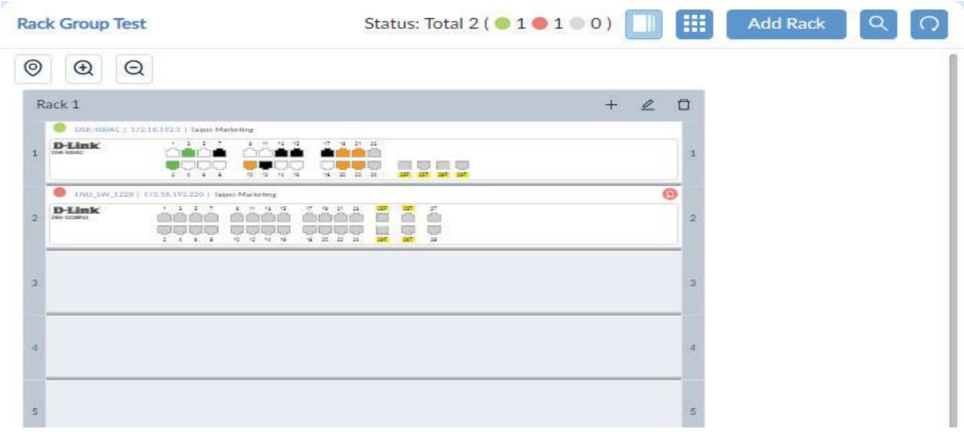

Rack-Taipei Office
Status: Total 2 (2 0 0)
Add Rack
Rack-Room02
Position:(X1,Y1)
Switch (192.168.110.112 | LAB-LAN220
D-Link
Rack-Room01
Switch (192.168.110.113 | LAB-LAN220
D-Link
1
2
3
4
5
6
7

9.2. View and Modify a Rack Group

You can modify and delete existing rack groups.

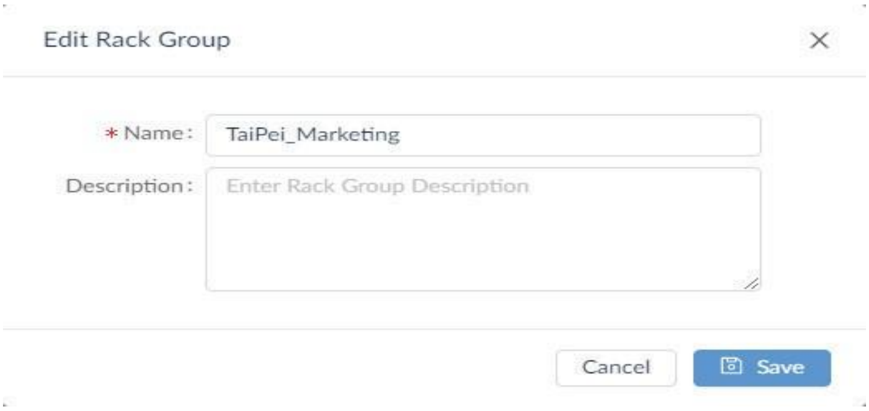
To modify an existing rack group:

1. Go to **Monitoring > Rack View**.
2. The Group List page displays.
3. Select a rack group.



4. To edit the group settings, click **Edit** ✎ in the Group List column.

   The Edit Rack Group page displays.



Edit Rack Group

* Name: TaiPei_Marketing

Description: Enter Rack Group Description

5. To delete the group, click on the **Delete** button in the Group List column. A confirmation pop-up displays.
6. Click **Yes** to confirm.

NOTE: Deleting a rack group will delete all racks in the rack group at the same time.

Likewise, you can modify the racks of a rack group. Refer to the below section.

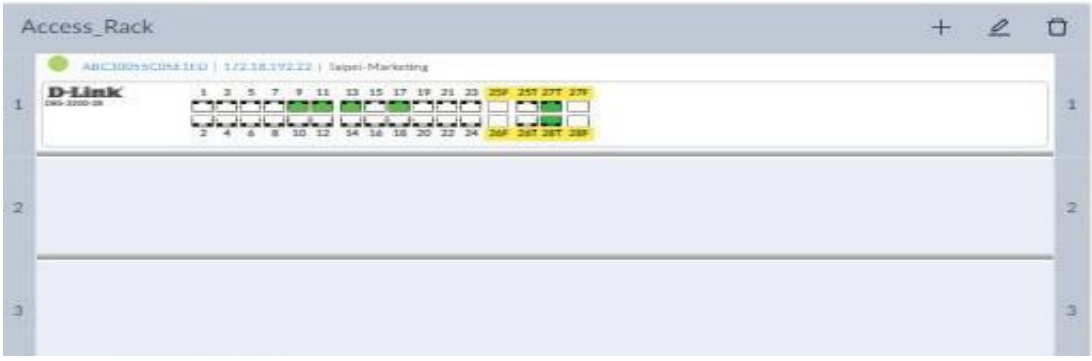
View and Modify a Rack

You can modify and delete an existing rack(s) from a group.

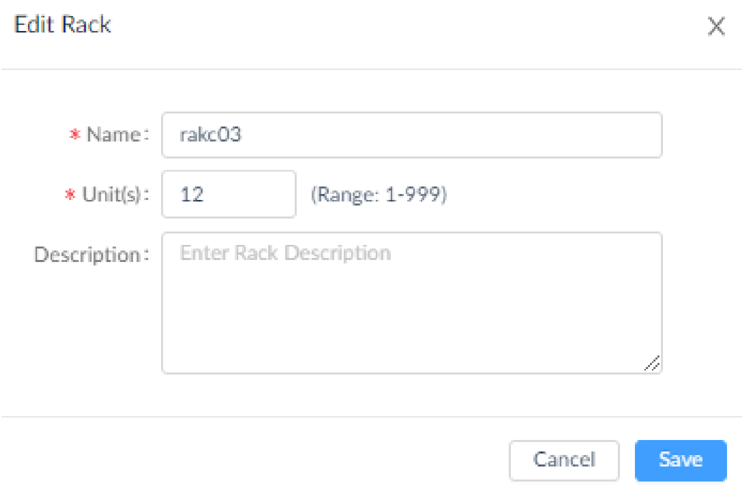
To modify an existing rack:

1. Go to **Monitoring > Rack View** to display the Group List page. Select an existing group to view the racks of the group.

2. At the top right of a rack display, click **Edit Rack** to modify the rack information.



The Edit Rack page displays:



Edit Rack ×

* Name: rakc03

* Unit(s): 12 (Range: 1-999)

Description: Enter Rack Description

Cancel | Save

3. Click **Save** to accept the new information.

You can also click **Delete** to remove the rack from the group. A confirmation pop-up displays.

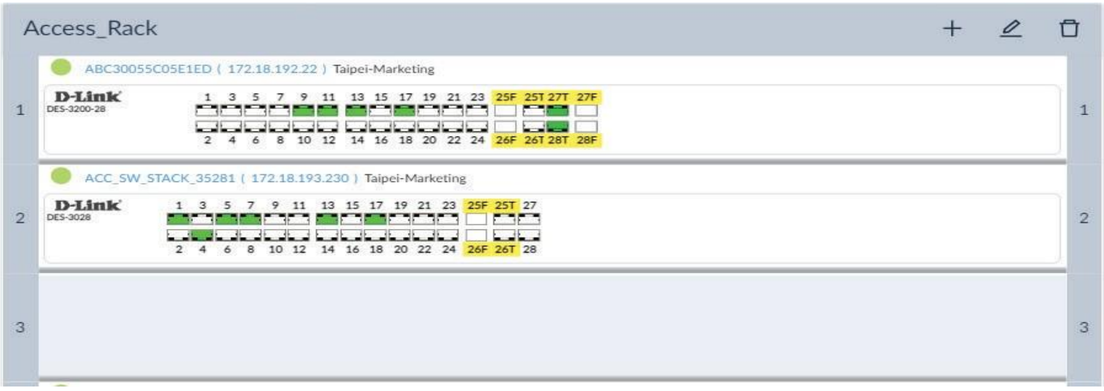
Click **Yes** to confirm the deletion.

NOTE: Deleting a rack will delete all devices in the rack at the same time.

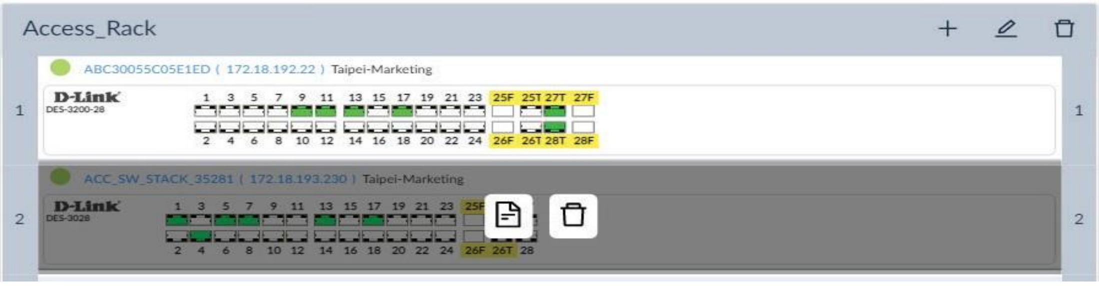
Place a Device on a Rack

You can view and change the location of a device on a rack simply by dragging and dropping it to a new slot on the rack. To view an existing device:

1. Go to **Monitoring > Rack View** to display the Group List page.
2. Select an existing group to view the racks of the group.

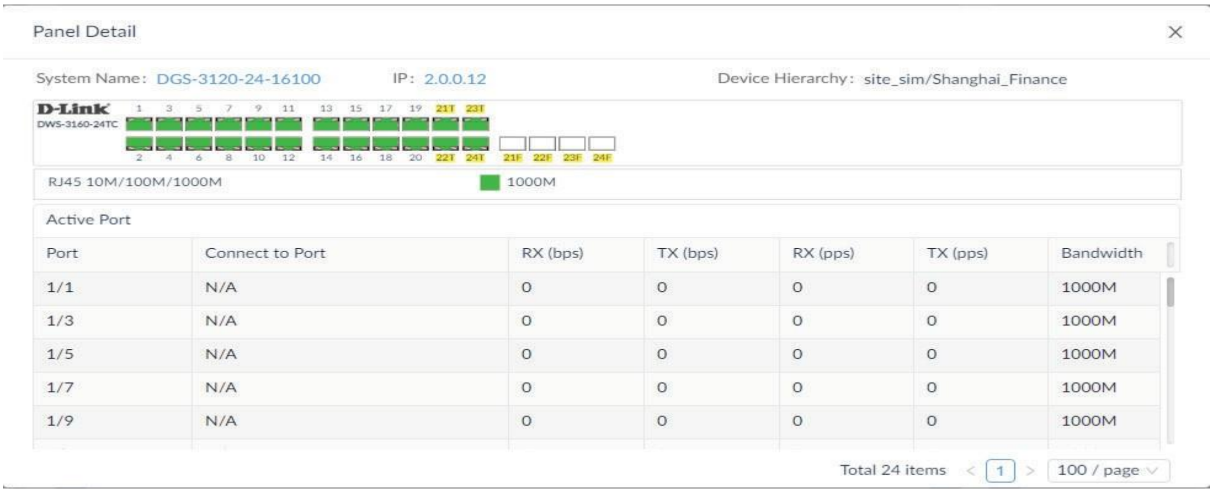

Access_Rack
ABC30055C05E1ED (172.18.192.22) Taipei-Marketing
D-Link
DES-3200-28
ACC_SW_STACK_35281 (172.18.193.230) Taipei-Marketing
D-Link
DES-3028
1
2
3

3. From the rack view, click on a device. The View and Delete icons appear.


Access_Rack
ABC30055C05E1ED (172.18.192.22) Taipei-Marketing
D-Link
DES-3200-28
ACC_SW_STACK_35281 (172.18.193.230) Taipei-Marketing
D-Link
DES-3028
1
2

4. Click **View** to display the device **Panel Detail** page.

The following is an example of a D-Link DGS-3120 device.



Panel Detail

System Name: DGS-3120-24-16100   IP: 2.0.0.12   Device Hierarchy: site_sim/Shanghai_Finance

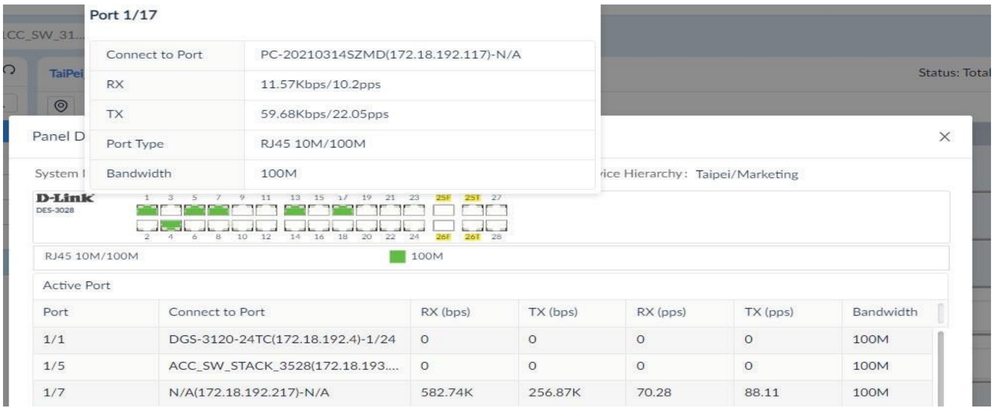
RJ45 10M/100M/1000M   🟩 1000M

Active Port

Port	Connect to Port	RX (bps)	TX (bps)	RX (pps)	TX (pps)	Bandwidth
1/1	N/A	0	0	0	0	1000M
1/3	N/A	0	0	0	0	1000M
1/5	N/A	0	0	0	0	1000M
1/7	N/A	0	0	0	0	1000M
1/9	N/A	0	0	0	0	1000M

Total 24 items < 1 > 100 / page

5. Mouse over any of the connected (green) ports to view port details.



Port 1/17

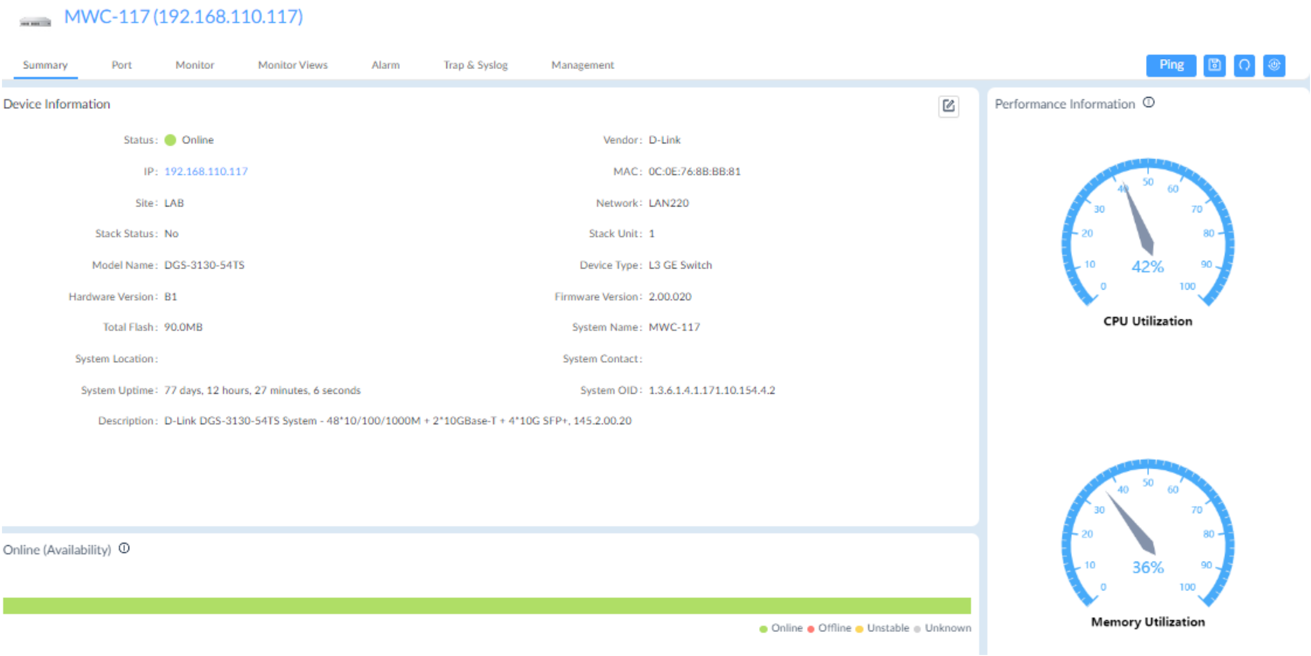
Connect to Port	PC-20210314SZMD(172.18.192.117)-N/A
RX	11.57Kbps/10.2pps
TX	59.68Kbps/22.05pps
Port Type	RJ45 10M/100M
Bandwidth	100M

Active Port

Port	Connect to Port	RX (bps)	TX (bps)	RX (pps)	TX (pps)	Bandwidth
1/1	DGS-3120-24TC(172.18.192.4)-1/24	0	0	0	0	100M
1/5	ACC_SW_STACK_3528(172.18.193....	0	0	0	0	100M
1/7	N/A(172.18.192.217)-N/A	582.74K	256.87K	70.28	88.11	100M

6. Click on the **IP address** to open the device management interface through one of the following protocols: HTTP, HTTPS, Telnet, or SSH.

7. Click on the **System Name** to open the device's information page.



MWC-117 (192.168.110.117)

Device Information

Status:	● Online	Vendor:	D-Link
IP:	192.168.110.117	MAC:	0C:0E:76:8B:BB:81
Site:	LAB	Network:	LAN220
Stack Status:	No	Stack Unit:	1
Model Name:	DGS-3130-54TS	Device Type:	L3 GE Switch
Hardware Version:	B1	Firmware Version:	2.00.020
Total Flash:	90.0MB	System Name:	MWC-117
System Location:		System Contact:	
System Uptime:	77 days, 12 hours, 27 minutes, 6 seconds	System OID:	1.3.6.1.4.1.171.10.154.4.2
Description:	D-Link DGS-3130-54TS System - 48*10/100/1000M + 2*10GBase-T + 4*10G SFP+, 145.2.00.20		

For more information on the Device Information page, refer to 4.2.2 Modify Device Information.

10 sFlow Monitoring

sFlow is only supported in the Enterprise version. The sFlow monitoring technology is designed for high-speed switched networks to aid in network usage visibility. The sFlow agent sends data to D-View 8 and it enables network administrators to monitor and analyze traffic effectively in the following areas:

- Detailed real-time bandwidth usage with respect to applications, protocols, and source and destination addresses
- Traffic flow for all ports
- Issues and abnormal traffic
- Traffic identified as a potential security threat
- Performance optimization information
- Billing and accounting

The sFlow function provides continuous monitoring as well as network performance reporting.

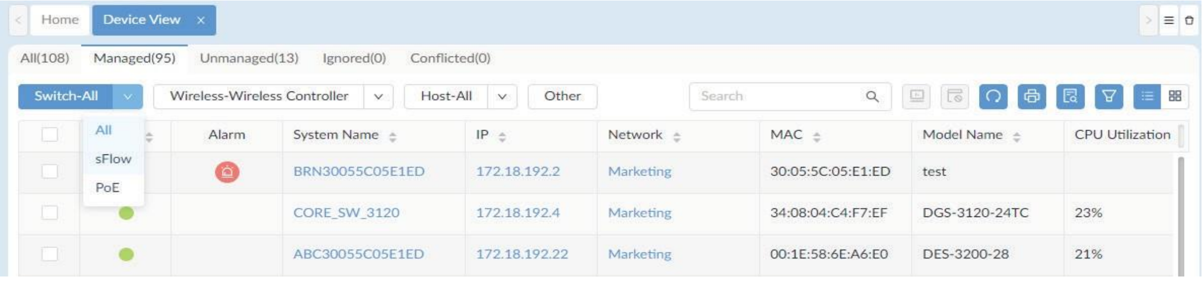
This section includes the following functions for sFlow management:

- Configure sFlow Monitor
- Manage sFlow Monitor
- View and Export sFlow Monitoring Results
- Configure sFlow in Supported Devices

10.1. Configure sFlow Monitor

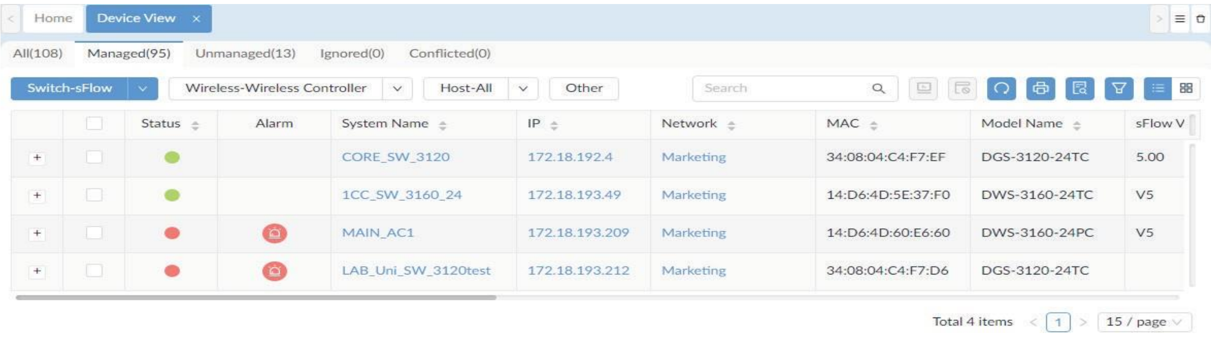
To configure the sFlow Monitor on an sFlow-enabled device:

1. Go to **Monitoring > Device View**. In the Device View page, click the **Managed** tab and select sFlow from the Switch-All drop-down menu.



□		Alarm	System Name	IP	Network	MAC	Model Name	CPU Utilization
□		🔔	BRN30055C05E1ED	172.18.192.2	Marketing	30:05:5C:05:E1:ED	test	
□	●		CORE_SW_3120	172.18.192.4	Marketing	34:08:04:C4:F7:EF	DGS-3120-24TC	23%
□	●		ABC30055C05E1ED	172.18.192.22	Marketing	00:1E:58:6E:A6:E0	DES-3200-28	21%

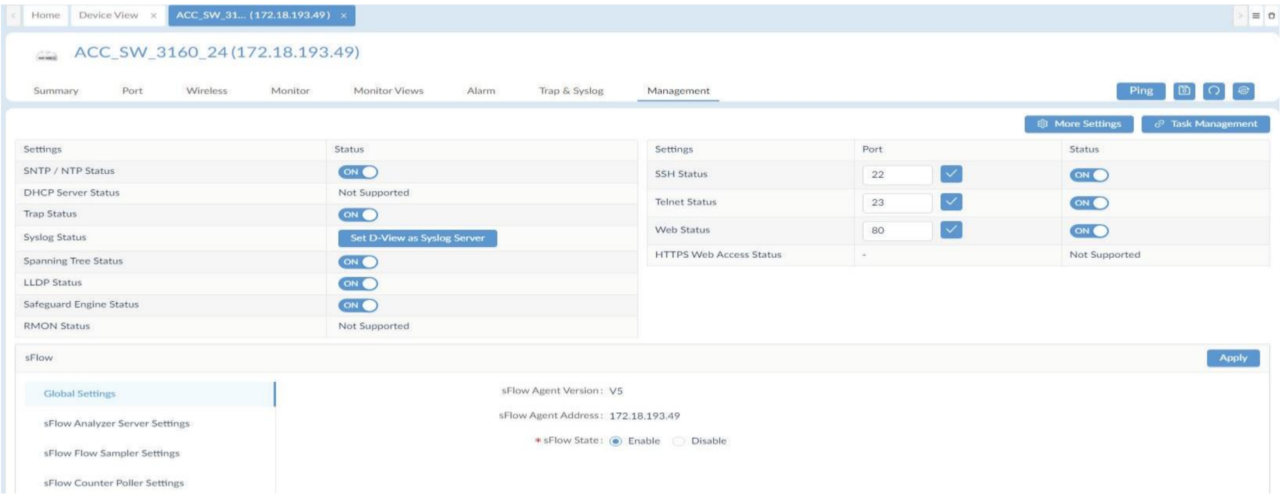
The Switch-sFlow devices table displays.



	□	Status	Alarm	System Name	IP	Network	MAC	Model Name	sFlow V
+	□	●		CORE_SW_3120	172.18.192.4	Marketing	34:08:04:C4:F7:EF	DGS-3120-24TC	5.00
+	□	●		1CC_SW_3160_24	172.18.193.49	Marketing	14:D6:4D:5E:37:F0	DWS-3160-24TC	V5
+	□	●	🔔	MAIN_AC1	172.18.193.209	Marketing	14:D6:4D:60:E6:60	DWS-3160-24PC	V5
+	□	●	🔔	LAB_Uni_SW_3120test	172.18.193.212	Marketing	34:08:04:C4:F7:D6	DGS-3120-24TC	

Total 4 items < 1 > 15 / page

2. Select a desired device by clicking on the System Name link. The Device Information page displays. Click the **Management** tab to view the device's sFlow settings.



ACC_SW_3160_24 (172.18.193.49)

Settings	Status
SNTP / NTP Status	ON
DHCP Server Status	Not Supported
Trap Status	ON
Syslog Status	Set D-View as Syslog Server
Spanning Tree Status	ON
LLDP Status	ON
Safeguard Engine Status	ON
RMON Status	Not Supported

Settings	Port	Status
SSH Status	22	ON
Telnet Status	23	ON
Web Status	80	ON
HTTPS Web Access Status	-	Not Supported

sFlow

Global Settings

sFlow Analyzer Server Settings

sFlow Flow Sampler Settings

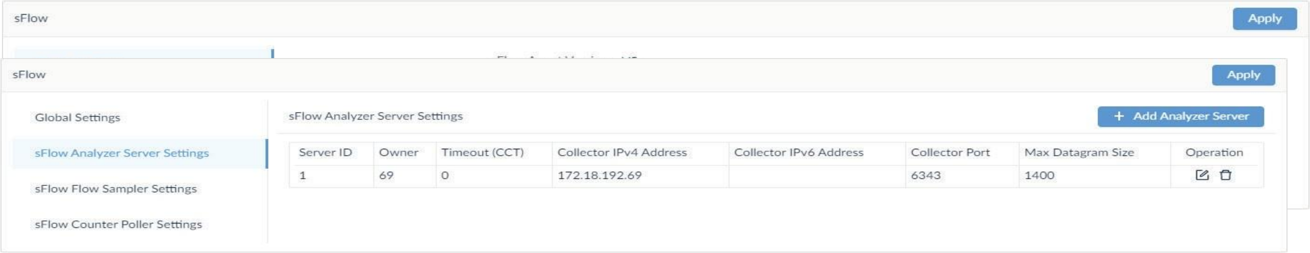
sFlow Counter Poller Settings

sFlow Agent Version: V5

sFlow Agent Address: 172.18.193.49

* sFlow State: ● Enable ○ Disable

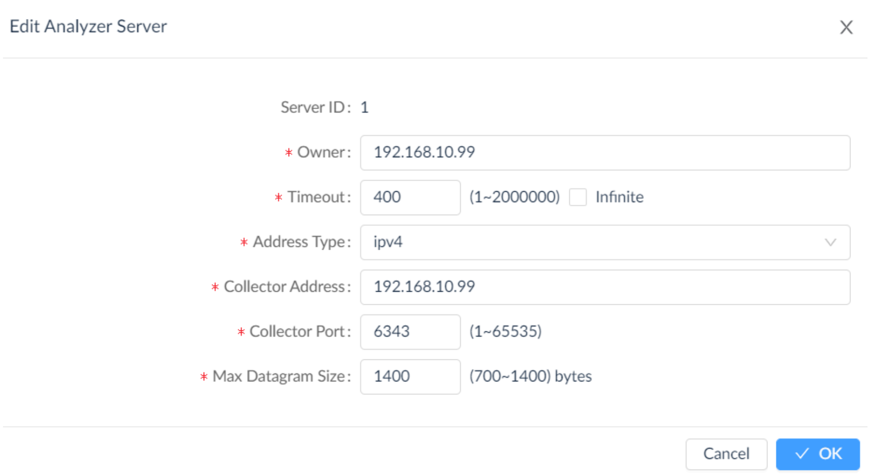
3. In the sFlow section, select the **Global Settings** tab.
4. Find the sFlow State control and select **Enable** to set the sFlow function.


sFlow
Apply
sFlow
Apply
Global Settings
sFlow Analyzer Server Settings
sFlow Flow Sampler Settings
sFlow Counter Poller Settings
+ Add Analyzer Server

sFlow Analyzer Server Settings

Server ID	Owner	Timeout (CCT)	Collector IPv4 Address	Collector IPv6 Address	Collector Port	Max Datagram Size	Operation
1	69	0	172.18.192.69		6343	1400	

5. In the sFlow section, click **sFlow Analyzer Server Settings**. The sFlow Analyzer Server Settings are displayed in the window.



Edit Analyzer Server

Server ID: 1

* Owner: 192.168.10.99

* Timeout: 400 (1~2000000) □ Infinite

* Address Type: ipv4

* Collector Address: 192.168.10.99

* Collector Port: 6343 (1~65535)

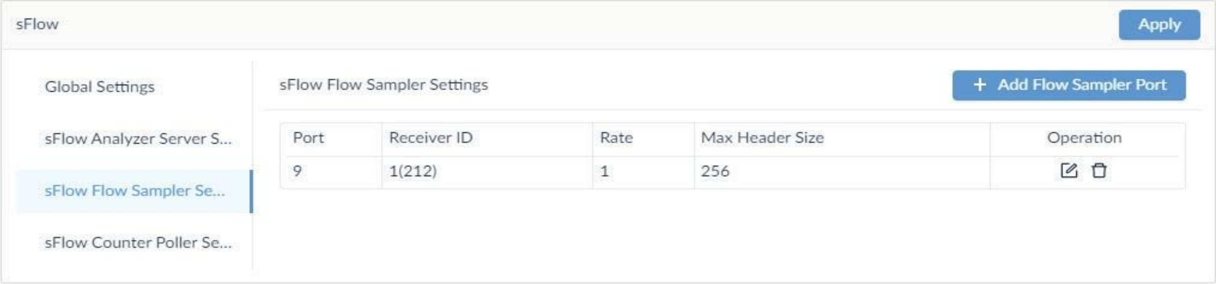
* Max Datagram Size: 1400 (700~1400) bytes

6. Click **+Add Analyzer Server** to display the Add Analyzer Server page.

Item	**Description**
Server ID	Click the indicator to assign an ID to the entry (1 – 4).
Owner	Enter the analyzer name for the device to send the sFlow data to. In general, this setting points to the D-View 8 probe server.
Timeout	Enter the collector timeout (1 ~ 2000000) value that will keep the collector settings valid. Alternatively, click **Infinite** to disable the timeout setting.
Address Type	Click the drop-down menu to define the IPv4 or IPv6 address type.
Collector IPv4/IPv6 Address	Enter the collector IP address for data collection. In general, this setting points to the D-View 8 probe server IP address.
Collector Port	Enter the port number of the above collector address (1-65535).

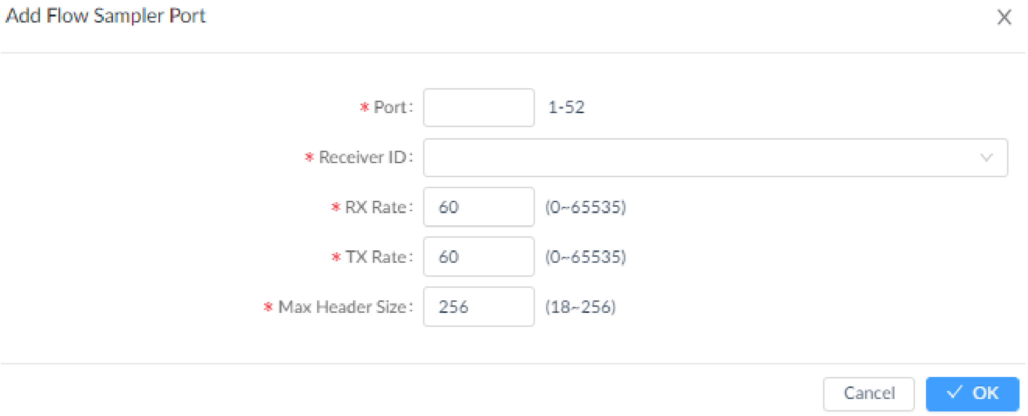
Max Datagram Size	Enter the maximum datagram size for the data packet in bytes (300 – 1400).
Cancel	Click **Cancel** to return to the previous menu without saving the settings.
OK	Click **OK** to create the sFlow setting.

7. Click **sFlow Flow Sampler Settings** to configure the flow packet sampling method.
8. Click **+Add Flow Sampler Port**. The Add Flow Sampler Port page displays.


sFlow
Apply
Global Settings
sFlow Analyzer Server S...
sFlow Flow Sampler Se...
sFlow Counter Poller Se...
sFlow Flow Sampler Settings
+ Add Flow Sampler Port

Port	Receiver ID	Rate	Max Header Size	Operation
9	1(212)	1	256	

9. Enter the following information.



* Port: 1-52

* Receiver ID:

* RX Rate: 60 (0~65535)

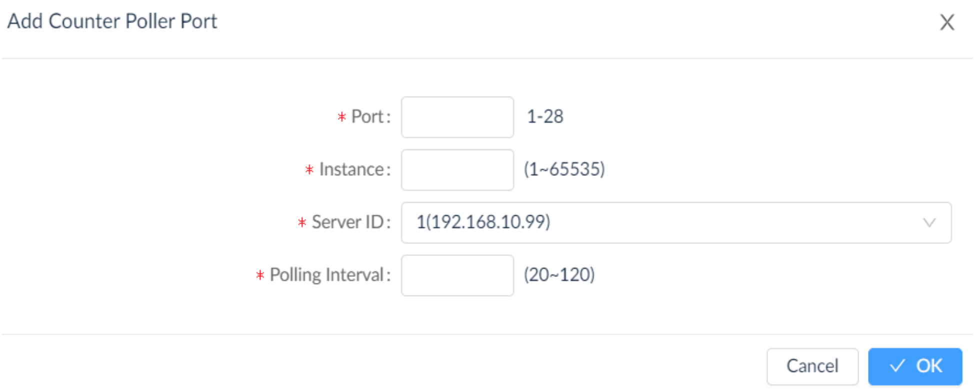
* TX Rate: 60 (0~65535)

* Max Header Size: 256 (18~256)

Item	Description
Port	Enter the port number on the device designated to send out sFlow data.
Instance	Enter an instance number for each sampling port.
Receiver ID	Click the drop-down menu to select a pre-configured analyzer server, see the previous step.
Mode	Select either inbound or outbound traffic.
Rate (RX/TX)	Enter the sampling rate (0-65536).
Max Header Size	Enter the maximum number of bytes (18- 256) to be copied from a sampled packet to an sFlow datagram.
Cancel	Click Cancel to return to the previous menu without saving the settings.
OK	Click OK to create sampler setting.

Note: The settings vary depending on the sFlow support capabilities. Even if the settings relevant for sFlow communication can be configured from the D-View application, sFlow Analyzer is only supported in the Enterprise version (refer to 10.3 Configure sFlow in Supported Devices for instructions about sFlow Analyzer.)

10. Click **sFlow Counter Poller** Settings to configure the counter sampling method.
11. Click **+Add Counter Poller Port** at the upper right. The **Add Counter Poller Port** page displays.



Add Counter Poller Port

* Port: 1-28

* Instance: (1~65535)

* Server ID: 1(192.168.10.99)

* Polling Interval: (20~120)

Enter the following information:

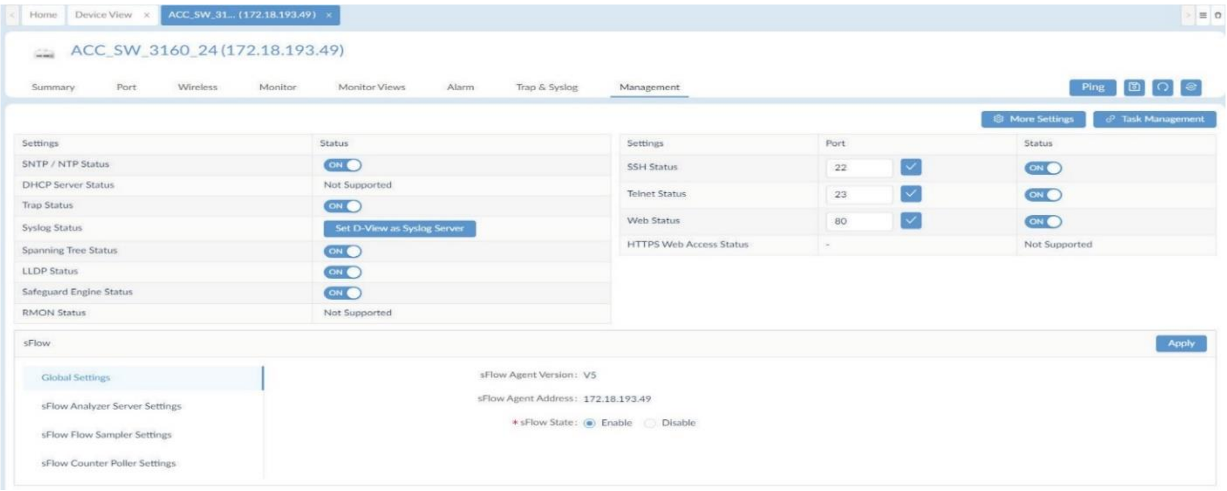
Item	Description
Port	Enter the port number on the device designated to send counter samples
Polling Interval	Click to set the interval for counter polling (0~120) for the time interval between counter poller samples.
Server ID	Click the drop-down menu to select a pre-configured analyzer server, see the previous step.
Cancel	Click **Cancel** to return to the previous menu without saving the settings.
OK	Click **OK** to create the counter poller port setting.

