

Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide

First Published: 2019-07-19

Last Modified: 2026-06-24

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)

© 2019–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

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

CHAPTER 3 **Cisco SD-WAN Manager Monitor Overview** 5

- Information About Customizing the Monitor Overview Dashboard 9
  - Benefits of Customizing the Monitor Overview Dashboard 10
- Restrictions for Customizing the Monitor Overview Dashboard 10
- Customize the Monitor Overview Dashboard 10
  - Add a Dashlet 10
  - Delete a Dashlet 11
  - Rearrange Dashlets 11
  - Restore Default Settings 12
- Filter the Dashboard Data 12
- Monitor Cellular Devices 13
  - View Cellular Device Count 13
  - View Cellular Health Dashlet 13
  - View Cellular Devices 15
- View Controller and Device Information 15
- View Cisco SD-WAN Manager Status 15
- View EoX Status 16
- View Certificate Status Pane 17
- View Licensing Pane 17
- View Reboot Pane 18
- View Control Status Pane 18
- View BFD Connectivity Pane 19

View Transport Interface Distribution Pane 20
View WAN Edge Inventory Pane 21
View WAN Edge Health Pane 22
View Transport Health Pane 23
View Top Applications Pane 24
View Application-Aware Routing Pane 26
View Web Server Certificate Expiration Date Notification 26
View Maintenance Windows Alert Notification 27
View Application Health Dashlet 27
View Tunnel Health Dashlet 28
View Top Alarms Dashlet 28
View temperature and energy usage dashlet 29
View underlay alarms dashlet 30
View data plane drops dashlet 30
View WAN Edge Health Dashlet 31
View WAN Edge Management Dashlet 32
View Site Health Dashlet 32
View Site Health in Table View 33
View Site Health in Heatmap View 34
View Sites in Global Network View 34
Security 36
View Top Threats 38
View Firewall Rule Counter 39
View Intrusion Prevention 40
View URL Filtering 40
View Advanced Malware Protection 41
View Security Events 42
View Security Appliance-UTD Container 43
View Application Offload 44
View Secure Internet Gateway Tunnels 44
View SecureX Ribbon 45
Troubleshooting 45
Cannot See Data 45
Multicloud 45

Explore 48
Energy management 49
Supported Platforms for Energy Management 50
Advisories 50
Benefits of Advisories 50
Prerequisites for Advisories 50
View Security Advisory 51
Perform a scan in Advisories 51
View Field Notices 52
Converged Dashboard for SD-WAN Analytics and SD-WAN Manager 52
Information About Converged Dashboard 52
Applications Dashboard 53
Sites Dashboard 54
Circuits Dashboard 55
Client Dashlet 55

CHAPTER 4 **Secure Cisco Catalyst SD-WAN with Live Protect** 57
Feature history for Live Protect 57
Live Protect for Cisco Catalyst SD-WAN 57
Benefits of Live Protect 58
Live Protect Vulnerability Shield lifecycle 58
Lifecycle policy scope 58
Vulnerability Shield availability 59
Configure Live Protect using Cisco SD-WAN Manager 60
Disable Live Protect using Cisco SD-WAN Manager 61
Monitor Live Protect 61
View shield status for Live Protect 61
View event statistics for Live Protect 62

CHAPTER 5 **Cisco SD-WAN Manager Data Storage** 63
Information About Cisco SD-WAN Manager Data Storage 63
Configure Cisco SD-WAN Manager Data Storage 63
View Cisco SD-WAN Manager Data Storage 66

CHAPTER 6 **Application Performance and Site Monitoring** 67

Overview of Application Performance and Site Monitoring 67

Restrictions for Application Performance and Site Monitoring 68

Configure Application Performance and Site Monitoring using Configuration Groups 69

Configure Application Performance and Site Monitoring Using a CLI Add-on Template 70

All Sites and Single Site View 71

View Application Health in Table View 72

View Application Health in Heatmap View 72

Troubleshoot Application Performance and Site Monitoring 73

CHAPTER 7 **Devices and Controllers** 77

View the Geographic Location of Your Devices 78

View System Status 81

View Device System Resource Utilization in Cisco SD-WAN Manager 82

View Device System Resource Utilization Using the CLI 82

View and Open TAC Cases 83

View the Status of a Cisco Catalyst SD-WAN Validator 84

View the Status of a Cisco Catalyst SD-WAN Controller 85

View Control Connections 86

View Devices Connected to Cisco Catalyst SD-WAN Manager 86

View Services Running on Cisco Catalyst SD-WAN Manager 86

View Device Status in the Overlay Network 87

View Device Information 87

View Device Health in Table View 88

View Device Health in Heatmap View 89

View Device Configuration 90

View the Software Versions Installed on a Device 90

View Device Interfaces 90

View WAN Interfaces 91

View Interfaces in Management VPN or VPN 512 92

View DHCP Server and Interface Information 92

View Interface MTU Information 93

View and Monitor Cellular Interfaces 93

View Colocation Cluster Information 95
View Cisco Colo Manager Health 96
View Cisco Catalyst SD-WAN Manager Cluster Information Using the CLI 97
View QoS statistics 97
QoS queue statistics 97
Benefits of QoS queue statistics 98
Restrictions for QoS statistics 98
Monitor the QoS statistics for interfaces 98
Interface QoS statistics 99
Monitor the QoS statistics for tunnels 100
Tunnel QoS statistics 100
Monitor real time tunnel QoS statistics 102
Collect System Information in an Admin-Tech File 103
Information About Admin Tech for Collecting System Information 104
Benefits of an Admin-Tech File for Collecting System Information 105
Prerequisites for Collecting System Information in an Admin-Tech File 105
Restrictions for Collecting System Information in an Admin-Tech File 105
Generate Admin-Tech Files 105
View Admin-Tech Files 107
Upload an Admin-Tech File to a TAC Case 108
Monitor Cflowd and SAIE Flows for Cisco IOS XE Catalyst SD-WAN Devices 108
Reboot a Device 109
Reset Interfaces 111
Make Your Device Invalid 111
Bring Your Device Back to Valid State 111
Stop Data Traffic 112
Perform a Factory Reset 112
Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices 113
Information About Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices 113
Supported Devices for Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices 115
Configure Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI 116

Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI 117

CHAPTER 8 **Hosted edge services** 119

Hosted edge services 119

Restrictions for monitoring hosted edge services 119

Start or stop the hosted edge services 120

Monitor the hosted edge services 120

CHAPTER 9 **Network** 125

View AppQoE Information 127

View a Configuration Commit List 127

Determine the Status of Network Sites 128

View Network Site Topology 129

Information About Site Topology 129

Supported Devices for Site Topology Visualization 130

Prerequisites for Site Topology Visualization 130

View Network Site Topology 130

Data Collection and Cisco Catalyst SD-WAN Telemetry 131

Information About Data Collection and Cisco Catalyst SD-WAN Telemetry 131

Enable or Disable Cisco Catalyst SD-WAN Telemetry 132

Enable or Disable Data Collection 133

Enable or Disable Cloud Services 133

Additional Steps to Enable Data Collection on an On-Premises Cisco Catalyst SD-WAN Manager Instance 134

Rediscover Network 135

View Routing Information 135

View Multicast Information 137

View Data Policies 138

BFD Protocol 139

View BFD Session Information 141

View BGP Information 142

View Cflowd Information 142

View Cloud Express Information 144

View ARP Table Entries 144
Run Site-to-Site Speed Test 145
View Network-Wide Path Insight 145
View NMS Server Status 146
View Cisco Catalyst SD-WAN Validator Information 146
Run a Traceroute 147
View Tunnel Loss Statistics 148
View SAIE Flows 148
View VNF Status 150
View TCP Optimization Information 150
View SFP Information 152
Monitor NAT DIA Tracker Configuration on IPv4 Interfaces 152
View TLOC Loss, Latency, and Jitter Information 153
View Tunnel Connections 154
View Tunnel Health in Table View 156
View Tunnel Health in Heatmap View 156
View License Information 157
View Logging Information 157
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels 158
View WiFi Configuration 159
View Control Connections in Real Time 159
View Cisco Umbrella Information 160
View VRRP Information 160
View PKI Trustpoint Information 160
View QoS Information 161
View WLAN Output 163
View Client Details 163
Check Traffic Health 164
View Tunnel Health 164
Check Application-Aware Routing Traffic 165
Capture Packets 166
Information About Bidirectional Packet Capture 166
Configure Packet Capture Using Cisco SD-WAN Manager 166
Configure Packet Capture Using a CLI Template 168

Simulate Flows 169
Security Monitoring 171
View Traffic, CPU, and Memory Usage 171
View the Health and Reachability of UTD 171
View the System Clock 172

CHAPTER 10 **Alarms, Events, and Logs** 173
Alarms 173
Information About Alarms 175
Alarms Details 176
View Alarms 178
Filter Alarms 180
Export Alarms 181
Alarm Notifications 181
Events 184
Information About Events 185
Events Details 186
View Events 188
Filter Events 188
Export Events 189
Monitor Event Notifications 189
ACL Log 190
Audit Logging 190
Information About Protecting Against Unauthorized Login Activity 190
Configure a Lockout Policy for Cisco SD-WAN Manager Using a CLI Template 191
Configure a Login-Rate Alarm Threshold for Cisco SD-WAN Manager Using a CLI Template 192
View Audit Log Information 193
View Log of Configuration Template Activities 194
Syslog Messages 194
Cisco SD-WAN Manager Logs 197
View Log of Certificate Activities 199
Binary Trace for Cisco Catalyst SD-WAN Daemons 200
Configure Binary Trace Level 201
View Binary Trace Level 202

View Messages Logged by Binary Trace for a Cisco Catalyst SD-WAN Process 202
View Messages Logged by Binary Trace for All Cisco Catalyst SD-WAN Processes 203
Traffic Logs 204
Information about traffic logs 204
Benefits of traffic logs 204
Restrictions for traffic logs 205
Generate traffic logs using Cisco SD-WAN Manager 205
Troubleshoot traffic logs 206
Safety Barriers 207
Safety Barriers 207

CHAPTER 11 Reports 209
Information About Reports 209
Restrictions for Reports 210
Run a Report 210
Run a Report 210
Configure Email Settings 211
View Generated Reports 212
Download a Report 212
Edit a Report 212
Rerun a Report 212
Cancel a Scheduled Report 213
Delete a Report 213

CHAPTER 12 Manage Software Upgrade and Repository 215
Manage Software Upgrade and Repository 216
Information about software upgrade 219
Device version compliance 220
Restrictions for software upgrade 222
Upgrade Virtual Image on a Device 223
Upgrade the Software Image on a Device 224
Activate a New Software Image 226
Upgrade a CSP Device with a Cisco NFVIS Upgrade Image 227
Delete a Software Image 228

Set the Default Software Version 228
Export Device Data in CSV Format 228
View Log of Software Upgrade Activities 229
Manage Software Repository 229
Register Remote Server 229
Enable devices to use a remote repository server 230
Manage Remote Server 230
Add Software Images to the Repository 231
View Software Images 233
Add Virtual Images to the Repository 233
Upload VNF Images 235
Create Customized VNF Image 237
View VNF Images 242
Delete a Software Image from the Repository 242
Delete VNF Images 243

CHAPTER 13 **Software Upgrade Workflow** 245
Information About Software Upgrade Workflow 246
Benefits of Software Upgrade Workflow 246
Information About Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later 247
Supported Devices for the Software Upgrade Workflow 247
Prerequisites for Using the Software Upgrade Workflow 248
Restrictions for software upgrade 248
Access the Software Upgrade Workflow 249
Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 and Later 250
Schedule Software Upgrade Workflow 251
Schedule a Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later 252
Cancel the Scheduled Software Upgrade Workflow 252
Delete a Downloaded Software Image 252

CHAPTER 14 **Software Maintenance Upgrade** 255

Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices 255
Information About Software Maintenance Upgrade 255
Supported Devices for Software Maintenance Upgrade 257
Manage Software Maintenance Upgrade Images 257
Install and Activate an SMU Image Using the CLI 259
Deactivate and Remove an SMU Image Using the CLI 262

CHAPTER 15 **Cisco Catalyst SD-WAN Control Components Upgrade Workflow 267**
Information About Cisco Catalyst SD-WAN Control Components Upgrade Workflow 268
Benefits of Using Cisco Catalyst SD-WAN Control Components Upgrade Workflow 268
Prerequisite for Cisco Catalyst SD-WAN Control Components Upgrade Workflow 269
Restrictions for Cisco Catalyst SD-WAN Control Components Upgrade Workflow 269
Upgrade Cisco Catalyst SD-WAN Control Components Using a Workflow 269
Scheduling Cisco Catalyst SD-WAN Control Components Upgrade Using Workflow 270
Reschedule a Cisco Catalyst SD-WAN Control Components Upgrade 271
Cancel a Scheduled Cisco Catalyst SD-WAN Control Components Upgrade 271

CHAPTER 16 **Configuration Consistency across Cisco Catalyst SD-WAN Controllers 273**
Information about Configuration Consistency across Cisco Catalyst SD-WAN Controllers 274
Multi-stage Approach for Configuration Consistency across Cisco Catalyst SD-WAN Controllers 274
Supported Devices for Configuration Consistency across Cisco Catalyst SD-WAN Controllers 275
Restrictions for Configuration Consistency across Cisco Catalyst SD-WAN Controllers 275
Scenarios for Offline Cisco Catalyst SD-WAN Controllers 276
Warning Messages for Offline Cisco SD-WAN Controllers 278
Verify Consistent Configuration across Cisco Catalyst SD-WAN Controllers 278

CHAPTER 17 **Export and Import Cisco SD-WAN Manager Configurations 281**
Information About Exporting and Importing Cisco SD-WAN Manager Configurations 281
Prerequisites for Exporting and Importing Cisco SD-WAN Manager Configurations 282
Restrictions for Exporting and Importing Cisco SD-WAN Manager Configurations 282
Use Cases for Exporting and Importing Cisco SD-WAN Manager Configurations 282
Export Cisco SD-WAN Manager Configurations 282
Import Cisco SD-WAN Manager Configurations 283

CHAPTER 18 **Cellular Modem Firmware Upgrade** 285

Cellular Modem Firmware Upgrade 285

Information About Cellular Modem Firmware Upgrade 286

Example Illustrating Cellular Modem Firmware Upgrade 287

Benefits of Cellular Modem Firmware Upgrade 288

Supported Platforms for Cellular Modem Firmware Upgrade 288

Supported Platforms for Wi-Fi module firmware upgrade 288

Prerequisites for Cellular Modem Firmware Upgrade 288

Prerequisites for Wi-Fi module firmware upgrades 289

Restrictions for Cellular Modem Firmware Upgrade 289

Order of firmware upgrade 289

Upgrade the Cellular Modem Firmware of a Device 290

View the Status of a Cellular Modem Firmware Upgrade 291

Configure a Remote File Server for Firmware Upgrade Images 292

Firmware upgrade for P-LTE-450 MHz modules 292

Firmware upgrade for Wi-Fi modules 293

Upgrading module firmware using Cisco SD-WAN Manager 293

Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules 294

CHAPTER 19 **Protocol Pack Management and Compliance** 297

Protocol Pack Management and Compliance 297

Information About Protocol Pack Management and Compliance 298

Upgrading when a device becomes compatible 299

Restrictions for Protocol Pack Management and Compliance 299

Upload a Protocol Pack to Cisco SD-WAN Manager 300

Upgrade a device Protocol Pack 301

Check Protocol Pack Compliance 301

View Protocol Pack Status 302

Delete Protocol Packs 303

CHAPTER 20 **Remote Server Support for ZTP Software Upgrade** 305

Information About Remote Server Support for ZTP Upgrade 305

Benefits of Remote Server Support for ZTP Upgrade 306

Supported Devices for Remote Server Support for ZTP Upgrade 307
Prerequisites for Remote Server Support for ZTP Upgrade 307
Restrictions for Remote Server Support for ZTP Upgrade 307
Enable Enforce Software Version (ZTP) 308
Upload Device List 308
Use Cisco Catalyst SD-WAN Manager to Configure and Upgrade a Device 309
Monitor the ZTP Software Install 310

CHAPTER 21 **Connectivity Fault Management** 311
Information About Connectivity Fault Management 311
Introduction to Ethernet CFM 311
Restrictions for Configuring Ethernet CFM 311
How CFM Works in Cisco Catalyst SD-WAN 312
Down Maintenance End Points 312
Ethernet CFM and Ethernet OAM Interaction 312
SNMP Traps 313
Configure Ethernet CFM using Cisco SD-WAN Manager CLI Template 313

CHAPTER 22 **Troubleshooting** 317
Troubleshoot Common Cellular Interface Issues 318
Troubleshoot WiFi Connections 321
Troubleshoot a Device 325
Check Device Bringup 325
Ping a Device 326
Speed Test 327
Information About Speed Test 327
Prerequisites for Speed Test 328
Run Speed Test 328
Troubleshooting Speed Test Issues 330
Run a Traceroute 330
Discover Underlay Paths 331
Diagnostic Monitoring Log Capture 331
Configure Diagnostic Monitoring Log Capture 332
BFD Tunnel Troubleshooting 332

On-Demand Troubleshooting 334
Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit 339
Cisco RADKit in Cisco SD-WAN Manager 340
Cisco RADKit Restrictions 340
Enable Cisco RADKit service in Cisco SD-WAN Manager 340
Use the Cisco RADKit Service APIs 341
Verify Cisco RADKit service in Cisco SD-WAN Manager 342

CHAPTER 23 **Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS** 345
Information About the Unified Debug Condition 345
Restrictions of the Unified Debug Condition 346
Use Cases for the Unified Debug Condition 346
Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI 346
Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS 348

CHAPTER 24 **Packet Trace** 353
Information About Packet Trace 354
Configure Packet Trace 355
Monitor Packet Trace 356
Monitor Packet Trace on Cisco vEdge devices 356
Monitor Packet Trace on Cisco IOS XE Catalyst SD-WAN Devices 357
View FIA Statistics 360
Configuration Examples for Packet Trace 361

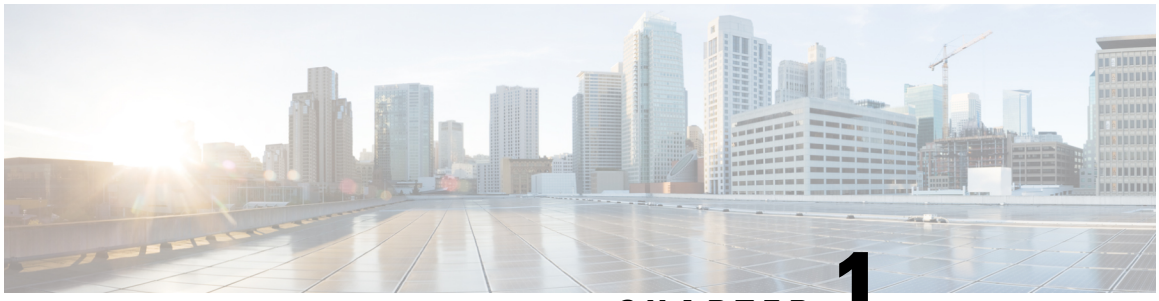
CHAPTER 25 **Underlay Measurement and Tracing Services** 363
Information About Underlay Measurement and Tracing Services 364
Benefits of Underlay Measurement and Tracing Services 365
Prerequisites for Underlay Measurement and Tracing Services 365
Restrictions for Underlay Measurement and Tracing Services 365
Configure Underlay Measurement and Tracing Services 366
Configure Underlay Measurement and Tracing Services Using a CLI Template 367
Trace and View Tunnel Paths On Demand 368
Troubleshooting Underlay Measurement and Tracing Services 369
Zero IP Address 369

Timeout Error 369
Configuration Example for Underlay Measurement and Tracing Services 369

CHAPTER 26 Analytics 371
Internet Outages 371
View Internet Outages 371

CHAPTER 27 Troubleshoot Cisco Catalyst SD-WAN Solution 373
Overview 373
Support Articles 373
Feedback Request 374
Disclaimer and Caution 374

CHAPTER 28 Appendix 375
Syslog Messages 375
UTD Syslogs 412
Permanent Alarms and Alarm Fields 416



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
- User Documentation for Cisco SD-WAN Release 20

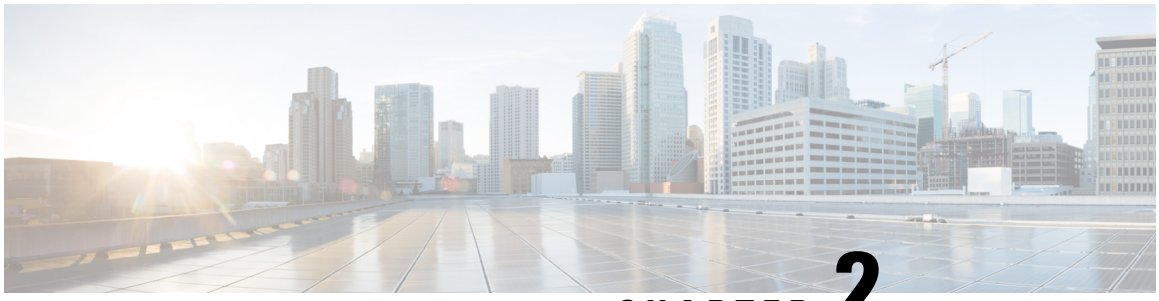
Communications, Services, and Additional Information

- 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 (SD-WAN) and Cisco Catalyst SD-WAN Releases

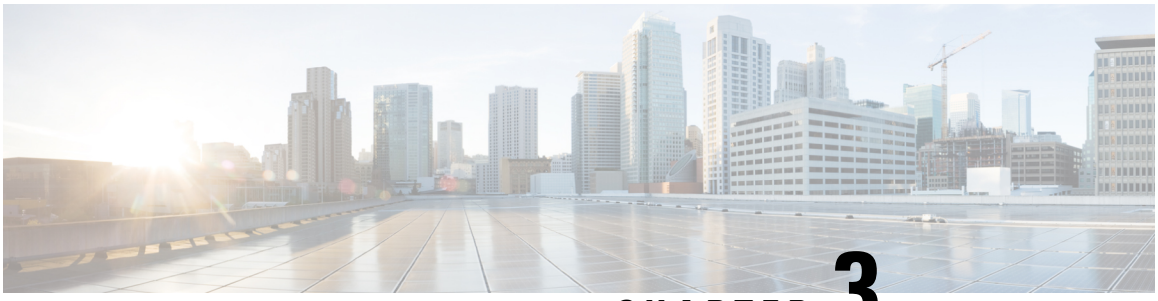
Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following links includes release-wise new and modified features that are documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

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

What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x

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

What's New in Cisco SD-WAN (vEdge) Release 19.x



CHAPTER 3

Cisco SD-WAN Manager Monitor Overview

Table 1: Feature History

Feature Name	Release Information	Description
Enhanced Cisco SD-WAN Manager User Interface for a Consolidated Monitoring View	Cisco vManage Release 20.7.1	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all the monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all the monitoring components have been organized into buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu for you to easily locate these features.
Customizable Monitor Overview Dashboard in Cisco SD-WAN Manager	Cisco vManage Release 20.9.1	This feature adds customizability to the **Monitor Overview** dashboard. It gives you the flexibility to specify which dashlets to view and sort them based on your personal preferences.
Time Filter in Monitor Overview and Monitor Security Dashboards in Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	The time filter option added to the **Monitor Overview** and **Monitor Security** dashboards in Cisco SD-WAN Manager enables you to filter the dashboard data for a specified time range.
View Sites in Global Topology View	Cisco vManage Release 20.11.1	You can view all sites or a single site in the global topology view for geographical regions worldwide by clicking the inverted-drop-shaped icon on the **Monitor Overview** dashboard.

Feature Name	Release Information	Description
View Top Alarms	Cisco vManage Release 20.11.1	You can view alarm details for a single site on the **Monitor Overview** dashboard. Click **View Details** to open the **Monitor** > **Logs** > **Alarms** window and view the alarm details.
View WAN Edge Management	Cisco vManage Release 20.11.1	You can view the WAN Edge Management dashlet on the **Monitor Overview** dashboard.
Security Dashboard Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enhances the security dashboard in Cisco SD-WAN Manager. The security dashboard introduces a **Actions** drop-down list that enables you to edit the security dashboard, reset the security dashboard, and view the **SecureX** ribbon in the security dashboard. Also, you can access the Cisco Talos portal from Cisco SD-WAN Manager. A hyperlink of the Cisco Talos portal is added to the security dashboard.
Global Network View with Network-Wide Path Insight Integration	Cisco Catalyst SD-WAN Manager Release 20.12.1	Network-Wide Path Insight is now integrated with the global network view. This feature also introduces enhancements to the geomap view by providing real-time monitoring of the health of each site. **Global Topology View** is now called as **Global Network View** in Cisco Catalyst SD-WAN Manager.
Security Dashboard Enhancements	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enhances the security dashboard to provide greater flexibility while troubleshooting security threats down to a device level in Cisco Catalyst SD-WAN.
Explore Menu Option	Cisco Catalyst SD-WAN Manager Release 20.13.1	An Explore page provides quick access to various Cisco resources relevant to specific job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. The resources include developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more, in a single pane of glass.

Feature Name	Release Information	Description
Security Dashboard Enhancements	Cisco Catalyst SD-WAN Manager Release 20.14.1	The Security dashboard in Cisco SD-WAN Manager has the following enhancements: • A **Security Appliance/UTD Container** dashlet is added to monitor the health status of the Firewall and UTD components, such as the Cisco Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), and Cisco URL filtering. • A new **Application Offload** dashlet is introduced that displays the breakdown of application traffic across SIG or Secure Service Edge (SSE) tunnels and Direct Internet Access (DIA), and provides more details about the application traffic. • Enhancements to existing dashlets to provide additional information about events. • A redirect is added from the Intrusion Prevention dashlet to the Talos website to view Snort rules.
Improved Monitoring of Cellular-Enabled Devices	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1 Cisco IOS CG Release 17.14.1	Cisco SD-WAN Manager provides detailed information about the connectivity of cellular-enabled devices, and the health of the connections, to provide a holistic view of cellular connectivity health. In addition, you can filter the device list to specifically display cellular-enabled devices, among other filter options.
Converged Cisco SD-WAN Manager and Cisco SD-WAN Analytics Dashboard	Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature introduces a converged dashboard in Cisco SD-WAN Manager that merges the monitoring and analytics capabilities from both Cisco SD-WAN Manager and Cisco SD-WAN Analytics. This converged dashboard displays management data from the Cisco SD-WAN Manager alongside analytical insights from Cisco SD-WAN Analytics. To view a converged dashboard in Cisco SD-WAN Manager, Cisco SD-WAN Analytics must be onboarded into Cisco SD-WAN Manager.
Energy Management	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature introduces a new dashboard that displays the Cisco SD-WAN Manager power utilization, energy usage, device capability, and consumption data.

Feature Name	Release Information	Description
Improved Monitoring of Cellular-Enabled Devices	Cisco Catalyst SD-WAN Manager Release 20.16.1	The following cellular monitoring dashlets in Cisco SD-WAN Manager have been enhanced to provide additional insights for building and maintaining a competitive cellular WAN solution: • Cellular Device Count • Cellular Health • Cellular Data Usage
Advisories	Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature provides centralized visibility into security vulnerabilities and critical field notices for your Cisco SD-WAN network. It offers EoX Status section that provides detailed End-of-Support and End-of-Sale information for effective replacement and upgrade planning.
Underlay Health Visibility	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature provides enhanced monitoring and troubleshooting capabilities for the underlying network infrastructure that supports your Cisco Catalyst SD-WAN overlay.

The following dashlets are available by default on the **Monitor** > **Overview** dashboard in Cisco SD-WAN Manager. (In Cisco vManage Release 20.6.1 and earlier releases, these dashlets are part of **Dashboard** > **Main Dashboard**.)

- **Site Health**
- **Tunnel Health**
- **WAN Edge Health**
- **Application Health**
- **Top Applications**
- **WAN Edge Management**

- Information About Customizing the Monitor Overview Dashboard, on page 9
- Restrictions for Customizing the Monitor Overview Dashboard, on page 10
- Customize the Monitor Overview Dashboard, on page 10
- Filter the Dashboard Data, on page 12
- Monitor Cellular Devices, on page 13
- View Controller and Device Information, on page 15
- View Cisco SD-WAN Manager Status, on page 15
- View EoX Status, on page 16
- View Certificate Status Pane, on page 17
- View Licensing Pane, on page 17
- View Reboot Pane, on page 18

• View Control Status Pane, on page 18
• View BFD Connectivity Pane, on page 19
• View Transport Interface Distribution Pane, on page 20
• View WAN Edge Inventory Pane, on page 21
• View WAN Edge Health Pane, on page 22
• View Transport Health Pane, on page 23
• View Top Applications Pane, on page 24
• View Application-Aware Routing Pane, on page 26
• View Web Server Certificate Expiration Date Notification, on page 26
• View Maintenance Windows Alert Notification, on page 27
• View Application Health Dashlet, on page 27
• View Tunnel Health Dashlet, on page 28
• View Top Alarms Dashlet, on page 28
• View temperature and energy usage dashlet, on page 29
• View underlay alarms dashlet, on page 30
• View data plane drops dashlet, on page 30
• View WAN Edge Health Dashlet, on page 31
• View WAN Edge Management Dashlet, on page 32
• View Site Health Dashlet, on page 32
• Security, on page 36
• Multicloud, on page 45
• Explore, on page 48
• Energy management, on page 49
• Advisories, on page 50
• Converged Dashboard for SD-WAN Analytics and SD-WAN Manager, on page 52

Information About Customizing the Monitor Overview Dashboard

Minimum release: Cisco vManage Release 20.9.1

By default, the **Monitor Overview** dashboard displays all the available dashlets that help you monitor the different components and services of a Cisco Catalyst SD-WAN overlay network. The customizable dashboard feature enables you to do the following:

- Add dashlets
- Delete dashlets
- Rearrange dashlets
- Restore default settings

The customized dashboard settings are saved in a database. These settings are retrieved in the following scenarios:

- When you log in to Cisco SD-WAN Manager again.
- When you navigate from another window to the **Monitor Overview** dashboard.
- When you upgrade Cisco SD-WAN Manager from an earlier release to a new release.

Note We recommend that you use Google Chrome browser to access Cisco SD-WAN Manager. However, Firefox browser is also supported.

This feature is available in both single-tenant and multitenant deployments. However, in multitenant deployments, this feature is available only for the tenant dashboard.

Note Users belonging to all the standard and custom user groups, regardless of the read or write permissions, can customize the **Monitor Overview** dashboard.

Benefits of Customizing the Monitor Overview Dashboard

- Flexibility: Customizing the dashboard enables you to view the most relevant dashlets, and to reduce clutter by removing the dashlets that are less relevant for your purposes.
- Efficiency: You can view all the key metrics at a glance, and evaluate and analyze them more quickly.
- Easy Organization: You can drag and drop the dashlets and organize the dashboard according to your requirements. For example, you can easily drag a dashlet that is particularly relevant to you, to the top.

Restrictions for Customizing the Monitor Overview Dashboard

Minimum release: Cisco vManage Release 20.9.1

- In multitenant deployments, this feature is available only for the tenant dashboard.
- This feature is available only for the **Monitor Overview** dashboard.
- The menu bar, which runs across the top of the **Monitor Overview** dashboard, is not customizable.
- When the dashboard is in edit mode, other actions, such as selecting a time period for which to display data, viewing real-time data, and so on, are disabled.

Customize the Monitor Overview Dashboard

Minimum release: Cisco vManage Release 20.9.1

Add a Dashlet

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Edit Dashboard**.
3. Click **Add Dashlet**.

Note The **Add Dashlet** option is available only if additional dashlets are available to be added. It is not available on the default dashboard.

4. Choose the dashlets that you want to add.
5. Click **Add**.
6. Click **Save**.

You can customize the following dashlets:

- **Transport Health**
- **Site BFD Connectivity**
- **Transport Interface Distribution**
- **WAN Edge Inventory**
- **Application-Aware Routing**
- **Remote Access Sessions**
- **Remote Access Headends**

Note The remote access sessions and remote access headends dashlets are available from Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases.

Delete a Dashlet

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Edit Dashboard**.
3. Click the **Delete** icon adjacent to the corresponding dashlet name.
4. To confirm the deletion of the dashlet, click **Yes**.
5. Click **Save**.

Rearrange Dashlets

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Edit Dashboard**.
3. Drag and drop the dashlets according to your requirements.
4. Click **Save**.

Restore Default Settings

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Reset to Default View**.
3. Click **Apply**.

Filter the Dashboard Data

Minimum release: Cisco vManage Release 20.10.1

You can view the data on the **Monitor Overview** and **Monitor Security** dashboards based on a specified time range. A time filter option is available on these dashboards. On the **Monitor Overview** dashboard, the time filter option is applicable to the following dashlets:

- **Site Health**
- **Tunnel Health**
- **WAN Edge Health**
- **Application Health**
- **Transport Health**
- **Top Alarms**
- **Top Applications**

This feature is available in both single-tenant and multitenant deployments. In multitenant deployments, this feature is available only in the tenant dashboard.

Only in the **Transport Health** dashlet, the data is available up to 7 days. In the **Site Health**, **Tunnel Health**, **WAN Edge Health**, **Application Health**, and **Top Applications** dashlets, the data is available up to 24 hours.

Default: 24 hours

To filter the data, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** or **Monitor** > **Security**.
2. From the time filter drop-down list, choose a value.

   The dashlets display the data based on the chosen time.

You also can apply the time filter at the dashlet level. To do this, click **View Details** in the corresponding dashlet, and choose a time filter value in the right navigation pane. The time filter value applied at the dashboard level, and not at the dashlet level, is preserved after closing the navigation pane.

Monitor Cellular Devices

View Cellular Device Count

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the **Cellular Carriers Details** dashlet has been renamed to **Cellular Device Count** dashlet.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1

The **Cellular Device Count** dashlet has been enhanced to provide additional information about cellular devices managed by Cisco SD-WAN Manager. The **Cellular Device Count** dashlet displays the total number of cellular devices in a donut chart, showing active devices and standby devices. Active devices are those with the cellular link in use, while standby devices are those with the cellular link not in use. The data on the dashlet changes based on the selected filter.

Filter Options

The dashlet offers different filtering options:

Count by Product: This filter shows the top 5 products and their count by status. It also provides details on the types of cellular devices, such as PIM modules, integrated devices, NIM modules, and dongles. Click **View Details** for more information about the types of products.

Count by Carrier: This allows you to filter the devices by different cellular carriers. This also displays the number of devices associated with each carrier.

Count by Radio Access Technology: This filter shows the number of devices using different radio technologies such as 3G, 4G, and 5G. For 5G, it shows the split between NSA and SA. If 5G NR-NSA is configured, both radio access technologies are counted but considered a single cellular device. In a Dual PIM scenario, if both PIMs are active, they are counted as two cellular devices.

Click **View Details** to see more granular information about the **Cellular Device Count** dashlet.

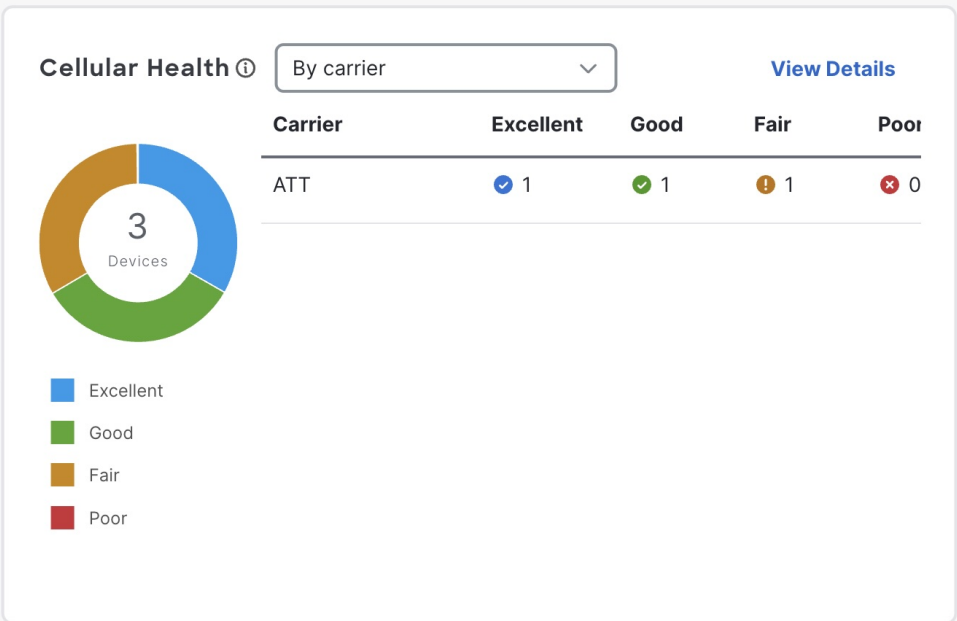
View Cellular Health Dashlet

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1.

View detailed information about the connectivity of cellular-enabled devices, and the health of the connections using the **Cellular Health** dashlet in the **Monitor > Overview** page.

This is the Cellular Health dashlet:

Figure 1: Cellular Health



Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the **Cellular Health** dashlet has been enhanced to provide additional information about the health status of cellular connections managed by Cisco SD-WAN Manager. It displays the health metrics of cellular devices categorized based on different filters such as carriers and radio technology. The donut chart displays the total number of cellular devices, with health details represented by color codes: Excellent, Good, Fair, and Poor.

Color Coding

The health status is color-coded to indicate the quality of the connection:

- Excellent: Blue
- Good: Green
- Fair: Orange
- Poor: Red

Filter Options

The dashlet offers different filtering options:

By Carrier: This filter shows the health status of cellular devices based on their carriers. It displays the number of devices under each health category for each carrier.

By Radio Technology: This filter categorizes the health of devices based on the technology used, such as 4G, 5G, and others. It provides a breakdown of health status within each technology type.

Health Metrics: Metrics such as Received Signal Strength Indicator (RSSI), Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), Signal-to-Interference-plus-Noise Ratio (SINR), and Energy per Chip per Interference (EC/IO) are used to determine the health status.

Click **View Details** to see more granular information about the **Cellular Health** dashlet.

Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the cellular link uptime is reported in real-time instead of minutes.

View Cellular Devices

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click the **Summary** pane to expand. Under **Type** choose **Cellular**.

   View all the cellular-enabled devices on your Cisco SD-WAN Manager.

View Controller and Device Information



Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

The **Control Components** and **WAN Edges** areas of the menu bar, which runs across the top of the **Monitor** > **Overview** page, display the total number of Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Manager instances in the overlay network. They also display the status of the devices in the network.

When you click a device number, the **Monitor** > **Devices** page displays detailed information about each device. Click **...** adjacent to the corresponding device to access the device dashboard or the Real Time view or to access the **Tools** > **SSH Terminal**.

In addition to routers in controller mode, from Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco SD-WAN Manager can monitor routers that are in autonomous mode and not part of the Cisco Catalyst SD-WAN overlay network. You can use the **show version | include mode** command to check the mode of a router. On various pages such as the **Devices** page (**Monitor** > **Devices**), these routers appear with the label **SD-Routing** in the **Device Model** column to distinguish them from routers that are part of the overlay network.

In Cisco vManage Release 20.6.x and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Control Components** and **WAN Edges** areas are grouped together in the **Summary** area. (The **Summary** area is part of the **Dashboard** > **Main Dashboard** page.)
- When you click a device number, a pop-up window that displays detailed information of each device, opens.
- The device dashboard or the Real Time view is part of the **Monitor** > **Network** page.

View Cisco SD-WAN Manager Status

You can view details about the health of a device or controller, and the CPU and memory usage on Cisco SD-WAN Manager.

Note When you enter any keyword in the search table filter, results that partially match your search will display. For more accurate results, use the column search feature. This allows you to search within a specific column, ensuring that the results are more relevant to your query. This applies to all pages within the SD-WAN Manager where the search table filter and column search filters are visible.

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

   In the table, the **Health** column shows the device or controller health. Place the cursor over the icon in the column to display **Good**, **Fair**, or **Poor**.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the following are the health status indicators for edge devices:

   - **Good**: Edge device is using less than 88% of available memory, and less than 80% of CPU resources.
   - **Fair**: Edge device is using greater than or equal to 88% of available memory, or 80% of CPU resources.
   - **Poor**: Edge device is using greater than or equal to 93% of available memory, or 90% of CPU resources.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, Cisco SD-WAN Manager uses the same threshold values as those used by edge devices to measure the health of all edge devices. This ensures that health status is shown consistently on the device and on the Cisco SD-WAN Manager.

2. Click a Cisco SD-WAN Manager controller in the table.
3. Under **SECURITY MONITORING**, click **System Status**.

   The **Device 360** page shows the CPU and memory usage.

Note If a Cisco SD-WAN Manager controller is using more than 90% of total memory or CPU, its performance may be degraded. If you cannot log in to Cisco SD-WAN Manager, contact Cisco TAC for assistance.

View EoX Status

From Cisco Catalyst SD-WAN Manager Release 20.18.1 you can access detailed information about End-of-Support and End-of-Sale to plan replacements or upgrades effectively.

Procedure

Step 1 From Cisco SD-WAN Manager, click **Monitor** > **Devices**.

Step 2 Under **EoX Status**, you can view end-of-life and end-of-support announcements for Cisco products.

View Certificate Status Pane

The **Certificate Status** pane displays the state of all certificates on all controller devices, and it shows a count of all expired or invalidated certificates. Click the **Certificate Status** pane to open the **Monitor** > **Devices** > **Certificate** page, which displays the hostname and system IP of the device on which the certificate is installed, the serial number of the certificate, and its expiration date and status.



Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Certificate Status** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of the **Monitor** > **Devices** > **Certificate** page when you click the **Certificate Status** pane.

View Licensing Pane

The **Licensing** pane displays the total number of devices configured and the number of devices licensed. Click the **Licensing** pane to open the **Monitor** > **Devices** > **Licensing** page, which displays the following information of a device:

- Hostname
- Chassis number and device model
- IP address
- Template name
- Smart account and virtual account of the device
- Master software license agreement (MSLA)
- License status of the device
- License type and license name
- Subscription ID

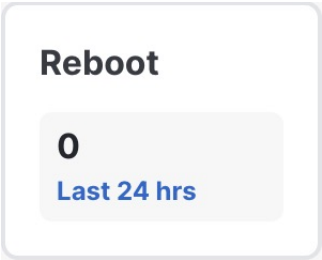


Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Licensing** pane is part of the **Dashboard** > **Main Dashboard** page.

- A pop-up window opens instead of the **Monitor** > **Devices** > **Licensing** page when you click the **Licensing** pane. The pop-up window displays the name of the device, number of licensed devices, number of total licenses, and last assigned on status.

View Reboot Pane



The **Reboot** pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Whewn you click **Reboot**, the **Reboot** sidebar appears, which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than once, each reboot option is reported separately.

In the **Reboot** sidebar, click **Crashes** to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Reboot** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of a sidebar when you click **Reboot**.

View Control Status Pane

The **Control Status** pane is available only in Cisco vManage Release 20.7.1 and earlier releases.

The **Control Status** pane displays whether Cisco SD-WAN Controller and WAN Edge devices are connected to the required number of Cisco SD-WAN Controllers. Each Cisco SD-WAN Controller must connect to all other Cisco SD-WAN Controllers in the network. Each WAN Edge router must connect to the configured maximum number of Cisco SD-WAN Controllers.

The **Control Status** pane shows three counts:

- **Up**: Total number of devices with the required number of operational control plane connections to a Cisco SD-WAN Controller.
- **Partial**: Total number of devices with some, but not all, operational control plane connections to Cisco SD-WAN Controllers.
- **Down**: Total number of devices with no control plane connection to a Cisco SD-WAN Controller.

Note The **Control Status** pane depends upon both Cisco SD-WAN Manager control connection and Cisco SD-WAN Controller control connection states.

Click the UP/Down/Partial data, and the **Monitor** > **Devices** page appears. For the desired device, click **...** to access Device Dashboard or Real Time view or to access the **Tools** > **SSH Terminal**.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Control Status** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Up**, **Partial**, and **Down** statuses are titled **Control Up**, **Partial**, and **Control Down**, respectively.
- A status bar instead of a doughnut chart displays the data.
- A pop-up window opens instead of the **Monitor** > **Devices** page when you click the data.

View BFD Connectivity Pane

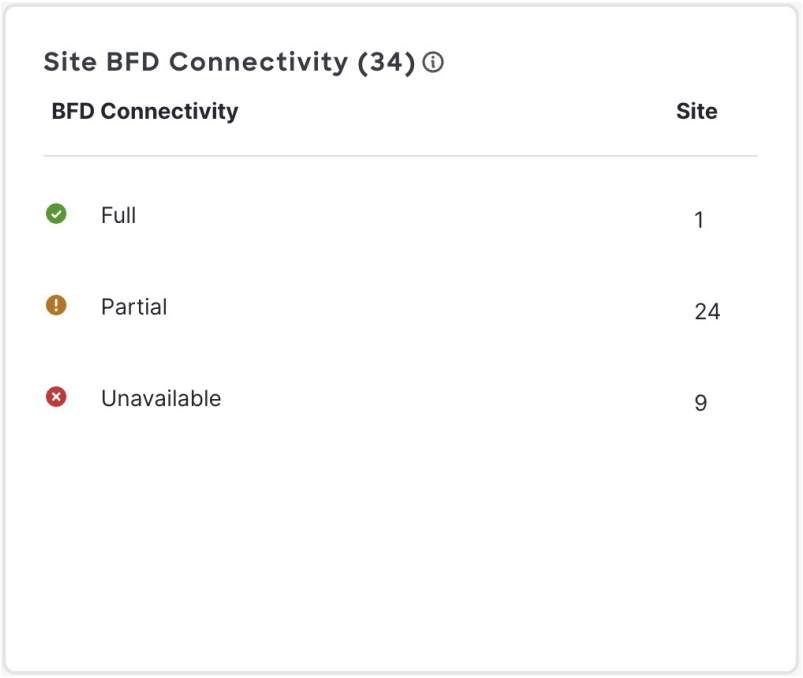
A site is a specific physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each device at a site is identified by the same site ID.

The **Site BFD Connectivity** pane displays the state of a site's data connections. When a site has multiple WAN Edge routers, this pane displays the state for the entire site, not for individual devices. The **Site BFD Connectivity** pane displays three states:

- **Full**: Total number of sites where all BFD sessions on all WAN Edge routers are in the up state.
- **Partial**: Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- **Unavailable**: Total number of sites where all BFD sessions on all WAN Edge routers are in the down state. These sites have no data plane connectivity.

Note The Site Count includes only sites with the installed devices that are up and running. Some sites are excluded from the Site Count if one of the installed devices in the site is down or if TLOC or tunnels are down (relevant for sites with two devices).

