Managed SD-WAN Platform User Guide

Nokia Cloud Managed SD-WAN Platform Release 22.2.R1

Issue 1

Ziply Fiber Confidential

Contents

About this document

Purpose

This guide provides information on the Nokia Cloud Managed SD-WAN Platform.

Conventions used

This guide uses the following typographical conventions:

Appearance	Description
*	Mandatory parameter.
GUI	Text that is displayed in a graphical user interface or in a hardware label.
Emphasis	Text that is emphasized.

Intended audience

This manual is intended for:

- Service provider or partner system administrators under reseller organizations who are responsible for enterprise network configuration, and
- Administrators for the Nokia Cloud Managed SD-WAN Platform.

It is assumed that the reader is familiar with virtualization and networking technologies. Other assumptions are explicitly called out in the relevant chapters.

How to comment

To comment on this document, go to the Online Comment Form (https://documentation.nokia.com/comments/) or email your comments to the Comments Hotline (mailto:comments@nokia.com).

1 Introduction

1.1 Nokia Cloud Managed SD-WAN Platform Overview

SD-WAN services are an essential part of the network infrastructure employed by enterprise networks. This technology drives Service Providers (SPs) and System Integrators (SIs) to enhance their portfolios by including them as a service offering. However, there are barriers that may prevent some SPs and SIs from entering this market and reaping the benefits of offering this technology as a service.

Hosting an SD-WAN service can include large startup and hosting costs with a delayed time to revenue. In addition, ongoing operations and maintenance of the service may not be appealing to some SPs. These factors may discourage smaller SPs or SIs from hosting this service.

Nuage Networks from Nokia has introduced a solution to this problem with their SD-WAN service based on industry-leading Nuage Networks technology. With this service, Nuage Networks operates the SD-WAN infrastructure on behalf of SPs and SIs, allowing them to offer an industry-leading SD-WAN service and also providing an accelerated time to revenue and reduced startup costs.

1.2 End user staff requirements

1.2.1 Roles

A single Admin account is provided to get started with the SD-WAN Portal for an end user organization. This account should be used to create individual user accounts for staff who will access the portal. The Admin account is a special account that has access to all features of the platform and which cannot be modified. All other user accounts will access only those areas of the system permitted through their user group permissions.

1.2.2 Knowledge and training

General knowledge of networking is required for end user staff to use the Nokia Cloud Managed SD-WAN Platform. Knowledge of basic networking including a basic understanding of:

- LANs
- Zones
- Subnets
- Virtual LANs (VLANs)
- Network monitoring, operations, and policies
- BGP

1.2.3 Supported browsers

The Nokia Cloud Managed SD-WAN Platform is designed to work with the following web browsers:

- Mozilla Firefox

1.3 SD-WAN Portal Password Complexity and Management

The SD-WAN Portal is configured by Nokia to utilize the following password complexity rules when users create or update their passwords:

- At least one upper case - English letter
- At least one lower case - English letter
- At least one digit
- At least one special character
- Minimum 8 characters and maximum 32 characters

2 Web Filtering Service

2.1 Web filtering

Web filtering of the Nokia Cloud Managed SD-WAN Platform is active at the NSG and allows network administrators to create and enforce security policies at the branch level to police web traffic originating from the access ingress. This functionality allows the reseller or enterprise to block or allow branch traffic based on web category or domain destination. Web filtering protects branch user access to the internet while enabling organizations to ensure compliance with their security policy.

Key use cases for web filtering include the following:

- Content filtering: Filter branch user access to inappropriate content based on website domain name or web category.
- Web-based malware protection: Block branch user access to malware and phishing sites based on website domain name or web category.
- Cloud services access: Allow branch user access to specific cloud services based on website domain name.

The Web Filtering service provides web category information on URLs from a list of predefined categories. The predefined web categories can be used to create FQDN or category-based web filtering security policy entries.

Key functionality of web filtering includes the following:

- Granular policy control for branch user access to internet sites by filtering DNS queries as part of an ingress security policy.
- Management of web filtering policies as part of ingress security policies, as configured by the Cloud Managed Operations team through ticket request
- ACL logging of blocked or allowed websites and categories for compliance and auditing.
- Automated updates of websites and web categories with over 180 predefined categories.
- Web filtering to block websites or web categories (for example, to block malware, adult content, or streaming media).
- End-user access denied webpage notification for blocked websites.
- Web filtering is supported for L3 domains only

The web filtering functionality employs outbound security policies as its core mechanism.

The Web Filtering service is configured on SD-WAN Portal via the security policies, specifically the outbound security policies, as described in the following sections:

- 12.45 “Adding or Editing Outbound or Inbound Security Policies” (p. 162)
- 12.46 “Adding or Editing Rules for Inbound or Outbound Security Policies” (p. 164)
- 16.20 “Assigning Web Domains to Web Categories” (p. 285)
- 16.21 “Unassigning Web Domains from Web Categories” (p. 286)

3 Introduction to the Advanced Subscriber Organization Portal

3.1 System Requirements

Supported browsers are the latest versions of:

- Google Chrome
- Mozilla Firefox

Recommended Display Resolutions:

- Full high-definition screen resolution (1920x1080 pixels)
- General laptop resolution (1366x768 pixels)

3.2 Conventions Used

This guide uses the following typographical conventions:

Appearance	Description
*	Mandatory parameter.
GUI	Text that is displayed in a graphical user interface or in a hardware label.
Emphasis	Text that is emphasized.

3.3 SD-WAN Portal Menu

The available menu items to navigate to the organization dashboard depends on the organization the user belongs to.

Figure 6-1 Subscriber Organization Dashboard as a Reseller

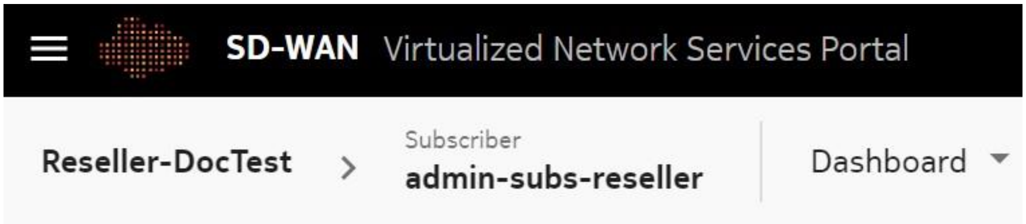


Figure 6-2 Subscriber Organization Dashboard as a Subscriber

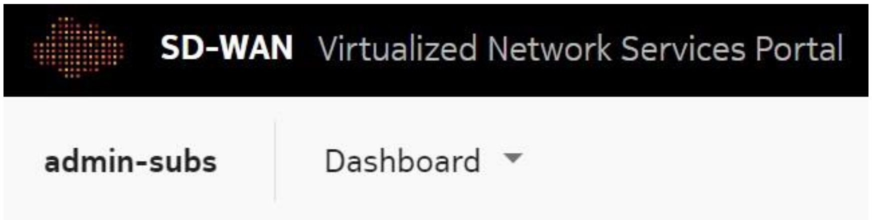
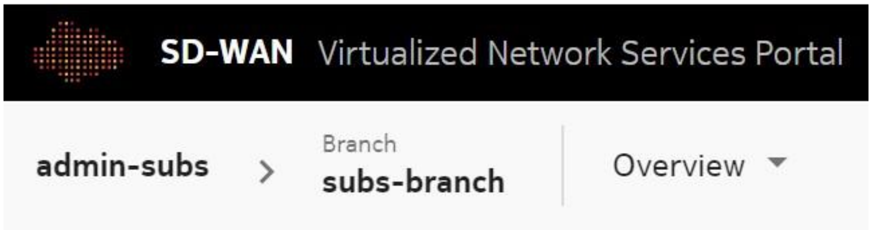


Figure 6-3 Branch Dashboard as a Subscriber


SD-WAN Virtualized Network Services Portal

admin-subs > Branch subs-branch

3.4 Typical Error Messages

The following table lists the typical error messages that display due to network connectivity and server issues:

Error message	Description	Resolution
Unable to Communicate with VNS Platform	This error message is displayed when the portal connectivity to VNS platform fails due to network connectivity issues.	If you are a subscriber organization user, contact your reseller organization. If you are a reseller organization user, contact Nokia Cloud Managed SD-WAN Platform Operations.
Unexpected server error while retrieving statistics	This error message is displayed when the ES request is timed out or ES returns any errors even without any network connectivity issues.	If you are a subscriber organization user, contact your reseller organization. If you are a reseller organization, contact Nokia Cloud Managed SD-WAN Platform Operations.

4 Getting Started

4.1 Logging in to the SD-WAN Portal

1

Enter the login credentials in the **Username**, **Password**, and **Organization** fields.

2

Select a preferred language from the **Language** list.

3

Click **LOG IN**.

- If you login as a reseller organization user, the Organization page opens, displaying the list of subscriber organizations managed by the reseller organization.
- If you login as a subscriber organization user, the Subscriber Organization Dashboard opens, displaying the widgets.

END OF STEPS

Upon the user account creation, a “New Account” email is sent to the user’s registered email ID with a link to set your password. The password must be set before you can log in.

Note: If you attempt to log in with an incorrect password more than five times, your account will be locked out temporarily for security reasons. The SD-WAN Portal displays a message indicating that you can log in again with the correct password after a specified time interval.

Note: A user can access the SD-WAN portal for the configured duration of a user session. After the user session expires, the user is redirected to the login page.

4.2 Recovering a User Password

1

Click **Forgot Password** in the login page, if you forgot your user password.

2

Enter the login credentials in the following fields:

- **Username**
- **Email Address** used while creating your account
- **Organization** name

3

Click **RECOVER PASSWORD**. You will receive an email in the registered email ID with a link to reset the password. You can click the link to reset the password. Enter the new password, confirm the password and click **RESET PASSWORD**.

You can log into the SD-WAN Portal using this password. See 7.1 “Logging in to the SD-WAN Portal” (p. 39).

End of steps

4.3 Updating User Account Settings

1

From the user menu, click **Account Settings**.

2

In the Account Settings page, configure the following parameters:

Parameter	Description
User Information	
First Name*	Enter the first name of the user. Applicable only for reseller and subscriber organizations.
Last Name*	Enter the last name of the user. Applicable only for reseller and subscriber organizations.
Email Address*	Enter the email address of the user.
Primary Phone	Enter the phone number of the user. Applicable only for reseller and subscriber organizations.
Mobile Phone	Enter the mobile number of the user. Applicable only for reseller and subscriber organizations.
Username*	The username is displayed.
Language*	Select a preferred language from the language list.
Change Password	
Current Password	Enter the password for the current user.
New Password	Enter the new password for the current user.
Retype New Password	Re-enter the new password for confirmation.

3

Click **OK**.

End of steps

4.4 Logging out of the SD-WAN Portal

1

From the user menu, click **SIGN OUT**. You are logged out of the portal. The login page is displayed.

End of steps

4.5 Viewing Notifications

The Notification icon 🔔 is displayed beside the user menu at the top right corner of the page. A red filled circle 🔔 displays next to the Notification icon if a new notification message is received. Click the icon ⓘ to view messages. The red filled circle disappears once the issue is resolved (for example, a license expiration issue is resolved) or the notification is manually cleared by clicking the information icon ⓘ or by clicking CLEAR ALL.

4.5.1 Viewing the Notification Status

Notifications are displayed on the top right page when operations are performed. Click the information icon ⓘ to view the status of the operations performed.

Table 7-1 Status and Icons of Notifications

Status	Icon	Description
Success	✓	Indicates that the operation is successfully executed.
Warning	⚠	Indicates that some executions have failed.
Error	❗	Indicates that some executions have errors.
Information	ⓘ	Indicates that there are no notifications.

5 Managing Branches

5.1 Viewing, Exporting and Filtering the Branch List

1 Navigate to your organization's Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

From the branch-level menu, select **Branch List**. The list of branches associated with the organization is displayed in a table.

Note: This list does not include the Blocklisted branches.

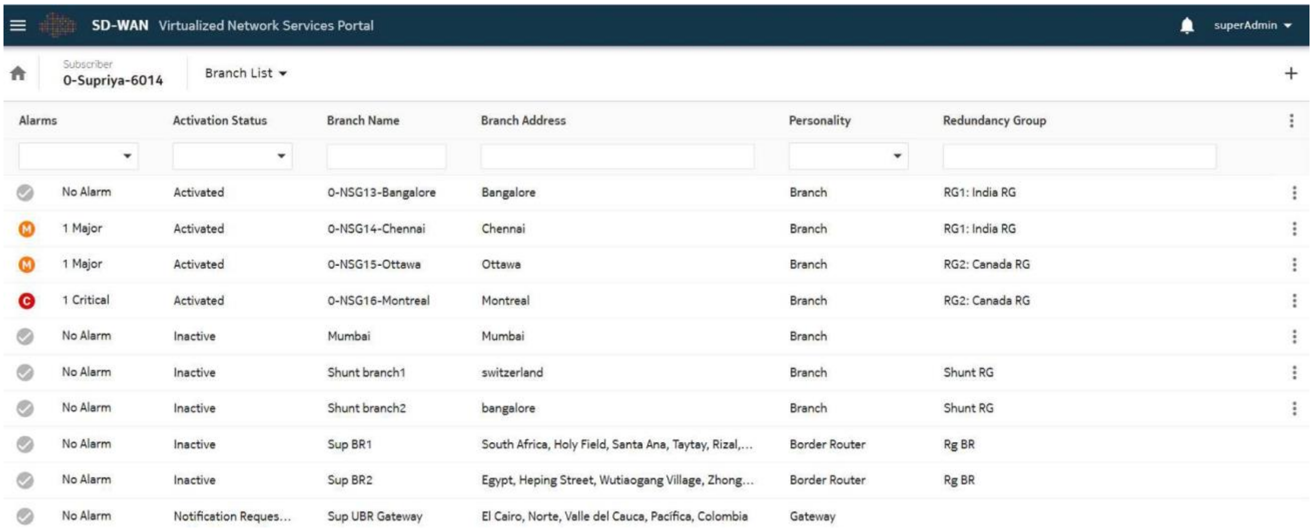
If required, you can export the list. From the ellipsis icon ⋮ at the right side of the table header row, select **Export to CSV** to export the branch list to a CSV file.

You can filter the branch list page by the following criteria:

Parameter	Description
Alarms	Select the required alarm type from the list. The following options are: • Critical • Major • Minor • Info • Healthy • No Alarm
Activation Status	Select the required activation status from the list. The following options are: • Activated • Inactive • Certificate Signed • Notification Request Acknowledged • Notification Request Sent • Quarantined • Revoked • Non-active

Parameter	Description
Branch Name	Enter a branch name.
Personality	Select the required personality type from the list. The following options are: • Branch • Border Router • Gateway **Note:** Branches with personality as Branch only can be edited and can be navigated to the Dashboard.
Redundancy Group	Enter the redundancy group name.

Figure 9-1 Sample Branch List



Alarms	Activation Status	Branch Name	Branch Address	Personality	Redundancy Group
No Alarm	Activated	0-NSG13-Bangalore	Bangalore	Branch	RG1: India RG
M 1 Major	Activated	0-NSG14-Chennai	Chennai	Branch	RG1: India RG
M 1 Major	Activated	0-NSG15-Ottawa	Ottawa	Branch	RG2: Canada RG
C 1 Critical	Activated	0-NSG16-Montreal	Montreal	Branch	RG2: Canada RG
No Alarm	Inactive	Mumbai	Mumbai	Branch	
No Alarm	Inactive	Shunt branch1	switzerland	Branch	Shunt RG
No Alarm	Inactive	Shunt branch2	bangalore	Branch	Shunt RG
No Alarm	Inactive	Sup BR1	South Africa, Holy Field, Santa Ana, Taytay, Rizal,...	Border Router	Rg BR
No Alarm	Inactive	Sup BR2	Egypt, Heping Street, Wutiaogang Village, Zhong...	Border Router	Rg BR
No Alarm	Notification Reques...	Sup UBR Gateway	El Cairo, Norte, Valle del Cauca, Pacífica, Colombia	Gateway	

End of steps

5.2 Viewing the Branch Overview

Note: For inactive or operationally down branches, historical statistics cannot be viewed since ability to select different date ranges will be disabled.

The View Branch Dashboard permission should be enabled for the user to view the branch dashboard widgets. See also 15.9 “Adding or Editing a User Group” (p. 256) to enable View Branch Dashboard.

1

Navigate to your organization’s Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, select **Branch List**. The list of branches associated with the organization is displayed in a table.

3

Double-click a branch to view its dashboard.

Click the duration icon 🕓 to view the data for the selected duration. Click the Auto-Refresh option if you want the dashboard data to be refreshed automatically. For more information, see 8.4.1 “Auto-Refresh for Dashboards” (p. 48). Auto-Refresh is enabled only for an active branch.

Click the **Reset Dashboard** icon ▦ to reset the widgets to their default positions. If the user does not have the permission to view a widget, blank space is displayed in the Dashboard. The user must manually rearrange the widgets in the dashboard to remove the blank space.

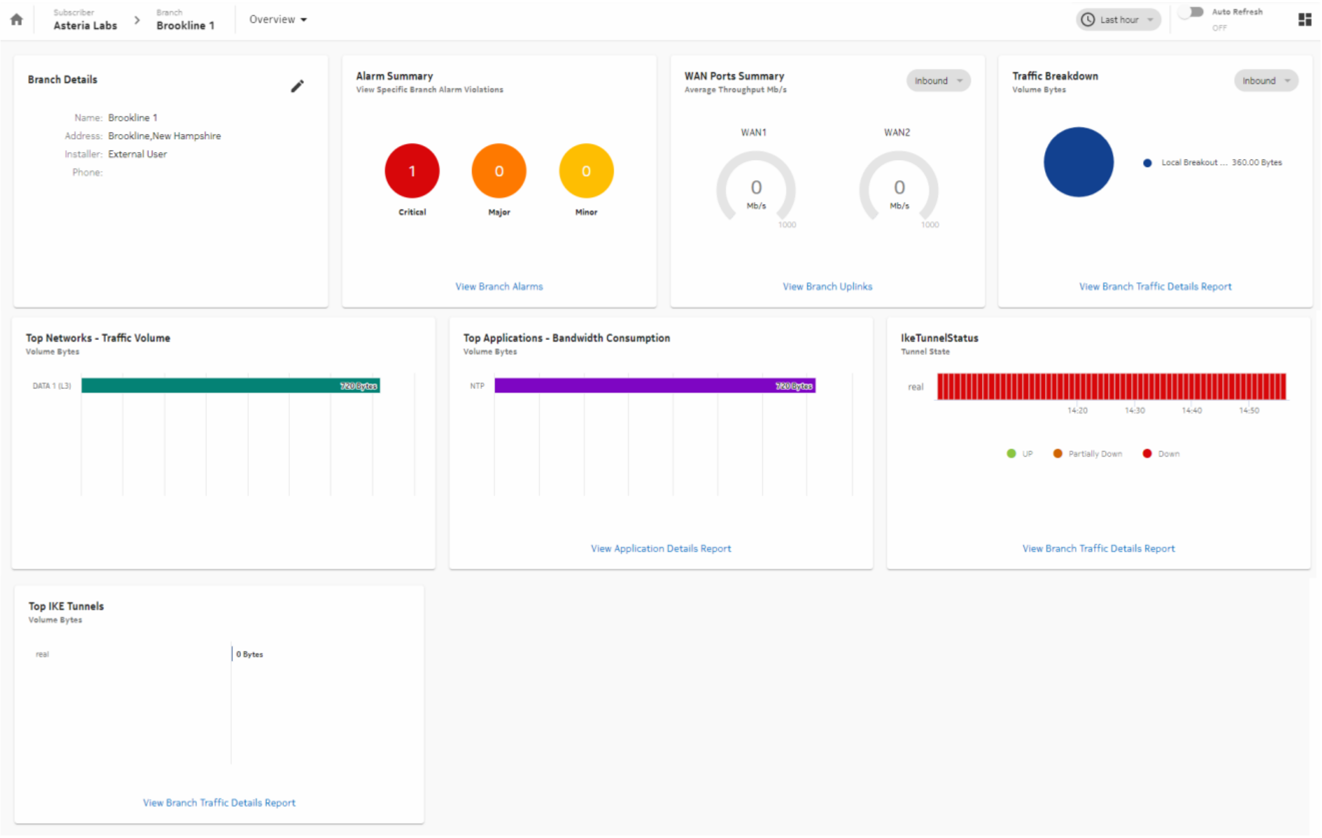
The Branch Dashboard comprises the following widgets:

Widget	Description
DEVICE NOT ACTIVE – NOTIFY INSTALLER	Indicates that the branch is in the Inactive State. By clicking on the link, a notification displays indicating that the device activation message is sent to the installer. Applicable only to branches awaiting activation.

Widget	Description
DEVICE QUARANTINED - LIFT QUARANTINE	Indicates that the branch status is “Quarantined.” Clicking on this link lifts the branch from quarantined state to an activated state. When the branch is lifted to the active state the banner is also removed. You can also lift the quarantined state of the branch from the Device page. See 9.8 “Managing Operations Based on Branch Status” (p. 63).
Branch Details	Provides the branch details. Click the **Edit** icon ✎ to edit the branch address.
Alarm Summary	Provides the count of critical, major and minor alarms. Click on any of these icons to navigate to the alarm list page for the selected alarm severity. The **View Branch Alarms** link provides a quick access to the Alarms page.
WAN Ports Summary	Provides a summary of WAN uplinks (total average throughput per WAN Uplink in Mb/s with the maximum uplink speed as the range) and Auxiliary Uplinks for a selected duration. **Note:** Signal strength is displayed only for an active WWAN port. Click **Inbound** or **Outbound** to view the traffic direction. Select **Uplink** to view the Uplink Summary. The user must have the View VLANs permission to view the uplink summary. **Note:** If auxiliary uplinks are not configured, the uplink summary displays only the WAN uplinks. The **View Branch Uplinks** link provides a quick access to the Uplinks page and displays port statistics.
Traffic Breakdown	Displays a pie chart for the branch traffic breakdown. Move the mouse over the pie chart to view the percentage of the traffic breakdown for each category of the traffic. Click or Inbound or Outbound to view the required traffic direction. The **View Branch Traffic Details Report** provides a quick access to the Branch Traffic Details Report Page.
Top Networks - Traffic Volume	Displays a graphical representation of the top five L2 and L3 networks based on traffic volume for a selected duration.
Top Applications - Bandwidth Consumption	Displays a graphical representation of the top five applications based on traffic volume for a selected duration. The **View Application Details Report** provides a quick access to the Application Details Report page.

