



D-View 8

Network Management Software

User Manual

Network Management System

 **User Manual**



Table of Contents

内容

1	Introduction	7
1.1.	D-Link D-View 8 Network Management Software	7
1.2.	D-View 8 Features	7
1.3.	D-View 8 License Types.....	9
1.4.	90 Days Free Trial.....	9
1.5.	D-View 8 Server System Requirements	10
1.6.	D-View 8 Remote Probe Requirements	10
1.7.	D-View 8 Client Requirements	10
1.8.	Network Environment Models	11
1.9.	Device Groups	12
1.10.	User Authentication Types.....	12
1.11.	Preparing Network Devices for Discovery	12
1.12.	Continuing with D-View 8	12
2	Installation.....	14
2.1.	Requirements.....	14
2.2.	Windows Installation Guide.....	14
2.2.1.	Standalone Edition Installation.....	14
2.2.2.	Cluster Mode Installation (Only Enterprise Edition License Available).....	12
2.2.3.	Probe Package Installation	22
2.3.	Linux Installation Guide	24
2.3.1.	Standalone Edition Installation.....	24
2.3.2.	Cluster Mode Installation (Only Enterprise Edition License Available).....	25
2.4.	Software Upgrade	32
2.4.1.	Upgrading under Windows.....	32
2.4.2.	Upgrading under Linux.....	33
2.5.	Uninstalling.....	34
2.5.1.	Uninstalling under Windows.....	34
2.5.2.	Uninstalling under Linux.....	34

2.6. Software Migration	34
2.6.1. D-View 7 and D-View 8 Architecture	35
2.6.2. Installing a New D-View 8 Server.....	35
2.6.3. Installing D-View 8 in a D-View 7 Server.....	37
3 Getting Started	41
3.1. Logging In and Basic Configurations	41
3.2. Launching D-View 8 Web GUI	41
3.3. Understanding the Web Dashboard	43
3.3.1. Common Features	43
3.3.2. Menus and Toolbars.....	44
3.3.3. Annunciators.....	52
3.3.4. Workspace Preferences.....	53
3.4. Change the User Password	53
3.5. Change Account Information	55
3.6. Configure Email Server Alerts & Alarm Notifications.....	55
3.6.1. Configuring the Mail Server Settings.....	56
3.7. Configure the Notification Center	57
4 Overview and Management.....	61
4.1. Discovery Modes.....	61
4.1.1. Using Network Discovery	61
4.1.2. Using Device in Group	67
4.1.3. Add or Modify a Network Discovery Profile	67
4.1.4. Execute a Network Discovery Job.....	68
4.1.5. Delete a Network Discovery Profile	69
4.2. Manage Network Wired & Wireless Devices.....	69
4.2.1. View device information	69
4.2.2. View Discovered Device Information.....	70
4.2.3. View wireless device information.....	72
4.2.4. Modify device information	72
4.2.5. Ping or reboot a device	73
4.2.6. View and export an Interface List.....	74
4.3. Manage device groups.....	74

4.3.1. Add a device group	74
4.3.2. Edit (Remove) a device group.....	76
4.3.3. Add a Device to a Group.....	77
4.3.4. Remove a Device from a Group.....	79
5 Monitoring the Network	81
5.1. Viewing the default dashboard	81
5.2. Switch Dashboard	81
5.3. Wireless Dashboard.....	82
5.4. Host Dashboard	82
5.5. sFlow Dashboard	83
5.6. PoE Dashboard.....	83
5.7. Customizing the Dashboard.....	83
5.7.1. Create a Customized Dashboard	83
5.7.2. Modify a Customized Dashboard	87
5.8. View and Export Logs	89
5.9. View Report Settings.....	90
5.10. View Firmware Version.....	92
5.11. View D-View 8 Notifications.....	94
6 Manage Configuration and Firmware Settings	97
6.1. Creating Configuration and Profiles	97
6.1.1. Add a Configuration Task.....	97
6.1.2. Add a Configuration Profile	98
6.1.3. Modify and Delete a Configuration Profile	100
6.2. Managing Tasks	105
6.2.1. Viewing Current Tasks	105
6.2.2. Viewing Historical Tasks	107
6.3. Execute and Schedule a Firmware Upgrade	110
6.4. Backing Up Device Configurations.....	111
6.4.1. Add or Modify a Backup Profile.....	111
6.4.2. Restoring Device Configurations.....	113
6.5. Network File Management	114

6.5.1. Firmware Management	116
6.5.2. Configuration Management	120
7 Manage Alarms and Logs	125
7.1. View and Manage Alarms	125
7.2. View and Manage Traps and Syslog	126
7.3. Manage Trap Editor	126
7.4. Monitor and Manage Alarms	126
7.4.1. Add an Alarm Rule	127
7.4.2. View Monitor Settings	128
7.5. View and Manage Network Event Notifications	129
7.5.1. View and Manage Notification Events	129
8 Manage Architecture Topologies	137
8.1. View and Manage Network Topologies	137
8.1.1. View a Network Topology and Device Details	137
8.2. Creating a Topology View	140
8.3. Modify and Delete a Topology View	142
9 Manage Rack Groups	145
9.1. Add a Rack Group	145
9.2. View and Modify a Rack Group	147
10 Manage sFlow	153
10.1. Configuring sFlow Monitor	153
10.2. Manage sFlow Monitor	156
10.3. sFlow Network Monitor	157
10.4. View and Export sFlow Monitoring Results	159
10.5. Configure sFlow in Supported Devices	160
10.6. Configure sFlow Via CLI	162
11 View and Generate Reports	163
11.1. Generate Scheduled and My Reports	163
11.2. Manage Report Templates	164
11.2.1. Add a Report Template	165

11.2.2. Delete a Report Template	167
11.3. View and Remove Reports	168
12 Manage Users and Security Profiles	169
12.1. Profile Role Types	169
12.2. Authentication Credentials	171
12.2.1. Join an AD Server	171
12.2.2. View and Remove an AD Server	172
12.2.3. Join a RADIUS Server.....	173
12.2.4. Remove a RADIUS Server	175
12.3. Add a Profile	175
12.4. Modify or Remove a Profile	177
13 Manage Global Settings	179
13.1. Set Up Organization	179
13.2. Set Up a Mail Server	180
13.3. Set Up a Forward Trap	181
13.4. Set Up a Forward Syslog.....	181
13.5. Generate a REST API	182
13.6. Set Up SNMP Credentials	183
13.7. Set Up sFlow Settings	185
13.7.1. Application Mapping	186
13.7.2. DSCP Mapping	187
13.7.3. IP Alias Mapping.....	188
13.7.4. MAC Address Mapping.....	189
13.8. Set Up System Preferences	191
14 Manage Resources	193
14.1. Use a MIB Browser.....	193
14.2. MIB Compiler Tool	194
14.2.1. Add MIB Files.....	194
14.2.2. Compile MIB Files	195
14.2.3. Manage Device in MIB Browser	196
14.3. Perform an ICMP Ping.....	197

14.4.	Perform a SNMP Test.....	197
14.5.	Perform a Trace Route Test.....	199
14.6.	Configure Network Management from the CLI	200
14.7.	Compare Configuration Files.....	201
15	Appendix A D-View 8 Cluster Mode Installation Guide ..	202

1 Introduction

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

D-View 8 is a comprehensive wired and wireless network management tool based on the server and probe architecture, supporting the troubleshooting, configuration, performance and security of your network. It provides end-to-end business management of IT, scalability of system architecture, and accommodation of new technology and infrastructure while supporting the management of D-Link and third-party devices.

D-View 8's standard, enterprise and license options handle any network requirements, from SMBs to Enterprise deployments. The standard licence can manage up to 500 nodes for a single organization on multiple sites. Enterprise license handles up to 5000 nodes and supports multiple server probes, local or remote, across multiple sites and networks.



Figure 1 D-View 8 Interface

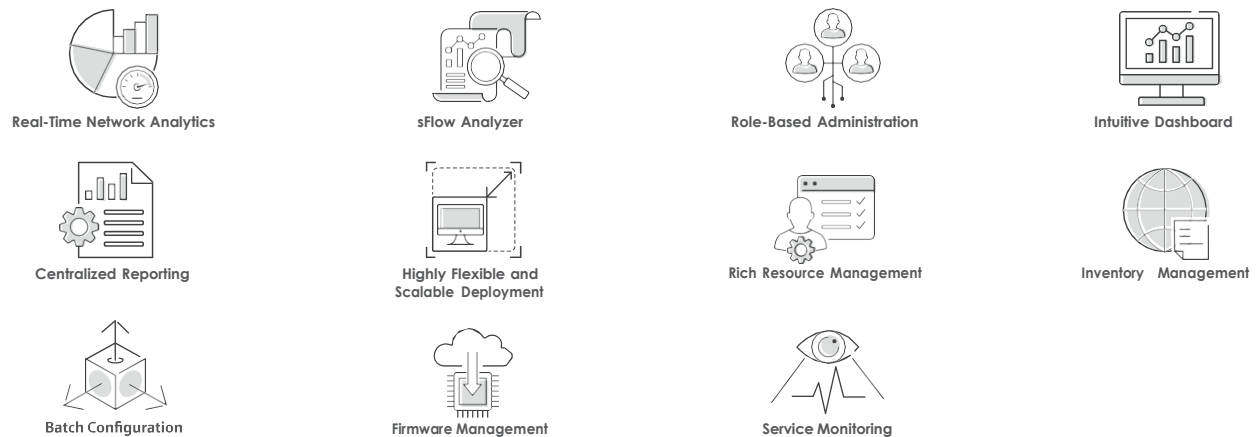







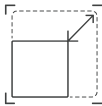


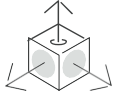
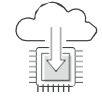

Figure 2 Features Overview

1.2. D-View 8 Features

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

This manual is intended for network administrators.

This release of the D-View 8 supports the following features:

D-View 8 Features		
	Real-Time Network Analytics	Real-time network analysis provides insight into network operations, where network visibility is extremely important. With D-View 8 you can gain insight on device statistics, critical alarms of managed devices, running status of wired and wireless devices, CPU/memory utilization, wired and wireless throughput of devices.
	sFlow Analyser	D-View 8 uses 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 reports.
	Role-Based Administration	Provides administrators with both the tools and the ability to grant access and privileges to only those features and resources operators need.
	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 many more.
	Centralized Reporting	Provides performance of administrator, operator performance, and options for resource reporting configuration and configuration changes, network device and connection status, for network properties, alarms, and the health of network equipment. Report types are issued in real time and personalized easily. Device data is given for status, mark, IP address, MAC address, type of device, model, supplier, the location and many more.
	Highly Flexible and Scalable Deployment	Depending on your network size, D-View 8 has you covered with a whole suite of network capabilities and deployment options.
	Rich Resource Management	Provides the exploration and topology of the network, including comprehensive network inventory and Precise representations of how it is configured. Sponsored views include both Layer 2 and Layer 3, as well as similar VLAN topology and the ability, like a dashboard home page, to create custom views.
	Inventory Management	Provides holistic management using a single pane of glass for multi-vendor devices. Administrators can access tools to control and monitor several facets of a network topology, IP, or custom view, the system connects devices to the network and displays devices. Administrators may also assess a system's health through the specifics of the device page, which reveals real-time data, summary information, connectivity testing, and more.
	Batch Configuration	Configure multiple devices at the same time using SNMP or telnet.
	Firmware Management	Conveniently upgrade firmware for multiple devices from a centralized location.
	Service Monitoring	Monitors the availability and responsiveness of common network services via probes that you configure. The probes reside on local and remote D-View 8 software agents and test services from servers and devices that you select when configuring the probes.

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 website.

NOTE: For the latest firmware updates with new features and bug fixes, visit the D-View website. Some devices are designed to regularly download and update new firmware, or only possess a manual update function. If the features of the devices are not described in this guide, you may need to update the firmware.

1.3. D-View 8 License Types

License Types	
Standard (DV-800S)	Target Customer: SMB <ol style="list-style-type: none"> 1. Nodes: < 500 2. D-View Server and Probe: <ul style="list-style-type: none"> • Single server, no support for redundancy. • Single probe. 3. Supports local probe only. 4. The Org-Site-Network Architecture: <ul style="list-style-type: none"> • Single Organization • Multiple Sites • Multiple Networks 5. Supports limited features.
Enterprise (DV-800E)	Target Customer: Enterprise <ol style="list-style-type: none"> 1. Nodes: <5000 2. D-View Server and Probe: <ul style="list-style-type: none"> • Supports 2 servers and HA (High Availability) • Multiple Probes 3. Supports both local and remote probes. 4. The Org-Site-Network Architecture: <ul style="list-style-type: none"> • Single Organization • Multiple Sites • Multiple Networks 5. Supports all features.

1.4. 90 Days Free Trial

Network administrators need cutting edge tools to help maintain and effectively manage their network systems. D-Link is at the edge of innovation and fully committed to the development of applications to match their new hardware functionality and exceed the demands of the marketplace.

Download the D-View 8 application and test it free for 90 days.

The current version of the application is available for download at <http://dview.dlink.com/>.

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)	<ul style="list-style-type: none"> • Windows Server 2012 64-bit (Standard Edition or above with the latest patches) • Windows Server 2012 R2 64-bit (Standard Edition or above with the latest patches) • Windows Server 2016 64-bit (Standard Edition or above with the latest patches) • Windows Server 2019 64-bit (Standard Edition or above with the latest patches) • Windows 10 64-bit (Professional Edition or above with the latest patches) • Ubuntu 18.04 64-bit or above • Debian 10 64-bit or above
Database	MongoDB 4.0 or above
Web Browser	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Windows Server 2012 64-bit (Standard Edition or above with the latest patches) • Windows Server 2012 R2 64-bit (Standard Edition or above with the latest patches) • Windows Server 2016 64-bit (Standard Edition or above with the latest patches) • Windows Server 2019 64-bit (Standard Edition or above with the latest patches) • Windows 10 64-bit (Professional Edition or above with the latest patches) • Ubuntu 18.04 64-bit or above • Debian 10 64-bit or above
Managed Capability	500 Nodes

1.7. D-View 8 Client Requirements

Client System Requirements	
CPU	Dual-core, 3.0 GHz or above
RAM	4 GB or above
Storage	100 GB or above

Client System Requirements	
Web Browser	<ul style="list-style-type: none"> • Chrome • Firefox • Safari • Edge

1.8. Network Environment Models

The application resides on the D-View 8 server at a static IP address on the local area network (LAN). By design the application manages the D-Link and third-party devices on the network.

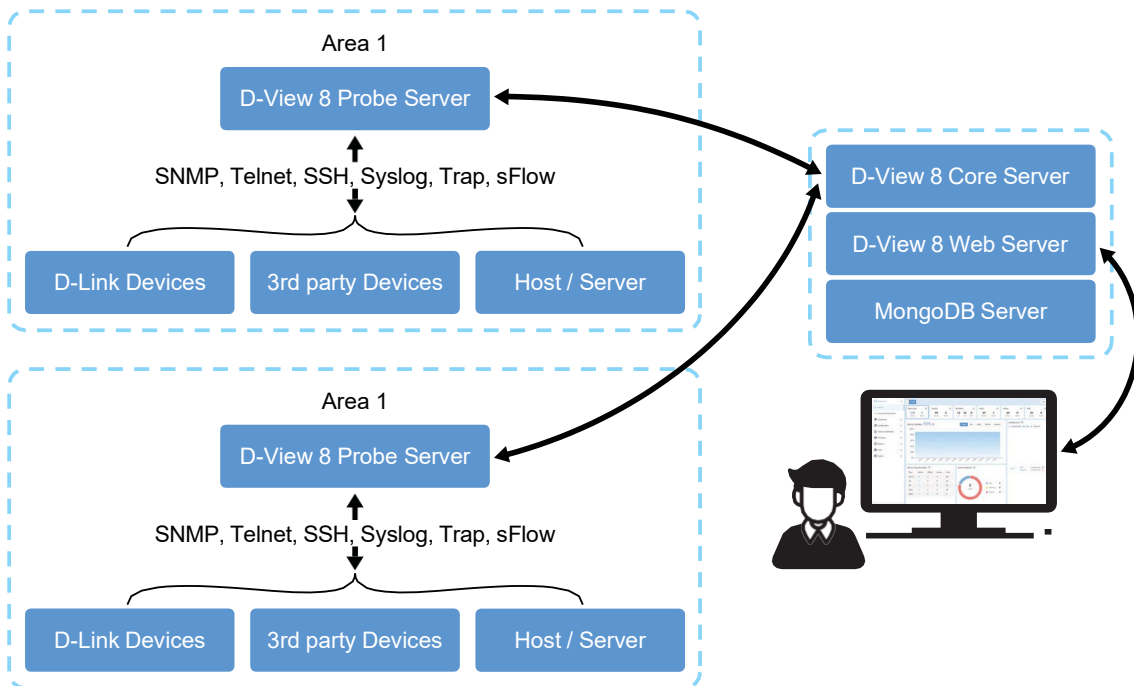


Figure 3 The Network Management System

The D-View 8 application is accessed through a web browser. If the IP address is located outside the Internet gateway, access to the network must first be permitted.

The application supports the following devices:

- D-Link devices supporting SNMP protocol
For further information about supported D-Link devices, including model numbers, see the official D-View website.

1.9. Device Groups

Network management is simplified with the D-View 8 through the use of the device group's function. Device Groups can be identified by site, network, location, vendor, device type, device model, category and IP address.

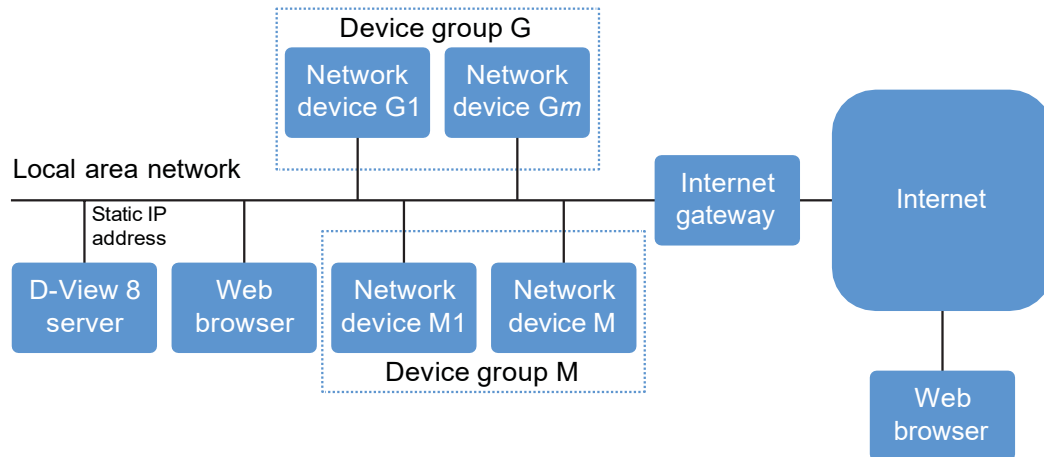


Figure 4 Device groups

1.10. User Authentication Types

User authentication for the D-View 8 application is available in three specific types. By associating an authentication profile to a user, privilege and access to the network is easily managed. See the following types of authentications supported:

- 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. Preparing Network Devices for Discovery

Preparing any device on your network requires setup and configuration to allow for effective management. The D-View 8 edition (Standard, Enterprise) determines the number of devices that can be managed.

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 is configured to use IPv4 or IPv6 settings.

1.12. Continuing with D-View 8

Making full use of the D-View 8 management system requires performing a few basic configuration tasks and discovering your networks along with the corresponding devices.

Chapter 2: "Installation"

Chapter 3: "Getting Started"

This page is intentionally left blank.

2 Installation

The D-View 8 software supports installation on a Linux or Windows operating system. The following section provides guidance for the installation of the software on both platforms.

To begin the installation process, download the D-View 8 setup application from the D-View website. Once downloaded, the wizard-based package allows for a simple installation process.

2.1. Requirements

See the following for further information, “1.5. D-View 8 Server System Requirements” on page 04.

2.2. Windows Installation Guide

2.2.1. Standalone Edition Installation

To begin the installation process, download and locate the software package.

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



Figure 5 Welcome Screen Installation Wizard

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

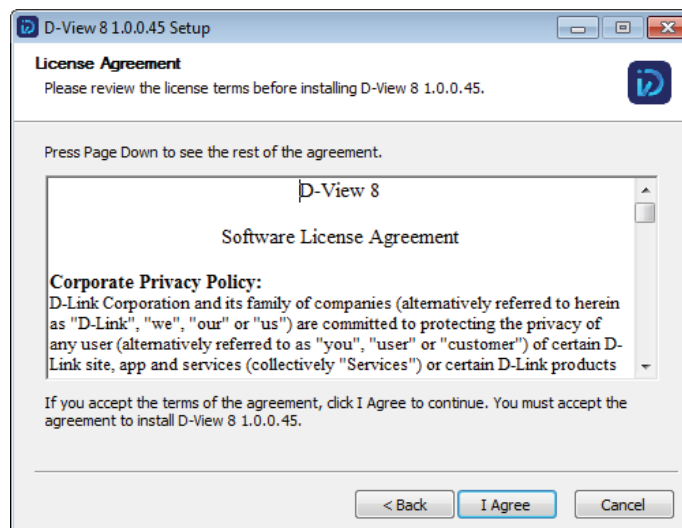


Figure 6 License Agreement Screen

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 relevant local IP address.
6. Click **Check** to test the service port availability. If Check Pass turns green, the test passed.
7. Click **Next** to continue.

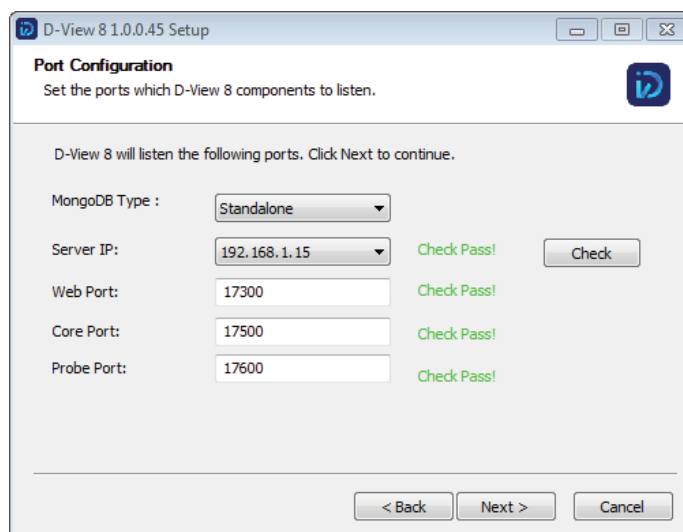


Figure 7 Port Configuration Screen

D-View 8 requires a database service such as MongoDB. By installing the MongoDB, the installation process will register it on the server. You can select to install a new database or use an existing one, see the following options.

To install a new MongoDB database:

- a. Select Install a new MongoDB if not already selected.
- b. Click **Next** to continue.

In order to access the database, a username and correlating password must be assigned to access the database.
- c. In the MongoDB Port field, enter the designated port which is used to provide access to the database.
- d. Enter the username and password to use to authenticate the access.
- e. Click **Next** to continue the process.

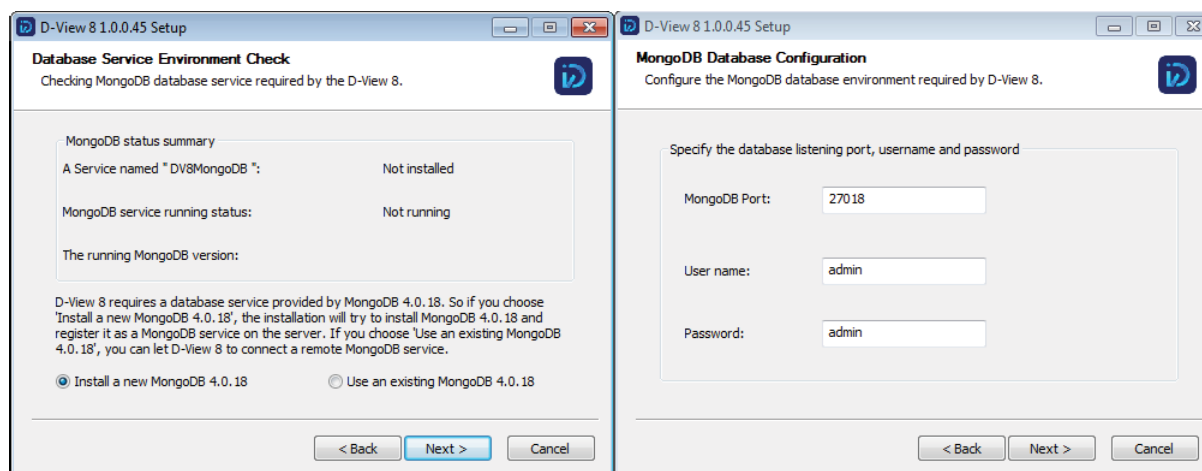


Figure 8 Service Environment and Database Configuration Screens

To install by using an existing MongoDB database:

- a. Select **Use an existing MongoDB** if not already selected.
- b. Click **Next** to continue.

In order to configure the database environment, provide the required settings to access the existing database.

- c. In the MongoDB Address field, enter the current address and port linked to 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 confirmed, the **Next** button is enabled.

If the connection cannot be confirmed, check the settings and re-enter the related information.

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

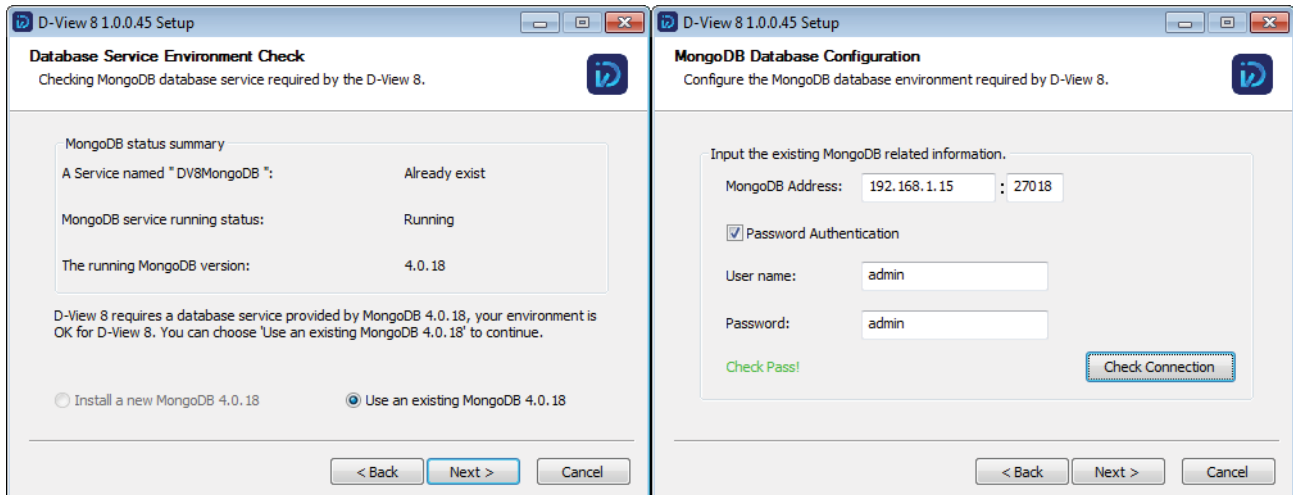


Figure 9 Service Environment and Database Configuration Screens

The Choose Installation Location page displays.

8. In the Destination Folder field, click **Browse** to select a specific folder.
9. Click **Install** to continue or **Back** or **Cancel** to restart the process.

The installation process continues as shown in the Installing page.

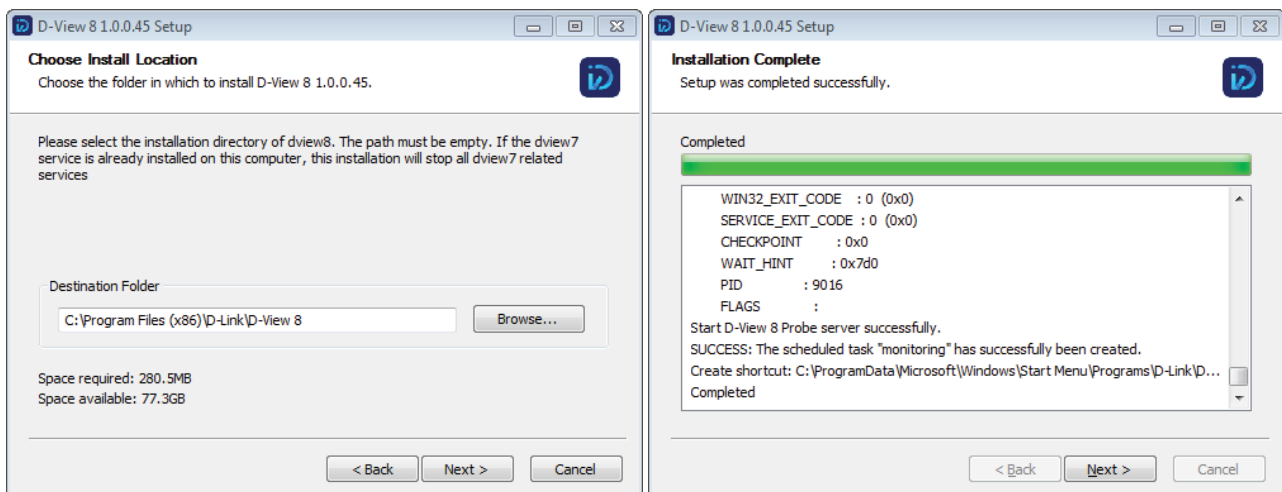


Figure 10 Installation Location Screen

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

10. Select Launch D-View 8 and click **Finish** to display the user interface on the default browser.



Figure 11 Completion Setup Wizard Screen

The following instance is a First-use scenario of the login process.

The D-View 8 login page displays. By default, the Account Type field displays Local. First time users can choose to enter an activation code or use a trial account.

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

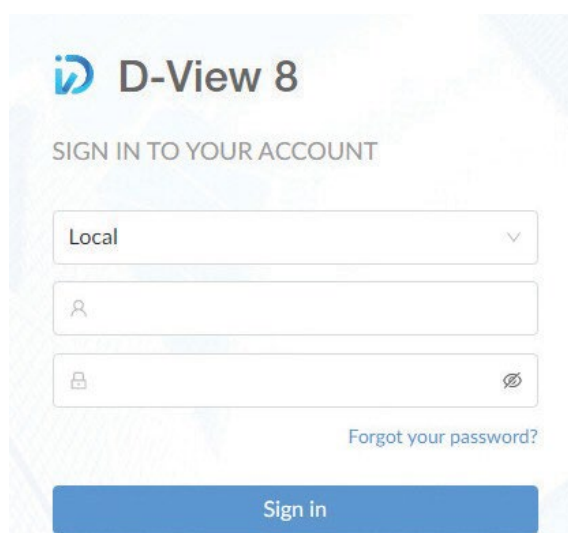


Figure 12 Login Screen

The Add License page displays. From this screen, you can set a specific language (default: English) prior to registering a license.

12. Under the Choose Activation Mode panel, select a license type to activate, or click **Try System** 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 the 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.
 - Try System: try a 90-day trial version of the application. Download the trial from the official D-Link website: <http://dview.dlink.com/>.

13. Click **Next** to continue.

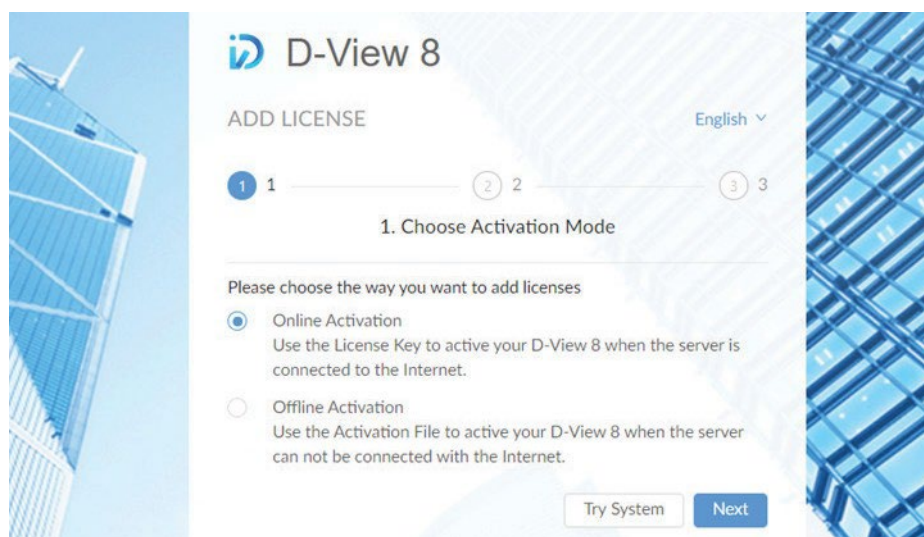


Figure 13 Activation Screen

The D-View 8 Wizard page displays. Based on the account privilege, the available information for configuration displays in the page.

- D-View 7 Upgrade: the option allows for the migration of D-View 7 database and probes to the current application.
- Discovery: the option allows for the discovery and configuration of the available network or connected devices.
- Monitoring: the option allows for the creation of topologies, rack simulations, and dashboard to help monitor the network.
- Alarm: the option allows for the configuration of system wide notifications and alarms.

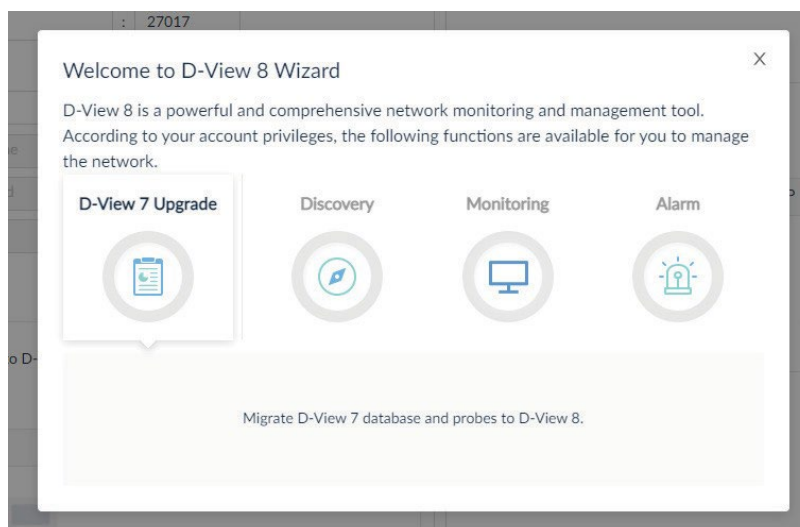


Figure 14 Upgrade Wizard Screen

You can elect not to use the Wizard function by clicking the Cancel (X) option at the top of the page.

Once the installation is complete, the user interface displays. See the following figure to view the D-View 8 Dashboard.

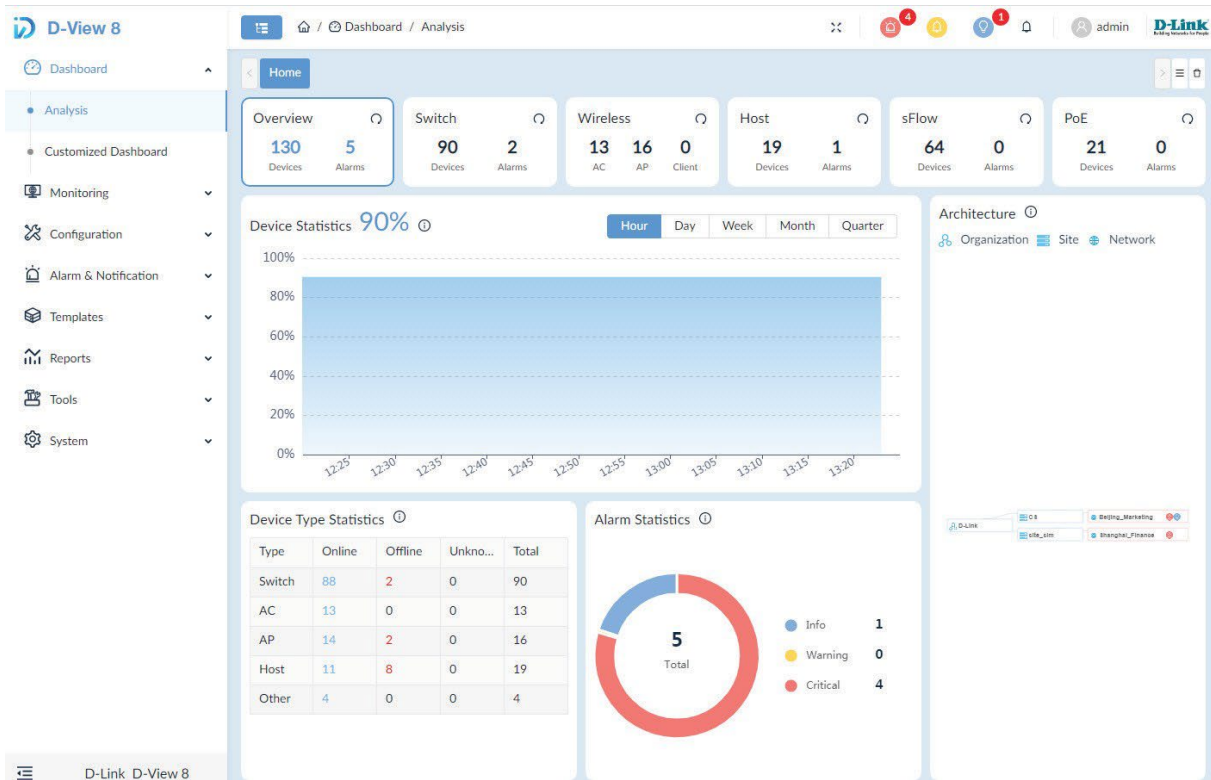


Figure 15 D-View 8 Dashboard

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

2.2.2.1. Cluster Architecture

The D-View 8 supports redundancy and load balancing features. The following diagram provides a descriptive illustration of the cluster architecture.

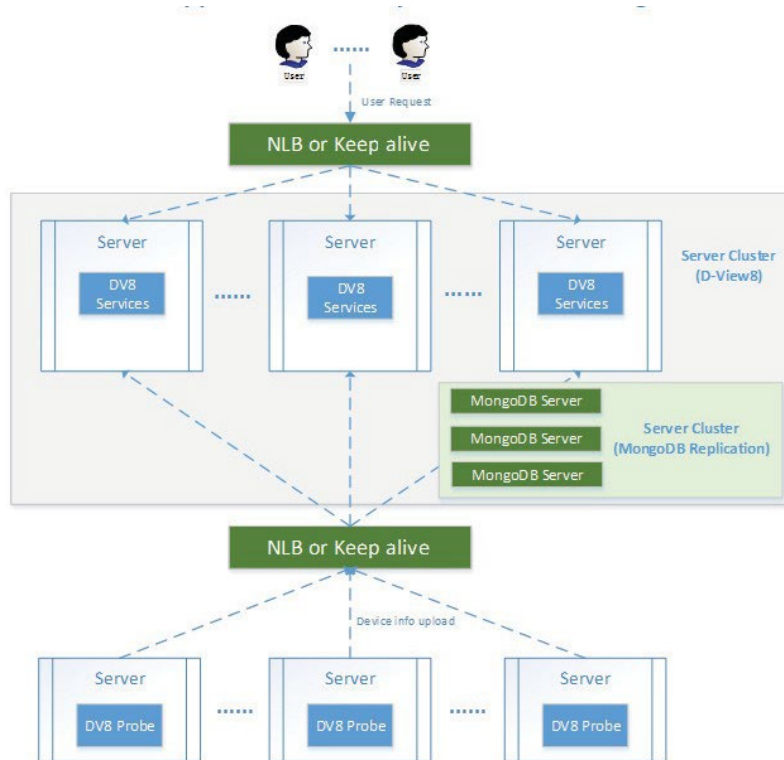


Figure 16 Cluster Architecture

The following is a diagram of the D-View 8 and MongoDB set frame. The set frame includes a primary, secondary, and arbiter. In the architecture design, the application connects to the primary and secondary. By design

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

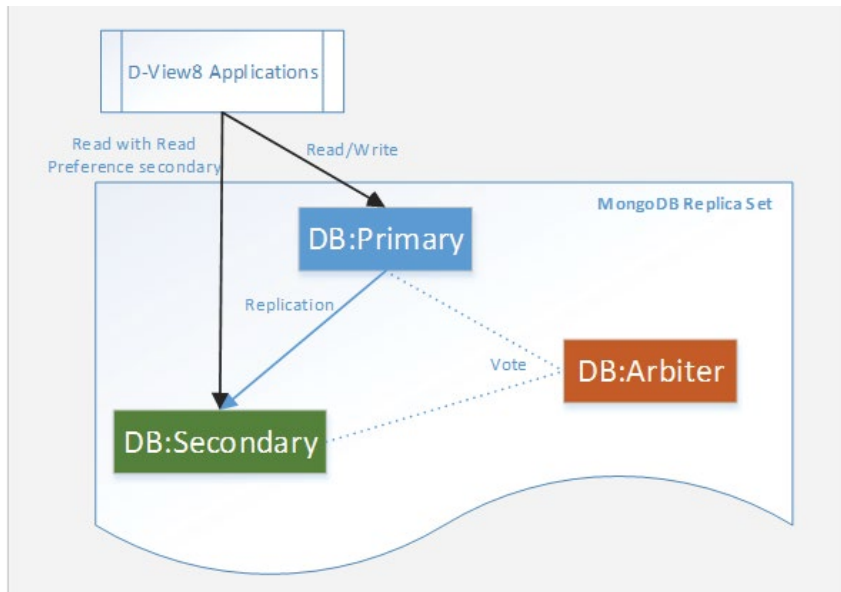


Figure 17 MongoDB Set frame Diagram

2.2.2.2. Cluster Building Steps

Building clusters is outlined through the following steps. The illustrations are intended to server as examples of the process.

To support data redundancy:

1. Allocate three servers and install MongoDB.

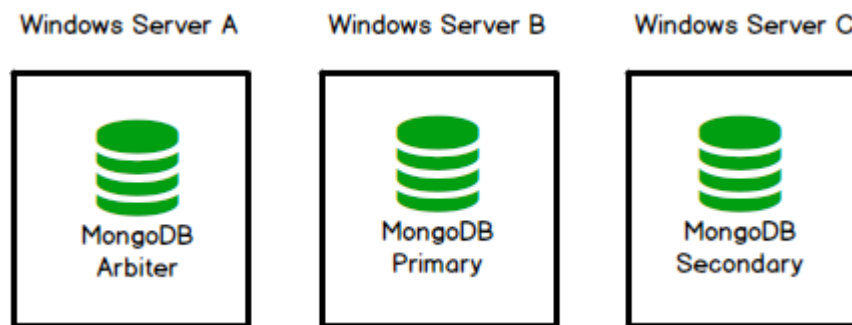


Figure 18 Multiple Server Diagram

2. Install D-View 8 in multiple servers and connect the application to the MongoDB cluster.

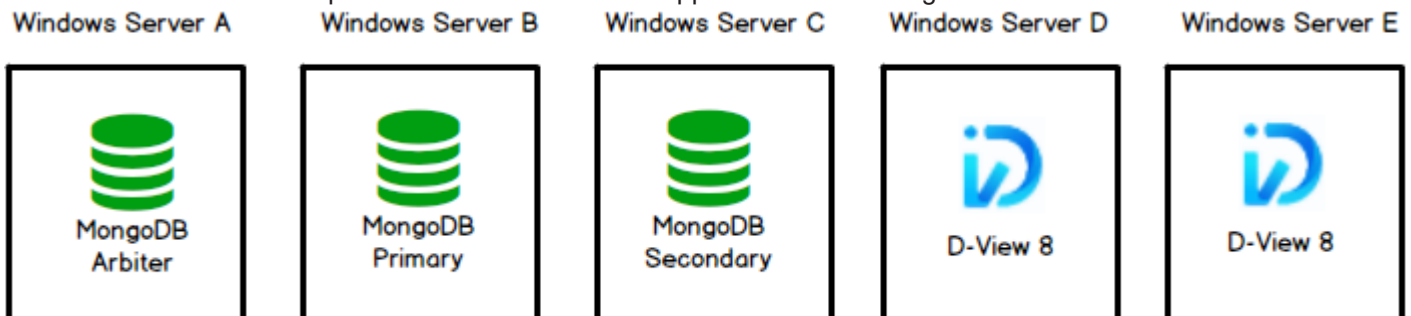


Figure 19 Connecting to a Cluster

To support server load balancing:

3. In Windows server, install NLB.

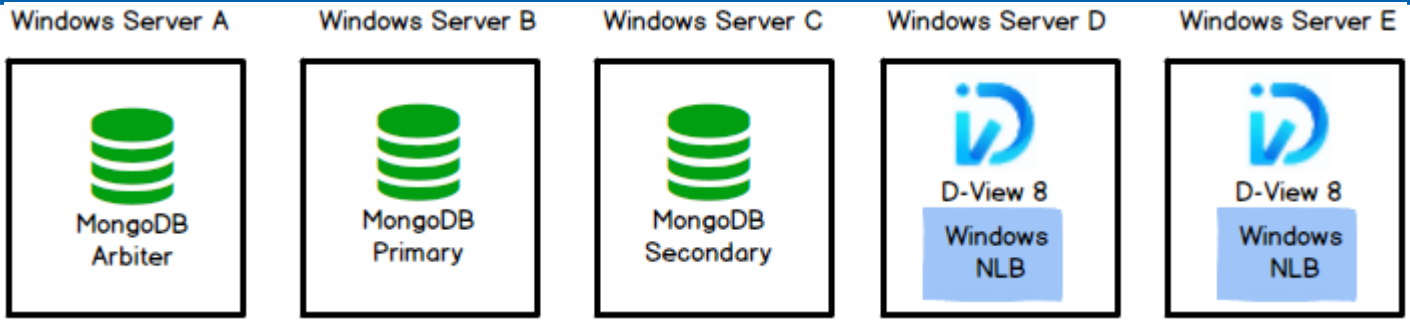


Figure 20 NLB Installation Diagram

4. To manage additional devices, add a probe in an additional server and connect the application through NLB.

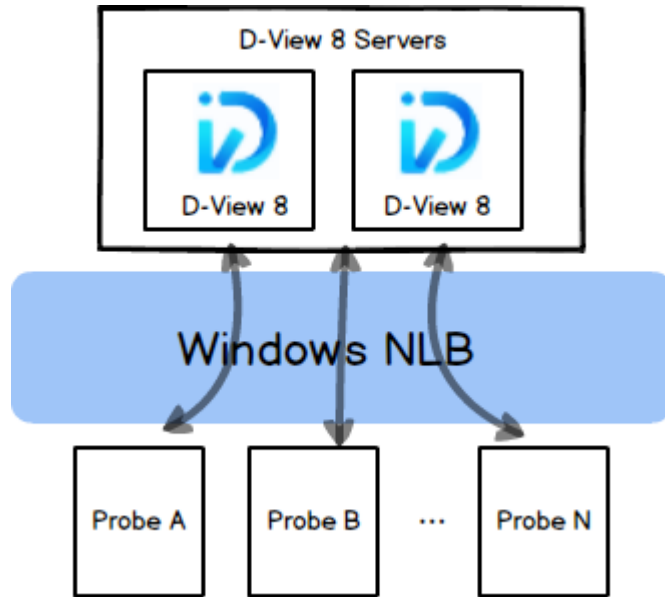


Figure 21 NLB Architecture Diagram

Data Redundancy Support

Building a cluster is expanded in the following section which describes the data redundancy support.

1. First allocate three servers to install MongoDB
2. Download the D-View 8 MongoDB installation package.
3. Install the package on all three servers, A, B., and C, respectively.
4. In the Connection Configuration page, click MongoDB Type drop-down menu and select **Replication**.
5. Enter the MongoDB port number configured for server access.

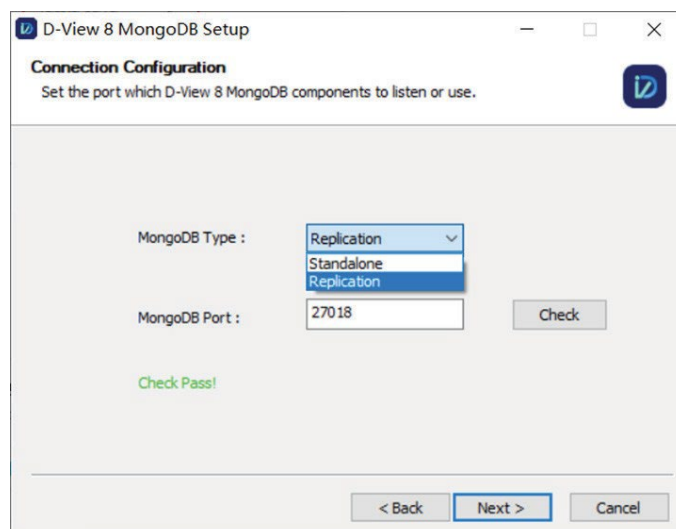


Figure 22 Configuring MongoDB Type

6. Click **Check** to test the setting. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port setting and re-enter the value.
7. Click **Next** to continue.

Multiple Server Installation

The following section provides information to install the D-View 8 application in multiple servers and connect them to the MongoDB cluster.

1. Download the D-View 8 Installation package.
2. Install the package on the target server.
3. In the Connection Configuration page, click MongoDB Type drop-down menu and select **Replication**.
4. In the Server IP field enter the target server's IP address.
5. In the Web Port field, enter the port number authorized to provide web access.
6. In the Core Port field, enter the port number representing the core server.
7. In the Probe Port field, enter the port number designated for the probe access.

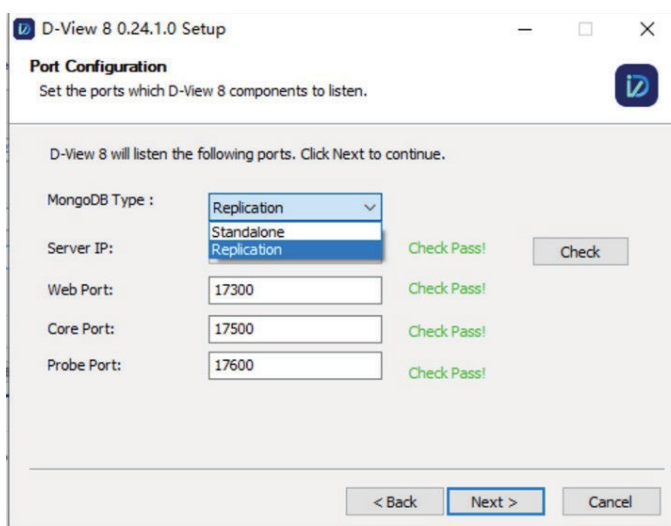


Figure 23 Configuring Probe Port

8. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the port settings and re-enter the values.
9. Click **Next** to continue.

The MongoDB Database Configuration page displays.

The following steps will help to configure the MongoDB database environment to establish a connection with the application

10. In the Primary field, enter the IP address and port number of the primary instance. The primary server receives write and read operations.
11. In the Secondary field, enter the IP address and port number of the secondary instance. The secondary is relegated to a primary environment if the current primary becomes unavailable.
12. In the Arbiter field, enter the IP address and port number of the arbiter instance. The arbiter is part of the replica set but does not hold data, does not provide redundancy. It does, however, participate in elections

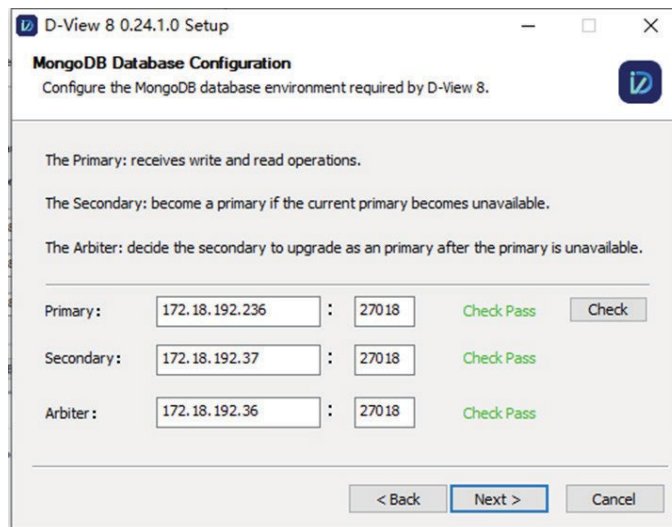


Figure 24 Configuring MongoDB Database Environment

13. Click **Check** to test the settings. If configured correctly, a **Check Pass!** notification displays. If the test fails, verify the environment settings and re-enter the values.
14. Click **Next** to continue.
The Choose Install Location page displays.
15. Click **Browse** to select the destination folder, and click **Install** to continue.
16. Once the installation completes the Setup Wizard page displays, select Launch D-View 8 to launch the application after the wizard is closed.
17. Click **Finish** to complete the installation process.



Figure 25 Completing Setup Wizard Screen

Network Load Balance for Load Balancing Deployment

Server load balancing is supported by the application. The following are requirements to install and run a network load balancing cluster.

- Operating system: Windows server 2008 R2, Windows Server 2012, Windows Server 2016 or Windows Server 2019
- Service needed: Network Load Balancing (NLB)

Hardware requirements

- All hosts in the cluster must reside on the same subnet.

Topological structure:

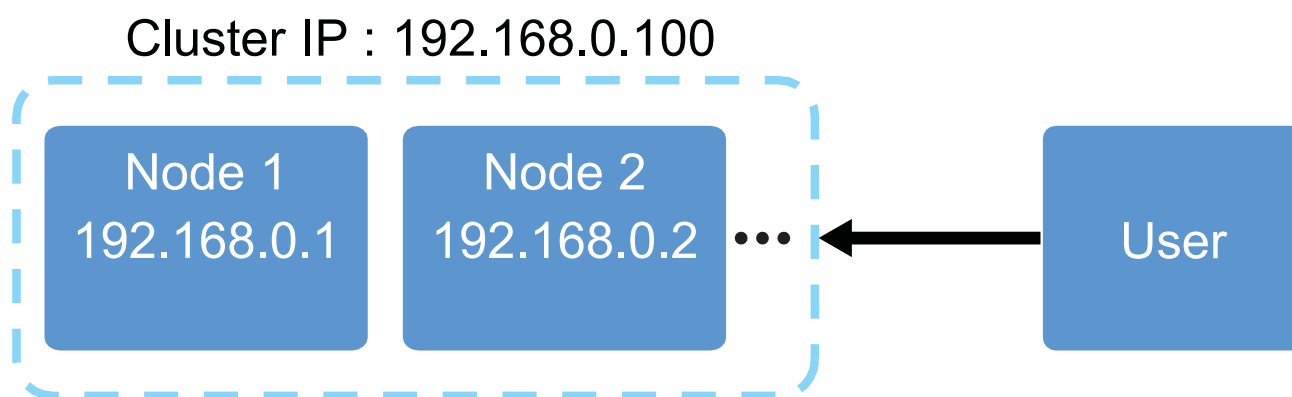


Figure 26 Cluster Topological Diagram

To install NLB:

1. Prepare two servers, minimum, with either a Windows Server 2008 R2 or Windows Server 2012.
2. Configure the node server IP address within the same net segment.
3. Install the Network Load Balancing service.
4. From Administrative Tools -> Tools start Network Load Balancing Manager.
5. In NLB Manager, right click **Network Load Balancing Cluster** to display the available options.
6. Click **New Cluster** to open the New Cluster: Connect.

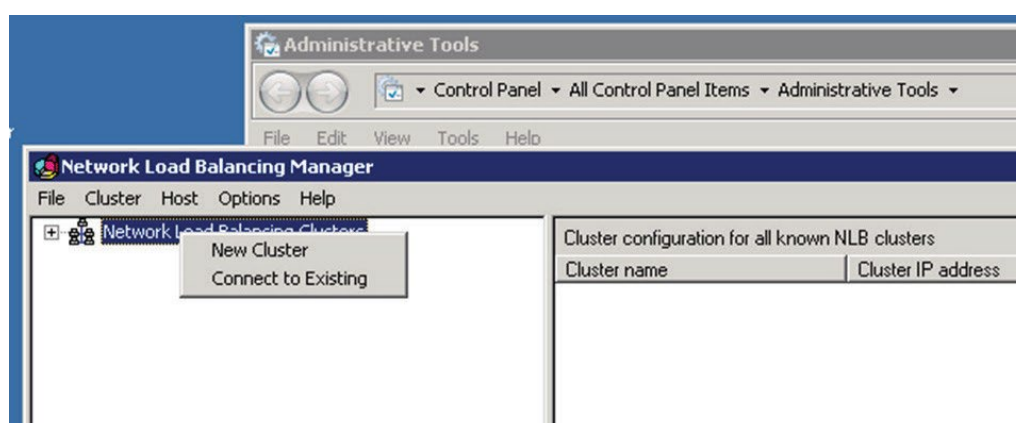


Figure 27 Network Load Balancing Manager

7. In the Host field, enter the node server IP address.
8. Click **Connect** to add the defined node to the cluster.
Added nodes now available for the new cluster appear in the Interfaces available pane.

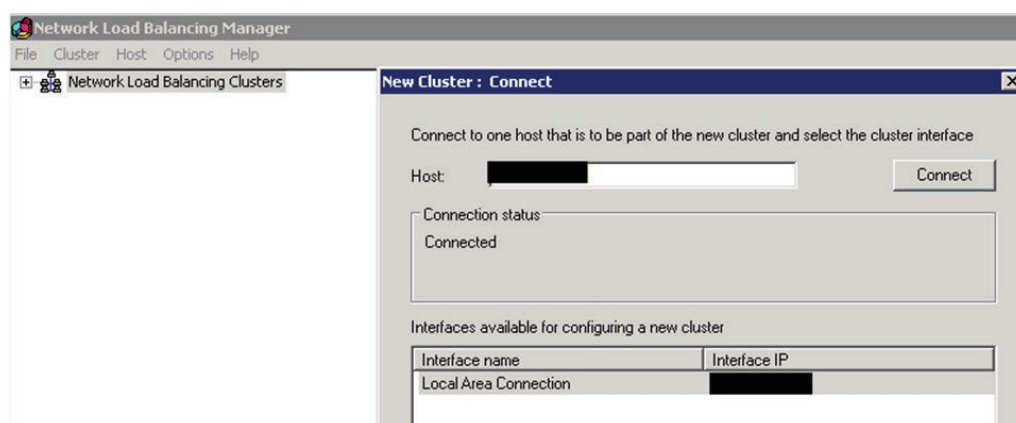


Figure 28 New Cluster Connection Setup

9. Click **Next** to continue. The Host Parameters page displays.
10. Click the Priority drop-down menu to set the host priority. By definition the lower the priority identifier the higher

the performance. Priorities for all hosts must be unique in the cluster.

11. To include additional dedicated addresses, click **Add** and enter the required information.
12. To modify existing entries, click **Edit** and modify the posted information.
13. To delete an entry, select an entry and click **Remove**.

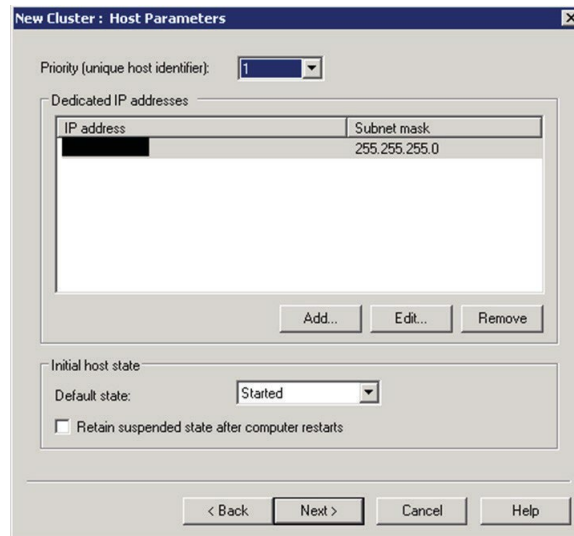


Figure 29 Configuring Host Parameters

14. From the Default state field, click the drop-down menu to determine what happens when the NLB host starts up. Host state options are described as follows:
 - To have the host immediately join the cluster when Windows starts up, select the **Started** option.
 - To manually join the host to the cluster after starting, select the **Stopped** option.
 - To have the host start without joining the cluster and enter a suspended state, select **Suspended**.

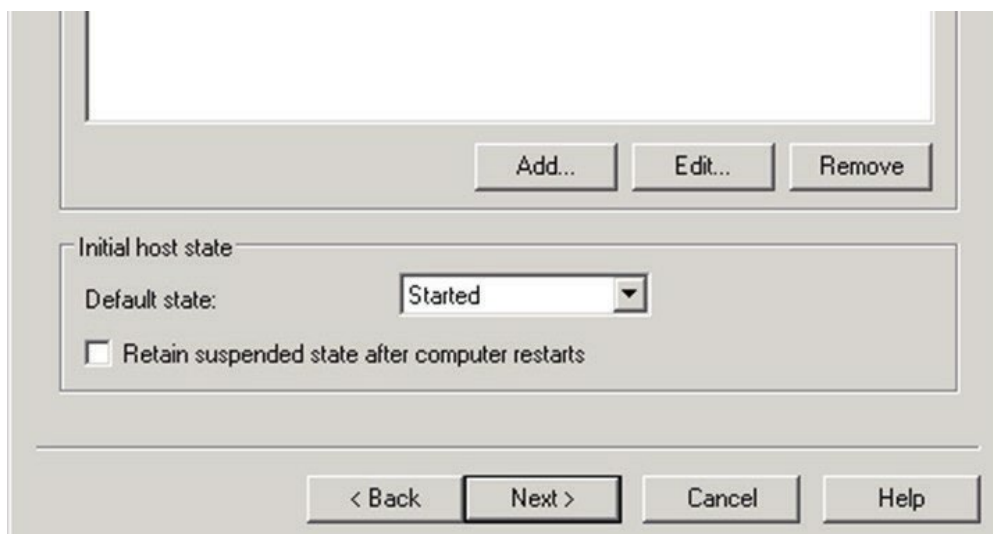


Figure 30 Configuring Default State



NOTE: If host is suspended, it will not take part in any clustering operations until the resume command is issued; all other cluster commands are ignored by the host with the exception of the query command. You can instruct the host to resume NLB cluster operation from either the command line or by using the Network Load Balancing Manager

15. Click **Next** to continue. The New Cluster: Cluster IP Addresses page displays.
16. Click **Add** to include a cluster IP address(es). The addresses are shared by every member of the cluster group for load balancing. The first IP address entered is designated as the primary cluster IP address for cluster heartbeats. The Add IP Address page displays.
17. Select either **Add IPv4 address** or **Add IPv6 address** to specify a static address.

18. Alternatively, select **Generate IPv6 addresses** automatically generate IPv6 addresses for the IPv6 Address resources on your networks.
19. Click **OK** to continue.

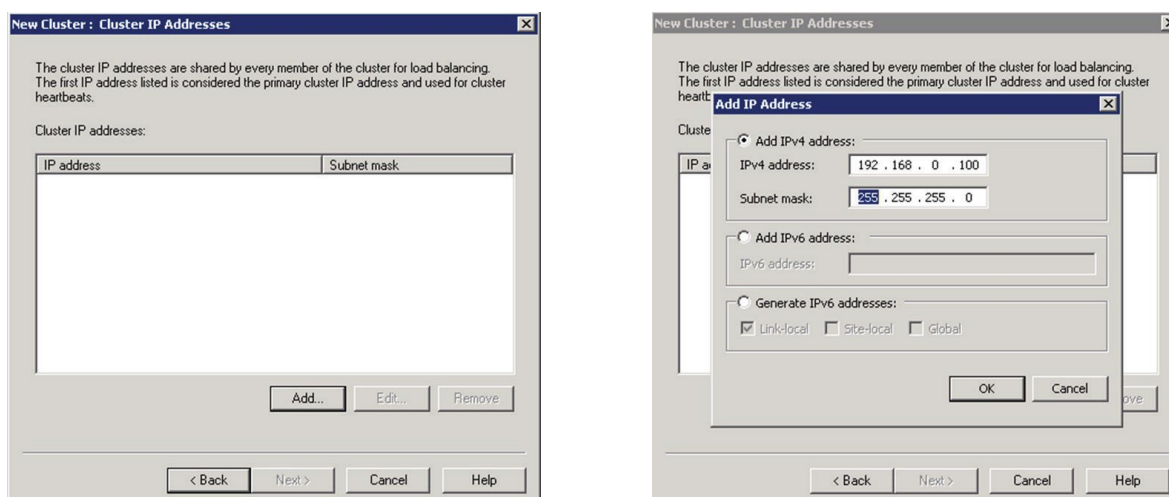


Figure 31 Configuring Cluster IP Addresses

The New Cluster: Cluster Parameters page displays.

The following demonstrates the configuration of the cluster parameters. The IP address is defined in the previous step.

20. In the Full Internet name field, enter the registered domain name.
21. In the Network address field, enter the correlating address associated with the registered name.

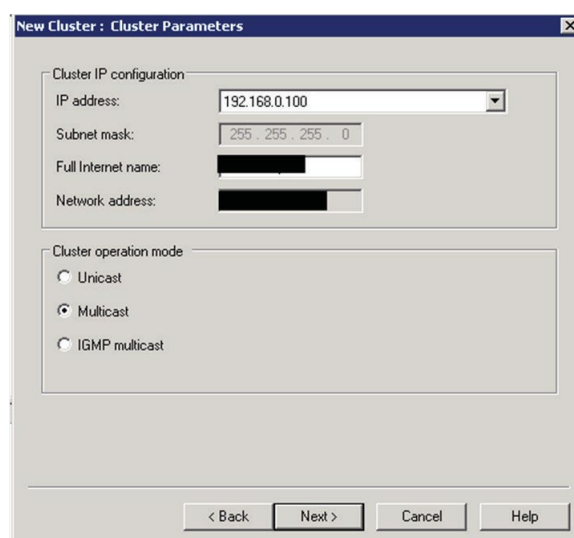


Figure 32 Configuring Network Address

The cluster operation mode determines how the cluster network address is configured and how that address relates to the existing network adapter addresses. All nodes within a cluster must use the same cluster operations mode.

- **Unicast Mode:** all nodes in the cluster use the MAC address assigned to the virtual network adapter. NLB substitutes the cluster MAC address for the physical MAC address of a network card and used with the cluster. Use two network adapters if selecting unicast, one to manage.
- **Multicast Mode** Multicast mode is a suitable solution when each node in the cluster has a single network adapter (multicast cluster MAC address). The cluster IP address resolves to the multicast MAC address. Each cluster node uses its network adapter's MAC address for management and internode communication.
- **IGMP Multicast Mode** This version of multicast uses Internet Group Membership Protocol (IGMP) for communication, improving network traffic due to traffic passing only to switch ports the cluster uses.

22. In the Cluster operation mode panel, select Multicast mode.
23. Click **Next** to continue to configure the port rules. The Port Rules page displays

24. Select a defined port rule and click **Edit**. The Add/Edit Port Rule page displays.
25. From the Filtering mode panel, select **None** for Affinity.
26. Click **OK** to continue.

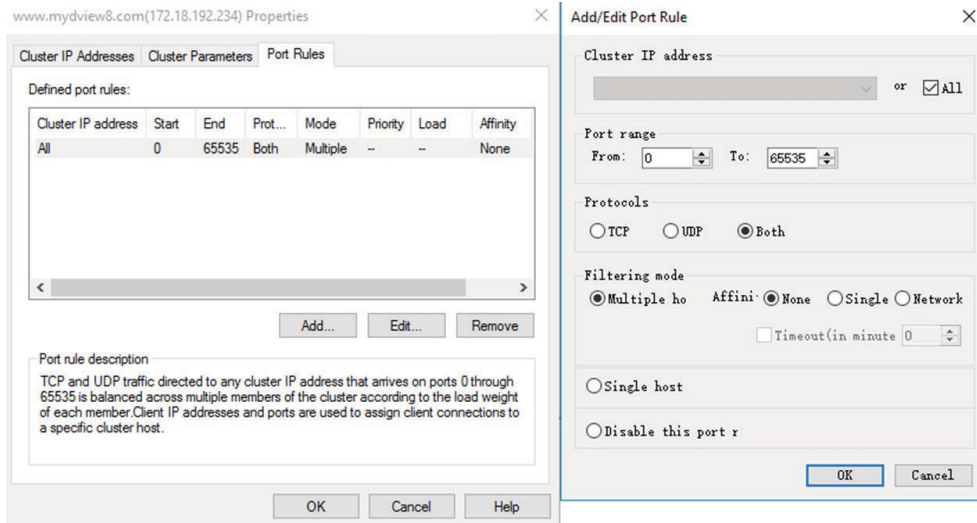


Figure 33 Adding Port Rule

The Network Load Balancing Manager displays.

27. Select the defined cluster and right click to open the properties menu.
28. Click **Add Host to Cluster**. The Add Host to Cluster: Connect page displays.

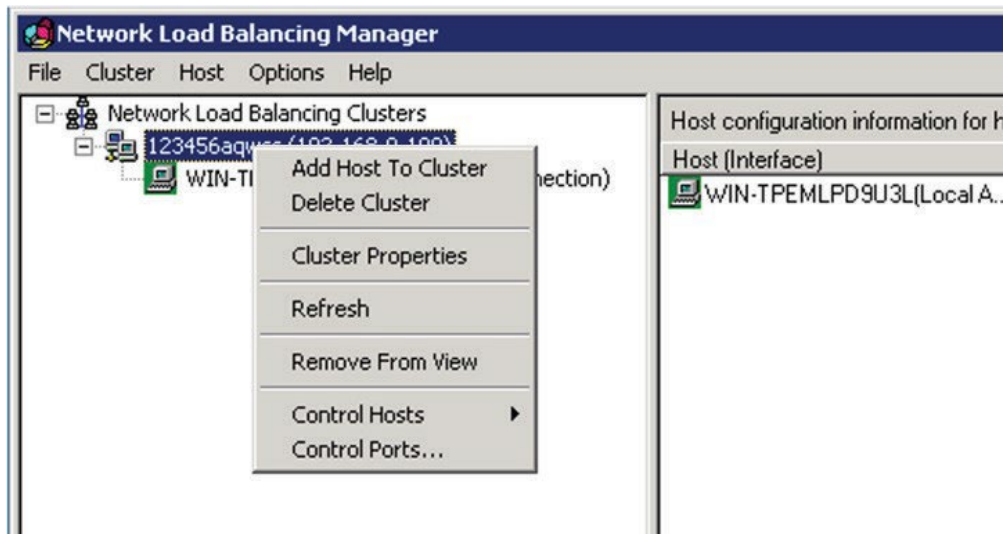


Figure 34 Adding Host to Cluster

29. In the Host field, enter the node (2) server IP address.
30. Click **Connect** to establish the cluster entry. After connecting, the interface displays in the Interface pane.
31. Click **Next** to continue. Follow the procedures as instructed in the previous node.
32. Open the Network Load Balancing Manager displays on node 2.
33. Select the cluster and right click to open the properties menu.

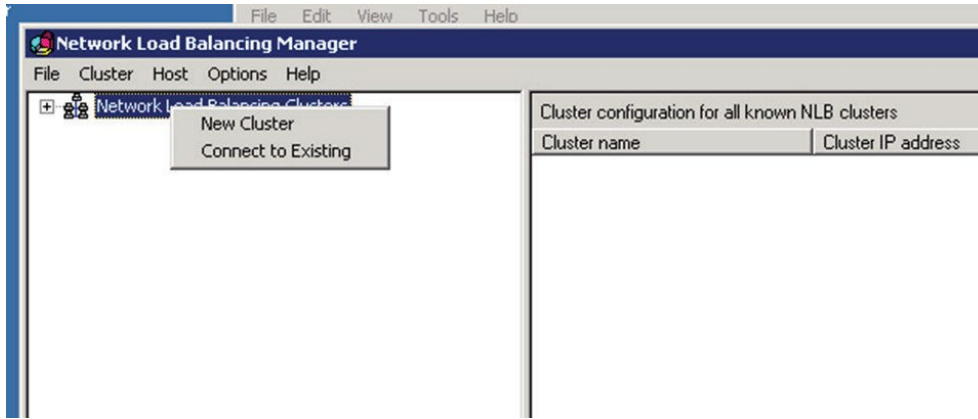


Figure 35 Selecting a Cluster

- 34. Click **Connect to Existing**. The Connect to Existing: Connect page displays.
- 35. In the Host field, enter the node 1 server IP and click **Connect**.

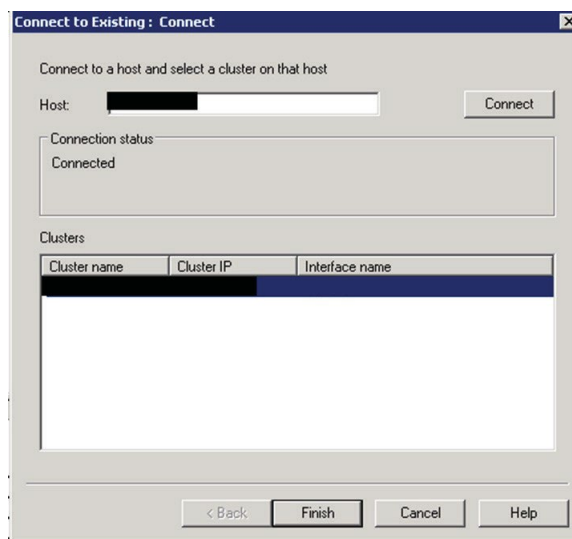


Figure 36 Adding a Node Server IP

- 36. Once the connection is established, click **Finish** to return to the Network Load Balancing Manager.

To determine the configuration information, view the Status column. The determiner displays Converged if the cluster configuration of the servers is established.

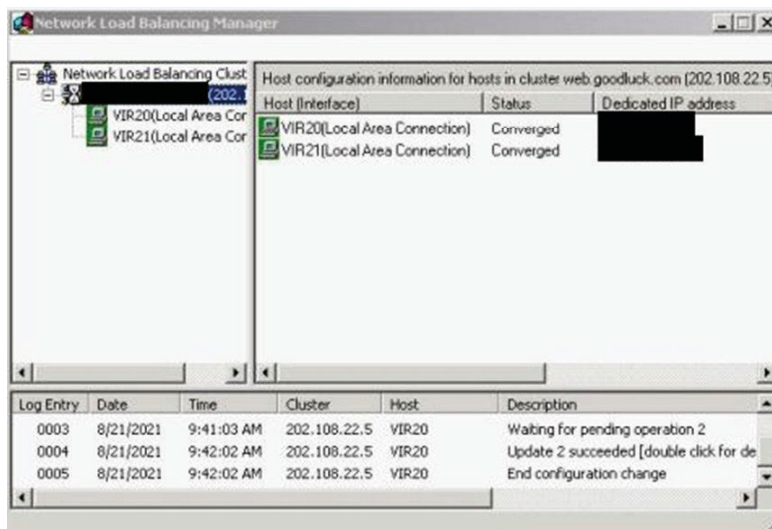


Figure 37 Verifying an Established Cluster

The NLB cluster is configured with two nodes. Both nodes can be accessed through the cluster IP.

2.2.3. Probe Package Installation

The D-View 8 probe installation can be accomplished through the setup wizard. Prior to starting the process, it is recommended to 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 setup package and double click on it to bring the wizard. The Probe Setup page displays.
2. Click **Next** to continue the installation process.



Figure 38 D-View 8 Probe Setup Wizard

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 setup.

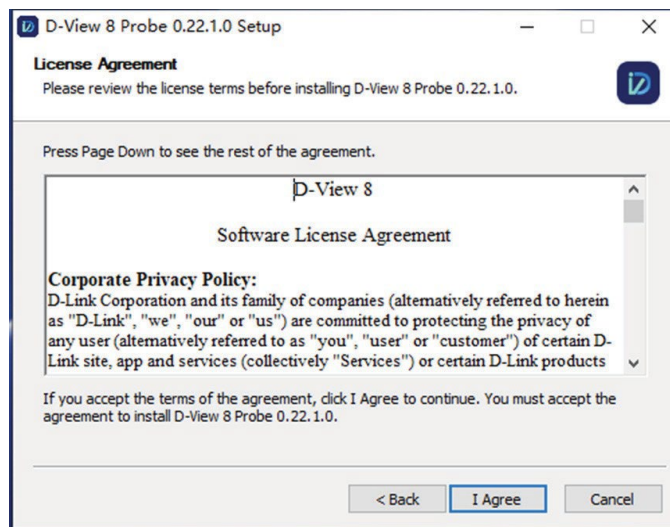


Figure 39 Reviewing a License Agreement

4. The Connection Configuration page displays.
5. Click the Local IP drop-down menu to select an existing IP address.
6. In the Probe Port field, enter the port with authorized access to allow traffic through the IP address.
7. Click **Check** to validate the configuration. A Check Pass! message displays if the local IP is properly setup. Otherwise, re-start the configuration process.
8. Click **Next** to continue the installation process.

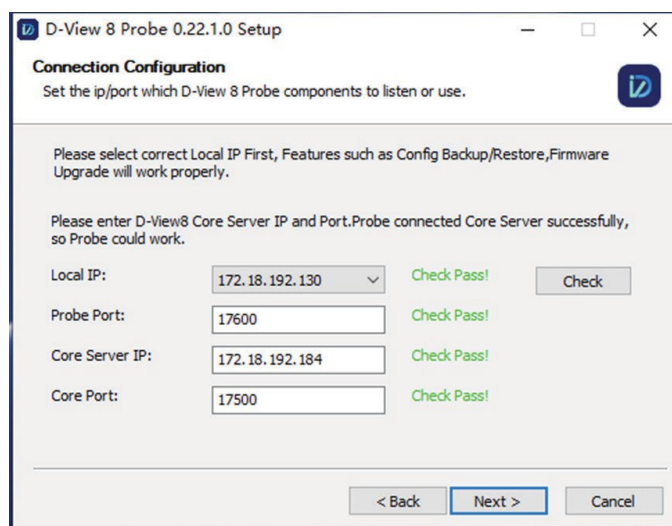


Figure 40 Connecting a Core Server

The Choose Install Location page displays.

9. Click **Browse** to select a destination folder.
10. Once selected, click **Install** to begin the process. The Completing Setup Wizard page displays.
11. Click **Finish** to end the process.

The Probe Setup process is completed and a shortcut is generated on the desktop containing the following D-Link D-View 8 Probe files:

- D-View 8 Service Management Tool
- Uninstall

The Service Management Tool allows for management of the probe. See the following figure for further information.

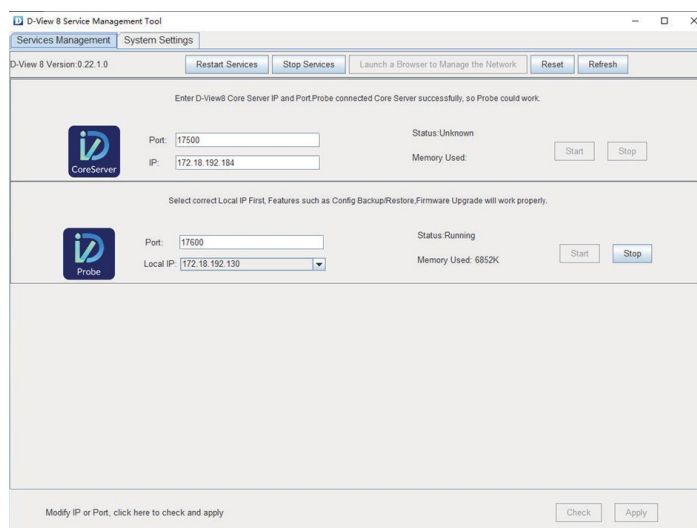


Figure 41 Viewing Service Management Tools

The Probe Setup is completed.

2.3. Linux Installation Guide

2.3.1. Standalone Edition Installation

To begin the installation process, download the installation package.

1. Download the package:

```
DVIEW8_1.0.0.4.deb
```

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

```
dpkg -i DVIEW8_1.0.0.4.deb
```

3. At the prompt enter the local IP address:

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



NOTE: The listed IP address is for reference only. The local IP address of the server is required.

The D-View 8 application requires a database service (MongoDB) to function. If this is a first time installation, a new 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 correlating password. Enter it again in Confirm Password.

```
Password: [admin]
```

```
Confirm Password: [admin]
```

The installation process continues, service files and local services are installed. The web, core, and probe services are also installed, and the process is completed once the services are running.

