ExtremeCloud OS ONE SD-WAN v30.26.2.0 User Guide

Comprehensive Configuration and Management

9041210-00 Rev AA
August 2026

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

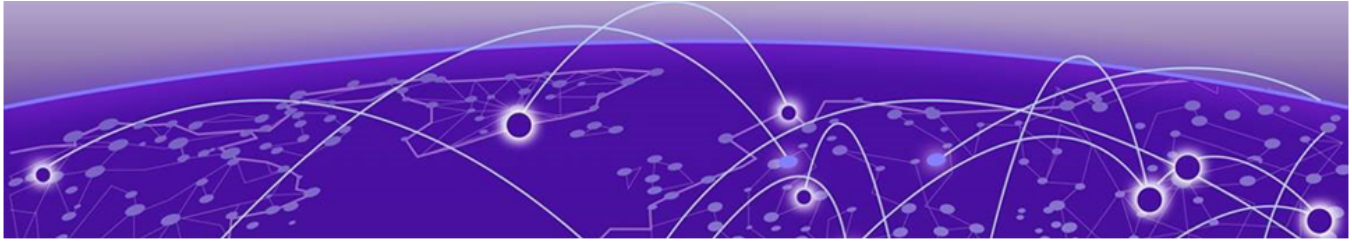
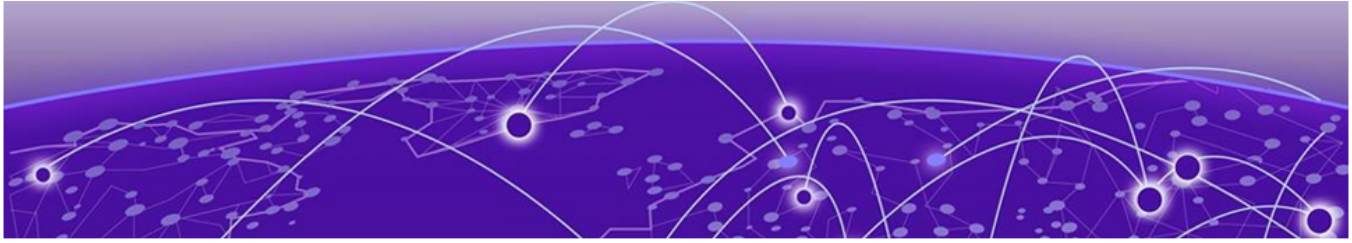


Table of Contents



Abstract

This user guide for ExtremeCloud OS ONE SD-WAN version 30.26.2.0 provides comprehensive configuration and management guidance for enterprise SD-WAN deployments. The document addresses SD-WAN infrastructure setup, network policy configuration, appliance management, and application performance monitoring. Core functionality includes network onboarding wizards, site and appliance provisioning, overlay routing with BGP AS number configuration, and Fabric Extend integration enabling zero-touch deployment over SD-WAN infrastructure. The guide covers appliance templates, application performance policies with Experience Quality Score (EQS) metrics, and WAN service management. Key sections detail policy settings including NTP and DNS configuration, RBAC-based administrator/observer access controls, and Fabric Local Breakout settings with IP connectivity tracking. Technical sections address dashboard widgets, real-time application flow visualization, tunnel performance metrics (throughput, delay, jitter, packet loss), and IPv4/IPv6 compatibility considerations. Deployment guidance includes supported hardware platforms (2200ax-F, 2200ax-T, 40ax V2, 420ax) with LED indicator diagnostics, advanced troubleshooting mode access via remote console, and system-level configuration through the ExtremeCloud IQ orchestrator. The document targets technical administrators responsible for SD-WAN architecture, policy implementation, and operational monitoring, delivering procedural steps for configuration tasks, performance optimization guidance, and hardware troubleshooting information suitable for professional network operations environments.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

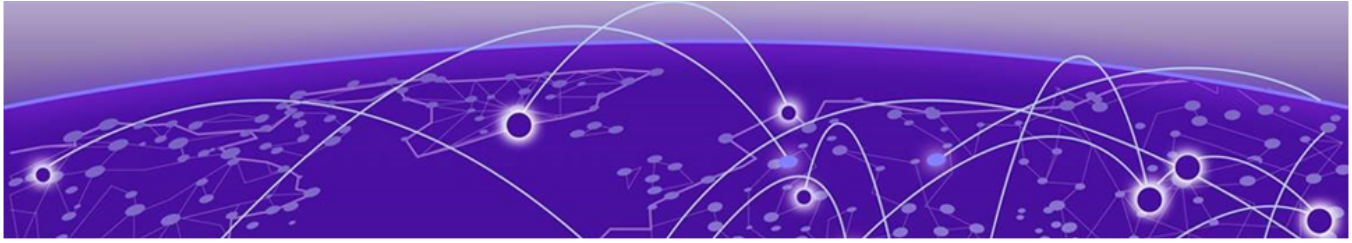
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Welcome to OS ONE SD-WAN

Prerequisite Port Connections on page 11
Log In From ExtremeCloud IQ on page 13

ExtremeCloud OS ONE SD-WAN depends on cloud-native system architecture and closely integrates the following solution components:

- ExtremeCloud OS ONE SD-WAN Orchestrator, which is cloud-hosted and part of ExtremeCloud IQ, providing a single pane of glass interface for configuration and policy definition across the entire wide-area network (WAN). Policy includes SD-WAN appliances and SD-WAN topology.
- Hardware SD-WAN Appliances that offer a routed deployment and site resiliency features designed to ensure risk-free SD-WAN technology introduction. These appliances are proprietary hardware, deployed on site, between the WAN devices and the LAN switch. Extreme Networks provides SD-WAN appliances as part of the ExtremeCloud IQ SD-WAN solution.
- Integration between Extreme Fabric Extend and ExtremeCloud OS ONE SD-WAN facilitates the extension of an existing campus network-based Fabric, with all its functions, toward remote sites equipped only with Internet connectivity.

Related Links

Prerequisite Port Connections on page 11
Log In From ExtremeCloud IQ on page 13

Prerequisite Port Connections

To ensure a smooth connection between every SD-WAN appliance and the cloud-enabled devices deployed in your network, ensure that the following ports are

open. These ports enable communication between the orchestrator, appliances, and supporting services.

Table 4: Open Ports

Cloud Server Portal	Communication Protocol	Port
SD-WAN Orchestrator, ZTP provisioning and configuration	https	8443
Upgrade and Orchestrator – Appliance (gRPC Communications)	https	443
Orchestrator – Appliance (SSE Communications)	TCP	9670
NTP clock synchronization	UDP	123

Appliances in IPsec overlays:

- Spoke Site: UDP:500 and UDP:4500 outbound connections.
- Hub Site: Local port forwarding of UDP:500 and UDP:4500, inbound from the public IP address to the hub appliance.

Extended Port Requirements

Open the following ports to allow SD-WAN appliances to communicate with cloud-hosted services such as ZTP, SD-WAN Orchestrator, Inlet Server, and NTP.

Table 5: Network Port Access

Port	Direction	Description
TCP DPORT 443	Appliance to GDC	The appliance connects to the ZTP server using this port. If the ZTP server is hosted in the PRDC, enable this port towards the PRDC.
TCP DPORT 9670	Appliance to RDC	The appliance uses this port to communicate with the SD-WAN Orchestrator. If the SD-WAN Orchestrator is hosted in the PRDC, enable this port towards the PRDC.
TCP DPORT 6667	Appliance to RDC	The appliance uses this port to connect to the Inlet Server. If hosted in the PRDC, enable this port towards the PRDC.
UDP DPORT 123	NTP Server	The appliance synchronizes time through this port. Ensure that a private NTP server in the Data Center is accessible within the PRDC network. For public NTP servers, ensure accessibility by applying the necessary changes in the PRDC network, such as opening the firewall.
UDP 500, UDP 4500	IKE and Data packet	The appliance uses these ports for IKE and IPSec data traffic. These packets bypass the PRDC, so allow them through the ISP.

Log In From ExtremeCloud IQ

Use this task to log in to ExtremeCloud OS ONE SD-WAN.

1. Using your ExtremeCloud IQ credentials, log into ExtremeCloud IQ.
2. Select , and then select **ExtremeCloud OS ONE SD-WAN**.

Related Links

Onboarding on page 21

Navigation and Dashboard

Use the ExtremeCloud OS ONE SD-WAN menu bar to access all the functions of the interface. The menu bar is located to the left of the interface so that you can easily navigate to all pages:

- **Sites**
- **Onboard**
- Application
- **Appliances**
- **WAN**
- **Reports & Templates**
- **Settings**
- **Alarms Management**

Related Links

Main Menu on page 14
Dashboard on page 15

Main Menu

Table 6 describes the available icons on the ExtremeCloud OS ONE SD-WAN main menu.

Table 6: ExtremeCloud OS ONE SD-WAN **Main Menu Icons**

	Description
	Opens the **Dashboard**, which provides a graphical overview of your network and also enables you to access ExtremeCloud OS ONE SD-WAN supervisory functions.
	Opens the **Sites** page, which provides an overview of all the sites and some detailed information for each site.
	Guides you through the onboarding process to create the Network Policy, Sites and Appliances, and to deploy your network.

Table 6: ExtremeCloud OS ONE SD-WAN **Main Menu Icons (continued)**

	Description
	Opens the **Applications** page for supervising applications and application flows.
	Opens the **Appliances** page for managing, upgrading and troubleshooting appliances.
	Opens the **WAN** page for supervising WAN Services.
	Opens the **Reports** page for creating and managing reports.
	Opens the **Settings** page for configuring and editing Network Policy, which is the basis of a healthy and efficient network.
	Opens the **Alarms Management**.
	Opens the **ExtremeCloud Apps** page.
	Displays the ExtremeCloud OS ONE SD-WAN build number and version.
ADMIN ST FSA Administrator	Displays the User Name.

Related Links

Dashboard on page 15

Dashboard

The ExtremeCloud OS ONE SD-WAN Dashboard provides an overview of your network, at a glance. To access the **Dashboard**, from the main menu, select .

Note
In this release, Fabric Support is enabled by default.

Related Links

Time Range Selector and Timeline on page 18
Dashboard Connections on page 15
Dashboard Widgets on page 16
Tunnels and Connections on page 17
Appliance Configuration on page 17
Application Configuration on page 17

Dashboard Connections

Google Maps displays your network sites. The display includes Hub Sites and Branch Sites. When sites are located close together, the map aggregates them into one cluster

site that indicates the number of sites that form the cluster, including their IPSec overlays.

To display tooltip information, such as the number of hubs and spokes, mouse over the tooltip icon.

Note
A red cluster icon indicates a raised alarm in the site cluster. Select to zoom in and view all sites within the cluster, including their IPsec overlay connections.

You can customize the dashboard view as follows:

- Select a site icon to view the **Site Summary**: site name, associated appliance status, throughput, number of connections with their status, and active alarms.

  When the sites are clustered, select the cluster to zoom into the region. After the zoom granularity reaches the site level, the **Site Summary** opens.
- Select a connection line between two sites to determine the number of tunnels and the operational status of each tunnel.

  The icon indicates the number of IPsec overlay connections on a multi-connection link. Select a multi-connection link to display detailed information, such as overlay details, connection status, appliance name, and WAN.
- Select in the upper right corner of the map to monitor connection display; either select or deselect the following options: connection status, connection type, and overlays.
- Select to open the Tunnels and Connections dashboard. This dashboard lists all configured connections, and indicates whether they are up or down.
- Select **Back** to return to the initial graph of your network.

Related Links

Onboarding on page 21
Edit the Appliance Configuration on page 62

Dashboard Widgets

The widgets at the bottom of the dashboard display the following counters for the whole network:

- **Appliances**: Connected and disconnected appliances. Select the widget header to display the Appliance Overview on page 60 page.
- **Sites**: Total number of configured sites and average throughput. Select the widget header to display the Sites on page 19 page.
- **Alarms**. Number of alarms. Select the widget to display the Alarms Management on page 102 page.
- **WAN**. Select the widget to display the WAN page.

Tunnels and Connections

To display tunnel information on the dashboard:

From the main menu, select **Dashboard** > **Tunnels**.

The **Tunnels** page displays information for each connection in your network.

Tunnels Overview

The **Tunnels Overview** table lists your network connections. You can sort the display by column:

- Tunnel
- Type of tunnel
- Tunnel status (up, down or unknown)
- Source site and destination site
- Source appliance and destination appliance

Take the following actions:

- To refresh the display, select .
- To filter the display, select .
- To clear the defined filters, select **Clear All Filters**.
- To download the table data as a `Tunnel_Data.csv` file, select .

Appliance Configuration

Select to display the **Appliances** page, or go to **Dashboard** > **Appliances widget**.

The Appliance Configuration dashboard enables you to quickly check and modify the configuration of the SD-WAN appliances used with Fabric Support.

For more information about appliance configuration settings, refer to Edit the Appliance Configuration on page 62.

Related Links

Fabric Support on page 50
Configuring Fabric over SD-WAN on page 50

Application Configuration

Select to display the **Application** page, or go to **Dashboard** > **Application widget**.

The Application Configuration dashboard allows you to view and manage the applications used in your SD-WAN deployment.

For more information about application configuration settings, refer to Applications on page 52.

Time Range Selector and Timeline

The following ExtremeCloud OS ONE SD-WAN pages display the **Time Range Selector and Timeline**:

- **Sites**
- **Appliances**
- **WAN**

The **Timeline** graph displays data for a specific time range. The timeline evolution graph shows data for throughput and raised alert curves that correspond to the chosen time range. Position your cursor over any point in the evolution curve to view the values for **Throughput** and **Raised Alerts** at a specific point in time.

Time Range Selector

To specify the range and span of the **Timeline** graph:

- Select a **Time Range** period: **Last Day** , **Last Week**, **Last Month**, **Custom**.
- Select a **Time Span**.

  Available time span options appear, according to the chosen time range, to the right of the **Time Range Selector**. Select from the following time span options: 5 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days.

  Note
  You can customize the time span by defining the date and time manually.

Timeline evolution graph

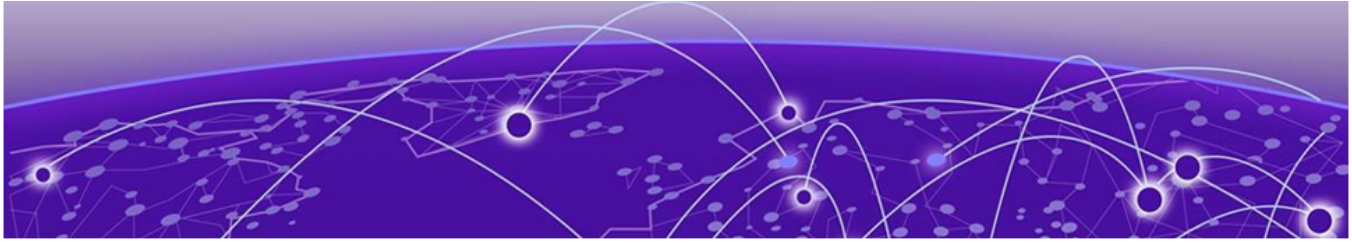
A timeline evolution graph shows **Active**, and **Cleared** alert curves, corresponding to the chosen time range.

You can interact with the graph in the following ways:

- To view the number of alerts at a specific time, position your cursor over any point in the evolution curve.
- To toggle the display of the curve, select a curve label.
- To toggle the display of the timeline, select **Show/Hide Timeline**.
- To zoom in on the timeline curves, drag the mouse over a specific time range. Select **Reset** to return to the default zoom settings.
- To reset the chart to the default time settings (Last Day, 24 hours), select **Reset**.
- To configure notification settings to inform you of alarms, select the **Notification Rules** button and configure alarm notification settings. You can configure notifications for raised and cleared alarms.

Related Links

Sites on page 19
Appliances on page 60



Sites

Sites Overview on page 19

Use sites to define boundaries for fast roaming and session mobility without interruption. A site represents a physical, geographic area in your network, and defines a roaming domain.

Select to display the **Sites** page, or go to **Dashboard** > **Sites** widget.

The **Sites** page displays the following:

- Time Range Selector and Timeline—Select a Time Range period, then position your cursor over any point of the evolution curve to view the Throughput and Raised Alerts values at a specific time.
- Overview table—View detailed information for a single site.

Related Links

Time Range Selector and Timeline on page 18
Sites Overview on page 19

Sites Overview

The **Sites Overview** table provides information on throughput and raised alerts based on the selected timeline.

- Select a time period:
  - Last Day: 5 minutes, 1 hour, 2 hours, 4 hours, 8 hours, or 24 hours
  - Last Week: 1 day, 2 days, or 7 days
  - Last Month: 7 days, 14 days, 30 days, 90 days.
  - Custom: Provide a custom date and time.
- Select the tab that corresponds to the data direction: **LAN** > **WAN** or **WAN** > **LAN**:
  - Site/Appliance/WAN interface: name of the site, associated appliance, WAN interface. Select the name to display details about the selected site.
  - The Site links usage and quality with the following fields. Consider the data for each direction tab. **LAN** > **WAN** or **WAN** > **LAN**
    - Throughput
    - Capacity: WAN access throughput (maximum bandwidth)

    - Utilization: Usage of the link, displayed both as a percentage of the link size and as a bar, the size of which is proportional to the usage.
- Adjust the EQ Score slider to filter flows within a specific quality range. Drag the left or right handles to set the minimum and maximum EQ Score, refining the displayed results based on the associated score colors. The EQ Score ranges from 0 - 10. Zero, indicating extremely poor quality and ten, indicating excellent quality.

Onboarding

Network Policy on page 21
Add Sites on page 46
Add Appliances on page 47

Use the **Onboarding Wizard** to configure your SD-WAN network, creating the basic components of your network. Subsequently, go to **Settings** on the main menu to make configuration changes.

Select **Onboard** to open the **Onboarding Wizard**.

The wizard guides you through the following steps.

1. Create a network policy.
2. Add Sites.
3. Add Appliances.
4. Deploy the configuration.

Note
By default, any newly created account is provisioned in Legacy Mode. To switch the account to NG Mode, raise a request through GTAC.

Related Links

Policy Settings on page 22
Add Sites on page 46
Add Appliances on page 47

Network Policy

The network policy settings determine the behavior of the SD-WAN network. Network Policy includes network security, appliance templates, and overlay management. Configure a network policy so that ExtremeCloud OS ONE SD-WAN appliances can provide clients with network access.