Widget	Description
IKE Tunnel Status	The user must have the View VLANs and View IKE connections permissions to view the IKE Tunnel Status widget. Displays a graph of the status of IKE tunnels based on traffic volume for a selected duration. The **View Branch Traffic Details Report** provides a quick access to the Branch Traffic Details Report Page.
Top IKE Tunnels	The user must have the View VLANs and View IKE connections permissions to view the Top IKE Tunnels widget. Displays a graph of the top IKE tunnels based on traffic volume for a selected duration. The **View Branch Traffic Details Report** provides a quick access to the Branch Traffic Details Report Page.

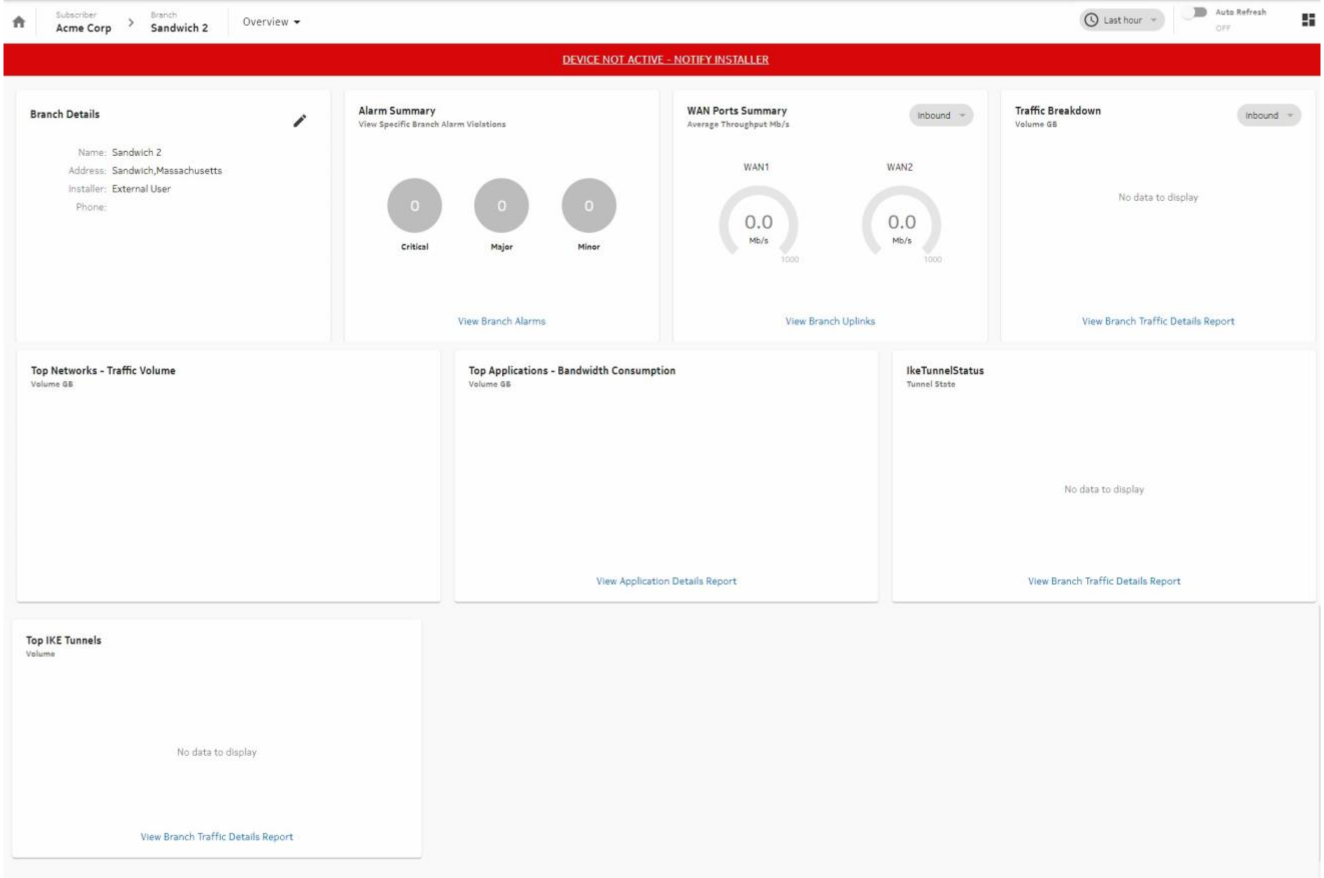
Figure 9-2 Branch Overview for an Active Device



Subscriber: Asteria Labs
Branch: Brookline 1

Name: Brookline 1
Address: Brookline,New Hampshire
Installer: External User
Phone:

Figure 9-3 Branch Overview for a Device Not Activated

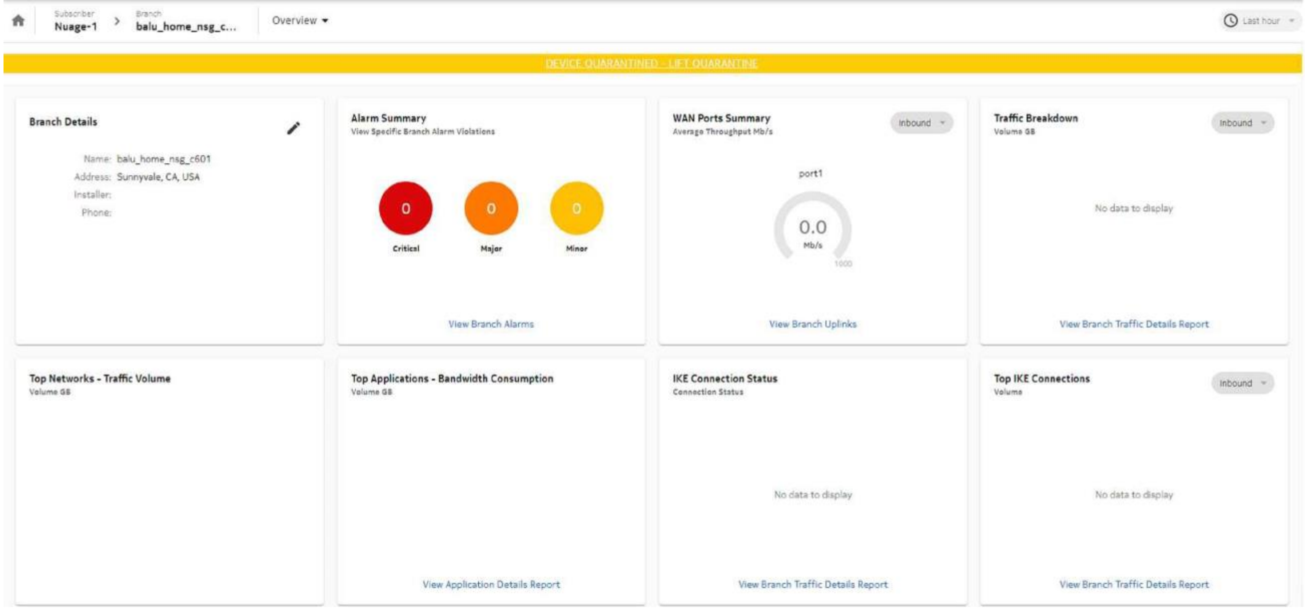


DEVICE NOT ACTIVE - NOTIFY INSTALLER

Branch Details

Name: Sandwich 2
Address: Sandwich,Massachusetts
Installer: External User
Phone:

Figure 9-4 Branch Overview for a Quarantined Device



DEVICE QUARANTINED - LIFT QUARANTINE

Branch Details

Name: balu_home_nsg_c601
Address: Sunnyvale, CA, USA
Installer:
Phone:

End of steps

5.3 Viewing the Branch Map

1

Navigate to your organization’s Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, select **Branch Map**. A map view of the branch locations is displayed.

Icon	Icon Name	Description
⛶	Fit to screen	Allows to fit the map to available screen area.

Icon	Icon Name	Description
⌖	Adjust clustering	Allows to manage multiple markers on the map. Allows to select clustering on or off, turn cluster charts and cluster show area on or off, adjust cluster screen, network threshold, and inclusion range. • Clustering: allows to select clustering view on or off • Cluster charts: allows to select clustering charts view on or off Clustering should be enabled • Cluster show area: allows to select the area of cluster view on or off • Cluster inclusion range: allows to increase or decrease the cluster inclusion range • Cluster threshold - Network: allows to increase or decrease the network cluster threshold • Cluster threshold - Screen: allows to increase or decrease the screen cluster threshold
●	Adjust vertexes	Allows to adjust vertex size, turn vertex labels on or off, and turn vertex nameplates on or off.
🌐	Map view	Provides the bird’s-eye view of the map inside the map window. Branch locations are indicated as pins. **Note:** The hidden branches do not display as pins in the map view panel. However, the total number of branches in the Summary section of the Branch Map also includes the hidden gateways count. Therefore, if there is a mismatch between the number of branches in the Summary section and the number of pins in the map view, it means that few branches are hidden due to blocklisting.
⊞	Zoom in	Allows to zoom in to the map.
⊟	Zoom out	Allows to zoom out of the map.

The following details are displayed beside the branch map:

Section	Description
Summary	Provides the count of total, active, and non-active branches. The **View Branch List** provides a quick access to the Branch List page. **Note:** The hidden branches do not display as pins in the map view panel. However, the total number of branches in the Summary section of the Branch Map also includes the hidden gateways count. Therefore, if there is a mismatch between the number of branches in the Summary section and the number of pins in the map view, it means that few branches are hidden due to blocklisting.
Active Branches Health Status	Provides the count of branches with the following statuses:
	• Healthy (Minor, Informational or No Alarms)
	• With Critical Alarms
	• With Major Alarms

3

Click **VIEW LIST** to view the list of missing branches.

Note: This option displays only if a subscriber organization have any branches with incorrect address.

End of steps

5.4 Adding or Editing a WiFi Port of a Branch

Note: Only one WiFi port can be configured.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**.

3

Perform any of the following actions:

- Click the **ADD WIFI** icon + to configure a WiFi port. The WiFi Configuration window opens.
- Select the port and click the **More** icon ⋮ and then click **Edit Port** icon ✎ corresponding to the WiFi Port in the WiFi Port section.

  The WiFi Configuration window opens.

4

Configure the following parameters:

Parameter	Description
WiFi Name*	Enter the WiFi Port name.
Description	Enter a description.
Frequency*	Select a frequency: • 2.4 GHz • 5.0 GHz
Country*	Select a country from the **Country** list.
Channel*	Select a channel from the **Channel** list. The available channels are dependent on country and frequency. Select **Automatic Channel Selection** to choose the channel automatically.
Mode*	Select a mode. When the selected frequency is 2.4 GHz, the available modes are: • 802.11b/g • 802.11b/g/n When the selected frequency is 5.0 GHz, the available modes are: • 802.11a • 802.11a/ac • 802.11a/n • 802.11a/n/ac

5

Click **OK**. The WiFi port displays as *wlan0* with a WiFi icon along with the other port icons, and is also listed in the WiFi Port section. You can add SSIDs to the WiFi port.

End of steps

Note: When a WiFi port is added, a primary SSID (Nuage_Admin) is added by default which will be deleted only on deletion of the WiFi port.

5.5 Viewing Branch Uplinks

You can view the branch uplinks page only if the Branches and Uplink Ports are enabled and you are assigned the View Branch Uplink permission. The related permissions are:

- View Egress QoS Policies
- View L2 Networks
- View L3 Networks

- View L2 Network Application Groups
- View L3 Network Application Groups
- View VLANs
- View Applications
- View Branch WAN Egress QoS Policy

1

Navigate to the Branch Overview. See 9.4 "Viewing the Branch Overview" (p. 55).

2

From the branch-level menu, select **Uplinks**. The Uplinks page opens.

3

To generate the report for a specific period, configure the following parameters:

Parameter	Description
View	Select an option from the list. The following options are available: • Uplinks Overview (default) • Top 10 Applications 1. Network Type - Select either All (by default) or only L2 or L3 network type to display the inbound and outbound traffic. It is not mandatory to select a network to view the inbound and outbound traffic for the selected network type. 2. Network - Enter text to search for a network. Select a network from the list. Select either All (by default) or only one network at a time. 3. Application Type - Select an option from the list. The following options are available: Discovered Applications Application Groups: This option is greyed out when the All option for Network is selected. This option is available only when a Network is selected. 4. Application - Enter text to search for an application. Select an application from the list. Select either All (by default) or only one application at a time. Available only when an Application Type is selected.
Time Range	Select one of the time options for the report – Last hour (default), Last 4 hours, Last 12 hours, Last 24 hours or Last 7 days.

A graphical representation of the uplinks report displays with the following details:

Section	Description
Throughput (Uplinks Overview)	The details are displayed for each VLAN. Displays the inbound to branch, outbound from branch traffic and QoS policy for each selected network(s). A line graph displays the traffic statistics of the network depending on the selected option: • Inbound: Displays the inbound traffic to branch. • Outbound: Displays the outbound traffic from branch. • QoS Policy: Displays the QoS policy of the branch. If the auxiliary mode is enabled, for an uplink, the role is displayed as Auxiliary and the mode as Hot Standby or Cold Standby. Otherwise, it displays the role as Primary/Secondary with Normal mode. Hover over the graph to view date, time, network and data usage. **Note:** The WAN throughput line graph includes the blocklisted traffic and regular traffic and receives data from port statistics in ES.
Top 10 Applica-tions Throughput	Displays the percentage usage for each of the top ten applications per-uplink. A line graph displays the traffic throughput for the application. Hover over the graph to view date, time, network and data usage.

End of steps

5.6 Viewing the Branch Access

1

Navigate to the Branch Dashboard. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Access**. The Access page opens.

3

To generate the report for a specific period, select one of the time options – Last hour (default), Last 4 hours, Last 12 hours, Last 24 hours or Last 7 days.

A graphical representation of the uplinks report displays with the following details:

Section	Description
VLAN	Displays the inbound access traffic to branch, outbound access traffic from branch and VLAN port network details for the selected network(s).

SSID	Displays the inbound access traffic to branch, outbound access traffic from branch and WiFi port network details for the selected network(s).
Throughput	A line graph displays the traffic statistics of the network depending on the selected option: • Inbound: Displays the inbound traffic to branch. • Outbound: Displays the outbound traffic from branch. Hover over the graph to view date, time, network and data usage.

End of steps

5.7 Viewing the Branch Usage

1

Navigate to the Branch Dashboard. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Usage**. The Usage page opens.

3

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type	Select All (by default) to include all networks or select L3 or L2 from the list.
Network	Enter text to search for a network. Select a network from the list. By default, **All** is selected to include all networks.
Traffic Type	Select All (by default) to include all traffic types in the report or select one type from the list.
Source Branch Personalities	Select All Personalities (by default) to include all the source branch personalities or select from the list. The available options are: • Branch • Gateway • Border Router
Source Branch	By default, displays the branch context and cannot be changed.
Destination Branch Personalities	Select All Personalities (by default) to include all the destination branch personalities or select from the list. The available options are: • Branch • Gateway • Border Router
Destination Branch	Enter text to search for a destination branch. Select a destination branch from the list. By default, **All** is selected to include all destination branches.
Application Type	Select an option from the list. The following options are available: • All: Displays traffic data all the applications groups. • Discovered Applications: Displays the traffic data for default application groups. • Application Groups: Displays the traffic data for user-defined application groups. This option is enabled when a network is selected.
Application Group	Select an application group from the list. This field is enabled when the application type is application group.

Parameter	Description
Application	Enter text to search for an application. Select an application from the list. By default, **All** is selected to include all applications. Available only when Built-in applications for Application Type is selected.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

4

Click **RUN REPORT**.

The usage report displays a table listing each application, a graph of the inbound and outbound traffic, and other traffic data.

The list with expandable rows allows users to view traffic throughput per application. Hover over the graph to view date, time, network and data usage.

End of steps

5.8 Viewing the Alarms of a Branch

1

Navigate to the Branch Dashboard. See 9.4 "Viewing the Branch Overview" (p. 55).

2

From the branch-level menu, select **Alarms**.

The Alarms page displays the alarms list of the selected branch with the following details:

Section	Description
Severity	Provides the Critical, Info, Major, Minor, and Warning severity of alarms.
Time	Provides the view of alarms sorted by time.
Title	Provides the view of alarms sorted by title.
Alarmed Object	Provides the view of alarms sorted by devices.
Description	Provides the description of the alarm.

End of steps

6 Managing WiFi Ports

6.1 Deleting a WiFi Port of a Branch

Note: Deleting a WiFi port is service-affecting. When the WiFi port is deleted, all SSIDs and its network links are deleted.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The WiFi port is displayed in the WiFi Port section.

3

Select the WiFi port, click the **More** icon ⋮ and click the **Delete** icon 🗑 to delete a WiFi port.

4

Click **DELETE**.

End of steps

6.2 Adding or Editing an SSID for a WiFi Port

An SSID is the primary name associated with a wireless local area network.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of existing SSIDs is displayed in the WiFi Port section.

3

Perform any of the following actions:

- Select a port and click the arrow icon ⌄ beside it to expand. Click the + SSID icon to add an SSID. The Add SSID window opens.
- Select an SSID, click the **More** icon ⋮ and click the **Edit SSID** icon ✎ to edit the SSID. The Edit SSID window opens.

Configure the following parameters:

Parameter	Description
SSID*	Enter the SSID name.
Description	Enter a description.
Broadcast	Toggle the button to enable or disable broadcast. If enabled, the SSID name is broadcast to the connected devices.

Authentication*	Select an authentication type from the Authentication list: • **Captive Portal** • **Open WiFi** • **WEP** • **WPA** • **WPA2** • **WPA/WPA2 Mixed Mode** When you select **Captive Portal**, following options appear: • New Profile • Use Existing Profile
Redirect URL	Enter the website for URL redirection. This field is visible only when the Authentication type is Captive Portal.
Available Profiles*	Select the required profile from the Available Profiles list and click **DONE**. This field is visible only when the Authentication type is Captive Portal, and when you select Use Existing Profile.
Profile Name*	Enter the profile name. This field is visible only when the Authentication type is Captive Portal, and when you select New Profile.

Parameter	Description
Profile Description	Enter the optional profile description. This field is visible only when the Authentication type is Captive Portal.
Terms and Conditions	Displays the default text of the terms and conditions. This field is visible only when the Authentication type is Captive Portal.
Passphrase*	Enter a passphrase. This field is visible only when the Authentication type is WEP, WPA, WPA2, or WPA/WPA2 Mixed Mode.
MAC Filtering	Toggle the button to enable or disable MAC filtering.
Allowlist or Denylist	Select one of these options when adding a MAC address. These options are visible only when MAC Filtering is enabled. If a MAC address is added to the Allowlist, the NSG restricts access to all except those MAC addresses contained in the MAC Filter List panel. If a MAC address is added to the Denylist, all listed MAC addresses are completely blocked from network access. If both Denylist and Allowlist is available, then Allowlist will take priority.
MAC Address	Enter a valid MAC address and click **ADD MAC ADDRESS** to add the MAC address to the list. Click the Delete icon 🗑 corresponding to a MAC address to delete it. The MAC address format is AA:BB:CC:DD:EE:FF. This field is visible only when MAC Filtering is enabled.

5

Click **OK**.

End of steps

6.3 Linking an SSID to the WiFi Port

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The WiFi port is displayed in the WiFi Port section.

Unlinking an SSID from a WiFi Port

3

Click the arrow icon ⌄ beside the WiFi port to view the SSIDs of the port.

4

Select an SSID, click the **More** icon ⋮ and click the **Link SSID** icon 🔗 to link an SSID to the network. The Link SSID window opens.

5

Configure the following parameters:

Parameter	Description
Network Type*	Select an L2 or L3 network.
Network*	Select a network and click **DONE**.
Subnet*	Select a subnet and click **DONE**. Applicable only for L3 network.
Link Type*	Select a link type: • Bridge • Host
IP Address*	Enter the IP address. This field is applicable only if you select Host as the link type.
MAC Address*	Enter the MAC address. This field is applicable only if you select Host as the link type.

6

Click **OK**.

End of steps

6.4 Unlinking an SSID from a WiFi Port

ℹ **Note:** This procedure is service-affecting.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of WiFi ports is displayed in the WiFi Port section.

3

Click the arrow icon ⌄ beside the WiFi port to view the SSIDs of the port.

4

Select an SSID, click the **More** icon ⋮ and click the **Unlink SSID** icon to unlink an SSID to the network. The Unlink SSID window opens.

5

Click **UNLINK**.

End of steps

6.5 Assigning an Egress QoS Policy to an SSID

Note: The organization must have egress policies assigned to it.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The Wifi Port is displayed in the WiFi Port section.

3

Click the arrow icon ˅ beside the WiFi port to view the SSIDs of the port.

4

Select an SSID, click the **More** ⋮ icon and then click the **Policies** icon to assign a policy.

5

In the Policies window, select a policy from the **Egress Policy** list and click **DONE**.

6

Click **OK**.

End of steps

6.6 Deleting an SSID from a WiFi Port

Note: If an SSID is linked to a network, it cannot be deleted.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

Editing WAN Ports of a Branch

2

From the branch-level menu, select **Device**. The WiFi port is displayed in the WiFi Port section.

3

Click the arrow icon ˅ beside the WiFi port to view the SSIDs of the port.

4

Select an SSID, click the **More** icon ⋮ and click the **Delete SSID** icon 🗑 to delete the SSID. The Delete SSID window opens.

5

Click **DELETE**.

End of steps

6.7 Editing the Uplink Connection of a WAN Port

Note: The uplink settings of Branches created from NSG templates in Nokia Policy Manager cannot be edited.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of WAN ports is displayed in the WAN Ports section.

3

Click the arrow icon ⌄ beside a WAN port to view the VLANs associated with the port.

4

Select a VLAN in the table, click the **More** icon ⋮ and then click the **Edit Uplink Settings** icon ⚙ to edit the uplink connection.