When you click **Full**, **Partial**, or the **Unavailable** status, a sidebar appears displaying detailed information of each site, node, or tunnel. For the desired device, click **...** to access the Device Dashboard or Real Time view in the **Monitor** > **Devices** page or to access **Tools** > **SSH Terminal**.



Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

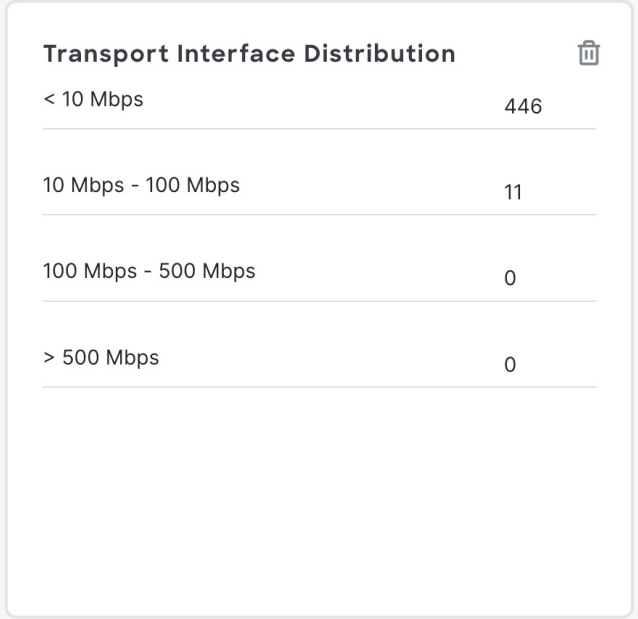
- The **Site BFD Connectivity** pane is titled **Site Health**. The **Site Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Full**, **Partial**, and **Unavailable** statuses are titled **Full WAN Connectivity**, **Partial WAN Connectivity**, and **No WAN Connectivity**, respectively.
- A pop-up window opens instead of a sidebar when you click the data.
- The Device Dashboard or Real Time view is part of the **Monitor** > **Network** page.

View Transport Interface Distribution Pane

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces.

This is the Transport Interface Distribution dashlet:

Figure 2: Transport Interface Distribution



When you click the usage statistics, a sidebar appears, displaying the System IP, Interface, and Average details of interface usage.

Click **View Percent Utilization** to view the interface usage in the last 24 hours for all WAN Edge interfaces in graphical format. The graph is depicted for TLOC Distribution Utilization (%) Vs Interface Count. The tabular statistics displays the Hostname, Interface, Average/Low/High Upstream (%), Average/Low/High Downstream (%), and Bandwidth Utilization information.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Transport Interface Distribution** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of a sidebar when you click the usage statistics.

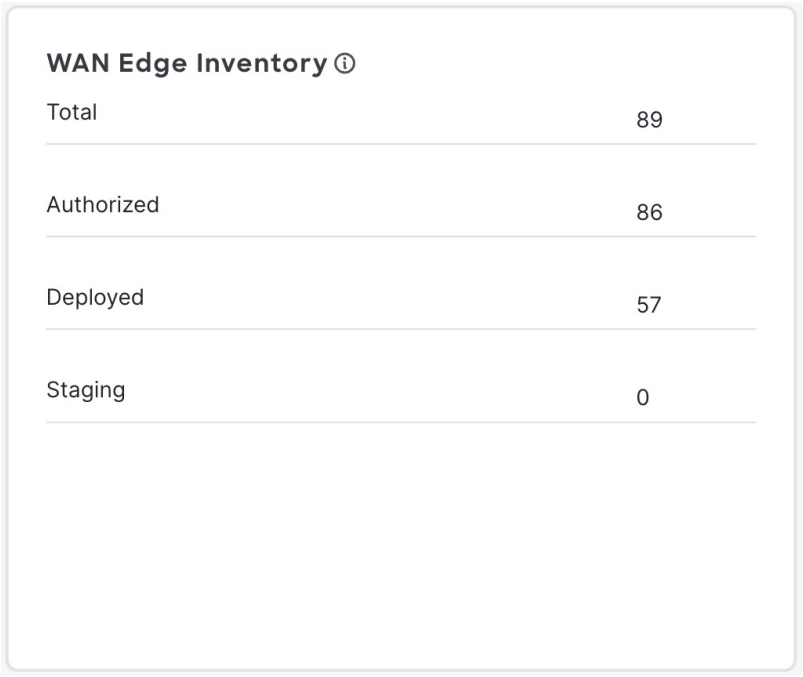
View WAN Edge Inventory Pane

The **WAN Edge Inventory** pane provides four counts:

- Total: Total number of WAN Edge routers whose authorized serial number has been uploaded on theCisco SD-WAN Manager server. The serial number is uploaded in the **Configuration** > **Devices** page.
- Authorized: Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid in the **Configuration** > **Certificates** > **WAN Edge List** page.
- Deployed: Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.

- Staging: Total number of WAN Edge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These routers do not take part in any routing decisions nor do they affect network monitoring through the Cisco SD-WAN Manager.

When you click any statistics, a sidebar appears displaying a table with the hostname, system IP, site ID, and other details of each router.



Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **WAN Edge Inventory** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of a sidebar when you click the data.

View WAN Edge Health Pane

The **WAN Edge Health** pane displays an aggregated view for each router state and a count of how many WAN Edge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- **Good**: Number of routers with memory, hardware, and CPU in good state. Using less than 88% of total memory and 80% of total CPU is classified as good.
- **Fair**: Number of routers with memory, hardware, or CPU in fair state. Using equal to or greater than 88% of total memory and equal to or greater 88% of total memory is classified as in a fair state.
- **Poor**: Number of routers with memory, hardware, or CPU in poor state. Using more than 93% of total memory and more than 93% of total CPU is classified as in a poor state.

The **WAN Edge Health** dashlet displays details about the thresholds of good, fair, and poor devices.

Conditions	Good Devices	Fair Devices	Poor Devices
Reachability	Reachable	Reachable	Not Reachable
Control Plane	All control Connections up	One control connection up	No control connections up
Data Plane	All BFD tunnels up and all TLOCs up	One BFD tunnels up and one TLOCs up	No BFD tunnels up and no TLOCs up
Resources	CPU Usage < 80% Memory Usage < 88%	CPU Usage >=80% Memory Usage >=88%	CPU Usage >= 90% Memory Usage >= 93%
Attributes	All attributes met	Any attributes met	Any attribute met

When you click the statistics, a sidebar appears displaying a table with the last one hour of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. For the desired hostname, click **...** to access the Device Dashboard or Device Details view in the **Monitor** > **Devices** page or to access the **Tools** > **SSH Terminal** page.

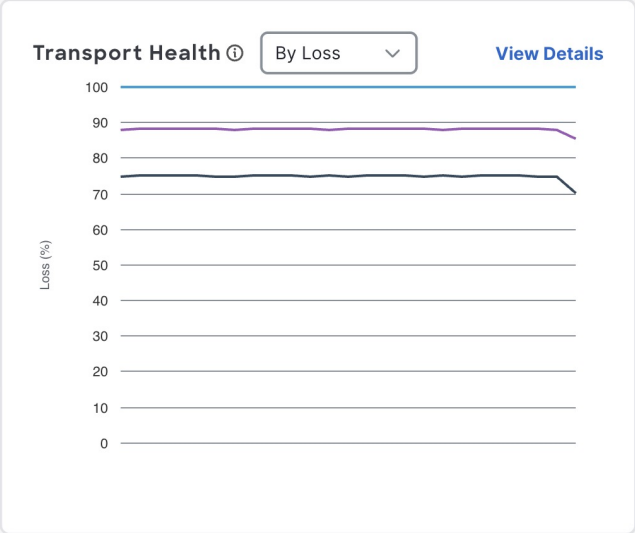
Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **WAN Edge Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Good**, **Fair**, and **Poor** statuses are titled **Normal**, **Warning**, and **Error**, respectively.
- A pop-up window opens instead of a sidebar when you click the data.
- The Device Dashboard or Device Details view is part of the **Monitor** > **Network** page.

View Transport Health Pane

The **Transport Health** pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

- From the **Type** drop-down list, select loss, latency, or jitter.
- Click the **Time** drop-down list to select a time period for which to display data.
- Click **View Details**, and the sidebar displays the information in tabular format. You can change the displayed type and time period as described above.



Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Transport Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Transport Health** pop-up window.

View Top Applications Pane

The **Top Applications** pane in the Cisco SD-WAN Manager **Monitor** > **Overview** page displays the SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting WAN Edge routers in the overlay network.

Note In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

To list top applications by VPN, select a VPN from the drop-down list. To select a time period for which to display data, click the **Time** drop-down list.

To list top applications in a sidebar:

1. Click **View Details** to open the **Top Applications** sidebar. It displays a more detailed view of the same information.
2. In **SAIE Application**, from the **VPN** drop-down list, select the desired VPN, and then click **Search**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Application** is called **DPI Application**.

- Click **Chart** to list the applications.
- Click **Details** to display more information about the applications.

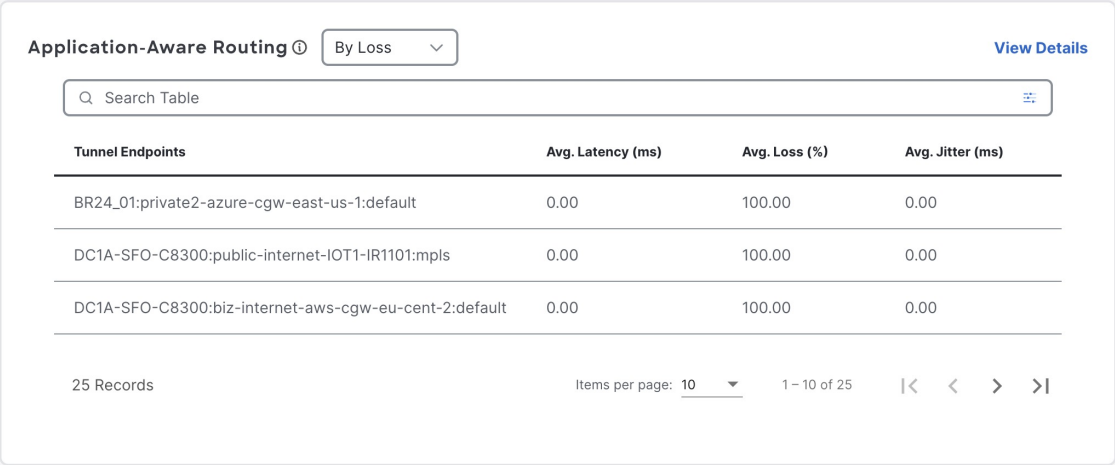
3. Click **SSL Proxy**, from the **View by Policy Actions** drop-down list, select the policy action. All Policy Action, Encrypted, Un-Encrypted, Decrypted view are supported. From the **VPN** drop-down list, select the desired VPN, and then click **Search**. The **Hour** option displays statistics for the selected hour duration.
   - Click **Chart** to list the SSL applications.
   - Click **Details** to display more information about the SSL applications.
4. Click **X** to close the window and return to the **Monitor** > **Overview** page.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Top Applications** pane is part of the **Dashboard** > **Main Dashboard** page.
- A filter icon instead of a drop-down list lists the VPN options and indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Top Applications** pop-up window.

Note Flow DPI data is collected by Cisco SD-WAN Manager on schedule but processed on user requests. Flow DPI based reports are available after data is processed.

View Application-Aware Routing Pane



The **Application-Aware Routing** pane displays the 10 worst tunnels based on criteria you specify from the **Type** drop-down list, which includes loss, latency, and jitter. So, if you choose loss, this pane shows the 10 tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down for specifying a custom time period.

Click **View Details** to open the **Application-Aware Routing** sidebar. It displays the 25 worst tunnels based on criteria you specify from the **Type** drop-down list, which includes loss, latency, and jitter.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Application-Aware Routing** pane is part of the **Dashboard** > **Main Dashboard** page.
- An expand icon instead of the **View Details** button opens the **Application-Aware Routing** pop-up window.

View Web Server Certificate Expiration Date Notification

When you establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you configure the time period for which the certification is valid, in the **Administration** > **Settings** screen. At the end of this time period, the certificate expires. The Web Server Certificate shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco SD-WAN Manager **Monitor** > **Overview** page displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

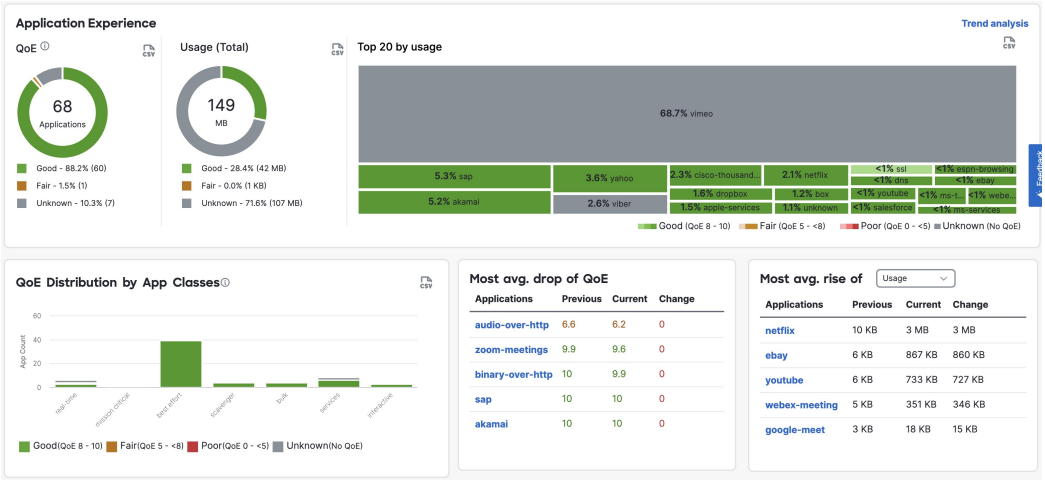
Note In Cisco vManage Release 20.6.1 and earlier releases, the **Dashboard** > **Main Dashboard** page displays the certificate expiry notification.

View Maintenance Windows Alert Notification

If an upcoming maintenance window is configured on the Cisco SD-WAN Manager server, in the **Administration** > **Settings**, the Cisco SD-WAN Manager **Monitor** > **Overview** page displays a maintenance window alert notification two days before the start of the window.

Note In Cisco vManage Release 20.6.1 and earlier releases, the **Dashboard** > **Main Dashboard** page displays the maintenance window alert notification.

View Application Health Dashlet



Minimum supported release: Cisco vManage Release 20.10.1

You can view a summary of the health of all applications on the **Application Health** dashlet on **Monitor Overview** dashboard.

You can view the usage of applications across all sites in a graphical format. The graph indicates whether the application performance is **Good**, **Fair**, or **Poor** based on the application Quality of Experience (QoE).

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays the application bandwidth usage information and changes in bandwidth from the last time period for each application. You can filter the applications based on the health status using the drop-down list for **Good Performing Applications**, **Fair Performing Applications**, and **Poor Performing Applications**.

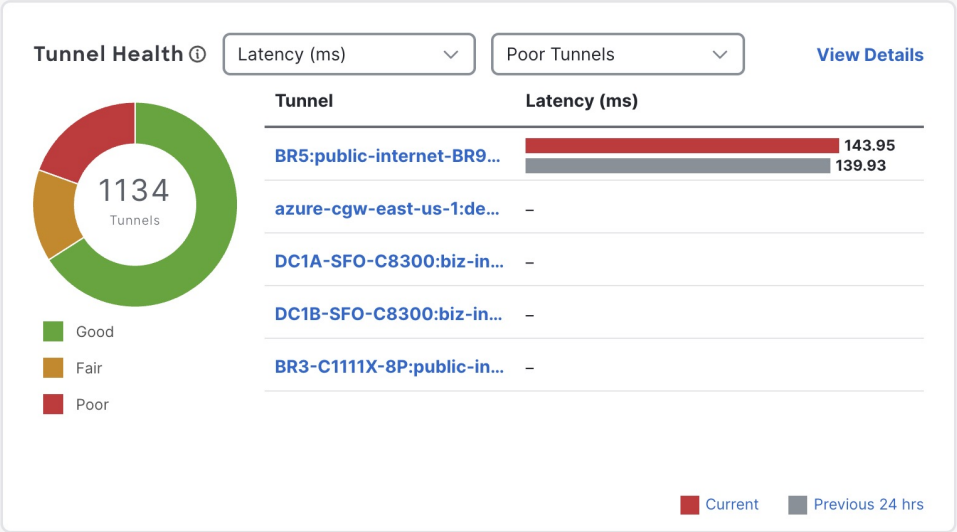
Click **View Details** to open the **Monitor > Applications** window.

View Tunnel Health Dashlet

Minimum supported release: Cisco vManage Release 20.10.1

You can view details about the tunnel health on **Monitor Overview** dashboard. This is the Tunnel Health dashlet:

Figure 3: Tunnel Health



The **Tunnel Health** dashlet lists the following information about all tunnel end points:

- Health
- Average latency, loss, and jitter data

You can view the tunnel health across all sites in a graphical format. You can also filter the tunnel information based on the health status using the drop-down list for **Good Tunnels**, **Fair Tunnels**, and **Poor Tunnels**, and **Latency**, **Loss**, and **Jitter**.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays current status of the tunnel and the change in status from the last time period.

Click **View Details** to open the **Monitor > Tunnels** window to view the tunnel health in table view.

View Top Alarms Dashlet

Minimum supported release: Cisco vManage Release 20.11.1

You can view all critical and major alarms for a site in the **Top Alarms** dashlet on the **Monitor Overview** dashboard.

All the critical and major alarms appear based on the alarm type such as CPU usage, SLA violations, and so on. Click **View Details** to open the **Monitor** > **Logs** > **Alarms** page to view more details about the alarms for a site.

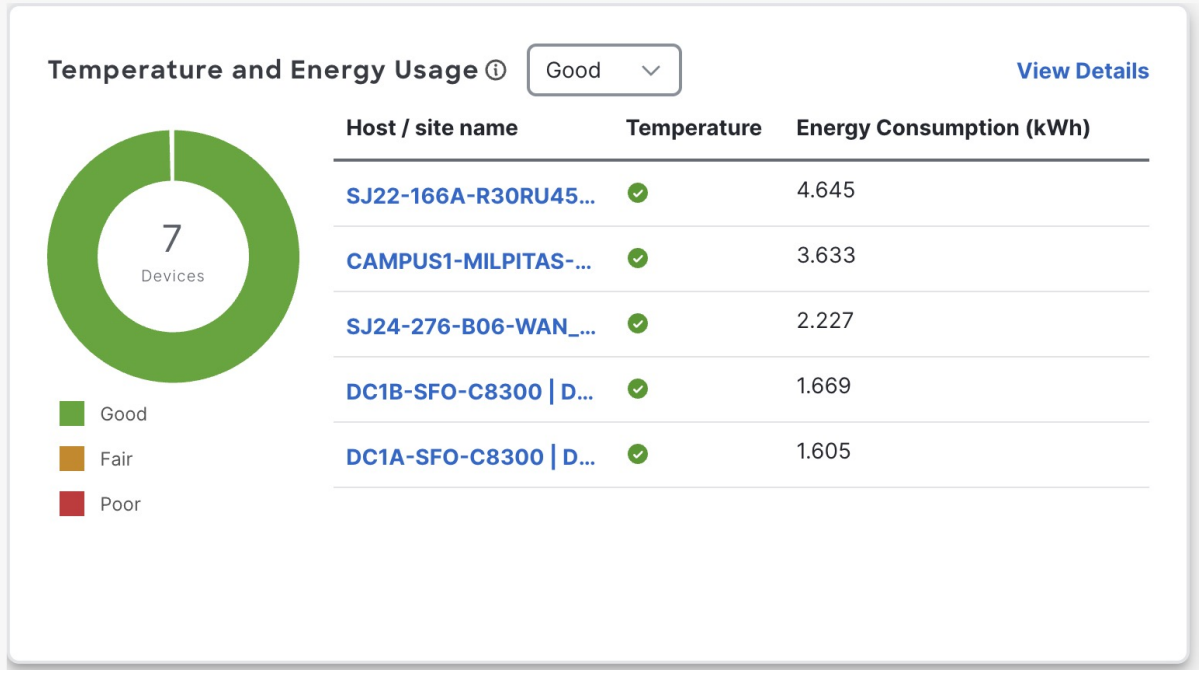
View temperature and energy usage dashlet

The Temperature and Energy Usage dashlet is a new dashlet that allows you to view:

- The status of the temperature sensor, and
- The status of the power consumption

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

You can view the status of the temperature sensor and power consumption of the Cisco IOS XE Catalyst SD-WAN devices in the **Temperature and Energy Usage** dashlet on **Monitor Overview** dashboard.

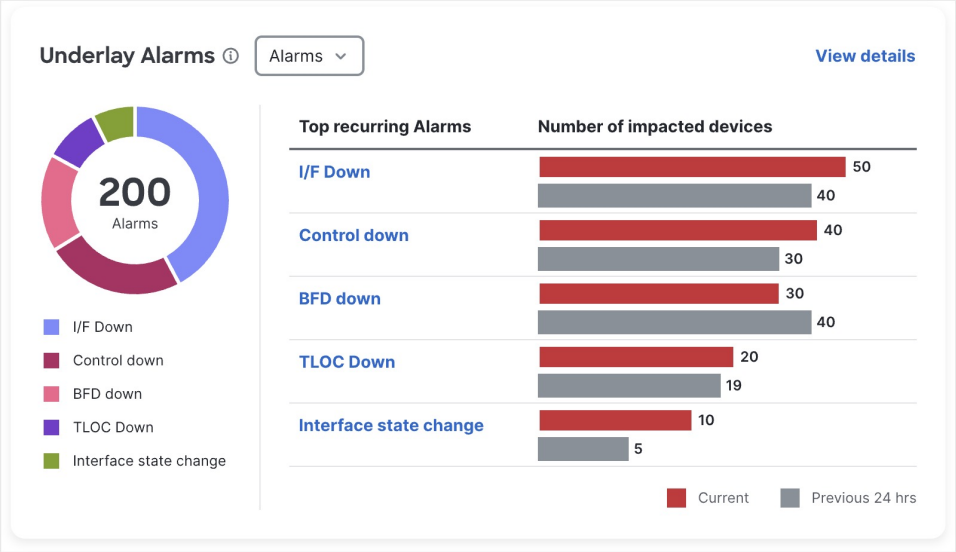


The health status is categorized as Good, Fair, or Poor based on predefined temperature thresholds:

- Good: The current temperature reading is below the minor threshold.
- Fair: The current temperature reading is at or above the minor threshold but below the critical threshold.
- Poor: The current temperature reading is at or above the critical threshold. You can filter the view based on the health status using the drop-down list.

  Click **View Details** to go to the **Monitor** > **Devices** page. Click the host name to navigate to the Device page and view the temperature and energy usage history chart in the **System Status** tab.

View underlay alarms dashlet



Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

The Underlay Alarms dashlet provides an overview of critical and major underlay alarms affecting your network. This dashlet displays only VPN-0 interface alarms. When you navigate to **View Details** from this dashlet, you may also see alarms for non-VPN-0 interfaces.

- **Critical Alarms** include: Interface State-Change, Interface Admin State Change, Control All Vsmarts Down, Control Site Down, Control Vsmart Down, Control Node Down, Control Vmanage Down, BFD Site Down, and BFD Node Down.
- **Major Alarms** include: Control TLOC Down and BFD TLOC DOWN.

  Click **View Details** to query these alarms and redirect to the Alarms page for a comprehensive view.

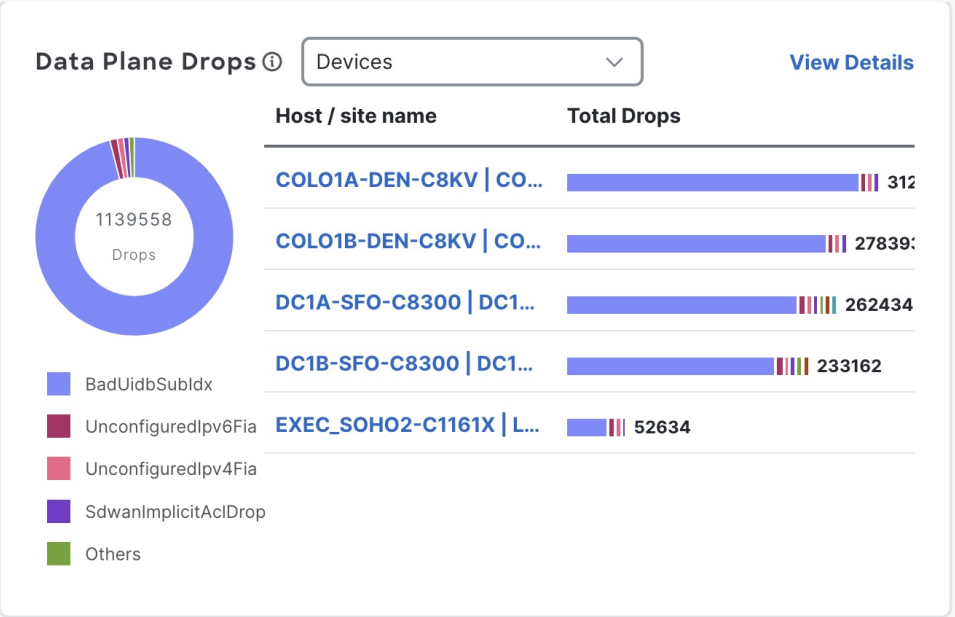
View data plane drops dashlet

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

You can view the various drops seen on the data plane on the Cisco IOS XE Catalyst SD-WAN devices.

This is the Data Plane Drops dashlet:

Figure 4: Data Plane Drops



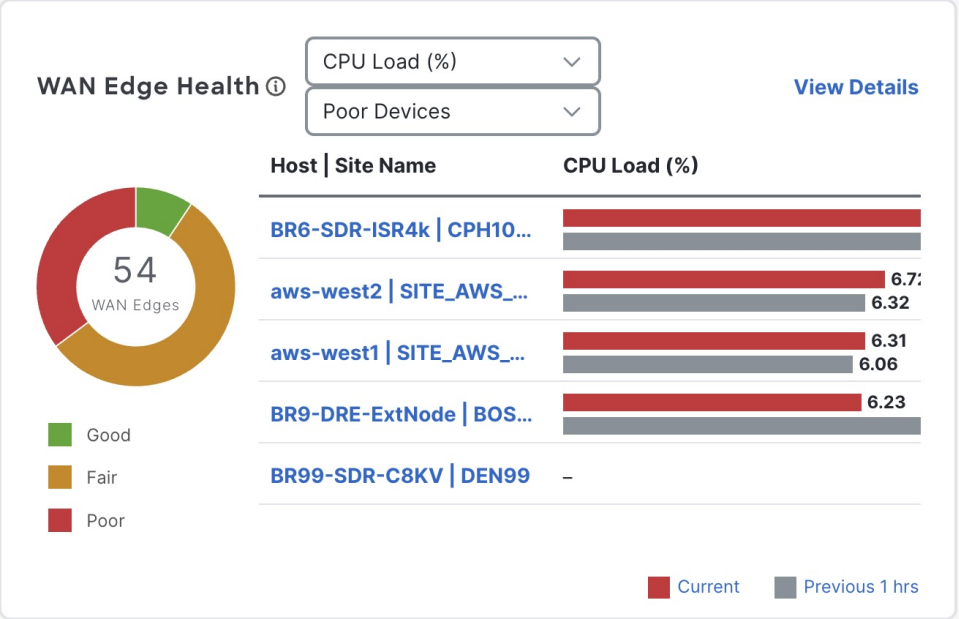
The dashlet displays historical data from device statistics. Only non-zero drop statistics are displayed. Click **View Details** to access more detailed data plane drop information.

View WAN Edge Health Dashlet

Minimum supported release: Cisco vManage Release 20.10.1

You can view the state for each WAN edge device and the number of WAN edge devices in that state in the **WAN Edge Health** dashlet on **Monitor Overview** dashboard:

Figure 5: WAN Edge Health



Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar chart displays the CPU utilization of WAN edge devices at a site, and the changes in CPU utilization from the last time period.

You can filter the **WAN Edge Health** dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load** and **Memory Load**.

Click **View Details** to open the **Monitor > Devices** window to view the device health in table view.

View WAN Edge Management Dashlet

Minimum supported release: Cisco vManage Release 20.11.1

You can view the state for each WAN edge device and the number of WAN edge devices in that state in the **WAN Edge Management** dashlet on **Monitor Overview** dashboard.

You can filter the **WAN Edge Management** dashlet view based on the configuration type using the drop-down list for **Locked Devices** and **Unlocked Devices**.

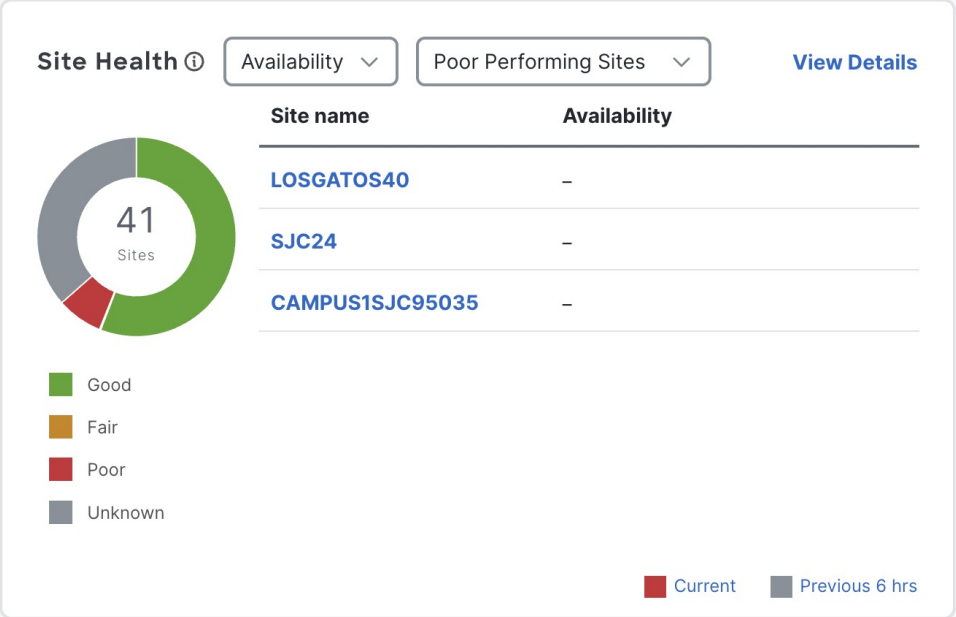
Click **View Details** to open the **Monitor > Devices** window to view the configured device details in table view.

View Site Health Dashlet

Minimum supported release: Cisco vManage Release 20.10.1

You can view the overall health across all sites in the **Site Health** dashlet on the **Monitor Overview** dashboard.

Figure 6: Site Health Dashlet



The **Site Health** dashlet displays the health, which is calculated by the average Quality of Experience (QoE) across all sites. The site health depends on the health metrics of devices, tunnels, and applications at that site.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays the bandwidth usage information for each site, and changes in bandwidth from the last time period. You can filter the view based on health status using the drop-down list for **Good Performing Sites**, **Fair Performing Sites**, and **Poor Performing Sites**.

Click **View Details** to open the site table view window.

View Site Health in Table View

Minimum supported release: Cisco vManage Release 20.10.1

In the sites table view you can view the site health, tunnel health, device health, application health, and application usage.

The sites table view displays all the sites by default and the overall health scores for sites, devices, tunnels, and applications. The table also displays the application usage data for the last one hour.

Site Health Metrics

The average health metric of sites is calculated as follows:

Health	Condition
Good	All applications, WAN edge devices, and tunnels are in good state.
Fair	Any one application, WAN edge device, or tunnel in fair state.

Health	Condition
Poor	Any one application, WAN edge device, or tunnel in poor state.

View Site Health in Heatmap View

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, the grid of colored squares displays the site health as **Good**, **Fair**, or **Poor**. You can hover over a square or click to display additional details of a site at a specific time. The data shown here in the aggregated dats for the last three hours. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

View Sites in Global Network View

Minimum supported release: Cisco vManage Release 20.11.1

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

You can view sites in the global topology view by clicking the drop pin icon on the **Monitor Overview** dashboard.

You must configure the latitude and longitude on the routers to view the sites in the corresponding geographical location on the map.

You can view all the WAN edge devices and sites for geographical regions worldwide. When you click an individual site, you can view the site details such as **Hostname**, **Site ID**, **Device Model**, **System IP**, **Health**, **Reachability**, and so on, in the side pane. When you click on the troubleshooting options available in the side pane, Cisco Catalyst SD-WAN Manager displays the relevant troubleshooting pages. Aggregated sites show the number of sites. The color of the aggregated site shows the site health.

To view the site topology of a specific site, click **Site Topology**. To view a specific site dashboard, click **Site Dashboard**. When you click **View Tunnels** available in the side pane, you can see the tunnels associated to a specific site. Click the tunnel line to view detailed tunnel information. Click the back button to go back from the tunnel view to the Global Network view.

You can filter the global topology view based on the health status of the sites using the **Good**, **Fair**, and **Poor** filter options.

Note For a new deployment, Cisco Catalyst SD-WAN Manager may take up to 30 minutes to populate the Global Network View based on when Cisco Catalyst SD-WAN Manager collects and processes the site health information from all the WAN edge devices in the overlay.

In the **Global Network View** page, the alarms heatmap does not appear for the last 30 minutes, which is the default selection. To view the alarms heatmap, select any of the other time range values from the drop-down list.

Time Interval, Search, and Network Hierarchy

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1

Select the time from the drop-down list to select 30 minutes, 1, 3, 6, 12, or 24 hours. If you select any option other than 30 minutes, you can view the heatmap view of the site health.

You can use the search option to filter the sites based on the configuration groups, policy groups, tags and so on, using the **Contains** and **Match** options.

You can filter the global topology view based on the health status of the sites and tunnels using the **Good**, **Fair**, and **Poor** filter options.

When you click the summary icon, the topology view of the site and tunnel health across geographical locations is displayed. You can view the site and tunnel health details by clicking the non-zero number in the topology view. If you click the eye icon, you can view the tunnel connection with aggregated tunnel health between the sites.

Click the arrow on the left to open the network hierarchy menu. Click an individual site from this menu, to view the following site details in the side pane:

- You can view the following details for control components or WAN edge device details for the selected site:
  - **Device Health**
  - **Reachability**
  - **BFD**
  - **Controller Control**
  - **CPU Load**
  - **Memory Utilization**
  - **Device Model**
  - **System IP**
  - **Configuration Group**
  - **Policy Group**

  If a device from the site is attached to a configuration group or policy group, click the configuration group or policy group to view or modify the configurations.

- Network Wide Path Insight:

  The Network-Wide Path Insight feature is integrated with the global network view and it is supported only on WAN edge devices. With the Network-Wide Path Insight feature, Cisco Catalyst SD-WAN Manager lets you initiate application tracing and displays the trace results collected from multiple devices in a consolidated view. Click **Create a trace** to start a new trace. For more information, see Start a New Trace.

  To view more information about the trace, click **Insight Summary**. The **Insight Summary** window displays information about the trace from this site from the last 24 hours, including the number of traces, trace start time, and trace stop time. The traffic flow for applications and events is displayed in a pie chart. The application distribution, the event distribution, and event impacts to application are also

displayed on this window. There are four events that are displayed in this page: Local Drop, WAN Loss, SLA Violation and Qos Congestion.

To start another trace, click **Start a New Trace** from the **Insight Summary** page. To view Network-Wide Path Insight details, click **NWPI Details**.

- Troubleshooting:

  When you click the troubleshooting options available in the side pane, Cisco Catalyst SD-WAN Manager displays the relevant troubleshooting pages.

- Detailed Information:
  - To view the site topology of a specific site, click **Site Topology**.
  - To view a specific site dashboard, click **Site Dashboard**.
  - To view the tunnels associated to a specific site, click **View Tunnels**. Click a tunnel line to view detailed tunnel information.

Global Region View

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

If Multi-Region Fabric is enabled, click **Region** to display a topology diagram showing the access regions and the core region. The diagram indicates the number of border sites and edge sites in each access region. For access regions that have a border router providing connectivity to the core region, the diagram shows a link between the access region and the core region.

Click a region in the diagram to show which other regions it has connectivity to through the core region—links to those regions are highlighted.

Click a link between an access region and the core region to display BFD session information related to connections between the two regions, similar to the information provided by the **show sdwan bfd sessions** command.

Security

The following dashlets and options are available on the **Monitor** > **Security** page in Cisco SD-WAN Manager:

Note In Cisco vManage Release 20.6.x and earlier releases, these options and dashlets are part of the **Dashboard** > **Security** page.

Table 2: Dashlets

Dashlet Name	Version
Actions	Cisco vManage Release 20.11.1 and later releases
Top Threats	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases

Dashlet Name	Version
Firewall Rule Counter	Cisco vManage Release 20.6.1 and earlier releases **Note** Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases, **Firewall Enforcement** is renamed to **Firewall Rule Counter**.
URL Filtering	Cisco vManage Release 20.6.1 and earlier releases
Advanced Malware Protection	Cisco vManage Release 20.6.1 and earlier releases
Intrusion Prevention	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
SIG/SEE Tunnels	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
Security Events	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
Security Appliance/UTD Container	Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases
Application Offload	Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases

Actions

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1.

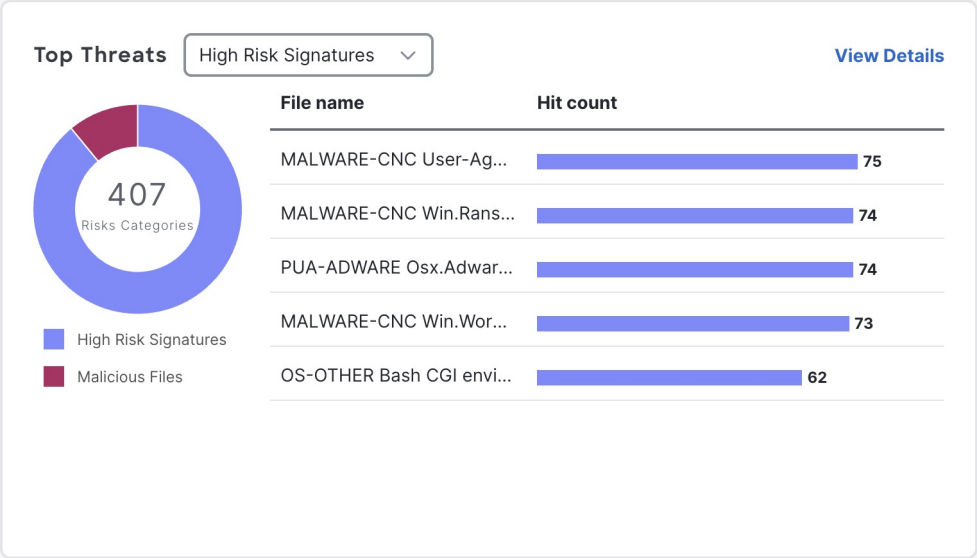
The **Actions** drop-down list in the security dashboard has the following options:

Table 3: Actions

Option	Description
Edit Security Dashboard	Choose this option to edit the security dashboard. You can perform the following actions: • Rearrange: Drag and move the dashlets within the security dashboard. • Delete: Click **Delete** to delete a dashlet.
Show SecureX Ribbon	Click **Show SecureX Ribbon** to view the **SecureX** ribbon in the security dashboard. You can use the **SecureX** ribbon to access the **SecureX** portal from the security dashboard. For more information, see View SecureX Ribbon.

Option	Description
Reset to Default View	This option is displayed if you have edited the security dashboard page. Click this option to revert to the default view of the security dashboard.

View Top Threats



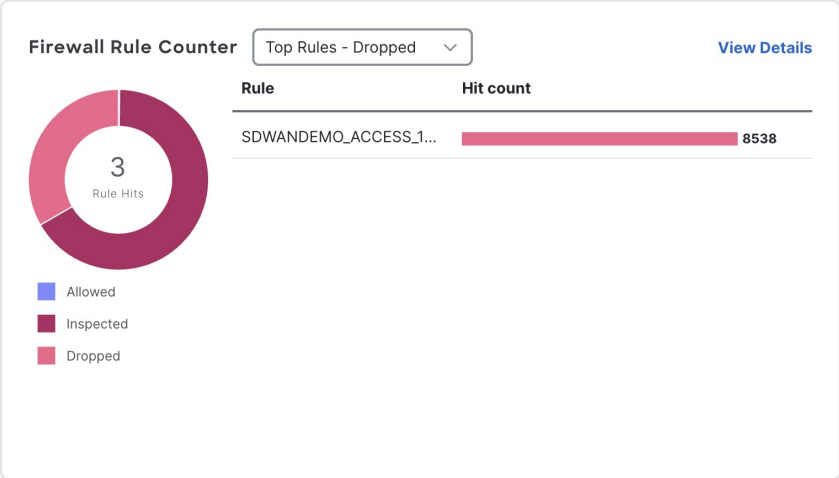
Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Top Threats** dashlet provides a high level view of top five threats found in the network-based on Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) data. You can view the threat information for malicious files or high risk signatures by choosing from the options in the **Top Threats** drop-down list.

To view more information about the threats such as file name, type of event, device name, and more, click **View Details**. Click a device number in the **Devices Impacted** column to view the threat details at a device level.

Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

View Firewall Rule Counter



Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Firewall Rule Counter** dashlet counts the hits on each rule and displays the counters for each rule. Choose the options in the **Top Rules** drop-down list to view the top five rules according to traffic that was allowed, inspected, or dropped.

Click **View Details** to view additional details for a rule. Click a device number in the **Device Hits** column to view the rules at a device level.

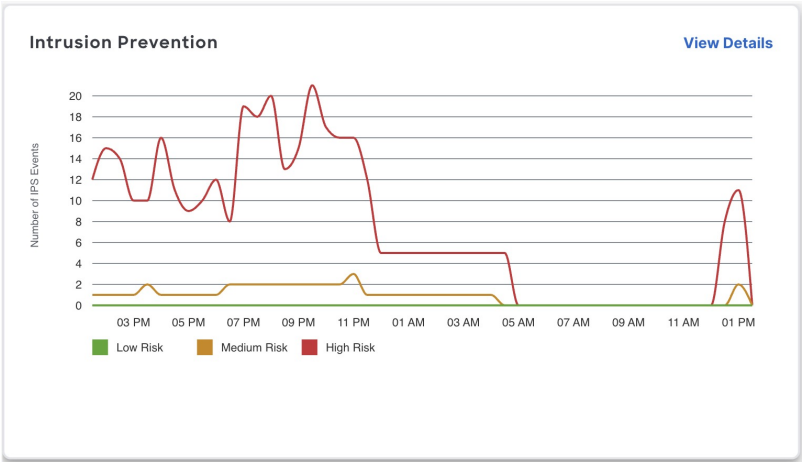
Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for data traffic inspection. Zone-based firewalls allow inspection of TCP, UDP, and ICMP data traffic. A zone can contain a group of one or more VPNs. Grouping VPNs into zones allows users to establish security boundaries in the overlay network so that users can control all data traffic that passes between zones.

A firewall policy defines the conditions that the data traffic flow from the source zone must match to allow the flow to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged.

Note In Cisco vManage Release 20.6.x and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **FireWall Enforcement** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **FireWall Enforcement** pop-up window.

View Intrusion Prevention



Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Intrusion Prevention** dashlet displays threats that are categorized as low risk, medium risk, and high risk threats.

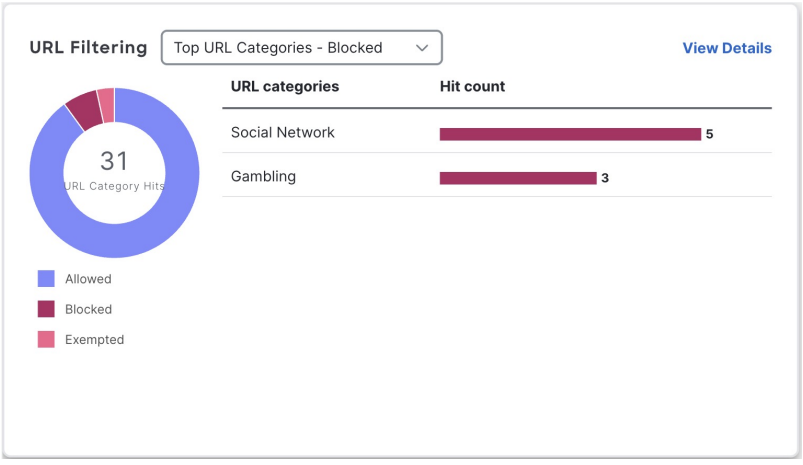
Click **View Details** to view to more details about a threat.

Click an entry in the **Signature ID** column to be directed to the Talos website, which will display the Snort rules that are used to report vulnerabilities.

Click a device number in the **Device Impacted** column to view more details about the threats at a device level.

Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

View URL Filtering



The **URL Filtering** dashlet displays the categories of URLs that are allowed, blocked, or exempted from blocking.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new URL filtering category, **Exempted**, has been added to the **URL Filtering** dashlet.

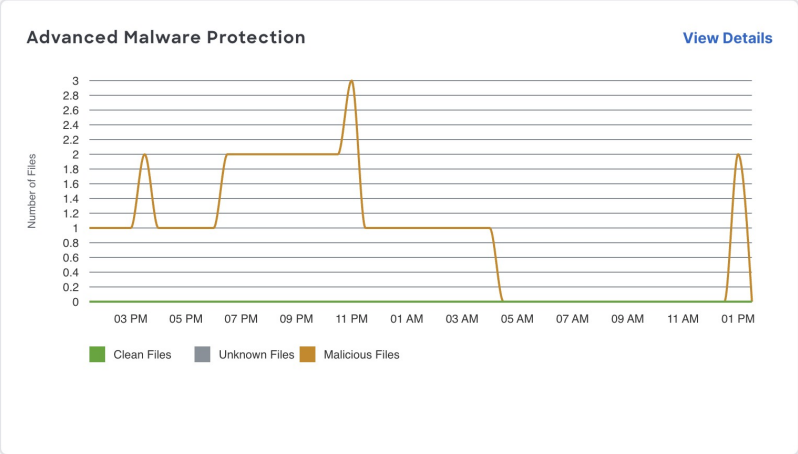
Choose an option in the **Top URL Categories** drop-down list to filter the URL categories and view information about a particular URL category.

Click **View Details** to view more information about the URL categories. Click a device number in the **Device Accessed** column to view additional details for a URL category at a device level.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **URL Filtering** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **URL Filtering** pop-up window.

View Advanced Malware Protection



The **Advanced Malware Protection** dashlet displays the number of malicious files, unknown files, and clean files that AMP has identified over a specific time period.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new category **Clean Files** hase been added to the **Advanced Malware Protection** dashlet.