12. Click **Apply** at the upper right in the sFlow section to accept the new sFlow configuration.

10.2. Manage sFlow Monitor

To configure the sFlow Monitor settings:

1. Click **Monitoring** > **Device View**.
2. Click the **Managed** tab and select sFlow from the Switch-All drop-down menu.The Switch-sFlow devices table displays.
3. Select the target device by clicking the System Name. The Device Information page displays.
4. Click the **Management** tab to view the device’s sFlow settings.


Home
Device View ×
ACC_SW_31... (172.18.193.49) ×
ACC_SW_3160_24 (172.18.193.49)
Summary
Port
Wireless
Monitor
Monitor Views
Alarm
Trap & Syslog
Management
Ping
More Settings
Task Management
sFlow
Apply
Global Settings
sFlow Analyzer Server Settings
sFlow Flow Sampler Settings
sFlow Counter Poller Settings

Settings	Status
SNTP / NTP Status	ON
DHCP Server Status	Not Supported
Trap Status	ON
Syslog Status	Set D-View as Syslog Server
Spanning Tree Status	ON
LLDP Status	ON
Safeguard Engine Status	ON
RMON Status	Not Supported

Settings	Port	Status
SSH Status	22 ✓	ON
Telnet Status	23 ✓	ON
Web Status	80 ✓	ON
HTTPS Web Access Status	-	Not Supported

sFlow Agent Version : V5
sFlow Agent Address : 172.18.193.49
* sFlow State : ● Enable ○ Disable

5. Under the sFlow section, configured analyzer servers are listed. For each configured server, you can perform the following:

   Edit: allows you to modify the existing settings.
   Delete: removes the entry from the list.

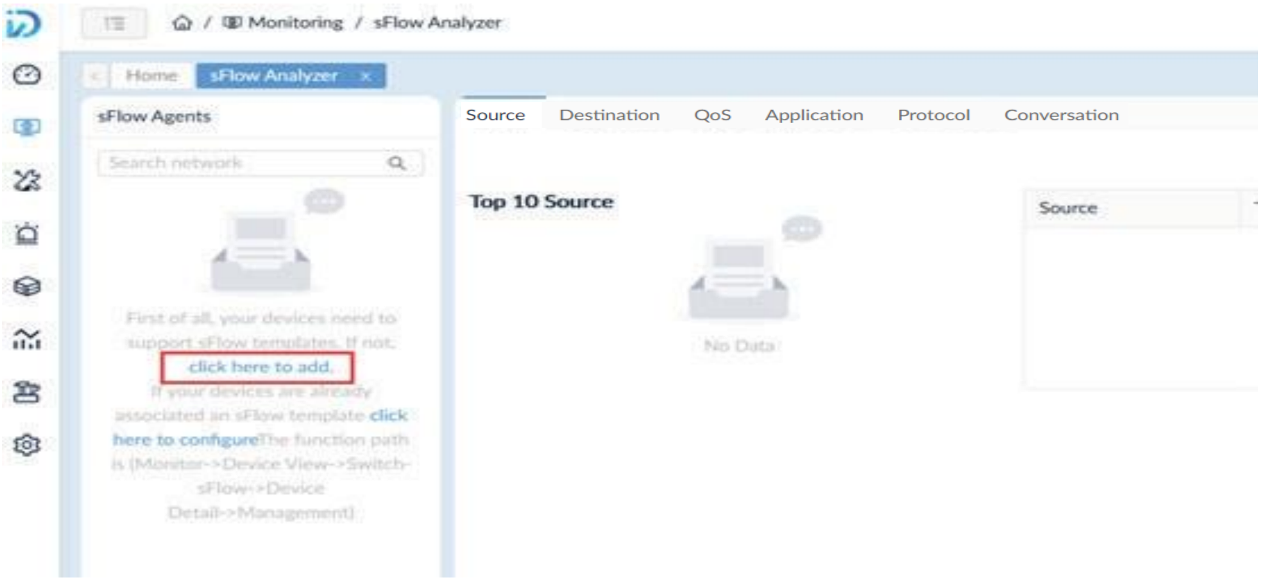
The sFlow Flow Sampler Settings and Counter Poller Settings can also be configured by clicking the respective tab.

10.3. Configure sFlow in Supported Devices

D-View 8 makes it easy for you to configure and manage devices that support sFlow. Note that sFlow Analyzer is only supported in Enterprise version.

To configure sFlow using sFlow Analyzer wizard:

1. Go to **Monitoring > sFlow Analyzer**. The sFlow Analyzer overview displays.

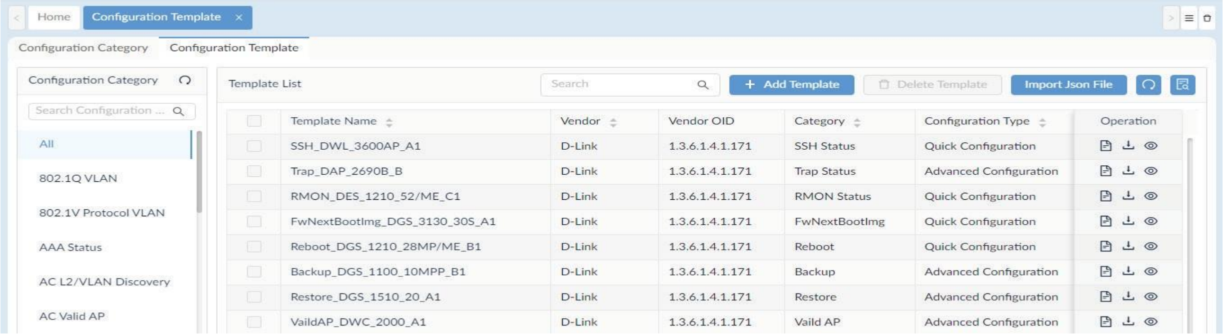


First of all, your devices need to support sFlow templates. If not, click here to add. If your devices are already associated an sFlow template click here to configureThe function path is (Monitor->Device View->Switch-sFlow->Device Detail->Management)

2. In the left pane, click the **Click Here to Add** link to add and configure a device for sFlow.

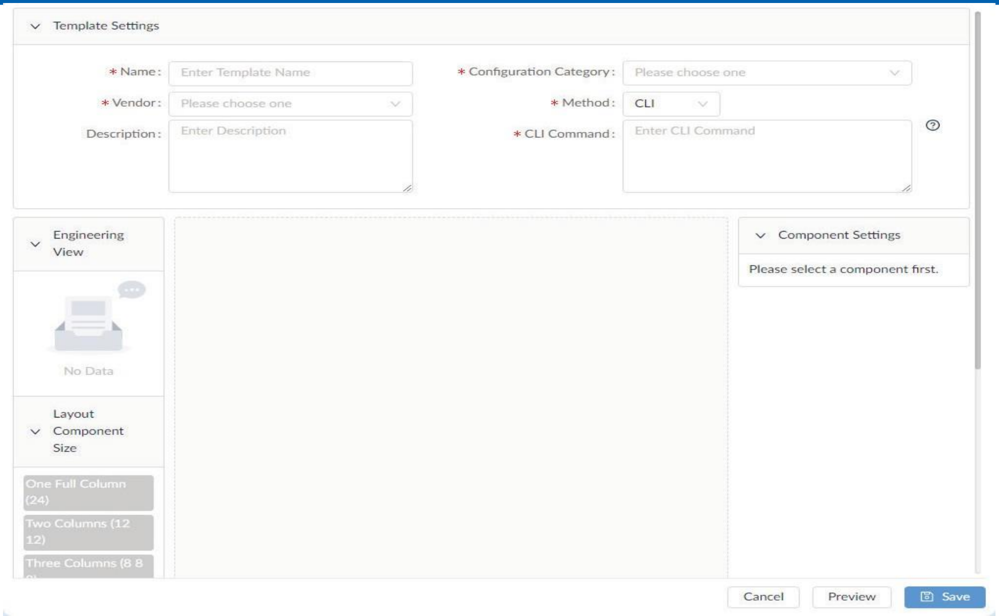
To configure sFlow using templates:

1. Go to the **Templates > Configuration Template**. Then click the **Configuration Template** tab.



□	Template Name	Vendor	Vendor OID	Category	Configuration Type	Operation
□	SSH_DWL_3600AP_A1	D-Link	1.3.6.1.4.1.171	SSH Status	Quick Configuration	
□	Trap_DAP_2690B_B	D-Link	1.3.6.1.4.1.171	Trap Status	Advanced Configuration	
□	RMON_DES_1210_52/ME_C1	D-Link	1.3.6.1.4.1.171	RMON Status	Quick Configuration	
□	FwNextBootImg_DGS_3130_30S_A1	D-Link	1.3.6.1.4.1.171	FwNextBootImg	Quick Configuration	
□	Reboot_DGS_1210_28MP/ME_B1	D-Link	1.3.6.1.4.1.171	Reboot	Quick Configuration	
□	Backup_DGS_1100_10MPP_B1	D-Link	1.3.6.1.4.1.171	Backup	Advanced Configuration	
□	Restore_DGS_1510_20_A1	D-Link	1.3.6.1.4.1.171	Restore	Advanced Configuration	
□	VaildAP_DWC_2000_A1	D-Link	1.3.6.1.4.1.171	Vaild AP	Advanced Configuration	

2. Click the **sFlow** category and click **+Add Template** at the upper right. The Template Settings page displays.



Template Settings

* Name: Enter Template Name

* Configuration Category: Please choose one

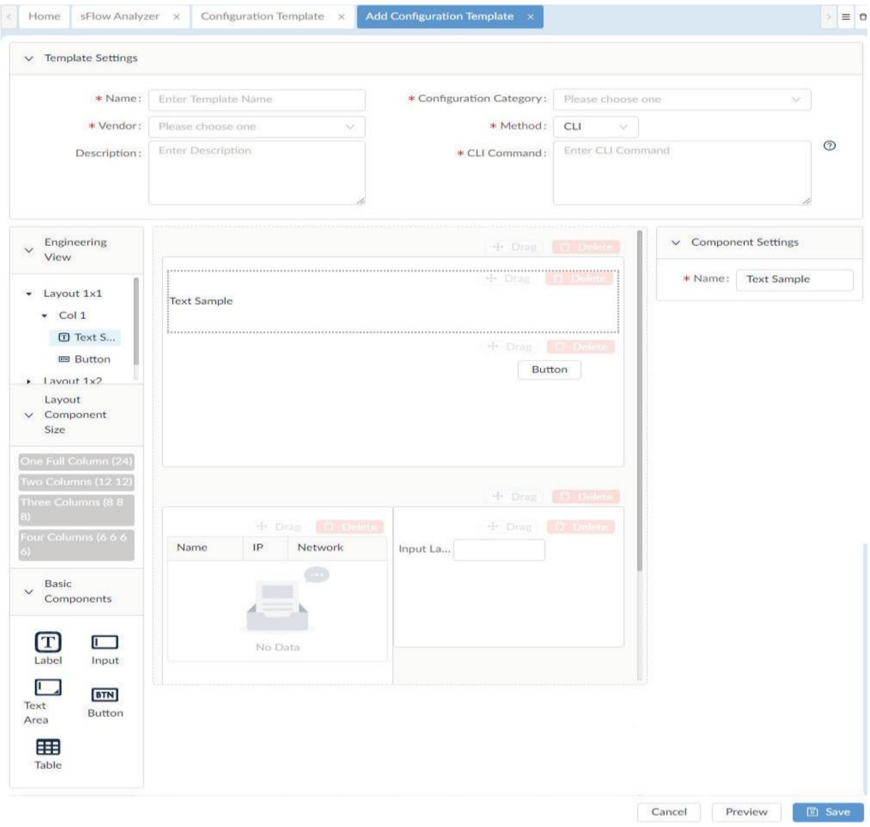
* Vendor: Please choose one

* Method: CLI

Description: Enter Description

* CLI Command: Enter CLI Command

From the template settings, you can configure a template to include features such as device layout and basic components such as labels, input fields, buttons, radio buttons, text areas, toggle switches and tables for configuration input control.



Template Settings

* Name: Enter Template Name

* Configuration Category: Please choose one

* Vendor: Please choose one

* Method: CLI

Description: Enter Description

* CLI Command: Enter CLI Command

Component Settings

* Name: Text Sample

Click **Cancel** to discard the changes and **Save** to add the template to the library. You can click **Preview** to view the configuration menu layout.

Once the sFlow configuration template is created, you need to associate it to a related device template to con figure the sFlow parameters (Go to **Templates > Device Template**). Refer to the below 11.1 Generate Device Template.

10.4. sFlow Network Monitor

sFlow (sampled flow) utilizes packet sampling to monitor switched networks to provide data for network usage and performance monitoring. Note that sFlow Analyzer is only supported in Enterprise version.

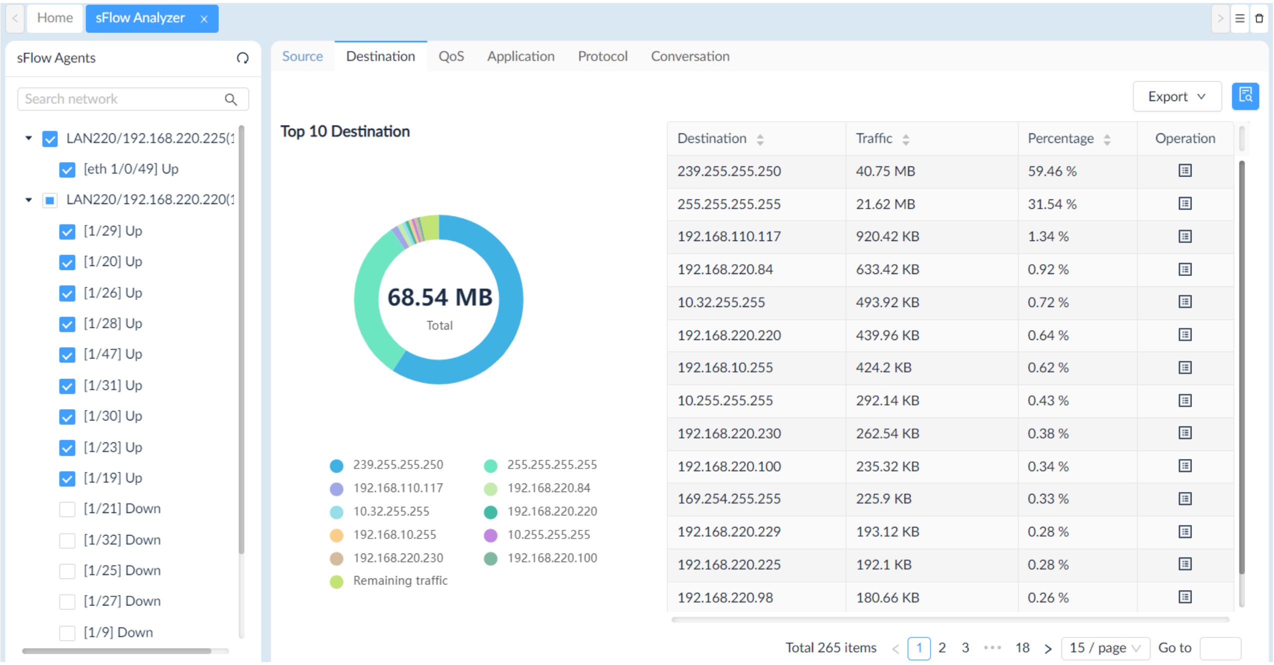
Once configured, the sFlow function will start monitoring and analyzing the network from the collected data using packet sampling or counter sampling.

To configure or view the sFlow monitoring:

1. Go to **Monitoring > sFlow Analyzer**.
2. The supported devices with configured port of the sampled packets will be displayed in the left pane. If there are no available data sources, you need to configure sFlow and enable sFlow sampling on the supported devices first. Refer to 10.1 Configure sFlow Monitor and 10.3 Configure sFlow in Supported Devices.

The sFlow Analyzer overview displays. Click a tab to view the related sFlow statistics in one of the following categories:

- Source
- Destination
- QoS
- Application
- Protocol
- Conversation



☑ LAN220/192.168.220.225(1
☑ [eth 1/0/49] Up
■ LAN220/192.168.220.220(1
☑ [1/29] Up
☑ [1/20] Up
☑ [1/26] Up
☑ [1/28] Up
☑ [1/47] Up
☑ [1/31] Up
☑ [1/30] Up
☑ [1/23] Up
☑ [1/19] Up
□ [1/21] Down
□ [1/32] Down
□ [1/25] Down
□ [1/27] Down
□ [1/9] Down

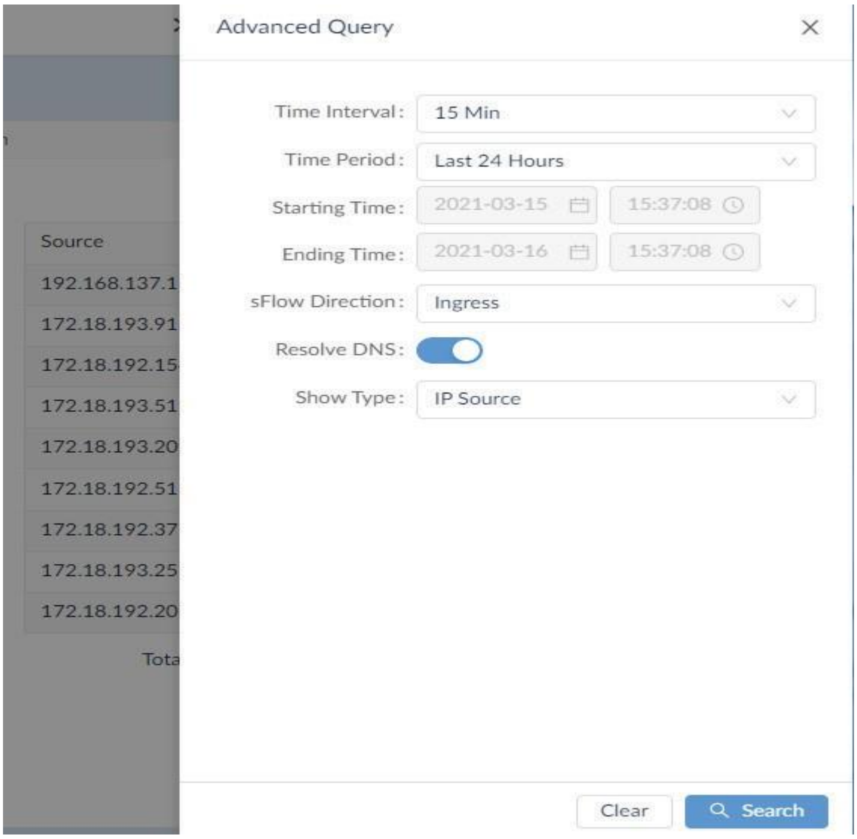
- ● 239.255.255.250
- ● 255.255.255.255
- ● 192.168.110.117
- ● 192.168.220.84
- ● 10.32.255.255
- ● 192.168.220.220
- ● 192.168.10.255
- ● 10.255.255.255
- ● 192.168.220.230
- ● 192.168.220.100
- ● Remaining traffic

Destination	Traffic	Percentage	Operation
239.255.255.250	40.75 MB	59.46 %	▤
255.255.255.255	21.62 MB	31.54 %	▤
192.168.110.117	920.42 KB	1.34 %	▤
192.168.220.84	633.42 KB	0.92 %	▤
10.32.255.255	493.92 KB	0.72 %	▤
192.168.220.220	439.96 KB	0.64 %	▤
192.168.10.255	424.2 KB	0.62 %	▤
10.255.255.255	292.14 KB	0.43 %	▤
192.168.220.230	262.54 KB	0.38 %	▤
192.168.220.100	235.32 KB	0.34 %	▤
169.254.255.255	225.9 KB	0.33 %	▤
192.168.220.229	193.12 KB	0.28 %	▤
192.168.220.225	192.1 KB	0.28 %	▤
192.168.220.98	180.66 KB	0.26 %	▤

Total 265 items < 1 2 3 ••• 18 > 15 / page Go to

3. Click the Advanced Query at the top right to set filter conditions to display information limited to a time range or any of the following conditions:
   - Specify the counter sampling interval.
   - Select the direction of packet passing a port: **Ingress**, **Egress**, or **Ingress and Egress**.
   - Slide the **Resolve DNS** or **Resolve User** to enable or disable the option.
   - Select the device identifier type: IP or MAC address to be displayed in the report.
   - Select the time range for data displayed.

- Click Search to start the query or Clear to reset the settings.



Advanced Query

Time Interval: 15 Min

Time Period: Last 24 Hours

Starting Time: 2021-03-15 15:37:08

Ending Time: 2021-03-16 15:37:08

sFlow Direction: Ingress

Resolve DNS:

Show Type: IP Source

10.5. View and Export sFlow Monitoring Results

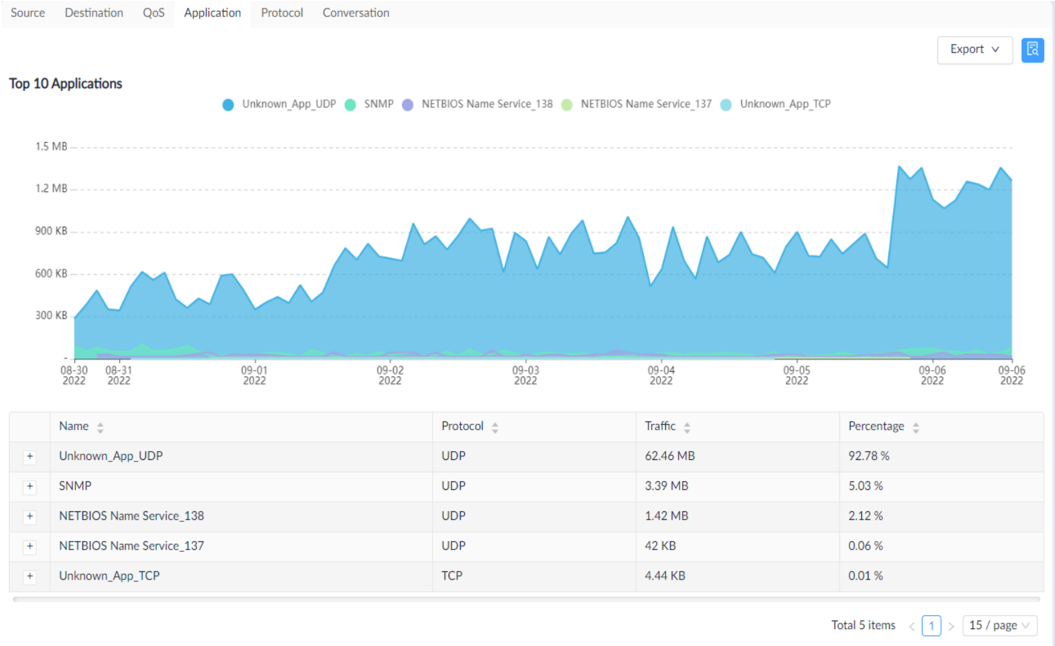
After specifying the conditions of sFlow information, with traffic transmitting through the monitoring sources, the results of sFlow can be obtained and analyzed. Note that sFlow Analyzer is only supported in Enterprise version.

The following information can be polled and displayed:

- Source: Display the source device. By default, the application displays information about the top 10 sources. Note that IP addresses or MAC addresses can be interpreted with configured aliases (go to **System > Basic Settings > sFlow Settings > IP Alias Mapping** or **System > Basic Settings > sFlow Settings > MAC Address Mapping**.)
- Destination: Display the destination device. By default, the application displays information about the top 10 destinations. You can also choose to display the destination by its IP address or MAC address. Note that MAC addresses can be interpreted with aliases (go to **System > Basic Settings > sFlow Settings > IP Alias Mapping** or **System > Basic Settings > sFlow Settings > MAC Address Mapping**.)
- QoS: Display the top 10 QoS. The DSCP is defined in sFlow Settings (go to **System > Basic Settings > sFlow Settings** and choose the **DSCP Mapping** tab.)
- Application: Display the application usage. It displays information about the top 10 applications. For mapping between an application and an alias, go to **System > Basic Settings > sFlow Settings > Application Mapping**.
- Protocol: Display the network protocol usage.
- Conversation: Display the conversation between devices.

To view the results of sFlow monitoring:

1. Go to **Monitoring > sFlow Analyzer**. The sFlow Analyzer page displays.



	Name	Protocol	Traffic	Percentage
+	Unknown_App_UDP	UDP	62.46 MB	92.78 %
+	SNMP	UDP	3.39 MB	5.03 %
+	NETBIOS Name Service_138	UDP	1.42 MB	2.12 %
+	NETBIOS Name Service_137	UDP	42 KB	0.06 %
+	Unknown_App_TCP	TCP	4.44 KB	0.01 %

2. Select the corresponding tab to display related sFlow data in that category.
3. At the top right, click the **Export** menu and select from the following file types to export the displayed data.

The data is saved to the default download folder of your browser.

11 Templates

Templates are designed for quick setup of device monitoring and configuration tasks and to ensure consistent configuration among devices of the desired model. In addition to monitoring and configuration tasks, they are also efficient for device provisioning.

11.1 Generate Device Templates

Device Templates are useful in batch provisioning and configuration as well as monitoring.

To generate a device template:

1. Go to **Templates > Device Template.** Then Click **Add Device Template** in the upper right corner**.**

2. Enter the following information:

Item	Description
Model Name	Enter the desired model for configuration
Device Type	Select the device type from the drop-down menu. Or click New at the right to add a new device type. For more information about device type, go to **Templates > Device Support**.
Vendor Name	Select the vendor with the vendor OID from the drop-down menu. Or click **New** at the right to add a new vendor. For more information about vendor, go to **Templates > Device Support**.
SOID	Enter the device’s system OID. You can also click **Search** at the right to find the specific device SOID using device IP and other SNMP connection parameters.
Hardware Version	Enter the hardware version of the device
Extended Information	Use this menu to add more properties to the device.

If you would like to associate a panel template, monitor template or configuration template to the device template, use the following procedure:

Click **Associate Panel Template** to associate a panel template to the model. You can customize a panel template to add to the system. For more information about panel template, refer to the below section 11.3 Generate Panel Template.

Click **Associate Monitor Template** to add a monitor template to the model. You can customize a monitor category and template to add to the system. For more information about monitor template, refer to the below section 11.4 Generate Monitor Template. Once a monitoring template is associated with a model, you can control its monitoring status or edit the polling interval. Refer to the above section 7.5.2 Monitor Settings.

Click the **Configuration** tab to add a configuration template to the model. You can customize a configuration category and template to add to the system. For more information about configuration template, refer to the below section 11.5 Generate Configuration Template. Once a configuration template is associated with a model, it can then be used for batch configuration. Refer to 6.1.Create Configuration and Profiles and 4.5.2 Batch Configuration.

Note: some of the system-built templates that have been employed as system-defaults on managed devices are still undergoing the verification process and may not work correctly; please visit the D-View website (https://dview.dlink.com/supportedModel) to obtain the latest list of supported models.

11.2 Manage Device Vendor and Device Type

Vendors and device types are key device properties. They are used for many configuration items and search criteria.

To add a new vendor:

1. Go to **Templates > Device Support > Vendor.** Then click **+ Add Vendor** in the upper right corner**.**

2. Enter the following information:

Item	Description
Vendor Name	Enter a vendor name for configuration.
Vendor OID	Enter the corresponding OID (object identifier) for the vendor.

To add a new device type:

1. Go to **Templates > Device Support > Device Type.** Then click **+ Add Device Type** in the upper right corner**.**

2. Enter the following information:

Item	Description
Device Type Name	Enter a name for the new device type.
Device Category	Select the category from the device category list. To add a new device category, go to the **Device Category** tab.
Description	Enter a description for this new device type.

You can also modify or delete a vendor or device type after it is created. Select the **Edit** or **Delete** button under the **Operation** column.

11.3 Generate Panel Templates

Panel templates are used for displaying the front panel which might include the ports and connectors as well as the vendor logo for easy identification.

To generate a panel template:

1. Go to **Templates > Panel Template**. Then click **Add Template** at the top right.

2. Enter the following information:

Item	Description
Template Name	Enter a name for the template.
Description	Enter a brief description for the template.
Vendor Logo	Upload a picture as the logo image for the panel. Note the file must be in JPG or PNG with size less than 2 MB.
Panel Height	Select the panel height:1 or 2 U.
Panel Width	Select the width of the panel: full, 2/3 or customized width (an decimal between 0 and 1)
Port Numbering Rule	Select the rule for numbering the ports: vertical or horizontal.
Port Starting Number	Enter the start number for the ports.
Port Start ifIndex	Enter the start number for port’s interface index.

To add ports to the panel, select the specific port appearance and drag and drop it on the designated port.

To label a port, click on a port and enter a name for Port Name.

To group/ungroup the ports, select **Group/Ungroup** from the **Draw a box to** drop-down menu, then circle the ports to group them together as a unit. Repeat this step to make multiple units of ports of the front panel.

Click **Save** to create the port layout for the panel template.

11.4 Generate Monitor Templates

Monitor templates are useful for configuring monitoring functions. You need to add a monitor category first before creating a monitor template. To add a monitor category:

1. Go to **Templates > Monitor Template**. Then select the **Monitor Category** tab.

2. Click **+Add Category** at the upper right.

3. Enter the following information:

Item	**Description**
Category Name	Enter a name for configuration.
Units	Select the unit for configuration.
Protocol	Select the protocol for configuration: SNMP, HTTPs, or WMI.
Line Chart	Enable or disable the line chart function which will display the monitoring results in graphic representation. Open the **Device Information** page (go to **Monitoring > Device View** and click the **System Name** link of a desired device) and select **Monitor > Customized Monitor** to view the added monitoring results.
Description	Enter a brief description for the category.
Data Source Definition	Click Add to define a name with value type for each data type.

Click **Save** to create the monitor category.

To add a monitor template:

1. Go to **Templates > Monitor Template** and select the **Monitor Template** tab. Select the desired category from the Monitor Category pane at the left. Then Click **Add Monitor Template** in the upper right corner**.**

2. Enter the following information:

Item	**Description**
Template Name	Enter a name for the template.
Monitor Category	Select the desired category for configuration.
Vendor Name	Select the vendor with the vendor OID from the drop-down menu. Or click **New** at the right to add a new vendor. For more information about vendor, refer to **Templates > Device Support**.
Monitoring Interval	Select the polling interval for monitoring: 60, 300, 600, 1800, and 7200. The default is 60 seconds.
Description	Enter a brief description for this template.
Data Source Definition	Click Add to define a name with value type for the specific data object obtained from the monitored devices.
Script	Enter a script to process the value of the added data source for the monitor template in Groovy.

Click **Save** to create the monitor template. Once a template is created, you can associate it to a device model. It can then be configured for monitoring a device with the preset system metrics, go to **Templates > Device Template** and **Alarm & Notification** > **Monitor & Alarm Settings**. You can also enable or disable a monitor function on a per-device basis; go to **Monitoring > Device View** and select the **Device Information** page via the **System Name** link. Then click the **Monitor tab** then click the **Monitoring Settings** button. (Refer to 4.2.2 Modify Device Information).

11.5 Generate Configuration Templates

Configuration templates are useful for consistent device configuration management. You need to add a configuration category first before creating a configuration template.

To add a configuration category:

1. Go to **Templates > Configuration Template**. Then select the **Configuration Category** tab.

2. Click **Add Category** at the upper right.

3. Enter the following information:

Item	Description
Category Name	Enter a name for configuration.
Description	Enter a brief description to help identify the category.
Configuration Type	Select either Quick or Advanced Configuration. The Quick Configuration type will be displayed as a category for Quick Configuration in Batch Configuration (go to **Configuration > Batch Configuration** and select the **Quick configuration** tab). The Advanced Configuration will only be available for configuration profiles for **Advanced Configuration** in **Batch Configuration** (go to **Configuration > Batch Configuration** and select the **Advanced Configuration** tab**).**

4. Click **Next** to continue. The template design page for the configuration category appears. First, choose the desired column layout for the template category. Then choose the control/input elements from the Basic Components pane.

5. Click **Save** to continue.

To add a configuration template:

1. Go to **Templates > Configuration Template.** Then select the **Configuration Template** tab.

2. Select the desired category from the Configuration Category pane at the left. Then Click **Add Template** at the upper right**.**

3. Enter the following information:

Item	Description
Name	Enter a name for the template.
Configuration Category	Select the desired category for configuration.
Vendor	Select the vendor with the vendor OID from the drop-down menu.
Protocol	Select the protocol used for configuration: SSH/Telnet or SNMP.
Description	Enter a brief description for this template.
CLI Command	Enter the CLI command to configure the device if using SSH/Telnet. Observe the following when writing CLI command: 1. Lines begin with a '#' will be considered as comments and will not be considered as commands. 2. Use '%' before and after the word to label it as a variable, for example, %IP%. 3. The value of the variables can be set in the 'Name' field in the Component Settings. 4. Each line must contain no more than one CLI command. 5. Avoid endless CLI commands to prevent deadlock operation. Example: ping 10.0.0.1. 6. Avoid CLI commands that may require special inputs to interrupt the operation. Example: show ports. Sample script: config ssh authmode password enable

	config ssh server contimeout 120 enable SSH Sample script with variables: config fdb aging_time %TimeoutSeconds% Sample comments: # this is a comment
Engineering View	The template design page at the bottom allows you to configure the component settings of the preset configuration layout and items. You can also add more control or input elements to the design.

Click **Save** to create the configuration template. Once a template is created, you can associate it to a device model. It can then be used for configuration changes and settings, go to **Configuration > Batch Configuration**. For more information, refer to **Add a Configuration Task** and 4.5.2 Batch Configuration. You can also adjust the settings of the configuration on a per-device basis; go to **Monitoring > Device View** and select the **Device Information** page via the **System Name** link of a desired model. Then click the **Management** tab then click the **More Settings** button. (Refer to 4.2.2 Modify Device Information.)

12 Reports

Reports are available as either built-in templates or customized ones. They can be generated once only or repeatedly according to a recurrence pattern.

12.1 Generate Scheduled Reports and My Reports

Scheduled reports can be generated through existing report templates. You can also create time-based reports to designate a date and time for a recurrent schedule.

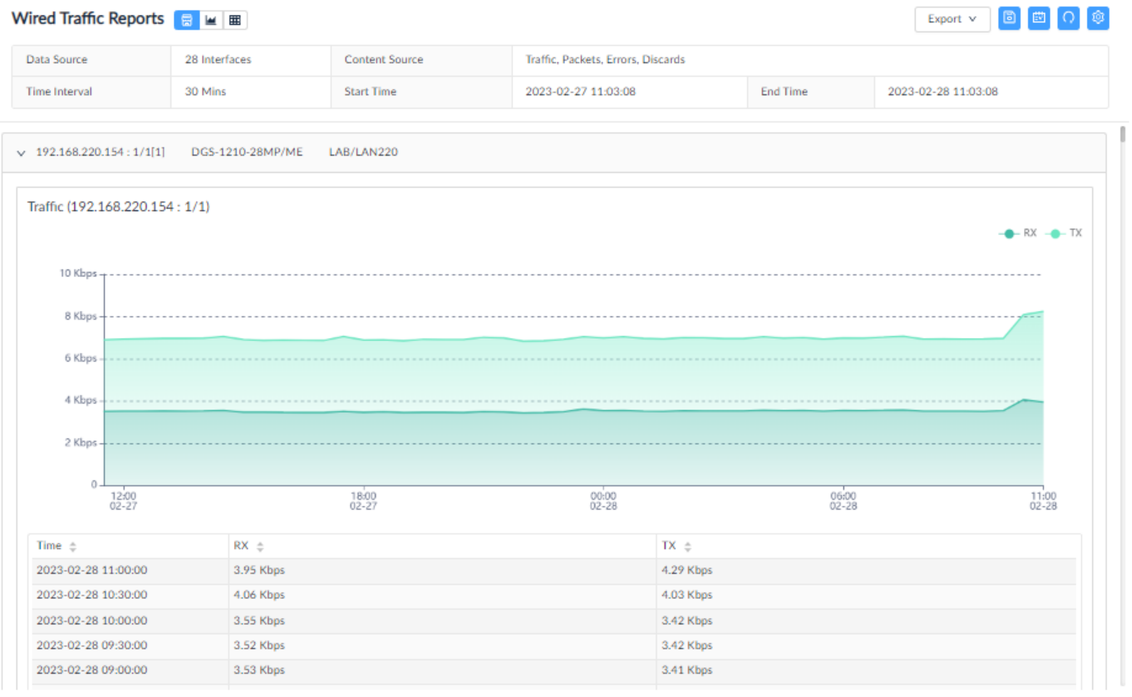
To generate a scheduled report:

1. Go to **Reports** > **General Reports** to display the General Reports page.

In order to create a scheduled report, an existing report must be present. See the below **Add a Report** section for further information.

2. Select a specific category from the reports list: Device Reports, Wired Interface Reports, Wireless Reports, or Advanced Reports.

The below example uses Wired Traffic category for demonstration.