5

In the Uplink Connection window, configure the following parameters:

Parameter	Description
Connection Type*	Select the required connection type from the **Connection Type** list. The following options are available:
	• Dynamic
	• PPPoE
	• Static
	• LTE (Enabled only when the WAN physical port name is 'lte'.)
	The connection type can be changed only if it is not set in the NSG template.
Role*	Select a role from the list. The following options are available: • Primary (default option) • Secondary
Uplink Order	Select the uplink order from the list.

Parameter	Description
Auxiliary Uplink	Toggle the button to enable or disable the auxiliary uplink.
Auxiliary Mode	Displays the auxiliary uplink mode. By default, it is Hot Standby for Dynamic, Static, PPPOE connection type. This cannot be modified. By default is Cold Standby for LTE and can be changed to Hot Standby.
IP Address/Mask	Enter an IP Address and Netmask. Netmask value must be the range of 1–32. Applicable only if Connection Type selected is Static.
Gateway	Enter the gateway IP address. Applicable only if Connection Type selected is Static.
DNS	Enter the DNS IP address. Applicable only if Connection Type selected is Static.
Username*	Enter a username. Applicable only if Connection Type selected is PPPoE.
User Password	Enter a password in the User Password and Confirm User Password. Applicable only if Connection Type selected is PPPoE.
LTE Configuration-Interface	Interface type, Automatic is selected by default. To enable an LTE uplink connection, the WAN port must be named 'lte.' Applicable only if Connection Type selected is LTE.
Custom Properties	Applicable only if Connection Type selected is LTE. This parameter is optional. Click **New Property** to add a custom property. You can add up to five custom properties as Name-Value pairs. Select a custom property and click **Delete** icon 🗑 to delete the custom property.
Underlay Options	
Breakout Options*	Select an option from the list. The following options are available: • Disabled • Default (NAT/Routing) • NAT Based Local Breakout • Routing Based Local Breakout
Underlay Tags	Lists the Underlay Tags available to the organization, including the ones marked as global.

6

Click **OK**.

End of steps

6.8 Editing LAN Ports of a Branch

Note:

- A warning message is displayed over the LAN grid, when a redundancy group only has one NSG, or when the second NSG does not have matching LAN ports.
- If there are any redundancy ports, an information message is displayed on the secondary NSG to indicate that the ports can be managed from the primary NSG. Click the link to convert the secondary branch to an authoritative branch.

The maximum number of LAN ports that can be displayed is 100.

1

Navigate to the Branch Overview. See 9.4 "Viewing the Branch Overview" (p. 55).

2

From the branch-level menu, select **Device**.

The list of LAN Ports is displayed in the LAN Ports section.

3

Select a LAN Port , click the More icon ⋮ and then select the **Edit Port** icon ✎ .

The **Port Display Name** window opens.

4

Modify the **Display Name** and click **OK**.

End of steps

7 Managing Branch Diagnostics

7.1 Running the Diagnostics Report for a Branch

You can view and access the diagnostic results and select a branch or a VLAN, if you have Branches and Diagnostics enabled and have the “View Diagnostic Test Results” permission. You can run the diagnostic reports only if you have the “Run Diagnostics Tests” permissions. The related permissions to view the diagnostics reports are:

- View Branches
- View Branch Access Port
- View VLANs
- View Branch WiFi Port
- View SSIDs
-

Deleting Test Results in a Diagnostic Report for a Branch

You can generate a diagnostics report only if the LAN port is connected to a subnet.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

Perform any of the following actions:

- From the branch-level menu, select **Diagnostics**.
- From the branch-level menu, select **Device**.

  The list of LAN ports is displayed in the LAN Ports section.

  Select a LAN port which is connected to a subnet. Click the **More** icon ⋮ and select **Diagnostics** icon ∿ .

  Select a VLAN under a LAN port, click the **More** icon ⋮ and click the **Diagnostics** icon ∿ .

3

To run the diagnostics report , see Step 5 of 12.40 “Running Diagnostics for an L3 Network” (p. 155).

End of steps

7.2 Deleting Test Results in a Diagnostic Report for a Branch

You can delete test results of a linked VLAN, if you have Branches and Diagnostics enabled and have the “Delete Diagnostic Test Results” permission.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

Perform any of the following actions:

- From the branch-level menu, select **Diagnostics**.
- From the branch-level menu, select **Device**.

The list of LAN ports is displayed in the LAN Ports section.

Select a LAN port which is connected to a subnet. Click the **More** icon ⋮ and select the **Diagnostics** icon -∿- .

3

Select a test suite, click the ellipsis icon ⋮ and click **Delete Test Suite.**

A confirmation message displays.

4

Click **DELETE**.

End of steps

7.3 Deleting Bulk Test Results in a Diagnostic Report for a Branch

You can delete test results of a linked VLAN, if you have Branches and Diagnostics enabled and have the “Delete Diagnostic Test Results” permission.

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

Perform any of the following actions:

- From the branch-level menu, select **Diagnostics**.
- From the branch-level menu, select **Device**.

  The list of LAN ports is displayed in the LAN Ports section.

  Select a LAN port which is connected to a subnet. Click the **More** icon ⋮ and select **Diagnostics** icon -∿- .

3

Click **Delete All** in the left pane to delete all the test results.

A confirmation message displays.

4

Click **DELETE**.

When bulk test results are deleted, notifications are displayed at the bottom of the page to indicate that the operation has started and is completed. When the deletion is completed, the notification icon with a red circle 🔔 at the top right corner indicates that the bulk operation is completed. The notification panel displays an information icon ⓘ to view the status of bulk operations.

5

Click the information icon.

The Delete - Test Suite Run window opens.

ℹ **Note:** The icon beside the bulk operation in the notification panel indicates the status of the operation. For more information see, 7.5.1 “Viewing the Notification Status” (p. 41).

ℹ **Note:** You can view details such as the user and organization names, and successful and failed numbers in the create window.

6

Click **OK**.

End of steps

7.4 Adding or Editing VLANs of a LAN/WAN Port

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of LAN/WAN ports is displayed in the LAN/WAN Ports section.

3

Click the arrow icon ⌄ beside a LAN/WAN port to view the VLANs associated with the port.

4

Perform any of the following actions:

- Click + VLAN icon to add a VLAN. The Add VLAN window opens.
- Select an existing VLAN of the LAN/WAN port, click the **More** icon ⋮ and click the **Edit VLAN** icon ✎ to edit.

5

Configure the following parameters:

Parameter	Description
VLAN*	Enter the number of VLANs to be added (between 0 and 4094). This field cannot be modified.
Description	Enter an optional VLAN description.
VSC Profile	This option is available only on VLANs of a WAN port and when the Type selected is standard. Select a VSC profile from the list and click **Done**.

6

Click **OK**.

End of steps

ℹ **Note:** Each port can display a maximum of 100 VLANs.

7.5 Linking a VLAN to an L3 or L2 Network

Note: The following steps describe how to link a VLAN to a network. You can also link an L3 network to a VLAN. See 12.37 “Linking a Subnet with a VLAN/SSID of a Branch LAN/WiFi Port” (p. 152).

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of LAN ports is displayed in the LAN Ports section.

3

Click the arrow icon ⌄ beside a LAN port to view the VLANs associated with the port

4

Select a VLAN under a LAN port, click the **More** icon ⋮ and select **Link** icon 🔗 to link a VLAN to an L3 network. The Link VLAN window opens.

5

Configure the following parameters:

Parameter	Description
Select Network Type*	Select **L3** from the **Network Type** list.
Select Network*	Select a network name from the **Network** list and click **DONE**.
Subnet*	Select a subnet within the L3 network from the **Subnet** list and click **DONE**. This field is applicable only when the Network Type is L3.
Link Type*	Select a type of link from the **Link Type** list. • **Host** • **Bridge**
IP Address*	Enter a valid IP address of the host interface. This field is applicable only when Select Network Type is **L3** and Link Type is **Host**.
MAC Address*	Enter a valid MAC address of the host interface. This field is applicable only when the link type is **Host**.

Unlinking a VLAN from an L3 or L2 Network

6

Click **OK**.

End of steps

7.6 Unlinking a VLAN from an L3 or L2 Network

Note: This procedure is service-affecting.
You can also unlink an L3 network from a VLAN. See 12.38 “Unlinking a Subnet from a VLAN/SSID of a Branch LAN/WiFi Port” (p. 153).

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The WAN ports and LAN ports are displayed in the WAN ports or LAN Ports section.

3

Click the arrow icon ⌄ beside a port to view the associated VLANs.

4

Select a VLAN, click the **More** icon ⋮ and click the **Unlink** icon to unlink a VLAN from the L3 or L2 network. The Unlink VLAN window opens.

5

Click **UNLINK**.

End of steps

7.7 Deleting VLANs from a LAN Port

Note: If a VLAN is linked to an L3 or L2 network, it cannot be deleted. You need to unlink a VLAN from the network before deleting the VLAN. See 9.22 “Unlinking a VLAN from an L3 or L2 Network” (p. 77).

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of LAN ports is displayed in the LAN Ports section.

3

Click the arrow icon ⌄ beside a LAN port to view the associated VLANs.

4

Select a VLAN and click the **More** icon ⋮ and then click the **Delete** icon 🗑 to delete the VLAN. The **Delete VLAN** window opens.

5

Click **DELETE**.

End of steps

7.8 Assigning an Egress QoS Policy to a WAN or LAN Port

Note: Ensure that the organization has Egress QoS Policy assigned to them (or made global).

1

Navigate to the Branch Overview. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Device**. The list of WAN and LAN ports is displayed.

3

Click the arrow icon ⌄ beside a port to view the associated VLANs.

4

Select a VLAN and click the **More** icon ⋮ and click the **Policies** icon to assign a policy.

5

In the Policies window, select a policy from the **Egress QoS Policy** list and click **DONE**.

6

Click **OK**.

End of steps

7.9 Viewing the Branch Access

1

Navigate to the Branch Dashboard. See 9.4 “Viewing the Branch Overview” (p. 55).

2

From the branch-level menu, select **Access**. The Access page opens.

3

To generate the report for a specific period, select one of the time options – Last hour (default), Last 4 hours, Last 12 hours, Last 24 hours or Last 7 days.

A graphical representation of the uplinks report displays with the following details:

Section	Description
VLAN	Displays the inbound access traffic to branch, outbound access traffic from branch and VLAN port network details for the selected network(s).
SSID	Displays the inbound access traffic to branch, outbound access traffic from branch and WiFi port network details for the selected network(s).
Throughput	A line graph displays the traffic statistics of the network depending on the selected option: • Inbound: Displays the inbound traffic to branch. • Outbound: Displays the outbound traffic from branch. Hover over the graph to view date, time, network and data usage.

End of steps

7.10 Viewing the Branch Usage

1

Navigate to the Branch Dashboard. See 9.4 "Viewing the Branch Overview" (p. 55).

2

From the branch-level menu, select **Usage**. The Usage page opens.

3

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type	Select All (by default) to include all networks or select L3 or L2 from the list.
Network	Enter text to search for a network. Select a network from the list. By default, **All** is selected to include all networks.
Traffic Type	Select All (by default) to include all traffic types in the report or select one type from the list.
Source Branch Personalities	Select All Personalities (by default) to include all the source branch personalities or select from the list. The available options are: • Branch • Gateway • Border Router
Source Branch	By default, displays the branch context and cannot be changed.
Destination Branch Personalities	Select All Personalities (by default) to include all the destination branch personalities or select from the list. The available options are: • Branch • Gateway • Border Router
Destination Branch	Enter text to search for a destination branch. Select a destination branch from the list. By default, **All** is selected to include all destination branches.
Application Type	Select an option from the list. The following options are available: • All: Displays traffic data all the applications groups. • Discovered Applications: Displays the traffic data for default application groups. • Application Groups: Displays the traffic data for user-defined application groups. This option is enabled when a network is selected.
Application Group	Select an application group from the list. This field is enabled when the application type is application group.

Parameter	Description
Application	Enter text to search for an application. Select an application from the list. By default, **All** is selected to include all applications. Available only when built-in applications for Application Type is selected.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

4

Click **RUN REPORT**.

The usage report displays a table listing each application, a graph of the inbound and outbound traffic, and other traffic data.

The list with expandable rows allows users to view traffic throughput per-application. Hover over the graph to view date, time, network and data usage.

End of steps

7.11 Viewing the Alarms of a Branch

1

Navigate to the Branch Dashboard. See 9.4 "Viewing the Branch Overview" (p. 55).

2

From the branch-level menu, select **Alarms**.

The Alarms page displays the alarms list of the selected branch with the following details:

Section	**Description**
Severity	Provides the Critical, Info, Major, Minor and Warning severity of alarms.
Time	Provides the view of alarms sorted by time.
Title	Provides the view of alarms sorted by title.
Alarmed Object	Provides the view of alarms sorted by devices.
Description	Provides the description of the alarm.

End of steps

8 Managing Security

8.1 Viewing the Security Dashboard

You can view the Security dashboard if you have Manage Subscribers and Security enabled, and have any of the following permissions:

Permissions	Widget visible on Security Dashboard
View Web Category and Domain Widgets	• Top Web Categories • Top Web Domains **Note**: The Web Filtering option must be enabled at the organization profile from the VSD to view the web category and web domain widgets on the security dashboard.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, select **Security**.

By default, Overview is selected.

3

Select a time from the duration icon 🕓 to view the data on the dashboard.

Toggle the Auto-Refresh button to enable auto-refresh. For more information, see 8.4.1 "Auto-Refresh for Dashboards" (p. 48).

The Security Dashboard displays the following widgets:

Widget	Description
Top Web Categories	Displays the top web categories. By default, **Allowed** is selected. Click **Denied** to view the denied web categories. **Note**: Polices are created at the web category level to define the traffic action.
Top Web Domains	Displays the top web domains. By default, **Allowed** is selected. Click **Denied** to view the denied web domains. Polices are created at the web domain level to define the traffic action.

End of steps

Based on the View selected, the Security Dashboard displays different pages. The list of options available are:

- Overview
- 12.43.1 “Event Explorer” (p. 161)

8.2 Overview

- Select a time range from **Duration**. Data related to security event types, security events of top networks, top web categories, top web domains, is displayed.
- Enable the Auto-Refresh option to refresh the dashboard data automatically. For more information, see 8.4.1 “Auto-Refresh for Dashboards” (p. 48).
- Click the **Reset Dashboard** icon ▦ to reset the widgets to their default positions. If the user does not have the permission to view a widget, blank space is displayed in the Dashboard. The user must manually rearrange the widgets in the dashboard to remove the blank space.

The Security Dashboard comprises the following widgets:

Widget	Description
Top Networks	Displays a bar graph for top five L2 or L3 networks based on the security events. Click an L3 network link to navigate to the L3 Networks security dashboard. The L3 network link is enabled only if you have the “View L3 Networks” permission. The type of network (L2/L3) is displayed in brackets next to the network name. When the timestamp is changed in the Security Dashboard, and the user navigates to the L3 Network Dashboard, the timestamp in the L3 network security dashboard is also updated. The **View Event Explorer** provides a quick access to the Event Explorer page.
Security Event Types	Displays a pie chart for the different types of security events. Hover over the pie chart to view the security event types and number of events in percentage. The **View Event Explorer** provides a quick access to the Event Explorer page.
Top Web Categories	Displays the top web categories. By default, **Denied** is selected. Click **Allowed** to view the allowed web categories. **Note**: Polices are created at the web category level to define the traffic action.
Top Web Domains	Displays the top web domains. By default, **Denied** is selected. Click **Allowed** to view the allowed web domains. Polices are created at the web domain level to define the traffic action.

9 Reports

Reports are available to organizations that have been assigned with appropriate customer profiles and users with appropriate roles.

Note: The data points used for graphs are based on the reporting period.

- For report periods up to 1 hour, there is one data point per each minute.
- For report periods between 1 to 4 hours, there is one data point per every 5 minutes.
- For report periods between 4 to 24 hours, there is one data point per every 15 minutes.
- For report periods between 1 day to 30 days, there is one data point per each hour.
- For report periods between 30 days to 90 days, there is one data point per every 3 hours.
- For report periods between 90 days to 1 year, there is one data point per every 6 hours.
- For report periods above 1 year, there is one data point per every 24 hours.

9.1 Generating the Branch Traffic Details Report

The View Branch Traffic Detail Report, View Branch Network Port, View Branches, and View VLANs should be enabled for the user to view the branch traffic details report. See also 15.9 "Adding or Editing a User Group" (p. 256) to enable View Branch Traffic Detail Report.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Branch Traffic Details Report**.

The Branch Traffic Details Report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Branch	Enter text to search for a branch. Select a branch from the list and click **DONE**.

Parameter	Description
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last14 days.

5

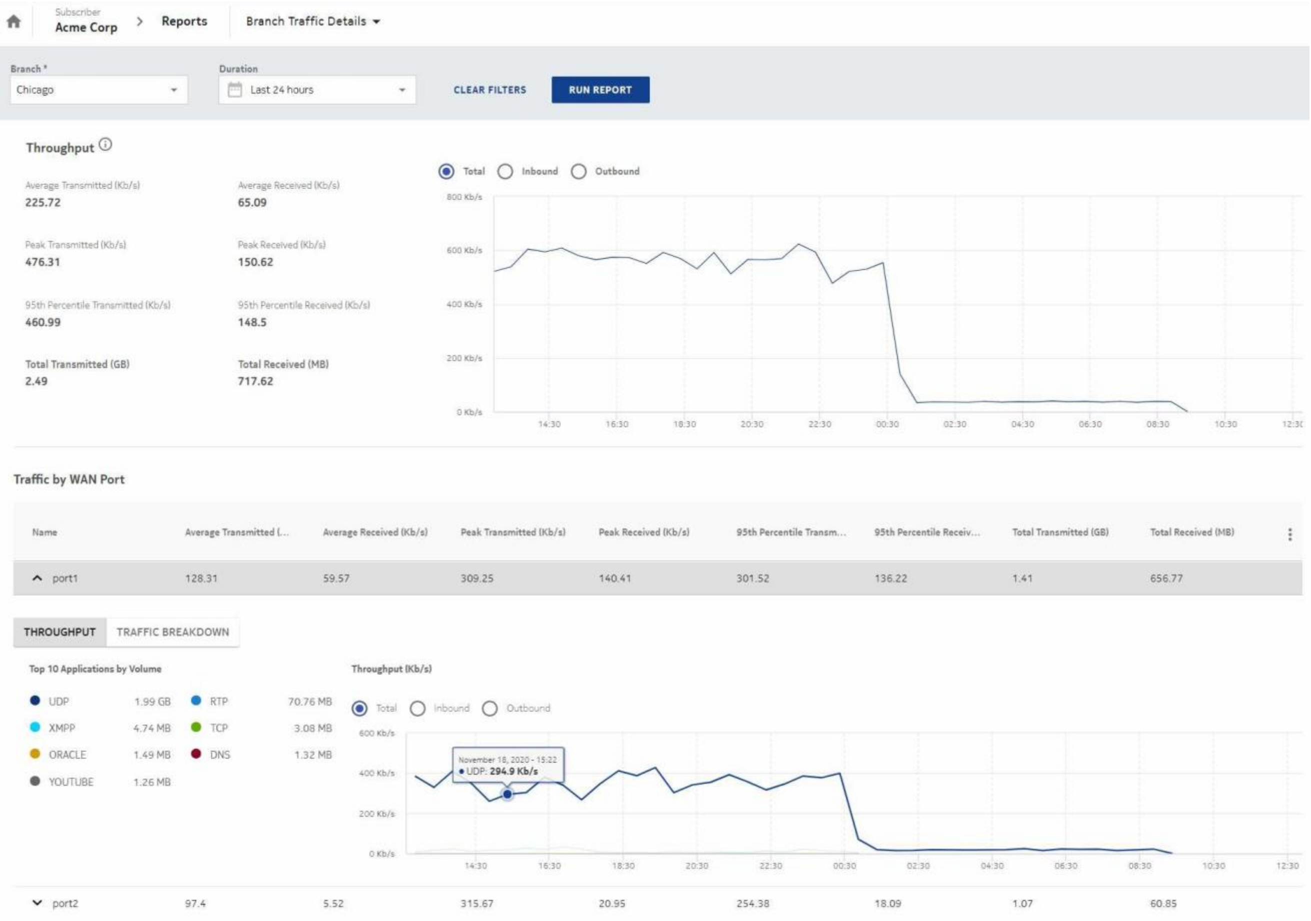
Click **RUN REPORT**.

A graphical representation of the branch traffic details report displays with the following details:

Section	Description
Throughput	The VLAN throughput line graph includes the blocklisted traffic and regular traffic and receives data from port statistics in ES. Displays the total throughput (total transmitted and total received) traffic of a selected branch. Traffic details are from a branch point of view. Inbound traffic means traffic coming into a branch, and Outbound traffic indicates traffic going out of a branch. A graph displays the traffic statistics of the network depending on the selected option: • Total: Displays the total traffic (inbound and outbound) for the selected branch. • Inbound: Displays the inbound traffic for the selected branch. • Outbound: Displays the outbound traffic for the selected branch. Hover over the graph to view date, time, network and data usage.

Section	Description
Traffic by WAN Port	A table displays the average transmitted/received, peak transmitted/received, 95th percentile transmitted/received and total volume of traffic transmitted/received for each branch’s WAN port. Click the arrow beside the port name to view the following: • **Throughput** The Throughput tab displays a graph with the top 10 applications along with the total, inbound and outbound traffic. You can also deselect the application by clicking on the application and remove the traffic representation in the graph. • **Traffic Breakdown** Click the Traffic Breakdown tab to view the pie chart for the top 10 applications. Select a pie or a legend to view the top 5 destination branches. The table displays the top 5 destinations for the selected category with the total, inbound and outbound traffic. • **IKE Throughput** Click the IKE Throughput tab to view the IKE statistics. Click an IKE tunnel name to view the total, inbound and outbound traffic.
Traffic by Uplink	The Traffic by Uplink section displays the traffic details of each port.

