ExtremeCloud OS ONE SD-WAN v30.26.2.0 Fabric Deployment Guide

Comprehensive Configuration and Management

9041212-00 Rev AA
August 2026

Copyright © 2026 Extreme Networks, Inc. All rights reserved.

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/

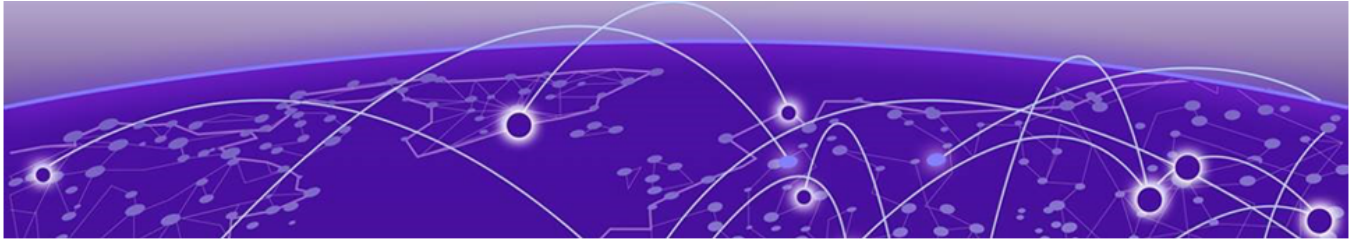


Table of Contents

Abstract v

Preface 6
- Text Conventions 6
- Documentation and Training 7
  - Open Source Declarations 8
  - Training 8
- Help and Support 8
  - Subscribe to Product Announcements 9
- Send Feedback 9

About this Document 10

Overview of Fabric over SD-WAN 11
- SD-WAN Fabric Architecture 11

Prerequisites 13
- Supported Software Version 13
- Supported Appliance Models 14
- Network Environment Requirements 14
- Example Network Architecture 14

Initial Setup 16
- Connecting ExtremeCloud OS ONE SD-WAN Appliances 16
- Configuring WAN Interfaces 16
- Manual IP Configuration (CLI) 17
- Configuring VLAN-based WAN Interface 18
- Upgrading Firmware using the ExtremeCloud OS ONE SD-WAN Orchestrator 19

Configuring Network Policies 20
- General Policy Settings 20

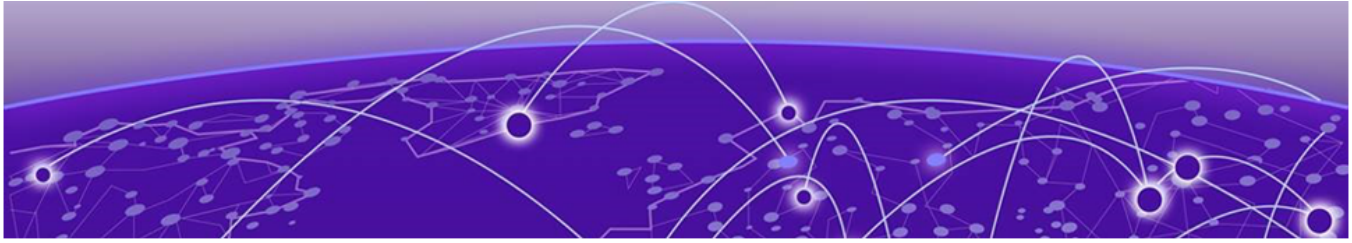
Creating Overlays 25

Onboarding Hub Site 27
- Creating a Hub Template 27
- Adding Hub Sites and Appliances 32
- Configuring Hub Appliances 32
- Hub Fabric Engine Switch Configuration 41

NTP Verification 45

Onboarding Spoke Site 46
- Creating a Spoke Template 46
- Adding Spoke Sites and Appliances 51
- Configuring Spoke Appliances 51
- Branch Fabric Engine Switch Configuration 59

SD-WAN Orchestrator Verification..... 65
SD-WAN Tunnels..... 65
LLDP Signaling..... 65
SD-WAN Tunnel Verification..... 66



Abstract

This Fabric Deployment Guide for ExtremeCloud OS ONE SD-WAN version 30.26.2.0 provides configuration and deployment guidance for integrating SD-WAN appliances with Extreme Fabric Connect in hub-and-spoke environments. It covers Fabric over SD-WAN architecture, prerequisites, supported appliances and software, WAN and VLAN-based WAN configuration, network policies, IPsec overlays, and centralized onboarding through SD-WAN Orchestrator. Procedures describe creating hub and spoke templates, configuring appliances and Fabric Engine switches, using ZTP, LLDP auto-sensing, dynamic IP assignment, NTP, Fabric Local Breakout, static routes, and service overlays. Security configuration includes IPsec authentication, encryption, integrity, and Perfect Forward Secrecy settings. The guide also addresses connectivity requirements, firewall ports, MTU considerations, and appliance throughput. Verification procedures cover SD-WAN tunnels, LLDP signaling, Fabric connectivity, and tunnel status. It includes 5420 onboarding into Site Engine, workflow execution, and troubleshooting guidance. The guide is intended for network administrators and engineers with an intermediate-to-advanced technical understanding of SD-WAN and Fabric networking.

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.

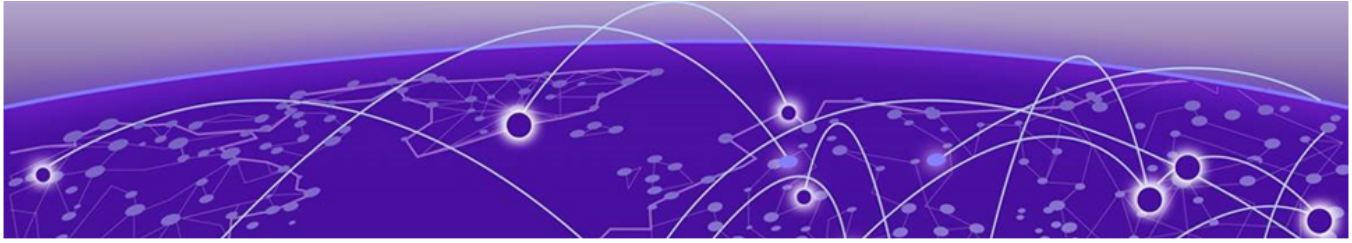
Send Feedback

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.

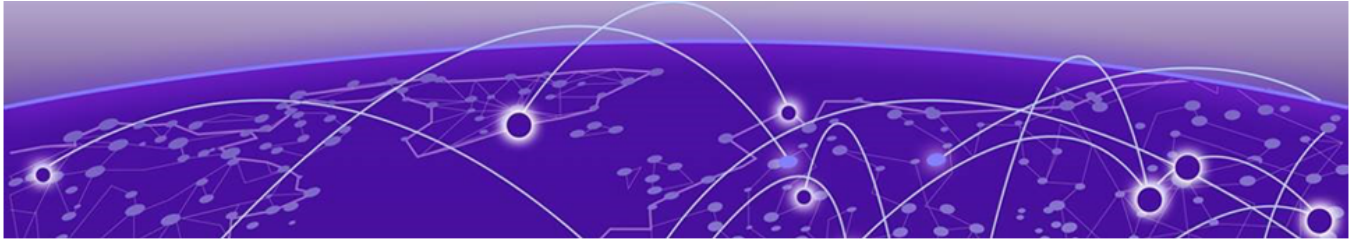
Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About this Document

The ExtremeCloud OS ONE SD-WAN Fabric Deployment Guide explains how to deploy ExtremeCloud OS ONE SD-WAN in a Fabric-enabled network environment. Use the information in this guide to set up and manage SD-WAN appliances that integrate with Extreme Fabric Connect.

It outlines the steps to prepare your environment, onboard appliances, configure Fabric Extend, and validate connectivity across hub-and-spoke sites. Key topics include LLDP auto-sensing, dynamic IP assignment, overlay tunnel creation, and service integration with Fabric infrastructure.



Overview of Fabric over SD-WAN

SD-WAN Fabric Architecture on page 11

SD-WAN Fabric deployment refers to the integration of **ExtremeCloud OS ONE SD-WAN appliances** with **Extreme Fabric Connect** switches (running Fabric Engine), allowing for automated extension of a Fabric-based network over a WAN infrastructure. This approach enables to:

- Extend Layer 2 and 3 Fabric connectivity from data centers or campus networks to remote or branch locations using internet or MPLS links.
- Simplify network onboarding using ZTP, dynamic IP addressing, and centralized configuration templates.
- Establish secure IPsec tunnels between appliances with automated key exchange, policy enforcement, and overlay management.
- Maintain time synchronization and IP consistency using NTP configuration.
- Reduce manual provisioning by enabling Auto-sense and SD-WAN aware Fabric VLANs, VRFs, and BGP integration.

SD-WAN Fabric Architecture

ExtremeCloud OS ONE SD-WAN integrates with Fabric Connect to create a unified architecture that spans both WAN and LAN domains. SD-WAN appliances establish secure IPsec tunnels over public internet or MPLS connections. These appliances connect to Fabric Engine switches through LAN ports configured in auto-sense mode, which triggers automated creation of VXLAN tunnels for Fabric Extend.

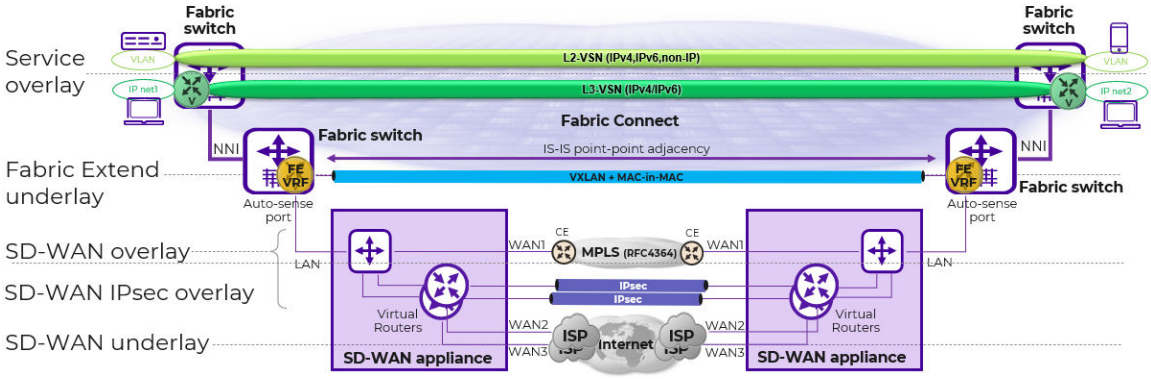
The VXLAN tunnels form the underlay for carrying MAC-in-MAC encapsulated traffic between sites. These tunnels support dynamic routing through IS-IS adjacencies and are bound to a dedicated VRF, ensuring isolation from traffic.

