

Cisco Catalyst SD-WAN AppQoE Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2020-12-19

Last Modified: 2025-12-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **What's New in Cisco IOS XE (Catalyst SD-WAN)** 3

CHAPTER 3 **AppNav-XE for Cisco Catalyst SD-WAN** 5

- Overview of AppNav-XE 5
- Components of AppNav-XE 7
- Supported Platforms 8
- Managing AppNav-XE in Cisco Catalyst SD-WAN 8
- Configure AppNax-XE on Cisco IOS XE Catalyst SD-WAN Devices 9
  - Register WCM in Cisco SD-WAN Manager 9
  - Attach Cisco IOS XE Catalyst SD-WAN Device to WCM Partner 11
  - Register Cisco XE SD-WAN Device with WCM 11
  - Configure AppNav-XE Cluster for SD-WAN 12
- Monitor and Troubleshoot AppNav-XE 12

CHAPTER 4 **TCP Optimization** 15

- Topology and Roles 16
- Supported Platforms 17
- Limitations and Restrictions 21
- TCP Optimization Configuration Examples 21
- Monitor TCP Optimization 24

CHAPTER 5 **External Service Nodes for AppQoE Services** 27

- Supported Devices for AppQoE Controllers and External Service Nodes 28
- Restrictions for External AppQoE Service Nodes 30

Information about External AppQoE Service Nodes 31
Overview of External AppQoE Service Nodes 31
How External Service Nodes and Standalone Controllers Work 32
Best Practices and Recommendations 34
Configure AppQoE Controllers and Service Nodes in Cisco SD-WAN Manager 34
Configure AppQoE Using a Configuration Group 36
Configure AppQoE Service Controllers and Nodes Using the CLI 38
Monitor AppQoE Service Controllers and Nodes 40
Monitor AppQoE Service Controllers and Nodes Using the CLI 41

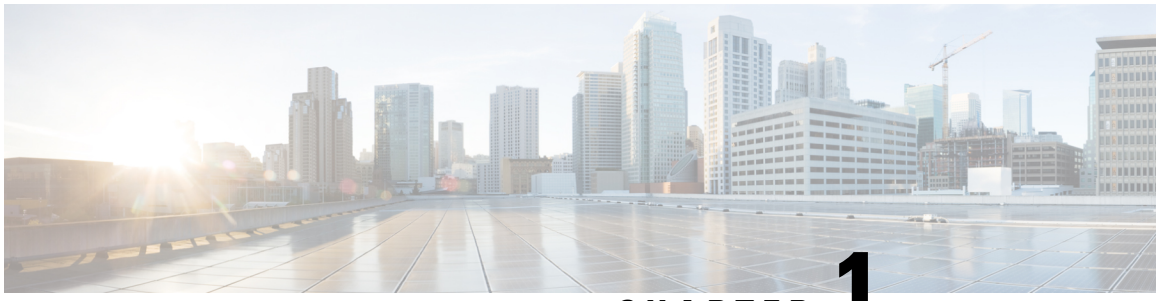
CHAPTER 6 **Traffic Optimization with DRE** 47
Information About DRE 48
Overview of DRE 48
Overview of DRE Profiles 50
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V 50
Overview of SSL Proxy 50
Benefits of SSL Proxy Support for TLS 1.3 51
Information About DRE Optimisation Using Configuration Groups 51
Supported Devices for DRE 51
Disk Recommendations for DRE 54
Secondary Disk Recommendations for DRE 55
Supported DRE Profiles 55
Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V 59
Restrictions for DRE 60
Configure DRE 61
Upload DRE Container Image to the Software Repository 61
Enable DRE Optimization 62
Create Security Policy for SSL Decryption 63
Update Device Template 63
Create a Centralized Policy for TCP and DRE Optimization 64
Configure DRE using Configuration Groups 64
Configure DRE Using the CLI 65
Create Security Policy for SSL Decryption using Policy Groups 66
Create a Centralized Policy for TCP and DRE Optimization using Policy Groups 67

Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization 68
Configure UCS E-Series Server 69
Deploy Cisco Catalyst 8000V on UCS E-Series Server 69
Configure AppQoE Feature Template for Cisco Catalyst 8000V Instances 70
Configure the Controller Cluster Types 70
Monitor DRE 72
Verify and Monitor and Troubleshoot DRE Using CLI 73
Monitor SSL Proxy 78
Verify SSL Proxy Support for TLS 1.3 Using CLI 79

CHAPTER 7 HTTP CONNECT 81
Information About HTTP CONNECT 81
Prerequisites for HTTP CONNECT 81
Restrictions For HTTP CONNECT 82
Use Cases Of HTTP CONNECT 82
Configure HTTP CONNECT Using a CLI Add-On Template 82
Configure HTTP CONNECT Using CLI 82
Verify HTTP CONNECT Configuration 83
Monitor HTTP CONNECT Using the CLI 84

CHAPTER 8 AppQoE Verification and Troubleshooting 85

CHAPTER 9 Troubleshoot Cisco Catalyst SD-WAN AppQoE 87
Overview 87
Support Articles 87
Feedback Request 88
Disclaimer and Caution 88



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

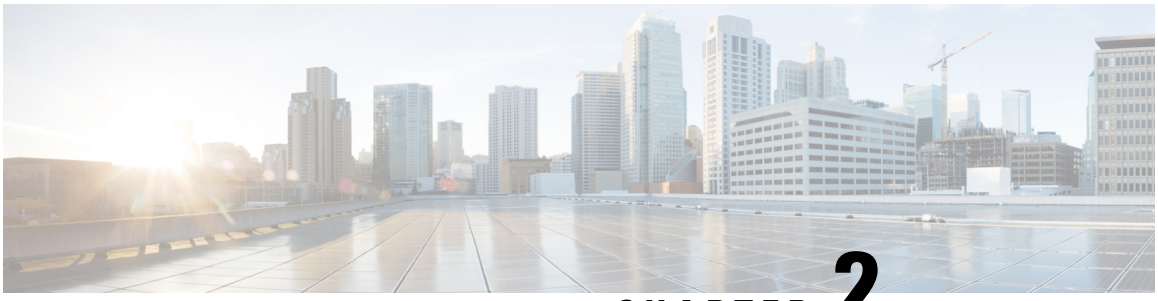
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

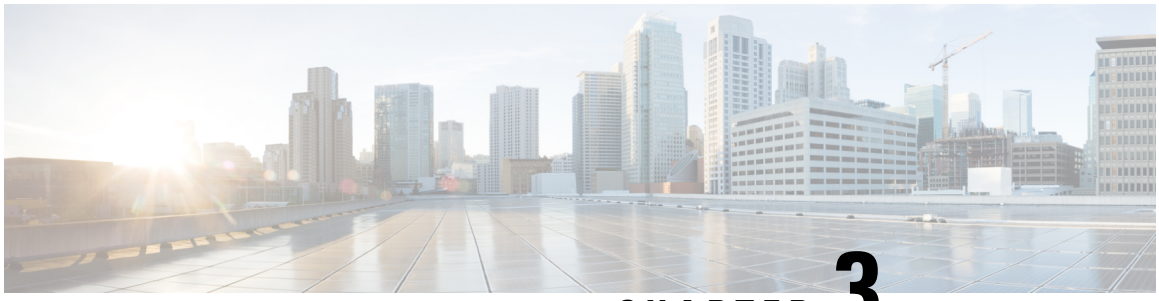


CHAPTER 2

What's New in Cisco IOS XE (Catalyst SD-WAN)

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x

What's New in Cisco SD-WAN (vEdge) Release 20.x



CHAPTER 3

AppNav-XE for Cisco Catalyst SD-WAN

Table 1: Feature History

Feature Name	Release Information	Description
AppNav-XE	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature lets you configure policy-based redirection of LAN-to-WAN and WAN-to-LAN traffic flows to WAAS nodes for WAN optimization on Cisco IOS XE Catalyst SD-WAN devices . This feature was already available on Cisco IOS XE platforms and is being extended to Cisco IOS XE Catalyst SD-WAN platforms in this release.

- Overview of AppNav-XE, on page 5
- Components of AppNav-XE, on page 7
- Supported Platforms, on page 8
- Managing AppNav-XE in Cisco Catalyst SD-WAN, on page 8
- Configure AppNax-XE on Cisco IOS XE Catalyst SD-WAN Devices, on page 9
- Monitor and Troubleshoot AppNav-XE, on page 12

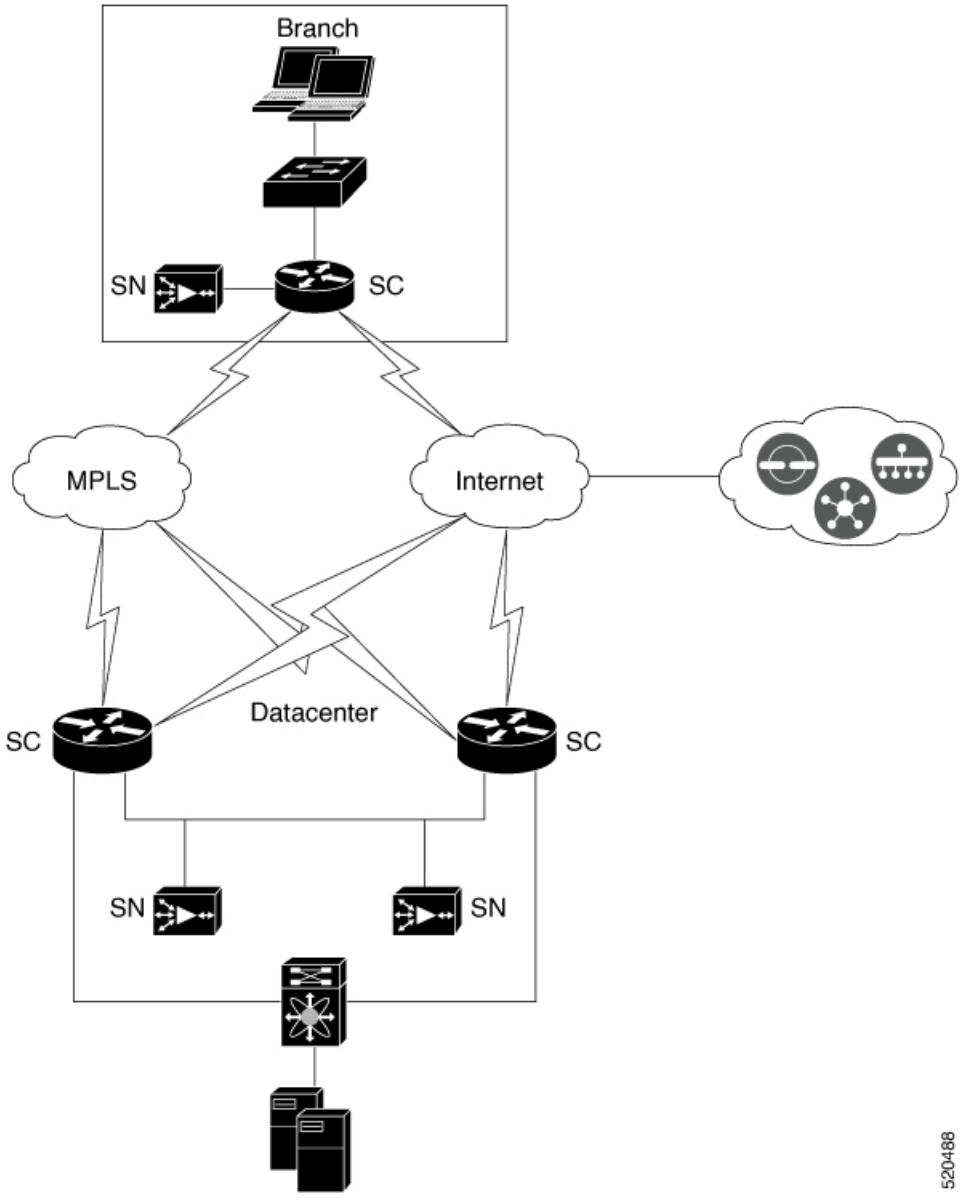
Overview of AppNav-XE

The AppNav-XE feature facilitates intelligent distribution of traffic flows to WAAS devices. WAAS devices are used for WAN optimization.

AppNav-XE reduces dependency on the intercepting router by distributing traffic among WAAS devices for optimization using a class and policy mechanism. You can use WAAS nodes (WNs) to optimize traffic based on sites and/or applications. The AppNav-XE solution can scale up to available capacity by taking into account WAAS device utilization as it distributes traffic among nodes. The solution provides high availability of optimization capacity by monitoring node overload; and by providing configurable failure and overload policies.

Topology Example

Figure 1: Example Topology



*SN: Service nodes or WAAS nodes (up to 64)
*SC: A Cisco IOS XE Catalyst SD-WAN device acting as a service controller (up to 4)

The image above shows an example of Cisco Catalyst SD-WAN deployment with AppNav-XE. The Cisco IOS XE Catalyst SD-WAN devices at the data center and branches are enabled with the AppNav-XE feature and form an AppNav cluster with WAAS nodes.

Benefits of AppNav-XE

- Enables enterprises to expand services efficiently and cost-effectively.
- Supports the use of flexible policy definitions.
- Integrated with Cisco Catalyst SD-WAN network services, which eliminates the need for any additional hardware.
- Intelligently redirects new flows based on the load on each service node. This also includes the load on individual L7 application accelerators.
- For flows that don't require any optimization, service nodes can inform the AppNav Controller to directly pass-through the packets, thus minimizing the latency and resource utilization.
- Has minimal impact to traffic when adding or removing service nodes.
- Supports VRFs, so that the VRF information is preserved when traffic returns from a service node.
- Supports optimization of asymmetric flows through AppNav controller groups.



Note An asymmetric flow is when the traffic in one direction goes through one AppNav Controller and the return traffic goes through a different AppNav Controller; but both AppNav Controllers redirect the traffic to the same service node.

- Provides inter-router high availability to keep traffic flows uninterrupted, where if one router goes down, the traffic can be re-routed to a different router within the AppNav Controller group.

Components of AppNav-XE

- AppNav Cluster: A group of all AppNav controllers and WAAS nodes at a site. Typically, each enterprise site, such as branch and data center, has an AppNav cluster.
- AppNav Controller: A device that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WAAS nodes (WNs) for optimization. The device in this context is a Cisco IOS XE Catalyst SD-WAN device running AppNav-XE.
- WAAS Nodes: Wide Area Application Services (WAAS) nodes or service nodes are WAAS optimization engines or vWAAS instances that optimize and accelerate traffic based on the optimization policies configured on the device.



Note WAAS service nodes are outside the scope of this document.

- WAAS Central Manager (WCM): WCM devices host WCM, a Web-based interface that allows you to configure, manage, and monitor AppNav controllers and WAAS nodes in your network. In AppNav-XE for Cisco Catalyst SD-WAN, WCM communicates with Cisco SD-WAN Manager, which is the network management system used to configure Cisco IOS XE Catalyst SD-WAN devices. Cisco SD-WAN Manager then pushes the AppNav-XE configuration to the Cisco IOS XE Catalyst SD-WAN devices. However, WAAS nodes in an AppNav cluster still receive their configuration through WCM. Monitoring

of WAAS nodes and AppNav-XE on Cisco IOS XE Catalyst SD-WAN devices is done directly through WCM.

- Cisco SD-WAN Manager: This is the primary management system in Cisco Catalyst SD-WAN. Therefore, WCM sends the AppNav-XE configuration to Cisco SD-WAN Manager, which in turn pushes it to the AppNav-XE controllers.

Supported Platforms

The following platforms support AppNav-XE for Cisco Catalyst SD-WAN.