Figure 14-1 Sample Branch Traffic Details Report



Subscriber Acme Corp > Reports | Branch Traffic Details ▾

Branch *: Chicago ▾

Duration: Last 24 hours ▾

CLEAR FILTERS | RUN REPORT

Throughput ⓘ

Average Transmitted (Kb/s) 225.72	Average Received (Kb/s) 65.09
Peak Transmitted (Kb/s) 476.31	Peak Received (Kb/s) 150.62
95th Percentile Transmitted (Kb/s) 460.99	95th Percentile Received (Kb/s) 148.5
Total Transmitted (GB) 2.49	Total Received (MB) 717.62

◉ Total ○ Inbound ○ Outbound

Traffic by WAN Port

Name	Average Transmitted (...	Average Received (Kb/s)	Peak Transmitted (Kb/s)	Peak Received (Kb/s)	95th Percentile Transm...	95th Percentile Receiv...	Total Transmitted (GB)	Total Received (MB)
^ port1	128.31	59.57	309.25	140.41	301.52	136.22	1.41	656.77
˅ port2	97.4	5.52	315.67	20.95	254.38	18.09	1.07	60.85

THROUGHPUT | TRAFFIC BREAKDOWN

Top 10 Applications by Volume

● UDP	1.99 GB	● RTP	70.76 MB
● XMPP	4.74 MB	● TCP	3.08 MB
● ORACLE	1.49 MB	● DNS	1.32 MB
● YOUTUBE	1.26 MB		

Throughput (Kb/s)

◉ Total ○ Inbound ○ Outbound

November 18, 2020 - 15:22
● UDP: **294.9 Kb/s**

End of steps

9.2 Generating the Network Traffic Summary Report

The View Network Traffic Summary Report, View L3 Networks and View L2 Networks should be enabled for the user to view the network traffic summary reports. See also 15.9 "Adding or Editing a User Group" (p. 256) to enable View Network Traffic Summary Report.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Network Traffic Summary**.

The Network Traffic Summary Report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type*	Select L2 or L3 network type. **Note**: If you have the permissions to view the L2 and L3 network, then by default, L3 network is selected. If you have either of the permissions, then only those network types are visible.
Networks*	Enter text to search for a network. Select a network from the list. You can select multiple networks to include in the report. This option is enabled only if a network type is selected.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

5

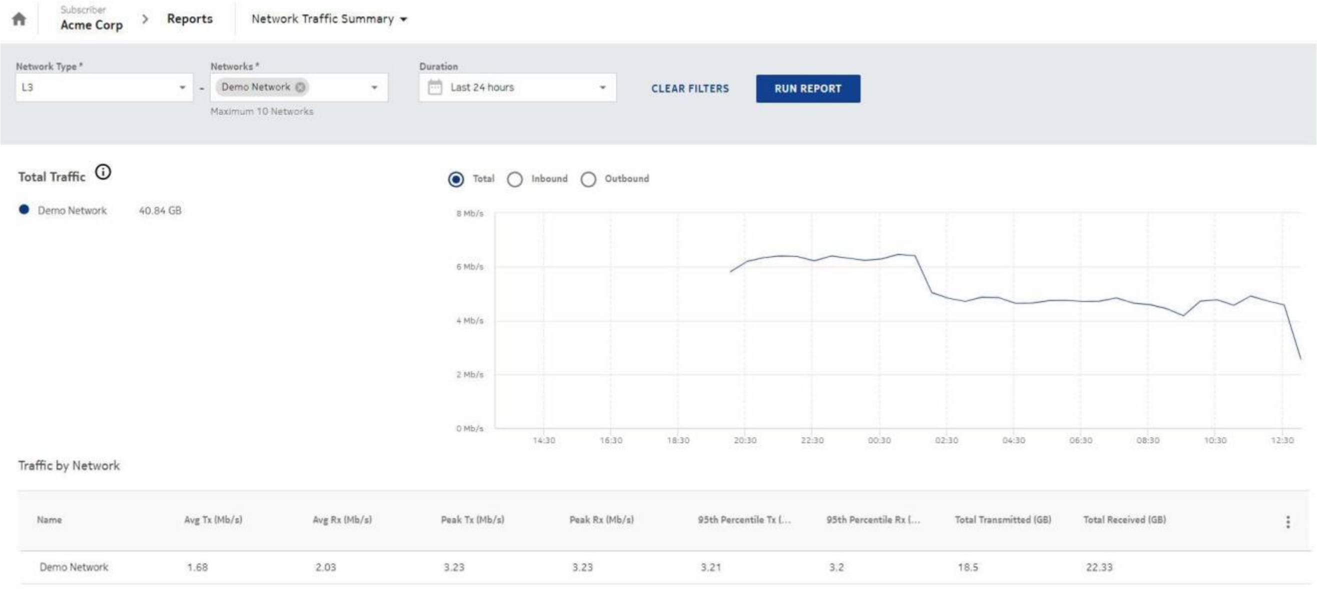
Click **RUN REPORT**.

Select a network in the Traffic by Network section and click the arrow icon → that appears beside the network name to navigate to the Network Traffic Details Report page.

A graphical representation of the network traffic summary report displays with the following details:

Section	Description
Total Traffic	Displays the total traffic for each selected network(s). Traffic details are from a branch point of view. Inbound traffic means traffic coming into a branch, and Outbound traffic indicates traffic going out of a branch. A line graph displays the traffic statistics of the network depending on the selected option: • Total: Displays the total traffic (inbound and outbound) for the selected networks. • Outbound: Displays the outbound traffic for the selected networks. • Inbound: Displays the inbound traffic for the selected networks. Hover over the graph to view date, time, network, and average throughput in Mb/s.
Traffic by Network	A table displays the network name (L7classification), average transmitted/received, peak transmitted/received, 95th percentile transmitted/received, and total traffic throughput for an organization's L3 or L2 network.

Figure 14-2 Sample Network Traffic Summary Report



Network Type *: L3

Networks *: Demo Network

Maximum 10 Networks

Duration: Last 24 hours

● Total

● Demo Network 40.84 GB

Traffic by Network

Name	Avg Tx (Mb/s)	Avg Rx (Mb/s)	Peak Tx (Mb/s)	Peak Rx (Mb/s)	95th Percentile Tx (...	95th Percentile Rx (...	Total Transmitted (GB)	Total Received (GB)
Demo Network	1.68	2.03	3.23	3.23	3.21	3.2	18.5	22.33

End of steps

9.3 Generating the Application Details Report

The View Application Details Report, View Application Groups, View Application Signatures, View Branches, View L3 Networks, View L3 Network Application Groups, View L2 Networks and View L2 Network Application Groups should be enabled for the user to view the application details report.

See also 15.9 “Adding or Editing a User Group” (p. 256) to enable View Application Details Report.

1

Navigate to your organization's Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Application Details**.

The Application Details report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type	Select All (by default) to include all networks or select L3 or L2 from the list.
Network	Enter text to search for a network. Select a network from the list. Select either All (by default) or only one network at a time.
Traffic Type	Select All (by default) to include all traffic types in the report or select one type from the list.
Source Branch	Enter text to search for a source branch. Select a source branch from the list.
Destination Branch	Enter text to search for a destination branch. Select a destination branch from the list.

Parameter	Description
Application Type	Select an option from the list. The following options are available: • All: Displays all the traffic data of the application groups (aggregation is performed based on the L7 classification). • Discovered Applications: Displays traffic data for the application groups named as "Default Application Group." Aggregation is performed based on L7 classification. • Application Groups: Displays traffic data for all the application groups but aggregation is performed based on application name within the selected application group. **Note**: It is enabled when a network is selected.
Application Group	Select an application group from the list. This field is enabled when the application type is application group.
Application	Select an application from the list. It is enabled when an application type is selected. When the Application Type is All or Discovered, application signatures are listed. Else, applications under the selected application groups are listed.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

5

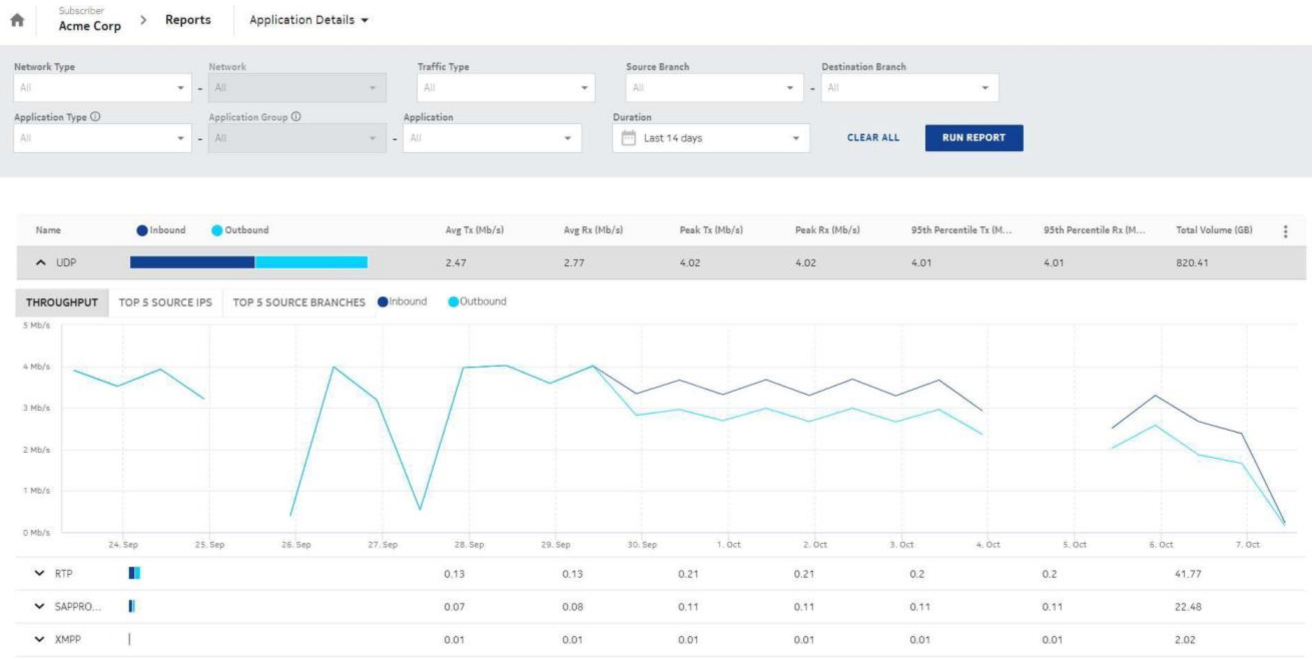
Click **RUN REPORT**.

The application details report displays the application name (L7 Classification), volume (inbound/outbound), average transmitted/received, peak transmitted/received, 95th percentile transmitted/received and total volume of traffic for an organization’s network. Click the pull-down arrow beside the application name. The THROUGHPUT tab displays a graph for the inbound and outbound traffic.

Click the TOP 5 SOURCE IPS tab to view the details of the top 5 source IPS, source branch and network. It also displays the inbound and outbound traffic details. Click the TOP 5 SOURCE BRANCHES to view the top 5 source branches. Select a source branch to view the associated top 5 destination branches by clicking the arrow icon → that appears beside the branch name.

Click the TOP 5 SOURCE BRANCHES to view the top 5 source branches. Select a source branch to view the associated top 5 destination branches by clicking the arrow icon → that appears beside the branch name.

Figure 14-3 Sample Application Details Report



Network Type: All - Network: All
Traffic Type: All
Source Branch: All - Destination Branch: All
Application Type: All - Application Group: All - Application: All
Duration: Last 14 days

Name	● Inbound ● Outbound	Avg Tx (Mb/s)	Avg Rx (Mb/s)	Peak Tx (Mb/s)	Peak Rx (Mb/s)	95th Percentile Tx (M...	95th Percentile Rx (M...	Total Volume (GB)
UDP		2.47	2.77	4.02	4.02	4.01	4.01	820.41
RTP		0.13	0.13	0.21	0.21	0.2	0.2	41.77
SAPPRO...		0.07	0.08	0.11	0.11	0.11	0.11	22.48
XMPP		0.01	0.01	0.01	0.01	0.01	0.01	2.02

End of steps

9.4 Generating the Branch Device Metrics Report

The View Branch Device Metrics Report, Branches and View Branches permissions must be enabled for the user to view the branch device metrics report.

See also 15.9 "Adding or Editing a User Group" (p. 256) to enable Branch Device Metrics Report.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Branch Device Metrics** to view the report page.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Branches*	Enter text to search for a branch or select a branch from the list and click **DONE**. You can select a maximum of 10 branches.
Status For	Select one of the options: • CPU • Memory • Storage
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

5

Click **RUN REPORT**.

When CPU or Memory is selected in the Status For field, the report displays a table with the branch, redundancy group, latest utilization percentage, recorded at, peak, and average utilization percentage.

When Storage is selected in the Status For field, the report displays a table with the branch, redundancy group, latest utilization percentage, recorded at, latest utilization (GB or MB) and total number of partition counts.

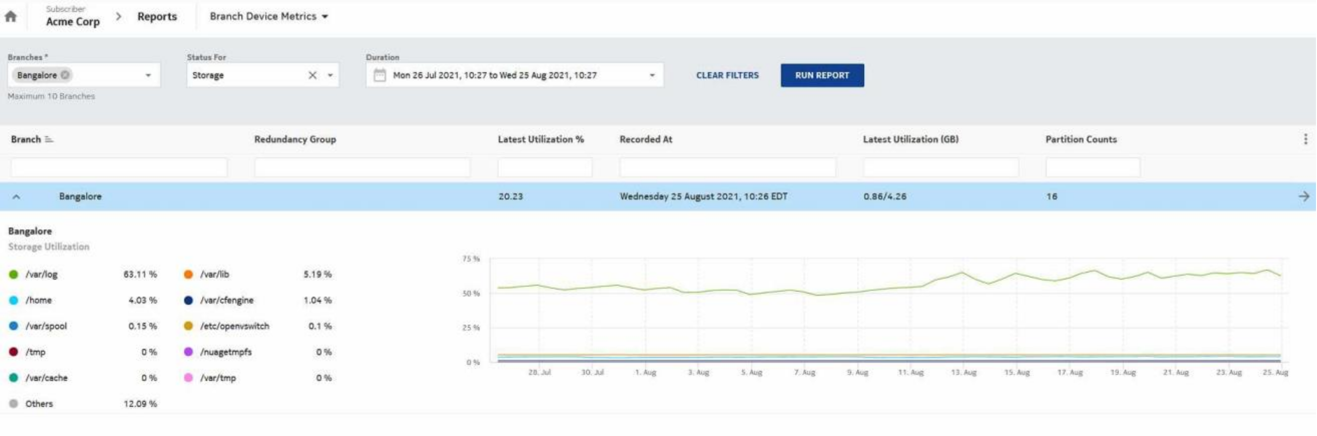
Note:

- The four partitions (/, /dev*, /run*, /sys) are always classified under **Others**.
- The partition **Others** will also include partitions which are not in the top 10.

Select a branch and click the arrow icon → to navigate to the Branch Overview page.

Select a branch and click the arrow icon ⌄ to view the graphical representation for the selected status. You can generate reports on CPU utilization, Memory Utilization and Storage Utilization.

Figure 14-4 Sample Branch Device Metrics Report for Storage



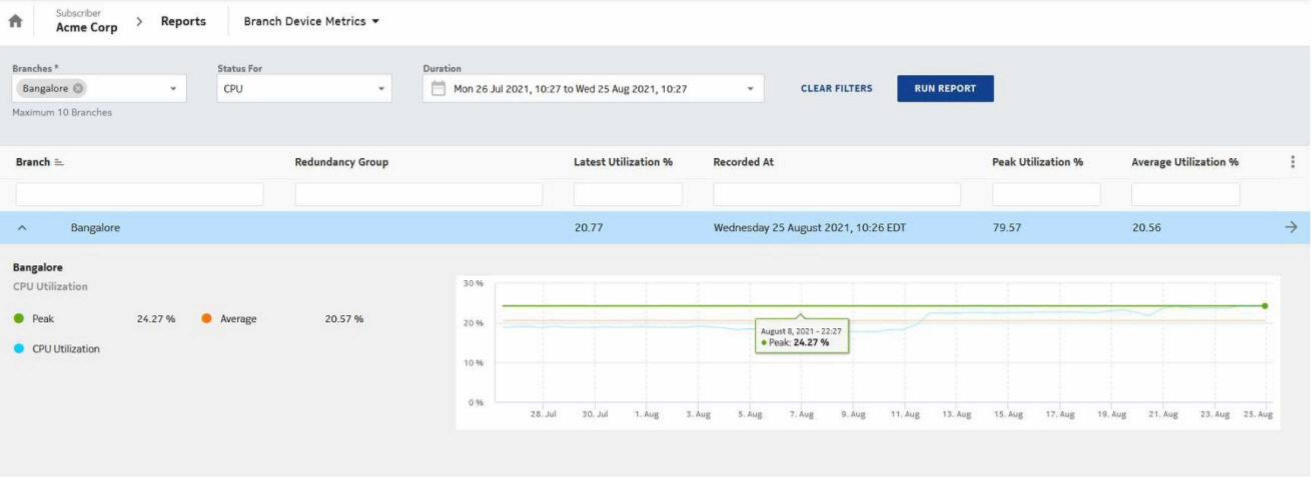
Branches *: Bangalore
Maximum 10 Branches
Status For: Storage
Duration: Mon 26 Jul 2021, 10:27 to Wed 25 Aug 2021, 10:27

Branch	Redundancy Group	Latest Utilization %	Recorded At	Latest Utilization (GB)	Partition Counts
Bangalore		20.23	Wednesday 25 August 2021, 10:26 EDT	0.86/4.26	16

Bangalore
Storage Utilization

/var/log	63.11 %	/var/lib	5.19 %
/home	4.03 %	/var/cfengine	1.04 %
/var/spool	0.15 %	/etc/openvswitch	0.1 %
/tmp	0 %	/nuagetmpfs	0 %
/var/cache	0 %	/var/tmp	0 %
Others	12.09 %		

Figure 14-5 Sample Branch Device Metrics Report for CPU/Memory



Branches *: Bangalore
Maximum 10 Branches
Status For: CPU
Duration: Mon 26 Jul 2021, 10:27 to Wed 25 Aug 2021, 10:27

Branch	Redundancy Group	Latest Utilization %	Recorded At	Peak Utilization %	Average Utilization %
Bangalore		20.77	Wednesday 25 August 2021, 10:26 EDT	79.57	20.56

Bangalore
CPU Utilization

Peak	24.27 %	Average	20.57 %
CPU Utilization			

End of steps

9.5 Generating the User Activity Report

The View User Activity Report should be enabled for the user to view the user activity reports. See also 15.9 "Adding or Editing a User Group" (p. 256) to enable View User Activity Report.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **User Activity**.

The User Activity report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Organizations	Select an organization from the list and click **Done**. **Note**: This field is available only if you have logged in as a Reseller organization user.
Users	Select either All (by default) or only one user from the list and click **Done**. **Note**: If you have logged in as a reseller, the Users option is enabled only when an organization is selected. The list displays names of users that belong to the selected organization.
Events	Select either All (by default) or one of the events from the list.
Objects	Select either All (by default) or one of the objects from the list.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

5

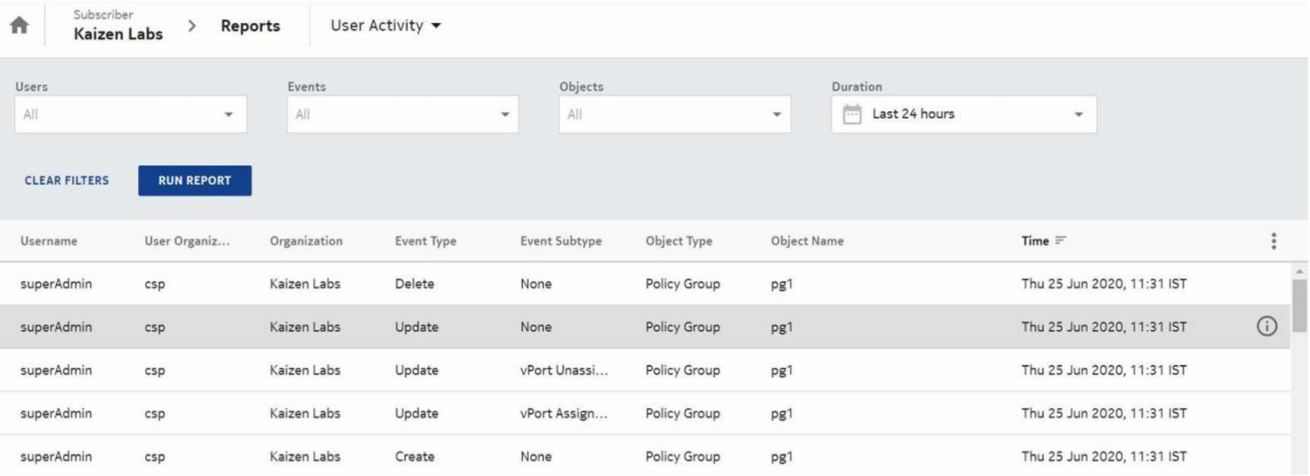
Click **RUN REPORT**.

The user activity report displays the Username, User ID, User Organization, Organization, Organization ID, Event Type, Event Subtype, Object Type, Object Name and Time.

ℹ **Note**: If an organization is deleted from the portal and re-imported, the report continues to display the data, showing both the deletion of the organization, and it is re-imported with a new ID.

The organization and user lists can be filtered by entering a partial name. The list of users and organizations is based on the audit data. If an organization or users have not performed any operations that generated an audit entry, then their names will not display in the list.

Figure 14-6 Sample User Activity Report



Users: All

Events: All

Objects: All

Duration: Last 24 hours

Username	User Organiz...	Organization	Event Type	Event Subtype	Object Type	Object Name	Time
superAdmin	csp	Kaizen Labs	Delete	None	Policy Group	pg1	Thu 25 Jun 2020, 11:31 IST
superAdmin	csp	Kaizen Labs	Update	None	Policy Group	pg1	Thu 25 Jun 2020, 11:31 IST
superAdmin	csp	Kaizen Labs	Update	vPort Unassi...	Policy Group	pg1	Thu 25 Jun 2020, 11:31 IST
superAdmin	csp	Kaizen Labs	Update	vPort Assign...	Policy Group	pg1	Thu 25 Jun 2020, 11:31 IST
superAdmin	csp	Kaizen Labs	Create	None	Policy Group	pg1	Thu 25 Jun 2020, 11:31 IST

6

Click the **Event Information** icon ⓘ for the required user to view the event information for the selected duration.