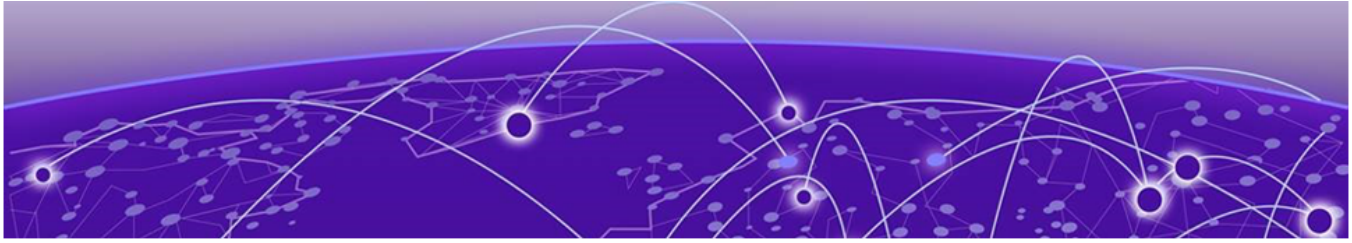
On top of the Fabric Extend underlay, the Fabric Connect architecture supports service overlays that deliver Layer 2 and Layer 3 Virtual Service Networks (VSNs). L2-VSNs transport IPv4, IPv6, and non-IP traffic, while L3-VSNs enable routed IP domains. These overlays provide secure, scalable, and isolated networking across distributed locations.

Key components of this architecture include:

- **Auto-sense Port**: Automatically detects SD-WAN appliances and initiates dynamic configuration for Fabric Extend.
- **SDWAN-VRF**: Terminates VXLAN tunnels and maintains routing adjacencies through IS-IS.

- **NNI (Network-to-Network Interface)**: Connects multiple Fabric switches, enabling extension of the Fabric overlay.
- **SD-WAN Overlay**: Transports encrypted data between SD-WAN appliances using IPsec tunnels.
- **Service Overlay**: Delivers end-to-end L2 and L3 services using Fabric VSNs for application traffic.





Prerequisites

Supported Software Version on page 13
Supported Appliance Models on page 14
Network Environment Requirements on page 14
Example Network Architecture on page 14

This section lists the requirements needed before starting the deployment:

- Licenses: Access the ExtremeCloud OS ONE SD-WAN Orchestrator with linked licenses.
- Network Requirements: Internet connectivity with DHCP support or static IP capability for WAN interfaces.
- Time Synchronization: Accessible NTP server for time synchronization (critical for delay/jitter/loss measurements).
- DNS Requirements: Ensure the appliance can resolve the following:
  - SD-WAN Orchestrator FQDN (for ongoing management)
  - GDC (Global Delivery Cloud) endpoints (for ZTP onboarding)
  - NTP server FQDNs (if using domain-based NTP configuration)

    Without DNS resolution, ZTP will fail and the appliance cannot register with the Orchestrator.
- Proxy Configuration: If you use a proxy, ensure it is transparent for SD-WAN communications. The following traffic must be permitted:
  - **IKE:** UDP/500 (IPsec tunnel negotiation)
  - **NAT-T:** UDP/4500 (IPsec with NAT traversal)
  - **ESP:** IP Protocol 50 (encrypted data transport)
  - **Management/ZTP:** TCP/443 (Orchestrator communication and Zero-Touch Provisioning)

Supported Software Version

- SD-WAN Appliance Software: Version 25.1.2 or later.
- Fabric Engine (VSP) Software: Version 9.2.0.0 or later.

Supported Appliance Models

Platform	Interface Type	Throughput	Use Case
ipe40ax v2	RJ45 100/1000 Base-TX	Up to 1 Gbps	Small branch offices
ipe420ax	RJ45 100/1000 Base-TX	Up to 1.5 Gbps	Medium branch offices
ipe2200ax-T	RJ45 100/1000 Base-TX	Up to 1.5 Gbps	Large sites and data centers
ipe2200ax-F	SFP+ 10G Base-SR/LR	Up to 10 Gbps	Large sites and data centers

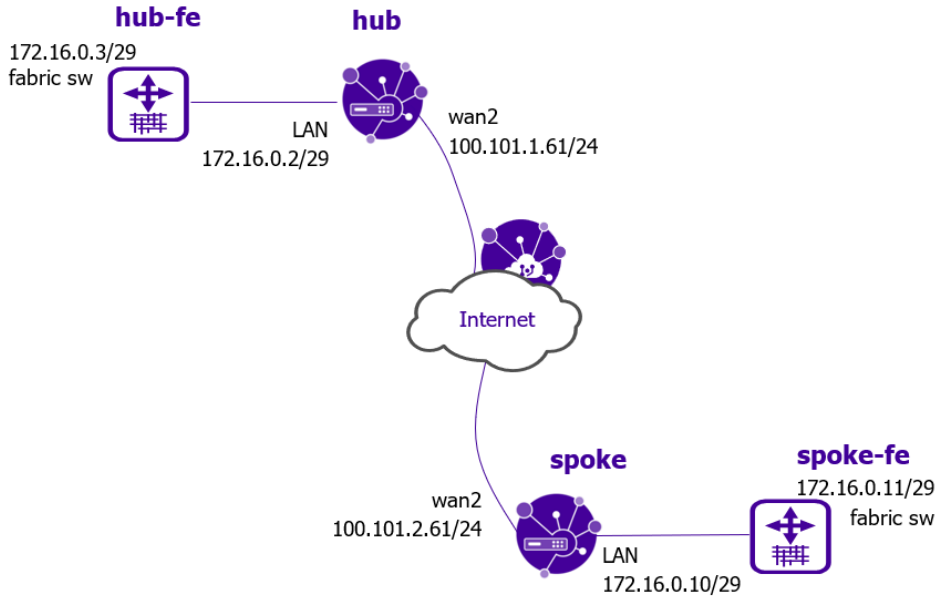
Network Environment Requirements

- **Internet Connectivity**: Ensure broadband internet access with sufficient bandwidth to support SD-WAN traffic.
- **DHCP Server:** Provide a DHCP server on WAN networks or configure static IP addresses as needed.
- **Firewall Ports**:
  - Allow **TCP/443** for Orchestrator communication.
  - Allow **UDP/500** and **UDP/4500** for IPsec tunnel establishment. For hub-and-spoke overlay topologies, spokes act as initiators and hubs act as responders.
- **MTU Considerations:** Use an internet connection that supports a minimum MTU of 1500 bytes.
- **Public IP Requirements:** Assign at least one static public IP address to each hub site.

Example Network Architecture

An example network diagram illustrates the hub and spoke topology using SD-WAN and Fabric Connect. Each site includes an ExtremeCloud OS ONE SD-WAN appliance and a Fabric Engine switch. The diagram depicts an IPv4 underlay deployment; ExtremeCloud OS ONE SD-WAN also fully

supports IPv6 and dual-stack (IPv4 + IPv6) underlay and overlay addressing.



Initial Setup

This section describes the steps to connect and configure ExtremeCloud OS ONE SD-WAN appliances for various network environments.

Note
Appliances are configured with DHCP by default. When an IP address is configured manually via the CLI, once the appliance connects to the ExtremeCloud OS ONE SD-WAN Orchestrator and pulls its configuration, the Orchestrator configuration will overwrite all manually entered settings from the CLI.

Connecting ExtremeCloud OS ONE SD-WAN Appliances

If WAN uses DHCP, appliances automatically onboard after Zero-Touch Provisioning (ZTP).

Configuring WAN Interfaces

Appliances are configured with DHCP by default. You can configure DHCP or a static IP on WAN interfaces based on your network requirements. ExtremeCloud OS ONE SD-WAN supports both IPv4 and IPv6 for WAN interface configuration.

WAN Interface and VRF Mapping Reference

When configuring WAN interfaces, the physical port names used in CLI commands differ from the logical interface names displayed in the ExtremeCloud OS ONE SD-

WAN Orchestrator. Use the following table to cross-reference physical ports with their corresponding Orchestrator interface names and VRF instances:

Table 4: WAN Interface and VRF Mapping

Physical Interface (CLI)	Orchestrator Interface Name	VRF Name
Ethernet 0/2	WAN1	wan1vrf
Ethernet 0/4	WAN2	wan2vrf
Ethernet 0/5	WAN3	wan3vrf

Note
CLI commands (for example, show **`ipv4 route vrf wan1vrf`** or **`interface ethernet 0/2`**) use physical port and VRF names. The Orchestrator displays these same interfaces as wan1, wan2, and wan3 in templates and monitoring dashboards.

DHCP Configuration

WAN interfaces operate in DHCP mode by default and automatically request IPv4 or IPv6 addresses upon boot without requiring manual CLI configuration.

To verify that an address has been allocated via DHCP:

```
ipe# show ipv6 interface ethernet <slot>/<port>
ipe# show ipv6 dhcp interface ethernet <slot>/<port>
```

If an interface was previously configured with a static IP address and you need to revert it to DHCP, use the following CLI commands:

```
ipe(config)# interface ethernet <slot>/<port>
ipe(config-if-eth-<slot>/<port>)# ipv6 address dhcp
ipe(config-if-eth-<slot>/<port>)# no shutdown
ipe(config-if-eth-<slot>/<port>)# exit
```

Manual IP Configuration (CLI)

For static IP WAN deployments, use the following CLI commands to manually configure network settings on the SD-WAN appliance. The same configuration steps apply for IPv4 deployments, replace the IPv6 addresses and commands with the corresponding IPv4 equivalents.