- Cisco 1000 Series Aggregation Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series
- C8500-12X4QC and C8500-12X Series Aggregation Services Routers
- C8300 Series Integrated Services Routers

Managing AppNav-XE in Cisco Catalyst SD-WAN

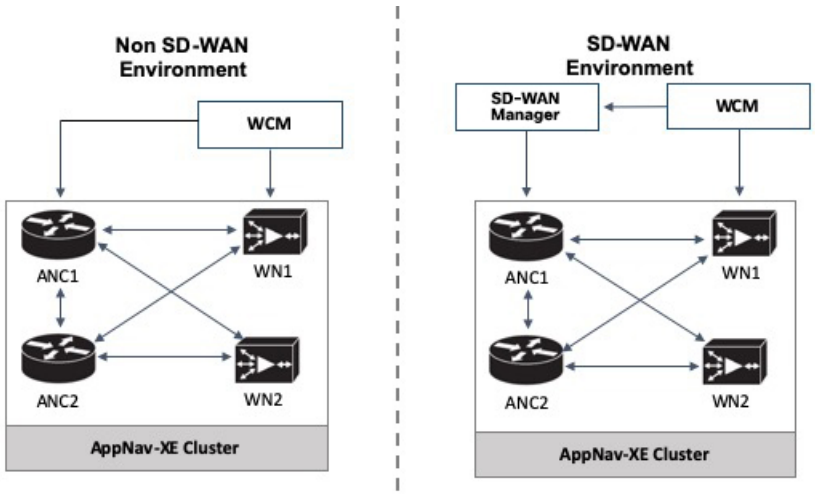
The AppNav-XE feature was already supported on IOS XE platforms. However, starting from Cisco IOS XE Release 17.2, the feature is extended to Cisco IOS XE Catalyst SD-WAN platforms. Note that for this feature to work, Cisco SD-WAN Manager should be running release 20.1.1 or later.

AppNav-XE in SD-WAN versus non-SD-WAN Environments

How AppNav-XE is configured in SD-WAN is different from how it's configured in non-SD-WAN environments. The major difference is the involvement of Cisco SD-WAN Manager, which acts as an intermediary between WCM and AppNav-XE controllers, to push the AppNav policy configuration to Cisco IOS XE Catalyst SD-WAN devices. Cisco IOS XE Catalyst SD-WAN devices act as AppNav-XE controllers.

The following image shows the differences in the deployment of AppNav-XE in SD-WAN and non-SD-WAN environments.

Figure 2: Comparison: AppNav-XE in SD-WAN versus non Catalyst SD-WAN Environments



AppNav-XE in IOS XE: The WCM GUI directly communicates with the AppNav Controller (ANC) and the WAAS Nodes (WN) in the AppNav cluster to push the configuration.

AppNav-XE in IOS XE SD-WAN: The major difference is in terms of how the AppNav policy configuration is pushed to the AppNav Controllers (ANC). Here, the feature is configured through both WCM GUI and Cisco SD-WAN Manager. You continue to configure the AppNav-XE feature in WCM. WCM then sends the configuration to Cisco SD-WAN Manager, which in turn pushes the configuration to AppNav controllers. The communication between WCM and Cisco SD-WAN Manager is achieved through registering WCM as a third-party controller with Cisco SD-WAN Manager. WCM still directly sends the configuration to the WAAS nodes.

Configure AppNax-XE on Cisco IOS XE Catalyst SD-WAN Devices

Perform the following procedures to configure AppNav-XE on Cisco IOS XE Catalyst SD-WAN devices.

1. Register WCM as a third-party controller with Cisco SD-WAN Manager.
2. Attach the Cisco IOS XE Catalyst SD-WAN device to the WCM partner.
3. Register the Cisco IOS XE Catalyst SD-WAN device with the WCM partner attached to Cisco SD-WAN Manager.
4. Configure AppNav-XE Cluster for SD-WAN, on page 12

Register WCM in Cisco SD-WAN Manager

This topic describes how to access Cisco WAAS Central Manager (WCM) and register WCM as s third-party controller on Cisco SD-WAN Manager. It also describes how to attach an Cisco IOS XE Catalyst SD-WAN device to the WCM partner through Cisco SD-WAN Manager.

Access the WCM GUI

To access the WAAS Central Manager GUI, enter the following URL in your web browser:

https:// *WAE_Address* :8443/

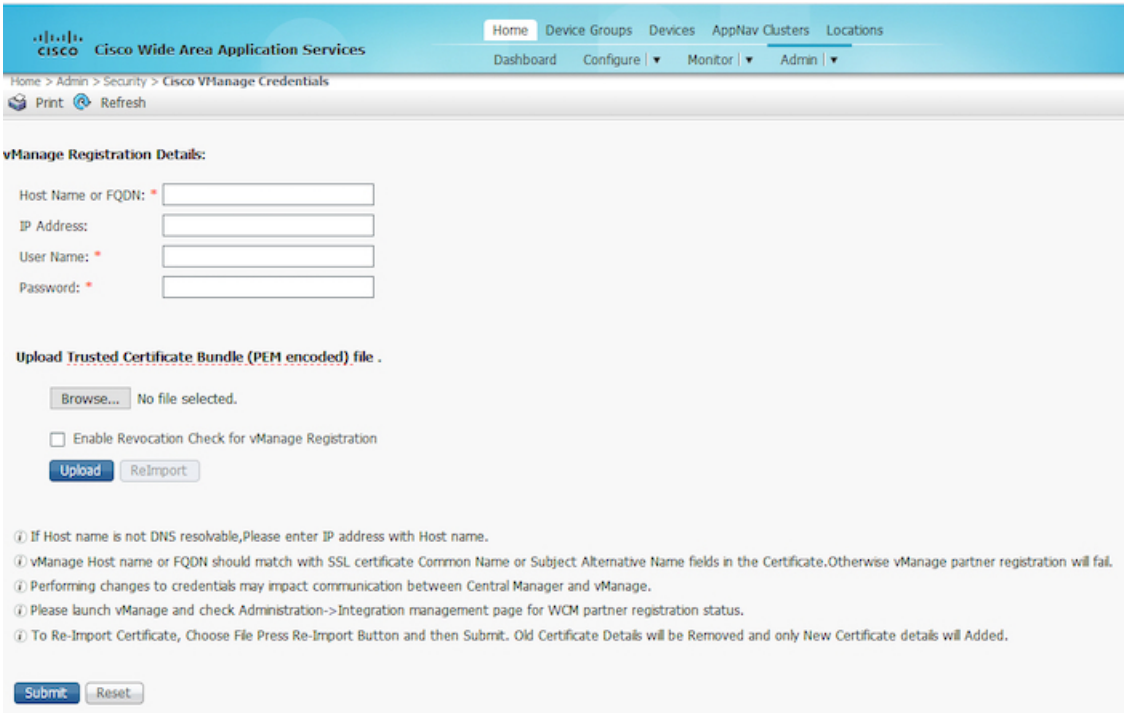
The *WAE_Address* value is the IP address or host name of the WAAS Central Manager device.

The default administrator username is *admin* and the password is *default*.

Integrate WCM with Cisco SD-WAN Manager

1. From the WCM GUI homepage,choose **Admin**.
2. Next, choose **Security** > **Cisco vManage Credentials**.
3. Provide the requested information.

Figure 3: WCM GUI



To register using a Fully Qualified Domain Name (FQDN), enter the FQDN in the Host Name field. The IP Address field should remain empty.

4. Upload the trusted issuer certificate bundle in PEM format for the Cisco SD-WAN Manager web server certificate.

Note Use the re-import button to re-upload the trusted issuer certificate bundle, which replaces the existing certificate bundle.

5. To enable revocation check of the Cisco SD-WAN Manager web server certificate, choose the **Revocation Check** option.

   Note that only OSCP based revocation check is supported.

6. Click **Submit**.

Once integrated, the WCM partner can be seen from the Cisco SD-WAN Manager menu by choosing **Administration** > **Integration Management**.

Attach Cisco IOS XE Catalyst SD-WAN Device to WCM Partner

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Integration Management**.

   You'll see the list of third-party controllers registered on Cisco SD-WAN Manager.

2. For the desired WCM partner, click **...** and choose **Attach Devices**.
3. In the **Available Devices** column on the left, choose a device from the list.
4. Click **Attach**.
5. To configure AppNav-XE on the device, register the device in WCM next.

Register Cisco XE SD-WAN Device with WCM

Prerequisites

- The device being registered should be in Manager mode in the Cisco SD-WAN Manager GUI.
- The device being registered must have HTTPS configuration attached to it. The HTTPS configuration can be attached to the device using the Global Settings template in Cisco SD-WAN Manager.

  1. From Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
  2. Click **Feature Templates** then click **Add Template**.



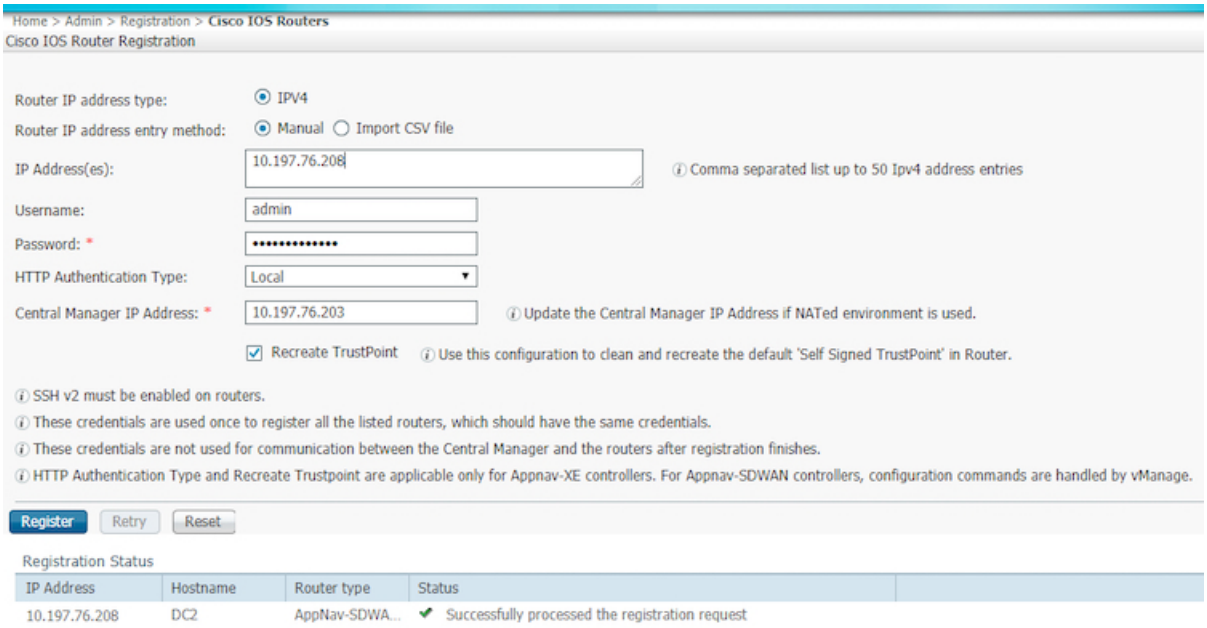
Note In Cisco vManage Release 20.7.x and earlier releases **Feature Templates** is called **Feature**.

  3. Under the **Basic Information** area in the right pane, choose the **Global Settings** template.
  4. Click **Services**.
  5. For both the fields—HTTP Server and HTTPS Server, from the drop-down list, choose **Global** and choose **On**.

Register the Device on WCM

1. In WCM, navigate to the **Admin** section.
2. Choose **Registration** > **Cisco IOS Routers**.

3. Enter the requested details and click **Register**.



The registration status of the device is displayed in the lower part of the screen.

4. Click **Submit**.

Configure AppNav-XE Cluster for SD-WAN

The configuration of AppNav-XE clusters for Cisco Catalyst SD-WAN environments through WCM remains the same as the configuration for non-Cisco Catalyst SD-WAN environments, except for a few different steps. Refer to the following links from the AppNav-XE configuration guide. Any difference in configuration for Cisco Catalyst SD-WAN has been called out with notes.

- Create a Cisco AppNav-XE Cluster with the AppNav Cluster Wizard
- Configure a Class Map on an AppNav-XE Cluster
- Configure AppNav-XE Policy Rules on an AppNav-XE Cluster
- Configure AppNav Controller Settings for an AppNav-XE Device
- Manage AppNav-XE Policies
- Enable Cisco WAAS Service Insertion on AppNav-XE Device Interfaces

Monitor and Troubleshoot AppNav-XE

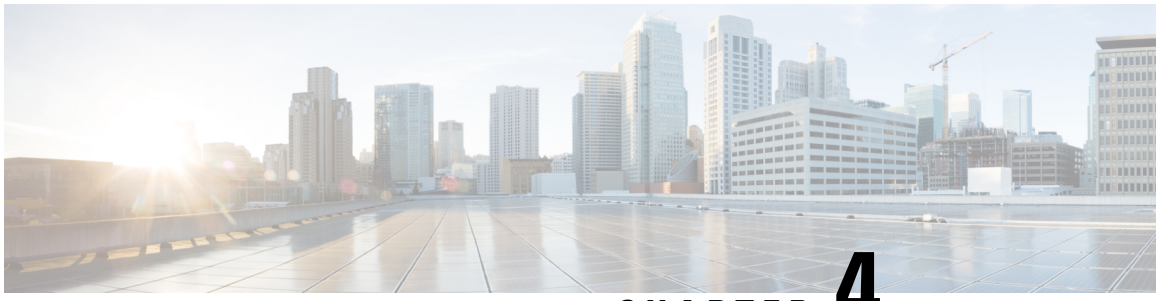
The AppNav-XE component on your Cisco IOS XE Catalyst SD-WAN devices can be monitored through CLI on your devices and through the WCM GUI.

Monitor AppNav-XE

- **Through CLI:** See Monitoring the AppNav-XE Component
- **Through WCM GUI:** See Monitoring an AppNav Cluster

Troubleshoot AppNav-XE

For information on common problems and how to troubleshoot them using various debug commands, see Troubleshooting AppNav-XE.



CHAPTER 4

TCP Optimization

Table 2: Feature History

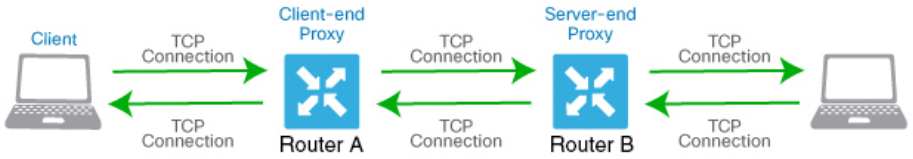
Feature Name	Release Information	Description
TCP Optimization	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	TCP optimization support extended to Cisco 1000 Series Integrated Services Routers (ISRs) and Cisco 4000 Series Integrated Services Routers (ISRs). See Supported Platforms for more information.
	Cisco IOS XE Catalyst SD-WAN Release 16.12.1d	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput.

TCP optimization fine tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput.

This article describes optimizing TCP traffic in service-side VPNs on Cisco IOS XE Catalyst SD-WAN devices.

Optimizing TCP traffic is especially useful for improving TCP traffic performance on long-latency links, such as transcontinental links and the high-latency transport links used by VSAT satellite communications systems. TCP optimization can also improve the performance of SaaS applications.

With TCP optimization, a router acts as a TCP proxy between a client that is initiating a TCP flow and a server that is listening for a TCP flow, as illustrated in the following figure:



The figure shows two routers acting as proxies. Router A is the proxy for the client, and is called the client proxy. Router B is the proxy for the server, called the server proxy. Without TCP optimization, the client establishes a TCP connection directly to the server. When you enable TCP optimization on the two routers, Router A terminates the TCP connection from the client and establishes a TCP connection with Router B.

Router B then establishes a TCP connection to the server. The two routers cache the TCP traffic in their buffers to ensure that the traffic from the client reaches the server without allowing the TCP connection to time out.