End of steps

9.6 Generating the User Security Report

The View User Security Report permission should be enabled for the user to view the user security report.

See also 15.9 "Adding or Editing a User Group" (p. 256) to enable User Security Report.

1

Perform any of the following actions as per your role:

- If you are a reseller organization user, from the reseller organization menu, select **Reports**.
- If you are a subscriber organization user, from the organization dashboard-level menu, select **Reports**.

The Reports page is displayed.

2

Click **User Security**.

The User Security Report page opens.

3

To generate the report for a specific period, configure the following parameters:

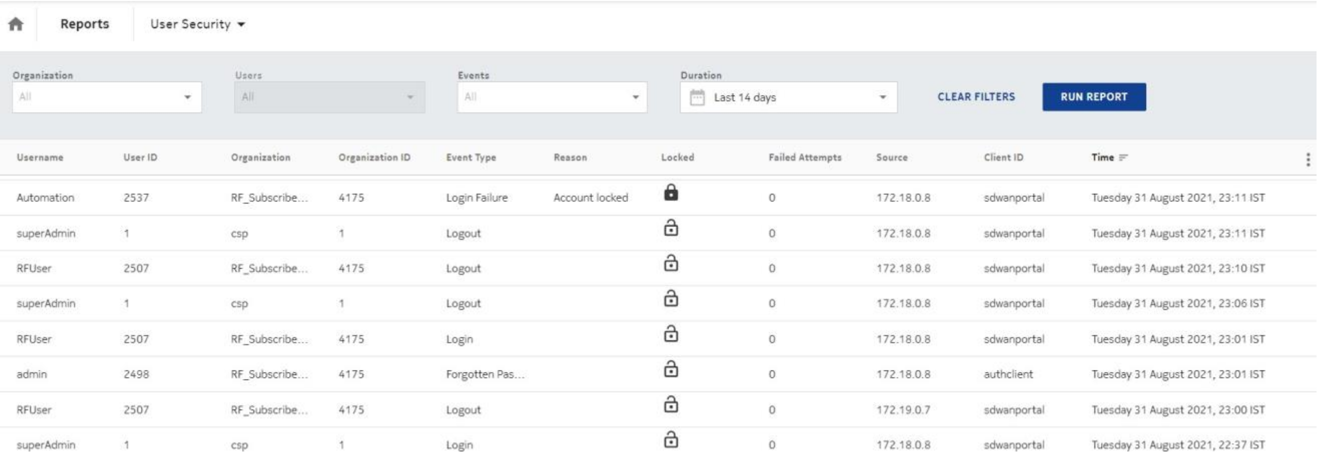
Parameter	Description
Organization	Select an organization from the list and click **Done**. **Note**: This field is available only if you have logged in as a Reseller user.
Users	Select either All (by default) or only one user from the list and click **Done**. **Note**: If you have logged in as a CSP or a reseller, the Users option is enabled only when an organization is selected. The list displays names of users that belong to the selected organization.
Events	Select an event from the following: • Change Password • Change Password Failure • Forgotten Password Failure • Forgotten Password Request • Forgotten Password Reset • Login • Login Failure • Logout
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

4

Click **RUN REPORT**.

The table displays details such as Username, User ID, Organization ID, Organization, Event Type, Reason, Locked, Failed Attempts, Source, Client ID and Time.

Figure 14-7 Sample User Security Report



Username	User ID	Organization	Organization ID	Event Type	Reason	Locked	Failed Attempts	Source	Client ID	Time
Automation	2537	RF_Subscribe...	4175	Login Failure	Account locked	🔒	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 23:11 IST
superAdmin	1	csp	1	Logout		🔓	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 23:11 IST
RFUser	2507	RF_Subscribe...	4175	Logout		🔓	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 23:10 IST
superAdmin	1	csp	1	Logout		🔓	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 23:06 IST
RFUser	2507	RF_Subscribe...	4175	Login		🔓	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 23:01 IST
admin	2498	RF_Subscribe...	4175	Forgotten Pas...		🔓	0	172.18.0.8	authclient	Tuesday 31 August 2021, 23:01 IST
RFUser	2507	RF_Subscribe...	4175	Logout		🔓	0	172.19.0.7	sdwanportal	Tuesday 31 August 2021, 23:00 IST
superAdmin	1	csp	1	Login		🔓	0	172.18.0.8	sdwanportal	Tuesday 31 August 2021, 22:37 IST

End of steps

9.7 Generating the Application Group Performance Report

The View Application Group Performance Report, View Branches, View L3 Networks, View L3 Network Application Groups, View Branch Uplink, View L2 Networks, View L2 Network Application Groups and View Traffic Throughput Statistics should be enabled for the user to view the application group performance report. See also 15.9 “Adding or Editing a User Group” (p. 256) to enable Application Group Performance Report.

The Application Group Performance Report provides performance details of all applications within a selected application group that is attached to a network. The performance details include the application group adherence and performance metric, along with SLA violation details for the selected application group.

1

Navigate to your organization's Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Application Group Performance**.

The Application Group Performance report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type*	Select L2 or L3 network type from the list. **Note**: If you have the permissions to view the L2 and L3 network, then by default, L3 network is selected. If you have either of these permissions, then only those network types are visible.
Network*	Select a network from the list. You can select only one network at a time.
Application Group*	Select a network to enable Application Group. Select a performance monitored enabled application group from the list. Aggregation is performed based on the application name.
Source Branch*	Enter text to search for a source branch. Select a source branch from the list.
Destination Branch*	Enter text to search for a destination branch. Select a destination branch from the list.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date, or range of time for the report. The start date and end date selection range is limited to 30 days or less.

5

Click **RUN REPORT**.

ℹ **Note**: Performance statistics shown in Application Group Performance report like Latency, Jitter and Packet Loss are dependent only on branches selected for source and destination branch pickers. It is independent of the Network selected in the Network picker in the report.

The report identifies peak and average latency (ms), peak and average jitter (ms), and peak and average packet loss (%) for each Source-Destination branch for the selected network. The report consists of a table, containing the average peak and average values of latency, jitter and packet loss for the reporting period. With associated latency, jitter and packet loss graphs of the averaged data over the same period. The data in the report is not representative of the raw latency, jitter and packet loss values, but is instead averaged out over the time slices in the reporting period. It is therefore expected that some degree of smoothing in the results will be apparent as the requested range of the report is increased. For the best accuracy, smaller reporting intervals should be used.

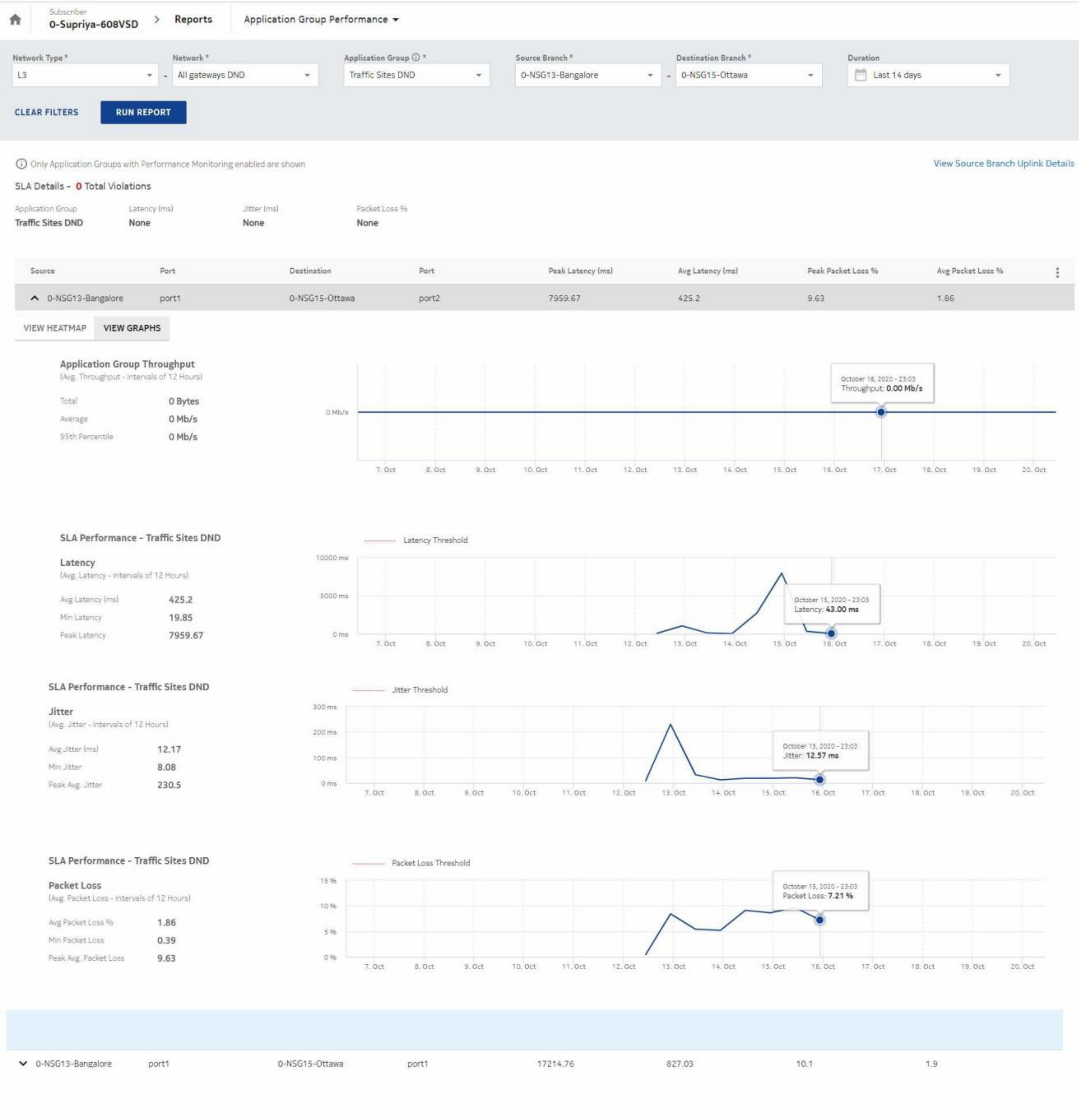
Click View Source Branch Uplink Details link at the top right corner to navigate to the Uplinks page. This link is available only if there is data available for the report and you have the permissions to view the branch uplinks.

On clicking the link, the Uplinks page for the source branch is displayed and is filtered for the selected network and application group.

A graphical representation of the application group performance report displays with the following details:

Section	Description
SLA Details	Displays the total violations including the application SLA group, latency, jitter and packet loss for the selected application group.
	A table displays the source branch and port, destination branch and port, latency (peak and average), packet loss (peak and average) and peak for an application group. Click the pull-down arrow beside the application name to display. • **VIEW HEATMAP -** displays the application names. • **VIEW GRAPHS** - Application Group Throughput: Displays the total, average, 95th percentile and a line graph displays the statistics of the application group throughput. - SLA Performance (Latency, Jitter and Packet Loss): Displays the average, minimum, and peak threshold statistics of the application group throughput.

Figure 14-8 Sample Application Group Performance Report



Subscriber
0-Supriya-608VSD > Reports | Application Group Performance ▾

Network Type *	Network *	Application Group ⓘ *	Source Branch *	Destination Branch *	Duration
L3	All gateways DND	Traffic Sites DND	0-NSG13-Bangalore	0-NSG15-Ottawa	Last 14 days

CLEAR FILTERS | RUN REPORT

ⓘ Only Application Groups with Performance Monitoring enabled are shown

View Source Branch Uplink Details

SLA Details - 0 Total Violations

Application Group	Latency (ms)	Jitter (ms)	Packet Loss %
Traffic Sites DND	None	None	None

Source	Port	Destination	Port	Peak Latency (ms)	Avg Latency (ms)	Peak Packet Loss %	Avg Packet Loss %
^ 0-NSG13-Bangalore	port1	0-NSG15-Ottawa	port2	7959.67	425.2	9.63	1.86
˅ 0-NSG13-Bangalore	port1	0-NSG15-Ottawa	port1	17214.76	827.03	10.1	1.9

VIEW HEATMAP | VIEW GRAPHS

Application Group Throughput
(Avg. Throughput - Intervals of 12 Hours)

Total	0 Bytes
Average	0 Mb/s
95th Percentile	0 Mb/s

October 16, 2020 - 23:03
Throughput: 0.00 Mb/s

SLA Performance - Traffic Sites DND

Latency
(Avg. Latency - intervals of 12 Hours)

Avg Latency (ms)	425.2
Min Latency	19.85
Peak Latency	7959.67

October 15, 2020 - 23:03
Latency: 43.00 ms

SLA Performance - Traffic Sites DND

Jitter
(Avg. Jitter - Intervals of 12 Hours)

Avg Jitter (ms)	12.17
Min Jitter	8.08
Peak Avg. Jitter	230.5

October 15, 2020 - 23:03
Jitter: 12.57 ms

SLA Performance - Traffic Sites DND

Packet Loss
(Avg. Packet Loss - Intervals of 12 Hours)

Avg Packet Loss %	1.86
Min Packet Loss	0.39
Peak Avg. Packet Loss	9.63

October 15, 2020 - 23:03
Packet Loss: 7.21 %

End of steps

9.8 Generating the Application Performance Inventory Details Report

The View Application Performance Inventory Report, View Application Groups, View L3 Network Application Groups, L3 Networks (View L3 Networks) and Branches (View Branches) View L2 Networks, View L2 Network Application Groups should be enabled for the user to view the application performance inventory details report. See also 15.9 "Adding or Editing a User Group" (p. 256) to enable Application Performance Inventory Details Report.

The Application Performance Inventory Details report lists the applications of different networks and branch pairs by their performance score (High, Medium and Low) thereby enabling options for further targeted analysis.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Application Performance Inventory Details**.

The Application Performance Inventory Details report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Performance	An application performance is categorized based on percentage of flows which are within the SLA limits. The following options are available: • High: Minimum InSLA % is 70 and maximum InSLA % is 100 • Moderate: Minimum InSLA % is 16 and maximum InSLA is 69 • Low: Minimum InSLA % is 0 and maximum InSLA % is 15
Network Type	Select either All (by default) or only L2 or L3 networks.
Network	Enter text to search for a network. Select a network from the list. Select either All (by default) or only one network at a time. **Note**: This option is enabled only when a network type is selected.

Parameter	Description
Source Branch	Enter text to search for a source branch. Select a source branch from the list.
Destination Branch	Enter text to search for a destination branch. Select a destination branch from the list.
Application Group	**Note**: Select a network to enable this option. Application groups that are associated to the selected network are only displayed in the drop-down list. Select only performance monitored enabled application group from the list. Aggregation is based on the application name.
Application	**Note**: Select a network and an application group to enable this option. Select an application from the list.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

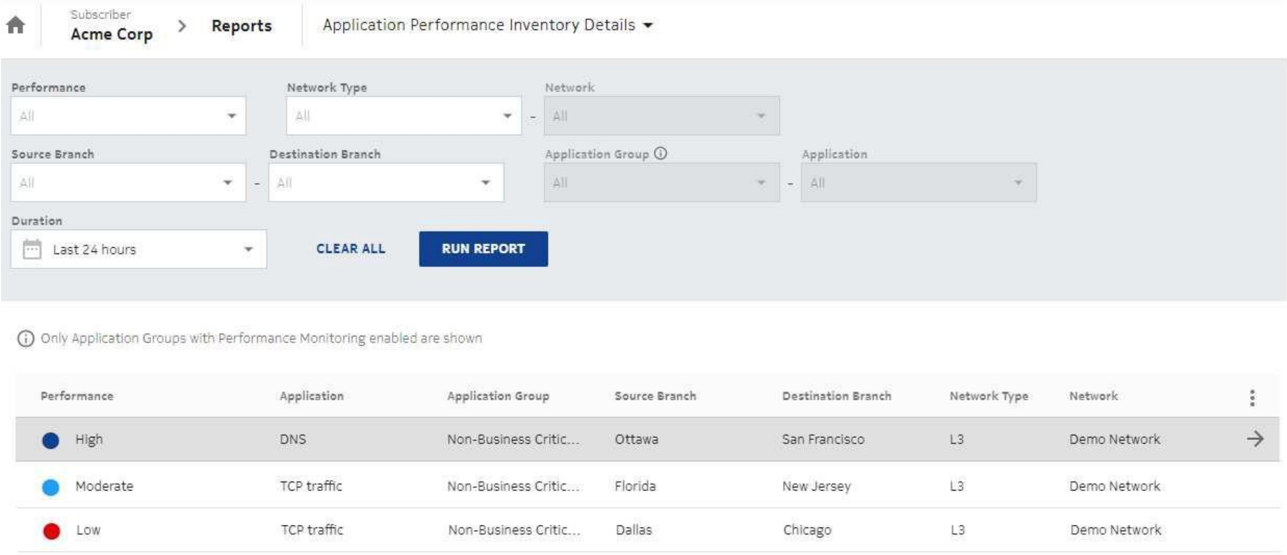
5

Click **RUN REPORT**.

The application performance inventory details report displays a table listing each application’s group, source and destination branch, and network categorized as High, Moderate or Low. The report displays the application groups which have the performance monitoring enabled.

To view details of an application group and its performance report, select an application and click the arrow icon → that appears beside it. The View Application Group Performance Report, View L3 Network Application Groups and Branches (View Branches) should be enabled for the user to view the application group performance report.

Figure 14-9 Sample Application Performance Inventory Details Report



Subscriber
Acme Corp > Reports | Application Performance Inventory Details ▾

Performance: All ▾
Network Type: All ▾ - Network: All ▾
Source Branch: All ▾ - Destination Branch: All ▾
Application Group ⓘ: All ▾ - Application: All ▾
Duration: Last 24 hours ▾

CLEAR ALL | RUN REPORT

ⓘ Only Application Groups with Performance Monitoring enabled are shown

Performance	Application	Application Group	Source Branch	Destination Branch	Network Type	Network
● High	DNS	Non-Business Critic...	Ottawa	San Francisco	L3	Demo Network
● Moderate	TCP traffic	Non-Business Critic...	Florida	New Jersey	L3	Demo Network
● Low	TCP traffic	Non-Business Critic...	Dallas	Chicago	L3	Demo Network

End of steps

9.9 Generating the Network Performance Report

The View Network Performance Report and View Branches should be enabled for the user to view the network performance report. See also 15.9 “Adding or Editing a User Group” (p. 256) to enable Network Performance Report.

1

Navigate to your organization's Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

Perform any of the following actions:

- From the dashboard-level menu, click **Reports**.
  The reports page is displayed.
  Click **Network Performance**.
  The Network Performance report page opens.
- See 12.9 “Viewing Network Performance Report” (p. 123).

3

To generate the report, configure the following parameters:

Parameter	Description
Source Branch*	Enter text to search for a source branch. Select a source branch from the list.
Destination Branch*	Enter text to search for a destination branch. Select a destination branch from the list.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date or time range for the report.

4

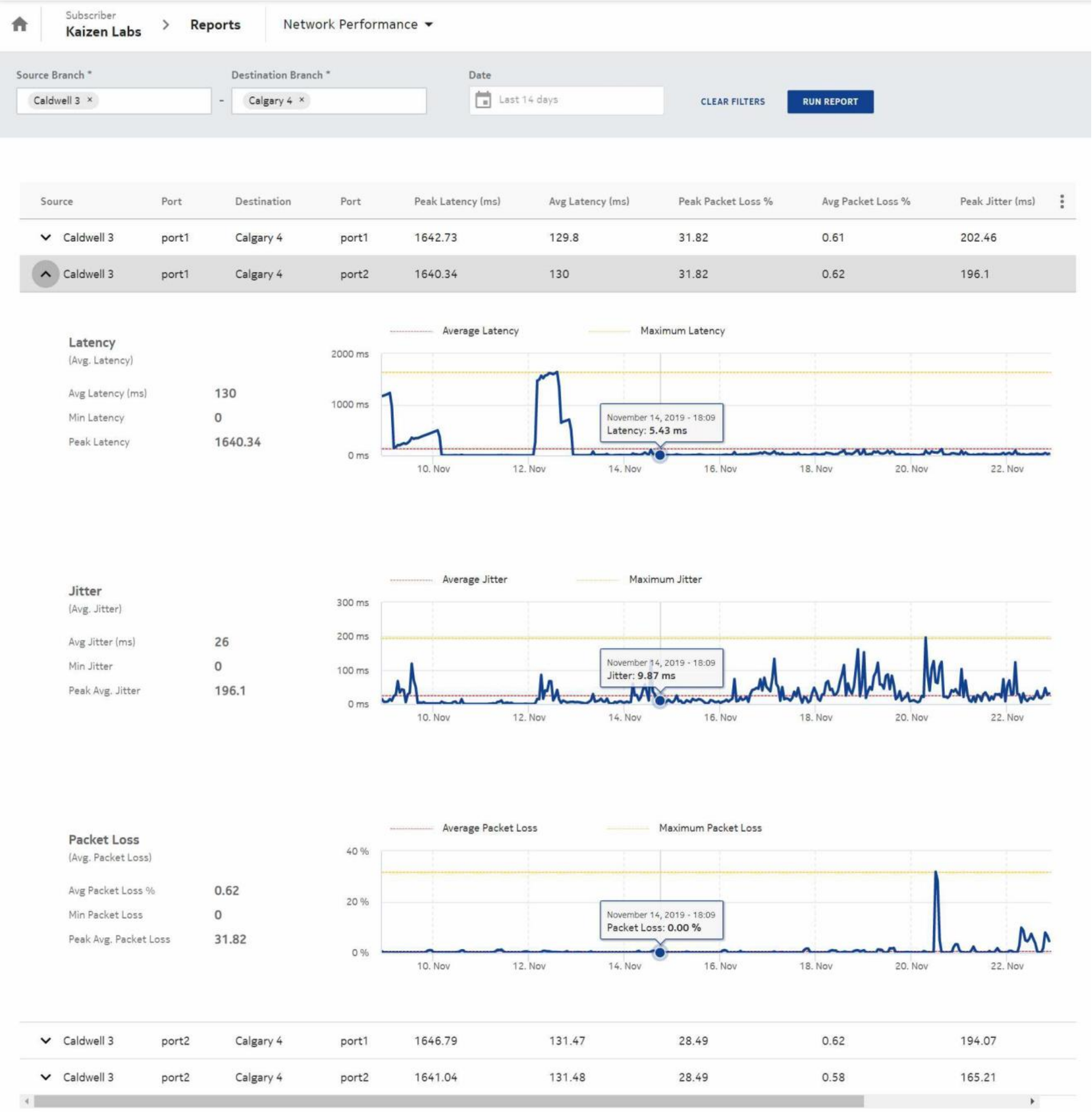
Click **RUN REPORT**.