Configure network policy from the **Onboarding Wizard** for initial setup, or subsequently go to **Settings** on the main menu.

Related Links

Policy Settings on page 22
Appliance Templates on page 25
Network Overlay on page 41
Application Performance Policy on page 44

Policy Settings

Configure network policy from the **Onboarding Wizard** for initial setup, or subsequently go to **Settings** on the main menu.

Configure the following policy settings.

Table 7: Policy settings

Setting	Description
	**Configure Policy**
General Details	
Policy Name	Network policy name
Description	Optional description
Fabric Support	With this feature, Extreme Fabric Switches automatically establish Fabric Extend tunnels over the SD-WAN infrastructure. Fabric with IPv6 and IPv4 facilitates network setup through zero touch deployment. **Fabric Support** is enabled by default. For information on configuring switches for fabric deployment see the following Extreme Networks documentation: • Fabric Engine User Guide • Fabric Manager User Guide: Integration with ExtremeCloud IQ Site Engine, Fabric Configuration, and Network Automation.
Fabric Extend IP network	Fabric IP address pool.
Default Fabric Local Breakout Settings	Local breakout settings are disabled by default. You can also enable or disable local breakout for individual appliances. See Fabric Support for more information regarding configuring the local breakout settings.
Advanced Settings	

Table 7: Policy settings (continued)

Setting	Description
NTP	Specify the Network Time Protocol (NTP) server addresses. You can configure NTP in one of the following ways: • Manual Entry: Type up to three NTP server IP addresses or Fully Qualified Domain Names (FQDNs). Supported formats include IPv4, IPv6, or domain names. Select + and type each server address. • Auto-lookup: Enable **Auto-lookup** to use predefined NTP servers automatically. ◦ By default, **Auto-lookup** is enabled. ◦ When auto-lookup is enabled, the NTP servers used in the configuration are displayed in tool tips during setup. ◦ These servers are also shown on the policy page when auto-lookup is enabled.
Default DNS Settings	With Default DNS Settings, the system enables Auto via DHCP as backup by default. You can add up to three DNS servers by entering each server address under Servers.
Overlay Routing	Defines IPSec tunnel settings. Use router mode to attach overlays to a WAN interface. Type the following values: • **Overlay IP Network**: Subnet address from where ExtremeCloud OS ONE SD-WAN selects the addresses of the appliance internal interfaces. • **AS Number Range**: The ExtremeCloud OS ONE SD-WAN application uses this range of values to configure Site autonomous systems automatically. When BGP is enabled on the first appliance at a site, the orchestrator assigns the next available AS number from this range to the site. All additional appliances at the same site inherit the same AS number. You can override the auto-assigned AS at the appliance level. • **AS Number Exclusion**: Values or a range of values that you want to exclude from the AS Number Range reserved values. Authorized separators are ",|;" Simple values: N where 1<= N <= 65535 Value ranges: N-M where N<M and 1 <= N, M <= 65535 Multi-format example: 65002,65012-65024|65042;65122

Table 7: Policy settings (continued)

Setting	Description
Appliance Management Settings	Defines credentials for the different user access levels for managing appliances within the policy configuration. • **Administrator/Operator Access**: Grants full control over appliance setting, including configuration changes, updates, and troubleshooting. • **Observer Access**: Provides read-only access, allowing users to monitor appliance settings and performance without making any modifications. **Note:** When creating a password, ensure the following requirements are met: • Include at least one uppercase letter, lowercase letter, number, and special character. • Use a minimum of 14 characters.
Additional Settings	
Templates	The appliance template defines the interface behavior of appliances with similar use. Each appliance must be associated with a template. You can override most settings in a template at the appliance level. • To create a template, select +. • To view or edit a template: 1. Select **Templates**. 2. Select a template from the list. 3. Select **Edit Template**. For more information, see Appliance Templates on page 25 and Appliance Template Settings on page 25.
Application Performance Policy	An application performance policy defines how to manage an application group. It includes the criticality level of the application group. To add an application performance policy, click **Add Policy** and select the application group and criticality level from the list. For more information about adding an application group, see Application Group on page 94.
Overlays	Overlays define the IPSec tunnel settings. Use router mode to attach overlays to a WAN interface. • To create an overlay, select +. • To view or edit an overlay, select **Overlays**, and then select an overlay from the list. For more information, see Network Overlay on page 41.

Related Links

Appliance Templates on page 25

Network Overlay on page 41
Edit the Appliance Configuration on page 62

Appliance Templates

Configure a template to apply configuration settings to multiple appliances of the same deployment type. You can create different templates and apply them to appliances under one network policy. Create a template for every appliance deployment type that is used in your network. Always associate an appliance with a template. Some template parameters can be overwritten when you configure the appliance.

Note
Only Router Mode is supported. Router Mode refers to a deployment where all the WAN interfaces are configured in Router Mode (L3). Use ExtremeCloud OS ONE SD-WAN to build an overlay network of site connections through IPsec tunnels.

Important
To break out traffic to the Internet (IACL action set to DTI), configure at least one WAN interface with IPv4.

Related Links

Appliance Template Settings on page 25
Example Template: Create SD-WAN HUB Appliance on page 39
Example Template: Create SD-WAN Spoke Appliance on page 38

Appliance Template Settings

Use this procedure to create an appliance template that defines the hardware configuration, network interfaces, and path settings for your SD-WAN deployment. After creation, you can apply the template to multiple sites to maintain consistent network architecture.

1. Go to **Onboard** > **Additional Settings** > **Templates** > **Create Template**.
2. Continue to create a new template and configure the following template details:
   a. Template Name
   b. Description
   c. Appliance Type
      - **IPE**: For IPE series appliances.
      - **XSE-600**: For the Extreme Secure Edge 600 hardware.
   d. Select **Next - Setup Interface**.

3. Configure your interface architecture by enabling the LAN and WAN ports needed for your deployment.Table 8

Table 8: Interface Architecture Settings

Field	Description
Interface Configuration: IPE The IPE series appliances provide a port layout with dedicated RJ45 Ethernet ports for LAN and WAN interfaces.	
LAN Interface	**LAN 1**: Primary local network interface. This is the single LAN port on IPE appliances. It connects the appliance to your site's internal switch or router and is enabled by default. **Path Mode**: Dynamic WAN Switching is automatically enabled. DWS continuously monitors link health and directs traffic to the best available path.
WAN Interfaces	• **WAN 1**: Primary WAN link. Standard RJ45 Ethernet port for your Internet or MPLS connection. • **WAN 2**: Secondary WAN link. Standard RJ45 Ethernet port for redundancy or load balancing. • **WAN 3**: Third WAN link. Standard RJ45 Ethernet port providing an additional wired connection. • **WAN 4 (USB)**: Optional fourth WAN interface through USB LTE/5G modem. This port enables cellular backup connectivity when wired WAN links are unavailable or degraded. WAN 4 is exclusive to the IPE-40ax-V2, and IPE-420ax. This release supports only the Fujisoft FS040U modem model. APN settings must be pre-provisioned on the modem prior to deployment.
Interface Configuration: Extreme Secure Edge 600 The XSE-600 appliance features eight network ports divided into two distinct port groups. Each port group supports the same logical roles for LAN and WAN connectivity, allowing you to choose between high-speed fiber (SFP/SFP+) or standard copper (2.5G/1G RJ45) connections based on your site requirements.	
LAN Interface	**LAN 1**: You can use either Port 1 (SFP/SFP+) or Port 5 (2.5/1G Copper) for your primary local network connection. This allows you to connect a physically isolated network segment directly to the appliance. Port 1 is enabled by default for LAN 1.

Table 8: Interface Architecture Settings (continued)

Field	Description
WAN Interfaces	• **WAN 1**: Your primary internet or MPLS link can be connected to either Port 2 (SFP/SFP+) or Port 6 (2.5/1G Copper). Port 2 is enabled by default for WAN 1. • **WAN 2**: A secondary WAN link for redundancy can be connected to either Port 3 (SFP/SFP+) or Port 7 (2.5/1G Copper). Port 7 is enabled by default for WAN 2. Note that WAN 2 defaults to the copper interface rather than the SFP+ interface. • **WAN 3**: A third WAN link is available through either Port 4 (SFP/SFP+) or Port 8 (2.5/1G Copper). Both ports are disabled by default. For initial onboarding and Zero-Touch Provisioning (ZTP), only the following ports are active out of the box: • **Port 1** (LAN 1) • **Port 2** (WAN 1 - Fiber) • **Port 7** (WAN 2 - Copper) ZTP will attempt to establish orchestrator connectivity sequentially through Port 2 or Port 7. Once connectivity is established, you can modify the port mappings within the defined constraints. Select the **SFP/SFP+ ports (1 - 4)** if your deployment requires fiber connectivity for long distances, 10G speeds, or if you are using specialized copper SFP modules. Select the **2.5/1G copper ports (5 - 8)** if your site uses standard RJ45 Ethernet cabling and 1G or 2.5G speeds are sufficient for your bandwidth requirements. **Note:** For each logical role, you must enable only one physical port. For example, if you enable Port 2 for WAN 1, the corresponding copper Port 6 must remain disabled. Do not connect to both ports for the same role simultaneously.
Advanced Setup Settings	Select the appliance as a Spoke (Branch Office) or a Hub (Data Center). Tunnels, which are generated on router interfaces, are always built from the spokes to the hub. To configure site-to-site connections, set the role to Spoke for both appliances.
Adaptive QoS	Enable **Adaptive QoS** to detect WAN-to-LAN congestion and apply traffic shaping on the remote link. For more information, see Adaptive QoS Overview on page 32.

4. **Configure LAN Interface**: For LAN interfaces, configure the following Additional Settings. Table 9

Table 9: LAN Interface Settings

Field	Description
LAN Interface Speed	By default, set to Auto, allowing the system to determine the LAN interface speed. The full-duplex speed is measured in megabits per second and includes includes the following options: • Auto • 100 FD • 1000 FD
MTU	Enter the MTU value, which defines the maximum number of bytes in the payload. The valid range is 1280–9194 bytes, defaults to 2000.
DNS	Select **Apply Default Policy Settings** to use DNS from the network policy or enter custom servers.

5. Select **Next - WAN Settings**
6. **Configure WAN Interface**: For WAN interfaces, define each interface: WAN1, WAN2, WAN3 and WAN4. Only Router mode is supported. Select the IP version for the WAN interface. If you are using WAN4 LTE interface, see LTE (WAN4) Interface Configuration on page 34 for additional configuration options. Table 10

Table 10: WAN interfaces Settings

Field	Description
Interface	
Description	Optional description of the WAN.
Bandwidth Up	Maximum upload bandwidth in Mbps. Default: 10000.
Bandwidth Down:	Maximum download bandwidth in Mbps. Default: 10000.
Interface Speed	Set to **Auto** by default to let the system define the speed of the WAN interfaces, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
MTU	Enter the MTU value that corresponds to the maximum number of bytes loaded in the payload. The default value is 1500.
TCP MSS Adjustment	Enable or disable TCP MSS adjustment to optimize packet transmission efficiency and prevent fragmentation across WAN links. Select one of the following options: • **No Adjustment**: Keeps the TCP MSS value unchanged. • **Adjusted MSS**: Adjusts the MSS value for TCP packets. Enter a value between 536 and 1460 bytes. Values outside this range are not allowed. The default value is 1300.

Table 10: WAN interfaces Settings (continued)

Field	Description
WAN Service	Defines the type of WAN connectivity for this interface. This affects how the orchestrator builds overlay tunnels. • **Internet**: Standard Internet connection. Supports overlay tunnels and DTI breakout. • **MPLS**: Private MPLS circuit. Supports site-to-site tunnels only. DTI is not available. • **Internet**: Broadband connection. To create a WAN service, select **Create WAN Service** and provide the **WAN Service Name** and **Description**.
DTI	Select the Direct-to-Internet (DTI) option to allow traffic out to the Internet through this WAN interface. • Enabled - Traffic matching DTI policies exits directly to the Internet through this WAN interface without traversing the overlay. Network Address Translation (NAT) is automatically applied to outbound DTI traffic. A stateful firewall is activated, allowing only return traffic for connections initiated from within the LAN. • Disabled - All traffic is forwarded through the SD-WAN overlay tunnels regardless of destination. No local Internet breakout occurs on this interface. Note: These values are inherent from the appliance template. You can override these settings if necessary. However, after you override a template setting, the appliance no longer uses the template settings for this WAN interface.
Routing	

Table 10: WAN interfaces Settings (continued)

Field	Description
Default BGP Local Preference	Border Gateway Protocol (BGP) local preference value applied to all overlay tunnels on this WAN interface. Higher values indicate a more preferred path. This can be overridden at the per-tunnel level. Default: empty (system default of 100 is used). When you configure a local preference value, custom policies are automatically created to apply this preference to your tunnels: For Hub & Spoke Deployments: Custom policy is created based on the local preference configuration for the tunnel. If a local preference is configured for a specific tunnel, that tunnel-specific value is used. If not configured for the tunnel, the WAN local preference for the Hub is applied. Policy naming format: Custom_ln_<tunnel_name> Example: Custom_ln_conn-dev-6-wan1-dev-9-wan1-hns-ipv6-6-auto-1518 For Site-to-Site Deployments: Custom policy is created based on the WAN local preference for the initiator of the connection. Policy naming format: Custom_ln_<tunnel_name> Example: Custom_ln_conn-dev-10-wam1-dev-6-wan1-hns-ipv6-4-user-1542 Note: These custom policies are automatically managed by the system. Do not manually edit or delete them, as they are required for proper BGP local preference operation.
BFD Transmit Interval	Interval in milliseconds between Bidirectional Forwarding Detection (BFD) keepalive packets sent over overlay tunnels on this WAN interface. Lower values detect failures faster. Range: 50 - 30,000 ms. Default: 1000.
BFD Multiplier	Number of consecutive missed BFD packets before declaring the session down. Range: 3 - 50. Default: 7.
Additional Settings	
Tunnel Underlay IP Address	If Public IP Address is selected, configure the port forwarding of the internet access router to send UDP packets to the appliance's WAN on port 500 (IKEv2) and port 4500 (IPsec NAT Traversal). If the appliance is a hub, a Public IP address is mandatory. If the appliance is a spoke, a Public IP address is optional unless there is a need for a site-to-site tunnel.
WAN Interface IP	Configure **WAN Interface IP** for direct public IPs.

Table 10: WAN interfaces Settings (continued)

Field	Description
LLDP Settings	Enable or disable Link Layer Discovery Protocol (LLDP) on this WAN interface. LLDP allows the appliance to advertise its identity and discover neighboring devices on the WAN link. When Enabled, LLDP packets are sent and received on this interface. LLDP Settings is not available for WAN 4 (USB).
Overlay	Select an Overlay you previously created and apply it to the interface. Select **Configure Tunnel** to view the Overlay Details.
Security Gateway	Select a previously created Security Gateway and apply it to the interface. You can edit and customize the selected gateway from this panel.

7. WAN Configuration (Cellular WAN 4 USB - IPE Only)

   Configure the WAN4 (USB) interface by using the same WAN interface settings described in the Configure WAN Interface. For LTE deployments, configure the following settings Table 11:

Table 11: LTE WAN Configuration

Field	Description
Modem	Select the USB modem model. This release supports only the Fujisoft FS040U modem model.
MTU	WAN MTU: Set to 1420 bytes (default) Tunnel MTU: Set to 1300 bytes Tunnel Type: IPv6 only These settings help reduce packet fragmentation and improve throughput over cellular networks.
TCP MSS Adjustment	Enable Adjusted MSS and set the MSS Value to 1100 bytes.

Table 11: LTE WAN Configuration (continued)

Field	Description
Routing	• **Default BGP Local Preference**: 100 (or adjust based on your path preference) • **BFD Transmit Interval**: 1000 ms • **BFD Multiplier**: 15
Additional Settings	**Preemptively Reset Modem:** Enable this option to schedule periodic modem resets. Configure the following parameters: • **Time Zone**: Select the appliance's local time zone. • **Frequency**: Specify how often to reset the modem (for example, **1** for daily). • **Time**: Select the time of day to perform the reset during a low-traffic period. **Note:** During a scheduled modem reset, WAN4 (USB) is temporarily unavailable while the modem reconnects to the LTE network. If other WAN interfaces are available, traffic automatically fails over and resumes on WAN4 after the LTE connection and tunnels are re-established For recommended LTE configuration values and deployment considerations, see LTE (WAN4) Interface Configuration on page 34.

8. Select **Next - Summary**.
9. In the Summary section, review the visual architecture map and configuration checklist, then select **Create Template** to save the template. Verify all settings match your deployment plan before saving.

Related Links

Example Template: Create SD-WAN HUB Appliance on page 39
Example Template: Create SD-WAN Spoke Appliance on page 38
LTE (WAN4) Interface Configuration on page 34

Edit the Appliance Configuration on page 62
Adaptive QoS Overview on page 32

Adaptive QoS Overview

Adaptive QoS dynamically applies rate limiting to prioritize critical traffic during WAN-to-LAN congestion. When congestion is detected, the appliance communicates bandwidth restrictions to the remote peer so that it can reduce lower-priority traffic and preserve bandwidth for critical applications.

Enable **Adaptive QoS** to allow appliances to exchange congestion information and apply rate limiting based on available bandwidth.

How Adaptive QoS Works

Adaptive QoS helps manage WAN-to-LAN congestion by dynamically applying rate limiting to prioritize critical traffic.

In a typical hub-and-spoke deployment, when the hub detects WAN-to-LAN congestion, it sends bandwidth restriction information to the spoke. The spoke then applies rate limiting to lower-priority traffic, helping preserve bandwidth for critical applications. Rate limiting is triggered based on the Bandwidth Down value configured for the WAN interface of Hub.

Adaptive QoS applies rate limiting only when the feature is enabled on both devices:

- **Hub**: Detects congestion and sends bandwidth restriction information to the spoke.
- **Spoke**: Receives the congestion information and applies rate limiting to outbound traffic.

Adaptive QoS also works in the reverse direction. When the spoke detects WAN-to-LAN congestion, it notifies the hub to apply rate limiting. This allows the feature to manage congestion bidirectionally.