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]
```

If any instances are detected a prompt display.

- b. At the prompt, enter n 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. At the prompt, enter the IP address of the existing instance:

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

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

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



NOTE: The listed IP address and port information is for reference only. The relevant information for the existing instance is required.

- e. At the prompt validate authentication, enter y if access is required:
Do MongoDB access require authentication? [y/n]
 - f. If required, at the prompt enter the user name and password authorized to access the instance.
Username: root
Password: root
5. Once the instance is created or connected, start the application in a web browser.
 6. Open the browser and enter the IP address for the D-View 8 application in the address bar. In the following figure the IP address is listed 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 support
```

Figure 42 Entering Application IP Address

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

2.3.2.1. Cluster Architecture

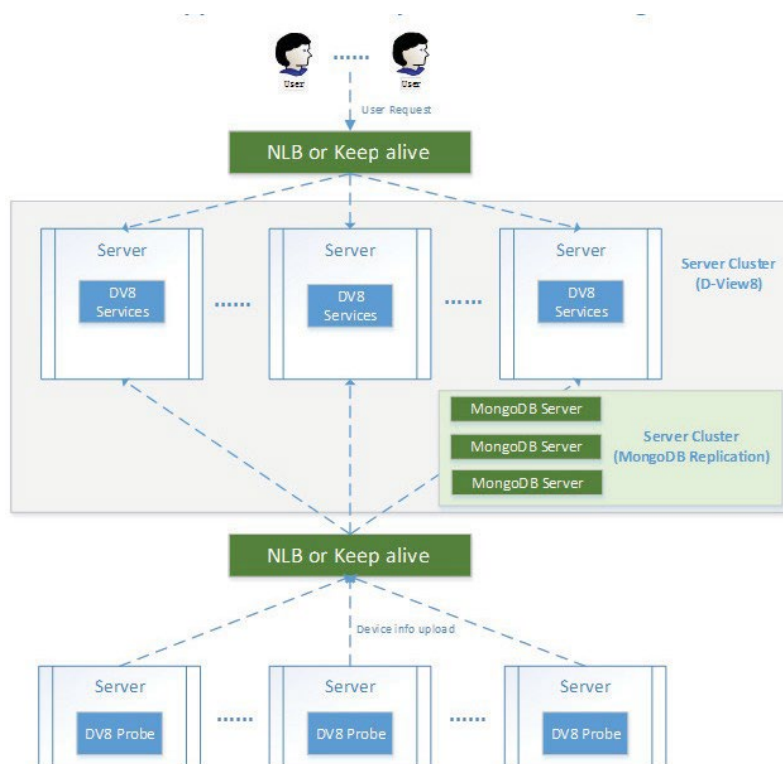


Figure 43 Cluster Architecture Diagram

The following is a diagram of the D-View 8 and MongoDB set frame. The set frame includes a primary, secondary, and arbiter. In the architecture design, the application connects to the primary and secondary. By design a primary database may become a secondary one, while the secondary may be designated as a primary. By default, clients read from the primary, but a read preference can be configured to send read operations to secondary database designations.

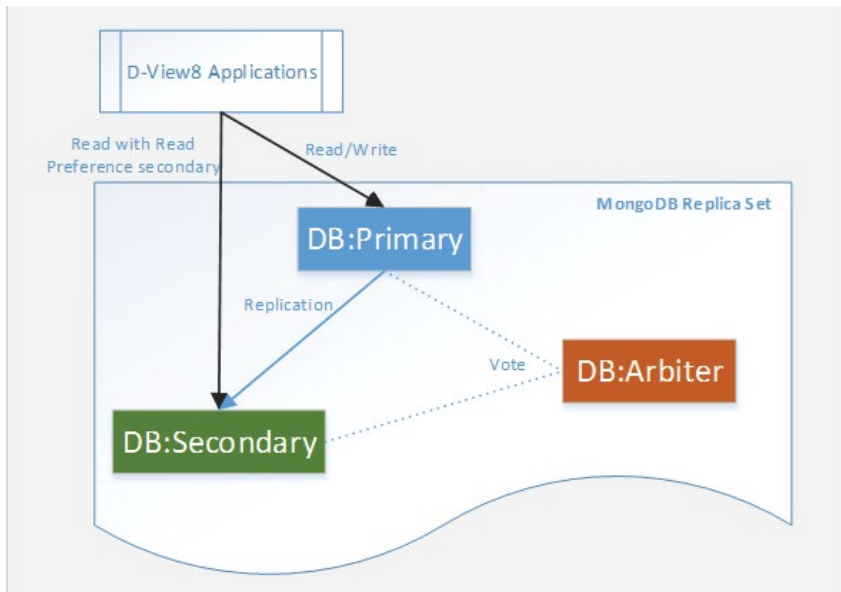


Figure 44 Database Diagram

2.3.2.2. Cluster Building Steps

Building clusters is outlined through the following steps. The illustrations are intended to serve as examples of the process.

To support data redundancy:

1. Allocate three servers and install MongoDB.

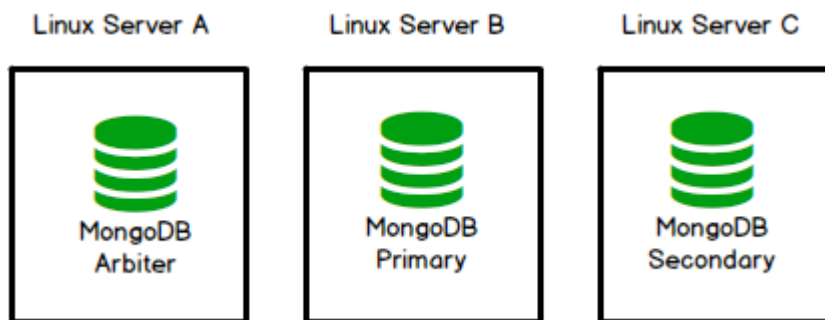


Figure 45 Allocating MongoDB Servers

2. Install D-View 8 in multiple servers and connect the application to the MongoDB cluster.

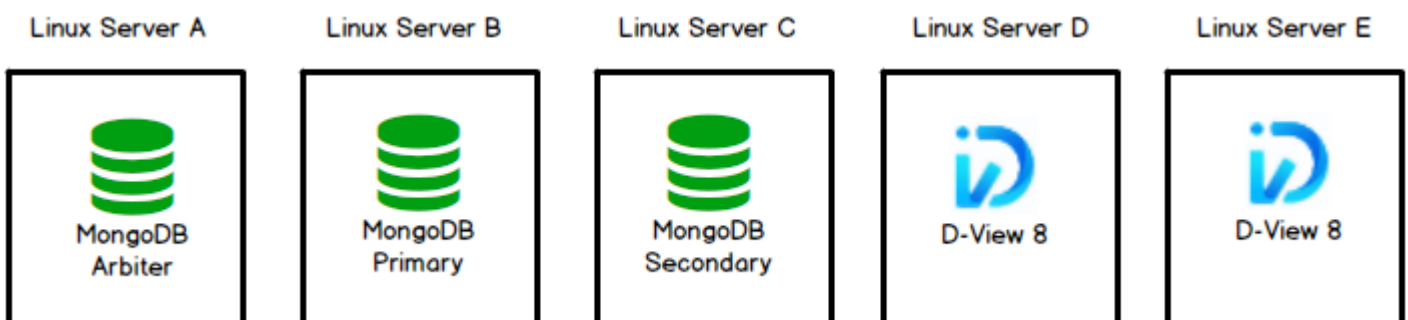


Figure 46 Installing Multiple Servers

To support server load balancing:

3. In Linux, install Keepalived.

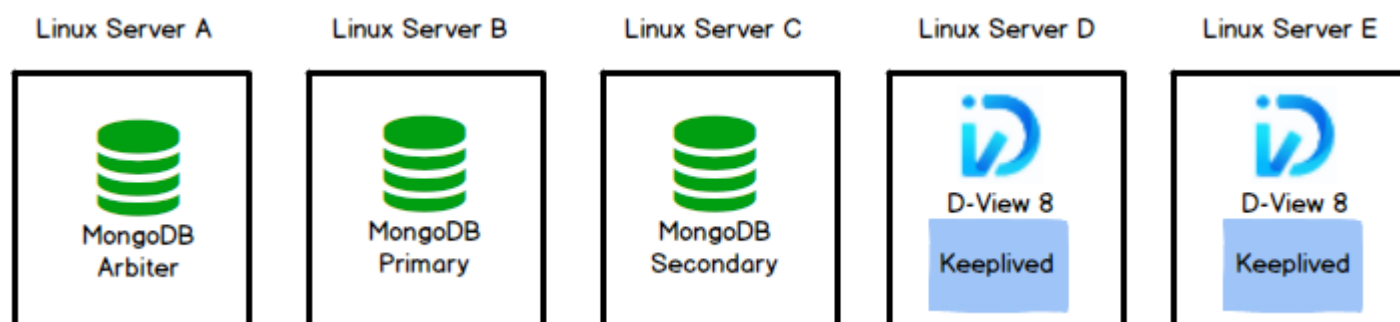


Figure 47 Keepalived Diagram

4. To manage additional devices, add a probe in each additional server and connect the application through Keepalived.

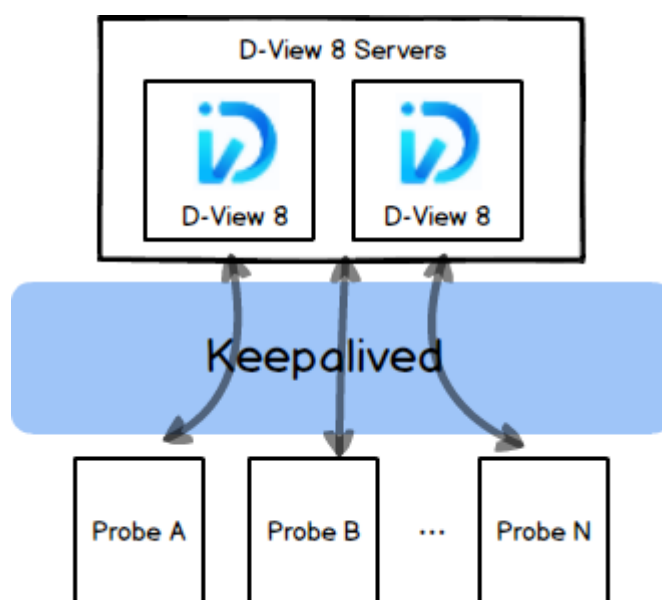


Figure 48 Application Connection Diagram

Support Data Redundancy

Data redundancy requires the use of three MongoDB server instances.

1. Download the D-View8 - MongoDB Installation Package.
2. In the command line, enter the following to initiate the process:

```
tar -xvzf mongodb-linux-x86_64-4.0.0-DView8.tgz
```

3. Install MongoDB on the intended servers' instances: Server A, Server B, and Server C, respectively.
4. In the command line, locate the D-View 8 directory by entering:

```
./init_mongo.sh
```

5. During first start, you will need to import the built-in data. Enter y to continue:

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

6. Designate the use of cluster MongoDB by starting the instance in replication mode, enter Y:

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

The server is prepared and setup for connections. The following scripts are populated in the D-View 8 directory:

- restart_mongo.sh: restart MongoDB

- status_mongo.sh: show the status of MongoDB
- stop_mongo.sh: stop MongoDB

Installing in a Different Server

To install D-View 8 in multiple servers, the instance must be connected to the MongoDB cluster. See the following for further details.

1. Logon with the su command to obtain root access rights.
2. Download the package:
`DVIEW8_1.0.0.4.deb`
3. In the root menu enter the following command to select the downloaded package:

```
dpkg -i DVIEW8_1.0.0.4.deb
```

4. At the prompt enter the local IP address:

Input the local IP: 172.18.192.256



NOTE: The listed IP address is for reference only. The local IP address of the server is required.

The D-View 8 application requires a database service (MongoDB) to function.

5. At the prompt, enter 2 to select the MongoDB cluster installation.

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

6. At the prompt, enter the IP address and Port for the primary, secondary and arbiter nodes.

Once installed, you can access the dashboard by opening a web browser and entering the assigned IP address in the browser's address field.

Support Server Load Balance

The following are required to support server load balancing:

- OS: Ubuntu18.04 or above, Debian10 or above
 - Service: Keepalived
 - Topological structure:

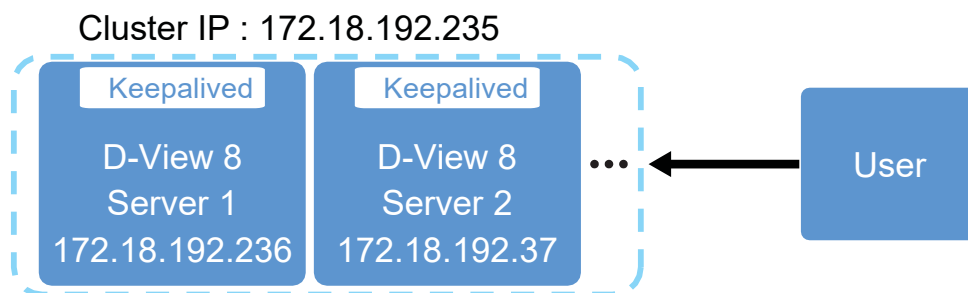


Figure 49 Load Balancing Support

VIP	Virtual IP, through which users can access DV8 service
MASTER	Load balancing master server
BACKUP	Load balancing backup server
IP 1	Dv8 service real IP address
IP 2	Dv8 service real IP address

1. Logon with the su command to obtain root access rights.
2. In the command line, enter the following to install Keepalived:

```
sudo apt-get install keepalived
```

Once **Keepalived** is installed, the configuration and shell files can be located and moved.

- keepalived.conf
- vip_service.sh

3. In the command line, enter the following to move the files:

```
cp /usr/local/dview8/keepalived.conf /etc/keepalived/
cp /usr/local/dview8/vip_service.sh /etc/keepalived/
```

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

- First, set a global unique virtual routing ID.
- Secondly, set the cluster IP address.
- Third, add the real node IP address to the LVS cluster.

The following information is an illustration of the modification requirements:

- (1) routing ID
- (2) the cluster IP
- (3) real node IP
- (4) virtual routing ID

```
! Configuration File for keepalived
global_defs
{
    router_id
        LVS_36
}

vrrp_instance VI_1
{
    state MASTER
    interface ens192
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        172.18.192.235
    }
}

virtual_server 172.18.192.235 17300 {
    delay_loop 6
    lb_algo rr
    lb_kind DR
    lb_algo rr
    lb_kind DR
    persistence_timeout 50
    protocol TCP
}

real_server 172.18.192.236 17300 {
    weight 1
    TCP_CHECK {
        connect_timeout 10
        retry 3
        delay_before_retry 3
        connect_port 17300
    }
}

real_server 172.18.192.37 17300 {
    weight 1
    TCP_CHECK {
        connect_timeout 10
        retry 3
        delay_before_retry 3
        connect_port 17300
    }
}
```

Figure 50 Configuring Keepalived

```
virtual_server 172.18.192.235 17500 {
    delay_loop 6
    lb_algo rr
    lb_kind DR
    persistence_timeout 10
    protocol TCP
}

real_server 172.18.192.236 17500
    weight 1
    TCP_CHECK {
        connect_timeout 10
        retry 3
        delay_before_retry 3
        connect_port 17500
    }
}

real_server 172.18.192.37 17500 {
    weight 1
    TCP_CHECK {
```

```

        connect_timeout 10
        retry 3
        delay_before_retry 3
        connect_port 17500
    }
}
}

```

Figure 51 Virtual Server Definitions

As displayed in the previous figures, the virtual_server is configured first with the IP address. A delay_loop then is set to configure the amount of time (in seconds) between health checks. For availability, the lb_algo option is specified (rr for Round-Robin). The lb_kind option determines the routing method.

Once the Virtual Server is configured, the real_server options are configured. The IP Address first is first specified. By using TCP, the TCP_CHECK stanza checks for availability of the real server. The connect_timeout configures the time in seconds before a timeout occurs.

5. Modify the vip_service.sh shell as follows:
 - a. First, set the cluster IP addresses. See the following figure for further information.

```

#!/bin/bash
SNS_VIP=172.18.192.235
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 Stopped"
    ;;
*)
    echo "Usage: $0 {start|stop}"
    exit 1

```

Figure 52 Setting Cluster IP Address

6. Start up Keealived by entering the following in the command line.


```

chmod a+x /etc/keepalived/vip_service.sh
/etc/keepalived/vip_service.sh start
sudo service keepalived start

```
7. Verify the run status of Keepalived by entering the following in the command line.
 - a. Restart keepalived: service keepalived restart
 - b. Stop keepalived: service keepalived stop

- c. Show keepalived status: service keepalived status

```
root@ubuntu:/etc/keepalived# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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 172.18.192.235/32 brd 172.18.192.235 scope global lo:0
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:1c:60:26 brd ff:ff:ff:ff:ff:ff
    inet 172.18.192.236/23 brd 172.18.193.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet 172.18.192.235/32 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe1c:6026/64 scope link
        valid_lft forever preferred_lft forever
```

Figure 53 Viewing Run Status

- d. View the load balancing status, enter: `ipvsadm -Ln --stats`
If the command is not supported, enter the following: `sudo apt-get install ipvsadm`

```

root@ubuntu:/etc/keepalived# ipvsadm -Ln --stats
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port          Conns  InPkts  OutPkts  InBytes  OutBytes
-> RemoteAddress:Port
TCP 172.18.192.235:17300          20     1888M   0        98188M   0
-> 172.18.192.37:17300          20     1888M   0        98200M   0
-> 172.18.192.236:17300          0      0       0        0        0
    
```

Figure 54 Viewing Load Balancing Status

Keepalived is now installed on the D-View 8 server.

2.4. Software Upgrade

2.4.1. Upgrading under Windows

The D-View 8 application is upgraded from time to time to increase the performance and functionality of the software to the benefit of the user. Upgrading the software can be done by downloading an upgrade package.

The following provides details to upgrade through a downloadable package.

1. Download the D-View 8 upgrade package from the D-View website.
2. Once downloaded, locate the package file and double click on it to open the installer.

The Update Setup wizard displays.

3. Click **Upgrade** to begin installing.

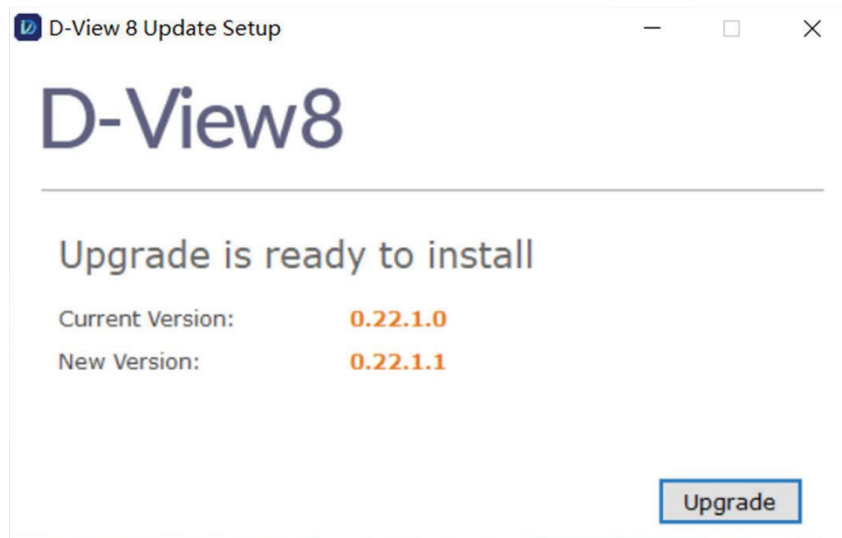


Figure 55 Upgrading D-View 8

Once the process is completed an *Upgrade is successful* prompt displays. The upgraded version is listed signifying the successful upgrade.

4. To verify the current version of the application, open the interface by logging in through a browser, see “3.2. Launching D-View 8 Web GUI” on page 41 for further details.
5. In the application interface, navigate to **System > About** to view the Software Version number. See the following figure for further information.

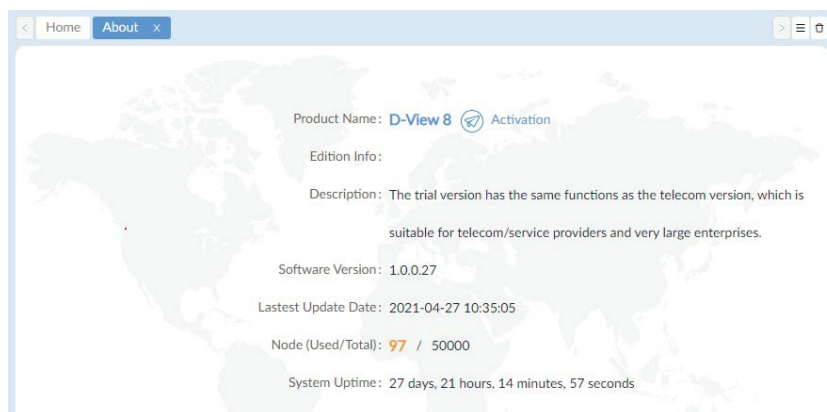


Figure 56 Viewing Version Number

2.4.2. Upgrading under Linux

The D-View 8 application is upgraded from time to time to increase the performance and functionality of the software to the benefit of the user. Upgrading the software can be done by downloading an upgrade package or through the Firmware Management function.

The following provides details to upgrade through a downloadable package.

1. Logon with the su command to obtain root access rights.
2. Download the D-View 8 upgrade package from the D-View website.
3. Log in to the root menu.
4. Once downloaded, locate the package file and unpack it. Enter the following in the command menu:

```
dpkg -i DVIEW8_1.0.0.4.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 support)
```

Figure 57 Viewing Application Corresponding IP Address

For Cluster versions:

9. Select the type of MongoDB type, enter 2 to select MongoDB cluster.

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

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

```
dpkg -s dview8
```

11. Auto upgrade is supported through the remote probe.

2.5. Uninstalling

2.5.1. Uninstalling 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. Uninstalling 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 from 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

Both methods can be performed through the D-View 8 web interface, see System > D-View 7 Upgrade in the dashboard menu.

Before you start, make sure your anti-virus software is disabled through the migration process to prevent the upgrade of the software.

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

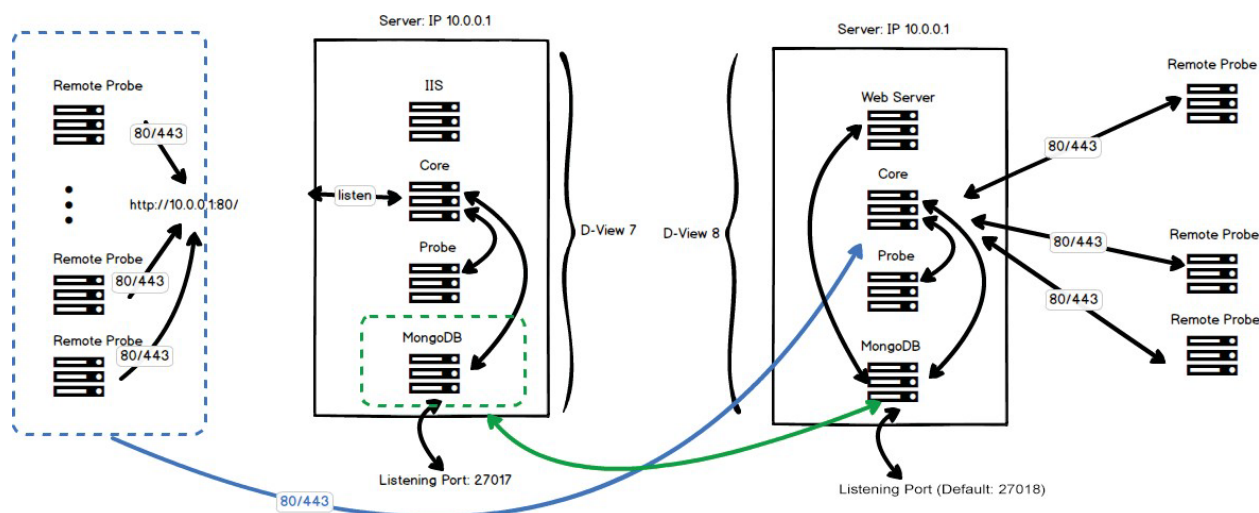


Figure 58 D-View Architecture

2.6.2. Installing a New D-View 8 Server

1. Open the D-View-7 Service Management Tool.
2. In the Services Management tab, click **Stop** to stop the D-View 7 services. However, do not stop the MongoDB instance.

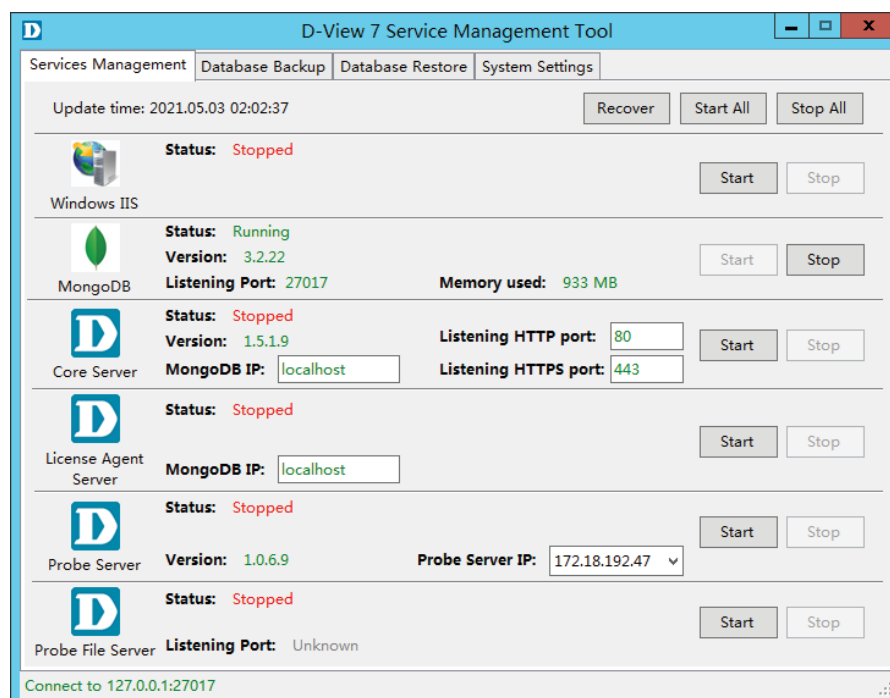


Figure 59 Stopping D-View 7 Services

3. Change the D-View 7 server's IP address. 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. Keep the current IP address for use to configure the new D-View 8 server. This is the address that will be used to install the D-View 8 node.
4. Download the D-View 8 package to a local directory.
5. Click on the installation package to begin installing. See "2 Installation" on page 07 for further information.
6. 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 (default). 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 with the installation process and follow the installation wizard to completely setup the new node.

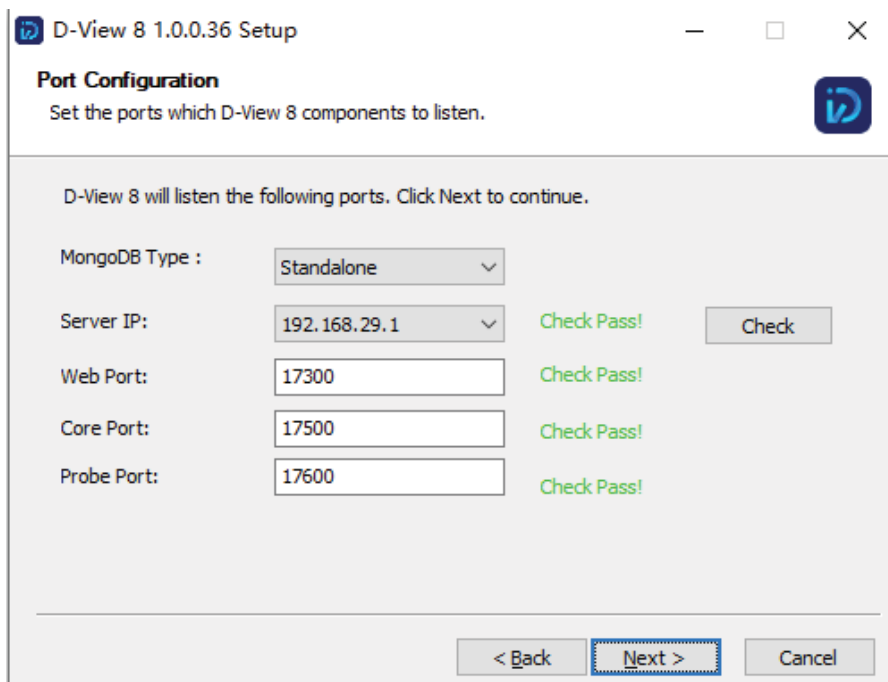


Figure 60 Port Configuration

9. Once the installation process for the D-View 8 node is complete, log into the application interface. See “3.1. Logging In and Basic Configurations” on page 41.
10. Navigate to System > D-View 7 Upgrade. The D-View 7 Upgrade page displays.

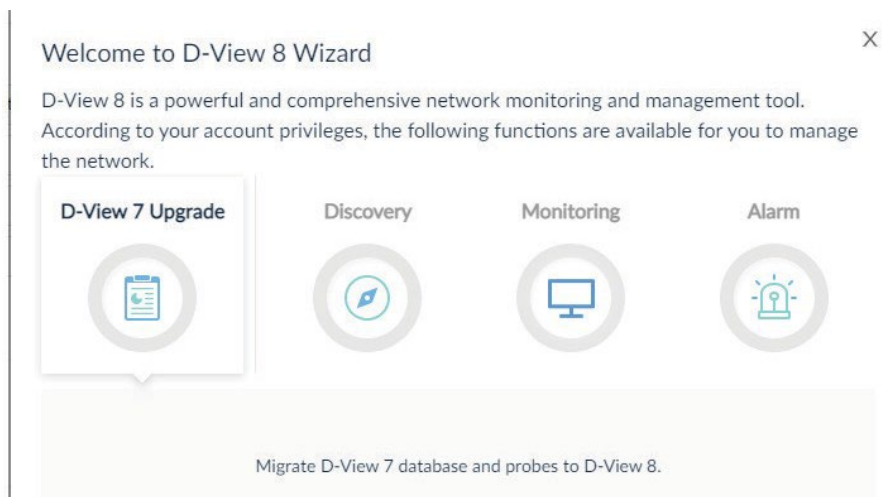


Figure 61 Selecting D-View 7 Upgrade

11. 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 node. The Database Migration page displays.

The following settings are required to establish a connection to the relevant MongoDB instance:

- In the MongoDB Address field, enter the new IP address and port as previously configured, see previous steps (Example used: 10.0.0.3):

IP address: 10.0.0.3

Port: 27017

- If the MongoDB instance 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 a connection once again.

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

Figure 62 Initiating D-View 7 MongoDB Instance

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 complete it.



NOTE: In the event of an interruption in the migration process, re-start the process by clicking on **System > D-View 7 Upgrade** and selecting D-View7 Upgrade from the wizard panel.

Figure 63 Continuing D-View 7 Migration

Once the process is completed, the D-View 7 remote probes automatically connect to the D-View 8 node. The D-View 8 node upgrades the D-View 7 instance to D-View 8.

2.6.3. Installing D-View 8 in a D-View 7 Server

1. Open the D-View-7 Service Management Tool.
2. In the Services Management tab, click **Stop** to stop the D-View 7 services. However, do not stop the MongoDB instance.

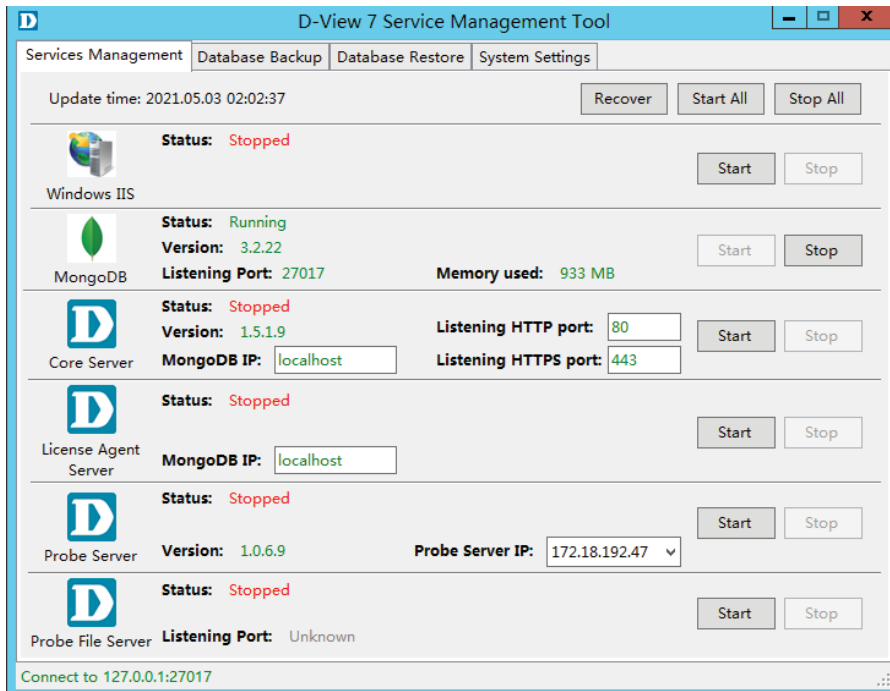


Figure 64 Disabling D-View 7 Server Services

3. Download the D-View 8 package to a local directory.
4. Click on the installation package to begin installing. See “2 Installation” on page 07 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 (default). In the Port Configuration page, locate the Core Port field and change the value to 80.
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 the new node.

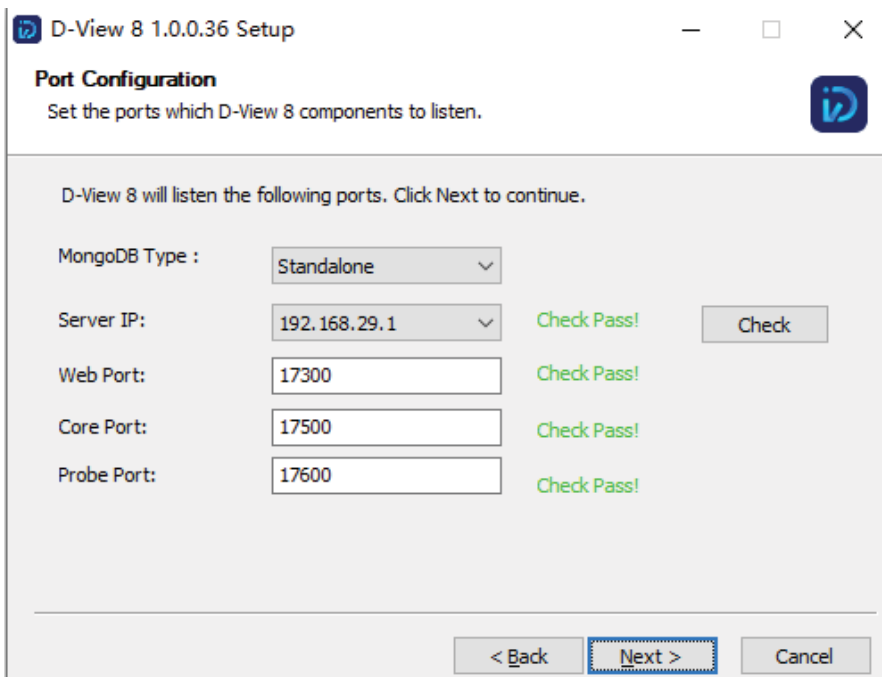


Figure 65 Setting Up a New Node

8. Once the installation process for the D-View 8 node is complete, log into the application interface. See “3.1. Logging In and Basic Configurations” on page 41.
9. Navigate to System > D-View 7 Upgrade. The D-View 7 Upgrade page displays.

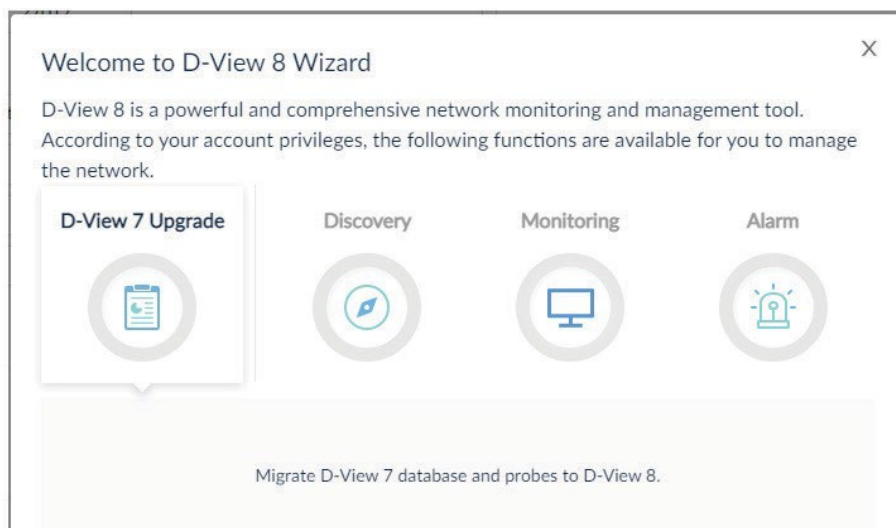


Figure 66 Selecting D-View 7 Upgrade

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 node.
The Database Migration page displays.

The following settings are required to establish a connection to the relevant MongoDB instance:

- In the MongoDB Address field, enter the IP address and port of the MongoDB instance:
IP address: 127.0.0.1
Port: 27017
- If the MongoDB instance 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 a connection once again.

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

Figure 67 Initiating D-View 7 MongoDB Instance

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, re-start the process by clicking on **System > D-View 7 Upgrade** and selecting **D-View7 Upgrade** from the wizard panel.

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.

Skip All 2/3 Previous Next

Figure 68 Continuing D-View 7 Migration

Once the process is completed, the D-View 7 remote probes automatically connect to the D-View 8 node. The D-View 8 node upgrades the D-View 7 instance to D-View 8.

This page is intentionally left blank.

3 Getting Started

3.1. Logging In and Basic Configurations

Once logged in to the application, it is highly recommended to change your password and account information, after which, configure the email settings for alert notifications.

- Log in to D-View 8
- Change the User Password and Account Information
- Configure Email Settings for Alerts and Alarm Notifications

3.2. Launching D-View 8 Web GUI

The application is accessible through a browser server architecture. All users can access the D-View 8 from a supported browser.

Before logging in to the application, make sure the following items apply:

The D-View 8 application is installed on a server with a static IP address.

The browser in use is cleared of any cache before attempting to use the application.



NOTE: The D-View 8 supports multiple concurrent users. If a user is modifying a page, a different user can inadvertently make changes to the same page. To prevent management issues, it is recommended that users coordinate the management of activities prior to any work on the D-View 8.

To log in to the application:

1. Open a browser and enter the assigned IP address of the D-View 8 server.
 - If connecting from the same D-View 8 server in which the application is installed, enter the respective URL. In the following example the default port 17300 is used.
http://localhost:17300
 - If connecting to a remote computer, in the address bar enter the IP address of the D-View 8 server.

The following displays the User Login page.

Figure 69 D-View 8 Login Screen

2. From the account type drop-down menu, select the defined account type of the user:
 - 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.

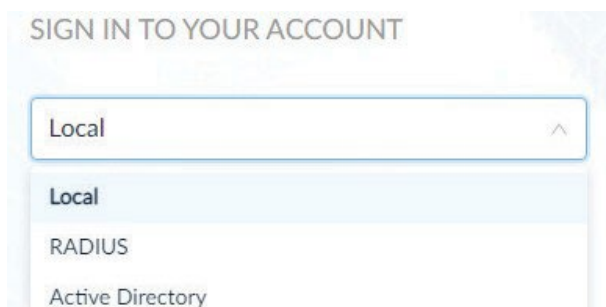


Figure 70 Signing in to an Account

3. Enter the assigned user name and password.
By default, the administrator user name is **admin** and the default password is also **admin**.
An administrator level account is required to create user names and passwords for the various types of users.

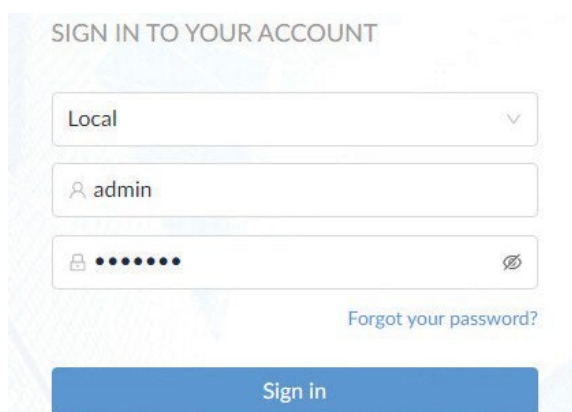


Figure 71 Entering User and Password Credentials

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

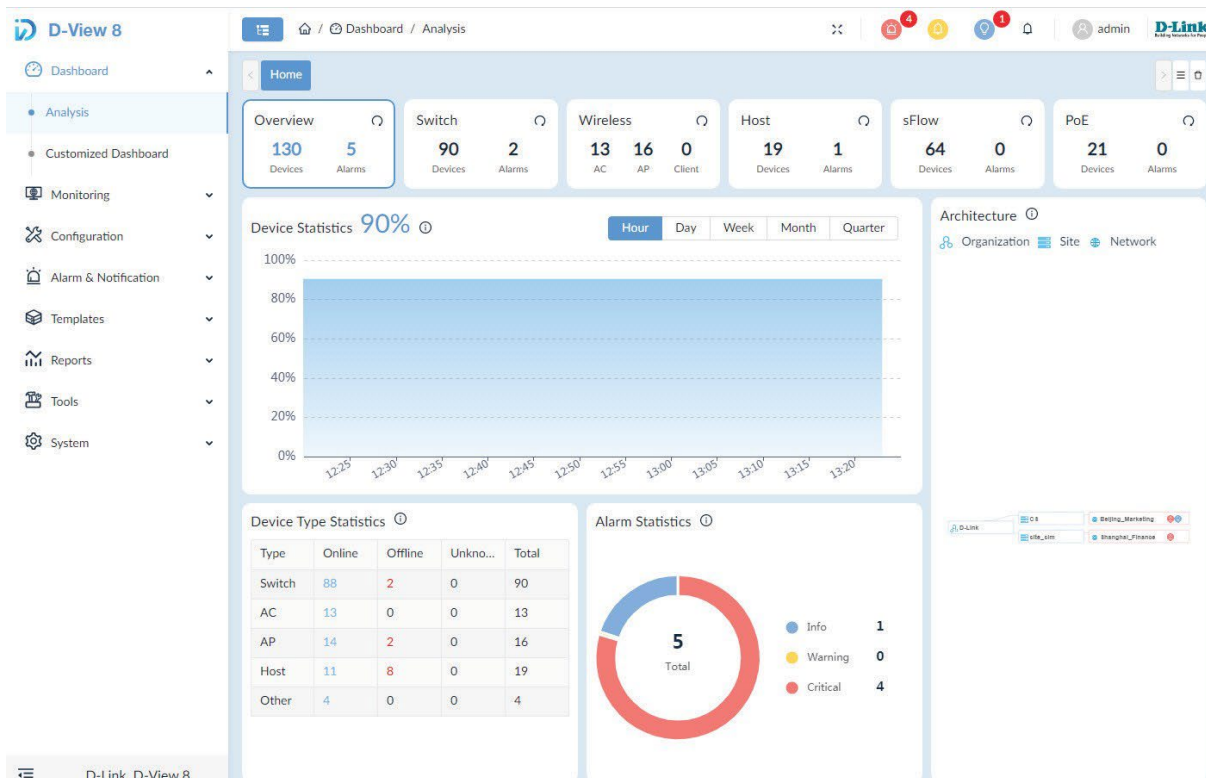


Figure 72 Viewing a D-View 8 Dashboard

For more information on the **Dashboard** overview, see “3.3. Understanding the Web Dashboard” on page 43.

3.3. Understanding the Web Dashboard

The D-View 8 Dashboard features and functionality are accessed through the menus and toolbar in the web interface. Whether a particular tool is displayed is determined by the selected user type configuration environment, see “1.10. User Authentication Types” on page 06 for further information.

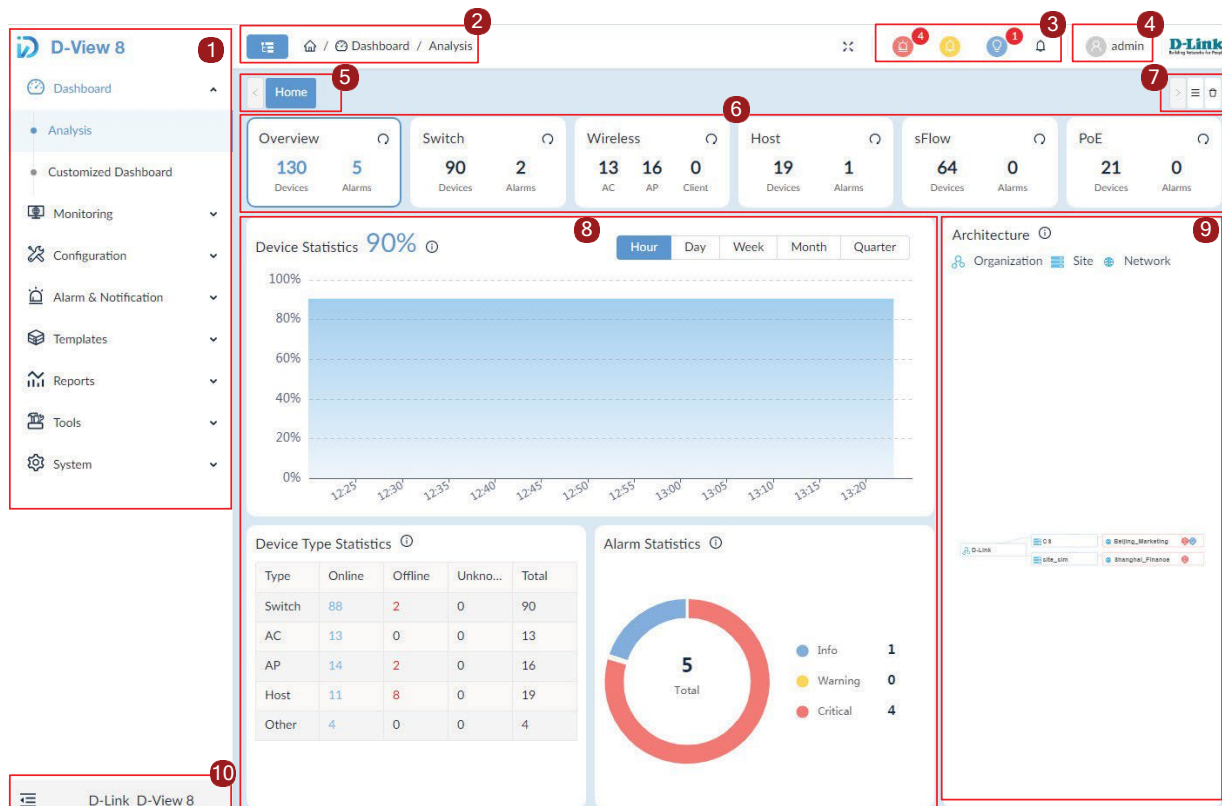


Figure 73 Dashboard Outlined

Web Dashboard Annotations			
1.	Main menu	2.	Title bar
3.	Annunciators	4.	User Menu
5.	Menu selection indicator	6.	Environment widget menu
7.	Environment menu selector	8.	Widget status information
9.	Architecture diagram	10.	Collapse/expand sidebar

3.3.1. Common Features

There are several features that are common to nearly all interface menus on the D-View 8 dashboard.

- **Menus** access tools and user actions.
 - Sort and Filter menus help you to modify table data sorting and filtering.
 - Actions menus help you to access features that are almost always specific to a particular page, typically accessed through toolbar buttons.
- **Help** menus in the form of an icon (i) provide additional information relevant to the displayed action.
- **Toolbars** give quick access to the common functions to access actions or open pages corresponding to menu options.
- **Annunciators** also called indicators offer a visual notification for 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 are dependent on the user type, license type, and configured hardware options.

3.3.2.1. System Configuration

Item	Description
Basic Settings	<ul style="list-style-type: none"> • Organization <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ▪ Configures mail server information and associated parameters • Forward Trap <ul style="list-style-type: none"> ▪ Configures the trap receiver to receive incoming device trap messages • Forward Syslog <ul style="list-style-type: none"> ▪ Configures the system log receiver to receive incoming device syslog messages to the D-View server • REST API <ul style="list-style-type: none"> ▪ To generate the API key which will be used by other application to acquire a token from D-View 8 ▪ Third party applications can use tokens to acquire needed information from D-View 8 without sending username and password • SNMP Credentials <ul style="list-style-type: none"> ▪ Configures the SNMP protocol types, community name and related parameters • sFlow Settings <ul style="list-style-type: none"> ▪ Configures sFlow collector's associated information • System Preferences <ul style="list-style-type: none"> ▪ Configures the table display parameter and theme of D-View 8
User Management	<ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> ▪ Listing user information which contains user's email address, username, login time, authentication type etc. ▪ Add, delete, remove users. • Role Privileges <ul style="list-style-type: none"> ▪ Listing the types of user role which includes Organization/ Site/ Network Administrator roles. ▪ Listing each role's associated function privilege. • AD Server <ul style="list-style-type: none"> ▪ Configures the Windows Active Directory Server's information. • RADIUS Server <ul style="list-style-type: none"> ▪ Configures the RADIUS Server's information. ▪ Supports Primary and Secondary RADIUS Server configuration

Item	Description
Scheduling	<ul style="list-style-type: none"> • Configures the “Recurrent Schedule” and “Time Range Schedule” • Recurrent Schedule List <ul style="list-style-type: none"> ▪ Allows user to configure recurrent schedules with customized frequency and duration • Time Range Schedule List <ul style="list-style-type: none"> ▪ Allows user to configure a specific range of time, i.e., work hours or holidays
Server Management	<ul style="list-style-type: none"> • To monitor the status of D-View Core Server, Web Server and Probe • To check the real-time report of each server’s status, which includes the utilization of CPU memory, hard drive and the network traffic
D-View 8 Log	<ul style="list-style-type: none"> • D-View 8 features three types of logs: User Operation Log, System Log, Device Maintenance Log • User Operation Log: <ul style="list-style-type: none"> ▪ Records user operational activity while logged in • System Log: <ul style="list-style-type: none"> ▪ Keeps the records of D-View 8’s running status for server and probes • Device Maintenance Log: <ul style="list-style-type: none"> ▪ Keeps users’ configuration action log for devices
D-View 7 Upgrade	<ul style="list-style-type: none"> • The D-View 7 Upgrade page allows for the following upgrade functions: • Database Migration • Remote Probe Upgrade
About Page	<ul style="list-style-type: none"> • The About page keeps the following information: • D-View 8’s edition, such as Standard or Enterprise • Brief description for the purchased edition • Software version • The latest update date • The number of supported and used nodes • System uptime information

3.3.2.2. Dashboard

Item	Description
Analysis	<ul style="list-style-type: none"> • By default, there are six tabs in the analysis page, user can click each tag to display dedicate information. The Analysis page includes following tabs: <ul style="list-style-type: none"> ▪ Overview ▪ Switch ▪ Wireless ▪ Host ▪ sFlow ▪ PoE • Provides an overview of alarm statistics, on/off-line status, CPU/memory utilization, performance status, traffic statistics, and other information • Different categories may have slight variations in the information provided
Customized Dashboard	<ul style="list-style-type: none"> • Allows user to configure the dashboard to display the information they need and apply it to the homepage

3.3.2.3. Monitoring

Item	Description
Network Discovery	<ul style="list-style-type: none"> • Allows user to configure the network discovery parameters, which include: <ul style="list-style-type: none"> ▪ Basic Information: the name of the network and site to discover. The discovered devices manage rule ▪ Probe Mode: to choose the primary and secondary probe ▪ Discovery Range: the range includes single IPv4/v6 Address, an IPv4/v6 Address range, an IPv4/v6 subnet or importing the range from a file ▪ Schedule: to define the discovery schedule which includes one-time discovery or recurrent discovery • Displays all discovery rules' running status and associated detail information
Device View	<ul style="list-style-type: none"> • Includes 5 categories: All, Managed, Unmanaged, Ignored and Conflicted • Displays several device types: Switch, Wireless, Host and Other • Displays the summary and detailed information of each device • User can click "System Name" to check each device's detailed information • User can click "IP" to select a protocol to log in to the device
Interface View	<ul style="list-style-type: none"> • Listing devices' connection relationship, which includes: <ul style="list-style-type: none"> ▪ System/Model Name ▪ Device's IP address ▪ Interface and MAC address information ▪ VLAN information ▪ Uptime information ▪ D-View's organization information • Each item in the table provides search capability • MAC Locator: user can look up for specific MAC address by using the search function in the "Connected MAC" column.
Topology Map	<ul style="list-style-type: none"> • Displays connections between devices • Displays the on/off-line status of devices • Displays the link status of devices • PNG or JPG format files can be uploaded as the topology's background image • Supports Star, Tree, Circular and Grid type topology maps • Zoom in and out the topology map • Users can to create customized topologies

Item	Description
Connection View	<ul style="list-style-type: none"> • Listing the interface link information which includes: <ul style="list-style-type: none"> ▪ Link status ▪ Link name ▪ Name and IP address of two devices ▪ The connected interface of each device ▪ The connected devices and interface information ▪ Traffic statistics of TX and RX ▪ Link utilization ▪ Link type (LACP or general) ▪ Link's related info update time ▪ Source of the detection, such as LLDP or FDB • Clicking the link interface name's hyper link, more detailed information will be displayed, such as: <ul style="list-style-type: none"> ▪ Summary information of the selected link ▪ Monitor information of the selected link ▪ Alarm information of the selected link
Rack View	<ul style="list-style-type: none"> • Provides users visualization of the actual device rack
sFlow Analyzer	<ul style="list-style-type: none"> • Collects the sFlow data from devices and generates related statistics reports • The statistics report information includes: <ul style="list-style-type: none"> ▪ Report based on the source or destination of packets ▪ Report based on QoS rules ▪ Report based on layer 4 applications ▪ Report based on two nodes' conversation
Device Group	<ul style="list-style-type: none"> • Allows users to create device groups • Device grouping to simplify the firmware or configuration file maintenance

3.3.2.4. Configuration

Item	Description
Batch Configuration	<ul style="list-style-type: none"> • Allows customer to simultaneously configure multiple devices' parameters at the same time • Two sub-features: <ul style="list-style-type: none"> ▪ Quick Configuration: provides a GUI template for each function to apply the settings to multiple devices ▪ Advanced Configuration: allows user creating a profile for a specific type of device and the profile contains multiple features' parameters. User can apply the profile to multiple devices which have the same type/model as the profile.
Task Management	<ul style="list-style-type: none"> • Lists all user created tasks to understand the execution result • This feature includes: <ul style="list-style-type: none"> ▪ Current Tasks lists the descriptions of current tasks ▪ Historical Tasks lists the descriptions of historical tasks • Each task result will include a message to describe the success status. If a failure happens, it will also describe the reason of failure.
Firmware Management	<ul style="list-style-type: none"> • Allows users to manage device's firmware via D-View 8 • Uploading or downloading the firmware to or from the device • Upgrading device by specifying schedule • If firmware image already exists in D-View 8, user can just select the file without uploading a new one again • Displays the failure message to understand the root cause

Item	Description
Configuration Management	<ul style="list-style-type: none"> • Allows users to manage device configuration via D-View 8 • Users can backup or restore multiple device configuration files at the same time • Users can backup or restore the file by specifying a schedule • Supports baselined configuration file comparison, auto restore and generate alarm feature
File Management	<ul style="list-style-type: none"> • Allows users to compare configuration files to verify the differences between the two files • Allows users to upload or delete configuration or firmware files on D-View • Allows users to set the configuration file as the baselined file

3.3.2.5. Alarms & Notifications

Item	Description
Alarms	<ul style="list-style-type: none"> • Displays all alarm information collected from network devices. The alarms include: <ul style="list-style-type: none"> • Active Alarms <ul style="list-style-type: none"> ▪ Lists all unresolved or unacknowledged network alarms • Historical Alarms <ul style="list-style-type: none"> ▪ Lists all resolved or acknowledged network alarms
Trap & Syslog	<ul style="list-style-type: none"> • Displays the trap and system log receiving from devices or the system. The trap log's information contains: <ul style="list-style-type: none"> ▪ Time received ▪ Device system name ▪ Device IP address ▪ SNMP version ▪ Generic type ▪ Trap description ▪ Original message of the trap ▪ The associated alarm of the trap (Users can select optional columns to display) ▪ The site and network which the related device belongs to (Users can select optional columns to display) • The syslog information contains: <ul style="list-style-type: none"> ▪ Time received ▪ System name of device generating the syslog ▪ Device IP address ▪ Syslog severity levels ▪ Syslog messages ▪ The associated alarm of the syslog (Users can select optional columns to display) ▪ The site and network of related devices (Users can select optional columns to display)
Trap Editor	Allows customer to edit a readable trap message for a specific trap OID

Item	Description
Monitor & Alarm Settings	<ul style="list-style-type: none"> • Monitor Settings <ul style="list-style-type: none"> ▪ Configure the monitor status to let D-View collect data according to the established time intervals • Alarm Settings <ul style="list-style-type: none"> ▪ Configure alarm rules to let D-View generate alarms when collected data matches user configured thresholds ▪ Configure the CLI to let devices and D-View servers execute when the alarms are triggered • Alarmable Items Definition <ul style="list-style-type: none"> ▪ Define the items for customized monitors and set thresholds to trigger alarms
Notification Center	<ul style="list-style-type: none"> • Allows user to set the notification method when alarms are triggered. The methods include: Web Scrolling Message, Email, and Execute script.

3.3.2.6. Template

Item	Description
Device Template	<ul style="list-style-type: none"> • This feature allows user to easily add a device to be managed by D-View 8 if it's not in the default managed list; a useful tool especially for managing third party devices • Allows user to customize device's information by providing: <ul style="list-style-type: none"> ▪ Model Name ▪ Device Type ▪ Vendor Name ▪ Device's System OID (SOID) ▪ Panel Template • Allow users to expand D-View's monitoring and configuration capabilities for device models. Provide a way to associate the existed monitor and configuration templates
Device Support	<ul style="list-style-type: none"> • Allows user to create useful information to manage third party vendor and devices, which includes: • Vendor <ul style="list-style-type: none"> ▪ Vendor name ▪ Vendor OID • Device Category <ul style="list-style-type: none"> ▪ Category name ▪ Photo of the category. The file type can be PNG or JPG format (less than 2 MB in size) • Device Type <ul style="list-style-type: none"> ▪ Type name ▪ Device category (data comes from Device Category) ▪ Description

Item	Description
Panel Template	<ul style="list-style-type: none"> • Includes D-Link default device panel templates • For third party devices, user can create customized panels • Customizable panel details: <ul style="list-style-type: none"> ▪ Panel name ▪ Stacking support status ▪ Description • Customizable Panel diagrams: • Panel logo (PNG/JPG files less than 2 MB in size) • Panel height and width • Port numbering rule • Port layout design using drag and drop
Monitor Template	<ul style="list-style-type: none"> • Provides different monitoring templates for collection of device information • Customizable categories to identify specific monitoring index factors. The following attributes are displayed for each category entry: <ul style="list-style-type: none"> ▪ Category name ▪ Unit (-, °C, %, bits, bps, ms, pps, rpm) ▪ Protocol (ICMP, SNMP/ HTTP(S)) ▪ Line chart (not supported, default/supported) ▪ Build type (system / user) ▪ Description ▪ Operation (User: edit, delete, alarmable item definition; System: view) • Customizable Monitor Template to monitor and collect defined objects <ul style="list-style-type: none"> ▪ Template name ▪ Category ▪ Vendor ▪ Vendor OID ▪ Interval ▪ Build type ▪ Description ▪ Operation (User: edit, download, delete; System: download, view)
Configuration Template	<ul style="list-style-type: none"> • Configuration Template • Provides multiple configuration templates to configure specific devices via D-View 8 • Multiple config templates can be assigned to Device Template to configure a specific device. • Customizable Configuration Category templates classified by function <ul style="list-style-type: none"> ▪ Category name ▪ Configuration type ▪ Template description ▪ Category feature parameter information • Customizable Configuration Template to configure specific devices via D-View 8 <ul style="list-style-type: none"> ▪ Configuration template name ▪ Vendor name ▪ Template description ▪ Selected configuration template to configure device ▪ Method of configuration (CLI or SNMP) ▪ CLI commands list (if selected) ▪ Programmable GUI object to simplify continuous operation

3.3.2.7. Report

Item	Description
General Report	<p>Each report type can have configurable parameters such as data range and data collection time interval. When reports are generated, they can be exported immediately, saved to My Report, or upgraded to Scheduled Report according to the configured report parameters.</p> <ul style="list-style-type: none"> • 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 Report	<p>Each report type can be a one-time report or recurrent report. User can designate data source device(s) and levels of alarms to be displayed in the reports.</p> <ul style="list-style-type: none"> • Alarm Report • Trap Report • Syslog Report
My Reports	<p>The My Reports category displays the saved list of reports categorized as My Reports from the general report pool. Up to 500 report entries can be saved. The following attributes are listed:</p> <ul style="list-style-type: none"> • Report Name • Report Category • Content Source • Time Created • Result • Operation

3.3.2.8. Tools

Item	Description
MIB Browser	<ul style="list-style-type: none"> • Retrieves and displays MIB data in readable format • Provides a graphical format to read MIB information
MIB Compiler	<ul style="list-style-type: none"> • Compiles device MIB files into D-View 8
ICMP Ping	<ul style="list-style-type: none"> • Checks device operation status and network performance
SNMP Test	<ul style="list-style-type: none"> • Checks device SNMP capabilities using SNMPv1, SNMPv2c or SNMPv3
Trace Route	<ul style="list-style-type: none"> • Checks the route and measures transit delay of packets crossing the network
Command Line Interface (CLI)	<ul style="list-style-type: none"> • Terminal interface for user to connect with device
File Comparison	<ul style="list-style-type: none"> • Lets user compare differences between two configuration files • Differences are highlighted in different colors to identify modification types

3.3.3. Annunciators

Annunciators (indicators) are typically located at the top right corner of the workspace as symbols and text-based notifications of the system statuses. The following annunciator alerts are displayed for the status listed as follows:

Item	Description	Icon
Notifications	Non-critical Information regarding system status.	
Info Alarm	Information regarding system function requiring further attention to avoid affecting system operation.	
Warning Alarm	Information regarding system errors or faults that may affect system operation.	
Critical Alarm	Information regarding system error or faults if not resolved specified function failure will occur.	

3.3.3.1. User Menu

Item	Description
User Profile	Displays the available information for the current user
Wizard	<ul style="list-style-type: none"> • D-View 7 Upgrade: migrate D-View 7 database and probes to D-View 8 • Discovery: discover the network or add devices from the network • Monitoring: create customized topologies, simulate racks, and create customized dashboards • Alarm: customize related network alarms (Configure Alarms) and notifications (Configure Notifications)
Network Discovery Records	Display a list record of the discovered network
Sign out	Logs the current user out of the interface

3.3.4. Workspace Preferences

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

3.3.4.1. Selecting Data

Many of the panels in the dashboard allow for references to be selected for subsequent reference, such as Device Type Statistics or Alarm Statistics.

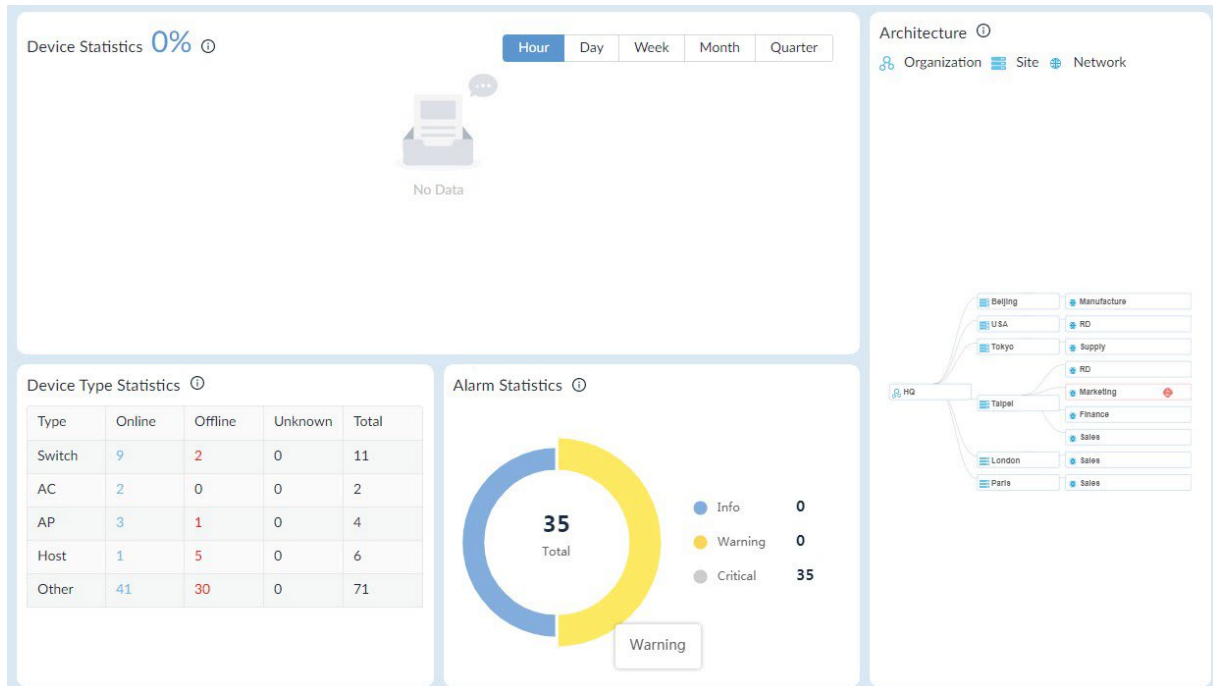


Figure 74 Dashboard Workspace Widgets

The workspaces are designed to allow for access to important information through a centralized interface.

To select specific information, click on any of the hyperlinked content and the related information display. As seen in the previous Alarm Statistics panel, the indicator Critical has been disabled resulting in the graph displaying only Warning and Info statistics.

3.4. Change the User Password

It is highly recommended to change your password to a secure password. As an Organization Administrator, you can create usernames and the respective password for other user types.

To change your password:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Locate the User Menu and click to display the available options.
3. Select **User Profile** to display the user’s personal information page.

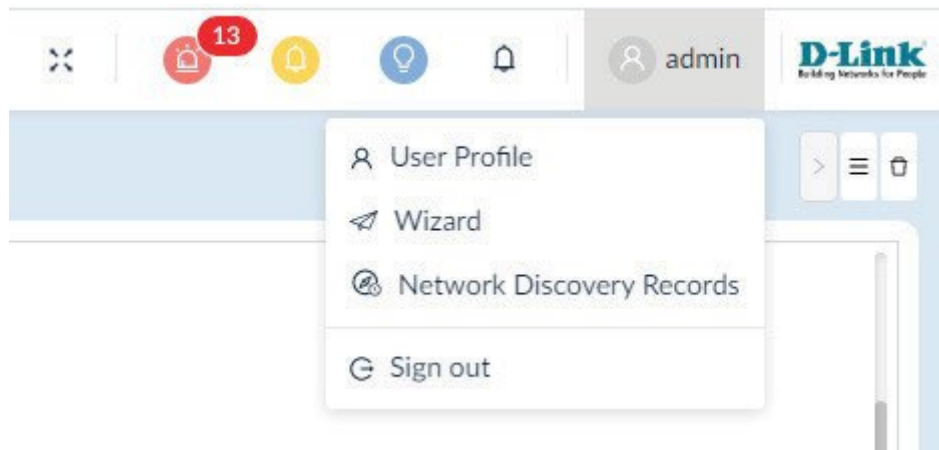


Figure 75 Selecting a User Profile

The Personal Information page displays.

A screenshot of the 'Personal Information' page for the user 'admin'. The page is divided into several sections:

- Profile Summary:** Shows a placeholder for a profile picture (JPG or PNG file, Less than 2 MB), the name 'admin', the role 'Super Administrator', and the email 'admin@qq.com'.
- Personal Information:** Fields for Nickname (Super Administrator), Location (Enter Location), Telephone (Enter Telephone Number), and Description (Enter Description). A 'Save' button is at the bottom right.
- Change Password:** Fields for Current Password (Enter current password), New Password (Enter new password), and Retype Password (Retype password). A 'Save' button is at the bottom right.
- Reset Password:** A 'Reset' button. Text below explains that clicking 'Reset' will send an email to the account's address.
- Change Email:** Field for Email Address (admin@qq.com) and a 'Change' button.
- Personal Settings:** A toggle switch for 'Sign Out Automatically'.

Figure 76 Modifying a User Profile

4. Under the Change Password section, enter the Current Password.
5. Enter a New Password, then retype the New Password to validate it.
6. Click **Save** to set the new settings.
The password is updated.

3.5. Change Account Information

Changing the general account settings such as the Email address and contact number is achieved through the User Profile page.

To change your personal information:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In the Personal Information section, enter your relevant information.

The screenshot shows the 'User Profile' page in a web browser. On the left is a user profile card for 'admin', identified as 'Super Administrator' with email 'admin@qq.com'. The main content area is titled 'Personal Information' and contains several form sections:

- Personal Information:** Fields for Nickname (filled with 'Super Administrator'), Location, Telephone, and Description. A 'Save' button is at the bottom right.
- Change Password:** Fields for Current Password, New Password, and Retype Password. A 'Save' button is at the bottom right.
- Reset Password:** A text block explaining the process and a 'Reset' button.
- Change Email:** A field for Email Address (filled with 'admin@qq.com') and a 'Change' button.
- Personal Settings:** A 'Sign Out Automatically' toggle switch.

Figure 77 Entering Personal Information

3. Click **Save** to set the new settings.
The Personal Information is updated.

3.6. Configure Email Server Alerts & Alarm Notifications

Prior to sending notifications, the Email server must be configured. Only an admin user can configure the email server settings.



NOTE: For information about adding an alarm notification profile with an email address to which the application can send a notification, see Configure the Notification Center.

3.6.1. Configuring the Mail Server Settings

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click the **System** and select **Basic Settings**.
3. Select the **Mail Server Settings** tab.
The **Mail Server Settings** page displays.

Figure 78 Configuring Mail Server

4. In the Domain Name field, enter the Email domain.
5. In Mail Server, enter the following information:

Item	Description
Mail Server	
SMTP Host	Enter the address as provided by the Email host.
Port	Enter the SMTP port used by the correlating outgoing mail server.
From Email Address	Enter the initiating Email address.
From Name	Enter the name to associate with the outgoing Email address.
Security Type	Select the encryption method used by the outgoing mail server (optional), settings: None, SSL.
Encoding Type	Select the character encoding key to convert 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: <ul style="list-style-type: none"> • Username: Enter the username with authority to access the server. • Password: Enter the correlating password of the given username.
Save	Click Save to enter the Mail Server settings.

- In the Test Mail Server field, enter a valid Email to send a validation test for the Mail Server settings. If correctly configured, the received Email functions to validate the new settings. If there is no received Email, check the settings and retry the test mail function. The new Mail Server is configured.

3.7. Configure the Notification Center

Before the D-View 8 can deliver alarm notifications, the Notification Rule must be configured. Only Administrators and Organization Administrators can configure notification settings.

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Click the Alarm & Notification and select Notification Center. The Notification Center information displays.
- Click **Add Notification Rule**.

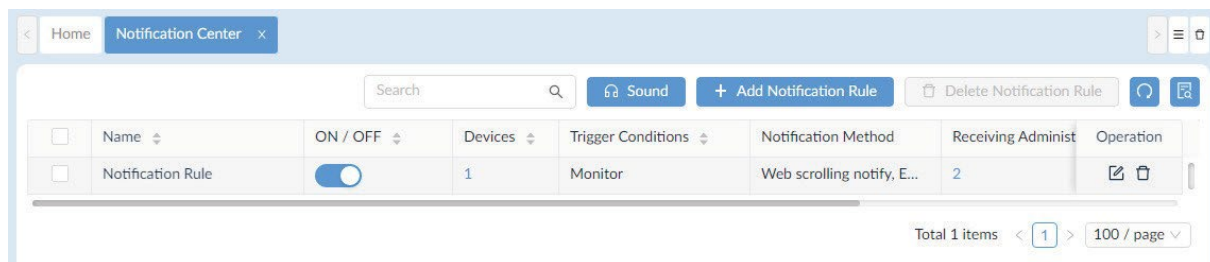


Figure 79 Adding a Notification Rule

The Notification Management Details page displays.

- Fill in the Basic Information.
- Click the **ON/OFF** slider button to enable or disable the rule.

The screenshot shows the 'Notification Management Details' form. It is divided into three main sections: 'Basic Information', 'Source Devices', and 'Trigger Conditions'.
 - **Basic Information:** Includes a 'Name' field (required, labeled '* Name:'), a 'Description' field, and an 'ON / OFF' slider button.
 - **Source Devices:** Includes a '+ Add' button and a table with columns: System Name, IP, Network, Model Name, and Operation. The table is currently empty, showing 'No Data' and 'Total 0 items' with a '15 / page' dropdown.
 - **Trigger Conditions:** Includes a '* Condition Type:' dropdown menu (set to 'Monitor') and a text input field with the placeholder 'Please choose one or more'. Below this is a '* Alarm Level:' section with checkboxes for 'All', 'Critical', 'Warning', and 'Info', all of which are checked.
 At the bottom right of the form, there are 'Cancel' and 'Save' buttons.

Figure 80 Adding a Notification Rule

- In Source Devices, click **Add** to select the target device. The Batch Select Devices page displays.
- From the Device List, select the device(s) to include in the notification rule.

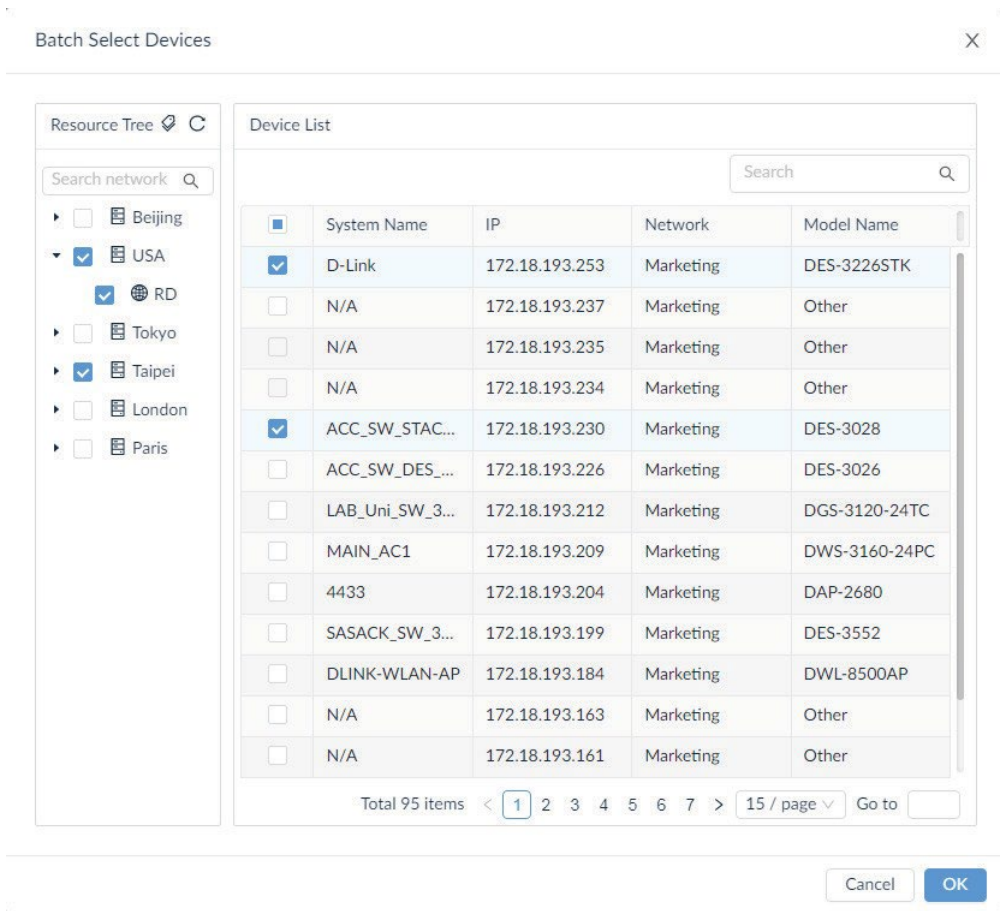


Figure 81 Batch Device Selection

- Click **OK** to accept the device selection and return to the previous menu.
- In the Notification Management Details page, locate Trigger Conditions, click the **Condition Type** drop-down menu to select the threshold condition. In the following figure, Monitor is selected. See the following table for further information on available options.

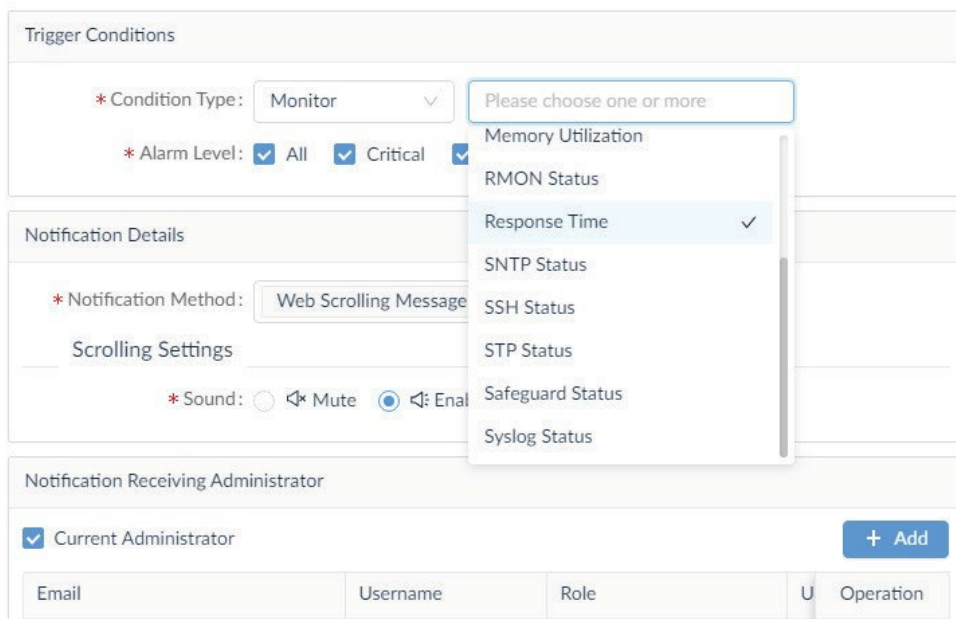


Figure 82 Trigger Condition Specification

Item	Description
Condition Type	
	The type of monitoring condition available is dependent on the selected device.
Monitor	<ul style="list-style-type: none"> • 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	After selecting Trap as the condition type for the notification, alarms generated by the trap alarm rule will trigger a specified notification. To set trap alarm rules navigate to Alarm & Notification > Monitoring & Alarm Settings > Alarm Settings , under Type select Trap .
Syslog	After selecting Syslog as the condition type for the notification, alarms generated by the syslog alarm rule will trigger a specified notification. To set trap alarm rules navigate to Alarm & Notification > Monitoring & Alarm Settings > Alarm Settings , under Type select Syslog .
Wired Traffic	After selecting Wired Traffic as the condition type for the notification, alarms generated by the syslog alarm rule will trigger a specified notification. To set trap alarm rules navigate to Alarm & Notification > Monitoring & Alarm Settings > Alarm Settings , under Type select Monitor > Wired Traffic .
Alarm Level	Select the type of alarm to trigger the notification: All: all alarm levels are selected for notification. Critical: error information condition indicating failure or malfunction. Warning: error information conditions that may cause future problems Info: information-only level conditions

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

Item	Description
Notification Method	
Web Scrolling Message	Select the Screen Scrolling Setting for the alert: Mute sound or Enable Voice.
Email	<ul style="list-style-type: none"> • Click to enable the Current Administrator setting. • Click Add to select a specific user to receive the Email notifications. Enter specific criteria (Email, Username, Role) to search for a defined user. • Click OK to accept. Click Cancel to return to the previous screen.
Execute Script	<ul style="list-style-type: none"> • In the Command Line, enter the script to execute. • Select the device to apply the script when trigger is enabled.

11. Under the Notification Suspension Period, click **Add** to select a schedule. The Select Schedule page displays.

12. Select a defined schedule period and click **OK** to accept. Click **Cancel** to return to the previous screen.

13. Click **Save** to accept the notification rule. Click **Cancel** to return to the previous screen. The notification rule is saved.

This page is intentionally left blank.

4 Overview and Management

Before you can manage your network, you must let the application find the devices that are on your network and perform other setup tasks that could simplify the management of your network.

This chapter covers the following topics:

- Discovery modes
- Using Network Discovery
- Using Device Discovery
- View and manage the wired and wireless devices on a network
- Manage device groups

4.1. Discovery Modes

D-View 8 is designed to function through the use of probes as the primary component used to connect network devices. They effectively run as a background process performing the discovery function for devices polling existing devices for statistics data, and acting as a staging point for forwarding data to the D-View 8 server for networks behind a firewall or in a NAT environment.

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

Deploying individual probes for a particular network segment helps to alleviate bandwidth constraints, as that 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 of the devices communicating directly with the server. Separating network devices into groups also becomes easier as identification based on a number of criteria can more easily be applied for a given network topology.