The report displays a table indicating peak and average values of latency (ms), jitter (ms) and packet loss (%) for the reporting period, for each source and destination branch. It also depicts a graph with average and maximum latency, jitter and packet loss for the same period. The data in this report is not representative of the raw latency, jitter and packet loss values, but is instead averaged out over the time slices in the reporting period. For best accuracy, smaller reporting intervals should be used.

For details on the interval used when calculating the averages of latency, jitter and packet loss, refer to the data point information Chapter 14, “Reports.”

Click the pull-down arrow beside the branch name to view a graph of the average, minimum and peak threshold statistics of the Latency, Jitter and Packet Loss.

Figure 14-10 Sample Network Performance Report



Subscriber **Kaizen Labs** > **Reports** Network Performance ▾

Source Branch * Caldwell 3 × – Destination Branch * Calgary 4 × Date Last 14 days

Source	Port	Destination	Port	Peak Latency (ms)	Avg Latency (ms)	Peak Packet Loss %	Avg Packet Loss %	Peak Jitter (ms)
Caldwell 3	port1	Calgary 4	port1	1642.73	129.8	31.82	0.61	202.46
Caldwell 3	port1	Calgary 4	port2	1640.34	130	31.82	0.62	196.1
Caldwell 3	port2	Calgary 4	port1	1646.79	131.47	28.49	0.62	194.07
Caldwell 3	port2	Calgary 4	port2	1641.04	131.48	28.49	0.58	165.21

Latency
(Avg. Latency)

Avg Latency (ms)	130
Min Latency	0
Peak Latency	1640.34

November 14, 2019 - 18:09
Latency: **5.43 ms**

Jitter
(Avg. Jitter)

Avg Jitter (ms)	26
Min Jitter	0
Peak Avg. Jitter	196.1

November 14, 2019 - 18:09
Jitter: **9.87 ms**

Packet Loss
(Avg. Packet Loss)

Avg Packet Loss %	0.62
Min Packet Loss	0
Peak Avg. Packet Loss	31.82

November 14, 2019 - 18:09
Packet Loss: **0.00 %**

End of steps

9.10 Generating the Network Traffic Details Report

The View Network Traffic Details Report, View L3 Networks, View L2 Networks, and View Branches should be enabled for the user to view the network traffic details report. See also 15.9 "Adding or Editing a User Group" (p. 256) to enable View Network Traffic Details Report.

The Network Traffic Details Report provides volume and throughput usage for aggregate traffic for a selected network over a reporting period along with a full traffic breakdown against each virtual port (vPort) attached to the network.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Network Traffic Details Report**.

The Network Traffic Details Report page opens.

4

To generate the report for a specific period, configure the following parameters:

Parameter	Description
Network Type*	Select a L2 or L3 network type from the list. **Note**: If you have the permissions to view the L2 and L3 network, then by default, L3 network is selected. If you have either of the permissions, then only those network types are visible.
Network*	Enter text to search for a network. Select only one network at a time from the list. This option is enabled only if a network type is selected.
Connections	Enter text to search for a connection or select from the list. Up to 10 connections can be selected.
Duration	Click the calendar icon 📅 to open the calendar and select the start date, end date or range of time for the report. Alternatively, you can select one of the options – Last hour, Last 4 hours, Last 12 hours, Last 24 hours (default), Last 7 days or Last 14 days.

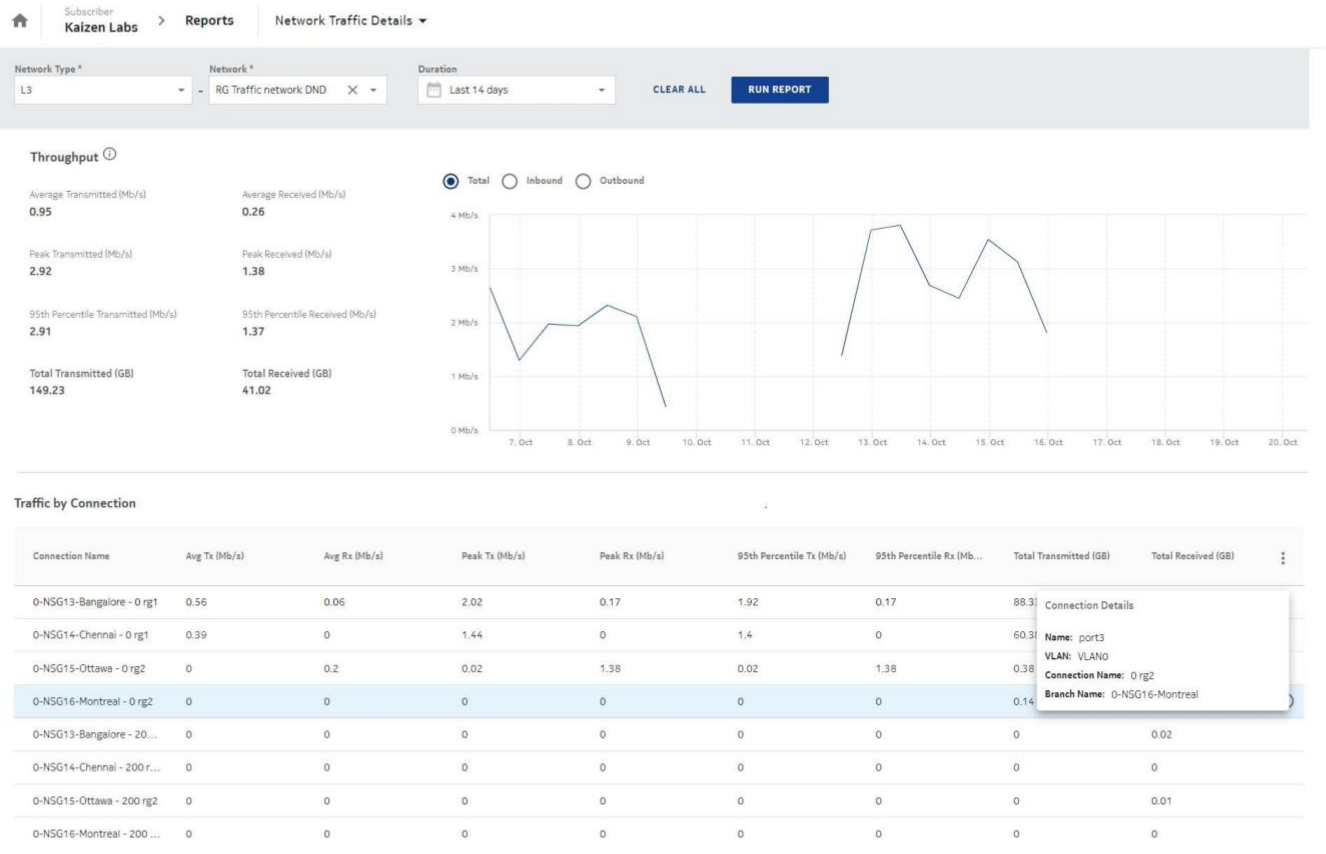
5

Click **RUN REPORT**.

A graphical representation of the network traffic details report displays with the following details:

Section	Description
Throughput	Displays the total throughput (total transmitted and total received) traffic of a branch for selected network(s). A line graph displays the traffic statistics of the network depending on the selected option: • Total: Displays the total traffic (inbound and outbound) for the selected networks. • Inbound: Displays the inbound traffic for the selected networks. • Outbound: Displays the outbound traffic for the selected networks. Hover over the graph to view date, time, network and data usage.
Traffic by Connection	A table displays the connection name, average transmitted/received, peak transmitted/received, 95th percentile transmitted/received, and total volume of traffic transmitted/received for each network's virtual port (vPort). The data provided in the **Connection Name** column is displayed in the format "Branch - vPort Name". To view additional details associated with a port, click the Connection Details icon ⓘ on the right corner of a particular row. The **Connection Details** popup panel opens as shown in the graphic below displaying the following details: • Name • VLAN • Connection Name • Branch Name

Figure 14-11 Sample Network Traffic Details Report



Network Type *: L3

Network *: RG Traffic network DND

Duration: Last 14 days

Throughput

Average Transmitted (Mb/s): 0.95

Average Received (Mb/s): 0.26

Peak Transmitted (Mb/s): 2.92

Peak Received (Mb/s): 1.38

95th Percentile Transmitted (Mb/s): 2.91

95th Percentile Received (Mb/s): 1.37

Total Transmitted (GB): 149.23

Total Received (GB): 41.02

Traffic by Connection

Connection Name	Avg Tx (Mb/s)	Avg Rx (Mb/s)	Peak Tx (Mb/s)	Peak Rx (Mb/s)	95th Percentile Tx (Mb/s)	95th Percentile Rx (Mb...	Total Transmitted (GB)	Total Received (GB)
0-NSG13-Bangalore - 0 rg1	0.56	0.06	2.02	0.17	1.92	0.17	88.3	
0-NSG14-Chennai - 0 rg1	0.39	0	1.44	0	1.4	0	60.3	
0-NSG15-Ottawa - 0 rg2	0	0.2	0.02	1.38	0.02	1.38	0.38	
0-NSG16-Montreal - 0 rg2	0	0	0	0	0	0	0.14	
0-NSG13-Bangalore - 20...	0	0	0	0	0	0	0	0.02
0-NSG14-Chennai - 200 r...	0	0	0	0	0	0	0	0
0-NSG15-Ottawa - 200 rg2	0	0	0	0	0	0	0	0.01
0-NSG16-Montreal - 200 ...	0	0	0	0	0	0	0	0

Connection Details

Name: port3

VLAN: VLAN0

Connection Name: 0 rg2

Branch Name: 0-NSG16-Montreal

End of steps

9.11 Generating the Network Security Policies Report

You can generate the Network Security Policies Report only if your customer profile and user group have View Network Security Policies Report enabled. The other related permissions to generate the report are:

- View L3 Networks
- View Outbound Security Policies
- View Outbound Security Policy Rules
- View Inbound Security Policies
- View Inbound Security Policy Rules

See also 15.9 “Adding or Editing a User Group” (p. 256) to enable Network Security Policies Report.

1

Navigate to your organization’s Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Network Security Policies**.

The Network Security Policies page opens.

4

To generate the report, configure the following parameters:

Parameter	Description
L3 Network*	Select an L3 network from the list.
Policy Type	Select **Inbound Security** or **Outbound Security** from the list.
Rule Traffic Action	By default, it is set to **Drop**. When the Allow or Drop selection is cleared, the option **ALL** is available to the user. **Note**: Option **ALL** includes **Allow**, **Drop** and **Transparent** traffic actions.
Duration	Click the calendar icon 📅 to open the calendar and select the start date and end date, or the time range for the report. Alternatively, you can select one of the options: • Last hour • Last 4 hours • Last 12 hours • Last 24 hours (default) • Last 7 days • Last 14 days

5

Click **RUN REPORT**.

The table can display a maximum of 100 policies. The report displays a table listing the Priority, Status, Policy Name, Forward all IP Traffic, Forward all Non IP Traffic and Allow Source Address Spoofing/Install Implicit rules (based on the policy type selected).

Enter a search term or select an option from the list to filter the policies.

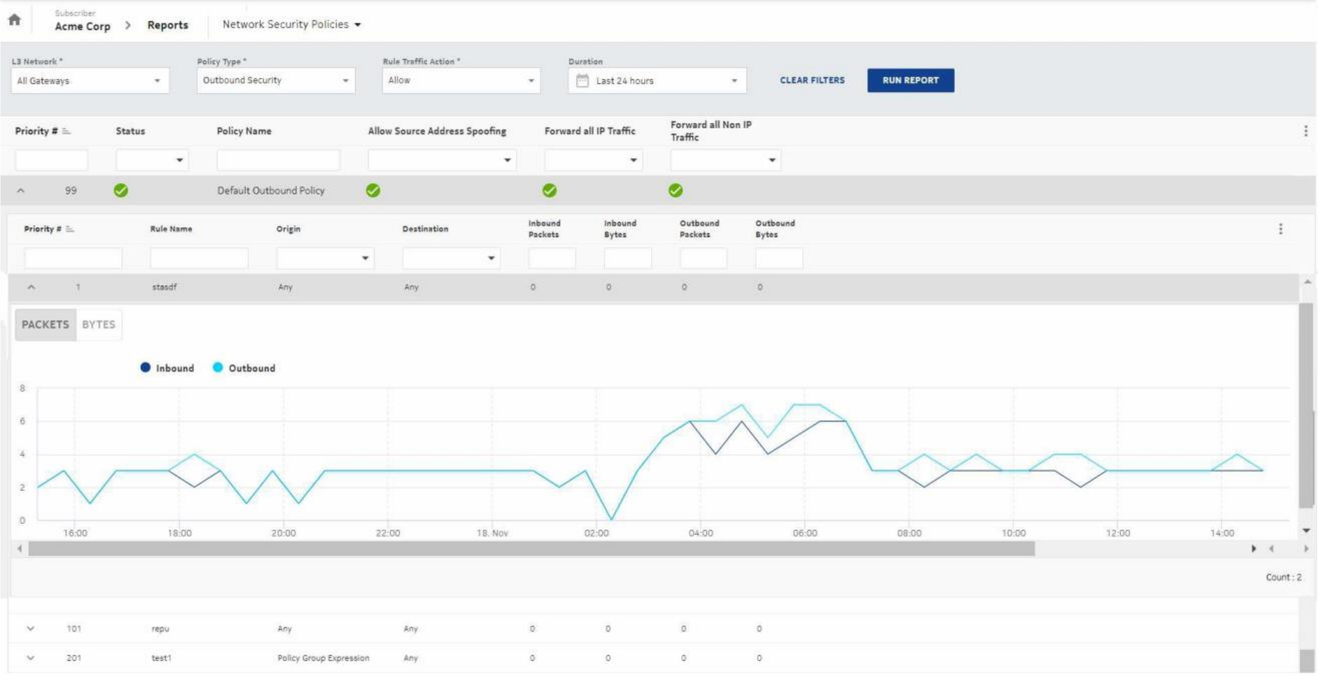
Select a policy. Click the down arrow icon ⌄ to view the rules for the selected policy. The table can display maximum of 200 rules and this is configurable in Platform Settings (Maximum Number Of Rules Per Policy For Network Security Policies Report). By default, the table lists Priority, Rule Name, Origin, Destination, Inbound Packets, Inbound Volume (Bytes), Outbound Packets and Outbound Volume (Bytes). Additionally, the user can include the Application Aware, Stateful, Web Filter and Protocol columns.

Enter a search term or select a rule and click on the down arrow icon ⌄ again to see the inbound and outbound packets and the bytes volume.

Note: Click the down arrow to view multiple policies and rules at the same time.

Click **PACKETS** or **BYTES** to view the inbound and outbound traffic for the selected rule.

Figure 14-12 Sample Network Security Policies Report



Subscriber
Acme Corp > Reports | Network Security Policies ▾

L3 Network *: All Gateways
Policy Type *: Outbound Security
Rule Traffic Action *: Allow
Duration: Last 24 hours

CLEAR FILTERS | RUN REPORT

	Priority #	Status	Policy Name	Allow Source Address Spoofing	Forward all IP Traffic	Forward all Non IP Traffic
^	99	✓	Default Outbound Policy	✓	✓	✓

	Priority #	Rule Name	Origin	Destination	Inbound Packets	Inbound Bytes	Outbound Packets	Outbound Bytes
^	1	stasdf	Any	Any	0	0	0	0
⌄	101	repu	Any	Any	0	0	0	0
⌄	201	test1	Policy Group Expression	Any	0	0	0	0

Count : 2

End of steps

9.12 Generating the Top Talkers Report

The View Top Talkers Report, View Branches, View L3 Networks and View L2 Networks permissions should be enabled for the user to view the Top Talkers report. This report displays the bar graph of the top host IP addresses and their source branches consuming total volume for inbound and outbound traffic. See also 15.9 “Adding or Editing a User Group” (p. 256) to enable Top Talkers Report.

1

Navigate to your organization's Dashboard. See 8.4 "Viewing the Subscriber Organization Dashboard" (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **Top Talkers**.

The Top Talkers page opens.

4

To generate the report, configure the following parameters:

Parameter	Description
Traffic Direction*	Select Inbound or Outbound from the list.
Source IP	Enter text to search for a specific source IP address. Select an IP address from the list.
Network Type	Select All (by default) or select L2 or L3 network type from the list.
Network	Select All (by default) to include all networks in the report or enter text to search for a specific network. Select one network from the list.
Source Branch	Select All (by default) to include all branches in the report or enter text to search for a specific branch. Select one branch from the list. Select a source branch from the list.
Application Type	Select an option from the list. The following options are available: • Discovered Applications: Displays traffic data for the default application groups. • Custom Applications: Displays traffic data for user-defined application groups. **Note**: Select a network to enable a custom application.

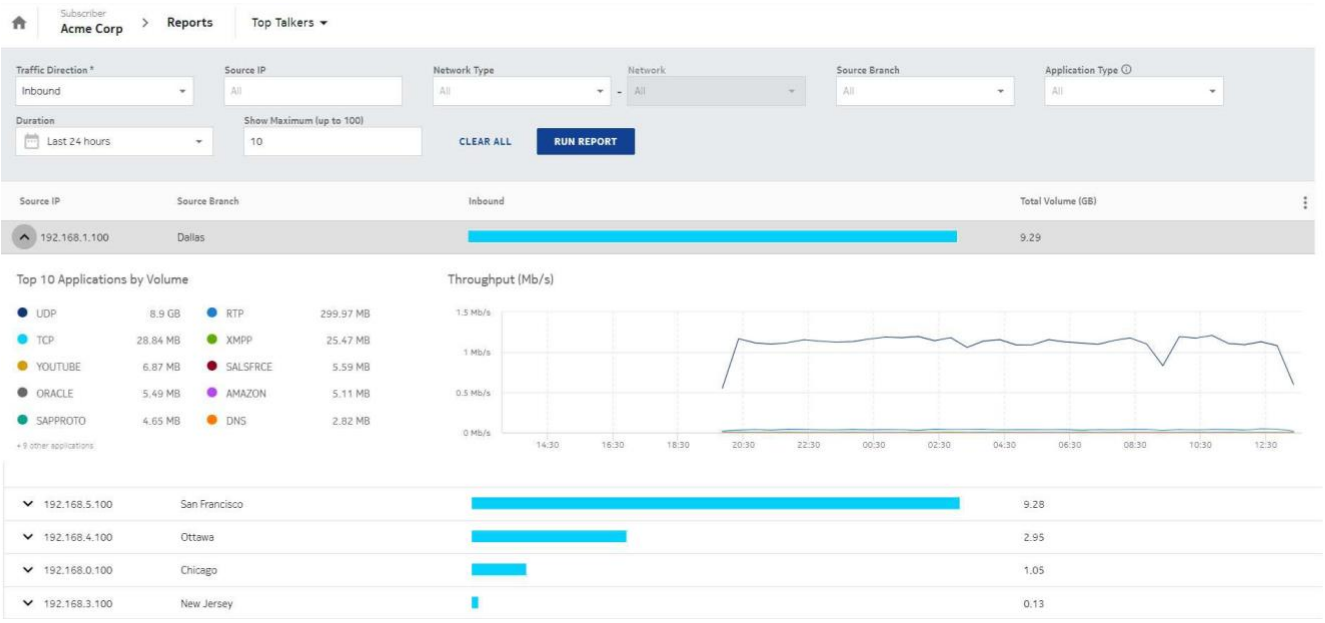
Parameter	Description
Duration	Click the calendar icon 📅 to open the calendar and select the start date and end date, or the time range for the report. Alternatively, you can select one of the options: • Last hour • Last 4 hours • Last 12 hours • Last 24 hours (default) • Last 7 days • Last 14 days
Show Maximum (up to 100)	Enter the number of application top talkers to be displayed.

5

Click **RUN REPORT**.

The report displays a table listing the maximum number of host IP addresses specified and a corresponding bar graph of inbound and outbound and the total volume consumed by the associated source branch. Hover over the bar graph to view the volume of inbound and outbound. Click the pull-down arrow to view the list of top 10 applications of the source branch and a corresponding line graph of the total, inbound or outbound throughput traffic.

Figure 14-13 Sample Top Talkers



Subscriber Acme Corp > Reports Top Talkers ▾

Traffic Direction * : Inbound
Source IP: All
Network Type: All - Network: All
Source Branch: All
Application Type ⓘ: All
Duration: Last 24 hours
Show Maximum (up to 100): 10

Source IP	Source Branch	Inbound	Total Volume (GB)
192.168.1.100	Dallas		9.29
192.168.5.100	San Francisco		9.28
192.168.4.100	Ottawa		2.95
192.168.0.100	Chicago		1.05
192.168.3.100	New Jersey		0.13

Top 10 Applications by Volume

● UDP	8.9 GB	● RTP	299.97 MB
● TCP	28.84 MB	● XMPP	25.47 MB
● YOUTUBE	6.87 MB	● SALSFRCE	5.59 MB
● ORACLE	5.49 MB	● AMAZON	5.11 MB
● SAPPROTO	4.65 MB	● DNS	2.82 MB

+ 9 other applications

End of steps

9.13 Generating the QoS Statistics Report

The View QoS Statistics Reports, View Branches, View Branch Network Port, View Branch Access Port, View Egress QoS Policies, View Branch WiFi Port, View Branch LAN Egress QoS Policy, View Branch WAN Egress QoS Policy, View VLANs, and View SSIDs should be enabled for the user to view the QoS Statistics report. See also 15.9 “Adding or Editing a User Group” (p. 256) to enable QoS Statistics Report.