Traffic reporting considerations

When Adaptive QoS rate limiting is applied:

- Rate limiting is applied per criticality class to ensure critical applications are given higher priority during congestion. Applications with the same criticality level may receive varying bandwidth allocations, as traffic classification is based on criticality level.
- When incoming TCP traffic is sent as bursts, the Real-Time Graph (RTG) might not depict the traffic limiting effect precisely because the TCP client congestion window adjustment is unpredictable, resulting in applying and reverting rate limiters in quick intervals.

Limitations:

Adaptive QoS is not supported over LTE interfaces.

Related Links

Example Template: Create SD-WAN HUB Appliance on page 39
Example Template: Create SD-WAN Spoke Appliance on page 38
LTE (WAN4) Interface Configuration on page 34

Edit the Appliance Configuration on page 62
Adaptive QoS Overview on page 32

WAN Interface IP Address

When configuring your appliance, you must specify a WAN Interface IP address on the Appliance 360 configuration page.

Choose between an IPv4 address or an IPv6 address. The specific details for each configuration are outlined here.

- The default IP Address range for the WAN Setup is IPv4. The default values for Tunnel Underlay and WAN Interface IP Address depend on the IP Address range selected for WAN Setup.

  When using the IPv4 address range for the WAN:
  - The Tunnel Underlay value defaults to **Public IP Address**.
  - And the WAN Interface IP Address defaults to **Enable DHCP**.

    With a Public IP address, the Tunnel Underlay uses the external Public IP address. When selecting this option, you must supply the Public IP address for each appliance under Appliance 360. Available settings are DHCP or manual. This option is best when the Public IP addresses are static.

  When using the IPv6 address range for the WAN:
  - The Tunnel Underlay value defaults to **WAN Interface IP Address**.
  - The WAN Interface IP Address value defaults to **Enable IPoE**.

    With a WAN interface IP address, the internal WAN interface IP address is obtained from the WAN interface IP setting. Available settings are IPoE or SLAAC (manual). IPv6 is not recommended when the WAN has Network Address Translation (NAT) applied.

LTE (WAN4) Interface Configuration

LTE (4G Long-Term Evolution) cellular networks present distinct operational characteristics that require careful tuning of tunnel parameters. Unlike fixed-line connections, LTE networks operate within inherent constraints imposed by cellular protocols, carrier infrastructure, and radio frequency conditions. These constraints affect packet transmission, fragmentation behavior, IP address lifecycle management, and tunnel stability.

This section outlines the specific configurations required to optimize tunnel performance, ensure reliable failover capability, and maintain consistent connectivity across LTE underlays.

Configuration Overview

LTE (WAN4) interface configuration can be performed through two methods:

- Template-Based Configuration: Configure LTE settings as part of an appliance template during the onboarding process. This applies consistent LTE parameters across multiple appliances.

- **Appliance-Level Configuration:** Override or configure LTE settings directly on individual appliances after deployment through **Edit the Appliance Configuration**.

Note
Only the Fujisoft FS040U USB modem is supported in this release 30.26.2, before connecting the USB modem to the SD-WAN appliance, you must pre-provision the APN profile directly onto the dongle externally. Refer to the official Fujisoft FS040U documentation for APN configuration instructions.

BFD Configuration for LTE Tunnels

LTE networks require tailored BFD (Bidirectional Forwarding Detection) settings to accommodate latency variability while maintaining robust tunnel monitoring.

To accommodate the LTE inherent variability while maintaining reliable tunnel monitoring, configure the following:

- **BFD Transmit Interval:** 1000 milliseconds
- **BFD Multiplier:** 15
- **Detection Interval:** 15 seconds (1000ms × 15)

This configuration provides sufficient time for BFD packet exchanges while supporting LTE network latency fluctuations, reducing false-positive tunnel failure detections.

Tunnel-Level BFD Configuration for Remote Endpoints

When a tunnel is configured and originates from an LTE WAN4 interface, it uses the BFD profile settings configured for the LTE WAN4 interface.

Firmware Compatibility Note:

For accurate traffic reporting and WAN4 interface recognition in deployments with mixed wired and LTE interfaces, both appliances must be running firmware version 30.26.2.0 or later. When appliances running different firmware versions communicate over LTE WAN4, traffic may not be accurately reported in the Orchestrator by the appliance running the older firmware version.

To configure BFD settings:

1. Go to **Appliances > Select LTE appliance > Edit Configuration**.
2. Navigate to the **WAN 4** tab.
3. Under **Routing Settings**, configure:
   - **Default BGP Local Preference:** 100 (or adjust based on path preference)
   - **BFD Transmit Interval:** 1000 ms
   - **BFD Multiplier:** 15
4. Select **Save**.

MTU Configuration for LTE Interfaces

LTE carrier networks typically enforce a Maximum Transmission Unit (MTU) of 1420 bytes at the underlay layer. To prevent IPv6 underlay packet fragmentation, tunnel MTU must be configured lower than the LTE underlay MTU.

Recommended Tunnel MTU Setting: Tunnel MTU - 1300 bytes

To configure Tunnel MTU:

1. Go to **Settings > Common Objects > Overlays**.
2. Select the overlay to edit, locate **MTU**.
3. Set **MTU** to **1300** bytes.
4. Select **Save**.

TCP MSS Clamping for LTE Interfaces

TCP Maximum Segment Size (MSS) clamping optimizes packet sizes to prevent fragmentation across LTE networks, which have stricter MTU constraints than wired networks.

Recommended MSS Clamping Configuration:

- **TCP MSS Adjustment:** Enabled
- **MSS Value:** 1100 bytes

LTE networks are sensitive to packet fragmentation. The 1100-byte MSS value ensures that TCP segments, when combined with IP and overlay tunnel headers, remain within the LTE underlay MTU of 1420 bytes, minimizing retransmissions and improving application responsiveness.

To configure MSS clamping:

1. Go to **Appliances > Select LTE appliance > Edit Configuration**.
2. Navigate to the **WAN 4** tab.
3. Under **Interface** settings, locate **TCP MSS Adjustment**.
4. Enable **TCP MSS Adjustment**.
5. Set **MSS Value** to **1100** bytes.
6. Select **Save**.

Preemptive IP Reset for LTE Connectivity

LTE carrier networks periodically reclaim stale IP addresses by enforcing a mandatory reset cycle, typically every 24 hours. This reset causes the LTE modem to obtain a new public IP address, triggering IPsec tunnel re-establishment, which takes approximately 3 minutes.

To minimize traffic loss, the appliance provides a preemptive reset capability. This allows you to schedule IP refresh at a controlled time such as during low-traffic periods rather than waiting for the carrier to impose an uncontrolled reset during active traffic flow.

To configure Preemptive IP Reset:

1. Go to **Appliances > Select LTE appliance > Edit Configuration**.
2. Navigate to the **WAN 4** tab.
3. Locate **WAN Configuration (Cellular WAN 4 USB - IPE Only)** section.
4. Configure the following:
   - **Preemptively Reset Modem:** Enable
   - **Select Time Zone:** Choose the appliance's local time zone
   - **Frequency:** Enter reset interval in days (1 for daily)
   - **Time:** Select the time of day to perform reset (02:00 AM for off-peak hours)
5. Select **Save**.

What Happens During Preemptive Reset

At the scheduled time, the appliance initiates a modem power-cycle. Within 30 seconds, the modem re-boots and initiates LTE authentication. By 60 seconds, the modem obtains a new public IP from the carrier. Between 60 to 180 seconds, IPsec tunnels re-establish. In approximately 3 minutes, all tunnels are operational and traffic is fully restored.

If secondary WAN links (WAN1, WAN2, WAN3) are configured and active, traffic automatically fails over during the 3-minute window. If no secondary links exist, traffic is unavailable for the duration. After tunnels re-establish, traffic returns to normal.

Best Practices for Preemptive Reset

Schedule resets during known low-traffic periods such as early mornings, nights, or weekends. Avoid times when your organization experiences critical business operations or remote-access usage.

Ensure that secondary WAN links are active and configured with lower BGP local preference values than WAN4 (LTE). This ensures traffic automatically reroutes during the 3-minute reset window.

Set the preemptive reset frequency to match or precede your carrier's typical IP recycling interval. Most carriers use a 24-hour cycle, so daily (frequency = 1) is recommended.

After enabling preemptive reset, monitor tunnel status and traffic metrics for 1-2 weeks. During this time, confirm the modem consistently resets at the scheduled time, tunnels reliably re-establish within 3-minutes, traffic properly fails over to secondary links, and no unexpected disruptions occur outside the scheduled reset window.

Note
Preemptive reset causes a 3-minute service disruption on the LTE link. Ensure you have secondary WAN links configured and active to maintain traffic continuity during this window. Without secondary links, users will experience a brief outage at the scheduled reset time.

Related Links

Example Template: Create SD-WAN HUB Appliance on page 39
Example Template: Create SD-WAN Spoke Appliance on page 38
LTE (WAN4) Interface Configuration on page 34

Edit the Appliance Configuration on page 62
Adaptive QoS Overview on page 32

Example Template: Create SD-WAN Spoke Appliance

To configure the template of an SD-WAN spoke appliance with one Internet Access link and optional LTE backup, proceed as follows:

1. Go to **Onboard > Additional Settings > Templates > Create Template**.

   The Template Wizard displays the main steps of the procedure.
2. Select **Continue**.
3. Type the **Template Name**, **Description** and **Appliance Type**.
4. Select **Next - Setup Interface**.
5. The Setup graph displays the following fixed settings:
   - **LAN1** is enabled by default.
   - **Path Mode** is set to **Dynamic WAN Switching (DWS)** by default.

   Configure the following WAN interface settings:
   - **Enable WAN 1**, **WAN 2**, and **WAN 3** as appropriate for your network configuration.
   - **(Optional) Enable WAN 4** if deploying LTE cellular backup.
6. Under Advanced Setup Settings, configure:
   - Select the role of the appliance as a **Spoke**.
   - Enable Adaptive QoS to apply rate limiting on the remote interface based on the interface bandwidth, to ensure prioritize critical traffic. This feature is not supported on LTE interfaces.
7. Select **Next - Configure Interface**.
8. In the **LAN** panel, leave all the parameters to their default values.
9. Select **Next - WAN Settings** or select the **WAN** tab next to the Configure Interface title.
10. Configure the WAN1 interface:
    a. Either select MPLS as the Transport Network or create a Transport Network. Then, select the new Transport Network you have created.
    b. Leave **Additional Settings** to their default values.
11. Configure the WAN 2 interface by using the same procedure as for WAN 1.
12. Configure the WAN 3 interface:
    a. Either select **Internet** as the Transport Network or create a Transport Network. Then, select the new Transport Network you have created.
    b. Leave **Additional Settings** to their default values.

13. Configure the WAN 4 (LTE) interface:
    - **Description:** Custom description
    - **Bandwidth Up:** Specify maximum outbound bandwidth. This value is used by Adaptive QoS to track outbound capacity.
    - **Bandwidth Down:** Specify maximum inbound bandwidth. **This value is critical, it triggers Adaptive QoS congestion detection.**
    - **Interface Speed:** Auto
    - **MTU:1300** (critical for LTE)
    - **TCP MSS Adjustment:Enabled**
    - **MSS Value:1100** (critical for LTE)
    - **WAN Service:** Select or create a cellular-specific WAN Service.
    - **Default BGP Local Preference:50** (lower than wired links to ensure wired paths are preferred).
    - **BFD Transmit Interval:1000 ms**
    - **BFD Multiplier:15**
    - **IP Version:** Select the IP version for the WAN interface. For LTE WAN4 deployments, only IPv6 is supported.
    - **Tunnel Underlay:** Select the tunnel underlay type:
      - **IPv4:** Public IP Address (for wired WAN interfaces).
      - **IPv6:** WAN Interface IP Address (for IPv6-capable WAN interfaces).

      For LTE WAN4 deployments, only IPv6 is supported. Use the WAN Interface IP Address for tunnel underlay.
    - **WAN Configuration (Cellular WAN 4 USB - IPE Only):**
      - **Modem Selection:** Select your LTE modem model
      - **Preemptively Reset Modem:Enable**
      - **Select Time Zone:** Choose appropriate time zone
      - **Frequency:1** (daily)
      - **Time:** low-traffic period
14. Select **Next - Summary**.

    Review the visual architecture map and configuration checklist. Verify all settings match your deployment plan.
15. Select **Create Template**.

The new template is displayed in the **Template** panel of the **Policy Configuration** window.

Related Links

Example Template: Create SD-WAN HUB Appliance on page 39

Example Template: Create SD-WAN HUB Appliance

Configure a template for an SD-WAN hub appliance. Compared to the Spoke appliance template, a Hub typically does not require LTE since it is located in a data center

with redundant wired connectivity. However, LTE can be configured as an emergency backup if required.

1. Go to **Onboard > Additional Settings > Templates > Create Template**.

   The Template Wizard displays the main steps of the procedure.
2. Select **Continue**.
3. Type the **Template Name** and **Description**.
4. **Appliance Type:** Select **IPE** or **XSE-600** as appropriate.
5. Select **Next - Setup Interface**.
6. The Setup graph displays the following fixed settings:
   - **LAN 1** is enabled by default.
   - **Path Mode** is set to Dynamic WAN Switching (DWS), which is automatically enabled.

   Configure the following WAN interface settings:
   - Enable WAN 1, WAN 2, and WAN 3 as appropriate for your network configuration.
7. Under Advanced Setup Settings, configure:
   - Select the role of the appliance as a **Hub**.
   - Enable Adaptive QoS to enable dynamic rate limiting for congestion management. This feature monitors WAN-to-LAN traffic and sends bandwidth restriction information to Spokes during congestion.
8. Select **Next - Configure Interface**.
9. In the **LAN** panel, leave all the parameters to their default values.
10. Select **Next - WAN Settings** or select the **WAN** tab next to the Configure Interface title.
11. Configure the WAN 1 interface:
    - **Bandwidth Up:** Specify the maximum outbound (LAN-to-WAN) capacity in Mbps.
    - **Bandwidth Down:** Specify the maximum inbound (WAN-to-LAN) capacity in Mbps. If Adaptive QoS is enabled, this value determines congestion detection thresholds.
    - Either select **MPLS** as the Transport Network or create a Transport Network. Then, select the new Transport Network you have created.
    - **Default BGP Local Preference:100** (standard Hub preference).
    - **BFD Transmit Interval:1000 ms** (standard wired default).
    - **BFD Multiplier:7** (standard wired default).
    - Leave Additional Settings to their default values.
12. Configure the WAN 2 interface by using the same procedure as for WAN 1.
13. Configure the WAN 3 interface:
    - **Bandwidth Up** and **Bandwidth Down:** Specify values appropriate for your link capacity.
    - Either select **Internet** as the Transport Network or create a Transport Network. Then, select the new Transport Network you have created.
    - Leave Additional Settings to their default values.

14. Configure WAN 4 (LTE) as emergency backup (if required):
    - **Description**: Custom description
    - **Bandwidth Up:** Specify the maximum outbound capacity (for example, 5 Mbps for basic LTE plan).
    - **Bandwidth Down:** Specify the maximum inbound capacity (for example, 5 Mbps for basic LTE plan). **If Adaptive QoS is enabled on both Hub and Spokes, this value triggers congestion detection for rate limiting.**
    - **Interface Speed:** Auto
    - **MTU:1300** (critical for LTE)
    - **TCP MSS Adjustment:Enabled**
    - **MSS Value:1100** (critical for LTE)
    - **Default BGP Local Preference:10** (much lower than wired to use only if other links fail).
    - **BFD Transmit Interval:1000 ms**
    - **BFD Multiplier:15**
    - **WAN Configuration (Cellular WAN 4 USB - IPE Only):**
        - **Modem Selection:** Select your LTE modem model.
        - **Preemptively Reset Modem:Enable**
        - **Select Time Zone:** Choose appropriate time zone.
        - **Frequency:1** (daily)
        - **Time:**low-traffic period (coordinate with Spoke reset time if desired).
15. Select **Next - Summary**.

    Review the visual architecture map and configuration checklist. Verify all settings match your deployment plan.
16. Select **Create Template**.

Related Links

Example Template: Create SD-WAN Spoke Appliance on page 38

Network Overlay

SD-WAN creates a network overlay that manages a communication tunnel between two networks, eliminating the need for hard-coded network communication. Overlay networks can make your network more secure by segmenting traffic and restricting network access. ExtremeCloud OS ONE SD-WAN supports Hub & Spoke Overlays.

Select **Onboard** to open the **Onboarding Wizard**.

Create an overlay from the **Onboarding Wizard** for initial setup, or subsequently go to **Settings** on the main menu.

Related Links

Hub and Spoke Overlay Settings on page 42
Define a Hub and Spoke Overlay on page 42
Apply Hub and Spoke Overlay to Appliances on page 44

Example Template: Create SD-WAN HUB Appliance on page 39
Example Template: Create SD-WAN Spoke Appliance on page 38

Define a Hub and Spoke Overlay

You can define a Hub & Spoke overlay to create standard VPN connections between appliances and exchange traffic.

Create a Hub & Spoke overlay from the **Onboarding Wizard** for initial setup, or subsequently go to **Settings** on the main menu.

Use this task to create an overlay from the **Settings** menu.

1. Go to **Settings** > **Policy Configuration**.
2. Select **Add Overlay**.
3. From the **Type** field, select **Hub & Spoke**.
4. Type the **Name** of the overlay.
5. Select the IP version of the WAN.
6. Configure the overlay parameters.
7. Select **Save**.

Your new overlay appears in the **Overlays** section of the **Policy Configuration** window.

- To edit, select the overlay.
- To delete, select **View All** and select the overlay to delete.

Related Links

Hub and Spoke Overlay Settings on page 42
Apply Hub and Spoke Overlay to Appliances on page 44
Network Overlay on page 41
Onboarding on page 21

Hub and Spoke Overlay Settings

ExtremeCloud OS ONE SD-WAN supports Hub & Spoke Overlay. Configure the following settings to create an overlay.