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

You can discover networks and devices by using the following methods:

- Network Discovery:
- Device Discovery: this method allows for the discovery of devices within a confirmed network location.

With both methods, D-View 8 can discover wired devices, wireless devices, D-Link devices, and third-party devices that support standard SNMP MIBs.

For wireless access points (APs), the type of AP determines whether it can be discovered:

- Standalone AP
- Controller-managed AP

4.1.1. Using Network Discovery

Network discovery allows an administrator to monitor and manage active networks that are paired with the D-View 8 server. Each network is listed in the Architecture frame of the dashboard. The number of managed devices is also displayed, along with device statistics, alarm statistics and an overview for each of the paired devices.

1. Login to the Dashboard, see "3.2. Launching D-View 8 Web GUI" on page 41.
2. Click the **Monitoring** and select **Network Discovery**. The **Network Discovery** information displays.
3. Click **Add Network**.

Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest Discovery Status	Discovery Range	Operation
CS	Beijing_Marketing	Primary; LocalProbe-172....	29	Enabled	End	1.172.18.192.1/24	[Edit] [Refresh] [Delete]
site_sim	Shanghai_Finance	Primary; LocalProbe-172....	101	Enabled	End	1.2.0.0-2.0.0.9	[Edit] [Refresh] [Delete]

Total 2 Networks

Total 2 items < 1 > 100 / page

Figure 83 Adding a Network

The Add Network page displays.

4. Click **Add Network**.

Add Network

Manage SNMP devices automatically

Probe Mode

*Primary:

Standby:

Discovery Range

Discovery Range	Type	Selected SNMP Credentials	Operation
172.95.1.1	IP	Sample v2 x	[Edit] [Delete]

Total 1 items < 1 > 15 / page


Schedule Information

Schedule Type: One Time Recurrent

One-Time Type: Immediately Select a Date

Figure 84 Configuring Network Information

5. Enter the new network information as follows:

Item	Description
Basic Information	
Network Name	Enter a text string to identify the new network entry.
Site Name	Click the drop-down menu to select an existing site or click New to enter a text string for the site.
Discover all pingable devices	Select to enable (default) or disable the function to automatically discover all pingable devices.
Manage SNMP devices automatically	Select to enable (default) or disable the automatic management of all SNMP devices.
Probe Mode	
Primary	Click the drop down menu to configure the probe mode settings to designate it as primary.
	 <p>NOTE: If the probe mode is identified as primary, it cannot be designated as a Standby probe.</p>

Item	Description
Standby	Click the drop-down menu to configure the probe mode as standby.
Discovery Range	
Add Discovery Range	Click the Add Discovery Range button to define a range set for a network search event.
Discovery Range	List of the configured range settings defining the network. See “Adding a Discovery Range” for further information.
Type	Lists the category of device.
Select SNMP Credentials	Click the SNMP field and select the credential in use by the remote device: Sample v2, Sample v1, or Add SNMP Credential. See Adding an SNMP Credential for more details.
Edit	Click the Edit button to modify the discovery range.
Delete	Click the Delete button to remove the discovery range.
Schedule	
Schedule Type	Select the occurrence rate for the network discovery function: <ul style="list-style-type: none"> • One Time: in the One-Time Type option specify the period to initiate the discovery function. • Recurrent: In the Schedule field, define the period(s) to activate the discovery function.
Cancel	Click Cancel to return to the previous page.
Save	Click Save to add the new network.

The added network successfully displays after the new network discovery profile is created.

4.1.1.1. Adding a Discovery Range

To add a discovery range:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click the **Monitoring** and select **Network Discovery**.
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	✎ 🔄 🗑️

Total 9 items < 1 > 15 / page

Figure 85 Network Discovery Page

3. Click **Add Network** to display the Add Network page.
4. Select Probe Mode and click **Add Discovery Range**.
The Add Discovery Range page displays.

Figure 86 Configuring Discovery Range

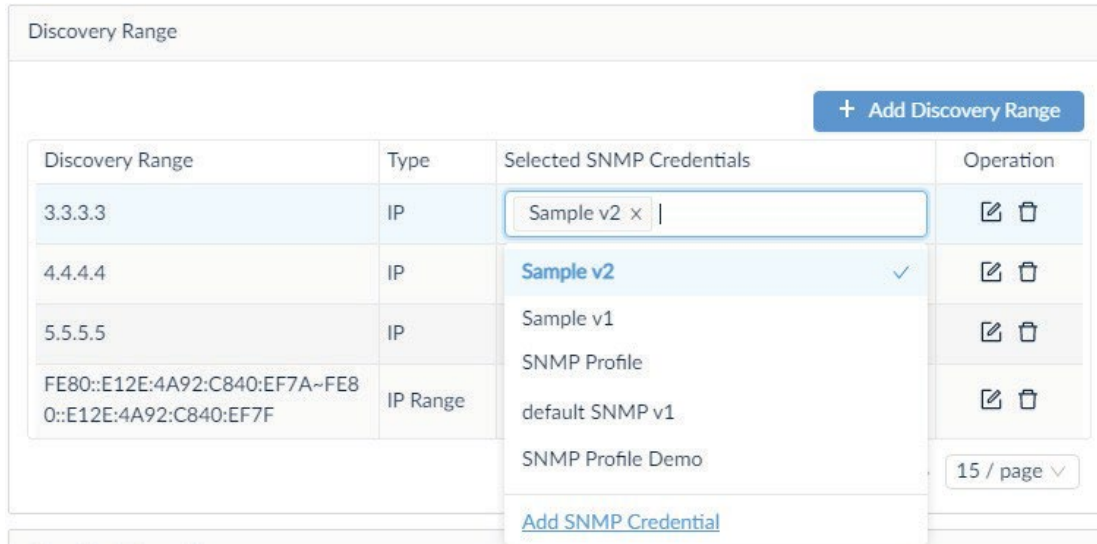
Item	Description
Type	Click to select the coverage range: IP, IP Range, Subnet, Import CSV File.
IP	Enter a single IP address as the discovery range. Select IPv4 or IPv6 to specify the IP protocol for the coverage type.
IP Range	Enter the starting IP and ending IP addresses to define the range. <ul style="list-style-type: none"> • 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 to define the discovery range. Select IPv4 or IPv6 to specify the subnet protocol for the coverage type.
Import CSV File	<p>Click Upload File to select a pre-specified file.</p> <p>To Upload a File:</p> <ol style="list-style-type: none"> 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, the discovery rule parameters must not include a comma “,”. 4. The order of SNMP v2 parameters is: Discover IP, SNMP Version, RO Community, RW Community. 5. SNMP v3 parameters order: Discover IP, SNMP Version, UserName, Mode, Auth Algorithm, Auth Password, Private Algorithm, Private Password. 6. Parameters can be set to the following values: <ul style="list-style-type: none"> ▪ Mode: authNoPriv, noAuthNoPriv ▪ Auth Algorithm: MD5, SHA ▪ Private Algorithm: 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 the subnet. 10. The “Import from File” method only supports discovery of SNMP V1/V2/V3 devices. The available “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. <p>Sample rule:</p> <pre> 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, initial, noAuthNoPriv 192.168.1.1-192.168.1.17, V3, initial, AuthNoPriv, SHA, password 192.168.1.0/24, v3, initial, authPriv, MD5, password, AES, password </pre>
Cancel	Click Cancel to return to the previous page.
OK	Click OK to add the new range.

The new discovery range is created.

4.1.1.2. Adding an SNMP Credential

To add an SNMP credential to a network range:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click the **Monitoring** and select **Network Discovery**.
The **Network Discovery** information displays.
3. Select a network entry and click Edit. The Edit Network page displays.
4. Select Discovery Range, select an existing range and click the Selected SNMP Credentials field.
5. From the SNMP field, click **Add SNMP Credential**.



6.

Figure 87 Configuring SNMP Credentials for Range

The Add SNMP Credential page displays.

7. In the Selected SNMP Credentials field, click to select a defined credential or click Add SNMP Credential to define one.

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

Add SNMP Credential

SNMP Protocol Version: SNMP v1 SNMP v2c SNMP v3

* Name:

* Port:

* Timeout [s]:

* Retransmit:

* Read Community: [Clear]

Write Community: [Clear]

* Non-Repeaters:

* Max-Repetitions:

Description:

Cancel

Figure 88 Configuring SNMP Credentials

Item	Description
SNMP Protocol Version	<p>Click to select the SNMP version. By default, the SNMP v2c information is displayed.</p> <ul style="list-style-type: none"> • If SNMP v1 or SNMP v2c are selected, specify the write community and read community strings. • If SNMP v3 is selected, specify the username and, if required, the authentication protocol.
Name	Enter the display name for the credential.
Port	Enter the SNMP port and read only credential (default: 161).
Timeout (s)	Enter the time (in seconds) in which a response is expected. The default is four seconds.
Retransmit	Enter the number of attempts to make if a response is not received. The default is three.
SNMP v1/v2c	
Read Community	Enter the community used for SNMP read access to the defined host(s). For SNMP v1 and v2c credentials only.
Write Community	Enter the community used for SNMP write access to the defined host(s). For SNMP v1 and v2c credentials only.
Description	Enter a string text to describe the SNMP credentials.
SNMP v2c/v3	
Non-Repeaters	Enter the value (default: 0) to specify the number of variables in the variable bindings list for which a single lexicographic successor is to be returned. To perform a GETBULK request, an OID and two other parameters, Max Repetitions and Non-Repeaters values, are required.
Max-Repetitions	Enter the value to specify the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list. To perform a GETBULK request, an OID and two other parameters, Max Repetitions and Non-Repeaters values, are required.
SNMP v3	
User Name	Enter the username for SNMP v3 credentials only.
Context Name	Enter the octet string (no length limitation), minimum of a single management entry, to uniquely identify the SNMP entity within an administrative domain
Security Level	<p>For SNMP v3 credentials only. Displays the security level selected using the authentication and privacy protocols.</p> <ul style="list-style-type: none"> • authPriv: authentication and privacy (default). • authNoPriv: authentication, no privacy. • noAuthNoPriv: no authentication and no privacy. <p>There is no setting for privacy without authentication.</p>
Authentication Protocol	<p>Click the drop-down menu to select the protocol used to encrypt the authentication with the client.</p> <p>For SNMP v3 credentials only. Select one of the following:</p> <ul style="list-style-type: none"> • MD5: select to enter an authentication passphrase. The MD5 hashed passphrase is used to access the target device. • SHA: select to enter an authentication passphrase. The SHA hashed passphrase is used to access the target device.
Authentication Password	Enter the password (passphrase) for the correlating Authentication Protocol which is used to encrypt the credentials. For SNMP v3 credentials only, and only if you have chosen an authentication protocol.
Privacy Protocol	<p>The protocol used to encrypt data retrieved from the target. This is for SNMP v3 credentials only if you have chosen an authentication protocol. Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • DES: privacy key to encrypt data using the DES algorithm. • AES: privacy key to encrypt data using the AES algorithm.

Item	Description
Privacy Password	Enter the password (passphrase) which will be used to encrypt the data. For SNMP v3 credentials only if privacy protocol is selected.
Description	Enter text string to describe the SNMP credential.
Cancel	Click Cancel to return to the previous page.
OK	Click OK to save the new credential.

The new SNMP credential is created.


4.1.2. Using Device in Group

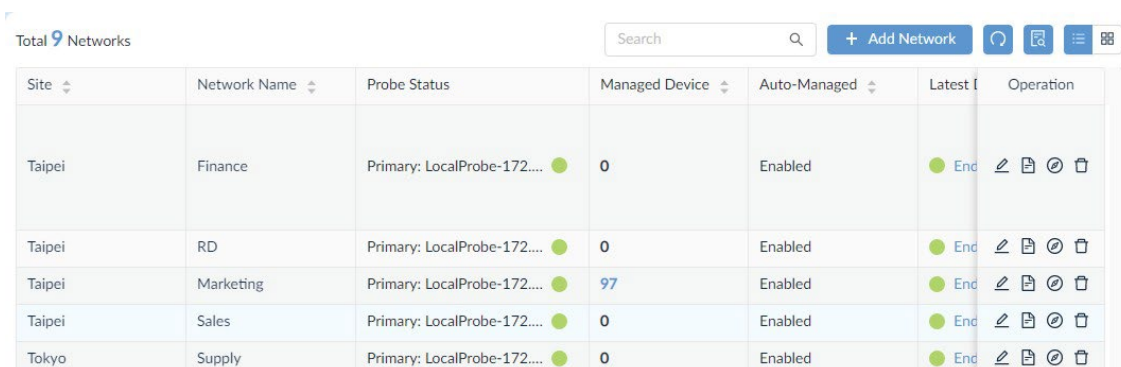
See “4.3.3. Add a Device to a Group” on page 77 for additional information.

4.1.3. Add or Modify a Network Discovery Profile

A network discovery profile encompasses the network information that D-View 8 can detect. The application can discover devices through an IP address range, IP subnet address, a single IP address, a list of IP addresses, or device host name.

To add a discovery profile or modify an existing discovery profile:

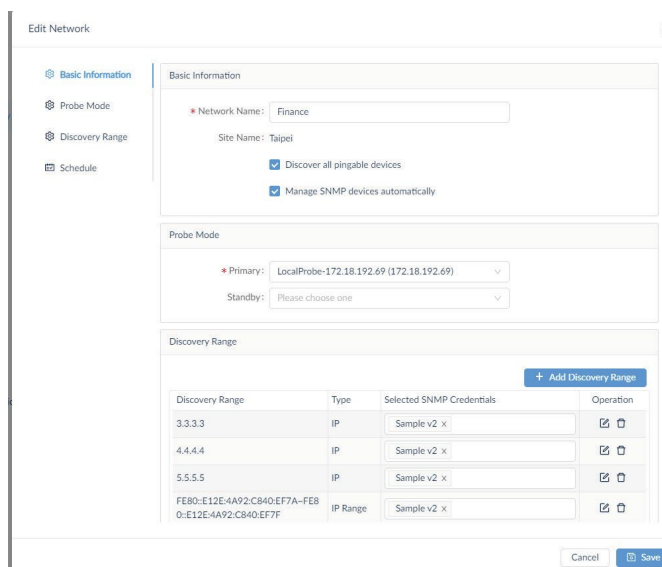
1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Network Discovery**. The **Network Discovery** information displays.
3. Select an existing Network profile to edit, and click Edit  to change the settings.



Site	Network Name	Probe Status	Managed Device	Auto-Managed	Latest I	Operation
Taipei	Finance	Primary: LocalProbe-172....	0	Enabled	End	
Taipei	RD	Primary: LocalProbe-172....	0	Enabled	End	
Taipei	Marketing	Primary: LocalProbe-172....	97	Enabled	End	
Taipei	Sales	Primary: LocalProbe-172....	0	Enabled	End	
Tokyo	Supply	Primary: LocalProbe-172....	0	Enabled	End	

Figure 89 Configuring Existing Profile

The Edit Network page displays.



The Edit Network page displays the following configuration options:

- Basic Information:**
 - Network Name: Finance
 - Site Name: Taipei
 - Discover all pingable devices
 - Manage SNMP devices automatically
- Probe Mode:**
 - Primary: LocalProbe-172.18.192.69 (172.18.192.69)
 - Standby: Please choose one
- Discovery Range:**

Discovery Range	Type	Selected SNMP Credentials	Operation
3.3.3.3	IP	Sample v2 x	
4.4.4.4	IP	Sample v2 x	
5.5.5.5	IP	Sample v2 x	
FE80-E12E-4A92-CB40-EF7A-FE80-E12E-4A92-CB40-EF7F	IP Range	Sample v2 x	


Figure 90 Configuring Network Entry

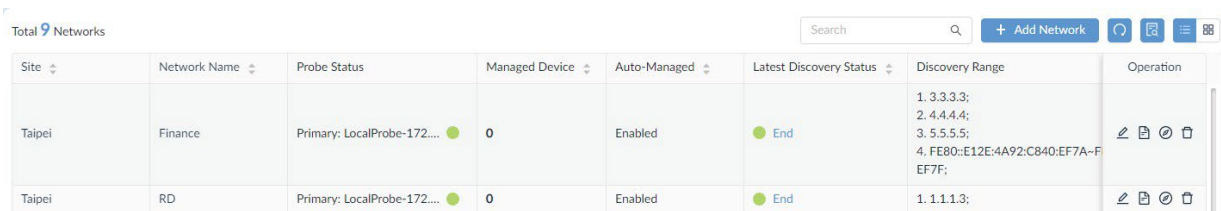
4. Add or Edit an existing profile.
To add a new network profile, see “4.1.1. Using Network Discovery” on page 61.
To modify an existing network profile, see the following:
 - a. From the Basic Information pane, edit the network name and enable/disable Discover all pingable devices and Manage SNMP devices automatically.
 - b. From the Probe Mode pane, select the primary and standby probes for the network.
 - c. From the Discovery Range pane, configure the network range to search for available devices.
 - d. From the Schedule pane, configure the timeframe to initiate the network discovery.
5. Click **Save** to set the new settings or **Cancel** to return to the previous menu.

4.1.4. Execute a Network Discovery Job

The D-View 8 provides a one-time discovery job, which can be executed immediately.

To execute a discovery job:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Network Discovery**.
The **Network Discovery** information displays.
3. Select an existing Network profile and click Discover Now  to start the discovery job.



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-FEF7F;	
Taipei	RD	Primary: LocalProbe-172...	0	Enabled	End	1. 1.1.1.3;	

Figure 91 Initiating a Discovery Task

The Latest Discovery Status field displays Create when the job is started.

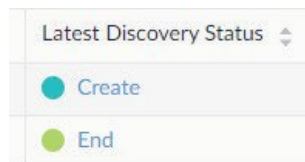


Figure 92 Discovery Starting Status

The field displays Running when the job is in process.

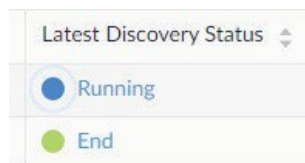
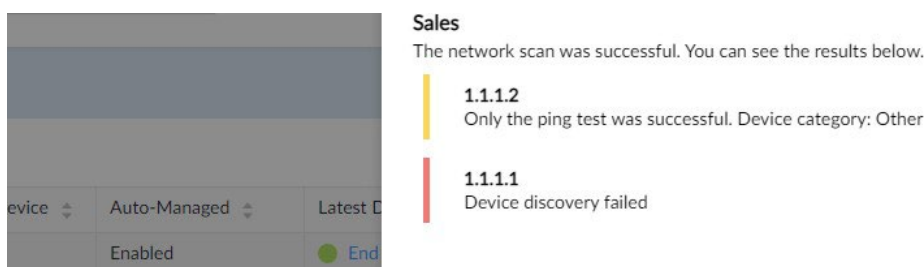


Figure 93 Discovery In Process Status

The Last Discovery Results page displays. The listing of discovered devices found by the application are displayed in the results.



Device	Auto-Managed	Latest Discovery Status
	Enabled	End

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

- **1.1.1.2**
Only the ping test was successful. Device category: Other
- **1.1.1.1**
Device discovery failed

Figure 94 Discovery Results Display

4.1.5. Delete a Network Discovery Profile

If you delete a network discovery profile from the networks list, the application deletes the profile along with the correlating data information.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Network Discovery**.
The **Network Discovery** information displays.

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;	[Edit] [Refresh] [Delete]
site_sim	Shanghai_Finance	Primary: LocalProbe-172...	101	Enabled	End	1. 2.0.0.0~2.0.0.99;	[Edit] [Refresh] [Delete]
CS	Beijing_Marketing	Primary: LocalProbe-172...	32	Enabled	End	1. 172.18.192.1/23;	[Edit] [Refresh] [Delete]

Figure 95 Network Discovery Results

3. Select a network discovery profile and click Delete .
A confirmation page displays.
4. Click **OK** to delete the profile or **Cancel** to return to the previous menu.
A Deleted successfully prompt displays when the network discovery profile is deleted.

4.2. Manage Network Wired & Wireless Devices

D-View 8 device management function helps you to more effectively manage your device infrastructure. This section covers the following sections:

- View device information
- View wireless device information
- Modify device information
- Remove device information
- Ping or reboot a device
- View and export a device list

4.2.1. View device information

The **Device View** section shows devices listed by type and additional information. The default view is All. For each category of device, the status, most recent event, and other relevant information such as IP, MAC address, and others is shown. Clicking on a system name displays the device’s detail page.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device View**.
The **Device View** information 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

Figure 96 Device Information Page

Item	Description
Device Type (tab)	The device types are categorized by function and include: All, Managed, Unmanaged, Ignored, and Conflicted device types. To select a specific type, click on the specific device tab to view the available entries.
Status	Click to sort the list by status. Options: Online (Green), Offline (Red), Unknown (Grey).
System Name	Click to sort the list by system name (ascending or descending alphabetical order).
IP	Click to sort the list by IP address (ascending or descending numerical order).
MAC	Click to sort the list by MAC address (ascending or descending alphabetical order).
Device Type	Click to sort the list by device type (ascending or descending alphabetical order).
Model Name	Displays the device's model name.
Site Name	Displays the defined correlating network site of the device.
Network	Click to sort the list network name (ascending or descending alphabetical order).
CPU Utilization	Displays the CPU utilization in a percentage of the device.
Vendor	Displays the originating vendor name of the device.
Discovered Time	Displays the latest discovered time of the device.
Management Type	Displays whether the device is managed or unmanaged.

4.2.2. View Discovered Device Information

To view discovered device types and select specific device categories:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring**, and select **Device View**. The **Device View** information displays.
3. From the category menu select a specific tab to view the correlating devices. The following is the **Managed** device category, **Host-All** is selected.

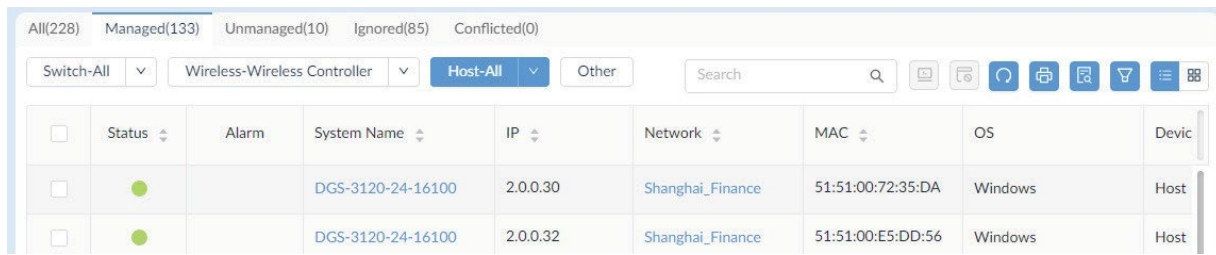









Figure 97 Selecting Device Categories

Item	Description
All	Displays all detected devices available to the user.
Managed	Displays all managed devices available to the user.
	Switch-All: click the drop-down menu to list All, sFlow, or PoE designated switch devices.
	Wireless-Wireless Controller: click the drop-down menu to list Wireless Controller, Access Point, SSID, Wireless Client, or Rogue Ap designated devices.
	Host-All: click the drop-down menu to list All, Process, or Software hosting devices.
Other: click to list any devices not given a device category designation.	
Unmanaged	Displays all unmanaged devices available to the user.
Ignored	Displays all ignored devices available to the user.
Conflicted	Displays the discovered data, whose data does not match existing IP address data.
Management toolbar	
Search	Enter a key variable and select the matching header to display the correlating devices.
Unmanage	 Click to configure the selected device as unmanaged in the application.
Ignore	 Click to configure the selected device as ignored in the application.
Refresh	 Click to refresh the device and view listed information.
Export	 Click to export the discovered devices as a CSV file. Up to 5000 entries can be downloaded in one export job.
Advanced query	 Click to enable an advanced search job. Enter correlating information for the specific device to search.
Columns Selector	 Click to display the table header page. Select specific status categories to display on the table heading. 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 the slider bar to view the Device View table as either a list or a graphical representation.



NOTE: Toolbar options are device specific and only available when the related device type is selected.

4.2.3. View wireless device information

To view discovered wireless devices in the Device View > Managed tab:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device View**.
The **Device View** information displays.
3. From the category menu select the Managed tab.
The **Managed** devices list displays.
4. Click the **Wireless-Wireless Controller** drop-down menu and select **Wireless Controller**.

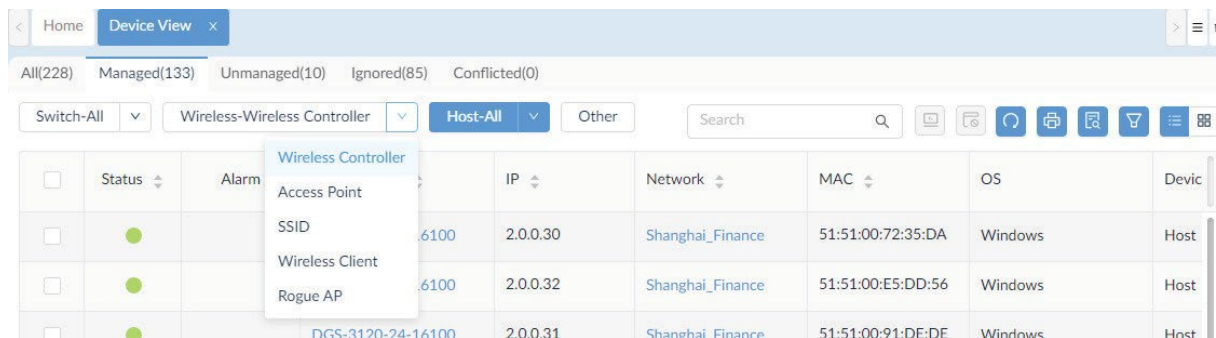


Figure 98 Selecting Wireless Controller

The Wireless Controller panel displays.

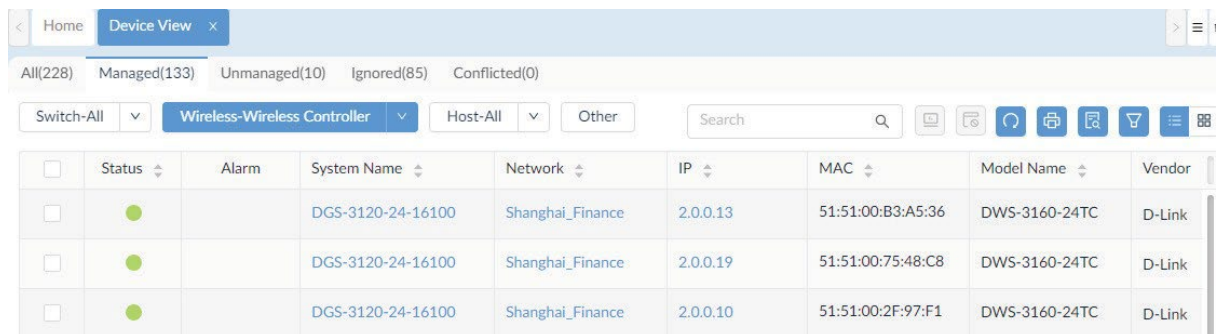


Figure 99 Viewing a Wireless Controller Panel

The page displays the devices discovered by the application.

5. To filter the device list, click a table category. You can filter by criteria such as Status, System Name, Network, etc.
6. To view the details of a device, click the device’s System Name.
7. To modify the configuration profile of a device, select the device and click on a Management Toolbar function. See View Device Type.

4.2.4. Modify device information

Device information can be modified for wired and wireless devices. You can modify the system name, system location, system contact, and additional information that is displayed by the application.

To modify a device’s information:


1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device View**.
The **Device View** information displays.
3. From the category menu select the Managed tab.
4. Click the **Wireless-Wireless Controller** drop-down menu and select **Wireless Controller**.
5. Select a device and click the **System Name** to edit it.
The device’s listed information page displays.

The screenshot displays the D-Link Web GUI for a device named '1CC_SW_3160_24 (172.18.193.49)'. The interface is divided into several sections:

- Device Information:** Shows status as 'Online', IP as '172.18.193.49', and various hardware and system details like 'Vendor: D-Link', 'MAC: 14-D6-4D-5E-37-F0', and 'Firmware Version: Build 1.00.038'.
- Performance Information:** Contains two gauges: 'CPU Utilization' at 21% and 'Memory Utilization' at 89%.
- SNMP Protocol Preferences:** A form for configuring SNMP settings, including protocol version (SNMP v2c selected), port (161), timeout (3), and community strings.
- LACP Working Status:** A table showing LACP channel group configurations.

Channel Group ID	Master Port	Member Port	Active Ports	Aggregator Type
1	4	4-5	N/A	Static
9	20	20-21	N/A	Static

Figure 100 Wireless Device Information

6. From the Device Information pane, click the edit button .
7. Modify the device information.
8. Click Save to update the device information.

4.2.5. Ping or reboot a device

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

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device View**. The **Device View** information displays.
3. The Switch-All category menu is listed.
4. Select a device from the list and click its System Name. The **Device Information** page displays.

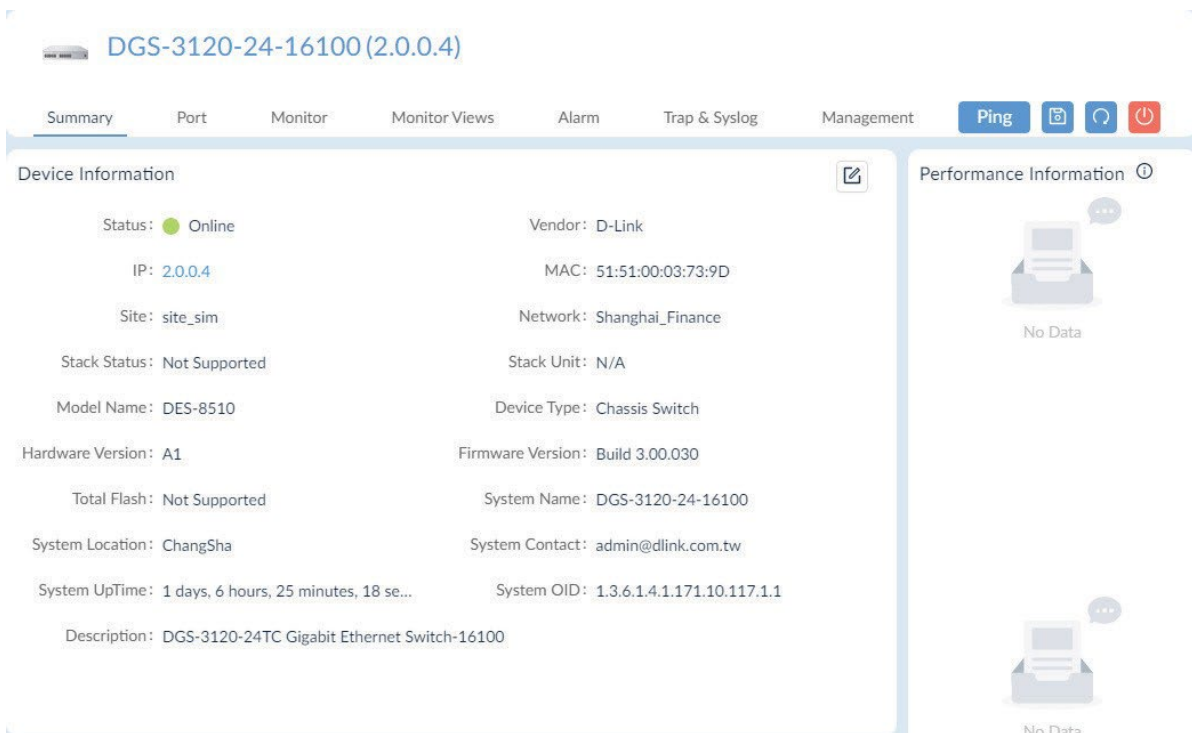


Figure 101 Summary Display of Device

- From the toolbar on the top right, perform one of the following actions:
 - Ping the device: click Ping to initiate a ping action on the device.
 - Save the settings: click Save to save the device information to the device.
 - Refresh the information: click Refresh to synchronize the information with that of the device.
 - Reboot the device: click Reboot to re-start the device.

4.2.6. View and export an Interface List

You can view the interface of device(s) managed by the application, and export the table to a tabular formatted (.csv) file. The export list is only available for managed devices.

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Click **Monitoring** and select **Interface View**. The **Interface View** information displays.
- From the toolbar menu, click Export. Up to 10000 entries can be downloaded in one export job.
- To save the CSV file, follow the browser instructions.

4.3. Manage device groups

Device groups are intended to simplify the management of the network devices. Once a device is discovered it can be added to a group. Groups can be separated by organization, site, or network.

4.3.1. Add a device group

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Click **Monitoring** and select **Device Group**. The **Device Group** page displays.
- Click **Add Device Group**.

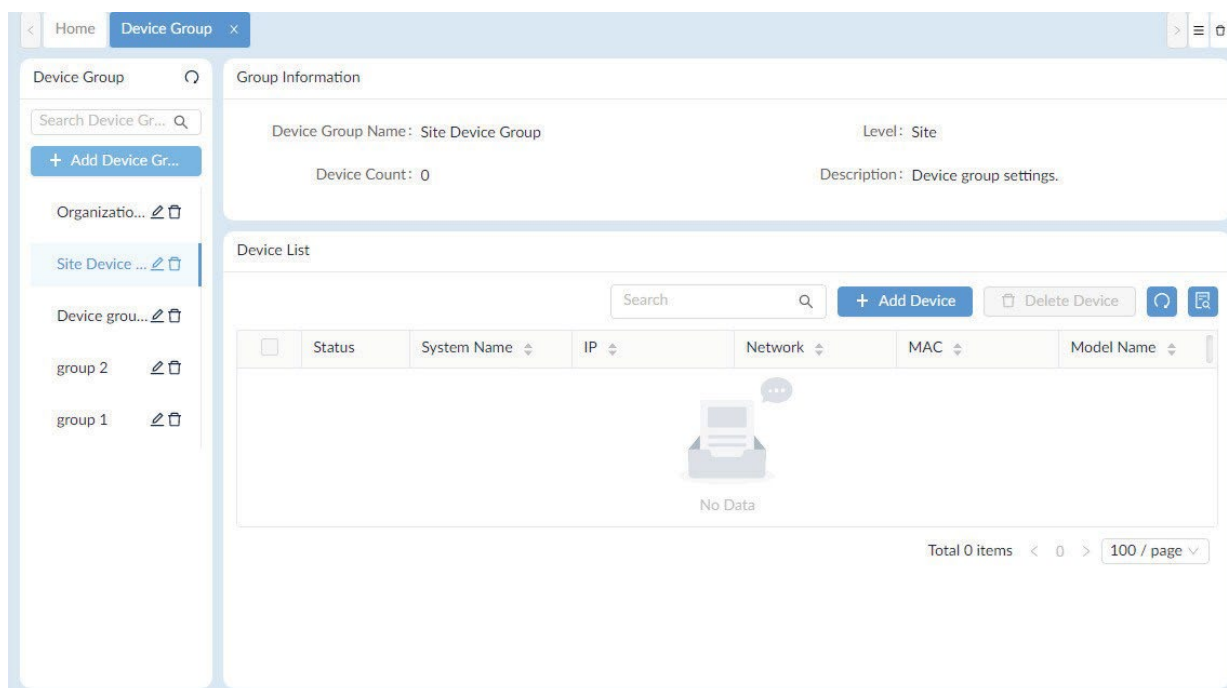


Figure 102 Adding Device Group

The Add Device Group page displays.

4. Enter the group information.

Figure 103 Configuring Group Information

Item	Description
Name	Enter the name for the group.
Level	Click to select the group level (default: Organization).
Organization	Add all discovered devices within the organization are selected for the group.
Site	Click the Range drop-down menu to select the devices within the designated site.
Network	Click the Range drop-down menu to select the devices within the designated network.
Description	Enter a short description to help identify the group.
Cancel	Click Cancel to return to the previous screen.
Save	Click Save to create the group.

5. Click **Save** to create the group.
The Group Information page displays.

6. Click **Add Device**.
The Add Device page displays listing all the devices discovered under the level (Organization, Site, Network) designation.
7. Click on a device to select it or either enter an IP address or model name to specify a device.
8. Click **Save** to add the selection to the group.

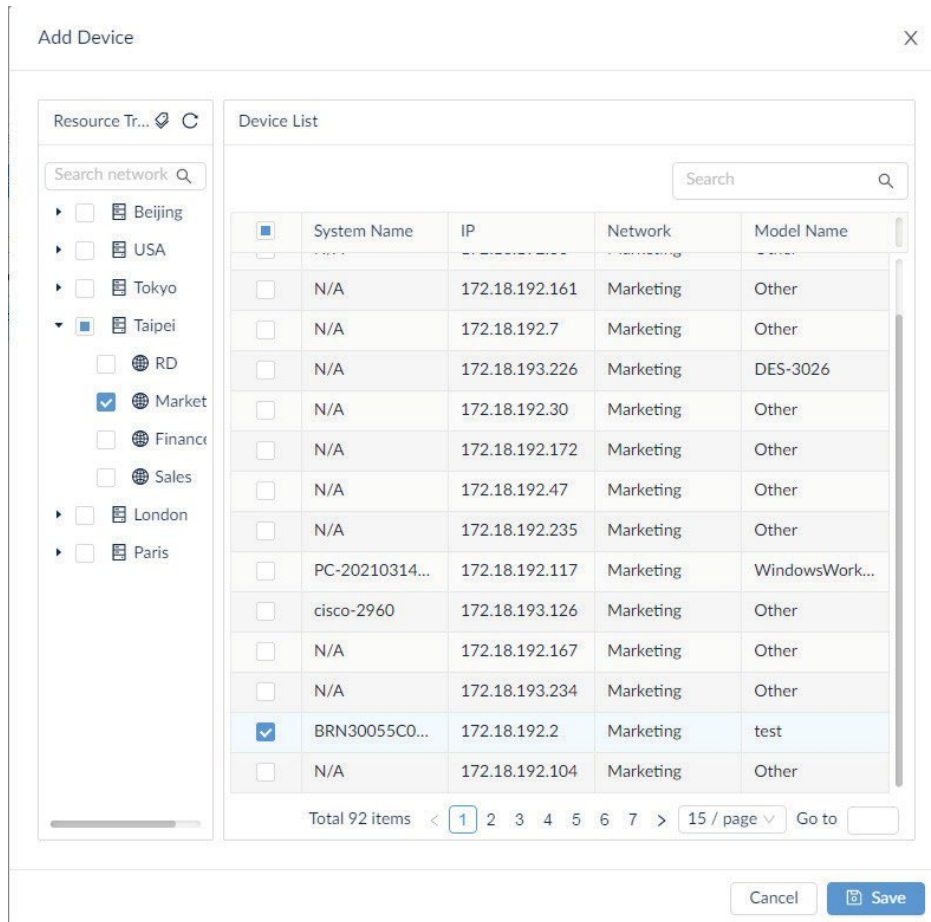


Figure 104 Adding a Device to a Group

4.3.2. Edit (Remove) a device group

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device Group**.
The **Device Group** page displays.

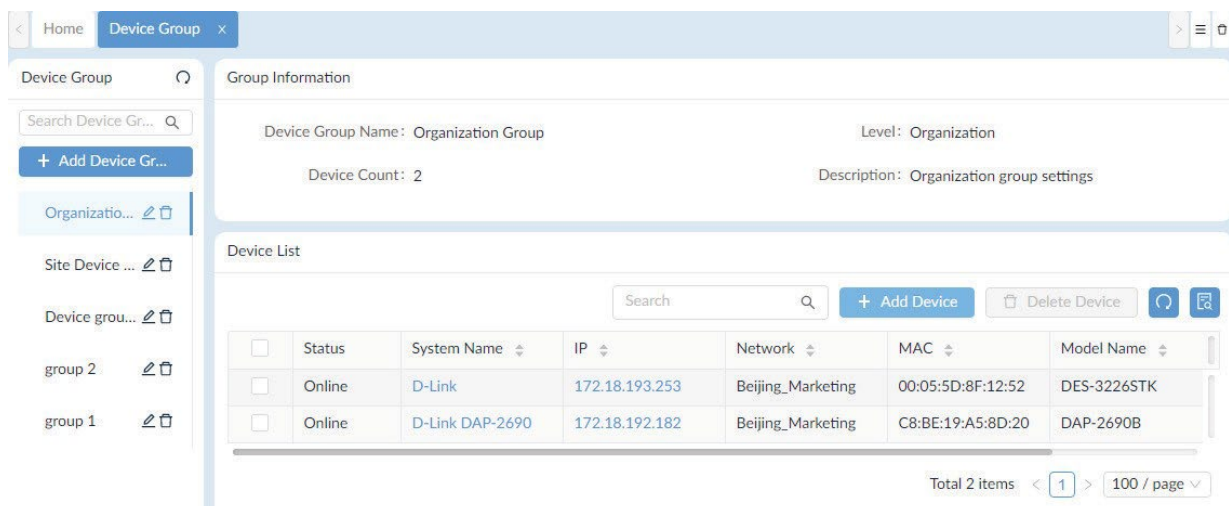


Figure 105 Selecting a Device to Monitor

3. Select an existing device group and perform the following:
 - Edit: click to edit the device group information.
 - Delete: click to remove the device group.

Edit Device Group

* Name:

Level: Organization Site Network

Range: All Devices

Description:

Cancel Save

Figure 106 Configuring a Device Group

The action to the device group is performed.

4.3.3. Add a Device to a Group

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device Group**.
The **Device Group** page displays.
3. Select a Device Group from the **Device Group** column.
The Device List page displays and lists the devices in the group.

Home Device Group

Device Group

Search Device Gr... Q

+ Add Device Gr...

Organization...

Site Device ...

Device grou...

group 2

group 1

Group Information

Device Group Name: Organization Group

Level: Organization

Device Count: 2

Description: Organization group settings

Device List

Search

+ Add Device

<input type="checkbox"/>	Status	System Name	IP	Network	MAC	Model Name
<input type="checkbox"/>	Online	D-Link	172.18.193.253	Beijing_Marketing	00:05:5D:8F:12:52	DES-3226STK
<input type="checkbox"/>	Online	D-Link DAP-2690	172.18.192.182	Beijing_Marketing	C8:BE:19:A5:8D:20	DAP-2690B

Total 2 items < 1 > 100 / page

Figure 107 Adding a Device Group

4. From the Device List, click **Add Device**.
The Add Device displays.

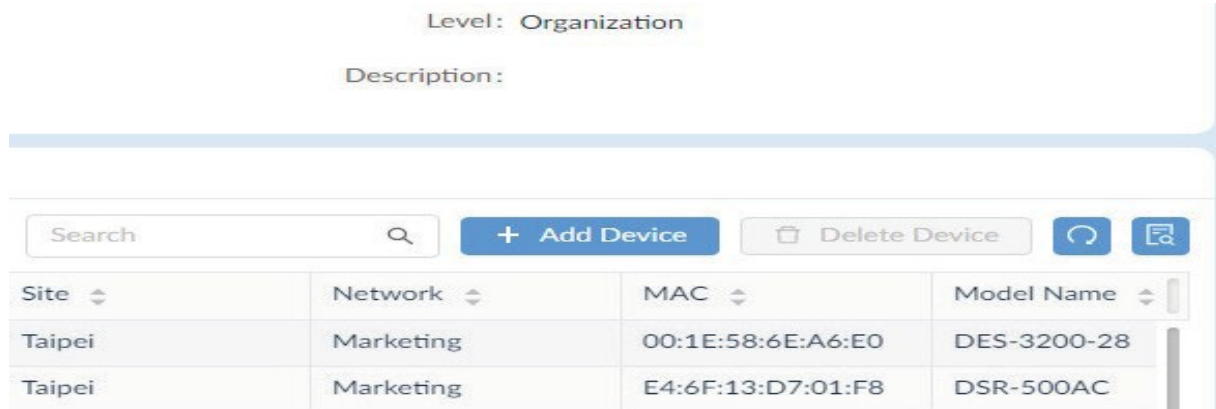


Figure 108 Selecting a Device Group

- From the Resource Tree column, select the group to populate the Device List.

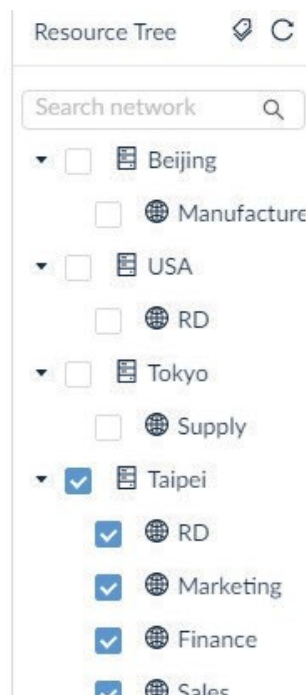


Figure 109 Selecting a Device Group Entry

- From the entries in the Device List, select a device to include in the selected group.
- Alternatively, click the Search field to enter an IP address (range) or model name to filter the search results. From the search results, select a device to include in the list

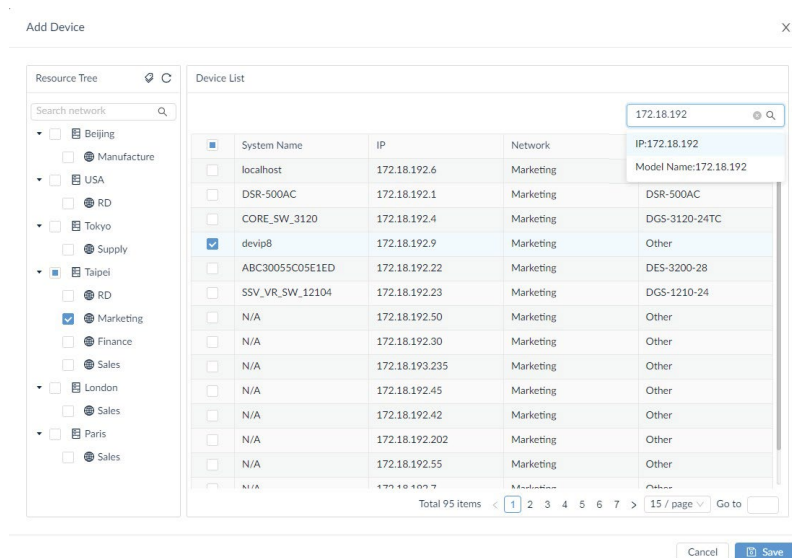


Figure 110 Selecting a Device Group Entry

8. Click **Save** to include the selected device and return to the previous menu.
The device is now included in the defined Device Group.

4.3.4. Remove a Device from a Group

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click **Monitoring** and select **Device Group**.
The **Device Group** page displays.
3. Select a Group from the **Device Group** column.
The Device List page displays and lists the devices in the group.
4. Select a device and click **Delete Device** to remove it.

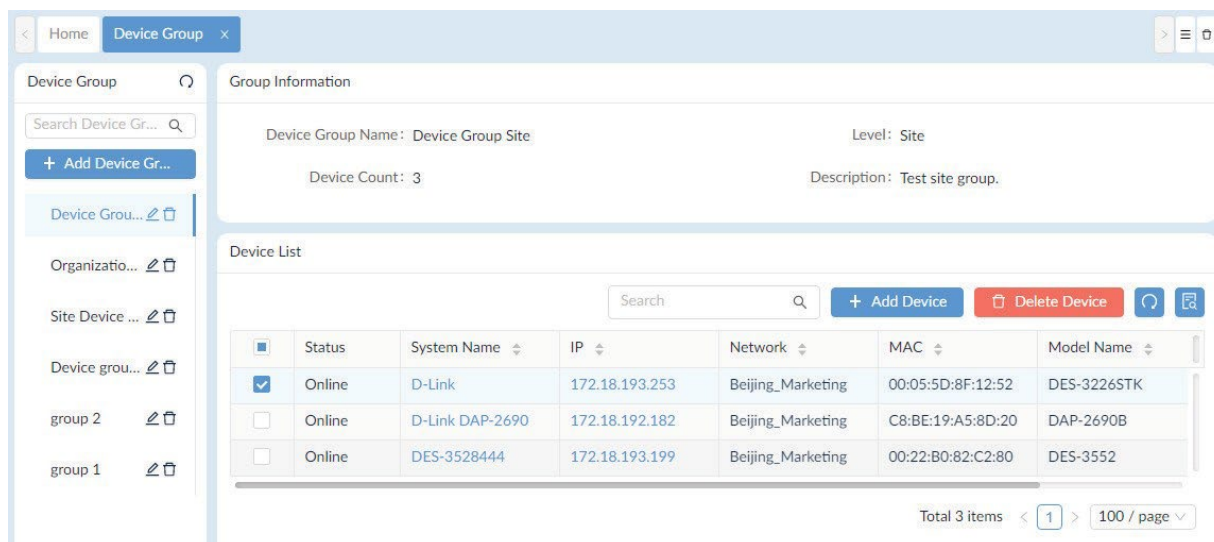


Figure 111 Removing a Device from a Group

5. A confirmation prompt displays. Click **Yes** to remove the device from the group or **No** to return to the previous menu.
The device is removed from the group.

This page is intentionally left blank.

5 Monitoring the Network

You can monitor your network through the Dashboard and other various functions. The information on display can be customized on the Customized Dashboard page.

- Viewing the default dashboard
- Customizing the Dashboard

5.1. Viewing the default dashboard

The default dashboard displays provides information related to the distribution and management of resources connected to the application. The information can be used to assess, utilize, and centrally manage all your critical networks.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.

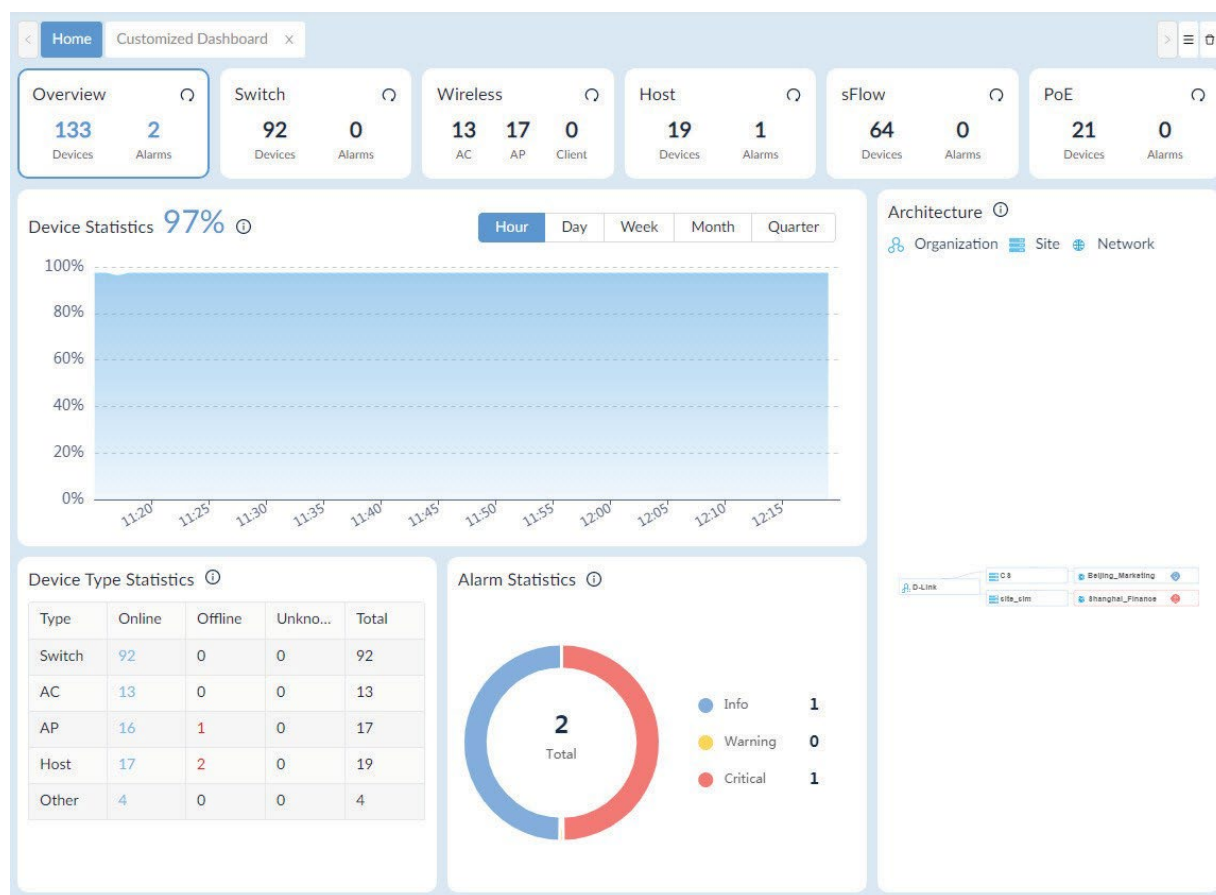


Figure 112 Dashboard Overview

By default, overview displays the following widgets.

Widget	Description
Device Statistics	Managed devices online status statistics.
Architecture	Displays D-View 8 network architecture diagram
Device Type Statistics	Displays statistics on the online status of different types of managed devices.
Alarm Statistics	Displays statistics on the proportion of alarm levels of managed devices.

5.2. Switch Dashboard

From the Dashboard, click the Switch details panel.

The Switch Dashboard displays the following widgets.

Widget	Description
Alarm Statistics	Displays statistics on the alarm level of switches.
Running Status	Displays statistics on the running status of switch devices.
Temperature Statistics	Displays statistics on the specified temperature range of switch devices.
Top 10 Wired Throughput (Rx / Tx)	Displays the top 10 switches that currently send and receive the most traffic.
Top 10 Memory Utilization	Displays the top 10 switches with the highest current memory utilization.
Top 10 CPU Utilization	Display the top 10 switches with the highest CPU utilization.
Top 10 Response Times	Display the top 10 switches with the longest response time.

5.3. Wireless Dashboard

From the Dashboard, click the Wireless details panel.

The Wireless panel displays the following widgets.

Widget	Description
Alarm Statistics	Displays statistics on the proportion of wireless device alarm levels.
Running Status	Displays statistics on the running status of wireless (AC/AP) devices.
AP Summary	Displays statistics on the proportions of AP device types.
Top 10 Wireless	Display the top 10 wireless devices that currently send and receive the most traffic.
Top 10 Wireless Error Throughput	Display the top 10 wireless devices with the most error packets.
Clients by 802.11 Protocol	Statistics on the proportion of 802.11 protocol types used by the client.
Clients by Authentication Type	Displays statistics on the proportions of client authentication type.
Top 10 Critical Alarms by Device	Display the top 10 wireless devices that generated the most critical alarms.
Top 10 Current Clients by SSID	Display the top 10 SSIDs with the most clients currently connected.
Top 10 Response Times	Display the top 10 wireless devices with the longest current response times.
Top 10 Current Clients by AP	Display the top 10 APs with the most clients currently connected.

5.4. Host Dashboard

From the Dashboard, click the Host details panel.

The Host panel displays the following widgets.

Widget	Description
Alarm Statistics	Displays statistics on the proportion of host alarm levels.
Running Status	Displays statistics on the running status of host.
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 current memory utilization
Top 10 Most Installed Applications	Display the top 10 applications with the most installed on the host in network.
Top 10 Volumes with Most Disk Usage	Display the top 10 volumes with the most disk usage in network.
Top 10 Response Times	Display the top 10 switches with the longest response time.
Top 10 Volumes with Least Disk Usage	Display the top 10 volumes with the least disk usage in network.

5.5. sFlow Dashboard

sFlow is only supported in the Enterprise version. From the Dashboard, click the sFlow details panel.

The sFlow panel displays the following widgets.

Widget	Description
Top 10 Endpoints	Display the top 10 most used endpoints.
Recent Alarms Statistics	Display the proportion of sFlow alarm levels in the managed network.
Top 10 Applications	Display the top 10 applications with the most traffic.
Top 10 QoS	Display the top 10 QoS with the most traffic.
Top 10 Conversations	Display the top 10 conversations with the most traffic.

5.6. PoE Dashboard

From the Dashboard, click the PoE details panel.

The PoE panel displays the following widgets.

Widget	Description
Alarm Statistics	Displays statistics on the alarm level of the PoE devices.
Running Status	Statistics on the running status of the managed PSE devices.
Top 10 PSEs by Current PD Count	Display the top 10 PoE devices by the number of powering devices.
Top 10 Ports by Current Flow	Displays the top 10 PoE device ports with the highest current flow.
Top 10 Ports by Power Consumption	Display the top 10 PoE ports by power consumption.
Top 10 Devices by Power Consumption	Display the top 10 PoE devices that are consuming the most power.
Top 10 Response Time	Display the top 10 PoE devices with the longest current response times.

5.7. Customizing the Dashboard

By default, the application displays a dashboard with standard information. You can customize the dashboard views and select one or more widgets.

5.7.1. Create a Customized Dashboard

To create a customized dashboard:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. From the Dashboard menu, click **Customized Dashboard**.
The Customized Dashboard page displays.

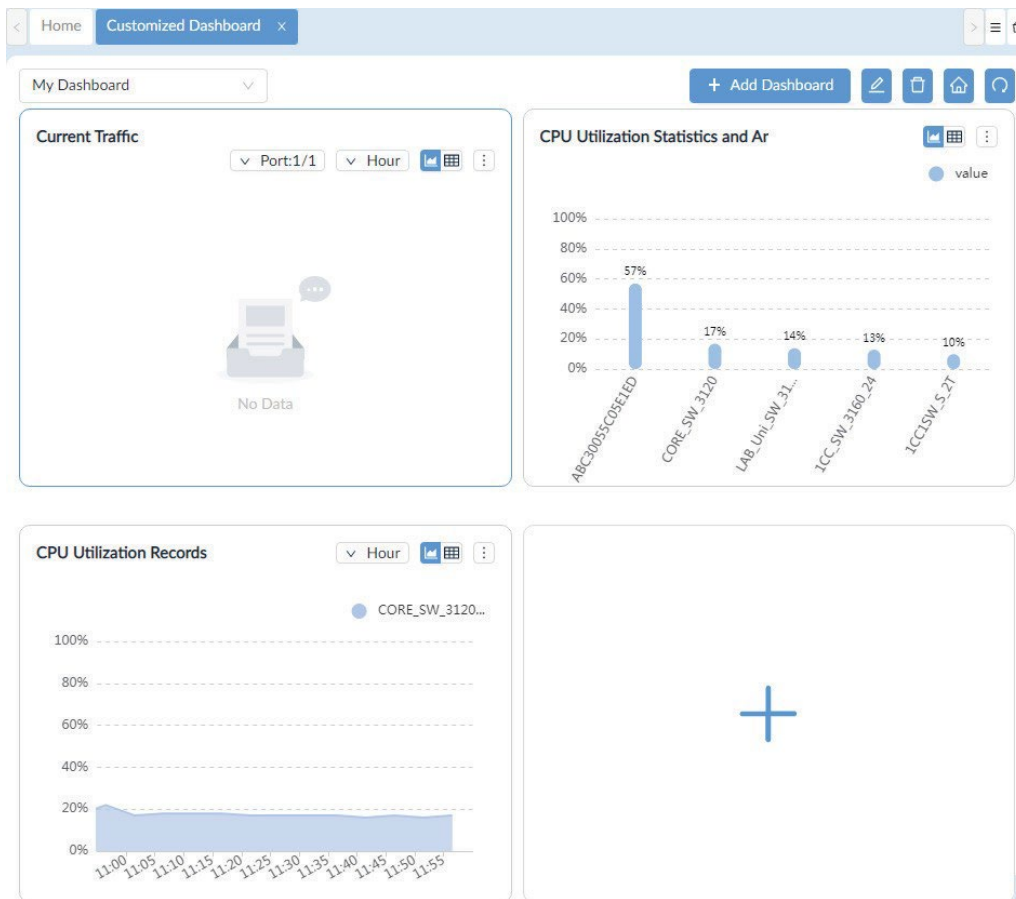


Figure 113 Creating a Customized Dashboard

3. Click the **Add Dashboard** button.
The Add Customized Dashboard overview displays

The 'Add Customized Dashboard' dialog box contains the following fields and options:

- Name:** A text input field with the placeholder 'Enter Name'.
- Level:** Radio buttons for 'Organization' (selected), 'Site', and 'Network'.
- Range:** A dropdown menu set to 'All Devices'.
- Description:** A large text area with the placeholder 'Enter Description'.
- Sharing Status:** A toggle switch currently set to 'OFF'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

Figure 114 Adding a Customized Dashboard

4. Enter the following information:

Item	Description
Name	Enter the name for the new dashboard.
Level	Click to select the group level (default: Organization).
Organization	Add all discovered devices within the organization are selected for the group.
Site	Click the Range drop-down menu to select the devices within the designated site.
Network	Click the Range drop-down menu to select the devices within the designated network.
Description	Enter a short description to help 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 will be able to view, edit and delete it.
Save	Click Save to create the group.

5. Click **Save** to create the customized dashboard.

The customized dashboard is created. The Customized Dashboard page displays.

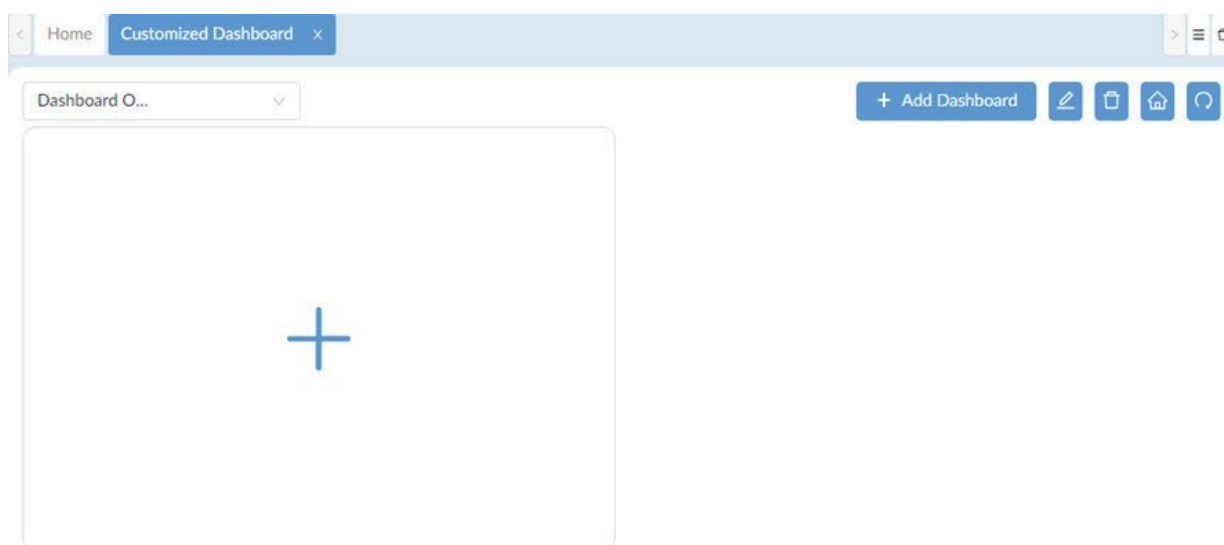


Figure 115 Overview of Customized Dashboard

6. From the dashboard, click + (Add) to add a graph widget to the dashboard.

The Add Graphics page displays.

7. In the Select device step, click to select a listed device(s) for the source data. Alternatively, use the Search field to specify a device(s). Available fields are:

- System Name
- IP
- Model Name
- Device Category
- Network Name

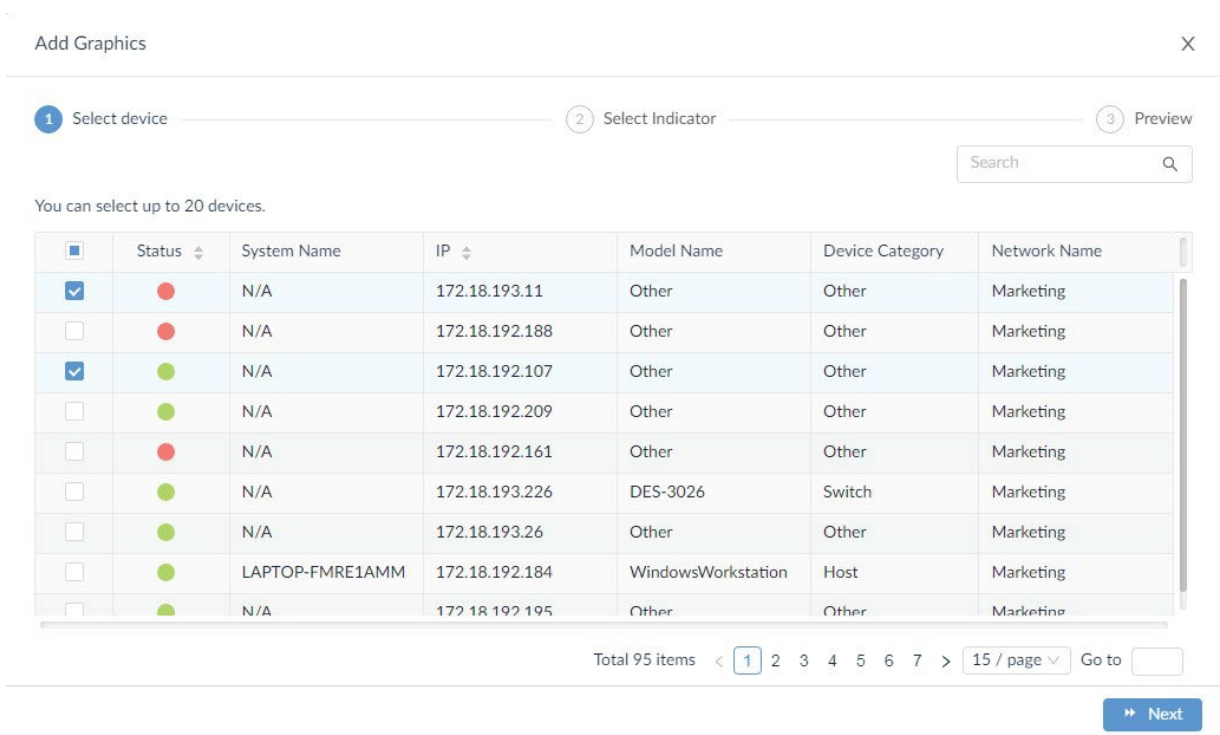


Figure 116 Selecting Device Source

8. Click **Next** to continue.

The Select Indicator page displays.

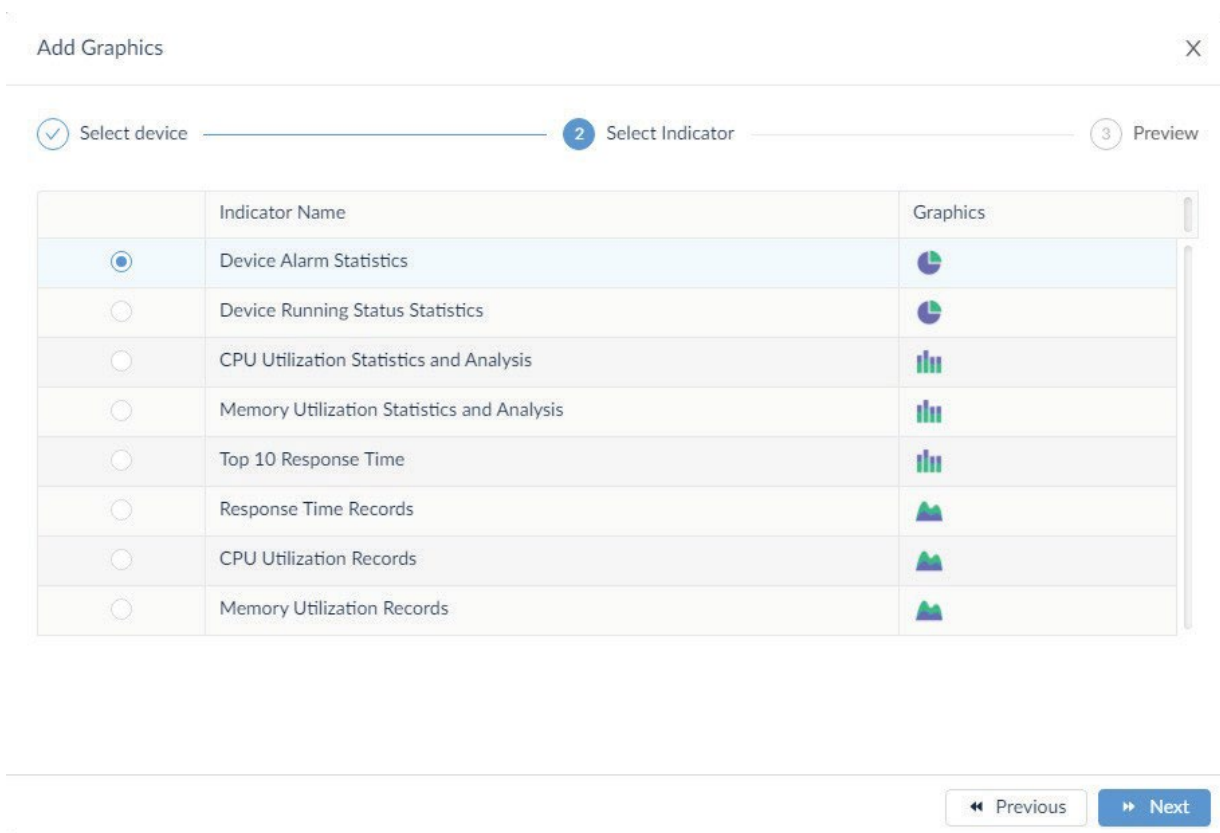


Figure 117 Selecting Graphical Indicators

9. Click on an indicator to define the widget category. Available categories are dependent on the supported device functions. See the following for further information.

<ul style="list-style-type: none"> • Device Alarm Statistics • Device Running Status Statistics • CPU Utilization Statistics and Analysis • Memory Utilization Statistics and Analysis • Top 10 Response Time • Response Time Records • CPU Utilization Records • Memory Utilization Records • Wireless Throughput (Bytes) • Total Bytes Transmitted • Total Packets Transmitted • Current Traffic • Packets Per Second 	<ul style="list-style-type: none"> • 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.

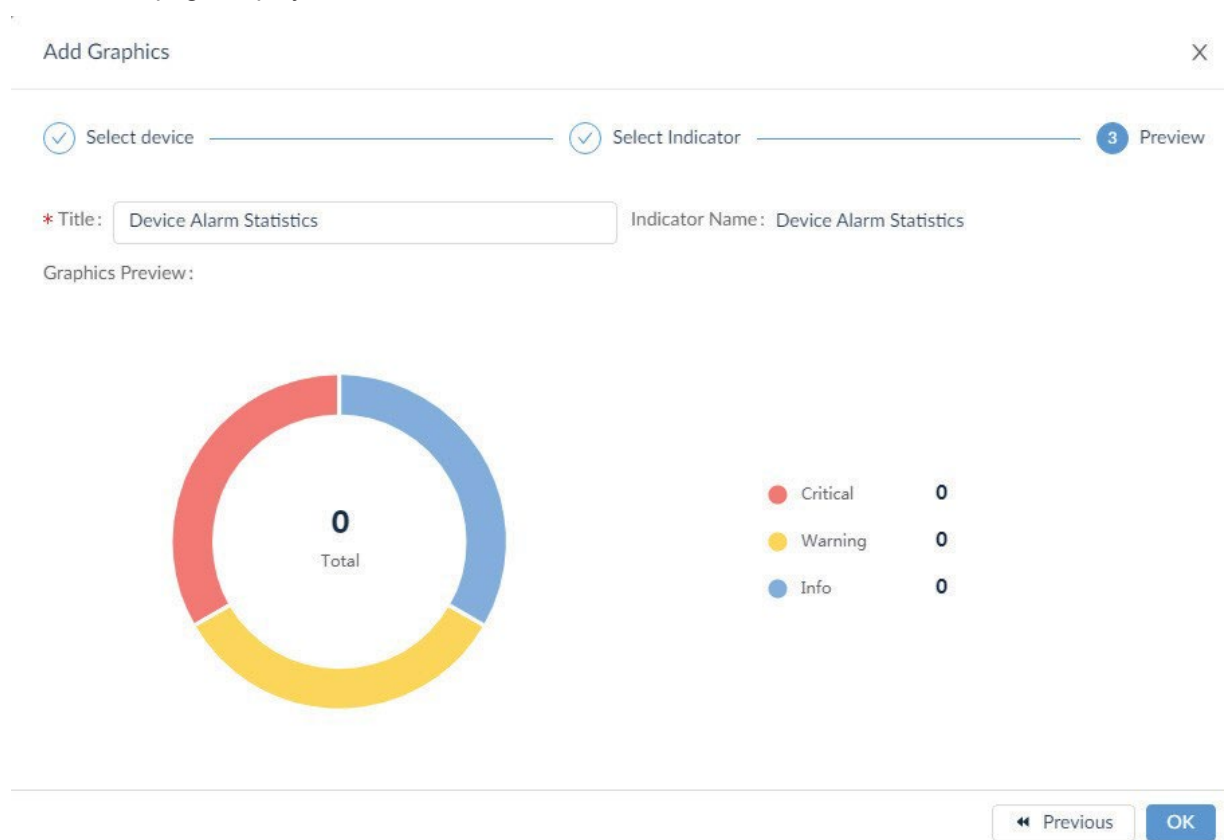


Figure 118 Overview of Preview Page

1. Click **OK** to create the new widget. Click **Previous** to return to the previous menu.

5.7.2. Modify a Customized Dashboard

To modify a customized dashboard:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. From the Dashboard, click Customized Dashboard.
The **Customized Dashboard** page displays.

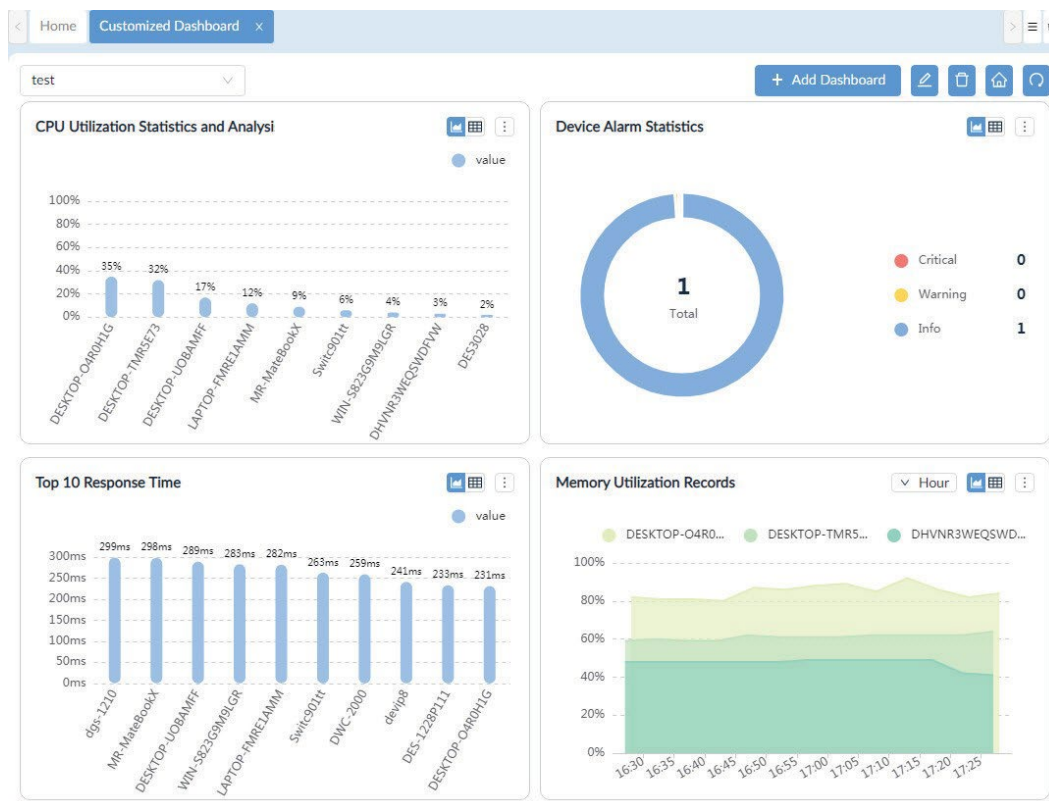


Figure 119 Customized Dashboard Overview

For demonstration purposes, the CPU Utilization Statistics and Analysis widget is used.

- Click on the Settings button. Available options are dependent on the widget function.

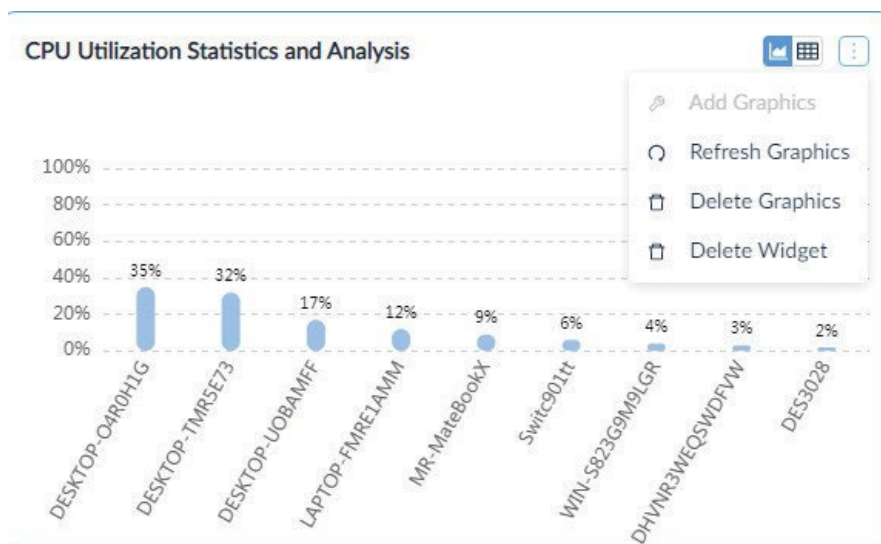


Figure 120 Settings Overview

- Click to perform an action:
 - Refresh Graphics: re-sync the function information.
 - Delete Graphics: remove the graphic from the widget frame.
 - Add Graphic: when the graphic is deleted, add a new monitor function.
 - Delete Widget: remove the widget from the dashboard.
 - Reselect Devices: specify a different device(s).

The widget is updated.

5.8. View and Export Logs

The D-View 8 auditing function provides the method to view information regarding the initiated tasks on the network.

The following reports are available:

- General Reports
- Scheduled Reports
- My Reports

The logs are saved according to the scheduled retention period.

To view and export reported logs:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Select the report criteria from the General Reports column.

Report Category	Category	Event
General Reports	Device Reports	Device Health
		Trap
		Syslog
		Device Top N
	Wired Interface Reports	Wired Traffic
		Wired Top N
	Wireless Reports	Wireless Client Count
		Wireless Traffic
Advanced Reports	Inventory	
Scheduled Reports	One Time	
	Recurrent	
My Reports	My Reports	

3. From Reports, click **General Reports**.
The default Device Health Reports page displays.

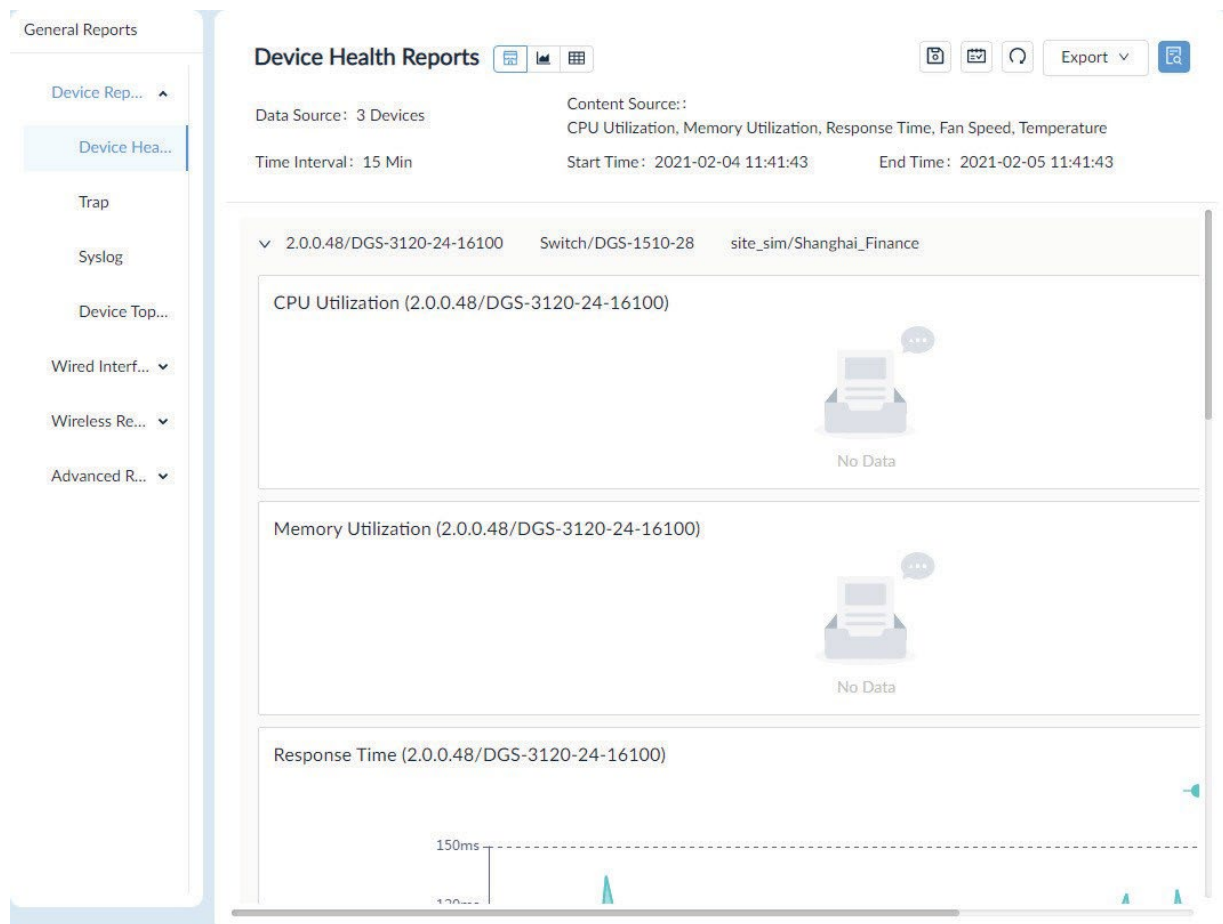


Figure 121 Device Health Report Overview

The report parameters may not be configured. You will need to configure the settings if a report does not display any data.