It is recommended that you configure TCP optimization on both the routers, the router closer to the client and the router closer to the server. This configuration is sometimes called a dual-ended proxy. It is possible to configure TCP optimization only on the router closer to the client, a scenario called single-ended proxy, but this configuration is not recommended because the TCP optimization process is compromised. TCP is a bidirectional protocol and operates only when connection-initiation messages (SYNs) are acknowledged by ACK messages in a timely fashion.

If both the client and the server are connected to the same router, no TCP optimization is performed.

To use TCP optimization, first enable the feature on the router. Then define which TCP traffic to optimize. Before you configure TCP optimization, to start with the configuration transaction, you can use the following command such as,

```
ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

Note The toptalker feature is supported exclusively on Cisco vEdge devices. For Cisco IOS XE Catalyst SD-WAN devices, use the AppQoE TCP optimization options.

- Topology and Roles, on page 16
- Supported Platforms, on page 17
- Limitations and Restrictions, on page 21
- TCP Optimization Configuration Examples, on page 21
- Monitor TCP Optimization, on page 24

Topology and Roles

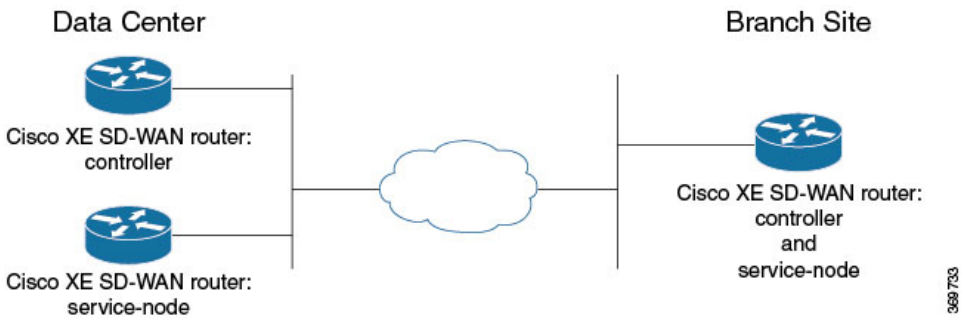
For a branch, the Cisco IOS XE Catalyst SD-WAN device acts as both controller and service-node.

Data Center

For a data center, the controller and service-node roles are performed by separate Cisco IOS XE Catalyst SD-WAN devices. This optimizes performance and enables handling more traffic.

The service-node is an external node that has control connections to Cisco SD-WAN Manager to receive configurations.

Note The service-node Cisco IOS XE Catalyst SD-WAN device must have an underlay connection to the controller on the global VRF to establish an appnav tunnel.



Supported Platforms

Integrated Service Nodes

Devices	Release
• Cisco 4331 Integrated Services Router (ISR 4331) • Cisco 4431 Integrated Services Router (ISR 4431) • Cisco 4321 Integrated Services Router (ISR 4321) • Cisco 4351 Integrated Services Router (ISR 4351) • Cisco 4451 Integrated Services Router (ISR 4451) • Cisco 4461 Integrated Services Router (ISR 4461) • Cisco CSR 1000v Cloud Services Router (CSRv)	Cisco IOS XE Release 17.2.1r and later.
• Cisco 4221 Integrated Services Router (ISR4221) • Cisco Integrated Services Virtual Router (ISRv) • Cisco 1000 Series Integrated Services Routers **Note** The support is only applicable on Cisco 1000 Series Integrated Services Routers that have a RAM of 8 GB or more. See Cisco 1000 Series Integrated Services Routers Data Sheet for platform specifications.	Cisco IOS XE Release 17.3.1a and later
• Cisco ISR 1100X Series Integrated Services Routers • Cisco Catalyst 8000V	Cisco IOS XE Release 17.4.1a

Devices	Release
Cisco Catalyst 8300 Series Edge Platforms: • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X	Cisco IOS XE Release 17.5.1a and later
Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T	Cisco IOS XE Release 17.6.1a and later
Cisco 8100 Series Secure Routers: • C8161-G2 • C8151-G2 Only the above Cisco 8100 Series Secure Router variants support 8GB DRAM, which allows them to support TCP Optimization. See Cisco 8100 Series Secure Routers Data Sheet for platform specifications.	Cisco IOS XE Release 17.18.1a and later
Cisco 8200 Series Secure Routers: • C8231-E-G2 • C8235-E-G2	Cisco IOS XE Release 17.18.1a and later
Cisco 8200 Series Secure Routers: • C8231-G2 • C8235-G2 C8231 and C8235 do not support SSL proxy.	Cisco IOS XE Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8375-E-G2	Cisco IOS XE Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8351-G2 • C8355-G2	Cisco IOS XE Release 17.18.1a and later

Devices	Release
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE Release 17.15.3 and later
Cisco 8100 Series Secure Routers: • C8131-G2 • C8151-CVAI-G2 • C8151-CVAP-G2 Only the above Cisco 8100 Series Secure Router variants support 8GB DRAM, which allows them to support TCP Optimization. See Cisco 8100 Series Secure Routers Data Sheet for platform specifications.	Cisco IOS XE Catalyst SD-WAN Release 26.1.1

Service Controllers

Supported Devices	Release

• Cisco ASR 1000 Series Aggregation Services Routers
  • ASR1001X
  • ASR1002X
  • ASR1001-HX
  • ASR1002-HX
 	
• **Cisco Catalyst 8500 Series Edge Platforms:**
  • C8500-12X4QC
  • C8500-12X
 	
• Cisco Catalyst 8000V
 	
Note
If you configure Cisco Catalyst 8000V as a service controller, you cannot use the same instance as a service node.
	Cisco IOS XE SD-WAN Release 17.4.1a and later

• Cisco Catalyst 8500 Series Edge Platforms
  • C8500L-8S4X
 	
• Cisco ASR 1000 Series Aggregation Services Routers
  • ASR1006-X
	Cisco IOS XE SD-WAN Release 17.5.1a and later

Supported Devices	Release
Cisco Catalyst 8500 Series Edge Platforms • C8500-20X6C	Cisco IOS XE SD-WAN Release 17.10.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8500 Series Secure Routers: • C8570-G2 • C8550-G2	Cisco IOS XE SD-WAN Release 17.15.4a Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later

External Service Nodes

Devices	Release
Cisco Catalyst 8000V	Cisco IOS XE SD-WAN Release 17.4.1a and later
C8500L-8S4X C8500L supports SSL Proxy function when used as external service node for AppQoE.	Cisco IOS XE SD-WAN Release 17.5.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

TCP optimization is not supported on DNS traffic and C8200L platforms.

Disk Provisioning Recommendation for Cisco Catalyst 8000V Deployment

While deploying Cisco Catalyst 8000V instances, choose Thick Provision Eager Zeroed as the disk format.

For information on deploying Cisco Catalyst 8000V instances on supported hypervisors, see:

- ESXi
- KVM

Minimum Resource Requirements

- The platforms must have a minimum of 16 GB of DRAM.
- The Cisco CSR1000V and Cisco Catalyst 8000V platforms must have eight data cores.

Limitations and Restrictions

- TCP optimization in Cisco Catalyst SD-WAN uses the Bottleneck Bandwidth and Round-trip Propagation Time (BBR) algorithm for congestion control. Because BBR is used, if clients request for Explicit Congestion Notification (ECN), the proxy disables it because it is not supported.
- TCP optimization is not supported for Cisco Catalyst 8000V when deployed on Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) on CSP devices.
- Packet Duplication cannot be enabled with AppQoe on the same connection.

TCP Optimization Configuration Examples

Example: Configure Service Insertion using CLI – Branch Router

This example configures a branch Cisco IOS XE Catalyst SD-WAN device to act as controller and service-node.

Note By default, subnet 192.168.1.1/30 and 192.0.2.1/30 used for VPG0 and VPG1 (UTD) and 192.168.2.1/24 used for VPG2 (APPQOE) is configured through Cisco SD-WAN Manager. Use any RFC 1918 subnet for Transport and Service VPN configurations other than these netmask.

```
service-insertion appnav-controller-group ACG-APPQOE
 appnav-controller 192.3.3.1
!
service-insertion service-node-group SNG-APPQOE
 service-node 192.3.3.2
!
service-insertion service-context appqoe/1
 appnav-controller-group ACG-APPQOE
 service-node-group      SNG-APPQOE
 enable
 vrf global
!