Wired Traffic Reports

Data Source	28 Interfaces	Content Source	Traffic, Packets, Errors, Discards		
Time Interval	30 Mins	Start Time	2023-02-27 11:03:08	End Time	2023-02-28 11:03:08

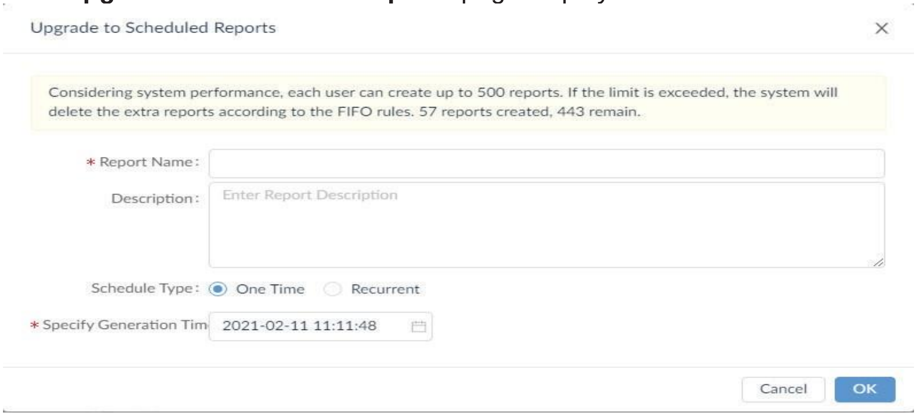
192.168.220.154 : 1/1[1] DGS-1210-28MP/ME LAB/LAN220

Traffic (192.168.220.154 : 1/1)

Time	RX	TX
2023-02-28 11:00:00	3.95 Kbps	4.29 Kbps
2023-02-28 10:30:00	4.06 Kbps	4.03 Kbps
2023-02-28 10:00:00	3.55 Kbps	3.42 Kbps
2023-02-28 09:30:00	3.52 Kbps	3.42 Kbps
2023-02-28 09:00:00	3.53 Kbps	3.41 Kbps

3. At the top right, click **Upgrade to Scheduled Reports**.

The **Upgrade to Scheduled Reports** page displays.



Upgrade to Scheduled Reports

Considering system performance, each user can create up to 500 reports. If the limit is exceeded, the system will delete the extra reports according to the FIFO rules. 57 reports created, 443 remain.

* Report Name:

Description: Enter Report Description

Schedule Type: ● One Time ○ Recurrent

* Specify Generation Tim 2021-02-11 11:11:48

NOTE: A maximum of 500 reports per user can be created to maintain optimal system performance. When the maximum is reached, older reports will be deleted.

4. Enter the required information:
   - Report Name: enter a name for the report
   - Description: enter a description to identify the report
   - Schedule Type: select the scheduling method for the report, One Time or Recurrent.

   For recurrent schedule, select a pre-defined schedule from the Schedule list or click Add Schedule to define a new schedule by selecting the frequency and effective duration to create reports:

   Specific Days: Executes the report task a single time or multiple times for a single day at a specified date(s)/time(s). Choose times for a day and specify dates.

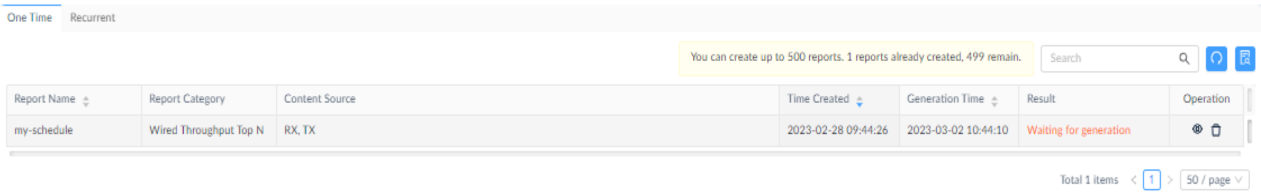
   Daily: Executes the report task at a specified time or different times of the day. Choose daily interval between executions: 1 to execute the task every day, 2 to execute the task every other day, and so on.

   Weekly: Executes the report task at a specified time or different times of a designated weekday or weekdays. Choose weekly interval between executions: 1 to execute the task on the specified weekday every week, 2 to execute the job every other week, and so on.

   Monthly: Executes the report task at a specified time or different times on designated day or days of the month. Specify a month or months: Jan to Dec and the days of the month.

5. Click **OK** to configure the scheduled report or click **Cancel** to return to the previous menu.

Select **Scheduled Reports** under the Reports menu to view the added report. If the report is defined as One Time, it will be listed under the **One Time** tab. If it is recurrent, click the **Recurrent** tab to view the report.



You can create up to 500 reports. 1 reports already created, 499 remain.

Report Name	Report Category	Content Source	Time Created	Generation Time	Result	Operation
my-schedule	Wired Throughput Top N	RX, TX	2023-02-28 09:44:26	2023-03-02 10:44:10	Waiting for generation	

Total 1 items 1 50 / page

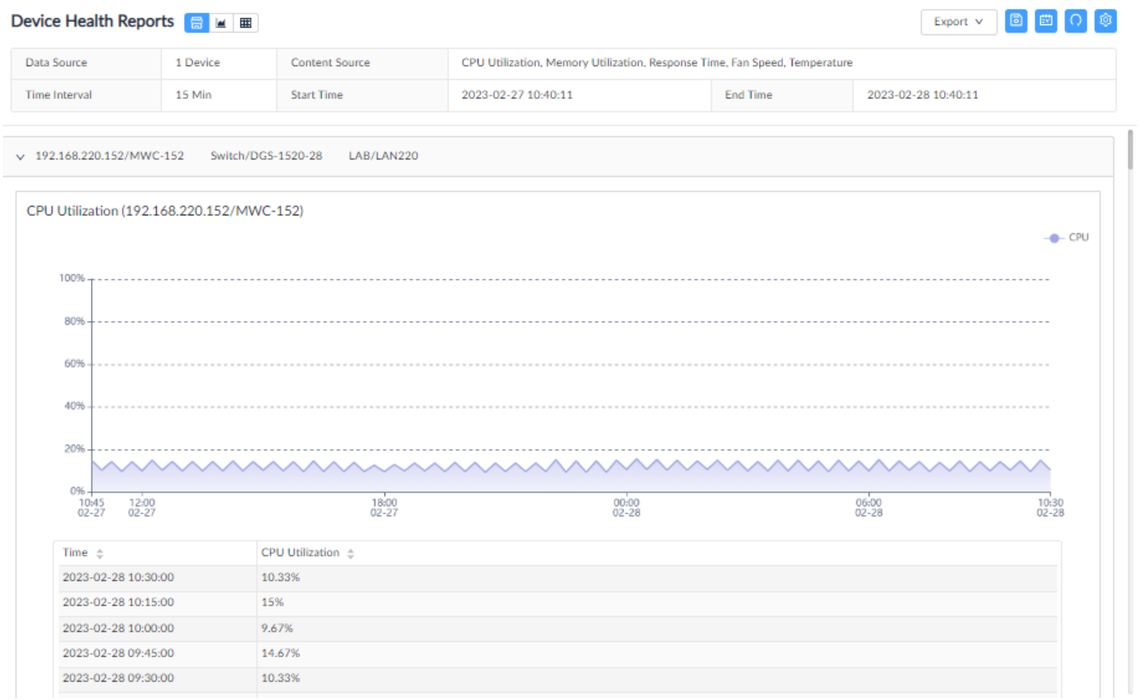
If **My Reports** is selected, the **Save to My Reports** page displays. For My Reports, enter a name and description to save it as My Reports.

To view the My Reports listing, select **Reports** > **My Reports**.

12.2 Manage Report Templates

The D-View 8 provides built-in report templates for the supported devices to accommodate a variety of monitoring and reporting cases.

The following table shows the menu of the default templates along with the types of reports available.



Device Health Reports

Data Source	1 Device	Content Source	CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature		
Time Interval	15 Min	Start Time	2023-02-27 10:40:11	End Time	2023-02-28 10:40:11

192.168.220.152/MWC-152 Switch/DGS-1520-28 LAB/LAN220

CPU Utilization (192.168.220.152/MWC-152)

Time	CPU Utilization
2023-02-28 10:30:00	10.33%
2023-02-28 10:15:00	15%
2023-02-28 10:00:00	9.67%
2023-02-28 09:45:00	14.67%
2023-02-28 09:30:00	10.33%

Report	Type	Category
General Reports	Device Reports	Device Health: CPU Utilization, Memory, Utilization, Response Time, Fan Speed, and Temperature. Trap: trap event reports Syslog: syslog message reports Device Top N: shows the top 10 device statistics of the selected devices with respect to the following performance indicators: CPU Utilization, Memory Utilization, Response Time, Tx/Rx traffic, Trap and Syslog messages.
	Wired Interface Reports	Wired Traffic: shows statistics of Rx and Tx traffic for all interfaces of the selected devices.
		Wired Throughput Top N: shows the Rx/Tx traffic statistics of the top 10 device ports of the selected devices
	Wireless Reports	Wireless Client Count: shows the number of wireless clients of the selected wireless devices.
		Wireless Traffic: shows the wireless traffic of the selected wireless devices.
	Advanced Reports	Inventory: shows the distribution of the selected devices with respect to device category and model.
Scheduled Reports	One Time Reports	An automatic report generated at a specified time.
	Recurrent Reports	An automatic report generated repeatedly at specified times.

My Reports	Customized Reports	A saved snapshot of the selected report from General Reports.

The following demonstrates how to generate a Syslog report using the provided template:

1. Click **HERE** on the page to configure a new report.

2. Select devices from the device list. Note that the managed devices must have D-View configured as a Syslog Server for D-View to collect logs (go to **Monitoring > Device View** and select the **System Name** link to open the Device Information page. Then click the **Management** tab to find the Trap and Syslog status switch).

3. Configure duration by clicking the drop-down menu to determine the timespan of the report: last hour, last 6/12/24 hours, today, yesterday, last 7 days, this week, last week, last 30 days, this month, last month, or customized. For customized, select the Start/End date and time.

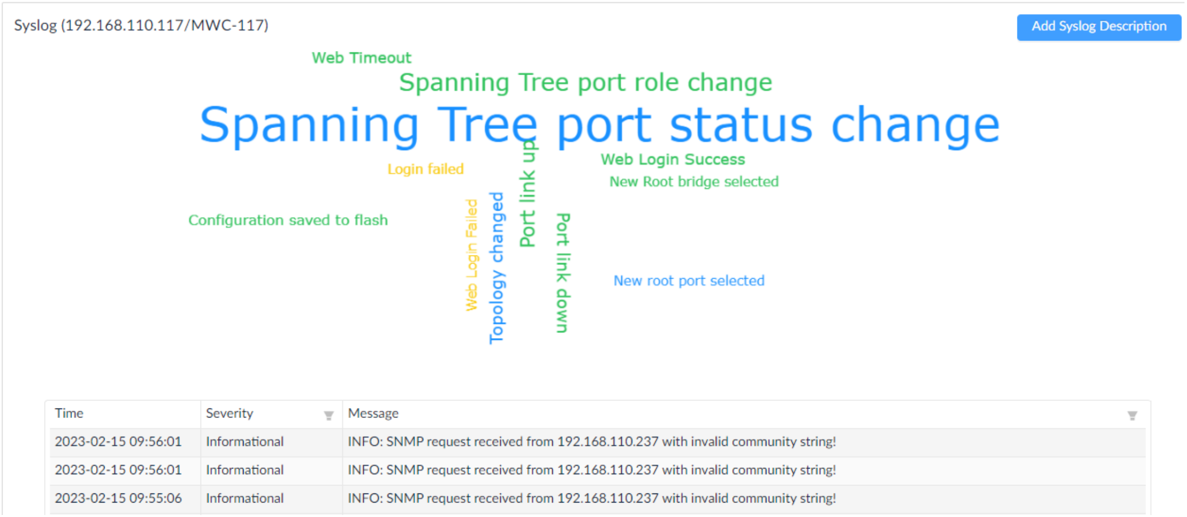
4. Click **Save** to display the generated report. Or click Reset to clear setting entered.

5. The buttons next to **Syslog Reports** control the representation of the report: show chart or table or both .

6. The **Add Syslog Description** button at the top right can be configured to represent a selected syslog message using descriptive text in the chart along with the number of occurrence and severity level. Hoover over a defined syslog description to display related information.

7. To add a syslog description, click **Add Syslog Description**. Enter a description that will be displayed as highlight text associated with matching keywords of the logs to signify a particular logged event. Then click **Save**. The new description entry will also be listed in **Alarm & Notification > Trap & Syslog Editor > Syslog Editor**.

8. The following shows the display of the syslog report using Syslog Description. Note that the larger the text, the higher the occurrence of the defined system log.



Syslog (192.168.110.117/MWC-117)

Time	Severity	Message
2023-02-15 09:56:01	Informational	INFO: SNMP request received from 192.168.110.237 with invalid community string!
2023-02-15 09:56:01	Informational	INFO: SNMP request received from 192.168.110.237 with invalid community string!
2023-02-15 09:55:06	Informational	INFO: SNMP request received from 192.168.110.237 with invalid community string!

The Trap report also displays highlight text of OID description to signify trap events. Refer to **7.3 Trap Editor** for more information.

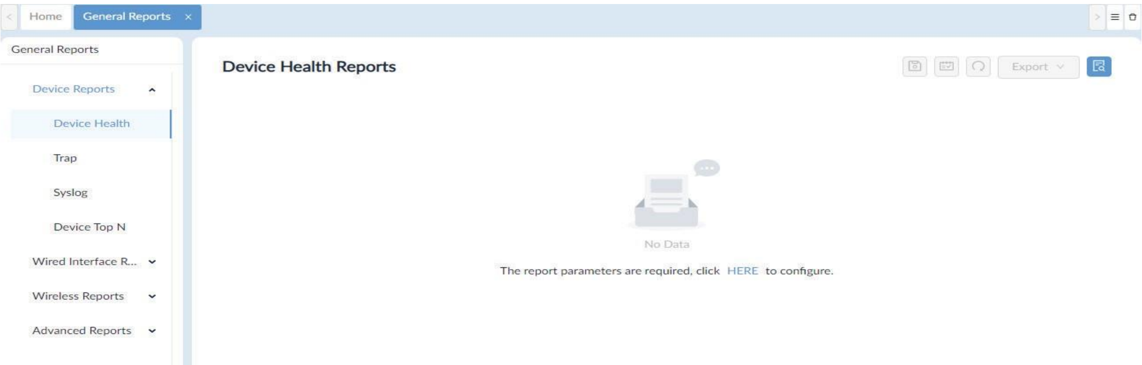
12.2.1. Add a Report

There are numerous templates for different reporting and summary purposes. By selecting a template, you can easily generate reports to help you maintain an effective network.

To select a report template or modify an existing one:

1. Go to **Reports > General Reports** to display the General Reports page.
2. Select a specific category from the reports list.

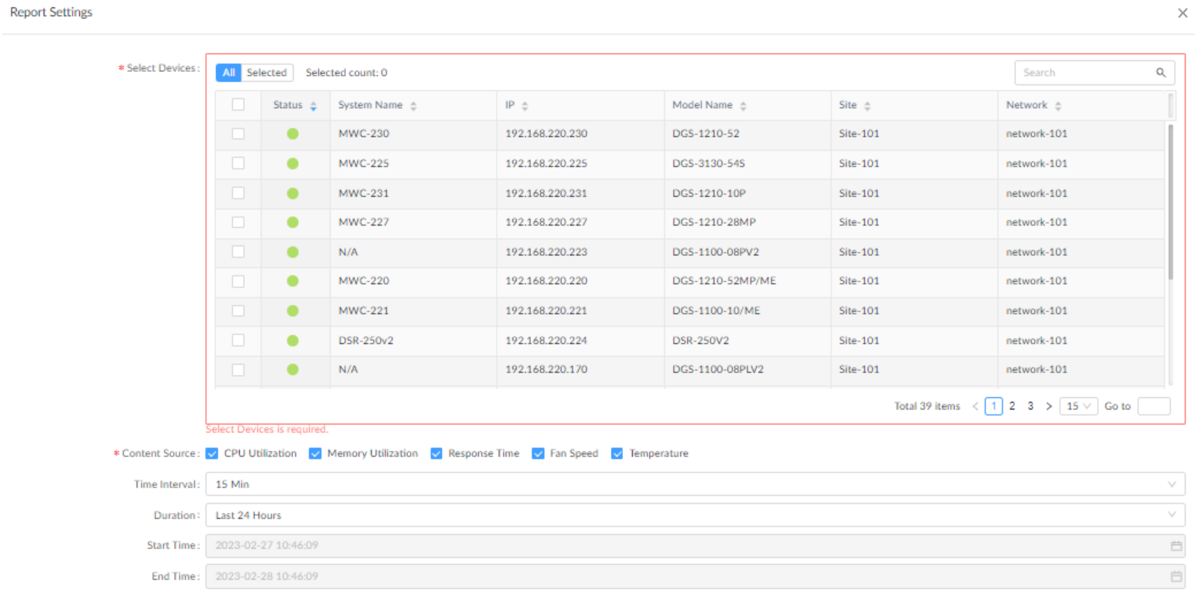
The following demonstration uses the Device Health Reports.



Device Health Reports

The report parameters are required, click HERE to configure.

3. Click **HERE** to configure report settings.



Report Settings

* Select Devices: All | Selected   Selected count: 0   Search

□	Status	System Name	IP	Model Name	Site	Network
□	●	MWC-230	192.168.220.230	DGS-1210-52	Site-101	network-101
□	●	MWC-225	192.168.220.225	DGS-3130-54S	Site-101	network-101
□	●	MWC-231	192.168.220.231	DGS-1210-10P	Site-101	network-101
□	●	MWC-227	192.168.220.227	DGS-1210-28MP	Site-101	network-101
□	●	N/A	192.168.220.223	DGS-1100-08PV2	Site-101	network-101
□	●	MWC-220	192.168.220.220	DGS-1210-52MP/ME	Site-101	network-101
□	●	MWC-221	192.168.220.221	DGS-1100-10/ME	Site-101	network-101
□	●	DSR-250v2	192.168.220.224	DSR-250V2	Site-101	network-101
□	●	N/A	192.168.220.170	DGS-1100-08PLV2	Site-101	network-101

Total 39 items < 1 2 3 > 15 Go to

Select Devices is required.

* Content Source: ☑ CPU Utilization ☑ Memory Utilization ☑ Response Time ☑ Fan Speed ☑ Temperature

Time Interval: 15 Min

Duration: Last 24 Hours

Start Time: 2023-02-27 10:46:09

End Time: 2023-02-28 10:46:09

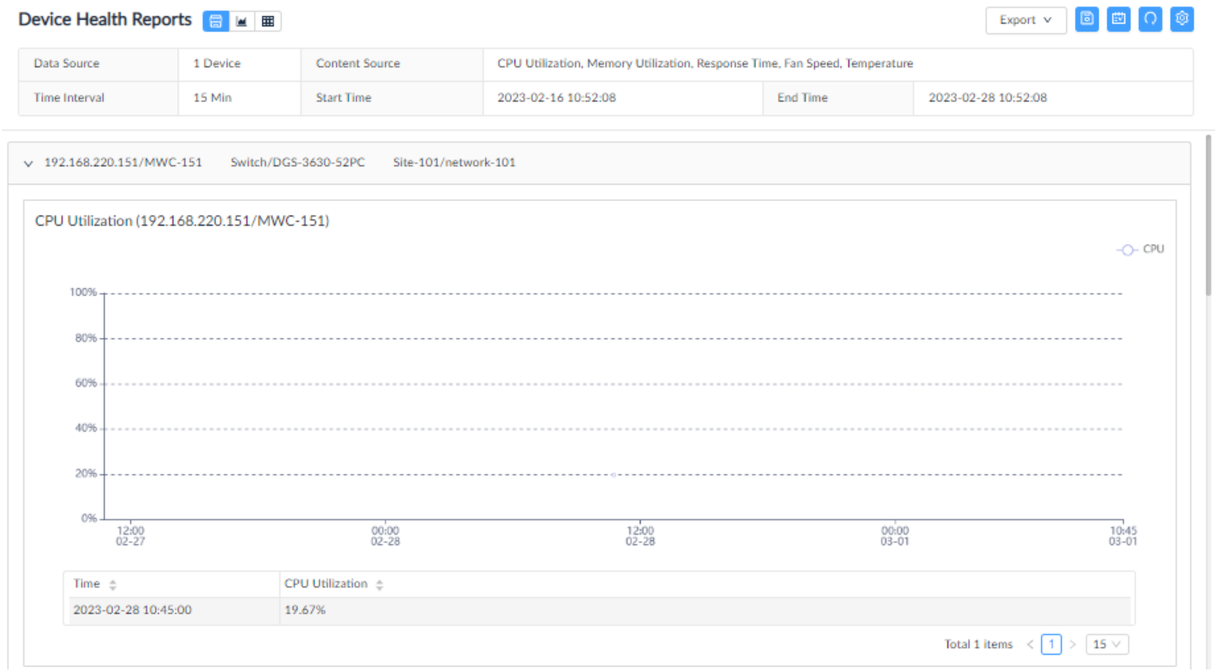
The Report Settings page displays.

4. Configure the following:

Item	Description
Select Devices	Scroll through the list to select devices or use the Search field to filter the list by System Name, IP, Model Name, Site or Network. Up to 15 devices can be selected for a single report in this category.
Content Source	Click to select the type of report data: CPU Utilization, Memory Utilization, Response Time, Fan Speed, or Temperature.
Time Interval	Select the interval for the data: 15 min, 2 hours, 8 hours, or 1 day
Duration	Click the drop-down menu to determine the timespan of the report: last hour, last 6/12/24 hours, today, yesterday, last 7 days, this week, last week, last 30 days, this month, last month, or customized.
Start Time	Set the starting date if customized duration is selected.

End Time	Set the ending date if customized duration is selected.
Note: The configurable settings vary depending on the type of report.	

5. Click **Save** to create the report or click **Reset** to clear settings entered.



Device Health Reports

Export

Data Source	1 Device	Content Source	CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature		
Time Interval	15 Min	Start Time	2023-02-16 10:52:08	End Time	2023-02-28 10:52:08

192.168.220.151/MWC-151 Switch/DGS-3630-52PC Site-101/network-101

CPU Utilization (192.168.220.151/MWC-151)

Time	CPU Utilization
2023-02-28 10:45:00	19.67%

Total 1 items < 1 > 15

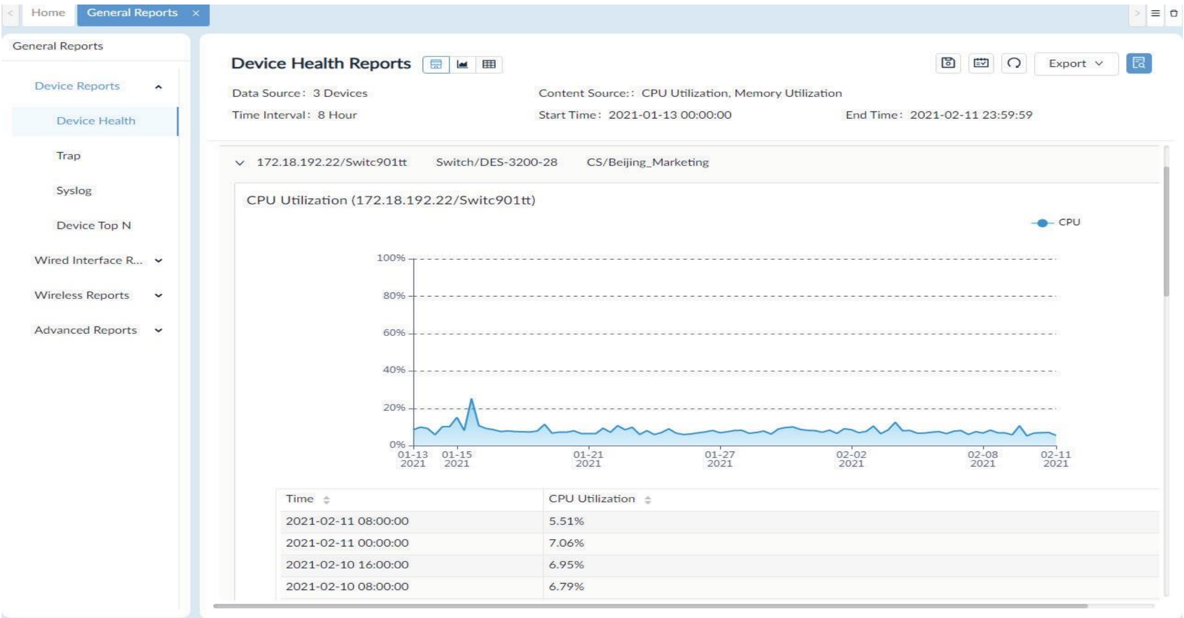
You can then view the report data in the default format, chart, or table by using the control buttons .

12.2.2. Modify a Report

A report can be removed without deleting the template. However, the data generated by the report is deleted. We recommend that you save the reports using the Export function before deleting them.

To delete or modify an existing report:

1. Go to **Reports > General Reports** to display the General Reports page.
2. Select a specific category from the reports list: Device Reports, Wired Interface Reports, Wireless Reports, or Advanced Reports.



Device Health Reports

Data Source： 3 Devices

Content Source：： CPU Utilization, Memory Utilization

Time Interval： 8 Hour

Start Time： 2021-01-13 00:00:00

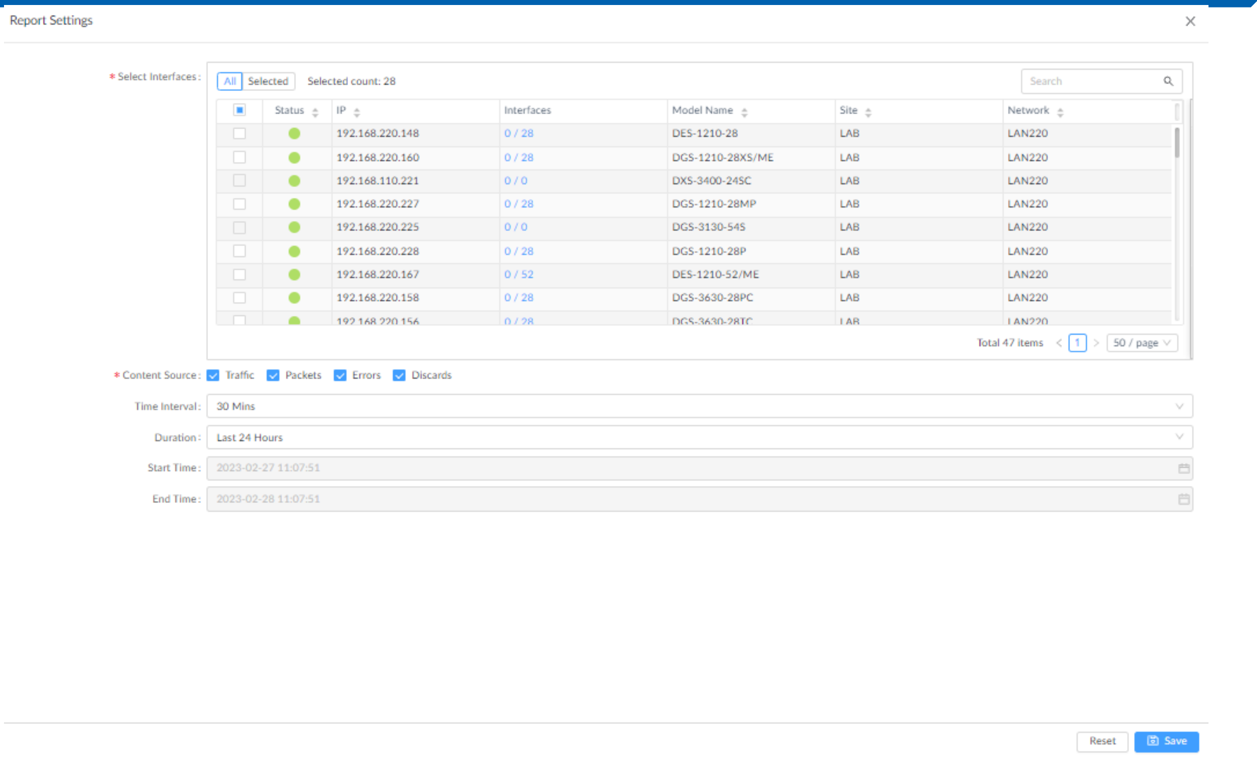
End Time： 2021-02-11 23:59:59

172.18.192.22/Switc901tt Switch/DES-3200-28 CS/Beijing_Marketing

CPU Utilization (172.18.192.22/Switc901tt)

Time	CPU Utilization
2021-02-11 08:00:00	5.51%
2021-02-11 00:00:00	7.06%
2021-02-10 16:00:00	6.95%
2021-02-10 08:00:00	6.79%

3. For demonstration, the Device Health category is selected and the existing report also displays.
4. Click **Report Settings** at the top right. The Report Setting page displays.



Report Settings

* Select Interfaces: All | Selected   Selected count: 28

■	Status	IP	Interfaces	Model Name	Site	Network
□	●	192.168.220.148	0 / 28	DES-1210-28	LAB	LAN220
□	●	192.168.220.160	0 / 28	DGS-1210-28XS/ME	LAB	LAN220
□	●	192.168.110.221	0 / 0	DXS-3400-24SC	LAB	LAN220
□	●	192.168.220.227	0 / 28	DGS-1210-28MP	LAB	LAN220
□	●	192.168.220.225	0 / 0	DGS-3130-54S	LAB	LAN220
□	●	192.168.220.228	0 / 28	DGS-1210-28P	LAB	LAN220
□	●	192.168.220.167	0 / 52	DES-1210-52/ME	LAB	LAN220
□	●	192.168.220.158	0 / 28	DGS-3630-28PC	LAB	LAN220
□	●	192.168.220.156	0 / 28	DGS-3630-28TC	LAB	LAN220

Total 47 items < 1 > 50 / page

* Content Source: ☑ Traffic ☑ Packets ☑ Errors ☑ Discards

Time Interval: 30 Mins

Duration: Last 24 Hours

Start Time: 2023-02-27 11:07:51

End Time: 2023-02-28 11:07:51

5. To modify the current report, re-configure the settings and click **Save**.
6. To clear all settings, click **Reset.** The report and the data will be removed from the **General Reports** page.

12.3 View and Remove Reports

All reports can be viewed for the period they are retained. Reports can also be removed.

To remove a Scheduled Report:

1. Click **Scheduled Reports** to view the list of scheduled reports.
2. Select the One Time or Recurrent tab.
3. Under **Operation**, click the **View report** or **Delete this report** to view or remove the report.

To view or remove a saved report from My Report:

1. Click **My Reports** to view all reports saved in this type.
2. Under **Operation**, click the **View report** or **Delete this report** to view or remove the report.

13 Users and Security Profiles

The system lets you manage users efficiently with profiles that define a set of function rights on the system.

This section covers the following topics:

- Profile Role Types
- Authentication Credentials
- Add a Profile

In addition to limiting the ability of users with function rights, you can also assign privileges that restrict access to a site or network (refer to 13.3 Add a User Profile)

13.1 Profile Role Types

The D-View 8 has the following built-in user roles:

- Super Administrator: The user can perform all functions including licensing and system upgrade.
- Organization Administrator: The user can perform all administrative functions, including the management of users and security profiles within an organization.
- Site Administrator: The user can perform administrative functions within a site.
- Network Administrator: The user can perform all administrative functions within a network.

Function	Super Administrator	Organization Administrator	Site Administrator	Network Administrator
Dashboard				
Analysis				
Overview	Read and Write	Read and Write	Read and Write	Read Only
Switch	Read and Write	Read and Write	Read and Write	Read Only
Wireless	Read and Write	Read and Write	Read and Write	Read Only
Host	Read and Write	Read and Write	Read and Write	Read Only
sFlow	Read and Write	Read and Write	Read and Write	Read Only
PoE	Read and Write	Read and Write	Read and Write	Read Only
Customized Dashboard	Read and Write	Read and Write	Read and Write	Read Only
Monitoring				
Network Discovery	Read and Write	Read and Write	Read Only	Read Only
Device View	Read and Write	Read and Write	Read and Write	Read and Write
Interface View	Read and Write	Read and Write	Read and Write	Read and Write
Topology Map	Read and Write	Read and Write	Read and Write	Read Only
Connection View	Read and Write	Read and Write	Read and Write	Read and Write
Rack View	Read and Write	Read and Write	Read and Write	Read Only
sFlow Analyzer	Read and Write	Read and Write	Read and Write	Read and Write
Device Group	Read and Write	Read and Write	Read and Write	Read and Write
Configuration				
Batch Configuration				
Quick Configuration	Read and Write	Read and Write	Read and Write	Read and Write
Advanced Configuration	Read and Write	Read and Write	Read and Write	Read and Write
Task Management				
Current Task	Read and Write	Read and Write	Read and Write	Read and Write

Historical Task	Read and Write	Read and Write	Read and Write	Read and Write
Firmware Management	Read and Write	Read and Write	Read and Write	Read and Write
Configuration Management				
Backup	Read and Write	Read and Write	Read and Write	Read and Write
Restore	Read and Write	Read and Write	Read and Write	Read and Write
File Management	Read and Write	Read and Write	Read and Write	Read and Write
Alarm & Notification				
Alarm				
Active Alarms	Read and Write	Read and Write	Read and Write	Read and Write
Historical Alarms	Read and Write	Read and Write	Read and Write	Read and Write
Trap & Syslog				
Trap	Read and Write	Read and Write	Read and Write	Read Only
Syslog	Read and Write	Read and Write	Read and Write	Read and Write
Trap Editor	Read and Write	Read and Write	Read and Write	Read Only
Syslog Editor	Read and Write	Read and Write	Read and Write	Read Only
Monitor & Alarm Settings				
Alarm Settings	Read and Write	Read and Write	Read and Write	Read and Write
Monitor Settings	Read and Write	Read and Write	Read and Write	Read and Write
Notification Center	Read and Write	Read and Write	Not Available	Not Available
Templates				
Device Template	Read and Write	Read and Write	Not Available	Not Available
Device Support				
Vendor	Read and Write	Read and Write	Not Available	Not Available
Device Category	Read and Write	Read and Write	Not Available	Not Available
Device Type	Read and Write	Read and Write	Not Available	Not Available
Panel Template	Read and Write	Read and Write	Not Available	Not Available
Monitor Template				
Monitor Category	Read and Write	Read and Write	Not Available	Not Available
Monitor Template	Read and Write	Read and Write	Not Available	Not Available
Configuration Template				
Configuration Category	Read and Write	Read and Write	Not Available	Not Available
Configuration Template	Read and Write	Read and Write	Not Available	Not Available
Reports				
General Reports	Read and Write	Read and Write	Read and Write	Read and Write
Schedule Reports	Read and Write	Read and Write	Read and Write	Read and Write
My Reports	Read and Write	Read and Write	Read and Write	Read and Write
Tools				
MIB Browser	Read and Write	Read and Write	Read Only	Read Only
MIB Compiler	Read and Write	Read and Write	Not Available	Not Available
ICMP Ping	Read and Write	Read and Write	Read and Write	Read and Write
SNMP Test	Read and Write	Read and Write	Read and Write	Read and Write
Trace Route	Read and Write	Read and Write	Read and Write	Read and Write
CLI	Read and Write	Read and Write	Read and Write	Read and Write
File Comparison	Read and Write	Read and Write	Read and Write	Read and Write
System				
Basic Settings				
Organization	Read and Write	Read and Write	Not Available	Not Available

Mail Server Settings	Read and Write	Read and Write	Not Available	Not Available
Forward Trap	Read and Write	Read and Write	Not Available	Not Available
Forward Syslog	Read and Write	Read and Write	Not Available	Not Available
REST API	Read and Write	Read and Write	Not Available	Not Available
Credentials	Read and Write	Read and Write	Not Available	Not Available
sFlow Settings	Read and Write	Read and Write	Not Available	Not Available
System Preferences	Read and Write	Read and Write	Read and Write	Read and Write
User Management				
Users	Read and Write	Read and Write	Read Only	Not Available
Role Privileges	Read and Write	Read and Write	Not Available	Not Available
AD Server	Read and Write	Read and Write	Not Available	Not Available
RADIUS Server	Read and Write	Read and Write	Not Available	Not Available
Scheduling	Read and Write	Read and Write	Read Only	Read Only
Server Management				
Probe	Read and Write	Read and Write	Not Available	Not Available
Core Server	Read and Write	Read and Write	Not Available	Not Available
Web Server	Read and Write	Read and Write	Not Available	Not Available
D-View 8 Logs				
User Operation Log	Read Only	Read Only	Read Only	Read Only
System Log	Read Only	Read Only	Read Only	Read Only
Device Maintenance Log	Read Only	Read Only	Read Only	Read Only
D-View 7 Upgrade	Read and Write	Not Available	Not Available	Not Available
About	Read and Write	Read Only	Read Only	Read Only

13.2 Authentication

User management and access rights are controlled by user profiles and roles. The system provides three mechanisms for the control of user authentication and privileges and other related policies:

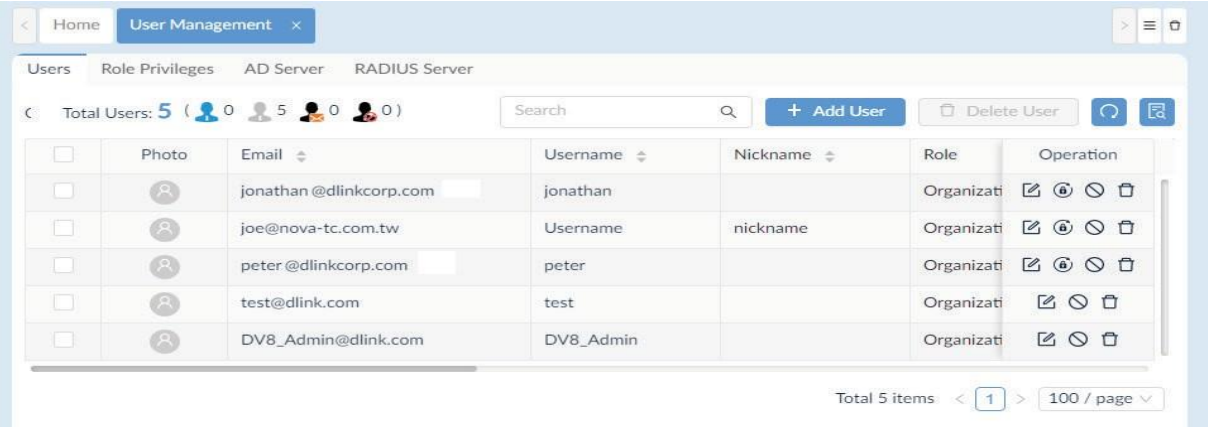
- Local authentication
- RADIUS authentication
- AD authentication

13.2.1. Join an AD Server

You can join the D-View 8 system to an AD domain. When you join an AD server, you will need the following:

- Domain name
- Domain controller address

1. Go to **System > User Management** to display the User Management page.

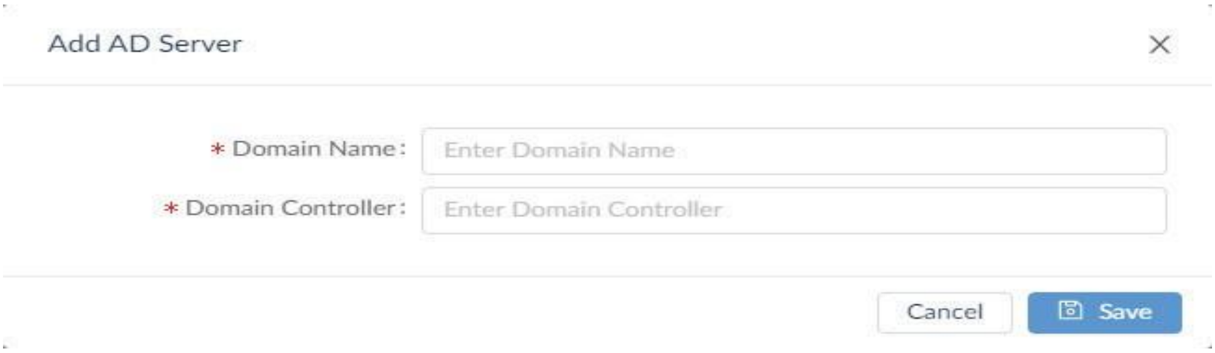


Total Users: 5 (0 5 0 0)

	Photo	Email	Username	Nickname	Role	Operation
☐		jonathan@dlinkcorp.com	jonathan		Organizati	
☐		joe@nova-tc.com.tw	Username	nickname	Organizati	
☐		peter@dlinkcorp.com	peter		Organizati	
☐		test@dlink.com	test		Organizati	
☐		DV8_Admin@dlink.com	DV8_Admin		Organizati	

Total 5 items < 1 > 100 / page

2. Click the AD Server tab. Then click **+Add AD Server**.
3. In the **Add AD Server** page, enter the domain name and controller information of the AD server.