Table 12: Hub & Spoke Overlay Settings

Setting	Description
General Information	
Name	Overlay name
IP Version	Valid values: IPv4 and IPv6
Type	Hub & Spoke
Hub & Spoke Configuration	

Table 12: Hub & Spoke Overlay Settings (continued)

Setting	Description
IKE policy	Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs). Refer to RFC 5996. • Encryption: Drop-down list to choose the encryption algorithm (mandatory) • Authentication: Integrity drop-down list to choose the data integrity hash method • DH Group drop-down list to choose the Diffie-Hellman group: 1 (768-bit), 2 (1024-bit), 5 (1536-bit), 14, 19, 20, 21 and 24 • rekeytime (120-86400): Time in seconds between each IKE SA rekey.
IPsec Concentrator authentication	If a Pre-Shared Key (PSK) is already configured, select it from the list. The PSK is used for all the tunnels between appliances, and is automatically generated by the system for each customer. However, you can enter a new PSK as a string of at least 32 characters. You have the option to display or hide the key.
IPsec policy	• Encryption: drop-down list to choose the encryption algorithm (mandatory). The available options are the same as for IKE policy encryption plus NULL • Authentication: integrity drop-down list to choose the data integrity hash method (mandatory); see IKE policy integrity • DH Group (PFS only): drop-down list to choose the Diffie-Hellman group: 1 (768-bit), 2 (1024-bit) or 5 (1536-bit), 14, 19, 20, 21, 24 and PFS disabled (PFS ensures that the same key will not be generated again, so forces a new Diffie-Hellman key exchange. Both sides of VPN should support PFS in order for PFS to work. Therefore using PFS provides a more secure VPN connection) • SA lifetime (seconds) Security Association lifetime (86,400 s that is: 24 hours by default; mandatory). The authorized range of values is (120-86400) The time in seconds between each IKE SA rekey. • MTU (bytes): maximum number of bytes loaded in the Payload. The default value is 1400. This value applies to all IPsec tunnels.

Related Links

Define a Hub and Spoke Overlay on page 42
Onboarding on page 21
Apply Hub and Spoke Overlay to Appliances on page 44

Apply Hub and Spoke Overlay to Appliances

First define the overlay.

Use this task to apply an overlay to one or more appliances.

1. From the main menu, select **Appliances**.
2. Select the **Spoke** appliance and the **WAN** tab.
3. Select the appropriate WAN interface in Router mode.
4. From the **Overlay** list, select the **Hub & Spoke** overlay that will establish the VPN tunnel.
5. Select **Done**.
6. Select the Hub appliance and the **WAN** tab.
7. Select the appropriate WAN interface in Router mode and apply the same Hub & Spoke overlay as for the Spoke appliance.
8. Select **Done**.

Creation of the new tunnel is complete.

Related Links

Define a Hub and Spoke Overlay on page 42
Hub and Spoke Overlay Settings on page 42
Application Performance Policy on page 44

Application Performance Policy

With Application Performance Policy you can group applications and define how they are treated across the network based on priority and performance objectives. These policies ensure that the critical applications consistently receive optimal performance and appropriate path selection through Dynamic WAN Selection (DWS).

Each policy applies to an Application Group, which serves as the unit for traffic classification and policy enforcement. Application groups define how the system identifies, prioritizes, and steers traffic based on priority and performance objectives.

Defining Application Groups

Define an application group by grouping applications that share common performance requirements or priorities. For example,

SD-WAN classifies traffic by evaluating it against the defined application groups in order. It assigns each packet to the first matching group and applies the corresponding Application Performance Policy.

Select **Settings** from the main menu to open the **Policy Configuration** window.

Select **View All** in the **Application Performance Policy** section to see all configured application groups.

Each Application Performance Policy includes:

- Application Groups
- Defined Business Criticality level.
- Application SLA to enforce service-level objectives.
- Dynamic WAN Selection (DWS) Policy to guide path selection based on performance.

To add Application Performance Policy:

1. Go to **Settings** > **Policy Configuration**.
2. Under **Application Performance Policy**, select **Add Application Performance Policy**.
3. Define the application performance policy parameters:

Table 13: Application Performance Policy Settings

Settings	Description
Add general information	
Application Group	Name of the application group
Business Criticality	Indicates the priority level of the application group: • Top • High • Medium • Low
Application SLA	Defines performance thresholds such as delay, jitter, and packet loss. Select the application SLA from the list, refer to Application SLA to add a new Application SLA.
DWS Policy	
Primary WAN Services	Select the preferred WAN service(s) for this Application Group.
Secondary WAN Services	Select alternative WAN services. Choose between **Performance Based** (default) or **Backup**, when Primary path is unavailable or performance is degraded.

Table 13: Application Performance Policy Settings (continued)

Settings	Description
Tertiary WAN services	Select **Performance Based** or **Backup** (default), when both Primary and Secondary are unavailable or degraded.
Advanced Parameters	Return Path - Determines how return traffic is routed for a session: • Same as Received: Return traffic follows the same WAN path that was used for the original traffic. This ensures that the response traffic follows the same path as the initial request and bypasses DWS for the return direction. • Dynamic: Return traffic is evaluated using DWS. The return traffic is evaluated against the configured policy and current WAN conditions, and the system may choose a different path than the original traffic to meet the defined SLA and performance requirements. Granularity - Determines how traffic is evaluated for DWS decisions: • Per Session • Per Packet Default Action - Defines the action to take when no valid path is available: • Forward: The device forwards traffic to one of the available routes, not to NAP 0. • Drop: If a path becomes non-compliant with the SLA or degraded, the system chooses the most optimal path from the remaining available options.

Related Links

Add Sites on page 46
Add Appliances on page 47

Add Sites

A site represents a physical, geographic area in your network. Use this task to add a network site.

1. Select **Onboard** to open the **Onboarding Wizard**.
2. Select **Add Site** > **Add Site**.
3. Specify the following parameters:
   - Site Name
   - Street Address

- City
- State/Province
- Country
- Postal Code

4. Select **Save Site**.
5. Select **Next** to provision appliances.

Related Links

Add Appliances on page 47

Add Appliances

You can identify the type of SD-WAN appliance by the appliance Serial Number:

- For all the appliances *except* ipe-2200ax- F — The Serial Number is made of 12 characters and is indicated on the appliance chassis.
- For appliances ipe-2200ax-F only — The Serial Number is made of 15 characters and is indicated on the appliance chassis.

Note
To add multiple appliances, you can import a comma-separated values (CSV) file with the appliance identification data.

Use this task to manually add an appliance.

1. Select **Onboard** to open the **Onboarding Wizard**.
2. Select **Add Appliance** > **Add Appliance**.
   - To add individual appliances manually, select the **Serial Number** tab.
   - To download a sample CSV file, select **?** beside **Import CSV**. For more information about adding appliances using a CSV file, see Import CSV File on page 48.

   To manually add an appliance, select the **Serial Number** tab and provide the following information:
   - Select an existing site.
   - Select an existing appliance template.
   - Provide the appliance name.
   - Provide the appliance serial number.
3. Select **Save**.
4. Select **Next - Review Configuration**.

   The different models of provisioned appliances appear with their serial numbers.

5. Select **Next - Deploy Configuration**.

   Note

   - To later edit the appliance configuration, go to **Appliances** from the main menu.
   - The appliance attempts to connect to the ZTP server automatically. The default ZTP server is:

     ```
     https://ztp01.extremecloudiq.com/api
     ```

     If the appliance does not connect within a few minutes, verify the following:

     - The ZTP server URL is correctly configured on the appliance.
     - The ZTP server is reachable from the appliance's network environment.

Related Links

Import CSV File on page 48
Edit the Appliance Configuration on page 62
Appliance Templates on page 25
Add Sites on page 46

Import CSV File

Before you can add an appliance to the network, you must have configured a site and an appliance template. While adding the appliance to the network, you are prompted to associate the appliance to a site and an appliance template.

Use this task to add multiple appliances by importing a CSV file.

1. Select **Onboard** to open the **Onboarding Wizard**.
2. Select **Add Appliance** > **Add Appliance**.
3. Select the **?** beside **Import CSV** to download a sample CSV file.
4. Provide the appliance name and serial number for each appliance in the downloaded CSV file.
5. Save the CSV file locally.
6. Select **Import CSV**, then select the **Choose File** field.
7. Navigate to the completed CSV file and select **Open**.
8. Select **Import Appliances**.
9. Select **Next - Review Configuration**.

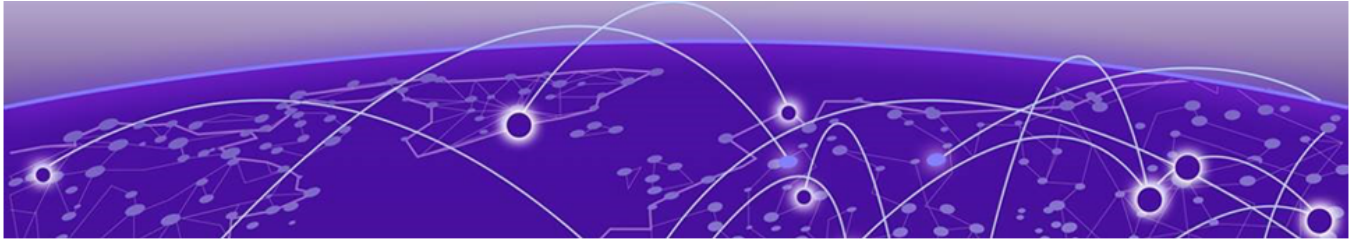
   The system lists the different models of provisioned appliances, along with their serial numbers.

10. Select **Next - Deploy Configuration**.

Note
To later edit the appliance configuration, go to **Appliances** from the main menu.

Related Links

Add Appliances on page 47
Edit the Appliance Configuration on page 62
Appliance Templates on page 25
Add Sites on page 46



Configuring Fabric over SD-WAN

Fabric Support is a feature that simplifies the management and connectivity of the networks. It offers network setup with zero touch deployment. With this feature, Extreme Fabric Switches automatically establish Fabric Extend tunnels over the SD-WAN infrastructure.

Related Links

Fabric Support on page 50
Appliance Configuration on page 17

Fabric Support

Use the following task to enable Fabric Support and configure Fabric Support over SD-WAN.

1. Navigate to **Settings** > **Policy Configuration**.
2. Select **Edit**.
3. **Fabric Support**: Enable or disable the Fabric support based on the operating mode. For more information, refer to Fabric Connect.

   Fabric Support is enabled by default, slide the Fabric Support toggle to disable. Disabling permanently resets parts of the configuration, including:

   - Fabric switch LAN IP addresses and Fabric switch AS in the appliance configuration
   - IS-IS metrics in the appliance configuration
   - Local Breakout settings
4. **Fabric Extend IP Network:** In the **Fabric Extend IP Network** field, enter the IPv4 address for the global subnet. This IPv4 address automatically allocates subnets to each LAN interface.
5. **Export Management IP Address:** Select **Export Management IP Address** to export the management IP address for SSH on LAN.
6. **Fabric Local Breakout Settings:** Local breakout settings are disabled by default. You can also enable or disable local breakout for individual appliances, see Policy settings.

   a. Select Fabric Local Breakout Settings to expand the section.

b. Add prefixes that are required for local breakout. These are destination IPv4 addresses to which traffic needs to break out locally.
   - To add a prefix, type the prefix address and select **Add Prefix**.
   - To remove a prefix, select the delete icon next to the prefix.

   Note
   Internet prefixes are configured as static-network routes on SD-WAN appliances regardless of whether local breakout is enabled or not.

c. **Configure the IP Connectivity Tracker**: The IP connectivity tracker enables the SD-WAN solution in fabric mode to verify internet connectivity for local breakout traffic.
   - Target: IPv4 Target IP address to check the Internet reachability
   - Retry: Retry count (default 3)
   - Interval: in seconds (default 10)

Limitations of the LBO Setting:

- Static Internet Prefixes: Internet prefixes are configured as static routes on SD-WAN appliances, even if local breakout is disabled.
- Export Management IP Behavior: The Export Management IP Address option are enabled independently of the local breakout setting. However, if local breakout is disabled, the BGP session with the Fabric Edge (FE) device will not be established. As a result, the exported management IP becomes ineffective for remote access from the FE side.
- Per-Appliance Export of Management IP: Exporting a unique management IP address for each appliance is currently not supported.
- IPv6 Support: The local breakout settings does not support pure IPv6 deployments.

Related Links

Appliance Configuration on page 17

Appliance Configuration

Select to display the **Appliances** page, or go to **Dashboard** > **Appliances widget**.

The Appliance Configuration dashboard enables you to quickly check and modify the configuration of the SD-WAN appliances used with Fabric Support.

For more information about appliance configuration settings, refer to Edit the Appliance Configuration on page 62.

Related Links

Fabric Support on page 50
Configuring Fabric over SD-WAN on page 50

Applications

Select  to display the **Applications** page or go to **Dashboard** > **Applications** widget.

The graph shows key application flow metrics across a selected time period. Use this graph to monitor performance trends and correlate metrics in real time or over historical intervals.

The graph includes the following metrics:

- **Throughput** (blue line) – Shows the data transfer rate for the selected application flow.
- **Raised Alert** (yellow line) – Highlights any alerts triggered during the selected time frame.
- **EQS** (purple line) – Plots the Experience Quality Score, which reflects the perceived application quality on a scale from 0 (poor) to 10 (excellent).

Time Range Selector To specify the range and span of the **Timeline** graph:

- Select a **Time Range** period: **Last Day (default)**, **Last Week**, **Last Month**, **Custom**.
- Select a **Time Span**.

  Available time span options appear, according to the chosen time range, to the right of the **Time Range Selector**. Select from the following time span options: 5 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

Use the Custom time filter to select a specific date and time range. Hover over a point on the timeline to view the corresponding metric values. Select **Reset** to return to the default time window.

Note
Flow data is polled from appliances at 1-minute intervals and then processed and stored in the orchestrator database. The user interface refreshes at one minute intervals. Because of this processing delay, the timeline begins 2 minutes behind the current time. Therefore, the most recent two minutes of data may not yet be displayed.

Select **Hide Timeline** to collapse the graph.

Related Links

Applications Overview on page 53

Applications Tab on page 54
Application Flows on page 54
Application Performance on page 58

Applications Overview

The Overview dashboard provides a comprehensive view of application performance and traffic patterns. Select the filter icon to refine the data displayed on the application dashboard. The filter panel allows you to narrow the results based on specific criteria so you can focus on relevant application traffic and performance metrics.

Top 10 Volume per Application and Application Performance Policy

This bar chart highlights the top 10 applications and application performance policy based on the total data volume generated or consumed during the selected time range. This identifies individual applications that are added in the Application Performance Policy.

Throughput

This line chart displays how traffic throughput changes over the selected time range.

- **Application Performance Policy:** Shows the collective throughput of grouped applications to assess overall group performance.
- **Criticality**: Highlights traffic trends based on the assigned criticality such as Top, High, Medium, Low.
- **Top 10 Applications**: Breaks down the throughput based on the value of the throughput per application.

Lowest 10 EQS per Application and Application Performance Policy

This bar chart highlights the lowest 10 applications and application performance policies based on Experience Quality Score during the selected time range. It helps identify applications with poor network performance and those included in an Application Performance Policy.

EQS Per

- **Application Performance Policy**: Displays EQS per policy to assess overall group performance.
- **Criticality**: Categorizes applications based on their assigned priority.
- **Worst 10 Applications**: Identifies the applications with the lowest EQS, helping diagnose performance issues and optimize network configurations.

Related Links

Applications Tab on page 54
Application Flows on page 54
Application Performance on page 58

Applications Tab

The **Applications** tab provides a detailed view of all detected applications in the network with the following column information:

- **Application:** Name of the application
- **Category:** Application groups based on their functionality.
- **Protocol:** The protocol used by each application.
- **Sites:** Indicates the network sites where the application traffics are detected.
- **Active Sessions:** -The cumulative number of sessions opened for the application for the selected time interval.
- **Total Volume:** The total amount of data consumed or generated by the application.

Related Links

Application Flows on page 54
Application Performance on page 58

Application Flows

The **Application Flows** tab provides detailed visibility into all active application flows within the network. It helps you to monitor, analyze, and manage application traffic in real-time. Table 12 describes the Application Flows tab columns on this tab.

Note
If the Application Flows table does not appear, try hiding the timeline or reducing browser zoom to 90-95%. This may occur on 1920×1080 displays with 125% browser scale.

Table 14: Application Flows Columns

Column	Description
Search and Filter Options	
Search Field	Find specific flows by typing the name of the flow or application.
Filters	Apply filters for precise analysis: • **Local Site:** Select the originating site. • **Remote Site:** Specify the destination site. • **Application Performance Policy:** Flows associated with a particular group. • **Application:** Filter by individual application names.

Table 14: Application Flows Columns (continued)

Column	Description
EQ Score Slider	Adjust the **EQ Score** slider to filter flows within a specific quality range. Drag the left or right handles to set the minimum and maximum EQ Score, refining the displayed results based on the associated score colors. The EQ Score ranges from 0 - 10. Zero, indicating extremely poor quality, and ten, indicating excellent quality. The score is color-coded to indicate quality levels: • **Green**: Excellent • **Yellow**: Degraded • **Red**: Poor **Note:** EQS interpretation is based on typical parameters. Actual experience may vary depending on user sensitivity and Application SLA configuration. When EQS degrades or drops, the system highlights the affected metrics delay, jitter, or loss using the same color. This helps you identify whether the flow missed its performance objectives (yellow) or exceeded defined thresholds (red). The system sets EQS to 100 when it cannot compute the score. This happens when: • The system classifies the flow as real-time, and the bandwidth objective is either not applicable or not met. • The system cannot measure delay, jitter, or loss for the flow. • The flow uses UDP, or the application SLA disables RTT, TCP retransmissions, and SRT metrics.
Topology	
Local Site/App/WAN	Displays the local site, application, and the specific WAN interface from where the traffic is coming out.
Direction	Direction of the flow: outgoing (the local Site is the source) or incoming (the local Site is the destination).
Remote Site/App/WAN	Displays the remote site, application, and WAN details for the destination. Select the names to view the flow information for the specified site and time range.
EQS	Displays the Experience Quality Score of the flow.
Classification	
Application Performance Policy	Name of the application group where the flow is classified.
Application	Name of the application.
Criticality	Criticality level of the flow, Top, High, Medium or Low.
LAN	

Table 14: Application Flows Columns (continued)

Column	Description
Throughput (kbps)	**LAN Throughput (kbps)**: Amount of data transmitted per second at the IP layer. **LAN Goodput (kbps)**: Volume of useful data received at the application layer on the downstream path. This includes only the payload of TCP and UDP packets. Retransmitted, out-of-sequence, and lost packets are excluded. **Note:** LAN Goodput is not reported in the current release.
Sessions	Number of sessions, represented by the average activity for the duration of the Correlation Record (by default: T = 1 minute). For example, 1 session running during T plus 1 session running during half this period gives 1 + 0.5 = 1.5 session. A session is identified by the following parameters: • TCP or UDP: source address, destination address, protocol (TCP or UDP), source port and destination port. • Other protocols over IP, for example ICMP: source address, destination address, protocol.
Loss (%)	Packet loss rate measured between the LAN port of the source appliance and the LAN port of the destination appliance.
Delay (ms)	One-way delay measured between the LAN ports of the source and destination appliances. Displays Min, Avg, and Max values.
WAN	
Throughput (kbps)	Amount of data transmitted per second at the IP layer over the WAN interface.
Loss (%)	Packet loss rate measured between the WAN port of the source appliance and the WAN port of the destination appliance.
Delay (ms)	One-way delay measured between the WAN ports of the source and destination appliances. Displays Min, Avg, and Max values.
Jitter (ms)	Variation in one-way delay between the WAN port of the source appliance and the WAN port of the destination appliance.
TCP	
SRT (ms)	Server Response Time (SRT) measures the delay between the last request packet and the first server acknowledgment, indicating application responsiveness.
RTT (ms)	Round Trip Time measures the total time required to establish a TCP connection.