interface VirtualPortGroup2
 no shutdown
 ip address 192.3.3.1 255.255.255.0
 service-insertion appqoe
exit
```

Example: Configure Service Insertion Using Cisco SD-WAN Manager – Branch Router

For a branch, the Cisco IOS XE Catalyst SD-WAN device acts as both controller and service-node.

This example configures the branch Cisco IOS XE Catalyst SD-WAN device as controller and service-node.

Note When enabling the AppQoE feature on a device through Cisco SD-WAN Manager, ensure that you remove any Virtual Port Groups (VPG) that already have **service-insertion appqoe** in their configuration and have an IP address that differs from the one you are pushing through Cisco SD-WAN Manager. Enabling AppQoE on a device that has an existing **service-insertion appqoe** configuration on a VPG could lead to a conflict in configurations. This conflict may result in the AppQoE status remaining indeterminate.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. Choose a device from one of the device options listed.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Enter a name and description for the template.
6. Click the **Controller** option.
7. Enter the following details for the controller option:
   - Controller IP: Corresponds to the appnav-controller value that would be configured by the service-insertion appnav-controller-group command when configuring by CLI.
   - Internal: Check this check box.
   - Service Node IP: Corresponds to the service-node value that would be configured by the service-insertion service-node-group command when configuring by CLI.
8. Click **Save**.
9. Add the feature template that was created in a previous step, to a device template page. In the AppQoE drop-down menu, choose the name of the feature template. Add the AppQoE template you created in the previous step following the steps below.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **Device**.

   c. From the devices listed in the window, click **...**for the device you want to attach the AppQoE template to. Click **Edit**.
   d. Click **Additional Templates** and under the AppQoE drop-down list, choose the AppQoE template created.
10. Click **Update**.

Example: Configure Service Insertion Using Cisco SD-WAN Manager – Data Center Controller

1. From the Cisco SD-WAN Manager, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. Under **Select Devices**, choose the branch device to configure.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Enter a name and description for the template.
6. Click the **Controller** option.
7. Create a feature template for the Cisco IOS XE Catalyst SD-WAN device acting as controller. Enter:
   - Controller IP: Corresponds to the appnav-controller value that would be configured by the service-insertion appnav-controller-group command when configuring by CLI.
   - Internal: Leave this option unchecked.
   - Service Node IP: Corresponds to the service-node value that would be configured by the service-insertion service-node-group command when configuring by CLI.
8. Click **Save**.
9. Add the feature template that was created in a previous step, to a device template. In the AppQoE drop-down menu, choose the name of the feature template. Add the AppQoE template you created in the previous following the steps below.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**
   b. Click **Device Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **Device**.

   c. From the devices listed on the page, select the device you want to attach the AppQoE template to and click the More Options icon (**…**) next to the selected device. Click **Edit**.
   d. Click **Additional Templates** and under the AppQoE drop-down menu, choose the AppQoE template created.
10. Click **Update**.

Example: Configure Service Insertion UsingCisco SD-WAN Manager – Data Center Service-Node

Note When enabling the AppQoE feature on a device through Cisco SD-WAN Manager, ensure that you remove any Virtual Port Groups (VPG) that already have **service-insertion appqoe** in their configuration and have an IP address that differs from the one you are pushing through Cisco SD-WAN Manager. Enabling AppQoE on a device that has an existing **service-insertion appqoe** configuration on a VPG could lead to a conflict in configurations. This conflict may result in the AppQoE status remaining indeterminate.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. Under **Select Devices**, choose the branch device to configure.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Click the **Service Node** button.
6. Create a feature template for the Cisco IOS XE Catalyst SD-WAN device acting as service-node. Enter:
   - Template Name
   - Service Node IP: Corresponds to the appnav-controller value that would be configured by the service-insertion service-node-group command when configuring by CLI.
   - Virtual Port Group IP: Corresponds to the service-node value that would be configured by the interface VirtualPortGroup2 command when configuring by CLI.
7. Click **Save**.
8. Add the feature template that was created in a previous step, to a device template page. In the AppQoE drop-down list, choose the name of the feature template.
9. Click **Create**.

Monitor TCP Optimization

To view the AppQoE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.
- Add the following commands to the device configuration:
  - **policy ip visibility features multi-sn enable**
  - **policy ip visibility features sslproxy enable** (for SSL traffic)

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic or applications optimized by TCP optimizaton using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor the traffic or applications optimized by TCP optimizaton.

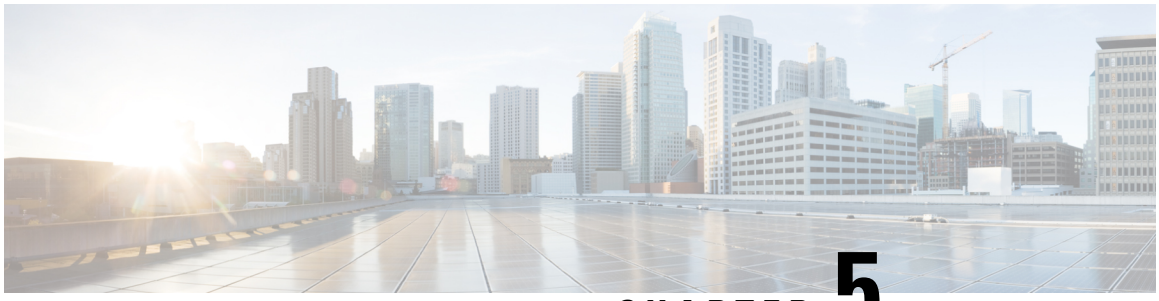
1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **AppQoE TCP Optimization**.
4. Choose **Redirected Traffic**, **Passthrough Traffic** or **Application**, depending on what you want to monitor.
5. Choose **Service Nodes**, **Service Node Groups** or **Control Components.**.

Chart and Table View Options

The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

- From the **Filters**drop-down list, you can view the data by **Bytes** or **Flow**.
- From the **Filters**drop-down list, you can choose the typr of traffic you want to view.
- You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.



CHAPTER 5

External Service Nodes for AppQoE Services

Table 3: Feature History

Feature Name	Release Information	Description
Support for Multiple, External AppQoE Service Nodes	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to configure multiple AppQoE service nodes that are external to the intercepting edge routers or AppQoE service controllers. It extends AppQoE support to edge routers in which AppQoE can't run as an integrated service node. This feature also allows AppQoE to scale, where integrated AppQoE has limitations on the throughput and number of connections. The ability to configure multiple AppQoE service nodes help meet the scale and throughput requirements of large enterprise sites, such as data centers.
Support for Additional Platforms as Controllers for AppQoE Service Nodes	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This release extends the service controller role to additional device models—C8500L-8S4X and ASR1006-X.
Support for Automated MTU Setting for Tunnel Adjacency	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This feature enables a programmatic setting of the maximum transmission unit (MTU) size to 1500 for the network connecting the service controllers and service nodes. This automation prevents broken communication due to packet fragmentation that can bring down the throughput requirements.
IPv6 Support for AppQoE Services	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature allows AppQoE clusters to handle both IPv4 and IPv6 traffic.

- Supported Devices for AppQoE Controllers and External Service Nodes, on page 28
- Restrictions for External AppQoE Service Nodes, on page 30
- Information about External AppQoE Service Nodes, on page 31

• Configure AppQoE Controllers and Service Nodes in Cisco SD-WAN Manager, on page 34
• Configure AppQoE Using a Configuration Group, on page 36
• Configure AppQoE Service Controllers and Nodes Using the CLI, on page 38
• Monitor AppQoE Service Controllers and Nodes, on page 40
• Monitor AppQoE Service Controllers and Nodes Using the CLI, on page 41

Supported Devices for AppQoE Controllers and External Service Nodes

Devices Supported as Service Controllers

Supported Devices	Release

• **Cisco ASR 1000 Series Aggregation Services Routers**
  • ASR1001X
  • ASR1002X
  • ASR1001-HX
  • ASR1002-HX
• **Cisco Catalyst 8500 Series Edge Platforms:**
  • C8500-12X4QC
  • C8500-12X
• Cisco Catalyst 8000V
Note If you configure Cisco Catalyst 8000V as a service controller, you cannot use the same instance as a service node.
	Cisco IOS XE SD-WAN Release 17.4.1a and later

• **Cisco Catalyst 8500 Series Edge Platforms**
  • C8500L-8S4X
• **Cisco ASR 1000 Series Aggregation Services Routers**
  • ASR1006-X
	Cisco IOS XE SD-WAN Release 17.5.1a and later

Cisco Catalyst 8500 Series Edge Platforms • C8500-20X6C	Cisco IOS XE SD-WAN Release 17.10.1a and later

Supported Devices	Release
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE Catalyst SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8500 Series Secure Routers: • C8570-G2 • C8550-G2	Cisco IOS XE SD-WAN Release 17.15.4a Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later

Devices Supported as External Service Nodes

Supported Platforms	Release
• Cisco Catalyst 8000V **Note** If you configure Cisco Catalyst 8000V as a service node, you cannot use the same instance as a service controller.	Cisco IOS XE SD-WAN Release 17.4.1a and later
Cisco Catalyst 8500 Series Edge Platforms • C8500L-8S4X C8500L supports SSL Proxy function when used as external service node for AppQoE.	Cisco IOS XE SD-WAN Release 17.5.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later

Note If you configure Cisco Catalyst 8000V as a service node, you cannot use the same instance as a service controller.

Note For information on platforms supported as external service nodes for Data Redundancy Elimination (DRE), see Traffic Optimization with DRE.

Restrictions for External AppQoE Service Nodes

- Only Cisco Catalyst 8000V instances can be configured with the service node role.
- When Cisco Catalyst 8000V is configured as a service node, it can't act as a service controller, even though Cisco Catalyst 8000V supports the service controller role.
- Only one service cluster is supported per site.
- Only one service context is supported per device. Within a service context, only one AppNav controller group (ACG) is allowed, and that group can contain only one AppNav controller (service controller). Service nodes are organized into service node groups (SNGs); each SNG must be named starting with SNG-APPQOE followed by an index (for example, SNG-APPQOE1), with valid indices from 1 to 31 (plus one default SNG-APPQOE at index 0). A maximum of 64 service nodes can be configured per device across all SNGs. For the Integrated Service Node (ISN) cluster type, each SNG is limited to one service node.
- Only one service node group is supported per AppQoE cluster.
- VRRP is not supported for service controller to service node connectivity.
- A dedicated VRF needs to be setup for the service nodes and service controllers.
- Although handling of asymmetrical flows isn't built into AppQoE, you must configure flow symmetry for all stateful features in Cisco SD-WAN Manager.
- If a service controller fails, the flows handled by that service controller are reset.
- AppQoE Service Nodes is not supported for Cisco Catalyst 8000V when deployed on Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) on CSP devices.
- When you are migrating from IPv4 to IPv6 or vice-versa, you need to remove all the AppQoE configurations and re-apply the configurations with the required IP format.
- Ensure that the bootstrap configuration for the Cisco Catalyst 8000V instance being configured as the AppQoE service node is modified as follows:
  - Exclude any controller groups from the TLOC interfaces (**exclude-controller-group** *0*)
  - Ensure that the configuration includes **omp shutdown**



Note This configuration prevents the AppQoE service node from participating in the SD-WAN data plane. The absence of this modification in the bootstrap configuration leads to generation of alarms indicating that OMP and Control Connections are down in Cisco SD-WAN Manager. However, the alarms are harmless and can be ignored if the recommended configuration is absent from bootstrap configuration.

Restrictions for AppQoE Services with IPv6 Addresses

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

The restrictions for AppQoE service nodes with IPv6 addresses are:

- The control plane of an AppQoE cluster operates on either IPv4 or IPv6 traffic.
- The control plane of an AppQoE cluster that operates on IPv6 traffic supports only external service nodes.
- IPv6 traffic on Internal Service Nodes (ISN) does not support UTD.

Information about External AppQoE Service Nodes

Overview of External AppQoE Service Nodes

The support for configuring multiple, external Application Quality of Experience (AppQoE) service nodes provides high availability for TCP and DRE optimization. When AppQoE service nodes are external to the edge router acting as the service controller, the dependency on this intercepting router is reduced. Prior to the release of this feature, AppQoE service instances had to be configured on the service controller itself. You can now configure supported devices with the AppQoE service node role to optimize traffic based on sites and applications. This solution addresses the requirement of larger enterprises to have higher throughput and more number of connections.



Note The maximum Application Optimization Interconnect Manager (AOIM) peers supported is 255. The MAX number of peers that DRE nodes can connect to is 255.

IPv6 Support for AppQoE Services

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, any AppQoE cluster (integrated-service-node, external-service-node, and hybrid-service-node) supports IPv6 traffic.

Components of AppQoE Solution with External Service Nodes

- **AppQoE Cluster:** An AppQoE controller and a group of AppQoE service nodes at a site.

  Typically, data centers or regional data center sites, which require higher aggregated throughput, have an AppQoE cluster with external service nodes for TCP and DRE optimization.

- **AppQoE Controller:** A supported Cisco IOS XE Catalyst SD-WAN device that intercepts network traffic. Based on the AppQoE policy, the device distributes that traffic to one or more AppQoE service nodes.

- **AppQoE Service Nodes:** Devices that are configured as AppQoE service nodes are TCP optimization instances that optimize and accelerate traffic. The optimization is based on the configuration in control policies.

From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the service nodes can also run the DRE feature to eliminate data redundancy and reduce bandwidth usage. For more information, see Traffic Optimization with DRE .

How External Service Nodes and Standalone Controllers Work

With Cisco Catalyst SD-WAN supporting the creation of external service nodes from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, service nodes are decoupled from the intercepting edge router or the service controller. You now have the option to configure supported devices as standalone service controllers and connect them to devices that are configured with the service node role.

Using Cisco SD-WAN Manager device templates, you can configure the following roles on supported devices:

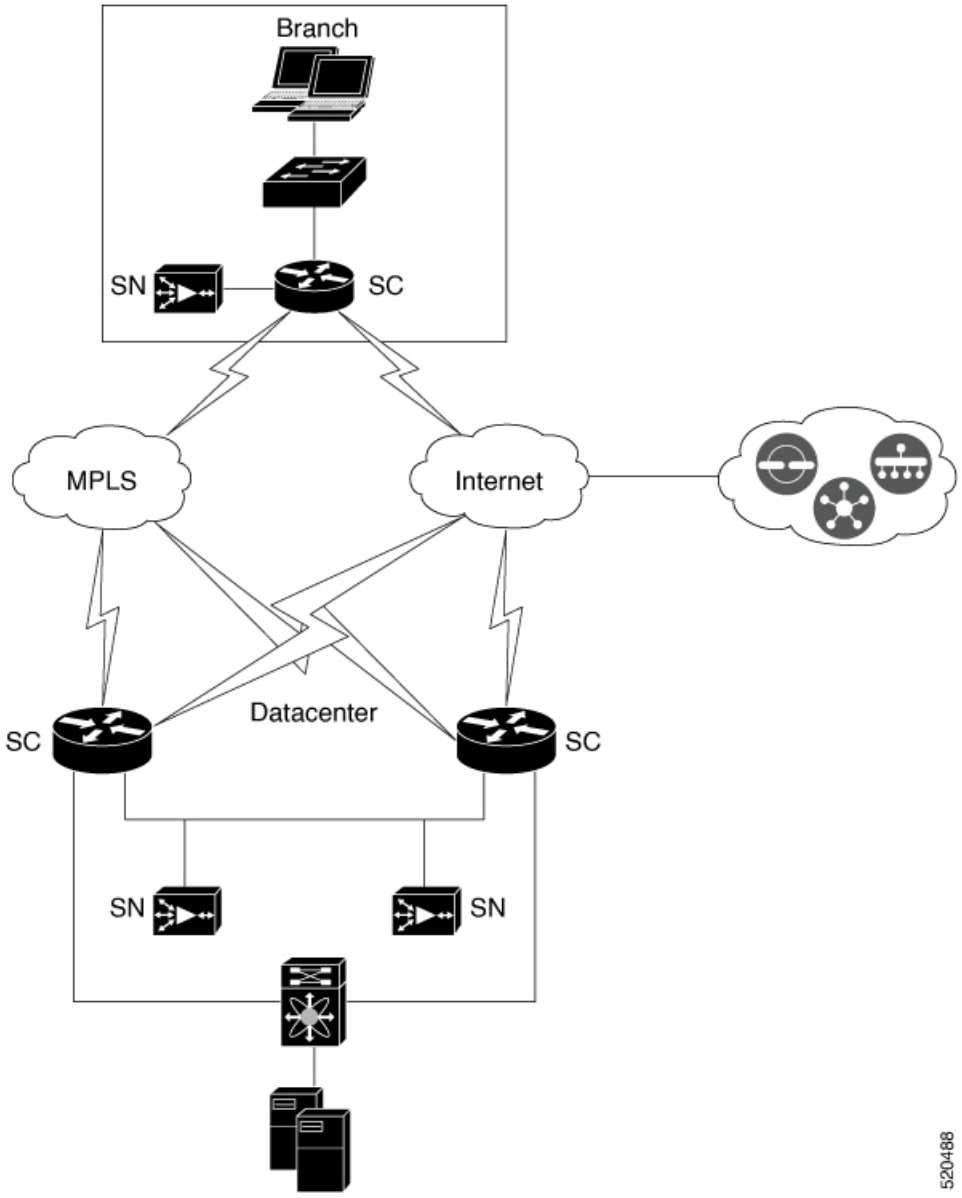
- Service Node
- Service Controller

How Service Controllers and Service Nodes Interact

- In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, only Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) can be configured with the service node role. When you configure Cisco Catalyst 8000V instances with the service node role, a default AppQoE template is attached to them, which cannot be modified.
- Service nodes in a site and the service controllers that they are connected to form a service cluster.
- Service nodes do not communicate with each other and are not aware of the other service nodes in the cluster.
- Service controllers initiate communication with the service nodes connected to them. This configuration is set up in the AppQoE feature template associated with a device template that has the service controller role defined.
- Service controllers and service nodes can be adjacent to each other, or next or multiple hops away.
- Service controllers communicate with the service nodes through service VPNs. However, service nodes communicate with service controllers through transport VPN or VPN 0.
- Service nodes only respond to the service controller that they are connected with.
- In Cisco SD-WAN Manager, the health of each AppQoE service node is represented by the colors Green or Yellow. Only nodes with Green status are considered for distribution of new flows. Any ongoing flows to service nodes showing as Yellow are redirected.

Sample Topology

Figure 4: Sample Topology with External Service Nodes



*SN: Service node (up to 64 per controller)
*SC: Service controller (up to 8 per site)

The image above shows an example of Cisco Catalyst SD-WAN deployment with service nodes that are external to the service controller. The image shows the deployment at both a branch site and a data center. Cisco IOS XE Catalyst SD-WAN devices at the data center and branches form an AppQoE cluster with service nodes at their respective sites.

Best Practices and Recommendations

- To ensure that the service nodes have sufficient capacity for AppQoE services, don't configure any other features on devices that have been configured with the service node role.
- When you create an AppQoE cluster containing service controllers and service nodes, ensure that all the cluster members have the same ID as the site.
- Ensure that service controllers and service nodes that form a cluster share the same Cisco Catalyst SD-WAN site ID. If there's a mismatch in the site IDs, the service nodes are reported as Yellow on the controller. This leads the service nodes being disregarded from the distribution of flows for optimization.
- Ensure that the maximum transmission unit (MTU) size of the network connecting the service controllers and service nodes is uniform across the complete traffic path. Otherwise, it can lead to broken communication due to packet fragmentation.

Configure AppQoE Controllers and Service Nodes in Cisco SD-WAN Manager

Configure AppQoE Service Nodes

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.



Note In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **Device**.

3. In the **Device Model** field, choose **C8000v**.



Note Only Cisco Catalyst 8000V instances can be configured as AppQoE service nodes. If you choose any other device, the Service Node option isn't available in the Device Role field.

4. In the **Device Role** field, choose **Service Node** from the drop-down list.
5. Enter **Template Name** and **Description**.
6. Click **Additional Templates**. In the AppQoE field, notice that the Factory Default AppQoE External Service Node template is attached by default.

   No further configuration is required for devices configured as AppQoE service nodes. Additional configuration for connecting the service nodes to a service node controller is done through the AppQoE controller configuration screens in Cisco SD-WAN Manager.
7. Attach the device template to the device.

Configure AppQoE Service Controller

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **Device**.

3. In the **Device Model** field, choose any one of the devices that support the service controller role. See the Supported Platforms section in this chapter for a complete list of devices that support the service controller role.
4. In the **Device Role** field, choose **SDWAN Edge** from the drop-down list.

Note The **SDWAN Edge** option is only visible for devices that support the service controller role.

5. Enter **Template Name** and **Description**.
6. Click **Additional Templates**. In the AppQoE field, you can either choose an existing AppQoE feature template or create a new one. This procedure includes steps to create a new AppQoE template for the device being configured with the service controller role.
7. Click the drop-down list for the AppQoE field and then click **Create Template.**
8. In the **Template Name** and **Description** fields, enter a name and description for your template respectively.
9. In the **Controller** area, enter the requested details.
   a. **Controller IP address:** Enter the service-side interface IPv4 or **IPv6** address of the controller. This is the IP address that the controller uses to communicate with the service nodes connected to it in a service cluster.
   b. **Service VPN:** Specify the service VPN ID in which the LAN-side connections of the service nodes reside. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
   c. **Service Node IP 1:** Enter the IPv4 or IPv6 of the service nodes to enable the service controllers to communicate with the service nodes.

Note Click + next to the Service Node IP field to add more service nodes. You can add up to 64 service nodes for a single service controller.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, an AppQoE cluster can either operate on IPv4 protocol or IPv6 protocol in the control plane.

Note From Cisco vManage Release 20.6.1, the AppQoE feature template allows you to configure multiple service node groups and add the external service nodes to such groups. You can configure a maximum of 32 service node groups per cluster. The name range of a service node group is SNG-APPQOE0 to SNG-APPQOE31.

However, if the version of the device that you are configuring as a service controller is lower than Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and you use Cisco vManage Release 20.6.1 to configure the AppQoE template for such device, ensure that you configure only one service node group, even though the template allows you to configure multiple service node groups.

10. Attach the device template to the device.

Configure AppQoE Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a AppQoE feature in a Service profile.

a. Configure Basic Parameters.

Table 4: Basic Configuration

Field	Description
Device AppQoE Role *	
Service Node	Choose the **Service Node** option if you want to configure the device as a service node. **Note** **Service Node** is the default option. Choose both the **Service Node** and **Forwarder** options if you want to configure the device as an integrated service node.

Field	Description

Forwarder:	Choose **Forwarder** if you want to configure the device as a forwarder. The forwarder redirects traffic to other service nodes.
	Note
	From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, an AppQoE cluster can either operate on IPv4 protocol or IPv6 protocol in the control plane.
	• **Forwarder IP Address***: IP address of the device you've configured as a forwarder.
	• **AppQoE Service VPN***: Choose the service VPN attached to the interface of the forwarder.
	• **Service Node Group**: Click **Add Service Node Group** and enter the following details for the service node group:
	  • **Group Name**: Select the AppQoe group name.
	  • **Add Service Node**: Click **Add Service Node** and enter the IP address of the service nodes to enable the service controllers to communicate with the service nodes.
	  Click the + icon to add up to 32 service nodes for the group. The starting value for the service node is SNG-APPQOE, following which, you can provide a value in the range SNG-APPQOE1 to SNG-APPQOE31.

b. Configure advanced parameters.

Table 5: Advanced

Field	Description
DRE Optimisation	Enable DRE optimisation
Resource Profile	Choose **Global** to choose a profile size from the options available in the drop-down list. Choose **Default**to apply the default DRE profile size for the device. Choose **Device Specific** to enter a value for the profile.

What to do next

Also see Deploy a configuration group.

Configure AppQoE Service Controllers and Nodes Using the CLI

This section provides example CLI configurations to configure TCP optimization using external service nodes and standalone service controllers connected to such service nodes.

Configure an External Service Node

1. Enable TCP optimization.