Click **View Details** to view an analysis of the files. Click a device number in the **Device Impacted** column to view additional details about the files at a device level.

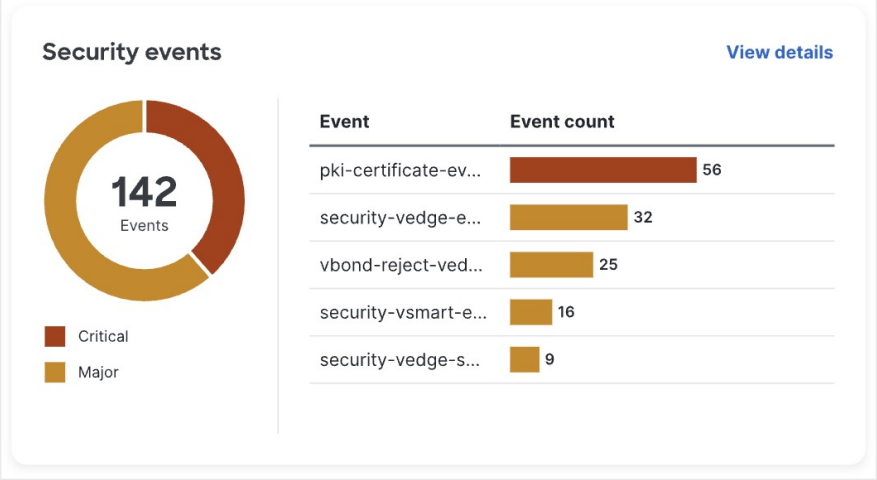
Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

Cisco Advanced Malware Protection (AMP) blocks malware based on file reputation and uploads unknown files to Cisco AMP Threat Grid for further analysis. This pane shows the number of file reputation and file analysis events over the specified time period.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **Advanced Malware Protection** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Advanced Malware Protection** pop-up window.

View Security Events

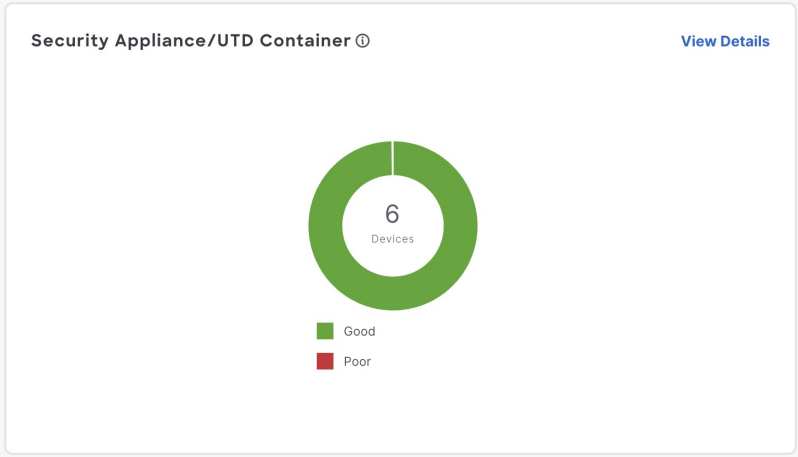


Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Security Events** dashlet displays a count of all security events that have occurred within the Cisco Catalyst SD-WAN overlay, and classifies them either major or crucial.

Click **View Details** to view additional details about the security events.

View Security Appliance-UTD Container



Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1.

The **Security Appliance/UTD Container** dashlet displays the health status of the Next-Generation Firewall (NGFW) and the security processes running on the Cisco IOS XE Catalyst SD-WAN devices.

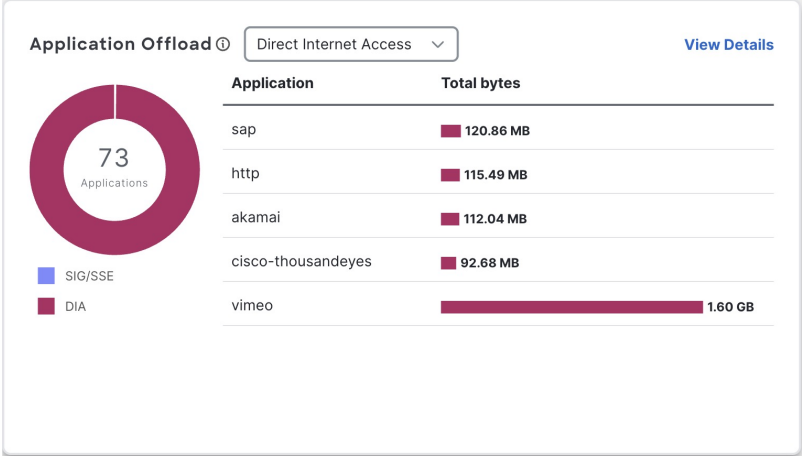
The dashlet provides an overview of various security components and monitors the following:

- Device security health
- Operational state of the UTD container
- IPS signature update status
- Cloud connectivity for:
  - URL filtering
  - Advanced Malware Protection

If everything is functioning properly, the health status is displayed in green. When issues arise with two or more components, the status is displayed in red.

To view more information about the health status of **Security Appliance/UTD Container**, click **View Details**.

View Application Offload



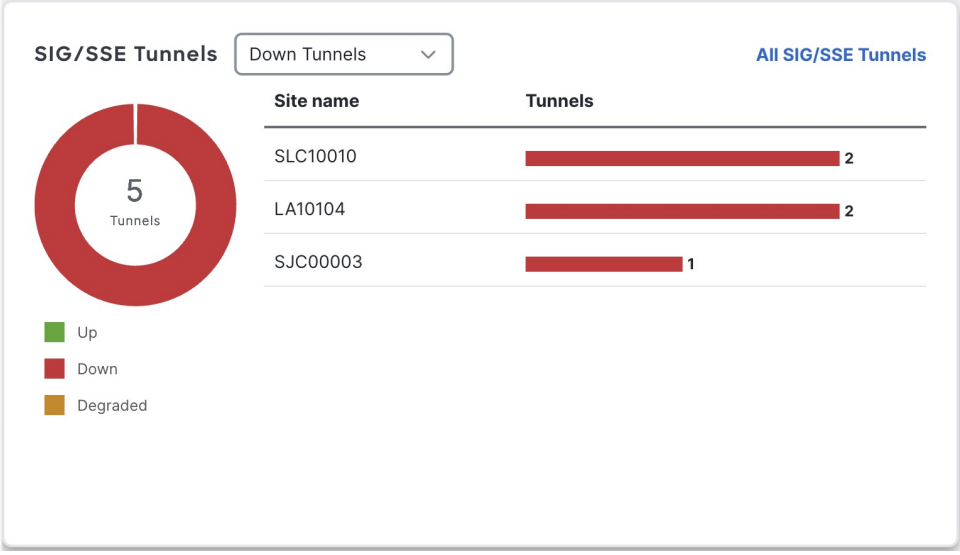
Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1.

The **Application Offload** dashlet provides a high-level overview of the application traffic. You can view the application traffic information by choosing SIG/SSE tunnels or DIA options from the drop-down list.

The **Application Offload** dashlet represents the application traffic information using a doughnut chart and a bar chart. While the doughnut chart displays a breakup of the applications by SIG or Secure Service Edge (SSE) tunnels or DIA, the bar chart displays the top five applications in descending order of usage based on the option chosen from the drop-down list. Hover the mouse pointer over the chart elements to view the names and values that are associated with each application.

To view more information about the applications, click **View Details**.

View Secure Internet Gateway Tunnels



Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Secure Internet Gateway Tunnels** dashlet provides information about the number of Secure Internet Gateway (SIG) tunnels, their status, whether they are up, down, or degraded, as well as the site names of the tunnels that are being reported.

Click **All SIG Tunnels** to view additional details of the configured SIG tunnels.

View SecureX Ribbon



Note Starting with Cisco Catalyst SD-WAN Manager Release 20.12.6, the SecureX ribbon is no longer available in the Cisco SD-WAN Manager.

You use the **SecureX** ribbon to access the **SecureX** portal from the security dashboard.

The SecureX ribbon provides access to the applications you have configured in the SecureX portal. To access the SecureX portal, log in with your registered user credentials.

When you click **Show SecureX Ribbon** for the first time, the **SecureX Setup** dialog box is displayed. Perform the following steps to view the **SecureX** ribbon in the security dashboard:

1. From the **Current Region** drop-down list, choose a region for access to the SecureX portal.
2. Click **Enable SecureX** to enable your access to the SecureX portal. A validation code appears.
3. Click the **here** hyperlink to proceed with the authentication steps for SecureX.

On successful authentication with SecureX, the **SecureX** ribbon is displayed in Cisco SD-WAN Manager.

Troubleshooting

Cannot See Data

Problem

Cannot see the data in the Security dashboard.

Possible Causes

It takes up to one hour for the Security dashboard to display traffic data.

Solution

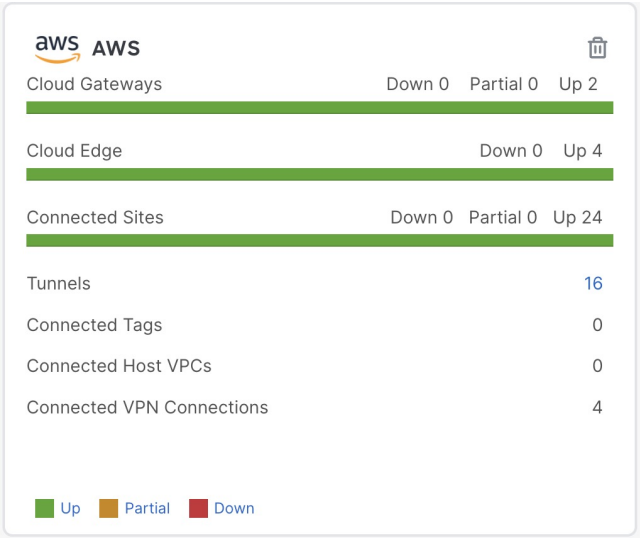
Choose a different time (1, 3, 6, or 24 hours) from the drop-down list.

Multicloud

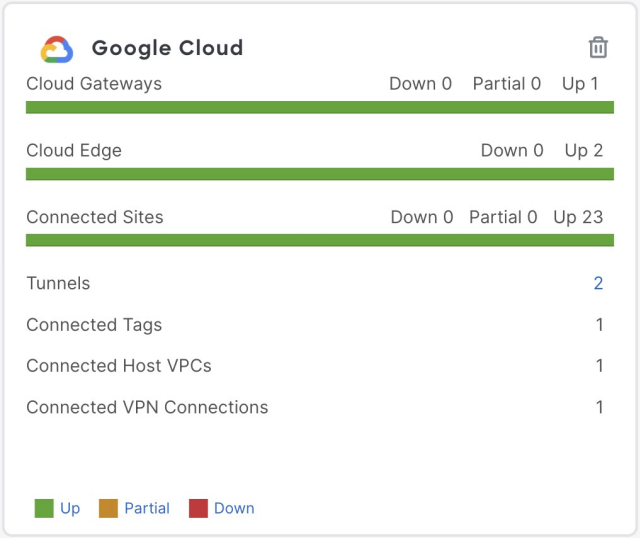
The following panes are available on the **Monitor** > **Multicloud** page in Cisco SD-WAN Manager:

Note In Cisco vManage Release 20.6.1 and earlier releases, these panes are part of the **Dashboard** > **Multicloud** page.

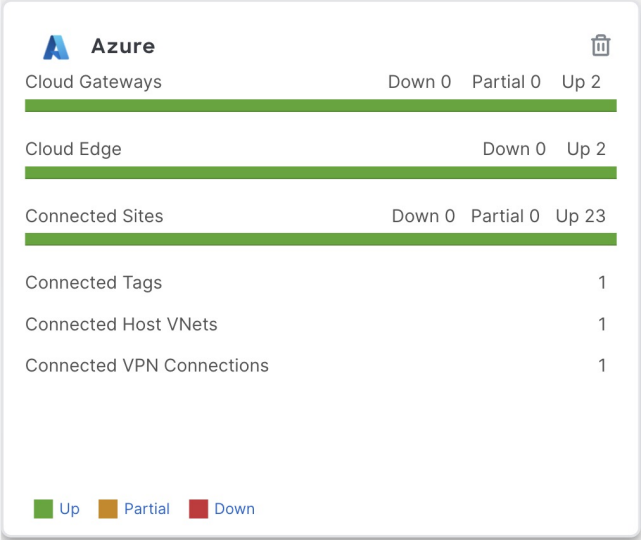
- **Amazon Web Service**



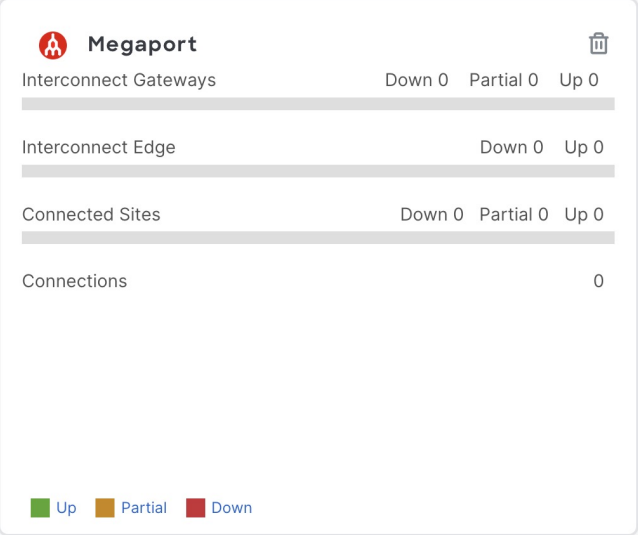
- **Google Cloud Platform**



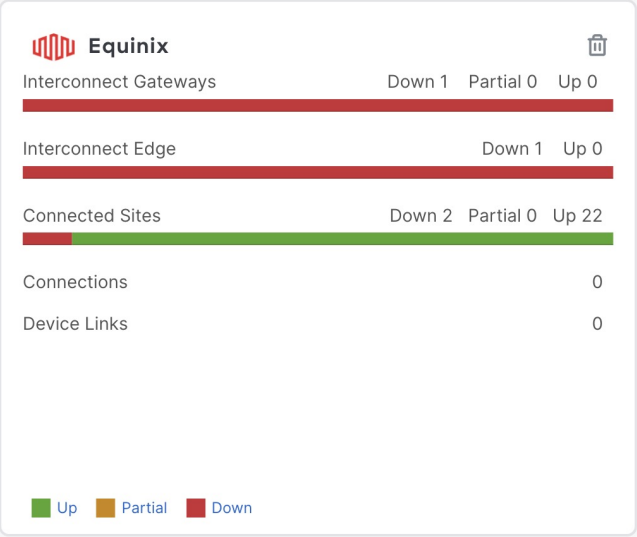
- **Microsoft Azure**



- **Megaport**



- **Equinix**



For more information about these panes, see Cisco SD-WAN Cloud OnRamp Configuration Guide.

Explore

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

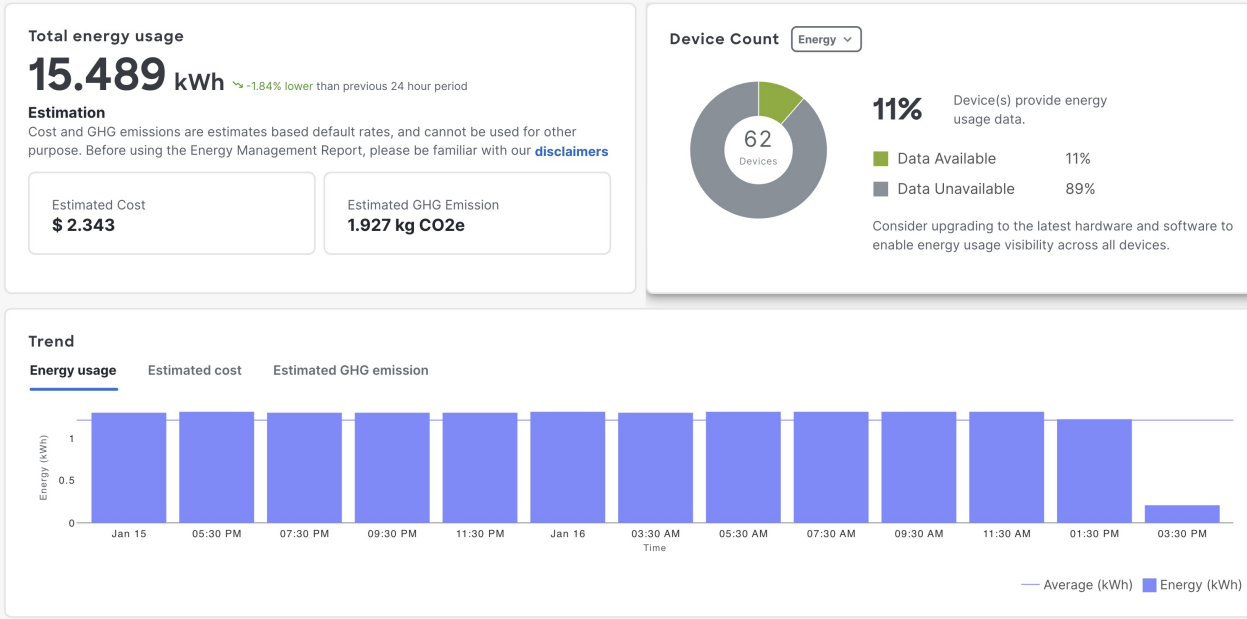
The **Explore** menu option opens a page presenting four job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. Based on the job role that you choose, the Explore page displays relevant Cisco Catalyst SD-WAN features, along with other Cisco resources such as developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more.

To view the Explore menu, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Explore**.
2. Click any of the following job roles to view and access various resources specific to your choice.
   - **NetOps**
   - **SecOps**
   - **AIOps**
   - **DevOps**

The resources appearing in each job role present relevant functionality pertaining to that job role.

Energy management



The **Monitor** > **Energy Management** page is available in Cisco SD-WAN Manager starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a. The table lists the available panes and their descriptions for energy management.

Table 4:

Pane	Description
Total energy usage	Displays total energy (in kWh) used by all devices in the last specified hours.
Device Capability	Displays the number of devices supporting power tracking, with Energy or Cost and Emission filters.
Energy usage trend	Displays power usage trend for the last specified hours, aggregated at intervals.
Consumption by sites	Displays site-based power consumption with a pie chart and detailed table.
Comparison	Displays energy usage comparison between two time periods.

Note Enable Cloud Services to see **Total energy usage**, **Device Capability**, **Energy usage trend**, **Consumption by sites**, and **Comparison** data.

Supported Platforms for Energy Management

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a these platforms are supported:

- Cisco Catalyst 8100 Series Edge
- Cisco Catalyst 8200 Series Edge
- Cisco Catalyst 8300 Series Edge
- Cisco Catalyst 8500 Series Edge

Advisories

The Cisco Catalyst SD-WAN Advisories feature is a solution that:

- Displays known security vulnerabilities, including potential known vulnerabilities on a Cisco secure WAN device, managed by the Cisco SD-WAN Manager.
- Displays field notices for non-security issues.
- Displays high and critical advisories, and field notices.

Flexible reporting

You can download security advisory data in CSV formats from Cisco SD-WAN Manager to analyze and manage network vulnerabilities. You can download this data for individual devices or the entire network.

Benefits of Advisories

- **Centralized visibility:**

  Provides a centralized dashboard to view security advisories across the entire Cisco SD-WAN network.

- **Actionable insights:**

  Provides recommended corrective actions to mitigate identified security risks.

Prerequisites for Advisories

- Enable cloud services from the **Admin** > **Settings** page using Cisco Smart Accountor Virtual Account credentials.
- For on-prem Cisco SD-WAN Managers, ensure the firewall is configured to allow access to the following URLs:
  - **SSP**: ssp.sdwan.cisco.com
  - **Okta**: id.cisco.com
  - **CX**: api-cx.cisco.com

View Security Advisory

To view and manage security advisories in Cisco SD-WAN Manager, follow these steps:

The following settings are enabled by default:

- Advisory collection: Enabled when you activate Cloud Services.
- Interval scan: Enabled
- Scan frequency: Set to once a week
- Advanced scan: Enabled and operates based on the device configuration.

Procedure

Step 1 From the Cisco SD-WAN Manager, choose **Monitor** > **Advisories**.

Step 2 Select **Security Advisory**.

Step 3 Select **Devices** or **Advisories** to view relevant security information.

- **Devices:** Lists all devices in your network and clearly indicates which devices have associated security risks.
- **Advisories:** Lists all active security advisories relevant to the network. Advisories can be either **Active**, requiring attention, or **Acknowledge**, indicating that action is being taken**.**

  To move an advisory to the acknowledged state, select the advisory and click **Acknowledge**.

Perform a scan in Advisories

Follow these steps to perform a scan to identify vulnerabilities, ensure compliance, and view actionable risk mitigation insights..

Procedure

Step 1 From Cisco SD-WAN Manager, select **Monitor** > **Advisories**

Step 2 Select **Security Advisory** > **More actions**.

Step 3 Choose **Scan now** from the drop down list to immediately check your network for vulnerabilities.

- **Affected**: Identifies devices known to be vulnerable based on Cisco SD-WAN Manager's analysis.
- **Potentially Affected**:Indicates a possible vulnerability and requires a detailed device analysis to confirm any vulnerabilities.

Note

After you add a new control component, run an on-demand advisory scan or wait for the next scheduled scan to update the Advisories inventory before performing Shield management operations.

View Field Notices

View Field Notices to stay informed about significant product-related issues, that may require upgrades, workarounds, or other actions.

Procedure

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

Step 2 Select **Field Notices**.

Converged Dashboard for SD-WAN Analytics and SD-WAN Manager

Information About Converged Dashboard

Access the Converged Dashboard in Cisco SD-WAN Manager

From Cisco Catalyst SD-WAN Manager Release 20.15.1, a converged dashboard is available that integrates data from both Cisco SD-WAN Analytics and Cisco SD-WAN Manager within a single interface. To access this converged dashboard, Cisco SD-WAN Analytics must be onboarded into Cisco SD-WAN Manager.

The converged dashboard renders Analytics pages within Cisco SD-WAN Manager as follows:

- Under the **Overview** menu: the pages for **Applications**, **Sites**, and **Circuits** are rendered.
- Under the **Analytics** menu: all menus are rendered except for **Internet Outages**.
- Under the **Logs** menu: the **Traffic Logs** page is rendered.

For more information about onboarding Cisco SD-WAN Analytics into Cisco SD-WAN Manager, see Onboard Cisco SD-WAN Analytics.

If Cisco SD-WAN Analytics is onboarded to Cisco SD-WAN Manager, the **Cloud Services** option in the **Administration** > **Settings** is enabled automatically. This means that a converged dashboard is available in Cisco SD-WAN Manager.

To disable Cisco SD-WAN Analytics, change its status to Disabled (or toggle the switch off).

View Cisco SD-WAN Analytics Data in Cisco SD-WAN Manager

When Cisco SD-WAN Analytics is enabled, the dashboard in Cisco SD-WAN Manager displays data from Cisco SD-WAN Analytics, including details on Applications, Circuits, Sites, and Clients through specific dashlets. You can click these dashlets for more detailed information instead of being redirected to Cisco SD-WAN Analytics.

View Reports in Converged Dashboard

All Applications Reports, which is a Cisco SD-WAN Analytics report, displays a view of how different applications are performing across an overlay for all sites. The **Executive Summary** report in the converged dashboard displays the same Executive Summary report as seen in the standalone Cisco SD-WAN Analytics when it is not part of the convergence. For more reports in Cisco SD-WAN Manager, see Information About Reports, on page 209.

Applications Dashboard

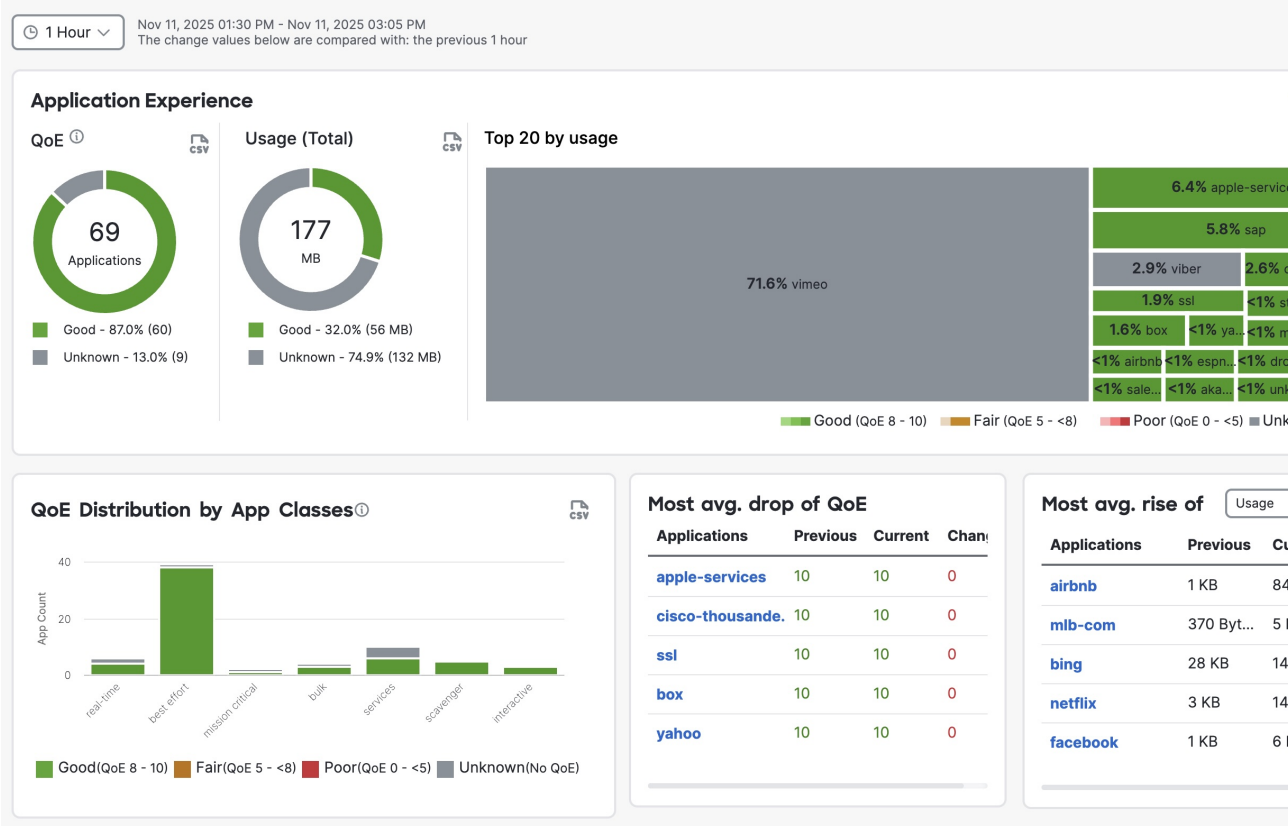
The **Applications** dashboard displays information on how different applications are performing across an overlay for all sites, and for a single site. The **Applications** dashboard gives an overview of Application performance for all applications across an overlay and across all sites, and compares it to other metrics such as overall bandwidth and bandwidth increase.

The **Applications** dashboard presents the performance metrics in these widgets:

- Application Experience
- Application Trend Analysis
- QoE Distribution by Application Classes, and
- Trending Applications

This is the Applications dashboard:

Figure 7: Application Experience



For more information about the **Applications** dashboard, see Application Dashboard in Cisco SD-WAN Analytics.

Note The **Applications** dashboard displays Cisco SD-WAN Analytics data only when viewed on a converged dashboard.

Sites Dashboard

The **Sites** dashboard provides visibility into site availability and usage across the entire network for the selected time period. The **Sites** page helps you to view the performance of applications on the overlay from a site perspective. It provides the ability to view overlay performance in terms of sites and provides insights into site performance in terms of availability, utilization and latency, and compares these parameters with the corresponding metrics from the previous time period.

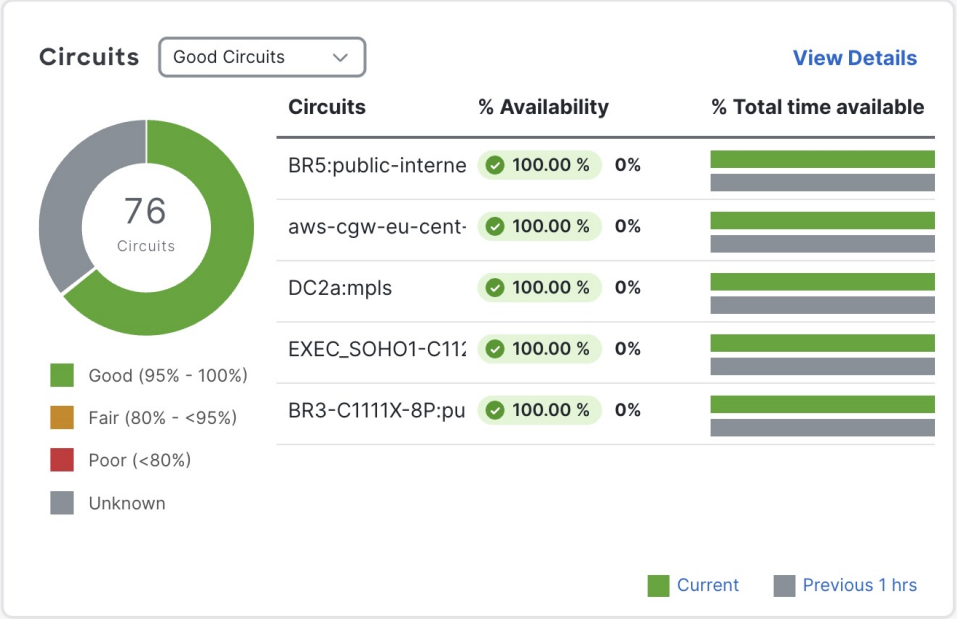
For more information about Sites analytics, see Site Dashboard in Cisco SD-WAN Analytics.

Circuits Dashboard

The **Circuits** dashboard provides valuable insights into circuit availability, utilization, and network performance. It offers a comprehensive overview of circuit performance across the entire fabric as well as for individual sites.

This is the Circuits dashlet:

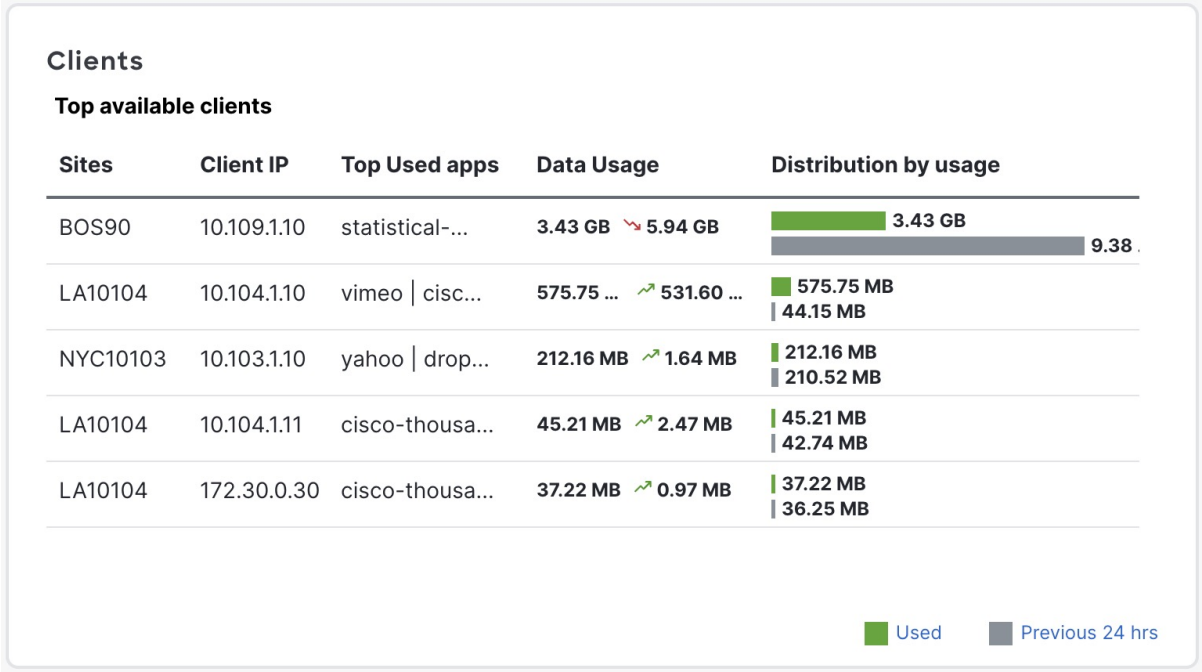
Figure 8: Circuits



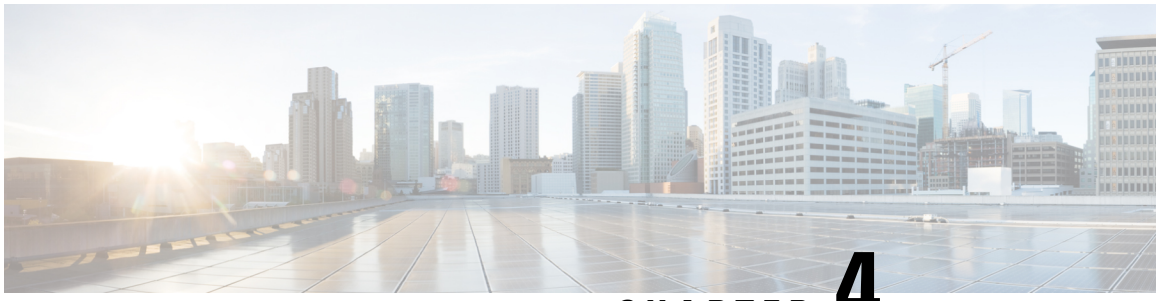
For more information about Circuits analytics, see Circuits Dashboard in Cisco SD-WAN Analytics.

Client Dashlet

The **Clients** dashlet displays the top clients of data in the overlay, the current usage of data and the changes in the usage of data from the last time period. The top clients are tracked by using respective client IP addresses in the overlay network. The dashlet also displays the top five applications that are used by the clients, and the data is ranked by bandwidth.



Note The **Clients** dashlet is not available by default. To view the **Clients** dashlet, you must add the dashlet. For more information about adding dashlets, see Add a Dashlet, on page 10.



CHAPTER 4

Secure Cisco Catalyst SD-WAN with Live Protect

- Feature history for Live Protect, on page 57
- Live Protect for Cisco Catalyst SD-WAN, on page 57
- Benefits of Live Protect, on page 58
- Live Protect Vulnerability Shield lifecycle , on page 58
- Configure Live Protect using Cisco SD-WAN Manager, on page 60
- Disable Live Protect using Cisco SD-WAN Manager, on page 61
- Monitor Live Protect, on page 61

Feature history for Live Protect

This table describes the developments of this feature, by release.

Feature name	Release information	Description
Live Protect for Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN Control Components Release 20.18.3	Live Protect validates Vulnerability Shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy Vulnerability Shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Protecting (Enforce) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire shields, enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risk until software upgrades or patches are deployed.

Live Protect for Cisco Catalyst SD-WAN

Live Protect is a security capability that

- enables compensating controls and vulnerability mitigation without software upgrades or reboots,
- allows you to manage Vulnerability Shields through Cisco SD-WAN Manager to protect against known vulnerabilities before patching.

Deployment modes

You can deploy Vulnerability Shields in two modes:

- Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action.
- Protecting (Enforce) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities.

Benefits of Live Protect

- Zero-downtime remediation: Provides temporary mitigation against vulnerabilities without requiring software upgrades or device reboots, designed to ensure continuous network availability until remediation.
- Dynamic security: Allows real-time enforcement of security policies.
- Flexible deployment: Allows you to deploy Vulnerability Shields in Monitoring mode to provide visibility into potential exploit attempts without enforcement, or in Enforce mode to actively apply mitigation policies and reduce exposure to known vulnerabilities.
- Centralized management: Allows you to manage Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components through Cisco SD-WAN Manager.
- Visibility: Provides hit statistics to help monitor Vulnerability Shield activity.

Live Protect Vulnerability Shield lifecycle

Live Protect Vulnerability Shields are designed to provide interim mitigation for vulnerabilities on Cisco Catalyst SD-WAN Control Components releases. You may temporarily use a Vulnerability Shield until you upgrade to a software release that contains the fix or install another applicable, supported Vulnerability Shield.

Lifecycle policy scope

This lifecycle policy defines how Cisco publishes, supports, and retires Live Protect Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components.

This lifecycle applies to:

- Cisco Catalyst SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller
- The Live Protect Agent (Tetragon) integrated into the control-component software image

- Cloud-hosted and cloud-tethered Cisco Catalyst SD-WAN deployments

The lifecycle policy does not apply to:

- Cisco Catalyst SD-WAN WAN-edge or data-plane routers
- Air-gapped Cisco Catalyst SD-WAN deployments

Vulnerability Shield availability

Cisco associates each Vulnerability Shield with a Cisco security advisory. A Vulnerability Shield can address one or more Common Vulnerabilities and Exposures (CVEs) identified in the advisory. Cisco SD-WAN Manager displays High and Critical security advisories and identifies the applicable Vulnerability Shields for affected Cisco Catalyst SD-WAN Control Components.

Availability and support policy

Policy item	Rule
Version support	Cisco creates Vulnerability Shields for the SD-WAN release that is current when the shield is published and for the two immediately preceding releases in each supported release train that includes Live Protect. In most cases, the current release already contains the fix for the vulnerability, so shields are created only for the two preceding releases. However, if an actively exploited vulnerability is disclosed before fixed software is available, Cisco may also create a shield for the current release.
Availability period	Cisco announces the download and support period when it publishes a Vulnerability Shield. The six-month period begins when Cisco releases a software fix for the vulnerability.
End of support	At the end of the six-month period, Cisco removes the Vulnerability Shield from download and ends support. Although the installed Vulnerability Shield is no longer supported, if it remains installed it will continue to operate until you manually remove it.
Software upgrades	Upgrading the SD-WAN control-component software removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, reinstall the appropriate Vulnerability Shield or deploy another applicable Vulnerability Shield.

Vulnerability Shield lifecycle

Stage	**Description**
Day 0 – Publication	Cisco publishes the Vulnerability Shield, makes it available for download, and announces its six-month download and support period.
Day 1 – Deployment	Deploy the Vulnerability Shield in Monitoring, Protecting (Enforce), or Disabled mode. Cisco SD-WAN Manager applies the selected mode to all applicable Cisco Catalyst SD-WAN Control Components.

Day 2 – Operation	Cisco SD-WAN Manager displays the installed Vulnerability Shield and its operating mode. The Vulnerability Shield continues protecting the applicable SD-WAN control components, even if it is no longer supported by Cisco, until you remove it or upgrade the software.
Day N – Upgrade or end of support	A software upgrade removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, deploy the appropriate, supported Vulnerability Shield again, if any. **Note** After the six-month download and support period ends, an installed Vulnerability Shield continues operating in its existing mode until you manually remove it. Although Cisco no longer provides support or downloads for the shield, it is not automatically removed from the control component.



Note Live Protect and its Vulnerability Shields may not fully mitigate risks during the device boot process, during which systems may remain temporarily exposed until security policies are initialized. They also do not mitigate the risk of system instability, including boot loops, resulting from incompatible Vulnerability Shields. Although Cisco uses commercially reasonable efforts to develop effective security technologies, Cisco does not represent or warrant that its offerings will provide absolute security or protect all files, systems, networks, or endpoints against all malware, malicious attacks, or other threats.

Configure Live Protect using Cisco SD-WAN Manager

Use these steps to deploy and configure Live Protect Vulnerability Shields in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, go to **Monitor** > **Advisories** > **Security Advisories**.

Step 2 Select **Control Components** to display the relevant information for your infrastructure.

Step 3 Select a specific security advisory to view its details.

Step 4 Select **Affected Control Components**.

Step 5 Choose **Deploy Shield**.

This shield is deployed to all applicable control components associated with the selected advisory. Individual control component selection for deployment is not supported.

Step 6 Choose the desired mode:

- Monitoring: Observes activity and logs events without blocking traffic.
- Protecting (Enforce): Enforces security policies to actively block exploit attempts.

Note
Shields provide temporary mitigation for identified vulnerabilities until affected components are upgraded to a software version that includes remediation.

Cisco strongly recommends upgrading to a software release containing the fix as soon as possible.

Disable Live Protect using Cisco SD-WAN Manager

Use these steps to disable a Live Protect shield.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Compliance** > **Advisories**.
Step 2 Select the advisory for which you want to deactivate the shield.
Step 3 Select **...** and choose **Disable Shield**.

Monitor Live Protect

You can monitor Live Protect through shield status and event statistics.

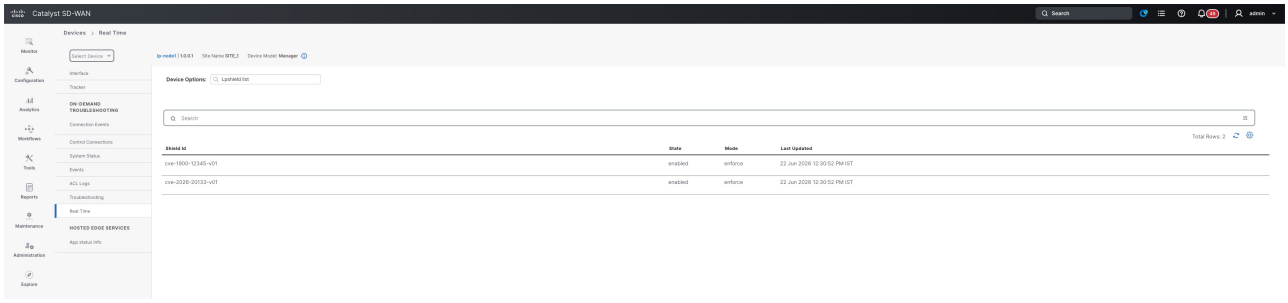
View shield status for Live Protect

Procedure

Step 1 From the Cisco SD-WAN Manager menu, go to **Monitor** > **Devices**.
Step 2 Select a device to open the Device360 page.
Step 3 Select **real-time monitoring** from the drop-down list and choose **Lpshield List**.

The Lpshield List view displays the installed shield status on the selected device.

Figure 9: View shield status



View event statistics for Live Protect

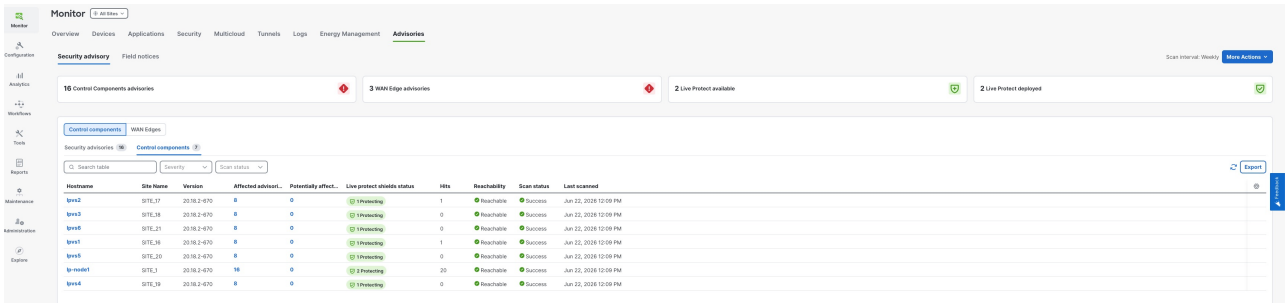
Procedure

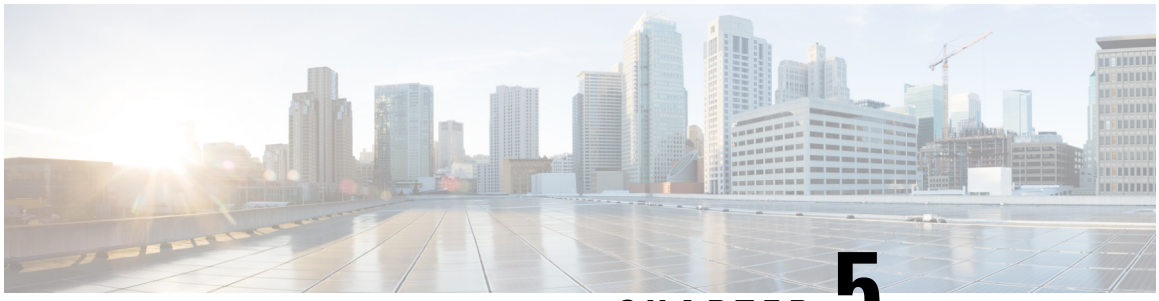
Step 1 From the Cisco SD-WAN Manager menu, go to **Monitor** > **Advisory**.

Step 2 Select **Control Components**.

The Hits field displays the event statistics for the deployed shields.

Figure 10: View event statistics





CHAPTER 5

Cisco SD-WAN Manager Data Storage

- Information About Cisco SD-WAN Manager Data Storage, on page 63
- Configure Cisco SD-WAN Manager Data Storage, on page 63
- View Cisco SD-WAN Manager Data Storage, on page 66

Information About Cisco SD-WAN Manager Data Storage

Cisco SD-WAN Manager stores broad range of information including device configuration information, alarms, audit logs, various metrics, firewall rules and so on, in a database.

Configure Cisco SD-WAN Manager Data Storage

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Statistics Database Configuration** section, to view the maximum space available for the database.
3. For each field in the **Statistics Type** column, assign the amount of storage to be allocated, in gigabytes (GB). The total value of all the fields cannot exceed the maximum available space.

Table	Description
Approute Index Name: approutestatsstatistics	SDWAN Tunnel SLA, which is used to Calculate Tunnel SLA
- Aggregated SAIE Index Name: aggregatedappsdpistatistics	Aggregated application data for certain edges and interfaces. this is used to calculate application usage for certain site/device
Audit Log	Audit Log
vnf statistics	Service Chain Health Statistics data for Clouddock
Firewall	Firewall rule and counters
IPS Alert	Intrusion Prevention System, which is used to Monitors network traffic and analyzes against a defined rule set.