Add AD Server

* Domain Name: Enter Domain Name

* Domain Controller: Enter Domain Controller

4. Click **Save** to accept the settings or click **Cancel** to return to the previous screen.

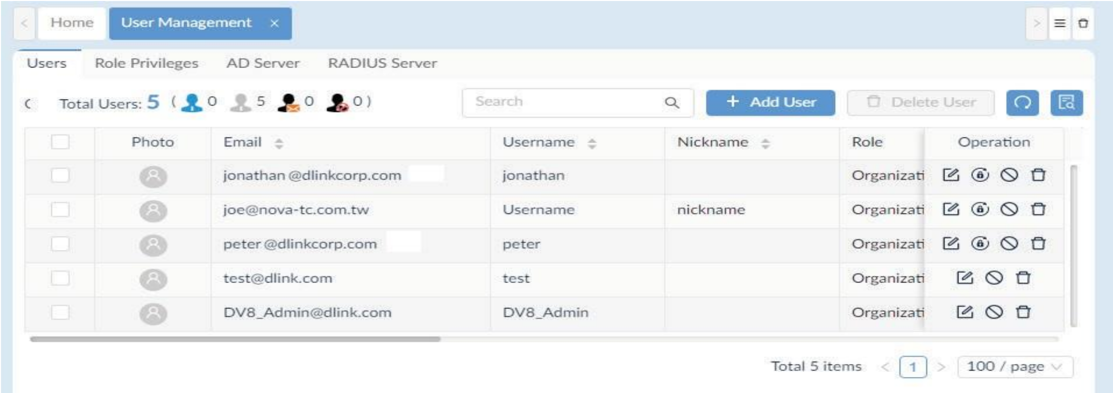
To delete or modify a specific entry, you can use the Search or Advanced Query function to filter the list. Then click the **Edit** or **Delete** button under **Operation**.

13.2.2. Join a RADIUS Server

This section describes how to employ a RADIUS server to the D-View 8 system.

To configure the D-View 8 with a RADIUS server:

1. Go to **System > User Management** to display the User Management page.

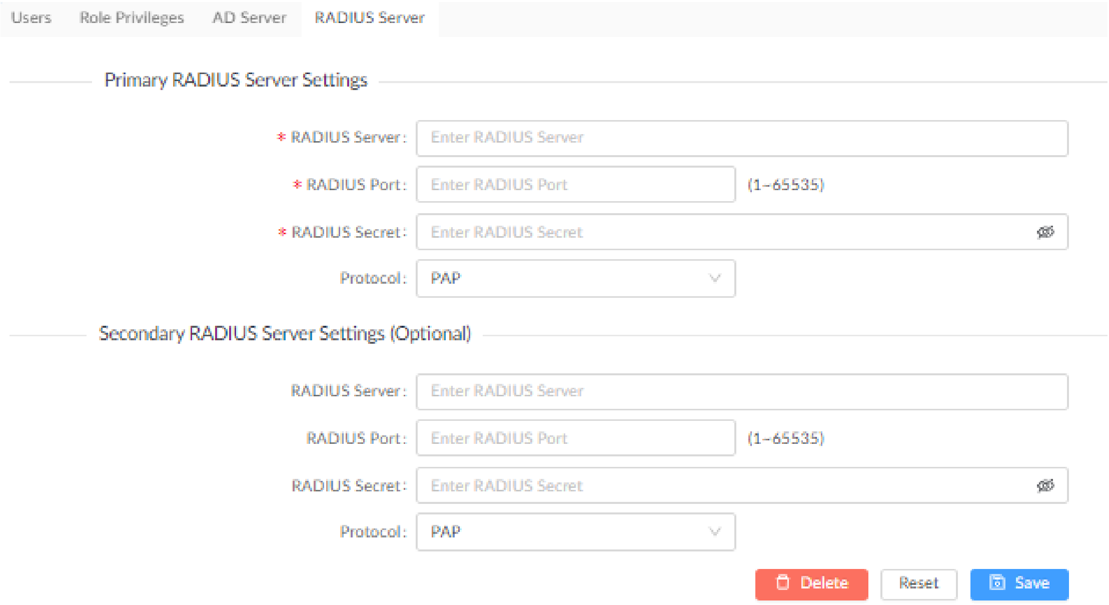


Total Users: 5 (0 5 0 0)

	Photo	Email	Username	Nickname	Role	Operation
□		jonathan @dlinkcorp.com	jonathan		Organizati	
□		joe@nova-tc.com.tw	Username	nickname	Organizati	
□		peter @dlinkcorp.com	peter		Organizati	
□		test@dlink.com	test		Organizati	
□		DV8_Admin@dlink.com	DV8_Admin		Organizati	

Total 5 items < 1 > 100 / page

2. Click **RADIUS Server** to display the RADIUS Server page.



Primary RADIUS Server Settings

* RADIUS Server: Enter RADIUS Server

* RADIUS Port: Enter RADIUS Port (1–65535)

* RADIUS Secret: Enter RADIUS Secret

Protocol: PAP

Secondary RADIUS Server Settings (Optional)

RADIUS Server: Enter RADIUS Server

RADIUS Port: Enter RADIUS Port (1–65535)

RADIUS Secret: Enter RADIUS Secret

Protocol: PAP

3. In the Primary RADIUS Server Settings, enter the following:

Item	Description
RADIUS Server	Enter the server IP address of the remote RADIUS server.
RADIUS Port	Enter port number for RADIUS service.
RADIUS Secret	Enter the authentication and encryption key string to communicate with the RADIUS server.
Protocol	Enter the authentication scheme used by the RADIUS server: PAP: Password Authentication Protocol. CHAP: Challenge Handshake Authentication Protocol. MSCHAP: Microsoft Challenge Handshake Authentication Protocol. MSCHAP2: Microsoft Challenge Handshake Authentication Protocol 2 with added mutual authentication between peers.
Secondary RADIUS Server Settings (Optional)	
RADIUS Server	Enter the server IP address of the remote RADIUS server.
RADIUS Port	Enter port number for RADIUS service.
RADIUS Secret	Enter the authentication and encryption key string used for the RADIUS service. The key is a text string that must match the encryption key defined in the RADIUS server.

Protocol	Enter the authentication scheme used by the RADIUS server: • PAP: Password Authentication Protocol. • CHAP: Challenge Handshake Authentication Protocol. • MSCHAP: Microsoft Challenge Handshake Authentication Protocol. • MSCHAP2: Microsoft Challenge Handshake Authentication Protocol with added mutual authentication between peers.
Delete	Click to remove the entry.
Reset	Click to clear all settings on the page.

4. Click **Save** to accept the new entry.

13.3 Add a User Profile

The D-View 8 uses role-based access control. To obtain the function rights of each role, go to **System > User Management** and select the **Role Privileges** tab. Users are created and managed using a profile. A user profile consists of username, password and privileges associated with the designated role.

To add a user profile:

1. Go to **System > User Management** to display the User Management page.

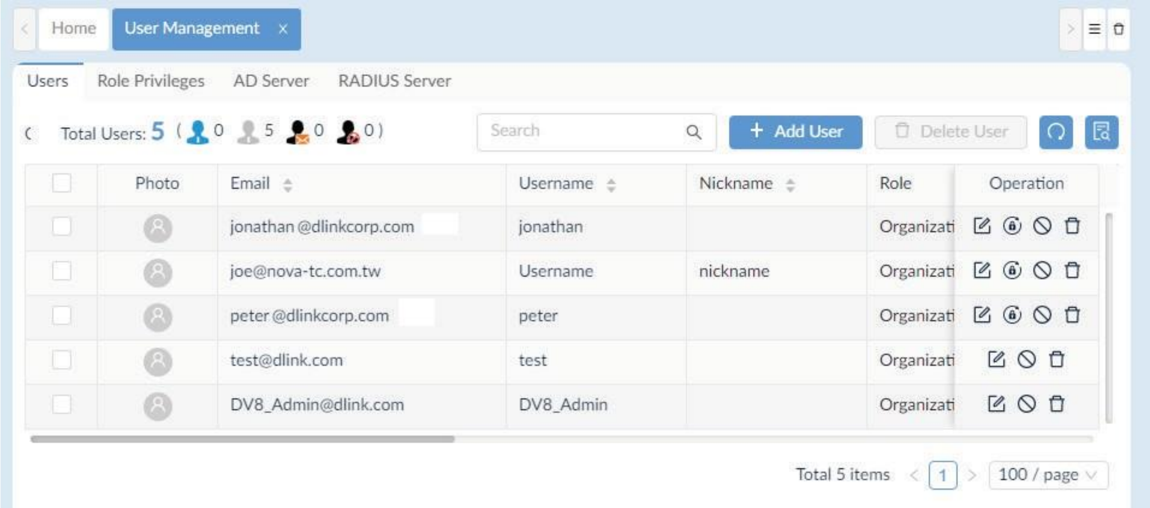
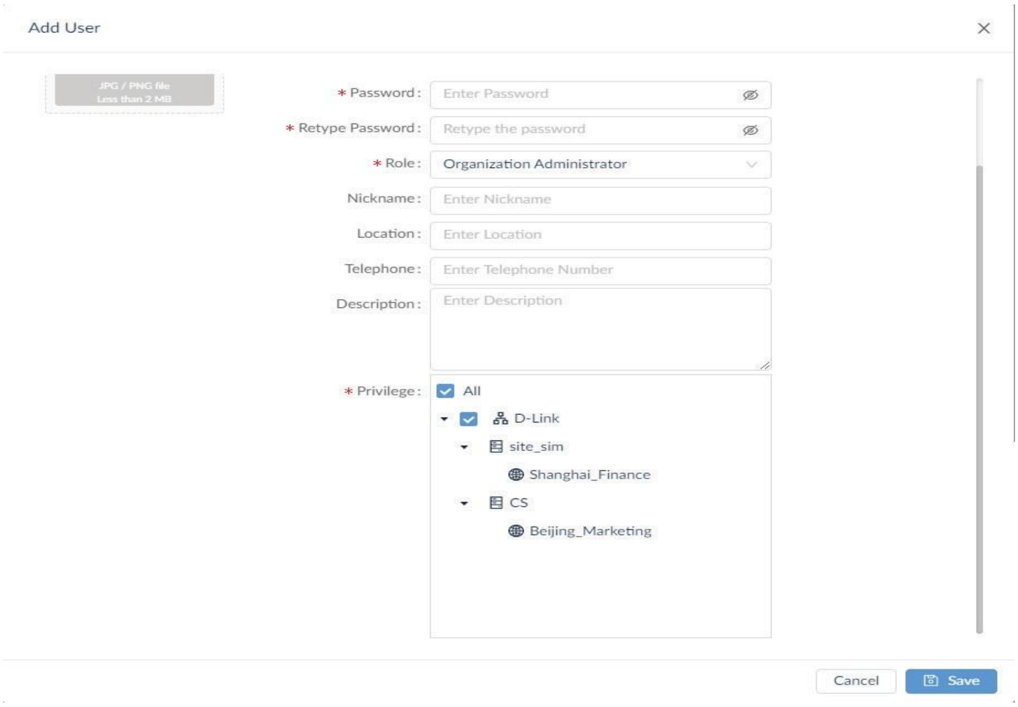


	Photo	Email	Username	Nickname	Role	Operation
□		jonathan@dlinkcorp.com	jonathan		Organizati	
□		joe@nova-tc.com.tw	Username	nickname	Organizati	
□		peter@dlinkcorp.com	peter		Organizati	
□		test@dlink.com	test		Organizati	
□		DV8_Admin@dlink.com	DV8_Admin		Organizati	

2. Click +**Add User**.



* Password: Enter Password

* Retype Password: Retype the password

* Role: Organization Administrator

Nickname: Enter Nickname

Location: Enter Location

Telephone: Enter Telephone Number

Description: Enter Description

* Privilege:
☑ All
☑ D-Link
site_sim
Shanghai_Finance
CS
Beijing_Marketing

3. Click the icon to browse and upload a JPG / PNG file to use it for the profile image.

4. Enter the following information:

Item	Description
Authentication type	Select one of the authentication methods: local, RADIUS or AD server.
Email	Enter the profile email.
Username	Enter the username for the profile.

Password	The password must be at least 6 alphanumeric characters consisiting of both numbers and letters. Symbols are also permitted.
Retype Password	Enter the same password to authenticate.
Role	Select the profile's security role.
Nickname (optional)	Enter a descriptive nickname.
Location (optional)	Enter the location of the profile.
Telephone (optional)	Enter the phone number of the profile, optional.
Description (optional)	Enter a description to identify the profile.
Privilege	For each Role type, select an organization, site, or network that the user can access with read-only or both read and write access rights. A read-only access right permits an authorized user to obtain information of the assets under a network hierarchy. It does not permit modification of configurations. Note that the Privilege here controls the access to a network or a site whereas the user roles group together a set of rights to perform system operations. Refer to 13.1 Profile Role Types.

5. Click **Save** to create the profile or click **Cancel** to return to the previous menu.

Once a profile is created, the system will send a verification email to the specified email address for account verification.

Once a user account is created, you can perform the following to modify its profile:

- Edit: modify the profile information
- Send Activation Email: send an account invitation email with activation link. (This is only available to the Super Admin role.)
- Activate: activate this user account
- Reset Password: generate a new password for the profile. The new password will be sent to the profile's email.
- Disable: deactivate this user account.
- Delete: remove this user account.

14 System Settings

You can configure global settings to be used for system-wide management and communication in the following areas:

- Organization
- Mail Server Settings
- Forward Trap
- Forward Syslog
- REST API
- SNMP/WMI/Telnet Credentials
- sFlow Settings
- System Preferences

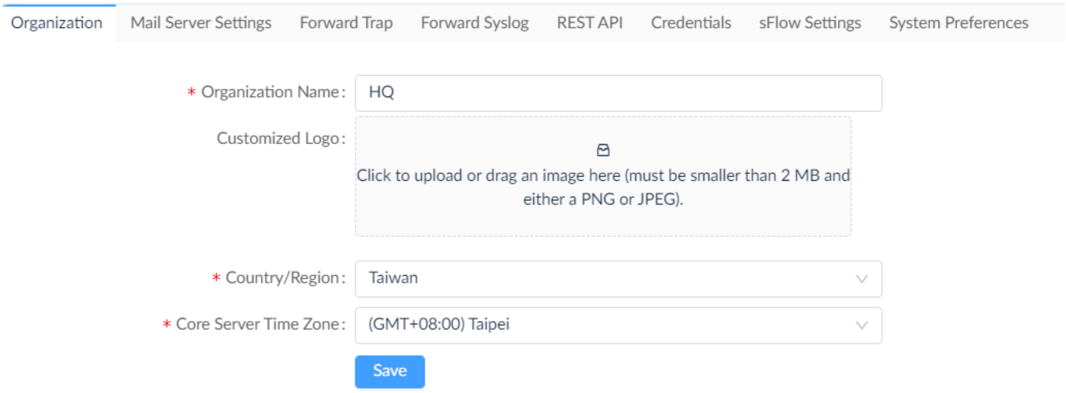
14.1 Configure Global Settings

Set Up Organization

The organization information is located under the Basic Settings menu. You can define the time zone, location, and name in the basic settings. The Organization information is required for Network Discovery and subsequent display of network architecture.

To set up organization information:

1. Go to **System > Basic Settings**.



* Organization Name: HQ

Customized Logo: Click to upload or drag an image here (must be smaller than 2 MB and either a PNG or JPEG).

* Country/Region: Taiwan

* Core Server Time Zone: (GMT+08:00) Taipei

2. Define the following information:

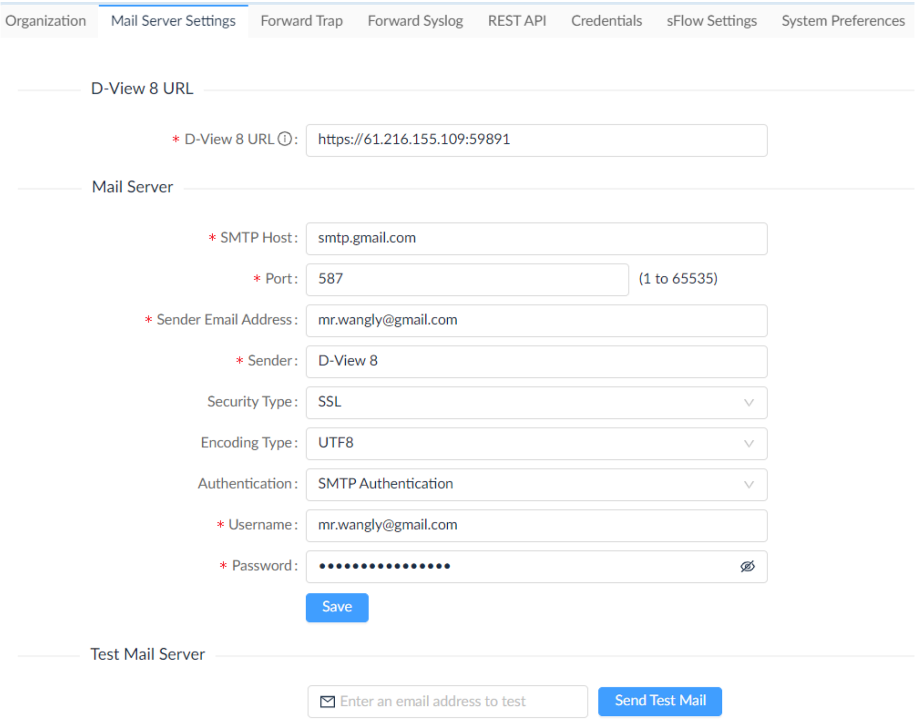
Item	Description
Organization Name	Enter the name to define the organization.
Customized Logo	Select an image to upload, which must be less than 2 MB in JPEG or PNG format.
Country/Region	Select the location of the organization.
Time Zone	Select the time zone corresponding to the specified location.

3. Click **Save**.

Set Up Mail Server

Setting up a mail server is required for email notifications. To set up mail server information:

1. Go to **System** > **Basic Settings** to display the Organization page.
2. Click the **Mail Server Settings** tab to display the Mail Server Settings.



D-View 8 URL

* D-View 8 URL ⓘ: https://61.216.155.109:59891

Mail Server

* SMTP Host: smtp.gmail.com

* Port: 587 (1 to 65535)

* Sender Email Address: mr.wangly@gmail.com

* Sender: D-View 8

Security Type: SSL

Encoding Type: UTF8

Authentication: SMTP Authentication

* Username: mr.wangly@gmail.com

* Password: •••••••••••••••

Test Mail Server

Enter an email address to test

3. Enter the following information:

Item	Description
D-View 8 URL	The URL will be used for email verification link and appear in the password reset emails.
SMTP Host	Enter the SMTP server address.
Port	Enter the port number of the SMTP server.
Sender Email Address	Enter the email address of the sender of the outgoing email.
Sender	Enter the sender’s name of the outgoing email.
Security Type	Select the security protocol for the domain, None or SSL.
Encoding Type	Select the type of transfer encoding (UTF8 or ASCII) for SMTP communication.
Authentication	Select whether the SMTP server requires authentication. And enter the following information if authentication is used.
Username	Enter a username authorized to access the SMTP server.
Password	Enter a password for the username.

4. Click **Save**.

Once a mail server is configured, test the settings with the **Test Mail Server** function.

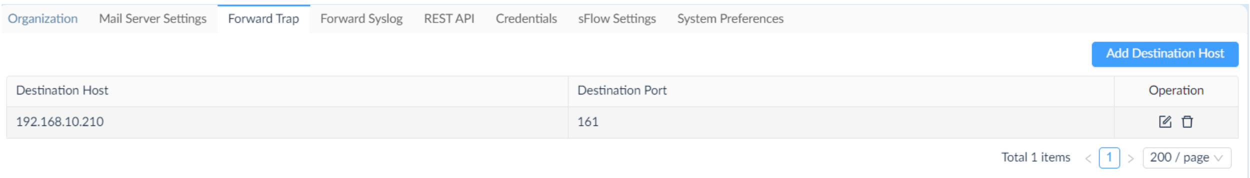
5. In the email address field, enter an email address to which the test email will be sent.
6. Click **Send Test Mail**.
7. Check the email account if the test email has been received.
8. If the email was not received, correct the mail server settings accordingly.

Set Up Forward Trap

D-View 8 provides SNMP trap forwarding with the Forward Trap function. The function allows you to forward traps to a specified server destination.

To configure Forward Trap:

1. Go to **System** > **Basic Settings**.
2. Click the **Forward Trap** tab to display the Forward Trap page.



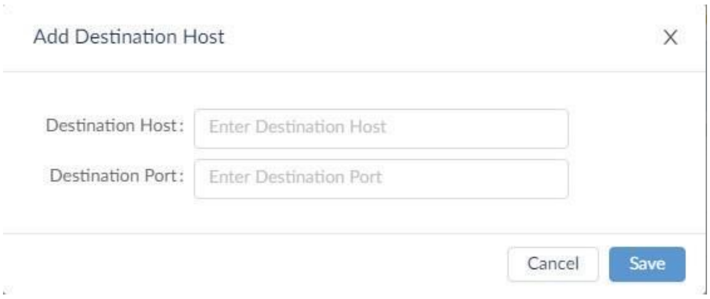
Destination Host	Destination Port	Operation
192.168.10.210	161	

3. Click **Add Destination Host**. Then enter the destination host (IPv4 or IPv6 address) and port to define the trap destination.
4. Click **Save**.

Set Up Forward Syslog

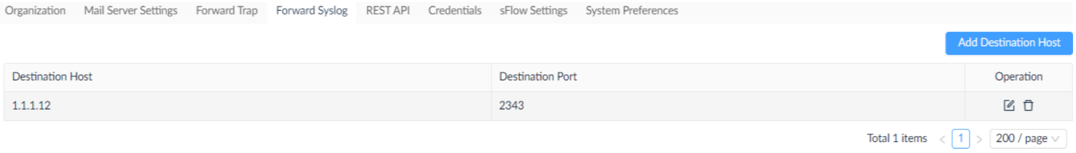
You can configure the system to send syslog messages to an external syslog server.

To configure Forward Syslog:



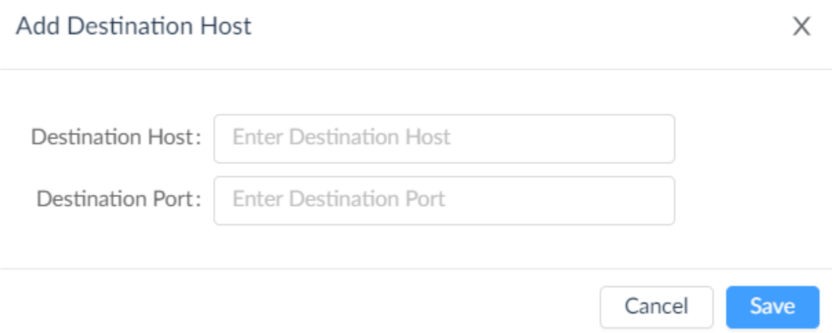
1. Go to **System > Basic Settings**.

2. Click the **Forward Syslog** tab to display the Forward Syslog page.



Destination Host	Destination Port	Operation
1.1.1.12	2343	

3. Click **Add Destination Host**. Then enter the destination host (IPv4 or IPv6 address) and port to define the syslog destination.



Add Destination Host

Destination Host: Enter Destination Host

Destination Port: Enter Destination Port

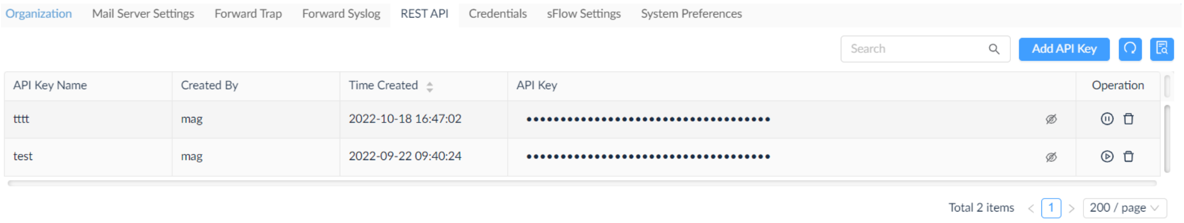
4. Click **Save**.

Generate REST API Key

REST API is only supported in the Enterprise version. REST API authentication uses HTTPS as the transport protocol for all REST API access. The authentication is required for third-party applications to access through APIs.

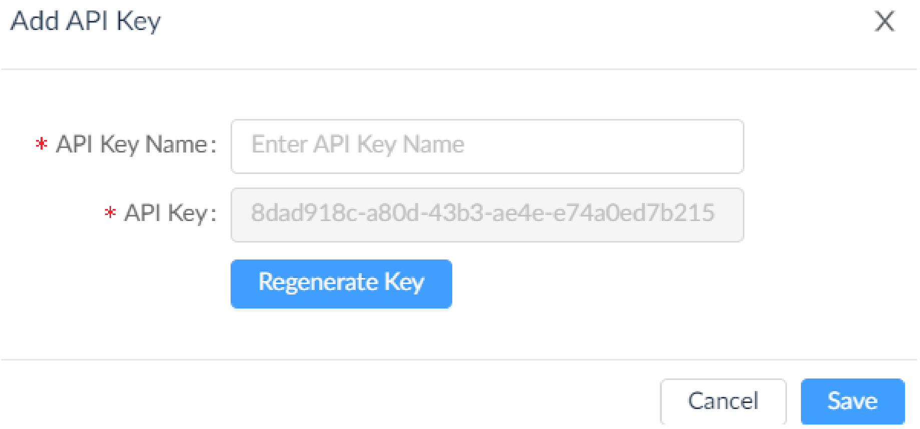
To configure REST API:

1. Go to **System** > **Basic Settings**.
2. Click the **REST API** tab to display the API Key.



API Key Name	Created By	Time Created	API Key	Operation
tttt	mag	2022-10-18 16:47:02	•••••••••••••••••••••••••••••••••••	
test	mag	2022-09-22 09:40:24	•••••••••••••••••••••••••••••••••••	

3. Click **Add API Key**. Then enter a name to identify the API key.



Add API Key

* API Key Name: Enter API Key Name

* API Key: 8dad918c-a80d-43b3-ae4e-e74a0ed7b215

4. Click **Regenerate Key** to create a new key.
5. Click **Save**.

Set Up Credentials

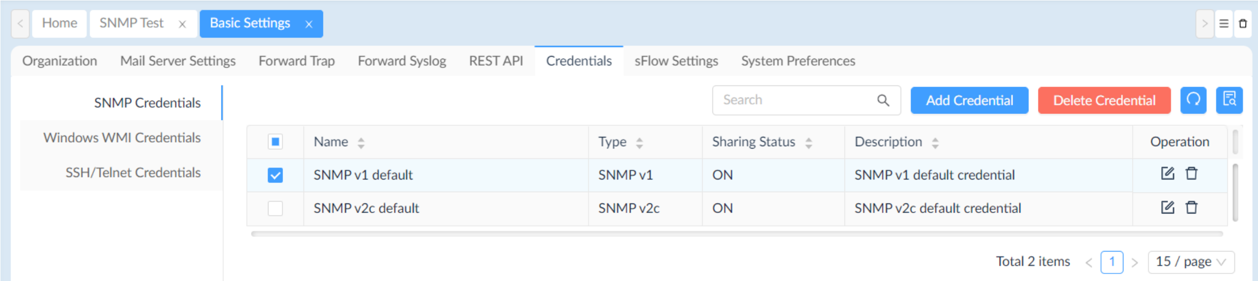
Set Up SNMP Credentials

The SNMP credentials manages access to SNMP-compatible devices. Storing the credentials is useful for when the system is scanning network devices in Network Discovery (go to **Monitoring > Network Discovery**). Refer to 4.1 Network Discovery for more information about Network Discovery.

To configure SNMP credentials:

1. Go to **System > Basic Settings** to display the Organization page.

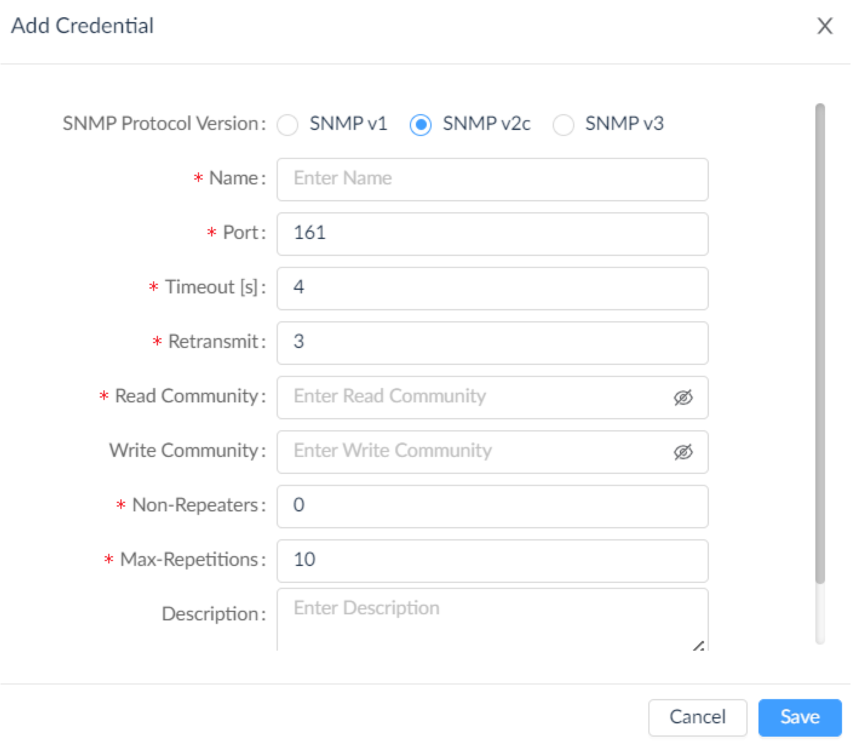
2. Click the **Credentials** tab and select **SNMP Credentials** from the left pane.



☐	Name	Type	Sharing Status	Description	Operation
☑	SNMP v1 default	SNMP v1	ON	SNMP v1 default credential	
☐	SNMP v2c default	SNMP v2c	ON	SNMP v2c default credential	

Total 2 items 1 15 / page

3. Click **Add Credential**.



SNMP Protocol Version: ○ SNMP v1 ● SNMP v2c ○ SNMP v3

* Name: Enter Name

* Port: 161

* Timeout [s]: 4

* Retransmit: 3

* Read Community: Enter Read Community

Write Community: Enter Write Community

* Non-Repeaters: 0

* Max-Repetitions: 10

Description: Enter Description

4. Select the SNMP version of the credential: SNMP v1, SNMP v2c, or SNMP v3. By default, D-View 8 uses SNMP v2c.

For SNMP v1:

- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retries (default: 3)
- Enter the read credential string (default: public).
- Enter the write credential string (default: private).
- Enter a description to help identify the profile (optional).
- Enable or disable **Sharing Status** to let other administrators with authorized role to view and edit this SNMP setting.

For SNMP v2c:

- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retires (default: 3)
- Enter the read credential string.
- Enter the write credential string.
- Enter the number of objects that can return in a single get-next instance (default: 0).
- Enter the number of Get Next operations to be performed on each variable (default: 10).
- Enter a description to help identify the profile (optional).
- Enable or disable **Sharing Status** to let other administrators with authorized role to view and edit this SNMP setting.

For SNMPv3:

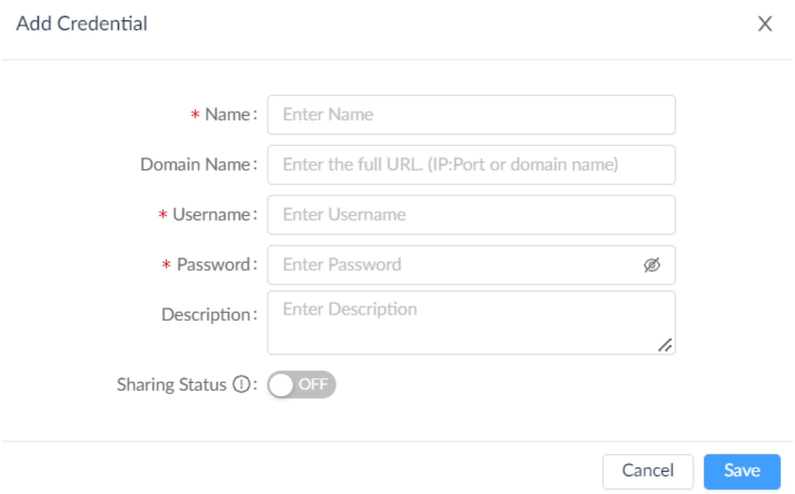
- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retries (default: 3)
- Enter the number of objects that can return in a single get-next instance (default: 0).
- Enter the number of Get Next operations to be performed on each variable (default: 10).
- Enter the Context Name (optional), which is used as the identifier for a named subset of the object instances.
- Select the Security Level:
    - authPriv: authentication and privacy (default).
    - authNoPriv: authentication, no privacy.
    - noAuthNoPriv: no authentication, no privacy.
- Select the Auth Protocol if authentication is used:
    - MD5 (MD5 message-digest algorithm): produces a 128-bit hash value to authenticate users.
    - SHA (Secure Hash Algorithm): produces a 160-bit has value to authenticate users.
- Enter the Authentication Password to be used with the Authentication Protocol.
- Select the Privacy Protocol if privacy is used:
    - DES (Data Encryption Standard) or AES (Advanced Encryption Standard) for data encryption.
- Enter the Privacy Password to be used with the Privacy Protocol.
- Enter a description to help identify the profile (optional).

6. Enable or disable **Sharing Status** to share the credentials with other administrators with authorized role.
7. Click **Save**.

Set Up Windows WMI Credentials

Windows Management Instrumentation (WMI) is used in Microsoft Windows systems to help retrieve information on a remote system and it requires appropriate permissions. Storing the credentials is useful when discovering network devices in Network Discovery (go to **Monitoring > Network Discovery**).

Enter the following to add a WMI credential profile:


Add Credential
X
* Name : Enter Name
Domain Name : Enter the full URL. (IP:Port or domain name)
* Username : Enter Username
* Password : Enter Password
Description : Enter Description
Sharing Status ⓘ : OFF
Cancel
Save

Name: Enter a name for this profile.

Domain Name: Enter the windows domain name.

Username: Enter the username with the Windows system administrator privilege or a user account with permissions to access WMI data.

Password: Enter a password for the above user account.

Description: Enter a description to help identify this profile.

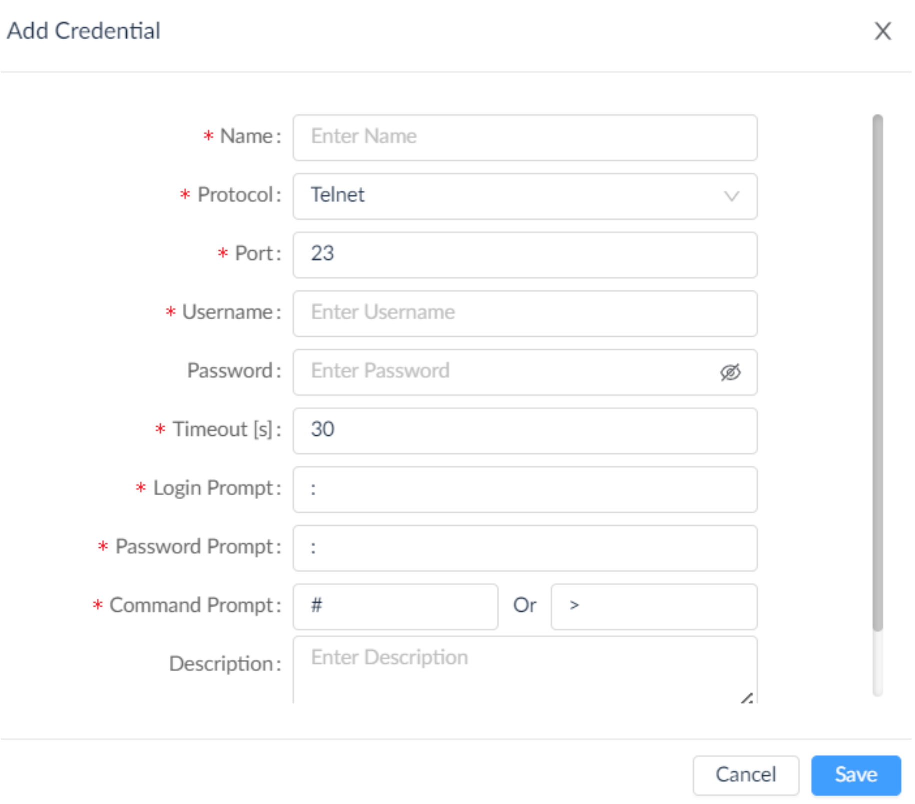
Sharing Status: Select whether other administrators with authorized role in the organization can view or modify this profile.