1. Connect to the appliance through a console connection.
2. Set terminal preferences for extended sessions.

```
ipe# terminal timeout 0
ipe# terminal length 0
```

3. Check current interface status.

```
ipe# show ipv6 interface brief
ipe# show interface brief
```

4. Remove default DHCP and assign a static IPv4 address.

```
ipe(config)# interface ethernet <slot>/<port>
ipe(config-if-eth-<slot>/<port>)# no ipv6 address dhcp
ipe(config-if-eth-<slot>/<port>)# ipv6 address <IPv6-address>/<prefix-length>
ipe(config-if-eth-<slot>/<port>)# no shutdown
ipe(config-if-eth-<slot>/<port>)# exit
```

Use the interface designated as your WAN uplink. The specific port varies by appliance model and deployment.

5. Add a default route in the appropriate VRF.

```
ipe(config)# vrf wan1vrf
ipe(config-vrf-wan1vrf)# static-route ::/0 <IPv6-nexthop>
ipe(config-vrf-wan1vrf)# end
```

6. Configure the DNS server. DNS server configuration is required to ensure the appliance can resolve hostnames, including the ExtremeCloud OS ONE SD-WAN Orchestrator address, after static IP assignment.

```
ipe(config)# vrf wan1vrf
ipe(config-vrf-wan1vrf)# name-server <primary-DNS-IPv6-address>
ipe(config-vrf-wan1vrf)# name-server <secondary-DNS-IPv6-address>
ipe(config-vrf-wan1vrf)# end
```

7. Verify the configuration.

```
ipe# show ipv6 route vrf wan1vrf
```

Configuring VLAN-based WAN Interface

In deployments where the WAN uplink requires VLAN tagging, configure a VLAN sub-interface on the WAN port. The same configuration steps apply for IPv4 deployments, replace the IPv6 addresses and commands with the corresponding IPv4 equivalents.

1. Remove default DHCP configuration on the parent interface.

```
ipe(config)# interface ethernet <slot>/<port>
ipe(config-if-eth-<slot>/<port>)# no ipv6 address dhcp
ipe(config-if-eth-<slot>/<port>)# exit
```

2. Create the VLAN sub-interface and assign the IPv6 address.

```
ipe(config)# interface ethernet <slot>/<port>
ipe(config-if-eth-<slot>/<port>)# subinterface vlan <vlan-id>
ipe(config-subif)# ipv6 address <IPv6-address>/<prefix-length>
ipe(config-subif)# no shutdown
ipe(config-subif)# exit
```

3. Associate the sub-interface with the WAN VRF and configure the default route.

```
ipe(config)# vrf wan1vrf
ipe(config-vrf-wan1vrf)# member ethernet <slot>/<port> vlan <vlan-id>
```

```
ipe(config-vrf-wan1vrf)# static-route ::/0 <IPv6-nexthop>
ipe(config-vrf-wan1vrf)# end
```

4. Configure DNS servers.

```
ipe(config)# vrf wan1vrf
ipe(config-vrf-wan1vrf)# name-server <primary-DNS-IPv6-address>
ipe(config-vrf-wan1vrf)# name-server <secondary-DNS-IPv6-address>
ipe(config-vrf-wan1vrf)# end
```

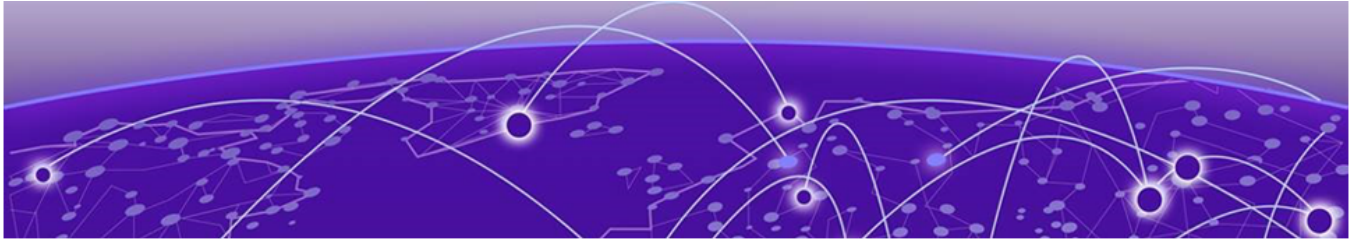
5. Verify the VLAN sub-interface and routing.

```
ipe# show ipv6 interface brief
ipe# show ipv6 route vrf wan1vrf
```

Upgrading Firmware using the ExtremeCloud OS ONE SD-WAN Orchestrator

Follow these steps to upgrade appliance firmware using the ExtremeCloud OS ONE SD-WAN Orchestrator:

1. Go to **Appliances**, or to the **Appliance Details** page.
2. Select an appliance from the list.
3. Select **Utilities** > **Firmware Upgrade**.
4. Upgrade the appliance to the latest firmware version that is specified, or select a specific version from the list.
5. Either select immediate activation or schedule the activation by specifying a date and time.
6. Select **Upgrade Device.**



Configuring Network Policies

General Policy Settings on page 20

General Policy Settings

Configure baseline policy settings required to enable Fabric over SD-WAN in the Orchestrator.

If you are configuring the Orchestrator for the first time, select **Let's get started!** when the onboarding workflow appears.

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

Prerequisites

Fabric Engine must be on version 9.2.0.0 or later.

1. Go to **Settings** > **Policy Configuration.**
2. Select **Edit.**
3. Configure the following policy settings.

Table 5: Policy settings

Setting	Description
General Details	
Policy Name	Network policy name
Description	Optional description

Table 5: 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	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**.
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. In the **Fabric Extend IP Network** field, enter the IPv4 address for the global subnet. This IPv4 address automatically allocates subnets to the LAN interface of each appliance. The Fabric Extend (FE) IP network shows a default subnet of **172.16.0.0/20**. You can change this subnet according to your network requirements. The ExtremeCloud OS ONE SD-WAN Orchestrator automatically subdivides the /20 into multiple /29 networks: • Appliance 1 LAN interface: **172.16.0.0/29** • Appliance 2 LAN interface: **172.16.8.0/29** • Appliance 3 LAN interface: **172.16.16.0/29**
Export Management IP Address	Select Export Management IP Address to advertise the appliance's LAN IP address as a host prefix to the fabric switch. This allows reachability from the fabric, such as SSH.

Table 5: Policy settings (continued)

Setting	Description
Default Fabric Local Breakout Settings	Local breakout settings are disabled by default. You can also enable or disable **Fabric Local Breakout** for individual appliances. 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 valid prefix address and select **Add Prefix**. • To remove a prefix, select the delete icon next to the prefix. 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).

Table 5: Policy settings (continued)

Setting	Description
Overlay Routing	Defines IPSec tunnel settings. Add 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
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.

4. Select Apply to save the settings.

Limitations for Fabric Local Breakout Settings

- Static Internet Prefixes: Internet prefixes are configured as static routes on ExtremeCloud OS ONE SD-WAN appliances, even if local breakout is disabled.
- Export Management IP Behavior: The Export Management IP Address option is 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**: When exporting management IP settings, the appliance LAN IP address is exported automatically and cannot be reconfigured with a distinct or custom management IP value.
- **IPv6 Support**: The local breakout settings do not support pure IPv6 deployments.

Creating Overlays

ExtremeCloud OS ONE 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.

Create an overlay from the **Onboarding Wizard** for the 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** > **Configure Policy** > **Add Overlay**.
2. Select **Hub & Spoke** topology.
3. Provide a pre-shared key for overlay authentication. The PSK is used for all the tunnels between appliances and is automatically generated by the system.
4. Select **Save**.

Table 6: Hub and Spoke Overlay Settings

Setting	Description
General Information	
Name	Specifies the overlay name
IP Version	Select **IPv4** or **IPv6**
Type	Set to **Hub & Spoke**
Hub & Spoke Configuration	
IKE policy	Internet Key Exchange (IKE) is used to authenticate IPsec peers, negotiate keys, and establish security associations. **Encryption:** Select an encryption algorithm to protect data exchanged during key negotiation. **Authentication:** Select a hash algorithm to ensure data integrity during key exchange. **DH group:** Choose a DH group to define the strength of the key exchange. **Rekey time:** Specify how often the IKE Security Association should be renegotiated, in seconds (120–86400).

Table 6: Hub and Spoke Overlay Settings (continued)

Setting	Description
IPsec Concentrator authentication	Define a pre-shared key (PSK) for tunnel authentication between appliances.
IPsec policy	Defines how data is encrypted, authenticated, and transmitted across the IPsec tunnel. **Encryption:** Select an encryption algorithm to protect tunnel traffic. **Authentication:** Choose a hash algorithm to verify data integrity within the IPsec tunnel. **DH Group (PFS):** Choose a DH group for Perfect Forward Secrecy (PFS), which forces a new key for every session. Optional. **SA lifetime:** Set how long an IPsec Security Association remains valid, in seconds (120–86400). Default is 86400. **MTU:** Define the maximum payload size for IPsec tunnel packets. Default is 1400 bytes.

Onboarding Hub Site

Creating a Hub Template on page 27
Adding Hub Sites and Appliances on page 32
Configuring Hub Appliances on page 32
Hub Fabric Engine Switch Configuration on page 41

This section describes how to onboard a hub site, configure its appliance, and integrate it with the Fabric Engine switch.

Note
The configuration shown in this template serves as an example. You can reuse or modify the template based on your specific deployment requirements, appliance roles, and network configuration.

Creating a Hub Template

A Hub template defines the configuration for your data center appliance. The Hub serves as the central aggregation point where all overlay tunnels from Spoke (branch) sites terminate. Because it is deployed in a data center with redundant wired connectivity, LTE is typically not required but can be configured as an emergency backup.

Follow these steps to create a hub template for ExtremeCloud OS ONE SD-WAN appliance deployment:

Use the following tasks to create a hub template, configure template settings, and configure the WAN interface.