4. Click the Export drop-down menu and select the type of file format to use: PDF, Excel, CSV. The report file is downloaded to the local drive.

5.9. View Report Settings

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. From Reports, click **General Reports**.
The default **Device Health Reports** page displays

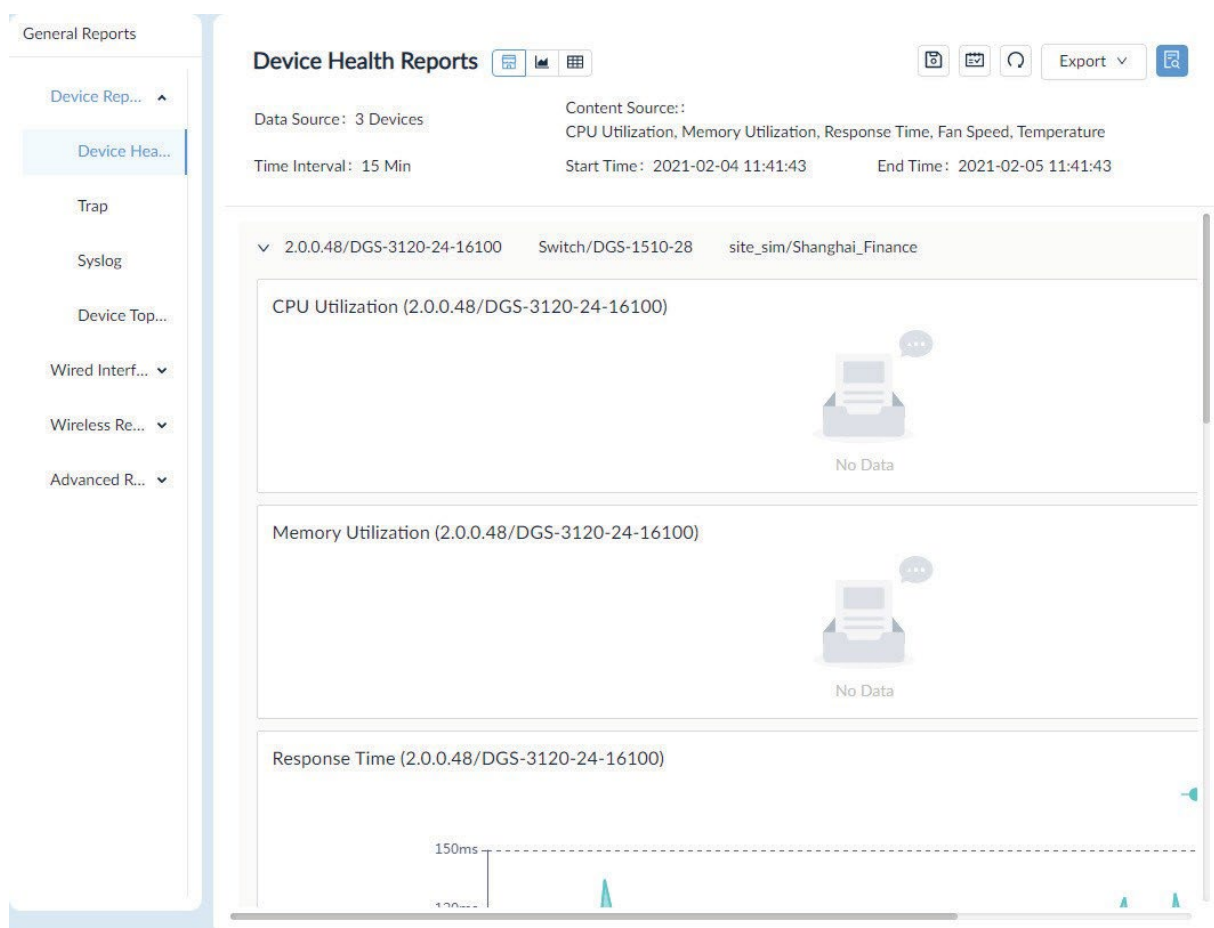


Figure 122 Device Health Report Overview

The toolbar displays available functions:

Item	Description
Show All	Displays all information.
Show Chart Only	Displays available information in a chart format.
Show Table Only	Displays available information in a table format.
Save to My Reports	Designates the current report as a My Report category.
Upgrade to Scheduled Reports	Designates the current report as a Scheduled category.
Refresh	Re-synchronizes the report information.
Export	Saves the information to a file.
Report Settings	Configure the settings for the current report category.

3. Click **Report Settings**. The **Report Settings** page displays.

* Select Devices: All Selected Selected count: 5

<input type="checkbox"/>	Status	System Name	IP	Model Name	Site	Network
<input checked="" type="checkbox"/>	●	DGS-3120-24-16100	2.0.0.48	DGS-1510-28	site_sim	Shanghai_...
<input checked="" type="checkbox"/>	●	DGS-3120-24-16100	2.0.0.12	DWS-3160-24TC	site_sim	Shanghai_...
<input checked="" type="checkbox"/>	●	DGS-3120-24-16100	2.0.0.75	DGS-1520-28	site_sim	Shanghai_...
<input checked="" type="checkbox"/>	●	DGS-3120-24-16100	2.0.0.64	DGS-3630-52PC	site_sim	Shanghai_...
<input checked="" type="checkbox"/>	●	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

Figure 123 Report Settings Overview

Available report settings available functions:

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 criteria and click Enter to search for the correlating device.
Content Source	Click the a log event to include in the report setting: CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature
Time Interval	Click to set the interval time to define the report period. Settings: Configured minimum interval, 15 min., 2 Hour, 8 Hour, 1 Day.
Duration	Click to select the start and stop duration of the report. Settings: Last 24 Hours, Today, Yesterday, Customized (select start and stop date:hour).
Reset	Click to re-sync the report settings to the default settings.
Save	Click Save to create the group.

5.10. View Firmware Version

You can view the firmware version for all discovered D-Link switches, wireless, wired, and PoE devices.

To view the firmware version:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. From Configuration, click **Firmware Management**. The default **Firmware Management** page displays.

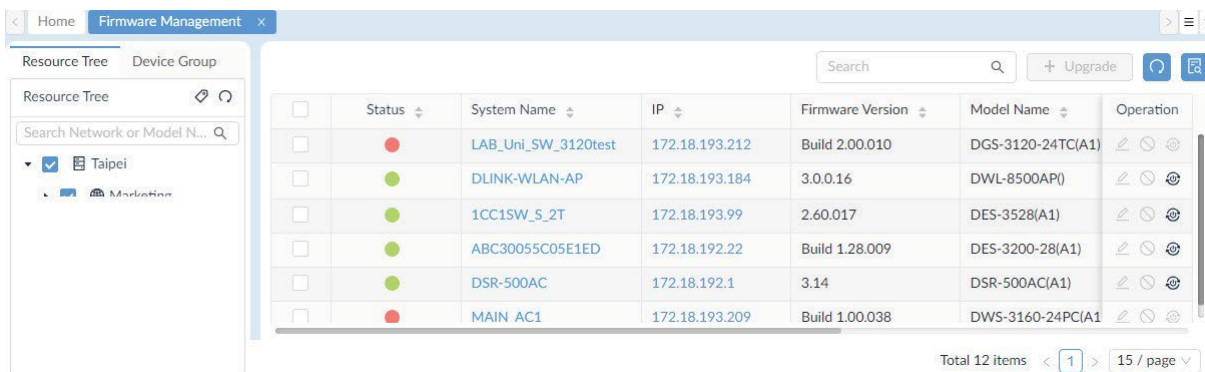


Figure 124 Firmware Management Overview

3. Select the device(s) to update by clicking on the check box.



NOTE: If multiple devices are selected, they must be of the same model for the firmware to correctly update.

4. Click **Upgrade** to display Firmware Upgrade page.
5. From Firmware File, click **Select Firmware File** to view available firmware sources.



NOTE: Make sure to confirm the firmware version and its compatibility with the device before proceeding.

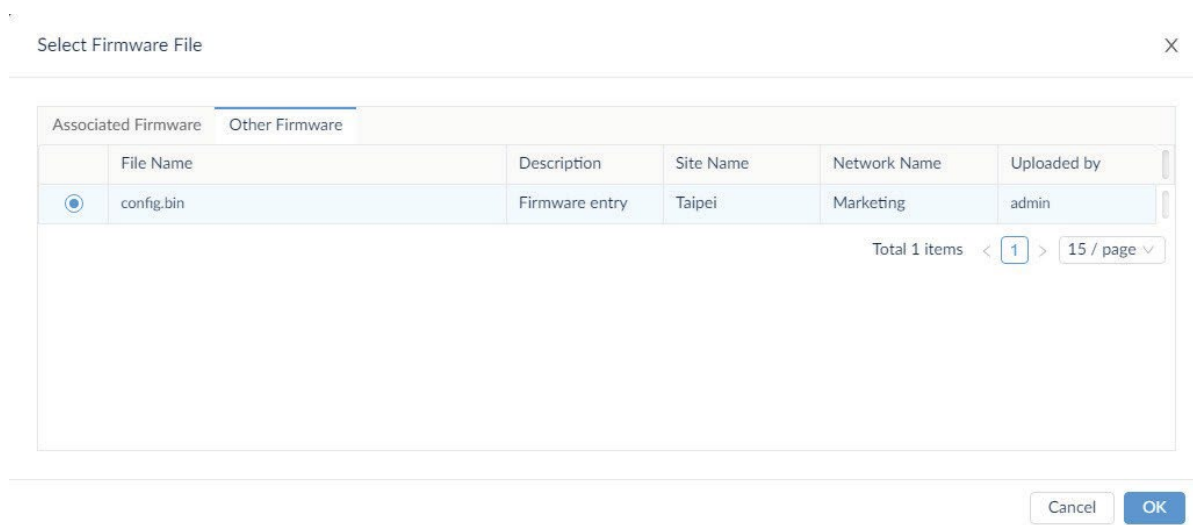


Figure 125 Selecting a Firmware File

6. In Other Firmware, select the appropriate file and click **OK** to continue.
7. Alternatively, the following option is available.
 - a. Select the Associate Firmware tab to view the associated firmware file entries.

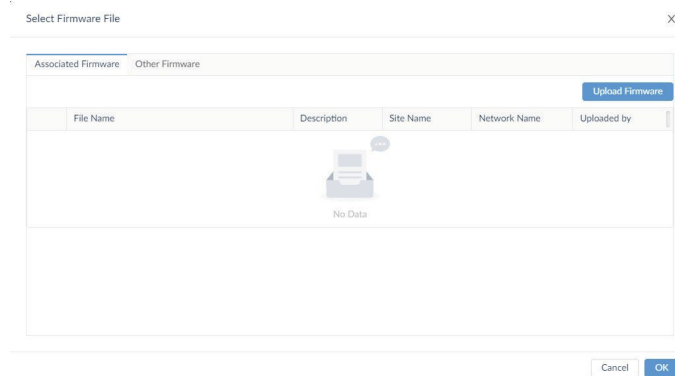


Figure 126 Associated Firmware Selection

- b. Click **Upload Firmware** to view the Upload Firmware page and select a specific source.

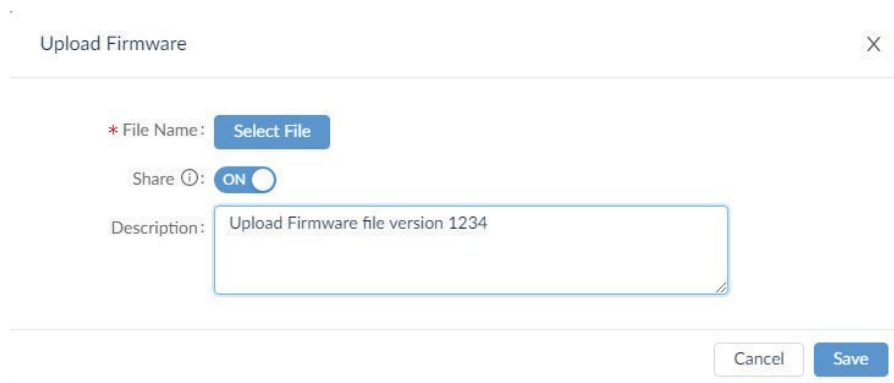


Figure 127 Uploading an Associated Firmware File

- c. Click **Select File** to browse the file location and select the firmware.
 - d. Click **Open** to select the file.
 - e. Click the Share slide bar to disable sharing with other networks.
 - f. Enter a brief description to better identify the file type.
 - g. Click **Save** to upload the file selection or **Cancel** to delete the upload.
8. From the Firmware Upgrade page, locate Schedule Information to set the Schedule:
 - Schedule Type: One Time
 - Execution Time:
 - Immediately: start the firmware updating once the task is saved.
 - Specify a Date: click the Date drop-down menu to select Now or Date and Time. Click **OK** to set the date.
 9. From Reboot Type, click Reboot by D-View 8 to enable a reboot through the application. By default, the Reboot by D-View 8 option is disabled. A reboot is typically 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 notification functions when tasks are completed or triggered. As an example, if a Trap job is completed, the application generates a notification describing the event and related details.

To view notifications:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.

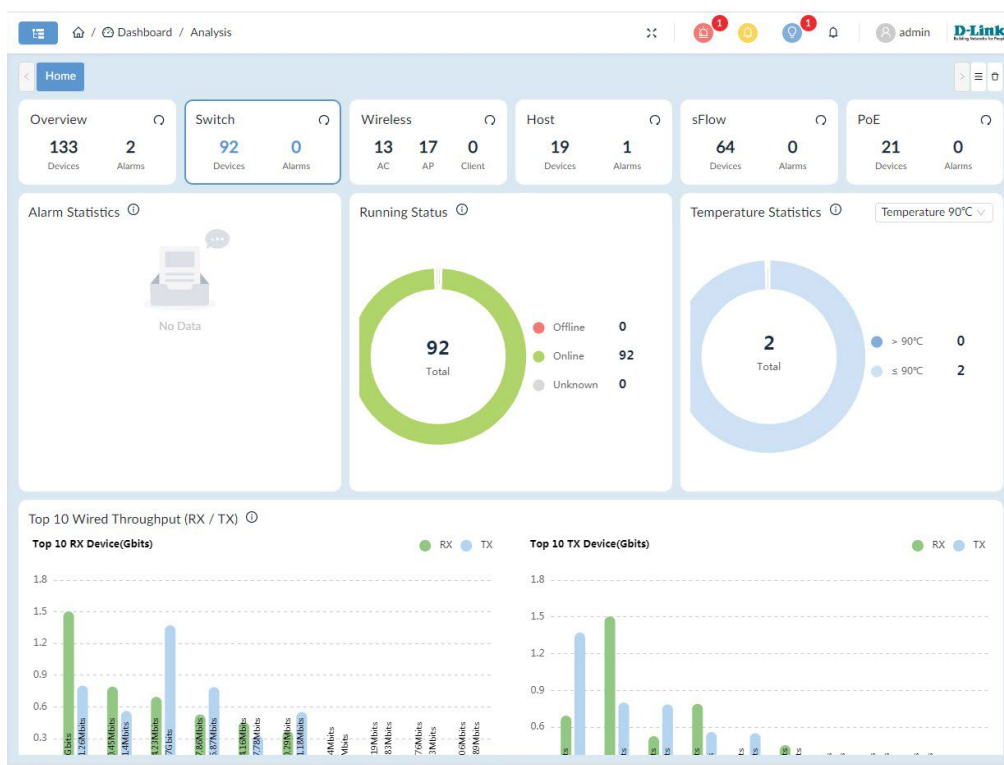


Figure 128 Notification Function Dashboard

- In the right side of the toolbar, click the Notification button . The Notification pop up page displays.

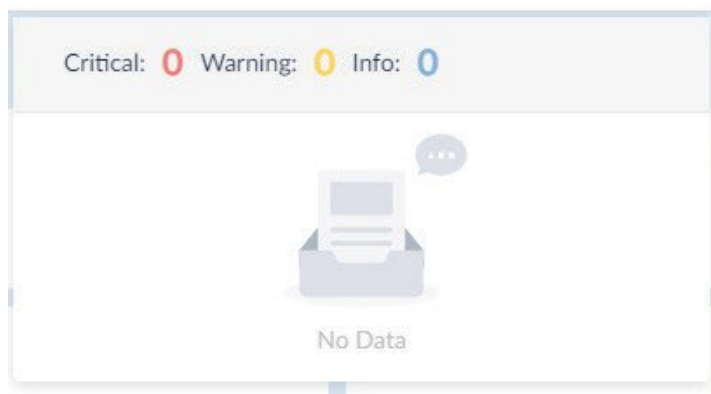


Figure 129 Toolbar Notification Overview

Alternatively, you can view the notifications from the Notification Center.

- From Alarm & Notification, click **Notification Center**. The Notification Center page displays.

<input type="checkbox"/>	Name	ON / OFF	Devices	Trigger Conditions	Notification Method	Receiving Administrator	De	Operation
<input type="checkbox"/>	Notification Job	<input checked="" type="checkbox"/>	2	Monitor	APP notification push	2	Job	
<input type="checkbox"/>	Notification Sample	<input checked="" type="checkbox"/>	4	Trap	Web scrolling notify	1	Sar	
<input type="checkbox"/>	Notification Rule	<input checked="" type="checkbox"/>	1	Monitor	Web scrolling notify, E...	2	Rul	

Total 3 items < 1 > 100 / page

Figure 130 Alarm Notification Overview

This page is intentionally left blank.

6 Manage Configuration and Firmware Settings

The D-View 8 makes it easy to backup and restore device configurations. In addition, you can upgrade the firmware on discovered devices.

The following sections are covered:

- Creating Configuration
- Managing Tasks
- Upgrading Firmware
- Backing up device configurations
- Restoring device configurations
- Importing Configuration and Firmware Files to a Network

6.1. Creating Configuration and Profiles

You can create specific configurations for discovered devices on the network. You can create quick or advanced configuration tasks for batch operations.

6.1.1. Add a Configuration Task

1. Open a browser and enter the IP address of the D-View 8 server in the address bar. A login page displays.
2. Click the drop-down menu and select the user type designated to the user.
3. Enter the user name and password in the fields.
4. Click the **Sign In** button. The Dashboard overview displays.
5. In Configuration, click the **Batch Configuration**. The Batch Configuration page displays.

The screenshot shows the 'Batch Configuration' page. On the left is a 'Configuration Category' sidebar with a search bar and a list of categories including AAA Status, DHCP Status, HTTPS Web Access Status, LLDP Status, RMON Status, SNMP / NTP Status, SSH Status, Safeguard Engine Status, Spanning Tree Status, Telnet Status, and Web Access Status. The main content area has a 'Task Information' section with 'Task Name' and 'Task Description' fields. Below that is 'Configuration Information' with 'Category: AAA Status' and 'Description: Configure the AAA status of devices.' and a toggle for 'AAA Status'. The 'Target Devices' section is a table with columns: Status, System Name, IP, Device Category, Model Name, Site, Network, and Operation. The table is empty with a 'No Data' message and a '+ Add' button. At the bottom is a 'Schedule' section with 'Schedule Type' options: One Time (selected) and Recurrent.

Figure 131 Batch Configuration Overview

6. From the Configuration Category select a category or enter specific criteria in the search frame.
7. Enter the task criteria to define the task. See the following information.

Item	Description
Add Task	Click to create the defined task.
Refresh	Click to re-sync the task form.
Task Management	Click to open the Task Management page.
Configuration Template	Click to open the Configuration Template page.
Task Information	
Task Name	Enter the name to define the task.
Task Description	Enter descriptive information to easily identify the task.
Configuration Information	
Category	Select the task category to set as defined in the following.
AAA Status	Select to set the Authentication, Authorization, and Accounting configuration 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
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
Web Access Status	Select to set the Web Access Status configuration task
Target Devices	
Add	Click to add the device(s) for inclusion in the configuration.
Schedule	
Schedule Type	Click to define the frequency period of the task, a single event or recurring task.
Execution Time	Click to define the period of task execution, immediately or specify a time and date.

- Once the criteria are defined, click Add Task to set the configuration. The task is saved successfully and appears under the Task Management menu.

6.1.2. Add a Configuration Profile

When you assign a profile to a device, you can configure specific device parameters. You can configure and manage profiles by using the Batch Configuration function.

Configuration profiles are designed to support rapid network deployment. Once a profile is defined, you can apply it to multiple devices in the network.

- Open a browser and enter the IP address of the D-View 8 server in the address bar. A login page displays.
- Click the drop-down menu and select the user type designated to the user.
- Enter the user name and password in the fields.
- Click the **Sign In** button. The Dashboard overview displays.
- In Configuration, click the **Batch Configuration**.
- From the menu tabs, select **Advanced Configuration**. The Advanced Configuration page displays.

<input type="checkbox"/>	Profile Name	Model Name	Related Tasks	Related Devices	Site	Network	Update Time	De	Operation
<input type="checkbox"/>	Configure Profile LACP	DGS-1210-24(A1)	0	1	CS	Beijing_Marketing	2021-02-06 13:51:44	De	✎ 🔄 + 🗑️
<input type="checkbox"/>	Switch Profile2	DES-3028(A1)	0	1	CS	Beijing_Marketing	2020-12-17 13:51:46		✎ 🔄 + 🗑️
<input type="checkbox"/>	Switch Profile	DGS-3120-24TC(A1)	0	2	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	✎ 🔄 + 🗑️

Total 3 items: < 1 > 100 / page

Figure 132 Advanced Configuration Overview

7. Click **Add Profile** to display the **Add Profile** page.

Add Profile

1 Profile Information

* Profile Name: * Device Hierarchy:

Profile Description:

* Configuration Feature:

<input type="checkbox"/>	Configuration Category	Description
<input type="checkbox"/>	AAA Status	
<input type="checkbox"/>	DHCP Status	
<input checked="" type="checkbox"/>	Telnet Status	
<input type="checkbox"/>	Syslog Status	
<input type="checkbox"/>	Spanning Tree Status	
<input type="checkbox"/>	SSH Status	
<input type="checkbox"/>	SNTP / NTP Status	
<input type="checkbox"/>	LLDP Status	
<input type="checkbox"/>	LACP	
<input type="checkbox"/>	Web Access Status	
<input type="checkbox"/>	Port Security	
<input type="checkbox"/>	MAC Notification	
<input type="checkbox"/>	802.1V Protocol VLAN	
<input type="checkbox"/>	Voice VLAN	
<input type="checkbox"/>	Loopback Detection	
<input type="checkbox"/>	MAC VLAN	

2 Configuration Feature

Next

Figure 133 Add Profile Overview

8. Enter the information to define the profile:

Profile Name	Enter the name to define the profile.
Device Hierarchy	Click the drop-down menu to select a hierarchy. The hierarchy represents the network's geographical locations. A network hierarchy has a predetermined hierarchy, see the following example: <ul style="list-style-type: none"> • Areas or Sites • Buildings • Floors
Profile Description	Enter descriptive information to easily identify the profile.

Profile Name	Enter the name to define the profile.	
Configuration Feature	Select the category-specific parameters for the profile <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Voice VLAN • Loopback Detection • MAC VLAN • RADIUS • DHCP Server Screening • TACACS+ • STP Settings • UDP Helper • VLAN Interface • Green • System Log Settings • Time and SNTP • sFlow • Safeguard Engine Status • 802.1Q VLAN
Next	Click Next to continue and configure the selected category feature.	

- Click **Next** to continue and define the selected feature. In the following figure the Telnet Status feature displays.
- Click **Save** after configuring the feature. Click Previous to return to the previous screen. The Configuration Profile is defined and appears in the Advanced Configuration list.

6.1.3. Modify and Delete a Configuration Profile

When you assign a profile to a device, you can configure specific device parameters. You can configure and manage profiles by using the Batch Configuration function.

Configuration profiles are designed to support rapid network deployment. Once a profile is defined, you can apply it to multiple devices in the network.

- Open a browser and enter the IP address of the D-View 8 server in the address bar. A login page displays.
- Click the drop-down menu and select the user type designated to the user, and enter the user name and password in the fields.
- Click the **Sign In** button. The Dashboard overview displays.
- In Configuration, click the **Batch Configuration**.
- From the menu tabs, select **Advanced Configuration**. The Advanced Configuration page displays. Any defined configuration profiles are listed.

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

Figure 134 Advanced Configuration Overview

- From the Operation column on the right, click on an icon to perform the following action:

Item	Description
Edit	Modify the configuration profile settings.
Share	Copy the profile to configure similar devices on the network.
Create Task	Create a specific task for the profile.
Delete	Remove the profile from the listing.

Editing a Profile

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Batch Configuration**.
3. From the menu tabs, select **Advanced Configuration**.
The Advanced Configuration page displays.
4. From the Operation column on the right, click **Edit** to modify the selected task profile.

Devices	Site	Network	Update Time	De	Operation
	CS	Beijing_Marketing	2021-02-06 13:51:44	De	
	CS	Beijing_Marketing	2020-12-17 13:51:46		
	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	

Figure 135 Selecting Task Profile Edit

The Edit Profile page displays.

Edit Profile
X

1 Profile Information
2 Configuration Feature List

* Profile Name: Site: Taipei

Network: Marketing Model Name: DGS-3120-24TC(A1)

Profile Description:

* Configuration Feature List:

	Configuration Category	Description
<input type="checkbox"/>	sFlow	
<input type="checkbox"/>	LACP	
<input checked="" type="checkbox"/>	SNTP / NTP Status	
<input type="checkbox"/>	Web Access Status	
<input type="checkbox"/>	Telnet Status	
<input type="checkbox"/>	Trap Status	
<input type="checkbox"/>	Safeguard Engine Status	
<input type="checkbox"/>	802.1Q VLAN	
<input type="checkbox"/>	Syslog Status	
<input checked="" type="checkbox"/>	Spanning Tree Status	
<input type="checkbox"/>	LLDP Status	
<input type="checkbox"/>	SSH Status	
<input type="checkbox"/>	ACL	

Figure 136 Editing a Task Profile

5. Enter the profile information to modify and select the configuration feature list to include or exclude.
6. Click **Next** to continue the modification.

The Configuration Feature List page displays. All the selected features corresponding to the task are listed in the left column.

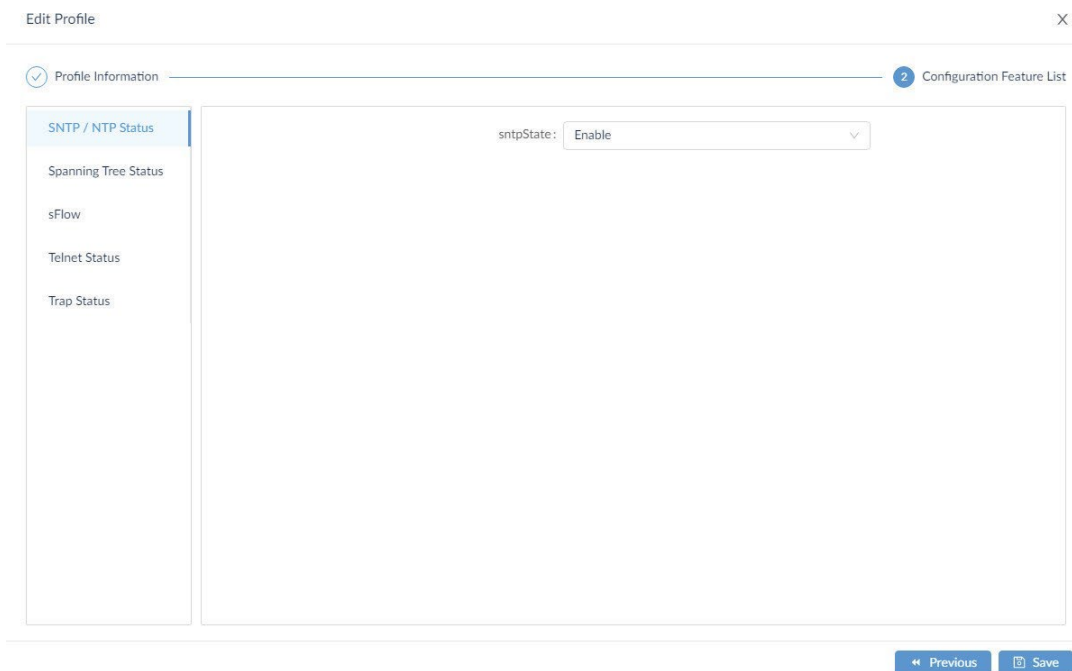


Figure 137 Editing Configuration Features

7. Select a feature from the left column to view the settings.
8. Once the new setting is modified, click **Save** to finalize the task profile. Alternatively, click **Previous** to return to the previous menu.

Sharing a Profile

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Batch Configuration**.
3. From the menu tabs, select **Advanced Configuration**.
The Advanced Configuration page displays.
4. From the Operation column on the right, click **Share** to include additional devices in the task.
Profiles are only applicable to the specific designated model in the designated network. If a user has devices of the same model in other networks, the devices can be similarly configured through the use of the Sharing Profile function.

Devices	Site	Network	Update Time	De	Operation
	CS	Beijing_Marketing	2021-02-06 13:51:44	De	
	CS	Beijing_Marketing	2020-12-17 13:51:46		
	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	

Figure 138 Selecting Task Profile Share

The Share Profile page displays. See the following figure.

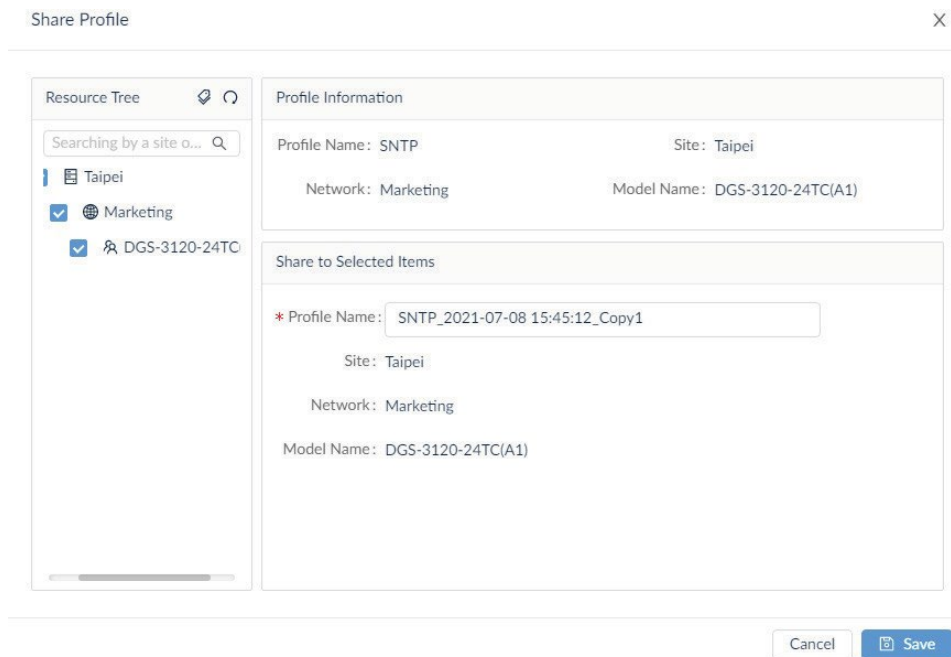


Figure 139 Sharing a Task Profile

- From the Resource Tree column, select the location and available device models to share the profile. The selected device displays in the Share to Selected Items pane.
- Click **Save** to accept the modification.

Applying a Profile to Devices (Task)

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- In Configuration, click the **Batch Configuration**.
- From the menu tabs, select **Advanced Configuration**. The Advanced Configuration page displays.
- From the Operation column on the right, click **Create Task** to apply the profile to devices by creating a task.

Devices	Site	Network	Update Time	De	Operation
	CS	Beijing_Marketing	2021-02-06 13:51:44	De	✎ 📄 + 🗑
	CS	Beijing_Marketing	2020-12-17 13:51:46		✎ 📄 + 🗑
	CS	Beijing_Marketing	2020-12-17 13:51:15	Sw	✎ 📄 + 🗑

Figure 140 Selecting Create Task Profile Edit

The Task Setting page displays. See the following figure.

Figure 141 Creating a Task Profile

5. Enter the information under Task Information to define the task identifiers.
6. To include additional devices to the task, Click **Add** to open the Batch Select Devices screen.
7. Click the target device(s). Alternatively, use the **Search** function to locate specific devices by model name or IP address. Click **OK** to return to the previous menu.
8. From the Task Settings page, click **Save** to create the new task and return to the previous menu.

Deleting a Profile

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Batch Configuration**.
3. From the menu tabs, select **Advanced Configuration**.
The Advanced Configuration page displays.
4. From the Operation column on the right, click **Delete** to remove the profile.
5. A prompt displays, click **Yes** to delete the task or **No** to cancel the function.

Figure 142 Deleting a Task Profile

6.2. Managing Tasks

The Task Management function lets you manage current and previously defined tasks. Tasks initiated on the platform can be edited, deleted, restarted, and view the task record.

6.2.1. Viewing Current Tasks

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click **Task Management**. The Task Management page displays.
3. By default, Current Tasks display. The current tasks are listed as seen in the following figure.

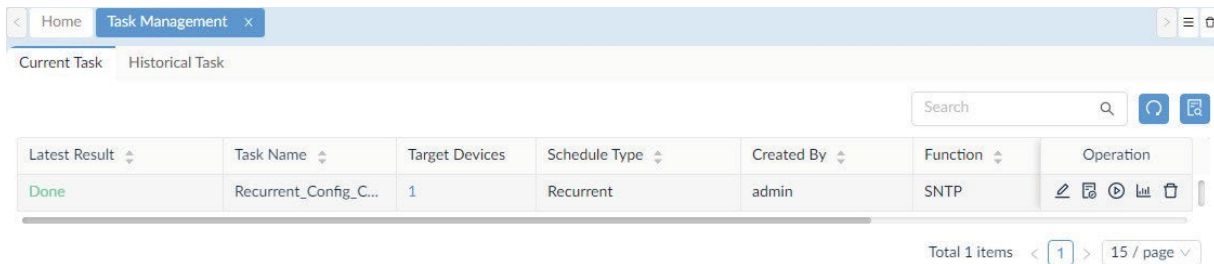


Figure 143 Task Management Menu

Item	Description
Latest Results	Displays the result status of the task: Partially done, Done.
Task Name	Displays the defined name of the task.
Target Devices	Displays the number of devices assigned to the device.
Created By	Displays the name of the task creator.
Function	Displays the functions 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 corresponding configuration file.
Edit Task	Click to modify the task settings.
Restart Task	Click to activate the task.
Show Task Record	Click to display the recorded events of the task, listed in chronological order.
Delete Task	Click to delete the task.

6.2.1.1. Edit Configuration

For further information see the following “Editing a Profile” on page 101.

6.2.1.2. Edit Tasks

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default the Current Task tab displays. Click Historical Task to view the Historical list.
3. From the Operations column, select **Edit Task**.

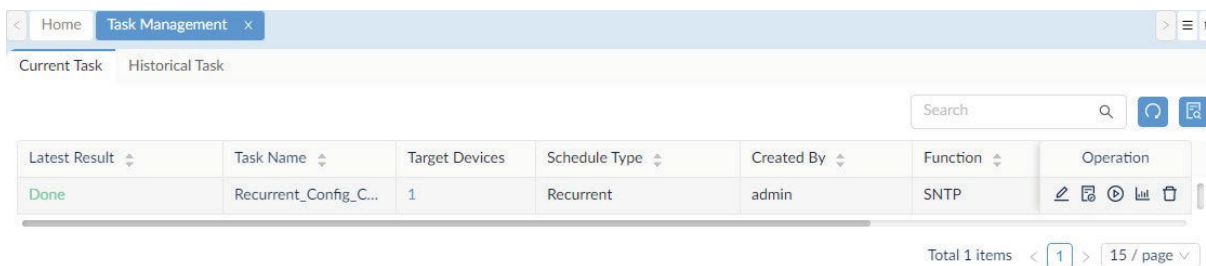


Figure 144 Selecting Edit a Task

The Task Settings page displays.

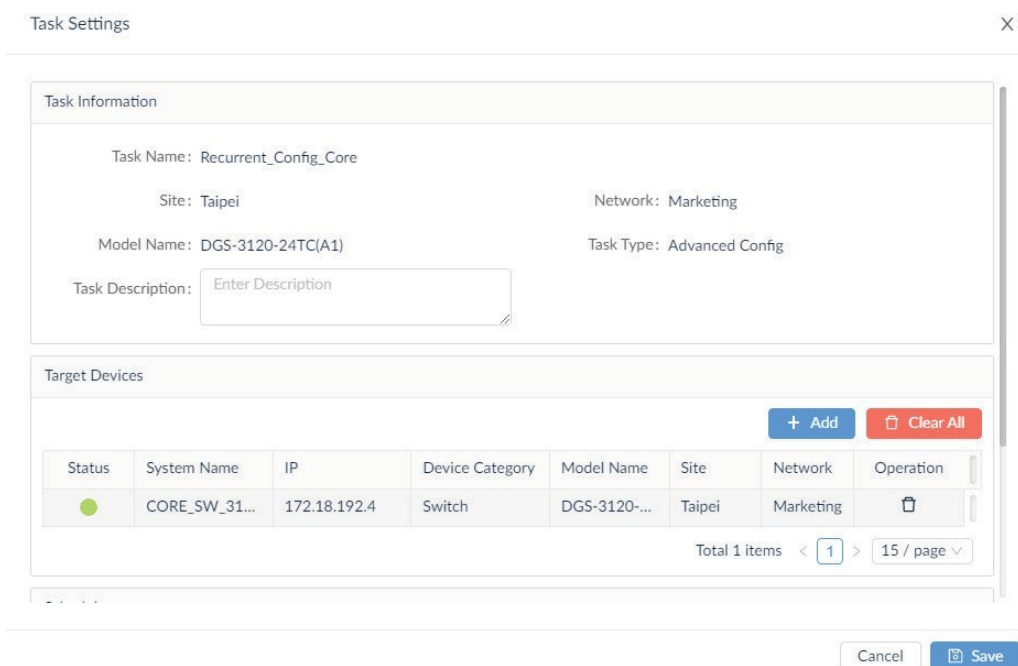


Figure 145 Editing a Task

The Task Settings page allows for the editing of an existing task. The task information as well as target devices can be modified.

4. Click **Save** to modify the task. Click **Cancel** to return to the previous page.

6.2.1.3. Restart Task

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default the Current Task tab displays. Click Historical Task to view the Historical list.
3. From the Operations column, click **Restart Task**.
4. A prompt displays. Click **Yes** to restart the task or **No** to cancel the function.

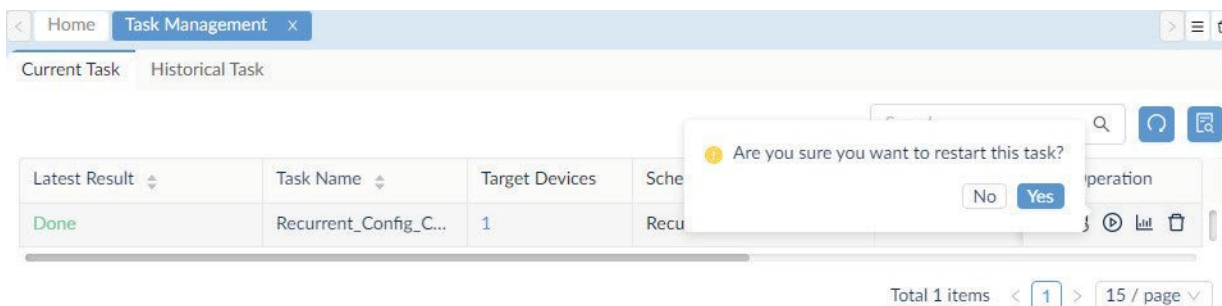


Figure 146 Restarting a Task Profile

6.2.1.4. Delete Task

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default the Current Task tab displays.
3. From the Operations column, select **Delete Task**.

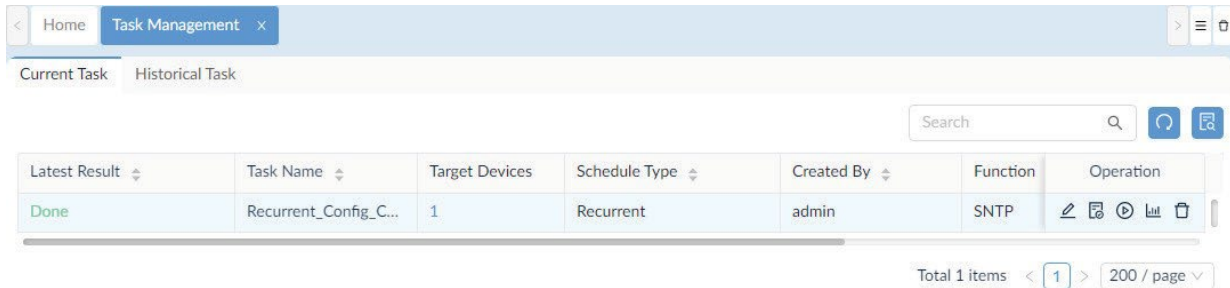


Figure 147 Selecting Delete a Task

4. A confirmation dialogue pops up. Click **Yes** to confirm the deletion or **No** to cancel.

6.2.2. Viewing Historical Tasks

6.2.2.1. Edit Configuration

For further information see the following “Editing a Profile” on page 101.

6.2.2.2. Re-execute Task

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default, the Current Task tab displays.
3. Click the Historical Task tab to view the Historical list.
4. From the Operations column, click **Re-execute Task**.

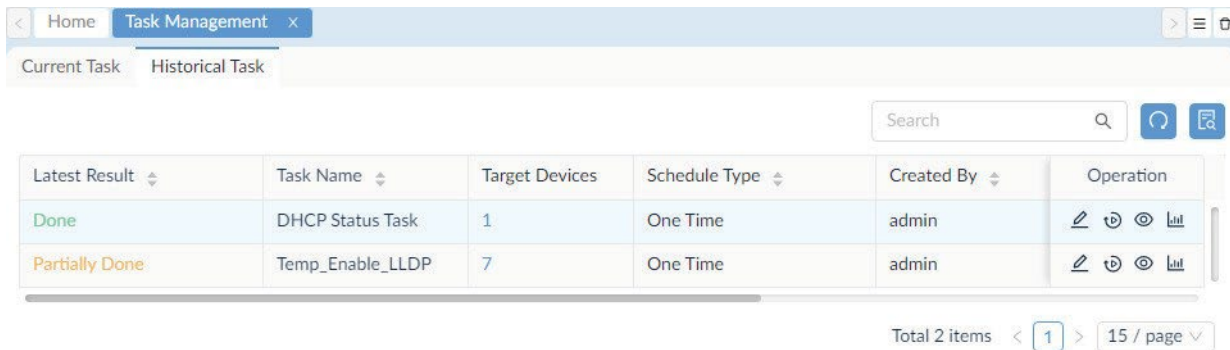


Figure 148 Selecting Re-executing a Task

The Task Settings page displays, see the following:

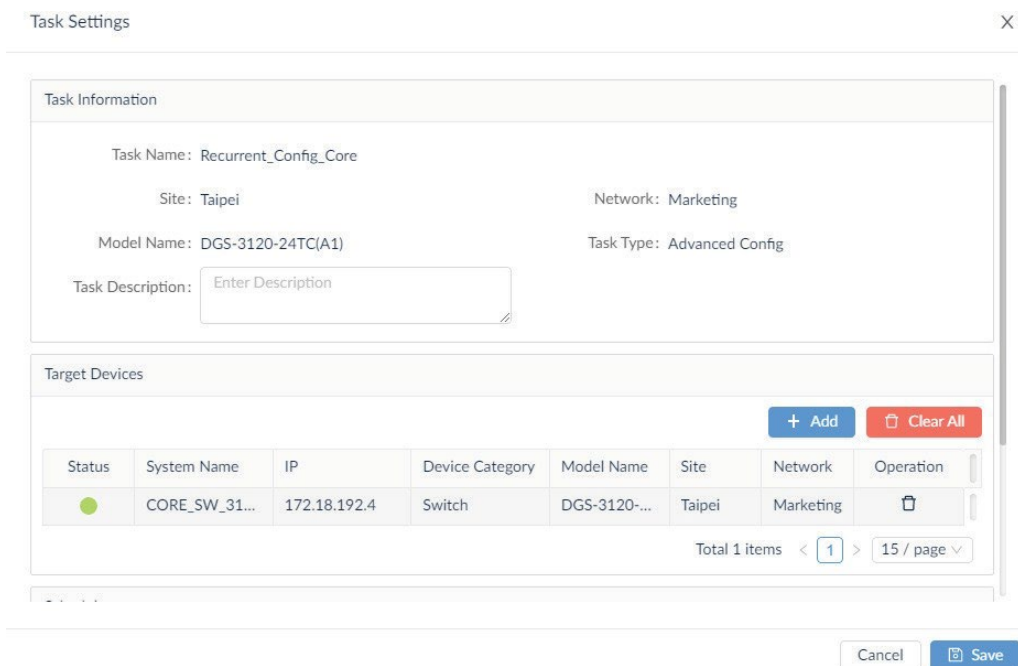


Figure 149 Editing a Task

The Task Settings page allows for the editing of an existing task. The task information as well as target devices can be modified.

5. Click **Save** to modify the task and re-execute the task.

6.2.2.3. Review Task

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default, the Current Task tab displays.
3. Click the Historical Task tab to view the Historical list.
4. From the Operations column, click **Review Task**.

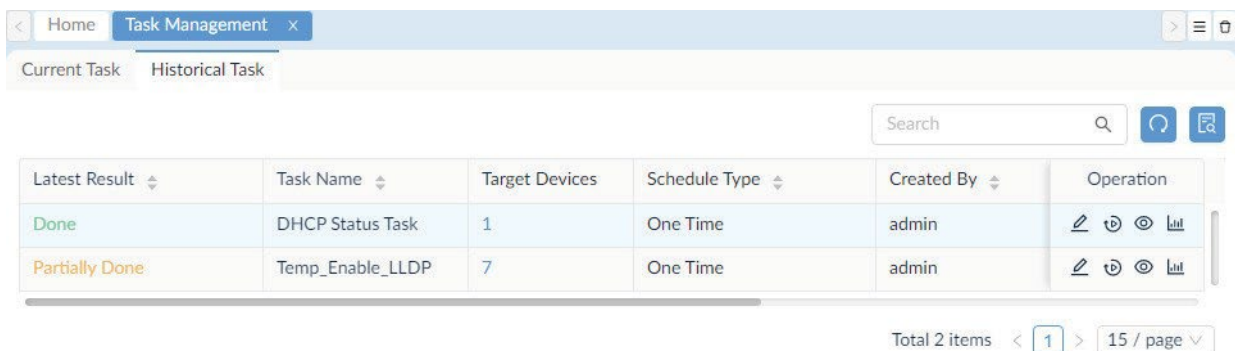


Figure 150 Selecting Review a Task

The Task Details page displays, see the following:

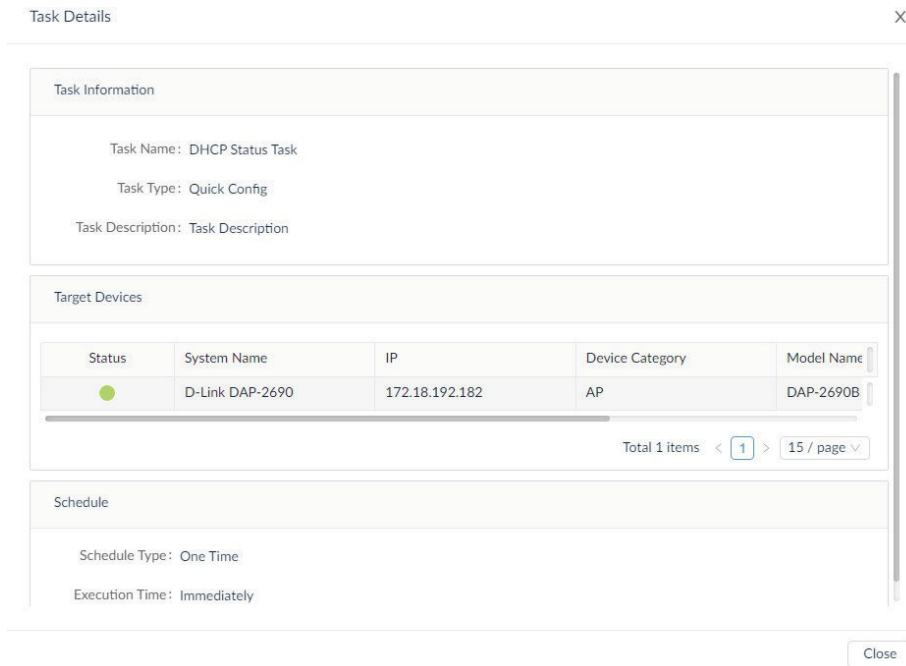


Figure 151 Reviewing a Task

The detailed settings of the task display include task name, operation user, operation time, and operation type.

5. Click **Close** to return to the previous menu.

6.2.2.4. Show Task Record

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Task Management**. By default, the Current Task tab displays.
3. Click the Historical Task tab to view the Historical list.
4. From the Operations column, click **Show Task Record**.

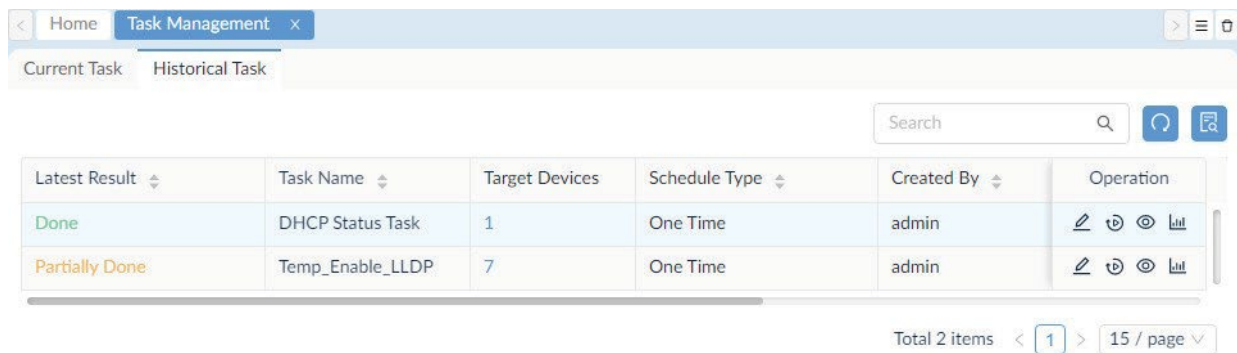


Figure 152 Selecting Show Task Record

The Task Record page displays, see the following.

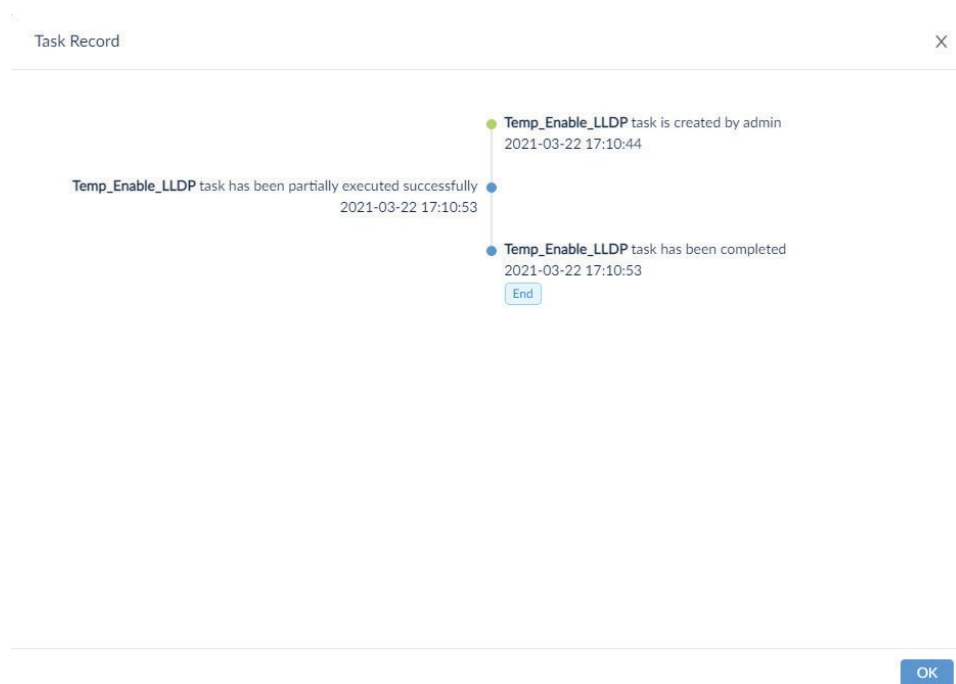


Figure 153 Viewing a Task Record

The detailed settings of the task display include task name, operation user, task operation time, and operation type.

5. Click **Close** to return to the previous menu.

6.3. Execute and Schedule a Firmware Upgrade

After creating or importing a firmware file in the File Management function, you can schedule or execute the firmware upgrade task.

To execute or schedule a firmware upgrade task:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Firmware Management**. The Firmware Management page displays.
3. From the Resource Tree column, select the site and network for the upgrade task. Alternatively, enter the key word/phrase in the Search field to locate the target network.
4. From the discovered devices, select a device from the available list.
5. Click **Upgrade** to configure the task.

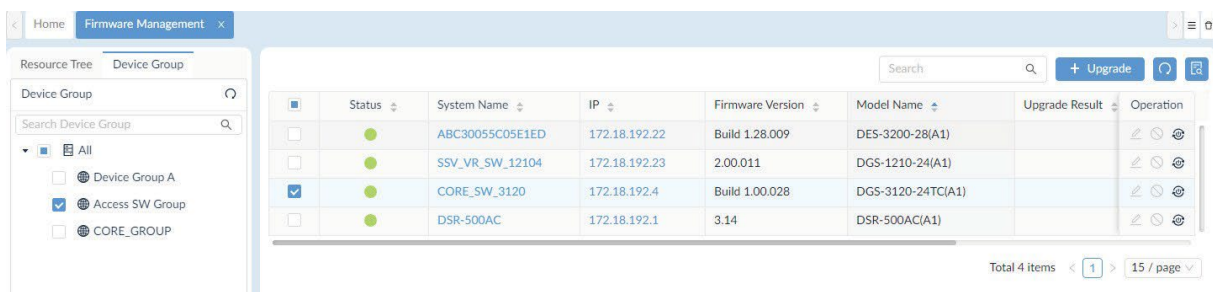


Figure 154 Configuring Upgrade Tasks

The Firmware Upgrade page displays.

6. Select a firmware file to upload to the specified device and enter additional schedule settings to define the task.

The screenshot shows the 'Firmware Upgrade' configuration interface. It includes a table for 'Selected Device' with columns for Site, Network, Model Name, Firmware File, and Operation. Below this is a 'Schedule' section with options for 'One Time' and 'Execution Time' (immediately or specify a date). The 'Reboot Type' section has a checked checkbox for 'Reboot by D-View 8'. The interface also features pagination controls and 'Cancel' and 'Save' buttons at the bottom.

Figure 155 Firmware Upgrade

The following describes the Firmware Upgrade settings.

Item	Description
Selected Device	Displays the device(s) selected for the task.
Select Firmware File	<ul style="list-style-type: none"> Click Select Firmware File to browse and select a firmware file from the local system. Enter a description for the file to easily identify the file. File size: displays the size in KB of the file. Click Delete to remove the specified device from the update task.
Schedule	
Schedule Type	The task is defined as a one time event.
Execution Time	Click to define the period to execution the task, immediately or a specific time and date.
Reboot Type	Click to enable or disable (default) the reboot function when required by the firmware update process.
Cancel	Click Cancel to return to the previous menu.
Save	Click Save to add the define configuration file.

7. Click **Save** to create the backup task. Click **Cancel** to return to the previous screen.

6.4. Backing Up Device Configurations

- The D-View 8 provides backup function to ensure configuration files are maintained and available for various requirements.

6.4.1. Add or Modify a Backup Profile

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click **Configuration Management**.
The Configuration Management page displays.
3. By default, Backup displays. Select a device or group of devices to back up the configuration.
4. Click **Backup** to configure the task.

	Status	System Name	IP	Firmware Version	Backup Result	Model Name	Site	Network	Operation
<input checked="" type="checkbox"/>	●	Switc901tt	172.18.192.22	Build 1.28.009		DES-3200-28	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	N/A	172.18.192.15	6.30.B008		DGS-1210-10	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	DWC-2000	172.18.193.98	4.7.4.2_Ax_WW		DWC-2000	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	DES3028	172.18.193.230	Build 2.00.B27		DES-3028	CS	Beijing_	⌵ ⌵
<input checked="" type="checkbox"/>	●	D-Link AP	172.18.192.20	4.3.0.2		DWL-8600AP	CS	Beijing_	⌵ ⌵
<input checked="" type="checkbox"/>	●	4911	172.18.193.49	Build 1.00.038		DWS-3160-24TC	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	dap3662	172.18.193.166	v2.01		DAP-3662	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	DES-3528	172.18.193.99	2.60.017		DES-3528	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	DLINK-WLAN-AP	172.18.193.184	3.0.0.16		DWL-8500AP	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	2126666	172.18.193.212	Build 3.10.012		DGS-3120-24TC	CS	Beijing_	⌵ ⌵
<input type="checkbox"/>	●	D-Link DAP-2690	172.18.192.182	3.16		DAP-2690B	CS	Beijing_	⌵ ⌵

Figure 156 Configuring Backup Task

The **Backup** page displays.

An existing configuration template can be used to compare a device's configuration settings. If the template and existing configuration settings are different an alarm is triggered.

To compare configuration settings:

5. Click Compare with specified file to enable the comparison function.
6. Under Alarm Level, select the specific alarm criteria threshold: Critical, Warning, or Info.
7. Select **Restore device if different** to enable the application to restore the configuration template when the device's current settings show a disparity. A configuration template must be selected.
8. Under a selected device, click the **Select File** drop-down menu and click **Upload File** to upload the configuration template.

Backup X

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

Figure 157 Uploading Configuration Template

9. The Upload File page displays. Click **Select File** to browse for a source file.
10. Click Baselined to define the approved configuration. D-View 8 compares baselines to the device configuration and reports if there is a mismatch.
11. Click **Save** to define the baseline file. Click **Cancel** to return to the previous screen.

Figure 158 Defining Baselines

12. Under Schedule, select the interval and time to initiate the task:
 - Schedule Type: click to define the frequency period of the task, a single event or recurring task.
 - Execution Time: click to define the period of task execution, immediately or specify a time and date.
13. Click **Save** to create the backup task. Click **Cancel** to return to the previous screen.

The task is created and is listed in the Backup page.

To Edit or Stop the task:

14. Under Operation, click the **Edit** or **Stop** button located to the right of the task.

	Status	System Name	IP	Firmware Version	Backup Result	Model Name	Site	Network	Operation
<input type="checkbox"/>	●	Switc901tt	172.18.192.22	Build 1.28.009	Waiting for backup 2021-02-18 16:15:00	DES-3200-28	CS	Beijing_	⌂ ⌂
<input type="checkbox"/>	●	D-Link AP	172.18.192.20	4.3.0.2	Waiting for backup 2021-02-18 16:15:00	DWL-8600AP	CS	Beijing_	⌂ ⌂
<input type="checkbox"/>	●	4911	172.18.193.49	Build 1.00.038	Waiting for backup 2021-02-18 16:15:00	DWS-3160-24TC	CS	Beijing_	⌂ ⌂

Figure 159 List of Backup Tasks

6.4.2. Restoring Device Configurations


Device configuration settings can be restored through a defined backup task assigned a configuration baseline file.

To restore a device configuration:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **Configuration Management**. The Configuration Management page displays.
3. Click the **Restore** tab to view the defined restore tasks.
4. Select a device with a predefined baseline file and click **Restore** to configure the task.

	Status	System Name	IP	Firmware Version	Restore Result	Restore File	Model Name	Site	Operation
<input type="checkbox"/>	●	D-Link AP	172.18.192.20	4.3.0.2		filematching.docx	DWL-8600AP	CS	⌂ ⌂
<input checked="" type="checkbox"/>	●	4911	172.18.193.49	Build 1.00.038		filematching.docx	DWS-3160-24TC	CS	⌂ ⌂
<input type="checkbox"/>	●	N/A	172.18.192.15	6.30.B008			DGS-1210-10	CS	⌂ ⌂
<input type="checkbox"/>	●	DWC-2000	172.18.193.98	4.7.4.2_Ax_WW			DWC-2000	CS	⌂ ⌂
<input type="checkbox"/>	●	dap3662	172.18.193.166	v2.01			DAP-3662	CS	⌂ ⌂
<input type="checkbox"/>	●	DES-3528	172.18.193.99	2.60.017			DES-3528	CS	⌂ ⌂
<input type="checkbox"/>	●	DLINK-WLAN-AP	172.18.193.184	3.0.0.16			DWL-8500AP	CS	⌂ ⌂

Figure 160 Restoring Device Configurations



NOTE: A baseline file can be assigned by clicking the Select button and directly uploading the configuration file. In this manner, baseline files can be easily managed.

In the Select Restoration File page, the following actions are available:

- Upload file
- Download
- Set as baseline configuration
- Show file content

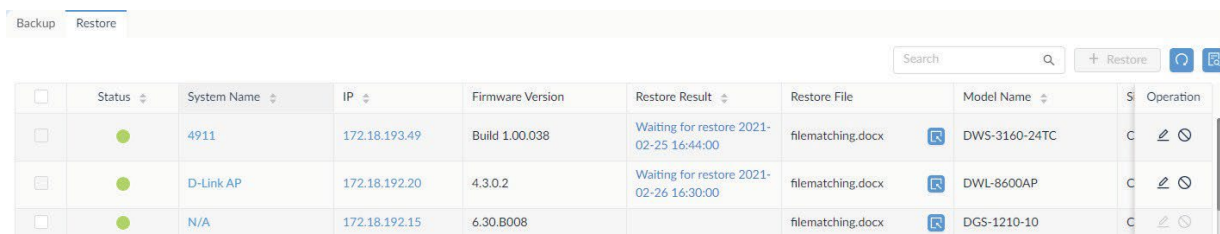
5. In the Restore page, under Schedule, select the interval and time to initiate the task:
 - Schedule Type: click to define the frequency period of the task, a single event or recurring task.
 - Execution Time: click to define the period of task execution, immediately or specify a time and date.

6. Click **Save** to create the restore task. Click **Cancel** to return to the previous screen.

The task is created and is listed in the Backup page.

To Edit or Stop the task:

7. Under Operation, click the **Edit** or **Stop** button located to the right of the task.



<input type="checkbox"/>	Status	System Name	IP	Firmware Version	Restore Result	Restore File	Model Name	Operation
<input type="checkbox"/>	●	4911	172.18.193.49	Build 1.00.038	Waiting for restore 2021-02-25 16:44:00	filematching.docx	DWS-3160-24TC	✎ ⏏
<input type="checkbox"/>	●	D-Link AP	172.18.192.20	4.3.0.2	Waiting for restore 2021-02-26 16:30:00	filematching.docx	DWL-8600AP	✎ ⏏
<input type="checkbox"/>	●	N/A	172.18.192.15	6.30.B008		filematching.docx	DGS-1210-10	✎ ⏏

Figure 161 Editing a Backup Task

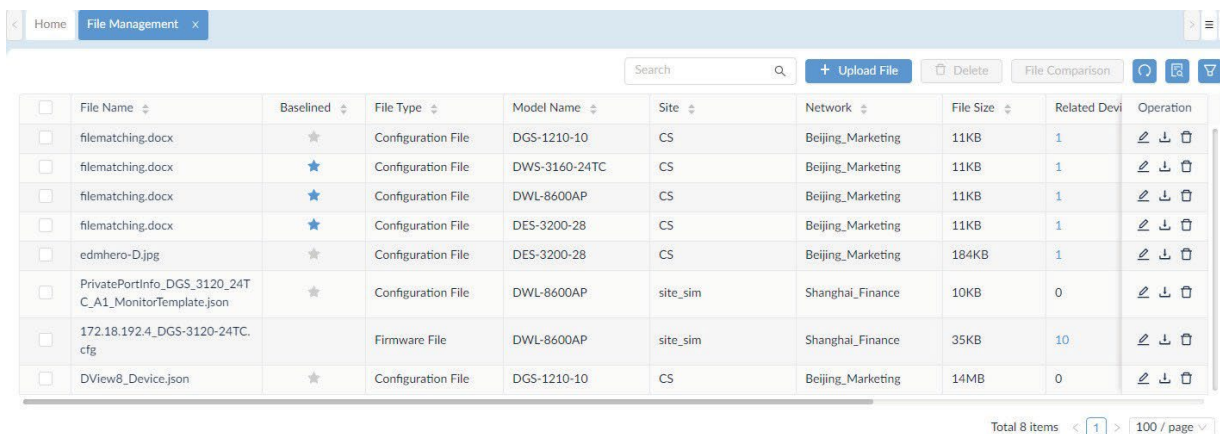
6.5. Network File Management

You can manage firmware and configuration files for various devices through the File Management function under Configuration. The function allows for uploading, deleting, file comparison, and searching to help organize and apply uploaded files. In this manner, templates for firmware and configuration settings can be utilized and expedite the maintenance process. With a single Firmware or Configuration template, an administrator user can manage an entire network of devices with just a few keystrokes.

The following section provides an overview of the File Management menus and a brief description of each.

To view the File Management menu:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.



<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	File Size	Related Devi	Operation
<input type="checkbox"/>	filematching.docx	★	Configuration File	DGS-1210-10	CS	Beijing_Marketing	11KB	1	✎ ⏏ 🗑️
<input type="checkbox"/>	filematching.docx	★	Configuration File	DWS-3160-24TC	CS	Beijing_Marketing	11KB	1	✎ ⏏ 🗑️
<input type="checkbox"/>	filematching.docx	★	Configuration File	DWL-8600AP	CS	Beijing_Marketing	11KB	1	✎ ⏏ 🗑️
<input type="checkbox"/>	filematching.docx	★	Configuration File	DES-3200-28	CS	Beijing_Marketing	11KB	1	✎ ⏏ 🗑️
<input type="checkbox"/>	edmhero-D.jpg	★	Configuration File	DES-3200-28	CS	Beijing_Marketing	184KB	1	✎ ⏏ 🗑️
<input type="checkbox"/>	PrivatePortInfo_DGS_3120_24TC_A1_MonitorTemplate.json	★	Configuration File	DWL-8600AP	site_sim	Shanghai_Finance	10KB	0	✎ ⏏ 🗑️
<input type="checkbox"/>	172.18.192.4_DGS-3120-24TC.cfg		Firmware File	DWL-8600AP	site_sim	Shanghai_Finance	35KB	10	✎ ⏏ 🗑️
<input type="checkbox"/>	DView8_Device.json	★	Configuration File	DGS-1210-10	CS	Beijing_Marketing	14MB	0	✎ ⏏ 🗑️

Total 8 items < 1 > 100 / page

Figure 162 File Management Overview

The following describes the available settings in the File Management page.

Item	Description
Search	Enter key phrase to filter the search criteria.
Delete	Select an entry and click Delete to remove it.
File Comparison	Select two configuration files to compare. Both files must be text based.
Refresh	Click to re-sync the table listings.
Advanced Query	Click to initiate an advanced search job. Enter the criteria to filter the task.
Column Selector	Click to add or remove columns from the File Management table. The following columns are available, enabled by default: File Name, Baselined, File Type, Model Name, Site, Network, File Size, Related Devices, Status, Upload Time, Description; Other: Uploaded by, MD5 Select All to enable all column options. Click Apply to confirm the new header selection.
File Name	Displays the file name of the listing.
Baselined	Displays the baseline status of the listing as marked by an enabled star icon, grayed-out if not defined as a baseline file.
File Type	Displays the type of file: Firmware or Configuration
Model Name	Displays the model name of the target device.
Site	Displays the site authorized to access the file.
Network	Displays the specified network corresponding to the selected site, which has access to the file.
File Size	Displays the size of the file.
Related Devices	Displays the number of compatible devices correlating to the defined device model name.
Status	Displays the status of the task: Already in use or Not used.
Upload Time	Displays the date and time of uploading of the file.
Description	Displays the description of the file.
Operation	
Edit	Click to edit the file listing.
Download	Click to export the file to a local system.
Delete	Click to remove the listing.

An overview of the Upload File menu is described as follows:

3. Click the **Upload File** to view the Upload File page.

Figure 163 Uploaded File Overview

The following describes the available settings in the Upload File page.

Item	Description
File Information	
Select File	Click to browse and define a configuration template.
File Type	Click the drop-down menu to select the type of file: Firmware File or Configuration File.
Baselined	Only available if Configuration File type is selected. Click to designate the file as a baseline template.
Description	Enter a short description to help identify the file type.
File Corresponding Device	
Site	Click the drop-down menu to select the corresponding site as defined in the network.
Network	Click the drop-down menu to select the corresponding network, as a subset of the selected site.
Model Name	Click the drop-down menu to select a pre-defined device type.
Device	Click the drop-down menu to select a discovered device correlating to the selected model type.
Cancel	Click Cancel to return to the previous menu.
Save	Click Save to add the define configuration file.

6.5.1. Firmware Management

Each device benefits from the latest firmware version. Check your device's support page to obtain the latest firmware version.

Caution:

When updating firmware, make sure the firmware is correct for the selected device. Select the correct device type and device model for a successful upload. The wrong firmware may cause damage to the device.

Caution:

When performing a batch firmware upgrade, make sure that all of the switches in the batch support the firmware selected.

The following topics are available in this section:

- Import a firmware file
- Modify a firmware file
- Export a firmware file
- Remove a firmware file
- Execute or schedule a firmware upgrade

6.5.1.1. Import a Firmware File

To import a firmware file:

1. Login to the Dashboard, see "3.2. Launching D-View 8 Web GUI" on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.
3. Click **+ Upload File** to display the Upload File page.

The screenshot shows a dialog box titled "Upload File" with a close button (X) in the top right corner. It is divided into two main sections: "File Information" and "Corresponding Device".

File Information:

- * File Name: A button labeled "Select File" with a downward arrow icon.
- * File Type: A dropdown menu currently set to "Firmware File".
- Share: A toggle switch that is currently turned on (blue).
- Description: A text input field containing the placeholder text "Enter Description".

Corresponding Device:

- * Site: A dropdown menu currently set to "Select site".
- * Network: A dropdown menu currently set to "Select network".
- Model Name: A dropdown menu currently set to "Select model name".

At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

Figure 164 Upload File Overview

4. Click **Select File** to browse for the target file.
5. From File Type, select Firmware File or Configuration File to designate the type of file.
6. Click the **Share** slide option to set as the baseline (default: enable).
7. In the Description field, enter a brief description of the file.
8. Click the **Site** drop-down field to select the corresponding site to associated.
9. Click the **Network** drop-down menu to select the corresponding network in the selected site.
10. Click the Model Name drop-down menu to designate the specific model series designated for the firmware.
11. Click the **Device** drop-down menu to select the specific device designated for the firmware.

This screenshot shows the same "Upload File" dialog box, but with specific values entered in the fields:

- * File Name: "Select File" button.
- * File Type: "Firmware File" dropdown.
- Share: Toggle switch is turned on.
- Description: "Firmware update" text input.
- * Site: "Taipei" dropdown.
- * Network: "Marketing" dropdown.
- Model Name: "DGS-1210-24(A1)" dropdown.

The "Cancel" and "Save" buttons are visible at the bottom right.

Figure 165 Selecting Firmware Destination Device

12. Click **Save** to create a firmware file entry or **Cancel** to return to the previous menu.

6.5.1.2. Modify a Firmware File

To modify an existing firmware file entry:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.
3. From the File Management page, select an existing entry from the list, and click **Edit**.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input checked="" type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
<input type="checkbox"/>	2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	N/A	Taipei	Marketing	Edit Download Delete

Total 7 items < 1 > 15 / page

Figure 166 Selecting Existing Firmware Entries

4. The File Information page displays. From this page you can modify listed information for this file.

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:

Corresponding Device

* Site: * Network:

Model Name:

Figure 167 File Information Overview

5. Enter a description to better identify the entry.
6. Modify the corresponding device information by selecting any of the following as required:
 - Site
 - Network
 - Model Name
7. Click **Save** to adopt the changes or **Cancel** to return to the previous menu.

6.5.1.3. Export a Firmware File

To export an existing firmware file:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	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

Figure 168 File Management Overview

3. From the File Management page, select an existing entry from the list, and click **Download**.

The file is downloaded to the designated folder on the local system. A successful download notification displays once the file is exported to the local system.

6.5.1.4. Remove a Firmware File

To remove a firmware file:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	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

Figure 169 File Management Overview

3. From the File Management page, select an existing entry from the list, and click **Delete File**.

A pop-up page displays to confirm the deletion of the file.

4. Click **Yes** to delete or **No** to cancel the process. The firmware entry is deleted after confirmation.

6.5.2. Configuration Management

D-View 8 application provides a simple function to allow you to back up and restore device configurations.

The following topics are available in this section:

- Import a configuration file
- Modify a configuration file
- Export a configuration file
- Remove a configuration file

6.5.2.1. Import a Configuration File

You can restore the configuration settings of D-Link devices on your network. You can also schedule tasks to be executed on a recurrent basis or as batch operations.

To import a configuration file see Importing Configuration and Firmware Files to a Network.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.
3. Click **+ Upload File** to display the Upload File page.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	✎ ↓ 🗑️
<input type="checkbox"/>	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

Figure 170 Uploaded File Entries Overview

4. Click **Select File** to browse for the target file.
5. From File Type, select Configuration File to designate the selection.
6. Click the **Share** slide option to allow sharing of the file with other networks (default: enable).
7. In the Description field, enter a brief description of the file.
8. Click the **Site** drop-down field to select the corresponding site to associated.
9. Click the **Network** drop-down menu to select the corresponding network in the selected site.
10. Click the Model Name drop-down menu to designate the specific model series designated for the configuration.
11. Click the **Device** drop-down menu to select the specific device designated for the configuration.

File Information

* File Name: Select File

* File Type: Configuration File

Set as Baseline:

Description: Configuration entry

Corresponding Device

* Site: Taipei * Network: Marketing

* Model Name: DSR-500AC(A1) * Device: DSR-500AC(172.18.192.1)

Cancel
Save

Figure 171 Selecting Devices for Configuration

12. Click **Save** to create a firmware file entry or **Cancel** to return to the previous menu.

6.5.2.2. Modify a Configuration File

A configuration file of any device can be used as a template to configure corresponding devices on the network. The first step is to modify the configuration file or customize it for the target device(s).

To modify an existing configuration file:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.
3. From the File Management page, select an existing entry from the list, and click **Edit**.

File Name	Baselined	File Type	Model Name	Site	Network	Operation
config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	Edit Download Delete
2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	Edit Download Delete
2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	Edit Download Delete
2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	Edit Download Delete
2021-03-22_17-52-01_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	N/A	Taipei	Marketing	Edit Download Delete

Total 7 items < 1 > 15 / page

Figure 172 Selecting Entries for File Management

4. The File Information page displays. From this page you can modify listed information for this file.

The screenshot shows a web interface for configuring file entries. At the top, the file name is "2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg". Below this, the "File Information" section displays: 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, and Set as Baseline: checked. A description field contains the placeholder text "Enter Description". The "Corresponding Device" section has four dropdown menus: Site (Taipei), Network (Marketing), Model Name (DWS-3160-24PC(A1)), and Device (MAIN_AC040712(172.18.193.209)). At the bottom right, there are "Cancel" and "Save" buttons.

Figure 173 Configuring File Entries

5. Click **Set as Baseline** to designate this file as a baseline for this type of device.
6. Enter a description to better identify the entry.
7. Modify the corresponding device information by selecting any of the following as required:
 - Site
 - Network
 - Model Name
 - Device
8. Click **Save** to adopt the changes or **Cancel** to return to the previous menu.

6.5.2.3. Export a Configuration File

To export an existing configuration file:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Configuration, click the **File Management**. The File Management page displays.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	↶ ↷ 🗑️
<input checked="" type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	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

Figure 174 File Management Overview

- From the File Management page, select an existing entry from the list, and click **Download**.

The file is downloaded to the designated folder on the local system. A successful download notification displays once the file is exported to the local system.

6.5.2.4. Remove a Configuration File

To remove a firmware file:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- In Configuration, click the **File Management**. The File Management page displays.

<input type="checkbox"/>	File Name	Baselined	File Type	Model Name	Site	Network	Operation
<input type="checkbox"/>	config.bin	N/A	Firmware File	DAP-2690B	Taipei	Marketing	↶ ↷ 🗑️
<input checked="" type="checkbox"/>	2021-03-30_09-32-27_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-57_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-29_20-12-16_172.18.193.212_DGS-3120-24TC.cfg	★	Configuration File	DGS-3120-24TC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-23_10-50-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	2021-03-22_17-30-00_172.18.193.209_DWS-3160-24PC.cfg	★	Configuration File	DWS-3160-24PC	Taipei	Marketing	↶ ↷ 🗑️
<input type="checkbox"/>	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

Figure 175 Removing a File Entry

- From the File Management page, select an existing entry from the list, and click **Delete File**.

A pop-up page displays to confirm the deletion of the file.

- Click **Yes** to delete or **No** to cancel the process. The firmware entry is deleted after confirmation.

This page is intentionally left blank.

7 Manage Alarms and Logs

Alerts and notifications are received when the an upper or lower threshold is exceeded. If the threshold is exceeded, an alarm is generated by the alarm configuration. You can receive the notification by email, web scrolling notification, or as an executed script.

The following topics are available in this section:

- View and Manage Alarms
- View and Manage Traps and Syslogs
- Manage Trap Editor
- Monitor and Manage Alarms
- View and Manage Network Event Notifications

7.1. View and Manage Alarms

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click **Alarm**.
The Alarm page displays.
The displayed list includes both active an historical alarm events.



Figure 176 Alarm Event Overview

Item	Description
Active Alarms	Displays a list of the current alarm events.
Historical Alarms	Displays a list of alarm events already completed or designated as removed.
Critical	Indicates a critical (highest) severity level for the alarm (red color indication).
Warning	Indicates a major severity level for the alarm (yellow color indication).
Info	Indicates an informative level for the alarm (blue color indication).
Search	Enter key phrase to filter the search criteria.
Acknowledge	Select an alarm event and click Acknowledge to stop further notifications of the event.
Column Selector	Click to add or remove columns from the File Management table. The following columns are available, enabled by default: Level, Last Updated, Duration, System Name, IP, Alarm Type, Latest Message; Other: Site, Network, Device Category, Time Generated. Select All to enable all column options. Click Apply to confirm the new header selection.
Refresh	Click to re-sync the table listings.
Export	Click to export the discovered devices as a CSV file. Up to 10,000 entries can be downloaded in one export job.
Advanced Query	Click to initiate an advanced search job. Enter the criteria to filter the task.

3. Click an alarm event to select it.
4. Click Acknowledge to stop the alarm from triggering further notifications.

7.2. View and Manage Traps and Syslog

The Trap & Syslog list displays the device trap events.

7.3. Manage Trap Editor

You can manage trap events in the Trap Editor function. The trap entries can be edited or deleted.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click Trap Editor.
The Trap Editor page displays.