Set Up SSH/Telnet Credentials

SSH and Telnet allows remote administration of a D-View 8 server and it requires configuration of communication port and access privileges.

Note: This function is not applicable in this release and will be fixed in the future release.

Enter the following to add an SSH/Telnet credential profile:



Add Credential

* Name: Enter Name

* Protocol: Telnet

* Port: 23

* Username: Enter Username

Password: Enter Password

* Timeout [s]: 30

* Login Prompt: :

* Password Prompt: :

* Command Prompt: # Or >

Description: Enter Description

Name: Enter a name for the profile.

Protocol: select the communication protocol for remote management: SSH or Telnet.

Port: select the associate port for the above protocol.

Username/Password: Enter the username and password that will be required to access the server.

Timeout: enter the session timeout value.

Login Prompt: enter the prompt to be displayed for login.

Password Prompt: enter the prompt to be displayed at the command line for entering password**.**

Command Prompt: Enter the prompt to be displayed at the command line for entering command.

Description: Enter a description to identify this profile.

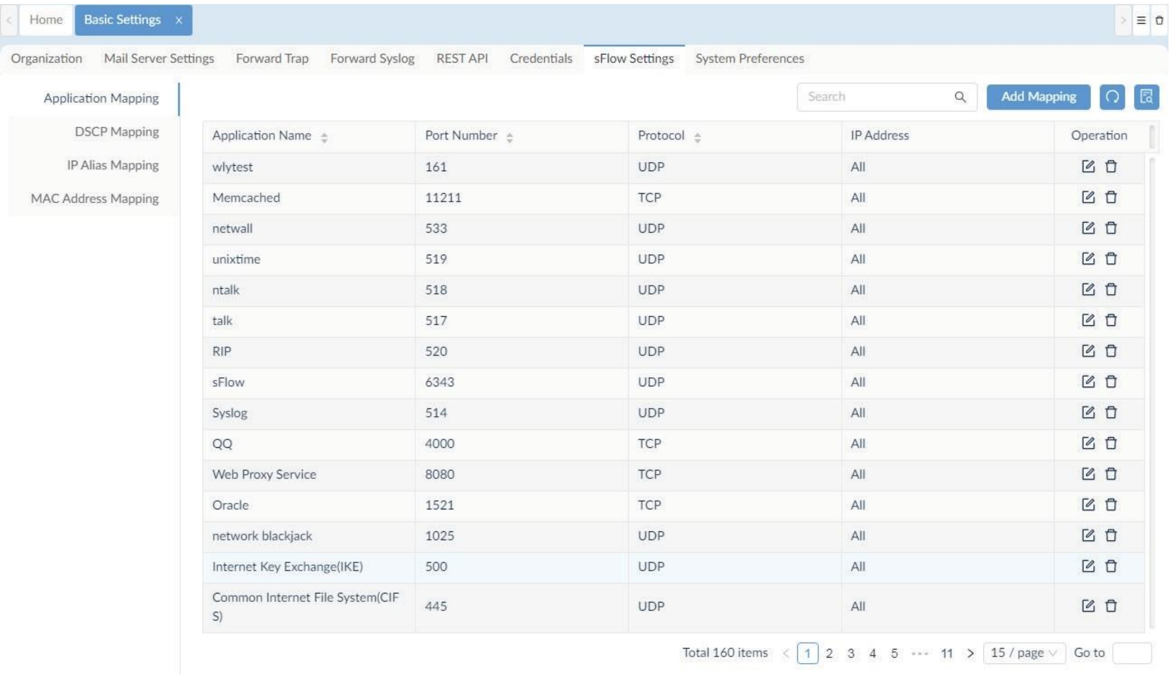
Sharing Status: Select whether other administrators with authorized role in your organization can view or modify this profile.

Set Up sFlow Settings

Effective management of applications and the network resources is one of the benefits of adopting the sFlow standard through D-View 8. These settings will help you observe traffic from sampled packets matched with the mapped applications or DSCP names in sFlow Analyzer (go to **Monitoring > sFlow Analyzer**). Note that the configuration of application mappings for sFlow Analyzer is only supported in Enterprise version.

To view and configure sFlow Settings:

1. Go to **System > Basic Settings**.
2. Click the **sFlow Settings** tab to display the sFlow Settings page.



Application Name	Port Number	Protocol	IP Address	Operation
wlytest	161	UDP	All	✎ 🗑
Memcached	11211	TCP	All	✎ 🗑
netwall	533	UDP	All	✎ 🗑
unixtime	519	UDP	All	✎ 🗑
ntalk	518	UDP	All	✎ 🗑
talk	517	UDP	All	✎ 🗑
RIP	520	UDP	All	✎ 🗑
sFlow	6343	UDP	All	✎ 🗑
Syslog	514	UDP	All	✎ 🗑
QQ	4000	TCP	All	✎ 🗑
Web Proxy Service	8080	TCP	All	✎ 🗑
Oracle	1521	TCP	All	✎ 🗑
network blackjack	1025	UDP	All	✎ 🗑
Internet Key Exchange(IKE)	500	UDP	All	✎ 🗑
Common Internet File System(CIFS)	445	UDP	All	✎ 🗑

Total 160 items < 1 2 3 4 5 ··· 11 > 15 / page Go to

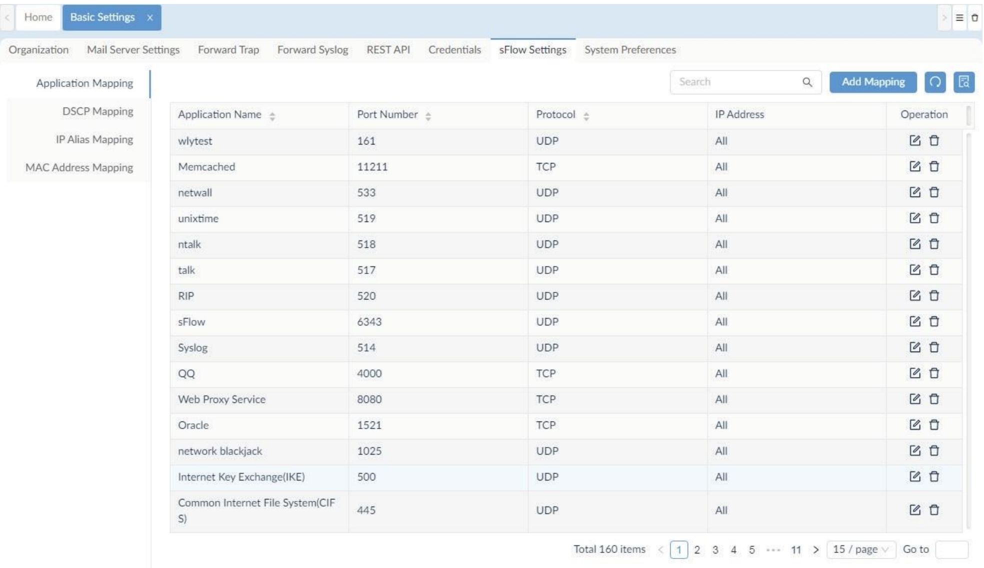
From sFlow Settings, the following mapping options are available:

- Application Mapping
- DSCP Mapping
- IP Alias Mapping
- MAC Address Mapping

Application Mapping

To add an application to be identified properly from the collected data:

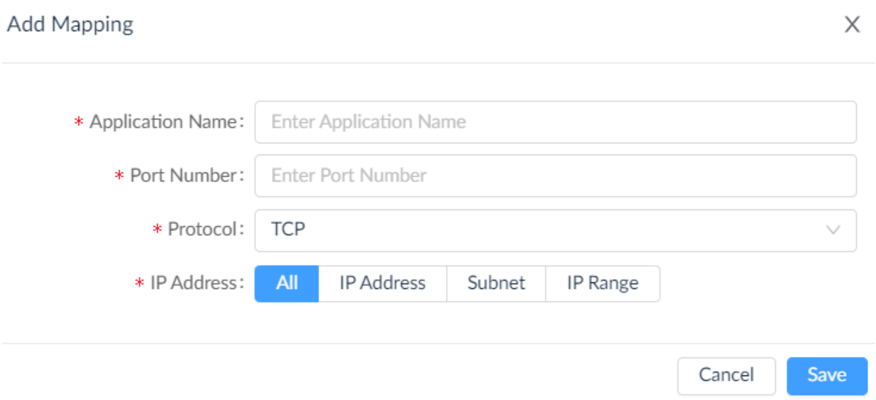
1. Go to **System > Basic Settings**.
2. Click the **sFlow Settings** tab to display the sFlow Settings page.
3. Click the **Application Mapping** tab.



Application Name	Port Number	Protocol	IP Address	Operation
wlytest	161	UDP	All	✎ 🗑
Memcached	11211	TCP	All	✎ 🗑
netwall	533	UDP	All	✎ 🗑
unixtime	519	UDP	All	✎ 🗑
ntalk	518	UDP	All	✎ 🗑
talk	517	UDP	All	✎ 🗑
RIP	520	UDP	All	✎ 🗑
sFlow	6343	UDP	All	✎ 🗑
Syslog	514	UDP	All	✎ 🗑
QQ	4000	TCP	All	✎ 🗑
Web Proxy Service	8080	TCP	All	✎ 🗑
Oracle	1521	TCP	All	✎ 🗑
network blackjack	1025	UDP	All	✎ 🗑
Internet Key Exchange(IKE)	500	UDP	All	✎ 🗑
Common Internet File System(CIFS)	445	UDP	All	✎ 🗑

Total 160 items < 1 2 3 4 5 ··· 11 > 15 / page Go to

4. Click **Add Mapping** at the upper right. Then enter the application name and its associated port.



Add Mapping

* Application Name: Enter Application Name

* Port Number: Enter Port Number

* Protocol: TCP

* IP Address: All | IP Address | Subnet | IP Range

5. In the **Protocol/Port Number** field, click the drop-down menu to select TCP or UDP and enter port number for the protocol.

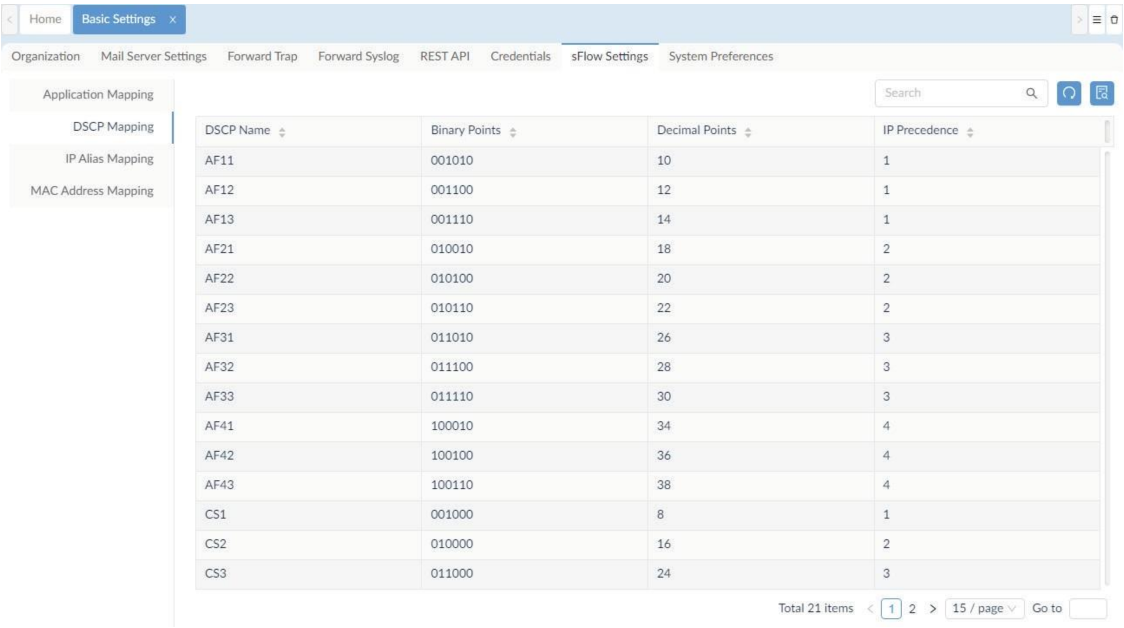
6. In the **IP Address** field, select All, IP Address, Subnet, or IP Range to specify the address range in the flow data.

7. Click **Save** to create the application mapping rule or **Cancel** to return to the previous menu.

DSCP Mapping

To view defined DSCP (Differentiated Services Code Point) sFlow mapping used for QoS:

1. Go to **System > Basic Settings**.
2. Click the **sFlow Settings** tab to display the sFlow Settings page.
3. Click the **DSCP Mapping** tab to obtain DSCP names and its mapped values.

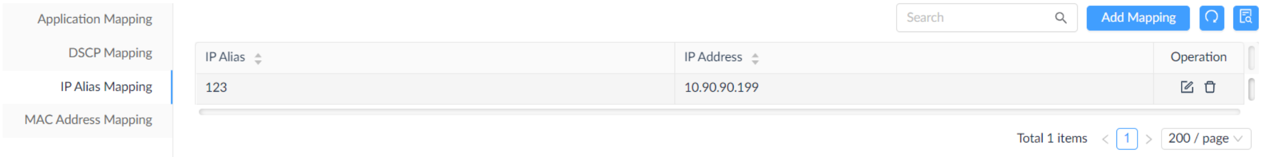


DSCP Name	Binary Points	Decimal Points	IP Precedence
AF11	001010	10	1
AF12	001100	12	1
AF13	001110	14	1
AF21	010010	18	2
AF22	010100	20	2
AF23	010110	22	2
AF31	011010	26	3
AF32	011100	28	3
AF33	011110	30	3
AF41	100010	34	4
AF42	100100	36	4
AF43	100110	38	4
CS1	001000	8	1
CS2	010000	16	2
CS3	011000	24	3

IP Alias Mapping

To add an IP address to be identified with the defined name from the collected data::

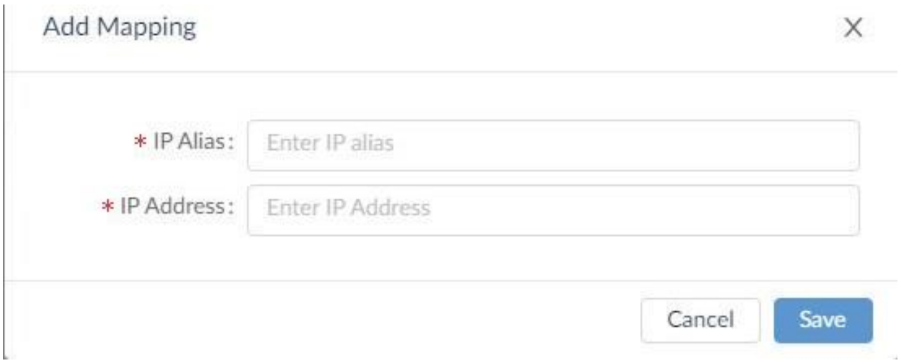
1. Go to **System > Basic Settings**.
2. Click the **sFlow Settings** tab to display the sFlow Settings page.
3. Click the **IP Alias Mapping tab** to display the IP Alias Mapping page.



IP Alias	IP Address	Operation
123	10.90.90.199	

Total 1 items < 1 > 200 / page

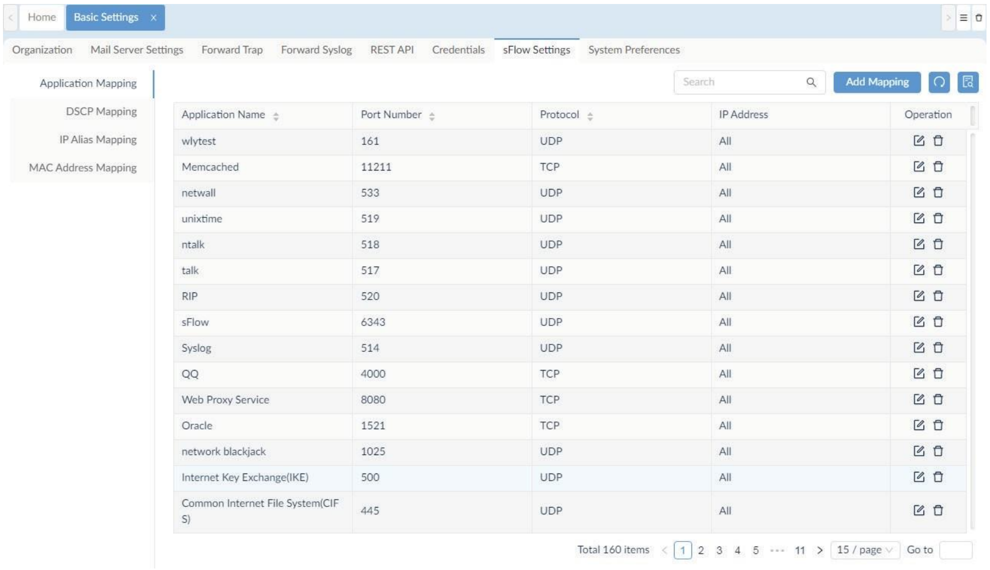
4. Click **Add Mapping** at the upper right.
5. Enter the IP Alias and IP address to define the mapping of an alias and IP address for flow data.
6. Click **Save** to create the IP address mapping rule or **Cancel** to return to the previous menu.



MAC Address Mapping

To add a MAC address to be identified with the defined name from the collected data:

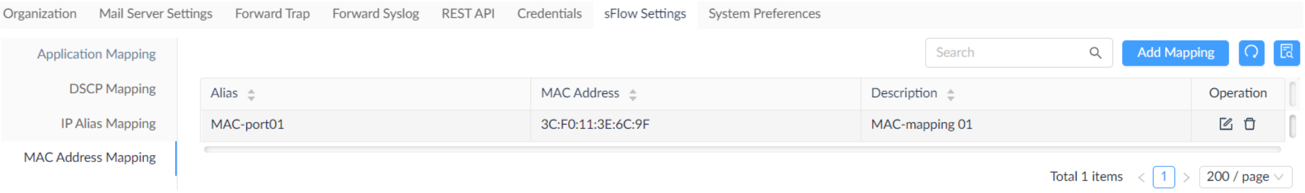
1. Go to **System > Basic Settings**.
2. Click the **sFlow Settings** tab to display the sFlow Settings page.



Application Name	Port Number	Protocol	IP Address	Operation
wlytest	161	UDP	All	
Memcached	11211	TCP	All	
netwall	533	UDP	All	
unixtime	519	UDP	All	
ntalk	518	UDP	All	
talk	517	UDP	All	
RIP	520	UDP	All	
sFlow	6343	UDP	All	
Syslog	514	UDP	All	
QQ	4000	TCP	All	
Web Proxy Service	8080	TCP	All	
Oracle	1521	TCP	All	
network blackjack	1025	UDP	All	
Internet Key Exchange(IKE)	500	UDP	All	
Common Internet File System(CIFS)	445	UDP	All	

Total 160 items < 1 2 3 4 5 ··· 11 > 15 / page Go to

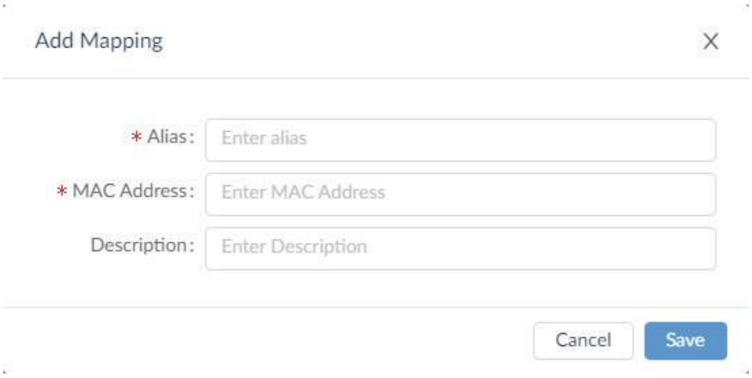
3. Click the **MAC Address Mapping** tab.



Alias	MAC Address	Description	Operation
MAC-port01	3C:F0:11:3E:6C:9F	MAC-mapping 01	

Total 1 items < 1 > 200 / page

4. Click **Add Mapping** at the upper right.



* Alias: Enter alias

* MAC Address: Enter MAC Address

Description: Enter Description

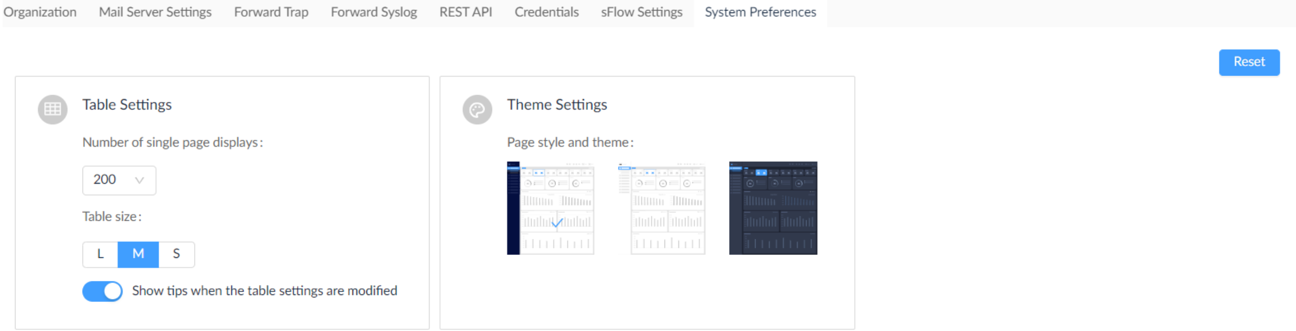
5. Enter Alias and MAC address to define the mapping of an alias and a MAC address.
6. Click **Save** to create the MAC Address mapping rule or **Cancel** to return to the previous menu.

Set Up System Preferences

Theme settings for the overall layout of the interface are configured through System Preferences. You can configure Table and Theme settings to set specific page styles.

To configure System Preferences:

1. Go to **System > Basic Settings**.
2. Click the **System Preferences** tab to display the System Preferences page.



Number of single page displays: 200

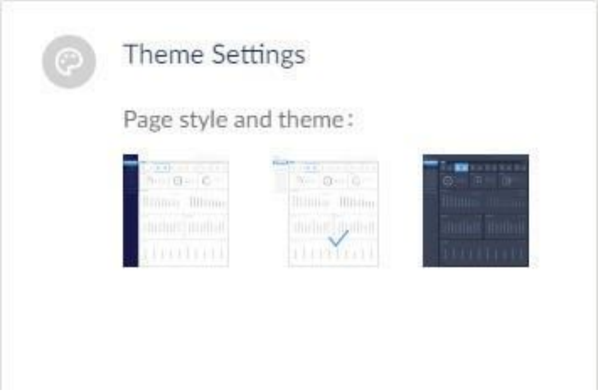
Table size: M

Show tips when the table settings are modified

Page style and theme:

3. Click the drop-down menu to select the number of single page display (rows) for all tables in D-View 8: 15 (default), 50, 100, or 200.
4. From the table size selector, set the size for all the tables in D-View 8: Large, Middle (default), or Small.
5. Enable the option: Show tips when the table settings are modified so that users will be notified of table setting changes via toast messages.

In **Theme Settings**, select a defined theme to apply to the interface. You can select a dark or light background or dark side pane with light background.



Theme Settings

Page style and theme:

To reset to the original settings, click the **Reset** button. All table and theme settings will be restored to the default.

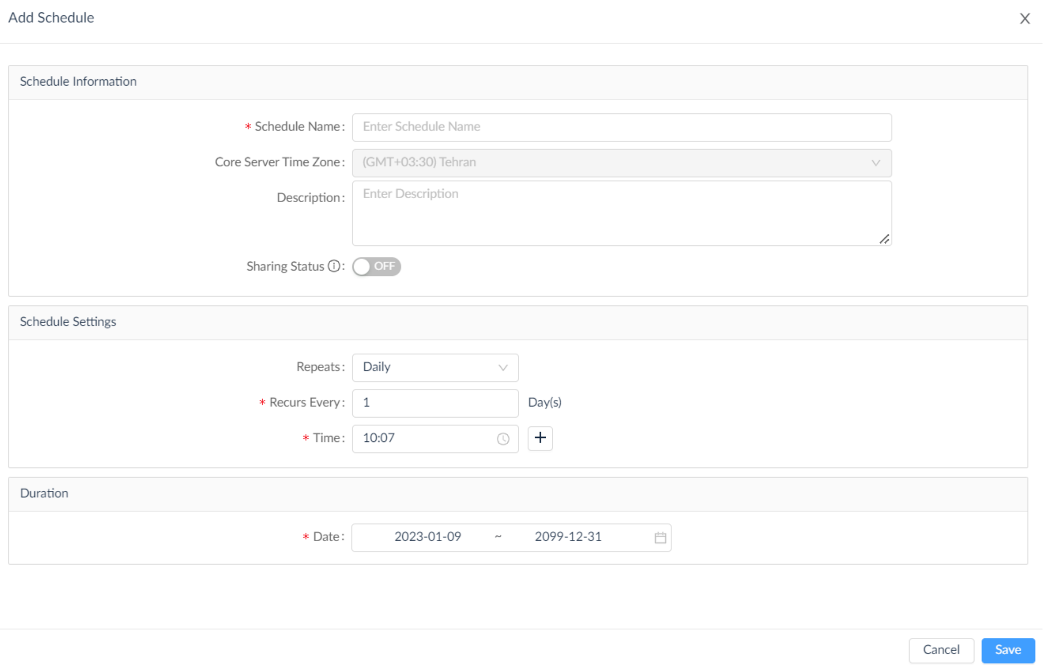
14.2 Scheduling

The scheduling function helps automate several functions periodically according to a defined recurrent frequency in the designated time span.

There are two types of scheduling options: Recurrent and Time-Range. The recurrent schedule can be assigned to network discovery, tasks, configuration backup and restore, and scheduled reports, whereas the time-range schedule can be assigned to alarm settings and notification rules.

To set a recurrent schedule:

1. Go to **System > Scheduling** and select the **Recurrent Schedule List** tab.
2. Click **Add Schedule** at the upper right. Then enter the following information:



Add Schedule

Schedule Information

* Schedule Name: Enter Schedule Name

Core Server Time Zone: (GMT+03:30) Tehran

Description: Enter Description

Sharing Status ⓘ: OFF

Schedule Settings

Repeats: Daily

* Recurs Every: 1 Day(s)

* Time: 10:07 +

Duration

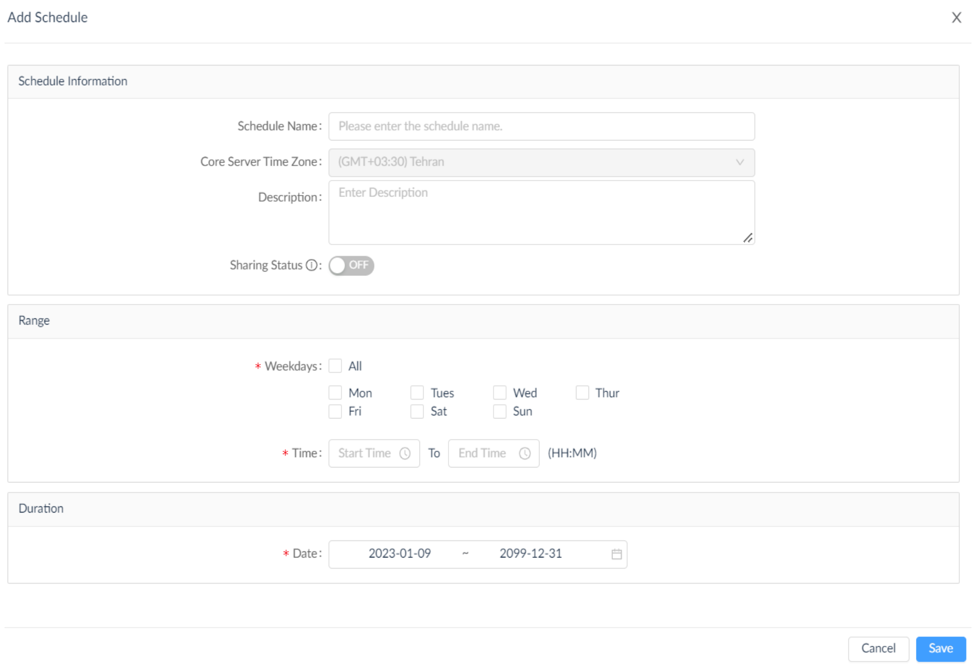
* Date: 2023-01-09 ~ 2099-12-31

Item	Description
Schedule Information	
Schedule Name	Enter a name for the schedule.
Core Server Time Zone	Select the time zone. (It can already be set in the Organization tab.)
Description	Enter a brief description for the schedule.
Sharing Status	Enable sharing to let other administrators with the authorized role to modify or view this schedule.
Schedule Settings	
Repeats	Select the frequency: Daily, Weekly, Monthly, or Specific Days.
Recurs Every	Specific Days: Schedule a single time or multiple times at a specified date(s)/time(s). Selecting multiple times will enable execution of the same task at different times for each date. Daily: Schedule a specified time of the day. Then choose daily interval between executions: 1 to execute the task every day, 2 to execute the task every other day, and so on. Weekly: Schedule a specified time of a designated weekday or weekdays. Then choose weekly interval between executions: 1 to execute the task every week, 2 to execute the job every other week, and so on. Monthly: Schedule a specified time on day(s) of the selected month(s): specify a month or months: Jan to Dec and the days of the month. Specific Days: Schedule a specified time and date(s).
Time	Select the time (24-hour clock): hh:mm for the schedule. Selecting multiple times will enable execution of the same task at different times of the same day.

Duration	Select the start and end dates to designate the effective time span.

To set a time-range schedule:

1. Go to **System > Scheduling** and select the **Time Range Schedule List** tab.
2. Click **Add Schedule** at the upper right. Then enter the following information:



Add Schedule X

Schedule Information

Schedule Name: Please enter the schedule name.

Core Server Time Zone: (GMT+03:30) Tehran

Description: Enter Description

Sharing Status ⓘ: OFF

Range

* Weekdays: □ All

□ Mon □ Tues □ Wed □ Thur
□ Fri □ Sat □ Sun

* Time: Start Time To End Time (HH:MM)

Duration

* Date: 2023-01-09 ~ 2099-12-31

Cancel Save

Item	**Description**
Schedule Information	
Schedule Name	Enter a name for the schedule.
Core Server Time Zone	Select the time zone. (It can already be set in the Organization tab.)
Description	Enter a brief description for the schedule.
Sharing Status	Enable sharing to let other administrators with the authorized role to modify or view this schedule.
Range	
Weekdays	Select all weekdays or a specific weekday(s).
Time (range)	Select the start and end time (24-hour clock): hh:mm for the schedule.
Duration	Select the start and end dates to designate the effective time span.

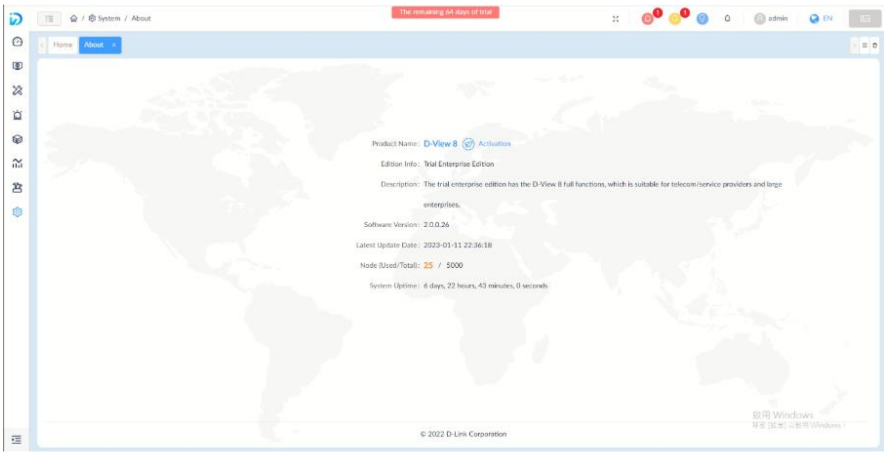
14.3 Licenses

Product registration and license expiration information can be obtained in the **About** page.

Note: Only Super Administrators can view the License page.

To obtain product information:

Go to **System > About**.



Product Name: D-View 8 Activation
Edition Info: Trial Enterprise Edition
Description: The trial enterprise edition has the D-View 8 full functions, which is suitable for telecom/service providers and large enterprises.
Software Version: 2.0.0.26
Latest Update Date: 2023-01-11 22:36:18
Node (Used/Total): 25 / 5000
System Uptime: 6 days, 22 hours, 43 minutes, 0 seconds

© 2022 D-Link Corporation

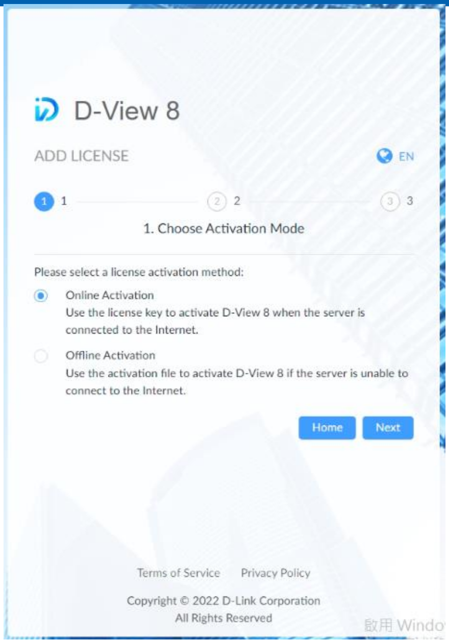
Product and software information is displayed:

Product Name	D-View 8, which indicates the name of the product.
Edition Info	The Standard or Enterprise Edition.
Description	A brief description of the product.
Software Version	The version of the current system software.
Latest Update Date	The date that the system was last updated.
Node (**Used/Total**)	The number of currently managed nodes/the total nodes allowed
System Uptime	The total number of days, hours, minutes and seconds that the system has been up and running.

The system will prompt you to activate your product with a valid license after the 3-month trial period.

To add a product key:

1. Click the **Activation** link next to D-View 8 displayed as the product name on the **About** page. And you will be directed to the login page to start the product activation process.
2. The **Add License** screen appears. Choose one of the following methods:



D-View 8

ADD LICENSE

1. Choose Activation Mode

Please select a license activation method:

● Online Activation
Use the license key to activate D-View 8 when the server is connected to the Internet.

○ Offline Activation
Use the activation file to activate D-View 8 if the server is unable to connect to the Internet.

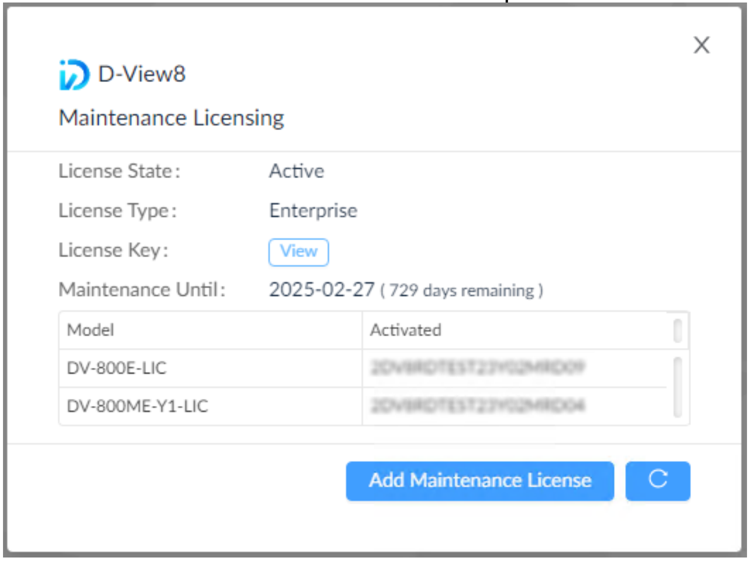
Copyright © 2022 D-Link Corporation
All Rights Reserved

- **Online Activation:** Use a license key to activate D-View 8. The server must be connected to the Internet. Click **Next** to continue and follow the on-screen procedure to complete the process. This method allows you to enter a license key obtained from your sales representative.
- **Offline Activation:** Use an activation file to activate D-View 8. The server does not have to be connected to the Internet. This method allows you to upload an activation file generated from an activation tool.

  The offline activation requires the use of an activation tool. Double-click on the executable file to start the program. Select **Standard/Enterprise License** from the License Type drop-down list. Enter the **License Key** (obtained from your sales representative) and the MAC address of the D-View 8 server for **Bound MAC** (the license key associates itself with the server's hardware), then click **Browse** to locate the output directory for the activation file. Click **Generate** to generate an activation.