Table 14: Application Flows Columns (continued)

Column	Description
Retransmission (%)	Percentage of TCP retransmissions.
Actions	Select to view the real-time graph for the selected flow. Real-Time Graphs are available only when the 5 mins timeline is selected. Selecting any other timeline window disables RTG.

Real-Time Graphs

You can open a real-time graph from any flow listed in the Application Flows table. You can open real-time graph windows for up to six different flows at once. Opening multiple windows for the same flow still counts as one real-time graph session. If an real-time graph window remains idle, the appliance automatically stops the session after three hours. Each real-time graph window includes source and destination details such as:

When launched, the graph appears blank and starts populating data within 10–20 seconds.

Note
Ensure your browser allows pop-up windows, or the RTG window may not open.

Each real-time graph window contains **Overview**, **LAN**, **WAN**, and **TCP** tabs. Table 13 describes the information available in each tab of the real-time graphs:

Table 15: RTG Tabs and Metrics

Tab	Graphs	What is shown
Overview	Avg. Delay (ms)	Average LAN-to-LAN (blue) and WAN-to-WAN (orange) delay
	Packet Loss (%)	LAN-to-LAN (blue) and WAN-to-WAN (orange) packet loss
	Avg. Sessions	Average number of sessions
	Throughput (kbps)	LAN-to-LAN (blue) and WAN-to-WAN (orange) throughput
LAN	Delay (ms)	LAN-to-LAN max (red), average (blue), and min (green) delays
	Packet Loss (%)	LAN-to-LAN packet loss
	Jitter (ms)	LAN-to-LAN jitter
	Throughput (kbps)	LAN-to-LAN Layer 3 (blue) and Layer 4 (green) throughput

Table 15: RTG Tabs and Metrics (continued)

Tab	Graphs	What is shown
WAN	Delay (ms)	WAN-to-WAN max (red), average (blue), and min (green) delays
	Packet Loss (%)	WAN-to-WAN packet loss
	Jitter (ms)	WAN-to-WAN jitter
	Throughput (kbps)	WAN-to-WAN Layer 3 throughput
TCP	SRT (ms)	Server Response Time: max (red), average (blue), and min (green)
	RTT (ms)	Round Trip Time: max (red), average (blue), and min (green)
	Retransmission (%)	TCP retransmissions
	Throughput (kbps)	TCP Layer 3 (blue) and Layer 4 (green) throughput

Use these real-time insights to monitor quality and diagnose performance issues as they occur across LAN, WAN, and TCP layers.

Application Performance

Application Performance provides detailed insights into application traffic metrics to help monitor, analyze, and optimize network performance.

Average Sessions

This tab displays data on the number of active sessions for applications or application groups over a selected time range.

- Displays the average number of concurrent sessions for each application.
- Identifies trends in session activity to understand the behavior and application load.
- Monitors peak session counts to ensure network resources are appropriately allocated.

Throughput

This tab provides real-time and historical data on application throughput, measuring the volume of data transferred for applications or application groups.

- Displays throughput metrics in Mbps or Gbps for specific applications.
- Identifies high-bandwidth applications that impact network performance.

You can filter throughput data by **Application**, **Application performance policy**, **Criticality**, **Local Site**, **Remote Site** or **Local WAN Service**, **Remote WAN Services** for granular analysis.

Delay & Jitter

This tab displays data on the variability in packet delay, which impacts real-time applications like VoIP.

- Displays the delay and jitter metrics to monitor performance consistency.
- Identifies fluctuations in packet timing that can affect voice and video quality.
- Monitors trends to ensure that the real-time applications maintain optimal performance.

Packet Loss

This tab provides insights into the percentage of packets lost during transmission, which affects data integrity.

- Displays packet loss metrics to identify potential network issues.
- Highlights trends in packet loss to diagnose recurring transmission problems.
- Monitors loss rates to ensure the data-sensitive applications perform effectively.

RTT & SRT

This tab displays data on the responsiveness of network connections and applications.

- Displays Round Trip Time (RTT) and Session Response Time (SRT) metrics to assess connection quality and application responsiveness.
- Identifies latency patterns that may indicate network congestion or performance bottlenecks.
- Monitors trends to optimize application performance and user experience.

Packet Retransmission

This tab tracks the number of packets that need to be resent due to errors, affecting network efficiency.

- Displays retransmission rates to identify potential reliability issues.
- Highlights areas with frequent retransmissions, which may indicate network congestion.
- Monitors trends to minimize the impact on latency and throughput.

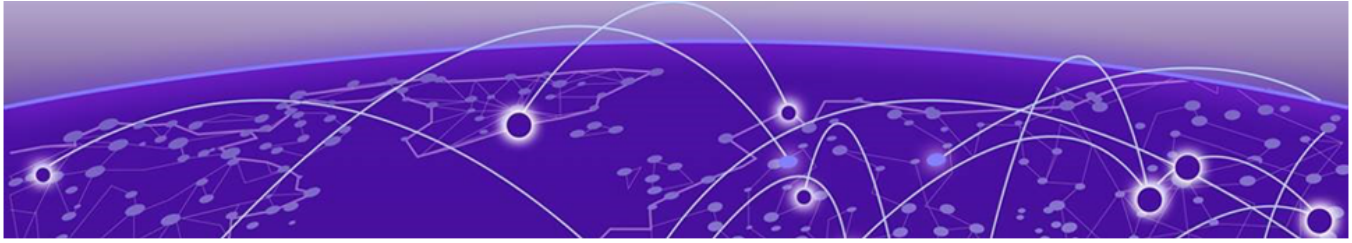
EQS

This tab provides an aggregated score reflecting the overall quality of service.

- Displays End-to-End Quality Score (EQS) metrics that combine delay, jitter, packet loss, and throughput.
- Identifies service quality trends to ensure SLA compliance.

Related Links

Application Flows on page 54



Appliances

Select to display the **Appliances** page, or go to **Dashboard** > **Appliances widget**.

Related Links

Edit the Appliance Configuration on page 62
Appliance Overview on page 60
Upgrade the Firmware for an Appliance on page 71
Access the Remote Console Shell on page 72
Access Advanced Troubleshooting Mode on page 73
Tech Support File on page 82
Swap the Appliance on page 83

Appliance Overview

The **Overview** table displays the appliances of your network with the following column information:

- **Appliances:** The name of the appliance.
- **Sites:** The associated site.
- **Appliance State:** If Managed, the appliance is managed by ExtremeCloud OS ONE SD-WAN. If the appliance is Unmanaged, it is not configured/deployed and there is no traffic routing, nor monitoring or alarming. The appliance license is not consumed.
- **Status:** Connected or disconnected in the network.
- **Fabric LLDP Signaling:** Indicates whether LLDP including Fabric Extend TLVs is received or not (due to missing configuration, LLDP exception, etc.). Available only if Fabric Support is enabled.
- **Configuration Status:** Indicates if the configuration is applied to the appliance.

- **Serial Number:** Device serial number
- **Firmware:** Firmware build number.
- **Firmware status:** Provides real-time visual feedback on the firmware upgrade state of each appliance. You can schedule upgrades for appliances independently of one another. A scheduled upgrade can be canceled at any time, provided the upgrade has not yet started. The status is represented using both progress bars and icons:
  - : Available for firmware upgrade
  - : Scheduled for firmware upgrade and will start at the defined time.
  - : Firmware upgrade is in progress. A progress bar indicates the percentage completed.
  - : Firmware upgrade has failed
- **Management IP:** Management IP address
- **Template:** The appliance template that is associated with the appliance.
- **Last update:** Last date the appliance was updated.
- **Action:** Available actions for the appliance, such as **Delete**.

Note
Select a column header to sort data in that column.

Appliance Details

From the **Overview** table, select the **Appliance Name** to show more details:

- The left pane of the window is a summary of the appliance configuration and policy. See the following topics:
  - Edit the Appliance Configuration on page 62
  - Appliance Templates on page 25
  - Policy Settings on page 22
- The **Fabric Support** summary contains Fabric Switch information and status as well as Peering information. You can also view the corresponding Fabric Engine page from ExtremeCloud IQ Site Engine.

  Select the **Peers** link to display the **Peering Status** table.

  Use the **Peering Status** table to monitor the state of Vxlan tunnels (Fabric Extend tunnels). Via the Remote SD-WAN Appliance name, IPSEC or MPLS connectivity state, Fabric Switch name and IS-IS adjacency state, you can monitor the state of Vxlan tunnels without using another tool, such as ExtremeCloud IQ Site Engine.
- - Go to **Managed by** > **Application** and select the **XIQSE** link to display the appropriate device page of ExtremeCloud IQ Site Engine.
  - See the *ExtremeCloud IQ SE documentation*.

On the map, a red flag represents the appliance location. All Appliance connections display the number of existing alarms. Select the **Alarms** widget to view alarm details. See Alarms Management on page 102.

- Select the **Connection Details** to display the connection details. For example, the overlays with their connection status, their destination site, and the destination appliance/interface. You can download this information as an `Appliance_Connection_Data.csv` file.

The lower panel summary displays the number of appliance interfaces with their throughput and CPU Usage.

Related Links

Upgrade the Firmware for an Appliance on page 71
Access the Remote Console Shell on page 72
Advanced Troubleshooting Information on page 73
Swap the Appliance on page 83

Edit the Appliance Configuration

All appliances receive their basic configuration from the associated appliance template. All appliances must be associated with a template. However, there are mandatory settings that must be manually configured for each appliance because the values are unique to the appliance.

Use this task to finish the configuration of your appliances.

1. Go to **Appliances** on the main menu.

   All your provisioned appliances appear in the list with their names, configuration statuses, assigned sites, serial numbers, and MAC addresses.
2. Select an appliance.

   The appliance landing page opens and provides the following information:

   - **Appliance State and Details**: Displays appliance name, site, model, serial number, firmware version, and management IP.
   - **Fabric Support**: Displays the associated fabric switch information, including the host name and MAC address.
   - **Peering Information**: Displays the overlay peering status, uptime, number of advertised peers, and the number of peer up/down events.
   - **Managed By:** Displays the management application and IP address.
   - **Appliance Status:** Displays operational information, including appliance uptime, orchestrator connection status, configuration synchronization status, the last configuration update time, and time synchronization status.
   - **Appliance Connections Map**: Displays the appliance's geographic location, connection role (Hub or Spoke), and alarms.

- **Interfaces**: Lists LAN and WAN interfaces with current throughput.
- **Appliance Usage Overview**: You can select:
  - **Status**: Displays the current real-time usage values such as
    - CPU Usage: Displays the current percentage of CPU resources utilized by the appliance. Monitoring CPU usage helps identify processing load and performance bottlenecks.
    - Memory Usage Percentage: Displays the percentage of system memory currently in use. High memory usage may indicate heavy workloads or memory-intensive processes running on the appliance.
    - Temperature: Displays the average temperature reading from all thermal sensors on the appliance. Monitoring temperature ensures the appliance operates within the recommended thermal range and helps prevent overheating.
  - **Trend**: Displays usage trends over the last 24 hours, including maximum CPU and memory usage values.

3. Select **Edit Configuration**.
4. Configure the following settings:

Note
Do not change values that are assigned by the template. Modifying template settings overwrites the configuration of the template and a message informs you that the current appliance is no longer associated with any template.

Table 16: Appliance Configuration Settings

Settings	Description
General Settings	
Managed State	Specifies that the appliance is managed by ExtremeCloud OS ONE SD-WAN. **Note:** Changing an appliance to the unmanaged state is similar to resetting the appliance to its default configuration: SD-WAN tunnels are closed, traffic routing is stopped as well as appliance monitoring and alarming. The appliance license is no longer consumed.
Appliance Name	You can change the name of the appliance.
Site	You can change the site that the appliance is associated with.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
Template	You can change the appliance template that the appliance is associated with. **Note:** If you select another template, all default settings are updated according to the default configuration of the new appliance template. All the other settings are extracted from the applied template.
Local AS	Set the Local AS to **Auto** (default) or provide a specific value. When set to Auto, the orchestrator assigns the next available AS number from the General Settings AS Number Range when BGP is first enabled at the site. All appliances at the same site share the same AS number. Users can override the auto-assigned value if needed.
Path Mode	Dynamic Path Mode is only supported.
Hub & Spoke	As a best practice, do not modify this setting. This setting affects all the tunnel relationships in your network configuration. Use caution.
Adaptive Qos	Detects WAN-to-LAN congestion and applies traffic shaping on the remote link. For more information, see Adaptive QoS Overview on page 32.
Internet Backhauling	Select this option to identify the appliance as a Backhauling Site.
LAN	
VLAN	Defines a logical network segment that groups a subset of devices within the same physical LAN to isolate and manage network traffic efficiently.
IP Interfaces	SD-WAN OS ONE defaults to Fabric mode. DHCP does not apply. **Prefix Length**: Defines the subnet mask for the LAN IP. Default: 24. **LAN IP**: Specifies the primary LAN interface IP address. Default: 10.0.0.1 **Fabric Switch LAN**: The Fabric Switch LAN IPv4 address is used as the Fabric Extend tunnel source IP address.The system automatically generates this value based on the global subnet defined during Fabric Support activation. You can modify this address. **Fabric Switch AS**: Defines the Autonomous System Number (ASN) for the Fabric Switch. **Default IS-IS Metric**: Optional metric for IS-IS routing configuration.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
Remote Fabric Extend Tunnel Endpoints	Displays information about remote endpoints in the Fabric Extend tunnel. • **Site**: The name of the remote site. • **IP Address**: The IP address of the remote appliance. • **Remote Appliance**: The hostname or identifier of the remote appliance. • **IS-IS Metric**: The default IS-IS Metric value applied to the Fabric Extend tunnel. You can choose to modify the IS-IS Metric value for both the local and remote appliances if needed.
Advanced Settings	
LAN Interface Speed	Set to **Auto** by default to let the system define the speed of the LAN interfaces, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
MTU	Enter the MTU value that corresponds to the maximum number of bytes loaded in the payload. The default value is 1500. Supported range: 1280 to 9194.
DNS Server Settings	**Apply Default Policy Settings** Enable this option to automatically apply predefined system default policy settings. **DNS Server Settings** Define DNS resolution behavior for the appliance by specifying up to three DNS server IP addresses under **Servers**. If you do not specify a DNS server, the system uses the DNS server provided via DHCP. When DNS server settings are disabled, the system enables auto via DHCP as backup by default.
Fabric Settings	
Fabric Local Breakout Settings	Fabric Local Breakout Settings are disabled by default. Disable Apply default policy settings to expand the Fabric Local Breakout for the individual appliance.
Static Route	A static route is a manually defined path that directs traffic to a specific network or host. It remains fixed and is commonly used for predictable routing in stable environments.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
Parameters	• **Prefix:** Destination network address. • **Prefix Length:** Subnet mask length of the destination. • **Next Hop:** IP address of the next forwarding device. To add a static route, select **Add Static Route** and enter the required parameters.
Subnet	A subnet is a logical segment of a larger network. Subnets help organize and route traffic efficiently within the SD-WAN fabric. You can define the subnet in the following ways: • **Subnets from VLANs**: ◦ **Prefix**: The network address. ◦ **Prefix Length**: The subnet mask length in bits. • **Subnets from Static Routes**: ◦ **Prefix**: The destination network address. ◦ **Prefix Length**: The subnet mask length in bits. • **Additional Subnet**: ◦ **Prefix**: The manually defined network address. ◦ **Prefix Length**: The corresponding subnet mask length. Use additional subnets to extend routing or to support network segmentation beyond VLAN or static route definitions.
WAN	
WAN 1, WAN 2, WAN 3	Select a WAN interface tab to view and configure WAN settings. The mode and IP address range for the selected WAN is indicated. Valid values for IP address range are: IPv4 or IPv6. These values cannot be changed. If you are using WAN4 LTE interface, see LTE (WAN4) Interface Configuration on page 34 for additional configuration options.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
Enabled	Enable or disable the WAN interface. • Enabled: Select to activate the WAN interface and allow the system to use the interface for WAN connectivity and traffic forwarding. • Disabled: Clear the option to deactivate the WAN interface. When disabled, the interface is not used for traffic forwarding or path selection. When a WAN interface is disabled, the appliance does not establish overlay tunnels or BGP sessions on that interface. If you configure VRRP object tracking to monitor this interface, the system adjusts the VRRP priority accordingly, potentially triggering a failover.
Interface	
Description	Optional description of the WAN.
Bandwidth Up and Down	• Bandwidth Up: Maximum upload bandwidth in Mbps. Default: 10000. • Bandwidth Down: Maximum download bandwidth in Mbps. Default: 10000.
Interface Speed	Set to **Auto** by default to let the system define the speed of the WAN interfaces, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
MTU	Enter the MTU value that corresponds to the maximum number of bytes loaded in the payload. The default value is 1500.
TCP MSS Adjustment	Enable or disable TCP MSS adjustment to optimize packet transmission efficiency and prevent fragmentation across WAN links. Select one of the following options: • No Adjustment: Keeps the TCP MSS value unchanged. • Adjusted MSS: Adjusts the MSS value for TCP packets. Enter a value between 536 and 1460 bytes. Values outside this range are not allowed. The default value is 1300.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
WAN Service	Defines the type of WAN connectivity for this interface. This affects how the orchestrator builds overlay tunnels. • **Internet**: Standard Internet connection. Supports overlay tunnels and DTI breakout. • **MPLS**: Private MPLS circuit. Supports site-to-site tunnels only. DTI is not available. • **Internet**: Broadband connection. To create a WAN service, select **Create WAN Service** and provide the **WAN Service Name** and **Description**.
VLAN ID	Specify the VLAN identifier used for tagged traffic on the WAN interface. When you configure a VLAN ID, the system processes incoming packets with the specified VLAN ID and tags outgoing traffic from the WAN interface with the same VLAN ID. Use this option when the upstream network requires VLAN-tagged traffic for WAN connectivity. **Note:** If you configure a VLAN interface through the CLI, the appliance uses that interface to obtain an IP address through DHCP and connect to the orchestrator. After the appliance connects, the orchestrator deploys the configured settings, which may overwrite or modify the CLI configuration on the appliance.
DTI	Select this option to allow traffic out to the Internet through this WAN interface. • **Enabled** — Traffic matching DTI policies exits directly to the Internet through this WAN interface without traversing the overlay. **NAT** is automatically applied to outbound DTI traffic. A stateful firewall is activated, allowing only return traffic for connections initiated from within the LAN. • **Disabled** — All traffic is forwarded through the SD-WAN overlay tunnels regardless of destination. No local Internet breakout occurs on this interface. **Note:** These values are inherent from the appliance template. You can override these settings if necessary. However, after you override a template setting, the appliance no longer uses the template settings for this WAN interface.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
LLDP Settings	Enable or disable Link Layer Discovery Protocol on this WAN interface. LLDP allows the appliance to advertise its identity and discover neighboring devices on the WAN link. When Enabled, LLDP packets are sent and received on this interface. LLDP Settings is not available for WAN 4 (USB).
IP Addresses	
Tunnel Underlay IP Address	• Public IP Address • WAN Interface IP Address If Public IP Address is selected: • Configure the port forwarding of the internet access router to send UDP packets to the appliance's WAN on port 500 (IKEv2) and port 4500 (IPsec NAT Traversal). • If the appliance is a hub, a Public IP address is mandatory. If the appliance is a spoke, a Public IP address is optional unless there is a need for a site-to-site tunnel.
WAN Interface IP Address	• IPv4 — Enable or disable DHCP • IPv6 — Enable or disable IPoE **Note:** In Appliance 360, if DHCP or IPoE are not enabled, the user must manually configure the IP addresses. The default values for Tunnel Underlay and WAN Interface IP Address depend on the selected IP address range. For more information, see WAN Interface IP Address on page 33.
Routing	
Routing Settings	Configure BGP and BFD settings for overlay tunnels on this WAN interface. • **Default BGP Local Preference**: BGP Local Preference value applied to all overlay tunnels on this WAN interface. Higher values indicate a more preferred path. This can be overridden at the per-tunnel level. Default: empty (system default of 100 is used). • **BFD Transmit Interval**: Interval in milliseconds between BFD keepalive packets sent over overlay tunnels on this WAN interface. Lower values detect failures faster. Range: 50 - 30,000 ms. Default: 1000. • **BFD Multiplier**: Number of consecutive missed BFD packets before declaring the session down. Range: 3 - 50. Default: 7. The settings apply to all overlay BGP sessions on this WAN interface.