Table	Description
CloudExpress	Cloud onRamp
AppHosting	
Alarm	Alarms
Performance Monitor	Application Performance, this is used to measure performance of each application and site.
NWPI	Network wide path insight trace, flow, packet, aggregation and task data
umts-monitoring	Underlay network performance measurement
URLF	URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in an URL list
Bridge Interface	Cisco vEdge devices bridge interface rx/tx statistics
Device Events	Events received from devices
EIO	EIO module 3G/4G/5G statistics
Device Configuration	Device Running Configuration
Interface	Device Interface Table
Wlan Client Info	
UtdDaqIox	
Speed Test	Speed Test Record
BridgeMac	Cisco vEdge device per interface/mac address rx/tx statistics
Device System Status	Device System Status including CPU, memory, disk etc
umts-event-tunnel-sla-change	underlay performance measurement triggered by tunnel SLA changes.
QoS	statistics/counters of each interface queues.
Tracker Statistics	Endpoint Tracker SLA metrics
Sleofflinereport	
Flow Log	Flowlog feature(should be applicable for Cisco vEdge devices only)
DeviceHealth	Device Health Table

Table	Description
Umbrella	Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device.
Network-wide Packet Insight (raw)	NWPI raw data storage
umts-event-tunnel-pmtu-change	Underlay performance measurement triggered by tunnel path MTU changes.
Security Unified Logging	This feature supports Unified Logging which is used to capture information about connection events across different security features at different stages during policy enablement and execution. With Unified Logging, you can have visibility to the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol or applications. Additionally, this feature also provides support for On-Demand Troubleshooting. On-Demand troubleshooting allows a user to view the connection events of different flows of traffic from a device within a configured period of time.
SiteHealth	Site Health Table
Artstatistics	
UMTS Rest Event	Underlay performance measurement triggered by other events except tunnel SLA change and Path MTU changes.
SAIE	Raw DPI record, per IP flow tx/rx counters.
Aggregated Tunnel SLA approutestatsstatistics_routing_summary	Aggregated 24 hours SLA for each tunnel
Aggregated Tunnel SLA approutestatsstatistics_transport_summary	Aggregated 24 hours SLA for each color combination

4. Click **Save**.

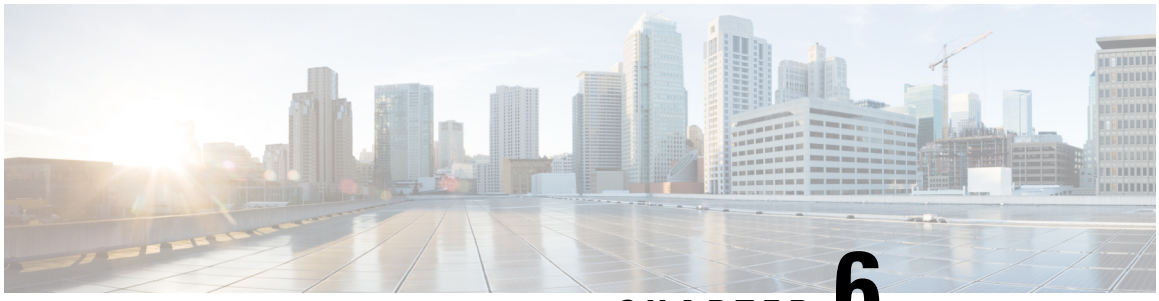
   Cisco SD-WAN Manager updates the storage allocations that you have assigned once a day, at midnight.

View Cisco SD-WAN Manager Data Storage

From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Statistics Database Configuration**.

This shows the space available for the database and the total amount of space currently being used by each data type.

For information about disk size recommendations and requirements, see the server recommendations for your release in Cisco Catalyst SD-WAN Controller Compatibility Matrix and Server Recommendations.



CHAPTER 6

Application Performance and Site Monitoring

Table 5: Feature History

Feature Name	Release Information	Description
Application Performance and Site Monitoring	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	You can monitor and optimize the application health and performance on all sites or a single site using Cisco SD-WAN Manager.

- Overview of Application Performance and Site Monitoring, on page 67
- Restrictions for Application Performance and Site Monitoring, on page 68
- Configure Application Performance and Site Monitoring using Configuration Groups, on page 69
- Configure Application Performance and Site Monitoring Using a CLI Add-on Template, on page 70
- All Sites and Single Site View, on page 71
- View Application Health in Table View, on page 72
- View Application Health in Heatmap View, on page 72
- Troubleshoot Application Performance and Site Monitoring, on page 73

Overview of Application Performance and Site Monitoring

The **Application Health** window displays the following:

- All applications running in all sites: table view and heat map view.
- All applications running at a specific site: table view and heat map view.
- Single application running in all sites: table view and heat map view.
- Single application running at a specific site: aggregated line chart and per path table view.

Applications Health Metrics

The applications health is calculated as follows:

Table 6:

Health	QoE
Good	QoE >= 8
Fair	QoE 5~8
Poor	QoE < 5

Restrictions for Application Performance and Site Monitoring

- Performance monitoring is supported only for IPv4 traffic.
- The following applications are not supported:
  - airplay
  - cisco-collab-control
  - cisco-ip-camera
  - cisco-jabber-control
  - cisco-phone-control
  - citrix
  - clearcase
  - conference-server
  - conferencing
  - espn-browsing
  - espn-video
  - exec
  - FTP (all)
  - google-downloads
  - icloud
  - isakmp
  - isatap-ipv6-tunneled
  - l2tp
  - modbus
  - oscar-filetransfer
  - pcoip
  - sixtofour-ipv6-tunneled

- skinny
- sunrpc
- telepresence-control
- tftp (all)
- vnc-http
- web-analytics
- webex-app-sharing
- webex-control
- webex-media
- windows-azure
- yahoo-voip-over-sip

Configure Application Performance and Site Monitoring using Configuration Groups

You can enable application performance and site monitoring using Cisco SD-WAN Manager by configuring **Performance Monitoring** under **System Profile** in a configuration group.

The application performance and site monitoring feature needs NBAR to be enabled on all LAN interfaces for application recognition.

If Application-Aware Routing (AAR) policy is configured then NBAR is automatically enabled. If AAR policy is not configured, then NBAR must be enabled on all LAN interfaces using a CLI add-on template. Use the **ip nbar protocol-discovery** configuration to enable NBAR on all LAN interfaces.

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 Performance Monitoring in a system profile.

a) Enter Application Performance Monitoring information.

Table 7: Monitoring

Field	Description
Monitoring	To enable monitoring, check the check box. You can enable monitoring only in Global mode. Enabling monitoring displays a list of application groups. Fourteen application groups are enabled by default. You can disable or enable more applications based on your requirements. Check the check box adjacent to an application group to enable monitoring.

b) Enter Underlay Measurement Track Service information.

Table 8: Underlay Measurement Track Service

Field	Description
Monitoring	Click **Monitoring** drop-down list, and choose **Global** to trace tunnel paths regularly according to a configured time interval. Click the toggle button to enable the continuous monitoring option in UMTS.
Monitoring Interval (Minutes)	In the **Monitoring Interval (Minutes)** field, choose a time. This option enables you to monitor exact path at a specific time period.
Event Driven	Click the **Event Driven** drop-down list, and choose **Global** to trace tunnel paths when triggered by one of the events as per the event type.
Event Type	Click the **Event Type** drop-down list, and choose an event type. The event types are: • **SLA Change**: Change in the service-level agreement (SLA) parameter for the tunnel. • **PMTU Change**: Change in the Path MTU (PMTU) parameter for the tunnel.

Step 3 To save the configuration, click **Save**.

What to do next

Also see Deploy a Configuration Group.

Configure Application Performance and Site Monitoring Using a CLI Add-on Template

You can enable application performance monitor using the CLI Add-on feature template in Cisco SD-WAN Manager. For more information see, Application Performance Monitoring.

If Application-Aware Routing (AAR) policy is configured then NBAR is automatically enabled. If AAR policy is not configured, then NBAR must be enabled on all LAN interfaces using a CLI add-on template. Use the **ip nbar protocol-discovery** configuration to enable NBAR on all LAN interfaces.

The following example shows the application performance monitoring configuration.

```
class-map match-any APP_PERF_MONITOR_APPS_0
    match protocol attribute application-group amazon-group
    match protocol attribute application-group box-group
    match protocol attribute application-group concur-group
    match protocol attribute application-group dropbox-group
    match protocol attribute application-group google-group
    match protocol attribute application-group gotomeeting-group
    match protocol attribute application-group intuit-group
    match protocol attribute application-group ms-cloud-group
    match protocol attribute application-group oracle-group
    match protocol attribute application-group salesforce-group
    match protocol attribute application-group sugar-crm-group
    match protocol attribute application-group webex-group
    match protocol attribute application-group zendesk-group
    match protocol attribute application-group zoho-crm-group
class-map match-any APP_PERF_MONITOR_FILTERS
    match class-map APP_PERF_MONITOR_APPS_0

performance monitor context APP_PM_POLICY profile sdwan-performance
    exporter destination local-sdwan source NULL0
    traffic-monitor art-aggregated class-and APP_PERF_MONITOR_FILTERS interval-timeout 300
 sampling-interval 100
    traffic-monitor media-aggregated class-and APP_PERF_MONITOR_FILTERS interval-timeout
300 sampling-interval 100

performance monitor apply APP_PM_POLICY sdwan-tunnel
performance monitor apply APP_PM_POLICY color-all-dia
performance monitor apply APP_PM_POLICY sdwan-sig
```

All Sites and Single Site View

All Applications All Sites View

The default setting for the applications window is the all sites view. You can view information for all sites by clicking the **All Sites** button on the top of the page, and clicking the radio button next to **All Sites**.

The all sites view displays information for all applications of all sites for the last one hour.

In the table, the **Health** column shows the application health. Place the cursor over the icon in the column to display **Good**, **Fair**, or **Poor** health status. The health of the application is measured by Quality of Experience (QoE).

Click the toggle button to switch to the application heatmap view.

In the heatmap view, the grid of colored squares displays the application health as **Good**, **Fair**, or **Poor**. You can hover over a square or click it to display additional details of an application at a specific time and click **View details** to view specific application details. Click the time interval drop-down list to change the time interval.

All Applications Single Site View

You can also view the health of all the applications on a single site. To enter single site view, click the **All Sites** button on the top of the page, and click the radio button next to **Single Site** to select the site of interest.

Single Application All Site View

For a single application on all sites, click a specific **Site ID** to navigate to single site monitoring. Click the application name to view further application specific details.

Single Application Single Site View

For a single application on a single site, a line graph shows the application health over a period of time. Select the time from the drop-down list to select 1, 3, 6, 12, or 24 hours. The table displays a list of paths that has processed application traffic over a time period. Select individual paths and view the individual QoE lines on the line graph. At a time five paths can be selected, and five line charts are displayed. You can also drag the top handles to focus on a particular point in time. When you change the time, the table automatically refreshes to show the health information for that time interval.

View Application Health in Table View

The **Application Health** window displays the following in table view:

- All applications for all sites: A selected list of applications that are enabled using the performance monitoring feature or the CLI add-on template from all the sites.
- All applications for a single site: A selected list of applications that are enabled using the performance monitoring feature or the CLI add-on template from a single site.
- All the sites of a single application: All the sites of a selected application that is enabled using the performance monitoring feature or the CLI add-on template, sorted by the status in the health column.

In the table, the **Health** column shows the application health. Place the cursor over the icon in the column to display **Good**, **Fair**, or **Poor** health status. The health of the application is measured by QoE.

Click the application name to view further application specific details. For a single application on all sites, click a specific **Site ID** to navigate to single site monitoring.

Click the toggle button to switch to application heatmap view.

View Application Health in Heatmap View

The **Application Health** window displays the following in heatmap view:

- All applications for all sites: A list of all applications health for different time selections.
- All applications for a single site: A selected list of applications that are enabled using the performance monitoring feature or the CLI add-on template from a single site.
- All the sites of a single application: A list of sites and health of each site at different time intervals for a single application.

In the heatmap view, the grid of colored squares displays the application health as **Good**, **Fair**, or **Poor**. You can hover over a square or click it to display the additional details of an application at a specific time and click **View details** to view specific application details. Click the time interval drop-down list to change the time interval.

Click the **Toggle** button to switch to the application table view.

Troubleshoot Application Performance and Site Monitoring

To check the basic network metrics that are used to calculate the application QoE, use the **show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record** and **show performance monitor cache monitor APP_PM_POLICY-media_agg detail format record** commands.

```
Device# show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record

 Monitor: APP_PM_POLICY-art_agg
 Data Collection Monitor:
  Cache type:                               Synchronized (Platform cache)
  Cache size:                                   112500
  Current entries:                                   6
  High Watermark:                                    6
  Flows added:                                       6
  Flows aged:                                        0
  Synchronized timeout (secs):                     300

FLOW DIRECTION:                             Output
TIMESTAMP MONITOR START:                    14:10:00.000
FLOW OBSPOINT ID:                           4294967298
INTERFACE OVERLAY SESSION ID OUTPUT:        0
IP VPN ID:                                  65535
APPLICATION NAME:                           layer7 share-point
connection server resp counter:             1477
connection to server netw delay sum:        10822  < --- SND_ samples
connection to server netw delay min:        100
connection to server netw delay max:        103
connection to client netw delay sum:        3559 < --- CND_ samples
connection to client netw delay min:        20
connection to client netw delay max:        198
connection application delay sum:           936
connection application delay min:           0
connection application delay max:           122
connection responder retrans packets:       2    <---- lost_samples
connection to server netw jitter mean:      0
connection count new:                       108      < ---- SND/CND_total
connection server packets counter:          2018     <---- total_samples

Latency(SND  ms) = SND_ samples/ SND/CND_total
Latency(CND  ms) = CND_ samples/ SND/CND_total
Loss ratio = lost_samples /total_samples

Device# show performance monitor cache monitor APP_PM_POLICY-media_agg detail format record


 Monitor: APP_PM_POLICY-media_agg

 Data Collection Monitor:

  Cache type:                               Synchronized (Platform cache)
  Cache size:                                    40000
  Current entries:                                   4
  High Watermark:                                    4

  Flows added:                                       4
  Flows aged:                                        0
  Synchronized timeout (secs):                     300

FLOW DIRECTION:                         Input
```

```
TIMESTAMP MONITOR START:             14:20:00.000
FLOW OBSPOINT ID:                    4294967310
INTERFACE OVERLAY SESSION ID INPUT:  132
IP VPN ID:                           65535
APPLICATION NAME:                    layer7 rtp-video
trns counter packets lost rate:      0.00
trns counter packets expect:         4696 < --- total_ packets
trns counter packets lost:           0        < --- lost_ packets
rtp jitter inter arrival mean:       0
rtp jitter inter arrival samples:    4666     < --- jitter_samples
rtp jitter inter arrival sum:        108324570 < --- jitter_ sum

Loss ratio = lost_ packets /total_ packets
Jitter (us) = jitter_ sum/jitter_samples
```

To check if the application performance is enabled, use the **show performance monitor context APP_PM_POLICY configuration** command.

```
Device# show performance monitor context APP_PM_POLICY configuration
!================================================================================
!               Equivalent Configuration of Context APP_PM_POLICY              !
!================================================================================
!Exporters
!==========
!
flow exporter APP_PM_POLICY-1
description performance monitor context APP_PM_POLICY exporter
destination local sdwan
export-protocol ipfix
option application-table export-spread 0
!
!Access Lists
!=============
ip access-list extended APP_PM_POLICY-art_agg_tcp
permit tcp any any
!
ip access-list extended APP_PM_POLICY-media_agg_udp
permit udp any any
!
!Class-maps
!===========
class-map match-all APP_PM_POLICY-art_agg
match class-map APP_PERF_MONITOR_FILTERS
match access-group name APP_PM_POLICY-art_agg_tcp
!
class-map match-any APP_PM_POLICY-media_agg_app
match protocol rtp in-app-hierarchy
!
class-map match-all APP_PM_POLICY-media_agg
match class-map APP_PERF_MONITOR_FILTERS
match access-group name APP_PM_POLICY-media_agg_udp
match class-map APP_PM_POLICY-media_agg_app
!
!Samplers
!=========
sampler APP_PM_POLICY-art_agg
granularity connection
mode time-based 1 out-of 100
!
sampler APP_PM_POLICY-media_agg
granularity connection
mode time-based 1 out-of 100
!
```

```
!Records and Monitors
!=====================
!
flow record type performance-monitor APP_PM_POLICY-art_agg
description ezPM record
match flow direction
match application name
match timestamp absolute monitoring-interval start
match flow observation point
match overlay session id output
match routing vrf service
collect connection new-connections
collect connection server counter responses
collect connection delay network to-server sum
collect connection delay network to-server min
collect connection delay network to-server max
collect connection delay network to-client sum
collect connection delay network to-client min
collect connection delay network to-client max
collect connection delay application sum
collect connection delay application min
collect connection delay application max
collect connection server counter packets long
collect connection server counter packets retransmitted
collect connection jitter network to-server mean
!
!
flow monitor type performance-monitor APP_PM_POLICY-art_agg
record APP_PM_POLICY-art_agg
exporter APP_PM_POLICY-1
cache entries 2700
cache timeout synchronized 300 export-spread 150
!
!
flow record type performance-monitor APP_PM_POLICY-media_agg
description ezPM record
match flow direction
match application name
match timestamp absolute monitoring-interval start
match flow observation point
match overlay session id input
match routing vrf service
collect transport packets lost rate
collect transport rtp jitter inter-arrival mean
!
!
flow monitor type performance-monitor APP_PM_POLICY-media_agg
record APP_PM_POLICY-media_agg
exporter APP_PM_POLICY-1
cache entries 960
cache timeout synchronized 300 export-spread 150
!

!Policy-maps
!============
policy-map type performance-monitor APP_PM_POLICY-in
parameter default account-on-resolution
class APP_PM_POLICY-art_agg
  flow monitor APP_PM_POLICY-art_agg sampler APP_PM_POLICY-art_agg
class APP_PM_POLICY-media_agg
  flow monitor APP_PM_POLICY-media_agg sampler APP_PM_POLICY-media_agg
!
policy-map type performance-monitor APP_PM_POLICY-out
parameter default account-on-resolution
```

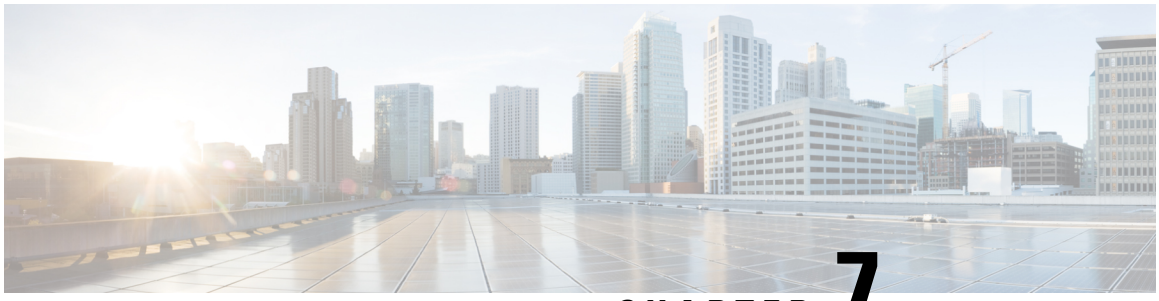
```
class APP_PM_POLICY-art_agg
  flow monitor APP_PM_POLICY-art_agg sampler APP_PM_POLICY-art_agg
class APP_PM_POLICY-media_agg
  flow monitor APP_PM_POLICY-media_agg sampler APP_PM_POLICY-media_agg
!
policy-map type performance-monitor APP_PM_POLICY-art-in
parameter default account-on-resolution
class APP_PM_POLICY-art_agg
  flow monitor APP_PM_POLICY-art_agg sampler APP_PM_POLICY-art_agg
!
policy-map type performance-monitor APP_PM_POLICY-art-out
parameter default account-on-resolution
class APP_PM_POLICY-art_agg
  flow monitor APP_PM_POLICY-art_agg sampler APP_PM_POLICY-art_agg
!
!Interface Attachments
!======================
interface Tunnel1
service-policy type performance-monitor input APP_PM_POLICY-in
service-policy type performance-monitor output APP_PM_POLICY-out
!
interface Tunnel4
service-policy type performance-monitor input APP_PM_POLICY-in
service-policy type performance-monitor output APP_PM_POLICY-out
!
interface GigabitEthernet1
service-policy type performance-monitor input APP_PM_POLICY-art-in
service-policy type performance-monitor output APP_PM_POLICY-art-out
!
interface GigabitEthernet4
service-policy type performance-monitor input APP_PM_POLICY-art-in
service-policy type performance-monitor output APP_PM_POLICY-art-out
!
interface Tunnel1000100
service-policy type performance-monitor input APP_PM_POLICY-art-in
service-policy type performance-monitor output APP_PM_POLICY-art-out
!
interface Tunnel1000200
service-policy type performance-monitor input APP_PM_POLICY-art-in
service-policy type performance-monitor output APP_PM_POLICY-art-out
!
```

To check pending object issues use the **show platform software object-manager fp active statistics** command.

```
Device#  show platform software object-manager fp active statistics

Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 1378
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 4
Backplane-objects: 0
Error-objects: 0
Number of bundles: 0
Paused-types: 3
```



CHAPTER 7

Devices and Controllers

Table 9: Feature History

Feature Name	Release Information	Description
Data Plane CPU and Memory Utilization	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature you can monitor data plane CPU and memory utilization on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
QoS statistics for interfaces and tunnels	Cisco Catalyst SD-WAN Manager Release 20.18.1	You can monitor traffic across network interfaces and tunnels with real-time and historical statistics. This feature extends the existing QoS interface-level view to include class-level traffic insights and per-tunnel QoS statistics.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

This section provides information on the Cisco Catalyst SD-WAN devices and control components.

- View the Geographic Location of Your Devices, on page 78
- View System Status, on page 81
- View Device System Resource Utilization in Cisco SD-WAN Manager, on page 82
- View Device System Resource Utilization Using the CLI, on page 82
- View and Open TAC Cases, on page 83
- View the Status of a Cisco Catalyst SD-WAN Validator, on page 84
- View the Status of a Cisco Catalyst SD-WAN Controller, on page 85
- View Control Connections, on page 86
- View Devices Connected to Cisco Catalyst SD-WAN Manager, on page 86
- View Services Running on Cisco Catalyst SD-WAN Manager, on page 86
- View Device Status in the Overlay Network, on page 87
- View Device Information, on page 87

- View Device Configuration, on page 90
- View the Software Versions Installed on a Device, on page 90
- View Device Interfaces, on page 90
- View WAN Interfaces, on page 91
- View Interfaces in Management VPN or VPN 512, on page 92
- View DHCP Server and Interface Information, on page 92
- View Interface MTU Information, on page 93
- View and Monitor Cellular Interfaces, on page 93
- View Colocation Cluster Information, on page 95
- View Cisco Colo Manager Health, on page 96
- View Cisco Catalyst SD-WAN Manager Cluster Information Using the CLI, on page 97
- View QoS statistics, on page 97
- Collect System Information in an Admin-Tech File, on page 103
- Monitor Cflowd and SAIE Flows for Cisco IOS XE Catalyst SD-WAN Devices, on page 108
- Reboot a Device, on page 109
- Reset Interfaces, on page 111
- Make Your Device Invalid, on page 111
- Bring Your Device Back to Valid State, on page 111
- Stop Data Traffic, on page 112
- Perform a Factory Reset, on page 112
- Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices, on page 113

View the Geographic Location of Your Devices

Use the **Geography** window in Cisco SD-WAN Manager to view information about the Cisco Catalyst SD-WAN devices and links in the overlay network. The **Geography** window provides a map displaying the geographic location of the devices in the overlay network.

Note The browser on which you are running Cisco SD-WAN Manager must have internet access. If you do not have internet access, ensure that the browser has access to "*.openstreetmaps.org."

To view the geographic location of the devices in the overlay network:

1. From the **VPN Group** list, choose a VPN group.
2. From the **VPN Segment** list, choose a VPN segment.
3. Set filters.

Set Map Filters

To select the devices and links you want to display on the map:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter**.

3. From the options that display, choose the device group. By default, the group **All** is selected and displays all devices in the overlay network. The group **No Groups** displays devices that are not part of a device group. If all devices are in a group, the **No Groups** option is not displayed.
4. Choose the devices you want to view. By default, the map displays all device types including edge devices, Cisco SD-WAN Validator, Cisco SD-WAN Controller, and Cisco SD-WAN Manager.
5. Choose the state of control and data links. By default, the map displays all control and data connections.
6. Close the **Filter** box by moving the cursor outside the box.

The map dynamically updates to display your selections.

View Device Information

To view basic information for a device, hover over the device icon. A pop-up box displays the system IP, hostname, site ID, device type, and device status.

To view detailed information for a device, double-click the device icon. Click **Device Dashboard**, **Device Details**, **SSH Terminal**, **Site Topology**, or **Links** to view more details for the device.

Note the following about links:

- A thin blue line displays an active control connection between two devices.
- A bold blue line displays multiple active connections between devices.
- A dotted red line displays a control connection that is down.
- A bold dotted red line displays multiple control connections that are down.
- A thin green line displays an active data connection between two devices.
- A bold green line displays multiple active data connections.
- A dotted red line displays a data connection that is down.
- A bold dotted red line displays multiple data connections that are down.
- A thick gray line displays an active consolidated control and data connection between two devices.

  If you hover over the line, a hover box tells you if the connection is up or down.

Configure and View Geographic Coordinates for a Device

To configure the geographic coordinates for a device, use the **System Feature** template under **Configuration** > **Templates**.

If the Cisco Catalyst SD-WAN device is not attached to a configuration template, you can configure the latitude and longitude directly on the device:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose a device from the left pane. The SSH Terminal window opens in the right pane.
3. Enter the username and password to log in to the device.
4. Use the `show system status` command to determine whether the device is attached to a configuration template:

```
Device# show system status...
    Personality:            vedge
    Model name:             vedge-cloud
    Services:               None
    vManaged:               false
    Commit pending:         false
    Configuration template: None
```

In the output, check the values in the `vManaged` and `Configuration template` output fields. If the `vManaged` field is false, the device is not attached to a configuration template, and the `Configuration template` field value is `None`. For such a device, you can configure the GPS coordinates directly from the CLI. If the `vManaged` field is `true`, the Cisco SD-WAN Manager server has downloaded the device configuration, and the `Configuration template` field value displays the name of the configuration template. For such a device, you cannot configure the GPS coordinates directly from the CLI. If you attempt to do so, the `validate` or `commit` commands fails with the following message:

```
Aborted: 'system is-vmanaged': This device is being managed by the vManage. Configuration
 through the CLI is not allowed.
```

5. Enter configuration mode:

   For Cisco vEdge devices:

   ```
   Device# config
       Device(config)#
   ```

   For Cisco IOS XE Catalyst SD-WAN devices:

   ```
   Device# configure-transaction
       Device(config)#
   ```

6. Configure the latitude and longitude for the device.

   ```
   Device(config)# system gps-location latitude
                              degrees.minutes.seconds
       Device(config-system)# gps-location longitude
                              degrees.minutes.seconds
   ```

7. Save the configuration.

   ```
   Device(config-system)# commit
       Device(config-system)#
   ```

Note For the device/site location in Cisco SD-WAN Manager, there are several data sources including network hierarchy, GPS, geo-fencing, manual configuration and system default.

- The device location priority is: GPS > geo-fencing > manual configuration > system default

  monitoring → device table

  monitoring → device360 information icon

- The site location priority is: network hierarchy > device (the first device in site) location

  monitoring → geographical view

View System Status

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

   Cisco SD-WAN Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device. If you choose a Cisco vEdge device, the window displays **System Status** by default.

   If you choose a Cisco IOS XE Catalyst SD-WAN device or any controller, click **System Status** in the left pane. The right pane displays information about the device.

Information About System Status Parameters

The **System Status** window displays the following:

- Reboot—Number of times the device has rebooted. For details about each reboot, click **Reboot**. The Reboot window opens and contains the following elements:
- Crash—Number of times the device has crashed. For details about each crash, click **Crash**. The Crash window opens and contains the following elements:
- Status of hardware components, applicable only if the selected device is a hardware:
  - Module
  - Temperature sensors
  - USB
  - Power supply
  - Fans

The status of a hardware component is represented in one of the following ways:

- Green check mark—Component is operational.
- Red circle with an X—Component is down.
- Orange triangle with an exclamation point—Component has an error.
- N/A—Not applicable since the selected device is not a hardware Cisco vEdge device.
- CPU & Memory—To the right are the time periods. Click a predefined or custom time period for which to display data.
  - CPU usage—Displays the CPU usage, as a percentage of available CPU, over the selected time range.
  - Memory usage—Displays the memory usage, as a percentage of available memory, over the selected time period.

View Device System Resource Utilization in Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IOS XE Catalyst SD-WAN device or a controller.
3. Click **System Status** in the left pane.

   The right pane displays information about the device.
4. On the **System Status** page, view system resource details, such as control plane CPU and memory, data plane CPU and memory, and power usage details in the **CPU & Memory** pane.
5. Click either **Real Time**, a predefined time period, or a custom time period for which you want to view data.

   Cisco SD-WAN Manager shows the CPU and memory utilization details for a device for a selected time duration. The device collects the utilization data every 10 seconds and stores it in an XML or a JSON file format on the device.

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, devices export data plane CPU and memory statistics to Cisco SD-WAN Manager. The system utilization graph displays these statistics.

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, Cisco SD-WAN Manager displays historical power usage data over a period of time.

View Device System Resource Utilization Using the CLI

System and Resource Status

The **show sdwan system status** command displays the system status for a device and shows the CPU utilization calculation.

For releases before Cisco SD-WAN Release 20.9.1, the user CPU time (in percentage) is used to calculate the CPU utilization of a device.

For releases Cisco SD-WAN Release 20.9.1 and later, both the user CPU time and the system CPU time (in percentage) are used to calculate the CPU utilization of a device, as indicated in the **show sdwan system status**.

The following example shows the system status for Cisco SD-WAN Manager devices:

```
Device# show sdwan system status
System logging to host  is disabled
System logging to disk is enabled
System state:            GREEN. All daemons up
System FIPS state:       Disabled
Last reboot:             Image Install
CPU-reported reboot:     Initiated by other
Boot loader version:     Not applicable
System uptime:           0 days 00 hrs 23 min 31 sec
Current time:            Mon Jan 30 10:24:44 UTC 2023
```

```
Hypervisor Type:          ESXI
Cloud Hosted Instance:    false
Load average:             1 minute: 1.10, 5 minutes: 1.67, 15 minutes: 1.71
Processes:                557 total
CPU allocation:           16 total,   1 control,   7 data
CPU states:           10.38% user,   1.47% system,   88.04% idle ---------CPU Utilization
Memory usage:             32820584K total,    4488868K used,   28331716K free
                          575156K buffers,  3859052K cache
Disk usage:               Filesystem      Size   Used  Avail   Use %  Mounted on
                       /dev/disk/by-label/fs-bootflash  45580M  2327M  40934M  5% /bootflash

                                387M  159M  223M   42   /bootflash/.installer
```

Quantum Flow Processor Status

View and Open TAC Cases

Table 10: Feature History

Feature Name	Release Information	Description
Access TAC Cases from Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco SD-WAN Manager without having to go to a different Case Manager portal.
SCM Integration Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature introduces various enhancements to the Settings page in Cisco SD-WAN Manager and the Support Case Manager (SCM) wizard.

Supported Devices

This feature is supported on both Cisco Catalyst SD-WAN and Cisco IOS XE Catalyst SD-WAN devices.

Overview

For any Cisco SD-WAN Manager troubleshooting issues, you raise a support case in the SCM portal. In Cisco SD-WAN Manager, there is a provision to upload an Admin-Tech File to a specific Service Request (SR) on the SCM server by providing the SR number and the token details.

Starting from Cisco vManage Release 20.9.1, you can access SCM portal from Cisco SD-WAN Manager. In the SCM portal, you can create, view, or upload an admin-tech file. For more information on Admin-tech files, see Admin-Tech File.

Prerequisites to Access TAC Cases

- You need active Cisco single sign-on (SSO) login credentials to access the SCM Wizard and the cloud server.

View TAC Cases

Perform the following steps to view TAC cases from Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **TAC Cases**.
2. Login to the SCM portal using Cisco SSO login.

   The TAC Support Cases portal displays a list of cases.

Open a TAC Case

Perform the following steps to open a TAC Case from Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **TAC Cases**.
2. In the **TAC Support Cases** page, click **Open a Case**.
3. Enter all the other relevant case details.
4. Click **Create**.

   The **TAC Support Cases** portal now displays the updated list of cases.

For more information about using SCM portal, refer Cisco TAC Connect.

View the Status of a Cisco Catalyst SD-WAN Validator

You have the following options to view the status of a Cisco Catalyst SD-WAN Validator.

Use the Dashboard Screen

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.
2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **Cisco vBond**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of Cisco SD-WAN Validator orchestrators in your overlay network.
3. To know the status of the Cisco Catalyst SD-WAN Validator, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

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

2. Click **Filter** and choose **vBond** under **Types**.
3. Click the Cisco SD-WAN Validator icon to check its status.

Use the Network Screen

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the Cisco Catalyst SD-WAN Validator that you want to view the status for. You can either scroll through the list of devices in the device table or enter **Validator** as the keyword in the search bar.
3. Click the relevant Cisco Catalyst SD-WAN Validator under the **Hostname** column. The **Control Connections** screen opens by default and displays information about all control connections that the device has with other controller devices in the network.

View the Status of a Cisco Catalyst SD-WAN Controller

You have the following options to view the status of a Cisco Catalyst SD-WAN Controller.

Use the Dashboard Screen

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.
2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **Cisco vSmart**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of Cisco SD-WAN Controller in your overlay network.
3. To know the status of the Cisco Catalyst SD-WAN Controller, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter** and choose **vSmart** under **Types**.
3. Click the Cisco SD-WAN Controller icon to check its status.

Use the Network Screen

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the Cisco Catalyst SD-WAN Controller that you want to view the status for. You can either scroll through the list of devices in the device table or enter **Validator** as the keyword in the search bar.
3. Click the relevant Cisco Catalyst SD-WAN Controller instance under the **Hostname** column. The **Control Connections** screen opens by default and displays information about all control connections that the device has with other controller devices in the network.

View Control Connections

To view all control connections for a device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Choose a device to view its control connections.

   If you select a controller device—a Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, or a Cisco Catalyst SD-WAN Controller, the **Control Connections** screen opens by default.
3. If you choose an edge device, the System Status screen displays by default. To view control connections for the device, click **Control Connections** in the left pane. The right pane displays information about all control connections that the device has with other controller devices in the network.

The upper area of the right pane contains the following elements:

- Expected and actual number of connections.
- Control connection data in graphical format. If the device has multiple interfaces, Cisco SD-WAN Manager displays a graphical topology of all control connections for each color.

The lower area of the right pane contains the following elements:

- Search bar—Includes the Search Options drop-down, for a Contains or Match.
- Control connections data in tabular format. By default, the first six control connections are selected. The graphical display in the upper part of the right pane plots information for the selected control connections.

View Devices Connected to Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. Under **Service Configuration**, click the hostname of the desired Cisco SD-WAN Manager server. The **Manager Details** screen appears.
3. Or alternatively:

   Under **Service Configuration**, for the desired Cisco SD-WAN Manager instance, click **...** and choose **Device Connected**.

View Services Running on Cisco Catalyst SD-WAN Manager

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

2. Under **Service Configuration**, click the hostname of the desired Cisco SD-WAN Manager server. The screen displays the process IDs of all the Cisco SD-WAN Manager services that are enabled on Cisco SD-WAN Manager.

View Device Status in the Overlay Network

You have the following options to view the status of a device in the overlay network.

Use the Dashboard Screen

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **WAN Edge**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of **WAN Edge** devices.

3. To know the status of the WAN edge device, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter** and choose **WAN Edge** under **Types**.
3. Click the router icon to check its status.

Use the Network Screen

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the WAN edge router that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Click the relevant WAN edge router under the **Hostname** column. The **System Status** screen opens by default.

View Device Information

You can view basic or detailed information for a device in the overlay network.

To view basic information:

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

2. Hover over the device icon.

   A pop-up box displays the system IP address, hostname, site ID, device type, and device status. To view more information for a device, double-click the device icon to open the **View More Details** pop-up box. Click **Device Dashboard**, **Device Details**, **SSH Terminal**, or **Links** to get further details for the device.

To view detailed information:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the WAN edge router to view the status. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.

3. Click the relevant device under the **Hostname** column. The right pane displays System Status by default. To view more detailed information for the device, choose one of the categories from the left pane.

Note Starting from Cisco vManage Release 20.9.2, the **Monitor** > **Devices** page displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration** > **Devices** page.

View Device Health in Table View

Minimum supported release: Cisco vManage Release 20.10.1

You can view details about the device health for the last one hour in the table view by default in the **Monitor Device** window.

The table displays:

- Device model
- Site ID
- System IP address
- Device health
- Device reachability
- Memory utilization
- CPU load
- RA session
- RA session breakdown

Starting from Cisco Catalyst SD-WAN Manager Release 20.14.1, you can view the devices with remote access in the **Devices** table. To view remote access devices, open the filters under **Devices**, and under **Type**, check the **Remote Access** checkbox.

You can also view the health of all the devices on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

Devices Health Metrics

The devices health is calculated as follows:

Health State	Reachability	Control Plane	Data Plane	Resources	Evaluation Logic
Good	Device reachable	All control connections up	All BFD tunnels up	CPU usage < 75% Memory usage < 75%	All attributes met
Fair	Device reachable	> = 1 control connections up	> = 1 BFD tunnels up	CPU usage > 75% Memory usage > 75%	Any attributes met
Poor	Device not reachable	No control connections up	No BFD tunnels up	CPU usage > 90% Memory usage > 90%	Any attributes met

For a single device record the health is calculated as follows:

Health	QoE
Good	10
Fair	5
Poor	0

The average health metric of devices is calculated as follows:

Health	QoE
Good	QoE >= 6.67
Fair	3.34 <= QoE < 6.67
Poor	0 < QoE < 3.34

View Device Health in Heatmap View

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, the grid of colored squares displays the device health as **Good**, **Fair**, or **Poor**. You can hover over a square or click it to display additional details of a device at a specific time. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

You can view the health of all the devices on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

View Device Configuration

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** .
2. Click **WAN Edge List** or **Control Components**.
3. To view the running configuration, for the desired device, click **…** and choose **Running Configuration**.

   To view the local configuration, for the desired device, click **…** and choose **Local Configuration**.

View the Software Versions Installed on a Device

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Software Versions**.

View Device Interfaces

To view information about interfaces on a device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Interface** in the left pane. The right pane displays interface information for the device.

The upper part of the right pane contains:

- Chart Options bar—Located directly under the device name, this bar includes:
  - Chart Options drop-down—Click **Chart Options** to choose how the data should be displayed.

    - IPv4 & IPv6 drop-down—Click **IPv4 & IPv6** to choose the type of interfaces to view. The information is displayed in graphical format. By default, the graph is Combined, showing interfaces on which both IPv4 and IPv6 addresses are configured. To view IPv4 and IPv6 interfaces in separate graphs, select the Separated toggle button.
    - Time periods—Click either **Real Time**, a predefined time period, or a custom time period for which to view the data.

- Interface information in graphical format.
- Interface graph legend—Choose an interface to display information for just that interface.

The lower part of the right pane contains:

- Filter criteria.
- Interface table, which lists information about all interfaces. By default, the first six interfaces are displayed. The graphical display in the upper part of the right pane plots information for the selected interfaces.
    - Check the check box to the left to select and deselect interfaces. You can select and view information for a maximum of 30 interfaces at a time.
    - To rearrange the columns, drag the column title to the desired position.
    - For cellular interfaces, click the interface name to view a detailed information about the cellular interface.

To view interface status and interface statistics, see show interface and show interface statistics.

View WAN Interfaces

Transport interfaces in VPN 0 connect to a WAN network of some kind, such as the Internet, Metro Ethernet network, or an MPLS network.

You can view information about WAN interfaces on a device using one of the following options:

Real Time Pane

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the window that opens, choose **Real Time** in the left pane.
5. From the **Device Options** drop-down in the right pane, choose **Control WAN Interface Information**.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new field **Bind Interface** is introduced to display mapping relationship between the loopback interfaces and the physical interfaces.

Interface Pane

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. From the **Device Groups** drop-down list, choose the device group to which the device belongs.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, choose **Interface**.

View Interfaces in Management VPN or VPN 512

VPN 512 is commonly used for out-of-band management traffic. To display information about the interfaces in VPN 512 on a router:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, click **Real Time**.
5. From the **Device Options** drop-down list in the right pane, choose **Interface Detail**.
6. In the **Select Filter** dialog box, click **Show Filters** if you want to use filters. Otherwise click **Do Not Filter**.
7. In the **Search bar**, enter **512**, which is the management VPN.

CLI equivalent: show interface vpn 512.

View DHCP Server and Interface Information

When you configure a tunnel interface on a device, several services are enabled by default on that interface, including DHCP. The device can act as a DHCP server for the service-side network to which it is connected, assigning IP addresses to hosts in the service-side network. It can also act as a DHCP helper, forwarding requests for IP addresses from devices in the service-side network to a DHCP server that is in a different subnet on the service side of the device.

To view DHCP server and interface information:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose the device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane. choose one of the following to view specific DHCP server and interface information:

Device Option	Command	Description
DHCP Servers	show dhcp server	View information about the DHCP server functionality that is enabled on the device
DHCP Interfaces	show dhcp interface	View information about the interfaces on which DHCP is enabled on an edge device or a Cisco SD-WAN Controller

View Interface MTU Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Interface Detail**.

View and Monitor Cellular Interfaces

This topic describes how to monitor the status of cellular interfaces in Cisco Catalyst SD-WAN devices.

Monitor Cellular Interfaces

You can verify signal strength and service availability using either Cisco SD-WAN Manager or the LED on the router. You can view the last-seen error message for cellular interfaces from Cisco SD-WAN Manager.

Verify Signal Strength

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. From the **Device Groups** drop-down list, choose a group that the device belongs to.
3. Choose a device by clicking its name in the **Hostname** column.
4. Click **Real Time** in the left pane.
5. From the **Device Options** drop-down list in the right pane, choose **Cellular Radio**.

   The values for the different cellular signals are displayed. If signal strength is poor, or there is no signal, see Troubleshoot Common Cellular Interface Issues.

CLI equivalent: **show cellular status**

Verify Radio Signal Strength Using the Router LED

To check signal strength and service availability of a cellular connection from the router, look at the WWAN Signal Strength LED. This LED is typically on the front of the routers, and is labeled with a wireless icon.

The following table explains the LED color and associated status:

Table 11:

Color	Signal Strength	State	Description
Off	—	—	LTE interface disabled (that is, admin status is down) or not configured
Green	Excellent	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data being received and transmitted)
Yellow	Good	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data being received and transmitted)
Orange	Poor	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data are being received and transmitted)
Red	Critical Issue	Solid	LTE interface enabled but faulty; issues include no connectivity with the base transceiver station (BTS) and no signal

View Error Messages for Cellular Interfaces

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Cellular Status**.

   The output displayed includes a column for Last Seen Error

CLI equivalent **show cellular status**

View Cellular Connections

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Cellular Connection**.

   The output displayed includes columns for **Profile APN** and the link time **Up Since**.

Table 12:

Field	Description
Profile APN	Displays the access point name for cellular connections.
Up Since	Displays the actual time since the connection was established.

CLI equivalent: **show cellular** <*interface*> **connection**

View Colocation Cluster Information

To view the cluster information and their health states. Reviewing this information can help you to determine which CSP device is responsible for hosting each VNF in a service chain.

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Click **Colocation Cluster**.

   All clusters with relevant information are displayed in a tabular format. Click a cluster name.

   From the primary part of the left pane, you can view the cluster topology. In the right pane, you can view the cluster information such as the available and the total CPU resources, available and allocated memory, and so on, based on the size of Cloud OnRamp for Colocation.

The detail part of the left pane contains:

- Filter criteria–choose the fields to be displayed from the search options drop-down.
- A table that lists information about all devices in the cluster (CSP devices and switches).

  Click a CSP cluster. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, and other core parameters that define performance of a network service.

3. Click **Services**.

   Under this area, you can view:

   - All service groups that are attached to the cluster in a tabular format. The first two columns display the name and description of the service chain within the service group.
   - Click **Diagram** to view the service group with all its service chains and VNFs in the design view window.
   - Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
   - Choose a service group from the **Service Groups** drop-down list. The design view displays the selected service group with all its service chains and VNFs.

View Cisco Colo Manager Health

To view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

2. Click a CSP device from the table.
3. From the left pane, click **Colo Manager**.

   The right pane displays information about the memory usage, CPU usage, uptime, and so on, for the colo manager.

View Cisco Catalyst SD-WAN Manager Cluster Information Using the CLI

Table 13: Feature History

Feature Name	Release Information	Description
Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI	Cisco vManage Release 20.9.1	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the **request nms cluster diagnostics** CLI command.

You can use the **request nms cluster diagnostics** command to verify the health of the Cisco SD-WAN Manager cluster and the status of the cluster services running on the cluster. Run the command directly on the Cisco SD-WAN Manager device for which you are running the Cisco SD-WAN Manager cluster.

The **request nms cluster diagnostics** command provides diagnostics information for the Cisco SD-WAN Manager cluster and status information for the following Cisco SD-WAN Manager services:

- Application server
- Messaging server
- Configuration database
- Statistics configuration database
- Coordination server

For more information on the **request nms cluster diagnostics** command, see the *Cisco Catalyst SD-WAN* Command Reference Guide.

View QoS statistics

QoS queue statistics

Quality of Service (QoS) is used to manage and prioritize network traffic. QoS queue statistics measure the performance and utilization of network traffic queues, including metrics such as transmitted packets and dropped packets. These statistics help evaluate how effectively the network is prioritizing and managing traffic flows.

The QoS feature in Cisco SD-WAN Manager enables you to

- monitor the performance of ingress and egress traffic classes to ensure optimal performance across the network
- view tranmission rates for interfaces and tunnel endpoints, both before and after policy application, and

- identify drops caused by policing configured via interfaces and tunnel endpoints, even when policing is enabled via CLI template.

From Cisco Catalyst SD-WAN Manager Release 20.18.1, when you display statistics for a single interface, you can filter by traffic class.

Benefits of QoS queue statistics

- Continuous monitoring: The **QoS Monitor** page in SD-WAN Manager provides real-time QoS statistics for interfaces, tunnel endpoints, and traffic classes.
- Historical data visibility: The **QoS Monitor** page enables you to view historical data for interfaces and tunnels by selecting a time interval.

Restrictions for QoS statistics

Per tunnel QoS statistics

SD-WAN Manager supports per-tunnel QoS statistics only in the controller mode.

Drop statistics

In custom QoS policer configurations that use color selection for conform, exceed, or violate actions, a device may retain exceed-action or violate-action drop packets. As a result, these packets are not included in the drop statistics.

Supported QoS actions

QoS actions like bandwidth, priority, random-detect, child-level shaping, and policing are supported and displayed in the statistics. If a class-map does not contain any of these actions, it will not be collected or displayed. Fair-queuing is not supported.