To obtain product licenses information:

1. Click the **Maintenance License** link to view product and maintenance licenses information:



D-View8

Maintenance Licensing

License State: Active

License Type: Enterprise

License Key: View

Maintenance Until: 2025-02-27 (729 days remaining)

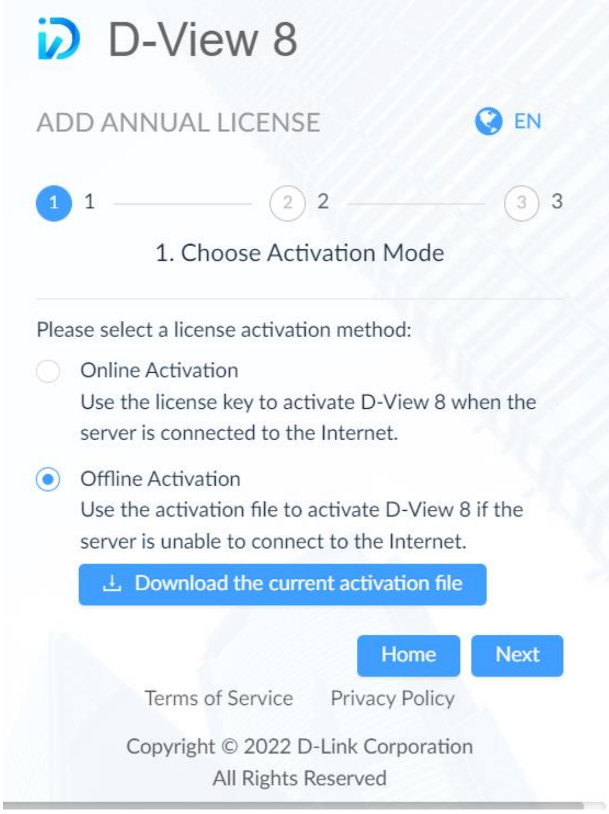
Model	Activated
DV-800E-LIC	[redacted]
DV-800ME-Y1-LIC	[redacted]

Item	Description
License State	Displays active or inactive status of the product license
License Type	The Standard or Enterprise license type.
License Key	Click to view the license keys purchased.
Maintenance Until	The number of days before the license expires. This can be an aggregated number of days of all licenses purchased.

The system will prompt you to buy a new maintenance license after the 1st year of product activation.

To add a maintenance license:

1. Click **Add Maintenance license**. And you will be directed to the login page to start the license purchasing process:
2. The **Add Annual License** screen appears. Choose one of the following methods:



D-View 8

ADD ANNUAL LICENSE

1. Choose Activation Mode

Please select a license activation method:

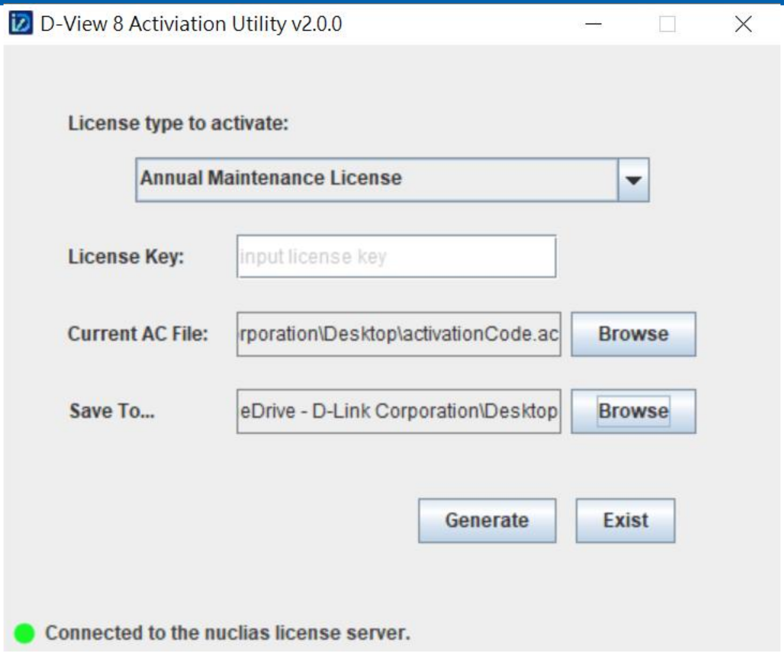
○ Online Activation
Use the license key to activate D-View 8 when the server is connected to the Internet.

● Offline Activation
Use the activation file to activate D-View 8 if the server is unable to connect to the Internet.

Copyright © 2022 D-Link Corporation
All Rights Reserved

- **Online Activation:** Use a license key to reactivate D-View 8 with maintenance service. The server must be connected to the Internet. Click **Next** to continue and follow the on-screen procedure to complete the process. This method allows you to enter a license key obtained from your sales representative.
- **Offline Activation:** Use an activation file to reactivate D-View 8 with maintenance service. The server does not have to be connected to the Internet. Click **Download the current activation file** to download the activation file to generate a reactivation file.

  The offline reactivation requires the use of an activation tool. Double-click on the executable file to start the program. Select **Annual Maintenance License** from the License Type drop-down list. Enter the **License Key** obtained from your sales representative and click **Browse** to locate the current AC file downloaded from the above step. Then click **Generate** to generate a new activation file.



D-View 8 Activiation Utility v2.0.0

License type to activate: Annual Maintenance License

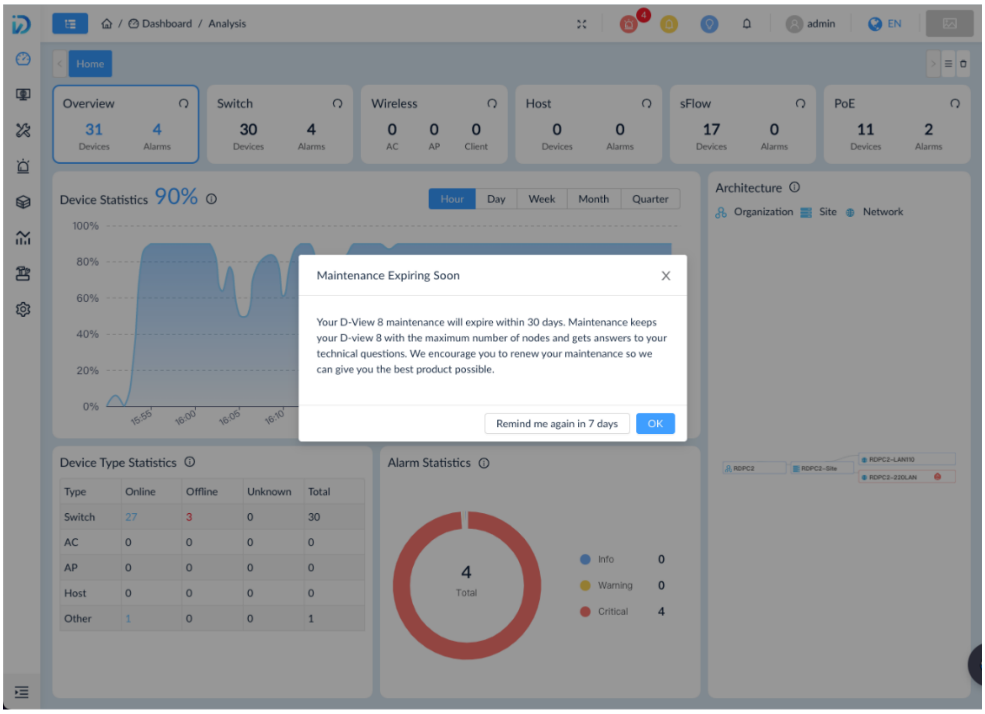
License Key: input license key

Current AC File: rporation\Desktop\activationCode.ac

Save To... eDrive - D-Link Corporation\Desktop

Connected to the nuclias license server.

Note: When the maintenance license is about to expire, the system will inform you of the soon-to-expired license 30 days before the expiration date.



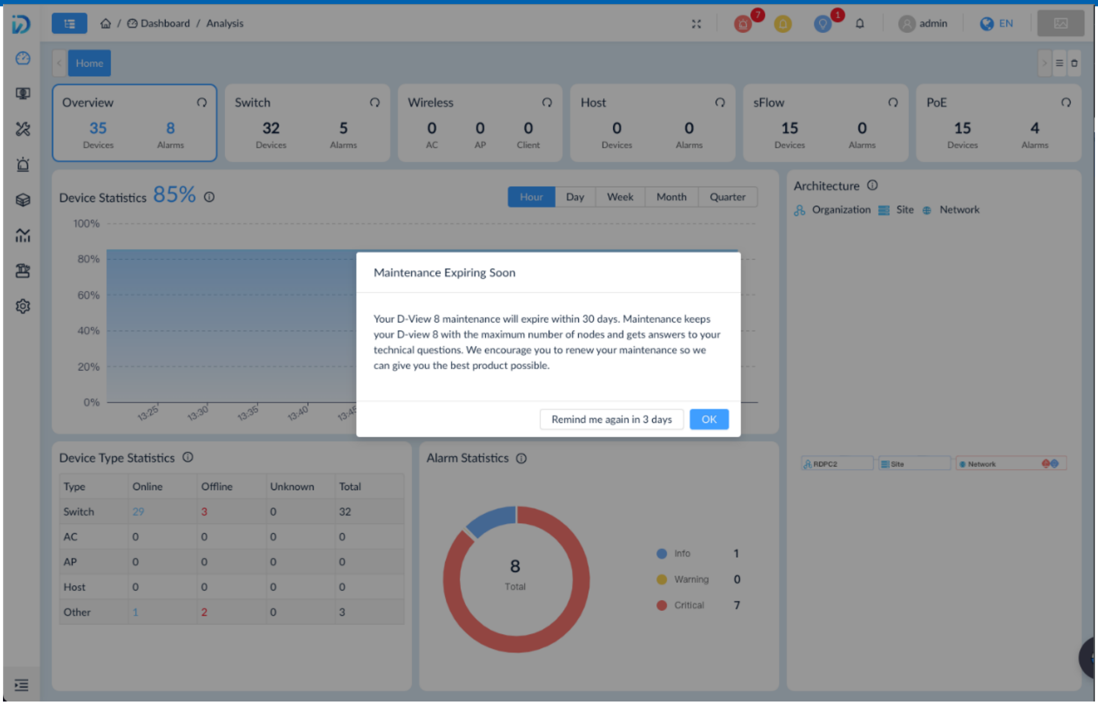
Maintenance Expiring Soon

Your D-View 8 maintenance will expire within 30 days. Maintenance keeps your D-view 8 with the maximum number of nodes and gets answers to your technical questions. We encourage you to renew your maintenance so we can give you the best product possible.

Device Type Statistics

Type	Online	Offline	Unknown	Total
Switch	27	3	0	30
AC	0	0	0	0
AP	0	0	0	0
Host	0	0	0	0
Other	1	0	0	1

You can opt to be reminded again 7 days before the expiration date. The system will notify you at the appropriate time as shown in the following screen. You can then choose to be reminded again 3 days before the expiration date.



Maintenance Expiring Soon

Your D-View 8 maintenance will expire within 30 days. Maintenance keeps your D-view 8 with the maximum number of nodes and gets answers to your technical questions. We encourage you to renew your maintenance so we can give you the best product possible.

Remind me again in 3 days | OK

Device Type Statistics

Type	Online	Offline	Unknown	Total
Switch	29	3	0	32
AC	0	0	0	0
AP	0	0	0	0
Host	0	0	0	0
Other	1	2	0	3

When the maintenance license expired, the system will alert you and the following pages of the D-View 8 web application will display alert messages: **Dashboard > Analysis**, **Monitoring > Device View**, **Monitoring > Topology Map, Configuration > Bach Configuration**, **Configuration> Firmware Management**, and **Configuration > Configuration Management**.

14.4 View D-View 8 Logs

The D-View 8 Log page displays different types of logs. The User Operation Log tab displays logs related to management operations and tasks performed by users. The System Log displays logs related to activities related to system services and probe agents. The Device Maintenance Log displays logs related to operations performed by users on the managed devices. Logs can be used to analyze device health and troubleshoot network connectivity as well as exam network security. Note that the D-View 8 logs are different from the device syslog, which are logs generated by managed devices (go to **Alarm & Notification > Trap & Syslog**).

Note: You can only view logs pertaining to the activities under your authorized level of network hierarchy.

To view user operation logs, go to **System > D-View 8 Log**. Click the **User Operation Log** tab. The log entries contain the following information:

Item	**Description**
Log Time	The timestamp of the user activity.
Terminal Type	The device and interface used to connect with the D-View 8 server.
User	Username
Operation Object	The object/menu category that the user operated on.
Detail	The detailed activity of the operation.

To view system logs, go to **System > D-View 8 Log**. Click the **System Log** tab. The log entries contain the following information:

Item	**Description**
Log Time	The timestamp of the system activity.
Log Type	A brief description of server activity.
Server	The affected server and IP address.
Detail	The detailed information of the server activity.

To view device maintenance logs, go to **System > D-View 8 Log**. Click the **Device Maintenance Log** tab. The log entries contain the following information:

Item	**Description**
Log Time	The timestamp of the device operation activity.
Result	The result of the device operation.
Configuration Type	The configuration category of the operation.
Function	The detailed information of the configuration.
System Name	The system name of the device.
Model Name	The model name of the device.
IP	The IP address of the device.
User	The username of the operator.
Site	The network site of the device.
Network	The network of the device.

You can filter these logs by time or activity. To create a filter, click **Advanced Query** at the top right. It allows you to specify the activity with timestamp of the log, function, configuration type, system name, IP address, username, etc. After the displayed records are refined according to the desired criteria, you can export it as a csv file.

15 Tools

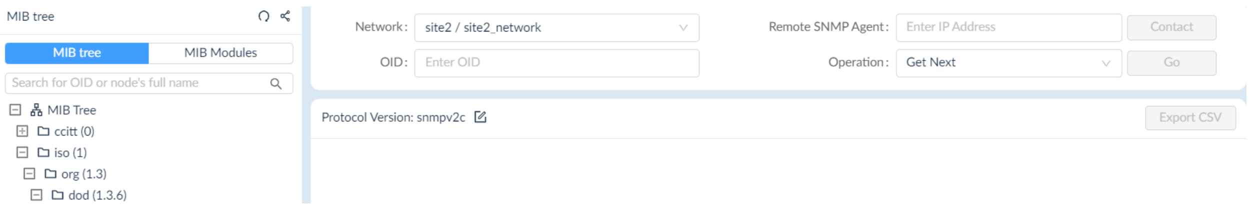
The D-View 8 has added management effectiveness of your network by offering convenient tools. These tools help troubleshoot network bottlenecks by providing transmission data and responses from nodes where the packets pass.

15.1 MIB Browser

The MIB browser allows you to retrieve SNMP information from supported devices. By polling SNMP-enabled devices, you can obtain device information in readable format with the OID search function. Note that MIB Browser is only supported in Enterprise version.

To select a MIB object and collect SNMP data:

1. Go to **Tools > MIB Browser** to display the MIB Browser page.



Network: site2 / site2_network

Operation: Get Next

Protocol Version: snmpv2c

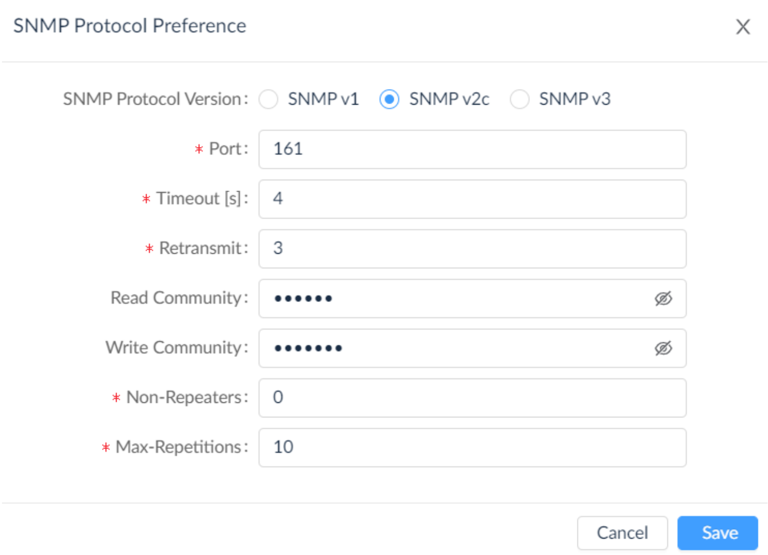
-

2. Enter SNMP connection parameters:
   - Click the drop-down menu to select the network.
   - Select from the list of managed devices or enter a remote SNMP agent address.
3. Click **Contact** to initiate a connection with a remote SNMP agent.
4. In the MIB tree pane, search for a specific OID by using one of the following methods:
   - Click the MIB tree tab, which contains MIB modules and objects in the hierarchical name space structure, to select a specific object or search for an OID or a node name.
   - Click MIB Modules to select a specific MIB module and node entry or use the search function to search for a MIB module. You can upload and compile your MIB file if it is not in the list (go to **Tools > MIB Compiler)**.
   - Click the drop-down menu to select an SNMP function:
     - Get (request) to retrieve a value
     - Get Next (request) to retrieve variables sequentially in a table
     - Get Bulk (request) to fill the response with up to the max-repetition number defined for Get Next requests
     - Walk to perform a sequence of SNMP Get Next operation
     - Table View for tabular objects
     - Instance View to display multiple related object instances
     - Set to set a value for an OID.
5. Click Go to start searching the specified object.

After a successful connection, the details for the objects will be displayed.

6. You can download the MIB data to a folder on your desktop in CSV file format. Click **Export CSV** to download.

The SNMP credentials for accessing an OID information can be modified by clicking the SNMP Protocol Preference Edit button ✎ at the top of the result pane.



SNMP Protocol Preference

SNMP Protocol Version: ○ SNMP v1 ● SNMP v2c ○ SNMP v3

* Port: 161

* Timeout [s]: 4

* Retransmit: 3

Read Community: ••••••

Write Community: •••••••

* Non-Repeaters: 0

* Max-Repetitions: 10

15.2 MIB Compiler Tool

The MIB Compiler Tool is only supported in the Enterprise version. The compiler extends the management capability to any SNMP-capable devices. It allows you to add SNMP objects to be discovered and queried in the MIB tree. The MIB Compiler only works with standard or proprietary MIBs but does not accept malformed MIBs.

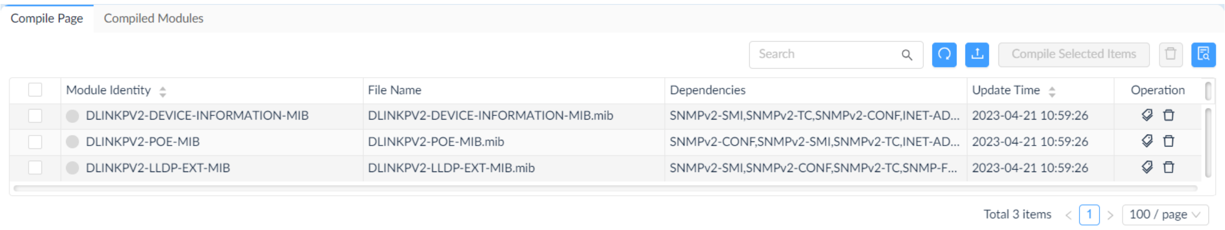
The compiled MIB module can then be loaded and managed in the MIB browser.

Add MIB Files

You can upload MIB files into the MIB browser.

To add MIB files:

1. Go to **Tools > MIB Compiler**.

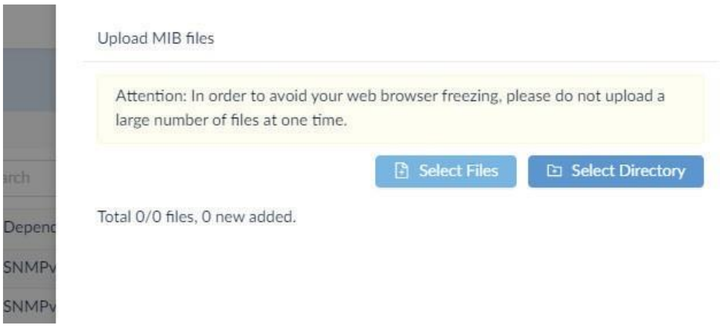


□	Module Identity	File Name	Dependencies	Update Time	Operation
□	DLINKPV2-DEVICE-INFORMATION-MIB	DLINKPV2-DEVICE-INFORMATION-MIB.mib	SNMPv2-SMI,SNMPv2-TC,SNMPv2-CONF,INET-AD...	2023-04-21 10:59:26	
□	DLINKPV2-POE-MIB	DLINKPV2-POE-MIB.mib	SNMPv2-CONF,SNMPv2-SMI,SNMPv2-TC,INET-AD...	2023-04-21 10:59:26	
□	DLINKPV2-LLDP-EXT-MIB	DLINKPV2-LLDP-EXT-MIB.mib	SNMPv2-SMI,SNMPv2-CONF,SNMPv2-TC,SNMP-F...	2023-04-21 10:59:26	

Total 3 items < 1 > 100 / page

2. On the **Compile Page** tab, click Upload MIB files to select a file(s) to upload.

3. The Upload MIB files page displays. Click **Select Files** to upload MIB files or click **Select Directory** to select all the files under the selected folder.



Attention: In order to avoid your web browser freezing, please do not upload a large number of files at one time.

Total 0/0 files, 0 new added.

4. The selection is detailed to show the upload status.

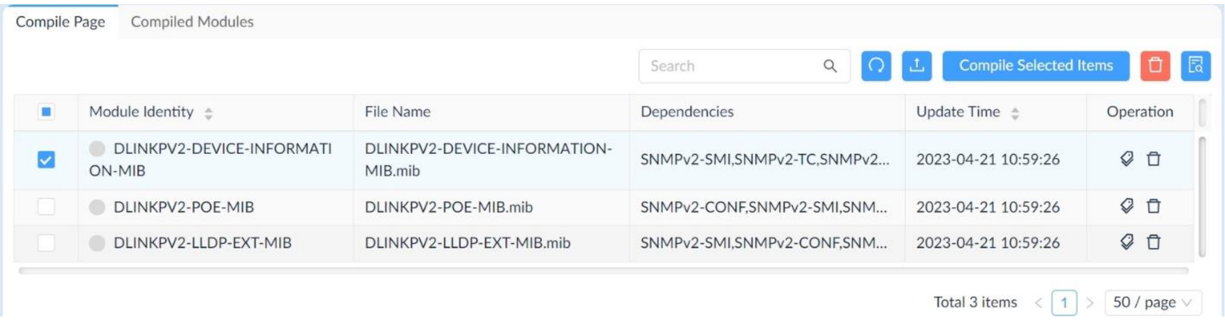
Compile MIB Files

You can compile MIB files in the uploaded list to make them available in the MIB browser.

To compile MIB files:

1. Go to **Tools > MIB Compiler** to display the MIB **Compile Page**.
2. In the Compile Page, select a file from the list and click **Compile Selected Items**.

The status of the MIB file will also be updated.



■	Module Identity	File Name	Dependencies	Update Time	Operation
☑	○ DLINKPV2-DEVICE-INFORMATION-MIB	DLINKPV2-DEVICE-INFORMATION-MIB.mib	SNMPv2-SMI,SNMPv2-TC,SNMPv2...	2023-04-21 10:59:26	
□	○ DLINKPV2-POE-MIB	DLINKPV2-POE-MIB.mib	SNMPv2-CONF,SNMPv2-SMI,SNM...	2023-04-21 10:59:26	
□	○ DLINKPV2-LLDP-EXT-MIB	DLINKPV2-LLDP-EXT-MIB.mib	SNMPv2-SMI,SNMPv2-CONF,SNM...	2023-04-21 10:59:26	

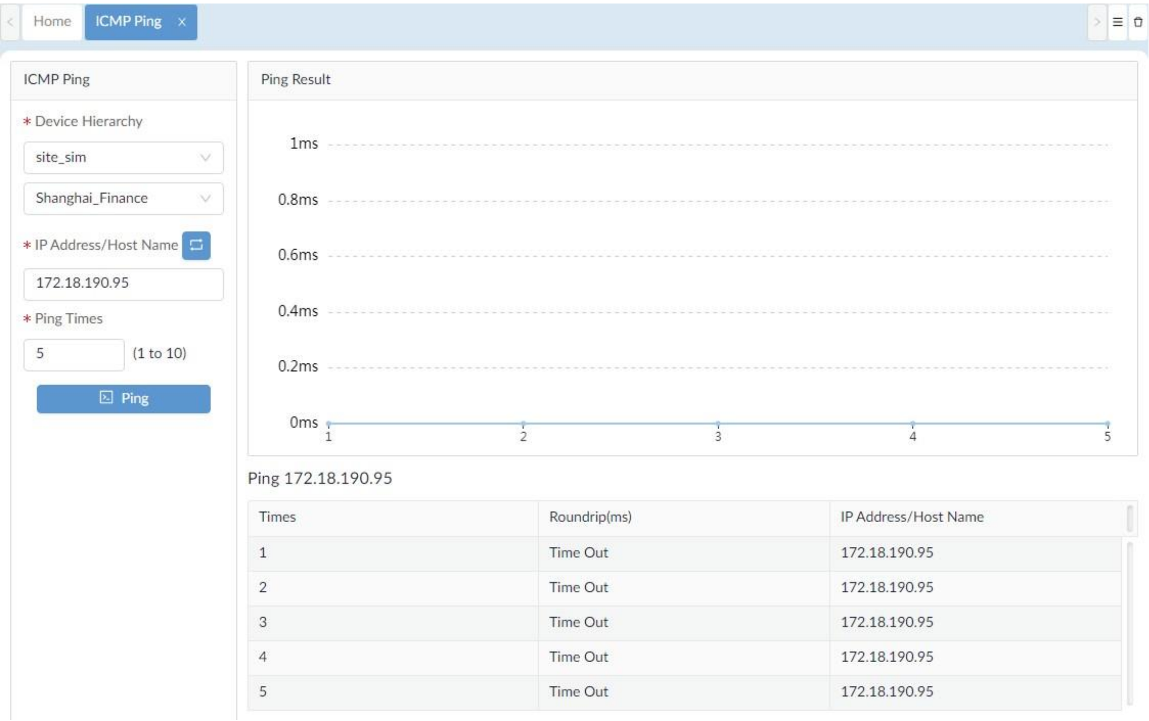
If a MIB is successfully compiled, it will be listed under Compiled Modules and can be accessed in the MIB Browser.

15.3 Perform an ICMP Ping

You can use Ping to diagnose the connectivity between two network devices.

To test a device with the Ping command:

1. Go to **Tools > ICMP Ping** to display the ICMP Ping page.



* Device Hierarchy: site_sim, Shanghai_Finance

* IP Address/Host Name: 172.18.190.95

* Ping Times: 5 (1 to 10)

Ping 172.18.190.95

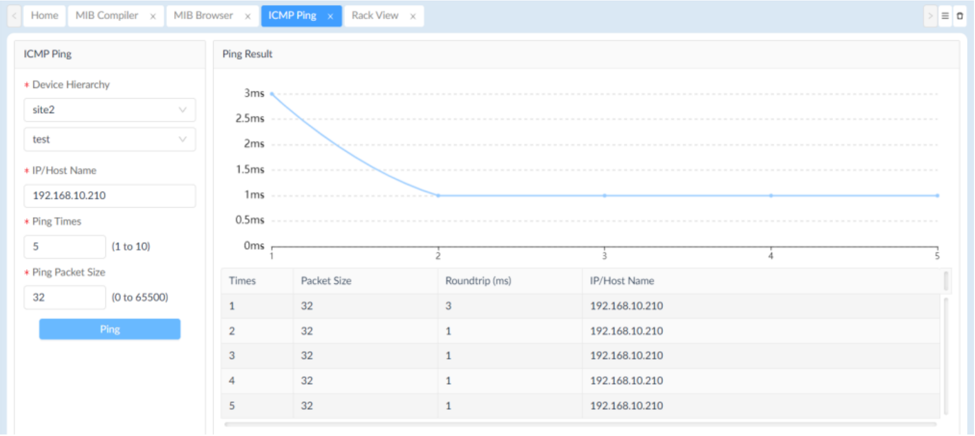
Times	Roundrip(ms)	IP Address/Host Name
1	Time Out	172.18.190.95
2	Time Out	172.18.190.95
3	Time Out	172.18.190.95
4	Time Out	172.18.190.95
5	Time Out	172.18.190.95

2. In the ICMP Ping pane, enter the following information to initiate a ping test:

- Device Hierarchy: click the drop-down menu to select site and network.
- Enter the destination host.
- Enter the number of times (1 to 10) to perform the ping test. The default is 5.
- Enter the packet size (in bytes) for the echo request messages. The default is 32.

3. Click **Ping** to initiate the test.

The Ping Result will be displayed on the right:



* Device Hierarchy: site2, test

* IP/Host Name: 192.168.10.210

* Ping Times: 5 (1 to 10)

* Ping Packet Size: 32 (0 to 65500)

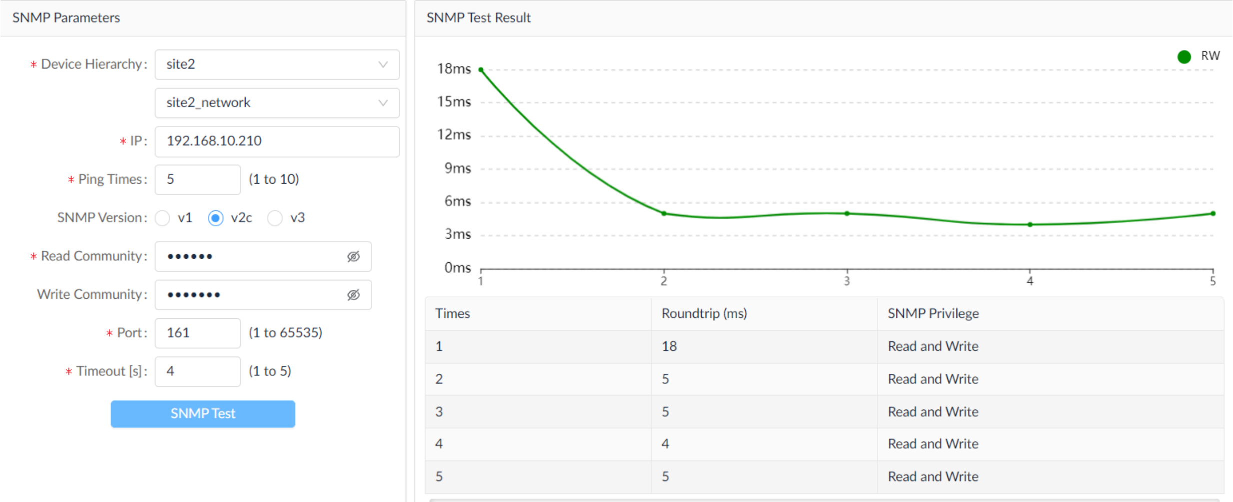
Times	Packet Size	Roundtrip (ms)	IP/Host Name
1	32	3	192.168.10.210
2	32	1	192.168.10.210
3	32	1	192.168.10.210
4	32	1	192.168.10.210
5	32	1	192.168.10.210

15.4 Perform an SNMP Test

SNMP lets administrators monitor discovered devices, allowing them to solve network problems and identify system health issues. For SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c) test, you need to specify an SNMP community string. For SNMP Version 3 (SNMPv3), you need to specify username and authentication and encryption (or privacy) settings.

To test a device with SNMP communication:

1. Go to **Tools > SNMP Test** to display the SNMP Parameters page.



SNMP Parameters

* Device Hierarchy: site2

site2_network

* IP: 192.168.10.210

* Ping Times: 5 (1 to 10)

SNMP Version: ○ v1 ● v2c ○ v3

* Read Community: ••••••

Write Community: •••••••

* Port: 161 (1 to 65535)

* Timeout [s]: 4 (1 to 5)

SNMP Test

SNMP Test Result

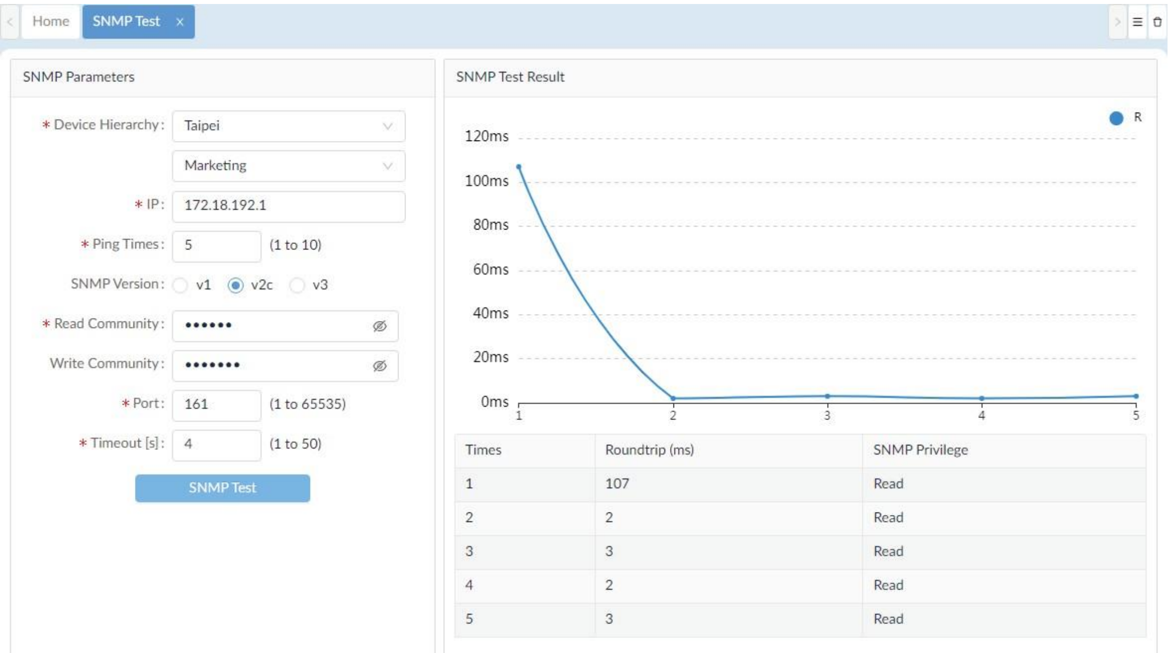
Times	Roundtrip (ms)	SNMP Privilege
1	18	Read and Write
2	5	Read and Write
3	5	Read and Write
4	4	Read and Write
5	5	Read and Write

2. From the SNMP Parameters column, enter the following information to initiate an SNMP trap test:

Item	Description
Device Hierarchy	Click the drop-down menu to select the site and network of the device for SNMP test.
IP	Enter the device’s IP address.
Ping Times	Enter the number of times (1 to 10) to perform the ping test.
SNMP Version	Select the SNMP version: v1, v2c, or v3.
Non-Repeaters (for v3 only)	Enter the number of objects that can return in a single get-next instance.
Max-Repetitions (for v3 only)	Enter the number of Get Next operations to be performed on each variable.
Username (for v3 only)	Enter the username for SNMP v3 requirement.
Context Name (for v3 only)	Enter the context name for SNMP v3 if it is used. It defines a named subset of the object instances in the MIB with access control.
Security Level (for v3 only)	Select whether authentication and privacy will be required and select the method accordingly. If authentication is used, enter the appropriate authentication parameters: protocol (MD5 or SHA) and password. If privacy is used, enter the appropriate privacy parameters (DES or AES) and password.
Read Community (for v1 and v2c only)	Specify the read community string.
Write Community (for v1 and v2c only)	Specify the write community string.
Port	Enter the Port number of the target device (1 to 65535, default: 161).
Timeout(s)	Enter the timeout (1 to 5, default: 4) value in seconds.
SNMP Test	Click SNMP Test to initiate the test.

3. Click **SNMP Test** to initiate the test.

The SNMP Test Result will be displayed:



* Device Hierarchy:	Taipei	
	Marketing	
* IP:	172.18.192.1	
* Ping Times:	5	(1 to 10)
SNMP Version:	○ v1 ● v2c ○ v3	
* Read Community:	••••••	
Write Community:	•••••••	
* Port:	161	(1 to 65535)
* Timeout [s]:	4	(1 to 50)

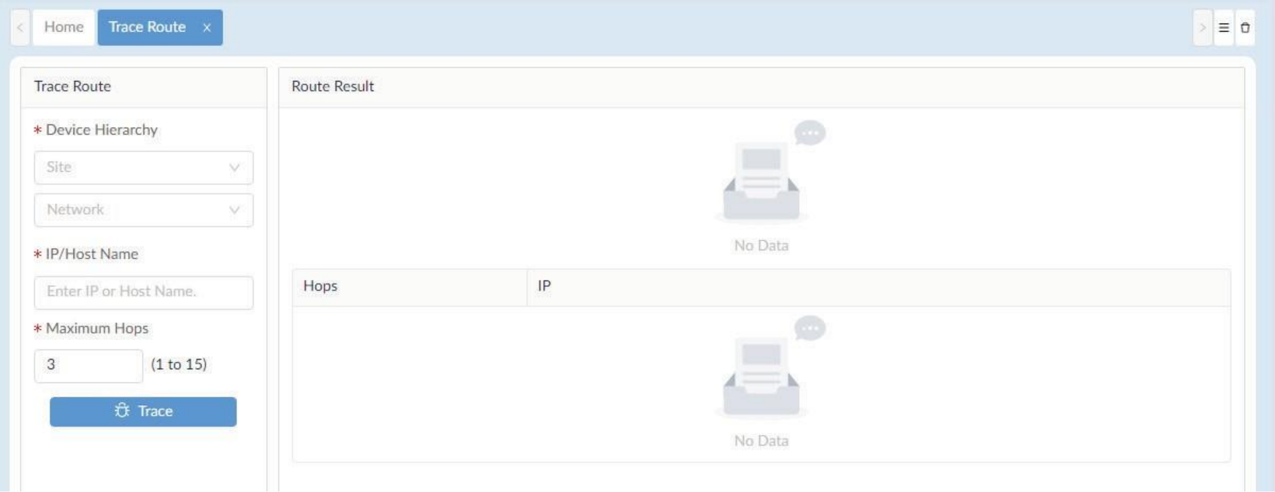
Times	Roundtrip (ms)	SNMP Privilege
1	107	Read
2	2	Read
3	3	Read
4	2	Read
5	3	Read

15.5 Perform a Trace Route Test

Trace route test diagnoses the path from one device to another.