Table 16: Appliance Configuration Settings (continued)

Settings	Description
Tunnels	
Overlay	Define and customize the network tunnels: Select an Overlay you previously created and apply it to the interface. Select **Configure Tunnel** to view the Overlay Details. Refer to Define a Hub and Spoke Overlay on page 42.
Security Gateway	Select a previously created Security Gateway and apply it to the interface. You can edit and customize the selected gateway from this panel. **External Secure Web Gateway:** Displays the name of the selected gateway. Select **Configure Tunnel** to modify the overlay settings and update any parameters. **Note:** Secure web Gateway cannot be added in the IPv6 mode
Site to Site Tunnels	To create a tunnel between two sites, select **Add Site-to-Site Tunnels**. Select the following setting values from the field stacks: • Remote Site • Remote Appliance • Remote WLAN Interface • Overlay Select **Add Tunnel**. Use the configure tunnel function to modify the **BGP Local Preference** setting or select another **Overlay**. Update the configuration.

5. After you have configured all your appliances, select **Save**.
6. To send your appliance configurations to the system, from the **Appliances** window, select **Deploy Configuration**.

Note
If a configuration update causes the appliance to lose connectivity with the orchestrator, the appliance automatically rolls back to the previous running configuration. This mechanism ensures that the appliance restores orchestrator connectivity and remains manageable. Before applying a configuration update, the appliance automatically saves a backup of the current configuration.

7. From the main menu, select **Dashboard**.

   Google Maps displays your sites and associated appliances on the map.

Related Links

Appliance Template Settings on page 25

Define a Hub and Spoke Overlay on page 42

Apply Hub and Spoke Overlay to Appliances on page 44
LTE (WAN4) Interface Configuration on page 34
Adaptive QoS Overview on page 32

Upgrade the Firmware for an Appliance

Use this task to upgrade the firmware for an appliance.

1. Go to **Appliances**, or to the **Appliance Details** page.
2. Select an appliance from the list.
3. Select **Utilities** > **Firmware Upgrade**.

   The **Device Firmware Upgrade** dialog opens.
4. The device firmware upgrade window allows you to upgrade firmware on one or more selected appliances. You can choose the firmware version and schedule the activation based on your requirements.
   a. Firmware Upgrade Options: You can select one of the following options:
      - **Upgrade to the latest version**: Installs the most recent firmware available. The version number is displayed next to the option.
      - **Upgrade to a specific version**: Enables you to select a previously available version, if applicable. This option is disabled if no previous versions are available.

   b. Schedule Activation: Specify the activation time for the upgrade:
      - **Activate Immediately**: Applies the firmware upgrade as soon as the upgrade process is triggered.
      - **Activate at a specific time**: Allows you to schedule the activation for a future time window. Use this option to avoid service interruptions during peak hours.
5. Select **Upgrade Device**.

Cancel Upgrade Schedule: You can cancel a previously scheduled firmware upgrade for the selected appliance. This option is only available when a future upgrade schedule is active.

Note
IPE appliances version 30.26.2.x cannot be downgraded directly to version 30.25.x. If a downgrade is required, first downgrade the appliance to version 30.26.1.0, and then downgrade to the required version 30.25.x. XSE-600 appliances cannot be downgraded to a version earlier than 30.26.2.1.

Related Links

Appliance Overview on page 60
Access the Remote Console Shell on page 72
Advanced Troubleshooting Information on page 73
Swap the Appliance on page 83

Access the Remote Console Shell

ExtremeCloud OS ONE SD-WAN offers a remote console that you can open on an appliance.

- You can start sessions for up to four appliances concurrently, but only one session per appliance.
- The commands available in the Remote Console depend on the user's access rights.

Note
Before you can log into the appliance through remote console, you must configure a default password.

1. Go to **Settings**.
2. Next to the **General** settings, select .
3. Scroll down to **Application Management Settings**.
4. Enter a default password for the appliance and confirm it.

Use this task to access the Remote Console shell.

1. Go to **Appliances**.
2. Select an appliance from the list.
3. Select **Utilities** > **Remote Console**.

   The **Remote Console** opens.
4. Type ? to display the list of available commands:
   - cat – show information
   - clear – Clear values
   - exit – Exit current mode and down to previous mode
   - list – Print command list
   - ls – List disk files
   - ping – Ping
   - quit – Exit current mode and down to previous mode
   - show – Show system information
   - terminal – Set terminal timeout parameters
   - traceroute – Traceroute

Related Links

Appliance Overview on page 60
Advanced Troubleshooting Information on page 73
Swap the Appliance on page 83
User Access Levels in Remote Console on page 73

User Access Levels in Remote Console

- **Administrator/Operator Access:** Grants full control over appliance settings, including configuration changes, updates, and troubleshooting. Administrator users access the Admin Shell, which provides an extended set of commands.
- **Observer Access:** Provides read-only access, allowing users to monitor appliance settings and performance without making modifications. Observer users access a restricted shell with limited commands.

Note
Each shell has provisions to change its password.

Access Advanced Troubleshooting Mode

ExtremeCloud OS ONE SD-WAN offers advanced troubleshooting information.

Use this task to access advanced troubleshooting information.

1. Go to **Appliances**.
2. Select an appliance from the list.
3. Select **Utilities** > **Advanced Troubleshooting**.

The **Advanced Troubleshooting** page opens.

Related Links

Advanced Troubleshooting Information on page 73

Advanced Troubleshooting Information

Access **Advanced Troubleshooting** tools from the **Appliances** page. Go to **Appliances** > **Utilities** > **Advanced Troubleshooting**.

The **Advanced Troubleshooting** window organizes configuration information for a specific appliance into tabs and sections. The data collection process starts when you open the window.

The main settings of the selected appliance appear in the left margin of the window.

Last updated lets you know when the data display last refreshed. The counter blinks when the connection with the appliance is lost.

System Health

The **System Health** tab displays the following information:

- The current CPU usage in percentage and an evolution graph of CPU usage over the last 15 minutes
- The current RAM usage in percentage and an evolution graph of RAM usage over the last 15 minutes

- The current traffic received from and sent to the network in bits/s and an evolution graph of received/sent traffic over the last 15 minutes

The previous metrics refresh every 1 to 40 seconds, whereas the time span of the graph corresponds to the last 15 minutes with 1s to 5s data points.

Note
You can also refresh the data manually by clicking in the top right corner of the window.

Note
The curves that represent sent traffic on the Network graph and outbound traffic on the Disks graph are not negative. They display that way for distinctness.

In the legend, select the labels or values to display only specific curves. To enable or disable curve display, simultaneously press the **Shift** or **Ctrl** key and select a label or value.

The following sections include tables of data and no graphs.

- Network Interfaces
- Tunnels
- Routing
- Additional Services

You can filter table information by entering a filter in the top row of every column. Select a column heading to sort the information in that column.

Network Interfaces

The **Network Interfaces** tab displays operational information for the appliance's physical and logical network interfaces. Use this page to monitor interface status, traffic statistics, MTU settings, and packet errors for troubleshooting network connectivity and performance issues.

Physical Network Interfaces

Displays information about physical WAN and LAN interfaces for the appliance.

Table 17: Physical WAN and LAN Interfaces

Field	Description
Name	Name of the physical interface.
State	Operational state of the interface, such as **Up** or **Down**.
IP Address	IP address assigned to the interface.
MAC Address	MAC address of the interface.
MTU	Maximum Transmission Unit (MTU) configured on the interface.

Table 17: Physical WAN and LAN Interfaces (continued)

Field	Description
RX Bytes	Total number of bytes received.
RX Packets	Total number of packets received.
RX Errors	Number of receive errors.
RX Dropped	Number of received packets that were dropped.
RX Overrun	Number of receiver overrun events.
RX DF Dropped	Number of received packets dropped because the Don't Fragment (DF) bit was set.
RX DF Override	Number of packets processed after overriding the DF setting.
TX Bytes	Total number of bytes transmitted.
TX Packets	Total number of packets transmitted.
TX Errors	Number of transmit errors.
TX Dropped	Number of transmitted packets that were dropped.
TX Carrier	Number of carrier errors detected during transmission.
TX Collision	Number of packet collisions detected during transmission.

Logical Network Interfaces

Displays operational information for logical interfaces configured on the appliance.

Table 18: Logical Network Interfaces Settings

Field	Description
Name	Name of the logical interface.
State	Operational state of the interface.
IP Address	IP address assigned to the logical interface.
MAC Address	MAC address associated with the interface.
MTU	Maximum Transmission Unit (MTU).
RX Bytes	Total number of bytes received.
RX Packets	Total number of packets received.
RX Errors	Number of receive errors.
RX Dropped	Number of received packets that were dropped.
RX Overrun	Number of receiver overrun events.
RX Length	Number of packets with invalid length.
RX CRC	Number of packets received with CRC errors.
RX Frame	Number of frame errors detected.

Table 18: Logical Network Interfaces Settings (continued)

Field	Description
TX Bytes	Total number of bytes transmitted.
TX Packets	Total number of packets transmitted.
TX Errors	Number of transmit errors.
TX Dropped	Number of transmitted packets that were dropped.
TX Carrier	Number of carrier errors detected during transmission.
TX Collision	Number of packet collisions detected during transmission.

Select **Refresh** to update the displayed interface statistics. The L**ast Updated** field indicates when the information was last refreshed.

Tunnels

The **Tunnels** tab displays information about the IPsec tunnels and security associations established between the local appliance and remote peers. Use this page to verify tunnel connectivity and identify the interfaces and IP addresses used for each tunnel.

IPsec Tunnels & Security Associations

Displays information about the IPsec tunnels configured on the appliance.

Table 19: IPsec Tunnels & Security Associations Settings

Field	Description
Initiator Site	Site that initiates the IPsec tunnel.
Initiator Appliance	Name of the appliance that initiates the tunnel.
Interface	WAN interface used to establish the tunnel.
Inner IP	Internal tunnel IP address assigned to the IPsec tunnel.
Outer IP	Public IP address used to establish the IPsec tunnel.
Responder Site	Remote site that terminates the IPsec tunnel.
Responder Appliance	Name of the remote appliance.
Responder Interface	WAN interface on the remote appliance.
Responder Inner IP	Internal tunnel IP address assigned to the remote end of the IPsec tunnel.
Responder Outer IP	Public IP address of the remote appliance used for the tunnel.

Use the **Refresh** to update the displayed tunnel information. The **Last Updated** field indicates when the information was last refreshed.

Routing

The **Routing** section contains the sub-tabs: IP Routes, BGP, BFD and ARP/ND.

The table information on the Routing sub-tabs does not automatically refresh when you navigate from one sub-tab to another. This makes it easier for you to compare data within the same data collection. To refresh the information for all Routing sub-tab tables, select in the top right corner of the window.

You can filter routes by **VRF All** or **mgmt-vrf** and by protocol **IPv4** or **IPv6**.

IP Routes

The **IP Routes** displays the list of IPv4 and IPv6 routes for the selected VRF.

Table 20: IP Routes Settings

Field	Description
VRF Name	Name of the virtual routing and forwarding (VRF) instance.
Prefix	Destination network prefix.
Origin	Source of the route, such as **Static**, **OSPF**, or **BGP**.
Preference	Administrative preference of the route.
Metric	Cost associated with the route.
Tag	Route tag value.
Age	Time elapsed since the route was learned.
Via	Next-hop IP address or interface.

BGP

The **BGP** page displays routing and peer information for the appliance. Use this page to view BGP routes, monitor peer status, and troubleshoot BGP connectivity across the configured VRFs.

The **Route Summary** table displays the BGP routes learned by the appliance.

Field	Description
VRF Name	Name of the VRF associated with the route.
Prefix	Network prefix for the route.
Next Hop	Next-hop IP address for the route.
Peer	BGP peer that advertised the route.
Flags	Status flags associated with the route.
AS Path	Autonomous System (AS) path for the route.
Age	Time elapsed since the route was learned.
Local Preference	Local preference value assigned to the route.
MED	Multi-Exit Discriminator (MED) value for the route.

Field	Description
Communities	BGP community attributes associated with the route.
Extended Communities	Extended community attributes associated with the route.

The **BGP Peer Table** displays information about the configured BGP peers. You can filter **BGP** data by **VRF All** or **mgmt-vrf**.

Field	Description
Common Information	
VRF Name	Name of the VRF associated with the peer.
Local AS	Local Autonomous System (AS) number.
Router ID	Router identifier configured for the BGP process.
Graceful Restart	Indicates whether BGP graceful restart is enabled.
BGP Peer Table	
Peer Group	Name of the peer group.
Peer IP	IP address of the BGP peer.
Peer AS	Autonomous System (AS) number of the peer.
Local IP	Local IP address used for the BGP session.
State	Current state of the BGP session.
Up Time	Duration for which the BGP session has been established.
RIB IN	Number of routes received from the peer.
RIB OUT	Number of routes advertised to the peer.
Health	Health status of the BGP peer.
Flags	Status flags associated with the BGP peer.

BFD

The **BFD** page displays Bidirectional Forwarding Detection (BFD) peer information for the appliance. Use this page to monitor BFD sessions, verify peer connectivity, and troubleshoot BFD operation.

BFD Peer Table

The **BFD Peer Table** displays the status, timers, counters, and session information for each BFD peer.

Table 21: BFD Peer Table

Field	Description
Common Information	
VRF Name	Name of the VRF associated with the BFD session.
Local IP	Local IP address used by the BFD session.
State	Current state of the local BFD session.
Diagnostic	Diagnostic information for the local BFD session.
Peer Information	
Peer IP	IP address of the BFD peer.
State	Current state of the peer BFD session.
Diagnostic	Diagnostic information reported by the peer.
Local Timers	
Min TX	Minimum transmit interval configured for the local BFD session.
Min RX	Minimum receive interval configured for the local BFD session.
Multiplier	Detection multiplier configured for the local BFD session.
Peer Timers	
Min TX	Minimum transmit interval advertised by the peer.
Min RX	Minimum receive interval advertised by the peer.
Multiplier	Detection multiplier advertised by the peer.
Counters	
RX Count	Number of BFD packets received.
TX Count	Number of BFD packets transmitted.
Discriminator	
Local	Local discriminator that uniquely identifies the BFD session.
Peer	Peer discriminator associated with the BFD session.
Session	
Heard Peer	Indicates whether BFD packets have been received from the peer.
Session ID	Unique identifier for the BFD session.
Applied Profile	BFD profile applied to the session.
Request Profile	BFD profile requested for the session.

Table 21: BFD Peer Table (continued)

Field	Description
Registered Protocols	Protocols registered to use the BFD session, such as BGP.
Up Time	Length of time the BFD session has remained operational.

Note
A BFD session going Down triggers the associated BGP session to tear down immediately, enabling fast reroute to an alternate path. When this occurs, both a BGP Failure alarm and a BFD Failure alarm are raised. Both alarms auto-clear when the respective sessions return to Established (BGP) or Up (BFD) state.