Create a Hub Template

1. Go to **Onboard** > **Additional Settings** > **Templates** > **Create Template**.
2. Continue to create a new template and configure the following template details:
   - Template Name
   - Description
   - Appliance Type
     - **IPE**: For IPE series appliances.
     - **XSE-600**: For the Extreme Secure Edge 600 hardware.
3. Select **Next - Setup Interface**.
4. Configure the interface architecture based on your appliance type:

Interface Configuration: IPE

Enable the logical interfaces required for your Hub deployment:

- **LAN 1**: Enabled by default for your local network connection.
- **Path Mode**: Dynamic WAN Switching (DWS) is automatically enabled.
- **WAN 1, WAN 2, and WAN 3**: Enable the wired WAN interfaces available at your data center.
- **WAN 4 (USB)**: Optional - Enable if LTE connectivity is required as a regular WAN link or emergency backup.

Interface Configuration: Extreme Secure Edge 600

The XSE-600 allows you to assign physical hardware ports to specific logical roles. Enable ports by toggling the corresponding switches in the interface diagram:

- **SFP/SFP+ (Ports 1- 4)**: High-speed slots that support fiber or copper SFP/SFP+ modules.
  - **Port 1**: Dedicated to your primary local network (**LAN 1**).
  - **Ports 2, 3, and 4**: Available for your external WAN connections (**WAN 1, WAN 2, and WAN 3**).
- **2.5/1G (Ports 5 - 8)**: Standard copper Ethernet ports supporting speeds up to 2.5 Gbps.
  - **Port 5**: Available for a secondary local network (**LAN 2**) if required.
  - **Ports 6, 7, and 8**: Available for additional WAN connectivity based on your data center requirements.

Note
Only the ports you enable in this step will be available for detailed configuration (such as IP addressing and bandwidth settings) in the subsequent steps.

5. Under Advanced Setup Settings, configure:
   - **Role in Hub & Spoke**: Select **Hub**.
   - **Adaptive QoS**: Enable. This allows the Hub to detect WAN-to-LAN congestion and send bandwidth restriction information to connected Spokes.
   - Select **Next - Configure Interface**.
6. Configure LAN Interface: For LAN interfaces, configure the following Additional Settings
   - 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.
  - NTP: Select Apply Default Policy Settings to use NTP from the network policy or enter custom NTP server addresses. Configure NTP to ensure accurate time synchronization across the Hub appliance and all connected Spoke sites. Accurate timekeeping is critical for certificate validation, logging, and event correlation across the SD-WAN fabric.
  - Select **Next - WAN Settings**.
7. For WAN interfaces, define each interface: WAN1, WAN2, WAN3 and WAN4. Only Router mode is supported. Select the IP version for the WAN interface:

Field	Description
Interface	
Description	Optional description of the WAN interface.
Bandwidth Up	Maximum upload bandwidth in Mbps. Set this value to match the contracted uplink capacity of the data center WAN connection. Default: 10000.
Bandwidth Down	Maximum download bandwidth in Mbps. This value is used by Adaptive QoS to detect WAN-to-LAN congestion and send bandwidth restriction signals to connected Spoke appliances. Set this value to match the contracted downlink capacity. Default: 10000. **Note:** Both Bandwidth Up and Bandwidth Down must be configured accurately on the Hub to ensure correct Adaptive QoS operation across all connected Spoke sites.
Min Bandwidth Up	Minimum guaranteed upload bandwidth in Mbps. This value defines the Committed Information Rate (CIR) for this WAN interface. Recommended value: 10 Mbps.
Min Bandwidth Down	Minimum guaranteed download bandwidth in Mbps. Recommended value: 10 Mbps.
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. **Note:** For WAN 4 (LTE), set the MTU to **1300** to account for cellular encapsulation overhead and avoid IPv6 fragmentation issues.

Field	Description
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. ◦ For wired WAN interfaces (WAN 1-3), set the MSS value based on your MTU requirements. ◦ For WAN 4 (LTE), set the MSS value to **1100**. This is required to prevent BFD, BGP, and IS-IS session flapping over the cellular underlay.
WAN Service	Defines the type of WAN connectivity for this interface. This is used as a label for application policy to identify and steer traffic across WAN interfaces. • **Internet**: Standard Internet connection. Supports overlay tunnels and DTI breakout. • **MPLS**: Private MPLS circuit. Supports site-to-site tunnels only. DTI is not available on MPLS interfaces. • **Broadband**: 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 to exit directly to the Internet through this WAN interface. • **Enabled**: Traffic matching DTI policies exits directly to the Internet 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. Enable DTI on Internet WAN interfaces where local breakout is required at the data center. • **Disabled**: All traffic is forwarded through the ExtremeCloud OS ONE SD-WAN overlay tunnels. **Note:** These values are inherited 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.

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. • **WAN 1, WAN 2, WAN 3 (Wired)**: Set to 100 to ensure wired interfaces are always preferred for overlay tunnel traffic. • **WAN 4 (LTE)**: Set to 10 to ensure the LTE interface is used only as an absolute last resort when all wired WAN links are unavailable. **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 BFD keepalive packets sent over overlay tunnels. Range: 50–30,000 ms. • **WAN 1, WAN 2, WAN 3 (Wired)**: Set to 1000 ms by default. Lower values (for example, 300 ms) may be configured based on the quality, latency, and stability of the specific WAN link if faster failure detection is required. • **WAN 4 (LTE)**: Set to **1000 ms** to accommodate the variable latency characteristics of LTE connections.
BFD Multiplier	Number of consecutive missed BFD packets before declaring the session down. Range: 3 - 50. • **WAN 1, WAN 2, WAN 3 (Wired)**: set to 7 by default. Combined with a 300 ms transmit interval, this provides a failure detection time of 900 ms on wired interfaces. • **WAN 4 (LTE)**: Set to **15**. A higher multiplier is recommended for LTE to prevent false BFD session drops due to cellular link instability.
Additional Settings	
Tunnel Underlay IP Address	Select the type of IP address used to establish overlay tunnels on this WAN interface. • **Public IP Address**: Use when the Hub appliance is behind a NAT device. Configure port forwarding on the internet access router to forward UDP port 500 (IKEv2) and UDP port 4500 (IPsec NAT Traversal) inbound to the Hub appliance's WAN interface IP address. **Note:** A Public IP address is **mandatory** for Hub appliances. All Spoke appliances initiate tunnels toward the Hub, which requires a stable, reachable public endpoint. • **WAN Interface IP Address**: Use when the Hub appliance has a directly assigned public IP address on the WAN interface with no NAT.

Field	Description
WAN Interface IP	Configure the IP address assigned to the physical WAN interface. Use this field when the appliance has a directly assigned public IP address on the WAN interface (no NAT). **Note:** When an IP address is configured manually via the CLI, once the appliance connects to the SD-WAN Orchestrator and pulls its configuration, the Orchestrator configuration will overwrite all manually entered settings from the CLI.
LLDP Settings	Enable or disable Link Layer Discovery Protocol (LLDP) on this WAN interface. When enabled, LLDP packets are sent and received on this interface, allowing the Hub appliance to advertise its identity and discover neighboring devices. **Note:** LLDP Settings is not available for WAN 4 (LTE/USB).
Overlay	Select a Hub & Spoke overlay you previously created and apply it to the interface. The Hub terminates all Spoke-initiated tunnels on this overlay. 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.

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.

Adding Hub Sites and Appliances

Use this task to add a hub site and its associated appliances.

1. In the left navigation pane, select **Onboard**.
2. Select **Add Site**, then enter the site name and address.
3. Select **Next - Add Appliances**.
4. In the appliance list, select the site and the hub template.
5. Enter the appliance name and serial number.
6. Select **Save Changes**.

Note
Use the **`show sysinfo chassis`** command to get the serial number.

Configuring Hub Appliances

Configure hub appliances after they are added. Follow these steps to complete the configuration:

If you are in the onboarding workflow, select **Configure Now** when prompted.