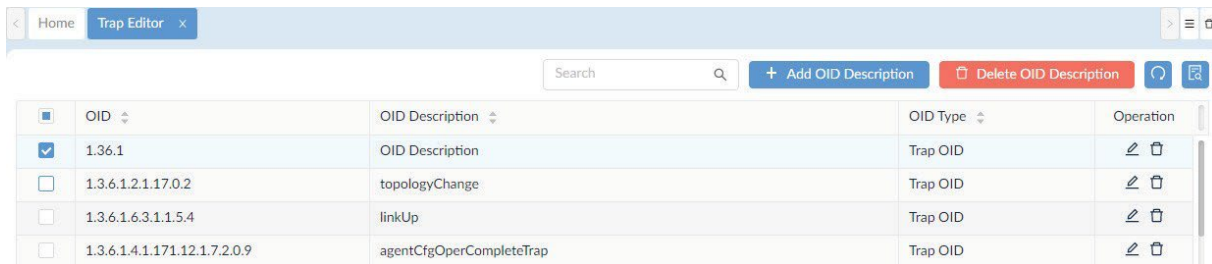


Figure 177 Trap Editor Overview

3. Click on a listed trap event to select it.
4. You can select any of the following options to edit the selected trap:

Item	Description
Search	Enter key phrase to filter the search criteria.
Add OID Description	Click Add OID description to add a unique object identifier value for use by an SNMP entity to identify the notification.
Delete OID Description	Click to delete the OID description.
Refresh	Click to re-sync the table listings.
Advanced Query	Click to initiate an advanced search job. Enter the criteria to filter the task.
Edit	Click Edit to directly modify the OID description.
Delete	Click to directly delete the OID description.

7.4. Monitor and Manage Alarms

You can manage monitor and alarm settings as well as alarm-able item definitions.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click Monitor & Alarm Settings.
By default, the Alarm Settings page displays.

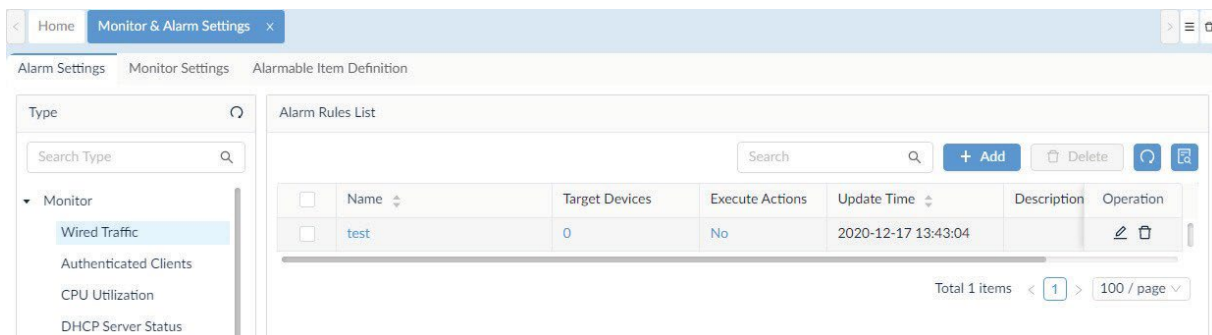


Figure 178 Alarm Settings Overview

From the Alarm Settings menu, you can set Monitor, Trap, Syslog, and sFlow rules.

Item	Description
Monitor	Wired Traffic Authenticated Clients CPU Utilization DHCP Server Status Device Common Information Fan HTTP Status HTTPS Status Installed Apps LACP LLDP Managed AP WLAN Traffic(packet) Memory Utilization Power Status Private Port RMON Status Response Time Running Software SIM Traffic SNTP Status SSH Status STP Status Safeguard Status Syslog Status Telnet Status Temperature Trap Status WLAN Traffic(bit) WLAN Traffic(packet) Wireless Access Points Wireless Error Packets
Trap	coldStart warmStart linkDown linkUp authenticationFailure egpNeighborLoss enterpriseSpecific
Syslog	Syslog
sFlow	sFlow

7.4.1. Add an Alarm Rule

To Add an alarm rule:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click Monitor & Alarm Settings.
By default, the Alarm Settings page displays.
3. From the Type column, select a setting to view the available categories. For this procedure, Wired Traffic is selected.
4. Click **Add** to configure a rule.

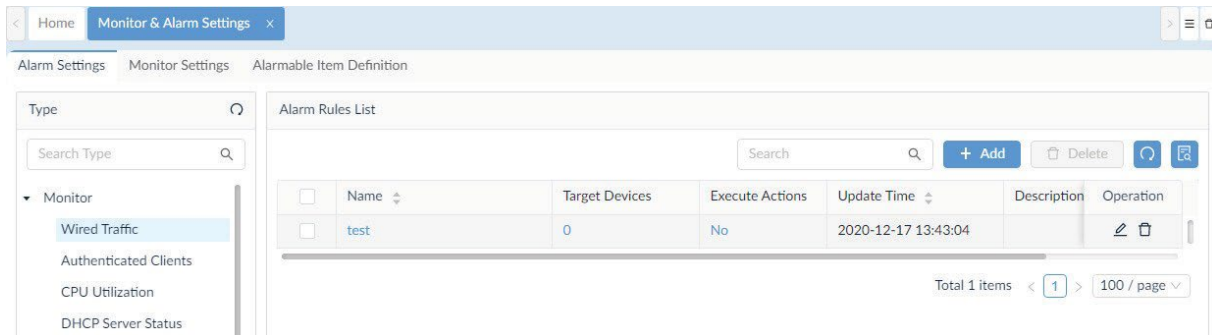


Figure 179 Configuring Rule Entries

The Add Alarm Rule page displays.

5. Each rule requires specific configurable information, which must be entered to define the rule task. The following information is required:
 - Set profile information
 - Set target device
 - Set actions
6. Click **Next** to continue the rule configuration.
7. Click **Save** to create the task once the rule is defined. Click **Cancel** to return to the previous menu. The new rule is saved and listed in the Alarm Rules List.

7.4.2. View Monitor Settings

Network monitoring is performed through the Monitor and Alarm settings menu. You can select specific categories to view available listings.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click Monitor & Alarm Settings. By default, the Alarm Settings page displays.
3. Click the **Monitor Settings** tab to view the Monitor List page.
4. To view the list by specific columns, click on the column name and the list is prepared in ascending/descending order.
5. From this list, you can select a batch monitor task or as a port batch assignment.

To assign a batch monitoring task:

6. Select the devices or perform a search to view the target devices.
7. Click **Batch Monitor Switch** to enable or disable the monitoring of the selected devices.

To select devices based on the port setting:

8. Select the target device(s).
9. Click Batch Select Port. A pop-up page displays.
10. Enter the port for the batch task.
11. Click **Apply** to assign the setting.

7.5. View and Manage Network Event Notifications

The Notification Center displays the notification rules for the entire network.

7.5.1. View and Manage Notification Events

To view and manage notification events:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click **Notification Center**.
The Notification Center page displays.

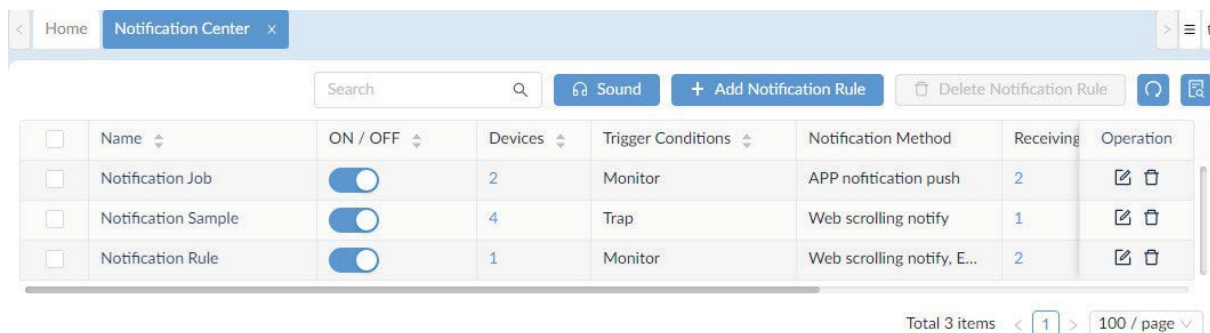


Figure 180 Notification Center Overview

Item	Description
Search	Enter key phrase to filter the search criteria.
Sound	Click to customize a ringtone to sound when the notification is triggered. Each alarm level can be customized with a built-in ringtone.
Add Notification	Click to define a notification rule.
Delete Notification	Click to remove a listed rule from the listing.
Refresh	Click to re-sync the table listings.
Advanced Query	Click to initiate an advanced search job. Enter the criteria to filter the task.
Name	Displays the task name.
ON / OFF	Click the slide button to enable or disable the rule.
Devices	Displays the number of devices connected to the rule.
Trigger Conditions	Displays specific alarm trigger condition.
Notification Method	Displays the method of notification for the rule.
Receiving Administrator	Displays the user profile to receive the notification.
Description	Displays a description of the rule.
Operation	
Edit	Click to edit the rule.
Delete	Click to remove the rule.

3. Click **Add Notification** to configure a new rule.
The Notification Management Details page displays.

Notification Management Details X

Basic Information

*Name:

Description:

ON / OFF:

Source Devices + Add

System Name	IP	Network	Model Name	Operation
No Data				

Total 0 items < 0 > 100 / page

Trigger Conditions

*Condition Type:

*Alarm Level: All Critical Warning Info

Cancel

Figure 181 Notification Center Overview

4. Enter the Basic Information to define the rule.
5. Click the **ON/OFF** slider button to enable or disable the rule.
6. In Source Devices, click **Add** to select the target device.
The Batch Select Devices page displays.

Batch Select Devices X

Resource Tree

Search network

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

Device List

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

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

Cancel

Figure 182 Device Batch Selection

130

- From the Device List, select the device(s) to include for the application of the notification rule.
- Click **OK** to accept the selection and return to the previous screen.

<input type="checkbox"/>	System Name	IP	Network	Model Name
<input checked="" type="checkbox"/>	D-Link	172.18.193.253	Marketing	DES-3226STK
<input type="checkbox"/>	N/A	172.18.193.237	Marketing	Other
<input type="checkbox"/>	N/A	172.18.193.235	Marketing	Other
<input type="checkbox"/>	N/A	172.18.193.234	Marketing	Other
<input checked="" type="checkbox"/>	ACC_SW_STAC...	172.18.193.230	Marketing	DES-3028
<input type="checkbox"/>	DLINK-WLAN-AP	172.18.193.184	Marketing	DWL-8500AP
<input type="checkbox"/>	N/A	172.18.193.163	Marketing	Other
<input type="checkbox"/>	N/A	172.18.193.161	Marketing	Other

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

Figure 183 Selecting Devices to Bind to Notification Rules

The Notification Management Details page displays.

- Under the Trigger Conditions, click the **Condition Type** drop-down menu to select a trigger condition type.

Trigger Conditions

* Condition Type: Monitor v Please choose one or more

Please select a category.

* Alarm Level: All Critical

Notification Details

* Notification Method: Web scrolling notify x

Screen Scrolling Settings

* Sound: Mute Enable

Notification Receiving Administrator

Current Administrator

Figure 184 Selecting Notification Condition Types

See the following table for further details.

Item	Description
Condition Type	
Monitor	<p>The available monitoring parameter is based on the selected device type. Not all parameters are available for all types of devices.</p> <ul style="list-style-type: none"> • CPU Utilization • HCP 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
Trap	<p>Select all or a specific trap event to trigger an alarm notification:</p> <ul style="list-style-type: none"> • All: all trap events trigger an alarm notification. • Critical: critical trap events trigger an alarm notification. • Warning: warning events trigger an alarm notification. • Info: informational events trigger an alarm notification.
Syslog	<p>Select all or a specific wired traffic event to trigger a Syslog alarm notification:</p> <ul style="list-style-type: none"> • All: all events trigger an alarm notification. • Critical: critical events trigger an alarm notification. • Warning: warning events trigger an alarm notification. • Info: informational events trigger an alarm notification.
Wired Traffic	<p>Select all or a specific system log event to trigger a wired traffic alarm notification:</p> <ul style="list-style-type: none"> • All: all events trigger an alarm notification. • Critical: critical events trigger an alarm notification. • Warning: warning events trigger an alarm notification. • Info: informational events trigger an alarm notification. <p>The selected model name displays, select all or a specific port to assign the trigger condition.</p>
Alarm Level	<p>Select the type of alarm to trigger the notification:</p> <p>All: all alarm levels are selected for notification. Critical: error information condition indicating failure or malfunction. Warning: error information conditions that may cause future problems Info: information-only level conditions</p>

10. Under Notification Details, click the Notification Method drop-down menu to define the delivery method.

Item	Description
Notification Method	
Web scrolling notify	Select the Screen Scrolling Setting for the alert: Mute sound or Enable Voice.

Item	Description
Email	<ul style="list-style-type: none"> Click to enable the Current Administrator setting. Click Add select a specific user to receive the Email notification. Enter specific criteria (Email, Username, Role) to search for a defined user. Click OK to accept. Click Cancel to return to the previous screen.
Execute script	<ul style="list-style-type: none"> In the Command Line, enter the script to execute. See “7.5.1.1. Executing Scripts” on page 134 for further information. Instructions are also available by scrolling over the help (?) menu.

- Under the Notification Receiving Administrator, click **Add** to identify the administrator profile to receive notifications when the rule is triggered.
- The Select User page displays. From the available list, select an administrative user to receive the notifications.
- Click **OK** to add the profile to the rule. Click **Cancel** to return to the previous page without selecting a profile.

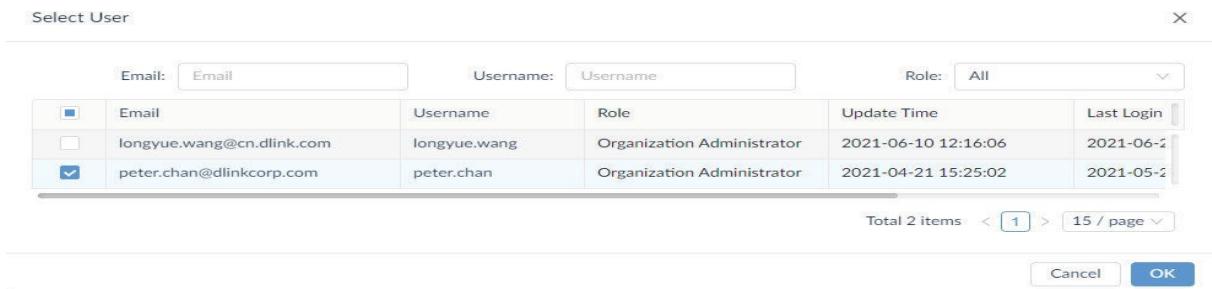


Figure 185 Selecting a Notification User Profile

The Notification Management Details page displays.

- Under the Notification Suspension Period, click **Add** to select a schedule.

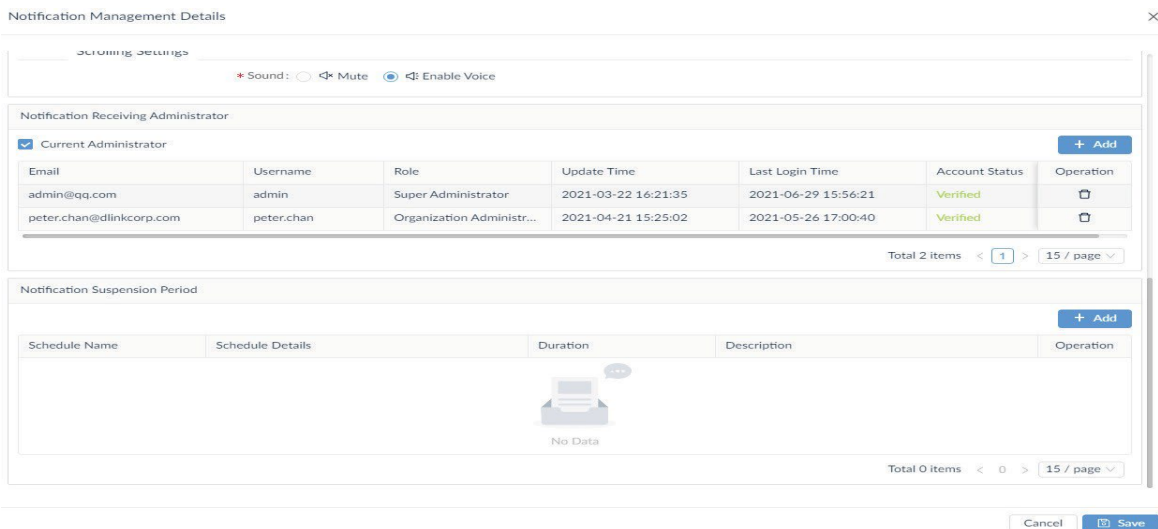


Figure 186 Selecting a Notification Suspension Period

The Select Schedule page displays.

- A defined schedule list displays in the page. Select a listing and click **OK** to set the suspension period.



Figure 187 Selecting a Set Schedule

16. Select a defined schedule period and click **OK** to accept. Click **Cancel** to return to the previous screen.
17. Click **Save** to accept the notification rule. Click **Cancel** to return to the previous screen. The notification rule is saved and displays as seen in the following figure.

The screenshot shows the 'Notification Management Details' interface with the following sections:

- Basic Information:** Name: Notification Rule, Description: Description of defined rule, ON / OFF:
- Source Devices:** Table with 1 item: WIN-SB23GPM9LGR, IP: 172.18.193.51, Network: Marketing, Model Name: WindowsServer, Operation:
- Trigger Conditions:** Condition Type: Monitor, CPU Utilization: %, Alarm Level: All, Critical, Warning, Info
- Notification Details:** Notification Method: Email, Web Scrolling Message, Scrolling Settings: Sound, Mute, Enable Voice
- Notification Receiving Administrator:** Table with 2 items:

Email	Username	Role	Update Time	Last Login Time	Account Status	Operation
admin@qq.com	admin	Super Administrator	2021-03-22 16:21:35	2021-06-29 15:56:21	Verified	<input type="checkbox"/>
peter.chan@dlinkcorp.com	peter.chan	Organization Administr...	2021-04-21 15:25:02	2021-05-26 17:00:40	Verified	<input type="checkbox"/>
- Notification Suspension Period:** Table with 1 item:

Schedule Name	Schedule Details	Duration	Description	Operation
test2	[Weekdays] Mon, Tues, Wed, Thur, Fri, Sat, Sun [Time] 11:16:00 - 11:19:00 [Time Zone] (GMT+08:00) Taipei	2021-06-10 - 2099-12-31		<input type="checkbox"/>

Buttons: Cancel, Save

Figure 188 Completed Notification Rule

7.5.1.1. Executing Scripts

- In the following instructions, lines beginning with a '#' are considered comments not commands.
- Use '%' before and after a string to label it as a variable. Example: %IP% labels IP as a variable.
- Each line must contain no more than a single CLI command.
- To prevent deadlock operation, avoid the use of endless CLI commands. Example: ping 10.0.0.1.
- To prevent deadlock operation, avoid using CLI commands requiring special input entries to exit. Example: show port.

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
```

7.5.2. Modify Notification Events

To view and manage notification events:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. In Alarm & Notification, click Notification Center.

The Notification Center page displays.

The screenshot shows the Notification Center page with a table of notification events. The table has columns for Name, ON/OFF, Devices, Trigger Conditions, Notification Method, Receiving, and Operation. There are three rows of data: Notification Job, Notification Sample, and Notification Rule. Each row has a checkbox in the Name column and a toggle switch in the ON/OFF column. The Operation column contains edit and delete icons for each row.

<input type="checkbox"/>	Name	ON / OFF	Devices	Trigger Conditions	Notification Method	Receiving	Operation
<input type="checkbox"/>	Notification Job	<input checked="" type="checkbox"/>	2	Monitor	APP notification push	2	
<input type="checkbox"/>	Notification Sample	<input checked="" type="checkbox"/>	4	Trap	Web scrolling notify	1	
<input type="checkbox"/>	Notification Rule	<input checked="" type="checkbox"/>	1	Monitor	Web scrolling notify, E...	2	

At the bottom of the table, there is a pagination control showing "Total 3 items" and "1 / 100 / page".

Figure 189 Modifying a Notification Policy

3. From the Operation column, click Edit or Delete on the target notification task. By using Edit, you can modify the defined settings of the task. Alternatively, a task can be deleted and removed from the current list.
4. Click Save to accept the new settings.
5. In Alarm & Notification, click Notification Center.

The Notification Center page displays.

This page is intentionally left blank.

8 Manage Architecture Topologies

You can view the network architecture through hierarchical maps.

The following topics are available in this section:

8.1. View and Manage Network Topologies

D-View 8 provides a network map to view architecture topology available on the dashboard.

8.1.1. View a Network Topology and Device Details

Locating devices within the network is can be accomplished through a hierarchical map. Further information such as device details and correlating rules and tasks is visible through the map function.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Architecture, select the network diagram by clicking on it. The Topology Map page displays.

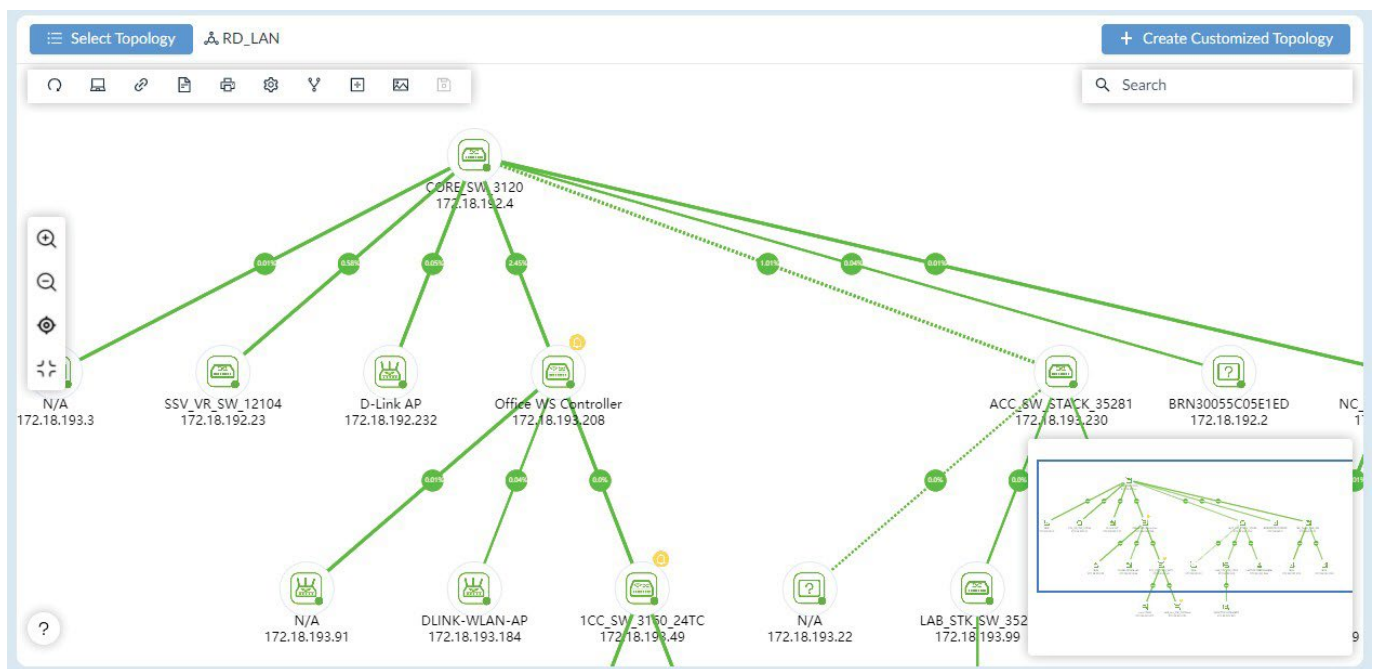



Figure 190 Network Diagram

Item	Description
Select Topology	Click to open the System Topology or Customized Topology library. The Search function allows the listing of available maps by entering keyword terms.
Create Customized Topology	Create a customized diagram based on specific organization, site, network or select devices.
Toolbar	

Item	Description
	<p>The following is a description of the toolbar icons from left to right.</p> <ul style="list-style-type: none"> • Refresh: synchronize the screen topology. • Device List: Displays the Device List menu. • Link List: Displays the Link List menu • Network Overview: Displays a basic overview of the network status, including devices, alarms, and disconnected links. • Export: Save the map as a .PNG file on the local drive. • Topology Settings: Change the current topology's information settings. Specify or disable visible information by clicking on the option. • Rediscover: Initiate a rediscovery of the architecture. • Link Edit: Enable or disable the link editing function. • Add Background: Add a background image to the map. • Save: Save the current topology map.
Search	Click to search for specific devices.
Control Bar	
	<p>The following is a description of the control bar icons from left to right.</p> <ul style="list-style-type: none"> • Zoom in • Zoom out • Focus on central node • Zoom fit
Help	<ul style="list-style-type: none"> • Topological Legend • Link Operation • Batch Select Nodes

- From the Topology Map, select a device.
When selected, the device is highlighted.

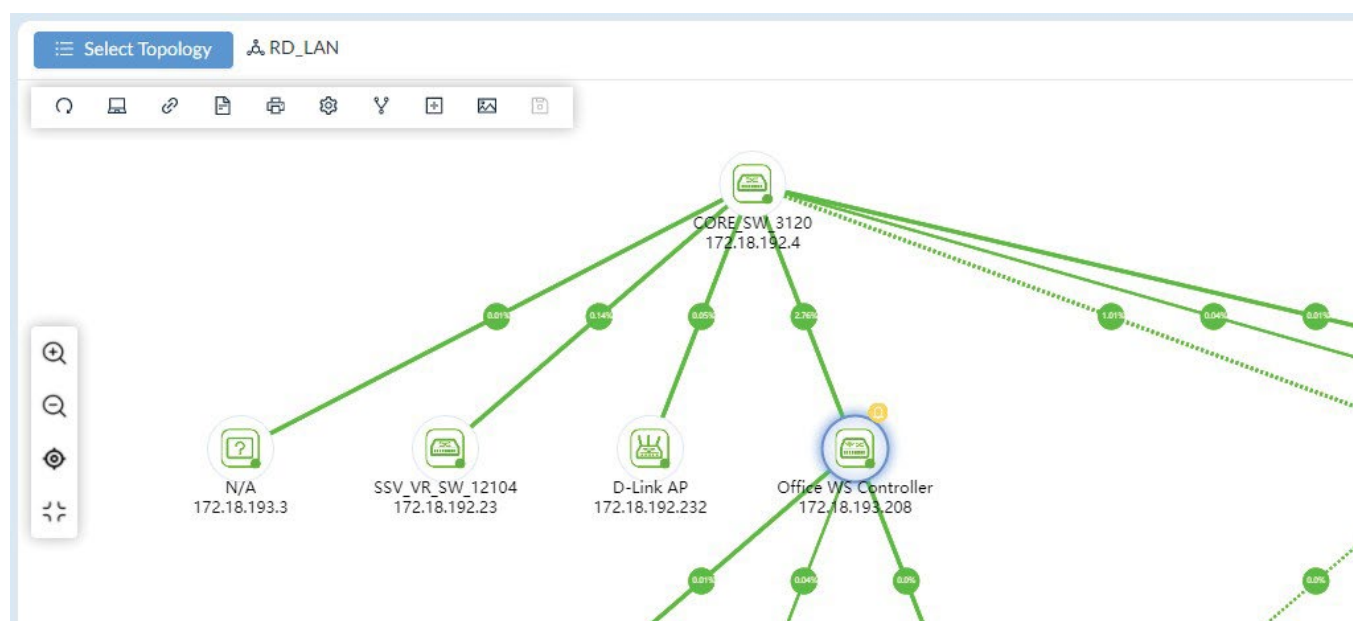


Figure 191 Selected Device in Topology Map

- Click on the device to display the device's information page.

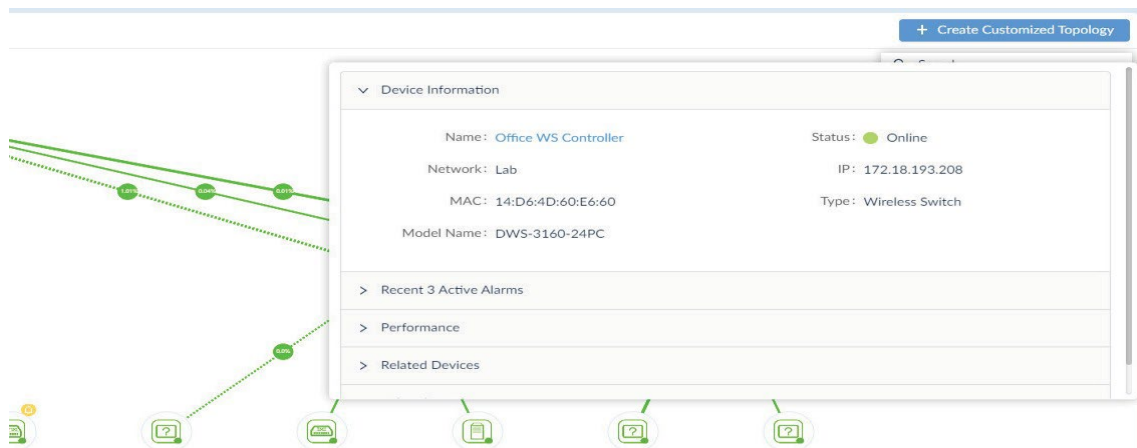


Figure 192 Displaying Device Information

5. From this page, the following content is available:

- Device Information
- Recent 3 Active Alarms
- Performance
- Related Devices
- Related Topology

6. To view details for a link, click a link to select it.

The Link Information page displays.

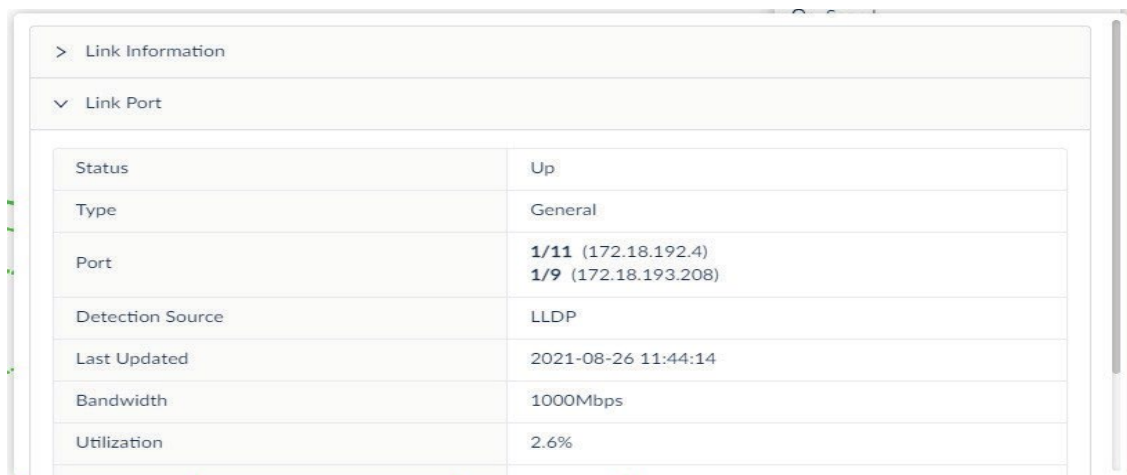


Figure 193 Link Information

7. From this page, the following content is available:

- Link Information
- Link Port
- Link Alarm

Viewing the topology map is done through the control bar or the navigation pop-up page.

8. From the control bar, select an icon to zoom in, zoom out, focus on central node or zoom fit to screen.

9. You can also use the navigation page to pinpoint an area on the map.

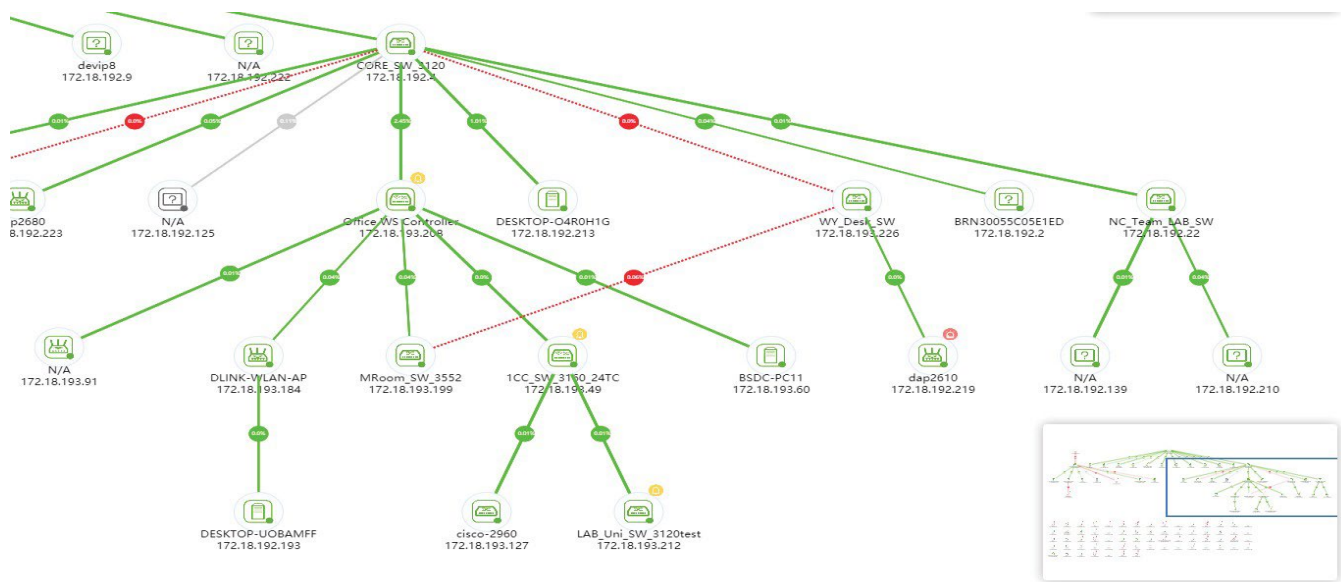


Figure 194 Using Navigation Pane

8.2. Creating a Topology View

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Architecture, select the network diagram by clicking on it. The Topology Map page displays.

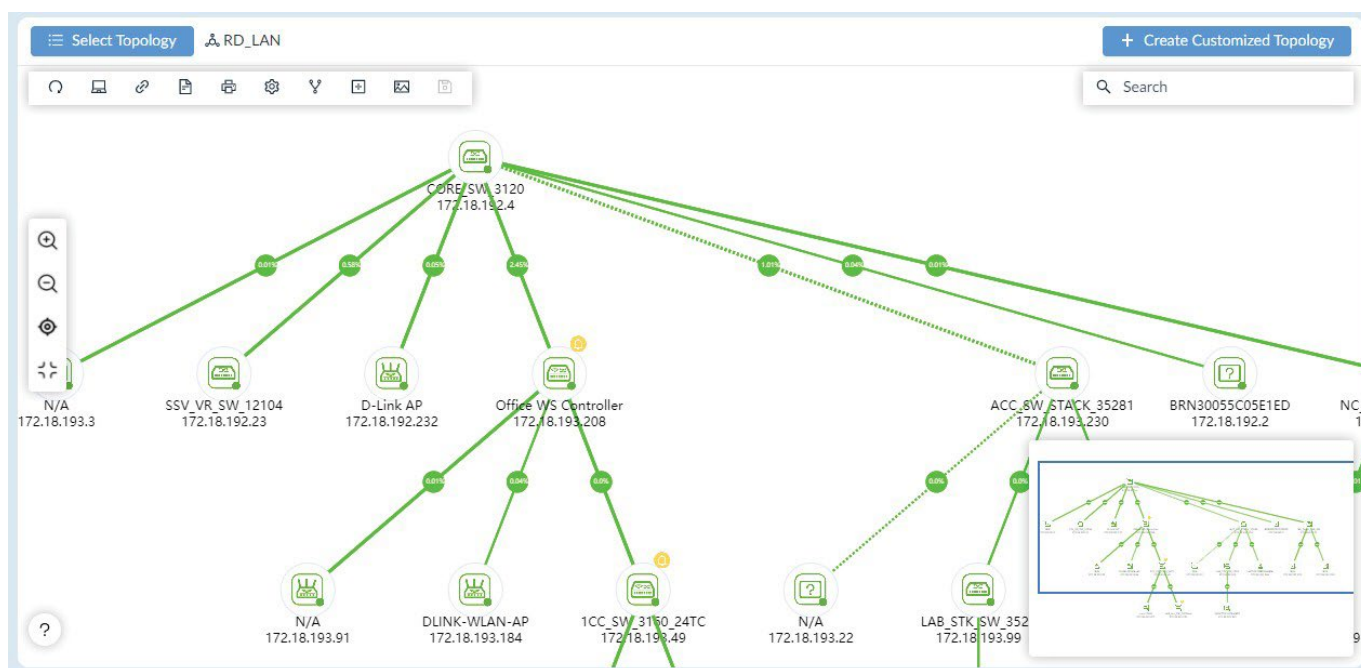


Figure 195 Selecting a Network Diagram

3. Click **Create Customized Topology**.
The Create Customized Topology page displays.

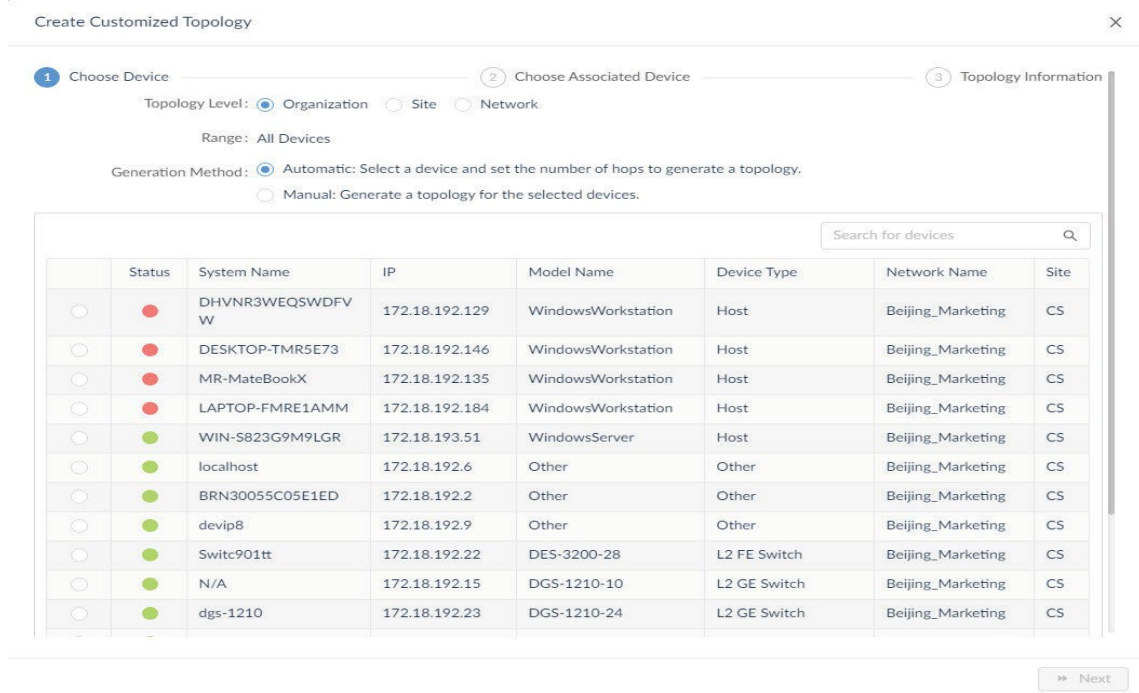


Figure 196 Creating a Customized Topology

4. Select the device(s) associated with the topology diagram. In Topology Level, select Organization, Site, or Network.
5. Selected the method to generate the diagram. Automatic (default): automatically selects a device and sets the number of hops to generate the topology. Manual: generates a topology for the selected diagram.
6. Select a device(s) to associate to the topology. Alternatively, you can search for a specific device(s) by using keywords in the search field.
7. Click **Next** to proceed.

The Choose Associated Device page displays.

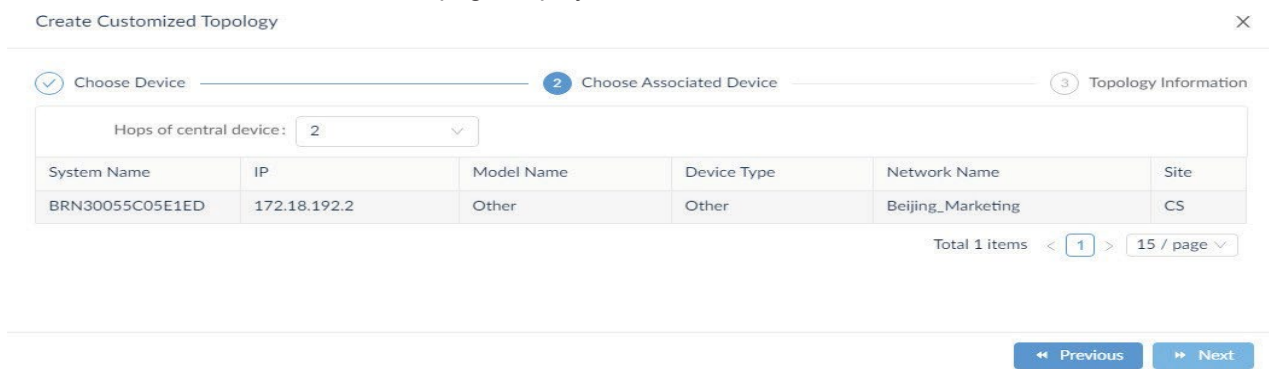


Figure 197 Selecting an Associated Device

8. Click the **Hops of central device** drop-down menu to define the number of hops (2 to 10) from the central device to associate additional devices.
9. Click **Next** to continue. Click **Previous** to return to the previous menu. The Topology Information page displays.

Create Customized Topology X

Choose Device Choose Associated Device **3** Topology Information

* Name:

Description:

Data source of links: Synchronization with system User-defined

Topology Layout: Star Tree Circular Grid

Sharing Status : OFF

Auto : OFF

Select Central Device Search

	System Name	IP	Model Name	Device Type	Netwc
<input type="radio"/>	1CC_SW_3160_24	172.18.193.49	DWS-3160-24TC	Wireless Switch	Marke
<input type="radio"/>	ABC30055C05E1ED	172.18.192.22	DES-3200-28	L2 FE Switch	Marke
<input type="radio"/>	ACC_SW_STACK_3528 1	172.18.193.230	DES-3028	L2 FE Switch	Marke
<input type="radio"/>	BRN30055C05E1ED	172.18.192.2	test	aaaa	Marke
<input type="radio"/>	CORE_SW_3120	172.18.192.4	DGS-3120-24TC	L2 GE Switch	Marke
<input type="radio"/>	D-Link	172.18.193.253	DES-3226STK	L2 FE Switch	Marke
<input checked="" type="radio"/>	D-Link DAP-2690	172.18.192.182	DAP-2690B	Standalone AP	Marke
<input type="radio"/>	DES-3226STK	172.18.193.253	DES-3226STK	L2 FE Switch	Marke

Figure 198 Viewing Customized Topology

10. In the Name field, enter the name for the topology map.
11. In the Description field, enter a description to identify the map.
12. In Data source of links, select either Synchronization with system or User-defined to specify the origin of the data link source.
13. Select the type of layout for the map: Star, Tree, Circular, or Grid.
14. Slide the Sharing Status slider to ON (default: OFF) to provide view, edit, and delete access to administrators.
15. Slide the Auto slider to ON (default: OFF) to control the selection mode of the central device to be displayed. ON indicates the system specifies the mode automatically. OFF indicates a manual specification of the mode.
16. From the Select Central Device menu, either Search for a specific device or click on the listing.
17. Click **Save** to create the topology map. Click **Previous** to return to the previous menu.

The topology map is created and appears in the Topology Map listings.

8.3. Modify and Delete a Topology View

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Architecture**, select the network diagram by clicking on it. The Topology Map page displays.

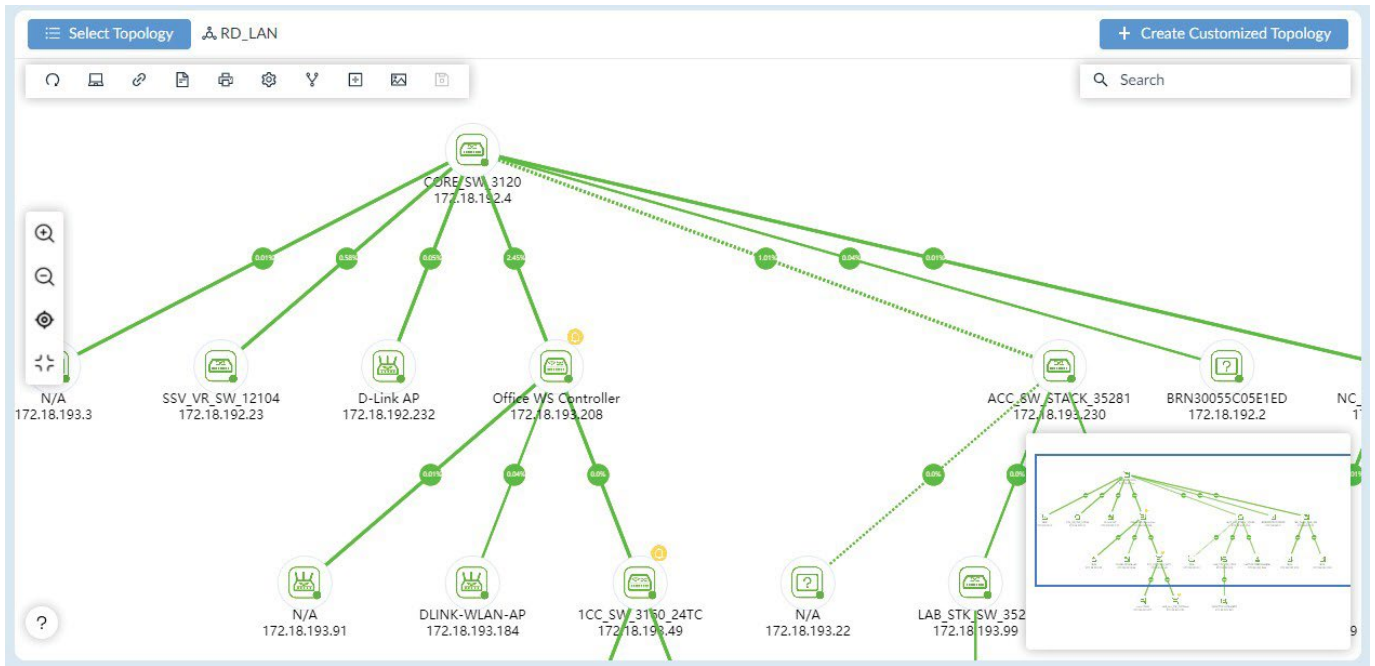


Figure 199 Viewing a Resource Tree

3. Click **Select Topology** to display the topology library. Only customized maps can be modified or deleted.
4. Click the **Customized Topology** tab.
5. Select a listing by using the Search function or clicking on a listed map.

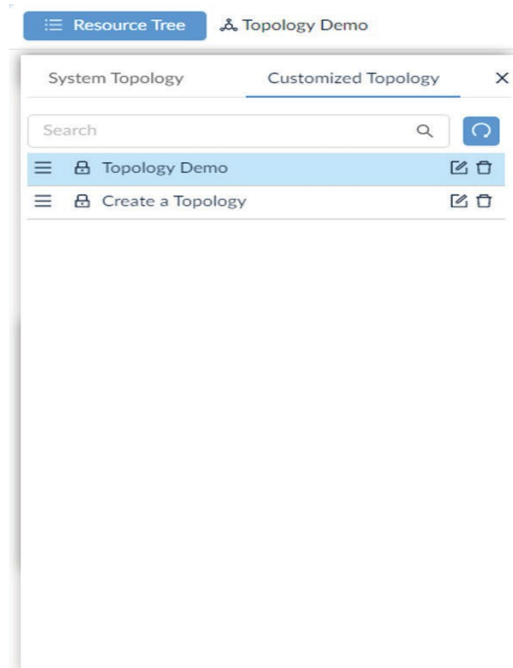


Figure 200 Selecting a Listed Map

6. On the selected map, click **Edit** to modify the information of the topology map.
7. Alternatively, click **Delete** to remove the map from the library.

This page is intentionally left blank.

9 Manage Rack Groups

In heterogeneous networks, administrators need to allocate an organized structure to more effectively view and manage the device infrastructure.

9.1. Add a Rack Group

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Monitoring, click **Rack View** to display the Group List page.

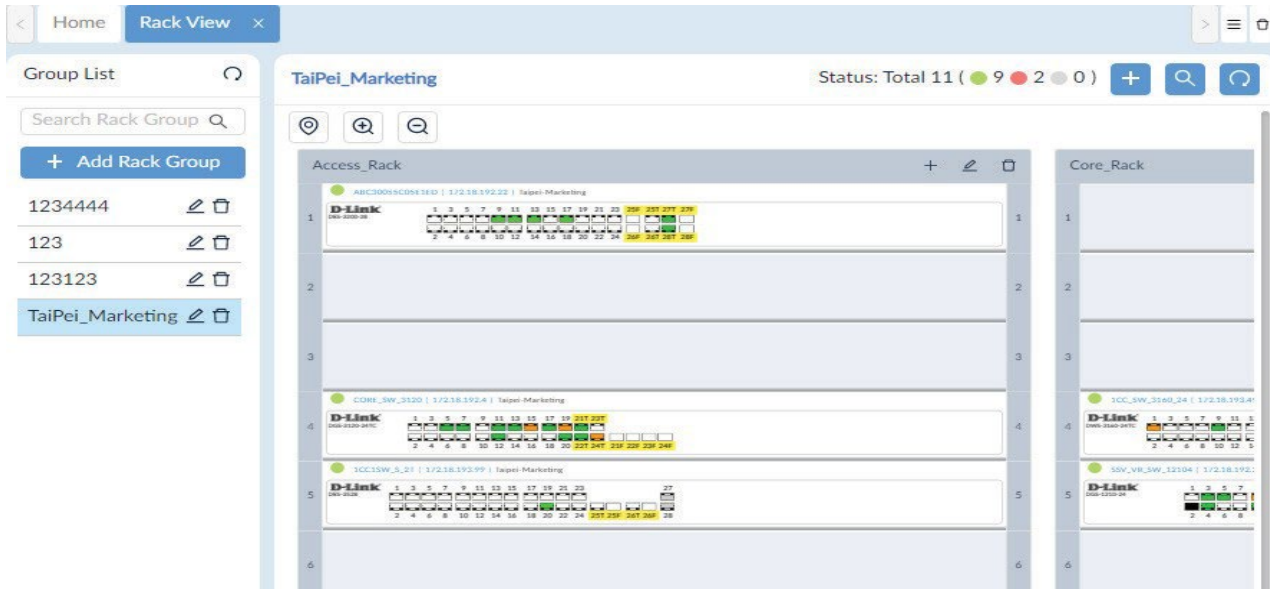


Figure 201 Viewing Group Lists

3. Click **Add Rack Group**.

The Add Rack Group page displays.

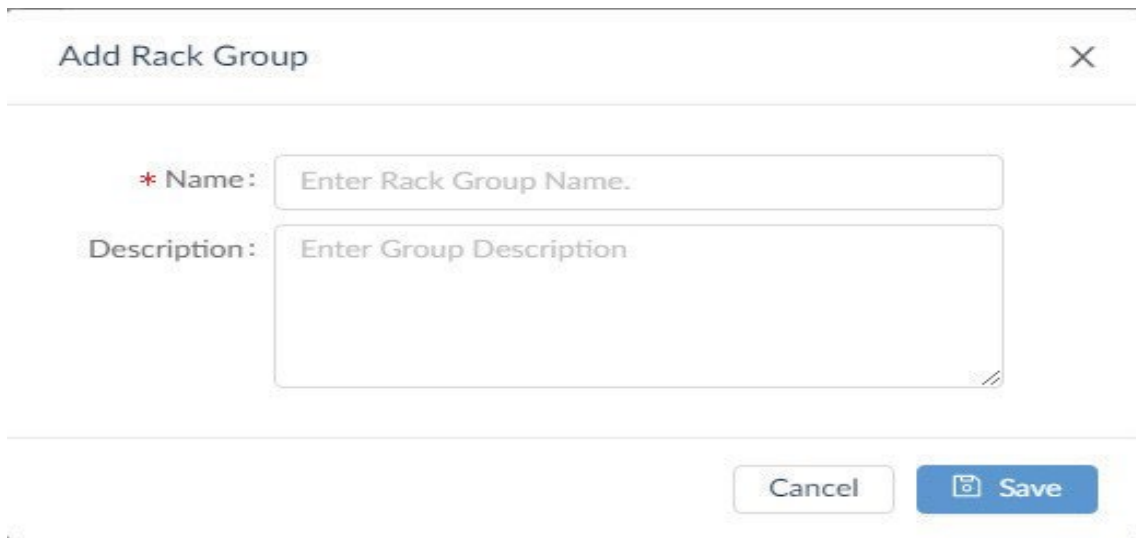


Figure 202 Adding a Rack Group

4. Enter the name and description to use for the group.
5. Click **Save** to create the group. Click **Cancel** to return to the previous screen.

When added successfully, the group page displays.

At this point there is no data to display.

6. Click **Add Rack** to populate the rack structure with devices.

The Add Rack page displays.

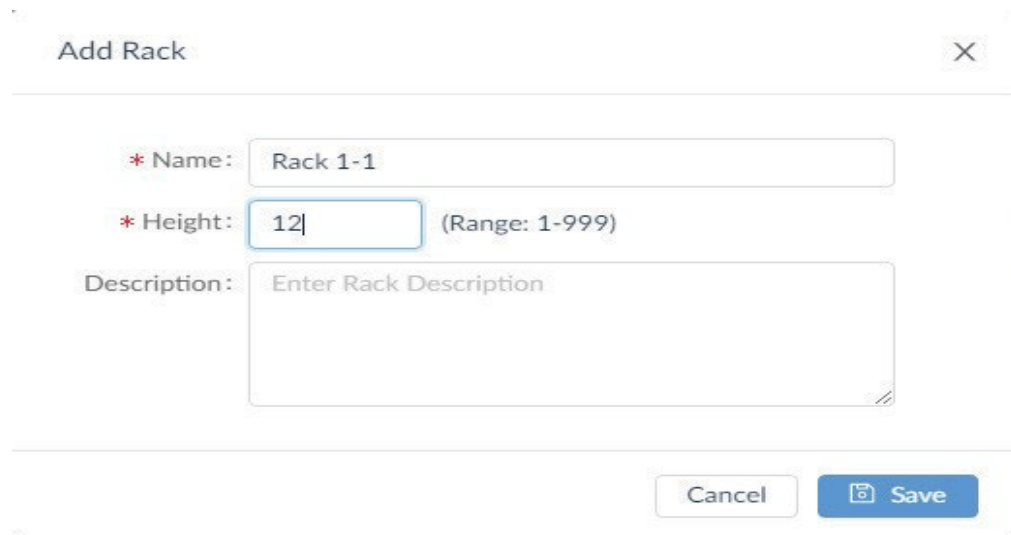


Figure 203 Adding a Rack to a Rack Group

7. Enter a name to identify the listing.
8. Enter the height value, a height of 1 equals 1 device. Range: 1 to 999.
9. Enter a description to identify the rack.
10. Click **Save** to create the rack. Click **Cancel** to return to the previous menu.

The create Rack Group page displays.

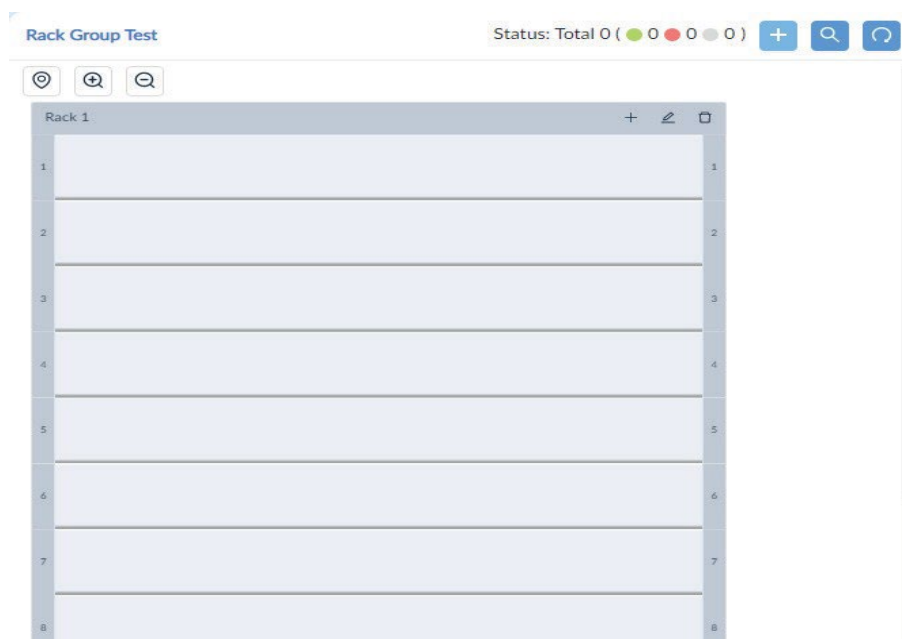


Figure 204 Viewing a Setup Rack Group

11. On the rack framework, click on a section panel to add a device.
The Available Devices page displays.
12. Select the device to insert into the panel.
13. Click **Save** to accept the selection.

The selected device is now inserted into the rack location.

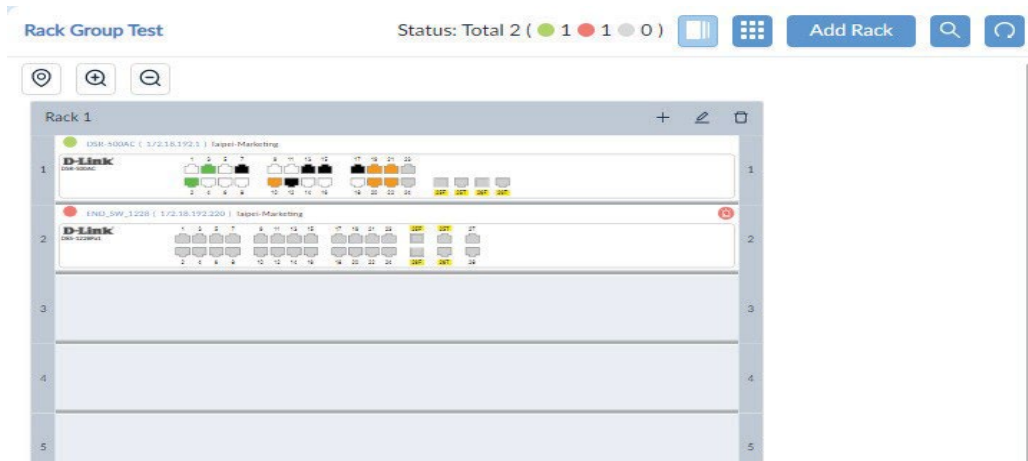


Figure 205 Device Selection in a Rack Group

9.2. View and Modify a Rack Group

You can modify and delete existing rack groups from a few different methods.

To modify an existing rack group:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Monitoring , click **Rack View** to display the Group List page.
3. Select an existing group.

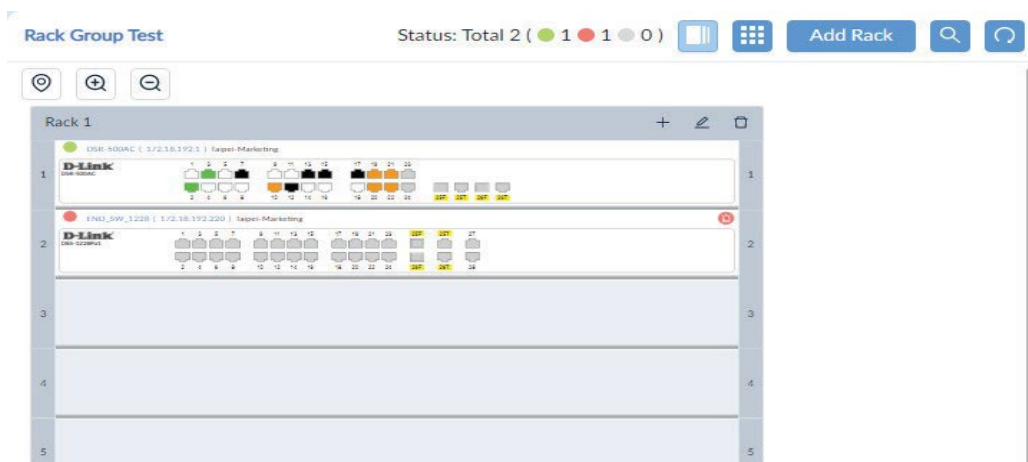


Figure 206 Viewing Group Lists

4. To edit the group settings, click on **Edit** in the Group List column. The Edit Rack Group information page displays. The listed information for the rack group displays.

Figure 207 Editing a Rack Group

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.

9.2.1.1. View and Modify a Rack

You can modify and delete an existing rack(s) from a group or delete multiple racks without deleting the group framework.

To modify an existing rack:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Monitor click Rack View to display the Group List page.
3. Select an existing group to view the included rack structures.
4. From the top right corner, click **Edit Rack** to modify the rack information.

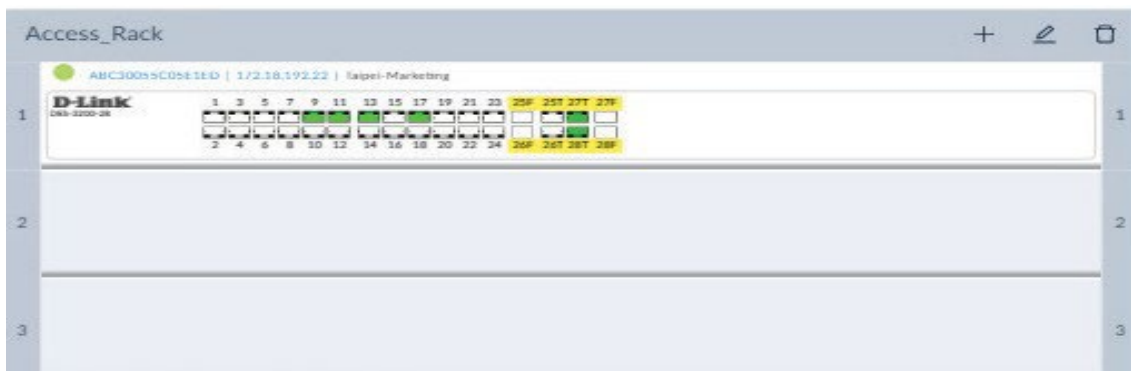


Figure 208 Viewing Rack Structures

5. Click **Save** to accept the new information.
6. By the same way, click **Delete** to remove the rack from the group.
7. Click **Yes** to confirm the process.



NOTE: Deleting a rack will delete all devices in the rack at the same time.

8. Viewing a close up or the full group structure is accomplished through the following:

- Default: click to set the viewing ratio to default
- Zoom in: click to enlarge the viewing area
- Zoom out: click to shrink the viewing area

Selecting a device on the rack will provide the following functions:

- View: click to display a complete view of the device and the related details
- Delete: click to remove the device from the rack entry

The order in which a rack is displayed can also be changed.

9. In the Rack Group page, click and hold anywhere on the rack outline and drag it to a new location. In this way, you can easily organize the order of the assigned rack structures.

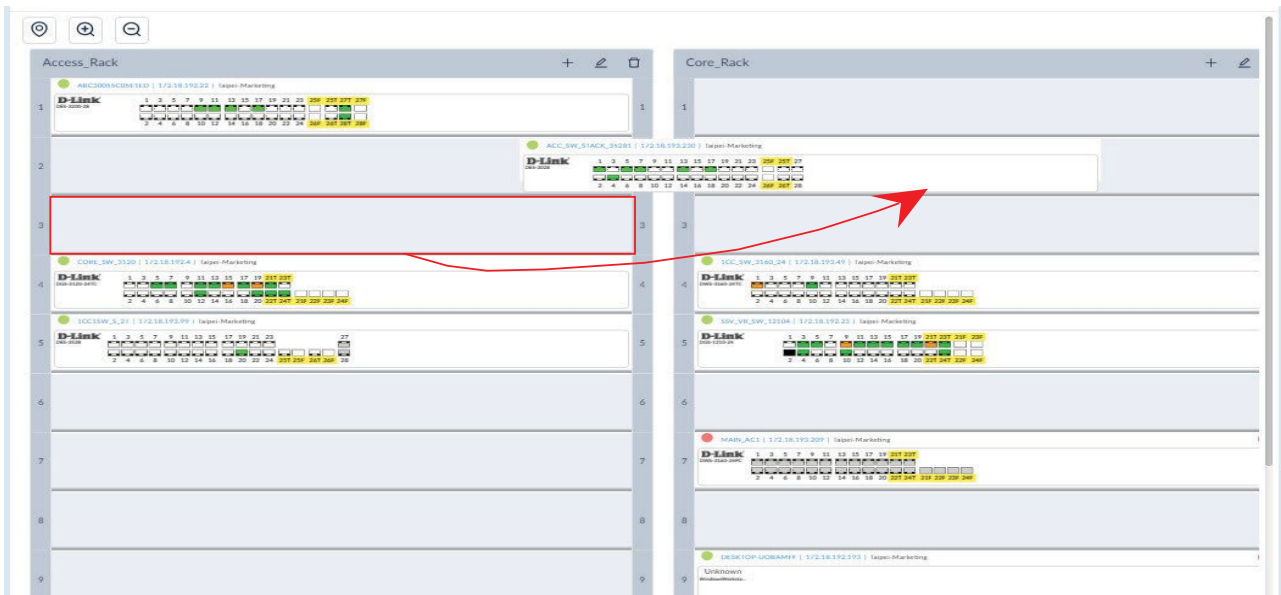


Figure 209 Ordering Assigned Rack Structures

9.2.1.2. View and Modify a Device in a Rack

You can view and change the location of the equipment panel by dragging and dropping in a new location on the rack.

To view an existing device:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Network Discovery, click **Rack View** to display the Group List page.
3. Select an existing group.

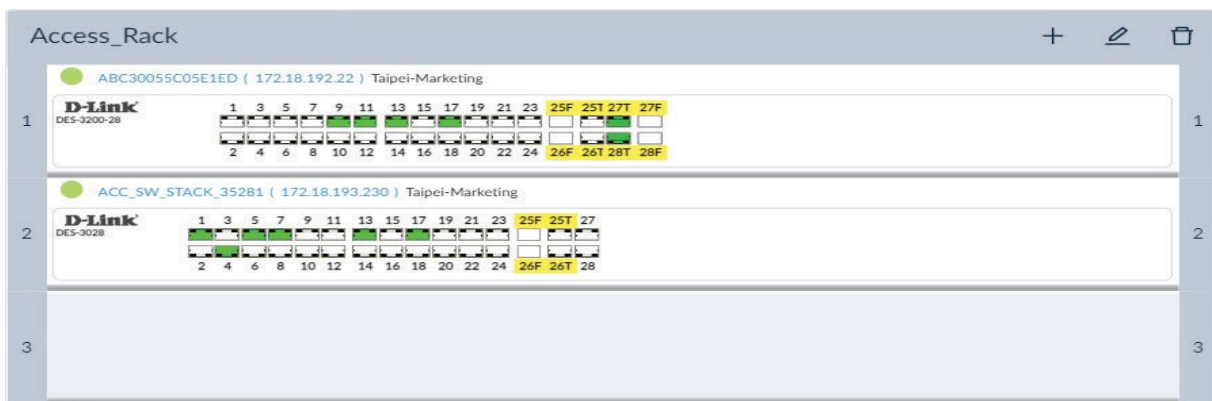


Figure 210 Selecting Existing Groups

4. From the rack view, click on a device space.



Figure 211 Selecting a Device Space

The View and Delete icons display.

To view the device information:

5. Click **View** to display the device Panel Details page. Device details are dependent on the device type. The following is an example of a D-Link DWS device.

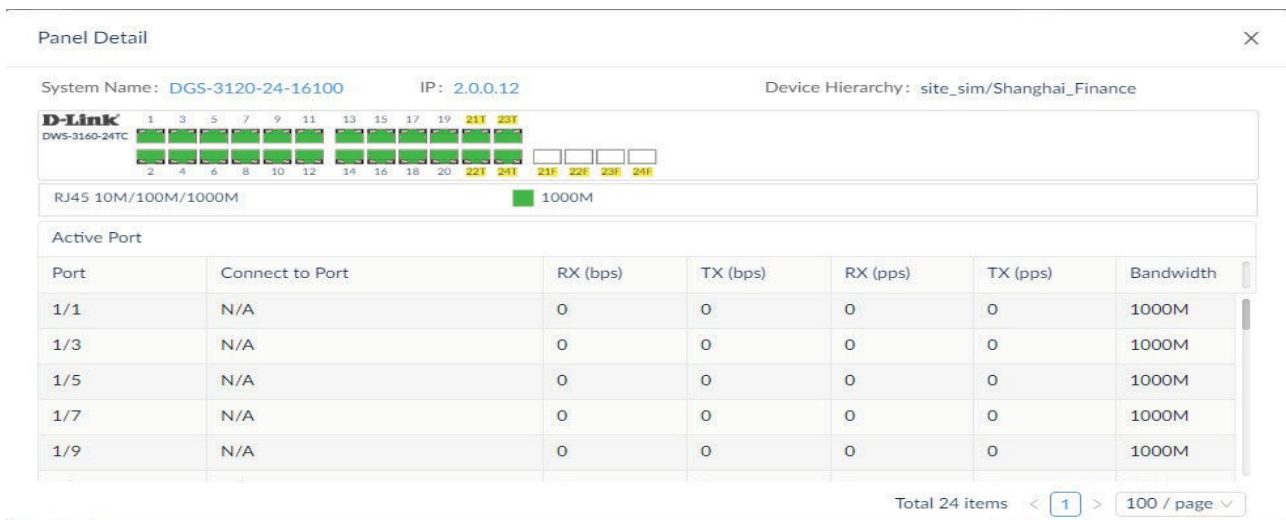


Figure 212 Viewing Device Details

6. Mouse over any of the connected (green) ports to view port details, see the following figure.

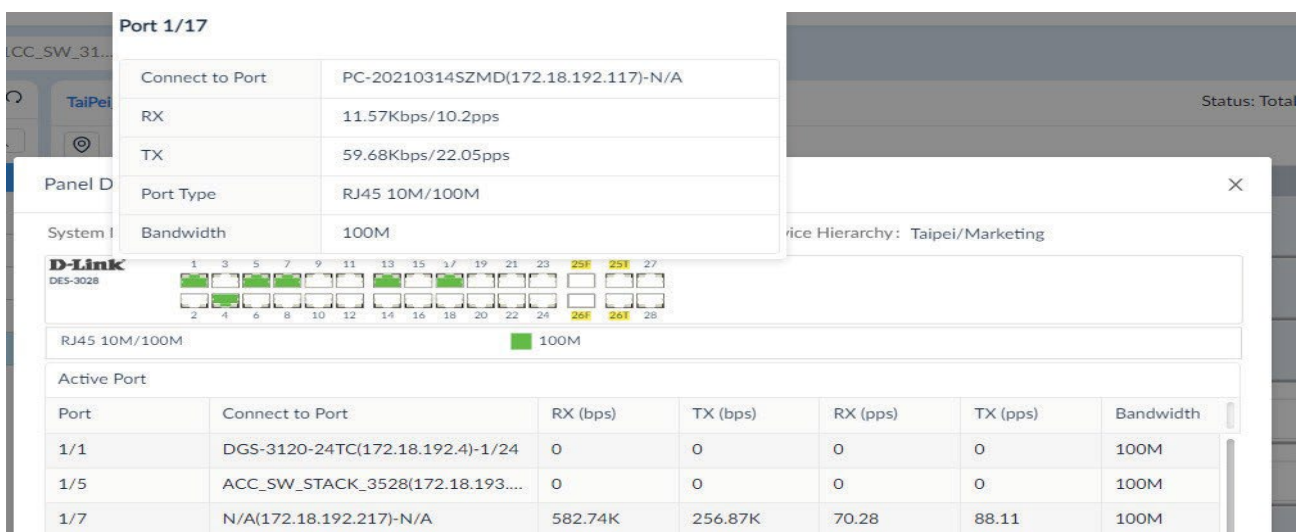


Figure 213 Viewing Port Details

7. Click on the **IP address** to open the device interface through one of the following protocols: HTTP, HTTPS, Telnet, or SSH.
8. Click on the **System Name** to open the device's panel details page.

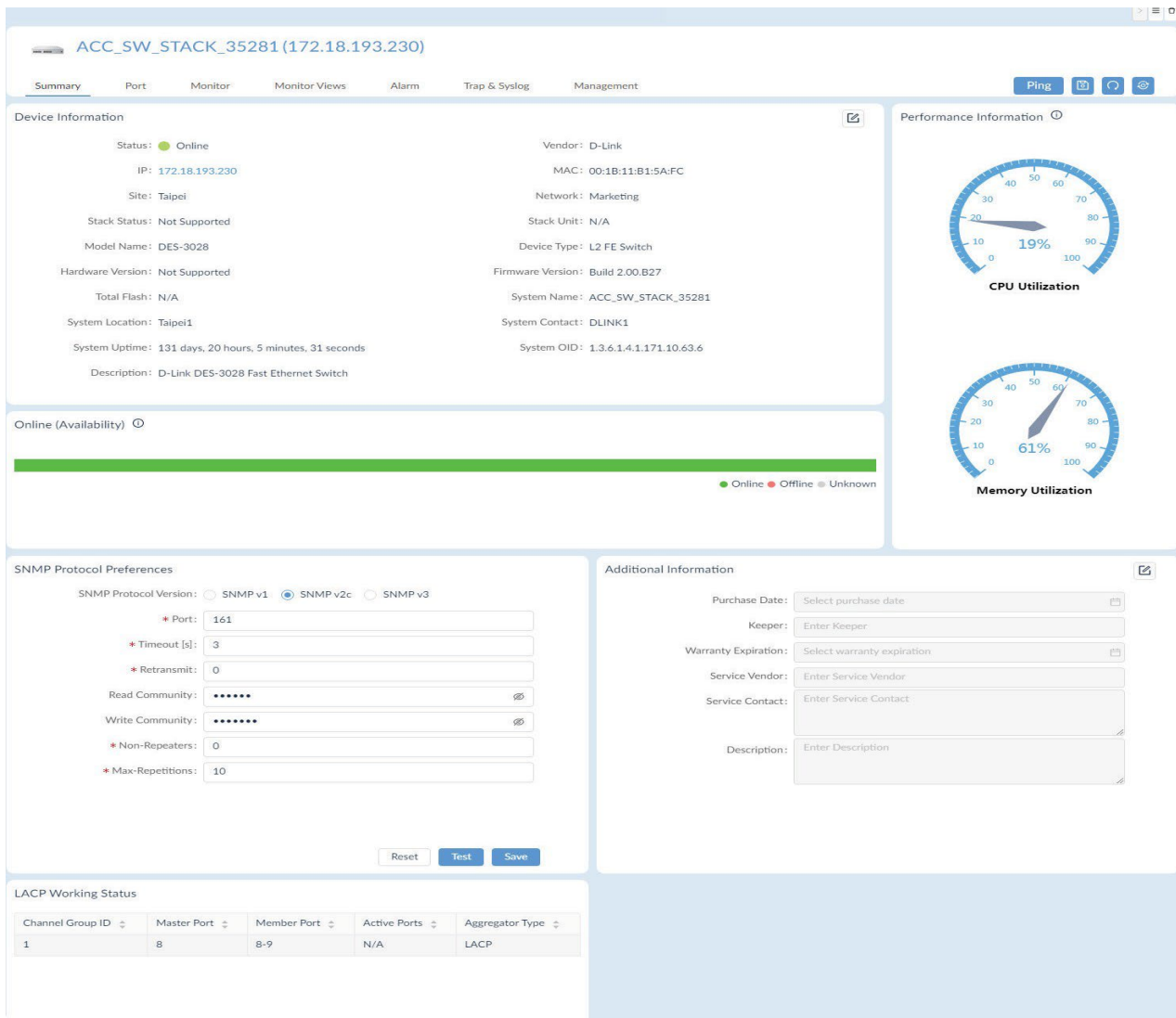


Figure 214 Viewing Device information

The following table describes the information available through the Device Information window.

Item	Description
Summary	
Port	Click to display the Port List overview page. The following information categories are available: Monitor, Comparison, and Alarm Settings.
Monitor	Click to view a graphical representation of the CPU, memory, and response time metrics collected. The information can be segmented by Hour, Day, Week, Month, or Quarter. Monitor Settings: click to select/deselect specific metric to monitor. The following categories are available: 802.1Q VLAN, Baseline, CPU Utilization, Device Common Information, LACP, LLDP, Memory Utilization, RMON Status, Response Time, SNMP Status, SSH Status, STP Status, Safeguard Status, Syslog Status.
Monitor Views	Click to view monitoring information in a topological format, includes: Rack View, System, and Customized topology.
Alarm	Click to view the active or resolved (historical) alarm events. Alarm Settings: click to select/deselect Monitor events triggers or view Trap and Syslog entries.
Trap & Syslog	Click to view the trap and syslog entries.
Management	Click to view and configure device settings and tasks, and manage firmware and configuration files.

Item	Description
Ping	Click to display the ICMP ping menu.
Save	Click to save the updated settings to the device.
Refresh	Click to sync the device and panel information.
Reboot	Click to reboot the device.
Device Information	<p>Displays an overview of the device information.</p> <p>Edit Device Information:</p> <ul style="list-style-type: none"> Click 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 metrics for the device's CPU and memory usage.
Online (Availability)	Displays the online status of the equipment in the past 24 hours.
SNMP Protocol Preferences	<p>Set the SNMP settings for the device. "Adding an SNMP Credential" on page 65.</p> <ul style="list-style-type: none"> Click Reset to discard any setting updates. Click Test to initiate the setting updates and confirm them. Click Save to accept the setting updates.
Additional Information	Click Edit Additional Information to include further device details.
LACP Working Status	Provides a graphical representation of the Link Aggregation Control Protocol (LACP) data.
Hardware Health	Provides a chart view of the operational status of the device's fan, power supply, and temperature.

To manage device panels on a rack:

See "View and Modify a Rack" on page 148 for further details.

In the same manner, rack organization is easily managed by dragging defined racks and placing them in a new location.

To delete the device:

1. Click **Delete** to remove the device from the rack space.
2. A pop-up page displays. Click **Yes** to confirm the process.

10 Manage sFlow

sFlow is only supported in the Enterprise version. The sFlow sampling technology is designed for high-speed switched networks for network usage visibility. The sFlow agent sends data to D-View 8 enabling network administrators to quickly obtain:

- Detailed real-time data usage related to interfaces, protocols, sources and destinations, including thresholds
- Traffic flows for all ports including Gigabit-speed ports
- Issues and abnormal traffic including cause indicators
- Traffic designated as a potential security threat
- Performance optimization information
- Billing and accounting

D-View 8 sFlow system provides the continual monitoring function for all network conditions, which includes network performance reporting.

This section includes the following:

- Configuring sFlow Monitor
- Manage sFlow Monitor
- sFlow Network Monitor
- View and Export sFlow Monitoring Results
- Manage sFlow Without Associated sFlow Templates

10.1. Configuring sFlow Monitor

To configure the sFlow Monitor:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Select Monitoring > Device View. In the Device View page, click the **Managed** tab and select sFlow from the Switch-All drop-down menu.

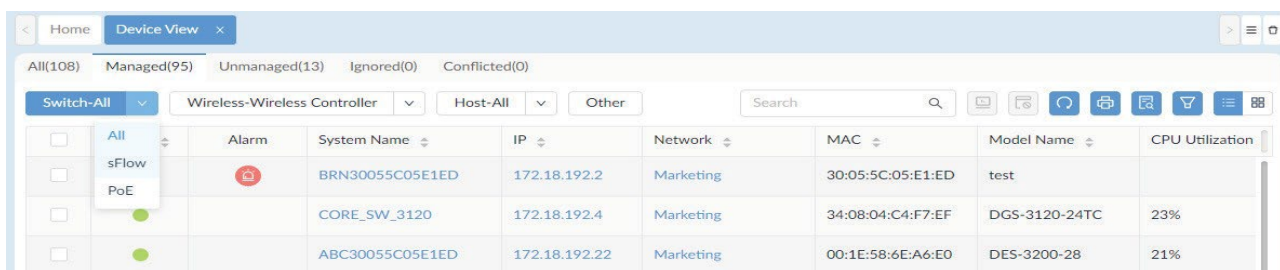


Figure 215 Selecting Switch-sFlow

The Switch-sFlow table overview displays.

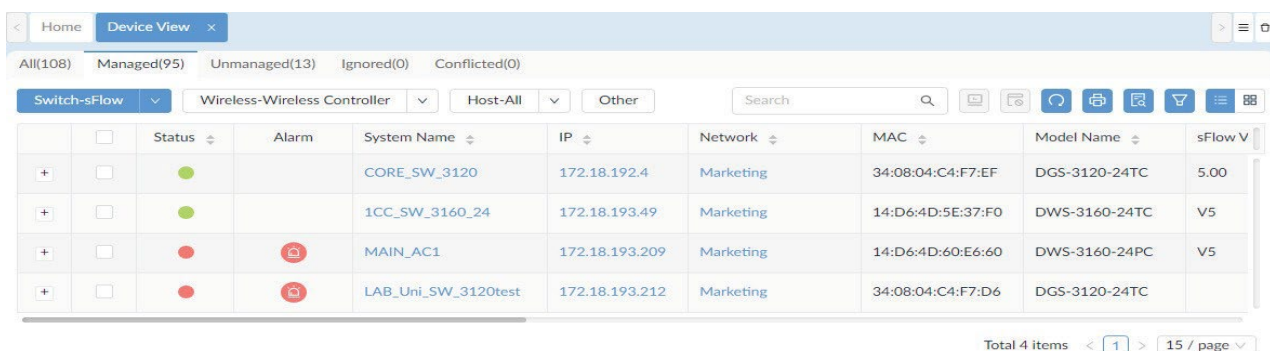


Figure 216 sFlow Overview

3. Select an available device by clicking on the System Name. The Device Information page.

4. Click the **Management** tab to view the device's sFlow settings

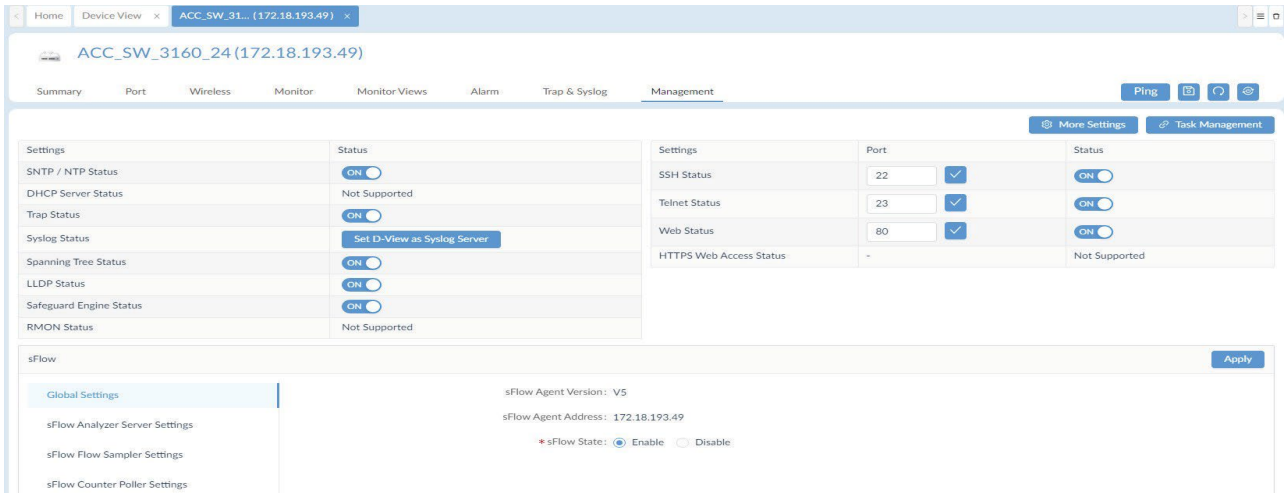


Figure 217 Device sFlow Settings

5. In the sFlow panel, locate the **Global Settings** tab and select it.

6. Locate sFlow State and select **Enable** to set the sFlow function.

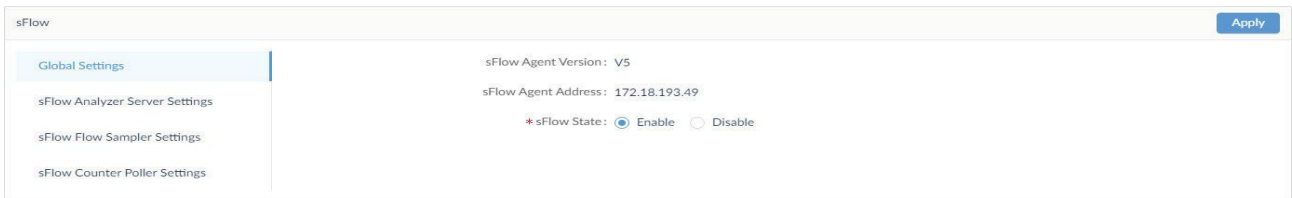


Figure 218 Configuring sFlow Function

7. In the sFlow menu, click **sFlow Analyzer Server Settings**.

8. Click **Add Analyzer Server Settings**. The Add Analyzer Server option is displayed in the frame.



Figure 219 sFlow Analyzer Settings

9. Click **Add Analyzer Server** to display the Add Analyzer Server page.

10. To configure the settings, enter the following information.

Add Analyzer Server X

* Server ID: (1~4)

* Owner:

* Timeout (CCT): (1~2000000) Infinite

* Address Type: v

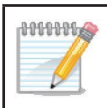
Collector IPv4 Address:

* Collector Port: (1~65535)

* Max Datagram Size: (300~1400)

Figure 220 Configuring Analyzer Server

Item	Description
Server ID	Click the indicator to assign an ID to the entry (1 – 4).
Owner	Enter the destination IP address which will be used by the device to send the sFlow data. Typically, this setting points at the D-View 8 probe server IP.
Timeout (CCT)	Enter the variable to define the controller configuration tool timeout (1 ~ 2000000). 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 relevant IP address designated to receive sFlow record packets.
Collector Port	Enter the port number correlating to the collector address as previously defined.
Max Datagram Size	Enter the variable designating the maximum datagram size (300 – 1400).
Cancel	Click Cancel to return to the previous menu without saving the settings.
OK	Click OK to create the sFlow setting.



NOTE: Settings marked with an * are required.

- Click **sFlow Flow Sampler Settings**. Configuring this setting allows for the sampler method to collect data. The following page displays.
- Click the **Add Flow Sampler Port**. The Add Flow Sampler Port page displays.

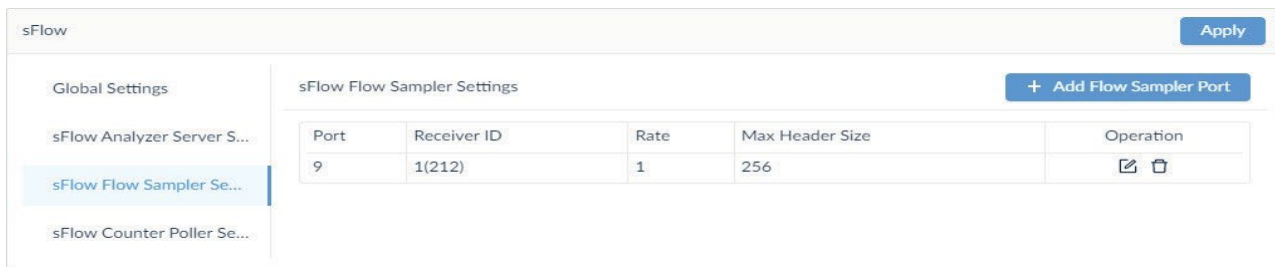


Figure 221 Configuring sFlow Sampler Port

- To configure the settings, enter the following information.

Figure 222 sFlow Sampler Port Overview

Item	Description
Port	Enter the port number (1 – 24) on the device designated to send out sFlow data.
Receiver ID	Click the drop-down menu to select a pre-configured analyzer server, see the previous step.
Rate	Enter the variable (0-65535) to define the ratio of frames passing through the data source.
Max Header Size	Enter the variable to designate the maximum number of bytes (18- 256) to be copied from a sampled packet to sFlow datagram.
Cancel	Click Cancel to return to the previous menu without saving the settings.
OK	Click OK to create sampler setting.

- Click **sFlow Counter Puller** Settings. Configuring this setting allows for the counter method to collect data. The following page displays.
- From the Management page, click **Add Counter Puller Port**.



Figure 223 sFlow Counter Puller Settings

The Add Counter Puller Port page displays.

To configure the settings, enter the following information.



Figure 224 Configuring Counter Poller Port

Item	Description
Port	Enter the port number (1 – 24) on the device designated to send out sFlow data.
Server ID	Click the drop-down menu to select a pre-configured analyzer server, see the previous step.
Polling Interval	Click to set the counter interval for polling.
Disabled	Select to enable (default) or disable the polling function.
Cancel	Click Cancel to return to the previous menu without saving the settings.
OK	Click OK to create the counter puller port setting.

- Click **OK** to save the Counter Puller Port settings.
- Click **Apply** from the sFlow pane to accept the new sFlow configuration.

10.2. Manage sFlow Monitor

To configure the sFlow Monitor:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Click **Monitoring > Device View**.

The Monitoring Dashboard overview displays

- Click the **Managed** tab and select sFlow from the Switch-All drop-down menu. The Switch-sFlow table overview displays.
- Select the target device by clicking on the System Name. The device’s summary overview displays.
- Click the **Management** tab to view the device’s sFlow settings.

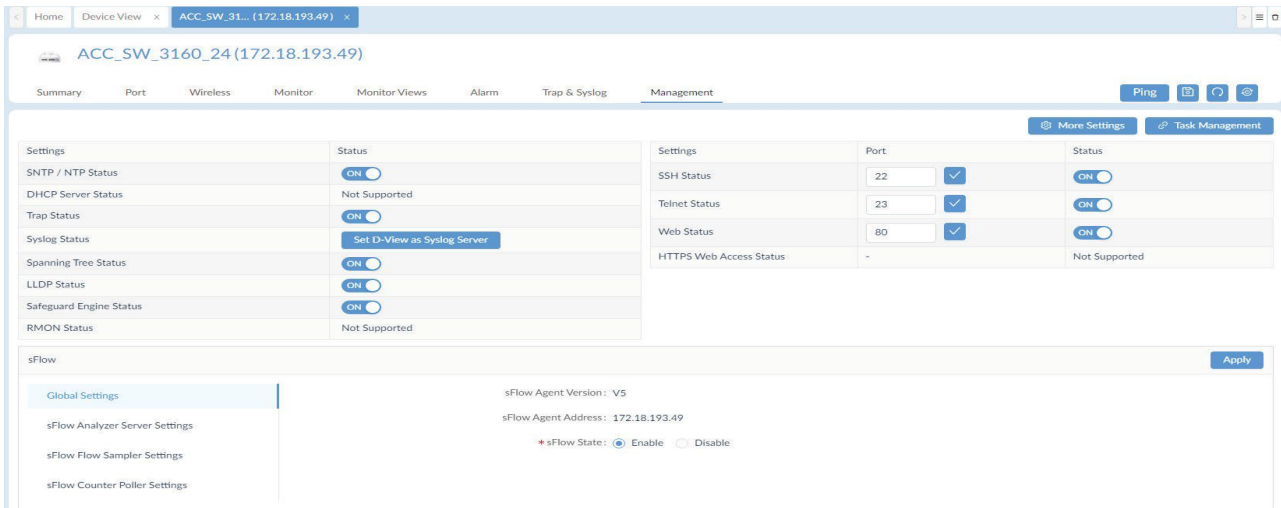


Figure 225 sFlow Management Settings Overview

6. In the sFlow menu, click sFlow Analyzer Server Settings.

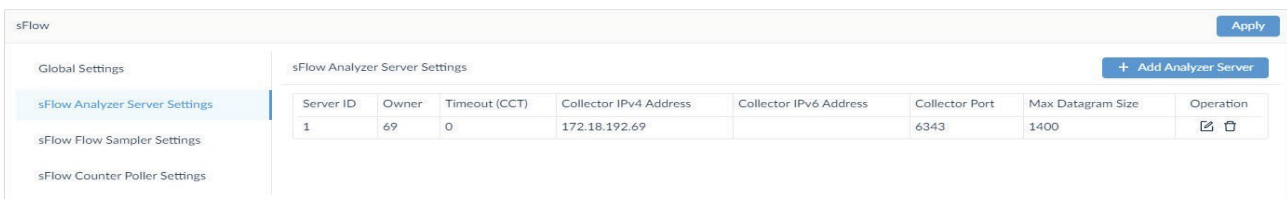


Figure 226 sFlow Analyzer Server Settings

7. The Settings page lists pre-configured servers. Locate the Operation category, the following options are available.

- Edit allows you to modify the existing settings.
- Delete removes the entry from the list. Click Delete and confirm the deletion of the entry.

8. Click the **Edit** or **Delete** icon to manage the server.

In the same way, the Sampler Settings and Counter Puller Settings can be managed.

10.3. sFlow Network Monitor

Once properly configured, the sFlow function allows for the monitoring of the network through the collected data.

To configure the sFlow monitoring settings:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click Monitoring > sFlow Analyzer.
The sFlow Analyzer overview displays. The results of the sFlow analysis can be viewed based on a specific category.
3. Click a menu from the tab bar to view the related settings:
 - Source
 - Destination
 - QoS
 - Application
 - Conversion

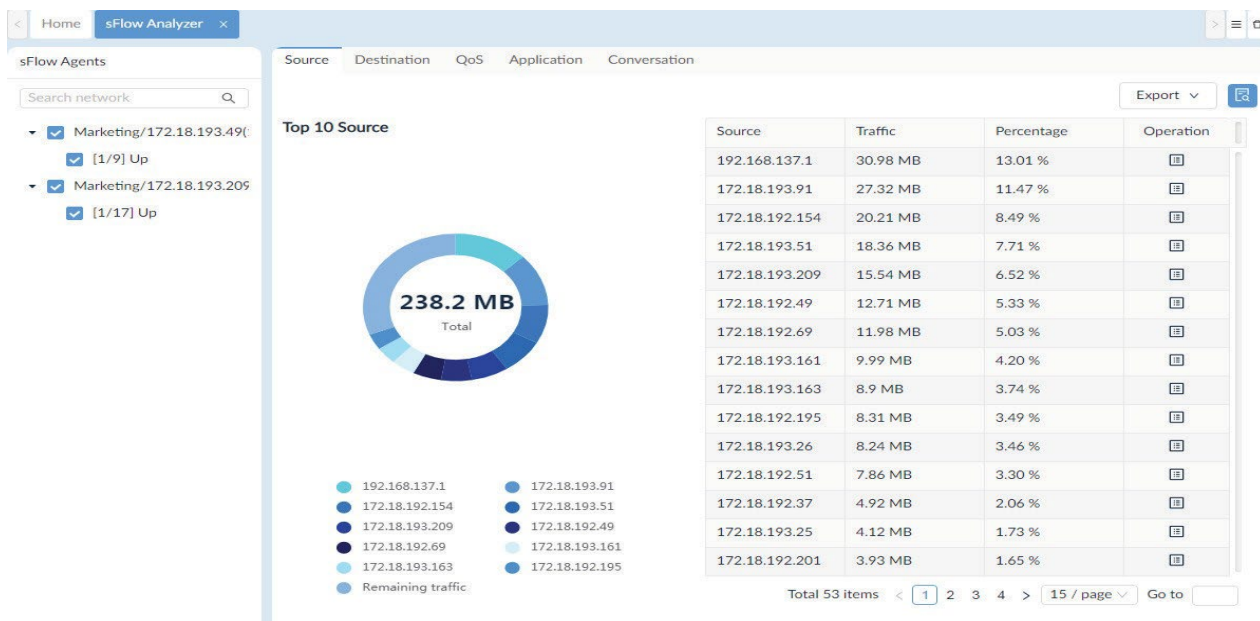


Figure 227 sFlow Analyzer Monitor Overview

- By clicking on the Advanced Query icon, you can set filter conditions to display different time interval charts.
 - Enter specific query information in the following fields.
 - Select the sFlow direction: Ingress, Egress, Ingress and Egress.
 - Slide the Resolve DNS to enable or disable the option.
 - Click the drop-down menu to display the identifier type: IP or MAC address.
 - Click Search to start the query process or Clear to refresh the screen.

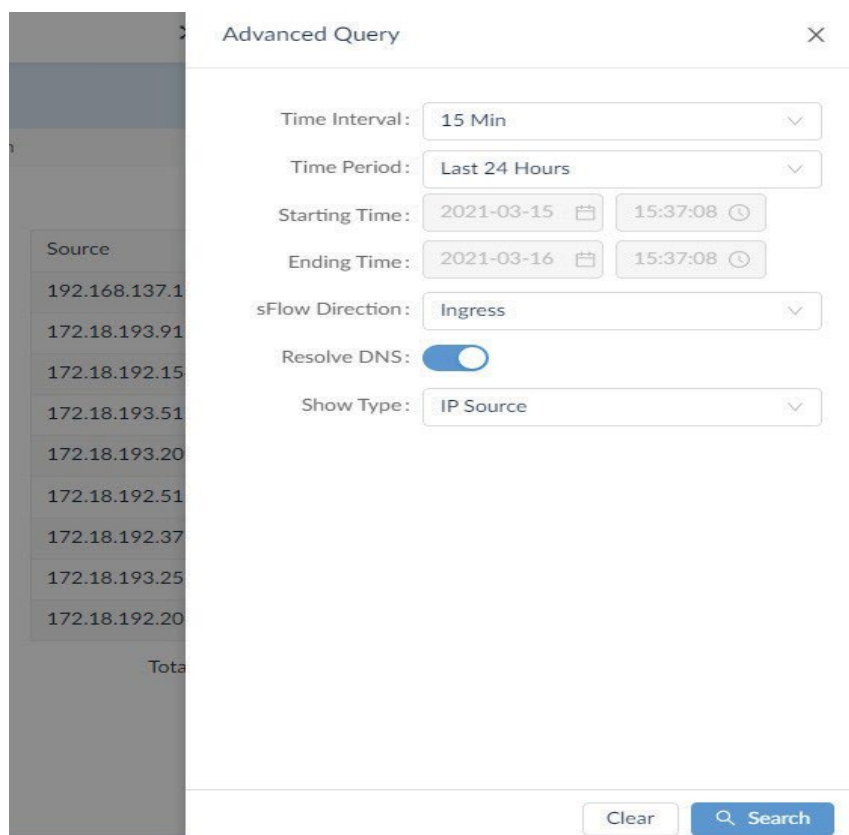


Figure 228 Filter Conditions Overview

- In the sFlow menu, click sFlow Analyzer Server Settings

10.4. View and Export sFlow Monitoring Results

After specifying sFlow sources, and traffic is present through the sources, the results of sFlow monitoring can be viewed through the interface.

The D-view 8 provides the following details and options in the results:

- Source: You can select to display the source device. By default, the application displays information about the top 10 sources.
- Destination: You can select to display the destination address. By default, the application displays information about the top 10 destinations.
- QoS: You can select to display the top 10 QoS.
- Application: You can select to display the application usage. By default, the application displays information about the top 10 applications.
- Conversation: You can select to display the conversation list between devices.

To view the results of sFlow monitoring:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click Monitoring > sFlow Analyzer.
The sFlow Analyzer overview displays.

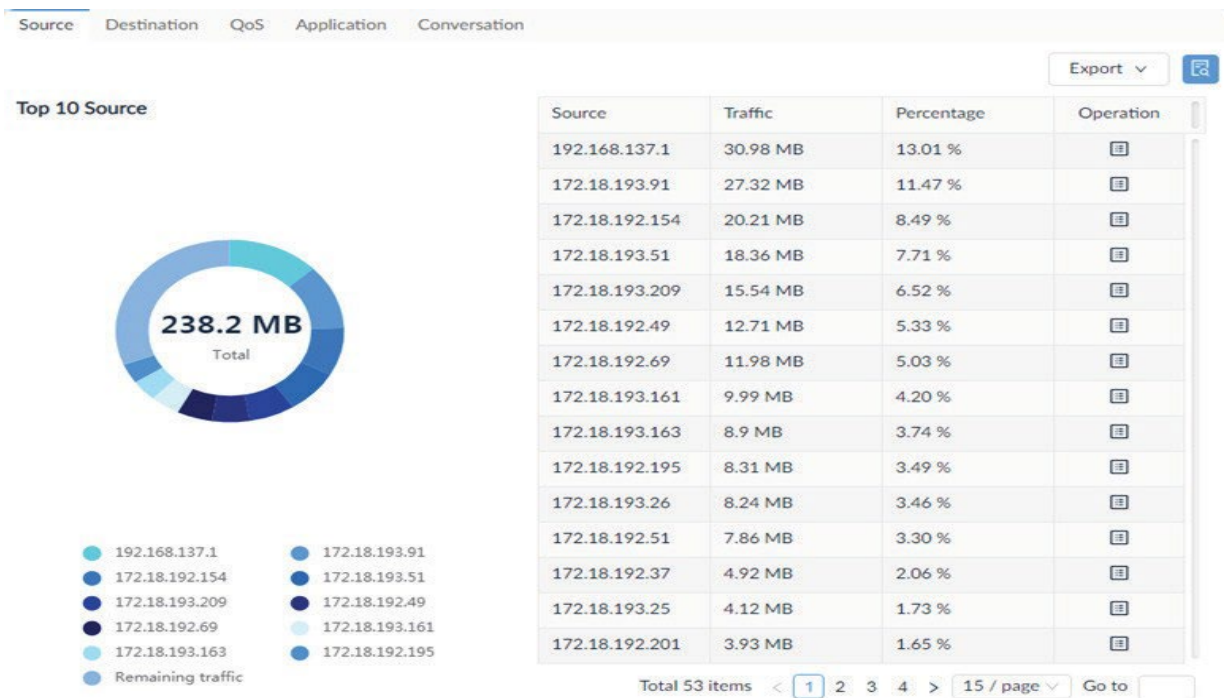


Figure 229 sFlow Monitoring Results Overview

3. Select the corresponding tab to select. The related sFlow data displays.
4. From the top right corner, click the drop-down Export menu and select from the following to export the listed data:
 - PDF
 - Excel
 - CSV

The data is saved to the default downloads folder of your browser.

The sFlow source data is available on display as well as to a saved file.

10.5. Configure sFlow in Supported Devices

D-View 8 can easily help you to manage devices which support sFlow configuration. sFlow management can take place without the use of an associated template by simply following configuring the device through the sFlow Agent function.

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click Monitoring > sFlow Analyzer.
The sFlow Analyzer overview displays.
3. From the sFlow Agent’s column, locate the hyperlink **Click Here to Add**.

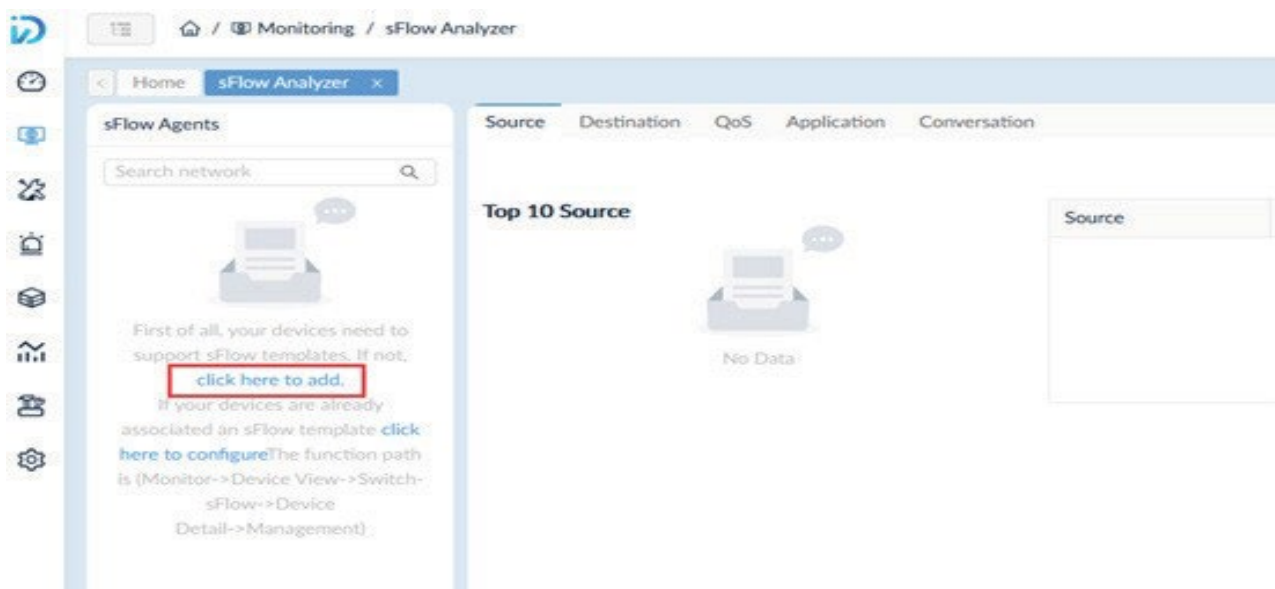


Figure 230 Configuring sFlow Analyzer Template

4. Alternatively, you can click Template and select the Configuration Template tab. The Template List page displays.

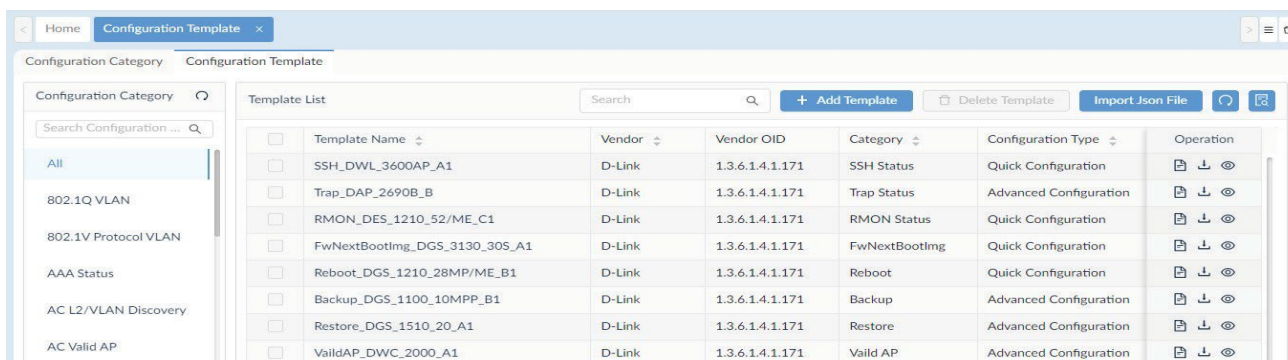


Figure 231 Viewing sFlow Analyzer Template

5. Click the **Add Template**. The Template Settings page displays.

Figure 232 Template Settings

From the template settings, you can setup the template and include features such as setting up a layout and adding basic components such as labels, input fields, button, text areas, and tables.

Figure 233 Configuring Template Settings

6. Once the template is setup and configures, click **Preview** to view a live version.
7. Click **Cancel** Preview to return to the settings menu.
8. Click **Save** to add the template to the library or **Cancel** to return to the previous menu.

Once the sFlow configuration template is created, you need to associate it to a related device template to configure the sFlow parameters.

10.6. Configure sFlow Via CLI

This section provides information on how to configure sFlow via CLI.

To add a sFlow configuration template using CLI:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Click Tools > CLI.
The CLI overview displays.
3. From the Session List column, select an existing session to open the CLI command interface, or add a new session. For demonstration purposes, the session Main_AC1 is used.
4. Click **Connect** to start the CLI session. The session page displays.

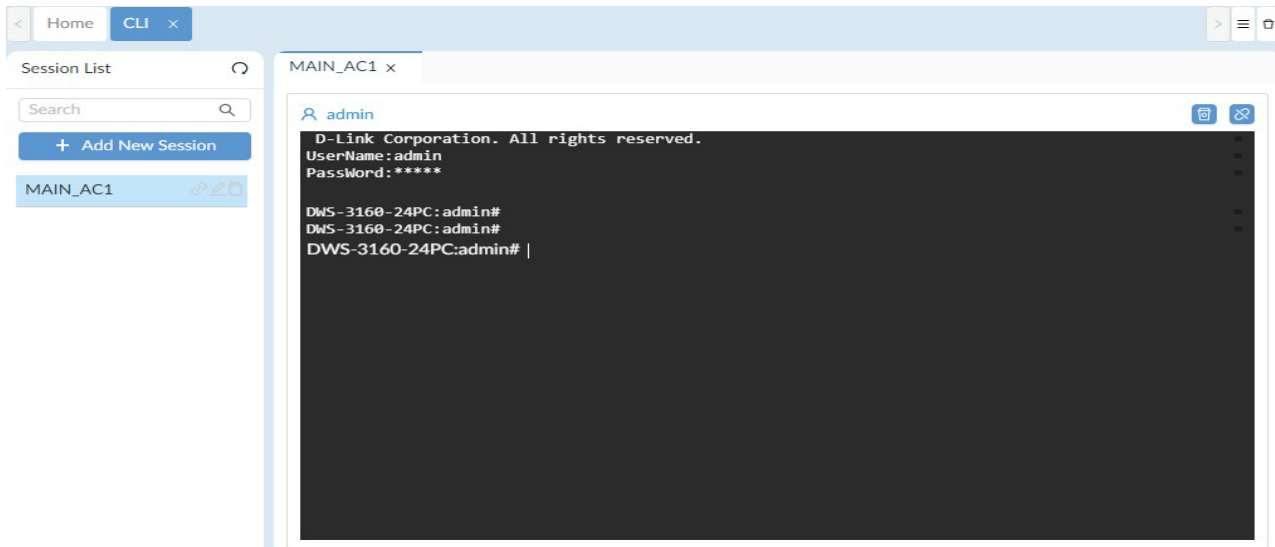


Figure 234 Starting CLI Sessions

The following guidelines provide instructions to help you configure the template settings.

Instructions:

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 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 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
```