ARP/ND

The **ARP/ND** page displays the Address Resolution Protocol (ARP) table for IPv4 and Neighbor Discovery (ND) table for IPv6 for the selected VRF. You can filter **ARP/ND** entries by **VRF All** or **mgmt-vrf** and by protocol **IPv4** or **IPv6**.

Table 22: Address Resolution Protocol (ARP) table

Field	Description
VRF Name	Name of the VRF.
IP Address	IP address of the device.
MAC Address	MAC address associated with the IP address.
Type	Type of ARP/ND entry, such as **Dynamic** or **Static**.
Interface	Interface through which the device is reachable.
L2 Interface	Layer 2 interface associated with the entry.
Age	Time elapsed since the entry was learned.

Additional Services

The **Additional Services** tab displays operational information for additional network services running on the appliance. Use this page to monitor IP probe status and verify LLDP interface and neighbor information for troubleshooting network connectivity and service availability.

The **IP Probes** page displays the status of IP tracker probes configured on WAN interfaces.

Field	Description
WAN Interface	WAN interface on which the IP probe is configured.
Target IP Address	IP address monitored by the probe.
Status	Current operational status of the IP probe.

LLDP

The **LLDP** page displays LLDP information for the appliance interfaces and neighboring devices.

The **Interface Summary** table displays LLDP configuration and operational information for each interface.

Table 23: Interface Summary

Field	Description
Interface	Name of the interface.
Status	Indicates whether LLDP is enabled on the interface.
Transmit	Indicates whether the interface transmits LLDP advertisements.
Receive	Indicates whether the interface receives LLDP advertisements.
Static Management IP	Static management IP address configured for the interface.
Suppressed TLVs	LLDP Type-Length-Value (TLV) information that is suppressed for the interface.
Fabric MTU	MTU configured for the Fabric interface.
Advertised IP	IP address advertised through LLDP.
Remote Appliance	Name of the discovered remote appliance.
Remote Status	Operational status of the remote appliance.
Fabric IP	Fabric IP address of the remote appliance.
IS-IS Metric	IS-IS metric advertised for the interface.
BGP Local ASN	Local BGP Autonomous System Number (ASN).
BGP Remote ASN	Remote BGP Autonomous System Number (ASN).
Local IP	Local IP address associated with the interface.

The **Neighbor Summary** table displays information about LLDP neighbors discovered by the appliance.

Table 24: Neighbor Summary

Field	Description
Chassis ID	Unique identifier of the neighboring device.
Local Port	Local interface connected to the neighboring device.
Dead Interval	Time before the neighbor information expires if no LLDP advertisements are received.
Remaining Life	Remaining time before the neighbor entry expires.
Remote Port ID	Identifier of the remote interface.

Table 24: Neighbor Summary (continued)

Field	Description
Remote Port Description	Description of the remote interface, if available.
System Name	System name of the neighboring device.

Tech Support File

With Tech Support File, you can generate and download diagnostic logs from one or more appliances. These files contain system, configuration, and performance data that assist in troubleshooting and support investigations.

Use this task to Access technical support files:

1. Go to **Appliances**.
2. Select an appliance from the list.
3. Select **Utilities** > **Tech Support File**.

Available Tech Support Files

The Tech Support File window lists all previously generated files for the selected appliances. Each file entry includes the following details:

Table 25: Tech Support Files

Column	Description
Time Created	The date and time the file is generated
Appliance Name	Name of the appliance associated with the file
Type	Indicates whether the file is created automatically (Auto) or manually (Manual)
Tech Support File	The filename assigned to the generated file
Size	The size of the file in megabytes
Actions	Options to download or delete the file

You can search for a specific appliance or file name using the Search box.

Generate Manual File

Use this task to manually create a new tech support file:

1. In **Tech Support File**, select the appliances for which you want to generate the file.
2. Select **Generate Manual File** > **Proceed**.

3. Wait for the generation process to complete.

Note
Collecting a tech support file is session-based. If you close the browser window during the process, the session ends and any ongoing actions such as file generation or download are aborted.

The new file appears in the Tech Support File list with the type marked as **Manual**.

Related Links

Swap the Appliance on page 83

Swap the Appliance

With **Swap Appliance**, you can replace an appliance during upgrades or RMA (Return Merchandise Authorization). This function transfers all settings including monitoring and alarms data from old to the new appliance.

Use this task to swap the appliance:

1. Go to **Appliances**.
2. Select an appliance from the list.
3. Select **Utilities > Swap Appliance**. A warning message appears.
4. Confirm, and type the new appliance's serial number.
5. Select:
   - **Cancel** to stop.
   - **Save** to complete.
6. Deploy the configuration to complete the appliance swap.

Related Links

WAN on page 84

WAN

Select to display the **WAN** page, or go to **Dashboard** > **WAN** widget.

The **WAN** page displays the following:

- Time Range Selector and Timeline—Select a Time Range period, then position your cursor over any point of the evolution curve to view the Throughput and Raised Alerts values at a specific time.
- Overview table—View detailed information for a single WAN.

Related Links

Time Range Selector and Timeline on page 18
WAN Overview on page 84
WAN Services on page 85

WAN Overview

The WAN Overview dashboard is an overview of Throughput per WAN Service during the specified time range of this dashboard. It displays Throughput in a bar and line chart.

- Select a time period:
  - Last Day: 5 minutes, 1 hour, 2 hours, 4 hours, 8 hours, or 24 hours
  - Last Week: 1 day, 2 days, or 7 days
  - Last Month: 7 days, 14 days, 30 days, 90 days.
  - Custom: Provide a custom date and time.
- Select the tab that corresponds to the data direction: **LAN** > **WAN** or **WAN** > **LAN**.

WAN Services

WAN Services provides key performance metrics for monitoring and analyzing network traffic across WAN links. Table 15 describes the columns on the WAN Services page:

Table 26: WAN Services Columns

Column	Description
WAN Services	Displays the WAN link name.
Throughput IN	Measures the incoming data rate on the WAN link.
Throughput OUT	Measures the outgoing data rate on the WAN link.
EQS	Indicates the overall network quality.
Delay	Reports the latency in milliseconds.
Jitter	Measures the variation in packet delay.
Packet Loss	Displays the percentage of lost packets.
RTT (Round Trip Time)	Records the time taken for a signal to travel to its destination and back.
SRT (Server Response Time)	Measures the time between a client request and server response.
Retransmission	Indicates the percentage of packets retransmitted due to errors.
Avg Sessions	Displays the average number of active sessions over a given period.

Reports and Templates

Go to **Reports & Templates** from the main menu.

A report requires a graphical content template. Before you can create a report, create the report template.

Related Links

Create Report Templates on page 86
View a Generated Report on page 89
Create Report on page 88
View a Generated Report on page 89

Create Report Templates

Note
ExtremeCloud OS ONE SD-WAN offers the following predefined templates:

- Application Overview
- Site Overview
- Site 360 Overview
- WAN Overview
- Application Performance
- Site 360 Performance

Use this task to create a new template.

1. Select the **Templates** tab.
2. Select the **Create Templates** icon.
3. Enter the **Template Name** and an optional **Description**.

4. Select the widgets to include in the template.

   The following categories are available:

   - Application Overview
   - Site Overview
   - WAN Overview
   - Site 360 Overview
   - Application Performance
   - Site 360 Performance

   For each category, select a widget from the list and select **Create Template**.

Related Links

Create Report on page 88
View a Generated Report on page 89
Create Report on page 88
View a Generated Report on page 89

View Generated Templates

ExtremeCloud OS ONE SD-WAN lists all your created templates and predefined templates with the following information:

- Template Name
- Template Usage: specifies the number of reports using the template
- Last Modified On: creation or modification date and time
- Actions: you can
  - Clone ( ) all the templates to create new templates
  - Delete ( ) the templates you have created. The predefined templates provided by ExtremeCloud OS ONE SD-WAN cannot be deleted
  - Edit ( ) the templates you have created. The predefined templates provided by ExtremeCloud OS ONE SD-WAN cannot be modified

To refresh the data display, select .

To download the Template data as a `Template_Overview.csv` file, select .

Related Links

Create Report Templates on page 86
Create Report on page 88
View a Generated Report on page 89

Create Report

Use this task to create a report.

1. Go to **Reports & Templates** .
   The **Reports** tab is selected.
2. Select **Create Report**.
   The **Create Report Flow** wizard opens.
3. In the **Create Report Flow** wizard, select **Continue**.
4. Type the **Report Name** and an optional **Description**.
5. Select a template from the list.
   The widgets that are associated with the template are automatically specified. If the template includes Site 360 widgets, select a site from the list.
6. From the wizard, select **Next - Report Schedule**.
   You can choose to create the report immediately or to schedule it. Table 27 describes each option.

Table 27: Report Scheduling Options

Choice	Do this
Create report now	Select the **Create Now**, and then specify the **Data Range**: • **Last 24 hours** • **Yesterday** • **Last Week** • **Last month** Or, select **Custom Range**, and then use the calendar controls to manually select the date and time range for the report.
Schedule the report.	Select **Schedule for later**, and then specify the **Data Range** and **Report Frequency**: • **Daily**—Use the time picker to select the time. • **Weekly**—Select the day of the week from the list, and use the time picker to select the time. • **Monthly**—Select the day of the month from the list, and use the time picker to select the time. You can edit a scheduled report by selecting .

7. (Optional) To send email notifications, configure **Email Notification**.
   a. Type the **Email Subject**.
   b. To add a recipient, type their email address, and then select +
8. In the wizard, select **Next - Report Summary** and check your report configuration.

   Note
   The only available format is PDF.

9. Select **Create Report**.

Related Links

View a Generated Report on page 89

View a Generated Report

The Reports table lists all generated reports. When the PDF report is available, the table displays it on a sub-line with the following information:

- **Schedule Type:** displays **Once** for a report created immediately or displays the report frequency for a scheduled (repeated) report
- **Report Generated Time:** creation date and time of the generated report
- **Status:**
  - Report definition: **Inactive** for immediately generated reports, and for repeated reports for which scheduling is deactivated
  - Generated report: **Report Generated** or **Report Generation** failed

Use this task to download and view a report in PDF format.

1. Go to **Reports & Templates**.
2. Select the **Reports** tab.
3. Select the arrow beside the report that you want to view.

   The sub-line appears.
4. To view the report PDF, select .

   To delete a report, select .

Related Links

Create Report on page 88

Settings

To complete the initial configuration of network policy, sites, and appliance templates in ExtremeCloud OS ONE SD-WAN, use the **Onboarding Wizard**. Initiate subsequent configuration changes and addition configuration from the **Settings** menu.

Go to **Settings** to configure the following:

- Policy Configuration
- Application Dictionary on page 92
- Application Group on page 94
- Common Objects
- Audit Logs

Note
To finish an appliance configuration or to override specific template settings:

1. Go to **Appliances**.
2. Select an appliance.
3. Select **Edit Appliance**.

Policy Configuration

Policy Configuration provides a centralized location to define and manage SD-WAN policies. It consolidates global attributes, security rules, and application performance priorities into a single configuration interface.

Policy Configuration is organized into the following tabs:

- **General**: Defines global parameters for the SD-WAN policy.
- **Security**: Contains policies for internet access.

- **Application Performance Policy**: Classifies and prioritizes application traffic based on business criticality and SLA.

Related Links

Application Performance Policy on page 44

General

The **General** tab displays global attributes of the SD-WAN policy:

- Name: Displays the policy name.
- NTP Servers (Auto-lookup): Displays the Network Time Protocol server configured for time synchronization.
- Fabric Support: Displays Fabric Support is enabled.

Security

The **Security** tab provides policies for managing traffic within and outside the SD-WAN network.

Internet Access

Use Internet Access policies to control traffic between sites and the Internet. These policies apply application filters to regulate access for specific IP Groups.

Table 28: Internet Access table

Column	Description
Name	The name of the Internet Access policy.
Status	Enable or disable the policy.
Sources	The source IP Groups for the policy.
Application Groups	The application groups included in the policy.
Action	Specifies the action for the traffic: **Allow**, **Deny**, or **DTI**.

Use this task to add an Internet Access Policy.

1. Navigate to **Settings** > **Policy Configuration** > **Security** > **Internet Access**.
2. Select **Add Filter**.
3. Configure the following parameters:
   - **Name**: Enter a name for the policy.
   - **Description**: Description for the policy.
   - **Status**: Enable or disable the policy.
   - **Sources**: Select one or more IP Groups as the source.
   - **Application Groups**: Select the application groups included in the rule.
   - **Action**: Choose **Allow**, **Deny**, or **DTI**.
4. Select **Save**.

Application Performance Policy

The **Application Performance Policy** tab classifies and prioritize application traffic based on business criticality and SLA requirements. These policies help ensure that critical applications receive appropriate bandwidth and optimized routing.

Table 29: Application Performance Policy table

Column	Description
Application Group	The application group associated with the policy.
Applications	The applications within the selected group.
Business Criticality	Indicates the importance of the application: **Top**, **High**, **Medium**, or **Low**.
Application SLA Name	The SLA profile applied to the application.
DWS Policy	The WAN or service policy associated with the application traffic.
Action	Delete the policy.

To add a new application performance policy, select **Add Application Performance Policy**. For detailed steps, see Application Performance Policy on page 44.

Related Links

Application Group on page 94
Network Allocation on page 94
Common Objects on page 95
Audit Logs on page 100

Application Dictionary

The Application Dictionary provides a list of applications and protocols to manage application-based policies. It supports application identification and classification for tasks such as creating applications and defining traffic policies.

Access and manage the **Application Dictionary** through the **Settings** menu.

Table 30: Application Dictionary Column

Column	Description
Application Name	Name of the application
Description	Description of the application
Application Group	Application group to which the application belongs
Protocol	Specifies the protocol used by the application for network communication
Attribute	Attribute of the application

Table 30: Application Dictionary Column (continued)

Column	Description
Client Subnets	Displays the subnets from which the application traffic originates
Server Subnets	Lists the subnets where the application's servers are hosted
Status	Application status
Action	Delete option to manage the application

Add applications to the **Application Dictionary** either by selecting predefined entries from the catalog or by creating a custom application.

Application Recognition

- When you add an application to the dictionary, the system begins recognizing and classifying traffic for that application.
- If traffic matches multiple applications, the custom application takes precedence over catalog applications.
- This ensures that user-defined applications override catalog entries in case of overlapping signatures.

Use this task to add a new application.

1. Navigate to **Settings** > **Application Dictionary**.
2. Select **Add application**.
3. Choose one of the following options:
   - From **Catalog**
     a. Select one or more applications from the catalog.
     b. Select Save.
   - **Custom Application**
     a. Select **Custom Application**.
     b. Add the following details:
        - **Name:** Name for the custom application.
        - **Description:** Description for reference.
        - **Protocol:** Select the protocol to associate with the application.
        - **Enabled:** Use the checkbox to enable or disable the application.
        - **Application Group:** Select the group to which the application belongs.
        - **Subnet Filter:** Select whether the filter applies to **Client** or **Server**.
        - **IP Version:** Choose **IPv4** or **IPv6**.
        - **Server Subnet:** Select **Add Subnet** and specify the subnet prefix and prefix length.

          The new application appears in the Application Dictionary list.

Related Links

Application Group on page 94
Network Allocation on page 94
Common Objects on page 95
Audit Logs on page 100

Application Group

With Application Group, you can group applications by specific criteria and configure performance, security, and optimization settings for each group. Configure Application Group from **Settings** on the main menu.

Note
The position of the application groups in the list determines how packets are classified. The system processes packets from the top of the list downward and assigns the first applicable classification. The **Other** group is always at the bottom

Use this task to add a new application group.

1. Navigate to **Settings** > **Application Groups**.
2. Select **Add Application Group**.
3. Type the **Application Group Name** and **Description.**
4. Select applications from the list or to create new applications, select **Create New Application**.
5. Select **Save**.

Related Links

Common Objects on page 95
Audit Logs on page 100

Network Allocation

The **Network Allocation** page displays DHCP address pool allocation details for each site and appliance.

Go to **Settings > Network Allocation** to view the configured DHCP information.

Use **Select VLAN** to filter the displayed information by VLAN.

Column	Description
Site	Site where the DHCP service is configured.
Appliance	Appliance providing the DHCP service.
IP Version	Specifies the IP version used by the DHCP configuration.

Column	Description
Subnet	Subnet associated with the DHCP address pool.
Gateway	Default gateway address assigned in the subnet.
Total Pool	Total number of IP addresses available in the subnet pool.
Exclude	IP addresses excluded from the DHCP pool.
Reserved	IP addresses reserved for static assignments.
Dynamic Pool	IP addresses available for dynamic allocation to DHCP.

Related Links

Audit Logs on page 100

Common Objects

Common Objects lists all common configurations that streamline network management and ensure consistency across policies. You can access and manage the **Common Objects** from **Settings** on the main menu.

Related Links

Application SLA on page 96

Overlays on page 97

IP Groups on page 98

Appliance Templates

Appliance Templates provide a centralized location to create and manage appliance templates across multiple network policies. The **Appliance Templates** page simplifies template administration by allowing you to reuse predefined configurations for multiple appliances.

You can search for a template by name using the **Search** field or refresh the list by selecting the refresh icon.

Table 31: Appliance Templates Page Overview

Column	Description
Name	The name of the appliance template. Select the template name to view or edit its configuration.
Type	Indicates the template type, such as Hub or Spoke.

Table 31: Appliance Templates Page Overview (continued)

Column	Description
Appliances	Displays the number of appliances currently using this template. Select the number to view the associated appliances. You can also assign appliances to the selected template from this view.
Action	Provides the option to delete a template.

Use this task to add an appliance template.

1. Select **Add Template**.
2. Configure the template by defining the following parameters:
   - **Template Name**, **Description** and **Appliance Type**
   - Interface configuration and type: Select **Hub** or **Spoke**
   - **WAN** and **LAN** interface settings
3. Select **Create Template** to save the configuration.

The new template appears in the appliance templates list. For more information, see Appliance Templates on page 25.

Related Links

Application SLA on page 96

Overlays on page 97

IP Groups on page 98

Appliance Template Settings on page 25

Adaptive QoS Overview on page 32

LTE (WAN4) Interface Configuration on page 34

Application SLA

Create, modify, and delete Service Level Agreements (SLA) from the **Application SLA** page. An SLA is a contract that outlines a level of service. Here, it defines the bandwidth per session.