Real-time QoS

- The **Real Time** view for **Tunnel QoS Summary Statistics** can display up to 4,000 entries.

Monitor the QoS statistics for interfaces

Monitor real-time and historical network traffic for interfaces.

Before you begin

To monitor QoS statistics on interfaces, enable the QoS feature on routers.

Procedure

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

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **QoS** to open the **QoS Monitor** page.

Step 4 Select a time interval for displaying QoS statistics.

Use the **Custom** option to define a specific range of start and end dates and times.

The **Post Policy Rate** and **Post Policy Counter** charts show the traffic and drop rates for the interfaces.

Interface QoS statistics

On the Interface page, you can view

- post-policy rate and post-policy counter charts for interfaces, and
- pre-policy transmission rates, post-policy transmission rates, and drop rates for each traffic class.

Table 14: Interface QoS charts

Chart	Description
Post Policy Rate	Displays data in kilobits per second (Kbps) and packet per second (PPS). • **Rate (Kbps)**: Displays the rate of traffic that successfully passed through the interface after the QoS policy was enforced. Hover over the chart to compare traffic rates across interfaces. • **Drop (Kbps)**: Displays the rate of traffic dropped due to policy enforcement on the interface. It provides basic drop statistics.
Post Policy Counter	Displays data in bytes and packets. • **Counter (bytes)**: Displays the total number of bytes forwarded through the interface after the QoS policy was applied. Hover over the chart to view byte or packet counts per interface. • **Drop (bytes)**: Displays the bytes dropped due to policy enforcement on the interface. It includes only basic drop statistics.

You can also view pre-policy, post-policy, and drop statistics for each interface to analyze class-level traffic details.

Each interface includes this:

Table 15: Interface QoS summary

Column	Description
Interface	Displays the name of the interface. Click an interface to view its classes, including pre-policy, post-policy, and drop rates.

Column	Description
Pre policy TX	Displays the rate of traffic transmitted before the policy was applied to the interface.
Post policy TX	Displays the rate of traffic transmitted after the policy was applied to the interface.
Drop	Displays the rate of traffic dropped after the policy was applied to the interface. The drop rate is the difference between post-policy and pre-policy transmission rates.

Monitor the QoS statistics for tunnels

Monitor real-time and historical network traffic for tunnels.

Before you begin

To monitor QoS statistics on tunnel endpoints, enable the QoS feature on routers.

Procedure

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

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **QoS** to open the **QoS Monitor** page.

Step 4 Click **Tunnel**.

Step 5 Select the time interval to display QoS statistics.

Use the **Custom** option to define a specific range of start and end dates and times.

The **Post Policy Rate** and **Post Policy Counter** charts show the traffic and drop rates for the tunnels.

Tunnel QoS statistics

On the Tunnel page, you can view

- post-policy rate and post-policy counter charts for tunnels, and
- pre-policy transmission rates, post-policy transmission rates, and drop rates for each traffic class.

Table 16: Tunnel QoS charts

Chart	Description
Post Policy Rate	Displays data in kilobits per second (Kbps) and packet per second (PPS). • **Rate (Kbps)**: Displays the rate of traffic that successfully passed through the interface after the QoS policy was enforced. Hover over the chart to compare traffic rates across tunnels. • **Drop (Kbps)**: Displays the rate of traffic dropped due to policy enforcement on the tunnel. It provides basic drop statistics.
Post Policy Counter	Displays data in Bytes and Packets. • **Counter (bytes)**: Displays the total number of bytes forwarded through the interface after the QoS policy was applied. Hover over the chart to view byte or packet counts per tunnel. • **Drop (bytes)**: Displays the bytes dropped due to policy enforcement on the tunnel. It includes only basic drop statistics.

You can also view pre-policy, post-policy, and drop statistics for each tunnel to analyze class-level traffic details.

Each tunnel includes this:

Table 17: Tunnel QoS summary

Column	Description
Tunnel Endpoints	Displays name of the tunnel endpoint. Click a tunnel endpoint to view its classes, including pre-policy, post-policy, and drop rates.
Remote System IP	Displays the IP address of the remote system.
Pre policy TX	Displays the rate of traffic transmitted before the policy was applied to the tunnel.
Post policy TX	Displays the rate of traffic transmitted after the policy was applied to the tunnel.
Drop	Displays the rate of traffic dropped after the policy was applied to the tunnel. The drop rate is the difference between post policy and pre policy transmission rates.

Monitor real time tunnel QoS statistics

Use the **Real Time** option to view QoS Statistics for each tunnel endpoint in real time.

Procedure

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

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose either of these:

- **Tunnel QoS Statistics**: Use this option to filter the tunnel endpoints.
- **Tunnel QoS Summary Statistics**: Use this option to view a summary for all tunnel endpoints.

You can view a summary for the tunnel endpoints.

Column	Description
Tunnel Endpoint	Combination of the system IP address of the selected device along with local color of the tunnel endpoint, remote IP address, remote color, and the tunnel encapsulation type.
Queued Pkts	Number of packets queued for the tunnel endpoint. When there are no drops, the queued packets and transmitted packets have the same value.
Queued Bytes	Count in bytes queued for the tunnel endpoint. When there are no drops, the queued bytes and transmitted bytes have the same value.
Tx Pkts	Number of packets transmitted through the tunnel endpoint. When there are no drops, the queued packets and transmitted packets have the same value.
Tx Bytes	Traffic (in bytes) transmitted through the tunnel endpoint. When there are no drops, the queued bytes and transmitted bytes have the same value.
Drop Pkts	Number of packets dropped during transmission.
Drop Bytes	Traffic (in bytes) dropped during transmission.
Last Updated	Timestamp when the statistics are generated on the device. These statistics are updated every 10 seconds.

Collect System Information in an Admin-Tech File

Table 18: Feature History

Feature Name	Release Information	Description
Admin-Tech Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This feature enhances the admin-tech file to include commands like **show tech-support memory**, **show policy-firewall stats platform**, **show sdwan confd-log netconf-trace** and so on in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.
Generate System Status Information for a Cisco SD-WAN Manager Cluster Using Admin Tech	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature adds support for generating an admin-tech file for a Cisco SD-WAN Manager cluster. The admin-tech file is a collection of system status information intended for use by Cisco Catalyst SD-WAN Technical Support for troubleshooting. Before this feature was introduced, Cisco Catalyst SD-WAN was only able to generate an admin-tech file for a single device.
View Generated Admin-Tech Files at Any Time	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature provides support for viewing the generated admin-tech files whenever the admin-tech files are available on a device. You can view the list of generated admin-tech files and then decide which files to copy from your device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.
Additional Diagnostics Information Added to Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enables you to upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests from Cisco SD-WAN Manager. This streamlines the steps required for working with TAC to troubleshoot a problem.

Feature Name	Release Information	Description
Generate an Admin-Tech File with the Feature Filter	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds new options for information to include in the admin-tech file. For Cisco IOS XE Catalyst SD-WAN devices, you can include information about IPsec and security policy. For Cisco Catalyst SD-WAN Control Components, you can include information about the forwarding information base and routing information base.
Include Custom CLI Command Output in an Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can include the output of specific **show** commands in an admin-tech file. This is helpful for troubleshooting.
Cellular Modem Auto-Collect Crash Data	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	You can use the **lte modem crash-action auto-collect** command to configure a router to collect essential information about cellular modem operation, ensuring that the admin-tech file contains necessary details for troubleshooting in the event of an LTE modem crash.

Information About Admin Tech for Collecting System Information

An admin-tech file is a collection of system status information used for troubleshooting a given issue. Send your Cisco SD-WAN Manager admin-tech files to Cisco Catalyst SD-WAN Technical Support to resolve your issue.

You can generate an admin-tech file for a single device or for all the nodes in a Cisco SD-WAN Manager cluster.

Note Starting from Cisco vManage Release 20.7.1, the admin-tech file includes additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.

Note The admin-tech generation fails if any malformed characters are present in the disk.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, the generation of admin tech in Cisco SD-WAN Manager fails when disk space usage exceeds the designated limits. When the total utilized space surpasses the limit, you may attempt to delete the existing admin tech data from Cisco SD-WAN Manager.

If this action is ineffective, or if there are no admin tech files available for deletion, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total utilized space at /opt/data/ remains below 80% and can attempt to delete admin tech across tenants in a multi-tenant setup.

Benefits of an Admin-Tech File for Collecting System Information

- Provides a consolidated file with system status information to submit to Cisco Catalyst SD-WAN Technical Support for diagnostics and troubleshooting.
- Provides support for directly uploading admin-tech files to Cisco Catalyst SD-WAN Technical Support

Prerequisites for Collecting System Information in an Admin-Tech File

- All of the nodes in the Cisco SD-WAN Manager cluster must be in a healthy state to generate an admin-tech file for all of the nodes in the cluster.

Restrictions for Collecting System Information in an Admin-Tech File

- All in-progress admin-tech requests are purged every three hours.
- You can have only one outstanding admin-tech request for a Cisco SD-WAN Manager cluster at a time. A second admin-tech request fails if there is an existing admin-tech request.
- Admin tech for a Cisco SD-WAN Manager cluster is successful only if admin tech is not running for individual devices.

Generate Admin-Tech Files

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. Do one of the following:
   - To generate an admin-tech file for all the nodes in a Cisco SD-WAN Manager cluster, click **Generate Admin Tech for Manager**.
   - To generate an admin-tech file for a single device, click ... adjacent to the device and choose **Generate Admin Tech for Manager**.
3. In the **Generate admin-tech File** pane, choose the content to include in the admin-tech tar file, as follows:

Field	Description
Logs	Include log files. **Note** The log files are stored in the `/harddisk/tracelogs` directory on the local device.
Core	Include core files. **Note** The core files are stored in the `/harddisk/core` directory on the local device.
Tech Features	**Note** From Cisco Catalyst SD-WAN Manager Release 20.15.1, this field is no longer available. This option is available in Cisco SD-WAN Manager Releases 20.13.x and 20.14.x. Choose additional information to include in the admin-tech file. The options depend on whether you are generating an admin-tech file for a single Cisco IOS XE SD-WAN device or for all devices and Cisco Catalyst SD-WAN Control Components. For Cisco IOS XE Catalyst SD-WAN devices: • **IPsec**: Include IPsec information. • **Security Policy**: Include security policy information. The technical information for the features is stored in a separate tech files in the folder /var/tech/ directory. By default, the admin file collects the technical information for IPsec and security features. The feature specific technical files are named as /var/tech/ipsec and /var/tech/security. For Cisco SD-WAN Control Components: • **All**: Include forward information base and route information base details. **Include fib detail**: Include forwarding information base details. **Include rib detail**: Include routing information base details.

Field	Description
Use Custom Commands	(Optional) Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 Enter **show** commands, separated by commas, to include **show** command output in the admin-tech file. The command output is available in the `/var/tech/custom` file path in the admin-tech zip file. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, some OMP and TTM commands are not supported. If you enter an unsupported command, the admin-tech file displays an error.

4. Click **Generate**.

   Cisco SD-WAN Manager creates the admin-tech file.

   The file name has the format *date-time*-admin-tech.tar.gz.

By default, the admin-tech file collects the technical information for IPsec and security features. The feature-specific technical files are named as `/var/tech/ipsec` and `/var/tech/security`.

For more information on admin-tech and technical support commands, see request admin-tech and show tech-support.

View Admin-Tech Files

You can perform any of the following operations after the admin-tech file is generated:

- View the list of the generated admin-tech files.
- Copy the selected admin-tech files from your device to Cisco SD-WAN Manager.
- Download the selected admin-tech files to your local device.
- Delete the selected admin-tech files from Cisco SD-WAN Manager, the device, or both.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **. . .** and choose **View Admin Tech List**.

   A tar file appears that contains the admin-tech contents of the device that you selected earlier. This file has a name similar to *`ip-address-hostname`*`-20210602-032523-admin-tech.tar.gz`, where the numeric fields are the date and the time.

   You can view the list of the generated admin-tech files and decide which files that you want to copy to Cisco SD-WAN Manager.
3. Click the **Copy** icon to copy the admin-tech file from the device to Cisco SD-WAN Manager.

   A hint appears letting you know that the file is being copied from the device to Cisco SD-WAN Manager.

4. After the file is copied from the device to Cisco SD-WAN Manager, you can click the **Download** icon to download the file to your local device.

   You can view the admin-tech file size after the file is copied to Cisco SD-WAN Manager.

5. After the admin-tech file is successfully copied to Cisco SD-WAN Manager, you can click the **Delete** icon and choose which files to delete from Cisco SD-WAN Manager, the device, or both.

For more information on admin tech and technical support commands, see request admin-tech and show tech-support.

Upload an Admin-Tech File to a TAC Case

From Cisco vManage Release 20.7.1, Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, and Cisco SD-WAN Release 20.7.1, you can upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case.

Before You Begin

Ensure that you have generated admin-tech files from Cisco SD-WAN Manager.

Upload an Admin-Tech File to a TAC Case

Perform the following steps to upload an admin-tech file to a TAC case:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. After you generate **Admin-Tech** files, click **Show Admin Tech List**.

   The **List of Admin-techs** window is displayed.
3. From the list of Admin-tech files, select the admin-tech file and click **Upload**.
4. In the **SR Number** and **Token** fields, enter the details.
5. Choose the **VPN** from the VPN options. The options are VPN 0 and VPN 512.
6. Click **Upload**.

   The selected admin-tech file is uploaded to the relevant service request.

Monitor Cflowd and SAIE Flows for Cisco IOS XE Catalyst SD-WAN Devices

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1

For more information on monitoring Cflowd traffic flows, see Traffic Flow Monitoring with Cflowd.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click **…** adjacent to the Cisco IOS XE Catalyst SD-WAN device name and choose **Real Time**.
3. From the **Device Options** drop-down list, choose one of the following options:
   - **cFlowd Flows/DPI**

- **cFlowd ipv6 Flows/DPI**

4. Click **Show Filters**.

   You can search for Cflowd flow records based on the selected filters.

Note The filters are displayed only if you selected one of the Cflowd flows with the DPI device options.

Table 19: Filters for Cflowd with DPI Device Options

Field	Description
VPN ID	Enter the VPN ID.
Source IP	Enter the source IPv4 or IPv6 address.
Destination IP	Enter the destination IPv4 or IPv6 address.
Application	Enter the name of the application for which you are configuring Cflowd and SAIE monitoring.
Application Family	Enter the name of the application family for which you are configuring Cflowd and SAIE monitoring.

5. Click **Search** or **Reset All** to reset all the search filters.

Reboot a Device

Use the Device Reboot screen to reboot one or more Cisco Catalyst SD-WAN devices.

Reboot Devices

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Click **WAN Edge**, **Control Components**, or **Manager** depending on the device type that you want to reboot..
3. Check the check boxes next to the device or devices that you want to reboot.
4. Click **Reboot**.

View Active Devices

To view a list of devices on which the reboot operation was performed:

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Reload a Security Application

The **Reload Services** option in the **Maintenance** > **Device Reboot** window lets you to recover a security application from an inoperative state. Ensure that you use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 110.

Ensure that a security application has already been installed on the device that you choose to reload services for. To reload one or more security applications:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Under **WAN Edge**, check the check box for the Cisco Catalyst SD-WAN device you want to choose.
3. Click **Reload Services**.

   The **Reload Container** dialog box appears.
4. If the security application version is correct, check the check box against the version of the security application.
5. Click **Reload**.

   The security application stops, is uninstalled, reinstalled, and restarted.

Reset a Security Application

The **Reset Services** option in the **Maintenance** > **Device Reboot** window enables you to recover a security application from an inoperative state.

Use the **Reset Services** option when the virtual network configuration of a security application changes, such as, the virtual port group configuration on a device.

- Ensure that a security application is already been installed on the device that you choose to reset services for.
- Ensure that the chosen security application is in a running state.

To reset one or more security applications:

1. Click **WAN Edge** and check against a Cisco Catalyst SD-WAN device to reload the security application.
2. Click **Reset Services**.

   The **Reset Container** dialog box opens.
3. If the security application version is correct, check the check box against the version of the device.
4. Click **Reset**.

   The security application is stopped, and then restarted.

Determine Security Applications in Inoperative State

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.

3. In the left pane, click **Real Time**.

   The real time device information appears in the right pane.

4. From the **Device Options** drop-down list, choose **App Hosting Details**.

   A table appears with the device-specific application hosting information. In the table, if the state of the device is ACTIVATED, DEPLOYED, or STOPPED, perform a reload or reset operation on the security application.

   If the state of the device is RUNNING, the security application is in an operative state.

5. From the **Device Options** drop-down list, choose **Security App Dataplane Global**.

   A table appears with the device-specific application data plane information. In the table, if the **SN Health** of the device is yellow or red, perform a reload or reset operation on the security application.

   If the **SN Health** of the device is green, the security application is in an operative state.

Reset Interfaces

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired template, click **…** and choose **Reset Interface**.
3. In the **Interface Reset** dialog box, choose the desired interface.
4. Click **Reset**.

Make Your Device Invalid

You can make your device invalid should your device go beyond its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Make Device Invalid**.
3. Confirm that you want to make the device invalid and click **OK**.

Bring Your Device Back to Valid State

1. From the Cisco Catalyst SD-WAN menu, choose **Configuration** > **Certificates**.
2. Choose the invalid device and look for the **Validate** column.
3. Click **Valid**.
4. Click **Send to Controllers** to complete the action.

Stop Data Traffic

You can stop data traffic to your device should your device exceed its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Stop Traffic**.
3. Confirm that you want to stop data traffic to your device and click **OK**.

Perform a Factory Reset

If your device is outside its target boundary, you may need to perform a factory reset of your device.

Note The **Factory Reset** operational command is supported only for Cisco ISR 1000 series and Catalyst 8K devices.

For more information on geofencing, see the *Cisco IOS XE Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Factory Reset**.
3. Choose one of the following options:
   - **Retain License**: Wipes all the device settings and partitions except for licenses. **Retain License** is a sub option to the factory-reset option.
   - **Full Wipe** factory-reset: Wipes all the device settings and partitions.

Note After a full-wipe operation, the device can only be booted up using a USB or TFTP.

4. Click **Reset**.

Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

Table 20: Feature History

Feature Name	Release Information	Description
Resource Monitoring on Cisco SD-WAN Controllers and Cisco vEdge Devices	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	With this feature, you can configure usage watermarks for resources such as CPU, memory, and disk on Cisco SD-WAN controllers and Cisco vEdge devices. In addition, in Cisco SD-WAN Manager servers, you can configure watermarks to monitor disk read and write speeds. Devices poll the resource usage and notify events to Cisco SD-WAN Manager. Cisco SD-WAN Manager raises alarms to alert you about changes in resource usage, or disk read or write speed so that you can take the necessary corrective action.

Information About Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

Note Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, there have been changes in how CPU utilization is calculated and reported on Cisco IOS XE Catalyst SD-WAN devices.

Before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1: CPU utilization was calculated as an average across all CPU cores (Control Plane, Data Plane, and Service Plane).

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, CPU utilization is calculated and reported based solely on the control plane CPU cores. This CPU utilization can be viewed from the **System Status** option in Cisco SD-WAN Manager. See View Device System Resource Utilization in Cisco SD-WAN Manager.

Additionally, this updated CPU utilization information is also available using the **show sdwan system status** and **show processes cpu platform profile CP** CLI commands. See show sdwan system status, show processes cpu platform.

Cisco SD-WAN Release 20.7.1and Cisco vManage Release 20.7.1 introduce a Monit-utility-based workflow for monitoring the usage of the CPU, memory, and disk on Cisco SD-WAN Control Components and Cisco

vEdge devices. While Cisco SD-WAN Release 20.6.x and earlier releases, and Cisco vManage Release 20.6.x and earlier releases allowed the monitoring of how these resources are being used, the monitoring and reporting was based on predefined watermarks and a default polling interval. From Cisco SD-WAN Release 20.7.1 and Cisco vManage Release 20.7.1, you can customize the watermarks and the polling interval as appropriate to the resources in your deployment.

To monitor the usage of the CPU, memory, and disk, you can configure high-usage, medium-usage, and low-usage watermarks, and how frequently a device must check and report resource usage to Cisco SD-WAN Manager. In addition, you can monitor the disk read and write speeds on Cisco SD-WAN Manager servers by configuring appropriate read and write watermarks and the polling interval. You can use CLI templates or log in to the device CLI to configure custom watermarks and polling intervals for various devices and control components, as necessary.

Default Configuration

Devices and control components have a default configuration for the usage watermarks and the polling interval for monitoring the CPU, memory, and disk usage:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

The disk read and write speeds on Cisco SD-WAN Manager do not have a default configuration and are only monitored after you configure the necessary watermarks and polling interval.

Polling, Events, and Alarms

Based on the configuration, the device or controller polls the resource usage through monit and notifies events based on the polled usage information to Cisco SD-WAN Manager. Cisco SD-WAN Manager compares the event information with the event information received for the previous polling interval. If Cisco SD-WAN Manager detects a change in resource usage, it raises an appropriate alarm.

Devices and control components notify the following events to Cisco SD-WAN Manager:

- CPU usage
- Disk Usage
- Memory Usage
- Disk read speed (Cisco SD-WAN Manager only)
- Disk write speed (Cisco SD-WAN Manager only)

The event notifications have the following severity and status based on how the polled usage value compares with the configured watermarks:

Comparison	Severity	Status
Above the high watermark	Critical	usage-critical
Between the medium and high watermarks	Major	usage-warning
Between the low and medium watermarks	Minor	usage-notice

Below the low watermark	Minor	usage-healthy

For more information on viewing and managing events, see Events.

Based on the events, Cisco SD-WAN Manager can raise the following types of alarms:

- CPU Usage
- Disk Usage
- Memory Usage
- Disk Read Speed (Cisco SD-WAN Manager only)
- Disk Write Speed (Cisco SD-WAN Manager only)

The alarms map to the event status and severity as follows:

Alarm	Severity	Status
Critical (Red)	Critical	usage-critical
Major (Orange)	Major	usage-warning
Minor (Yellow)	Minor	usage-notice
Minor (Green)	Minor	usage-healthy

- Initially, Cisco SD-WAN Manager raises an alarm when the event status is other than usage-healthy, indicating excessive resource usage.
- If a subsequent event has the same status as the event Cisco SD-WAN Manager received previously, the alarm remains unchanged.
- If a subsequent event is of lesser severity and indicates a healthier usage status, Cisco SD-WAN Manager raises an appropriate alarm. The new alarm clears the earlier higher-severity alarm.
- Cisco SD-WAN Manager raises the Minor (Green) alarm only when the resource usage returns from a more severe state to the usage-healthy state. The Minor (Green) alarm indicates that the resource usage has returned to a normal level from an earlier excessive level.

For more information on viewing and managing alarms, see Alarms.

Supported Devices for Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

- Cisco SD-WAN Manager server running Cisco vManage Release 20.7.1 or later
- Cisco SD-WAN Controller running Cisco SD-WAN Release 20.7.1 or later
- Cisco SD-WAN Validator running Cisco SD-WAN Release 20.7.1 or later
- Cisco vEdge devices running Cisco SD-WAN Release 20.7.1 or later

Configure Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI

You can configure the resource monitoring watermarks and polling interval using CLI commands in a CLI template.

This section provides sample CLI configurations to configure the watermarks and polling interval for resource monitoring.

Configure CPU Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage percentage
Device(config-cpu-usage)# medium-watermark-percentage percentage
Device(config-cpu-usage)# low-watermark-percentage percentage
Device(config-cpu-usage)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage 80
Device(config-cpu-usage)# medium-watermark-percentage 70
Device(config-cpu-usage)# low-watermark-percentage 50
Device(config-cpu-usage)# interval 10
```

Configure Memory Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage percentage
Device(config-memory-usage)# medium-watermark-percentage percentage
Device(config-memory-usage)# low-watermark-percentage percentage
Device(config-memory-usage)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage 80
Device(config-memory-usage)# medium-watermark-percentage 70
Device(config-memory-usage)# low-watermark-percentage 50
Device(config-memory-usage)# interval 10
```

Configure Disk Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage file-system-path
Device(config-disk-usage-/opt/data)# high-watermark-percentage percentage
```

```
Device(config-disk-usage-/opt/data)# medium-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# low-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage /opt/data
Device(config-disk-usage-/opt/data)# high-watermark-percentage 80
Device(config-disk-usage-/opt/data)# medium-watermark-percentage 70
Device(config-disk-usage-/opt/data)# low-watermark-percentage 50
Device(config-disk-usage-/opt/data)# interval 10
```

Configure Disk IO Speed Watermarks and Polling Interval on Cisco SD-WAN Manager

```
sd-wan-manager# config
sd-wan-manager(config)# system
sd-wan-manager(config-system)# alarms
sd-wan-manager(config-alarms)# disk-speed disk-partition
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps
speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps
speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval seconds
```

Example:

```
vManage# config
sd-wan-manager(config)# system
sd-wan-manager(config-system)# alarms
sd-wan-manager(config-alarms)# disk-speed /dev/nvme1n1
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps 1000
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps 500
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps 100
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps 1000
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps 500
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps 100
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval 100
```

Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI

Verify Configuration of CPU Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms cpu-usage** command and shows the configured CPU usage watermarks and the polling interval:

```
Device# show alarms cpu-usage

            HIGH        MEDIUM      LOW
            WATERMARK   WATERMARK   WATERMARK
CPU USAGE   PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-------------------------------------------------------------------
cpu-usage   80          70          50          10
```

Verify Configuration of Memory Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms memory-usage** command and shows the configured memory usage watermarks and the polling interval:

```
Device# show alarms memory-usage

              HIGH         MEDIUM       LOW
              WATERMARK    WATERMARK    WATERMARK
MEMORY USAGE  PERCENTAGE   PERCENTAGE   PERCENTAGE   INTERVAL
-----------------------------------------------------------------
memory-usage  80           70           50           10
```

Verify Configuration of Disk Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms disk-usage** command and shows the configured disk usage watermarks and the polling interval:

```
Device# show alarms disk-usage

             HIGH          MEDIUM        LOW
FILESYSTEM   WATERMARK     WATERMARK     WATERMARK
PATH         PERCENTAGE    PERCENTAGE    PERCENTAGE   INTERVAL
-----------------------------------------------------------------------
/rootfs.rw    90            75            60           5
/tmp          90            75            60           5
/opt/data     80            70            50           10
```

Verify Configuration of Disk IO Speed Watermarks and Polling Interval

The following is a sample output of the **show alarms disk-speed** command and shows the configured disk IO speed watermarks and the polling interval:

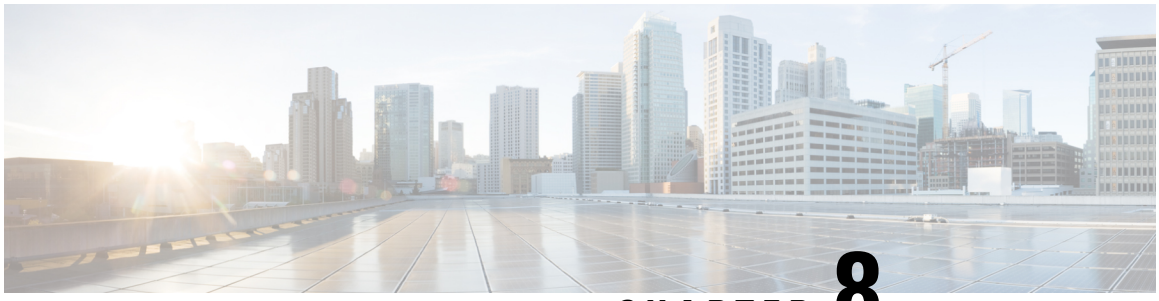
```
sd-wan-manage# show alarms disk-speed

                      READ                    WRITE       WRITE
            READ HIGH MEDIUM      READ LOW    HIGH        MEDIUM      WRITE LOW
            WATERMARK WATERMARK   WATERMARK   WATERMARK   WATERMARK   WATERMARK
DISK PATH   K BPS     K BPS       K BPS       K BPS       K BPS       K BPS       INTERVAL
-------------------------------------------------------------------------------------------
/dev/sda2   1000      500         100         1000        500         100         100
```

View Event Notifications on a Device

The following is a sample output of the **show notification stream viptela** command and shows a CPU usage event:

```
sd-wan-manager# show notification stream viptela
notification
 eventTime 2021-09-08T02:57:14.91578+00:00
 cpu-usage
  severity-level minor
  host-name vm12
  system-ip 172.16.255.22
  cpu-status usage-notice
  warning System CPU usage is above 50%
  cpu-user-percentage 40.9
  cpu-system-percentage 10.6
  cpu-idle-percentage 48.50
 !
!
```



CHAPTER 8

Hosted edge services

Table 21: Feature history

Feature name	Release information	Description
Hosted edge services	Cisco Catalyst SD-WAN Manager Release 20.18.1	You can monitor hosted edge services (IOx applications) for health, associated devices, version, and IOx state using the Cisco Catalyst SD-WAN Manager interface.You can also start or stop the hosted edge services.

- Hosted edge services, on page 119
- Restrictions for monitoring hosted edge services, on page 119
- Start or stop the hosted edge services, on page 120
- Monitor the hosted edge services, on page 120

Hosted edge services

Hosted edge services are Cisco IOx applications installed on WAN edge devices, improving their features and functionality beyond the core Cisco IOS XE Catalyst SD-WAN software. Cisco IOx applications can include both Cisco and third-party applications. Using Cisco SD-WAN Manager, you can

- monitor all hosted edge services installed on your edge devices for resource usage, device details, version, and more, and
- manage hosted edge services installed on your devices.

Restrictions for monitoring hosted edge services

Disk space calculation

If multiple hosted edge services are running on a device using any version older than Cisco IOS XE Catalyst SD-WAN Release 17.18.x, the disk space usage for some hosted edge services may not reflect correctly.

Upgrade to the latest version of Cisco IOS XE Catalyst SD-WAN Release 17.18.x to ensure proper disk space usage calculation.

Multitenancy

In a multitenant environment, you can monitor hosted edge services only at the tenant level and not at the provider level.

Start or stop the hosted edge services

Control the operation of the edge service installed on the device using these steps in SD-WAN Manager.

Before you begin

- Deploy a hosted edge service to one or more devices in the network and activate it. See the configuration instructions in Cisco Catalyst SD-WAN Integrations guide.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Hosted Edge Services**.

Step 2 Select a hosted edge service.

The page shows devices running the selected hosted edge service.

Alternatively, to manage the hosted edge service from the **Devices** page, use these steps:

a) From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
b) Select a device from the list.
c) Click **App Status Info** to view hosted edge services associated with the device.

Step 3 To start or stop a hosted edge service, click **…** adjacent to the device and select **Start edge service** or **Stop edge service**.

Note
You can stop a hosted edge service only if it is in **Running** state. Similarly, you can start a hosted edge service if it is in **Stopped** state. You cannot perform any operation on the hosted edge service if it is in **Deployed** or **Activated** state.

After the device metrics are refreshed, the **Edge service state** column shows the current state of the edge service.

Monitor the hosted edge services

Monitor the devices running hosted edge services, their resource usage, status of the hosted edge services on individual devices, and so on.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Hosted Edge Services**.

The hosted edge services view includes:

Table 22: Hosted edge services

Field	Description
Hosted edge service name	Name of the hosted edge service installed on your edge device to provide additional features.
Edge service author	Name of the organization that developed this edge service.
Number of sites installed	Total number of sites where the hosted edge service is currently installed.
Number of devices installed	Total number of edge devices on which the hosted edge service is installed.

Step 2 To monitor the hosted edge services on specific devices, use these steps:

a) From the **Hosted Edge Services** page, select a hosted edge service name.

The page shows the devices running the selected hosted edge service.

Table 23: IOx states and device details

Field	Description
IOx states	IOx states are hosted edge service states that indicate whether the service is operational. • **Stopped**: Indicates the hosted edge service has stopped and is no longer operational on the device. • **Running**: Indicates the hosted edge service is accessible and operational on the device. • **Deployed**: Indicates the hosted edge service is deployed to the device and the installation is successful. • **Activated**: Indicates the network configurations are successfully added to the hosted edge services and the application is now active. Click any state to filter the network devices as per the state of the hosted edge service.
Network device	Name of the network device on which the selected instance of hosted edge service is running.
Site name	Logical identifier that represents the operational grouping of the network device within the Cisco SD-WAN environment.

Field	Description
Resource usage health	Resource consumed by the hosted edge services. For a hosted edge service, the health status indicates: • **Good**: The hosted edge service's CPU, memory, or disk space resource usage is less than 50 percent of the allocated resources. • **Fair**: The hosted edge service's CPU, memory, or disk space resource usage lies between 50 and 75 percent of the allocated resources. • **Poor**: The hosted edge service's CPU, memory, or disk space resource usage is greater than 75 percent of the allocated resources. This reflects only the resource usage by the service. It does not reflect the total resource usage of the device.
Edge service state	Displays the IOx state of the hosted edge service: stopped, running, deployed, or activated.
Edge service version	The IOx application version running on the device, as defined in the package.yaml file.
Last update	Displays the latest timestamp when the device metrics were updated.

b) For a selected network device, click **...** and select **View edge service info**.

The drawer shows this information:

- **Resource usage**: Current health status along with resource consumption of CPU, RAM, and disk space.
- **Edge service details**: Current IOx state, hosted edge service version, and last data fetch details. Use the **Stop edge service** option to stop the hosted edge service instance on the device. Click **Refresh device metrics** to manually update the device metrics for the selected device.
- **Package information**: Hosted edge service name, CPU architecture, and author information.

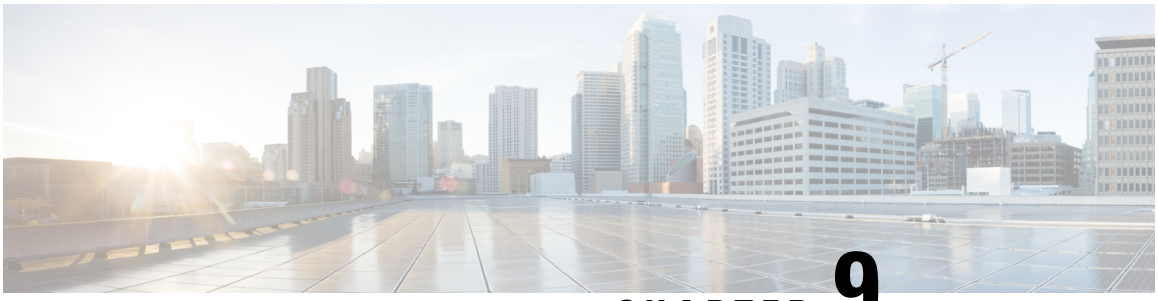
Step 3 To monitor the hosted edge services on a specific device from the **Devices** page, use these steps:

a) From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
b) Select a device from the list.
c) Click **App Status Info**.

The page shows the hosted edge services running on the device.

Field	Description
Edge service name	Name of the IOx application hosted on the device.
Edge service author	Name of the organization that developed the edge service.
Edge service version	The IOx application version running on the device as defined in the package.yaml file.

Field	Description
Resource usage health	Resource consumed by the hosted edge services. For a hosted edge service, the health status indicates: • **Good**: The hosted edge service's CPU, memory, or disk space resource usage is less than 50 percent of the allocated resources. • **Fair**: The hosted edge service's CPU, memory, or disk space resource usage lies between 50 and 75 percent of the allocated resources. • **Poor**: The hosted edge service's CPU, memory, or disk space resource usage is greater than 75 percent of the allocated resources. This reflects only the resource usage by the service. It does not reflect the total resource usage of the device. You can also view the health using the **Edge service resource usage health** column on the **Devices** page for all devices that have any hosted edge service.
Edge service state	Displays the IOx state of the hosted edge service: Stopped, Running, Deployed, or Activated.
CPU usage	Displays CPU resource usage in percentage.
Disk space usage	Displays disk space usage in percentage.
Memory usage	Displays memory usage in percentage.



CHAPTER 9

Network

Table 24: Feature History

Feature Name	Release Information	Description
Another Real Time Monitoring Support for Routing, License, Policy, and Other Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature adds support for real-time monitoring of numerous device configuration details, including routing, policy, Cloud Express, Cisco SD-WAN Validator, TCP optimization, SFP, tunnel connection, license, logging, and Cisco Umbrella information. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device. There are many device configuration details for Cisco SD-WAN Manager. However, only a subset of the device configuration details are added in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	This feature adds support for real-time monitoring for AppQoE and other device configuration details. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device.

Feature Name	Release Information	Description
Download Output of OMP Routes	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can download the output of the OMP Received Routes or OMP Advertised Routes real-time data for Cisco IOS XE Catalyst SD-WAN devices.
View Tunnel Health on Multiple Remote Devices and Circuits	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature, add multiple remote devices and circuits to view the tunnel health data in the line chart. You can add a maximum of five devices at a time and the tunnel health data is displayed for each path.

- View AppQoE Information, on page 127
- View a Configuration Commit List, on page 127
- Determine the Status of Network Sites, on page 128
- View Network Site Topology, on page 129
- Data Collection and Cisco Catalyst SD-WAN Telemetry, on page 131
- Rediscover Network, on page 135
- View Routing Information, on page 135
- View Multicast Information, on page 137
- View Data Policies, on page 138
- BFD Protocol, on page 139
- View BFD Session Information, on page 141
- View BGP Information, on page 142
- View Cflowd Information, on page 142
- View Cloud Express Information, on page 144
- View ARP Table Entries, on page 144
- Run Site-to-Site Speed Test, on page 145
- View Network-Wide Path Insight, on page 145
- View NMS Server Status, on page 146
- View Cisco Catalyst SD-WAN Validator Information, on page 146
- Run a Traceroute, on page 147
- View Tunnel Loss Statistics, on page 148
- View SAIE Flows, on page 148
- View VNF Status, on page 150
- View TCP Optimization Information, on page 150
- View SFP Information, on page 152
- Monitor NAT DIA Tracker Configuration on IPv4 Interfaces, on page 152
- View TLOC Loss, Latency, and Jitter Information, on page 153
- View Tunnel Connections, on page 154
- View License Information, on page 157
- View Logging Information, on page 157

- View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels, on page 158
- View WiFi Configuration, on page 159
- View Control Connections in Real Time, on page 159
- View Cisco Umbrella Information, on page 160
- View VRRP Information, on page 160
- View PKI Trustpoint Information, on page 160
- View QoS Information, on page 161
- View WLAN Output, on page 163
- View Client Details, on page 163
- Check Traffic Health, on page 164
- Capture Packets, on page 166
- Simulate Flows, on page 169
- Security Monitoring, on page 171
- View the System Clock, on page 172

View AppQoE Information

Minimum release: Cisco vManage Release 20.9.1

To view AppQoE information on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one the following commands:

Device Option	Command	Description
AppQoE Active Flow Details	show sdwan appqoe flow flow-id [flow_id]	Displays the details of a single specific flow.
AppQoE Expired Flows Summary	show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows.
AppQoE Active Flows Summary	show sdwan appqoe flow vpn-id [vpn_id] server-port [server_port]	Displays flows for a specific VPN.
AppQoE Expired Flow Details	show sdwan appqoe flow closed flow-id [flow_id]	Displays the AppQoE Expired Flow details for a single specific flow.

View a Configuration Commit List

Minimum release: Cisco vManage Release 20.9.1

To view a configuration commit list on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose the following command:

Device Option	Command	Description
Configuration Commit List	show configuration commit list	Displays the configuration commit list.

Determine the Status of Network Sites

A site is a particular physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each device at a site is identified by the same site ID.

To determine the status of network sites:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. Locate the **Site BFD Connectivity** dashlet, which displays the state of data connections of a site. When a site has multiple edge devices, this dashlet displays the state of the entire site and not for individual devices. The **Site BFD Connectivity** dashlet displays three states:

   - Full WAN Connectivity: Total number of sites where all BFD sessions on all devices are in the up state.
   - Partial WAN Connectivity: Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
   - No WAN Connectivity: Total number of sites where all BFD sessions on all devices are in the down state. These sites have no data plane connectivity.

   Click any of these to view more details. The details are displayed in a pop-up window.
3. For the desired row, click **...** and choose **Device Dashboard**, **SSH Terminal**, or **Real Time**. You will be redirected to the appropriate window based on your selection.

View Network Site Topology

Table 25: Feature History

Feature Name	Release Information	Description
Site Topology Visualization in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can now view the topology diagram of a site in Cisco SD-WAN Manager.
Site Topology Visualization in Cisco SD-WAN Manager (Phase II)	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature supports enhanced, interactive visualization of site topology, providing information about the health of devices and tunnels in the topology. It provides you with an improved monitoring and troubleshooting experience.

Information About Site Topology

Cisco SD-WAN Manager generates a topology diagram for each site featuring the Cisco IOS XE Catalyst SD-WAN devices that are deployed in a configuration group. For more information on configuration groups, see Configuration Groups and Feature Profiles.

This topology diagram displays the following information:

- Device information: The topology diagram displays all the devices that are deployed at a selected site. It displays the model and health status of each device. When you place the cursor over a device name, you can view the hostname and the system IP address of that device. Similarly, when you click a device name, you can view detailed information about the device in the right navigation pane. From this pane, you can navigate to the device dashboard to view more details.

  In Cisco vManage Release 20.8.1, the topology diagram displays only the model and the system IP address of a device.

- Transport information: The topology diagram displays VPN 0 and all the transport interfaces that are connected to a device, including details of the interface and the protocol. When you place the cursor over a transport interface name, you can view the average upstream and downstream speed in the last three hours.

- Service VPN information: The topology diagram displays the ID and name of the service VPNs. When you click the drop-down arrow adjacent to the name of a service VPN, you can view the protocol, the interfaces, and the average upstream and downstream speed in the last three hours.

  The topology diagram displays a maximum of 12 service VPNs. If there are more than 12 service VPNs, click the **More** button to see the complete list of service VPNs in the right navigation pane.

- Circuit health information: The color of the link between the circuit and the transport interface indicates the circuit health.

- If one site ID changed (for example, 100 to 200), you will see both 100 and 200 on the site topology view. The old site 100 will disappear after around 30mins.
- The global topology uses sites data from the site table API. The site table shows only the edge information. So if the Cisco SD-WAN Manager site ID is not same with any of the edge devices, then you'll not see the data for all the sites.

Note

- If a Cisco IOS XE Catalyst SD-WAN device is associated with a configuration group, but the device is not deployed, the topology diagram displays only the hostname and the system IP.

  However, if a device is associated with a configuration group and the device is also deployed, the topology diagram displays complete details of the device, including LAN and WAN details.
- If a site has devices that are not associated with a configuration group, the topology diagram displays the standalone devices with only the hostname and the system IP.
- There is no limit on the number of devices shown in the topology diagram for each site. However, if there are multiple devices in a site, the connections between the devices are not shown.
- Adjust the zoom level of the topology diagram by clicking the zoom-in and zoom-out icons. Similarly, you can view the topology diagram in a full screen by clicking the full-screen icon.
- Click the refresh icon to regenerate the topology diagram and view the latest data.
- View the details of the health metrics by clicking the legend ( ) icon.

Supported Devices for Site Topology Visualization

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

Prerequisites for Site Topology Visualization

- The device must be deployed to a configuration group.
- You must have role-based access control (RBAC) for the Device Monitoring feature.

View Network Site Topology

You have the following options to view the topology of a site.

Use the Devices Window

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Find the corresponding Cisco IOS XE Catalyst SD-WAN device in the table and click the value in the **Site ID** column adjacent to this device name.

   Alternatively, click the device name in the **Hostname** column, and then click the **Site ID** value in the device dashboard.

Cisco SD-WAN Manager displays the topology of the site.

Use the Geography Window

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click the corresponding Cisco IOS XE Catalyst SD-WAN device in the map.
3. Click the **Site ID** value.

Cisco SD-WAN Manager displays the topology of the site.

Data Collection and Cisco Catalyst SD-WAN Telemetry

Table 26: Feature History

Feature Name	Release Information	Description
Manage Data Collection for Cisco Catalyst SD-WAN Telemetry	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature allows you to disable data collection for Cisco Catalyst SD-WAN telemetry using Cisco SD-WAN Manager. Data collection for telemetry is enabled by default.

Information About Data Collection and Cisco Catalyst SD-WAN Telemetry

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

Network & Statistics Collection

Network and Statistics Collection is a feature in Cisco SD-WAN Manager that allows for the gathering of operational data from network devices, particularly Cisco IOS XE Catalyst SD-WAN devices. This data collection is typically initiated by network events, such as network connectivity issues or network flaps, which can affect connection stability across the network. This feature can be enabled or disabled according to your needs.

Additionally, you can customize the interval for device statistics collection. To do so, enter the desired interval (in minutes) in the **Collection Interval** field, which determines how frequently statistics are collected.

From Cisco Catalyst SD-WAN Manager Release 20.14.1, the **Data Collection** tab has been renamed to the **Data Collection & Statistics**, and relocated to **Administration** > **Settings** > **Network Statistics Configuration and Collection**. For more information, see Enable or Disable Data Collection, on page 133

SD-WAN Telemetry

SD-WAN Telemetry Data Collection is a feature in Cisco SD-WAN Manager that provides the capability to gather detailed telemetry information from the network's control components and network infrastructure. This feature is enabled by default when cloud services is enabled for Cisco Catalyst SD-WAN. For Cisco-provided cloud-hosted control components, this option is enabled at the time of provisioning the control components. For more information, see Enable or Disable Cisco Catalyst SD-WAN Telemetry, on page 132.



Note To collect BFD loss, latency, and jitter metrics from Cisco IOS XE Catalyst SD-WAN devices operating in controller mode, use one of the following supported methods:

- Cisco SD-WAN Manager REST APIs
- Simple Network Management Protocol (SNMP), with limited data availability
- Flexible NetFlow (FNF)

From Cisco vManage Release 20.6.1, the option to enable or disable data collection for Cisco Catalyst SD-WAN telemetry Cisco SD-WAN Manager can be found under **Administration** > **Settings** > **Data Collection**.

Before Cisco vManage Release 20.6.1, the **Data Collection** tab only had the option to enable or disable data collection, and not data collection for Cisco Catalyst SD-WAN telemetry.

From Cisco Catalyst SD-WAN Manager Release 20.14.1, the option to enable or disable data collection for Cisco Catalyst SD-WAN telemetry can be found under **Administration** > **Settings** > **Cloud Services** > **Terms & Conditions**.

Enable or Disable Cisco Catalyst SD-WAN Telemetry

Before You Begin

The Cloud Services feature must be enabled. See the following Cisco Catalyst SD-WAN scenarios:

- Cisco cloud-hosted scenario: The Cloud Services feature is enabled by default. For information about enabling or disabling, see Enable or Disable Cloud Services, on page 133.
- On-premises installation: The Cloud Services feature is disabled by default. For information about enabling or disabling, see Enable or Disable Cloud Services, on page 133.

Enable or Disable Cisco Catalyst SD-WAN Telemetry

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Cloud Services** and click the **Terms & Conditions** tab.

   (For Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, locate the **Data Collection** option and click **Edit**.)
3. SD-WAN telemetry involves the gathering of network performance data for monitoring and optimizing the network, with two available data collection options that can be enabled or disabled as needed:

- **SD-WAN Telemetry Basic**: By default this option is enabled if cloud services is enabled for Cisco Catalyst SD-WAN. This option enables Cisco SD-WAN Manager to collect telemetry data from the control components and the network.
- **SD-WAN Telemetry Advanced**: By default this option is enabled if cloud services is enabled for Cisco Catalyst SD-WAN. This option provides information about activated features and capabilities within the network. Cisco SD-WAN Manager anonymizes the data and does not send any sensitive information about the overlay to Data Collection Service (DCS).

(Cisco Catalyst SD-WAN Manager Release 20.12.2 only) To enable or disable advanced data telemetry collection, locate the **Advance Data Collection** option, click **Edit**, and enable or disable the option.

4. Click **Save**.

Enable or Disable Data Collection

To enable or disable the collection of operational data from network devices, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Network Statistics Configuration and Collection**.

   Before Cisco Catalyst SD-WAN Manager Release 20.14.1, the **Data Collection & Statistics** tab was referred as **Data Collection** and found under **Administration** > **Settings** > **Cloud Services**.

   (For Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, locate the **Data Collection** option and click **Edit**.)

2. In the **Collection Interval** field, you can set the frequency at which device statistics must be collected, such as interface statistics or application flow data. Enter a time (in minutes), which determines how frequently statistics are collected.

3. Enable or disable the **Additional Event Collection** option.

   This option allows for the gathering of operational data from network devices, particularly Cisco IOS XE Catalyst SD-WAN devices, When enabled, it facilitates the collection of operational data triggered by network events like connectivity problems or network flaps. This feature can be enabled or disabled according to your needs.

4. Click **Save**.



Note All platforms support this functionality with up to 250 interfaces configured. The recommended maximum number of interfaces to enable one-minute statistics collection for interface statistics is 250.

Enable or Disable Cloud Services

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

2. Click **Cloud Services**.

   (For Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, locate **Cloud Services** and click **Edit**.)

3. Enable or disable the **Cloud Services** option.

   (For Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, click **Enabled**.)

4. When enabling, do one of the following to authenticate:

   - Cisco Catalyst SD-WAN Manager Release 20.12.1 and later, and Cisco vManage Release 20.9.4 and later releases of 20.9.x:

     a. Enter your smart account credentials: user ID and password.

     b. Analytics is enabled by default. Use this option to disable or enable Cisco Catalyst SD-WAN Analytics.

   - Cisco vManage Release 20.11.x and earlier:

     a. Enter the OTP value. You can request the token from the Cisco CloudOps team by opening a Cisco TAC Support case.

     b. Leave the Cloud Gateway URL field blank.

     c. Approve permission to begin data collection and to upload the data to the cloud.

5. Click **Save**.

Additional Steps to Enable Data Collection on an On-Premises Cisco Catalyst SD-WAN Manager Instance

Configure the local firewall to allow outbound communication from Cisco SD-WAN Manager (interface VPN 0) on port 443 to the destinations in the following table. Choose the appropriate set of destinations based on the geographic location of your Cisco SD-WAN Analytics instance.

Location	Destinations
Americas	https://us-west.dcs.viptela.net (Cisco vManage 20.1.1 or earlier) https://us01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)
Americas (East)	https://us-east.dcs.viptela.net (Cisco vManage 20.1.1 or earlier) https://us02.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)

Europe	https://europe.dcs.viptela.net (Cisco vManage 20.1.1 or earlier) https://eu01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)
Australia	https://au01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)

You can use the cURL -k command from your Cisco SD-WAN Manager CLI to verify reachability to these destinations.

Rediscover Network

Use the **Rediscover Network** window to locate new devices in the overlay network and synchronize them with Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Rediscover Network**.
2. Choose a device or devices by checking the check box next to the device model. To find the device you are looking for scroll through the device table. Alternatively, choose a device group from the **Device Groups** drop-down list to see devices that belong to a specific device group.
3. To confirm resynchronization of the device data, click **Rediscover**.
4. In the **Rediscover Network** dialog box, click **Rediscover**.

View Routing Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands as relevant:

Device Options	Command	Description
IP Routes	show ip routes show ipv6 routes	Displays information about the IP route table entries. Displays the IPv6 entries in the local route table.

Device Options	Command	Description
IP FIB	show ip fib show ipv6 fib	Displays information about forwarding table entries. Display the IPv6 entries in the local forwarding table.
IP MFIB Summary	show ip mfib summary	Displays information about a summary of active entries in the multicast FIB.
IP MFIB OIL	show ip mfib oil	Displays information about outgoing Interfaces from the multicast FIB.
IP MFIB Statistics	show ip mfib stats	Displays information about statistics for active entries in the multicast FIB.
OMP Peers	show omp peers	Displays OMP peers and their peering sessions.
OMP Summary	show omp summary	Displays information about the OMP sessions running between Cisco SD-WAN Controller and the routers.
OMP Received Routes or OMP Advertised Routes	show omp routes show sdwan omp routes	Displays OMP routes. From Cisco vManage Release 20.11.1, you can download OMP route details in JSON or CSV formats for Cisco IOS XE Catalyst SD-WAN devices.
OMP Received TLOCs or OMP Advertised TLOCs	show omp tlocs	Displays OMP TLOCs.
OSPF Interfaces	show ospf interface	Displays information about the Interfaces running OSPF.
OSPF Neighbors	show ospf neighbor	Displays information about the OSPF neighbors.
OSPF Routes	show ospf routes	Displays routes learned from OSPF.
OSPF Database Summary	show ospf database-summary	Displays a summary of the OSPF link-state database entries.
OSPF Database	show ospf database	Displays information about the OSPF link-state database entries.

Device Options	Command	Description
OSPF External Database	Not applicable	Display OSPF external routes. External routes are OSPF routes that are not within the OSPF AS (domain).
OSPF Processes	show ospf process	Display the OSPF processes.
PIM Interfaces	show pim interface	Displays information about interfaces running PIM.
PIM Neighbors	show pim neighbor	Displays information about PIM neighbors.
PIM Statistics	show pim statistics	Displays information about PIM-related statistics.
Interface Detail	show ipv6 interface	Displays information about IPv6 interfaces on Cisco Cisco IOS XE Catalyst SD-WAN devices. From Cisco vManage Release 20.6.1, this device option is available on all Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

View Multicast Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that displays.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands as relevant:

Device Option	Command	Description
Multicast Topology	show multicast topology	View topology information about the Multicast Domain
OMP Multicast Advertised Autodiscover or OMP Multicast Received Autodiscover	show omp multicast multicast-auto-discover	View peers that support Multicast
Multicast Tunnels	show multicast tunnel	View information about IPsec tunnels between Multicast peers

Device Option	Command	Description
Multicast RPF	show multicast rpf	View Multicast reverse-path forwarding information
Multicast Replicator	show multicast replicator	View Multicast replicators
OMP Multicast Advertised Routes or OMP Multicast Received Routes	show omp multicast-routes	View Multicast routes that OMP has learned from PIM join messages

View Data Policies

A centralized data policy is configured and applied on Cisco SD-WAN Controllers, and is then carried in OMP updates to the edge devices in the site-list that the policy is applied to. Centralized data policy examines fields in the headers of data packets, looking at the source and destination addresses and ports, and the protocol and DSCP values, and for matching packets, it modifies the next hop in a variety of ways or applies a policer to the packets. The policy match operation and any resultant actions are performed on the router as it transmits or receives data traffic.

Localized data policy, also called access lists (ACLs), is configured directly on a local router and affects data traffic being transmitted between the routers on the Cisco Catalyst SD-WAN overlay network.

To view ACL information on a router, do the following:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that appears.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:

Command	Description
show policy access-list-names	View names of configured ACLs
show policy access-list-associations	View Interfaces to which ACLs are applied
show policy access-list-associations	View count of packets affected by ACLs

View Cisco Catalyst SD-WAN Controller Policy

To view policy information from Cisco Catalyst SD-WAN Controller on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that appears.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:

Device Option	Command	Description
Policy from vSmart	show policy from-vsmart show sdwan policy from-vsmart	Displays a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco Catalyst SD-WAN Controller has pushed to the Edge devices.

View Policy Zone-Based Firewall

To view policy information about zone-based firewalls on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands as relevant:

Device Option	CLI Command	Description
Policy Zone Based Firewall Statistics	`show policy zbfw filter-statistics`	Displays a count of the packets that match a zone-based firewall's match criteria and the number of bytes that match the criteria.
Policy Zone Pair Sessions	`show policy zbfw sessions`	Displays the session flow information for all zone pairs that are configured with a zone- based firewall policy.

BFD Protocol

The Role of BFD in Cisco Catalyst SD-WAN Solution

The BFD protocol detects links failures between routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.

For data plane resiliency, the Cisco Catalyst SD-WAN software implements the BFD protocol, which runs automatically on the secure IPsec and GRE connections between routers. These connections are used for the data plane, and for data traffic, and are independent of the DTLS tunnels used by the control plane.

BFD is enabled by default on all connections between Cisco vEdge devices. You cannot disable BFD. However, you can adjust the Hello packet and dead time intervals. If the timers on the two ends of a BFD link are different, BFD negotiates between the two devices and determines the transmission rate by the slower (higher) value of the two systems. See Configure BFD using Cisco SD-WAN Manager for information on configuring BFD for application-aware routing and configuring BFD on transport tunnels.

How BFD Works

After a Cisco vEdge device comes up and control connections are established, the Cisco Catalyst SD-WAN Controller advertises peer TLOC information to the Cisco vEdge device. Based on this TLOC information and other configuration, Cisco vEdge devices establish BFD sessions with all or some of the peer TLOCs.

BFD sends Hello packets periodically (by default, every 1 second) to determine whether the session is still operational. If a certain number of the Hello packets are not received, BFD considers that the link has failed and brings the BFD session down (the default multiplier time is 7 seconds). When BFD sessions goes down, any route that points to a next hop over that IPsec tunnel is removed from the forwarding table (FIB), but it is still present in the route table (RIB).

Interpret BFD States to Troubleshoot Connection Loss Between TLOCs

If a BFD session is down, it implies that no traffic can flow between those tlocs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the show bfd sessions or the show bfd history commands to check the status of your BFD sessions. These commands help you understand whether all the BFD sessions that should have been established, have indeed been established.

BFD sessions have three valid states: Down, Init, and Up.

- **Down:** Non-operational connections with other Cisco vEdge devices in the network.
- **Init:** Connections that are reachable but not up yet.
- **Up:** Operational connections with other Cisco vEdge devices in the network.

Each device sends an echo-request to its peer and also an echo-response for the request it receives. In the echo response, the device sends its current BFD state. Based on this, the peer changes its BFD state if required.

For information on BFD alarms generated by Cisco SD-WAN Manager, see the *Permanent Alarms and Alarm Fields*.

Changes in Session States Based on Echo Response from Peers

The following table shows how the BFD session states on a device change based on the session states that the peer responds with.

BFD Session State on Device	BFD State sent by Peer in Echo Response	BFD Status Change on Device
Up	Up or Init	Up (no change)
Up	Down	Down
Init	Up or Init	Up
Init	Down	Init (no change)
Down	Down	Init
Down	Init	Up

Down	Up	Down (no change)

BFD Sessions

In Cisco SD-WAN, the total number of BFD (Bidirectional Forwarding Detection) sessions is determined by the number of TLOCs (Transport Locators) advertised to the Cisco SD-WAN Controller. When a Cisco IOS XE Catalyst SD-WAN device establishes the control connection with the Cisco SD-WAN Controller, it advertises it's TLOC to the controller. The controller then propagates the TLOC information to all other Cisco devices in the network. As a result, the Cisco devices can establish IPSec sessions between them, which in turn enables the BFD sessions to come up.