1. If you are in the onboarding workflow, select **Configure Now** when prompted.
2. Configure the following settings:

Table 7: Appliance Configuration Settings

Settings	Description
General Settings	
Managed State	Specifies that the appliance is managed by ExtremeCloud OS ONE SD-WAN Orchestrator. **Note:** Changing an appliance to the unmanaged state reverts the appliance to its factory default configuration: any active SD-WAN overlay tunnels are torn down, IPsec configurations are removed, and traffic routing, monitoring, and alarming cease. 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.
Template	You can change the Hub appliance template associated with this appliance. **Note:** If you select another template, all default settings are updated according to the default configuration of the new appliance template. All other settings are extracted from the applied template.
Local AS	The Local AS is set to Auto by default, or you can specify a custom AS number. 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. **Note:** If multiple appliances are deployed at the same site for redundancy, the Orchestrator does not automatically match their AS numbers. You must manually ensure that all appliances at the same site are configured with the same Local AS number.
Path Mode	Dynamic Path Mode is only supported.
Hub & Spoke	This appliance is configured as a Hub. As a best practice, do not modify this setting. This setting determines which appliances initiate and respond to IPsec tunnel connections across the overlay network.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
Adaptive Qos	Detects WAN-to-LAN congestion at the Hub and sends bandwidth restriction signals to all connected Spoke appliances to apply traffic shaping on their remote links.
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	The Hub 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. The default value is a host IP address from the /29 subnet allocated to this appliance. • **Fabric Switch LAN**: The Fabric Switch LAN IPv4 address 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. Any modification to the IS-IS metric on the Hub is automatically replicated to all connected Spoke appliances.
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 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	Supported range: 1280 to 9194.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
DNS Server Settings	**Apply Default Policy Settings** Enable this option to automatically apply the predefined DNS settings from the Policy Configuration. **DNS Server Settings** Define DNS resolution behavior for the Hub 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. Hub appliances typically do not use local breakout because Internet-bound traffic at hub sites is routed through the hub site's perimeter firewall rather than directly out the hub appliance's WAN interface. If required for a specific deployment model, clear **Apply default policy settings** to expand and configure Fabric Local Breakout for this individual Hub appliance.
Static Route	**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.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
Subnet	Specifies the IP subnets associated with this appliance. In ExtremeCloud OS ONE SD-WAN, these subnet definitions enable the Orchestrator to identify the specific appliance where traffic originating from each subnet is located across the fabric. • 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.
WAN	
WAN 1, WAN 2, WAN 3	Select a WAN interface tab to view and configure its settings. The mode and IP address range for the selected WAN is indicated. Valid values for IP address range are: IPv4 or IPv6.
Enabled	Enable or disable the WAN interface. • Enabled: Activates the WAN interface and allows the system to use the interface for WAN connectivity and traffic forwarding. • Disabled: Deactivates the WAN interface. When disabled, the interface is not used for traffic forwarding or path selection. The Hub appliance does not establish overlay tunnels or BGP sessions on this interface.
Interface	
Description	Optional description of the WAN.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
Bandwidth Up and Down	• **Bandwidth Up**: Maximum upload bandwidth in Mbps. Set this value to match the contracted uplink capacity of the data center WAN connection. Default: 10000. • **Bandwidth Down**: Maximum download bandwidth in Mbps. This value is used by Adaptive QoS to detect WAN-to-LAN congestion and send bandwidth restriction signals to connected Spoke appliances. Set this value to match the contracted downlink capacity. Default: 10000. **Note:** Both Bandwidth Up and Bandwidth Down must be configured accurately on the Hub to ensure correct Adaptive QoS operation across all connected Spoke sites.
Interface Speed	The physical interface speed of the WAN port.
MTU	Maximum Transmission Unit size in bytes for this WAN interface. For WAN 4 (LTE), set the MTU to 1300 to account for cellular encapsulation overhead and avoid fragmentation issues.
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. ◦ For wired WAN interfaces (WAN 1–3), set the MSS value based on your MTU requirements. ◦ For WAN 4 (LTE), set the MSS value to **1100** to prevent BFD, BGP, and IS-IS session flapping over the cellular underlay.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
WAN Service	Defines the type of WAN connectivity for this interface. This is used as a label for application policy to identify and steer traffic across WAN interfaces. • **Internet**: Standard Internet connection. Supports overlay tunnels and DTI breakout. • **MPLS**: Private MPLS circuit. Supports site-to-site tunnels only. DTI is not available on MPLS interfaces. • **Broadband**: 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.
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 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. Enable DTI on Internet WAN interfaces where local breakout is required at the data center. DTI must remain disabled on MPLS interfaces. • 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.
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	

Table 7: Appliance Configuration Settings (continued)

Settings	Description
Tunnel Underlay IP Address	Select the type of IP address used to establish overlay tunnels on this WAN interface. • **Public IP Address**: Use when the Hub appliance is behind a NAT device (for example, an internet access router). Configure port forwarding on the internet access router to forward **UDP port 500** (IKEv2) and **UDP port 4500** (IPsec NAT Traversal) inbound to the Hub appliance's WAN interface IP address. **Note:** A Public IP address is mandatory for Hub appliances. All Spoke appliances initiate tunnels toward the Hub, which requires a stable, reachable public endpoint. • **WAN Interface IP Address**: Use when the Hub appliance has a directly assigned public IP address on the WAN interface with no NAT. The tunnel uses the IP address configured on the physical WAN interface itself.
WAN Interface IP Address	Configure the IPv6 address assigned to the physical WAN interface. Use this field when the Hub appliance has a directly assigned public IP address on the WAN interface (no NAT). **Note:** If DHCP or IPoE are not enabled, you must manually configure the IP addresses. Do not mix IP address configuration methods between CLI and the SD-WAN Orchestrator on the same WAN sub-interface. Use either the Orchestrator or the CLI exclusively for each interface to avoid configuration conflicts.
Routing	

Table 7: Appliance Configuration Settings (continued)

Settings	Description
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. • WAN 1, WAN 2, WAN 3 (Wired): Set to **100** to ensure wired interfaces are always preferred for overlay tunnel traffic. • WAN 4 (LTE): Set to **10** to ensure the LTE interface is used only as an absolute last resort when all wired WAN links are unavailable. **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. • WAN 1, WAN 2, WAN 3 (Wired): Set to **300 ms**. Tighter BFD timers are required on the Hub as it aggregates tunnels from multiple Spoke sites. • WAN 4 (LTE): Set to **1000 ms** to accommodate the variable latency characteristics of LTE connections. **BFD Multiplier**: Number of consecutive missed BFD packets before declaring the session down. Range: 3-50 The settings apply to all overlay BGP sessions on this WAN interface. Per-tunnel BFD profiles configured under Site-to-Site Tunnels can override these values for individual tunnels
Tunnels	
Overlay	Select a Hub & Spoke overlay you previously created and apply it to the interface. The Hub terminates all Spoke-initiated tunnels on this overlay. Select Configure Tunnel to view the Overlay Details.

Table 7: Appliance Configuration Settings (continued)

Settings	Description
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.

3. Select **Save**.
4. If you are in the onboarding workflow, select **Next – Review Configuration**, and then **Next – Deploy Configuration**.
5. If you are configuring via **Appliance** section, select **Deploy Configuration**. The ExtremeCloud OS ONE SD-WAN Orchestrator pushes the configuration immediately if the appliance is online or when it reconnects.
6. Select **Deploy** to complete the setup.

Hub Fabric Engine Switch Configuration

Use this task to verify the switch connectivity and fabric configuration for the hub appliances.

1. Connect the Fabric Engine switch to the ExtremeCloud OS ONE SD-WAN appliance.
2. Use the following command to confirm auto-sense state:

show interface gigabitEthernet auto-sense

```
Device#show interface gigabitEthernet auto-sense
********************************************************************************

********************************************************************************

================================================================================
=============
                                Port Auto-sense
```

```
================================================================================================
=============
------------------------------------------------------------------------------------------------
--------------------
PORT     AUTO-SENSE   AUTO-SENSE         AUTO-SENSE       AUTO-SENSE
NUM      STATUS       STATE              PORT-DATA-ISID   PORT-WAIT-INTERVAL
------------------------------------------------------------------------------------------------
--------------------
1/1      Enable       SD-WAN             --               35
1/2      Enable       DOWN               --               35
1/3      Enable       DOWN               --               35
1/4      Enable       DOWN               --               35
1/5      Enable       DOWN               --               35
1/6      Enable       DOWN               --               35
1/7      Enable       DOWN               --               35
1/8      Enable       DOWN               --               35
1/9      Enable       DOWN               --               35
1/10     Enable       DOWN               --               35
1/11     Enable       DOWN               --               35
1/12     Enable       DOWN               --               35
```

Output should show **AUTO-SENSE STATE** as **SD-WAN** on the connected port.

3. Verify that VRF sd-wan is automatically created:

show ip vrf

```
Device#show ip vrf
********************************************************************************

********************************************************************************


================================================================================================
===============
                                                                    VRF INFORMATION
================================================================================================
===============
VRF       VLAN      ARP       RIP       OSPF      BGP       PIM       NBRv6     RIPng
OSPFv3    PIM6
COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT
COUNT     COUNT
------------------------------------------------------------------------------------------------
------------------------------------------------
3         6         3         1         1         2         1         0         1
1         1

VRF                        VRF  VLAN   ARP
NBRv6                       UNICAST  SD-WAN LOCAL  VRF
NAME                       ID   COUNT  COUNT  RIP    OSPF   BGP    PIM    COUNT
RIPng  OSPFv3 PIM6   ACTIVE   BREAKOUT      ORIGIN
------------------------------------------------------------------------------------------------
------------------------------------------------
GlobalRouter               0    4      0      TRUE   TRUE   TRUE   TRUE   0
TRUE   TRUE   TRUE   TRUE     FALSE         DYNAMIC
sd-wan                     511  1      3      FALSE  FALSE  TRUE   FALSE  0
FALSE  FALSE  FALSE  TRUE     FALSE         DYNAMIC
MgmtRouter                 512  1      0      FALSE  FALSE  FALSE  FALSE  0
FALSE  FALSE  FALSE  TRUE     FALSE         DYNAMIC
```

```
3 out of 3 Total Num of VRF Entries displayed.
```

4. Confirm that VLAN 4047 is created and associated with the VRF:

show interfaces vlan vrfs vrf sd-wan

```
Device#show interfaces vlan vrfs vrf sd-wan
********************************************************************************

********************************************************************************

================================================================================
=============
                              VLAN VRF Association
================================================================================
=============
VLAN  VRF
ID    NAME
--------------------------------------------------------------------------------
--------------------
4047  sd-wan

All 5 out of 5 Total Num of Vlan VRF Association entries displayed
```

5. Check IP assignment to VLAN 4047:

show ip interface vrf sd-wan

```
Device#show ip interface vrf sd-wan
********************************************************************************

********************************************************************************

================================================================================
=============
                           IP Interface - VRF sd-wan
================================================================================
=============
INTERFACE    IP               NET              ADMIN      OPER     VLAN  BROUTER
IPSEC   IP
             ADDRESS          MASK             STATUS     STATE    ID    PORT
STATE   NAME
--------------------------------------------------------------------------------
--------------------
Vlan4047     172.16.0.12      255.255.255.248  enable     up       4047  false
disable SD-WAN Tunnel SrcIP


All 1 out of 1 Total Num of IP interfaces displayed
```

Confirm that VLAN 4047 is assigned an IP from the Fabric Extend network.

Note

On Static Routes:

- Each FE tunnel gets a /32 static route to the tunnel destination (next-hop: SD-WAN LAN IP).
- These routes do not interfere with existing ISIS/OSPF routes.

NTP Verification

Use these commands to confirm that the appliance is synchronized with the configured NTP servers before proceeding with further deployment steps.