7. To refresh the screen, click **Clear**.
8. Otherwise, click **Disconnect** to end the session.

11 View and Generate Reports

Reports are available as either built-in templates or customized ones. They can be viewed and generated as required as a one time-report or scheduled.

To generate a scheduled report:

- Manage Report Templates
- Generate Scheduled and My Reports

11.1. Generate Scheduled and My Reports

Scheduled reports are generated through existing report templates. You can create One Time or Recurrent reports that are generated immediately or scheduled to generate automatically.

To generate a scheduled report:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Reports, click **General Reports** to display the General Reports page.
In order to create a scheduled report, an existing report must be present. See Add a Report Template for further details.
3. Select a specific category from the reports list: Device Reports, Wired Interface Reports, Wireless Reports, or Advanced Reports.
To demonstrate, the Wired Traffic category is selected and the existing report also displays.

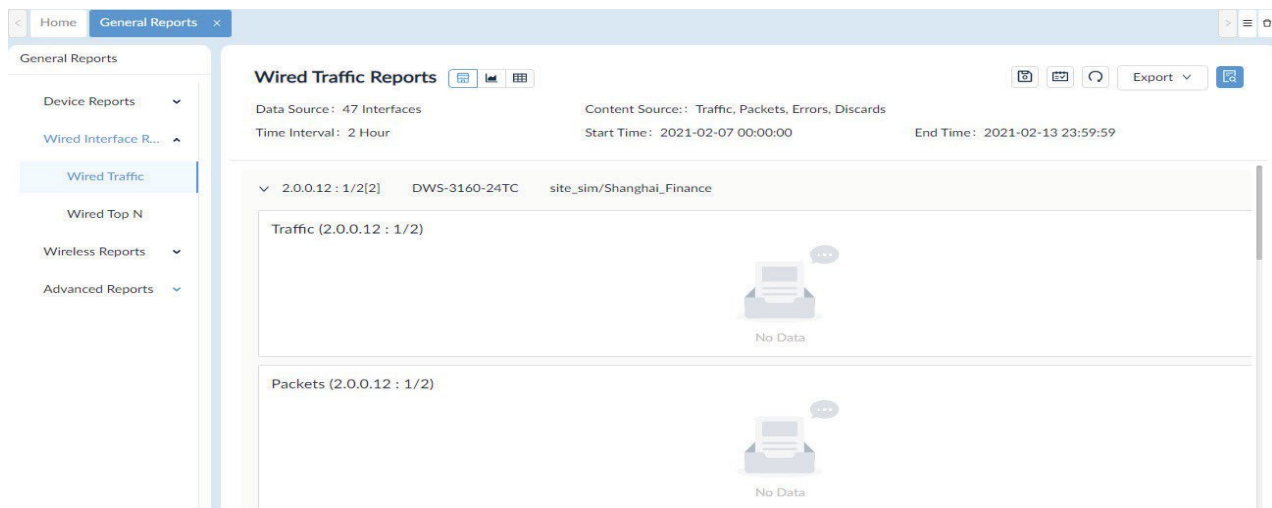


Figure 235 Wired Traffic Reports Display

4. At the top right of the frame, click **Upgrade to Scheduled Reports**. Alternatively, you can click **Save to My 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:

Schedule Type: One Time Recurrent

* Specify Generation Time:

Cancel OK

Figure 236 Upgrading to Scheduled Reports

If **My Reports** is selected, the **Save to My Reports** page displays.

NOTE: 500 reports per user can be created to maintain optimal system performance. Exceeding the limit results in the deletion of entries based on FIFO rules.

5. Enter the required information:

- Report Name: enter the name of the report
- Description: enter a descriptive statement to identify the report
- Schedule Type: select the schedule cycle for the report, One Time or Recurrent.

For recurrent schedules, select a defined time period from the Schedule list.

- Specify Generation Time: if One Time is selected, the period to enable the task is defined through the calendar pop-up page.

6. Click **OK** to generate the scheduled report. Click **Cancel** to return to the previous menu.

The scheduled report is successfully created.

7. Select Scheduled Reports under the Reports menu to view the created report schedule. If the report is defined as One Time, it appears under the default menu. If it is recurrent, click the **Recurrent** tab to view the report.

One Time Recurrent

You can create up to 500 reports. 57 reports created, 443 remain.

Enter Report Name

Report Category	Report Name	Data Source	Content Source:	Created By	Time Created	Result	Operation
Wired Traffic	Device Health Report Demo	48 Interfaces	Traffic, Packets, Errors, Discards	admin	2021-02-11 10:26:20	Waiting for generation	

Total 1 items < 1 > 100 / page

Figure 237 Report Schedule Overview

To view the My Reports listing, select my **Reports** and click **My Reports**.

- View and Remove Reports

11.2. Manage Report Templates

The D-View 8 provides built-in report templates for the supported devices. You can generate reports based on the device type. You can also add new reports using existing templates.

The following figure illustrates the default template along with the types of reports available.



Figure 238 Available Reports Overview

Report	Type	Category
General Reports	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	One Time Reports	
	Recurrent Reports	
My Reports	Customized Reports	

11.2.1. Add a Report Template

There are numerous templates for specific situations. 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. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Reports, click **General Reports** to display the General Reports page.
3. Select a specific category from the reports list:

Device Reports, Wired Interface Reports, Wireless Reports, or Advanced Reports.

The following provides an example to further demonstrate. For the example, the Device Health category is selected.

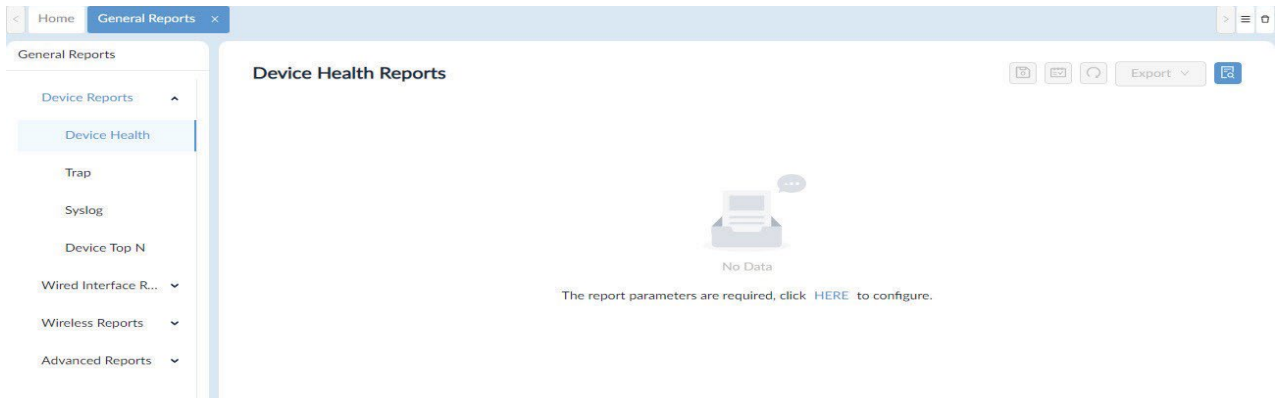


Figure 239 Device Health Template Overview

4. First time users need to configure the report parameters. Click **HERE** to configure the reports settings. The Report Settings page displays.

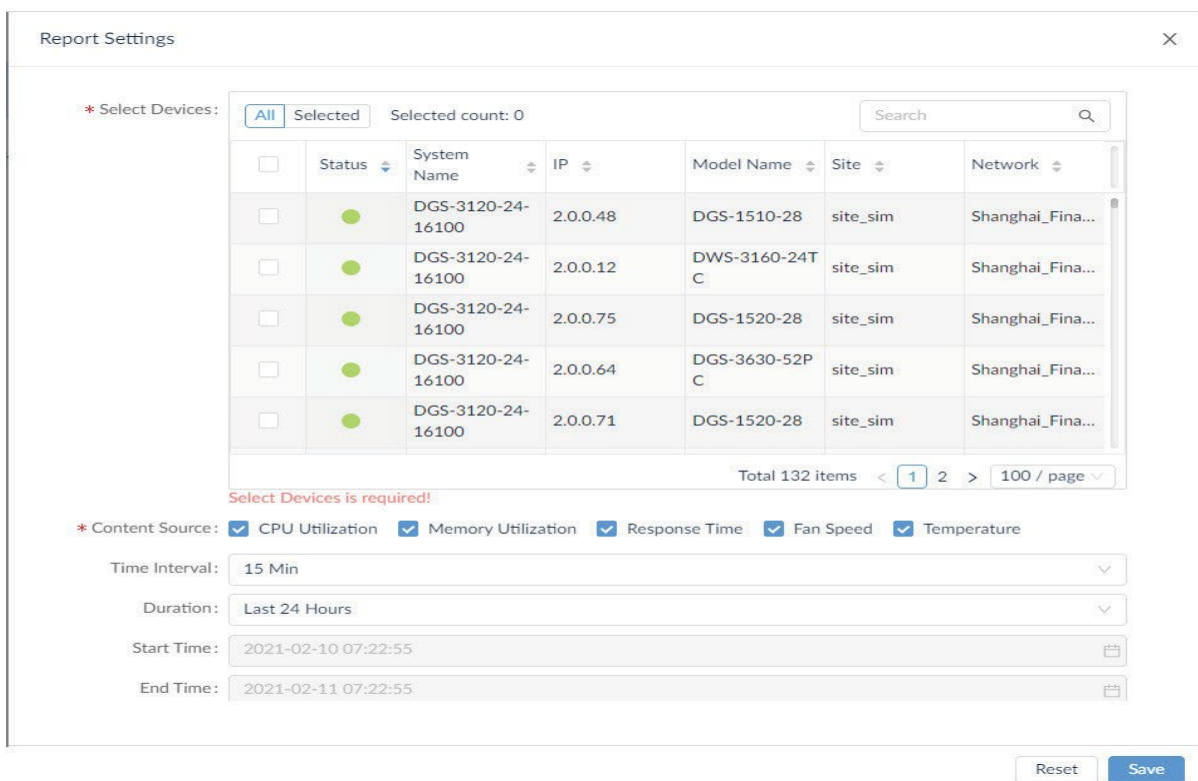


Figure 240 Configuring Report Parameters

5. Configure the following settings:

Item	Description
Select Device	Use the Search field to specify a device or scroll through the list to select available devices. Up to 15 devices can be grouped in a report.
Content Source	Click to select the source of the report data, CPU Utilization, Memory Utilization, Response Time, Fan Speed, Temperature.
Time Interval	Minimum interval configured, 15 min, 2 hours, 8 hours, 1 day
Duration	Click the drop-down menu to determine the lapsed duration of the record pool.
Start Time	Set the starting date if a customized duration period is selected.
End Time	Set the ending date if a customized duration period is selected.

6. Click **Save** to create the report. Click **Reset** to clear setting updates.

The report displays in the listings and includes any data acquired during the defined time period.



Figure 241 Configuration Report Overview

You can view the report data in the default format, chart, or table list.

At the top of the page, click the icon to designate the data view format.



11.2.2. Delete a Report Template

A report can be removed without deleting the template. However, the data generated by the report is deleted.

To delete or modify an existing report:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Reports, click General Reports to display the General Reports page.
3. Select a specific category from the reports list: Device Reports, Wired Interface Reports, Wireless Reports, or Advanced Reports.

To demonstrate, the Device Health category is selected and the existing report also displays.



Figure 242 Device Health Overview

4. At the top right corner of the frame, find the Report Settings icon. Click on it to open the report settings. The Report Settings page displays

Report Settings ×

* Select Devices: All Selected Selected count: 3 Search

<input type="checkbox"/>	Status	System Name	IP	Model Name	Site	Network
<input type="checkbox"/>	●	localhost	172.18.192.6	Other	CS	Beijing_Marke...
<input checked="" type="checkbox"/>	●	BRN30055C05 E1ED	172.18.192.2	Other	CS	Beijing_Marke...
<input checked="" type="checkbox"/>	●	devip8	172.18.192.9	Other	CS	Beijing_Marke...
<input checked="" type="checkbox"/>	●	Switc901tt	172.18.192.22	DES-3200-28	CS	Beijing_Marke...
<input type="checkbox"/>	●	N/A	172.18.192.15	DGS-1210-10	CS	Beijing_Marke...
<input type="checkbox"/>	●	dgs-1210	172.18.192.23	DGS-1210-24	CS	Beijing_Marke...
<input type="checkbox"/>	●	DESKTOP-TMR 5E73	172.18.192.131	WindowsWorks tation	CS	Beijing_Marke...

Total 132 items < 1 2 > 100 / page

* Content Source: CPU Utilization Memory Utilization Response Time Fan Speed Temperature

Time Interval: 8 Hour

Duration: Last 30 Days

Start Time: 2021-01-13 00:00:00

End Time: 2021-02-11 23:59:59

Figure 243 Report Settings Overview

- To modify the current report, re-configure the settings and click **Save**. The report is modified and is listed in the General Reports page.
- To remove the report, click **Reset**. You can click on the **Close** icon at the top right corner of the page or click outside the frame to return to the previous menu. The report is now removed from the General Reports page.

11.3. View and Remove Reports

All reports can be viewed for the period they are retained. All reports can also be removed from the three type of lists.

To remove a report:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Under Reports, click **General Reports** to display the General Reports page.
- To remove a general report entry, see Delete a Report Template for further information.

To remove a Scheduled Report, use the following information:

- Click **Scheduled Reports** to view the list of available entries.
- Select a One Time or Recurrent category.
- From the Operation column, click the **Delete this Report** icon to remove the report. The report is removed.

To view or remove an entry from My Report, use the following information:

- Click **My Reports** to view the list of available entries.
- From the Operation column, click the View icon to open the report details page.
- From the Operation column, click the **Delete this Report** icon to remove the report.
- The report is removed.

12 Manage Users and Security Profiles

Through the D-View 8 you can easily manage security profiles and the network user base.

The following information is available in this section.

- Profile Role Types
- Authentication Credentials
- Add a Profile
- Modify or Remove a Profile

12.1. Profile Role Types

The D-View 8 provides the following user role types:

- Super Administrator. The user can perform all functions across the entire organization.
- Organization administrator. The user can perform all administration functions, including the management of users and security profiles across the organization.
- Site administrator. The user can perform administrative functions such as monitoring user accounts.
- Network administrator. The user can perform all administration functions across a corresponding network(s).

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 Analyser	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 and Write
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
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
Alarmable item Definition	Read and Write	Read and Write	Not Available	Not Available
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
SNMP 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

12.2. Authentication Credentials

Access management and access rights are handled through the user profile and role. D-View 8 provides three systems for control of user permissions management to keep user information, roles, and related policies enforced. Profile authentication is configured by one of three protocols as listed in the following. See “1.10. User Authentication Types” on page 06 for further information.

- Local authentication
- RADIUS authentication
- AD authentication

12.2.1. Join an AD Server

You can join the D-View 8 application from the same deployment to an AD domain.

When you join a single AD node you will need the following:

- Domain name
 - Domain controller address
1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
 2. Under System, click User Management to display the User Management page.

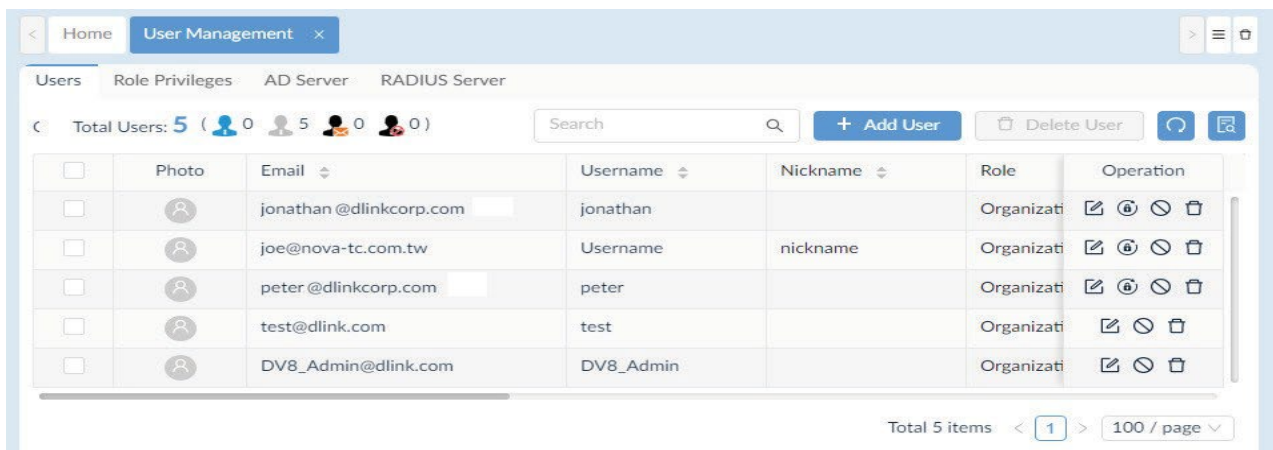


Figure 244 User Management Overview

3. From the tab menu bar, click AD Server to display the AD Server page.

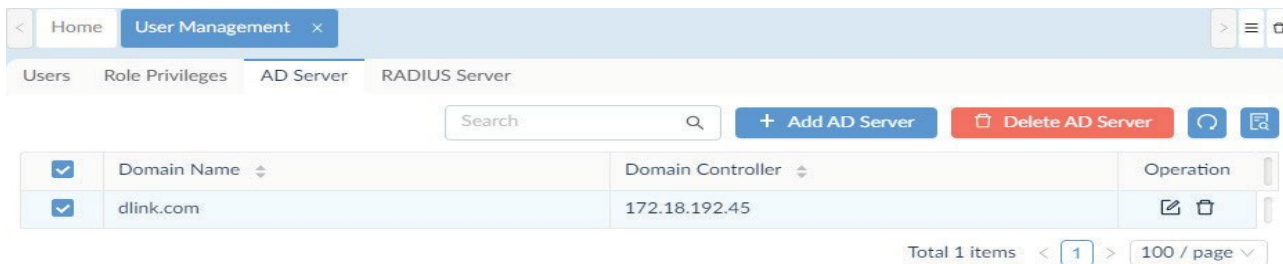


Figure 245 Ad Server Overview

4. Click Add AD Server.
5. In the Add AD Server page, enter the domain name and controller information associated with the AD server.

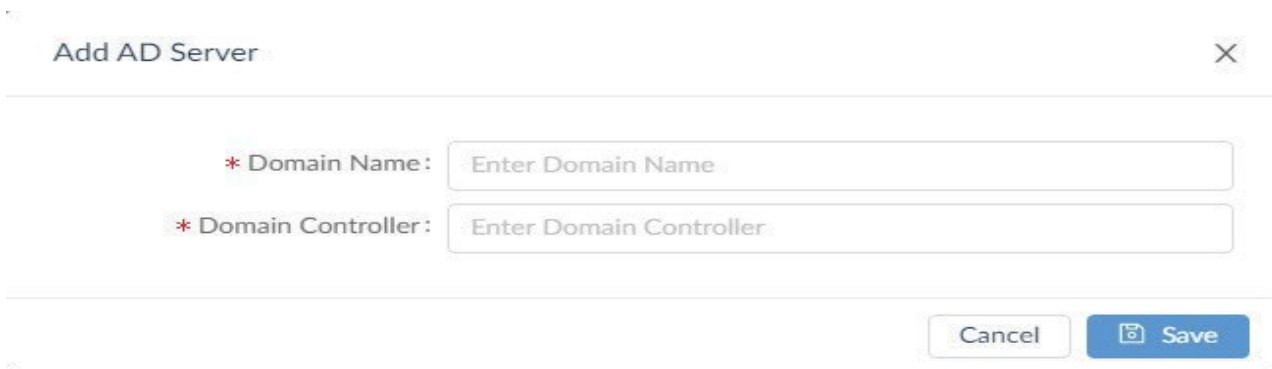


Figure 246 Configuring AD Server Settings

6. Click **Save** to accept the settings. Click **Cancel** to return to the previous screen. The new AD server entry lists in the main listings.

12.2.2. View and Remove an AD Server

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click User Management to display the User Management page.

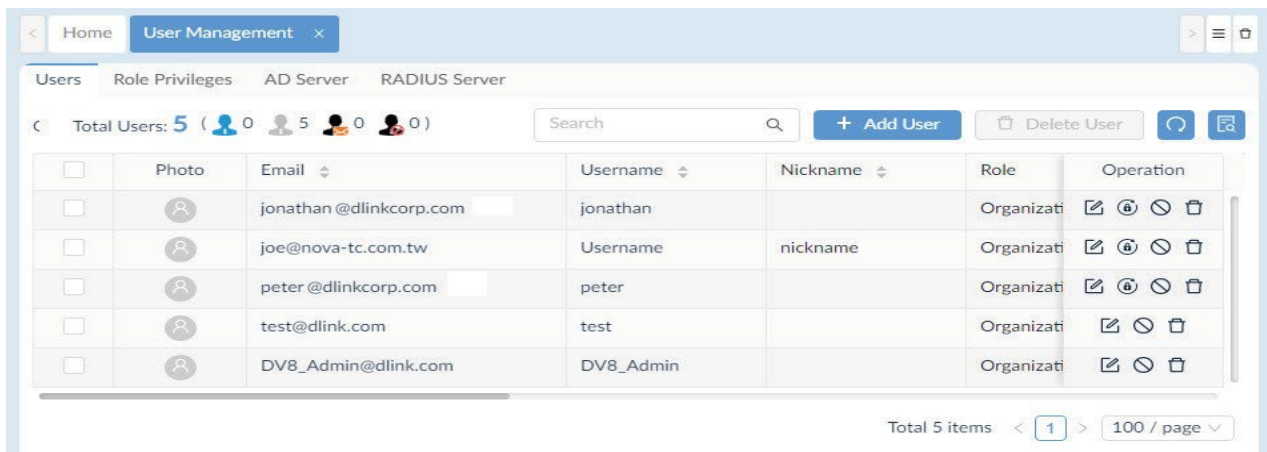


Figure 247 User Management Overview

3. From the tab menu bar, click AD Server to display the AD Server page.

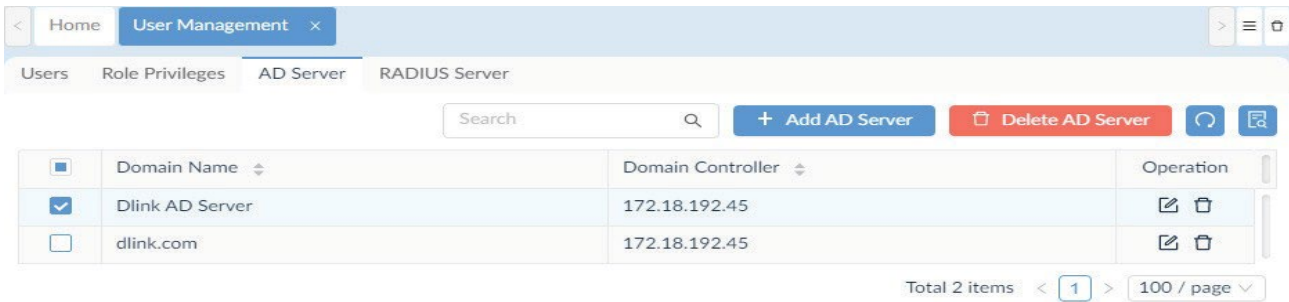


Figure 248 Selecting AD Server

To select a specific entry, you can use the Search function to discover entries by domain name or controller information. Alternatively, you can use the Advanced Query function to enter the correlating information.

Editing the settings on a defined entry is performed by the edit function.

Caution: Modifying or deleting an AD server may cause user login failures. Before proceeding, make sure all operations are saved and users have saved their related data to prevent loss of operation.

4. On the AD server entry, click the Edit button under Operation.

The Edit AD Server page displays.

5. Modify the settings and click OK to accept the new settings.
6. A pop-up confirmation page display. Click **Yes** to continue or **No** to return to the previous screen.

Deleting an AD server entry is performed by one of two methods.

7. To the right of the target entry, click the **Delete** icon.
8. A pop-up confirmation page display. Click **Yes** to continue or **No** to return to the previous screen. The entry is successfully deleted.

12.2.3. Join a RADIUS Server

This section describes how to configure the settings to join a RADIUS server to the D-View 8.

To configure the D-View 8 to access a RADIUS server:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **User Management** to display the User Management page.

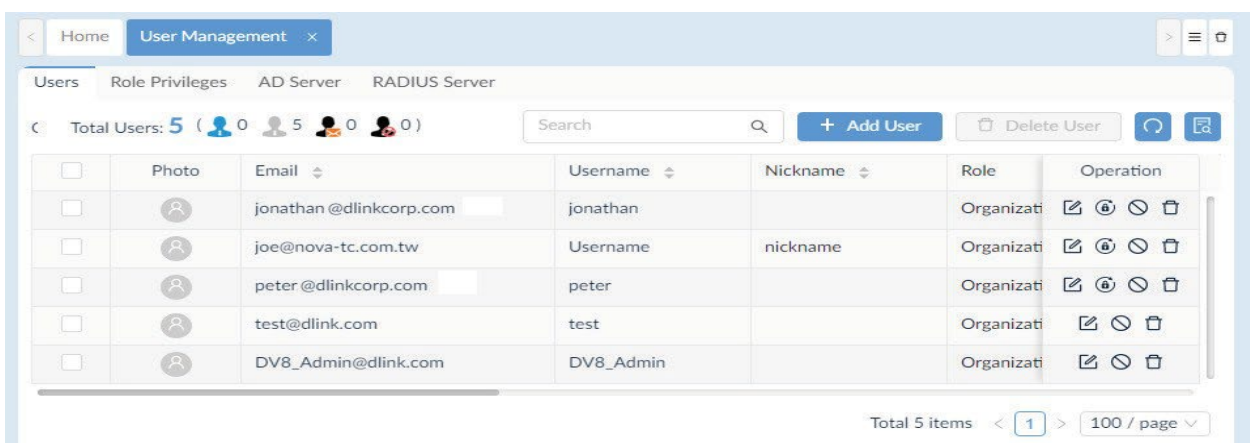


Figure 249 User Management Overview

3. From the tab menu bar, click **RADIUS Server** to display the RADIUS Server page.

The screenshot shows a web interface for configuring RADIUS servers. It is divided into two main sections: Primary RADIUS Server Settings and Secondary RADIUS Server Settings (Optional). The Primary section has four fields: RADIUS Server (172.18.192.53), RADIUS Secret (masked with dots), RADIUS Port (1812), and Protocol (PAP). The Secondary section has the same four fields but they are currently empty. At the bottom right, there are three buttons: Delete (red), Reset (light blue), and Save (dark blue).

Figure 250 Configuring RADIUS Server Settings

4. In the Primary RADIUS Server Settings, specify the following:

Item	Description
RADIUS Server	Enter the server IP address of the remote RADIUS server host.
RADIUS Port	Enter the UDP port destination for the requests.
RADIUS Secret	Enter the authentication and encryption key string running on the RADIUS server. The key is a text string that must match the encryption key as defined in the RADIUS server.
Protocol	Enter the authentication scheme used by the RADIUS server: <ul style="list-style-type: none"> • 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 by piggybacking a peer challenge on the response packet and an authenticator response on the success packet.
Secondary RADIUS Server Settings (Optional)	
RADIUS Server	Enter the server IP address of the remote RADIUS server host.
RADIUS Port	Enter the UDP port destination for the requests.
RADIUS Secret	Enter the authentication and encryption key string running on the RADIUS server. The key is a text string that must match the encryption key as defined in the RADIUS server.
Protocol	Enter the authentication scheme used by the RADIUS server: <ul style="list-style-type: none"> • 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 by piggybacking a peer challenge on the response packet and an authenticator response on the success packet.
Delete	Click to remove the entry.
Reset	Click to clear all settings from the page.
Save	Click to accept the new entry.

5. Click **Save** to accept the new entry.

12.2.4. Remove a RADIUS Server

This section describes how to configure the settings to join a RADIUS server to the D-View 8.

Caution: Modifying or deleting a RADIUS server may cause user login failures. Before proceeding, make sure all operations are saved and users have saved their related data to prevent loss of operation.

To configure the D-View 8 to access a RADIUS server:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **User Management** to display the User Management page.

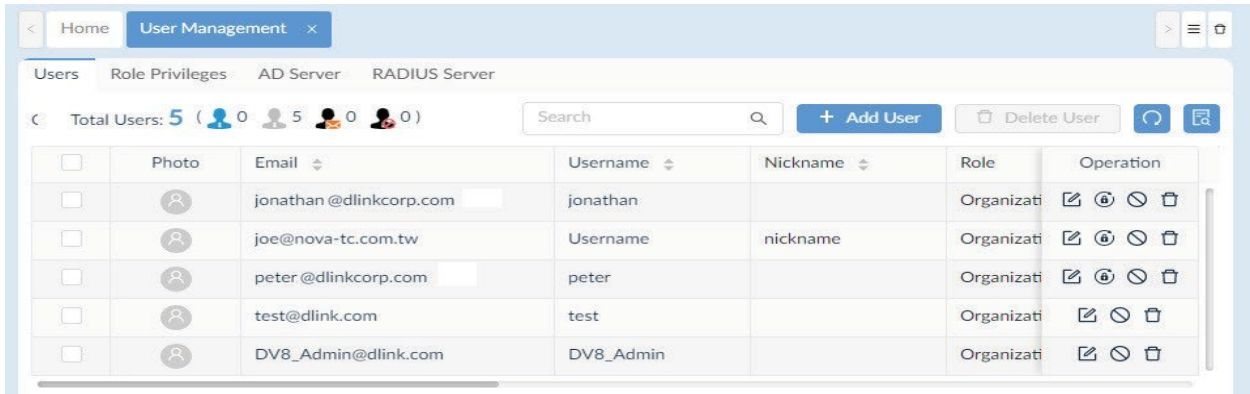


Figure 251 User Management Overview

3. From the tab menu bar, click **RADIUS Server** to display the RADIUS Server page.

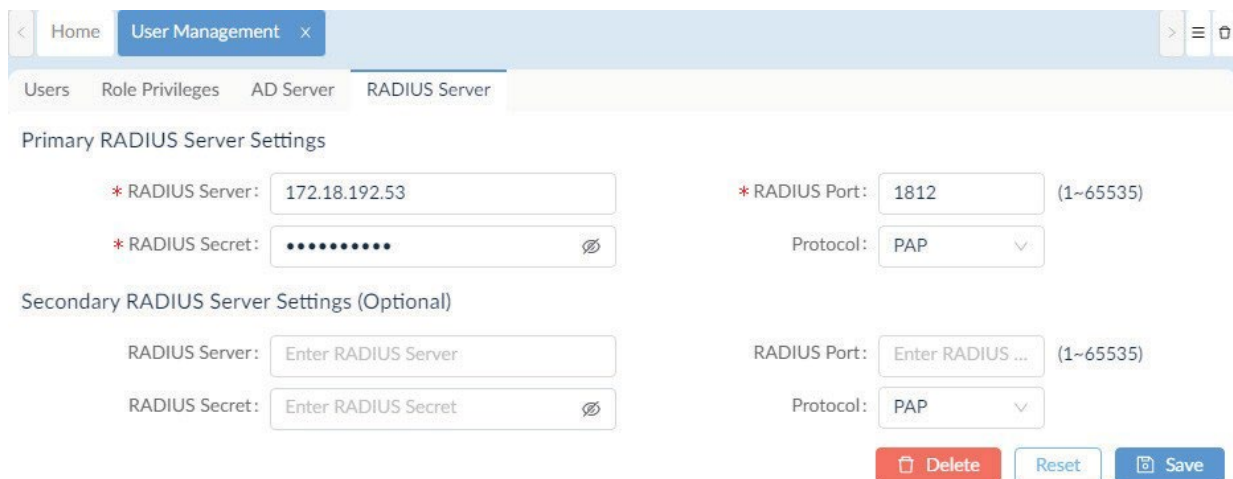


Figure 252 RADIUS Settings Overview

4. Click **Delete** to remove the entry.
5. A pop-up confirmation page display. Click **Yes** to delete the entry. Click **No** to return to the previous menu.

12.3. Add a Profile

The D-View 8 provides a default user profile with an admin security profile. You can add, modify, and remove profiles from the user base.

To add a user profile:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **User Management** to display the User Management page.

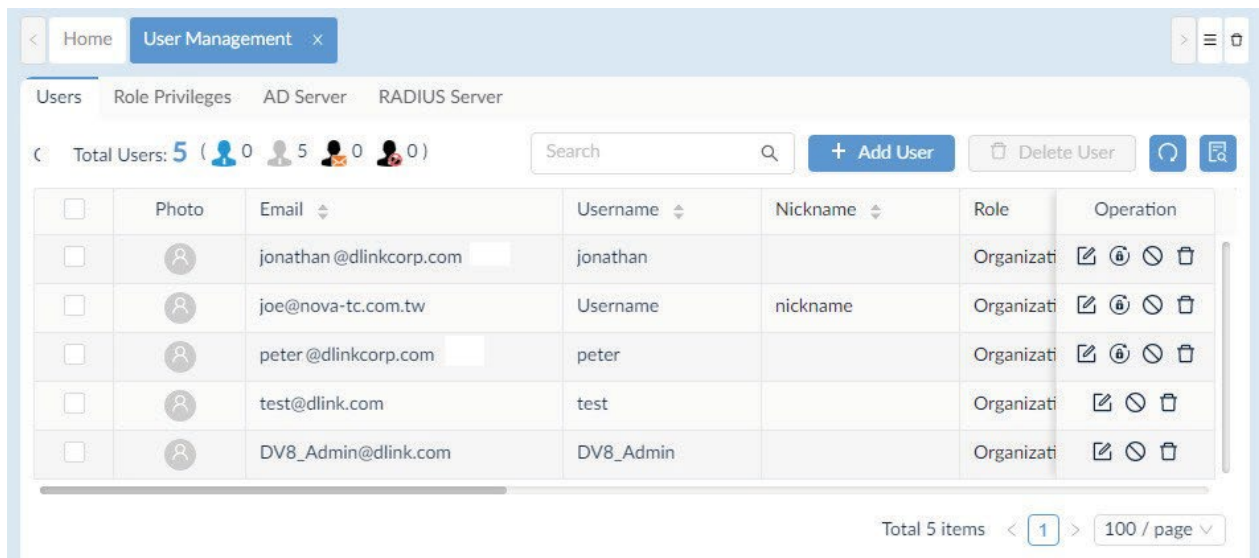


Figure 253 User Management Overview

3. Click **Add User** to display the Add User page.

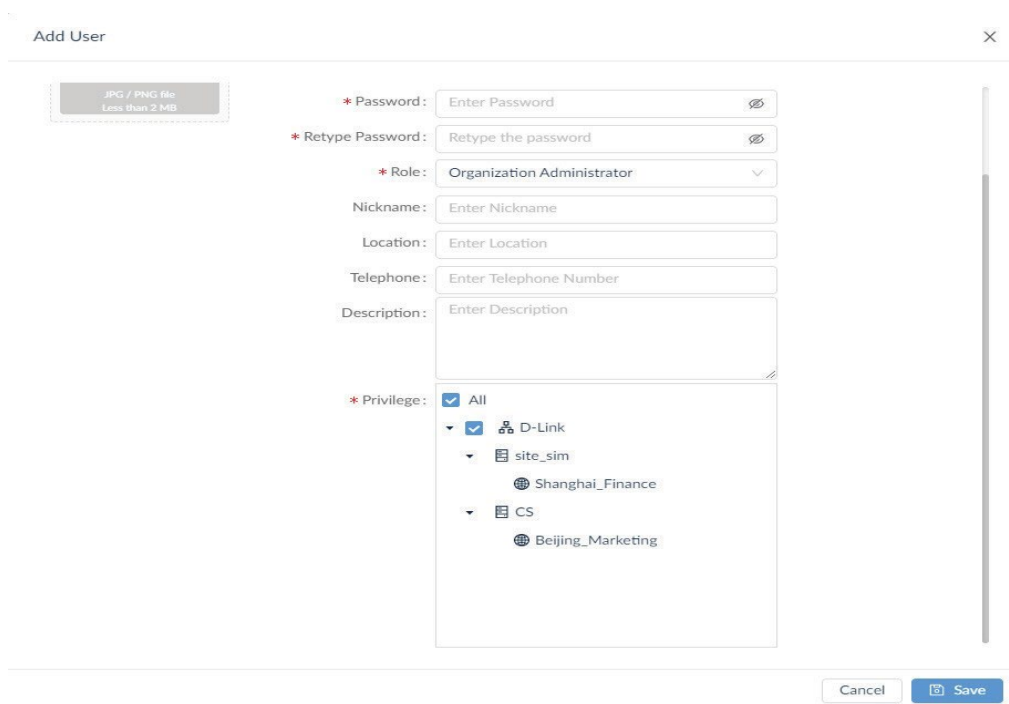


Figure 254 Configuring User Entries

4. Click the avatar icon to browse and upload a JPG / PNG file to use as the avatar image for the profile.
5. Add the following information:

Item	Description
Authentication type	Select from the security protocol.
Email	Enter the profile Email to use.
Username	Enter the username to describe the profile.
Password	The password must contain numbers and upper or lowercase letters. The use of visible symbols is optional.
Retype Password	Enter the same password to authenticate.
Role	Select the profile's security role.
Nickname	Enter a descriptive nickname, optional.
Location	Enter the location of the profile, optional.
Telephone	Enter the phone number of the profile, optional.

Item	Description
Description	Enter a description to easily identify the profile.
Privilege	Based on the Role type, select the organization, site, or network to provide access to the user profile.

- Click **Save** to create the profile. Click **Cancel** to return to the previous menu. Once the profile is created, the system sends a verification email to the defined address to authenticate the profile.
Optionally, you can manually send an activation email. See the following step to initiate an activation email.
- Click the **Send Activation Email** to deliver an Email to the defined Email account.



Figure 255 Activating Send Email Task

Once activated, the profile can be accessed.

12.4. Modify or Remove a Profile

To add a user profile:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Under **System**, click User Management to display the User Management page.

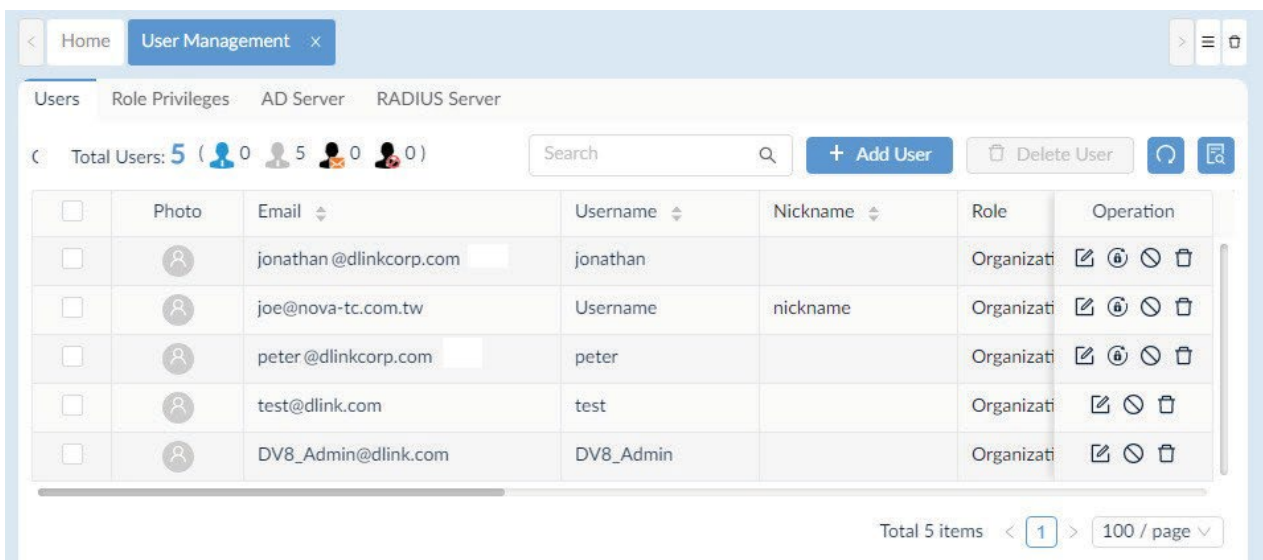


Figure 256 User Management Overview

- The following information is available under the Operation column:
 - Edit: modify the define profile information
 - Send Email Authentication: send an Email to confirm the profile
 - Reset Password: creates a new password for the profile.
 - Disable: inactivates the profile from the user pool.
 - Delete: removes the profile from the user pool.
- To edit the user, click the **Edit** icon to open the Edit User page.
- Modify the user information and click **Save** to accept the new settings. Click Cancel to return to the previous menu.

This page is intentionally left blank.

13 Manage Global Settings

You can customize global system settings and manage them from the Global Settings menu.

The following information is available in this section:

- Set Up Organization
- Set Up a Mail Server
- Set Up a Forward Trap
- Set Up a Forward Syslog
- Generate a REST API
- Set Up SNMP Credentials
- Set Up sFlow Settings
- Set Up System Preferences

13.1. Set Up Organization

The organization information is located under the Basic Settings menu. You can define the time zone, location and name under the menu.

To set up the organization information:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **System**, click Basic Settings to display the Organization page.

Figure 257 Organization Basic Settings Overview

3. Define the following information:

Item	Description
Organization Name	Enter the name to define the organization.
Customized Logo	Select an image to upload, image must be less than 2 MB in JPEG or PNG format.
Country	Select the main location of the organization.
Time Zone	Select the time zone correlating to the specified location.

4. Click **Save** to define the organization settings.

13.2. Set Up a Mail Server

To set up the organization information:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **System**, click **Basic Settings** to display the Organization page.
3. Click the **Mail Server Settings** tab to display the Mail Server Settings.

The screenshot shows the 'Mail Server Settings' page. At the top, there are navigation tabs: 'Home', 'Basic Settings' (selected), and a menu icon. Below the tabs are several sub-tabs: 'Organization', 'Mail Server Settings' (selected), 'Forward Trap', 'Forward Syslog', 'SNMP Credentials', 'sFlow Settings', and 'System Preferences'. The main content area is divided into sections: 'D-View 8 Domain' with a 'Domain Name' field containing 'https://222.244.145.29:17302'; 'Mail Server' with fields for 'SMTP Host' (smtp.163.com), 'Port' (25), 'Sender Email Address' (13714836715@163.com), 'Sender' (D-View 8), 'Security Type' (None), 'Encoding Type' (UTF8), 'Authentication' (SMTP Authentication), 'Username' (13714836715@163.com), and 'Password' (masked with dots). A 'Save' button is located below the password field. At the bottom, there is a 'Test Mail Server' section with an input field 'Enter an email addr...' and a 'Send Test Mail' button.

Figure 258 Mail Server Settings Overview

4. Define the following information:

Item	Description
Domain Name	Enter the domain name.
SMTP Host	Enter the SMTP server address.
Port	Enter the port number of the SMTP server.
Sender Email Address	Enter the Email address to define the sender email address.
Sender	Enter the name to use for sender.
Security Type	Select the security protocol for the domain, None or SSL.
Encoding Type	Select the type of transfer encoding (UTF8 or ASCII) to match the SMTP specifications.
Authentication	Select the security protocol assigned to the SMTP server.
Username	Enter the username with security access to the SMTP server. Available when SMTP authentication is selected under Authentication.
Password	Enter the password for the username. Available when SMTP authentication is selected under Authentication.

5. Click **Save** to define the mail server settings.

Once the Mail Server is configured, test the settings with the Send Test Mail function.

6. In the email address field, enter an accessible Email for the testing function.
7. Click **Send Test Mail**.
8. Open your Email application to view the successful test.
9. If the Email was not received, check the mail server settings and change settings as required.

13.3. Set Up a Forward Trap

D-View 8 provides an SNMP trap forwarding using the Forward Trap function. The function allows you to forward traps to a specified server destination.

To configure Forward Traps:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **System**, click Basic Settings to display the Organization page.
3. Click the **Forward Trap** tab to display the Forward Trap page.

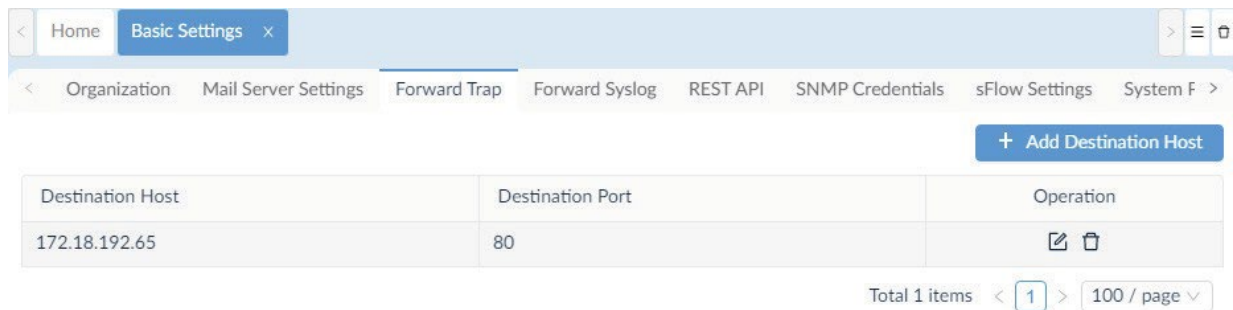


Figure 259 Forward Trap Overview

4. Click **Add Destination Host** to display the Add Destination Host page.

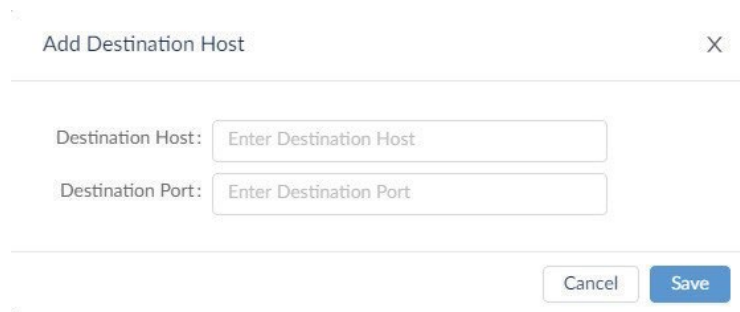


Figure 260 Configuring Destination Host

5. Enter the destination host and port to define the syslog destination.
6. Click **Save** to define the forward syslog. Click **Cancel** to return to the previous menu.
The host is saved successfully and lists in the Forward Trap list.
The trap listing can be edited or removed from the Operation panel.
7. Click **Edit** or **Delete** to modify the Forward Syslog entry.

13.4. Set Up a Forward Syslog

To configure a D-View 8 application for sending syslog messages to an external syslog server, see the following information.

To configure Forward Syslog:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.

- Click the **Forward Syslog** tab to display the Forward Syslog page.

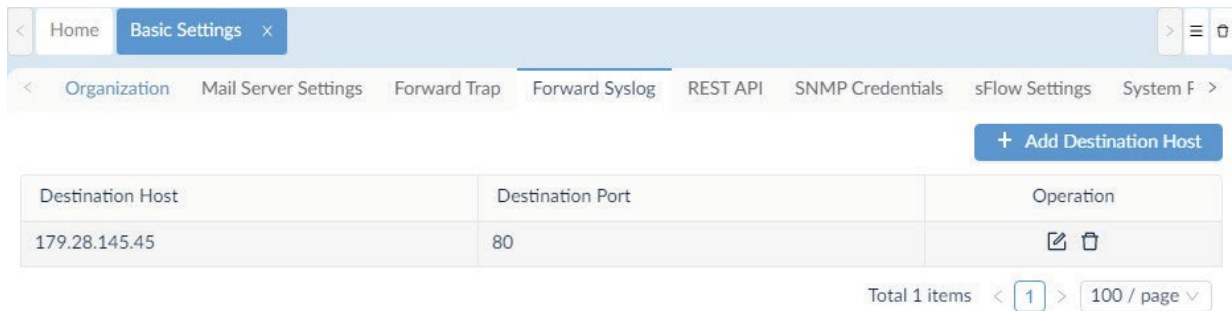


Figure 261 Forward Syslog Overview

- Click **Add Destination Host** to display the Add Destination Host page.

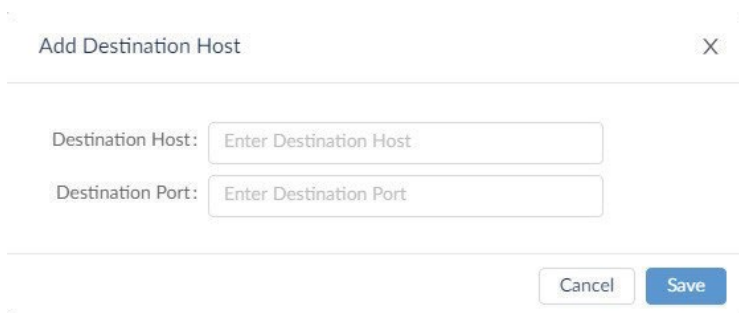


Figure 262 Configuring Destination Host

- Enter the destination host and port to define the syslog destination.
 - Click **Save** to define the forward syslog. Click **Cancel** to return to the previous menu.
- The host is saved successfully and lists in the Forward Syslog list.
The trap listing can be edited or removed from the Operation panel.

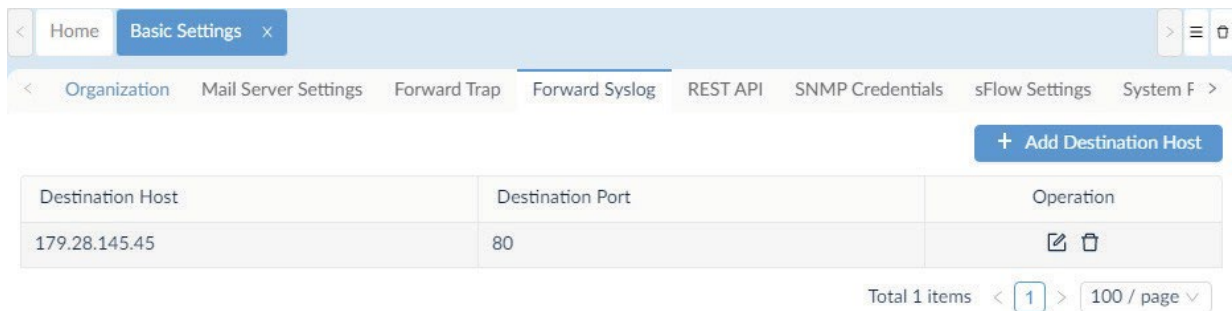


Figure 263 Syslog Listing Overview

- Click **Edit** or **Delete** to modify the Forward Syslog entry.

13.5. Generate a REST API

REST API is only supported in the Enterprise version. REST API authentication uses HTTPS as the transport for all the D-View 8 REST API access. The authentication service allows clients to perform authentication to invoke APIs.

To configure Forward Traps:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Under System, click **Basic Settings** to display the Organization page.
- Click the **REST API** tab to display the Add API Key page.