```
Device# show sdwan bfd summary
sessions-total         1
sessions-up            1
sessions-max           12
sessions-flap          38
poll-interval          123400
```

Cisco SD-WAN Manager dashboard indicates the following results:

1. **Control Connection Down**: When the control connection between the Cisco device and the Cisco SD-WAN Controller is lost, the total number of BFD sessions (sessions-total) becomes zero, and the number of active sessions (sessions-up) also becomes zero. Consequently, the BFD column indicates 0/0.
2. **Underlay Issue**: If the control connection to the Cisco SD-WAN Controller remains up, but due to an underlay issue, the connectivity or IPsec session between the two Cisco peer devices goes down, the total number of BFD sessions (sessions-total) still remains 1. However, the number of active sessions (sessions-up) becomes zero. In this case, the BFD column indicates 0/1.

To explain the restrict and max-control-connection options, consider an overlay of two sites each having two TLOCs. For example, private1 and private2 on both ends. In the condition where all the TLOCs are up, the total number of BFD sessions (sessions-total) remains 4.and number of active sessions (sessions-up) becomes 4. In this case, the BFD column indicates 4/4.

- **Restrict-option**: If the control connection to the Cisco SD-WAN Controller remains up, but the TLOC color is configured with a **restrict** option, the total number of BFD sessions (sessions-total) remains 3. However, the number of active sessions (sessions-up) becomes three. In this case, the BFD column indicates 3/3.
- **Max-control-connections 0 option**: If the control connection to the Cisco SD-WAN Controller remains up, but one of the TLOC on one site is configured with a **max-control-connections 0**, the total number of BFD sessions (sessions-total) remains 3. However, the number of active sessions (sessions-up) becomes three. In this case, the BFD column indicates 3/3.

View BFD Session Information

Bidirectional Forwarding Detection (BFD) sessions between routers start automatically when the devices come up in the network. BFD which runs on secure IPsec connections between the routers, is used to detect connection failures between the routers.

To view BFD information for a router:

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that displays.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands as relevant:
   - **BFD Sessions** (to view real-time BFD sessions)
   - **BFD History** (to view BFD session history)

View BGP Information

You can configure the Border Gateway Protocol (BGP) on routers to enable routing on the service side (site-local side) of the device, thus providing reachability to networks at the devices' local sites.

To view BGP information on a router:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands as relevant:

Option	Description
BGP Summary (**show bgp summary**	View BGP connection status.
BGP Neigbors (**show bgp neighbor**)	View BGP neighbors.
BGP Routes (**show bgp routes**)	View routes learned by BGP.

View Cflowd Information

Cflowd monitors traffic flowing through routers in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. For a traffic flow, Cflowd periodically sends template reports to a flow collector. These reports contain information about the flow and data extracted from the IP headers of the packets in the flow.

To configure Cflowd in a router, use centralized data policy to define a Cflowd template that specifies the location of a Cflowd collector and timers that control the flow collection.

To view Cflowd flow information for a router:

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices displayed.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands or options, as relevant:

Option	Description
Cflowd Template (**show app cflowd template**)	View the Cflowd template. Device option is displayed on Cisco vEdge devices.
Cflowd Collector (**show app cflowd collector**)	View Cflowd Collector information. Device option is displayed on Cisco vEdge devices.
Cflowd Flows (**show app cflowd flows**, **show app cflowd flow-count**)	View Cflowd flows. Device option is displayed on Cisco vEdge devices.
Cflowd Statistics (**show app cflowd statistics**)	View Cflowd statistics. Device option is displayed on Cisco vEdge devices.
cFlowd Flows/DPI (**show cflowd flows**)	View Cflowd traffic flow information and SAIE flow information. From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **cFlowd Flows/DPI** field is added for applying filters for monitoring specific SAIE applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Device option is displayed on Cisco IOS XE Catalyst SD-WAN devices.
cFlowd ipv6 Flows/DPI (**show cflowd flows**)	View Cflowd IPv6 traffic flow information and SAIE flows. From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **cFlowd ipv6 Flows/DPI** field is added for applying filters for monitoring specific SAIE applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Device option is displayed on Cisco IOS XE Catalyst SD-WAN devices.

View Cloud Express Information

To view Cloud Express information on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands:

Device Option	Command	Description
Cloud Express Applications	show sdwan cloudexpress applications	Displays the best path that Cloud onRamp for SaaS has selected for each configured SaaS application on Cisco IOS XE Catalyst SD-WAN devices.
Cloud Express Gateway Exits	`show sdwan cloudexpress gateway-exits`	Displays the Quality of Experience (QoE) measurements received from gateway sites, for Cloud onRamp for SaaS on Cisco IOS XE Catalyst SD-WAN devices.
Cloud Express Local Exits	`show sdwan cloudexpress local-exits`	Displays the list of applications enabled for Cloud onRamp for SaaS probing on Cisco IOS XE Catalyst SD-WAN devices, and the interfaces on which the probing occurs.

View ARP Table Entries

The Address Resolution Protocol (ARP) is used to resolve network layer addresses, such as IPv4 addresses) into link layer addresses (such as Ethernet, or MAC, addresses). The mappings between network and physical addresses are stored in an ARP table.

To view the entries in the ARP table:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that displays.
3. Click **Real Time** in the left pane.

4. From the **Device Options** drop-down list in the right pane, choose **ARP**.

CLI equivalent: **show arp**

Run Site-to-Site Speed Test

Before You Begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.
   - **Destination Device**: From the drop-down list, choose the remote device by its device name and system IP address.
   - **Destination Circuit**: From the drop-down list, choose the color of the tunnel interface on the remote device.
6. Click **Start Test**.

The right pane shows the results of the speed test, the download, and upload speed between the source and destination. The download speed shows the speed from the destination to the source, and the upload speed shows the speed from the source to the destination in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table in the lower part of the right pane.

From Cisco vManage Release 20.10.1, the **Speed Test** option is also accessible as follows:

- On the **Monitor** > **Devices** page, click **…** adjacent to the device name and choose **Speed Test**.
- On the **Monitor** > **Applications** page, click **…** adjacent to the application name and choose **Speed Test**.
- On the **Site Topology** page, click a device name, and then click **Speed Test** in the right navigation pane.

View Network-Wide Path Insight

For information about network-wide path insight, see Cisco Catalyst SD-WAN Network-Wide Path Insight User Guide.

View NMS Server Status

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a Cisco SD-WAN Manager device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose **NMS Server Running**.

Device Option	Command	Description
NMS Server Running	show nms-server running	Displays whether a Cisco SD-WAN Manager NMS server is operational. This device option is available from Cisco vManage Release 20.6.1.

View Cisco Catalyst SD-WAN Validator Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands:

Device Option	CLI Command	Description
Orchestrator Reverse Proxy Mapping	show orchestrator reverse-proxy-mapping	Displays the proxy IP addresses and port numbers that are configured for use by reverse proxy.
Orchestrator Statistics	show orchestrator statistics	Displays statistics about the packets that a Cisco Catalyst SD-WAN Validator has transmitted and received in the process of establishing and maintaining secure DTLS connections to a Cisco IOS XE Catalyst SD-WAN devices in the overlay network.

Device Option	CLI Command	Description
Orchestrator Valid vManage ID	show orchestrator valid-vmanage-id	Lists the chassis numbers of the valid Cisco SD-WAN Manager instance in the overlay network.

Run a Traceroute

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Trace Route**.
5. In the **Destination IP** field, enter the IP address of the corresponding device in the network.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
6. From the **VPN** drop-down list, choose a VPN to use to reach the device.
7. From the **Source/Interface for VPN** drop-down list, choose the interface to use to send the traceroute probe packets.
8. Click **Advanced Options**.
9. In the **Size** field, enter the size of the traceroute probe packets, in bytes.
10. Click **Start** to trigger a traceroute to the requested destination.

The lower part of the right pane displays the following information:

- Raw output of the path the traceroute probe packets take to reach the destination.
- Graphical depiction of the path the traceroute probe packets take to reach the destination.

If the traceroute is for the service-side traffic, a Cisco vEdge device generates traceroute responses from any of the interfaces on the service VPN.

From Cisco vManage Release 20.10.1, the **Trace Route** option can be accessed using one of these methods:

- Choose **Monitor** > **Devices**, click **…** adjacent to the device name, and choose **Trace Route**.
- In the **Site Topology** page, click a device or tunnel name, and then click **Trace Route** in the right navigation pane.

View Tunnel Loss Statistics

View Data Plane Tunnel Loss Statistics

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that displays.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose **Tunnel Statistics**.

View Traffic Loss for Application-Aware Routing

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. Scroll down to the **Application-Aware Routing** pane.

You can also use the **show app-route statistics** command to view traffic loss for application-aware routing.

View SAIE Flows

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   Starting from Cisco vManage Release 20.6.1, to view the detailed SD-WAN Application Intelligence Engine (SAIE) flow information such as source IP address, destination IP address, and port details, you need to add the devices to the on-demand troubleshooting list. Add the device to the on-demand troubleshooting list from **Tools** > **On Demand Troubleshooting**.

Note

- In Cisco vManage Release 20.6.1 and earlier releases, **On Demand Troubleshooting** is part of the **Monitor** menu.
- In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.
- Ensure that no Cisco or third-party APIs that instruct on-demand troubleshooting to stop are called. These APIs prevent on-demand troubleshooting from compiling information.

To enhance the application visibility, the data collection process on the device generates aggregated application statistics usage data, which in turn reduces the size of the statistics data files that are processed

by default on the management plane. This enhancement allows Cisco SD-WAN Manager to collect SAIE data efficiently and reduce the processing time of the management plane.

2. Under **Applications** in the left pane, click **SAIE Applications**. The right pane displays SAIE flow information for the device.



Note

- When displaying the SAIE flow usage, peak usage is shown to be higher from one time interval than for another for the same time period. This situation occurs because the data is not yet available from the statistics database to display in Cisco SD-WAN Manager. Cisco SD-WAN Manager displays only available data and then plots that data in the appropriate axis.
- In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Applications** is called **DPI Applications**.

The upper part of the right pane contains:

- Filter option: Click the **Filter** option to view a drop-down menu to choose the desired VPN and Local TLOC.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.14.1, in **Traffic Source**, you can choose LAN traffic, remote access traffic, or both the options to view the traffic data.

  Click **Search**. Click a predefined or custom time period for which to view the data.



Note Filtering **Local TLOC : Dia** is supported only for Cisco vEdge devices.

- SAIE flow information in graphical format.
- SAIE flow graph legend—Select an application family to display information for just that flow. Click the **Total Network Traffic** check box to display flow information as a proportion of total network traffic.

The lower part of the right pane contains:

- Filter criteria.
- SAIE flow information table that lists all application families sorted by usage. By default, the top six application families are selected. The graphical display in the upper part of the right pane plots the flow and usage of the selected application families.
  - Click the check box on the left to select or deselect application families. You can choose to view information for a maximum of six application families at one time.
  - Click an application family to view applications within the family.
  - Click an application to view the source IP addresses of the devices accessing the application. The Traffic per TLOC pie chart next to the graph displays traffic distribution per TLOC (color).
  - To re-arrange the columns, drag the column title to the desired position.

View VNF Status

Reviewing VNF status can help you to determine which VNF to use when you are designing a network service.

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a CSP device from the table.
3. From the left pane, click **VNF Status**.
4. In the table, click the VNF name. The right pane displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, disk utilization to monitor the resources utilization of a VNF.

   The primary part of the right pane contains:

   - Chart Options bar that includes the following options:
     - Chart Options drop-down—Click **Chart Options** to select the type of data to display.
     - Time periods—Click either a predefined time period, or a custom time period for which to display data.
   - VNF information in graphical format.
   - VNF graph legend—Select a VNF to display information for just that VNF.

The detailed part of the right pane contains:

- Filter criteria
- VNF table that lists information about all VNFs. By default, the first six VNFs are selected. The graphical display in the upper part of the right pane plots information for the selected VNFs.
  - Check or uncheck the check box at the left to select and deselect VNFs. You can select and display information for a maximum of six VNFs at one time.
  - To change the sort order of a column, click the column title.

View TCP Optimization Information

View WAN Throughput

If TCP optimization is enabled on a router, you can view information about how the optimization affects the processing and throughput of TCP data traffic on the router:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that displays.
3. In the left pane, click **WAN Throughput**. The right pane displays the WAN throughput, in megabits per second.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Filter Options drop-down and time periods. Click **Filter** to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
- Average optimized throughput information in graphical format.
- WAN graph legend—Identifies non-optimized and TCP optimized packet throughput.

The lower part of the right pane shows the hourly average throughput and the total optimized throughput, both in megabits per second.

Click **TCP Optimization–Connections** in the left pane to view status information about all the tunnels over which the most TCP-optimized traffic is flowing. The upper part of the right pane contains the following elements:

- TCP Optimization Connections in graphical format.
- Connection State boxes—Select the connection state or states to view TCP optimization information.

The lower part of the right pane contains the following elements:

- Filter criteria.
- Flow table that lists information about each of the tunnels, including the tunnel's connection state.

View TCP-Optimized Flows for Cisco vEdge Devices

To view information about TCP-optimized flows on a Cisco vEdge device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:



Note The following options are available when you choose a Cisco vEdge device.

Device Option	Command	Description
TCP Optimization Active Flows	show app tcp-opt	Displays information about active TCP-optimized flows.

Device Option	Command	Description
TCP Optimization Expired Flows	show app tcp-opt	Displays information about expired TCP-optimized flows.
TCP Optimization Summary	show app tcp-opt	Displays a summary of the TCP-optimized flows.

View SFP Information

To view SFP information on a router, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:

Device Option	Command	Description
SFP Detail	show interface sfp detail	Displays detailed SFP status and digital diagnostic information.
SFP Diagnostic	show interface sfp detail	Displays SFP digital diagnostic information.
SFP Measurement Value	show interface sfp detail	Displays SFP measurement data.
SFP Measurement Alarm	show interface sfp detail	Displays SFP alarm information for the measurements.

Monitor NAT DIA Tracker Configuration on IPv4 Interfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

View Interface DIA Tracker

To view information about DIA tracker on a transport interface:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices.

3. Click **Real Time**.
4. For single endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Info**.
5. For dual endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Group Info**.

View TLOC Loss, Latency, and Jitter Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. In the left pane, click **TLOC** under the **WAN** area. The right pane displays the aggregated average loss or latency/jitter information for all TLOC colors.

The upper part of the right pane contains the following elements:

- Chart Options— Includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to view. Click a predefined or custom time period for which to view data.
- TLOC information in graphical format. The time interval in the graph is determined by the value of the BFD application-aware routing poll interval .
- TLOC graph legend—Choose a TLOC color to display information for just that TLOC.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options filter.
- TLOC color table that lists average jitter, loss, and latency data about all TLOCs. By default, the first six colors are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  - Check the check box to the left to select and deselect TLOC colors. You can select and view information for a maximum of 30 TLOCs at one time.
  - Click **Application Usage** to the right to view the SD-WAN Application Intelligence Engine (SAIE) flow information for that TLOC.

Note

- Beginning with Cisco vManage Release 20.8.1, the **Application Usage** column and the **Application Usage** links are removed from the **Monitor** > **Devices** > **WAN – Tunnel** window. After you have configured on-demand troubleshooting for a device, you can view SAIE usage data based on the selected filters or based on application families sorted by usage.
- In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.

For more information on configuring on-demand troubleshooting, see On-Demand Troubleshooting. For more information on viewing SAIE flows, see View SAIE Flows.

View Tunnel Connections

To view details about the top 100 data plane tunnels between Cisco Catalyst SD-WAN devices with the lowest average latency, do the following:

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

   The Tunnels table lists the following information about all tunnel end points:

   - Health
   - State
   - Quality of Experience (QoE) score. The QoE score rates the quality of experience of an application that a network can deliver for a period of time.
   - Local IP and remote IP
   - Average latency, loss, and jitter data

   The health of a tunnel is defined based on the following criteria:

   - Good: If the QOE score is between 8 and 10, and the tunnel status is 1/1.
   - Fair: If the QOE score is between 5 and 7, and the tunnel status is 1/1.
   - Poor: If the QOE score is between 1 and 4, or the tunnel status is 0/1.

Note The tunnel information is available in Cisco SD-WAN Manager as a separate menu starting from Cisco vManage Release 20.7.1.

To view tunnel connections of a specific device, do the following:

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. In the left pane, click **TLOC** under the **WAN** area. The right pane displays information about all tunnel connections.
4. (Optional) Click the **Chart Options** drop-down list to choose the type of data to view.

   You can also choose a predefined time period or a custom time period to sort the data.
5. (Optional) In the lower part of the right pane, use the filter option in the search bar to customize the table fields you want to view.

   The tunnel table lists average latency, loss, and jitter data about all tunnel end points. By default, the first six tunnels are selected. The graphical display in the upper part of the right pane plots information for the selected tunnels.
6. (Optional) Click the check box to the left to select and deselect tunnels. You can select and view information for a maximum of 30 tunnels at one time.
7. (Optional) Click **Application Usage** to the right to view the SD-WAN Application Intelligence Engine (SAIE) flow information for that TLOC.



Note

- Beginning with Cisco vManage Release 20.8.1, the **Application Usage** column and the **Application Usage** links are removed from the **Monitor** > **Devices** > **WAN – Tunnel** window. After you have configured on-demand troubleshooting for a device, you can view SAIE usage data based on the selected filters or based on application families sorted by usage.
- In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

For more information on configuring on-demand troubleshooting, see On-Demand Troubleshooting. For more information on viewing SAIE flows, see View SAIE Flows.

View IPSec Tunnel Information

To view IPSec tunnel information on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:

Device Option	CLI Command	Description
IPsec Inbound Connections	show tunnel inbound-connections	Displays information about the IPsec tunnel connections that originate on the local router, showing the TLOC addresses for both ends of the tunnel.
IPsec Local SAs	show tunnel local-sa	Displays the IPsec tunnel security associations for the local TLOCs.

View Tunnel Health in Table View

Minimum supported release: Cisco vManage Release 20.10.1

In the **Monitor Tunnels** window the table shows information about the health of tunnels created in the last hour, displaying a maximum of 10,000 tunnels.

The tunnel information includes the following:

- Tunnel health
- State
- Quality of Experience (QoE)
- Average latency
- Average loss
- Average jitter
- Local IP address
- Remote IP address

You can also view the tunnel health on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

Tunnel Health Metrics

The average health metric of tunnels is calculated as follows:

Health	QoE	Status	Evaluation Logic
Good	QoE >= 8	UP	All attributes met
Fair	5 <= QoE < 8	UP	All attributes met
Poor	0 < QoE< 5	DOWN	Any attributes met

View Tunnel Health in Heatmap View

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, a grid of colored squares displays the tunnel health as **Good**, **Fair**, or **Poor**. You can hover over a square or click to display additional details of a tunnel at a specific time. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

You can view the tunnel health on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

View License Information

To view license information on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:

Device Option	Command	Description
Smart License <info>	show licenses	Display the licenses for the software packages used by Cisco Catalyst SD-WAN.

View Logging Information

To view logging information on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options** and choose the following command:

Device Option	Command	Description
Logging	show logging	Displays the settings for logging syslog messages.

View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels

View the loss percentage, latency, jitter, and octets for tunnels in a single chart option in Cisco SD-WAN Manager.

Table 27: Feature History

Feature Name	Release Information	Description
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature provides a single chart option in Cisco SD-WAN Manager for viewing tunnel information, such as packet loss, latency, jitter, and octets.

View Loss Percentage, Latency, Jitter, Octets, and Packet Duplication for Tunnels

You can choose the **Real Time** option or other time frames to view tunnel information in the graph.

To view loss percentage, latency, jitter, and octets in Cisco SD-WAN Manager:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.
3. In the left pane, click **Tunnel** under the WAN area. The right pane displays information about all tunnel connections.
4. In the right pane, click **Chart Options** to choose the format in which you want to view the information.

   Click **Loss Percentage/Latency/Jitter/Octets** for troubleshooting tunnel information.

The upper part of the right pane contains the following elements:

- Data for each tunnel is graphed based on time.
- Legend for the graph—Choose a tunnel to view information for just that tunnel. Lines and data points for each tunnel are uniquely colored.

The lower part of the right pane contains the following elements:

- Search bar—Includes the Search Options filter to filter the table based on a Contains or a Match criteria.
- Tunnel Table—Lists the jitter, latency, loss percentage, and other data about all the tunnel end points. By default, the first six tunnels are selected. The graphical display in the upper part of the right pane plots information for the selected tunnels.
  - Click the column drop-down lists to enable or disable all of the descriptions.
  - Check the check box to the left to select and deselect tunnels. You can choose and view information for a maximum of six tunnels at one time.

View WiFi Configuration

To view WiFi configuration for Cisco Catalyst SD-WAN routers that support wireless LANs (WLANs), such as the Cisco vEdge device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device.
3. Click **WiFi** in the left pane. The right pane displays information about WiFi configuration on the router.

The upper part of the right pane contains the following elements:

- AP Information bar—Located directly under the device name, it displays access point information and the Clients Details button. Click the Clients Details button to view information about clients connected to the WiFi access point during the selected time period.
- Radio frequency parameters for access points.
- SSID parameters for virtual access points (VAPs).

The lower part of the right pane contains the following elements:

- VAP receive and transmit statistics bar—Includes the time periods. Click a predefined or custom time period for which to display data.
- VAP receive and transmit statistics information in graphical format.
- VAP statistics graph legend—Select a VAP interface to display information for just that interface. Click the VAP interface again to return to the previous display.

View Control Connections in Real Time

To display a real-time view the control plane connections on a Cisco vEdge device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device.
3. Click **Troubleshooting** in the left pane.
4. Under the Connectivity area, click **Control Connections (Live View)**.

The control plane connection screen is updated automatically, every 15 seconds.

The upper part of the right pane shows figures illustrates the operational control plane tunnels between the edge device, Cisco Catalyst SD-WAN, and Cisco SD-WAN Controller.

The lower part of the lower pane contains a table that shows details for each of the control plane tunnels, including the IP address of the remote device and the status of the tunnel end points, including the reason for the failure of an end point.

View Cisco Umbrella Information

To view Cisco Umbrella information on a device, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose the following.

Device Option	Command	Description
Umbrella Device Registration	show umbrella deviceid	Displays Cisco Umbrella registration status for Cisco IOS XE Catalyst SD-WAN devices.

View VRRP Information

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.
3. Click **Real Time** from the left pane.
4. Click **Device Options**, and choose **VRRP Information**.

View PKI Trustpoint Information

Minimum Supported Release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Control Components 20.13.1.

Use the **View PKI Trustpoint** tab to view PKI Trustpoint related information including the validity.

1. From the Cisco SD-WAN Manager Menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that appear.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose **PKI Trustpoint**.

Option	Description
PKI Trustpoint	View PKI Trustpoint related information.

View QoS Information

View QoS statistics to know which traffic classes experienced the greatest number of drops on which devices in your network.

Table 28: Feature History

Feature Name	Release Information	Description
QoS Monitoring in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This release extends the capability of viewing interface-wise QoS information through Cisco SD-WAN Manager to support Cisco IOS XE Catalyst SD-WAN devices. Before this release, QoS information for Cisco IOS XE Catalyst SD-WAN devices could only be monitored through device CLI.

Note that this feature was already available for Cisco vEdge devices.

Limitations for QoS Monitoring

- This feature is not supported for sub-interfaces.
- This feature is not supported if per-tunnel QoS is enabled.

View QoS Information Chart

A QoS chart shows the packet speed and the number of packets dropped for each queue for the selected interface.

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that appears.
3. In the left pane, click **QoS** under the **Applications** area.
4. The upper part of the right pane has the following options to choose from.
   - **Interface Name**: From the drop-down menu, choose the interface for which you want to view QoS data.
   - **Time Range:** : Choose to view the information for a specified time range—Real time, predefined time ranges (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

     Real time QoS information can also be viewed in a tabular format. See the section View Real Time QoS Information Table.

5. From the Chart drop-down list, choose one of the following.

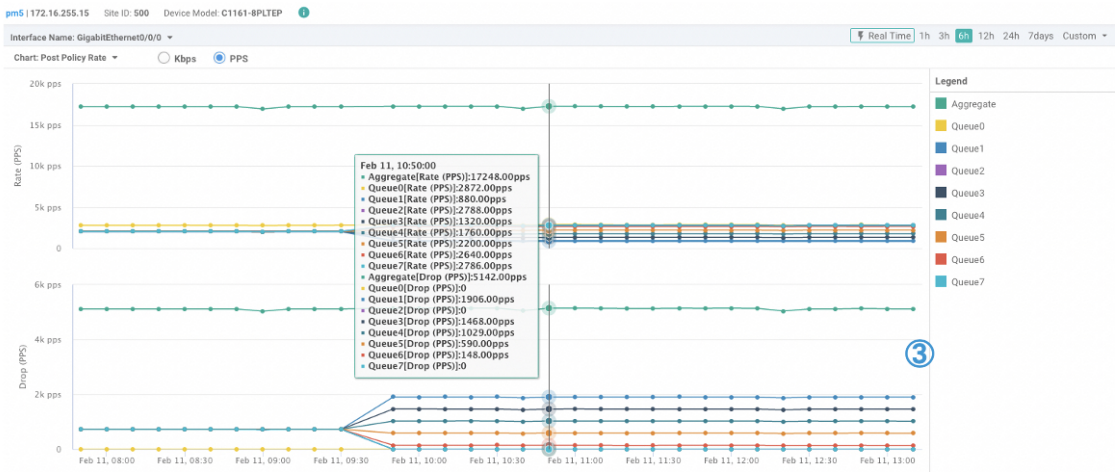
   - **Post Policy Rate:** This option displays the speed at which data travels per second in either kbps (default) or in packets per second (PPS). This value is calculated to get the per second speed by using the formula: Post Policy Counter/10.

   OR

   - **Post Policy Counter:** This option displays the number of packets (or the number of packets in bytes) that have gone through the queue in the last 10 seconds.

   The QoS chart displays. The following example shows QoS data for a specified, historical time range for the selected interface. In this chart, each data point represents 10 minutes. For longer time ranges, Cisco SD-WAN Manager aggregates data points.

Figure 11: QoS Chart



Cisco SD-WAN Manager also displays a table below the chart. However, the table always displays historical data even if you choose the Real Time option to generate a chart. Such historical tables generated below real time charts have no connection with the real time values in the chart.

The following example shows a table showing historical data that was generated below the real time QoS chart.

Figure 12: Historical QoS Table

Queue Name	Pre Policy Tx (in kbps)	Post Policy Tx (in kbps)	Drop (in kbps)
Aggregate	259230.875	199686.969	59543.344
Queue0	32538.344	32538.344	0
Queue1	32362.406	14931.094	17430.75
Queue2	32380.75	29467.031	2913.563
Queue3	32390.906	18288.25	14102.031
Queue4	32401.281	21645.594	10755.188
Queue5	32404.125	25002.75	7400.875
Queue6	32391.5	28359.969	4030.969
Queue7	32358.031	29450.25	2907.656

View Real Time QoS Information Table

To view real time QoS information in a tabular format, follow these steps:

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that appears.
3. In the left pane, click **Real Time** under the **Security Monitoring** area.
4. From the Device Options drop-down list, choose **Interface QoS Statistics**.

   A table of QoS statistics appears. You can filter the table by interface name by choosing an interface from the **Filter** drop-down list.

View WLAN Output

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

Use the **Wireless SSID** tab to view the WLAN output along with the VLAN ID assoicated.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IR1800 device from the list of devices.
3. Click **Real Time** in the left pane.
4. In the **Device Options** drop-down box, type **Wireless SSID**.

Option	Description
Wireless SSID	View the WLAN output.

View Client Details

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

Use the **Wireless Clients** tab to view the client details along with their MAC addresses.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IR1800 device from the device list.
3. Click **Real Time** in the left pane.
4. In the **Device Options** drop-down list, choose **Wireless Clients**.

Option	Description
Wireless Clients	View the client details along with their MAC addresses.

Check Traffic Health

View Tunnel Health

To view the health of a tunnel from both directions:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name under the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Traffic** area, click **Tunnel Health**.
5. The device you chose earlier is the **Local Device**. Choose the following:
   a. From the **Local Circuit** drop-down list, choose a source TLOC.
   b. From the **Remote Device** drop-down list, choose a remote device.
   c. From the **Remote Circuit** drop-down list, choose a destination TLOC.

   From Cisco Catalyst SD-WAN Manager Release 20.16.1, you can choose up to five of each: remote devices, local circuits, and remote circuits. The **Local Device** for the first selection instance is autopopulated. For the second and subsequent instances, the **Local Device** is autopopulated based on the entry in the **Remote Device**, which then becomes the **Local Device**.
6. Click **Go**. The lower part of the screen displays a chart for tunnel health data.

   From Cisco Catalyst SD-WAN Manager Release 20.16.1, individual charts are displayed for each instance of **Local Device** and **Remote Device**.
7. From the **Chart Options** drop-down list, choose one of these: Loss Percentage, Latency/Jitter, Octets.
8. (Optional) Choose a predefined or a custom time period on the left to view data for the specified time period.

The window displays:

- App-route data (either loss, latency, or jitter) in graphical format for all tunnels between the two devices in each direction.
- App-route graph legend—Identifies selected tunnels from both directions.

From Cisco vManage Release 20.10.1, the **Tunnel Health** option is also accessible as follows:

- On the **Monitor** > **Tunnels** page, click **…** adjacent to the tunnel name and choose **Tunnel Health**.
- On the **Monitor** > **Applications** page, click **…** adjacent to the application name and choose **Tunnel Health**.
- On the **Site Topology** page, click a tunnel name, and then click **Tunnel Health** in the right navigation pane.

Check Application-Aware Routing Traffic

To check application-aware routing traffic from the source device to the destination device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Click **Troubleshooting** in the left pane.
4. In the right pane, click **App Route Visualization** under **Traffic**.
5. From the **Remote Device** drop-down list, choose a destination device.
6. (Optional) Click **Traffic Filter**. Choose **No Filter** or **SAIE**. **No Filter** is chosen by default.



Note In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.

7. Click **Go**. The lower part of the screen displays:
8. From the Chart Options drop-down list, choose one of these: Loss Percentage, Latency/Jitter, Octets.
9. (Optional) Choose a predefined or a custom time period on the left to view data for the specified time period.

From Cisco vManage Release 20.10.1, the **App Route Visualization** option is also accessible from the **Monitor** > **Applications** page. Click **…** adjacent to the application name and choose **App Route Visualization**.

Capture Packets

Table 29: Feature History

Feature Name	Release Information	Description
Embedded Packet Capture	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device. The administrator can analyze these packets locally or save and export them for offline analysis using Cisco SD-WAN Manager. This feature gathers information about the packet format and helps in application analysis, security, and troubleshooting.
Embedded Packet Capture for Cisco vEdge Devices Using CLI Commands	Cisco SD-WAN Release 20.6.1	This feature provides an alternative method to capture traffic data to troubleshoot connectivity issues between Cisco vEdge devices and Cisco SD-WAN Manager using CLI commands. As part of this feature, the following commands are introduced to capture traffic details: request stream capture show packet-capture
Bidirectional Packet Capture for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enhances the embedded packet capture functionality to support bidirectional packet capture through Cisco SD-WAN Manager.
IPv6 Support for Bidirectional Packet Capture	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This feature adds support for bidirectional capture of IPv6 traffic data to troubleshoot connectivity issues using a CLI template.

Information About Bidirectional Packet Capture

You can capture the traffic flowing through an interface, or, for the control plane, in a single direction or in both directions (bidirectional). You can analyze the packets locally or export the captured traffic for offline analysis. From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, packet capture supports IPv6 traffic.

Configure Packet Capture Using Cisco SD-WAN Manager

Perform the following steps to capture control plane and data plane packets in real time, and to save these packets to a file available on edge devices.

Note Packet capture is not supported for a loopback interface.

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Traffic** area, click **Packet Capture**.
5. From the VPN drop-down list, choose a VPN.
6. From the **Interface** drop-down list, choose an interface.



Note From Cisco vManage Release 20.8.1, you can capture IPv6 packets for tracing and troubleshooting traffic. To do this, choose an IPv6 interface from the **Interface** drop-down list. (Prior to Cisco vManage Release 20.8.1, only IPv4 interface capture was supported.)

7. (Optional) Click **Traffic Filter** to filter the packets to capture based on values in their IP headers. Enter values for the following fields:
   a. In the **Source IP** field, enter the source IP address of the packet.

      For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

   b. In the **Source Port** field, enter the source port number of the packet.
   c. In the **Protocol** field, enter the protocol ID of the packet.
   d. In the **Destination IP** field, enter the destination IP address of the packet.

      For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

   e. In the **Destination Port** field, enter the destination port number of the packet.
8. For a Cisco IOS XE Catalyst SD-WAN device, to enable bidirectional packet capture, set the **Bidirectional** toggle button to **On**.



Note The bidirectional packet capture functionality is available from Cisco vManage Release 20.7.1.

9. Click **Start**.

   The packet capture begins, and progress is displayed:

   a. Packet Capture in Progress: Packet capture stops after the file of collected packets reaches 5 MB, or when you click **Stop**.
   b. Preparing file to download: Cisco SD-WAN Manager creates a file in libpcap format (a .pcap file).
   c. File ready, click to download the file: Click the download icon to download the generated file.

Note In the Cisco SD-WAN Manager cluster environments, you can run speed test and capture the packets in all the devices in the cluster irrespective of the Cisco SD-WAN Manager node that the devices are connected to. You can configure the data stream with one of the following:

- Management IP address and VPN 512 (Cisco CSR 1000v Series platform does not support Management IP address)
- Transport IP address and VPN 0

We do not recommend data stream configuration with the system IP address of a Cisco SD-WAN Manager node and VPN 0 in cluster environments because it limits speed test and packet capture to only the devices that are connected to the Cisco SD-WAN Manager node that is configured in the data stream.

Configure Packet Capture Using a CLI Template

Before You Begin

For more information about using CLI templates, see CLI Templates.

Note By default, CLI templates execute commands in global config mode.

Perform these steps and ensure that **Data Stream** in **Administration** settings is in **Enabled** state for the monitor packet capture CLI configurations to take effect:

1. From Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Data Stream**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Choose the **IP Address Type**. By default, **System** is selected. (**Transport** and **Management** types require additional **Hostname** and **VPN** settings.)
4. Click **Save**.

Configure Packet Capture for IPv4 Traffic

Define a core filter for monitoring IPv4 packet capture:

monitor capture *capture-name* **match ipv4** *source-prefix/length destination-prefix/length* **[bidirectional]**

Here is an example configuration to filter and capture IPv4 traffic:

```
monitor capture mycap match ipv4 198.51.100.0/24 host 198.51.100.1
```

Configure Packet Capture for IPv6 Traffic

Configure the filter for monitoring IPv6 packet capture for inbound traffic or outbound traffic or both inbound and outbound traffic (bidirectional), which passes through the interface or a control plane. Do one of the following:

- Configure packet capture for an interface:

```
monitor capture capture_name [interface interface-name interface-num {both | in | out}] match ipv6 {{ipv6-source-prefix/length| host ipv6-src-addr| any} {ipv6-destination-prefix/length| host ipv6-dest-addr| any}}
|protocol {<0-255>|tcp|udp}
{ipv6-source-prefix/length| host ipv6-src-addr| any} [{eq | lt| gt| neq |range port_number} port_number]
{ipv6-destination-prefix/length| host ipv6-dest-addr| any} [{eq | lt| gt| neq |range port_number} port_number]} [bidirectional]
```

- Configure packet capture for the control plane:

```
monitor capture capture_name [control-plane {both | in | out}] match ipv6 {{ipv6-source-prefix/length| host ipv6-src-addr| any} {ipv6-destination-prefix/length| host ipv6-dest-addr| any}}
|protocol {<0-255>|tcp|udp}
{ipv6-source-prefix/length| host ipv6-src-addr| any} [{eq | lt| gt| neq |range port_number} port_number]
{ipv6-destination-prefix/length| host ipv6-dest-addr| any} [{eq | lt| gt| neq |range port_number} port_number]} [bidirectional]
```

The following examples show how to configure to filter and capture IPv6 traffic:

```
monitor capture test interface GigabitEthernet 5 both match ipv6 protocol tcp host
2001:3c0:1::71 host 2001:380:1::71 bidirectional
monitor capture cap interface gig 2 in match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap interface gig 2 out match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap interface gig 2 both match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane in match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane out match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane both match ipv6 50::1/128 50::2/128 bidirectional
```

Simulate Flows

Table 30: Feature History

Feature Name	Release Information	Description
Forwarding Serviceability	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables service path and tunnel path under Simulate Flows function in the Cisco SD-WAN Manager template and displays the next-hop information for an IP packet. This feature enables Speed Test and Simulate Flow functions on the Cisco IOS XE Catalyst SD-WAN devices.

To view the next-hop information for an IP packet available on routers:

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that appears.
3. Click **Troubleshooting** in the left pane.
4. Under **Traffic**, click **Simulate Flows**.
5. To specify the data traffic path, choose values or enter data in the required fields:
   - **VPN**: VPN in which the data tunnel is located.
   - **Source/Interface**: Interface from which the cflowd flow originates.
   - **Source IP**: IP address from which the cflowd flow originates.

     For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
   - **Destination IP**: Destination IP address of the cflowd flow.

     For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
   - **Application**: Application running on the router.
   - **Custom Application** (created in CLI)
6. Click **Advanced Options**.
   a. In the **Path** field, choose **Tunnel** or **Service** to indicate whether the data traffic path information comes from the service side of the router or from the tunnel side.
   b. In the **Protocol** field, enter the protocol number.
   c. In the **Source Port** field, enter the port from which the cflowd flow originates.
   d. In the **Destination Port** field, enter the destination port of the cflowd flow.
   e. In the **DSCP** field, enter the DSCP value in the cflowd packets.
   f. (Optional) Check the **All Paths** check box to view all possible paths for a packet.
7. Click **Simulate** to determine the next hop that a packet with the specified headers would take.

For service path and tunnel path commands, see show sdwan policy service-path and show sdwan policy tunnel-path.

Security Monitoring

Table 31: Feature History

Feature Name	Release Information	Description
Enhanced Security Monitoring on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature allows you to view the CPU, memory, and traffic usage on your device. You can also view the health of individual UTD features.

View Traffic, CPU, and Memory Usage

1. From the Cisco SD-WAN Manager **Monitor** > **Devices** page, select the device.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager **Monitor** > **Network** page, select the device.

2. Under **Security Monitoring** in the left pane, select one of the UTD features **Intrusion Prevention**, **URL Filtering**, and so on.

3. By default, the traffic counter graph is displayed.

   You can also customize the time range to see traffic usage for specific time ranges such as **Real Time**, **1h**, **3h** or even specify a **Custom** time range. By default, a time range of **24h** is displayed. The time range cannot be more than 365 days.

4. To view CPU or memory usage, do the following:

   - To view CPU usage, click **UTD Stats: CPU Usage**.
   - To view memory usage, click **UTD Stats: Memory Usage**.

View the Health and Reachability of UTD

1. From the Cisco SD-WAN Manager **Monitor** > **Devices** page, select the device.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager **Monitor** > **Network** page, select the device.

2. Under **Security Monitoring** in the left pane, select one of the UTD features such as **Intrusion Prevention**, **URL Filtering**, and so on.

3. For all features, the health of UTD is displayed as one of the following:

   - Down: For example: UTD is not configured.
   - Green: UTD is healthy.
   - Yellow: For example: High memory usage.
   - Red: For example: One or more Snort instances are down.

If you configured UTD on the device and the status is not green, contact Cisco TAC for assistance.

4. Depending on the UTD feature that you choose, the following additional information is displayed:

UTD Feature	Status
Intrusion Prevention	Package Version IPS Last Updated Reason for last update status
URL Filtering	Cloud Reachability
Advanced Malware Protection	AMP Cloud Reachability Status TG Cloud Reachability Status
Umbrella DNS Redirect	Umbrella Registered VPNs DNSCrypt

View the System Clock

Minimum release: Cisco vManage Release 20.9.1

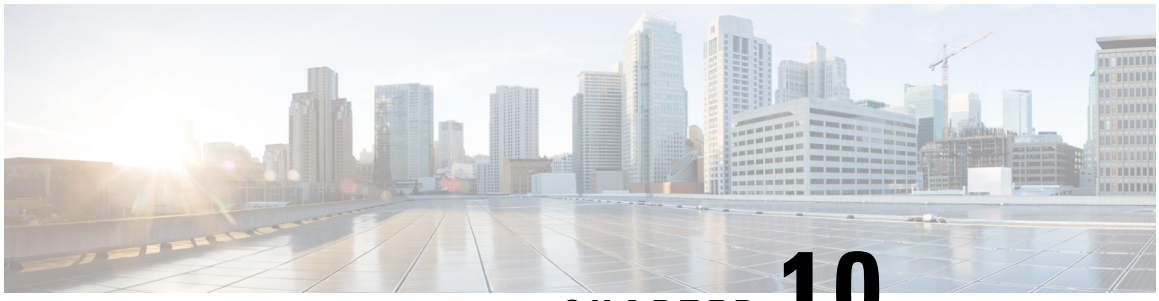
To view the system clock on a device, perform the following steps:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose the following command:

Device Option	Command	Description
System Clock	show clock	Displays the system clock date and time.



CHAPTER 10

Alarms, Events, and Logs

- Alarms, on page 173
- Events, on page 184
- ACL Log, on page 190
- Audit Logging, on page 190
- View Log of Configuration Template Activities, on page 194
- Syslog Messages, on page 194
- Cisco SD-WAN Manager Logs, on page 197
- View Log of Certificate Activities, on page 199
- Binary Trace for Cisco Catalyst SD-WAN Daemons, on page 200
- Traffic Logs, on page 204
- Safety Barriers, on page 207

Alarms

Table 32: Feature History

Feature	Release Information	Description
Optimization of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature optimizes the alarms on Cisco SD-WAN Manager by automatically suppressing redundant alarms. This allows you to easily identify the component that is causing issues. You can view these alarms from the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

Feature	Release Information	Description
Grouping of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The following enhancements are added to alarms: • Alarms are filtered and grouped for devices and sites based on severity. • View alarm details for a single site in the **Overview** dashboard. • View alarms for a particular device by clicking the … icon in the **Monitor > Devices** window. • View the top five alarms for a particular site in the **Monitor > Overview** window by choosing the **Site Topology** view icon and clicking the site. • View events related to an alarm in the **Related Event** column in the alarms filter.
Heatmap View for Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the alarms as **Critical**, **Major**, or **Medium & Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of alarms in a severity level.
Alarm Notifications Using WebHooks	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Configure a WebHook URL in Cisco SD-WAN Manager to receive alarm notifications in Webex or Slack.
Alarm Notifications Using Custom WebHooks Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.x Cisco Catalyst SD-WAN Manager Release 20.16.1	Configure alarm notifications using custom webhooks over management VPN 512 for increased security in a single-tenant or a multitenant setup.

Feature	Release Information	Description
Cloud OnRamp for SaaS Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	A Cisco IOS XE Catalyst SD-WAN device triggers three new alarms. These alarms indicate the status of CoR-SaaS application paths. This feature adds a **path-status** field to the **cloudexpress-application-change** notification. Alarms are categorized into into Major, Medium and Minor based on the path status (unreachable, reachachable, disabled).
Policy Download Failure Alarm	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download fails.

Information About Alarms



Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

When something of interest happens on an individual device in the overlay network, the device reports it by sending a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager then filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.

Use the Alarms screen to display detailed information about alarms generated by control components and routers in the overlay network.

When a site is down, Cisco SD-WAN Manager reports the following alarms:

- Site down
- Node down
- TLOC down

Cisco SD-WAN Manager displays alarms for each component that is down. Depending on the size of your site, you may see several redundant alarms such as alarms for each TLOC in a node as well as the node alarm. In Cisco vManage Release 20.5.1, Cisco SD-WAN Manager intelligently suppresses redundant alarms. For example, if all the TLOCs in a node are down, Cisco SD-WAN Manager suppresses the alarms from each TLOC and displays only the alarm from the node. For multitenant configurations, each tenant displays alarms for the sites in its tenancy.

Scenario	Alarms Displayed	
Cisco vManage Release 20.5.1	Previous Releases	

Scenario	Alarms Displayed	
Link 1 down Link 2 up.	bfd-tloc-1_down	bfd-tloc-1_down
Link 1 down Link 2 down	bfd-site-1_down bfd-node-1_down, bfd-tloc-1_down, and bfd-tloc-2_down are suppresed by the site alarm.	bfd-site-1_down bfd-tloc-1_down
Link 1 up Link 2 down	bfd-site-1_up bfd-node-1_up bfd-tloc-1_up bfd-tloc-2_up	bfd-site-1_up bfd-tloc-1_up

Alarms Details

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

The Cisco SD-WAN Manager generates alarms when a state or condition changes, such as when a software component starts, transitions from down to up, or transitions from up to down. The severity indicates the seriousness of the alarm. When you create email notifications, the severity that you configure in the notification determines which alarms you can receive email notifications about.

Alarm States

Cisco SD-WAN Manager alarms are assigned a state based on their severity:

- Critical (red)—Serious events that impair or shut down the operation of an overlay network function.
- Major (yellow)—Serious events that affect, but do not shut down, the operational of a network function.
- Medium (blue)—Events that might impair the performance of a network function.
- Minor (green)—Events that might diminish the performance of a network function.

Note From Cisco vManage Release 20.11.1, the Medium alarms appear in green and the Minor alarms appear in blue.

The alarms listed as Active generally have a severity of either critical or major.

To view alarm details such as alarm name, sevcerity, and alarm description:

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

2. Click **Export** to export data for all alarms to a file in CSV format.

   Cisco SD-WAN Manager downloads data from the alarms table to the default download location of your browser. The data is downloaded as a CSV file with the name *alarms-mm-dd-yyyy.csv*.

3. Open the downloaded file to view alarm details.

For detailed information on each alarm, please see Cisco IOS XE Catalyst SD-WAN Alarms Guide.

Alarm Fields

Alarm messages can contain the following fields that provide more information about the alarm:

Table 33: Alarm Fields

Field	Description
Acknowledged	Whether the alarm has been viewed and acknowledged. This field allows Cisco SD-WAN Manager to distinguish between alarms that have already been reported and those that have not yet been addressed. To acknowledge an alarm, use the following API post call: https://*vmanage-ip-address*:8443/dataservice/alarms/markviewed Specify the data as: {“uuid”: [<*uuids of alarms to acknowledge*>]}
Active	Whether the alarm is still active. For alarms that are automatically cleared, when a network element recovers, the alarm is marked as "active":false.
Cleared By	Universally Unique IDentifier (UUID) of alarm to clear current alarm.
Cleared Time	Time when alarm was cleared. This field is present of for alarms whose "active" field is false.
Component	The software component for this alarm.
Devices	List of system IP addresses or router IDs of the affected devices.
Entry Time	Time when the alarm was raised, in milliseconds, expressed in UNIX time.
Message	Short message that describes the alarm.
Possible Causes	Possible causes for the event.
Rule Name Display	Name of the alarm. Use this name when querying for alarms of a particular type.
Suppressed	Whether this alarm is suppressed by other alarm.
Tenant	Indicates the tenant ID.
Severity	Severity of the alarm: critical, major, medium, minor.
Severity Number	Integer value for the severity: 1 (critical), 2 (major), 3 (medium), 4 (minor)
UUID	Unique identifier for the alarm

Field	Description
Values	Set of values for all the affected devices. These values, which are different for each alarm, are in addition to those shown in the "devices" field.
Values Short Display	Subset of the values field that provides a summary of the affected network devices.

Use the Alarms screen to display detailed information about alarms generated by control components and routers in the overlay network.

When the notification events that Cisco SD-WAN Manager receives indicate that the alarm condition has passed, most alarms clear themselves automatically. Cisco SD-WAN Manager then lists the alarm as Cleared, and the alarm state generally changes to medium or minor.

View Alarms

You can view alarms from the Cisco SD-WAN Manager dashboard by clicking the bell icon at the top-right corner. The alarms are grouped into Active or Cleared.

From Cisco vManage Release 20.11.1, when you click the bell icon at the top-right corner, the **Notifications** pane is displayed. Click the gear icon in this pane to filter or group alarms based on the following criteria:

- **Object**: Alarms are grouped based on the device for which the alarm is generated.
- **Severity**: Alarms are grouped based on the alarm severity.
- **Type**: Alarms are grouped based on the alarm type.

By default, alarms are displayed for the last 24 hours.

Alternatively, follow these steps to view alarms from the **Alarms** screen in Cisco SD-WAN Manager.

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

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

   The alarms are displayed in graphical and tabular formats.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

2. To view more details for a specific alarm, click **…** for the desired alarm, and then click **Alarm Details**.

   The **Alarm Details** window opens and displays the probable cause of the alarm, impacted entities, and other details.

From Cisco vManage Release 20.11.1, a new column called **Related Event** is added to the alarms page. This column displays events, related to an alarm, that occurs around the time the alarm is generated.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can use the following commands to view more details about alarms:

- **show sdwan alarms detail**: Provides detailed information about each alarm separated by a new line.
- **show sdwan alarms summary**: Provides alarm details such as the timestamp, event name, and severity in a tabular format.

The following is a sample output of the **show sdwan alarms detail** command:

```
vm5#show sdwan alarms detail

alarms 2023-06-01:00:38:46.868569
 event-name     geo-fence-alert-status
 severity-level minor
 host-name      Router
 kv-pair        [ system-ip=:: alert-type=device-tracking-stop alert-msg=Device Tracking
stopped in Geofencing Mode latitude=N/A longitude=N/A geo-color=None ]
-----------------------------------------------------

alarms 2023-06-01:00:38:47.730907
 event-name     system-reboot-complete
 severity-level major
 host-name      Router
 kv-pair        [ ]
-----------------------------------------------------

alarms 2023-06-01:00:39:00.633682
 event-name     pki-certificate-event
 severity-level critical
 host-name      Router
 kv-pair        [ trust-point=Trustpool event-type=pki-certificate-install
valid-from=2008-11-18T21:50:24+00:00 expires-at=2033-11-18T21:59:46+00:00 is-ca-cert=true
subject-name=cn=Cisco Root CA M1,o=Cisco issuer-name=cn=Cisco Root CA M1,o=Cisco
serial-number=2ED20E7347D333834B4FDD0DD7B6967E ]
-----------------------------------------------------
```

The following is a sample output of the **show sdwan alarms summary** command:

```
vm5#show sdwan alarms summary

time-stamp                    event-name                                    severity-l

-------------------------------------------------------------------------------------------
2023-06-01:00:38:46.868569      geo-fence-alert-status                        minor

2023-06-01:00:38:47.730907      system-reboot-complete                        major

2023-06-01:00:39:00.633682      pki-certificate-event                       critical

2023-06-01:00:39:00.644209      pki-certificate-event                       critical

2023-06-01:00:39:00.649363      pki-certificate-event                       critical

2023-06-01:00:39:00.652777      pki-certificate-event                       critical

2023-06-01:00:39:00.658387      pki-certificate-event                       critical

2023-06-01:00:39:00.661119      pki-certificate-event                       critical

2023-06-01:00:39:00.665882      pki-certificate-event                       critical

2023-06-01:00:39:00.669655      pki-certificate-event                       critical

2023-06-01:00:39:00.674912      pki-certificate-event                       critical

2023-06-01:00:39:00.683510      pki-certificate-event                       critical

2023-06-01:00:39:00.689850      pki-certificate-event                       critical

2023-06-01:00:39:00.692883      pki-certificate-event                       critical

2023-06-01:00:39:00.699143      pki-certificate-event                       critical

2023-06-01:00:39:00.702386      pki-certificate-event                       critical
```

```
2023-06-01:00:39:00.703653      pki-certificate-event                       critical

2023-06-01:00:39:00.704488      pki-certificate-event                       critical

2023-06-01:00:39:01.949479      pki-certificate-event                       critical

2023-06-01:00:40:38.992382      interface-state-change                        major

2023-06-01:00:40:39.040929      fib-updates                                   minor

2023-06-01:00:40:39.041866      fib-updates                                   minor
```

For more information, see *Troubleshooting Commands* in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

Filter Alarms

You can filter alarms to view details about alarms of interest.

Set Alarm Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
2. Click **Filter**.
3. In the **Severity** field, choose an alarm severity level from the drop-down list. You can specify more than one severity level.
4. In the **Active** field, choose active, cleared, or both types of alarm from the drop-down list. Active alarms are alarms that are currently on the device but have not been acknowledged.
5. In the **Alarm Name** field, choose an alarm name from the drop-down list. You can specify more than one alarm name.
6. Click **Search** to look for alarms that match the filter criteria.

Cisco SD-WAN Manager displays the alarms in both table and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

Set Advanced Alarm Filters

From Cisco vManage Release 20.11.1, you can set advanced filters to search for alarms that are generated by sites or devices. To set advanced filters:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
2. Click **Advanced Filter**.
3. In the **Object Type** drop-down menu, choose either **Site** or **Device** for which you want to view alarms.
4. In the **Object List** drop-down menu, choose either **Site ID** or **Device IP** for which you want to view alarms.

   You can choose more than one site or device.
5. In the **Severity** drop-down menu, choose one or more alarm severity levels from the drop-down list.

6. In the **Type** drop-down menu, choose one or more alarm names from the drop-down list.
7. Click **Apply Filters** to view alarms that match the filter criteria.

   The **Custom Filter Condition** allows you to filter alarms based on the OR condition, for example, 1 OR 2 OR 3.

You can add up to five filters. To delete a filter, click the **Bin** icon.

Cisco SD-WAN Manager displays the alarms in both table and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

Export Alarms

To export data for all alarms to a file in CSV format, click **Export**.

Cisco SD-WAN Manager downloads data from the alarms table to the default download location of your browser. The data is downloaded as a CSV file with the name *alarms-mm-dd-yyyy.csv*, where mm, dd, and yyyy are the month, day, and year that the file was downloaded.

Alarms data displayed on the graph can also be looked up in the downloaded file.

For example, if the graph displays an alarm data (Critical 2, Major 274, Medium 4, Minor 405) with date and time as 15/Feb/2022 3:30 AM, the same alarm data is also available in the downloaded file against a date and time range between 15/Feb/2022 3:00 AM and 15/Feb/2022 3:29 AM.

Alarm Notifications

You can configure Cisco SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

Enable Email Notifications

Configure SMTP and email recipient parameters to enable email notifications for alarms. Configure the SMTP and email recipient parameters on this screen:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Alarm Notifications**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Check the **Email Settings** check box.
4. Choose the security level for sending the email notifications. The security level can be **None**, **SSL**, or **TLS**.
5. In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.
6. In the **SMTP Port** field, enter the SMTP port number. For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
7. In the **From address** field, enter the full email address to include as the sender in email notifications.

8. In the **Reply to address** field, enter the full email address to include in the Reply-To field of the email. This address can be a noreply address, such as noreply@cisco.com.
9. Check the **Use SMTP Authentication** check box to enable SMTP authentication to the SMTP server.

   Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. The password that you type is hidden.
10. Click **Save**.



Note The email is sent from Cisco SD-WAN Manager Public-IP of VPN0 (Transport Interface) as a source interface.

Send Alarm Notifications

Before you begin: Ensure that Email Notifications are enabled under **Administration** > **Settings**, check whether **Alarm Notifications** is enabled and, **Email Settings** check box is checked.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.

From Cisco Catalyst SD-WAN Manager Release 20.15.1, configure Slack or Webex webhooks to receive alarm notifications.

To send email notifications when alarms occur:

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

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. Click **Add Alarm Notifications**.
4. In the **Notification Name** field, enter a name for the email notification. The name can be up to 128 characters and can contain only alphanumeric characters.
5. Expand the **Alarm Type** filter and do the following to configure the parameters:
   - From the **Object Type** drop-down list, choose a site or device you want to view the alarms for.
   - From the **Object List** drop-down list, choose a site ID or a device based on the type of object you have selected.
   - From the **Severity** drop-down list, choose the alarm severity.
   - From the **Types** drop-down list, choose an alarm type.
6. Expand the **Delivery Method** filter and click the following options to configure the alarm delivery method.
   a. Check the **Email** check box to trigger an email an alarm notification event occurs.
      1. In the **Email** field, enter one or more email addresses.
      2. (Optional) Click **Add New Email List** and enter an email list, if desired.
      3. In the **Email Threshold** field, set the maximum number of emails to be sent per minute. The number can be a value from 1 through 30. The default is 5.

b. Check the **WebHook** check box to trigger an HTTP callback to a webhook channel when an alarm notification event occurs.

1. From the **Choose a Channel for Webhook** drop-down list, choose a webhook channel to receive alarm notifications in
   - Cisco Webex
   - Slack
   - Custom
2. In the **WebHook URL** field, enter the URL of the webhook server.

   To create a webhook URL for Slack, go to *api.slack.com* see the section "Sending messages using incoming webhooks".

   To create a webhook URL for Webex, go to WebEx App Hub and see the section Incoming Webhooks.
3. In the **WebHook Threshold** field, enter the threshold value.

   The value you enter indicates the number of notifications that you receive for that webhook URL per minute. For example, if the **WebHook Threshold** value is 2, you receive two notifications for that webhook URL per minute. Notifications that are generated beyond the threshold are not delivered.
4. (Optional) From Cisco Catalyst SD-WAN Manager Release 20.16.1, if you have chosen **Custom** from the **Choose a Channel for Webhook** option, configure these additional parameters:

Field	Description
Username	Enter a username for authentication.
Password	Enter a password for authentication.
Network Connectivity	
Source VPN	From the drop-down list, choose a source VPN. • **0**: Transport VPN • **512**: Management VPN. Configure these fields if you have specified the tenant to manage the webhook notification services. These fields do not appear if they are managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet (VXLAN tunnel VPN IP subnet) where the webhook server is located. • (Optional) **Destination VPN**: Enter the destination VPN of the webhook server.

7. Click **Add**.

View and Edit Email Notification

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

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. For the desired notification, click the **View** icon to the right of the row.
4. When you are done viewing the notification, click **OK**.

Edit an Email Notification

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

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. For the desired email notification, click the **Edit** icon.
4. When you are done editing the notification, click **Update**.

Delete an Email Notification

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

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. For the desired email notification, click the **Trash Bin** icon.
4. In the confirmation dialog box, click **OK**.

Events

Table 34: Feature History

Feature Name	Release Information	Description
Event Notifications Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for event notifications, for Cisco IOS XE Catalyst SD-WAN devices.

Feature Name	Release Information	Description
Monitoring Event Trace for OMP Agent and SD-WAN Subsystem	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This feature enables monitoring and controlling the event trace function for a specified SD-WAN subsystem. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems.
Grouping of Events	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	The following enhancements are added to events: • Events are filtered and grouped based on severity for devices and sites. • View events for a particular device by clicking the … icon in the **Monitor > Devices** window. • View the top five events for a particular site in the **Monitor > Overview** window by choosing the **Site Topology** view icon and clicking the site.
Heatmap View for Events	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the events as **Critical**, **Major**, or **Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of events in a severity level.
Policy Enforcement Status	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download is successful.

Information About Events

When something of interest happens on an individual device in the overlay network, the device reports the event in the following ways:

- Send a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.
- Send an SNMP trap to the configured trap target. For each SNMP trap that a device generates, the device also generates a corresponding notification message.
- Generate a system logging (syslog) message and place it in a syslog file in the /var/log directory on the local device and, if configured, on a remote device.

Notifications are messages that the device sends to the Cisco SD-WAN Manager server.

Note All task logs, including activity logs, adminstration, and device logs, are always displayed in UTC timezone. This is the default and only supported timezone for these logs, irrespective of the Cisco SD-WAN Manager or local timezone settings.

Cisco IOS XE Catalyst SD-WAN device can store a maximum of 256 events. When the event limit exceeds, the device drops the oldest events. As a result, Cisco SD-WAN Manager may not receive those dropped events.

Events Details

To view events and information about a device on which an event was generated:

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

   The screen displays events in both graphical and tabular format.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays the events.

2. Click **...** and choose **Device Details** to view detailed information about any event generated on a device.

View Events by Using the CLI

To view information about a device on which an event was generated, for Cisco vEdge devices, you can use the **show notification stream viptela** command. Here is an example of the command output. The first line of the output shows the time when the message was generated (the SNMP eventTime). The time is shown in UTC format, not in the device's local time. The second line of the notification contains a description of the event, and the third line indicates the severity level.

```
vEdge# show notification stream viptela
notification
 eventTime 2015-04-17T14:39:41.687272+00:00
 bfd-state-change
  severity-level major
  host-name vEdge
  system-ip 1.1.4.2
  src-ip 192.168.1.4
  dst-ip 108.200.52.250
  proto ipsec
  src-port 12346
  dst-port 12406
  local-system-ip 1.1.4.2
  local-color default
  remote-system-ip 1.1.9.1
  remote-color default
  new-state down
 !
!
notification
 eventTime 2015-04-17T15:12:20.435831+00:00
 tunnel-ipsec-rekey
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  color default
 !
!
```

```
notification
 eventTime 2015-04-17T16:56:50.314986+00:00
 system-login-change
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  user-name admin
  user-id 9890
 !
```

To view information about a device on which an event was generated, for Cisco IOS XE Catalyst SD-WAN devices, you can use the **show sdwan notification stream** command. Here is an example of the command output. The first line of the output shows the time when the message was generated (the SNMP eventTime). The time is shown in UTC format, not in the device's local time. The second line of the notification contains a description of the event, and the third line indicates the severity level.

```
Device# show sdwan notification stream
notification
 eventTime 2020-03-03T02:50:04.211317+00:00
sla-change
  severity-level major
  host-name SanJose
  system-ip 4.4.4.103
  src-ip 10.124.19.15
  dst-ip 10.74.28.13
  proto ipsec
  src-port 12426
  dst-port 12346
  local-system-ip 4.4.4.103
  local-color default
  remote-system-ip 4.4.4.106
  remote-color biz-internet
  mean-loss 17
  mean-latency 13
  mean-jitter 19
  sla-classes None
  old-sla-classes Voice-And-Video
!
!
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.3, the **alarms alarm bfd-state-change syslog** command is used to view the BFD state change syslog message for any BFD state change event in the device. For complete details, see alarms alarm bfd-state-change syslog command.

```
Device(config-system)# alarms alarm bfd-state-change syslog
Device(config-alarm-bfd-state-change)# commit
```

Here is an example for BFD state change syslog message:

```
Jul 10 07:09:07.583: %Cisco-SDWAN-vm5-FTMD-5-NTCE-1000009: BFD-session 10.1.15.15:12346 ->
 10.1.16.16:12366,
local-tloc-index: 32775 -> remote-tloc-index: 32777, TLOC- local sys-ip: 172.16.255.15,
local color: lte -> remote
sys-ip: 172.16.255.16, remote color: lte, encap: IPSEC, new state->UP delete:false,
reason:REMOTE_FSM
```

Running configuration after enabling BFD state change:

```
 Device# show sdwan running-config
system
 gps-location latitude 35.0
 gps-location longitude -120.0
 system-ip             170.16.1.1
```

```
 simulated-devices     27 2
 simulated-color       red blue
 simulated-wan-ip      192.168.1.1
 domain-id             1
 site-id               10000
 admin-tech-on-failure
 organization-name     "vIPtela Inc Regression"
 vbond 10.0.12.26
 alarms alarm bfd-state-change
  syslog
 !
!
```

View Events

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

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays the events.

2. Click **...** and choose **Device Details** to view device details for a specific event.

FailoverEvents

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1

Failover events notify users of SIM failover events. A SIM failover event occurs when the currently active cellular link, whether with the primary or secondary SIM or carrier, loses connection and switches to the other SIM or carrier. When this happens, the device sends a **sim-fail-over** event to Cisco SD-WAN Manager.

Filter Events

Set Event Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Click the **Filter** icon from the search box.
3. Choose the time of the event from the **Event Time** drop-down list.
4. Choose the name of the host, from the **Hostname** drop-down list.
5. Choose the system IP of the devices from the **System IP** drop-down list to view generated events.
6. Choose the event name, from the generated events, from the **Name** drop-down list. You can choose more than one event name.
7. Choose the event severity level from the **Severity** drop-down list.

   The events generated by Cisco Catalyst SD-WAN devices are classified as:

   a. Critical—indicates that action needs to be taken immediately.

   b. Major—indicates that the problem needs immediate attention from you but, is not critical enough to bring down the network.

   c. Minor—is informational only.

8. Choose one or more components that caused the event from the **Component** drop-down list.
9. Choose the relevant event details from the **Details** drop-down list.

View the filtered events in Cisco SD-WAN Manager both as tabular and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, view the events in a heatmap format.

Set Advanced Event Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Click the **Advanced Filter** option.
3. In the **Object Type** drop-down menu, choose either **Site** or **Device** for which you want to view events.
4. In the **Object List** drop-down menu, choose either **Site ID** or **Device IP** for which you want to view events.

   You can choose more than one site or device.
5. In the **Severity** drop-down menu, choose one or more event severity levels from the drop-down list.
6. In the **Type** drop-down menu, choose one or more event names from the drop-down list.
7. Click **Apply Filters** to view events that match the filter criteria.
8. The **Custom Filter Condition** enables you in filtering events based on the OR condition, for example, 1 OR 2 OR 3.
9. Click the + icon and add up to five filters.
10. Click the **Bin** icon to delete a filter.

View the filtered events in Cisco SD-WAN Manager both as tabular and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, view the events in a heatmap format.

Export Events

To export data for all events to a file in CSV format, click **Export**.

Cisco SD-WAN Manager downloads data from the events table to the default download location of your browser. The data is downloaded as a CSV file with the name *events-mm-dd-yyyy.csv*, where mm, dd, and yyyy are the month, day, and year that the file was downloaded.

Monitor Event Notifications

To monitor and control the event trace function for a specified SD-WAN subsystem, use the **monitor event-trace** command in privileged EXEC mode. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems. For more information on the commands, see monitor event-trace sdwan and show monitor event-trace sdwan.

ACL Log

Use the ACL Log screen to view logs for access lists (ACLs) configured on a router. Routers collect ACL logs every 10 minutes.

Set ACL Log Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **ACL Log**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **ACL Log**.
2. Click the **Filter**.
3. In the VPN field, choose the entity, for which you are collecting ACL logs, from the drop-down list. You can choose only one VPN.
4. Click **Search** to search for logs that match the filter criteria.

Cisco SD-WAN Manager displays a log of activities in table format.

Audit Logging

Table 35: Feature History

Feature Name	Release Information	Description
Compare Template Configuration Changes Using Audit Logs	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces a **Config Diff** option for audit logs of device templates and feature templates. The **Config Diff** option shows configuration changes made to the template, comparing the current configuration and previous configuration. The **Config Diff** option is available for audit logs to view the configuration changes when a template is not attached to a device.
Enhancements to Audit Logging	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature introduces enhanced audit logging to monitor unauthorized login activity.

Information About Protecting Against Unauthorized Login Activity

Cisco SD-WAN Manager displays a log of activities both in table and graphical format.

These logs enable traceability which is essential in co-management environments and for governance purposes. These logs provide insights in the form of events which are generated based on the audit logs.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the audit logs are enhanced to capture high login frequency and failed login attempts to Cisco SD-WAN Manager.

Configure a Lockout Policy for Cisco SD-WAN Manager Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.



Note By default, CLI templates execute commands in global config mode.

1. Enter system configuration mode.

   system

2. Enter aaa configuration mode.

   aaa

3. Configure the lockout policy, which prevents new login attempts after reaching a threshold of failed attempts.

   The **fail-attempts** keyword indicates the number of failed attempts to log in. The **fail-interval** keyword indicates the time span in which to count failed login attempts. The **lockout-interval** keyword specifies how long Cisco SD-WAN Manager waits before allowing new login attempts.

   See aaa lockout-policy for information about the ranges and defaults for each parameter.

   lockout-policy lockout-interval *lockout-duration* **fail-interval** *fail-duration* **fail-attempts** *fail-count*

The following is a complete configuration example for a lockout policy:

```
system
 aaa
  lockout-policy
   lockout-interval 600
   fail-interval    60
   fail-attempts    5
  !
 !
!
```

In the above example, **fail-attempts** is 5, **fail-interval** is 60, and **lockout-interval** is 600. The result is that if there are 5 failed attempts to log in within 60 seconds, then the Cisco SD-WAN Manager does not allow additional attempts for a period of 600 seconds (10 minutes).

Verify a Lockout Policy for Cisco SD-WAN Manager

To verify the lockout policy configuration, use the **show running-config system aaa lockout-policy** command.

Configure a Login-Rate Alarm Threshold for Cisco SD-WAN Manager Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This procedure enables an alarm when the number of logins to the Cisco SD-WAN Manager reaches a specified threshold.

1. Enter system configuration mode.

   system

2. Enter alarms configuration mode.

   alarms

3. Configure a login-rate threshold.

   The **interval** keyword indicates the time span in which to count logins to Cisco SD-WAN Manager. The **num-logins** keyword specifies the number of logins within the specified interval that trigger an alarm.

   See login-rate for information about the ranges for each parameter.

   login-rate {**interval** *login-interval* | **num-logins** *login-count*}

Note There is no default value for **login-interval** and **num-logins**.

The following is a complete example for configuring a login-rate threshold:

```
system
 alarms
  login-rate
  interval 60
  num-logins 3
 !
!
!
```

Verify a Login-Rate Alarm Threshold for Cisco SD-WAN Manager

To verify the login rate alarm configuration, use the **show running-config system alarms** command.

```
vmanage# show running-config system alarms
system
 alarms
  login-rate
    interval 60
      num-logins 3
      !
    !
  !
```

Monitor Notifications of Failed Login Attempts to Cisco SD-WAN Manager

To view the history of failed login attempts, use the **show alarms history** command.

In the following example, there were two failed login attempts, after which Cisco SD-WAN Manager prevented additional login attempts.

```
vmanage# show alarms history | inc aaa-user
07/10     16:07:18      aaa-login-anomaly    major    user-name:test    remote:host:192.0.2.1
07/10     16:07:10      aaa-login-anomaly    major    user-name:test    remote:host:192.0.2.1
07/10     16:07:00      aaa-user-locked      major    user-name:test    remote:host:192.0.2.1
```

Monitor System Login Rate Alarms

To view alarms configured by the **login-rate** command, showing when the number of logins to Cisco SD-WAN Manager exceeds a configured threshold, use the **show alarms history** command, and view alarms of type **system-login-rate**.

```
vmanage# show alarms history

DATE    TIME        TYPE                  SEVERITY    DETAILS
-----------------------------------------------------------------
07/10   16:08:05   system-login-rate      minor    num-logins:3 time-interval:60
login-message:3 logins were done in 0 hours 1 minutes 8 seconds
07/10   16:08:05   system-login-change    minor    user-name:admin    user-id:145
```

View Audit Log Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Audit Log**.



Note Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Audit Log**.

Cisco SD-WAN Manager displays a log of activities both in table and graphical format.

2. Click **Filter** and choose one or more modules to filter the view.

   You can choose more than one **Module** type.

3. To export data for all audit logs to a file in CSV format, click **Export**.

   Cisco SD-WAN Manager downloads all data from the audit logs table to an Excel file to a CSV format. The file is downloaded to your browser's default download location and is named Audit_Logs.csv.

4. To view detailed information about any audit log, for the desired row in the table, click **...** and choose **Audit Log Details**.

   The **Audit Log Details** dialog box opens, displaying details of the audit log.

5. To view configuration changes made to a **Template** type **Module**, for the desired row in the table, click **...** adjacent to a log row for a template module, and choose **Config Diff**.

   The **Config Difference** pane displays a side-by-side view of the differences between the configuration that was originally in the template and the changes made to the configuration. To view the changes inline, click **Inline Diff**.

Note You can view changes to previous and current configurations made only where the module type is template.

6. To view the updated configuration on the device, click **Configuration**.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco SD-WAN Release 20.6.1, for template and policy configuration changes, the **Audit Logs** option displays the action performed. To view the previous and current configuration for any action, click **Audit Log Details**. Audit logs are collected when you create, update, or delete device or feature templates, and localized or centralized, and security policies. Audit logs shows the changes in API payloads when templates or policies are attached or not attached.

View Log of Configuration Template Activities

To view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose **WAN Edge List** or **Controllers**, and choose a device.
3. For the desired device, click **...** and choose **Template Log**.

Syslog Messages

When something of interest happens on an individual device in the overlay network, one of the ways the device reports it is by generating a system logging (syslog) message and place it in a syslog file in the /var/log directory on the local device and, if configured, on a remote device.

On Cisco Catalyst SD-WAN devices, you can log event notification system log (syslog) messages to files on the local device or on a remote host, or both. On the local device, syslog files are placed in the /var/log directory.

Configure System Logging

Logging syslog messages with a priority level of "error," to the local device's hard disk, is enabled by default. Log files are placed in the local /var/log directory. By default, log files are 10 MB in size, and up to 10 files are stored. After 10 files have been created, the oldest one is discarded to create a file for newer syslog messages.

To modify the default syslog parameters from Cisco SD-WAN Manager, use the Logging feature template. From the CLI, include the **logging disk** or **logging server** commands in the device configuration.

View Syslog Logging Information

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and, ensure that **Data Stream** is enabled.

2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device from the list of devices that appears.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**, and choose a device from the list of devices that appears.

3. Click **Troubleshooting** in the left pane.
4. In the **Logs** area, click **Debug Log**.
5. In the **Log Files** field, choose the name of the log file. The lower part of the screen displays the log information.

To view the contents of a syslog file from the CLI, use the **show log** command. For example:

```
Device# show log auth.log tail 10==> /var/log/auth.log <==auth.info: Nov 14 14:33:35 vedge
 sshd[2570]: Accepted publickey for admin from 10.0.1.1 port 39966 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 14 14:39:42 vedge sshd[2578]:
 Received disconnect from 10.0.1.1 port 39966:11: disconnected by userauth.info: Nov 14
14:39:42 vedge sshd[2578]: Disconnected from 10.0.1.1 port 39966auth.info: Nov 16 10:51:45
 vedge sshd[6106]: Accepted publickey for admin from 10.0.1.1 port 40012 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 16 11:21:55 vedge sshd[6108]:
 Received disconnect from 10.0.1.1 port 40012:11: disconnected by userauth.info: Nov 16
11:21:55 vedge sshd[6108]: Disconnected from 10.0.1.1 port 40012auth.info: Nov 17 12:59:52
 vedge sshd[15889]: Accepted publickey for admin from 10.0.1.1 port 40038 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 17 13:45:13 vedge
sshd[15894]: Received disconnect from 10.0.1.1 port 40038:11: disconnected by userauth.info:
 Nov 17 13:45:13 vedge sshd[15894]: Disconnected from 10.0.1.1 port 40038auth.info: Nov 17
 14:47:31 vedge sshd[30883]: Accepted publickey for admin from 10.0.1.1 port 40040 ssh2:
RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1s
```

To view the configured system logging settings for a device, use the **show logging** command from the CLI. For example:

```
Device# show logging
System logging to host  in vpn 0 is disabled
Priority for host logging is set to: emerg

System logging to disk is disabled
Priority for disk logging is set to:  err
File name for disk logging is set to:  /var/log/vsyslog
File size for disk logging is set to:  10 MB
File recycle count for disk logging is set to:  10

Syslog facility is set to: all facilities
```

System Log Files

Syslog messages at or above the default or configured priority value are recorded in a number of files in the /var/log directory on the local device. These files include the following:

- auth.log—Login, logout, and superuser access events, and usage of authorization systems.
- kern.log—Kernel messages
- messages—Consolidated log file that contains syslog messages from all sources.
- vconfd—All configuration-related syslog messages
- vdebug—All debug messages for modules whose debugging is turned on and all syslog messages above the configured priority value. Debug logging supports various levels of logging based on the module. Different modules implement the logging levels differently. For example, the system manager (sysmgr)

has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. To enable debugging, use the **debug** operational command.

- vsyslog—All syslog messages from Cisco SD-WAN processes (daemons) above the configured priority value. The default priority value is "informational" (severity level 6), so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages (severity levels 5 through 0, respectively) are saved.

The Cisco Catalyst SD-WAN software does not use the following standard LINUX files, which are present in /var/log, for logging: cron.log, debug, lpr.log, mail.log, and syslog.

The writing of messages to syslog files is not rate-limited. This means that if many syslog messages are generated in a short amount of time, the overflow messages are buffered and placed in a queue until they can be written to a syslog file. The overflow messages are not dropped.

For repeating syslog messages—identical messages that occur multiple times in succession—only one copy of the message is placed in the syslog file. The message is annotated to indicate the number of times that the message occurred.

The maximum length of a syslog message is 1024 bytes. Longer messages are truncated.

Syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages files. Each time Cisco SD-WAN Manager logs in to a Cisco vEdge device to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages:

```
Device(config)# system aaa logsViptela(config-logs)# audit-disableViptela(config-logs)#
netconf-disable
```

Syslog Message Format

Syslog message generated by the Cisco Catalyst SD-WAN software have the following format:

```
facility.source
date - source - module - level - MessageID: text-of-syslog-message
```

Here is an example syslog message. This is logged with local7 facility and level "notice".

Syslog Message Acronyms

The following acronyms are used in syslog messages and in the explanations of the messages:

Table 36:

Acronym	Meaning
confd	CLI configuration process
FTM	Forwarding table manager
FP	Forwarding process

Acronym	Meaning
RTM	Route table manager
TTM	Tunnel table manager

Note The SYSLOG format for viptela daemons before Cisco Catalyst SD-WAN Manager Release 20.15.x:

%<FACILITY>-<host>-<MNEMONIC>-<SEVERITY>-<SEVERITY-name>-<SEVERITY>-<MessageId>: <MESSAGE TEXT>ex:*Dec 11 09:36:27.358: %Cisco-SDWAN-NR-C8200-1N-4T-FTMD-5-NTCE-1000026: **HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src: 192.168.104.16/0 Dst: 192.168.104.20/0 Proto: 1 TOS: 0 LogReason: SDWAN_SERV_ICMP_EXCEPT_TS Count: 1Bytes: 114

New SYSLOG format for viptela daemons starting from Cisco Catalyst SD-WAN Manager Release 20.15.x:

%<FACILITY>-<SEVERITY>-<MNEMONIC>: <MESSAGE TEXT>ex: Dec 20 18:47:33.237: %SDWAN-5-FTMD : **HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src: 10.1.17.14/12346 Dst: 192.168.60.100/12346 Proto: 17 TOS: 192 LogReason: SDWAN_SERV_UDP Count: 1Bytes: 171 Ingress-Interface: GigabitEthernet2 Egress-Interface: GigabitEthernet2

To see a list of the various syslog messages generated, see Syslog Messages in the Appendix.

Cisco SD-WAN Manager Logs

Table 37: Feature History

Feature Name	Release Information	Description
Manage Log Size	Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature lets you temporarily increase the log size for troubleshooting purposes.

When something of interest happens on a Cisco SD-WAN Manager device or a cluster, the device reports it. One of the ways it reports is by generating a logging message. Then the message is placed in a log file in the /var/log/nms directory on the local device.

Configure Cisco SD-WAN Manager Logs

Cisco SD-WAN Manager logs with a priority level of information to the local device's hard disk, is enabled by default. Log files are placed in the local /var/log/nms directory. By default, each log file is 16 MB in size. Cisco SD-WAN Manager rolls over and stores up to 10 log files every day. After creating 10 files, it discards the oldest one to make room for new Cisco SD-WAN Manager logs.

You can configure the following log files:

- vmanage-server
- vmanage-server-statistics
- vmanage-server-olap

- vmanage-server-deviceconfig-template
- vmanage-server-device-config

Manage Log Size

From Cisco Catalyst SD-WAN Manager Release 20.16.1, you can temporarily increase the log size to 250 MB for troubleshooting purposes. Use the Cisco Catalyst SD-WAN REST API call provided in the Cisco Developer Documentation.

When you restart Cisco SD-WAN Manager, the log size reverts to 16 MB by default.

View Cisco SD-WAN Manager Logs

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. Click **Generate Admin Tech for Manager** > **Logs** and click **Generate** to collect the logs from all the Cisco SD-WAN Managers in the system.

   Click the ellipsis icon under **Actions**, choose **Generate Admin Tech** > **Logs**, and click **Generate** to collect logs from a particular device in the system.
3. Click **Show admin-tech List** to view the progress of the download. You can access the file when it's available.

To view the contents of the Cisco SD-WAN Manager log file from the CLI, use the **show log** command. For example:

```
Device# show log nms/vmanage-server.log
```

Note All task logs, including activity logs, adminstration, and device logs, are always displayed in UTC timezone. This is the default and only supported timezone for these logs, irrespective of the Cisco SD-WAN Manager or local timezone settings.

Cisco SD-WAN Manager Log Files

Cisco SD-WAN Manager records logs that meet or exceed the default or configured priority in the /var/log/nms directory on the local device. Some of these files include:

- vmanage-server.log
- vmanage-appserver.log
- vmanage-server-olap.log
- vmanage-server-device-config.log
- vmanage-server-rest.log

Cisco SD-WAN Manager Log Format

Cisco SD-WAN Manager logs generated by the Cisco Catalyst SD-WAN software is of the following format:

```
                Date - Log Level - Restful API Tracing ID - Host Name - Class - Thread -
Tenant ID [Optional]
                 - message
```

Here is an example of a log entry using the local6 facility at the 'INFO' level:.

```
04-Apr-2023 10:22:27,969 CST INFO [af7c0465-1fca-4e6d-8d39-6c03b1357b4b] [vmanage_scale1]
[VmanageSyslogLogger] (default task-3459) |default| deviceAction: Request for action
```

View Log of Certificate Activities

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

To view the status of certificate-related activities, use the Cisco SD-WAN Manager **Configuration** > **Certificates** window.