Verify time synchronization using the following commands:

To display the current NTP synchronization status of the appliance.

show ntp status

```
BNLTE-IPE-1#
BNLTE-IPE-1# show ntp status
Clock is synchronized,  stratum 3, reference clock is 204.197.163.71,
precision is -23,
reference time is ec62931b.625397ad  Wed, Sep  3 2025 10:12:43.384,
clock offset is +3.212811, root delay is 70.462,
root dispersion is 195.367, peer dispersion is 55900,
NTP client mode is enabled (VRF: wan2vrf)
```

To list NTP associations and peers configured on the appliance.

show ntp association

```
BNLTE-IPE-1#
BNLTE-IPE-1#
BNLTE-IPE-1# show ntp association
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*204.197.163.71  177.115.13.154   2 u  410   64  100   69.745   +1.613   1.521

* synced, # selected, + candidate, - outlayer, x falseticker, ~ configured
BNLTE-IPE-1#
```

Onboarding Spoke Site

Creating a Spoke Template on page 46
Adding Spoke Sites and Appliances on page 51
Configuring Spoke Appliances on page 51
Branch Fabric Engine Switch Configuration on page 59

This section describes how to onboard a spoke site, configure its ExtremeCloud OS ONE SD-WAN appliance, and integrate it with the Fabric Engine switch.

Note
The configuration outlined here serves as an example. You can reuse or modify the template based on your specific deployment requirements, appliance roles, and network configuration.

Creating a Spoke Template

A Spoke template defines the configuration for your branch office appliance. The Spoke initiates all overlay tunnels toward the Hub and is typically deployed at remote sites with one or two wired WAN connections. LTE is commonly used as a backup link at branch locations.

Follow these steps to create a spoke template for ExtremeCloud OS ONE SD-WAN appliance deployment:

Use the following tasks to create a spoke template, configure template settings, and configure the WAN interface.

Create a Spoke Template

1. Go to **Onboard** > **Additional Settings** > **Templates** > **Create Template**.
2. Continue to create a new template and configure the following template details:
   - Template Name
   - Description
   - Appliance Type
     - **IPE**: For IPE series appliances.
     - **XSE-600**: For the Extreme Secure Edge 600 hardware.
3. Select **Next - Setup Interface**.
4. Configure the interface architecture based on your appliance type:

Interface Configuration: IPE

Enable the logical interfaces required for your Hub deployment:

- **LAN 1**: Enabled by default for your local network connection.
- **Path Mode**: Dynamic WAN Switching (DWS) is automatically enabled.
- **WAN 1, WAN 2, and WAN 3**: Enable the wired WAN interfaces available at your data center.
- **WAN 4 (USB)**: Optional - Enable if LTE connectivity is required as a regular WAN link or emergency backup.

Interface Configuration: Extreme Secure Edge 600

The XSE-600 allows you to assign physical hardware ports to specific logical roles. Enable ports by toggling the corresponding switches in the interface diagram:

- **SFP/SFP+ (Ports 1- 4)**: High-speed slots that support fiber or copper SFP/SFP+ modules.
  - **Port 1**: Dedicated to your primary local network (**LAN 1**).
  - **Ports 2, 3, and 4**: Available for your external WAN connections (**WAN 1, WAN 2, and WAN 3**).
- **2.5/1G (Ports 5 - 8)**: Standard copper Ethernet ports supporting speeds up to 2.5 Gbps.
  - **Port 5**: Available for a secondary local network (**LAN 2**) if required.
  - **Ports 6, 7, and 8**: Available for additional WAN connectivity based on your data center requirements.

Note
Only the ports you enable in this step will be available for detailed configuration (such as IP addressing and bandwidth settings) in the subsequent steps.

5. Under Advanced Setup Settings, configure:
   - **Role in Hub & Spoke**: Select **Hub**.
   - **Adaptive QoS**: Enable. The Spoke participates in link utilization exchange with the Hub, allowing the network to dynamically adjust traffic shaping and prevent congestion at the branch site when its WAN links become saturated.
   - Select **Next - Configure Interface**.
6. Configure LAN Interface: For LAN interfaces, configure the following Additional Settings
   - 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. Define DNS resolution behavior by specifying up to three DNS server IP addresses under Servers. If you do not specify a DNS server, you must manually configure the DNS server addresses.
- NTP: Select **Apply Default Policy Settings** to use NTP from the network policy or enter custom NTP server addresses. Configure NTP to ensure accurate time synchronization between the Spoke appliance and the Hub. Accurate timekeeping is critical for certificate validation, logging, and event correlation across the SD-WAN fabric.
- Select **Next - WAN Settings**.

7. For WAN interfaces, define each interface: WAN1, WAN2, WAN3 and WAN4. Only Router mode is supported. Select the IP version for the WAN interface:

Field	Description
Interface	
Description	Optional description of the WAN interface.
Bandwidth Up	Maximum upload bandwidth in Mbps. Set this value to match the contracted uplink capacity of the branch site WAN connection. Default: 10000.
Bandwidth Down	Maximum download bandwidth in Mbps. Set this value to match the contracted downlink capacity at the branch site. 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. **Note:** For WAN 4 (LTE), set the MTU to **1300** to account for cellular encapsulation overhead and avoid IPv6 fragmentation issues.

Field	Description
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. ◦ For wired WAN interfaces (WAN 1-3), set the MSS value based on your MTU requirements. ◦ For WAN 4 (LTE), set the MSS value to **1100**. This is required to prevent BFD, BGP, and IS-IS session flapping over the cellular underlay.
WAN Service	Defines the type of WAN connectivity for this interface. This is used as a label for application policy to identify and steer traffic across WAN interfaces. • **Internet**: Standard Internet connection. Supports overlay tunnels and DTI breakout. • **MPLS**: Private MPLS circuit. Supports site-to-site tunnels only. DTI is not available on MPLS interfaces. • **Broadband**: 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 to exit directly to the Internet through this WAN interface. • **Enabled**: Traffic matching DTI policies exits directly to the Internet 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. Enable DTI on Internet WAN interfaces where local breakout is required at the branch site. • **Disabled**: All traffic is forwarded through the ExtremeCloud OS ONE SD-WAN overlay tunnels toward the Hub. **Note:** These values are inherited 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.

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. • **WAN 1, WAN 2, WAN 3 (Wired)**: Set to 100 to ensure wired interfaces are always preferred for overlay tunnel traffic. • **WAN 4 (LTE)**: Set to 50 to ensure the LTE interface is used only as a backup when wired WAN links are unavailable, while still providing a viable alternate path. **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 BFD keepalive packets sent over overlay tunnels. Range: 50–30,000 ms. • **WAN 1, WAN 2, WAN 3 (Wired)**: Set to **1000** ms (default). Standard BFD timers are used on Spoke appliances since they typically maintain fewer tunnel sessions than the Hub. • **WAN 4 (LTE)**: Set to **1000 ms** to accommodate the variable latency characteristics of LTE connections.
BFD Multiplier	Number of consecutive missed BFD packets before declaring the session down. Range: 3 - 50. • **WAN 1, WAN 2, WAN 3 (Wired)**: Set to **7** (default). This provides a failure detection time of 7 seconds on wired interfaces. • **WAN 4 (LTE)**: Set to **15**. A higher multiplier is recommended for LTE to prevent false BFD session drops due to cellular link instability.
Additional Settings	
Tunnel Underlay IP Address	Select the type of IP address used to establish overlay tunnels on this WAN interface. • **Public IP Address**: Use when the Spoke appliance is behind a NAT device. Configure port forwarding on the internet access router to forward UDP port 500 (IKEv2) and UDP port 4500 (IPsec NAT Traversal) inbound to the Spoke appliance's WAN interface IP address. **Note:** For Spoke appliances, a Public IP address is optional unless a site-to-site tunnel between Spoke sites is required. • **WAN Interface IP Address**: Use when the Spoke appliance has a directly assigned public IP address on the WAN interface with no NAT. The tunnel uses the IP address configured on the physical WAN interface itself.

Field	Description
WAN Interface IP	Configure the IP address assigned to the physical WAN interface. Use this field when the appliance has a directly assigned public IP address on the WAN interface (no NAT). **Note:** When an IP address is configured manually via the CLI, once the appliance connects to the SD-WAN Orchestrator and pulls its configuration, the Orchestrator configuration will overwrite all manually entered settings from the CLI.
LLDP Settings	Enable or disable Link Layer Discovery Protocol (LLDP) on this WAN interface. When enabled, LLDP packets are sent and received on this interface, allowing the Spoke appliance to advertise its identity and discover neighboring devices. **Note:** LLDP Settings is not available for WAN 4 (LTE/USB).
Overlay	Select a Hub & Spoke overlay you previously created and apply it to the interface. The Spoke initiates all tunnels toward the Hub on this overlay. 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.

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.

Adding Spoke Sites and Appliances

Use this task to add a spoke site and its associated appliances.

1. In the left navigation pane, select **Onboard**.
2. Select **Add Site**, then enter the site name and address.
3. Select **Next - Add Appliances**.
4. In the appliance list, select the site and the spoke template.
5. Enter the appliance name and serial number.
6. Select **Save Changes**.

Configuring Spoke Appliances

Configure spoke appliances after they are added. Follow these steps to complete the configuration:

If you are in the onboarding workflow, select **Configure Now** when prompted.