To test a device by sending a trace route request:

1. Go to **Tools >Trace Route** to display the Trace Route page.



* Device Hierarchy

Site

Network

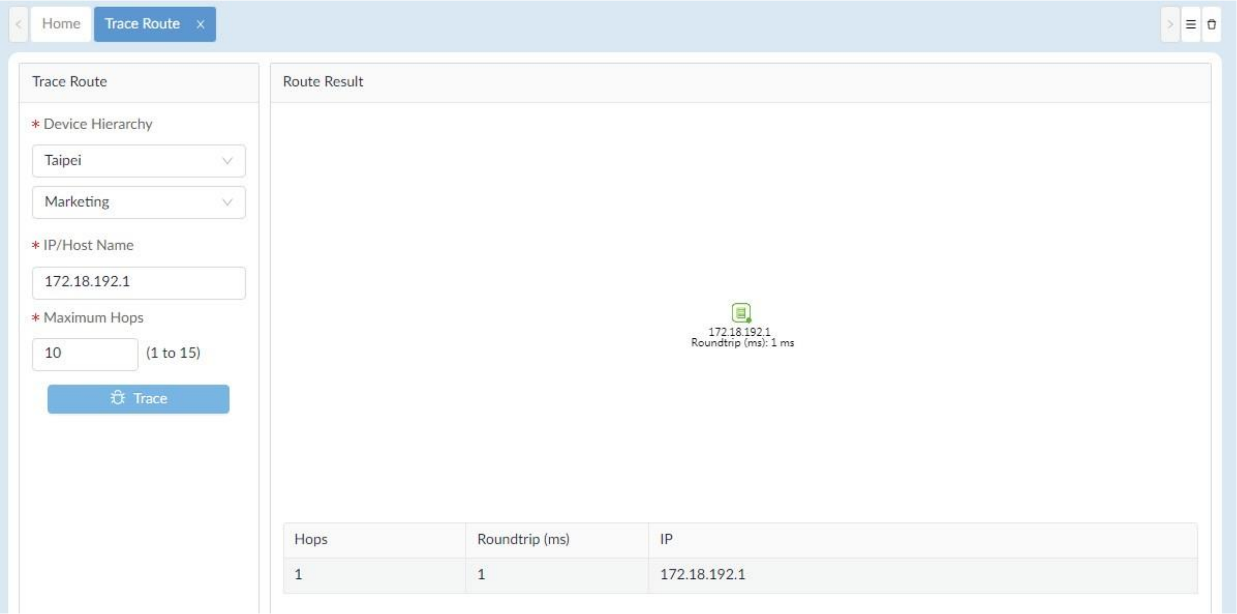
* IP/Host Name

Enter IP or Host Name.

* Maximum Hops

3 (1 to 15)

2. In the Trace Route pane, enter the following information to initiate a trace route test:
   - Device Hierarchy: click the drop-down menu to select site and network.
   - Enter the destination host.
   - Enter the maximum number of routers that a trace route packet can pass (1 to 15).
3. Click **Trace** to initiate the test.
4. The Route Result displays as follows:



* Device Hierarchy

Taipei

Marketing

* IP/Host Name

172.18.192.1

* Maximum Hops

10 (1 to 15)

172.18.192.1
Roundtrip (ms): 1 ms

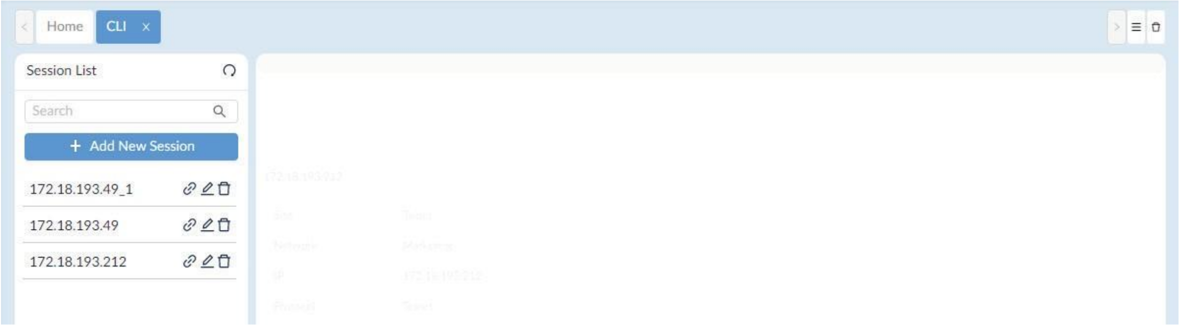
Hops	Roundtrip (ms)	IP
1	1	172.18.192.1

15.6 Configure Network Management from CLI

The D-View 8 interface is designed with access through command line interface for network configuration and management.

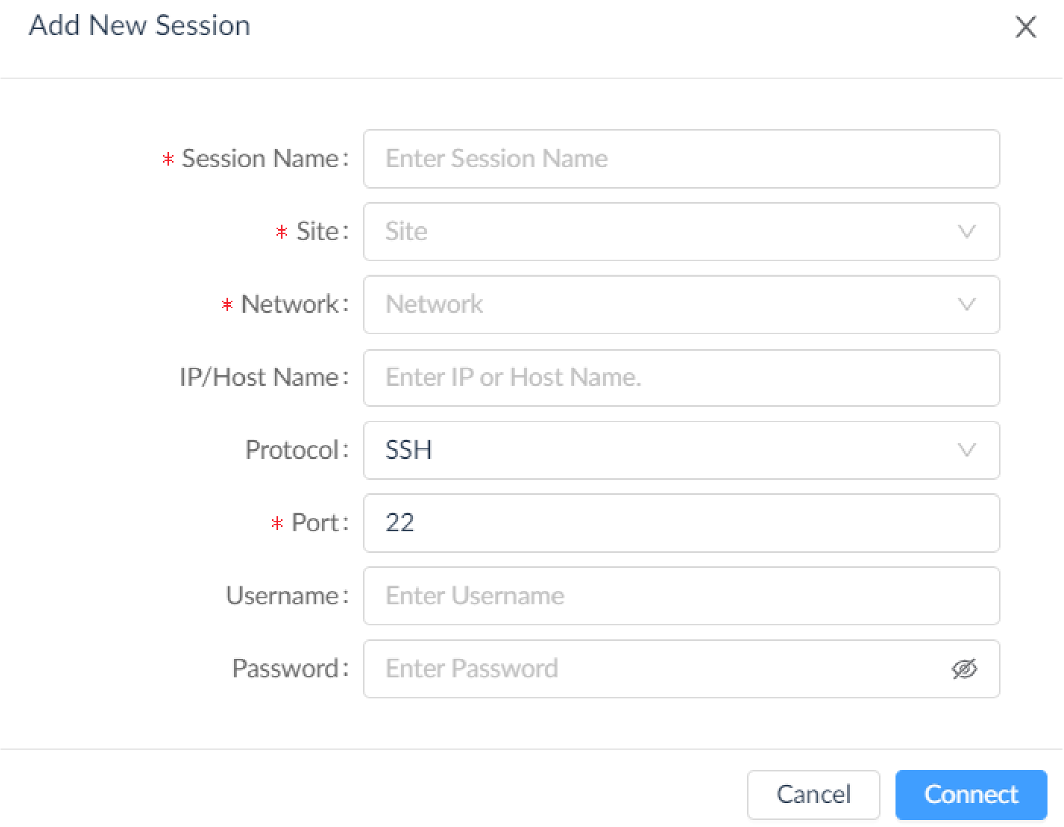
To add a new session:

1. Go to **Tools > CLI** to display the Session List page.
2. In the Session List pane, click **Add New Session**.



172.18.193.49_1
172.18.193.49
172.18.193.212

3. The Add New Session page displays.



Add New Session

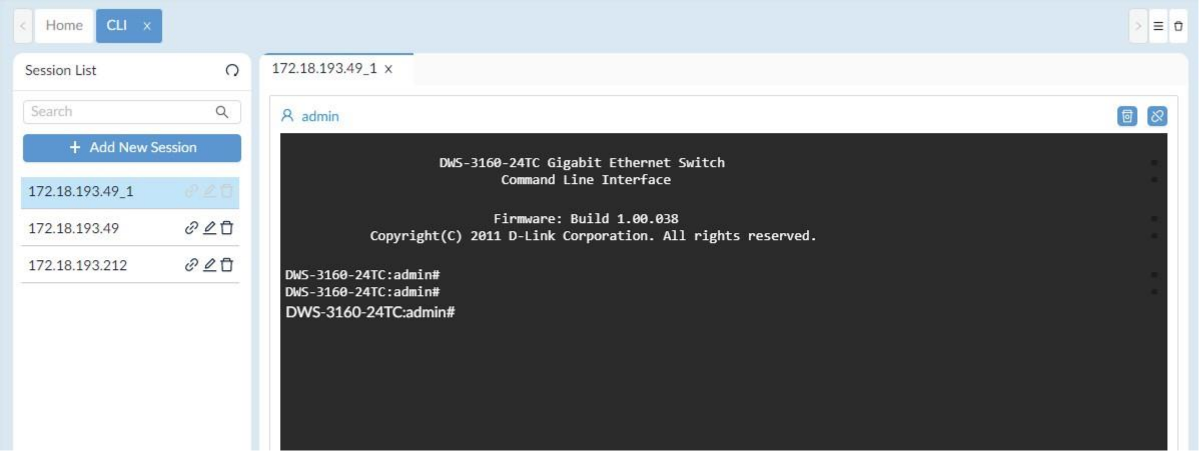
* Session Name:	Enter Session Name
* Site:	Site
* Network:	Network
IP/Host Name:	Enter IP or Host Name.
Protocol:	SSH
* Port:	22
Username:	Enter Username
Password:	Enter Password

4. Enter the following information to configure a CLI connection:

Item	Description
Session Name	Enter a name to define the CLI connection.
Site	Click the drop-down menu to select the desired site.
Network	Click the drop-down menu to select the desired network.
IP/Host Name	Enter the IP address or host name of the device to connect to.
Protocol	Click the drop-down menu to select the access protocol (SSH/Telnet).
Port	Enter the port number for the respective service (Telnet or SSH).
Username	Enter a username with authority to access the device.

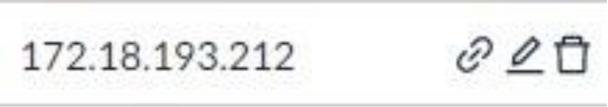
Password	Enter the password of the user account.
Cancel	Click to **Cancel** the session entry.
Connect	Click **Connect** to start the session.

5. Click **Connect** to start the connection. Click **Cancel** to cancel the connection request.The CLI Connection will be listed in the Session and open in the connection pane.



```
                    DWS-3160-24TC Gigabit Ethernet Switch
                           Command Line Interface

                           Firmware: Build 1.00.038
           Copyright(C) 2011 D-Link Corporation. All rights reserved.

DWS-3160-24TC:admin#
DWS-3160-24TC:admin#
DWS-3160-24TC:admin#
```

6. For each connection setting, you can modify or remove it from the connection list, click on the available options.



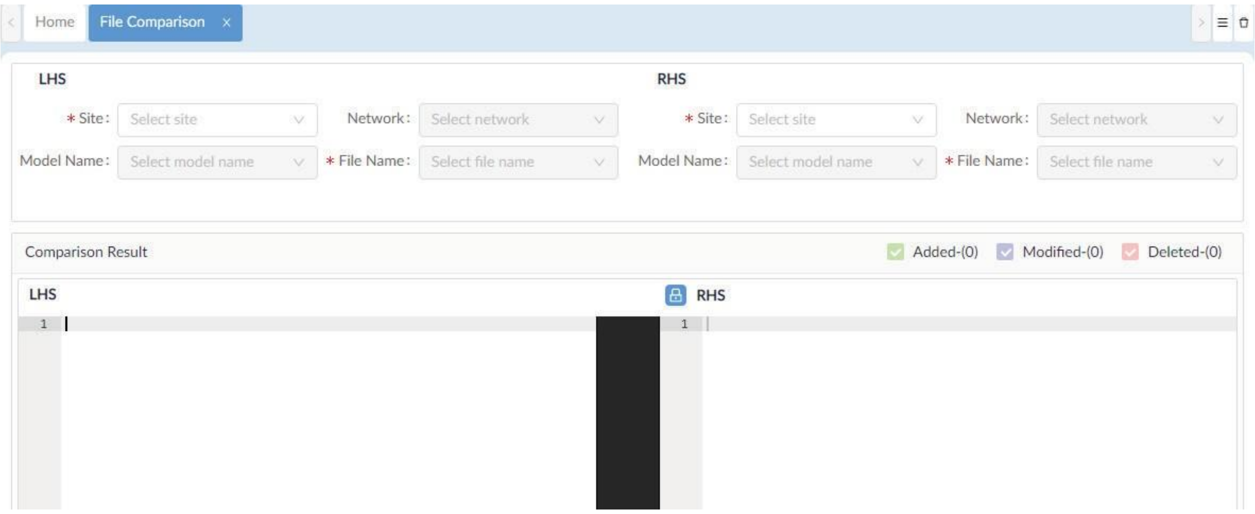
- Connect: initiate a connection
- Edit: modify the settings
- Delete: remove the entry from the list

15.7 Compare Configuration Files

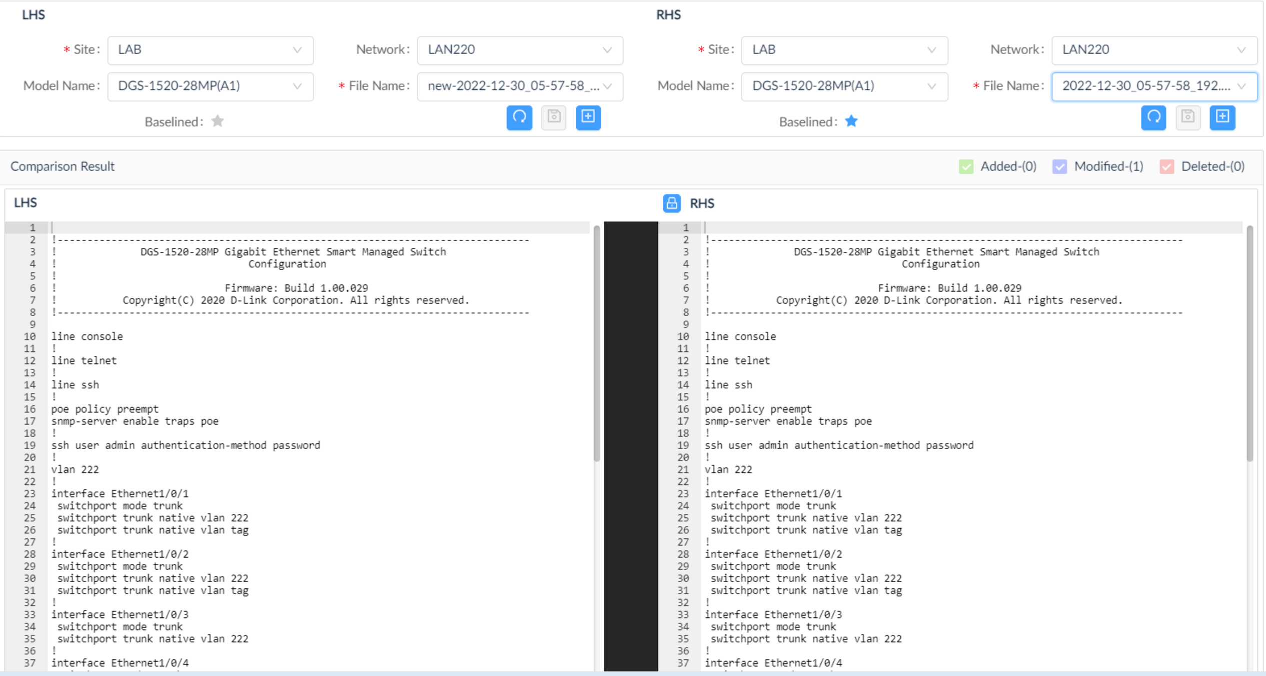
The File Comparison tool provides the function to compare two configuration files. Only text-based files can be compared.

To compare two files:

1. Go to **Tools > File Comparison**.



2. Select two configuration files by specifying the device's site, network and device model to start comparing.



LHS

Site: LAB
Network: LAN220
Model Name: DGS-1520-28MP(A1)
File Name: new-2022-12-30_05-57-58_...

RHS

Site: LAB
Network: LAN220
Model Name: DGS-1520-28MP(A1)
File Name: 2022-12-30_05-57-58_192....

LHS

```

!-------------------------------------------------------------------------------
!               DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                 Configuration
!
!                             Firmware: Build 1.00.029
!             Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
poe policy preempt
snmp-server enable traps poe
!
ssh user admin authentication-method password
!
vlan 222
!
interface Ethernet1/0/1
 switchport mode trunk
 switchport trunk native vlan 222
 switchport trunk native vlan tag
!
interface Ethernet1/0/2
 switchport mode trunk
 switchport trunk native vlan 222
 switchport trunk native vlan tag
!
interface Ethernet1/0/3
 switchport mode trunk
 switchport trunk native vlan 222
!
interface Ethernet1/0/4
```

RHS

```

!-------------------------------------------------------------------------------
!               DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                 Configuration
!
!                             Firmware: Build 1.00.029
!             Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
poe policy preempt
snmp-server enable traps poe
!
ssh user admin authentication-method password
!
vlan 222
!
interface Ethernet1/0/1
 switchport mode trunk
 switchport trunk native vlan 222
 switchport trunk native vlan tag
!
interface Ethernet1/0/2
 switchport mode trunk
 switchport trunk native vlan 222
 switchport trunk native vlan tag
!
interface Ethernet1/0/3
 switchport mode trunk
 switchport trunk native vlan 222
!
interface Ethernet1/0/4
```

3. The comparison result will be shown with the difference: added text in green, modified text in purple, and deleted text in red.

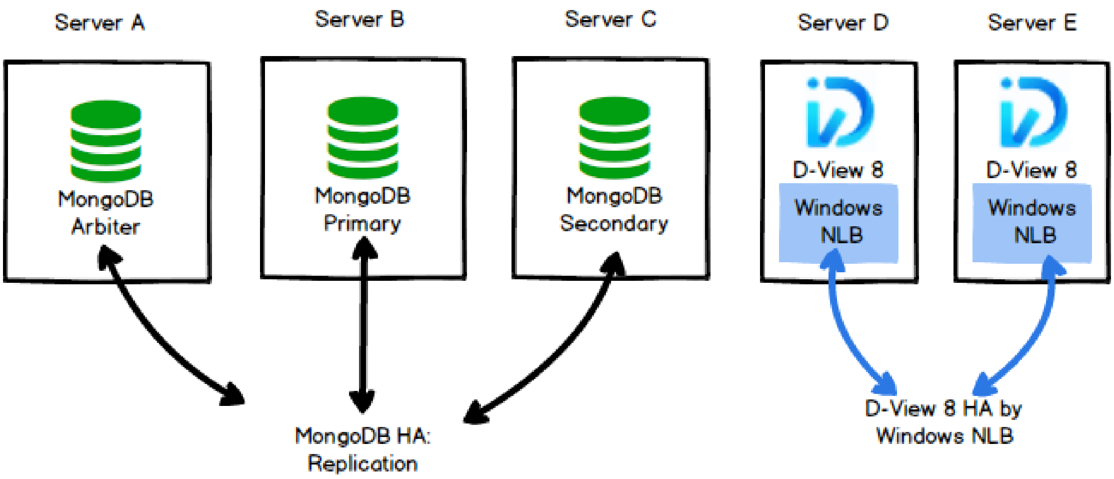
4. You can directly modify the file and save it as a new configuration file to upload to the server. Go to **Configuration > File Management** for the list of all uploaded configuration and firmware files.

5. The **Restore to Device** function allows you to schedule a restoration job using the currently displayed file. Go to **Configuration > Configuration Management > Restore** for the list of all restoration jobs.

Appendix A: Deployment with Five-server Topology

The D-View 8 can be deployed in server cluster in three-server or five-server topology. This section illustration the structure and the deployment procedure of the 5-server topology.

Structure



Preparation for five-server deployment:

When planning for server cluster deployment, you must first set up 5 Windows servers with the following system configuration:

- SERVER A

  OS: Windows 10, Windows Server 2016/ Windows Server 2019

  MongoDB

  IP Address: 192.168.1.205

  Replica set role: arbiter

- SERVER B

  OS: Windows 10, Windows Server 2016/ Windows Server 2019

  MongoDB

  IP Address: 192.168.1.203

  Replica set Role: primary

- SERVER C

  OS: Windows 10, Windows Server 2016/ Windows Server 2019

  MongoDB

IP Address: 192.168.1.204

Replica set Role: secondary

- SERVER D

  OS: Windows Server 2016/ Windows Server 2019

  D-View 8

  IP Address: 192.168.1.201

  NLB enabled with virtual IP: 192.168.1.200

23456789/-9123qwertyuop[]\][poi87ewq wertyuiop[

‘;loiuytrea

- SERVER E

  OS: Windows Server 2016/ Windows Server 2019

  D-View 8

  IP Address: 192.168.1.202

  NLB enabled with virtual IP: 192.168.1.200

Data Redundancy Support on the MongoDB Server Cluster

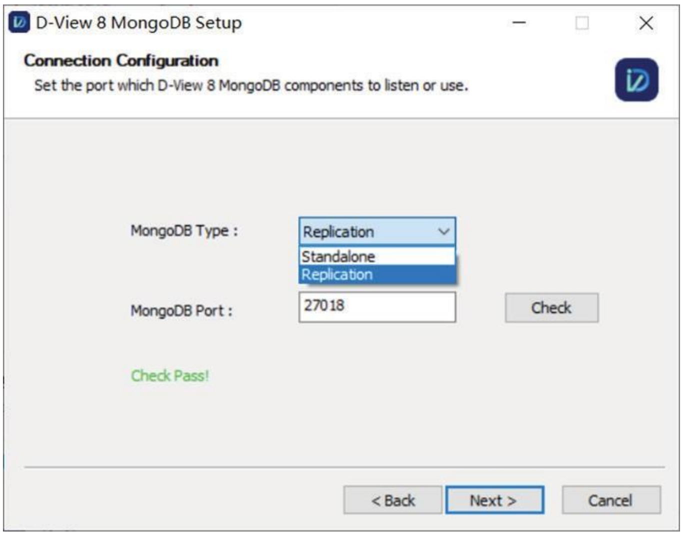
This section details the steps to install the required MongoDB databases and enable data redundancy in the database cluster.

MongoDB Cluster Installation

To install MongoDB in the database cluster:

1. Obtain the D-View 8 MongoDB installation package (e.g. D-View 8 MongoDB_1.0.0.70_Installation.exe).
2. Install the package on three servers, A, B, and C.
3. On the Connection Configuration page, select **Replication** in the MongoDB Type drop-down menu.

4. Enter the MongoDB port number for server communication.



D-View 8 MongoDB Setup

Connection Configuration

Set the port which D-View 8 MongoDB components to listen or use.

MongoDB Type : Replication

MongoDB Port : 27018

Check Pass!

5. Click **Check** to test the setting. If it is configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port setting and try again.
6. Click **Next** to continue and the installation should start.

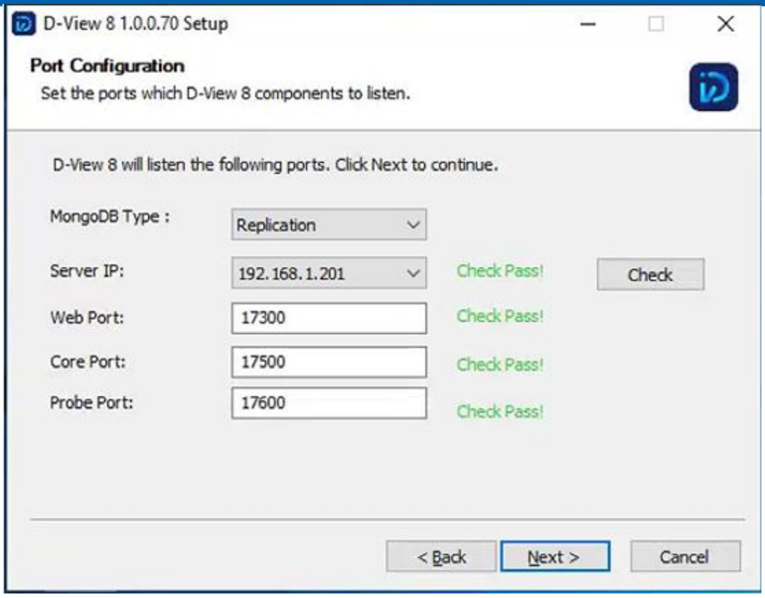
D-View 8 Installation

Use the following procedure to install D-View 8 on additional servers (e.g. server D & E) other than the database servers and connect them to the MongoDB cluster.

Perform the following procedure to install D-View 8 on server D and E.

Installation on server D

1. Obtain the installation package (e.g. D-View 8_1.0.0.70_Installation.exe).
2. Install the package.
3. In the Port Configuration page, select **Replication** in the MongoDB Type menu.
4. In the Server IP field, enter the host server's IP address. As for our example, 192.168.1.201.
5. For port settings, enter the port number required for web access, core communication, and probe communication: 17300, 17500, and 17600.
6. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port settings and try again.
7. Click **Next** to continue



D-View 8 1.0.0.70 Setup

Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Replication

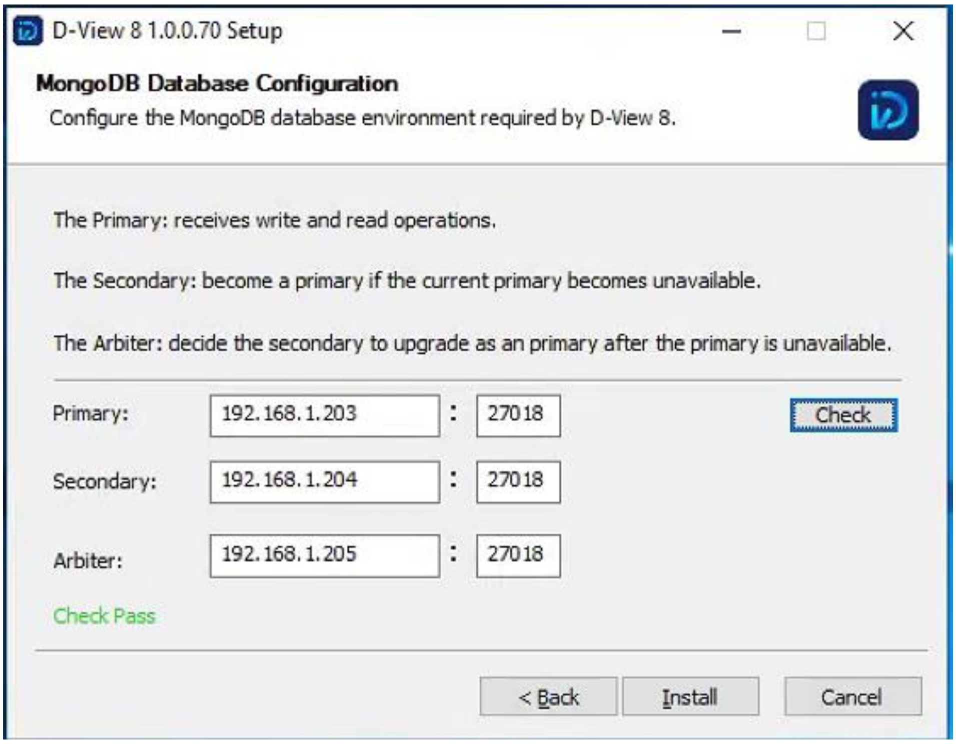
Server IP: 192.168.1.201 Check Pass!

Web Port: 17300 Check Pass!

Core Port: 17500 Check Pass!

Probe Port: 17600 Check Pass!

8. The MongoDB Database Configuration page displays. Enter IP addresses and port number for the database servers designated with the respective Replica Roles. Click Check to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port settings and try again.



D-View 8 1.0.0.70 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

The Primary: receives write and read operations.

The Secondary: become a primary if the current primary becomes unavailable.

The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.

Primary: 192.168.1.203 : 27018

Secondary: 192.168.1.204 : 27018

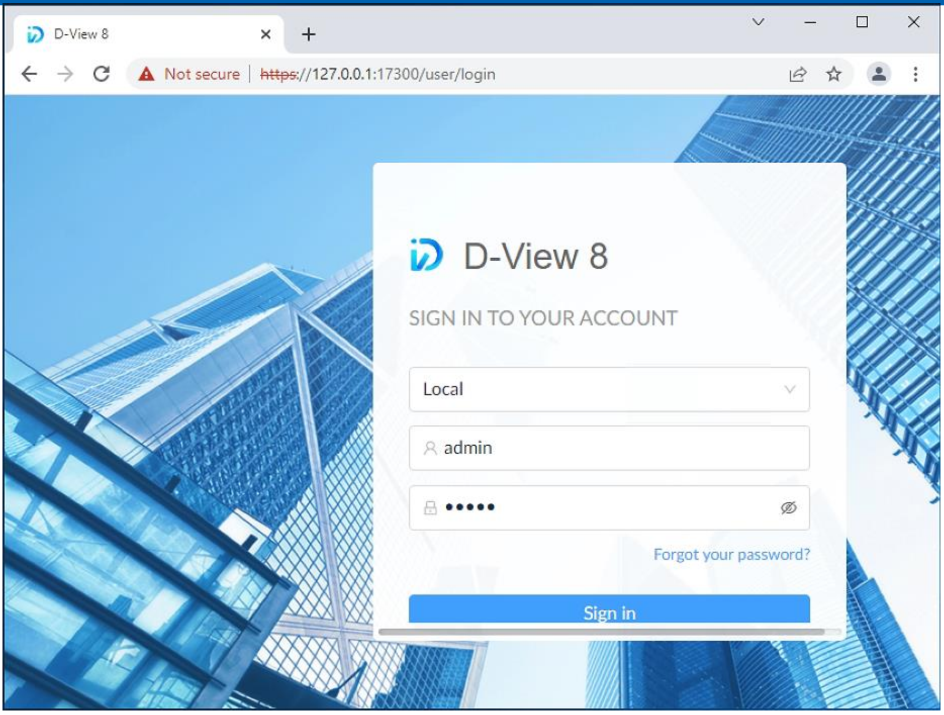
Arbiter: 192.168.1.205 : 27018

Check Pass

13. Click **Install** to continue.

14. Once the installation completes, click **Finish** to close the Setup Wizard.

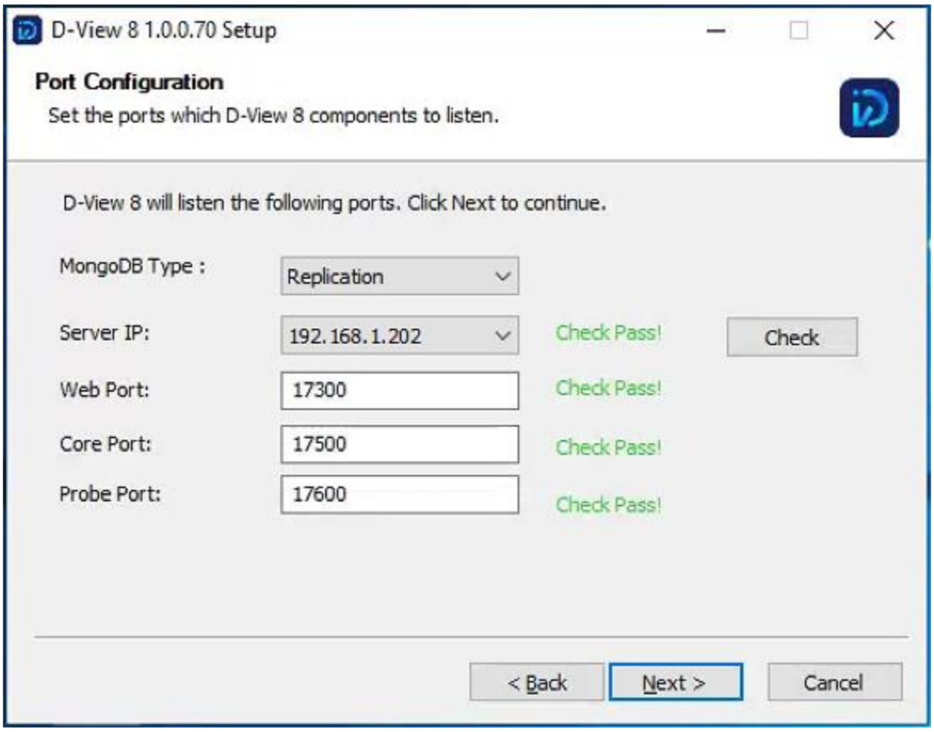
15. The D-View 8 Server can be accessed from a web browser on the server.



D-View 8
https://127.0.0.1:17300/user/login
Not secure
D-View 8
SIGN IN TO YOUR ACCOUNT
Local
admin
•••••
Forgot your password?
Sign in

Installation on server E

1. Start the Installation package.
2. In the Port Configuration page, select **Replication** in the MongoDB Type menu.
3. In the Server IP field, enter the host server's IP address. As for our example, 192.168.1.202.
4. For port settings, enter the port number required for web access, core communication, and probe communication: 17300, 17500, and 17600.
5. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port settings and try again.
6. Click **Next** to continue



D-View 8 1.0.0.70 Setup

Port Configuration

Set the ports which D-View 8 components to listen.

D-View 8 will listen the following ports. Click Next to continue.

MongoDB Type : Replication

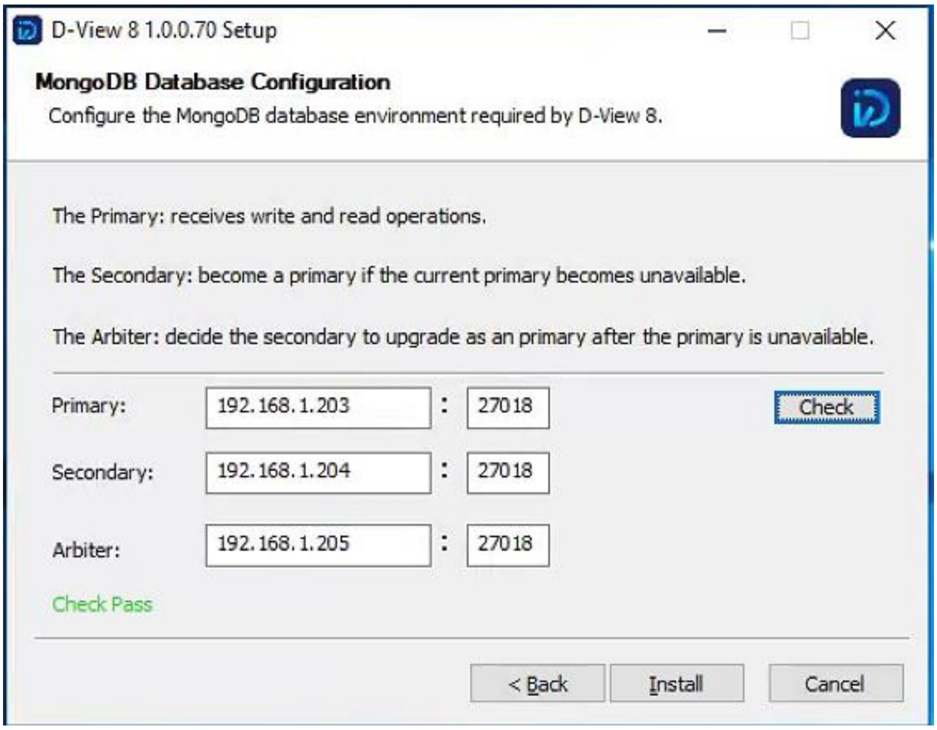
Server IP: 192.168.1.202 Check Pass!

Web Port: 17300 Check Pass!

Core Port: 17500 Check Pass!

Probe Port: 17600 Check Pass!

9. The MongoDB Database Configuration page displays. Enter IP addresses and port number for the database servers designated with the respective Replica Roles. Click Check to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port settings and try again.



D-View 8 1.0.0.70 Setup

MongoDB Database Configuration

Configure the MongoDB database environment required by D-View 8.

The Primary: receives write and read operations.

The Secondary: become a primary if the current primary becomes unavailable.

The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.