Table 32: Application SLA Page Overview

Column	Description
Name	Name of the Application SLA.
Description	A brief summary of the Application SLA.
Type	Defines the SLA category based on the application flows.
Obj Bandwidth	Specifies the nominal bandwidth per session. This value is mandatory and is enforced during network congestion.

Table 32: Application SLA Page Overview (continued)

Column	Description
Max Bandwidth	Defines the maximum bandwidth per session. If not specified, it defaults to 500 times the objective bandwidth.
Action	Delete option to manage the Application SLA.

Use this task to add a new Application SLA.

1. Go to **Settings > Common Objects > Application SLA**.
2. Define the **Application SLA** parameters.

Table 33: Application SLA Settings

Settings	Description
Name	Enter a unique identifier for the **Application SLA**.
Description	Provide a brief summary of the SLA's purpose.
Type	Select the type of application flow: • **Realtime**: For real-time applications (VoIP, video) sensitive to delay, jitter, and packet loss. • **Transactional**: For transactional applications (SAP, Telnet) sensitive to delay. • **Background**: For other non-time-sensitive applications.
Session Bandwidth (kbps)	Specify the bandwidth allocated per session: • **Objective Bandwidth**: Define the nominal bandwidth per session (mandatory). This value is enforced during network congestion. • **Maximum Bandwidth**: Set the upper limit for bandwidth per session (optional). If not specified, it defaults to 500 times the Objective Bandwidth.
Performance Metrics	Specify the Objective and Maximum values for: • **Delay (ms)** • **Jitter (ms)** • **Packet Loss (%)** • **SRT (Server Response Time, ms)** • **RTT (Round Trip Time, ms)** Select the boxes for the performance metrics to be enforced within the SLA and select **Done.**

Overlays

An overlay network involves logical connections for services. It handles the logical policies and traffic management, unlike the physical infrastructure of the underlay.

From this page, you can view existing overlays, their associated hubs and spokes, and manage overlay configurations.

Use the **Search** field to locate overlays by name or refresh the list using the refresh icon.

Table 34: Overlays Page Overview

Column	Description
Name	The name of the overlay. Select the name to view or edit its configuration.
Type	The overlay type, such as Hub & Spoke and Hub & Spoke IPv6.
Hubs	Displays the number of hub appliances associated with the overlay.
Spokes	Displays the number of spoke appliances associated with the overlay.
Site-to-Site Tunnels	Displays the number of active site-to-site tunnels established using this overlay.
Action	Provides the option to delete an overlay.

Use this task to create a new hub and spoke overlay.

1. Select **Add Overlay**
2. In the **Add Overlay** window, configure the following parameters:
   - **Name:** Enter a name for the overlay.
   - **Type:** Select the overlay type.
   - **IKE Policy:** Configure encryption, authentication, Diffie-Hellman group, and SA lifetime settings.
   - **IPsec Concentrator Authentication:** Define pre-shared key.
   - **IPsec Policy:** Define encryption, authentication, Perfect Forward Secrecy (PFS), and SA lifetime settings.
   - **MTU:** Specify the maximum number of bytes allowed in the payload. The default value is 1400 bytes.
3. Select **Save**.

For detailed steps on creating and configuring overlays, see Network Overlay on page 41.

Related Links

IP Groups on page 98

IP Groups

With IP Groups, you can define and manage reusable groups of IP addresses or subnets. You can reference these groups across multiple configurations to simplify policy management.

The **IP Groups** page displays both default and custom groups:

- Default IP Groups:
  - A default IP group is automatically created for every site during onboarding.
  - You cannot edit, rename or delete the default IP groups.
- Custom IP Groups:
  - You can create additional IP groups to classify traffic within a site or across multiple sites.
  - Custom groups provide finer control and flexibility when defining segmentation rules and filters.

Use the **Search** field to locate a specific IP group, or select **Refresh** to reload the list.

Table 35: IP Groups Columns

Column	Description
Name	The name of the IP group. Select the name to view or edit its configuration.
Description	A brief description of the IP group.
IP Groups	Displays nested IP groups associated with this group.
Subnets	Lists the IP subnets included in the group.
Internal Segments	Number of Internal Segmentation policies referencing this IP group.
Internet Application Filters	Number of Internet Access policies that reference this IP group.
Action	Provides the option to delete the custom IP group (default IP groups cannot be deleted).

Use this task to create a new IP group.

1. Go to the main menu, select **Settings** > **Common Objects** > **IP Groups**.
2. Select **Add IP Group**.
3. In the **Add IP Group** page, configure the following parameters:
   - **Name:** Enter a unique name for the IP group.
   - **Description:** Enter a short description for reference.
   - **Subnets:** Add one or more subnets in IPv4 or IPv6 format.
   - **IP Groups:** Include existing IP groups to create nested groups.
4. Select **Done** to save the configuration.

Related Links

Audit Logs on page 100

Audit Logs

Audit Logs provide a record of configuration changes made in the ExtremeCloud OS ONE SD-WAN application. This feature helps you track user activity, monitor changes, and maintain compliance.

Use the **Audit Logs** page to track all configuration changes in ExtremeCloud OS ONE SD-WAN. Go to **Settings** > **Audit Logs** from the main menu.

The **Audit Logs** page displays a list of log entries with the following column information.

Table 36: Audit Logs Columns

Column	Description
Time	Timestamp of the log entry. Each time a user saves a change, a new entry is created.
User Name	Name of the user.
E-mail	User e-mail address.
Category Type	Indicates the type of resource affected, such as configuration, deployment, firmware, alarms, or reports.
Subcategory Type	Specifies the affected configuration area, such as network policies, templates, overlays, security, or application performance.
Activity Type	Action performed: create, update, or delete.
Activity Status	Outcome of the action: success or failure.
Description	Additional details about the recorded activity.

If the table contains a significant number of objects, use the page navigation controls at the bottom of the window to navigate the list.

Filtering Data

To filter data display, select . Filter data in the audit logs by column:

- Users
- Category Type
- Subcategory Type
- Activity Type
- Activity Status

- To expand each filter, select the down arrow, or select **Expand All**.
- Then, select the appropriate elements and select **Apply Filters**.
- To clear the defined filters at any time, select the refresh icon , or select **Clear All Filters**.
- To download all table data as a CSV file, select .

Related Links

Alarms Management on page 102

Alarms Management

Go to **Alarms Management** or select the **Alarms** widget on the **Dashboard**.

The **Alarms Management** page contains two tabs to display active and cleared alarms.

You can also configure alarm notification rules.

Time Range Selector and Timeline

The following controls appear at the top of the **Alarms Management** window.

- Select the time range from the list: Last Day (default), Last Week, Last Month, Custom.
- Select a time span option. Available time span options depend on the selected time range, and appear to the right side of the time range selector.
  - **Last Day:** 5 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 24 hours.
  - **Last Week:** 1 day, 2 days, 7 days.
  - **Last Month:** 14 days, 30 days, 90 days.
  - **Custom:** Use the calendar controls to manually define the time range and span.

Note

Once an alarm is cleared, it remains in the database for 30 days from the time it was raised, not from the time it was cleared. For example, if Alarm A was raised on 1 May and cleared on 2 May, it remains in the database until 31 May. During this period, the alarm is visible under the **Cleared Alarms** tab.

Timeline Evolution Graph

The interactive timeline evolution graph shows curves for **Active** or **Cleared** alarms that correspond to the chosen time range. Select a tab and then position you cursor over any point on the evolution curve to view the number of active or cleared alarms at a specific time.

Customize your view:

- Toggle the display of the timeline: **Show Timeline**, **Hide Timeline**.
- To display or hide the evolution curve of each type of alarm separately, select the category label in the graph legend.
- To zoom in on the time series graph, select a specific section of the graph and drag the cursor to the right. The resulting graph displays more points at a lower display rate. Continue to zoom in until you reach the desired level of detail. Select to return to the default time settings of the curves.
- To reset the **Alarms Management** page to the default time settings (Last Day, 24 hours), select **Reset**.

Related Links

Alarm Types on page 103
Alarms by Category on page 105
Configure Alarm Notification on page 104

Alarm Types

Active Alarms

The **Active Alarms** tab displays active Critical, Major, and Minor alarms. Alarms raised during the specified time range are considered active.

You can filter active alarms by the following criteria:

- Severity
- Category
  - Underlay: The physical connection between devices (LAN, WAN) or appliance configuration
  - Overlay: The connection between appliances through IPsec tunnels
  - Services: Services provided with the appliance
  - Resources: Device local resources, such as, hardware monitoring
  - Management: The connection to components, such as the Orchestrator.
- Alarm
- Local site
- Local appliance: first appliance in the case of tunnel failure or end-to-end connectivity lost issue
- Remote site
- Remote appliance: second appliance in the case of tunnel failure or end-to-end connectivity lost issue

To apply filters:

1. Select .

   Note
   The **Filtering Options** contains only the previously raised alarms, not all the system alarms.

2. Select options.
3. Select **Apply Filters**.

To clear the defined filters, select **Clear All Filters**.

The following colors indicate the severity of alarms:

- Red = Critical
- Orange = Major
- Gray = Minor

The raised time for each alarm is specified.

You can sort column data by selecting the column header names.

- To search for specific alarms, type in the **Search** field.
- To refresh the display, select .
- To download alarms as an `Active_Alarms_Data.csv` file, select .

Cleared Alarms

The **Cleared Alarms** tab contains the same filters as the **Active Alarms** tab.

Information for each alarm includes the time each alarm was raised and cleared.

Related Links

Alarms by Category on page 105

Configure Alarm Notification

Configure alarm notification for when critical, major, and minor alarms are raised or cleared. ExtremeCloud OS ONE SD-WAN provides notifications about alarms when you are not actively viewing the **Active Alarms** tab.

Note
This function is only available to the Administrator and Network Manager profiles.

Use this task to create an alarm notification rule.

1. From the top of the **Alarms Management** page, select **Notification Rules**.
2. Select **Add Rule** and type a name for the notification rule.

3. From the **Category** list, select one or several options:
   - Underlay: physical connection between devices (LAN, WAN), VRRP state change, appliance configuration
   - Overlay: connection between appliances or external gateways through IPsec tunnels
   - Services: services provided with the appliances such as application visibility, application control, WAN optimization, dynamic WAN selection, firewall
   - Management: connection to components (Orchestrator, etc.)
   - Select All: all the categories are taken into account.
4. From the **Site** list, select one or several sites in your network.

   Note
   You receive notification of alarms related to selected sites only.

5. From the **Severity** list, define the type of alarm that triggers the notification message for each severity level:
   - Minor
   - Major
   - Critical
6. **Recipients**: Type the email address of one or more recipients.

   Note
   All recipients receive alarm notifications by email.

7. Select **Create**.

   The new notification rule appears in the **Notification Rule Details** table. To deactivate the notification rule, modify the **State** option.
8. Select to download the **Notification Rule Details** table as an `Alarm_Notification_ Data.csv` file.
9. To delete a notification rule, select .

Related Links

Alarms by Category on page 105

Alarms by Category

The following tables list the ExtremeCloud OS ONE SD-WAN alarms by category and briefly describe troubleshooting measures for when an alarm condition occurs. The alarm categories are as follows:

- Underlay: physical connection between devices (LAN, WAN), VRRP or HA state change, appliance configuration
- Overlay: connection between appliances or external gateways through IPsec tunnels
- Services: services provided with the appliances such as application visibility, application control, WAN optimization, firewall
- Management: connection to components

Underlay

Table 37: Underlay Alarms

Alarm	Severity	Troubleshooting
Network interface down [interface name]	Critical	Check physical connections with the device.
No IP address [Transport Network Identifier name]	Critical	Define a correct IP address for the configured WAN interface.
No default gateway [Transport Network Identifier name]	Critical	Define a default gateway for the configured WAN interface.
Configuration failure	Critical	The alarm is triggered due to a configuration version mismatch between the SD-WAN application and the appliance. This alarm is also raised when the appliance is in rollback state. In this case, the additional message **appliance is in rollback state** is displayed.

Overlay

Table 38: Overlay Alarms

Alarm	Severity	Troubleshooting
Tunnel failure (appliance)	Critical	Check the Tunnels/Connections Supervision table that you access from the main dashboard and verify the state of the GRE/IPsec tunnels.
External tunnel failure (External Gateway)	Critical	Verify that the definition of the External VPN Gateway and the tunnel configuration match the configuration of the remote VPN Gateway that the appliance is trying to connect to.
IS-IS adjacency lost	Critical	Check the IS-IS adjacency state on contact the neighbor switch. Contact ExtremeCloud SD-WAN Support.
BGP Failure (WAN)	Major	Check the network connection. BGP configuration. Contact ExtremeCloud SD-WAN Support.
BFD Failure (WAN)	Major	Check the network connection. BFD configuration. Contact ExtremeCloud SD-WAN Support.

Services

Table 39: Services Alarms

Alarm	Severity	Troubleshooting
Synchronization Lost	Major	Contact ExtremeCloud SD-WAN Support.

Resources

Table 40: Resources Alarms

Alarm	Severity	Troubleshooting
Disk is almost full (<5% left) on the volume [volume name]	Major	For hardware resource alarms, contact ExtremeCloud SD-WAN Support.
Reboot	Minor	

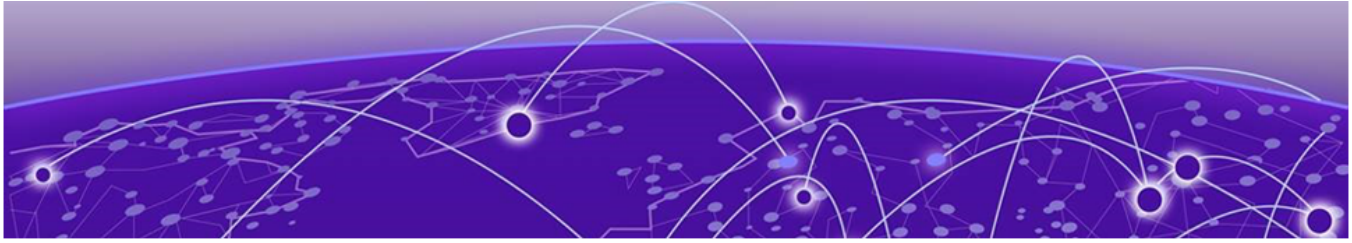
Management

Table 41: Management Alarms

Alarm	Severity	Troubleshooting
Disconnected from Orchestrator	Critical	One or several SD-WAN platform components are disconnected from the Orchestrator. (Disconnected status because they were never connected or because they were not recently connected.) Contact ExtremeCloud OS ONE SD-WAN Support.
Connectivity with Orchestrator impaired	Major	One or several SD-WAN platform components are disconnected from ZTP (Zero Touch Provisioning server). (Disconnected status because they were never connected or because they were not recently connected.) Contact ExtremeCloud OS ONE SD-WAN Support.

Related Links

Alarm Types on page 103



Network Troubleshooting

Port and System LED Indicators on page 108

Follow these steps to access a remote console where you can establish an SSH session for network troubleshooting:

1. Go to **Appliance** and select an appliance from the list.
2. Select **Utilities > Remote Console**.
3. A confirmation prompt appears. Select **Yes** to proceed.

   The SSH session opens in a new browser tab,
4. Enter the administrator credentials when prompted.
5. Use the following commands to troubleshoot network issues:
   - `start-shell` - Access the shell environment.
   - `sudo bash` - Gain root access for advanced diagnostics.

Advanced trouble shooting commands

- `tcpdump` - Capture and analyze network traffic.
- `netstat` - Displays active connections, listening ports, and network statistics.
- `nslookup` - Displays DNS records, you can resolve domain names and diagnose DNS issues.

Port and System LED Indicators

Port and system LED indicators on supported SD-WAN appliance platforms helps you verify link status, port speed, and system health during troubleshooting.

Port LED Indicators

Port LEDs provide information about link activity and port speed. The LED behavior and color depend on the platform model and the negotiated interface speed.

- Link/Activity LEDs indicate if a physical link is established and if traffic is present on the port.
- Speed LEDs indicate the operational speed of the port after auto-negotiation.
- Not all platforms support all port speeds, unsupported speeds are marked as Not supported or N/A in the tables.

Use the following table to interpret port LED behavior by platform.

Table 42: Port Link and Speed LEDs

Platform	LED	10G	1G	100M	10M
40ax V2	Link/Activity	N/A	Amber	Amber	Amber
	Speed	N/A	Orange	Green	Off
420ax	Link/Activity	N/A	Amber	Amber	Amber
	Speed	N/A	Orange	Green	Off
Note: On WAN3, the Link/Activity LED turns on only when traffic is present.					
2200ax-F	Link/Activity	Green	Green	N/A	N/A
	Speed	Green	Amber	N/A	N/A
2200ax-T	Link/Activity	N/A	Green	N/A	N/A
	Speed	N/A	Ports 1 to 4: Green Port 5: Orange	Ports 1 to 4: Orange Port 5: Green	Off

System LED Indicators

System LEDs provide information about the overall operational state of the appliance. These LEDs help you quickly determine whether the device has powered on successfully, completed the boot process, or encountered a hardware related issue.

System LEDs typically indicate:

- Power status
- Boot and operational state
- Disk activity
- Network activity
- Hardware fault conditions, such as power supply, fan, or thermal issues

2200ax-F and 2200ax-T Platforms

On 2200ax-F and 2200ax-T platforms, system LEDs indicate power, disk, LAN activity, and fault conditions. Blinking LEDs generally indicate active operations or attention-required states.

LED	Description
Power	Green when the device is powered on
Hard Disk	Blinks during disk access
LAN 1	Blinks on activity

LED	Description
LAN 2	Blinks on activity
'i' Power Fail / Over Heat / Fan Fail	Blinks when one PSU is plugged into the chassis but is not powered on **Note:** This does not turn green if both PSUs are up and running.

40ax V2 and 420ax Platforms

On 40ax V2 and 420ax platforms, system LEDs provide visibility into the boot process and hardware status. A green status LED indicates that the system has completed boot successfully, while a red status LED indicates a boot failure.

	40ax V2	420ax
LAN Bypass 1	Off	Off
LAN Bypass 2	Off	Off
Power	Green	Green
Status	Green - Boot complete Red - Boot failure	Green - Boot complete Red - Boot failure
Hard Disk	Blink on access	Blink on access