1. If you are in the onboarding workflow, select **Configure Now** when prompted.
2. Configure the following settings:

Table 8: Appliance Configuration Settings

Settings	Description
General Settings	
Managed State	Specifies that the appliance is managed by ExtremeCloud OS ONE SD-WAN Orchestrator. **Note:** Changing an appliance to the unmanaged state reverts the appliance to its factory default configuration: any active SD-WAN overlay tunnels are torn down, IPsec configurations are removed, and traffic routing, monitoring, and alarming cease. The appliance license is no longer consumed.
Appliance Name	You can change the name of the Spoke appliance.
Site	You can change the branch site that the Spoke appliance is associated with.
Template	You can change the Spoke appliance template associated with this appliance. **Note:** If you select another template, all default settings are updated according to the default configuration of the new appliance template. All other settings are extracted from the applied template.
Local AS	The Local AS is set to **Auto** by default, or you can specify a custom AS number. 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. **Note:** If multiple appliances are deployed at the same site for redundancy, the Orchestrator does not automatically match their AS numbers. You must manually ensure that all appliances at the same site are configured with the same Local AS number.
Path Mode	Dynamic Path Mode is only supported.
Hub & Spoke	This appliance is configured as a **Spoke**. As a best practice, do not modify this setting. This setting determines which appliances initiate and respond to IPsec tunnel connections across the overlay network.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
Adaptive Qos	Dynamically adjusts traffic shaping based on link utilization information exchanged between the Spoke and the Hub. The Hub considers both its local uplink capacity and the Spoke's downlink availability when making traffic-shaping decisions. This prevents congestion at the branch site when its WAN links become saturated and improves application performance across the network.
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	The Spoke 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. The default value is a host IP address from the /29 subnet allocated to this appliance. • Fabric Switch LAN: The Fabric Switch LAN IPv4 address 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. The Spoke inherits the IS-IS metric from the Hub unless overridden here.
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 modify the IS-IS Metric value for both the local and remote appliances if needed.
Advanced Settings	

Table 8: Appliance Configuration Settings (continued)

Settings	Description
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	Supported range: 1280 to 9194.
DNS Server Settings	**Apply Default Policy Settings** Enable this option to automatically apply the predefined DNS settings from the Policy Configuration. **DNS Server Settings** Define DNS resolution behavior for the Spoke appliance by specifying up to three DNS server IP addresses under **Servers**. If you do not specify a DNS server, you must manually configure the DNS server addresses. DHCP is not supported in Fabric mode.
NTP Settings	**Apply Default Policy Settings**: Enable this option to automatically apply the predefined NTP settings from the Policy Configuration. **NTP Server Settings**: Specify custom NTP server addresses for this Spoke appliance. Accurate time synchronization with the Hub is critical for certificate validation, event logging, and consistent routing behavior across the SD-WAN fabric.
Fabric Settings	
Fabric Local Breakout Settings	Fabric Local Breakout Settings are disabled by default. Disable **Apply default policy settings** to expand and configure Fabric Local Breakout for this individual Spoke appliance.
Static Route	**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.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
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 its settings. The mode and IP address range for the selected WAN is indicated. Valid values for IP address range are: IPv4 or IPv6.
Enabled	Enable or disable the WAN interface. • Enabled: Activates the WAN interface and allows the system to use the interface for WAN connectivity and traffic forwarding. • Disabled: Deactivates the WAN interface. When disabled, the interface is not used for traffic forwarding or path selection. The Hub appliance does not establish overlay tunnels or BGP sessions on this interface.
Interface	
Description	Optional description of the WAN.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
Bandwidth Up and Down	• **Bandwidth Up**: Maximum upload bandwidth in Mbps. Set this value to match the contracted uplink capacity of the data center WAN connection. Default: 10000. • **Bandwidth Down**: Maximum download bandwidth in Mbps. Set this value to match the contracted downlink capacity at this branch site. This value is exchanged with the Hub for Adaptive QoS traffic-shaping decisions. Default: 10000.
Interface Speed	The physical interface speed of the WAN port.
MTU	Maximum Transmission Unit size in bytes for this WAN interface. For WAN 4 (LTE), set the MTU to 1300 to account for cellular encapsulation overhead and avoid fragmentation issues.
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. ◦ For wired WAN interfaces (WAN 1–3), set the MSS value based on your MTU requirements. ◦ For WAN 4 (LTE), set the MSS value to **1100** to prevent BFD, BGP, and IS-IS session flapping over the cellular underlay.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
DTI	Select the Direct-to-Internet (DTI) option to allow traffic to exit directly to the Internet through this WAN interface. • **Enabled**: Traffic matching DTI policies exits directly to the Internet 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 ExtremeCloud OS ONE SD-WAN overlay tunnels toward the Hub. DTI must remain disabled on MPLS interfaces. **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.
LLDP Settings	Enable or disable Link Layer Discovery Protocol on this WAN interface. When enabled, LLDP packets are sent and received on this interface, allowing the Spoke appliance to advertise its identity and discover neighboring devices. LLDP Settings is not available for WAN 4 (USB).
IP Addresses	
Tunnel Underlay IP Address	Select the type of IP address used to establish overlay tunnels on this WAN interface. • **Public IP Address**: Use when the Spoke appliance is behind a NAT device. Configure port forwarding on the internet access router to forward UDP port 500 (IKEv2) and UDP port 4500 (IPsec NAT Traversal) inbound to the Spoke appliance's WAN interface IP address. **Note:** For Spoke appliances, a Public IP address is optional unless a site-to-site tunnel between Spoke sites is required. • **WAN Interface IP Address**: Use when the Spoke appliance has a directly assigned public IP address on the WAN interface with no NAT.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
WAN Interface IP Address	Configure the IPv6 address assigned to the physical WAN interface. Use this field when the Spoke appliance has a directly assigned public IP address on the WAN interface (no NAT). **Note:** Do not mix IP address configuration methods between CLI and the SD-WAN Orchestrator on the same WAN sub-interface. Use either the Orchestrator or the CLI exclusively for each interface to avoid configuration conflicts.
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. WAN 1, WAN 2, WAN 3 (Wired): 100. WAN 4 (LTE): 50 — lower than wired to ensure wired paths are always preferred, while still providing a viable backup path. **BFD Transmit Interval**: Interval in milliseconds between BFD keepalive packets. Range: 50–30,000 ms. WAN 1, WAN 2, WAN 3 (Wired): 1000 ms (default). WAN 4 (LTE): 1000 ms. **BFD Multiplier**: Number of consecutive missed BFD packets before declaring the session down. Range: 3–50. WAN 1, WAN 2, WAN 3 (Wired): 7 (default — failure detection time: 7 seconds). WAN 4 (LTE): 15 to prevent false BFD session drops due to cellular link instability. The settings apply to all overlay BGP sessions on this WAN interface. Per-tunnel BFD profiles configured under Site-to-Site Tunnels can override these values for individual tunnels.
Tunnels	
Overlay	Select a Hub & Spoke overlay you previously created and apply it to the interface. The Hub terminates all Spoke-initiated tunnels on this overlay. Select **Configure Tunnel** to view the Overlay Details.

Table 8: Appliance Configuration Settings (continued)

Settings	Description
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.

3. Select **Save**.
4. If you are in the onboarding workflow, select **Next – Review Configuration**, and then **Next – Deploy Configuration**.
5. If you are configuring via **Appliance** section, select **Deploy Configuration**. The SD-WAN Orchestrator pushes the configuration immediately if the appliance is online or when it reconnects.
6. Select **Deploy** to complete the setup.

Branch Fabric Engine Switch Configuration

Verify switch connectivity and confirm that the Fabric configuration is correctly applied for spoke appliances.

1. Connect the Fabric Engine switch to the ExtremeCloud OS ONE SD-WAN appliance's LAN1 port.
2. Enable auto-sense on all ports connected to the ExtremeCloud OS ONE SD-WAN appliance. This step is not required for factory-default switches.
3. Verify auto-sense state using the following command:

   Ensure the **`AUTO-SENSE STATE`** displays **`SD-WAN`** for the correct port.

   `show interface gigabitEthernet auto-sense`

```
Device#show interface gigabitEthernet auto-sense
********************************************************************************
```

```
********************************************************************************

================================================================================
=============
                                Port Auto-sense
================================================================================
=============
--------------------------------------------------------------------------------
--------------------
PORT     AUTO-SENSE   AUTO-SENSE         AUTO-SENSE       AUTO-SENSE
NUM      STATUS       STATE              PORT-DATA-ISID   PORT-WAIT-INTERVAL
--------------------------------------------------------------------------------
--------------------
1/1      Enable       SD-WAN             --               35
1/2      Enable       DOWN               --               35
1/3      Enable       DOWN               --               35
1/4      Enable       DOWN               --               35
1/5      Enable       DOWN               --               35
1/6      Enable       DOWN               --               35
1/7      Enable       DOWN               --               35
1/8      Enable       DOWN               --               35
1/9      Enable       DOWN               --               35
1/10     Enable       DOWN               --               35
1/11     Enable       DOWN               --               35
1/12     Enable       DOWN               --               35
```

4. Confirm the VRF **sd-wan** is automatically created:

   VRF **sd-wan** should appear as a dynamic entry.

   show ip vrf

```
Device#show ip vrf
********************************************************************************

********************************************************************************


================================================================================
===============
                                                                VRF INFORMATION
================================================================================
===============
VRF       VLAN      ARP       RIP       OSPF      BGP       PIM       NBRv6     RIPng
OSPFv3   PIM6
COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT     COUNT
COUNT    COUNT
--------------------------------------------------------------------------------
--------------------------------------------------
3         6         3         1         1         2         1         0         1
1        1

VRF                        VRF  VLAN   ARP
NBRv6                       UNICAST  SD-WAN LOCAL  VRF
NAME                       ID   COUNT  COUNT  RIP    OSPF   BGP    PIM    COUNT
RIPng  OSPFv3 PIM6   ACTIVE   BREAKOUT      ORIGIN
--------------------------------------------------------------------------------
--------------------------------------------------
GlobalRouter               0    4      0      TRUE   TRUE   TRUE   TRUE   0
TRUE   TRUE   TRUE   TRUE     FALSE         DYNAMIC
sd-wan                     511  1      3      FALSE  FALSE  TRUE   FALSE  0
```

```
FALSE  FALSE  FALSE  TRUE     FALSE         DYNAMIC
MgmtRouter                512  1      0      FALSE  FALSE  FALSE  FALSE  0
FALSE  FALSE  FALSE  TRUE     FALSE         DYNAMIC

3 out of 3 Total Num of VRF Entries displayed.
```

5. Confirm VLAN 4047 is created and associated with the **sd-wan** VRF:

   show interfaces vlan vrfs vrf sd-wan

```
Device#show interfaces vlan vrfs vrf sd-wan
********************************************************************************

********************************************************************************

================================================================================
=============
                              VLAN VRF Association
================================================================================
=============
VLAN  VRF
ID    NAME
--------------------------------------------------------------------------------
--------------------
4047  sd-wan

All 5 out of 5 Total Num of Vlan VRF Association entries displayed
```

6. Verify that VLAN 4047 has received an IP address:

   show ip interface vrf sd-wan

```
Device#show ip interface vrf sd-wan
********************************************************************************
                Command Execution Time: Tue Aug 25 19:29:06 2026 UTC
********************************************************************************

================================================================================
=============
                           IP Interface - VRF sd-wan
================================================================================
=============
INTERFACE    IP               NET              ADMIN      OPER     VLAN  BROUTER
IPSEC   IP
             ADDRESS          MASK             STATUS     STATE    ID    PORT
STATE   NAME
--------------------------------------------------------------------------------
--------------------
Vlan4047     172.16.0.12      255.255.255.248  enable     up       4047  false
disable SD-WAN Tunnel SrcIP


All 1 out of 1 Total Num of IP interfaces displayed
```

   Confirm the interface IP matches the SD-WAN Orchestrator configuration.