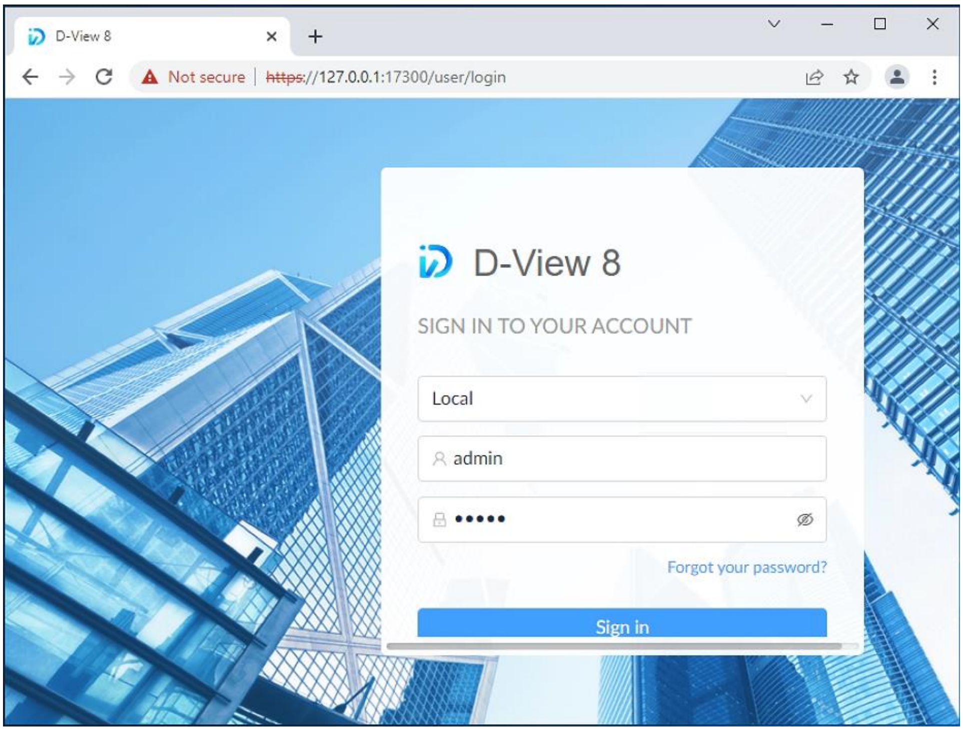
Primary: 192.168.1.203 : 27018

Secondary: 192.168.1.204 : 27018

Arbiter: 192.168.1.205 : 27018

Check Pass

10. After the installation, the D-View 8 Server can be accessed from a web browser on the server.

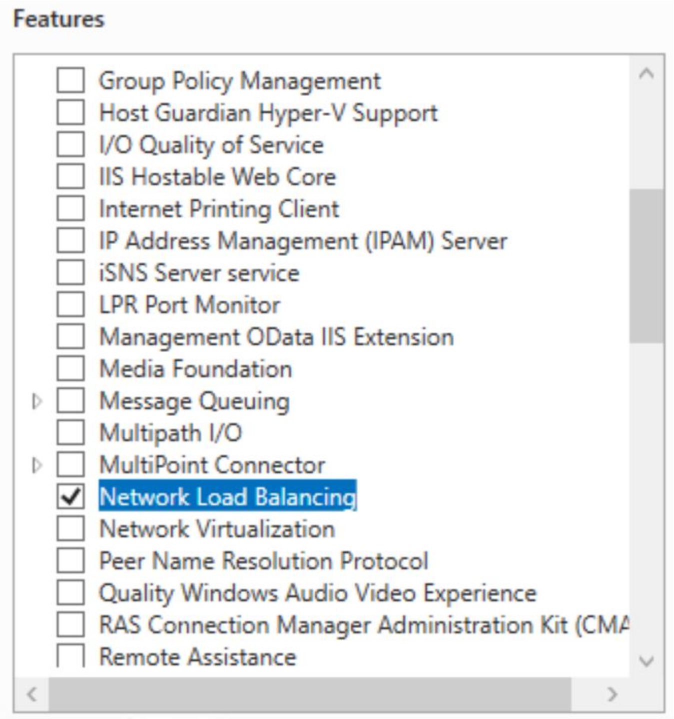


Network Load Balancing Setup on D-View 8 Servers

Server load balancing is supported on D-View 8. At least two Windows servers on the same subnet will be required to configure load balancing. For our deployment demonstration of five-server topology, use the following procedure to set up NLB on D-View 8 servers.

To set up NLB on server D & E:

1. Install the Network Load Balancing service on both server D & E.



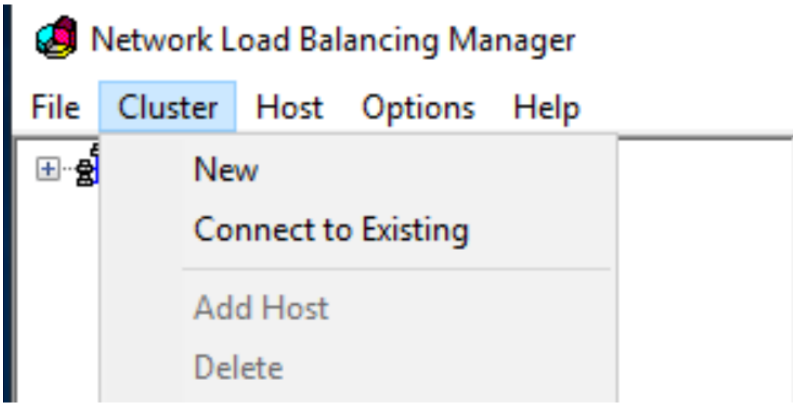
Features

- ☐ Group Policy Management
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ iSNS Server service
- ☐ LPR Port Monitor
- ☐ Management OData IIS Extension
- ☐ Media Foundation
- ☐ Message Queuing
- ☐ Multipath I/O
- ☐ MultiPoint Connector
- ☑ Network Load Balancing
- ☐ Network Virtualization
- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ RAS Connection Manager Administration Kit (CMA
- ☐ Remote Assistance

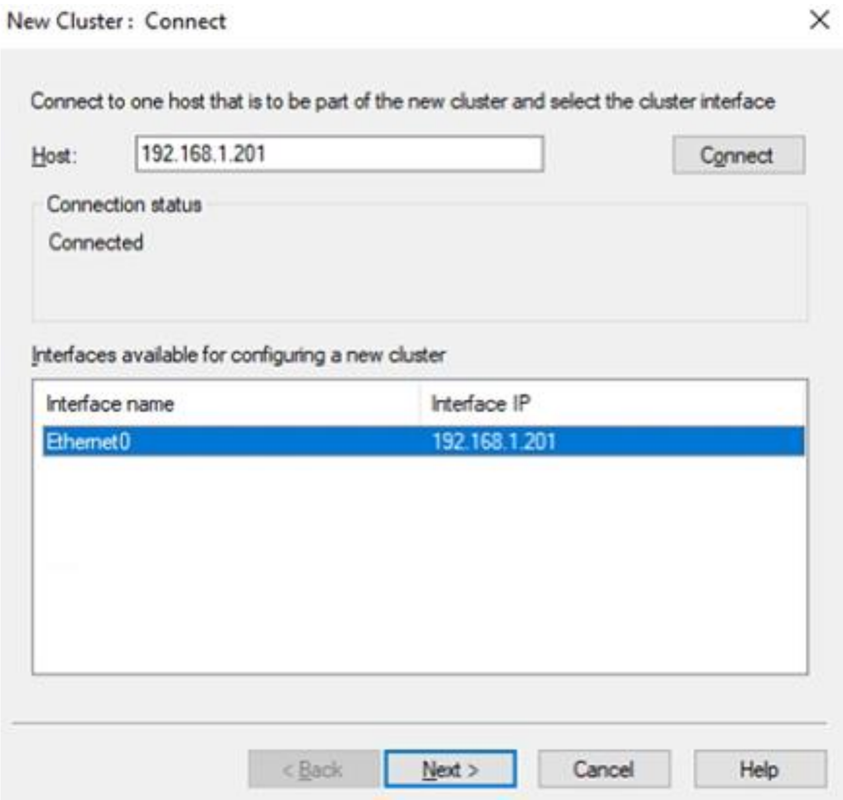
2. Start Network Load Balancing Manager on both servers. Then use the following procedure to configure them individually.

Configuration on server D

3. In NLB Manager, click **Cluster > New** to create a new cluster.



4. In the Host field, enter the IP address of SERVER D: 192.168.1.201 and click the **Connect** button.



New Cluster : Connect

Connect to one host that is to be part of the new cluster and select the cluster interface

Host: 192.168.1.201

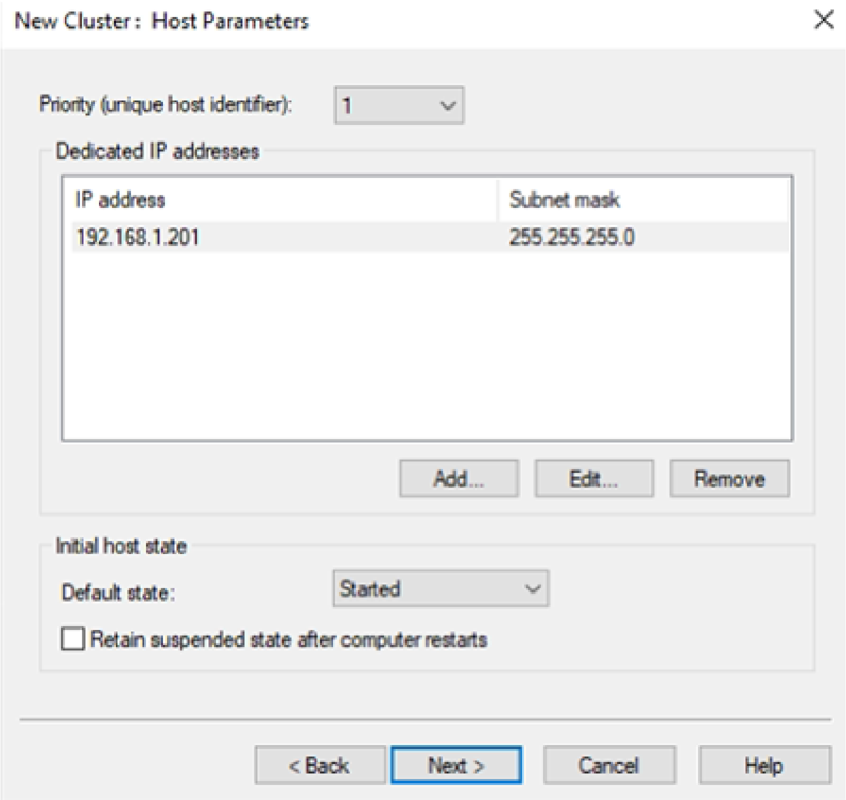
Connection status

Connected

Interfaces available for configuring a new cluster

Interface name	Interface IP
Ethernet0	192.168.1.201

5. Click **Next** to continue. The New Cluster: Host Parameters page displays.



New Cluster : Host Parameters

Priority (unique host identifier): 1

Dedicated IP addresses

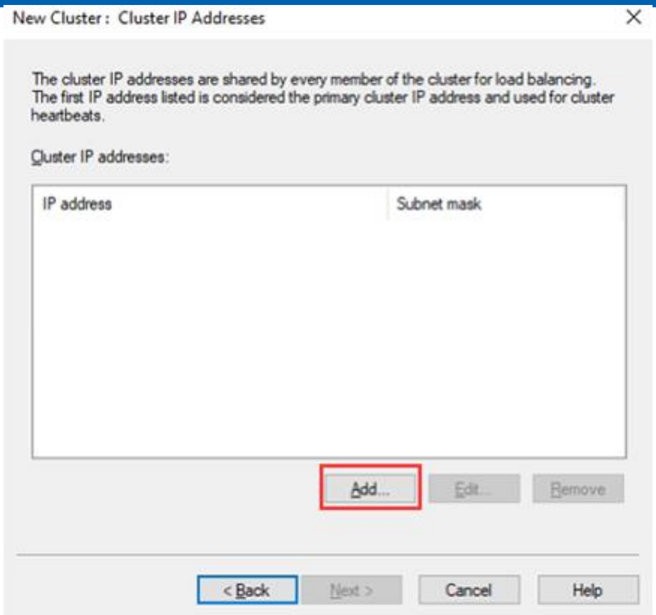
IP address	Subnet mask
192.168.1.201	255.255.255.0

Initial host state

Default state: Started

☐ Retain suspended state after computer restarts

6. Click **Next** to continue. The New Cluster: Cluster IP Addresses page displays.
7. Click **Add** to enter the cluster IP address.



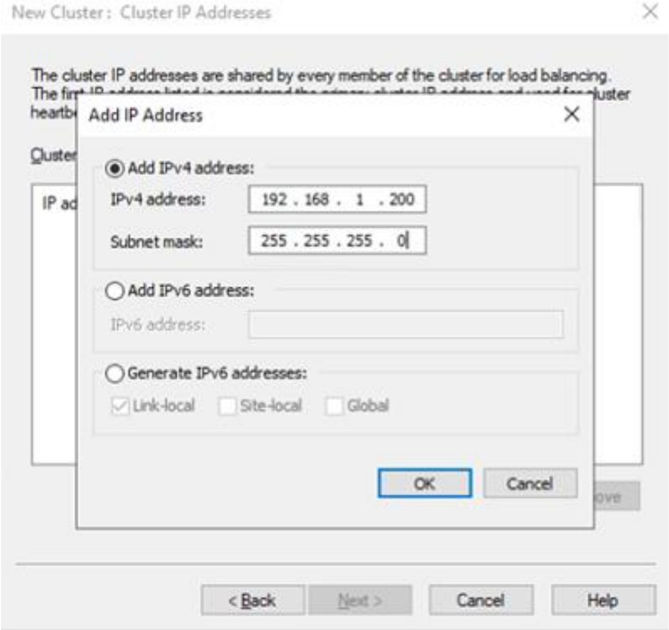
New Cluster : Cluster IP Addresses

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask

8. Enter a virtual IP and subnet mask that will be used as the Cluster IP and netmask. Then click **OK** to continue.



Add IP Address

● Add IPv4 address:

IPv4 address: 192 . 168 . 1 . 200

Subnet mask: 255 . 255 . 255 . 0

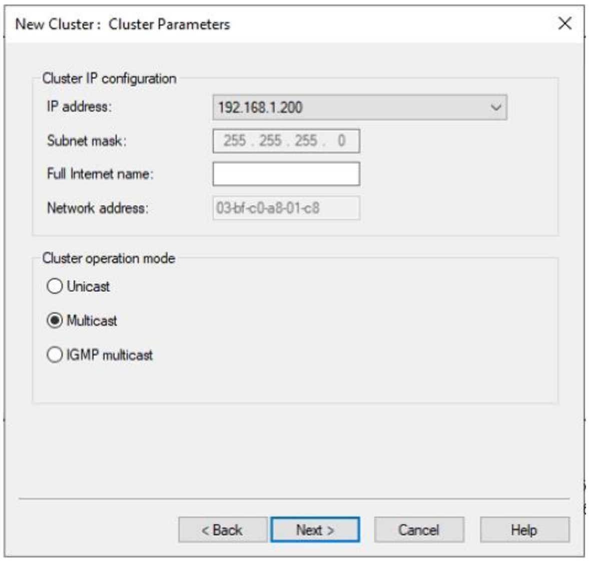
○ Add IPv6 address:

IPv6 address:

○ Generate IPv6 addresses:

☑ Link-local □ Site-local □ Global

9. Select **Multicast** for **Cluster Operation Mode** for optimal performance.



New Cluster : Cluster Parameters

Cluster IP configuration

IP address: 192.168.1.200

Subnet mask: 255 . 255 . 255 . 0

Full Internet name:

Network address: 03-bf-c0-a8-01-c8

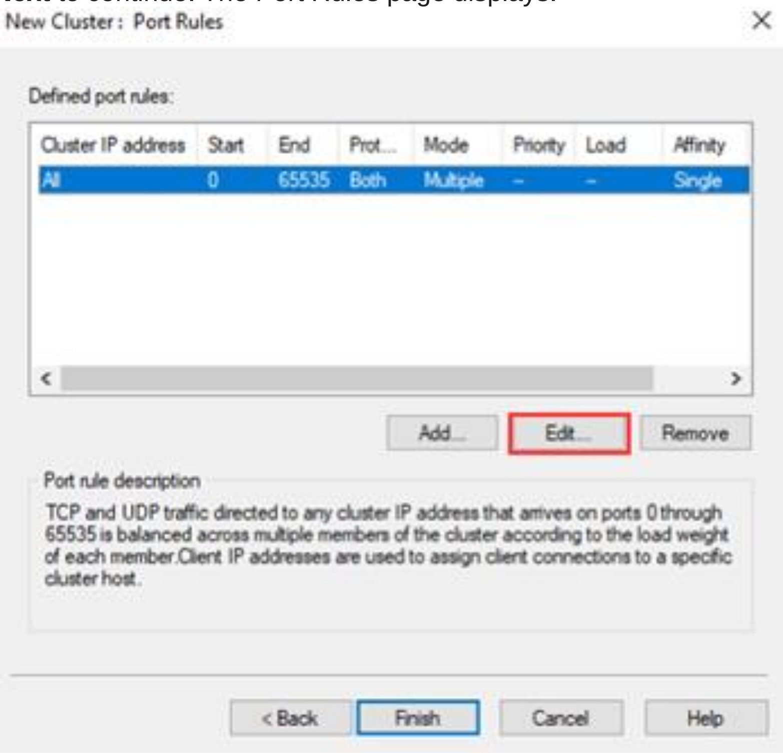
Cluster operation mode

○ Unicast

● Multicast

○ IGMP multicast

10. Click **Next** to continue. The Port Rules page displays.



New Cluster : Port Rules

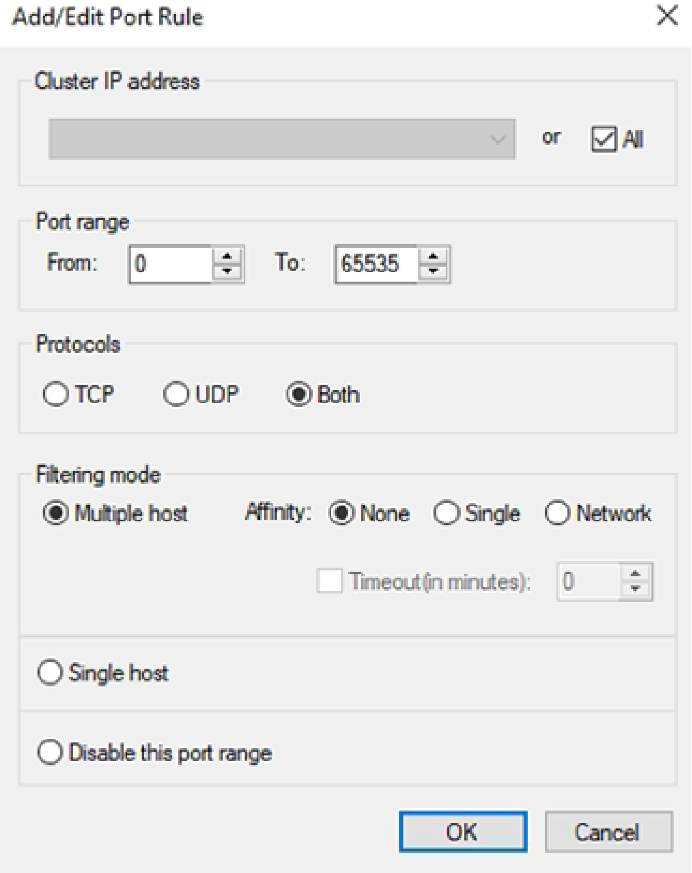
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	0	65535	Both	Multiple	–	–	Single

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced across multiple members of the cluster according to the load weight of each member.Client IP addresses are used to assign client connections to a specific cluster host.

11. Select the defined port rule and click **Edit**. The Add/Edit Port Rule page displays.



Add/Edit Port Rule

Cluster IP address

or ☑ All

Port range

From: 0 To: 65535

Protocols

○ TCP ○ UDP ● Both

Filtering mode

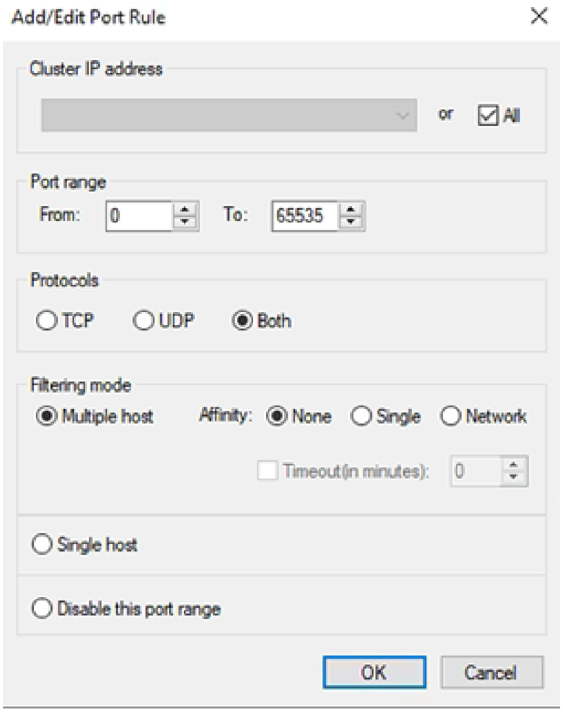
● Multiple host Affinity: ● None ○ Single ○ Network

□ Timeout (in minutes): 0

○ Single host

○ Disable this port range

12. In the Filtering mode section, Select **Multiple host** for **Filtering mode** and **None** for **Affinity**. Then click **OK** to continue.



Add/Edit Port Rule

Cluster IP address

or ☑ All

Port range

From: 0 To: 65535

Protocols

○ TCP ○ UDP ● Both

Filtering mode

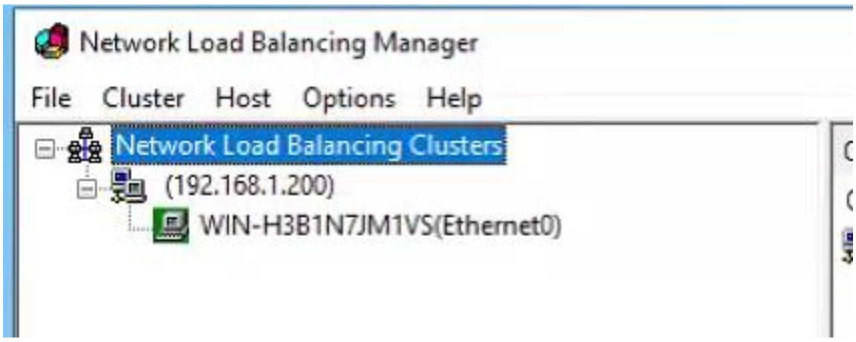
● Multiple host Affinity: ● None ○ Single ○ Network

□ Timeout(in minutes): 0

○ Single host

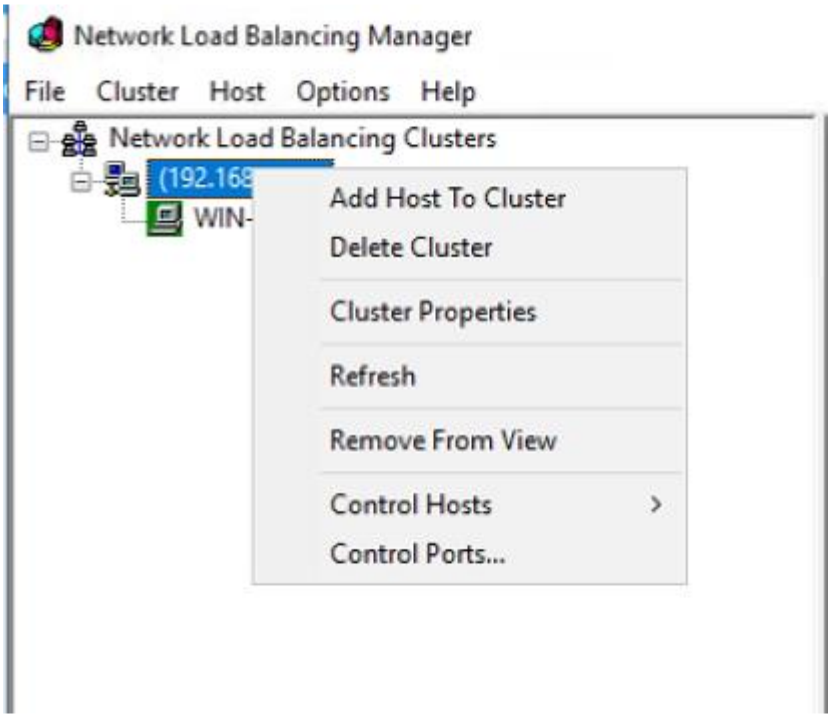
○ Disable this port range

13. An NLB cluster will be created as shown below.

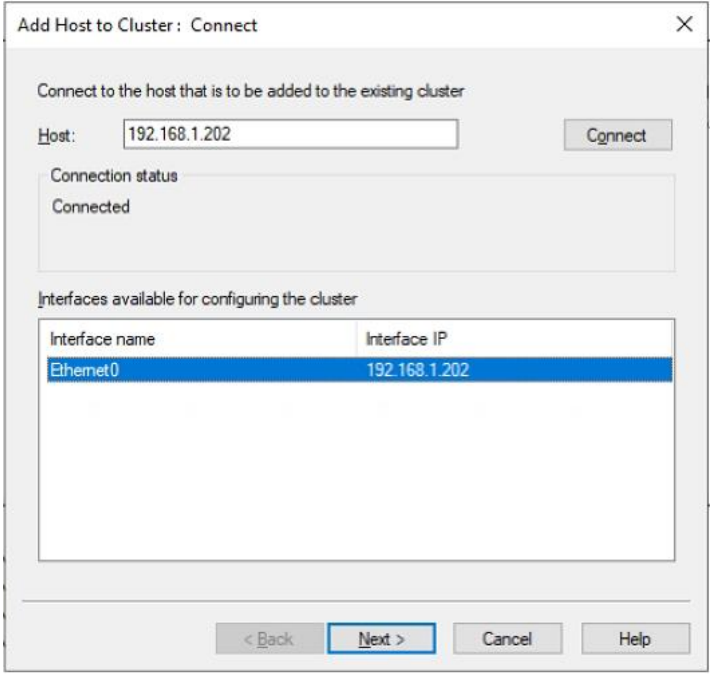


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
(192.168.1.200)
WIN-H3B1N7JM1VS(Ethernet0)

14. Add SERVER E to this cluster: Right-click the cluster node and click **Add Host To Cluster**.



15. Input the SERVER E’s IP address: 192.168.1.202, then click **Connect**.



Add Host to Cluster : Connect

Connect to the host that is to be added to the existing cluster

Host: 192.168.1.202

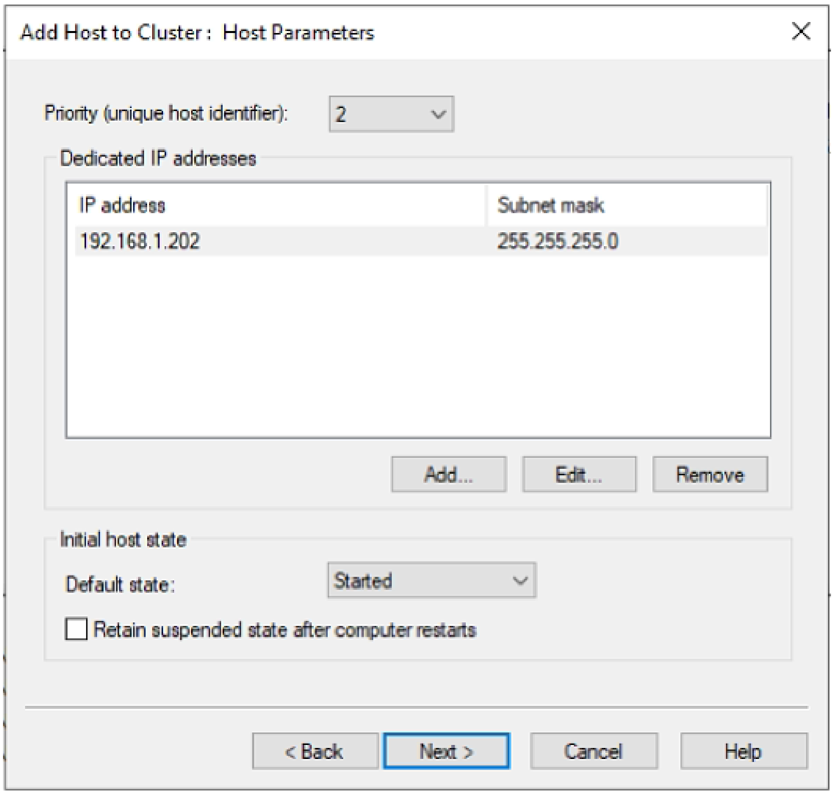
Connection status

Connected

Interfaces available for configuring the cluster

Interface name	Interface IP
Ethernet0	192.168.1.202

16. Click **Next** to continue.



Add Host to Cluster : Host Parameters

Priority (unique host identifier): 2

Dedicated IP addresses

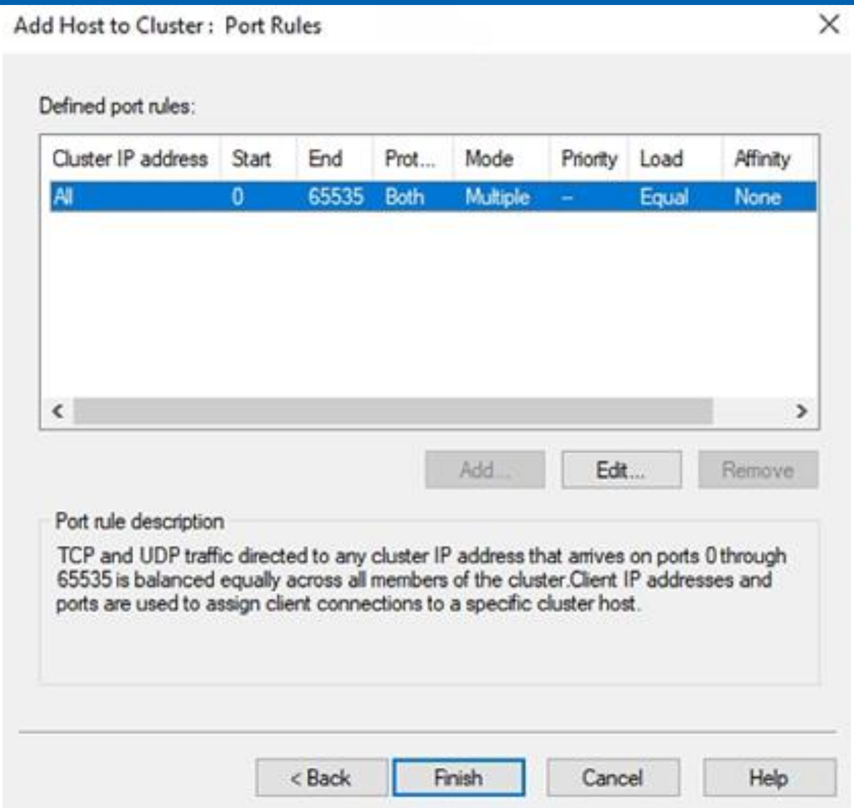
IP address	Subnet mask
192.168.1.202	255.255.255.0

Initial host state

Default state: Started

□ Retain suspended state after computer restarts

17. Click **Finish** to close the screen.



Add Host to Cluster : Port Rules

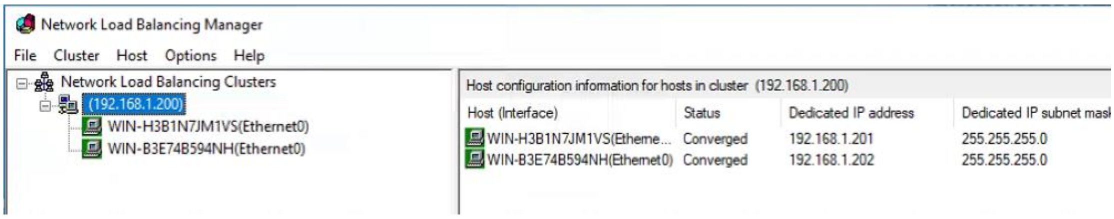
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	0	65535	Both	Multiple	-	Equal	None

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced equally across all members of the cluster.Client IP addresses and ports are used to assign client connections to a specific cluster host.

18. Open the Network Load Balancing Manager. Now a cluster containing both server D and E was created. And the D-View 8 can be accessed with the cluster IP.

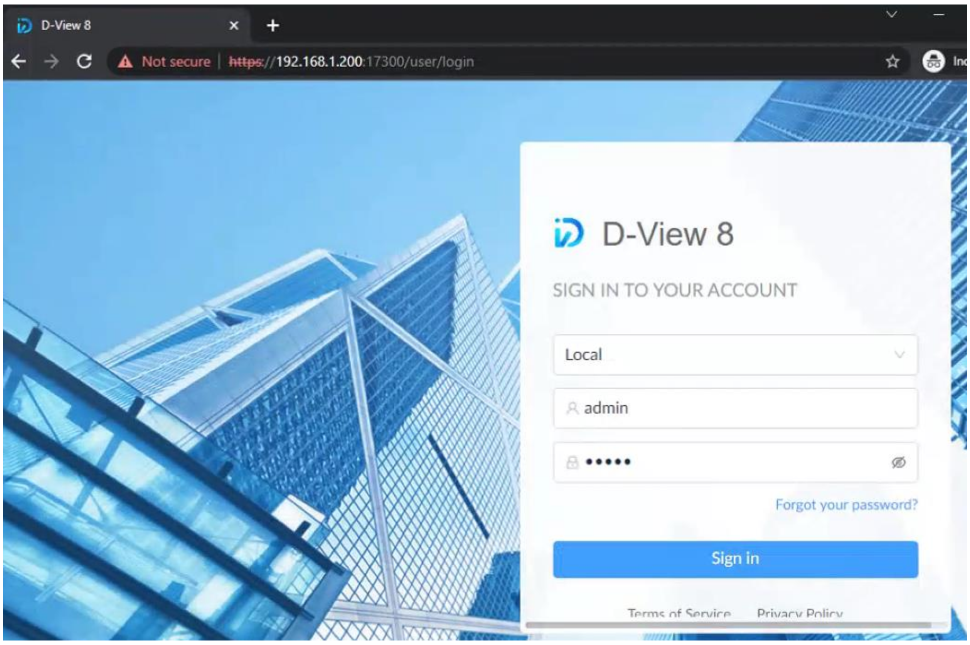


Network Load Balancing Manager
File
Cluster
Host
Options
Help
Network Load Balancing Clusters
(192.168.1.200)
WIN-H3B1N7JM1VS(Ethernet0)
WIN-B3E74B594NH(Ethernet0)

Host configuration information for hosts in cluster (192.168.1.200)

Host (Interface)	Status	Dedicated IP address	Dedicated IP subnet mask
WIN-H3B1N7JM1VS(Etherne...	Converged	192.168.1.201	255.255.255.0
WIN-B3E74B594NH(Ethernet0)	Converged	192.168.1.202	255.255.255.0

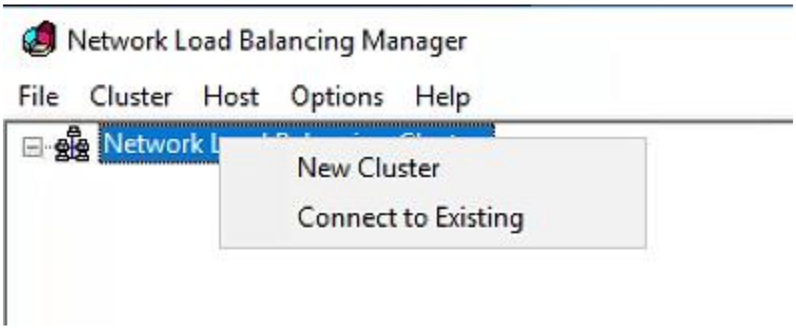
And the D-View 8 can be accessed with the cluster IP.



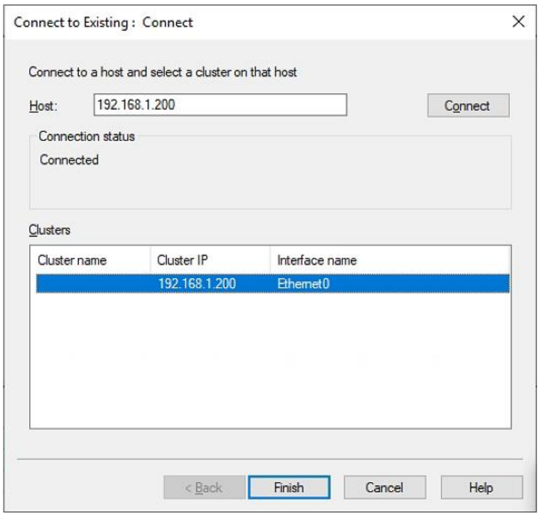
- On SERVER E

You can also manage the NLB cluster on server E by configuring NLB with the Network Load Balancing Manager.

1. Go to **Cluster > Connect to Existing.**



2. Enter the NLB cluster IP: 192.168.1.200, then click **Connect**.


Connect to Existing : Connect

Connect to a host and select a cluster on that host

Host: 192.168.1.200

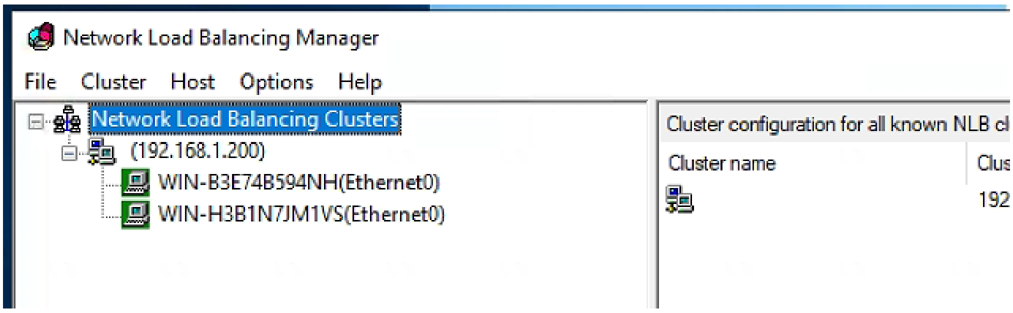
Connection status

Connected

Clusters

Cluster name	Cluster IP	Interface name
	192.168.1.200	Ethernet0

3. The NLB cluster will also be shown on server E.


Network Load Balancing Manager
File
Cluster
Host
Options
Help
Network Load Balancing Clusters
(192.168.1.200)
WIN-B3E74B594NH(Ethernet0)
WIN-H3B1N7JM1VS(Ethernet0)
Cluster configuration for all known NLB cl
Cluster name
Clus
192