1

Navigate to your organization's Dashboard. See 8.4 “Viewing the Subscriber Organization Dashboard” (p. 45).

2

From the dashboard-level menu, click **Reports**.

The reports page is displayed.

3

Click **QoS Statistics**.

The QoS Statistics page opens.

4

To generate the report, configure the following parameters:

Parameter	Description
Source Branch	Select a source branch from the list. **Note**: Only NSGs are supported.
Port*	Select a port from the list. Select a branch to enable this option.
VLAN*	Search for a VLAN from the list. Select a port to enable this option.

Parameter	Description
Queue	Select All (by default) to include all queues in the report or select one of the following options: • Q1 (Strict Priority) • Q2 (Weighted Round Robin) • Q3 (Weighted Round Robin) • Q4 (Weighted Round Robin) • Network Control Queue • Management Queue • Parent Queue **Note**: The Queue names are hard coded in the platform policy engine and cannot be created in the SD-WAN Portal. All queues are applicable for WAN ports. Network Control Queue and Management Queue options are not available for LAN ports.

Duration	Click the calendar icon 📅 to open the calendar and select the start date and end date, or the time range for the report. Alternatively, you can select one of the options: • Last hour • Last 4 hours • Last 12 hours • Last 24 hours (default) • Last 7 days • Last 14 days

5

Click **Run Report**.

The QoS Statistics report is generated for Volume (Packets), Volume (Bytes), and Bandwidth. The statistics are collected for Bytes (total number of bytes from the Queue), Packet Count (total number of packets egressing from the queue) and Inbound Dropped (total number of packets dropped from a queue after exceeding the configured rate limits).

Click QoS Details to view the details of QoS attached to the selected VLAN.

When the Volume (Packets) is selected, it displays three graphs for Total Volume, Per Queue Egress Statistics- Forwarded and Per Queue Egress Statistics- Dropped. The Total Volume displays the Inbound, Inbound Dropped and Inbound Errors in the graph while the Per Queue Egress Statistics displays the forwarded and dropped graphs for the selected Queues.

When the Volume (Bytes) tab is selected, it displays two graphs for Total Volume and Per Queue Egress Statistics. The Total Volume displays the statistics for Inbound and Outbound, and Per Queue Egress Statistics displays the graph for counts per selected queue and the QoS details.

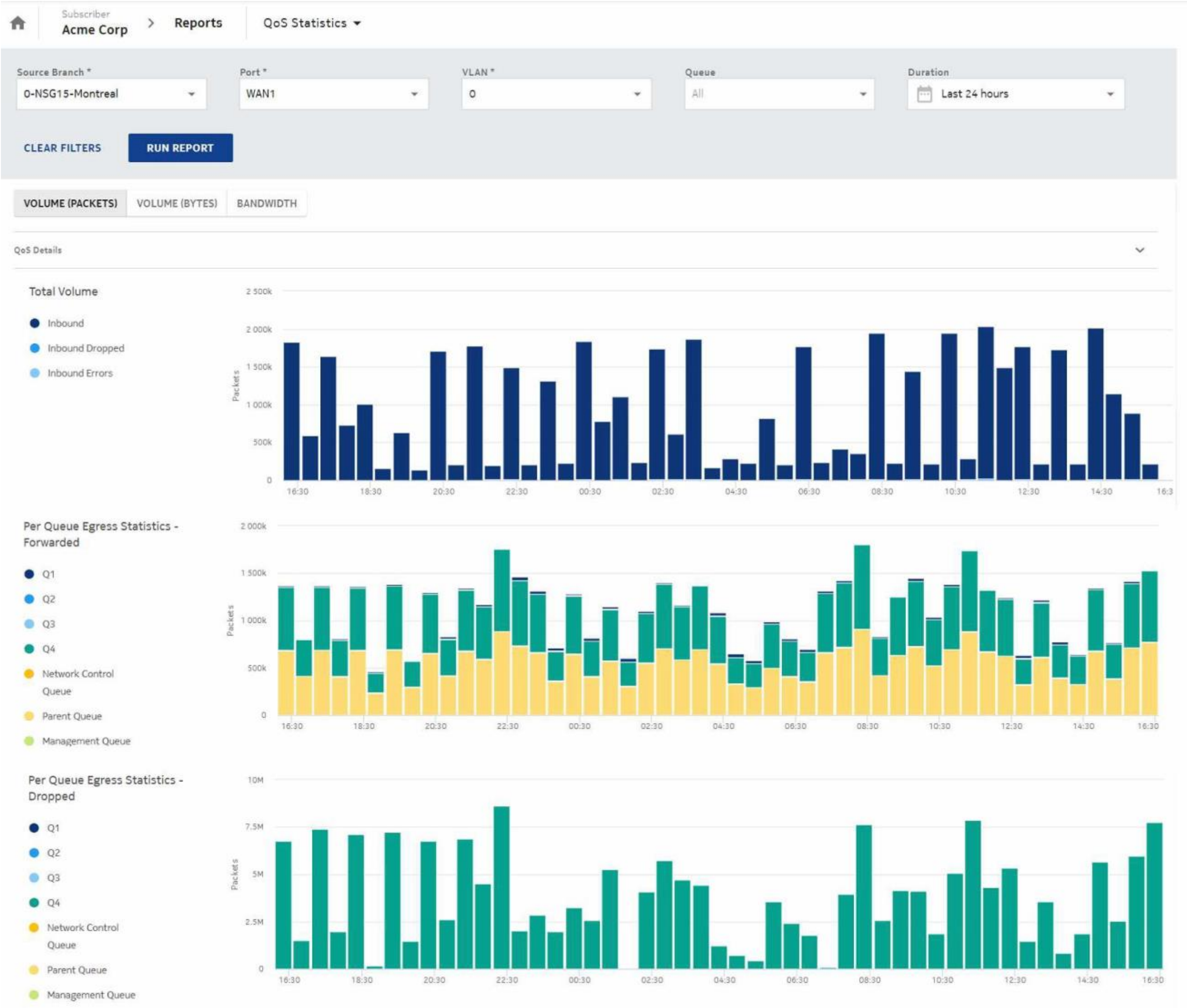
When Bandwidth is selected, it displays graphs for the data flow for the each of the selected Queues.

ℹ **Note**: Graph legend changes depending on the kind of port selected. If a WAN port is selected, the legend indicates that the statistics are for outbound, and if a LAN port is selected, the graph legend indicates that the statistics are for inbound. The network traffic details are displayed only for the LAN ports.

ℹ **Note**: When there are values with extremes in any graphs, lower extreme values may not be shown in the report due to the limitation in pie charts. For example, if any graph is scaled to GB and few values are in Bytes, such values may not be plotted in graphs.

End of steps

Figure 14-14 Sample QoS Statistics Report



Subscriber
Acme Corp > Reports | QoS Statistics

Source Branch *: 0-NSG15-Montreal

Port *: WAN1

VLAN *: 0

Queue: All

Duration: Last 24 hours

10 Managing Users and Groups

10.1 User Management Overview

The user management feature in the SD-WAN Portal handles both the authentication (identifying a user) and authorization (determining what the user can do or access within the SD-WAN Portal), as well as providing the ability to organize users into functional groups or organizations which share common attributes.

Note:

- The Admin user of a reseller or subscriber organization cannot be deleted.
- The Admin user group of a reseller or subscriber organization cannot be edited or deleted.

10.2 Viewing Users

If	Then
If you are logged in as a reseller organization user and want to manage users for the reseller organization	From the organization-level menu, click **Users**. The Users tab is selected by default and displays the list of the reseller organization's users.
If you are logged in as a reseller organization user and want to manage users for a subscriber organization managed by the reseller	Perform the following steps: 1. In the Organizations page, double-click a subscriber organization. 2. From the organization-level menu, click **Users**. The Users tab is selected by default and displays the users of the selected subscriber organization.
If you are logged in as a subscriber organization user	From the organization-level menu, click **Users**. The Users tab is selected by default and displays the users of the selected subscriber organization.

10.3 Adding or Editing a User

1

Open the Users page. See 15.2 "Viewing Users" (p. 253).

2

Perform any of the following actions:

- Click the **Add User** icon ⊕ to add a user.
  The **Add User** window opens.
- Select the user you want to modify and click the **Edit** icon ✎ to edit an existing user.
  The **Edit User** window opens.

3

Configure the following parameters:

Parameter	Description
First Name*	Enter the first name of the user.
Last Name*	Enter the last name of the user.
Email Address*	Enter the email ID of the user.
Primary Phone*	Enter the phone number of the user.
Mobile Phone	Enter the mobile number of the user.
Username*	Enter a username.
Language*	Select a preferred language from the language list.

4

Click **OK**.

Upon adding the new user, a “New Account” email is sent to the user’s registered email ID with a link to set your password. The password must be set before you can log in.

If a new user is added to an organization, the FQDN and logo of the organization will be included in the email for password reset. If the organization is a subscriber organization, its parent organization’s FQDN and logo will be included.

End of steps

10.4 Resetting a User's Password

1

Open the Users page. See 15.2 “Viewing Users” (p. 253).

2

Select a user and click the ellipsis icon ⋮ and select **Reset Password** icon 🔑 to reset a user password.

The Reset Password window opens.

3

Click **RESET**.

The user receives an email in the registered email ID with a link to reset the password. The user can click the link to reset the password.

End of steps

10.5 Locking a User Account

Note: Users cannot lock or unlock themselves.

1

Open the Users page. See 15.2 “Viewing Users” (p. 253).

2

Select a user and click the ellipsis icon ⋮ and select **Lock** icon 🔒 to lock the user's account.

The **Lock Account** window opens.

Select the check box to send a notification email in the registered email ID to the user.

You can also provide the reason for locking or unlocking the user account in the text box.

3

Click **OK**.

END OF STEPS

When the user account is locked, a lock icon 🔒 appears beside the user account.

10.6 Unlocking a User Account

Note: Users cannot lock or unlock themselves.

1

Open the Users page. See 15.2 “Viewing Users” (p. 253).

2

Select a user and click the ellipsis icon ⋮ and select **Unlock** icon 🔓 to unlock the user's account.

The **Unlock Account** window opens.

Select the check box to send a notification email in the registered email ID to the user.

You can also provide the reason for unlocking the user account in the text box.

The admin cannot reset the password for a user account which is locked.

3

Click **OK**.

End of steps

10.7 Deleting a User

Open the Users page. Se 15.2 “Viewing Users” (p. 253).

2

Select a user and click the ellipsis icon and click the **Delete** icon 🗑 to delete the user.

The Delete User window opens.

3

Click **OK**.

End of steps

10.8 Viewing User Groups

If	Then
If you are logged in as a reseller organization user and want to add or edit a user group for the reseller organization	1. From the organization-level menu, click **Users**. 2. Select **User Groups** in the left pane. A list of user groups of the reseller organization is displayed.
If you are logged in as a reseller organization user and want to add or edit a user group for a subscriber organization managed by the reseller	Perform the following steps: 1. In the Organizations page, double-click the subscriber organization for which you want to add or edit a user group. 2. From the organization-level menu, click **Users**. 3. Select **User Groups** in the left pane. A list of user groups of the subscriber organization is displayed.
If you are logged in as a subscriber organization user	1. From the organization-level menu, click **Users**. 2. Select **User Groups** in the left pane. A list of user groups of the subscriber organization is displayed.

10.9 Adding or Editing a User Group

1

Open the User Groups page. See 15.8 “Viewing User Groups” (p. 256).

2

Perform any of the following actions:

- Click the **Add User Group** icon ⊕ to add a user group.

  The **Add User Group** window opens.
- Select the user group you want to modify and click the **Edit** icon ✎ to edit an existing user group.

The **Edit User Group** window opens.

3

Enter the **User Group Name*** and set the group permissions.

The table in Table 15-1, “User Group Permissions” (p. 256) describes the roles associated with the permission categories. The roles in this table are only visible for selection if the license for that feature is included in the Customer Profile Manager settings.

4

Click **OK**.

End of steps

10.10 User Group Permissions

Table 15-1 User Group Permissions

Permission	Description	Applicability
Nokia Cloud Managed SD-WAN Platform		
View Branch Packages**	Enable users to view branch packages.	All Organizations
View Speed Tiers**	Enable users to view speed tiers.	All Organizations
Branch Packages		
View Branch Package Assignments**	Enable users to view branch package assignments.	Reseller only
Update Branch Package Assignments	Enable users to update branch package assignments.	Reseller only
Speed Tiers		
View Speed Tier Assignments**	Enable users to view speed tier assignments.	Reseller only
Update Speed Tier Assignments	Enable users to update speed tier assignments.	Reseller only
Manage Subscribers		
View Subscriber Organizations**	Enable users to view the subscriber organization.	All Organizations
View Subscriber Dashboard**	Enable users to view the subscriber dashboard.	All Organizations
Create Subscriber Organizations	Enable users to create subscriber organizations.	Reseller only
Update Subscriber Organizations	Enable users to edit subscriber organizations.	Reseller only
Update Subscriber Organization Names	Enable users to edit the subscriber organization’s name.	Reseller only
Delete Subscriber Organization	Enable users to delete subscriber organizations.	Reseller only
View Customer Profile	Enable users to view assigned customer profile.	All Organizations
View NSG Templates	Enable users to view assigned NSG templates.	All Organizations
View Egress QoS Policies	Enable users to view egress QoS policies assigned to the subscriber organizations.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
View Underlay Tags	Enable users to view underlay tags assigned to the subscriber organizations.	All Organizations
View Diagnostics Tests	Enable users to view diagnostics tests.	All Organizations
View Assigned Organization Profile	Enable users to view assigned organization profiles.	Reseller only
Users		
View Users** View User Groups**	Enable users to view the users and user groups.	All Organizations
Create Users	Enable users to create other users.	All Organizations
Update Users	Enable users to edit users.	All Organizations
Delete Users	Enable users to delete users.	All Organizations
Create User Groups	Enable users to create user groups.	All Organizations
Update User Groups	Enable users to edit user groups.	All Organizations
Delete User Groups	Enable users to delete user groups.	All Organizations
Assign User Groups	Enable users to assign user groups to a user.	All Organizations
Branches		
View Branches**	Enable users to view the branches.	All Organizations
View Branch Dashboard	Enable users to view and configure branch dashboard.	All Organizations
Create Branch	Enable users to create branches. Related permissions are: • View NSG Templates • View Users	All Organizations
Update Branch	Enable users to edit branches. Related permissions are: • View NSG Templates • View Users	All Organizations
Delete Branch	Enable users to delete branches.	All Organizations
Update Branch Network Acceleration	Enables users to edit branch network acceleration. Related permissions are: • Create Branch • Update Branch	All Organizations
View Branch Alarms	Enable users to view branch alarms.	All Organizations
View Redundancy Groups	Enables users to view redundancy groups.	All Organizations
Uplink Ports		

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
View Branch Uplink**	Enable users to view branch uplink. Related permissions are: • View Egress QoS Policies • View L3 Networks • View L2 Networks • View L3 Network Application Groups • View L2 Network Application Groups • View VLANs • View Applications • View Branch WAN Egress QoS Policy • View Underlay Tags	All Organizations
View Branch Network Port**	Enable users to view branch network port.	All Organizations
Edit Branch Uplink	Enable users to edit and manage branch uplink.	All Organizations
Edit Branch Network Port	Enable users to edit and manage branch network port. Related permissions are: • View Egress QoS Policies • View Underlay Tags	All Organizations
View PAT NAT Pools	Enable users to view a PAT NAT pool.	All Organizations
View Branch WAN Egress QoS Policy	Enable users to view branch WAN egress QoS policy.	All Organizations
Branch Device Management		
Deactivate Device	Enable users to deactivate the device. The related permission is Update Branch.	All Organizations
Reboot Device	Enable users to reboot the device. The related permission is Update Branch.	All Organizations
Reload Configuration for Device	Enable users to reload the configuration for the device. The related permission is Update Branch.	All Organizations
Quarantine Device	Enable users to Quarantine the device. The related permission is Update Branch.	All Organizations
Lift Quarantine for Device	Enable users to lift quarantine for a device. The related permission is Update Branch.	All Organizations
Access Ports		
View Branch Access Port**	Enable users to view branch access port.	All Organizations
View VLANs**	Enable users to view the VLANs.	All Organizations
Edit Branch Access Port	Enable users to edit and manage branch access port.	All Organizations
Create VLANs	Enable users to create a new VLAN.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Update VLANs	Enable users to edit a VLAN. Related permissions are: • View Egress QOS Policies • View Underlay Tags	All Organizations
Delete VLANs	Enable users to delete a VLAN.	All Organizations
Link Branch To a Network	Enable users to link a branch to a network. Related permissions are: • View L3 Networks • View L2 Networks	All Organizations
View Branch LAN Egress QOS Policy	Enable users to view branch LAN egress QOS policy.	All Organizations
WiFi Ports		
View Branch WiFi Port**	Enable users to view branch WiFi port.	All Organizations
View SSIDs**	Enable users to view SSIDs.	All Organizations
View Captive Portal Profiles**	Enable users to view captive portal profiles.	All Organizations
Create Branch WiFi Port	Enable users to create a new branch wifi port.	All Organizations
Edit Branch WiFi Port	Enable users to edit and manage branch wifi port.	All Organizations
Delete Branch WiFi Port	Enable users to delete branch wifi port.	All Organizations
Create SSIDs	Enable users to create a new SSID.	All Organizations
Edit SSIDs	Enable users to edit and manage SSIDs. Related permissions are: • View Egress QoS Policies • View Underlay Tags	All Organizations
Delete SSIDs	Enable users to delete SSIDs.	All Organizations
Create Captive Portal Profiles	Enable users to create a new captive portal profile.	All Organizations
Edit Captive Portal Profiles	Enable users to edit and manage captive portal profiles.	All Organizations
Delete Captive Portal Profiles	Enable users to delete captive portal profiles.	All Organizations
L3 Networks		
View L3 Networks**	Enable users to view L3 networks in the drop-down list.	All Organizations
Create L3 Networks	Enable users to create L3 Networks and define zones and subnets	All Organizations
Update L3 Networks	Enable users to update an existing L3 network name and description.	All Organizations
Delete L3 Networks	Enable users to delete L3 networks.	All Organizations
View L3 Network Application Groups	Enable users to view L3 network application groups.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Edit L3 Network Application Groups	Enable users to edit L3 network application groups. The related permission is View Application Group.	All Organizations
View L3 Static Routes	Enable users to view static routes assigned to L3 networks.	All Organizations
Update L3 Static Routes	Enable users to update static routes assigned to L3 networks.	All Organizations
View L3 Network Performance Monitor Groups	Enable users to view L3 network performance monitor groups.	All Organizations
View L3 Network DHCP Options	Enable users to view DHCP options of an L3 network.	All Organizations
Update L3 Network Performance Monitor Groups	Enable users to update performance monitor groups assigned to L3 networks.	All Organizations
Update L3 Network DHCP Options	Enable users to update DHCP options of an L3 network.	All Organizations
View L3 Network QoS	Enable users to view L3 network QoS policies.	All Organizations
Update L3 Network QoS	Enable users to update L3 network QoS policies.	All Organizations
L3 Zones		
View L3 Zone**	Enable users to view the list of zones defined under an L3 network.	All Organizations
Create L3 Zone	Enable users to create a zone under an L3 network.	All Organizations
Update L3 Zone	Enable users to edit an existing L3 zone name and description.	All Organizations
Delete L3 Zone	Enable users to delete L3 zones.	All Organizations
View L3 Zone DHCP Options	Enable users to view DHCP options of an L3 network zone.	All Organizations
Update L3 Zone DHCP Options	Enable users to update DHCP options of an L3 network zone.	All Organizations
View L3 Zone QoS	Enable users to view L3 Zone QoS policies.	All Organizations
Update L3 Zone QoS	Enable users to update L3 Zone QoS policies.	All Organizations
L3 Subnets		
View L3 Subnet**	Enable users to view the list of subnets defined under an L3 zone.	All Organizations
Create L3 Subnet	Enable users to create a subnet under an L3 zone.	All Organizations
Update L3 Subnet	Enable users to edit an existing L3 subnet name, description, and gateway IP address.	All Organizations
Delete L3 Subnet	Enable users to delete L3 subnets.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Link Network to a Branch	Enable users to link an L3 network to a branch. Related permissions are: • View VLANs • Create VLANs • View Branch Access Port	All Organizations
View Subnet Address Range	Enable users to view address range of a subnet.	All Organizations
Delete Subnet Address Range	Enable users to delete address range of a subnet.	All Organizations
View Subnet Address Assignment	Enable users to view address assignment of a subnet.	All Organizations
Update Subnet Address Assignment	Enable users to update address assignment of a subnet.	All Organizations
View BGP Neighbor	Enable users to view BGP neighbors. The related permission is View Routing Policies.	All Organizations
Update BGP Neighbor	Enable users to update BGP neighbors. The related permission is View Routing Policies.	All Organizations
View L3 Subnet DHCP Options	Enable users to view DHCP options of an L3 network subnet.	All Organizations
Update L3 Subnet DHCP Options	Enable users to update DHCP options of an L3 network subnet.	All Organizations
View L3 Subnet QoS	Enable users to view L3 subnet QoS policy.	All Organizations
Update L3 Subnet QoS	Enable users to update L3 subnet QoS policy.	All Organizations
Routing Policies		
View Routing Policies	Enable users to view routing policies.	All Organizations
Create Routing Policies	Enable users to create routing policies.	All Organizations
Update Routing Policies	Enable users to update routing policies.	All Organizations
Delete Routing Policies	Enable users to delete routing policies.	All Organizations
L2 Networks		
View L2 Networks**	Enable users to view L2 networks in the drop-down list.	All Organizations
Create L2 Networks	Enable users to create L2 networks.	All Organizations
Update L2 Networks	Enable users to update L2 networks.	All Organizations
Delete L2 Networks	Enable users to delete L2 networks.	All Organizations
Link L2 Network to a Branch	Enable users to link L2 network to a branch. Related permissions are: • View VLANs • Create VLANs • View Branch Access Port	All Organizations