```
config-transaction
 sdwan appqoe tcpopt enable
 no sslproxy enable
```

2. Create a virtual port group interface.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a AppQoE cluster handles both IPv6 and IPv4 traffic.

```
interface VirtualPortGroup virtual-port-group-number
service-insertion appqoe
ip address ip-address mask
```

3. Create a service node group.

```
service-insertion service-node-group appqoe  service-node-group-name
service-node service-node-ip-address
```

4. Configure the service node as service plane heavy.

```
platform resource service-plane-heavy
```

Note If you configure Cisco Catalyst 8000V as service-plane heavy, you need to reload it to enable the service plane..

Here's the complete configuration example for creating service nodes using IPv4 addresses:

```
sdwan appqoe tcpopt enable
 no sslproxy enable
 !

service-insertion service-node-group appqoe SNG-APPQOE

 device-role service-node
 service-node 192.168.2.2
 !

interface VirtualPortGroup1
 ip address 192.168.2.1 255.255.255.0
 service-insertion appqoe
 !
```

```
 interface GigabitEthernet 2
  description SN_LAN_Interface in VPN0
  ip address 192.0.2.1 255.255.255.0
  !

platform resource service-plane-heavy

system
 system-ip 198.51.100.1
 site-id 78200
!
```

Here's the complete configuration example for creating service nodes using IPv6 addresses:

```
sdwan appqoe tcpopt enable
 no sslproxy enable
 !

interface VirtualPortGroup2
 ip address 192.168.2.1 255.255.255.0
 ipv6 address FDF8::1/126
 service-insertion appqoe

service-insertion service-node-group appqoe SNG-APPQOE
 device-role service-node
 service-node 192.168.2.2
!
interface GigabitEthernet2
 ip address 172.16.200.35 255.255.255.0
 ipv6 address 2001:AA8:1234:200::35/64

 platform resource service-plane-heavy
```

Configure a Service Controller

1. Create a service controller and assign it to a service controller group.

   config-transaction
   service-insertion appnav-controller-group appqoe *appqoe-controller-group-name*
   D **appnav-controller** *controller-ip-address*

2. Create a service node group and add service nodes to it.

   service-insertion service-node-group appqoe *service-node-group-name*
   service-node *service-node-ip-address*

Note You can configure multiple external service nodes in a service node group.

3. Configure service context for the controller and service node groups.

   service-insertion service-context appqoe/1
   appnav-controller-group *appqoe-controller-group-name*
   service-node-group *service-node-group-name* **enable**
   vrf default

Here's a complete configuration example for creating service controllers using IPv4 addresses:

```
 service-insertion appnav-controller-group appqoe Test-ACgroup
  appnav-controller 198.51.100.1 vrf 200
  !

 service-insertion service-node-group appqoe Test-SNGroup
  service-node 192.0.2.2
  service-node 192.0.2.3
  service-node 192.0.2.4
  service-node 192.0.2.5
  !

 service-insertion service-context appqoe/1
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE
  cluster-type service-controller
  enable
  vrf default
  !

  interface GigabitEthernet 1
   description SC_To_SN_LAN_Interface in VPN200
   ip address 192.0.2.1 255.255.255.0
   vrf forwarding 200
   !

  system
   sytem-ip 198.51.100.10
   site-id 78200
   !
```

Here's a complete configuration example for creating service controllers using IPv6 addresses:

```
interface GigabitEthernet3
 vrf forwarding 2
 ip address 172.16.200.32 255.255.255.0
 ipv6 address 2001:AA8:1234:200::32/64
!

service-insertion service-node-group appqoe SNG-APPQOE
service-node 2001:AA8:1234:200::35
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 2001:AA8:1234:200::32 vrf 2
!
service-insertion service-context appqoe/1
 cluster-type service-controller
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
 vrf global
 enable
```

Monitor AppQoE Service Controllers and Nodes

Verify Device Role

Follow this procedure to verify the device role (service controller or service node) for a device after you configure the role using a device template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Ensure that you are in the **Device Templates** area .



Note In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **Device**.

A list of available device templates is displayed.

3. Check the **Device Role** column for a device to know its role. **SDWAN Edge** implies that the device is configured as a service controller.

Monitor Traffic on Service Controllers

Alarms and Events

If a cluster isn't formed or is not operational, the device sends a notification to Cisco SD-WAN Manager. You can view such event notifications from the **Monitor** page of Cisco SD-WAN Manager. For some of these events, Cisco SD-WAN Manager also generates alarms. For information on how to view alarms and events for your devices, see Alarms, Events, and Logs

Monitor AppQoE Service Controllers and Nodes Using the CLI

Use the following CLI commands to view the statistics for AppQoE service controllers, service nodes, and clusters.

Configuration Examples for AppQoE Service Controllers and Nodes on an IPv4 Address

The following sample output shows the configuration details of service node using IPv4 address in a service node group:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 10.1.1.1
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020

Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

The following sample output shows the traffic statistics for service node using IPv4 address in a service node group:

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
10.1.1.1
10.1.1.2

Aggregate of statistics from all SNs of the SNG:
------------------------------------------------
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
-----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

The following sample output shows the configuration details of service controller using IPv4 address :

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
10.1.1.100

AppNav Controller : 99.1.1.100
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
Current AC View of AppNav Controller
IP Address
10.1.1.100

Current SN View of AppNav Controller
IP Address
10.1.1.1
```

Configuration Examples for AppQoE Service Controllers and Nodes on an IPv6 Address

The following sample output shows the configuration details of service nodes using IPv6 addresses in a service node group:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 2001:DB8:1::1
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020

Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

The following sample output shows the traffic statistics for service nodes using IPv6 addresses in a service node group:

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
2001:DB8:1::1
2001:DB8:0:ABCD::1

Aggregate of statistics from all SNs of the SNG:
------------------------------------------------
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

The following sample output shows the configuration details of service controllers using IPv6 addresses in a controller group:

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
2001:DB8:0:ABCD::1

AppNav Controller : 99.1.1.100
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
Current AC View of AppNav Controller
IP Address
2001:DB8:0:ABCD::1

Current SN View of AppNav Controller
IP Address
2001:DB8:0:ABCD::1
```

The following sample output shows the configuration details of service nodes using IPv6 addresses in an AppQoE cluster :

```
Device# show service-insertion type appqoe cluster-summary
Service Context                           : appqoe/1
 Enabled                                  : TRUE
 Cluster type                             : Service-controller

 Service Controller Group      : ACG-APPQOE
   Service Controller IP       : 2001:40:92::1   VRF : 5
   Service Controller System IP: 192.168.1.11
   Service Controller Site ID  : 220

 Service Node Group : SNG-APPQOE ID: 32

 ------------------------------------------------------------------------------------------
|   Service Node IP    |    System IP    |  Site Id  |  Status |         Error          |
 ------------------------------------------------------------------------------------------
| 2001:40:92::5        | 192.168.1.11  | 220       | GREEN   |                        |
 ------------------------------------------------------------------------------------------
```

The following sample output provides information about AppQoE services that are using IPv6 addresses:

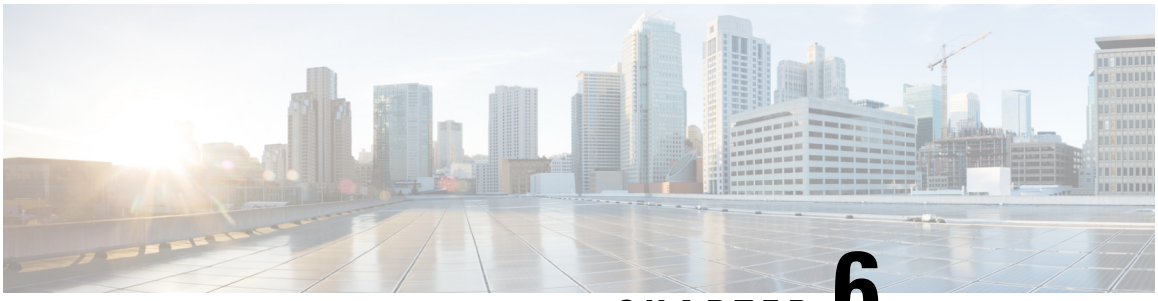
```
Device# show service-insertion type appqoe service-context
Service Context                           : appqoe/1
Cluster protocol VPATH version            : 2
Time service context was enabled          : Sun Dec 17 18:47:51 2023
Current FSM state                         : Operational
Time FSM entered current state            : Sun Jan  7 18:27:08 2024
Last FSM state                            : Converging
Time FSM entered last state               : Sun Jan  7 18:26:58 2024
Cluster operational state                 : Operational
Tunnel interface GRE                      : Tunnel2000000001
Tunnel interface VxLAN                    : Tunnel2000000002