7. Confirm the FE tunnel interface is operational:

The SD-WAN logical interface should show as **UP**.

show isis logical-interface

```
Device#show isis logical-interface
********************************************************************************

********************************************************************************
================================================================================================
===============
                                                                                ISIS Logical
Interfaces
================================================================================================
===============
IFIDX    NAME             ENCAP        L2_INFO                    TUNNEL
L3_TUNNEL_NEXT_HOP_INFO               BFD      TUNNEL          ORIGIN ISIS    SDWAN
                         TYPE         PORT/MLT   VIDS(PRIMARY)   DEST-IP
PORT/MLT   VLAN      VRF              STATUS   SRC-IP                 MTU     OPER
STATE
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
1        SD-WAN-1         IP           --         --              172.16.0.42
Port1/1    4047      sd-wan           disabled 172.16.0.12     ZTF    1600    DOWN
2        SD-WAN-2         IP           --         --              172.16.0.4
Port1/1    4047      sd-wan           disabled 172.16.0.12     ZTF    1600    UP

------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
 2 out of 2 Total Num of Logical ISIS interfaces
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
```

8. Verify ISIS adjacencies between spoke and hub:

   The output should confirm an active adjacency with the hub switch

show isis adjacencies

```
Device#show isis adjacencies
********************************************************************************

********************************************************************************

================================================================================================
===============
                                                              ISIS Adjacencies
================================================================================================
===============
INTERFACE         L STATE        UPTIME PRI HOLDTIME   SYSID             HOST-
NAME                 STATUS   AREA       AREA-NAME
------------------------------------------------------------------------------------------------
------------------------------------------
SD-WAN-2          1 UP      7d 15:01:29 127         26 a497.91ad.c484    5420F-24T-4XE-
FabricEngine ACTIVE   HOME

------------------------------------------------------------------------------------------------
------------------------------------------
Home:   1 out of 1 interfaces have formed an adjacency
------------------------------------------------------------------------------------------------
```

```
-----------------------------------------
```

9. Verify LLDP neighbor information for the connected port:

show lldp neighbor detail port 1/1

```
Device#show lldp neighbor detail port 1/1
********************************************************************************

********************************************************************************

================================================================================
===
                                      LLDP Detail
================================================================================
===
LLDP neighbor with index 5 discovered on port 1/1:
  Chassis:
    Index: 5
    Protocol: LLDP
    ID Subtype: MAC Address(4)
    ID: 00:07:32:c4:3d:d9
    Name: spoke-1
    Description: ExtremeCloud SDWAN S/N: A0525V0080A0
    Available Capabilities:
    Enabled Capabilities:
    Management addresses:
      IPv4: 172.16.0.9
  Port index: 1
  Protocol: LLDP
  Description: Ethernet 0/1
  MFS: 0

  DOT3:
    Autonegotiation: not present
    Advertised Autonegotiation: 0
    mau type: 65535
    Aggregation ID: 0
  Dot3_at: not present
  DOT1:
    p-vid: 0
    Vlans:
  Remote Call Servers: not present
  Remote File Servers: not present
  ZTF-FE:
    Auth: Ok
    Local IP: 172.16.0.12/29
    Gateway IP: 172.16.0.9
    MTU: 2000
    Switch BGP ASN: 4200064513
    SD-WAN BGP ASN: 64513
    BGP_VROUTER_IPV4_1: 172.16.0.9
    BGP_VROUTER_IPV4_2: 0.0.0.0
    BGP_VROUTER_IPV4_3: 0.0.0.0
   Group 1:
     Status: Enabled

     Metric: 20000
     Tunnel to: 172.16.0.4
   Group 2:
     Status: Disabled
```

```
     Metric: 20000
     Tunnel to: 172.16.0.42

-------------------------------------------------------------------------------------------
---
Total LLDP detailed entries displayed: 1
-------------------------------------------------------------------------------------------
---
```

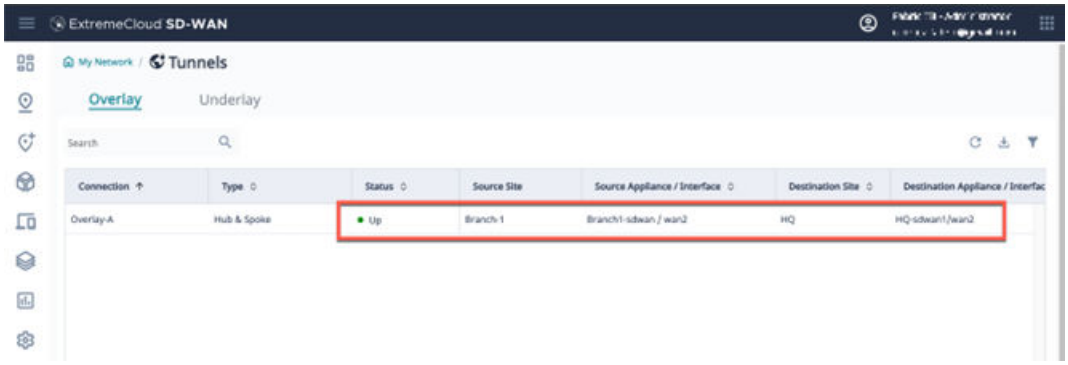
Ensure tunnel-related fields such as ZTF-FE, Tunnel to, and BGP parameters are correctly displayed.

SD-WAN Orchestrator Verification

Verify operational status and tunnel establishment from the ExtremeCloud OS ONE SD-WAN dashboard.

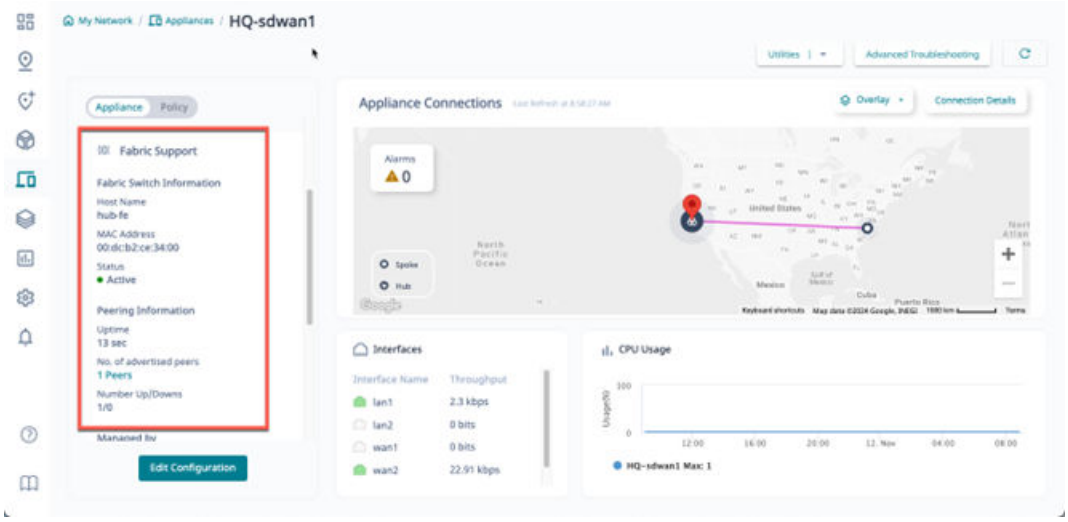
SD-WAN Tunnels

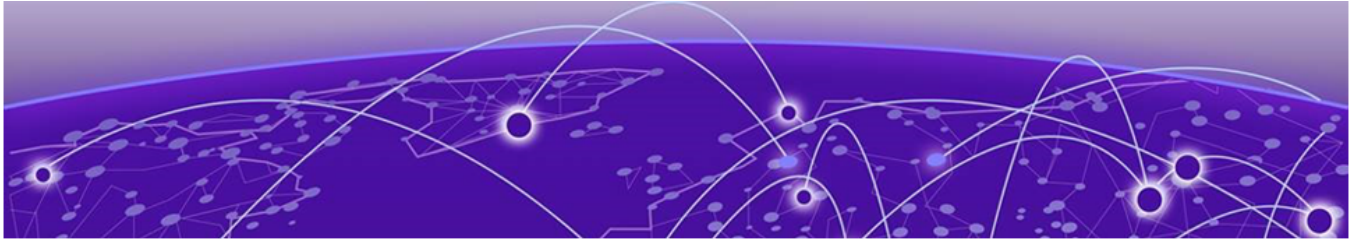
On the ExtremeCloud OS ONE SD-WAN home page, select to view current ExtremeCloud OS ONE SD-WAN tunnel status.



LLDP Signaling

- In the Appliances section, review the Fabric LLDP Signaling status.
- Select an appliance to view additional statistics, such as IP assignment and adjacency status.





SD-WAN Tunnel Verification

Verify tunnel configuration and status using the following CLI commands on SD-WAN appliances:

1. Displays the current tunnel interface configuration.

```
show running-config interface tunnel
```

2. Displays the configured IPsec parameters.

```
show running-config ipsec
```

3. Provides a summary of all configured tunnel interfaces and their operational states.

```
show interface tunnel brief
```

4. Displays detailed information for all active IPsec tunnels, including encryption, authentication, and endpoint settings.

```
show ipsec tunnel all detail
```