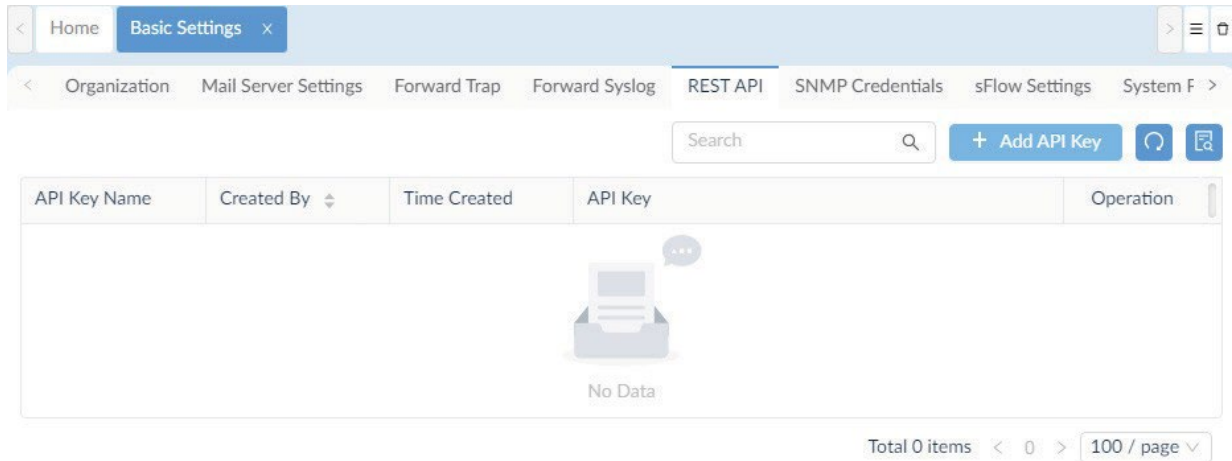


Figure 264 Configuring API Key

4. Click **Add API Key** to display the Add API Key page.

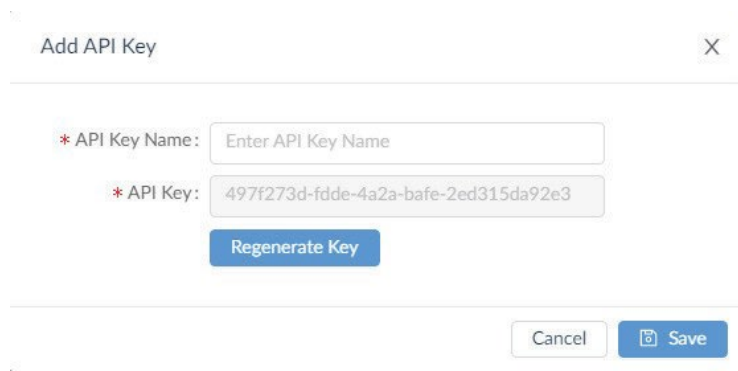


Figure 265 API Key Overview

5. Enter the name to identify the API key.
6. Click **Regenerate Key** to create a new key value.
7. Click **Save** to define the REST API key. Click **Cancel** to return to the previous menu.

The API key entry is saved successfully and lists in the REST API Key list.

The REST API listing can be disabled or removed from the Operation panel.

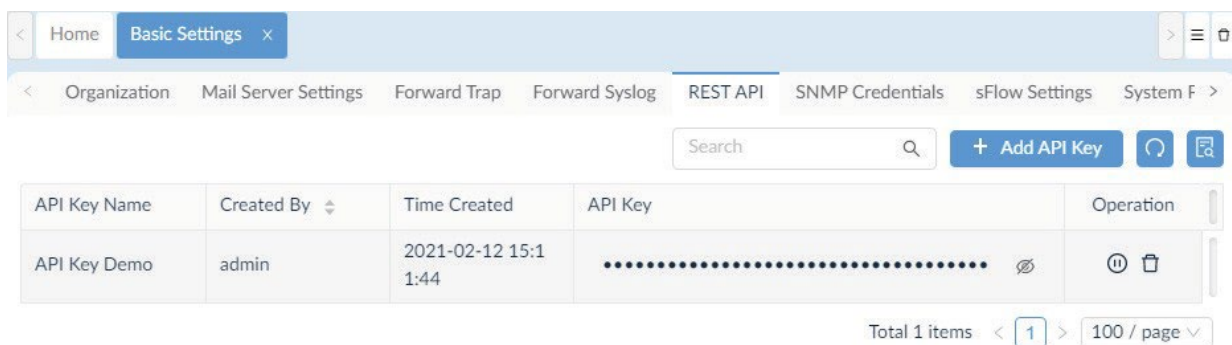


Figure 266 REST API Settings

13.6. Set Up SNMP Credentials

The SNMP credentials manages access to discover the different types of devices using the protocol. The credential can be stored for use when discovering the network devices.

To configure SNMP credentials:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.

2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **SNMP Credential** stab to display the page.

<input type="checkbox"/>	Name ↕	Type ↕	Description ↕	Operation
<input type="checkbox"/>	SNMP Profile Demo	SNMP v2c	SNMP profile for demo purpose	✎ 🗑
<input type="checkbox"/>	default SNMP v1	SNMP v1		✎ 🗑
<input type="checkbox"/>	testaaa	SNMP v2c		✎ 🗑
<input type="checkbox"/>	Sample v1	SNMP v1		✎ 🗑
<input type="checkbox"/>	SNMP v1 default	SNMP v1	SNMP v1 default credential	✎ 🗑
<input type="checkbox"/>	Sample v2	SNMP v2c	snmpv2c credit	✎ 🗑

Total 6 items < 1 > 200 / page

Figure 267 SNMP Credentials Overview

4. Click **Add SNMP Profile** to display the Add SNMP Profile page.

Add SNMP Profile

SNMP Protocol Version: SNMP v1 SNMP v2c SNMP v3

* Name:

* Port:

* Timeout [s]:

* Retransmit:

* Read Community:

Write Community:

* Non-repeaters:

* Max repetitions:

Description:

Cancel Save

Figure 268 Adding SNMP Credentials

5. Select the SNMP version of the credential: SNMP v1, SNMP v2c, or SNMP v3. By default, D-View 8 uses SNMPv2c.

For SNMP v1:

- Enter the name of the profile and SNMP Port.
- Enter the timeout period in seconds (default: 4).
- Enter the valid number of transmit times (default: 3)
- Enter the read only credential string (default: public).
- Enter the write only credential (default: private) string.
- Enter a description to easily identify the profile.

For SNMP v2c:

- Enter the variable to define how many Oid's in a request should be as Get Request variables (default: 0).
- Enter the maximum number of operations to perform (default: 10).
- Enter a description to easily identify the profile.

For SNMPv3:

- Enter the Context Name, serves as the identifier for the SNMPv3 entity.
- Select the Security Level:
 - authPriv: authentication and privacy (default).
 - authNoPriv: authentication, no privacy.
- Select the Auth Protocol:
 - MD5: select to enter an authentication pass phrase. The MD5 hashed pass phrase is used to access the target device.
 - SHA: select to enter an authentication pass phrase. The SHA hashed pass phrase is used to access the target device.
- Enter the Auth Password correlating to the Auth Protocol.
- Select the Privacy Protocol:
 - DES: privacy key to encrypt data using the DES algorithm.
 - AES: privacy key to encrypt data using the AES algorithm.
- Enter the Privacy Password: Enter the password (pass phrase) which will be used to encrypt the data. For SNMP V3 credentials only if privacy protocol is selected.

6. Click **Save** to create the profile. Click **Cancel** to return to the previous menu.

The SNMP profile listing can be modified or removed from the operation panel.

Click **Edit** or **Delete** to manage the profile.

Alternatively, you can select a listed profile to enable the Delete SNMP Profile option.

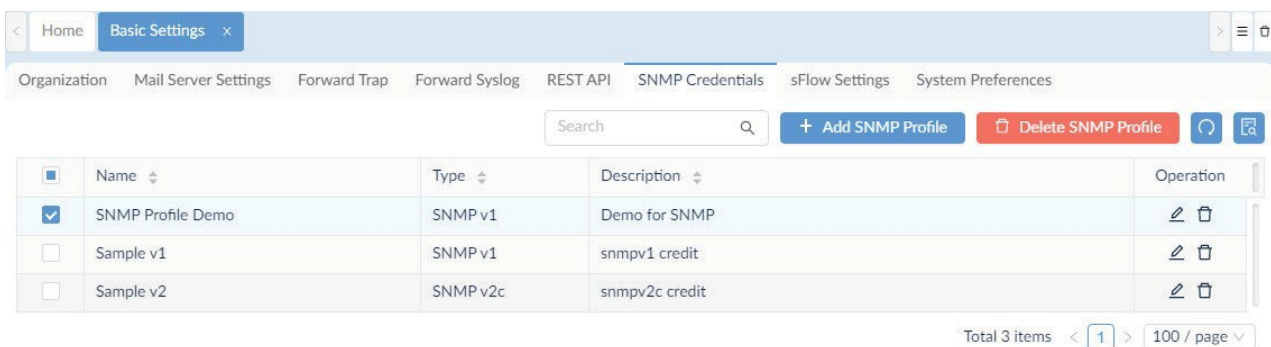


Figure 269 Deleting SNMP Profiles

13.7. Set Up sFlow Settings

Effective management between applications and the network resources is one of the benefits of adapting the sFlow standard through D-View 8. The application provides dependency tracking in real time using sFlow data.

To view and map sFlow Settings credentials:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **sFlow Settings** tab to display the sFlow Settings page.

The screenshot shows the 'sFlow Settings' page with the 'Application Mapping' tab selected. A table lists various applications and their configurations. The table has columns for Application Name, Port Number, Protocol, IP Address, and Operation. The 'Internet Key Exchange(IKE)' row is highlighted.

Application Name	Port Number	Protocol	IP Address	Operation
wlyttest	161	UDP	All	[Edit] [Delete]
Memcached	11211	TCP	All	[Edit] [Delete]
netwall	533	UDP	All	[Edit] [Delete]
unixtime	519	UDP	All	[Edit] [Delete]
ntalk	518	UDP	All	[Edit] [Delete]
talk	517	UDP	All	[Edit] [Delete]
RIP	520	UDP	All	[Edit] [Delete]
sFlow	6343	UDP	All	[Edit] [Delete]
Syslog	514	UDP	All	[Edit] [Delete]
QQ	4000	TCP	All	[Edit] [Delete]
Web Proxy Service	8080	TCP	All	[Edit] [Delete]
Oracle	1521	TCP	All	[Edit] [Delete]
network blackjack	1025	UDP	All	[Edit] [Delete]
Internet Key Exchange(IKE)	500	UDP	All	[Edit] [Delete]
Common Internet File System(CIFS)	445	UDP	All	[Edit] [Delete]

Figure 270 Configuring Application Mapping in sFlow Settings

From sFlow Settings, the following mapping options are available:

- Application Mapping
- DSCP Mapping
- IP Alias Mapping
- MAC Address Mapping

13.7.1. Application Mapping

To configure application mappings:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **sFlow Settings** tab to display the sFlow Settings page.

This screenshot is identical to Figure 270, showing the 'Application Mapping' tab selected in the 'sFlow Settings' page. The table lists various applications and their configurations, with the 'Internet Key Exchange(IKE)' row highlighted.

Application Name	Port Number	Protocol	IP Address	Operation
wlyttest	161	UDP	All	[Edit] [Delete]
Memcached	11211	TCP	All	[Edit] [Delete]
netwall	533	UDP	All	[Edit] [Delete]
unixtime	519	UDP	All	[Edit] [Delete]
ntalk	518	UDP	All	[Edit] [Delete]
talk	517	UDP	All	[Edit] [Delete]
RIP	520	UDP	All	[Edit] [Delete]
sFlow	6343	UDP	All	[Edit] [Delete]
Syslog	514	UDP	All	[Edit] [Delete]
QQ	4000	TCP	All	[Edit] [Delete]
Web Proxy Service	8080	TCP	All	[Edit] [Delete]
Oracle	1521	TCP	All	[Edit] [Delete]
network blackjack	1025	UDP	All	[Edit] [Delete]
Internet Key Exchange(IKE)	500	UDP	All	[Edit] [Delete]
Common Internet File System(CIFS)	445	UDP	All	[Edit] [Delete]

Figure 271 Configuring Application Mapping in sFlow Settings

4. Click the **Application Mapping** tab to display the Application Mapping page.

Add Mapping X

* Application Name:

* Port Number:

* Protocol: TCP ▼

* IP Address: All IP Address Subnet IP Range

Figure 272 sFlow Application Mapping

5. Enter the required information to identify the mapping rule.
6. In the Protocol field, click the drop-down menu to select TCP or UDP.
7. In the IP Address field, select All, IP Address, Subnet, or IP Range to specify the mapping range.

Add Mapping X

* Application Name:

* Port Number:

* Protocol: TCP ▼

* IP Address: All IP Address Subnet IP Range

* IP Address:

Figure 273 Adding sFlow Application Mapping

8. Click **Save** to create the application mapping rule or **Cancel** to return to the previous menu.

13.7.2. DSCP Mapping

To view DSCP sFlow mapping data:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **sFlow Settings** tab to display the sFlow Settings page.

Application Name	Port Number	Protocol	IP Address	Operation
wytest	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	

Figure 274 sFlow DSCP Mapping Data

4. Click the **DSCP Mapping** tab to view the DSCP Mapping data. The DSCP Mapping page displays.

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

Figure 275 sFlow DSCP Mapping Data

13.7.3. IP Alias Mapping

To configure sFlow IP alias mapping:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **sFlow Settings** tab to display the sFlow Settings page.

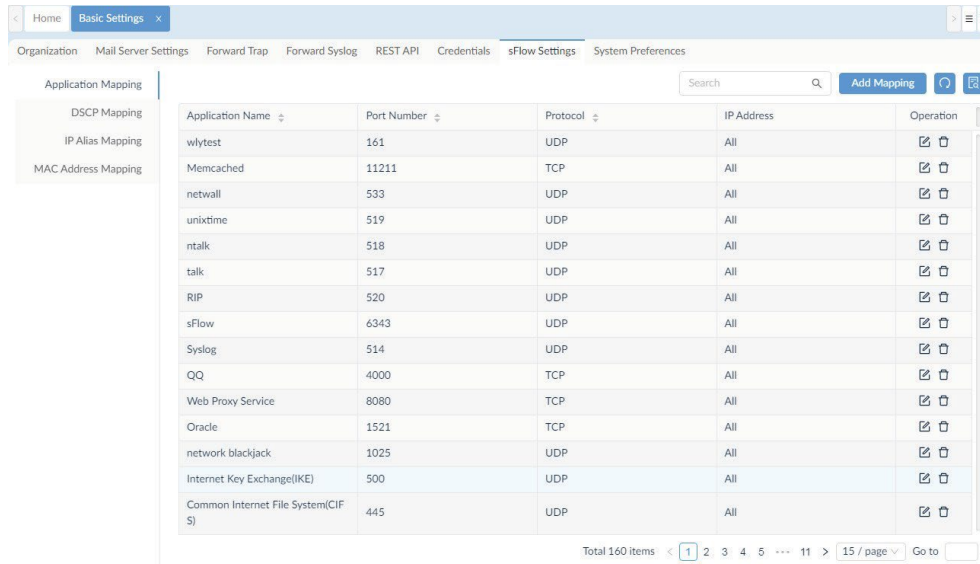


Figure 276 Configuring Application Mapping in sFlow Settings

- Click the IP Alias Mapping tab to display the MAC Address Mapping page.

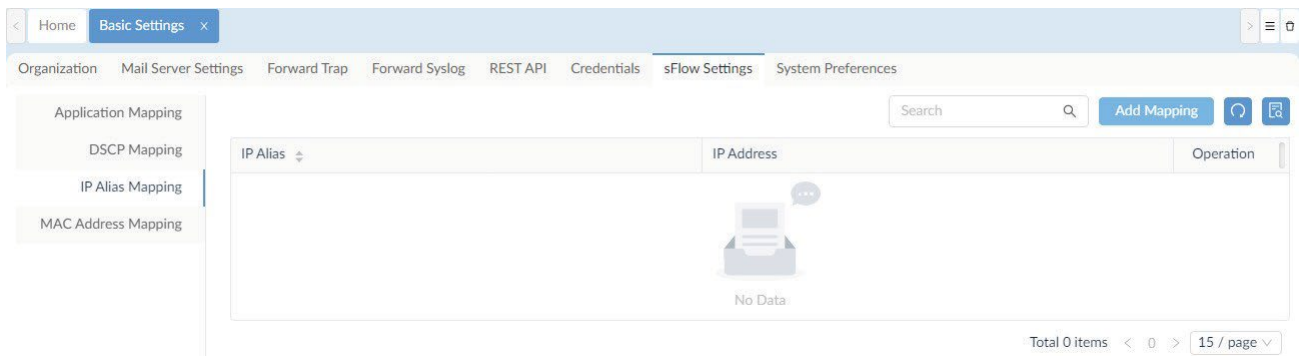


Figure 277 Configuring IP Alias Mapping in sFlow Settings

- Click **Add Mapping**. The Add Mapping window displays.



Figure 278 Adding sFlow IP Alias Mapping

- Enter the IP Alias and IP address to define the mapping entry.
- Click **Save** to create the IP alias mapping rule or **Cancel** to return to the previous menu.

13.7.4. MAC Address Mapping

The SNMP credentials manages access to discover the different types of devices using the protocol. The credential can be stored for use when discovering the network devices.

To configure sFlow Settings credentials:

- Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
- Under System, click **Basic Settings** to display the Organization page.

3. Click the **sFlow Settings** tab to display the sFlow Settings page.

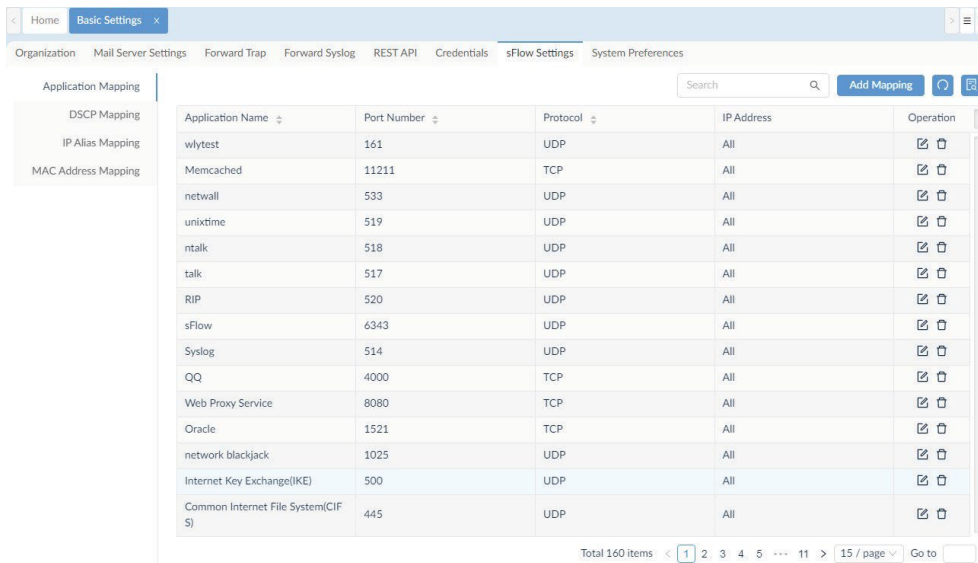


Figure 279 Configuring Application Mapping in sFlow Settings

4. Click the **MAC Address Mapping** tab to display the MAC Address Mapping page.

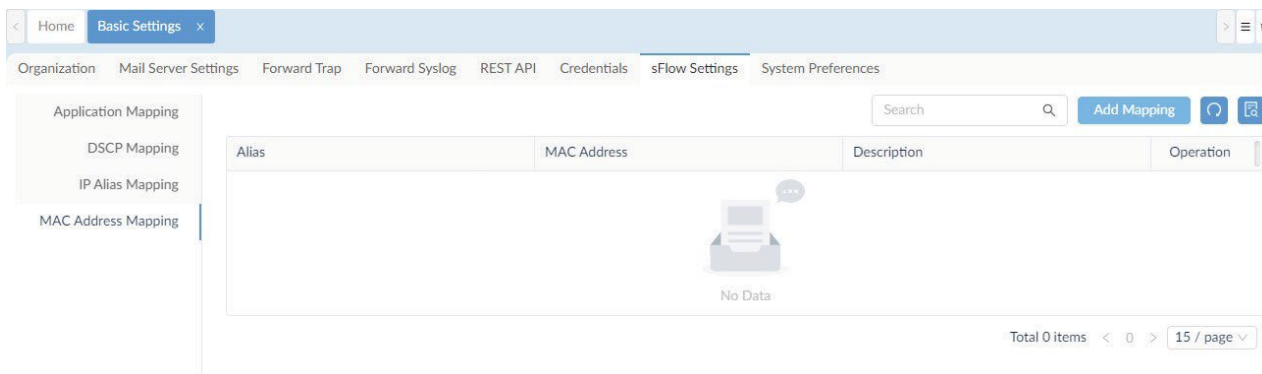


Figure 280 Configuring MAC Address Mapping in sFlow Settings

5. Click **Add Mapping**. The Add Mapping window displays.

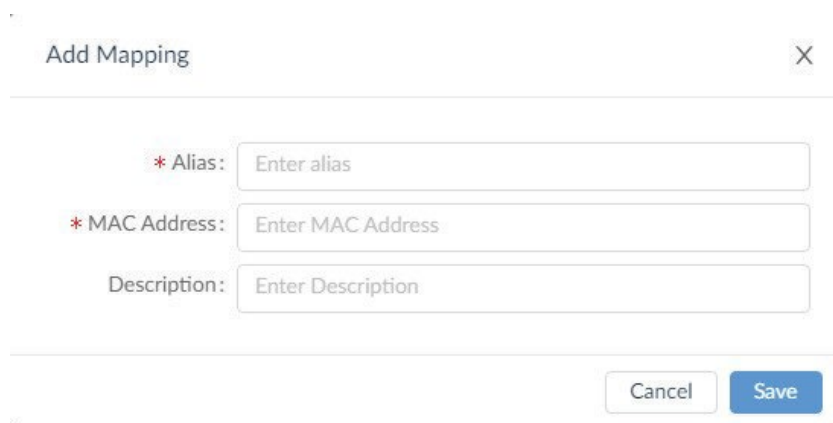


Figure 281 Adding sFlow MAC Address Mapping

6. Enter the Alias, MAC Address, and a brief description of the mapping entry.

7. Click **Save** to create the MAC Address mapping rule or **Cancel** to return to the previous menu.

13.8. Set Up System Preferences

Theme settings for the overall layout of the interface are configured through the System Preferences section. You can configure Table and Theme settings to set specific page styles.

To configure System Preferences:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under System, click **Basic Settings** to display the Organization page.
3. Click the **System Preferences** tab to display the System Preferences page.

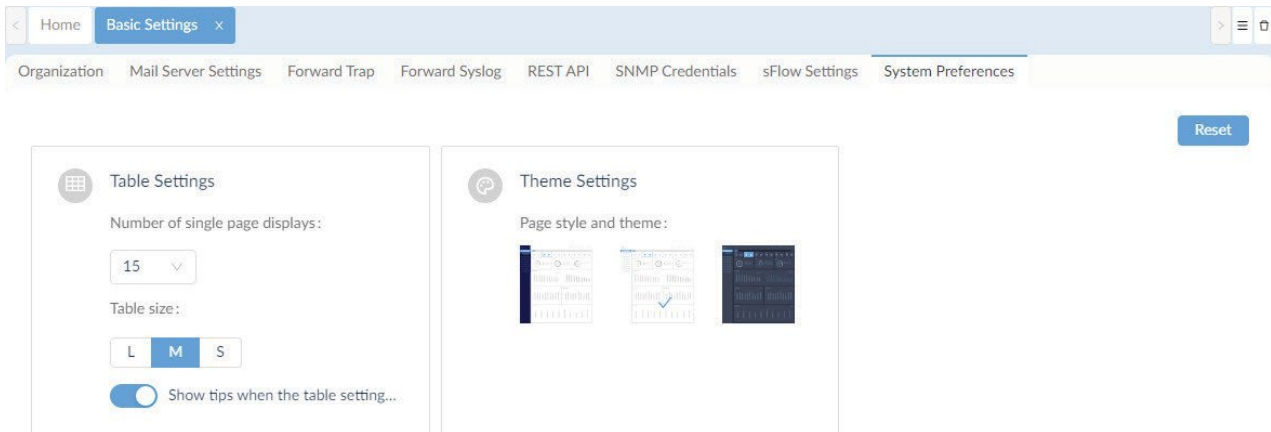


Figure 282 System Preferences Overview

In Table Settings, you can set the single page display and table size:

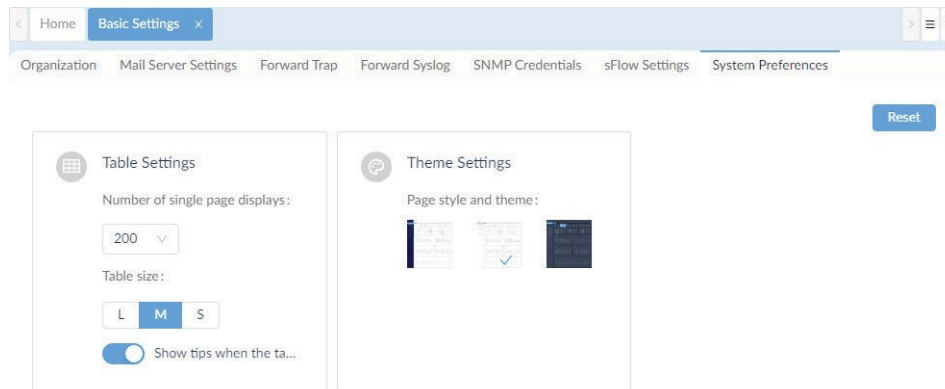


Figure 283 Display and Table Settings

4. Click drop-down menu to select the number of single page displays: 15 (default), 50, 100, or 200.
5. From the table size selector, click a selection to set the size of a displayed table: Large, Middle (default), or Small.

In Theme Settings, select a defined theme to apply to the interface.

6. Click on a theme style to select it. The setting takes effect across the interface.

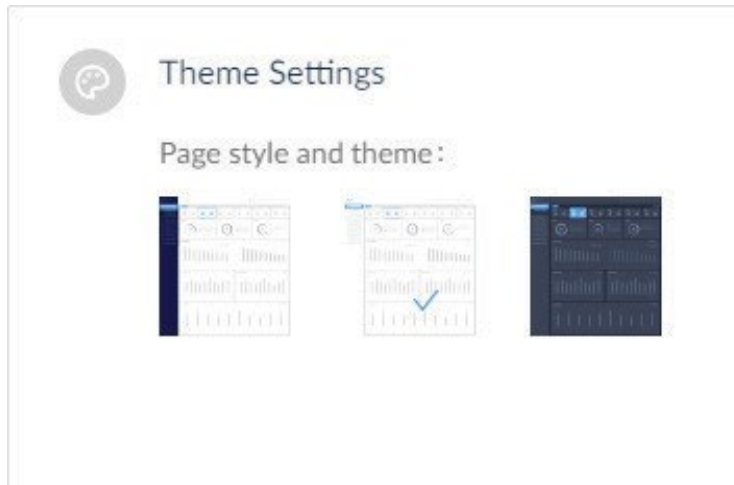


Figure 284 Configuring Theme Styles

To reset to the original settings, click the **Reset** button. All tale and theme settings are restored to default.

14 Manage Resources

Effective management of your network requires the tools and resources to discover your devices and apply setup tasks.

14.1. Use a MIB Browser

A MIB Browser is only supported in the Enterprise version. The MIB browser allows you to retrieve SNMP information from supporting devices. By pulling out data from SNMP enabled devices, you can see the data in a readable format and search for specific OIDs. The MIB data is presented in a MIB tree to identify all or a specific a device.

To select a MIB object and collect SNMP data:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click MIB Browser to display the MIB Browser page.

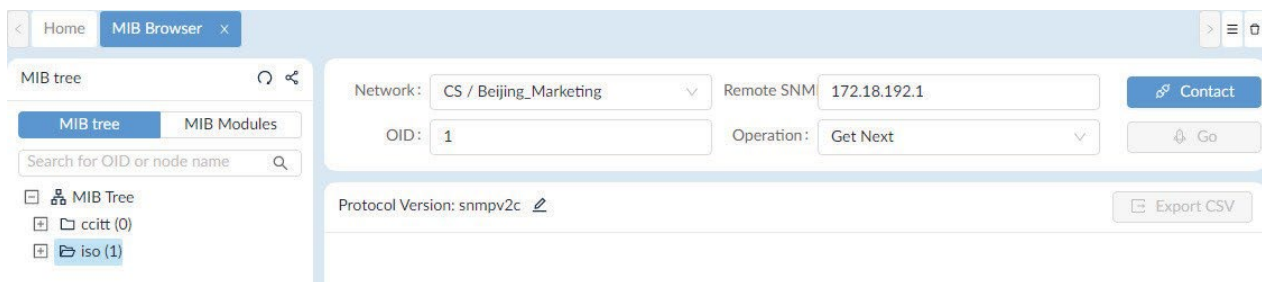


Figure 285 MIB Browser Overview

3. From the MIB tree column, search for specific MIBs by using one of the following methods:
 - Click the MIB tree tab to select a specific object.
 - Click MIB Modules to select a specific node entry.
 - Enter a specific OID in the search field to browse for an object or node.
4. Alternatively, you can directly specify the OID object by entering SNMP credentials:
 - Click the drop-down menu to select the Network.
 - Enter the Remote SNMP address.
 - Enter the OID number.
 - Click the drop-down menu to select an operation function:
 - Get
 - Get Next
 - Get Bulk
 - Walk
 - Table View
 - Instance View
 - Set ...
5. Click **Contact** initiate a connection with the remote SNMP agent. After a successful connection, the details for the object are displayed.
6. You can download the MIB data to a folder on your desktop in an CSV. Click Export CSV to initiate the download.

The SNMP credentials for the OID object can be modified by clicking the SNMP Protocol Preference edit button.
7. In the SNMP Protocol Preference page, modify the protocol settings. See Set Up SNMP Credentials.

14.2. MIB Compiler Tool

The MIB Compiler Tool is only supported in the Enterprise version. It is a key tool for managing SNMP objects. The compiler allows the extension of management capabilities to any SNMP hardware. You can add SNMP objects to be discovered and visible in the MIB tree.

14.2.1. Add MIB Files

You can upload MIB files into the MIB browser.

To add MIB files:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click MIB Compiler to display the MIB Compiler page.

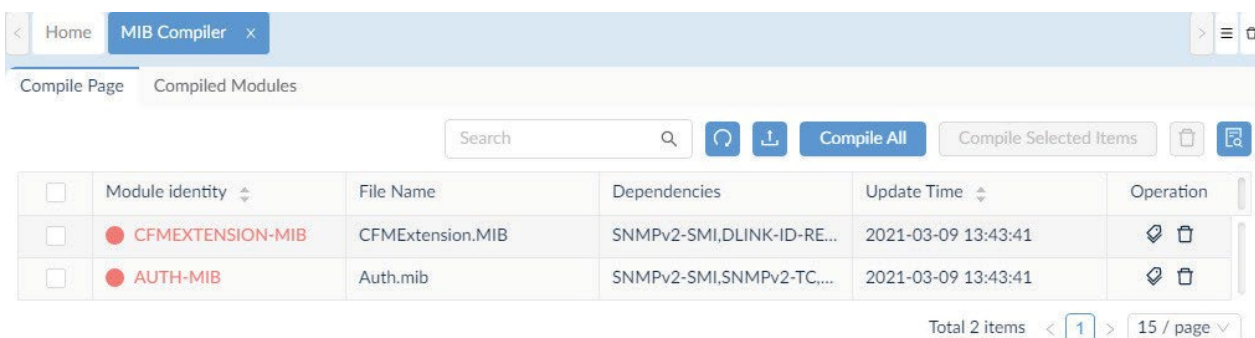


Figure 286 MIB Compiler Overview

3. In the Compile Page, click Upload MIB files to select a file(s) to upload.
4. The Upload MIB files page displays. Click **Select Files** to upload MIB files or click **Select Directory** to select all the files under the corresponding folder.

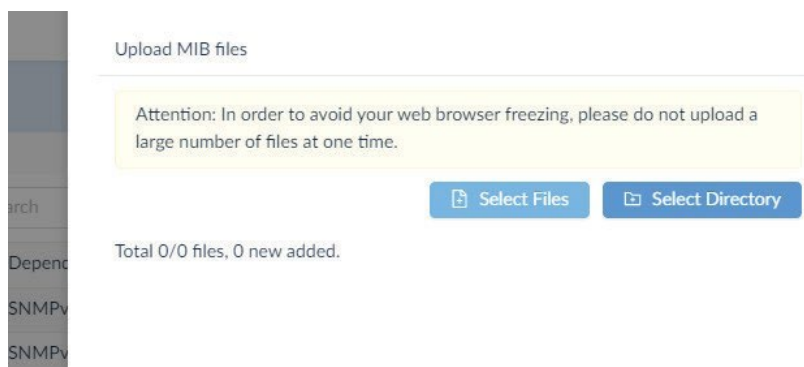


Figure 287 Selecting MIB File Uploading Directory

Once the file(s) is selected it is displayed as a list along with the upload status.

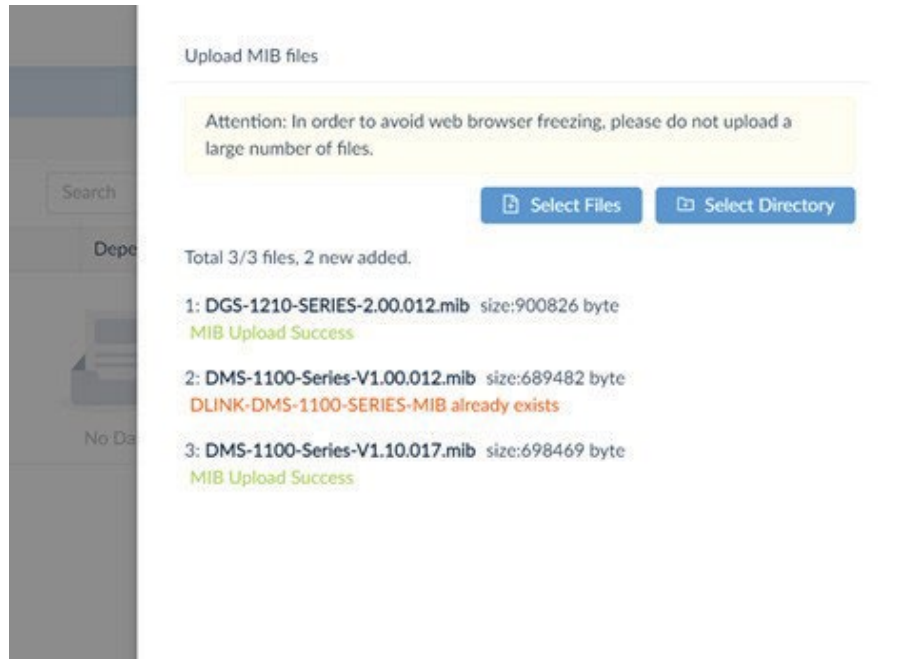


Figure 288 Uploaded Status Overview

14.2.2. Compile MIB Files

You can compile the available MIB files in the uploaded library to make them available in the MIB browser.

To compile MIB files:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click MIB Compiler to display the MIB Compile Page page.

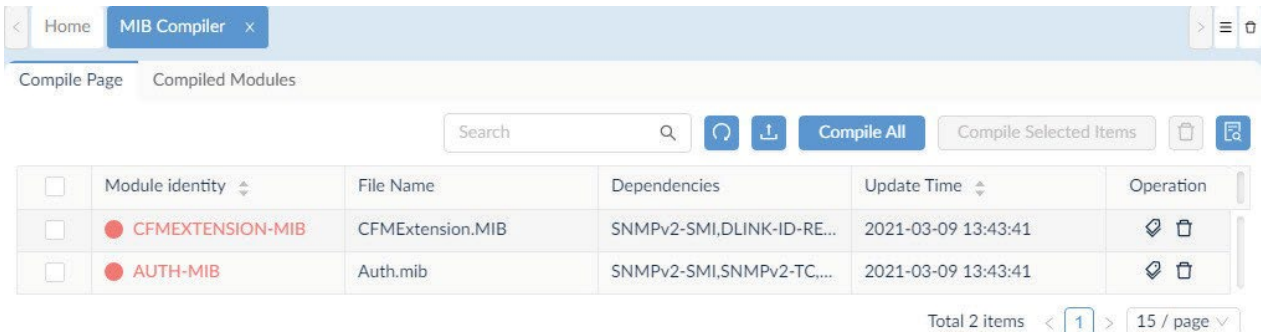


Figure 289 MIB Compile Overview

3. In the Compile Page, click **Compile All** or select an object from the list and click **Compile Selected Item**.

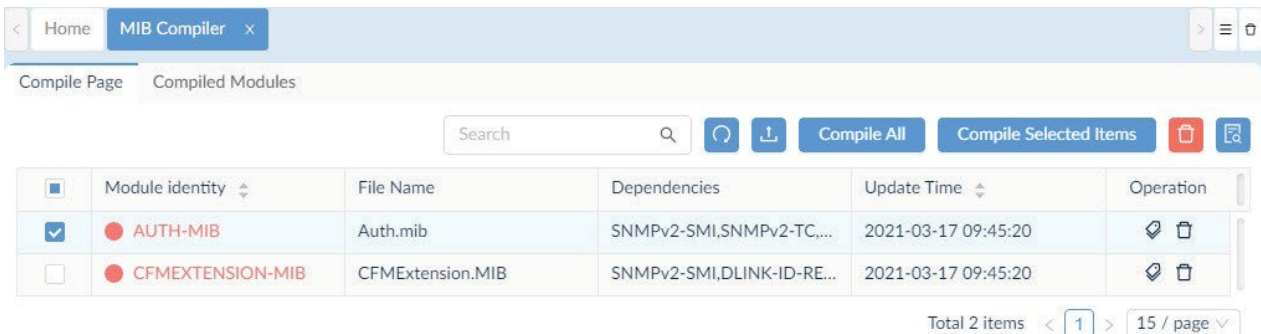


Figure 290 Compiling Selected Items

The compiling of the selected items initiates once the compile button is pressed.

14.2.3. Manage Device in MIB Browser

To manage a device in the MIB browser:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click MIB Browser to display the MIB Browser page.

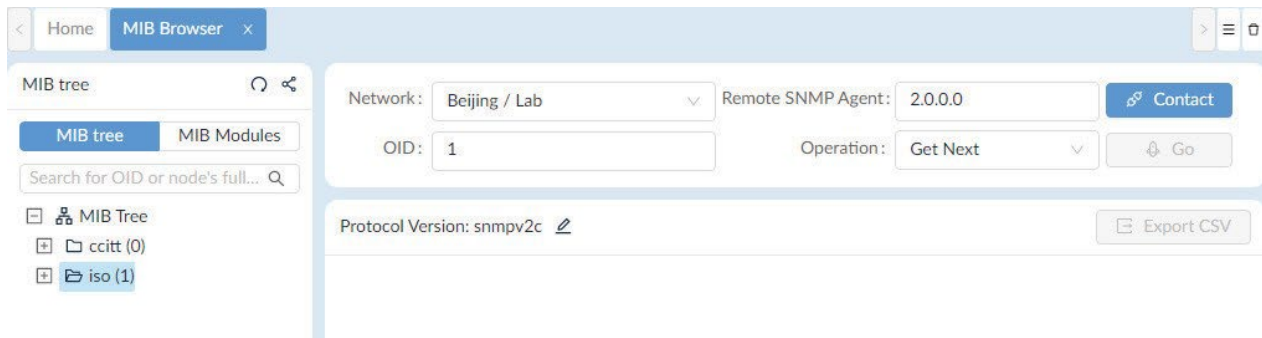


Figure 291 Tools MIB Browser Overview

3. Enter the required information in the Network, OID, Remote SNMP Agent (device IP) and click Contact. A session to the remote SNMP agent is initiated.

For Leaf nodes, an index is required in OID.

4. In the OID field, enter the index.
5. In the Operation drop-down menu, click to select an operation:
 - Get
 - Get Next
 - Get Bulk
 - Set
 - Table view
 - Instance View
 - Properties.
6. Click Go to view the results. The results are display in the main viewing pane.

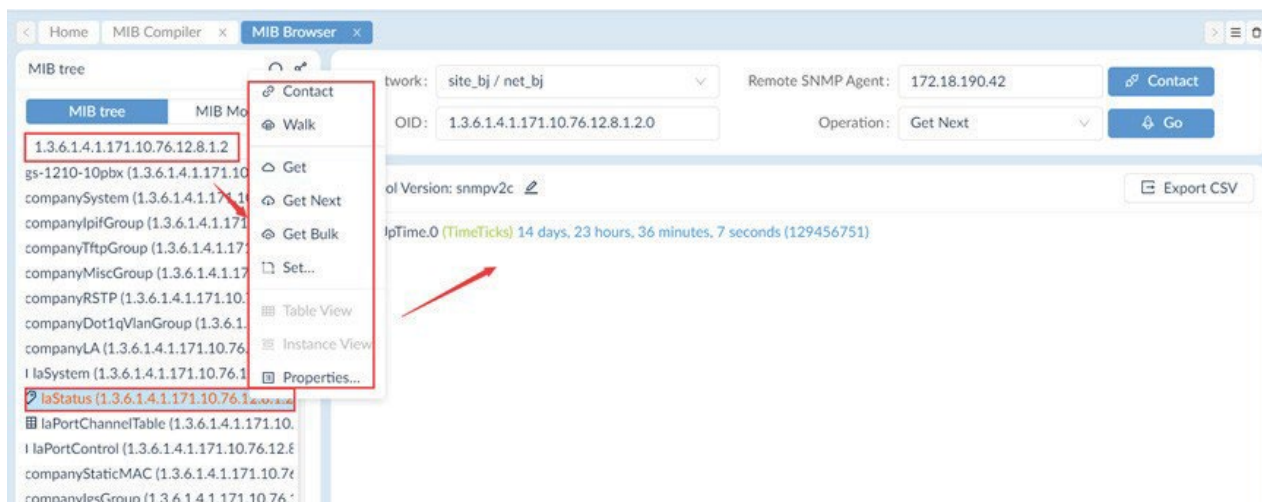


Figure 292 OID Operation Overview

14.3. Perform an ICMP Ping

You can ping a wired or wireless network device.

To test a device:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click ICMP Ping to display the ICMP Ping page.

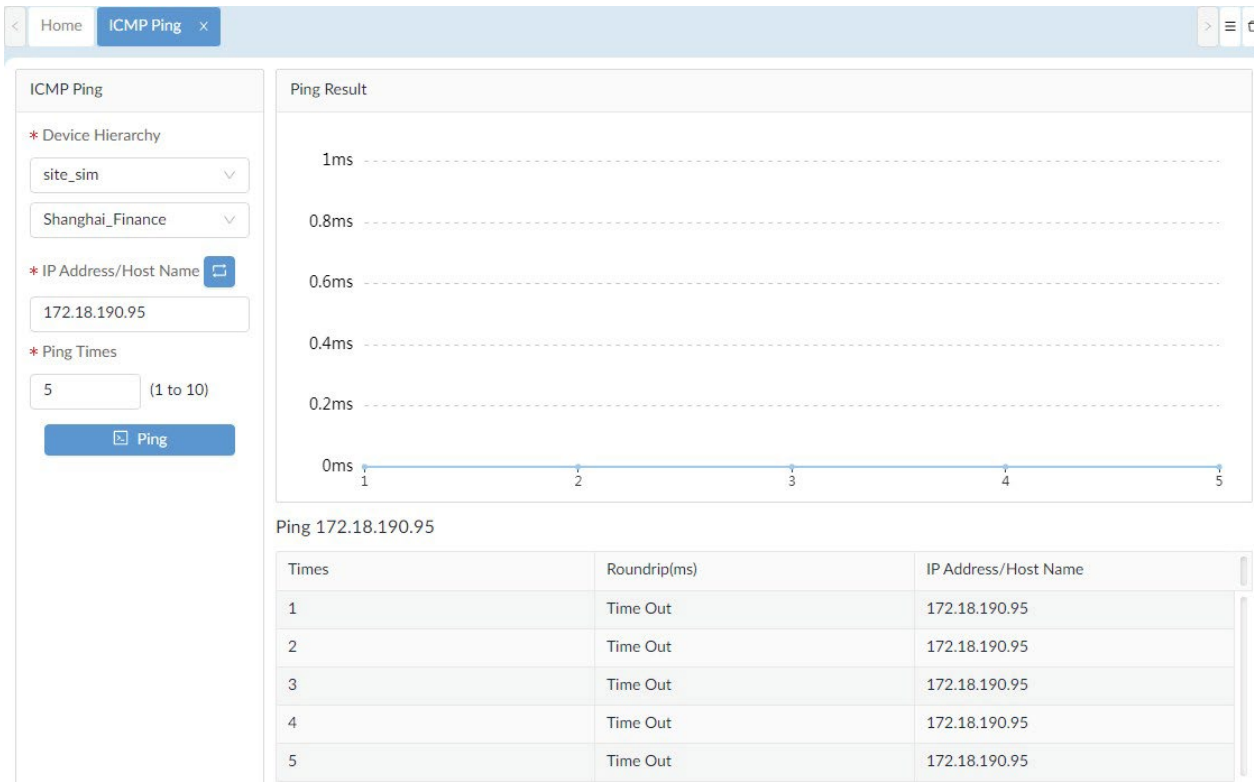


Figure 293 ICMP Ping Overview

3. From the ICMP Ping column, enter the following information to initiate a ping test:
 - Device Hierarchy: click the drop down menu to select the organization, site, and network.
 - Click the Switch Input Mode button to select a drop down menu or manually enter the object's IP address.
 - Enter the number of times (1 to 10) to perform the ping test.
4. Click **Ping** to initiate the test.
The Ping Results display as follows:

14.4. Perform a SNMP Test

SNMP lets administrators monitor discovered devices. You can ping or perform a trace route on a wired or wireless network device. You can specify an SNMP community string and trap. By enabling SNMP v3, you can specify authentication and encryption settings.

To test a device:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click SNMP Test to display the SNMP Parameters page.

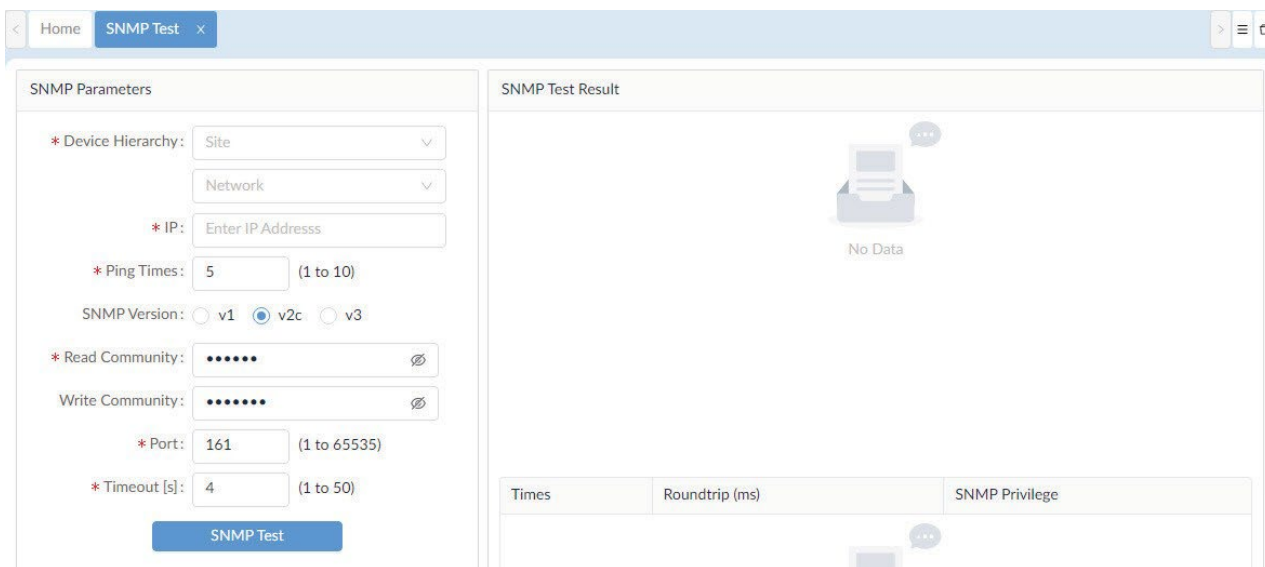


Figure 294 SNMP Parameters Overview

3. From the SNMP Parameters column, enter the following information to initiate a SNMP trap test:

Item	Description
Device Hierarchy*	Click the drop down menu to define the site and network of the SNMP parameters.
IP*	Enter the object's IP address.
Ping Times*	Enter the number of times (1 to 10) to perform the ping test.
SNMP Version	Select the SNMP credential version: v1, v2c, or v3.
Read Community*	Specify the read community string.
Write Community	Specify the write community string.
Port*	Enter the Port (1 to 65535, default: 161) number of the object.
Timeout(s)*	Enter the timeout (1 to 50, default: 4) period in seconds.
SNMP Test	Click SNMP Test to initiate the test.

* Designates required information.

4. Click **SNMP Test** to initiate the test.
The SNMP Test Results display as follows:

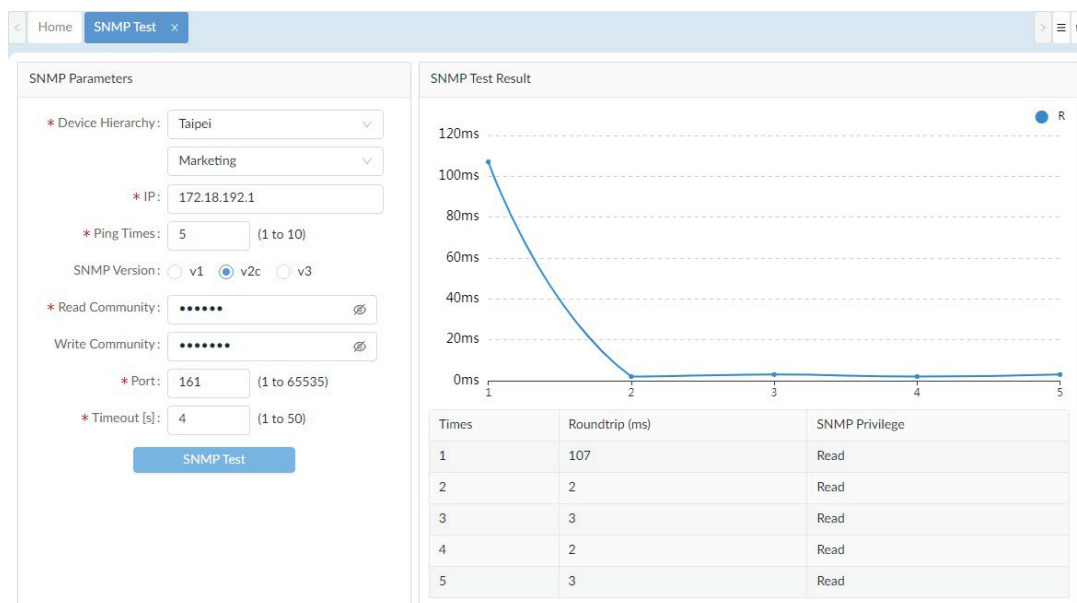
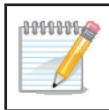


Figure 295 Initiating a SNMP Test

14.5. Perform a Trace Route Test

D-View 8 provides a tool to perform a traceroute test to diagnose the source of a device issues.



NOTE: For effective use of the traceroute tool, it must be run while the network incident is active.

To test a device:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Tools, click **Trace Route** to display the Trace Route page.

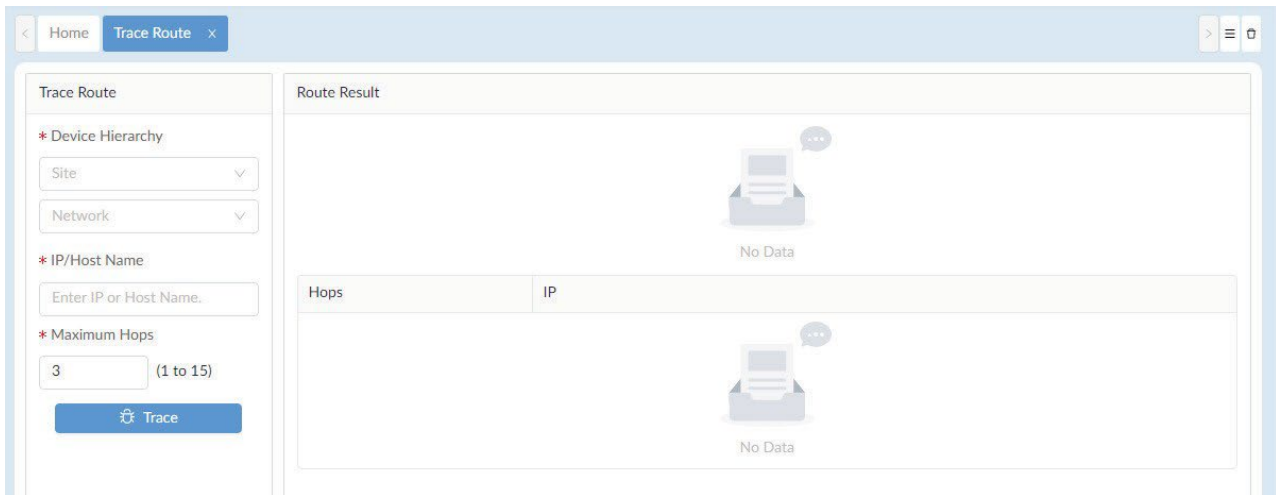


Figure 296 Trace Route Overview

3. From the Trace Route column, enter the following information to initiate a trace route test:
 - Device Hierarchy: click the drop-down menu to select the organization, site, and network.
 - Click the Switch Input Mode button to select a drop-down menu or manually enter the object’s IP address.
 - Enter the maximum number of hops (1 to 15) to take from the target host.
4. Click **Trace** to initiate the test.
The Route Results display as follows:

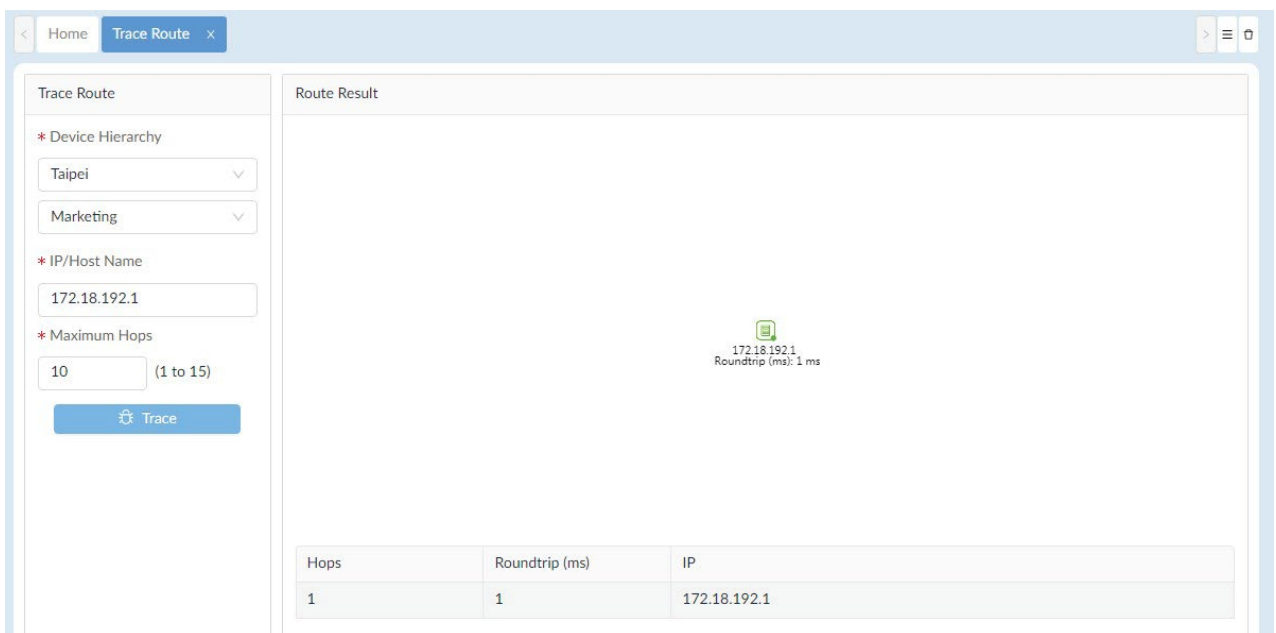


Figure 297 Trace Task Overview

14.6. Configure Network Management from the CLI

The D-View 8 interface is designed with access through command for network configuration and management.

To use the network configuration CLI commands:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under Tools, click **CLI** to display the CLI List page.
3. From the CLI List column, click **Add New Session**.



Figure 298 CLI List Overview
The Add New Session page displays.

Figure 299 Edit Connect Overview

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 an available site.
Network	Click the drop-down menu to select an available network.
IP/Host Name	Enter the IP address or host name of the device to configure.
Protocol	Click the drop-down menu to select the protocol access (SSH/Telnet).
Port	Enter the port number (default: 22) with access to the device.
Username	Enter a username with authority to access the device.
Password	Enter the password assigned to the correlating username.
Cancel	Click to Cancel the session entry.
Connect	Click Connect to initiate the defined session.

5. Click **Connect** to accept the entry. Click **Cancel** to return to the previous menu. The CLI Connection is listed in the CLI List and open in the connection pane.

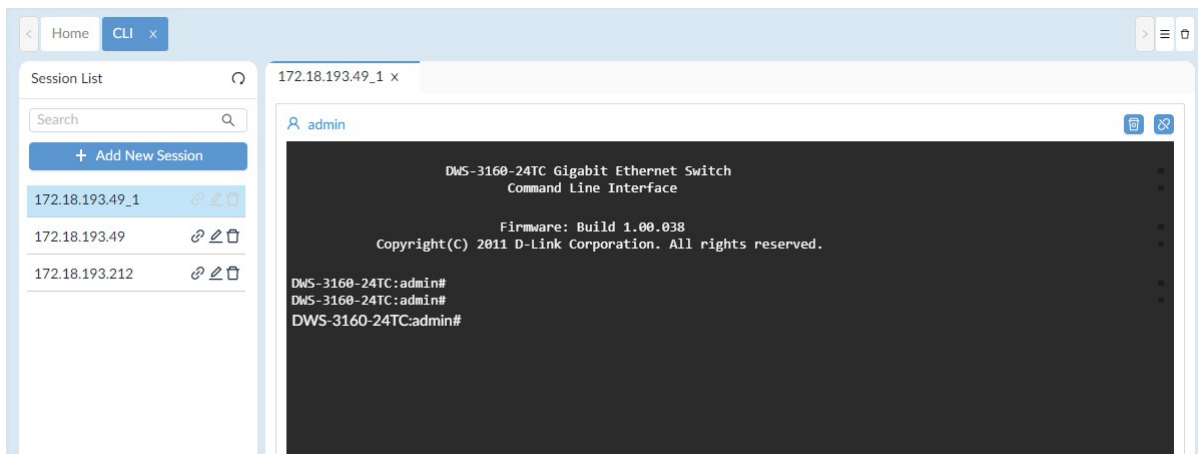


Figure 300 CLI Session Overview

6. To modify or remove a connection list, click on the available options.



Figure 301 CLI Connection Entries

- Connect: initiate a connection
- Edit: modify the settings, opens the Edit Connect page
- Delete: removes the entry from the list

14.7. Compare Configuration Files

The File Comparison tool provides the function to compare two configuration files. Only text files can be compared.

To compare two files:

1. Login to the Dashboard, see “3.2. Launching D-View 8 Web GUI” on page 41.
2. Under **Tools**, click File Comparison to display the File Comparison page.

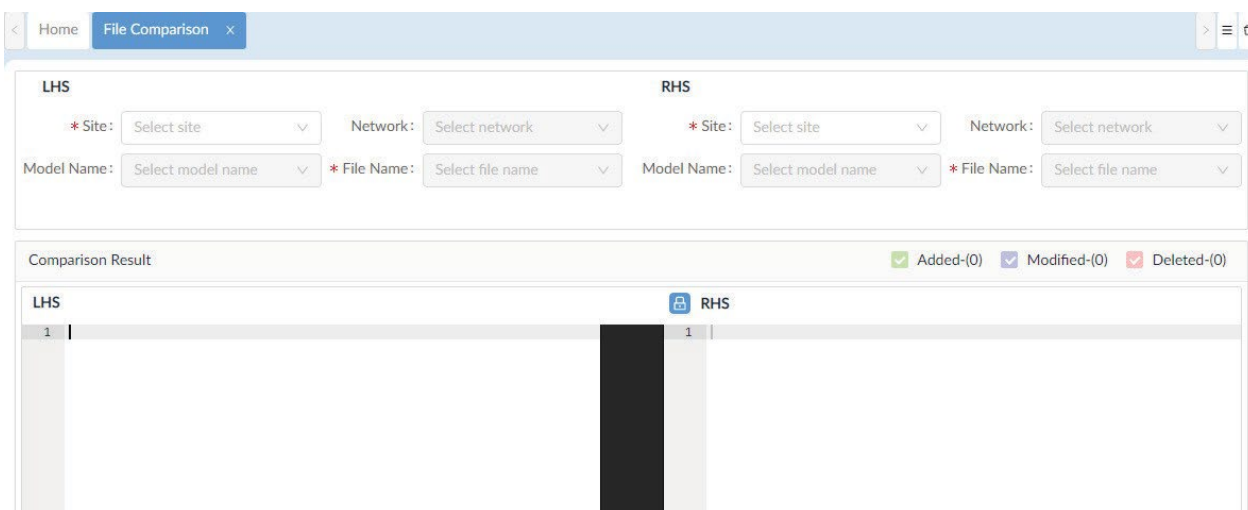


Figure 302 File Comparison Overview

You can select configuration files by criteria such as site, network, device model, and file type.

3. Select the two configuration files to compare.
4. The comparison results displays.

15 Appendix A D-View 8 Cluster Mode Installation Guide

D-View 8 Cluster Mode Installation Guide (1.0.0.2)

Revision History

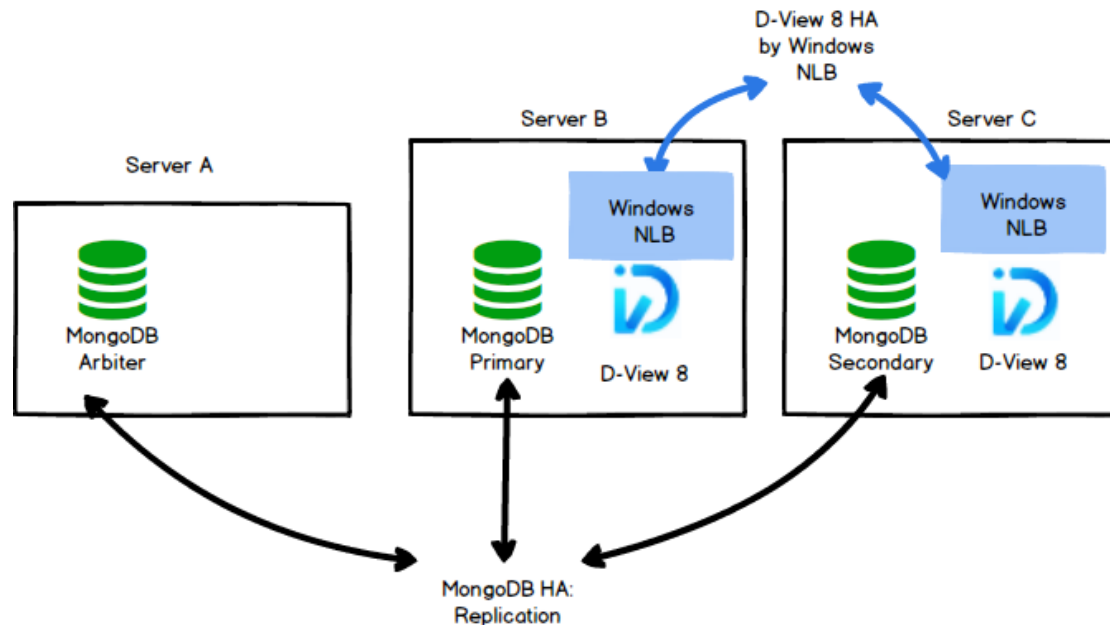
Ver.	Date	Description	Writer
1.0.0.0	2022/4/7	First Release	Longyue Wang
1.0.0.1	2022/4/11	Modified the Scenario 2 > Configuration, to let the description is match with the screenshot	Longyue Wang
1.0.0.2	2022/5/19	Updated the screenshot of "How to verified NLB" based on DJP's feedback.	Longyue Wang

Content

Revision History.....	1
Scenario 1: Install with 3 Windows Servers.....	3
Structure.....	3
Configuration	3
Installation Step	4
Step 1: Setup MongoDB Replication.....	4
Step 2: Setup D-View 8	4
Step 3: Setup NLB	9
How to verified NLB.....	18
Scenario 2: Install D-View 8 Cluster with 5 Windows Servers	24
Structure.....	24
Configuration	24
Installation Step	25
Step 1: Setup MongoDB Replication.....	25
Step 2: Setup D-View 8	25
Step 3: Setup NLB	30

Scenario 1: Install with 3 Windows Servers

Structure



Configuration

We have three Windows PCs and they installed below version.

- SERVER A
 - ◆ 192.168.1.203
 - ◆ MongoDB
 - ◆ OS: Windows 10, Windows Server 2016/ Windows Server 2019
 - ◆ Replica set Role: arbiter
- SERVER B
 - ◆ 192.168.1.201
 - ◆ MongoDB
 - ◆ Replica set Role: primary
 - ◆ OS: Windows Server 2016/ Windows Server 2019
 - ◆ NLB enabled
 - virtual IP: 192.168.1.200
- SERVER C
 - ◆ 192.168.1.202
 - ◆ MongoDB
 - ◆ Replica set Role: secondary

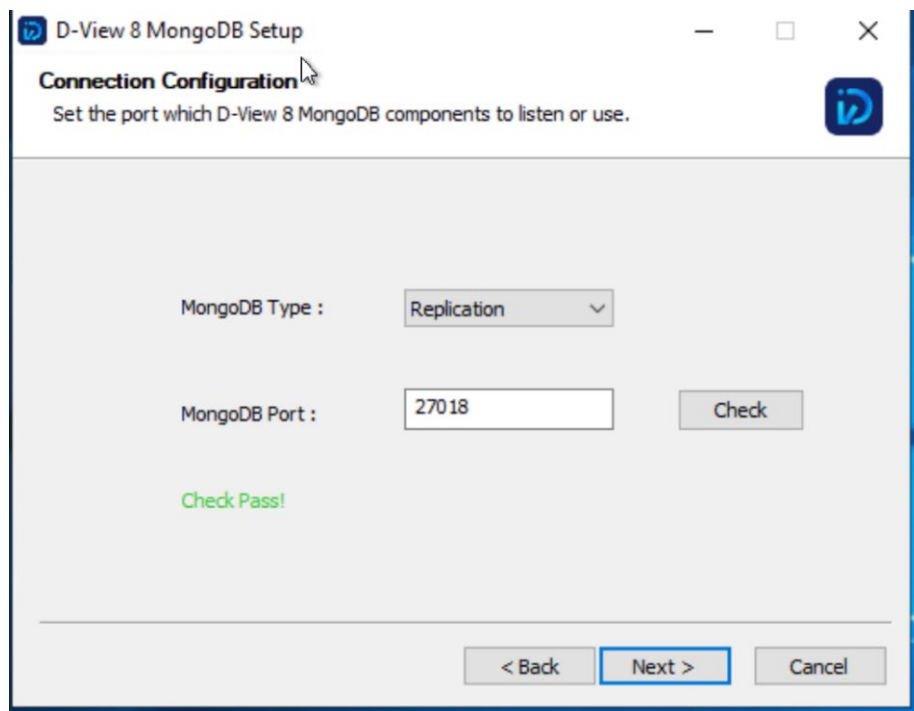
- ◆ OS: Windows Server 2016/ Windows Server 2019
- ◆ NLB enabled
 - virtual IP: 192.168.1.200

Installation Step

Step 1: Setup MongoDB Replication

Install D-View 8 MongoDB_1.0.0.70_Installation.exe to SERVER A, SERVER B and SERVER C

- Select MongoDB type as Replication



Step 2: Setup D-View 8

Install D-View 8_1.0.0.70_Installation.exe to SERVER B and SERVER C.

- SERVER B
 - ◆ Select MongoDB Type as Replication

D-View 8 1.0.0.70 Setup

Port Configuration

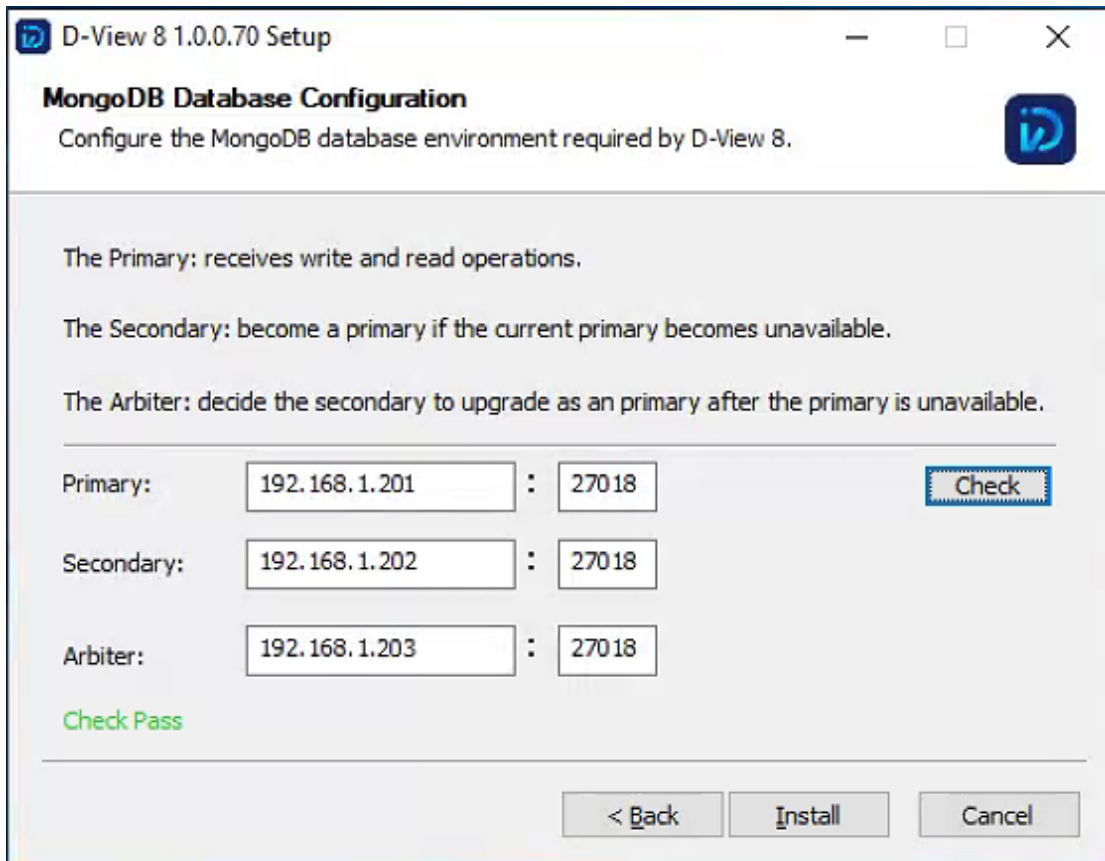
Set the ports which D-View 8 components to listen.

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

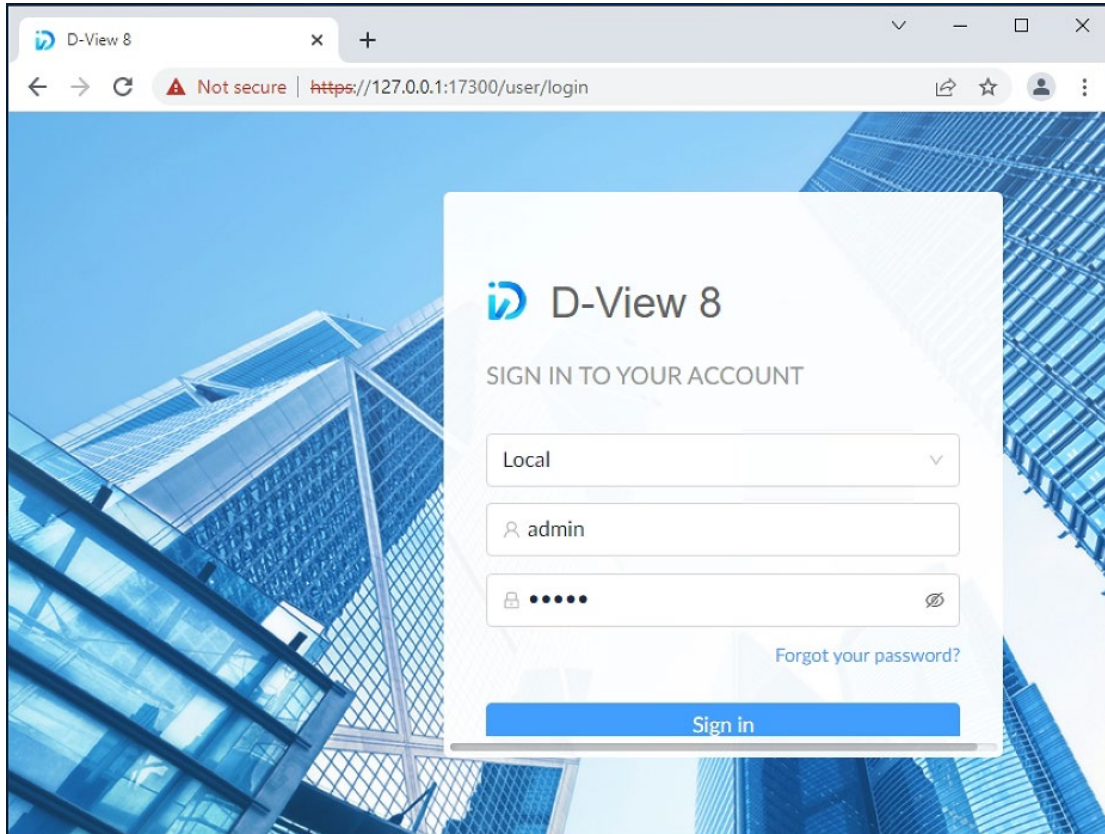
MongoDB Type :	Replication		
Server IP:	192.168.1.201	Check Pass!	Check
Web Port:	17300	Check Pass!	
Core Port:	17500	Check Pass!	
Probe Port:	17600	Check Pass!	

< Back **Next >** Cancel

- ◆ Enter IP address and Port of Primary, Secondary, Arbiter.
- ◆ Click the Check button
- ◆ Do this until the Green "Check Pass" is showed.



◆ Now, the DView8 Server should be accessible from the web browser.



- SERVER C
 - ◆ Select MongoDB type as Replication

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 :

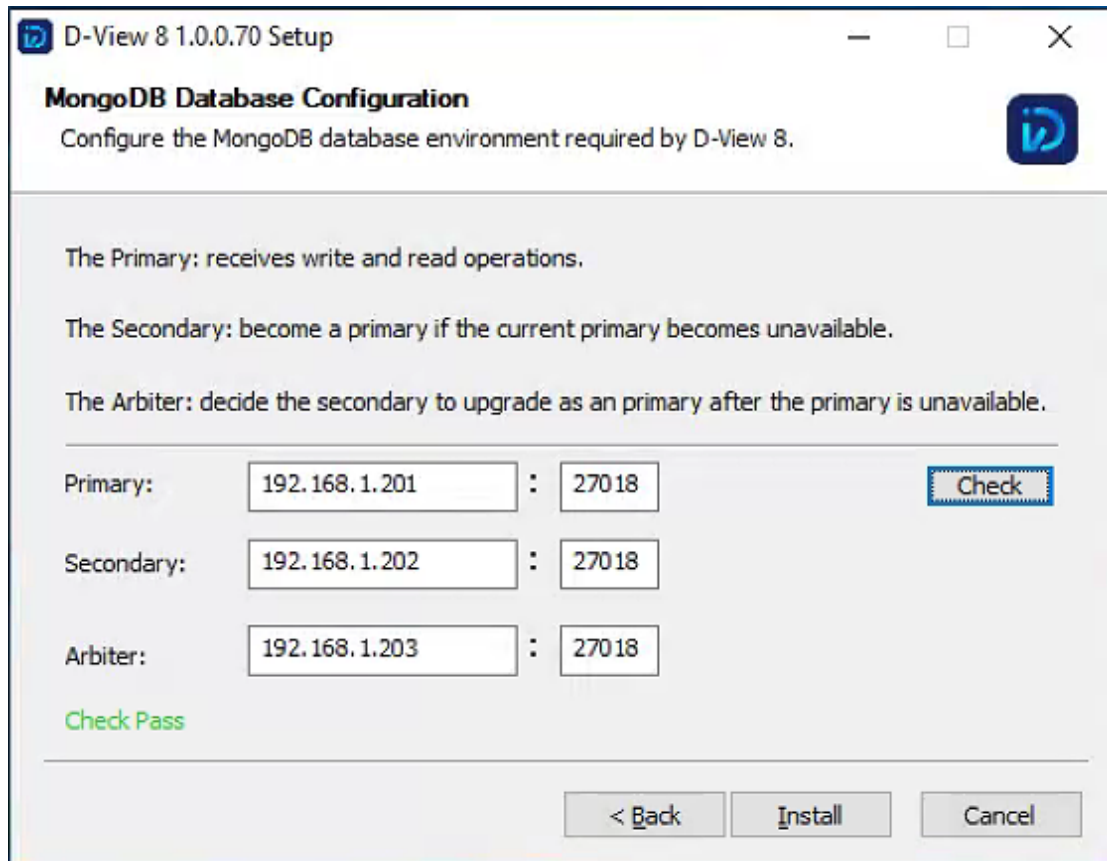
Server IP: Check Pass!

Web Port: Check Pass!

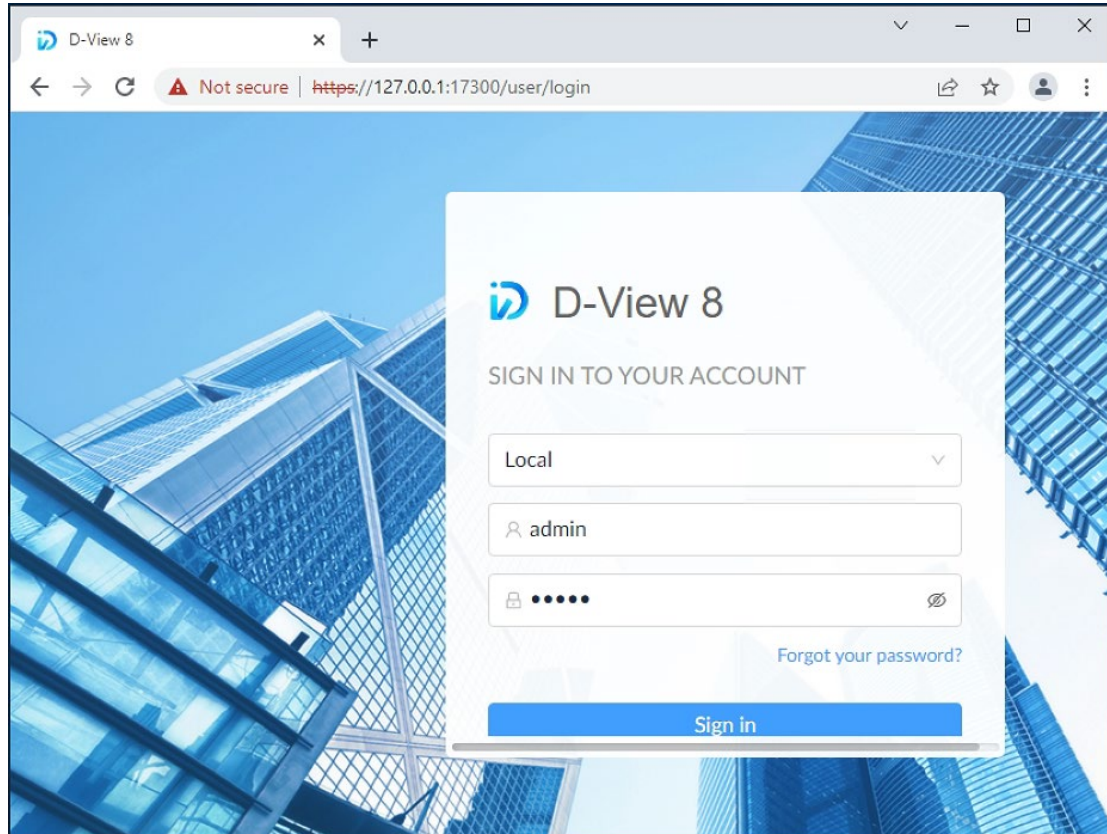
Core Port: Check Pass!

Probe Port: Check Pass!

- ◆ Enter IP address and Port of Primary, Secondary, Arbiter.
- ◆ Click the Check button
- ◆ Do this until the Green "Check Pass" is showed.

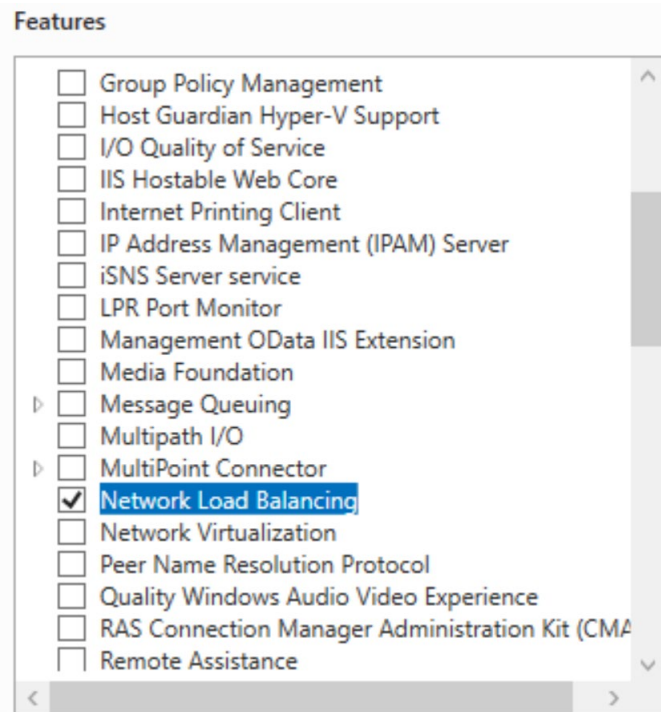


◆ Now the DView8 server should be accessible from the web browser.