Permission	Description	Applicability
View L2 Network QoS	Enable users to view L2 network QoS policies.	All Organizations
Update L2 Network QoS	Enable users to update L2 network QoS policies.	All Organizations
View L2 Network Application Groups	Enable users to view L2 network application groups.	All Organizations
Policies		
View Policy Groups**	Enable users to view policy groups of an L3 network.	All Organizations
View Web Categories**	Enable users to view web categories.	All Organizations
View Web Domains**	Enable users to view web domains.	All Organizations
View Network Macros**	Enable users to view network macros.	All Organizations
View Network Macro Groups**	Enable users to view network macro groups.	All Organizations
View Breakout Options**	Enable users to view the breakout options.	All Organizations
View Breakout Entries**	Enable users to view the breakout entries.	All Organizations
View Uplink Preference Settings	Enable users to view uplink preference settings. Related permissions are: • View Outbound Forwarding Policies • View Outbound Forwarding Policy Rules	All Organizations
Update Uplink Preference Settings	Enable users to update uplink preference settings. Related permissions are: • View Outbound Forwarding Policies • View Outbound Forwarding Policy Rules	All Organizations
Policy Groups		
Create Policy Groups	Enable users to create policy groups for L3 networks.	All Organizations
Update Policy Groups	Enable users to edit policy groups.	All Organizations
Delete Policy Groups	Enable users to delete policy groups.	All Organizations
Web Categories and Web Domains		
Create Web Categories	Enable users to create web categories.	All Organizations
Update Web Categories	Enable users to update web categories.	All Organizations
Delete Web Categories	Enable users to delete web categories.	All Organizations
Create Web Domains	Enable users to create web domains.	All Organizations
Update Web Domains	Enable users to update web domains.	All Organizations
Delete Web Domains	Enable users to delete web domains.	All Organizations
Network Macros and Macro Groups		
Create Network Macros	Enable users to create network macros.	All Organizations
Update Network Macros	Enable users to update network macros.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Delete Network Macros	Enable users to delete network macros.	All Organizations
Create Network Macro Groups	Enable users to create network macro groups.	All Organizations
Update Network Macro Groups	Enable users to update network macro groups.	All Organizations
Delete Network Macro Groups	Enable users to delete network macro groups.	All Organizations
Breakout Options and Entries		
Create Breakout Options	Enable users to create breakout options.	All Organizations
Update Breakout Options	Enable users to update breakout options.	All Organizations
Delete Breakout Options	Enable users to delete breakout options.	All Organizations
Create Breakout Entries	Enable users to create breakout entries.	All Organizations
Update Breakout Entries	Enable users to update breakout entries.	All Organizations
Delete Breakout Entries	Enable users to delete breakout entries.	All Organizations
Outbound Security Policies		
View Outbound Security Policies**	Enable users to view outbound security policies listed under an L3 network.	All Organizations
View Outbound Security Policy Rules**	Enable users to view the rules of an outbound security policy. Related permissions are: • View Application Signatures • View SaaS Applications	All Organizations
Create Outbound Security Policies	Enable users to create outbound security policies.	All Organizations
Update Outbound Security Policies	Enable users to update outbound security policies.	All Organizations
Delete Outbound Security Policies	Enable users to delete outbound security policies.	All Organizations
Create Outbound Security Policy Rules	Enable users to create the rules for an outbound security policy. Related permissions are: • View Application Signatures • View SaaS Applications	All Organizations
Update Outbound Security Policy Rules	Enable users to update rules of an outbound security policy. Related permissions are: • View Application Signatures • View SaaS Applications	All Organizations
Delete Outbound Security Policy Rules	Enable users to delete rules of an outbound security policy.	All Organizations
Inbound Security Policies		

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
View Inbound Security Policies**	Enable users to view inbound security policies listed under an L3 network.	All Organizations
View Inbound Security Policy Rules**	Enable users to view the rules of an inbound security policy. The related permission is View Application Signatures.	All Organizations
Create Inbound Security Policies	Enable users to create inbound security policies.	All Organizations
Update Inbound Security Policies	Enable users to update inbound security policies.	All Organizations
Delete Inbound Security Policies	Enable users to delete inbound security policies.	All Organizations
Create Inbound Security Policy Rules	Enable users to create rules for an inbound security policy. Related permission is View Application Signatures.	All Organizations
Update Inbound Security Policy Rules	Enable users to update rules of an inbound security policy. Related permission is View Application Signatures.	All Organizations
Delete Inbound Security Policy Rules	Enable users to delete rules of an inbound security policy.	All Organizations
Outbound Forward Policies		
View Outbound Forwarding Policies**	Enable users to view outbound forwarding policies. The related permission is View L3 Network Application Groups.	All Organizations
View Outbound Forwarding Policy Rules**	Enable users to view outbound forwarding policy rules. Related permissions are: • View L3 Network Application Groups • View Applications	All Organizations
Create Outbound Forwarding Policies	Enable users to create outbound forwarding policies. Related permission is View L3 Network Application Groups.	All Organizations
Update Outbound Forwarding Policies	Enable users to update outbound forwarding policies. Related permission is View L3 Network Application Groups.	All Organizations
Delete Outbound Forwarding Policies	Enable users to delete outbound forwarding policies.	All Organizations
Create Outbound Forwarding Policy Rules	Enable users to create outbound forwarding policy rules. Related permissions are: • View L3 Network Application Groups • View Applications • View SaaS Applications	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Update Outbound Forwarding Policy Rules	Enable users to update outbound forwarding policy rules. Related permissions are: • View L3 Network Application Groups • View Applications • View SaaS Applications	All Organizations
Delete Outbound Forwarding Policy Rules	Enable users to delete outbound forwarding policy rules.	All Organizations
Application Discovery		
View Application Discovery Settings**	Enable users to view application discovery settings.	All Organizations
View Application Signatures**	Enable users to view application signatures.	All Organizations
Application Performance Management		
View Application Groups**	Enable users to view application groups.	All Organizations
View Applications**	Enable users to view applications.	All Organizations
Create Application Groups	Enable users to create application groups.	All Organizations
Update Application Groups	Enable users to update application groups.	All Organizations
Delete Application Groups	Enable users to delete application groups.	All Organizations
Enable Application Group Performance	Enable users to enable application group performance. Related permissions are: • Create Application Groups • Update Application Groups	All Organizations
Edit Application Group Advance Settings	Enable users to edit application group advance settings. The related permission is Enable Application Group Performance.	All Organizations
Edit Application Group Service Class	Enable users to edit application group service class. The related permission is Enable Application Group Advance Settings.	All Organizations
Update Links between Applications and Groups	Enable users to update links between applications and groups.	All Organizations
Create Applications	Enable users to create applications.	All Organizations
Update Applications	Enable users to update applications.	All Organizations
Delete Applications	Enable users to delete applications.	All Organizations
SaaS Application Management		
View SaaS Applications	Enable users to view SaaS applications.	All Organizations
Network Traffic		
View Traffic Throughput Statistics	Enable users to view traffic throughput statistics.	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Manage Enterprises and Assignments		
View Created Customer Profile** View Domain and Certificate**	Enable users to view created customer profile, domain and certificate.	Reseller only
Create Customer Profile	Enable users to create customer profiles.	Reseller only
Update Customer Profile	Enable users to edit customer profiles.	Reseller only
Delete Customer Profile	Enable users to delete customer profiles.	Reseller only
Assign Customer Profile	Enable users to assign customer profiles to subscriber organizations.	Reseller only
Create Domain and Certificate	Enable users to create domain and certificate.	Reseller only
Update Domain and Certificate	Enable users to edit domain and certificate.	Reseller only
Update Password Policy	Enable users to update password policy.	Reseller only
Delete Domain and Certificate	Enable users to delete domain and certificate.	Reseller only
Resellers		
View Reseller Organizations**	Enable users to view and manage resellers.	Reseller only
Update Reseller Organizations	Enable users to edit reseller organizations.	Reseller only
Manage NSG Templates		
View NSG Template Assignments**	Enable users to view NSG templates.	Reseller only
Update NSG Template Assignments	Enable users to edit NSG template assignments.	Reseller only
Manage Underlay Tags		
View Underlay Tag Assignments**	Enable users to view underlay tag assignments.	Reseller only
Update Underlay Tag Assignments	Enable users to update underlay tag assignments.	Reseller only
Manage Egress QoS Policies		
View Egress QoS Policy Assignments**	Enable users to view egress QoS policy assignments.	Reseller only
Update Egress QoS Policy Assignments	Enable users to update Egress QoS policy assignments.	Reseller only
Manage Application Groups		
View Application Group Assignments**	Enable users to view application group assignments.	Reseller only
Update Application Group Assignments	Enable users to update application group assignments.	Reseller only
Manage Diagnostics		
View Diagnostics Test Assignments	Enable users to view Diagnostics test assignments.	Reseller only
Update Diagnostics Test Assignments	Enable users to update Diagnostics test assignments. The related permission is View Diagnostics Test assignments.	Reseller only
Manage IKE Template Assignments		

Permission	Description	Applicability
View IKE templates assignments	Enable users to view IKE template assignments.	Reseller only
Assign IKE templates	Enable users to assign IKE templates.	Reseller only
Manage VSC Profiles		
View VSC Profile Assignments**	Enable users to view VSC profile assignments.	Reseller only
Update VSC Profile Assignments	Enable users to update VSC profile assignments.	Reseller only
Reports and Metrics		
View List of Available Reports**	Enable users to view list of available reports.	All Organizations
View Application Details Report	Enable users to view application details report. The related permissions are: • View Application Groups • View Application Signatures • View Branches • View L2 Networks • View L3 Networks • View L2 Network Application Groups • View L3 Network Application Groups	All Organizations
View Application Group Performance Report	Enable users to view application group performance report. The related permissions are: • View Branches • View Branch Uplink • View L2 Networks • View L3 Networks • View L2 Network Application Groups • View L3 Network Application Groups • View Traffic Throughput Statistics	All Organizations
View Network Traffic Summary Report	Enable users to view network traffic summary report. The related permissions are: • View L2 Networks • View L3 Networks	All Organizations
View Network Traffic Details Report	Enable users to view network traffic details report. The related permissions are: • View Branches • View L2 Networks • View L3 Networks	All Organizations

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
View Application Performance Inventory Report	Enable users to view application performance inventory report. The related permissions are: • View Application Groups • View Branches • View L2 Networks • View L3 Networks • View L2 Network Application Groups • View L3 Network Application Groups	All Organizations
View Network Performance Report	Enable users to view network performance report. The related permission is View Branches.	All Organizations
View Top Talkers Report	Enable users to view top talkers report. The related permissions are: • View Branches • View L2 Networks • View L3 Networks	All Organizations
View Branch Traffic Detail Report	Enable users to view branch traffic detail report. The related permission is View Branches.	All Organizations
View QoS Statistics Report	Enable users to view the QoS statistics. The related permissions are: • View Branches • View Branch Network Port • View Branch Access Port • View Branch WAN Egress QoS Policy • View Branch LAN Egress QoS Policy • View Egress QoS Policies • View VLANs • View Branch WiFi Port • View SSIDs	All Organizations
View Branch Device Metrics Report	Enable users to view branch device metrics report. The related permissions are: • View Branches • View Redundancy Groups	All Organizations
View User Security Report	Enable users to view user security report.	All Organizations
Audit and Billing		
View User Activity Report**	Enable users to view user activity report.	All Organizations
Diagnostics		

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
View Diagnostic Test Results**	Enable users to view Diagnostic test results. The related permissions are: • View Branches • View Branch Access Port • View VLANs • View Branch WiFi Port • View SSIDs • View L3 Networks • View L3 Zone • View L3 Subnet • View L2 Networks	All Organizations
Run Diagnostic Tests	Enable users to schedule Diagnostic tests. The related permissions are View Diagnostic Test Results.	All Organizations
Delete Diagnostic Test Results	Enable users to delete Diagnostic test results. The related permissions are View Diagnostic Test Results.	All Organizations
Security		
View Web Category and Domain Widgets	Enable users to view web category and domain widgets.	All Organizations
IKE Settings		
View IKE configurations**	Enable users to view IKE configurations.	All Organizations
Create IKE configurations**	Enable users to create IKE configurations.	All Organizations
Update IKE configurations**	Enable users to update IKE configurations.	All Organizations
Delete IKE configurations**	Enable users to delete IKE configurations.	All Organizations
Manage IKE Configuration Templates		
View IKE templates	Enable users to view IKE templates.	All Organizations
Create IKE templates	Enable users to create IKE templates.	CSP and Reseller only
Update IKE templates	Enable users to update IKE templates.	CSP and Reseller only
Delete IKE templates	Enable users to delete IKE templates.	CSP and Reseller only
IKE Connections		
View IKE connections	Enable users to view IKE connections.	All Organizations
Create IKE connections	Enable users to create IKE connections.	All Organizations
Create IKE connections	Enable users to create IKE connections.	All Organizations
Delete IKE connections	Enable users to delete IKE connections.	All Organizations
Platform Extensions		

Table 15-1 User Group Permissions (continued)

Permission	Description	Applicability
Run Platform Extensions	Enable users to run platform extensions.	All Organizations

Notes:

1. ** Permissions which are provided by default for the enabled permission category. These permissions cannot be disabled unless the permission category is disabled.

10.11 Assigning User Groups to a User

1

Open the Users page. See 15.2 “Viewing Users” (p. 253).

2

Select a user and click the **User Group Assignments** icon 🔗 to assign user groups to the user.

The Assigned User Groups window opens.

3

Click the **Select User Groups to Assign**.

4

Select the user group and click the **Add** icon ⊕ to assign user group.

END OF STEPS

10.12 Deleting a User Group

1

Open the User Groups page. See 15.8 “Viewing User Groups” (p. 256).

2

Select the user group, click the ellipsis icon ⋮ and click the **Delete** icon 🗑 to delete a user group.

A confirmation message displays.

3

Click **DELETE**.

End of steps

10.13 Viewing the Admin User Group

1

Open the User Groups page. See 15.8 "Viewing User Groups" (p. 256).

2

Select the admin user group of the selected reseller or subscriber organization and click the **View** icon 🗎 to view the user group. A page displays the list of read-only permissions

End of steps

11 Settings

11.1 Viewing Settings

1

Perform the following:

If you are logged in as	Then
A reseller organization user	From the main menu at the top left corner of the SD-WAN Portal, click **Settings**. By default, the Account Details tab is displayed.
	1. In the Organizations page, double-click a subscriber organization. The Subscriber Organization Dashboard opens. 2. From the organization-level menu, click **Settings**. 3. Select **Assigned Customer Profiles** in the left pane. A list of customer profiles of the subscriber organization is displayed.
A subscriber organization user	From the dashboard-level menu in the Subscriber Organization Dashboard, click **Settings**. By default, the Account Details tab is displayed.

End of steps

11.2 Adding or Editing WiFi Captive Portal Profiles

Note: This procedure applies only to reseller and subscriber organization users.

1

Go to the Settings page. See 16.1 "Viewing Settings" (p. 273).

2

Select **WiFi Captive Portal Profiles** in the left pane.

A list of WiFi captive portal profiles of the organization is displayed.

3

Perform any of the following actions:

- Click the **Add Captive Portal Profile** icon ⊕ to add a WiFi captive portal profile.

  The Create Captive Portal Profile window opens.
- Select the WiFi captive portal profile and click the **Edit Profile** icon ✎ to edit an existing WiFi captive portal profile.

  The Edit Captive Portal Profile window opens.

4

Configure the following parameters:

Parameter	Description
Profile Name*	Enter the name of the profile.
Description	Enter the description.

Parameter	Description
Terms And Conditions*	Modify the default text of the terms and conditions, if required.

5

Click **OK**.

End of steps

11.3 Deleting the WiFi Captive Portal Profiles

Note: This procedure applies only to reseller and subscriber organization users.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **WiFi Captive Portal Profiles** in the left pane.

A list of WiFi captive portal profiles of the organization is displayed.

3

Select a WiFi captive portal profile and click the **Delete Profile** icon 🗑 to delete the WiFi captive portal profile.

4

Click **DELETE**.

End of steps

11.4 Viewing Web Categories

ℹ **Note:** Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

ℹ **Note:** This procedure applies only to subscriber organizations. You can view the web categories only if your customer profile and user group have the “Policies” and “View Web Categories” permissions enabled. There are two types of web categories namely the user-defined and pre-defined web categories. When a pre-defined web category is selected, the option to assign a web domain is not available. Also, actions such as edit or delete cannot be performed on the pre-defined web categories.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273)

2

Select **Web Categories** in the left pane.

A list of web categories of the organization is displayed. Toggle the button to view all the web categories or only user-defined web categories.

End of steps

11.5 Adding or Editing Web Categories

ℹ **Note:** Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

ℹ **Note:** This procedure applies only to subscriber organizations.

You can add or edit web categories only if your customer profile and user group have the “Policies” and “Web Categories and Domains” enabled and if you are assigned the following permissions:

- Create Web Categories
- Update Web Categories

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Web Categories** in the left pane.

A list of web categories of the organization is displayed.

3

Perform any of the following actions:

- Click **Category** icon + to add a web category.
  The **Create Web Category** window opens.
- Select the web category and click the **Edit** icon ✎ to edit an existing web category.
  The **Edit Web Category** window opens.

4

Configure the following parameters:

Parameter	Description
Name*	Enter the name of the web category.
Description	Enter the description.

5

Click **OK**.

End of steps

11.6 Deleting Web Categories

ℹ **Note:** Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

ℹ **Note:** This procedure applies only to subscriber organizations.

You can delete web categories only if your customer profile and user group have the “Policies” and “Web Categories and Domains” enabled and if you are assigned the “Delete Web Categories” permission.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Web Categories** in the left pane.

A list of web categories of the organization is displayed.

3

Select a web category and click the **Delete** icon 🗑 to delete the web category.

A confirmation message displays.

4

Click **DELETE**.

End of steps

11.7 Viewing Web Domains

ℹ **Note:** Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

ℹ **Note:** This procedure applies only to subscriber organizations.

You can view web domains only if your customer profile and user group have the “Policies” and “View Web Domains” permissions enabled.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Expand **Web Categories** in the left pane and click **Web Domains**.

A list of web domains of the organization is displayed.

End of steps

11.8 Adding or Editing Web Domains

Note: Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

Note: This procedure applies only to subscriber organizations.

You can add or edit web categories only if your customer profile and user group have the “Policies” and “Web Categories and Domains” enabled and if you are assigned the following permissions:

- Create Web Domains
- Update Web Domains

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Click **Web Categories** in the left pane and select **Web Domains**.

A list of web domains of the organization is displayed.

3

Perform any of the following actions:

- Click **Domain** icon + to add a web domain.
  The **Create Web Domain** window opens.
- Select the web domain and click the **Edit** icon ✎ to edit an existing web domain.
  The **Edit Web Domain** window opens.

4

Configure the following parameter:

Parameter	Description
Name*	Enter the name of the web domain.

5

Click **OK**.

End of steps

11.9 Deleting Web Domains

Note: Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

Note: This procedure applies only to subscriber organizations.

You can delete web domains only if your customer profile and user group have the “Policies” and “Web Categories and Domains” enabled and if you are assigned the “Delete Web Domains” permission.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Expand **Web Categories** in the left pane and select **Web Domains**.

A list of web domains of the organization is displayed.

3

Select a web domain and click the **Delete** icon 🗑 to delete.

A confirmation message displays.

4

Click **DELETE**.

End of steps

11.10 Assigning Web Domains to Web Categories

Note: Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

Note: This procedure applies only to subscriber organizations.

You can assign web domains to web categories only if your customer profile and user group have the ability to update web categories.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Web Categories** in the left pane.

A list of web categories of the organization is displayed.

3

Click **Domains** icon 🔗 in the right pane.

The **Assign Web Domain** window opens.

4

Select the web domains by clicking the check box and then click **Save**.

Note: The web domains are greyed out once they are assigned to the web categories and cannot be reassigned.

5

The selected web domains are displayed in the **Assigned Web Domains** in the right pane.

End of steps

11.11 Unassigning Web Domains from Web Categories

Note: Web Filtering must be enabled at the organization profile level. Please contact the Nokia Cloud Managed SD-WAN Platform Operations team to request this if it is not currently enabled.

Note: This procedure applies only to subscriber organizations.

You can unassign web domains to web categories only if your customer profile and user group have the ability to update web categories.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Web Categories** in the left pane.

A list of web categories of the organization is displayed.

3

Select a web category. The assigned web domains are displayed on the right pane. Select the web domain and click **Unassign** icon .

4

A confirmation message displays.

5

Click **UNASSIGN**.

End of steps

11.12 Viewing Routing Policies

ℹ **Note:** This procedure applies only to subscriber organizations. Routing Policies are available only if organization profile has “Routing Protocols” enabled.

You can view the routing policies only if your customer profile and user group have the “L3 Networks” and “Routing Policies” enabled and have the “View Routing Policies” permission.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Routing Policies** in the left pane.

A list of routing policies of the organization is displayed.

End of steps

11.13 Adding or Editing Routing Policies

ℹ **Note:** This procedure applies only to subscriber organizations.

You can add or edit the routing policies only if your customer profile and user group have the “L3 Networks” and “Routing Policies” enabled and have the following permissions:

- Create Routing Policies
- Update Routing Policies

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Routing Policies** in the left pane.

A list of routing policies of the organization is displayed.

3

Perform any of the following actions:

- Click **Add** icon + to add a routing policy.
  The **Create Routing Policy** window opens.
- Select an existing routing policy, click the ellipsis icon ⋮ and click **Edit Routing Policy** to edit the routing policy.

The **Edit Routing Policy** window opens.

4

Configure the following parameters

Parameter	Description
Name*	Enter a unique name of the routing policy.
Description	Enter a description.
Default Action	By default, Accept is selected. Select a default action type: • Accept • Reject
Policy Definition	Enter a policy definition.

5

Click **OK**.

End of steps

11.14 Deleting Routing Policies

Note: This procedure applies only to subscriber organizations.

You can delete the routing policies only if your customer profile and user group have the “L3 Networks” and “Routing Policies” enabled and have the “Delete Routing Policies” permission.

1

Go to the Settings page. See 16.1 “Viewing Settings” (p. 273).

2

Select **Routing Policies** in the left pane.

A list of routing policies of the organization is displayed.

3

Select an existing routing policy, click the ellipsis icon ⋮ and select **Delete Routing Policy**. The **Delete Routing Policy** window opens.

A confirmation message displays.

4

Click **DELETE**.

End of steps