Stable AppNav controller View:
   2001:40:92::1

Stable SN View:
   2001:40:92::5

Current AppNav Controller View:
   2001:40:92::1
```

```
Current SN View:
   2001:40:92::5
```



CHAPTER 6

Traffic Optimization with DRE

Table 6: Feature History

Feature Name	Release Information	Description
Traffic Optimization with DRE	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This release extends the DRE functionality to Cisco Catalyst SD-WAN. DRE is a compression technology that reduces the size of data transmitted over the WAN and enables more effective utilization of the WAN.
DRE Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides the flexibility to use resources for DRE based on your connection requirements by applying profiles such as S, M, L, and XL.
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature introduces support for deploying Cisco Catalyst 8000V instances, on supported routers, using UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.
UCS-E Series Next Generation Support for Deploying Cisco Catalyst 8000V	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature introduces support for deploying Cisco Catalyst 8000V Edge Software on supported routers, using the UCS-E1100D-M6 server module.
SSL Proxy Support for TLS 1.3	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature, SSL proxy in AppQoE supports the TLS protocol version 1.3.

Feature Name	Release Information	Description
DRE Optimisation Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	With this feature you can enable DRE optimization using **AppQoE** feature under **Service Profile** in a configuration group in Cisco SD-WAN Manager.
Cisco Secure Routers support for AppQoE	Cisco IOS XE Catalyst SD-WAN Release 17.15.3a Cisco Catalyst SD-WAN Manager Release 20.15.3	Added support for additional Cisco Secure Routers.
Cisco Secure Routers support for AppQoE	Cisco IOS XE Catalyst SD-WAN Release 17.18.1aCisco Catalyst SD-WAN Manager Release 20.18.1	Added support for additional Cisco Secure Routers.

- Information About DRE, on page 48
- Supported Devices for DRE, on page 51
- Disk Recommendations for DRE, on page 54
- Supported DRE Profiles, on page 55
- Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V, on page 59
- Restrictions for DRE, on page 60
- Configure DRE, on page 61
- Configure DRE using Configuration Groups, on page 64
- Configure DRE Using the CLI, on page 65
- Create Security Policy for SSL Decryption using Policy Groups , on page 66
- Create a Centralized Policy for TCP and DRE Optimization using Policy Groups , on page 67
- Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization, on page 68
- Monitor DRE, on page 72
- Verify and Monitor and Troubleshoot DRE Using CLI, on page 73
- Monitor SSL Proxy, on page 78
- Verify SSL Proxy Support for TLS 1.3 Using CLI, on page 79

Information About DRE

Overview of DRE

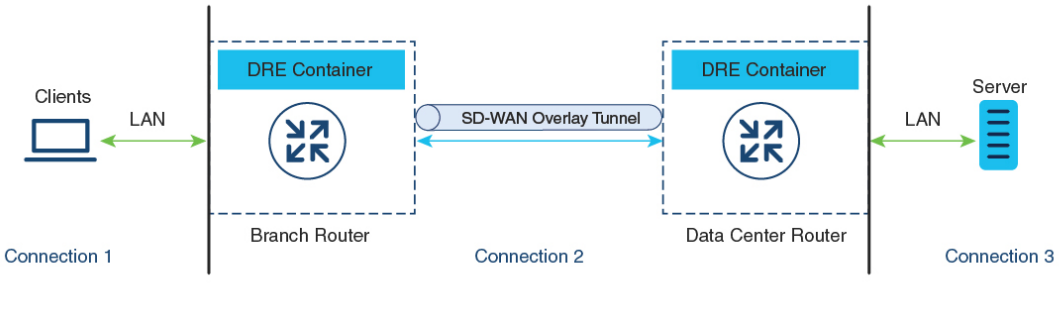
Data Redundancy Elimination (DRE) is a compression technology that reduces the size of data transmitted over the WAN. DRE reduces the size of transmitted data by removing redundant information before sending the data stream over the WAN. The DRE compression scheme is based on a shared cache architecture where each peer involved in compression and decompression shares the same redundancy cache. With the integration of DRE with Cisco Catalyst SD-WAN, DRE replaces repeated data in the stream with a much shorter reference,

and then sends the shortened data stream across the SD-WAN overlay. The receiving end uses its local redundancy cache to reconstruct the data stream before passing it along to the destination client or server.

Note Cisco IOS XE Catalyst SD-WAN devices need to be deployed at both ends of the Cisco Catalyst SD-WAN overlay tunnel.

How DRE and TCP Optimization Work Together

Figure 5: Interception of TCP Traffic



When DRE is configured, the TCP traffic is intercepted and it's separated into three connections:

Connection Type	Network
Client to the branch Cisco IOS XE Catalyst SD-WAN device: This connection exists in Local Area Network (LAN)	LAN
Branch router to the data center router	Through Cisco Catalyst SD-WAN overlay tunnel
Remote branch or data center router to the server	LAN

TCP connections in the Local Area Network (LAN) continue to send the original data. However, TCP connections through the Cisco Catalyst SD-WAN overlay tunnel send data that is compressed by DRE. The DRE container in the Cisco IOS XE Catalyst SD-WAN device at one side of the tunnel compresses the data before it's sent over the overlay tunnel. The DRE container in the Cisco IOS XE Catalyst SD-WAN device at the other side of the tunnel decompresses the data before it's sent to the server at the remote branch or data center side.

Components of DRE

DRE Cache: DRE cache uses secondary storage so that it can store a large amount of data. DRE cache is stored on both sides of the WAN and is used by edge devices to decompress the data. DRE cache in both devices (branch and data center) is synchronized, which means that if a chunk signature is present on one side, the other side has it too.

DRE Compression: DRE uses the Lempel-Ziv-Welch (LZW) compression algorithm for compressing data. DRE operates on large streams of data, typically tens to hundreds of bytes or more, and maintains a much larger compression history.

Overview of DRE Profiles

DRE profiles is a feature introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. This feature provides the flexibility to allocate resources to the DRE service based on the size of your branches and the number of connections required. DRE profiles are combinations of resource requirements and allocations that enable resource assignment based on your connection requirements.

The following DRE profiles are supported:

- Small (S)
- Medium (M)
- Large (L)
- Extra-large (XL)

To see the profiles supported on the devices that support the DRE feature, see the *Supported DRE Profiles* section in this chapter.

UCS-E Series Server Support for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be configured as external service nodes on supported UCS E-Series server modules. These server modules reside in Cisco 4000 Series Integrated Services Routers (Cisco 4000 Series ISR) and Cisco Catalyst 8000 Series Edge Platforms. These routers come with integrated service nodes. However, you can use supported UCS E-Series servers to deploy Cisco Catalyst 8000V instances on these routers, therefore enabling them to act as hybrid clusters with integrated service nodes and external service nodes. This capability ensures that AppQoE services such as DRE, that require higher CPU, can run on routers that otherwise have lower CPU and RAM.

How Cisco Catalyst 8000V Works on Cisco UCS E-Series Servers

- You can install VMware vSphere ESXi 6.7 hypervisors on UCS-E series server modules that reside in Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms.
- You can then install Cisco Catalyst 8000V on these servers.
- The installed Cisco Catalyst 8000V instances should be configured with the app-heavy profile. This ensures that more cores are allocated to the service plane. The app-heavy profile separates service plane and data plane cores, therefore improving service plane performance.

Overview of SSL Proxy

The Secure Sockets Layer (SSL) proxy feature in AppQoE provides a secure and transparent way of optimizing SSL traffic. An SSL Proxy serves as an intermediary between the client and server. It first decrypts the encrypted traffic, optimises it and then encrypts it back. This process ensures that all data remains secure while also allowing for optimization. For more information, see Overview of SSL/TLS Proxy.

The SSL proxy uses Transport Layer Security (TLS) as a protocol to secure and encrypt communication between the client and the server, and optimize the SSL traffic. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, SSL proxy supports TLS version 1.3. TLS version 1.3 is more widely deployed and is simpler, faster, and more secure than version 1.2.

Note In SSL proxy, the support for a TLS 1.3 version is enabled by default. When a TLS 1.3 version is not available, the SSL proxy switches to using the TLS 1.2 version.

For information about verifying the TLS version, see Verify SSL Proxy Support for TLS 1.3 Using CLI, on page 79

Benefits of SSL Proxy Support for TLS 1.3

The TLS 1.3 protocol is simpler, faster, and more secure than that of version 1.2, and is widely used.

Information About DRE Optimisation Using Configuration Groups

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can deploy and manage Cisco Catalyst SD-WAN network more efficiently by optimizing traffic based on sites and applications using configuration groups in Cisco SD-WAN Manager.

Supported Devices for DRE

Integrated Service Nodes

Devices	Release
Cisco Catalyst 8300 Series Edge Platforms: • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X For more information, see UCS-E Series Server Support for Deploying Cisco Catalyst 8000V and Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V. For information on platform default resources, see Cisco Catalyst 8300 Series Edge Platforms Data Sheet.	Cisco IOS XE SD-WAN Release 17.5.1a and later
Cisco Catalyst 8000V For information on platform default resources, see Cisco Catalyst 8000V Edge Software Data Sheet	Cisco IOS XE SD-WAN Release 17.5.1a and later

Devices	Release
• Cisco 4331 Integrated Services Router (ISR 4331) • Cisco 4351 Integrated Services Router (ISR 4351) • Cisco 4451 Integrated Services Router (ISR 4451) • Cisco 4461 Integrated Services Router (ISR 4461) For more information, see UCS-E Series Server Support for Deploying Cisco Catalyst 8000V and Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.	Cisco IOS XE SD-WAN Release 17.6.1a and later
Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T For information on platform default resources, see Cisco Catalyst 8200 Series Edge Platforms Data Sheet	Cisco IOS XE SD-WAN Release 17.6.1a and later
Cisco 8200 Series Secure Routers: • C8231-E-G2 • C8235-E-G2	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8375-E-G2	Cisco IOS XE Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8355-G2	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Service Controllers

Devices	Release

• **Cisco ASR 1000 Series Aggregation Services Routers**
  • ASR1001X
  • ASR1002X
  • ASR1001-HX
  • ASR1002-HX
For information on platform default resources, see Cisco ASR 1000 Series Aggregation Services Routers Data Sheet
• **Cisco Catalyst 8500 Series Edge Platforms:**
  • C8500-12X4QC
  • C8500-12X
• Cisco Catalyst 8000V
Note
If you configure Cisco Catalyst 8000V as a service controller, you cannot use the same instance as a service node.
	Cisco IOS XE SD-WAN Release 17.5.1a and later

Cisco Catalyst 8500 Series Edge Platforms • C8500L-8S4X For information on platform default resources, see Cisco Catalyst 8500 Series Edge Platforms Data Sheet	Cisco IOS XE SD-WAN Release 17.5.1a and later
Cisco Catalyst 8500 Series Edge Platforms • C8500-20X6C	Cisco IOS XE SD-WAN Release 17.10.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8500 Series Secure Routers: • C8570-G2 • C8550-G2	Cisco IOS XE Catalyst SD-WAN Release 17.15.4a

External Service Nodes

Devices	Release
Cisco Catalyst 8000V For information on platform default resources, see Cisco Catalyst 8000V Edge Software Data Sheet	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a
Cisco Catalyst 8500 Series Edge Platforms • C8500L-8S4X C8500L supports SSL Proxy function when used as external service node for AppQoE. For information on platform default resources, see Cisco Catalyst 8500 Series Edge Platforms Data Sheet	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Disk Recommendations for DRE

We recommend using solid-state drive (SSD) disks for deploying DRE as well as other AppQoE services.

Configure the following recommended parameters from Cisco Integrated Controller Manager (IMC). Ensure that you configure these before installing the hypervisor because some of the settings may require disk formatting.

Table 7: Recommended Disk Parameters

Parameter	Value
RAID level	RAID10
Read Policy	Always Read Ahead
Disk Cache Policy	Disabled
Write Policy	Write Back Good BBU
Strip Size	256 KB
I/O Cache Policy	Direct

Disk Provisioning Recommendation for Cisco Catalyst 8000V Deployment

While deploying Cisco Catalyst 8000V instances, choose Thick Provision Eager Zeroed as the disk format.

For information on deploying Cisco Catalyst 8000V instances on supported hypervisors, see:

- ESXi
- KVM

Secondary Disk Recommendations for DRE

While deploying Cisco Catalyst 8000V instances, the extra disk space is added after the basic system partitions are allocated under the /bootflash partition. However, if there is a need to increase the disk size, you must reinstall the instances to realize more usable disk space. The disk for Cisco Catalyst 8000V can be expanded at any time in the hypervisor. However, after the disk is formatted, the Cisco Catalyst 8000V cannot take the additional space.

Configure the following recommended parameters from Cisco Integrated Controller Manager (IMC). Ensure that you configure these before installing the hypervisor because some of the settings may require disk formatting.

Table 8: Recommended Disk Parameters

Cloud Type	Disk Type	Disk Size	Instance Type
AWS	Throughput Optimized HDD (st1)	2 TB	c5.4xlarge (16 vCPUs, 32 GB memory)
Microsoft Azure	SSD Persistent disk	2 TB	custom (16 vCPUs, 32 GB memory)
Google Cloud Platform (GCP)	Premium SSD	2 TB	Standard F16s_v2 (16 vCPUs, 32 GB memory)

For information about deploying a Cisco Catalyst 8000V on different platforms, see the following:

- Deploy Cisco Catalyst 8000V on AWS
- Deploy Cisco Catalyst 8000V on Microsoft Azure
- Deploy Cisco Catalyst 8000V on GCP

For deploying Cisco Catalyst 8000V on AWS, Azure, or GCP platforms, include a cloud-init configuration and attach the secondary disk during deployment.

Supported DRE Profiles

The following table provides this information:

- Devices that support DRE feature and their default DRE profiles.
- DRE profiles supported on the devices.
- The UTD profile supported along with the DRE profile size configured.
- Minimum resource recommendation for the supported DRE profiles.
- The maximum connections that the DRE profiles provide on the supported devices.

- The FanOut values that correspond to the DRE profiles configured on the devices. FanOut refers to the number of peers that a device can communicate with to form the DRE service.

Table 9: DRE Profiles, Resource Requirements, and Supported Connections and FanOut

Devices	Default DRE Profile	Supported DRE Profiles	Supported UTD Profiles	Additional Minimum Resource Recommendations *		Maximum Connections	FanOut
				RAM	Disk		
C8200-1N-4T	S	S	—	8 GB	120 GB	750	35
C8300-2N2S-6T C8300-1N1S-4T2X C8300-1N1S-6T	M	S	S	8 GB	120 GB	750	35
		M	—	8 GB	280 GB	5000	70
C8300-2N2S-4T2X	M	S	S, M	8 GB	120 GB	750	35
		M	S	8 GB	280 GB	5000	70
		L	—	16 GB	500 GB	10,000	256
C8500L-8G4X	M	S	—	8 GB	120 GB	750	35
		M	—	8 GB	280 GB	5000	70
		L	—	32 GB	500 GB	22,000	256
		XL	—	32 GB	1600 GB	36,000	256
Cisco Catalyst 8000V—6 core	S	S	—	8 GB	120 GB	750	35
Cisco Catalyst 8000V—8 core	S	S	—	8 GB	120 GB	750	35
		M	—	8 GB	280 GB	5000	70
Cisco Catalyst 8000V—12 core	S	S	—	8 GB	120 GB	750	35
		M	—	8 GB	280 GB	5000	70
		L	—	16 GB	500 GB	10,000	256
Cisco Catalyst 8000V—16 core	S	S	—	8 GB	120 GB	750	35
		M	—	8 GB	280 GB	5000	70
		L	—	32 GB	500 GB	22000	256
		XL	—	32 GB	1600 GB	36000	256

Devices	Default DRE Profile	Supported DRE Profiles	Supported UTD Profiles	Additional Minimum Resource Recommendations *		Maximum Connections	FanOut
				RAM	Disk		
Cisco 8200 Series Secure Routers: • C8225HG2	S	S	—	16 GB	120 GB	750	35
Cisco 8300 Series Secure Routers: • C8375HG2	M	M	S	16 GB	280 GB	5000	70
		L	—	32 GB	500 GB	10000	256
Cisco 8300 Series Secure Routers: • C8355G2	M	M	—	16 GB	280 GB	5000	70
Cisco 8400 Series Secure Routers: • C8455G2	M	L	—	32 GB	500 GB	16000	256
Cisco 8400 Series Secure Routers: • C8475G2	M	L	—	32 GB	500 GB	22000	256
		L	—	64 GB	500 GB	5000	70

* The resource recommendations specified in the table are in addition to the platform's default resources.

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

The following table provides this information:

- The memory, disk, and cache allocated based on the DRE profile configured on the supported devices.

Table 10: Profile-wise Resource Allocation

Devices and Default DRE Profile	DRE Profiles	Resource Allocation (GB)		
		Memory	Disk	Cache Size
C8200-1N-4T (S)	S	2	80	60
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	2	80	60
	M	4	250	230
C8300-2N2S-4T2X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
C8500L-8G4X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180
Cisco Catalyst 8000V—6 core (S)	S	2	80	60
Cisco Catalyst 8000V—8 core (S)	S	2	80	60
	M	4	250	230
Cisco Catalyst 8000V—12 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
Cisco Catalyst 8000V—16 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180
Cisco 8200 Series Secure Routers (S): • C8231-E-G2 • C8235-E-G2	S	2	80	60

Devices and Default DRE Profile	DRE Profiles	Resource Allocation (GB)		
		Memory	Disk	Cache Size
Cisco 8300 Series Secure Routers (M): • C8375-E-G2 • C8355-G2	S	2	80	60
	M	4	250	230
Cisco 8300 Series Secure Routers (M): • C8375-E-G2	L	8	480	460
Cisco 8400 Series Secure Routers (M): • C8455-G2 • C8475-G2	S	2	80	60
	M	4	250	230
	L	8	480	460

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be deployed on UCS E-Series server modules that reside in Cisco 4000 Series Integrated Services Routers and Cisco Catalyst 8300 Series Edge Platforms.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can deploy Cisco Catalyst 8000V instances on UCS E-Series UCS-E1100D-M6 server modules that are installed in Cisco Catalyst 8000 Series Edge platforms.

Device Family	Device Model	Supported UCS-E Module and DRE Profiles
Cisco 4000 Series Integrated Services Routers	Cisco 4461	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4451	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4351	UCS-E160S-M3/K9 (S)
	Cisco 4331	UCS-E160S-M3/K9 (S)

Device Family	Device Model	Supported UCS-E Module and DRE Profiles
Cisco Catalyst 8300 Series Edge Platforms	C8300-2N2S-4T2X	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L) UCS-E1100D-M6 (S)
	C8300-2N2S-6T	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L) UCS-E1100D-M6 (S)
	C8300-1N1S-4T2X	UCS-E160S-M3/K9 (S)
	C8300-1N1S-6T	UCS-E160S-M3/K9 (S)

Restrictions for DRE

- DRE is a dual-side solution. Therefore, flow symmetry is required to configure DRE optimization. DRE isn't supported for asymmetric flows.
- DRE is supported only if integrated service nodes or external service nodes are deployed at both ends of a Cisco Catalyst SD-WAN overlay tunnel.
- DRE isn't supported on devices that are configured as service controllers.
- In a scenario where Unified Threat Defense (UTD) is installed on a router and there is a data policy to redirect the traffic to an external service node, if the traffic is learned by UTD for a given VRF, then the same traffic cannot be redirected to an external service node.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a the default mode for SSL proxy is single-side. However, because DRE is a dual-side solution, it requires SSL on both, the sending and the receiving end, of the traffic. To optimize SSL performance for this dual-side use case, enable dual-side SSL optimization using the `dual-side optimization enable` command in Cisco SD-WAN Manager CLI templates. We don't recommended enabling dual-side SSL if you use GRE tunnels over the WAN.
- From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, SMB 311 auto bypass of encrypted traffic is enabled to the DRE. You can continue to manually enable the SMB311 encrypted traffic bypass policy to DRE, for the service nodes running on the devices prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.
- DRE optimization is not supported for Cisco Catalyst 8000V when deployed on Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) on CSP devices.

Restrictions for Installing Cisco Catalyst 8000V on UCS E-Series Servers

Note UCS E-Series Server support is applicable for installing Cisco Catalyst 8000V as an external service node starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only.

- Only the VMware vSphere ESXi (release 6.7) hypervisor is supported for deploying Cisco Catalyst 8000V instances on UCS-E Series server modules.
- Hyperthreading should be disabled on VMware vSpehere ESXi hypervisor.
- Hyperthreading is not supported for the app-heavy core allocation profile for Cisco Catalyst 8000V deployed on UCS E-Series servers.
- Cisco Catalyst 8000V instances on UCS-E series server modules can only have 6, 8, or 12 cores.
- Cisco Catalyst 8000V instances on UCS-E series server modules should be configured with the app-heavy core allocation profile to enable them to run the DRE service.
- Only one Cisco Catalyst 8000V instance can be installed on a supported UCS E-Series server.
- To change the DRE profile applied to a device, you need to uninstall DRE, reinstall it, and then apply the new DRE profile.

  Uninstalling DRE results in loss of cache data.
- Configuring AppQoE DRE medium profile using configuration groups is not supported on C8235-E-G2 platforms.

Configure DRE

Before You Begin

Cisco Catalyst 8000V instances on UCS and USC E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization. Ensure to reload the device in order to apply the core allocation.

The following example shows how to configure a device as app-heavy using the Cisco SD-WAN Manager CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Upload DRE Container Image to the Software Repository

Prerequisite

Download the DRE container image from Cisco software downloads page. To download the DRE container image navigate to Catalyst 8000V Edge Software page and select IOS XE SD-WAN Software. You can use the same container image across the Cisco 8000 platform.

Upload the Container Image to Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Under **Upload Virtual Image**, choose **Manager**.
4. Browse to the downloaded container image on your local machine, and then click **Upload**.

When the upload is complete, the image appears in the **Virtual Images** window.

Upgrade DRE Container Virtual Image

To upgrade the container image, see Upgrade Software Image on a Device.

Enable DRE Optimization

Configure AppQoE Template for DRE

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose a device that is supported for DRE.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose on of the following device roles:
   - **Controller:** Choose **Controller** if you want to configure the device as a controller with an integrated service node. For devices that support an integrated service node, the **Enable** checkbox is available. This option is grayed out for devices that don't support the integrated service node functionality.
   - **Service Node:** Choose the **Service Node** option if you want to configure the device as an external service node. The **External Service Node** check box is enabled by default.

     The **Service Node** option is not visible if the device that you chose cannot be configured as an external service node.
7. Under **Advanced**, enable **DRE Optimization**.

Note The Resource Profile field is applicable for DRE profiles. The DRE profiles feature was introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. Therefore, this option is not available in previous releases.

(Optional) In the **Resource Profile** field, choose **Global** from the drop-down list. Next, choose a profile size from the options available.

If you don't configure the **Resource Profile**, the default DRE profile size for the device is applied. For more information on the default profiles, see Supported DRE Profiles.

9. (Optional) To optimize HTTPS, FTPS, or any other encrypted traffic, enable **SSL Decryption**.

Note If you enable **SSL Decryption**, you must configure an SSL/TLS decryption security policy so that the TLS service can decrypt the traffic before it is sent to the DRE container, and then encrypted again after the traffic is optimized.

10. Click **Save**.

Create Security Policy for SSL Decryption

This procedure applies if you enable SSL decryption at the time of configuring the AppQoE feature template to enable DRE optimization.

Configure CA for SSL Proxy

To configure certificate authority for SSL proxy, see Configure CA for SSL/TLS Proxy.

Configure Security Policy for SSL Decryption

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. Choose **Application Quality of Experience** and click **Proceed**.
4. Click **Add TLS/SSL Decryption Policy** and choose **Create New**.
5. Click **Enable SSL Decryption**. Alternatively, toggle the **SSL Decryption** option to enable it.
6. Enter **Policy Name** and other requested details.
7. Click **Save TLS/SSL Decryption Policy**. Your new policy appears in the window.
8. Click **Next**.
9. Enter **Security Policy Name** and **Security Policy Description**.
10. To view the CLI configuration for the policy, click **Preview**. Otherwise, click **Save**.

Update Device Template

For the DRE configuration to take effect, attach the AppQoE policy with DRE enabled, to the device template of the device for which you created the AppQoE policy with DRE.

1. To create a new device template or update an existing one, see Create a Device Template from Feature Templates
2. In the **Additional Templates** area, for **AppQoE**, choose the template you created in the Configure AppQoE Template for DRE section.

Note To deactivate the DRE service, detach the AppQoE template from the device template.

Create a Centralized Policy for TCP and DRE Optimization

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Under **Centralized Policy**, click **Add Policy**.

Note For more information, see Configure Centralized Policies Using Cisco SD-WAN Manager.

3. In the policy configuration wizard, click **Next** until you are on the **Configure Traffic Rules** window.
4. Click **Traffic Data**, and then click **Add Policy**.
5. Enter a name and description for your policy.
6. Click **Sequence Type** and from the **Add Data Policy** dialog box, choose **Custom**.
7. Click **Add Sequence Rule**.
8. Under the **Match** option, you can choose any match conditions that are applicable to a data policy, such as, Source Data Prefix, Application/Application Family List, and so on.
9. Under the **Actions** option, choose **Accept**. Choose **TCP Optimization** and **DRE Optimization** from the options.

   From Cisco Catalyst SD-WAN Manager Release 20.14.1, AppQoE clusters can handle both IPv4 and IPv6 traffic.

Note Not all actions are available for all match conditions. The actions available to you depend on the match conditions you choose. For more information, see Configure Traffic Rules.

10. Click **Save Match And Actions**.
11. Click **Save Data Policy**.
12. Apply the centralized data policy to the edge devices at the sites between which DRE optimization should be triggered for traffic flows. For more information, see Apply Policies to Sites and VPNs.
13. Activate the centralized policy. For more information, see Activate a Centralized Policy.

Configure DRE using Configuration Groups

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can enable DRE optimisation using Cisco SD-WAN Manager by configuring **AppQoE** feature under **Service Profile** in a configuration group. For more information see, AppQoE.

To optimize HTTPS, FTPS, or any other encrypted traffic, configure and deploy **TLS/SSL Decryption** from policy groups. For more information see, Embedded Security Additional Settings.

Note You can configure DRE using configuration groups only on DRE supported device platforms. If you enable AppQoE DRE optimization in a configuration group and deploy a device that does not support DRE, the deployment fails.

Configure DRE Using the CLI

Install DRE Container Package

To install the DRE container package, use the following command:

```
app-hosting install appid < name > package bootflash:<name>.tar
```

Configure Virtual Port Group and Map it to DRE

The following example shows how to configure a virtual port group and map it to the DRE service, and then start the DRE service:

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre


Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Configure Virtual Port Group and Map it to DRE, and Assign a DRE Profile

Note The DRE Profiles feature is available starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only. This feature is not applicable to releases before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example shows how to configure a virtual port group, map it to the DRE service and assign a DRE profile to the device. This example shows the small (S) profile being assigned.

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252
```

```
Device(config-if)# app-hosting appid dre
Device(config-app-hosting)# app-resource profile-package small
```

```
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Activate DRE Service

The following example shows how to activate DRE service for the application named Bangalore:

```
Device# app-hosting activate appid Bangalore
```

Note Use the **app-hosting activate appid** command if you've already configured the DRE application, but haven't enabled it. Alternatively, you can use the **start** command in application hosting gateway configuration mode, as shown in the example in the preceding section.

Uninstall DRE

Follow these steps to deactivate and uninstall the DRE service.

1. Use the following command in privileged EXEC mode to stop the DRE service.

   ```
   Device# app-hosting stop appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be stopped.

2. Use the following command in privileged EXEC mode to deactivate the DRE service.

   ```
   Device# app-hosting deactivate appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be deactivated.

3. Use the following command in privileged EXEC mode to uninstall the DRE service.

   ```
   Device# app-hosting uninstall appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be uninstalled.

Create Security Policy for SSL Decryption using Policy Groups

Use this task to configure SSL decryption within the policy group framework. SSL decryption is managed via the Next-Generation (NG) Firewall settings within the Policy Group.

Prerequsites

Create a TLS/SSL decryption profile. For more information, see TLS/SSL Decryption in Configure a Security Policy Using a Policy Group.

Follow these steps to create a security policy for SSL decryption using policy groups.

1. From the SD-WAN Manager menu, choose **Configuration** > > **Policy Groups**, and then select **NGFW**.
2. Click **Additional Settings** to configure additional NGFW settings for a security policy.

3. Enter the required details. For more information, see Configure NGFW Additional Settings.
4. Choose the TLS/SSL decryption profile from the drop-down list.
5. Click **Save**.

The SSL decryption policy is successfully configured and mapped to the target devices within the policy group.

Create a Centralized Policy for TCP and DRE Optimization using Policy Groups

Use this task to enable TCP optimization and Data Redundancy Elimination (DRE) by configuring traffic rules within the policy group.

Follow these steps to create a centralized policy for TCP and DRE optimization using policy groups.

1. From the SD-WAN Manager menu, choose **Configuration** > > **Policy Groups**, and then select **+ Add Policy Group**.
2. Enter a policy group name, choose a solution from the drop-down list and provide a description (optional).
3. Click **Create**.

   Note: If you have already created a policy group, click the policy group from the list of available policy groups to edit.
4. Specify the name of the policy group.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
5. Provide a description for the policy group. It can contain up to 2048 characters including spaces.
6. Click NGFW to choose a firewall policy.

   If you created an SSL Proxy (TLS/SSL Decryption) policy before, select it here to map the SSL Proxy policy to the policy group. Otherwise, leave the **NGFW** field blank.
7. Choose an application priority for the policy group from the drop-down list. Click **Create New** to create a new application priority. Enter a policy name and description.
8. Click the **Advanced** button on the top-right corner of the window to swtich to the advanced view. The advanced view provides further options to configure the traffic policy along with rules, service level agreement (SLA) class, and QoS Map.
9. To configure the traffic policy, specify a name for the traffic policy.
10. Choose a VPN from the drop-down list.
11. Choose the direction for applying the policy:
    a. All: Bidirectional traffic flow
    b. Service: Incoming traffic from service
    c. Tunnel: Incoming traffic from tunnel

12. Choose one of the following default actions for the packets based on the rules:
    a. Accept
    b. Drop
13. Add rules for the traffic policy.
14. Specify a sequence number and name for the rule.
15. Choose a protocol from the drop-down list:
    a. IPv4
    b. IPv6
    c. Both
16. Choose a value for the match condition from the available options.
17. In the Match conditions, click **Source** and **Data Prefix**.
18. Click **Source Data Prefix**. To match a list of source prefixes, select the list from the drop-down. Otherwise, enter a value.
19. Click **Destination** and **Data Prefix**.
20. Click **Destination Data Prefix**. To match a list of destination prefixes, select the list from the drop-down. Otherwise, enter a value or a create new data prefix.
21. Click **+ Action** Actions, and then click **Counter**, and enter the name of the file in which to store packet counters.
22. Choose one of the following base actions for the packets based on the rules **Accept** or **Drop**.
23. Click **+ Add Action** conditions, click **AppQoE Optimization**. Choose the optimization type.
24. Click **Save Match and Actions**.
25. Click **Save** to save the traffic and policy settings.
26. Save the application priority for the policy group.
27. Click **+Add** adjacent to Associated field to select or unselect devices to associate or dissociate with the policy group. In the associate devices workflow, you can choose devices.
28. Click **Deploy** to select sites and deploy the policy group.

Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be installed as external service nodes on supported UCS E-Series servers that reside in specific router models. This functionality enables the routers to act as hybrid clusters with integrated as well as external service nodes.

Configuration Workflow

1. Configure the UCS E-Series server on the supported router.
2. Deploy Cisco Catalyst 8000V on the supported UCS E-Series server.
3. In Cisco SD-WAN Manager, configure AppQoE feature template for Cisco Catalyst 8000V instances on UCS E-Series servers.
4. In Cisco SD-WAN Manager, configure the AppQoE feature template for the service controllers, and add additional configuration using Cisco SD-WAN Manager CLI template and CLI Add-on feature template.

Configure UCS E-Series Server

Before You Begin

Insert the UCS E-Series server module into the supported device and connect two interfaces (TE2 and TE3) from the front panel. For more information, see UCS-E Series Servers Hardware Installation Guide.

Configure UCS E-Series Server on the Supported Router

The following is sample configuration to enable UCS E-Series server on a supported router:

```
Device(config)# ucse subslot 1/0
Device(config-ucse)# imc access-port shared-lom <ge1/te2/te3>
Device(config-ucse)# imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x
Device(config-ucse)# exit
Device(config)# interface ucse1/0/0
Device(config-if)# ip address x.x.x.1 255.255.255.0
```

Deploy Cisco Catalyst 8000V on UCS E-Series Server

Before You Begin

- Install the hypervisor on the UCS-E server module.
- Download the Cisco Catalyst 8000V 17.6.1 OVA file from the Cisco software download page for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and install it..

Configure IP Addresses for Cisco Catalyst 8000V

The following is a sample for configuring IP addresses for Cisco Catalyst 8000V on the UCS E-Series server:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# description Mgmt
Device(config-if)# ip addeess x.x.x.x x.x.x.x
Device(config)# int GigabitEthernet2
Device(config-if)# description WAN-CONTROLLER
Device(config-if)# ip address x.x.x.x x.x.x.x
Device(config-if)# exit
Device(config)# int GigabitEthernet3
Device(config-if)# description UCSE-INTF
Device(config-if)# ip addeess x.x.x.x x.x.x.x
```

Configure AppQoE Feature Template for Cisco Catalyst 8000V Instances

Before You Begin

Cisco Catalyst 8000V instances on UCS E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization. Ensure to reload the device in order to apply the core allocation.

The following example shows how to configure a device as app-heavy using the Cisco SD-WAN Manager CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Enable DRE Optimization for Cisco Catalyst 8000V Instances

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose **C8000v**.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose the **Service Node** option.
7. Under the **Advanced** section, enable **DRE Optimization**.
8. Click **Save**.

Configure the Controller Cluster Types

Add UCS E-Series Server Configuration in Cisco SD-WAN Manager

In Cisco SD-WAN Manager, create a CLI Add-on feature template and update it with UCS E-Series server configuration.

The following is sample configuration for UCS E-Series servers that can be added to the CLI Add-on feature template:

```
ucse subslot 1/0
imc access-port shared-lom te2
imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x

interface ucse1/0/0
vrf forwarding 5
```

Option 1: Configure Service Controller as the Cluster Type

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates** and then click **Add Template**.



Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. In the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Leave the **Integrated Service Node** check box unchecked.
7. In the **Controller IP address** field, enter the IP address of the controller.

   Alternatively, choose **Default** from the drop-down list. The AppQoE controller address is chosen by default.
8. In the **Service VPN** field, enter the service VPN number.

   Alternatively, choose **Default** from the drop-down list. The AppQoE service VPN is chosen by default.
9. In the **Service Nodes** area, click **Add Service Nodes** to add service nodes to the AppQoE service node group.
10. Click **Save**.
11. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:
    - CLI Add-on feature template with the UCS E-Series server configuration
    - AppQoE feature template

    For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as the integrated service node separately. For more information, see Enable DRE Optimization.

Option 2: Configure Hybrid as the Cluster Type

Routers that have Cisco Catalyst 8000V instances deployed on their UCS E-Series servers can be configured with cluster types as service-controllers or hybrid.

1. From theCisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.



Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.

5. Enter **Template Name** and **Description**.
6. For the **Integrated Service Node** field, check the **Enable** check box.
7. Click **Save**.
8. Create a CLI template to add the cluster-type hybrid configuration.

   The following is a sample configuration to configure the cluster type as hybrid on the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

```
interface VirtualPortGroup2
 vrf forwarding 5
 ip address 192.168.2.1 255.255.255.0

interface ucse1/0/0
 vrf forwarding 5
 ip address 10.40.17.1 255.255.255.0
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
service-insertion service-node-group appqoe SNG-APPQOE1
 service-node 10.40.17.5
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 10.40.17.1 vrf 5

service-insertion service-context appqoe/1
 cluster-type hybrid
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
 service-node-group SNG-APPQOE1
 vrf global
 enable
```

9. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:
   - AppQoE feature template
   - CLI Add-on feature template with the UCS E-Series server configuration
   - CLI template with the hybrid cluster configuration

   For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as integrated service node separately. For more information, see Enable DRE Optimization.

Monitor DRE

To view the AppQoE DRE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.
- Add the following commands to the device configuration:
  - **policy ip visibility features multi-sn enable**
  - **policy ip visibility features dre enable**
  - **policy ip visibility features sslproxy enable** (for SSL traffic)

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic or applications optimized by DRE using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor traffic or applications optimized by DRE.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **AppQoE DRE Optimization**.
4. Enable **On-Demand Troubleshooting** to view details of the selected device.
5. Choose **Optimized Traffic** or **Application**, depending on what you want to monitor.
6. Choose **Controller** or **Service Node**.

   If the chosen device has an integrated service node, you can view the data for either the controller role or the service node role. If the chosen device is an external AppQoE service node, you can view the monitoring data for the external service node, as well as the controller that it's connected to.

Chart and Table View Options

The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

- From the **Chart Options** drop-down list, you can view the data by **Bytes** or **Percentage Reduction**.
- You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

Verify and Monitor and Troubleshoot DRE Using CLI

DRE Optimization Status

The following is a sample output of the **show sdwan appqoe dreopt status** command:

```
Device# show sdwan appqoe dreopt status

DRE ID                                          : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                      : 18:27:43

Health status                                   : GREEN

Health status change reason                     : None

Last health status change time                  : 18:25:29
```

```
Last health status notification sent time        : 1 second
DRE cache status                                 : Active
Disk cache usage                                 : 91%
Disk latency                                     : 16 ms
Active alarms:
  None


Configuration:
  Profile type                             : Default
  Maximum connections                      : 750
  Maximum fanout                           : 35
  Disk size                                : 400 GB
  Memory size                              : 4096 MB
  CPU cores                                : 1
  Disk encryption                          : ON
```

To view the status in more detail, use the **show sdwan appqoe dreopt status detail** command.