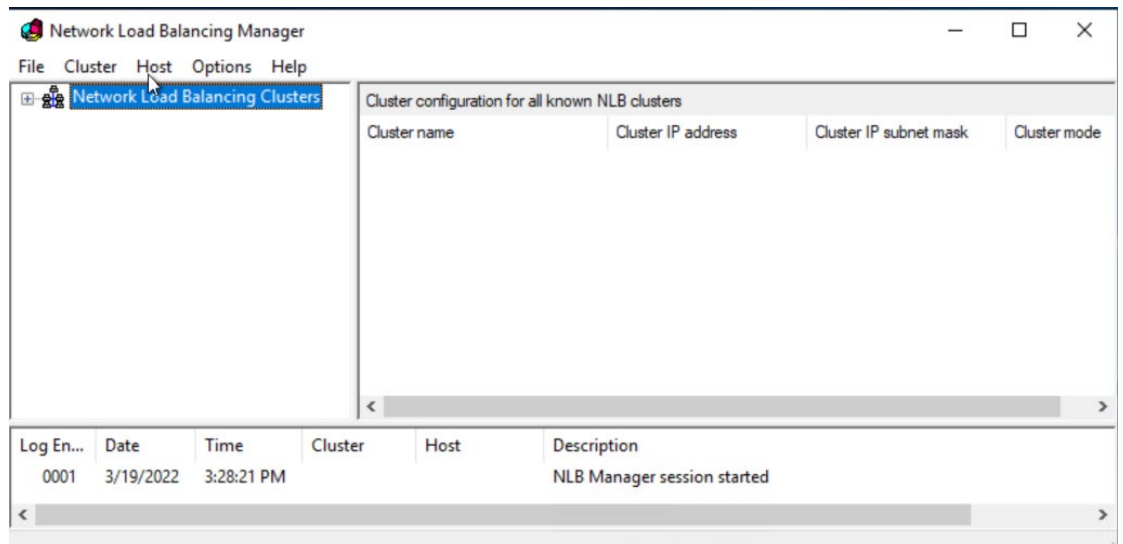


Step 3: Setup NLB

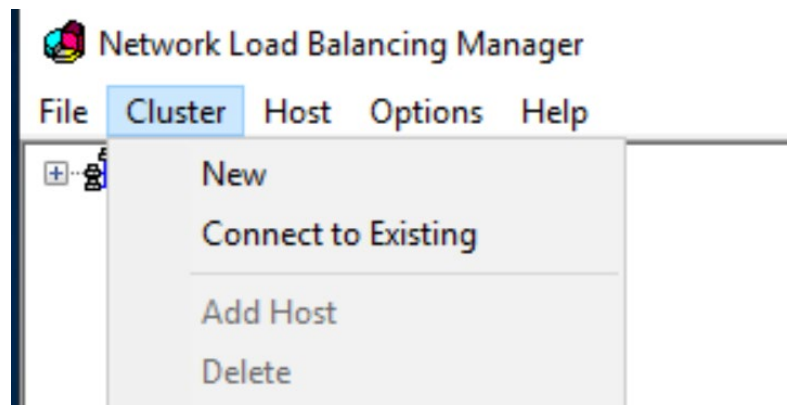
- Make sure the Network Load Balancing feature is installed on SERVER B and SERVER C.



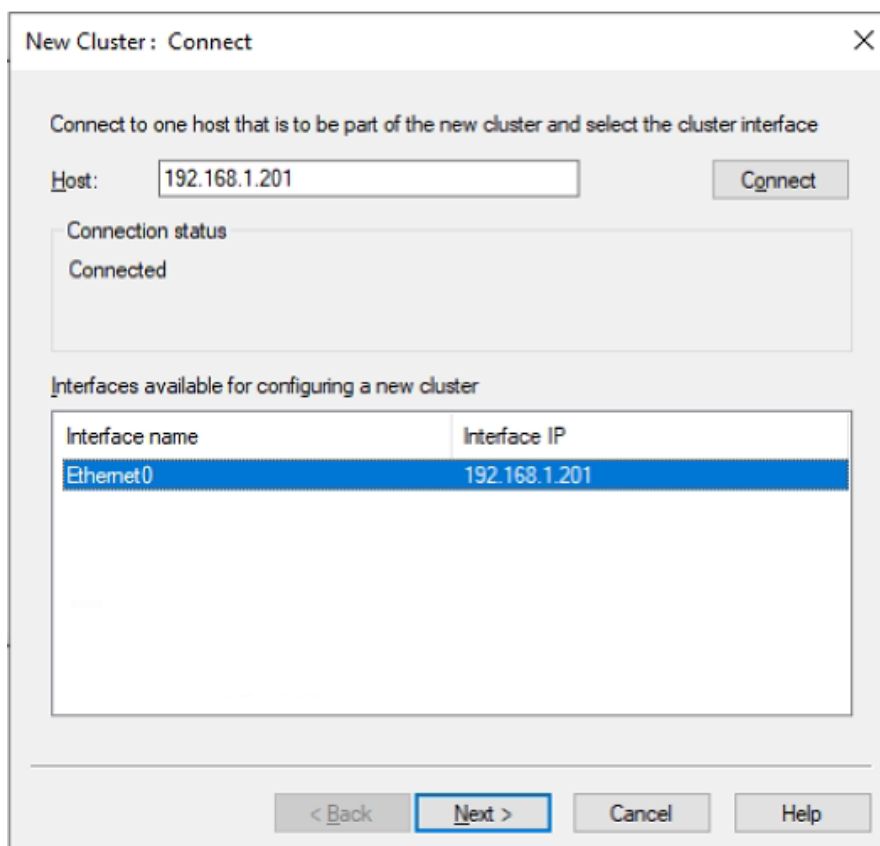
- Open the Network Load Balancing Manager on SERVER B and SERVER C respectively.



- SERVER B
 - ◆ Cluster -> New



- ◆ In this page, enter its IP, 192.168.1.201 and click the Connect button.



- ◆ In this page, click the Next button

New Cluster : Host Parameters

Priority (unique host identifier): 1

Dedicated IP addresses

IP address	Subnet mask
192.168.1.201	255.255.255.0

Add... Edit... Remove

Initial host state

Default state: Started

Retain suspended state after computer restarts

< Back Next > Cancel Help

◆ In this page, click the Add button.

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

Add... Edit... Remove

< Back Next > Cancel Help

- ◆ Enter a virtual IP and netmask that will be used as the Cluster IP and netmask.

The screenshot shows a 'New Cluster: Cluster IP Addresses' dialog box. It contains a text area with instructions: '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 heartbeat.' Below this is a list of cluster IP addresses. An 'Add IP Address' sub-dialog is open, allowing the user to add a new IP address. The sub-dialog has three radio buttons: 'Add IPv4 address:' (selected), 'Add IPv6 address:', and 'Generate IPv6 addresses:'. Under 'Add IPv4 address:', the IPv4 address is '192.168.1.200' and the subnet mask is '255.255.255.0'. Under 'Generate IPv6 addresses:', there are three checkboxes: 'Link-local' (checked), 'Site-local', and 'Global'. The sub-dialog has 'OK' and 'Cancel' buttons. The main dialog has '< Back', 'Next >', 'Cancel', and 'Help' buttons.

- ◆ In this page, select Multicast in Cluster Operation Mode to provide a better performance.

The screenshot shows a 'New Cluster: Cluster Parameters' dialog box. It has two main sections. The first section is 'Cluster IP configuration' and contains four fields: 'IP address:' with a dropdown menu showing '192.168.1.200', 'Subnet mask:' with '255.255.255.0', 'Full Internet name:' with an empty text box, and 'Network address:' with '03-bf-c0-a8-01-c8'. The second section is 'Cluster operation mode' and contains three radio buttons: 'Unicast', 'Multicast' (selected), and 'IGMP multicast'. The dialog has '< Back', 'Next >', 'Cancel', and 'Help' buttons.

- ◆ In this page, Click the Edit button

New Cluster : Port Rules

Defined port rules:

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

< >

Add... Edit... Remove

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.

< Back Finish Cancel Help

- ◆ In this page, Select the Filtering mode as “Multiple host”, select the Affinity as “None”

Add/Edit Port Rule [X]

Cluster IP address
 or All

Port range
 From: To:

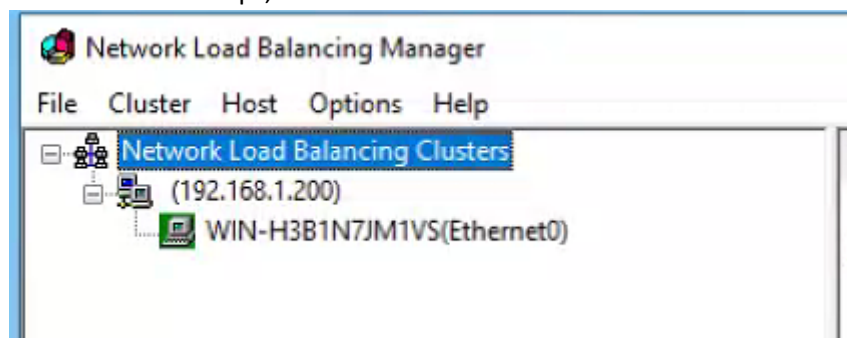
Protocols
 TCP UDP Both

Filtering mode
 Multiple host Affinity: None Single Network
 Timeout(in minutes):

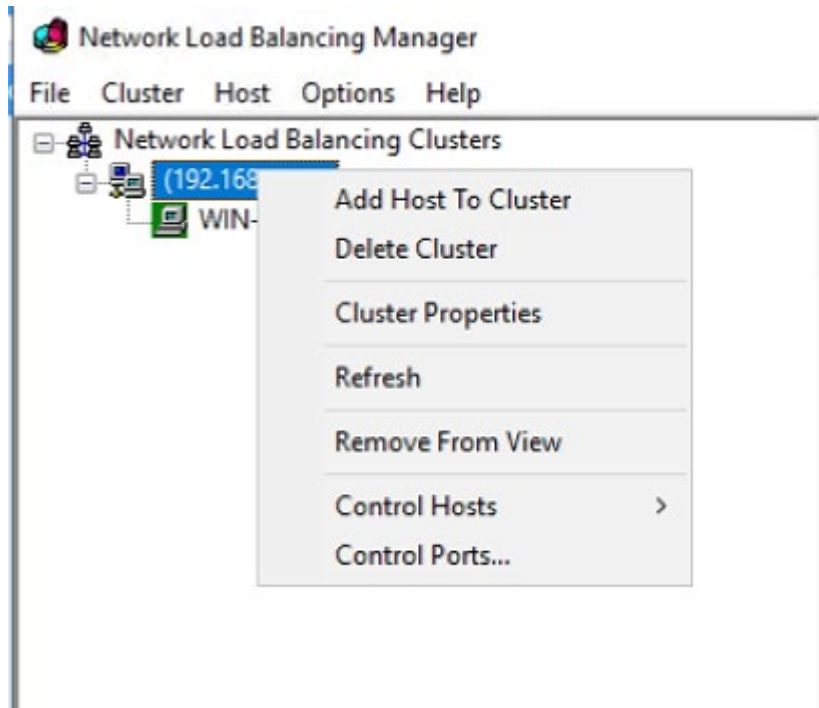
Single host

Disable this port range

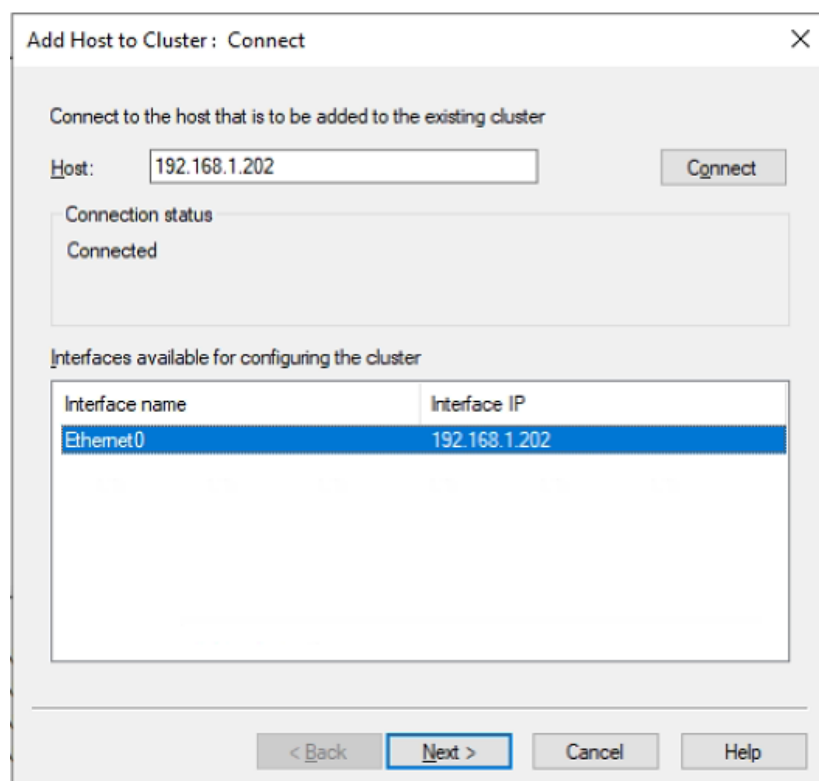
- ◆ After the above steps, a NLB cluster was created



- ◆ Then add the SERVER C to this cluster, Right click the cluster node, click the "Add Host To Cluster"



- ◆ In this page, input the SERVER C's IP (192.168.1.202) and click Connect button



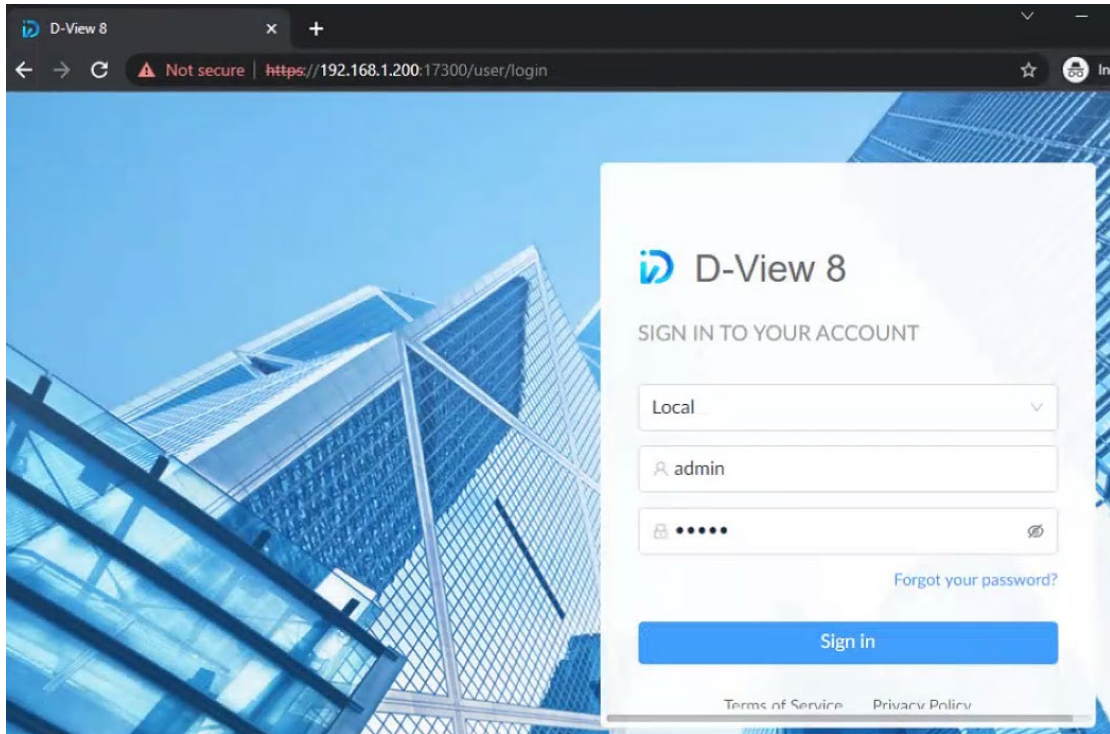
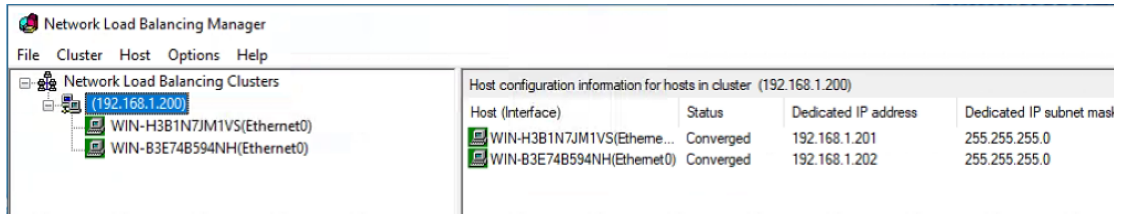
- ◆ In this page, click the Next button

The screenshot shows a dialog box titled "Add Host to Cluster: Host Parameters". At the top, there is a "Priority (unique host identifier):" dropdown menu set to "2". Below this is a section for "Dedicated IP addresses" containing a table with two columns: "IP address" and "Subnet mask". The table has one row with the values "192.168.1.202" and "255.255.255.0". Below the table are three buttons: "Add...", "Edit...", and "Remove". Underneath is the "Initial host state" section, which includes a "Default state:" dropdown menu set to "Started" and a checkbox labeled "Retain suspended state after computer restarts" which is currently unchecked. At the bottom of the dialog are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

- ◆ In this page, click the Finish button

The screenshot shows a dialog box titled "Add Host to Cluster: Port Rules". It features a table of "Defined port rules" with the following columns: "Cluster IP address", "Start", "End", "Prot...", "Mode", "Priority", "Load", and "Affinity". The first row is highlighted in blue and contains the values: "All", "0", "65535", "Both", "Multiple", "-", "Equal", and "None". Below the table are three buttons: "Add...", "Edit...", and "Remove". Underneath is a "Port rule description" text box containing the text: "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." At the bottom of the dialog are four buttons: "< Back", "Finish" (highlighted with a blue border), "Cancel", and "Help".

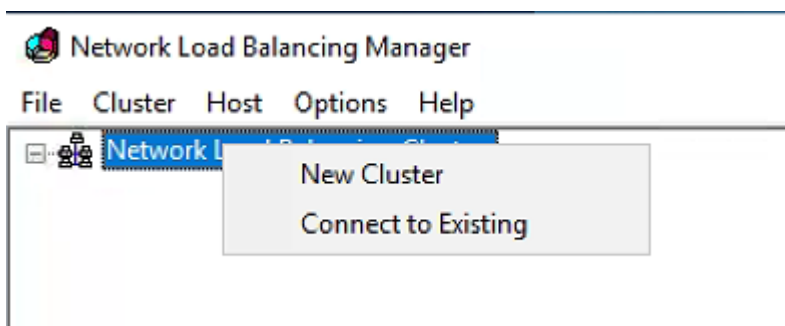
- ◆ Now a cluster includes SERVER B and SERVER C was created. And the DV8 can be accessed with the cluster IP.



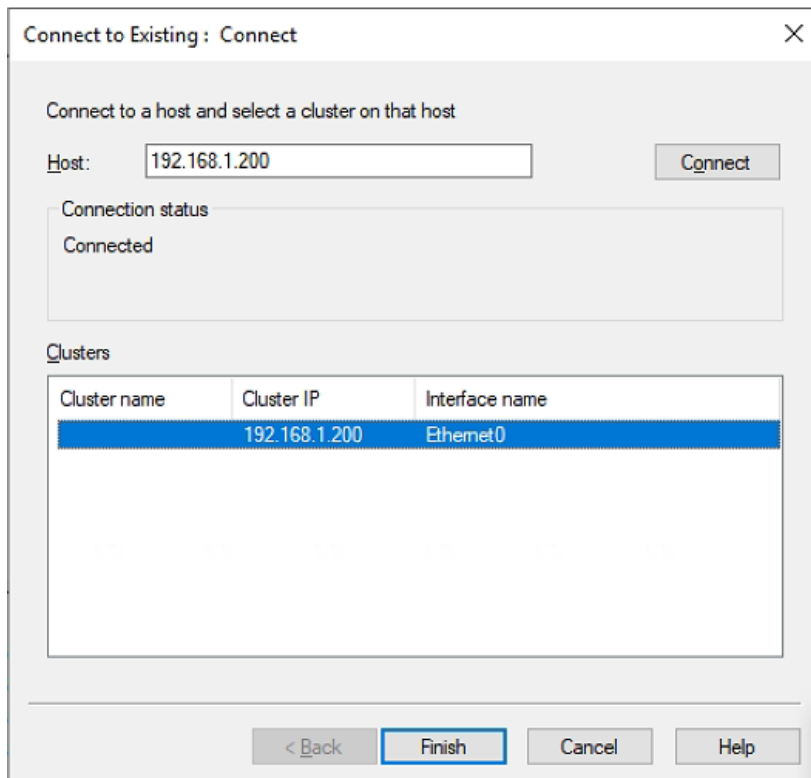
■ **SERVER C**

If you want to manage the NLB cluster on SERVER C, you can do the following steps:

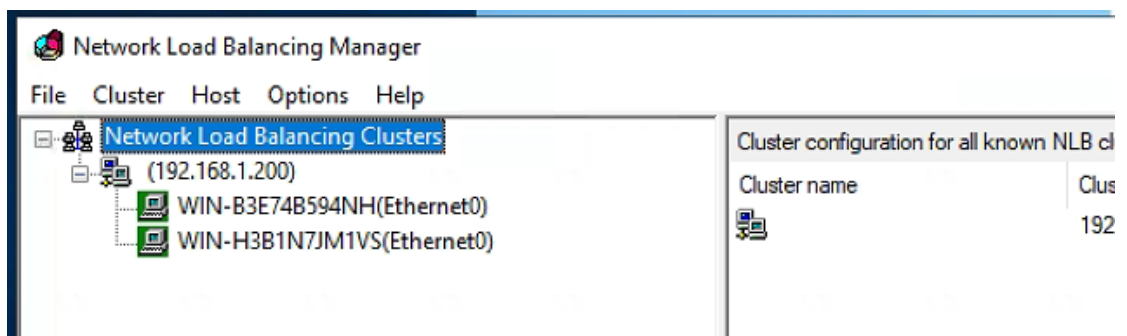
- ◆ Cluster -> Connect to Existing



- ◆ In this page, enter the NLB cluster IP, 192.168.1.200 and click the Connect button.

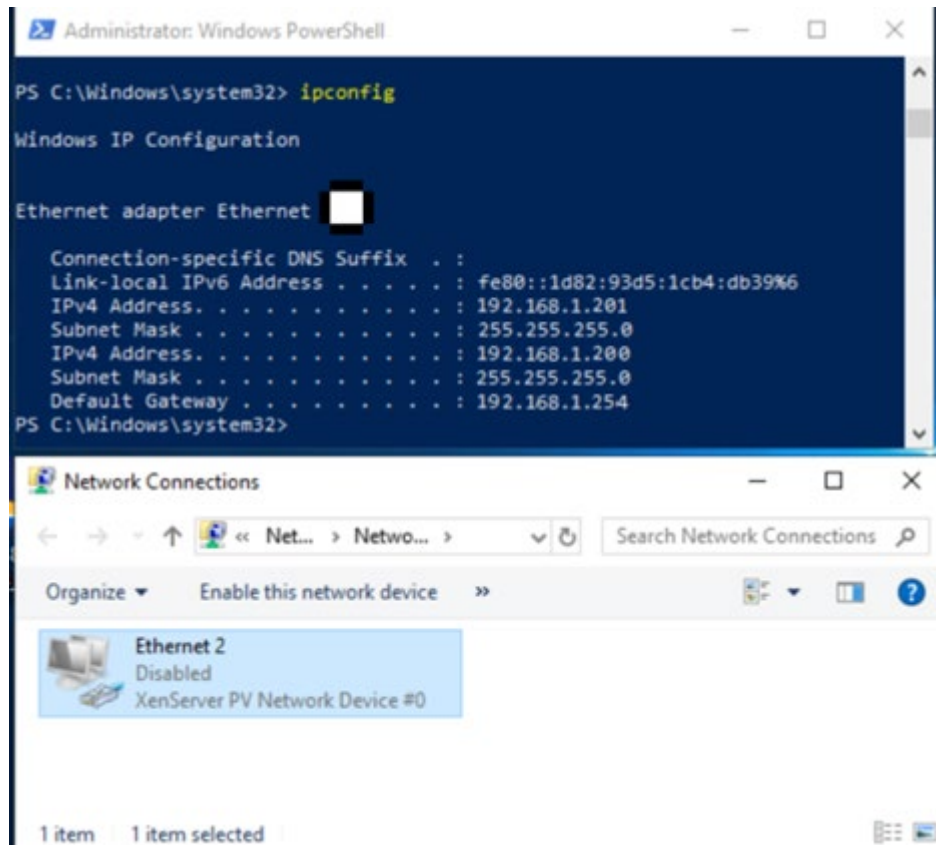


◆ After that, you can see the NLB cluster info in SERVER C.

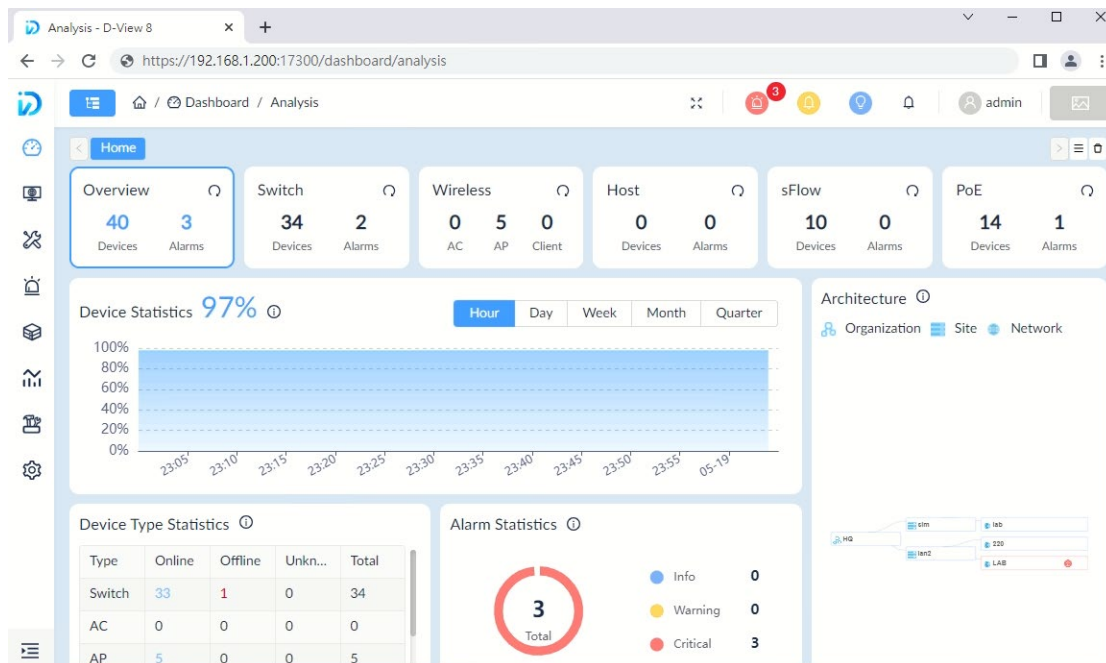


How to verified NLB.

- Disable SERVER B (192.168.1.201)'s network adaptor.



- Go to another PC, and open the <https://192.168.1.200:17300> OR <https://192.168.1.202:17300>, it connected via SERVER C. <https://192.168.1.201:17300> is inaccessible now.



The screenshot shows a web-based network management dashboard. The browser address bar displays the URL: `https://192.168.1.202:17300/dashboard/analysis`. The dashboard includes several widgets:

- Overview:** 40 Devices, 3 Alarms.
- Switch:** 34 Devices, 2 Alarms.
- Wireless:** 0 AC, 5 AP, 0 Client.
- Host:** 0 Devices, 0 Alarms.
- sFlow:** 10 Devices, 0 Alarms.
- PoE:** 14 Devices, 1 Alarm.
- Device Statistics:** A bar chart showing 97% availability over time.
- Architecture:** A tree view showing Organization, Site, and Network.
- Device Type Statistics:**

Type	Onli...	Offli...	Unk...	Total
Swit...	33	1	0	34
AC	0	0	0	0
AP	5	0	0	5
- Alarm Statistics:** 3 Total alarms, categorized as Info (0), Warning (0), and Critical (3).

Below the dashboard, a browser window shows the address `192.168.1.201` and the error message `ERR_CONNECTION_TIMED_OUT`.



無法連上這個網站

192.168.1.201 的回應時間過長。

建議做法：

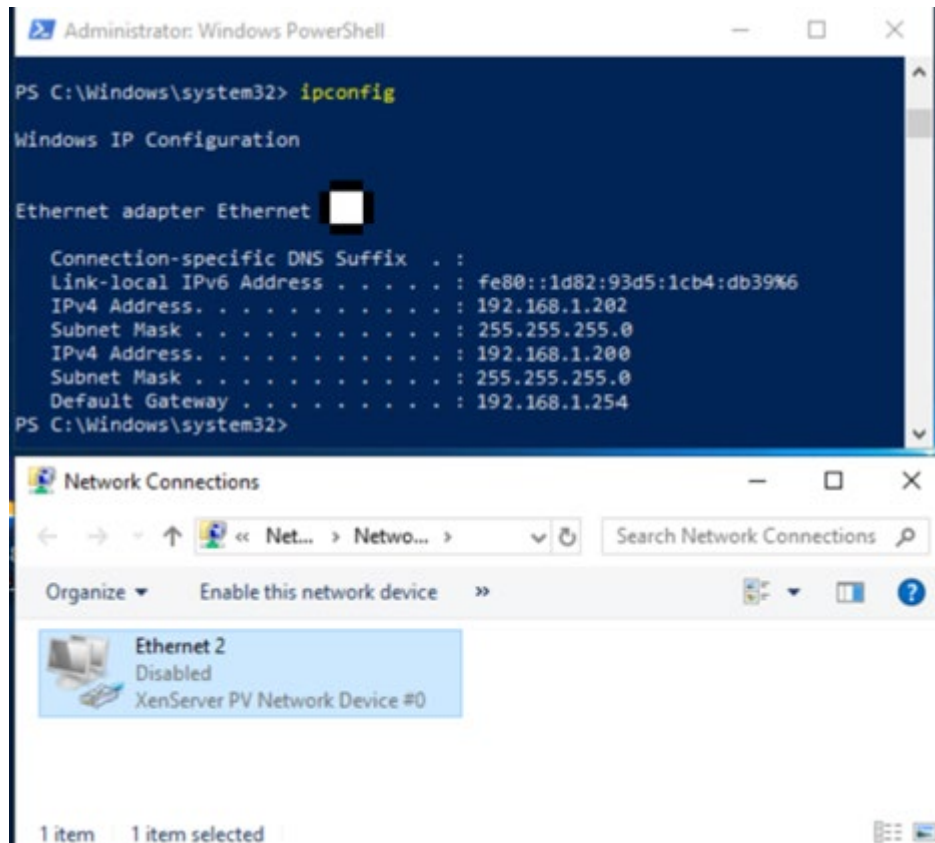
- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

ERR_CONNECTION_TIMED_OUT

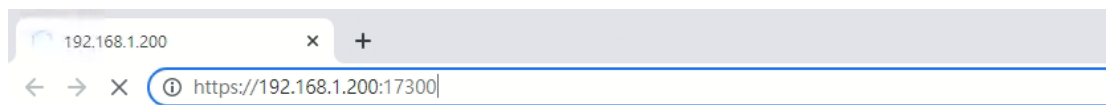
重新載入

詳細資料

- Disable SERVER C(192.168.1.202)'s network adaptor



- Go to another PC, all of the following url are inaccessible.
<https://192.168.1.200:17300>
<https://192.168.1.201:17300>
<https://192.168.1.202:17300>.



無法連上這個網站

192.168.1.200 的回應時間過長。

建議做法：

- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

ERR_CONNECTION_TIMED_OUT

重新載入

詳細資料



無法連上這個網站

192.168.1.201 的回應時間過長。

建議做法：

- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

ERR_CONNECTION_TIMED_OUT

重新載入

詳細資料



無法連上這個網站

192.168.1.202 的回應時間過長。

建議做法：

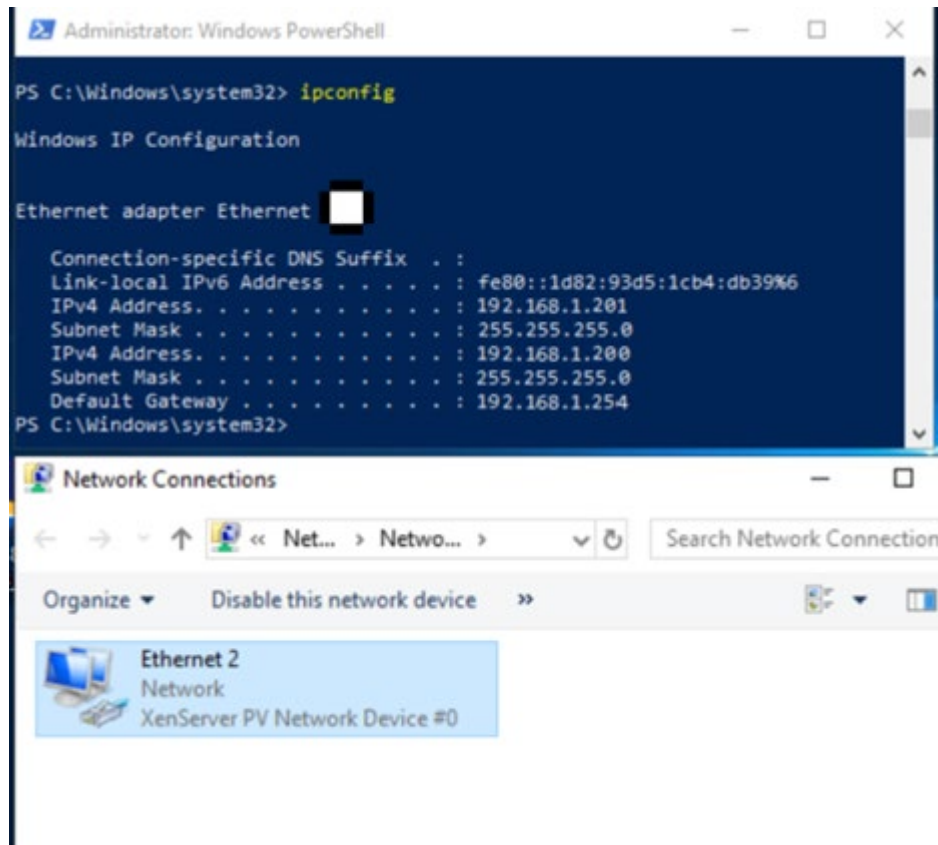
- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

ERR_CONNECTION_TIMED_OUT

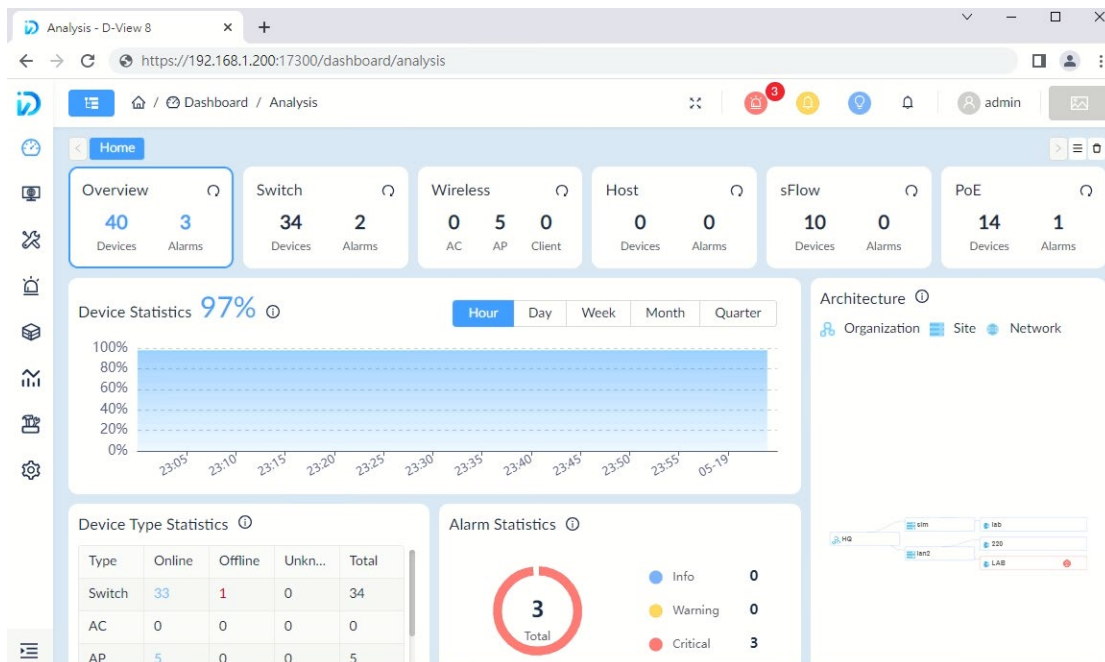
重新載入

詳細資料

- Enable SERVER B's network adaptor.

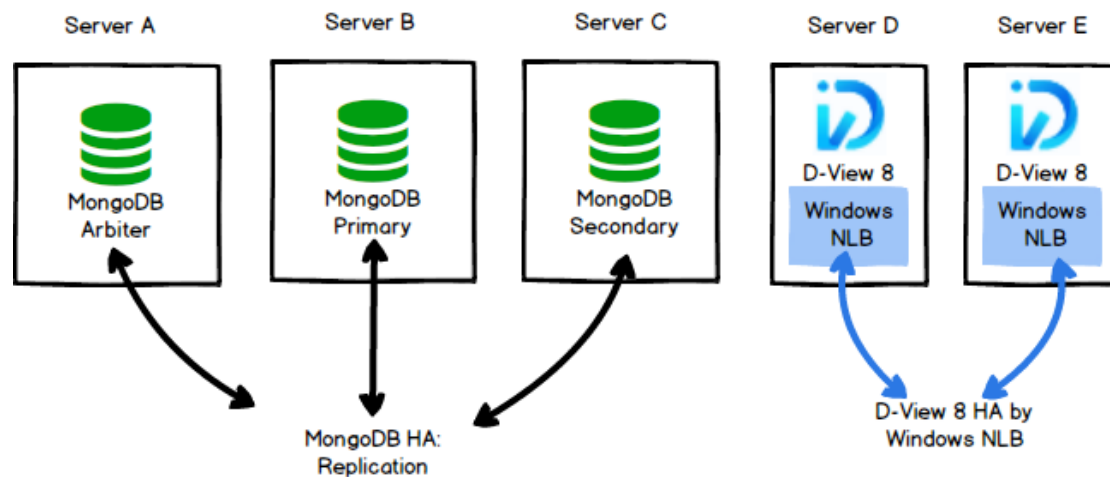


- Go to another PC, now <https://192.168.1.200> is accessible. It connected via SERVER B.



Scenario 2: Install D-View 8 Cluster with 5 Windows Servers

Structure



Configuration

We have five Windows PCs and they installed below version.

- SERVER A
 - ◆ 192.168.1.205
 - ◆ MongoDB
 - ◆ OS: Windows 10, Windows Server 2016/ Windows Server 2019
 - ◆ Replica set Role: arbitrator
- SERVER B
 - ◆ 192.168.1.203
 - ◆ MongoDB
 - ◆ Replica set Role: primary
 - ◆ OS: Windows 10, Windows Server 2016/ Windows Server 2019
- SERVER C
 - ◆ 192.168.1.204
 - ◆ MongoDB
 - ◆ Replica set Role: secondary
 - ◆ OS: Windows 10, Windows Server 2016/ Windows Server 2019
- SERVER D
 - ◆ 192.168.1.201

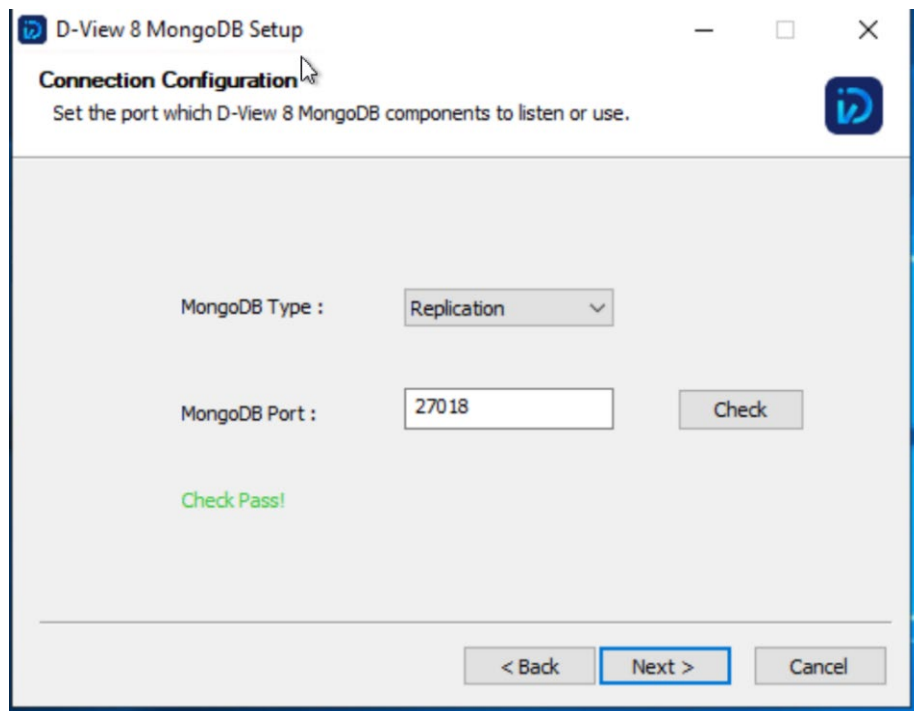
- ◆ D-View 8
- ◆ OS: Windows Server 2016/ Windows Server 2019
- ◆ NLB enabled
 - virtual IP: 192.168.1.200
- SERVER E
 - ◆ 192.168.1.202
 - ◆ D-View 8
 - ◆ OS: Windows Server 2016/ Windows Server 2019
 - ◆ NLB enabled
 - virtual IP: 192.168.1.200

Installation Step

Step 1: Setup MongoDB Replication

Install D-View 8 MongoDB_1.0.0.70_Installation.exe to SERVER A, SERVER B and SERVER C

- Select MongoDB type as Replication



Step 2: Setup D-View 8

Install D-View 8_1.0.0.70_Installation.exe to SERVER D and SERVER E.

- SERVER D

- ◆ Select MongoDB Type as Replication

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 :

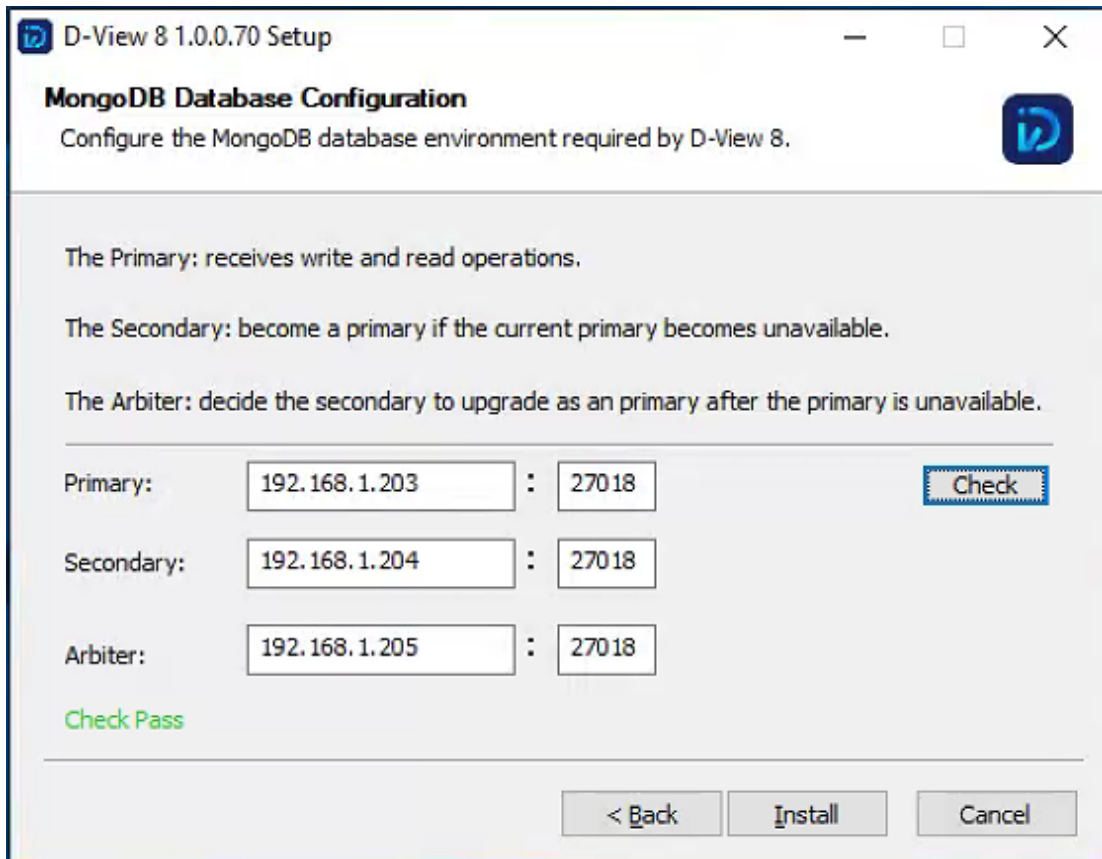
Server IP: Check Pass!

Web Port: Check Pass!

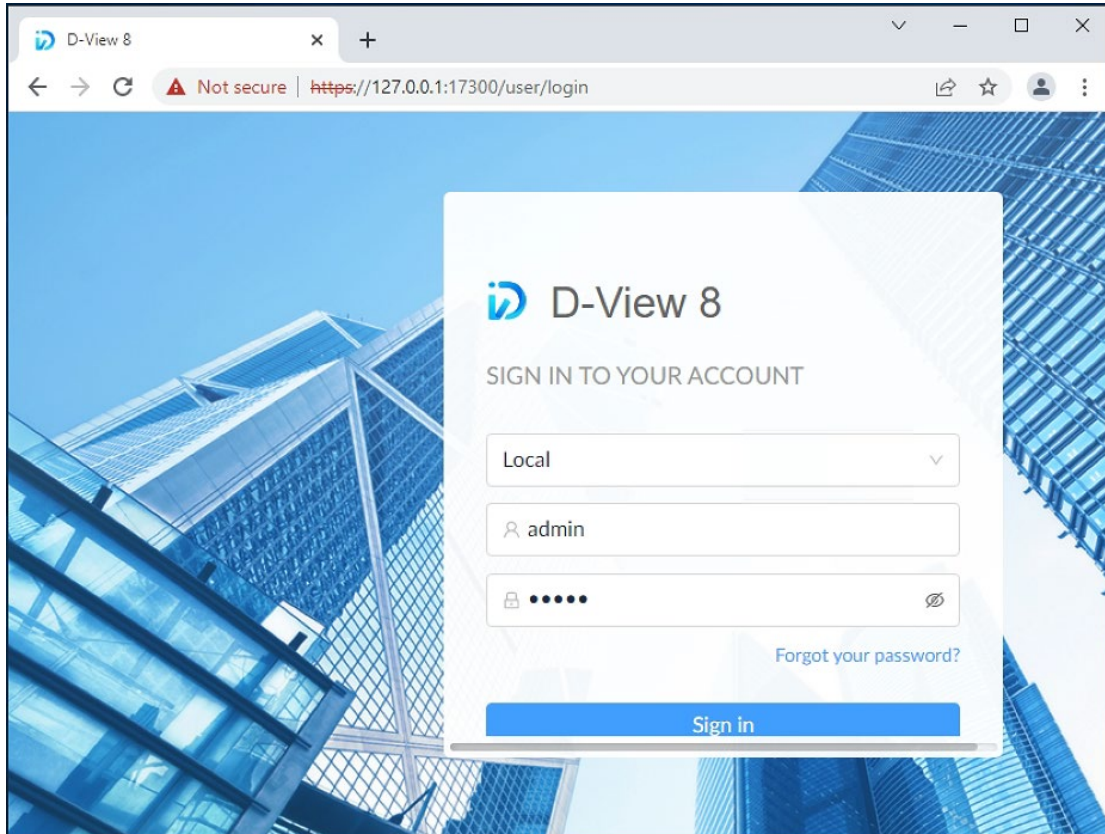
Core Port: Check Pass!

Probe Port: Check Pass!

- ◆ Enter IP address and Port of Primary, Secondary, Arbiter.
- ◆ Click the Check button
- ◆ Do this until the Green "Check Pass" is showed.



◆ Now, the DView8 Server should be accessible from the web browser.



- SERVER E
 - ◆ Select MongoDB type as Replication

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 :

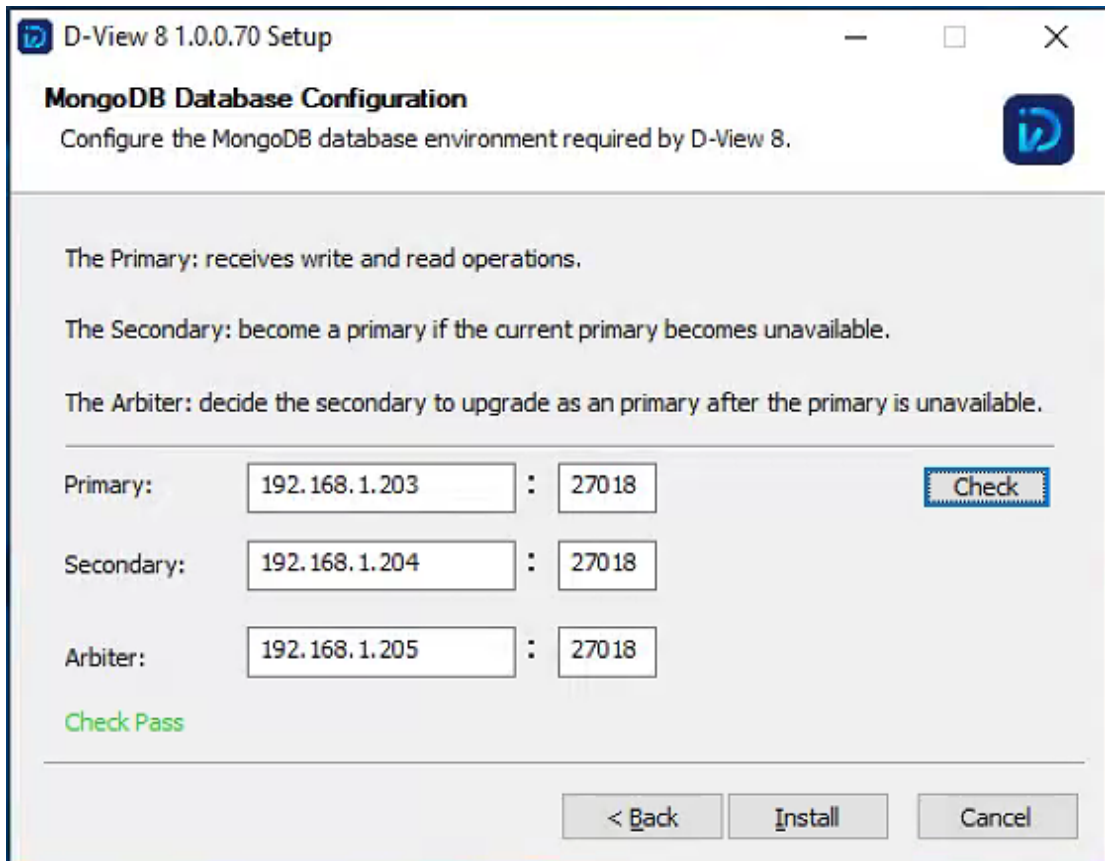
Server IP: Check Pass!

Web Port: Check Pass!

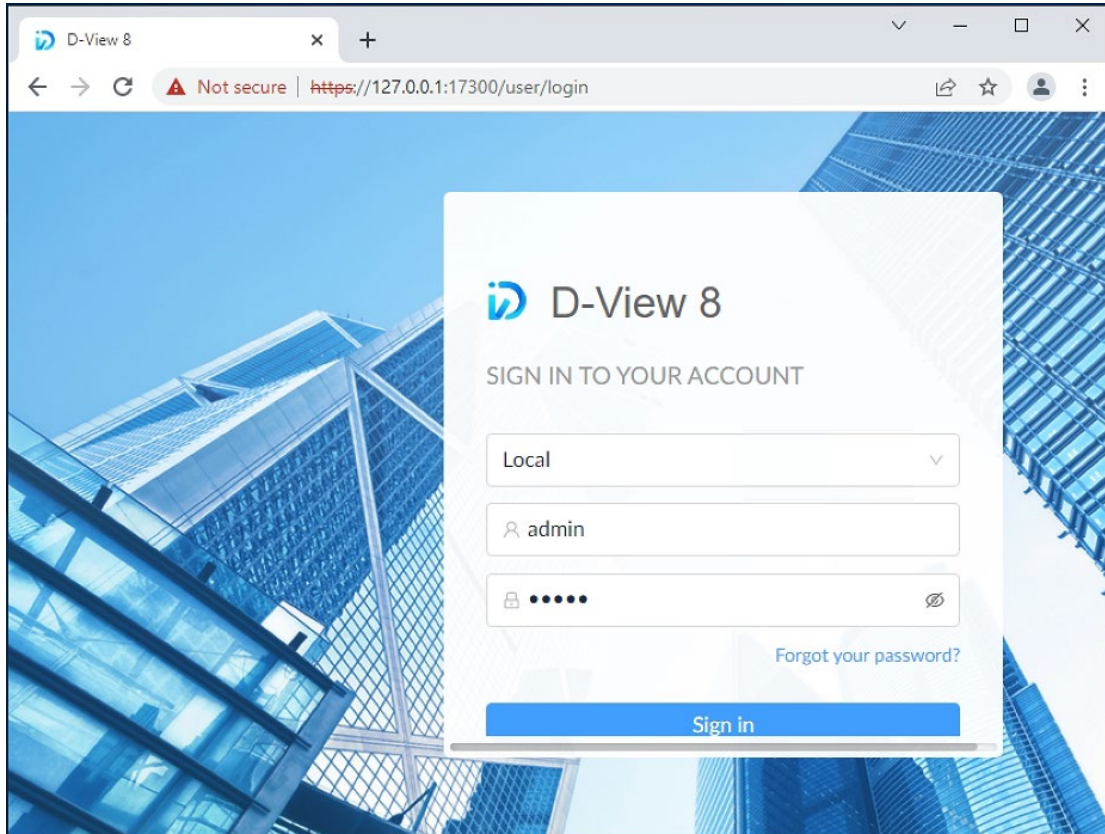
Core Port: Check Pass!

Probe Port: Check Pass!

- ◆ Enter IP address and Port of Primary, Secondary, Arbiter.
- ◆ Click the Check button
- ◆ Do this until the Green "Check Pass" is showed.

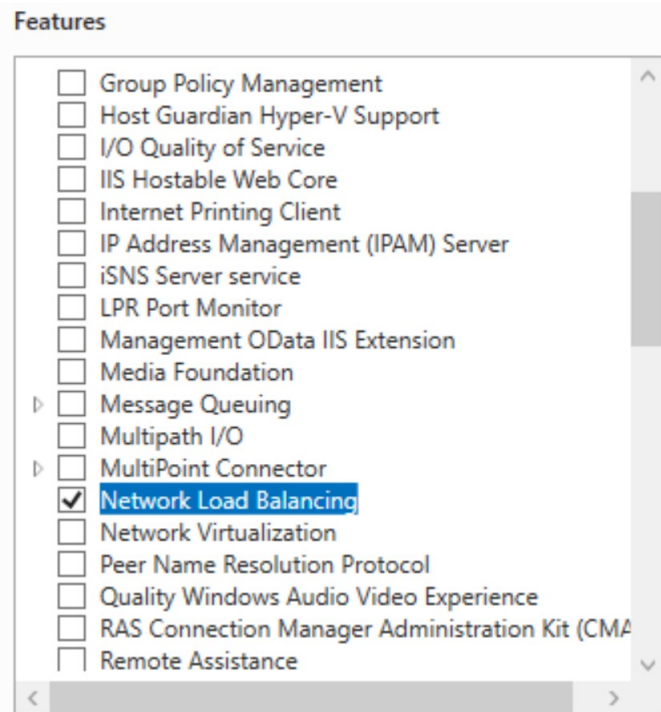


◆ Now the DView8 server should be accessible from the web browser.

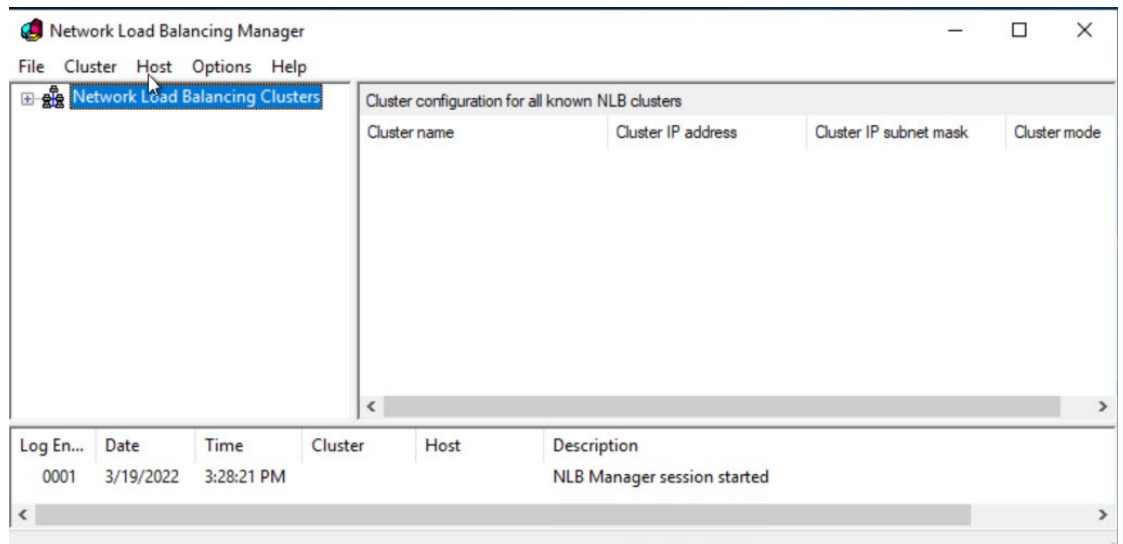


Step 3: Setup NLB

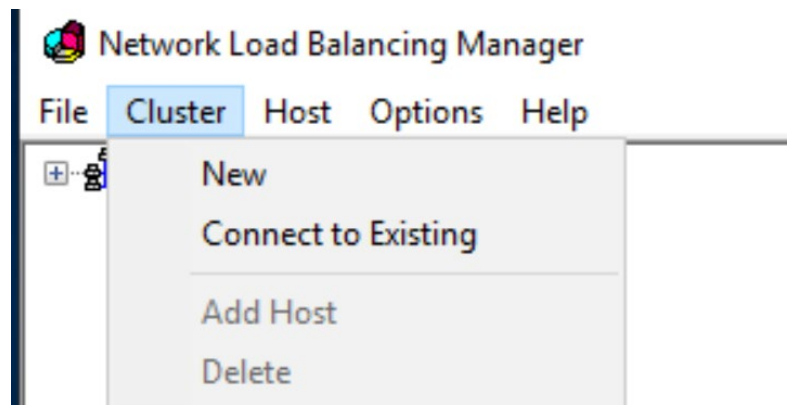
- Make sure the Network Load Balancing feature is installed on SERVER D and SERVER E.



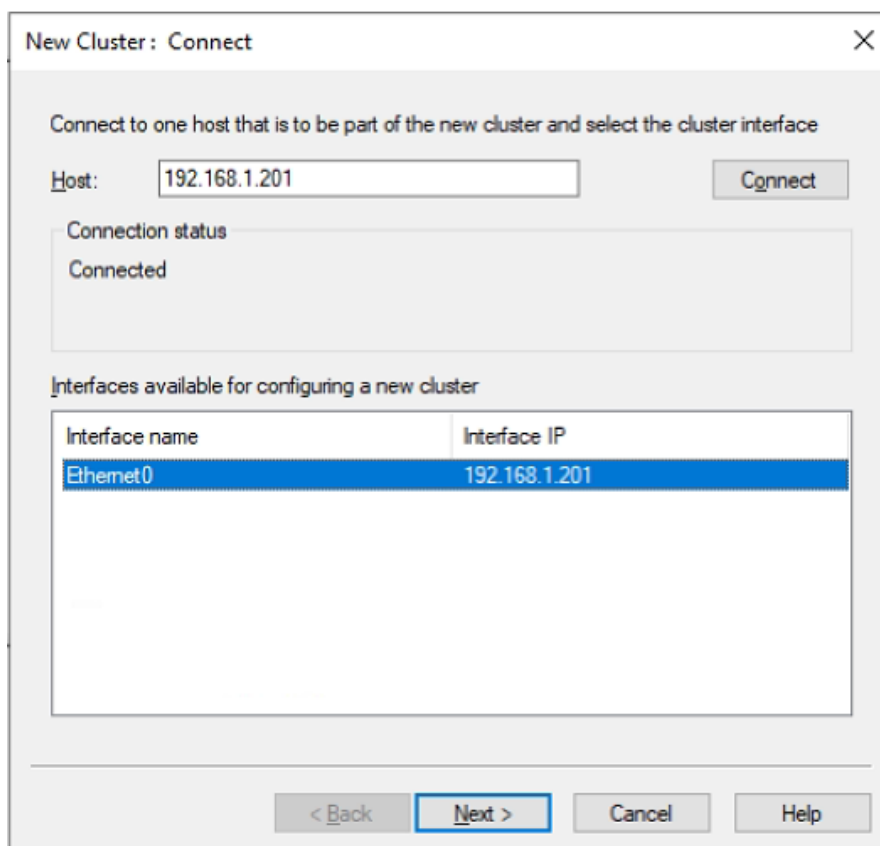
- Open the Network Load Balancing Manager on SERVER D and SERVER E respectively.



- SERVER D
 - ◆ Cluster -> New



- ◆ In this page, enter its IP, 192.168.1.201 and click the Connect button.



- ◆ In this page, click the Next button

New Cluster : Host Parameters

Priority (unique host identifier): 1

Dedicated IP addresses

IP address	Subnet mask
192.168.1.201	255.255.255.0

Add... Edit... Remove

Initial host state

Default state: Started

Retain suspended state after computer restarts

< Back Next > Cancel Help

◆ In this page, click the Add button.

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

Add... Edit... Remove

< Back Next > Cancel Help

- ◆ Enter a virtual IP and netmask that will be used as the Cluster IP and netmask.

The screenshot shows a 'New Cluster: Cluster IP Addresses' dialog box. It contains a sub-dialog titled 'Add IP Address'. The sub-dialog has three radio button options: 'Add IPv4 address:', 'Add IPv6 address:', and 'Generate IPv6 addresses:'. The 'Add IPv4 address:' option is selected. Below it, there are two text input fields: 'IPv4 address:' containing '192 . 168 . 1 . 200' and 'Subnet mask:' containing '255 . 255 . 255 . 0'. The 'Generate IPv6 addresses:' option has three checkboxes: 'Link-local' (checked), 'Site-local', and 'Global'. At the bottom of the sub-dialog are 'OK' and 'Cancel' buttons. The main dialog has a '< Back' button highlighted, and 'Next >', 'Cancel', and 'Help' buttons.

- ◆ In this page, select Multicast in Cluster Operation Mode to provide a better performance.

The screenshot shows a 'New Cluster: Cluster Parameters' dialog box. It is divided into two sections. The first section, 'Cluster IP configuration', has four fields: 'IP address:' with a dropdown menu showing '192.168.1.200', 'Subnet mask:' with '255 . 255 . 255 . 0', 'Full Internet name:' with an empty text box, and 'Network address:' with '03-bf-c0-a8-01-c8'. The second section, 'Cluster operation mode', has three radio button options: 'Unicast', 'Multicast' (which is selected), and 'IGMP multicast'. At the bottom of the dialog, the 'Next >' button is highlighted, along with '< Back', 'Cancel', and 'Help' buttons.

- ◆ In this page, Click the Edit button

New Cluster : Port Rules

Defined port rules:

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

< >

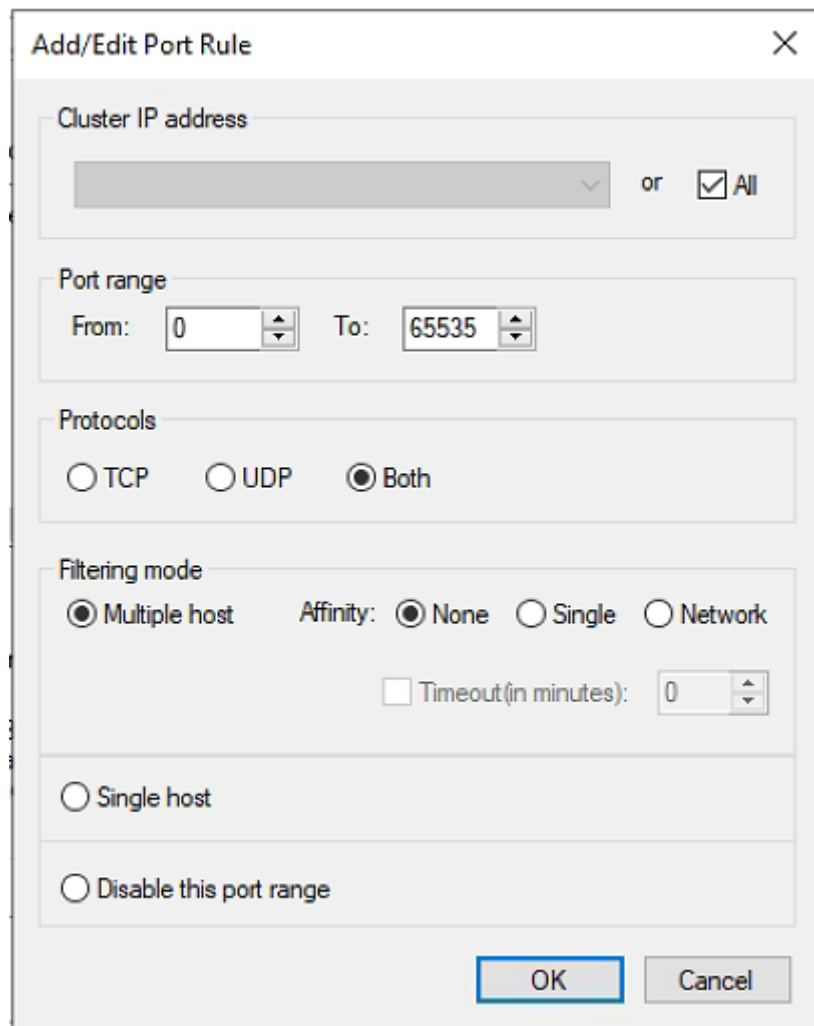
Add... Edit... Remove

Port rule description

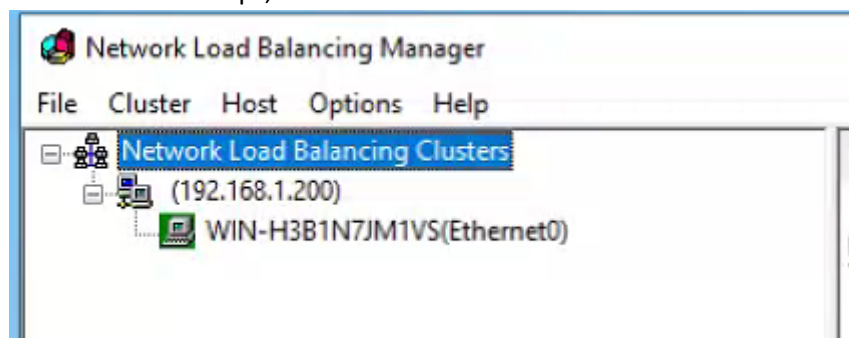
TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced across multiple members of the cluster according to the load weight of each member. Client IP addresses are used to assign client connections to a specific cluster host.

< Back Finish Cancel Help

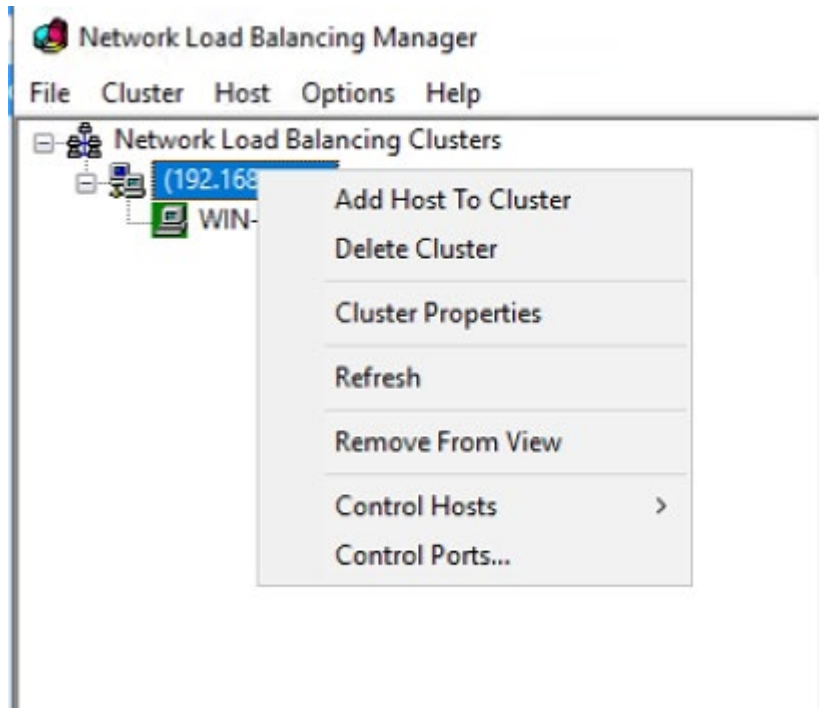
- ◆ In this page, Select the Filtering mode as “Multiple host”, select the Affinity as “None”



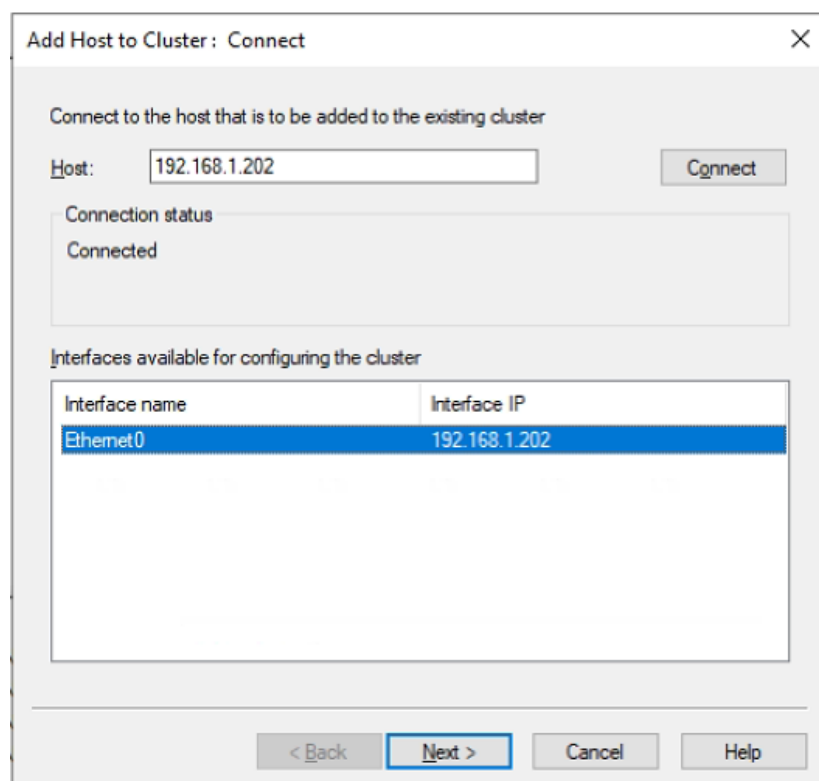
- ◆ After the above steps, a NLB cluster was created



- ◆ Then add the SERVER E to this cluster, Right click the cluster node, click the "Add Host To Cluster"



- ◆ In this page, input the SERVER E's IP (192.168.1.202) and click Connect button



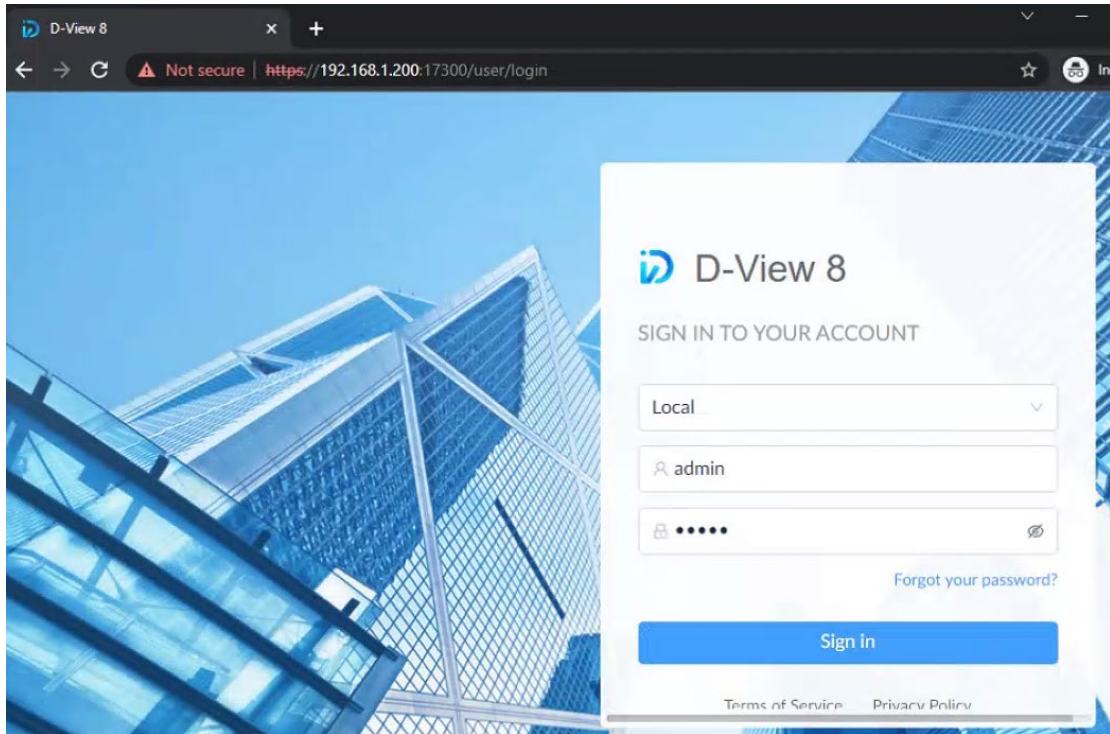
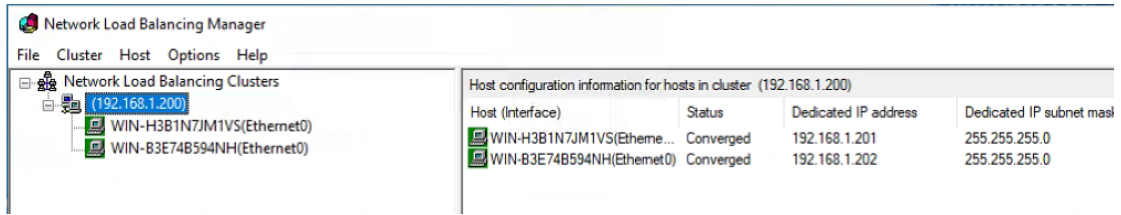
- ◆ In this page, click the Next button

The screenshot shows a dialog box titled "Add Host to Cluster: Host Parameters". At the top, there is a "Priority (unique host identifier):" dropdown menu set to "2". Below this is a section for "Dedicated IP addresses" containing a table with two columns: "IP address" and "Subnet mask". The table has one row with the values "192.168.1.202" and "255.255.255.0". Below the table are three buttons: "Add...", "Edit...", and "Remove". Underneath is the "Initial host state" section, which includes a "Default state:" dropdown menu set to "Started" and a checkbox labeled "Retain suspended state after computer restarts" which is currently unchecked. At the bottom of the dialog are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

- ◆ In this page, click the Finish button

The screenshot shows a dialog box titled "Add Host to Cluster: Port Rules". It features a table under the heading "Defined port rules:". The table has columns for "Cluster IP address", "Start", "End", "Prot...", "Mode", "Priority", "Load", and "Affinity". The first row is highlighted in blue and contains the values: "All", "0", "65535", "Both", "Multiple", "-", "Equal", and "None". Below the table are three buttons: "Add...", "Edit...", and "Remove". Underneath is a "Port rule description" text box containing the text: "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." At the bottom of the dialog are four buttons: "< Back", "Finish" (highlighted with a blue border), "Cancel", and "Help".

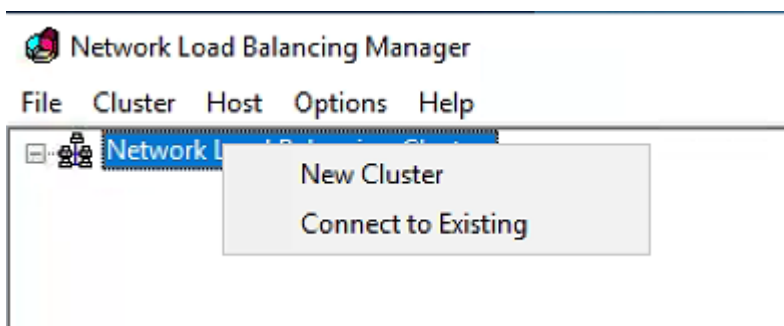
- ◆ Now a cluster includes SERVER D and SERVER E was created. And the DV8 can be accessed with the cluster IP.



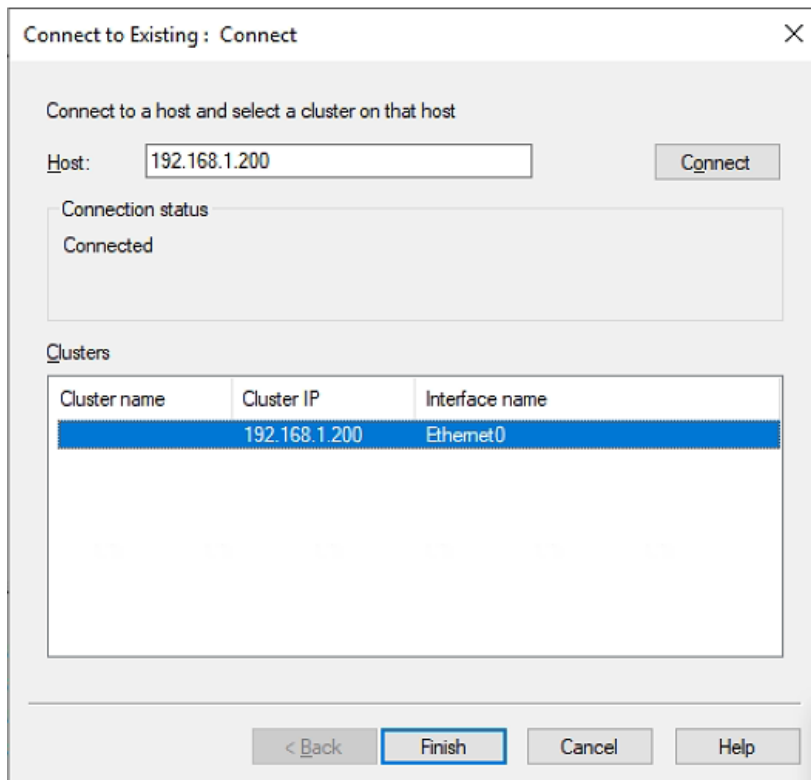
■ SERVER E

If you want to manage the NLB cluster on SERVER E, you can do the following steps:

- ◆ Cluster -> Connect to Existing



- ◆ In this page, enter the NLB cluster IP, 192.168.1.200 and click the Connect button.



◆ After that, you can see the NLB cluster info in SERVER E.