```
Device# show sdwan appqoe dreopt statistics detail
Total connections                 : 325071
Max concurrent connections        : 704
Current active connections        : 0
Total connection resets           : 297319
Total original bytes              : 6280 GB
Total optimized bytes             : 2831 GB
Overall reduction ratio           : 54%
Disk size used                    : 93%
Cache details:
  Cache status                      : Active
  Cache Size                        : 406573 MB
  Cache used                        : 93%
  Oldest data in cache              : 17:13:53:40
  Replaced(last hour): size         : 0 MB
  Cache created at                  : 27:14:13:43
  Evicted cache in loading cache    : 149610430464
```

```
Connection reset reasons:
  Socket write failures                              : 0
  Socket read failures                               : 0
  DRE decode failures                                : 0
  DRE encode failures                                : 0
  Connection init failures                           : 0
  WAN unexpected close                               : 297319
  Buffer allocation or manipulation failed           : 0
  Peer received reset from end host                  : 0
  DRE connection state out of sync                   : 0
  Memory allocation failed for buffer heads          : 0
  Other reasons                                      : 0
Connection Statistics:
  Alloc                                              : 325071
  Free                                               : 325071
Overall EBP stats:
  Data EBP received                                  : 1921181978
  Data EBP freed                                     : 1921181978
  Data EBP allocated                                 : 218881701
  Data EBP sent                                      : 218881701
  Data EBP send failed                               : 0
  Data EBP no flow context                           : 0
  Data EBP requested more than max size              : 46714730
```

DRE Auto-bypass Status

The following example shows the auto-bypass status of DRE optimization.

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
Update   Entry Age
-------------------------------------------------------------------------------------------------------

      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

DRE Optimization Statistics

The following example shows DRE optimization statistics.

```
Device# show sdwan appqoe dreopt statistics

Total connections                  : 3714

Max concurrent connections         : 552

Current active connections         : 0

Total connection resets            : 1081

Total original bytes               : 360 GB

Total optimized bytes              : 164 GB

Overall reduction ratio            : 54%

Disk size used                     : 91%

Cache details:

  Cache status                       : Active

  Cache Size                         : 407098 MB

  Cache used                         : 91%

  Oldest data in cache               : 03:02:07:55

  Replaced(last hour): size          : 0 MB
```

The following example shows DRE optimization statistics for a peer device.

```
Device# show sdwan appqoe dreopt statistics peer

  Peer No.  System IP          Hostname    Active connections    Cummulative connections
-----------------------------------------------------------------------------------------

         0  209.165.201.1       dreopt                     0                       3714
```

DRE Decryption Status

The following example shows how to send a decryption request to DRE and verify if the request was successfully received.

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT

1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

```
SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

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

DECRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

SIGNATURE BLOCK |     188616     188616          0

SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

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

Troubleshoot DRE

The following sample output displays the statistics for the auto discovery of peer devices. When connections are not optimized by DRE, run this command and share the output with Cisco Technical Support.

```
Device# show sdwan appqoe ad-statistics

============================================================

              Auto-Discovery Statistics

============================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99

 [Core] AD Negotiation Start                 : 10375

 [Core] AD Negotiation Done                  : 10329

 [Core] Rcvd ACK w/o AD options              : 0

 [Core] AOIM sync Needed                     : 0
```

The following sample output displays the statistics for one time exchange of information between peer devices.

```
Device# show sdwan appqoe aoim-statistics

============================================================

              AOIM Statistics

============================================================

 Total Number Of Peer Syncs      : 1

 Current Number Of Peer Syncs in Progress      : 0

 Number Of Peer Re-Syncs Needed      : 1

 Total Passthrough Connections Due to Peer Version Mismatch   : 0

 AOIM DB Size (Bytes): 4194304


 LOCAL AO Statistics

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

 Number Of AOs      : 2

 AO             Version   Registered

 SSL             1.2        Y

 DRE             0.23       Y


 PEER Statistics

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

 Number Of Peers      : 1

 Peer ID: 203.203.203.11

 Peer Num AOs      : 2

 AO             Version   InCompatible

 SSL             1.2        N

 DRE             0.23       N
```

The following example shows how to clear DRE cache. Clearing cache restarts the DRE service.

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```

Monitor SSL Proxy

To view the AppQoE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.

- Add the **policy ip visibility features sslproxy enable** command to the device configuration:

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic optimized by SSL Proxy using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor traffic optimized by SSL Proxy.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **SSL Proxy**.
4. Enable **On-Demand Troubleshooting** to view details of the selected device.
5. Choose **Traffic View** type from the drop-down menu to view data in graph or tabular format.

   You can also click **Filter** to choose by VPN, local or remote TLOC, traffic source and more.

Chart and Table View Options

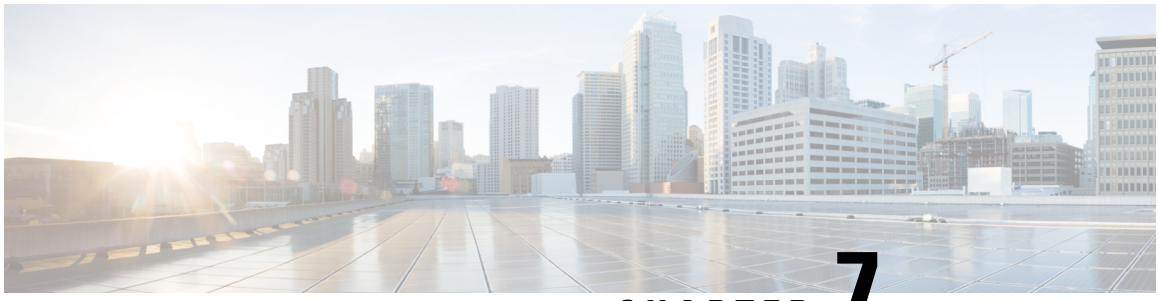
The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

Verify SSL Proxy Support for TLS 1.3 Using CLI

The following is a sample output from the **show ssl proxy statistics** command showcases SSL statistics and TLS flow counters. The count for the TLS flow counter for version 1.3 is shown as 8.

```
Device# show sslproxy statistics
============================================================
SSL Statistics:
============================================================
Flow Selected SSL/TLS version:
TLS 1.0 Flows : 0
TLS 1.1 Flows : 0
TLS 1.2 Flows : 0
TLS 1.3 Flows : 8
```



CHAPTER 7

HTTP CONNECT

Table 11: Feature History

Feature Name	Release Information	Description
HTTP CONNECT	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces support for handling the HTTP CONNECT method in AppQoE. With this support, services such as SSL Proxy and DRE optimize HTTP CONNECT encrypted traffic.

- Information About HTTP CONNECT, on page 81
- Prerequisites for HTTP CONNECT, on page 81
- Restrictions For HTTP CONNECT, on page 82
- Use Cases Of HTTP CONNECT, on page 82
- Configure HTTP CONNECT Using a CLI Add-On Template, on page 82
- Configure HTTP CONNECT Using CLI, on page 82
- Verify HTTP CONNECT Configuration, on page 83
- Monitor HTTP CONNECT Using the CLI, on page 84

Information About HTTP CONNECT

HTTP CONNECT method enables the source server to start two-way communications with the destination server using an explicit proxy server. Using the HTTP CONNECT you can create a HTTP proxy tunnel over a TCP connection between the source and destination servers. The HTTP CONNECT traffic handling enables SSL Proxy and DRE to optimize the encrypted data in the HTTP Tunnel.

For more information on SSL/TLS Proxy see, Information about SSL/TLS Proxy.

Prerequisites for HTTP CONNECT

- Ensure that the Cisco IOS XE Catalyst SD-WAN Devices are running the Cisco IOS XE Catalyst SD-WAN Release 17.9.1a.
- An explicit proxy hosted on a remote server is required to broadcast a HTTP CONNECT request.

Restrictions For HTTP CONNECT

- A HTTP CONNECT request is intended to be sent only to a proxy server.
- A HTTP CONNECT request can be sent only using the following standard ports Port 80, 8080, and 8088.
- HTTP CONNECT is not supported by United Threat Defense (UTD). Hence the configuration is blocked if UTD is enabled.

Use Cases Of HTTP CONNECT

SSL Proxy Traffic without HTTP CONNECT

In Cisco IOS XE Catalyst SD-WAN Release 17.x releases, without the decryption of data, DRE fails to observe repeating patterns in a flow and the DRE compression is not effective. And hence, bypassing the DRE for the flow is mandatory or the data flowing to the DRE should be in clear text. When a HTTP CONNECT request is placed, the SSL Proxy doesn't decrypt the HTTP CONNECT SSL traffic, which results in the encrypted traffic flowing to the DRE, that fails to optimize the traffic.

SSL Proxy Traffic with HTTP CONNECT

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, HTTP CONNECT handling in AppQoE enables the SSL Proxy to decrypt and send clear text data to the DRE for further optimizing.

Configure HTTP CONNECT Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure HTTP CONNECT Using CLI

1. Enter configuration mode.

   ```
   config-transaction
   ```

2. Enable HTTP CONNECT

   ```
   sdwan appqoe http-connect enable server-port <port-number>
   ```



Note You can only enter the following standard server port numbers to enable HTTP CONNECT: 80, 8080, and 8088.

If you don't enter a standard port number, the default server-port number is assumed as 80.

3. Commit the changes

   commit

   For example,

   sdwan appqoe http-connect enable server-port80

4. Attach the CLI add-on template to the respective device.

Verify HTTP CONNECT Configuration

The following is a sample output from the **show sslproxy statistics** command:

```
Device# show sslproxy statistics
=========================================================

              SSL Proxy Statistics

=========================================================

Connection Statistics:

Total Connections                 : 3

Proxied Connections               : 0

Non-proxied Connections           : 3

Clear Connections                 : 0

Active Proxied Connections        : 0

Active Non-proxied Connections    : 2

Active Clear Connections          : 0

Max Conc Proxied Connections      : 0

Max Conc Non-proxied Connections  : 2

Max Conc Clear Connections        : 0

Tunneled Proxied Connections      : 2

Tunneled Non-proxied Connections  : 0

Active Tunneled Proxied Flows     : 1

Active Tunneled Non-proxied Flows  : 0

Max Conc Tunneled Proxied Flows    : 1

Max Conc Tunneled Non-proxied Flows: 0

SSL Encrypted marked Non SSL Flows : 0

Total Closed Connections          : 2
```

In this output, **Tunnel Proxied Connections** and **Tunneled Non-proxied Connections** indicate that HTTP CONNECT request is successful.

Monitor HTTP CONNECT Using the CLI

Use the **show sdwan appqoe flow flow-id** command to monitor HTTP CONNECT on a device. The following is an example output:

```
Device# show sdwan appqoe flow flow-id 4278327056727738
Flow ID: 4278327056727738
VPN: 1  APP: 0 [Client 192.0.2.0:49470 - Server 192.0.2.24:8080]

HTTP Connect: 1
TCP stats
---------
Client Bytes Received   : 215
Client Bytes Sent       : 46
Server Bytes Received   : 208
Server Bytes Sent       : 193

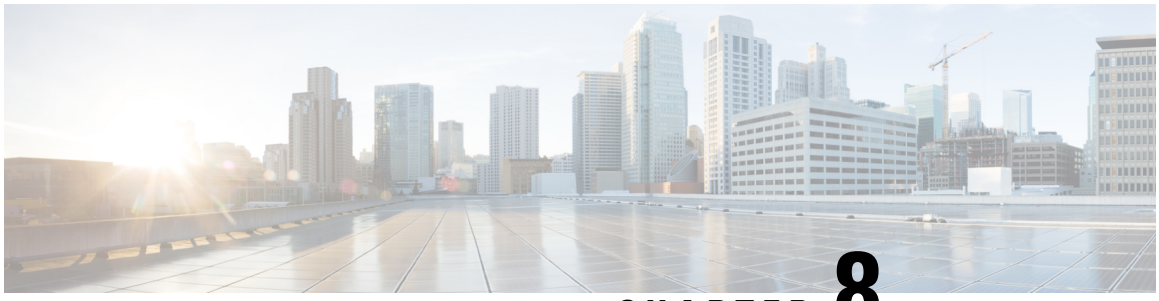
Client Bytes sent to SSL: 215
Server Bytes sent to SSL: 168

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 152
S2C HTX to DRE Pkts     : 4
C2S DRE to HTX Bytes    : 70
C2S DRE to HTX Pkts     : 3
S2C DRE to HTX Bytes    : 46
S2C DRE to HTX Pkts     : 2

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 129
S2C SVC Bytes to SSL    : 46
C2S SSL to TCP Tx Pkts  : 6
C2S SSL to TCP Tx Bytes : 193
S2C SSL to TCP Tx Pkts  : 2
S2C SSL to TCP Tx Bytes : 46
```

In this output, **HTTP Connect: 1** indicates that HTTP CONNECT request is successful.



CHAPTER 8

AppQoE Verification and Troubleshooting

Table 12: Feature History

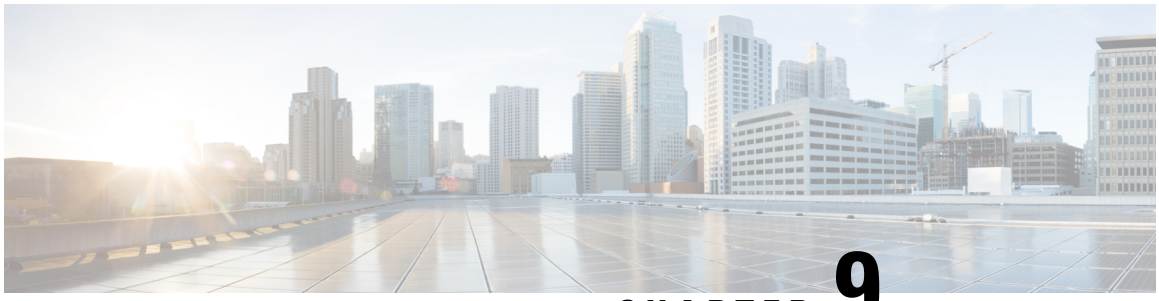
Feature Name	Release Information	Description
Enhanced Troubleshooting for AppQoE	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This release introduces additional show commands to verify and troubleshoot issues in AppQoE features. A few existing show commands for AppQoE have also been enhanced. - show sdwan appqoe error recent - show sdwan appqoe status - show sdwan appqoe flow closed (command modified to include the keyword error) - show sslproxy status (command output modified)

show Commands for AppQoE

Use the following commands to verify the configuration of various AppQoE features and troubleshoot common issues:

- show sdwan appqoe
- show sdwan appqoe dreopt
- show sdwan appqoe dreopt statistics
- show sdwan appqoe error recent
- show sdwan appqoe status
- show sdwan appqoe flow closed
- show sdwan appqoe flow flow-id
- show sdwan appqoe flow vpn-id

- show sslproxy status



CHAPTER 9

Troubleshoot Cisco Catalyst SD-WAN AppQoE

- Overview, on page 87
- Support Articles, on page 87
- Feedback Request, on page 88
- Disclaimer and Caution, on page 88

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following support article is associated with this technology:

Document	Description
Configure TCP Optimization Feature on Cisco IOS® XE SD-WAN cEdge Routers	This document describes the Transmission Control Protocol (TCP) Optimization feature on Cisco IOS® XE SD-WAN routers, which was introduced in 16.12 release in August 2019. The topics covered are prerequisites, problem description, solution, the differences in TCP optimization algorithms between Viptela OS (vEdge) and XE SD-WAN devices, configuration, verification and list of related documents.

Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.