1. From the Cisco SD-WAN Manager toolbar, click the tasks icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco SD-WAN Manager opens a status window displaying the status of the task and details of the device on which the task was performed.

Binary Trace for Cisco Catalyst SD-WAN Daemons

Table 38: Feature History

Feature Name	Release Information	Description
Binary Trace for Cisco Catalyst SD-WAN Daemons	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Binary trace enhances the troubleshooting of Cisco Catalyst SD-WAN daemons. Binary trace logs messages from the daemons in a binary format. Messages are logged faster in the binary format, improving the logging performance, and use lesser storage space than in the ASCII format. The binary trace CLI allows you to set the debug levels for additional process modules compared to the **debug** command. From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, binary trace is supported for the following Cisco Catalyst SD-WAN daemons: • fpmd • ftm • ompd • vdaemon **Note** Starting from Cisco Catalyst SD-WAN Control Components Release 20.15.1, when using the `debug vdaemon all` command, a warning will be displayed about the potential impact on the network performance. • cfgmgr

Binary trace collects messages from process modules and records the information in a binary format. You can configure the level at which binary trace logs messages and view the recorded messages for tracing and troubleshooting errors in process execution.

Binary trace improves run-time performance by recording messages faster in the binary format than is possible while recording messages in the ASCII format. The binary format also allows for more efficient storage than the ASCII format. The messages are decoded from the binary format to an ASCII format when you view or save the trace to file.

Supported Cisco Catalyst SD-WAN Daemons

Binary trace is supported for the following Cisco Catalyst SD-WAN daemons and their modules:

Cisco Catalyst SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Configure Binary Trace Level

Configure the binary trace level for one or all modules of a Cisco Catalyst SD-WAN process on a specific hardware slot.

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **set platform software trace** *process slot module level*

Example:

```
Device# set platform software trace fpmd R0 config debug
```

Configures the trace level for one or all the modules of a Cisco Catalyst SD-WAN process executing on the specified hardware slot.

- *process*: Specify a Cisco Catalyst SD-WAN process from among fpmd, ftm, ompd, vdaemon, cfgmgr.
- *slot*: Hardware slot from which process messages must be logged.
- *module*: Configure the trace level for one or all the modules of the process.
- *level*: Select one of the following trace levels:
  - debug: Debug messages
  - emergency: Emergency possible message
  - error: Error messages
  - info: Informational messages

- noise: Maximum possible message
- notice: Notice messages
- verbose: Verbose debug messages
- warning: Warning messages

View Binary Trace Level

View the binary trace levels for the modules of a Cisco Catalyst SD-WAN process executing on a specific hardware slot.

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show platform software trace level** *process slot*

Example:

```
Device# show platform software trace level fpmd R0
```

Displays the binary trace levels for all the modules of the process on the specified hardware slot.

- *process*: Specify a Cisco Catalyst SD-WAN process from among fpmd, ftm, ompd, vdaemon, cfgmgr.
- *slot*: Hardware slot from which process messages must be logged.

View Messages Logged by Binary Trace for a Cisco Catalyst SD-WAN Process

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show logging process** *process-name* [*filtering-options*]

Example:

```
Device# show logging process fpmd internal fru R0 reverse
```

Displays logs of the specified process or processes.

For *process-name*, specify a process from among fpmd, ftm, ompd, vdaemon, cfgmgr. You can also specify a comma-separated list of processes, for example, `fpmd, ftm`.

If you do not specify any *filtering-options*, command displays logs of the binary trace level information and higher severity levels that have been collected in the last 10 minutes.

For more information on the filtering options, see the command page for **show logging process**.

View Messages Logged by Binary Trace for All Cisco Catalyst SD-WAN Processes

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show logging profile sdwan** [*filtering-options*]

Example:

```
Device# show logging profile sdwan start last boot
```

Displays logs of all Cisco Catalyst SD-WAN processes and their modules in chronological order.

If you do not specify any *filtering-options*, command displays logs of the binary trace level information and higher severity levels that have been collected in the last 10 minutes.

For more information on the filtering options, see the command page for **show logging profile sdwan**.

Traffic Logs

Traffic logs is a network flow monitoring tool integrated into Cisco Catalyst SD-WAN Analytics. It allows authorized users to access and visualize filtered firewall connection event logs derived from voluminous flow records. Users can submit queries specifying criteria such as time frame, site name, devices to get logs on-demand.



Note Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager displays Cisco SD-WAN Analytics using a dynamic navbar in a converged user interface. You can see the traffic logs Tab when Cisco SD-WAN Analytics is enabled. Click on this tab to render the Cisco SD-WAN Analytics page.

Click on any other Cisco SD-WAN Manager menu or tab to go back to Cisco SD-WAN Manager.

Information about traffic logs

Traffic logs is a network flow monitoring tool integrated into Cisco Catalyst SD-WAN Analytics. It allows authorized users to access and visualize filtered firewall connection event logs derived from voluminous flow records. Users can submit queries specifying criteria such as time frame, site name, devices to get logs on-demand.



Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager displays Cisco SD-WAN Analytics using a dynamic navbar in a converged user interface. You can see the traffic logs Tab when Cisco SD-WAN Analytics is enabled. Click on this tab to render the Cisco SD-WAN Analytics page.

Click on any other Cisco SD-WAN Manager menu or tab to go back to Cisco SD-WAN Manager.

Benefits of traffic logs

- Provides detailed visibility into raw flow logs, including firewall connection events and related attributes.
- Supports scalable processing and analysis of high-volume flow data.
- Enables users to filter logs of interest to quickly narrow down large datasets, even across millions of records.
- Utilizes SD-WAN Analytics to deliver both the frontend and backend as a cloud-based solution.

Restrictions for traffic logs

- Only one request can be made at a time across the fabric.

  All users of the fabric have to wait for this request to complete.

- There are rate limits at the fabric level.

  24 requests can be made in a period of 24 hours, and 24 exports can be made in a period of 24 hours, which is calculated across all users of the fabric.

- Maximum of five devices can be queried at a time.
- Maximum time duration for filtering is seven days.
- The data fetched for a log query is limited to within the last month.
- Export is limited to 1,048,576 rows to be compatible with tools like Excel.

Generate traffic logs using Cisco SD-WAN Manager

Procedure

Step 1 Click the **Logs** tab.

Step 2 In the query builder section, specify the mandatory filters:

- Time period
- Site(s) (maximum five)
- Device(s) (maximum five)

Step 3 Click the **Get Logs** button.

Note
If available, the last traffic logs request would be fetched and visualized by default.

Table 39:

Field	Description
Event Time (in UTC)	Displays the exact date and time thta the event was logged, recorded in Coordinated Universal Time (UTC) for standardization.
Site	Displays the physical location, office, or branch where the event was generated.
Hostname	Displays the name given to a device on a network, which can be used to identify it. It can be up to 128 characters long.

Field	Description
System IP	Displays the IP address assigned to the system or device that generated the event log.
VPN ID	Displays an identifier (such as a number or string) representing the specific VPN tunnel or connection involved in the event.
Source IP	Displays the IP address from which the network traffic originated.
Destination IP	Displays the IP address to which the network traffic was sent.
Source Port	Displays the port number used by the source device in the network communication
Destination Port	Displays the port number used by the destination device in the network communication.
Protocol	Displays the communication protocol used for the network session.
Application Name	Displays the name of the application or service associated with the network traffic
Username/SGT	Displays the account name or ID of the user associated with the event, if available.
Firewall Rule	Displays the specific rule within the firewall that matched and processed the event.
FW Policy	Displays the name or identifier of the firewall policy that applies to the traffic or event.
FW Action	Displays the action taken by the firewall for this event.

Note
For the firewall attribute columns to be populated, you need to set NGFW policies up in Cisco SD-WAN Manager.

What to do next

Click the **Export** button to download the results for offline analysis.

Troubleshoot traffic logs

If you wish to troubleshoot traffic logs, contact Cisco TAC for assistance.

Safety Barriers

Table 40: Feature History

Feature	Release Information	Description
Safety barriers	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Safety barriers protect the Cisco SD-WAN Controller during resource constraints by monitoring CPU, memory, and disk usage. When thresholds are exceeded, safety barriers generate alarms and restrict services that can further impact resource availability.

Safety Barriers

The safety barriers protect the Cisco Catalyst SD-WAN Controller when system resources such as CPU, memory, and disk experience heavy usage. This feature provides resource-safeguarding actions and generates alarms in Cisco SD-WAN Manager to prevent system-wide critical failures. This feature acts as a guard to maintain the stability and reliability of only Cisco Catalyst SD-WAN Controllers.

Safety barriers provide regulating mechanisms to prevent system meltdowns caused by uncontrolled resource consumption. You can configure safety barriers using CLI or CLI template:

```
Device (config)# system safety-barriers
```

Safety barriers are disabled by default. All CPU or memory restrictive actions take place only when the safety barrier is configured on Cisco Catalyst SD-WAN Controller.

CPU alarm and actions

A CPU Barrier alarm is generated when CPU usage exceeds the 80% threshold for 300 seconds. Restrictive actions for CPU and Memory occur only if the safety-barriers are configured.

The following CPU actions take place to avoid system failure:

- Under high CPU barrier conditions, any system or policy configurations from Cisco SD-WAN Manager are delayed and re-attempted for five minutes, before indicating the failure.
- The following show commands (internal and external) are rejected:
  - **show omp tlocs**
  - **show omp services**
  - **show omp routes**
  - **show omp ipv6-routes**
  - **show omp peer**
  - **show omp l2-statuses**
  - **show omp l2-services**

- **show omp l2-routes**
- **show tenant omp**
- **show internal/support omp rib vroute**
- **show internal/support omp rib-list**
- **show internal/support ttmd groups**
- **show internal/support ttmd links**
- **show internal/support ttmd tlocs**

- **clear omp all** is rejected

Disk alarm and actions

A Disk Barrier alarm is generated when disk usage exceeds the 80% threshold for 5 seconds. The following disk actions take place to avoid system failure:

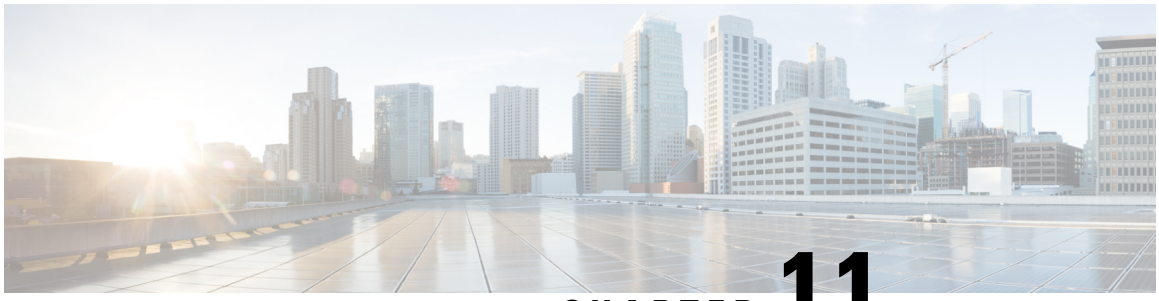
- Core files and admin tech files in the disk are cleaned up based on their age. Files are deleted in this order:
  - Admin techs and image files in home directories older than 2 days,
  - crash files in /var/crash/ older than 30 days,
  - admin tech files in /var/admin-tech older than 30 days,
  - crash files in /var/crash/ older than 7 days,
  - admin tech files in /var/admin-tech older than 7 days,
  - crash files in /var/crash/ older than 2 days
  - admin tech files in /var/admin-tech older than 2 days.

Memory alarm and actions

A Memory Barrier alarm is generated when memory usage exceeds the 80% threshold for 300 seconds. The following memory actions take place to avoid system failure:

- No new control connections are allowed for any new edge sites added to the overlay.
- Clear control connections are rejected.
- OMP peering is not allowed.
- No new RIB Ins (Routing Information Base) for existing peers are allowed.
- Configuration of Control-Policy sequences involving **Set TLOC**, **Set TLOC-List**, or **Set Service** is not allowed.

For more information about safety barrier alarms, refer to Alarm Details in the *Cisco IOS XE Catalyst SD-WAN Alarms Guide*.



CHAPTER 11

Reports

Table 41: Feature History

Feature Name	Release Information	Description
Reports	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Reports provide a summarized view of the health and performance of the sites, devices, and tunnels in your network. You can schedule a report, download it as a PDF document, and receive it as an email. The **Reports** menu has been added to Cisco SD-WAN Manager.
Additional Report Types and Formats	Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature introduces several new report types, including Security reports, which are available in CSV or PDF format.

- Information About Reports, on page 209
- Restrictions for Reports, on page 210
- Run a Report, on page 210
- Configure Email Settings, on page 211
- View Generated Reports, on page 212
- Download a Report, on page 212
- Edit a Report, on page 212
- Rerun a Report, on page 212
- Cancel a Scheduled Report, on page 213
- Delete a Report, on page 213

Information About Reports

In Cisco SD-WAN Manager, you can generate reports with information about the health of your sites, devices, and tunnels.

The following reports are available in Cisco SD-WAN Manager:

- Executive Summary Report
- Link Availability Report
- Site Availability Report

- Link Utilization Report
- Link SLA Report
- Application Usage Report
- IPS Event Collection Report
- Firewall Enforcement Report
- Malware File Collection Report
- Internet Browsing Report
- All Applications Report



Note The All Applications Report is available only on a Converged dasboard. For more information about Converged dashboard, see Converged Dashboard for SD-WAN Analytics and SD-WAN Manager.

You can generate these reports in PDF or CSV formats. You can generate up to 100 reports in PDF format, while CSV has no limit.

Restrictions for Reports

- Reports are available in both single-tenant and multitenant deployments. In a multitenant environment, the reports are accessible only through the tenant dashboard.
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, NMS service status is changed to an on-demand model.

  The command **request nms all status** shows **Enabled: false** and **Status: not running** when inactive.

Run a Report

Before You Begin

Ensure you configure email settings in Cisco SD-WAN Manager for scheduling reports. For more information, see Configure Email Settings, on page 211. This step is necessary only if you want the report to be emailed.

Run a Report

1. From the Cisco SD-WAN Manager menu, choose **Reports** > **Reports**.
2. Click **Report Templates**.
3. Choose a report and click **Generate** on the report.

Field	Description
Report Name	Enter a name for the report.
Sites	Choose the sites for which you want to generate the report.
File Type	Choose a file type in which to render the report.
Time Range	Choose the time range for which you want to generate the report. Default: 7 days
Schedule	Choose one of the schedule options. • **Run Now**: Run the report immediately. • **Run Later (One-Time)**: To run the report once, enter the start date and start time. • **Run Recurring**: To run the report periodically, enter the start date and start time, and choose a frequency from the **Repeats** drop-down list.
Delivery	• **Email Report**: Send the report via email. • **Email**: Enter up to five email addresses.

4. Click **Generate Report**.

Configure Email Settings

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Alarm Notifications**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Check the **Email Settings** check box.
4. Choose the security level for sending the email notifications. The security level can be **None**, **SSL**, or **TLS**.
5. In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.
6. In the **SMTP Port** field, enter the SMTP port number. For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
7. In the **From address** field, enter the full email address to include as the sender in email notifications.
8. In the **Reply to address** field, enter the full email address to include in the Reply-To field of the email. This address can be a no-reply address, such as noreply@cisco.com.
9. Check the **Use SMTP Authentication** check box to enable SMTP authentication to the SMTP server.

If you enable SMTP authentication and do not select an SMTP port (port 25), Cisco SD-WAN Manager internally sets the SSL protocol property when it sends the email notification. This ensures the email is sent securely.

Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. The password that you type is hidden.

10. Click **Save**.

View Generated Reports

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.

   The **My Reports** page displays all the generated reports. Use the filter options (schedule, status, and time frame) in the **Summary** pane or enter a keyword in the search bar to view the reports of your interest.

Download a Report

The download option is available only if the report generation is complete.

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **…** adjacent to the corresponding report name and choose **Download**.

Edit a Report

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **…** adjacent to the corresponding report name and choose **Edit**.
4. In the **Executive Summary Report** pane, review and edit the configured parameters of the report.
5. Click **Update Report**.

After you edit and update the report configuration, any future report generations reflect the new configuration.

Rerun a Report

The option to rerun a report is available when a report is in the scheduled, completed, or failed state.

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.

3. Click **…** adjacent to the corresponding report name and choose **Run Now**.

Cancel a Scheduled Report

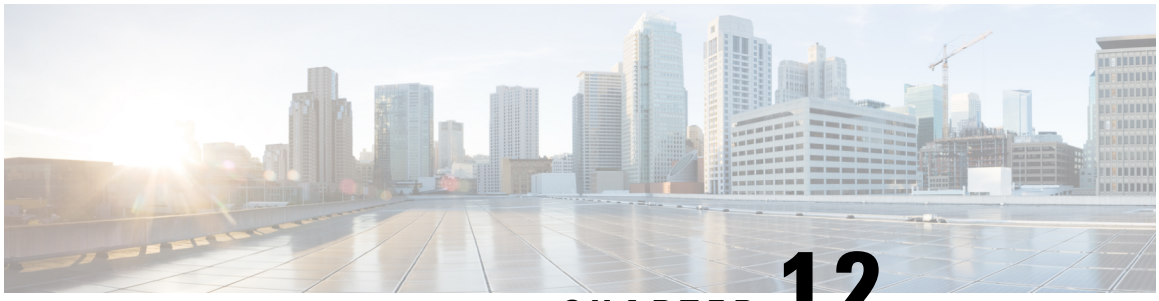
The cancel option is available only when a report is in the scheduled state.

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **…** adjacent to the corresponding report name and choose **Cancel**.

Delete a Report

The delete option is available when a report is in the scheduled, completed, or failed state.

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **…** adjacent to the corresponding report name and choose **Delete**.



CHAPTER 12

Manage Software Upgrade and Repository

- Manage Software Upgrade and Repository, on page 216
- Information about software upgrade, on page 219
- Restrictions for software upgrade, on page 222
- Upgrade Virtual Image on a Device, on page 223
- Upgrade the Software Image on a Device, on page 224
- Activate a New Software Image, on page 226
- Upgrade a CSP Device with a Cisco NFVIS Upgrade Image, on page 227
- Delete a Software Image, on page 228
- Set the Default Software Version, on page 228
- Export Device Data in CSV Format, on page 228
- View Log of Software Upgrade Activities, on page 229
- Manage Software Repository, on page 229

Manage Software Upgrade and Repository

Table 42: Feature History

Feature Name	Release Information	Description
Software Upgrade Using a Remote Server	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco SD-WAN Manager, and add locations of software images on the remote server to the Cisco SD-WAN Manager software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.

Feature Name	Release Information	Description
Device version compliance in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.x Cisco Catalyst SD-WAN Manager Release 20.18.1	

Feature Name	Release Information	Description
		The Device Version Compliance feature in Cisco SD-WAN Manager ensures device compatibility when upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1. The Cisco Catalyst SD-WAN Manager Release 20.18.1 supports devices up to N-2 long-lived releases and does not support older versions in the Cisco Catalyst SD-WAN overlay. This feature implements the following key aspects: • Upgrade Blocking: Prevents Cisco SD-WAN Manager upgrades through the user interface if the overlay contains devices with software versions older than N-2. • Post-Upgrade Notification: After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance banners and alarms. • Removal of End-of-Life (EOL) Platforms from ZTP Settings: Removes unsupported device families from the Zero Touch Provisioning settings page in Cisco SD-WAN Manager. • Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition: Changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system when they are added

Feature Name	Release Information	Description
		to and recognized by Cisco SD-WAN Manager. This change removes the Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers migration menu in Cisco SD-WAN Manager when Cisco IOS XE operating system is detected.

Information about software upgrade

Use the Software Upgrade window to download new software images and to upgrade the software image running on a Cisco Catalyst SD-WAN device.

From a centralized Cisco SD-WAN Manager, you can upgrade the software on Cisco Catalyst SD-WAN devices in the overlay network and reboot them with the new software. You can do this for a single device or for multiple devices simultaneously.

When you upgrade a group of Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices in either a standalone or Cisco SD-WAN Manager cluster deployment, the software upgrade and reboot is performed first on the Cisco Catalyst SD-WAN Validator, next on the Cisco Catalyst SD-WAN Controller, and finally on the Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices. Up to 40 Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices can be upgraded and rebooted in parallel, depending on CPU resources.

Introduced in the Cisco vManage Release 20.8.1, the software upgrade workflow feature simplifies the software upgrade process for the Cisco Catalyst SD-WAN edge devices through a guided workflow and displays the various device and software upgrade statuses. For more information on creating a Software Upgrade Workflow, see Software Upgrade Workflow.

Note

- You cannot include Cisco SD-WAN Manager in a group software upgrade operation. You must upgrade and reboot the Cisco SD-WAN Manager server by itself.
- You can create a software upgrade workflow only for upgrading the Cisco Catalyst SD-WAN edge devices.
- It is recommended that you perform all software upgrades from Cisco SD-WAN Manager rather than from the CLI.
- For software compatibility information, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are upgraded sequentially. If a device fails, subsequent upgrades are skipped.

Prior to Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are also upgraded sequentially. Even if a device fails, the remaining devices continue to upgrade.

The upgrade will proceed sequentially only if the certificate status of all devices with the same site ID is valid. If any device has an invalid certificate status, upgrades will occur in parallel.

Device version compliance

Device version compliance is a policy that

- ensures compatibility of network devices with Cisco SD-WAN Manager upgrades,
- supports devices in the overlay up to N-2 long-lived releases, and
- does not support devices older than this version in the overlay after an upgrade.

The release versions referenced in this policy are defined as follows:

- N: Represents the current Cisco SD-WAN Manager release (for example, Cisco Catalyst SD-WAN Manager Release 20.18.x).
- N-1: Refers to the prior long-lived release (for example, Cisco Catalyst SD-WAN Manager Release 20.15.x).
- N-2: Refers to the long-lived release two versions prior (for example, Cisco Catalyst SD-WAN Manager Release 20.12.x).

If you onboard a new device of any version, the device is still supported. However, after onboarding, this device will be flagged with a red banner in Cisco SD-WAN Manager, indicating that an upgrade is required.

Upgrade behavior

This feature changes the upgrade process depending on how the upgrade is initiated:

When a user initiates an upgrade to a newer Cisco SD-WAN Manager version (e.g., Cisco Catalyst SD-WAN Manager Release 20.18.x) through the UI, the upgrade is blocked if the overlay contains devices with software versions older than N-2 (e.g., Cisco Catalyst SD-WAN Manager Release 20.12.x).

For instance, if Cisco SD-WAN Manager is on version Cisco Catalyst SD-WAN Manager Release 20.15.1 and devices are on Cisco IOS XE Catalyst SD-WAN Release 17.9.x, an upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x will be blocked because the minimum supported device version for Cisco Catalyst SD-WAN Manager Release 20.18.x is Cisco Catalyst SD-WAN Manager Release 20.12.x. All devices in the network must be on version Cisco IOS XE Catalyst SD-WAN Release 17.12.x or above for the upgrade to proceed.

If a user performs the upgrade via the CLI, the upgrade proceeds even if devices are older than N-2. However, Cisco SD-WAN Manager displays a banner indicating the presence of less than N-2 devices and recommends upgrading them.

Device compliance notifications

Cisco SD-WAN Manager uses two primary methods to flag incompatible devices. If a user performs any operations on devices running versions older than N-2, it may lead to unexpected errors or device operational failures.

Compliance messages

A message appears in Cisco SD-WAN Manager when incompatible devices are detected. This message recommends upgrading those devices. Clicking the message redirects the user to the **Compliance & Conflicts** page, which displays the device status and software version.

- Error: If devices are less than N-2 versions, an error message appears:

```
Incompatible software version detected. Click here for details.
```

- Error: If devices are on N-3 version, or if Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Validator are on N-1 or N-2 versions, an error message appears:
  - N-3 devices with N version of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and WAN Edge have been
 detected. Upgrade the software immediately to avoid any disruptions.
```

  - N-3 devices with N-1 or lesser versions of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and Controller, Validator
 and WAN Edge have been detected. Upgrade the software immediately to avoid
 any disruptions.
```

Out of compliance alarm

An alarm is raised in the **Alarm Details** page in Cisco SD-WAN Manager when devices running versions older than N-2 are detected in the overlay. Multiple alarms may be raised if device versions change.

If the list of out-of-compliance devices contains five or fewer entries, the **Probable Causes** section displays the device hostnames. For more than five devices, the **Probable Causes** section displays only the count of out-of-compliance devices.

Unsupported devices

Starting with the Cisco Catalyst SD-WAN Manager Release 20.18.x release, Cisco SD-WAN Manager removes unsupported device families from the Zero Touch Provisioning (ZTP) settings page. These platform families include:

- Cisco vEdge Cloud
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 1002-X Series Aggregation Services Routers
- Cisco vEdge devices

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. As a result, Cisco SD-WAN Manager removes the Migration menu if it detects that a Cisco ISR 1100 and ISR 1100X Series Integrated Services Router is running Cisco IOS XE operating system. However, the Migration menu continues to be displayed for devices running Viptela operating system.

Restrictions for software upgrade

Upgrade only

The software upgrade process can only install a later release (upgrade) not an earlier release (downgrade). For example you can upgrade from 17.15.1 to 17.16.1.

Migration of the device configuration only when installing a release

A device migrates the current active configuration to another release only when installing the new release. If you have a release that is installed but out of sync with recent configuration changes, you can trigger a fresh migration of the current configuration. Uninstall the release that is out of sync, then re-install the release.

Reactivating an earlier release

A device can have more than one release installed, but only one release is active at a given time.

If a device is running release A (example: 17.15.1), you can install a later release B (example: 17.16.1). After you activate release B, the inactive release A keeps its configuration in the state when release A was last active. Configuration changes you make while release B is active do not affect the configuration stored with release A.

If you keep release A installed on the device and later reactivate release A, the device uses the stored configuration reflecting the state when release A was last active.

Device version compatibility

The following restrictions are the restrictions for device compatibility when upgrading Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.18.x:

Device software version support

Cisco Catalyst SD-WAN Manager Release 20.18.x supports devices running up to N-2 long-lived software releases. Devices running software versions older than N-2 are not supported in the Cisco Catalyst SD-WAN overlay. For more information, see Device version compliance, on page 220.

Upgrade blocking

Cisco SD-WAN Manager prevents upgrades through the user interface if the Cisco Catalyst SD-WAN overlay contains devices with software versions older than N-2. For more information, see the section Upgrade behavior in Device version compliance, on page 220.

Post-Upgrade notification

After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance notifications and alarms. For more information, see the section Device compliance notifications in Device version compliance, on page 220.

Removal of End-of-Life platforms in Cisco SD-WAN Manager

Cisco SD-WAN Manager removes unsupported device families from the **Zero Touch Provisioning** settings page. For more information, see the section Unsupported devices in Device version compliance, on page 220.

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. This change helps prevent upgrade blocks for these devices and removes the migration menu when Cisco IOS XE operating system is detected. For more information, see the section Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition in Device version compliance, on page 220.

Upgrade Virtual Image on a Device

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. To choose a device, check the check box for the desired device.
3. Click **Upgrade Virtual Image**.

   The **Virtual Image Upgrade** dialog box opens.
4. Choose **Manager** or **Remote Server - Manager**, as applicable.
5. From the **Upgrade to Version** drop-down list, choose the virtual image version to upgrade the device to.
6. Click **Upgrade**.

Upgrade the Software Image on a Device

Note

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco Catalyst SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, Upgrade Cisco SD-WAN Manager Cluster.
- Starting from Cisco vManage Release 20.11.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*

To upgrade the software image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager** based on the type of device for which you wish to upgrade the software.
3. In the table of devices, select the devices to upgrade by selecting the check box on the far left.

Note While upgrading Cisco SD-WAN Manager clusters, select all the nodes of the cluster in the table.

4. Click **Upgrade**.
5. In the **Software Upgrade** slide-in pane, do as follows:
   a. Choose the server from which the device should download the image: **Manager**, **Remote Server**, or **Remote Server – Manager**.

Note

- The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you chose **Remote Server**, ensure that the device can reach the remote server.
- Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
  - User ID: a-z, 0-9, ., _, -
  - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
  - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

Note Software images created before upgrading the Cisco SD-WAN Manager to version Cisco Catalyst SD-WAN Manager Release 20.18.1 lack platform family and version details. To use these images after the upgrade, edit them in **Maintenance** > **Software Repository** and add the required platform family and version information.

b. For **Manager**, choose the image version from the **Version** drop-down list.

c. For **Remote Server – Manager**, choose the **Manager OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.

d. For **Remote Server**, configure the following:

Remote Server Name	Choose the remote server that has the image.
Image Filename	Choose the image filename from the drop-down list.

e. Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

f. Click **Upgrade**.

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

6. Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.
7. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** and view the devices.
8. Click **WAN Edge**, **Controller**, or **Manager** based on the type of device for which you wish to upgrade the software.
9. In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

Note

- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge devices, which have a default time of 12 minutes.
- If you upgrade the Cisco vEdge device software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco vEdge device software.
- When upgrading a Cisco CSR1000V or Cisco ISRv device to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or later, the software upgrade also upgrades the device to a Cisco Catalyst 8000V. After the upgrade, on the Devices page, the **Chassis Number** and **Device Model** columns show the device as a Cisco CSR1000V or Cisco ISRv, but the device has actually been upgraded to a Cisco Catalyst 8000V. The reason for preserving the old name is to avoid invalidating licenses, and so on. To confirm that the device has been upgraded to a Cisco Catalyst 8000V, note that the **Current Version** column for the device indicates 17.4.1 or later.

Activate a New Software Image

Use this procedure to activate a software image that is currently loaded on a device. The software image may be a later release (upgrade) or earlier release (downgrade) than the current active release.

When you use Cisco SD-WAN Manager to upgrade the software image on a device, if you did not check the **Activate and Reboot** check box during the procedure, the device continues to use the existing configuration. Use this procedure to activate the upgraded software version.

Note To activate software for Cisco SD-WAN Manager while using a custom user group, you need read permission and read-write permissions to upgrade each software feature.

To activate a software image:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Choose **WAN Edge**, **Control Components**, or **Manager**.
3. For the desired device or devices, check the check box to choose the device or devices,
4. Click **Activate**. The **Activate Software** dialog box opens.
5. Choose the software version to activate on the device.
6. Click **Activate**. Cisco SD-WAN Manager reboots the device and activates the new software image.

If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge device, which have a default time of 12 minutes.

If the image activation fails, do not attempt to activate the image again. Remove the image from the device, then attempt to install and activate the image again.

Upgrade a CSP Device with a Cisco NFVIS Upgrade Image

Before you begin

Ensure that the Cisco NFVIS software versions are the files that have `.nfvispkg` extension.

Procedure

Step 1 From theCisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.

Step 2 Check one or more CSP device check boxes for the devices you want to choose.

Step 3 Click **Upgrade**. The **Software Upgrade** dialog box appears.

Step 4 Choose the Cisco NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

Step 5 To automatically upgrade and activate with the new Cisco NFVIS software version and reboot the CSP device, check the **Activate and Reboot** check box.

If you don't check the **Activate and Reboot** check box, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new Cisco NFVIS software version by choosing the device again and clicking the **Activate** button in the **Software Upgrade** window.

Step 6 Click **Upgrade**.

The **Task View** window displays a list of all running tasks along with total number of successes and failures. The window periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status window by clicking the **Task View** icon located in the Cisco SD-WAN Manager toolbar.

Note
If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happens in a sequence.

Note
The **Set the Default Software Version** option isn't available for the Cisco NFVIS images.

The CSP device reboots and the new NFVIS version is activated on the device. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually clicking **Activate** after choosing the CSP device again.

To verify if CSP device has rebooted and is running, use the task view window. Cisco SD-WAN Manager polls your entire network every 90 seconds up to 30 times and shows the status on th task view window.



Note You can delete a Cisco NFVIS software image from a CSP device if the image version isn't the active version that is running on the device.

Delete a Software Image

To delete a software image from a Cisco Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices from which to delete a software image.
4. Click the **Delete Available Software**.

   The **Delete Available Software** dialog box opens.
5. Choose the software version to delete.
6. Click **Delete**.

Set the Default Software Version

You can set a software image to be the default image on a Cisco Catalyst SD-WAN device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on the device and in your network.

In case of error, see Error message during software upgrade or setting default software version.

To set a software image to be the default image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices by checking the check box for the desired device or devices.
4. Click **Set Default Version**.

   The **Set Default Version** dialog box opens.
5. From the **Version** drop-down list, choose the software image to use as the default for the chosen device or devices.
6. Click **Set Default**.

Export Device Data in CSV Format

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices by checking the checkbox for the desired device or devices.
4. Click the download icon.

Cisco SD-WAN Manager downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named `Software_Upgrade.csv`

View Log of Software Upgrade Activities

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the arrow to see details of a task. Cisco SD-WAN Manager opens a status window displaying the status of the task and details of the device on which the task was performed.

Manage Software Repository

Register Remote Server

Register a remote server with Cisco SD-WAN Manager so that you can add locations of software images on the remote server to the Cisco SD-WAN Manager software repository and upgrade device or controller software using these software images. In multitenant Cisco Catalyst SD-WAN deployment, only the provider can register a remote server and perform software upgrade using images on the remote server.

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Add Remote Server**.
3. In the **Add Remote Server** slide-in page, configure the following:

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP, FTP, or SCP. • **Port**: Enter the access port number.
Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a-z, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?, :, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of the valid characters is supported starting from Cisco vManage Release 20.9.1.

Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN

4. Click **Add** to add the remote server.

Enable devices to use a remote repository server

See Enable Software Updates by a Remote Repository Server.

Manage Remote Server

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. For the desired remote server, click **…**
3. To view the remote server settings, click **View Details**.
4. To edit the remote server settings, click **Edit**. Edit any of the following settings as necessary and click **Save**.

Note You cannot edit the remote server settings if you have added locations of any software images on the remote server to the Cisco SD-WAN Manager software repository. If you wish to edit the remote server settings, remove the software image entries from the software repository and then edit the settings.

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP, FTP, or SCP. • **Port**: Enter the access port number.
Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a-z, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?, :, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of the valid characters is supported starting from Cisco vManage Release 20.9.1.

Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN.

5. To delete the remote server, click **Remove**. Confirm that you wish to remove the remote server in the dialog box.



Note Before deleting a remote server, remove any entries for software images on the remote server that you have added to the Cisco SD-WAN Manager software repository.

Add Software Images to the Repository

Before you can upgrade the software on an edge device, Cisco Catalyst SD-WAN Controller, or Cisco SD-WAN Manager to a new software version, you need to add the software image to the Cisco SD-WAN Manager software repository. The repository allows you to store software images on the local Cisco SD-WAN Manager server or add locations of software images stored on a remote file server.

The Cisco SD-WAN Manager software repository allows you to store images in three ways:

- On the local Cisco SD-WAN Manager server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst SD-WAN devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the Cisco SD-WAN Manager server might not be able to monitor the software installation on the device even though it is proceeding correctly.



Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, image uploads to the Cisco SD-WAN Manager repository fail when disk space limits are exceeded. In a cluster environment, the disk space is assessed on all nodes simultaneously. Even if one node is experiencing low disk space, the image upload will fail for all nodes.

When the total utilized space exceeds the limit, you may delete the existing image data on the local server. If this does not resolve the issue or if there is no existing image data to delete, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total used space at /opt/data/ remains below 80%.

- On the local Cisco SD-WAN Manager server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because

it bypasses any throttling that the device might perform and so the Cisco SD-WAN Manager server is able to monitor the software installation.

- On a remote server: From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco SD-WAN Manager server sends this URL to the Cisco Catalyst SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco Catalyst SD-WAN deployment, only the provider can register a remote server with Cisco SD-WAN Manager and add locations of software images on the remote server to the Cisco SD-WAN Manager repository.



Note Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:

- User ID: a-z, 0-9, ., _, -
- Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
- URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Software Images**.
3. Click **Add New Software**.
4. Choose the location for the software image:



Note Store NFVIS upgrade images on the local Cisco SD-WAN Manager server.

   a. To store the software image on the local Cisco SD-WAN Manager server and have it be downloaded to Cisco Catalyst SD-WAN devices over a control plane connection, choose **Manager**. The **Upload Software to Manager** dialog box opens.
      1. Drag and drop the software image file to the dialog box or click **Browse** to select the software image from a directory on the local Cisco SD-WAN Manager server.
      2. Click **Upload** to add the image to the software repository.

   b. To store the image on a remote Cisco SD-WAN Manager server and have it be downloaded to Cisco Catalyst SD-WAN devices over an out-of-band management connection, choose **Remote Server - Manager**. The **Upload Software to Remote Server - Manager** dialog box opens.
      1. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager server that is in a management VPN (typically, VPN 512).
      2. Drag and drop the software image file to the dialog box, or click **Browse** to select the software image from a directory on the local Cisco SD-WAN Manager server.
      3. Click **Upload**.

c. If the software image is stored on a remote server, choose **Remote Server (preferred)**. The **Add New Software via Remote Server** slide-in pane appears. Before choosing this option, ensure that you have registered a remote server with Cisco SD-WAN Manager.

1. Click **Image** to upload a new software image, or **SMU Image** to upload an SMU image. The default selection is **Image**.
2. From the **Remote Server Name** drop-down list, choose the desired remote server.
3. **Image Filename**: Enter the image filename, including the file extension. For an SMU image, the file extension must be `.smu.bin`.
4. For an SMU image, enter the correct **SMU Defect ID** and choose the correct **SMU Type**. An incorrect defect ID or SMU type selection can cause the software upgrade to fail.
5. Click **Save**.

View Software Images

From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Respository**.

The **Software Repository** window displays the images avaialable in the repository.

The **Software Version** column lists the version of the software image, and the **Controller Version** column lists the version of Cisco SD-WAN Control Components that is equivalent to the software version. The Cisco SD-WAN Control Components version is the minimum supported version. The software image can operate with the listed Cisco SD-WAN Control Components version or with a higher version.

The **Software Location** column indicates where the software images are stored, either in the repository on the Cisco SD-WAN Manager server, or in a repository in a remote location.

The **Available Files** column lists the names of the software image files.

The **Updated On** column shows when the software image was added to the repository.

The **...** option for a desired software version provides the option to delete the software image from the repository.

In Cisco vManage Release 20.6.1 and earlier releases, when two or more software images have the same software version but are uploaded with different filenames, the images are listed in a single row. The **Available Files** column lists the different filenames. This listing scheme is disadvantageous when deleting software images as the delete operation removes all the software images corresponding to a software version.

From Cisco vManage Release 20.7.1, when two or more software images have the same software version but are uploaded with different filenames, each software image is listed in a separate row. This enables you to choose and delete specific software images.

Add Virtual Images to the Repository

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Click **Add New Virtual Image** and choose one of the following options:
   - **Remote Server (preferred)**: Choose this option to link to an image that has been uploaded to a remote server.

Note Before choosing this option, ensure that you have registered a remote server with Cisco SD-WAN Manager. For more information on how to register a remote server, see Register Remote Server.

The **Add Virtual Image with Remote Server Details** slide-in pane appears. (This option does not store the image on the local Cisco SD-WAN Manager server).

For Cisco vManage Release 20.11.1 and later, follow these steps:

a. Click **Add New Virtual Image** and choose **Remote Server (preferred)**.

b. In the **Image Name** field, enter the file name of the image.

c. In the **Image description** field, enter a description of the image.

d. (Optional) Click the **Add Tags** field and choose tags for the virtual image file.

e. In the **Select service type** field, choose **App-Hosting**.

The following applications are supported:

- **UTD-Snort-Feature**
- **DRE-Optimization-Feature**
- **ThousandEyes-Enterpeise-Agent**
- **Cybervision-Enterprise-Agent**

For standard filenames, Cisco SD-WAN Manager automatically displays the attributes of the image file.

For non-standard filenames, enter the following manually:

- **App type**: Choose an application type from the drop-down list.
- **Enter version**: Enter the version as free text.

  Cisco SD-WAN Manager automatically chooses the x86_64 architecture. You can choose a different architecture if necessary from the drop-down list.

f. Click the **Remote Server Name** field and choose a remote server.

g. In the **Image File Path** field, enter a path from the root directory of the remote server.

If you do not enter a path, Cisco SD-WAN Manager uses the root directory.

h. (Optional) To provide another server that contains the image, click **Add Remote Server**, and enter the details of the additional server.

i. Click **Add**.

- **Manager**: Choose this option to upload a file to the local Cisco SD-WAN Manager repository using a control-plane connection. This option is useful for uploading small files.

The **Upload VNF's Package to Manager** dialog box opens.

a. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

b. In the **Description** field, enter the description.

c. In the drop-down list, choose **Image Package** or **Scaffold**.

d. Click the **Add Tags** field and choose tags for the virtual image file.

e. Click **Upload** to add the virtual image file to the repository.

- **Remote Server - Manager**: Choose this option to store the virtual image file on a remote Cisco SD-WAN Manager server and download the virtual image file to Cisco Catalyst SD-WAN devices over an out-of-band management connection.

  The **Upload VNF's Package to Remote Server - Manager** dialog box opens.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager server that is in a management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

  c. In the **Description** field, enter the description of the virtual image file.

  d. In the drop-down list, choose **Image Package** or **Scaffold**.

  e. Click the **Add Tags** field and choose tags for the virtual image file.

  f. Click **Upload**.

Note To upload virtual images using the **Manager** or **Remote Server - Manager** options, use files with extensions, .tar, .gz, .tar or .qcow2. For more information on the steps to upload virtual images with extensions .tar, gz, .tar or .qcow2, see Upload VNF Images, on page 235

Upload VNF Images

The VNF images are stored in the Cisco SD-WAN Manager software repository. These VNF images are referenced during service chain deployment, and then they are pushed to Cisco NFVIS during service chain attachment.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 To add a prepackaged VNF image, click **Virtual Images**, and then click **Upload Virtual Image**.

Step 3 Choose the location to store the virtual image.

- To store the virtual image on the local Cisco SD-WAN Manager server and download it to CSP devices over a control plane connection, click **Manager**. The **Upload VNF's Package to Manager** dialog box appears.

a. Drag and drop the virtual image file or the qcow2 image file to the dialog box or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server. For example, CSR.tar.gz, ASAv.tar.gz, or ABC.qcow2

b. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

c. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

   - Description of the image
   - Version number of the image
   - Checksum
   - Hash algorithm

   You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

   Note
   - It is mandatory to upload a scaffold file if you choose a qcow2 image file.
   - The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

d. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it available for installing on the CSP devices.

- To store the image on a remote Cisco SD-WAN Manager server and then download it to CSP devices, click **Remote Server - Manager**. The **Upload VNF's Package to Remote Server-Manager** dialog box appears.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on Cisco SD-WAN Manager server that is in the management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file or the qcow2 image file to the dialog box, or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server.

  c. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

  d. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

     - Description of the image
     - Version number of the image
     - Checksum
     - Hash algorithm

     You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

Note

- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

e. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

You can have multiple VNF entries such as a firewall from same or from different vendors. Also, you can add different versions of VNF that are based on the release of the same VNF. However, ensure that the VNF name is unique.

Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
- Day-0 configuration files–system and tokenized custom variables
- VM configuration–CPU, memory, disk, NICs
- HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 2 Click **Virtual Images** > **Add Custom VNF Package**.

Step 3 Configure the VNF with the following VNF package properties and click **Save**.

Table 43: VNF Package Properties

Field	Mandatory or Optional	Description
Package Name	Mandatory	The filename of the target VNF package. It's the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.
Name	Mandatory	Name of the VNF image.
Version	Optional	Version number of a program.
Type	Mandatory	Type of VNF to choose. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

Step 4 To package a VM qcow2 image, click **File Upload**, and browse to choose a qcow2 image file.

Step 5 To choose a bootstrap configuration file for VNF, if any, click **Day 0 Configuration** and click **File Upload** to browse and choose the file.

Include the following Day-0 configuration properties:

Table 44: Day-0 Configuration

Field	Mandatory or Optional	Description
Mount	Mandatory	The path where the bootstrap file gets mounted.
Parseable	Mandatory	A Day-0 configuration file can be parsed or not. Options are: **Enable** or **Disable**. By default, **Enable** is chosen.
High Availability	Mandatory	High availability for a Day-0 configuration file to choose. Supported values are: Standalone, HA Primary, HA Secondary.

Note
If any bootstrap configuration is required for a VNF, create a *bootstrap-config* or a *day0-config* file.

Step 6 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** next to the desired Day-0 configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note
The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the Custom Packaging Details for Shared VNF topic and additional references in Cisco SD-WAN

Cloud OnRamp for Colocation Solution Guide for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select, and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down list, and click **Done**. The highlighted property is replaced by the system variable name.
c) To add a custom variable, in the **CLI configuration** dialog box, choose and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter the custom variable name and choose a type from **Type** drop-down list.
e) To set the custom variable attribute, do the following:
   - To ensure that the custom variable is mandatory when creating a service chain, click **Type** next to **Mandatory**.
   - To ensure that a VNF includes both primary and secondary day-0 files, click **Type** next to **Common**.
f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 7 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an extra qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

Note
Ensure that you don't combine ephemeral disks and storage volumes when uploading extra VM images.

Step 8 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 45: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	The disk size that is required for the VM operation. If the size unit is GiB, the maximum disk size can be 256 GiB.
Size Unit	Mandatory	Choose size unit. The supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. By default, disk is chosen.
Location	Optional	The location of the disk or CD-ROM. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are: qcow2, raw, and vmdk. By default, it's raw.

Field	Mandatory or Optional	Description
Bus	Optional	Choose a value from the drop-down list. The supported values for a bus are: virtio, scsi, and ide. By default, it's virtio.

Step 9 To add VNF image properties, expand **Image Properties** and enter the following image information.

Table 46: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Enable or disable SR-IOV support. By default, it's enabled.
Monitored	Mandatory	VM health monitoring for those VMs that you can bootstrap. The options are: enable or disable. By default, it's enabled.
Bootup Time	Mandatory	The monitoring timeout period for a monitored VM. By default, it's 600 seconds.
Serial Console	Optional	The serial console that is supported or not. The options are: enable or disable. By default, it's disabled.
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. The options are: enable or disable. By default, it's disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. The options are: enable or disable. By default, it's enabled.

Step 10 To add VM resource requirements, expand **Resource Requirements** and enter the following information.

Table 47: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	The CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	The RAM supported by a VM. The RAM can range 2–32.
Disk Size	Mandatory	The disk size in GB supported by a VM. The disk size can range 4–256.
Max number of VNICs	Optional	The maximum number of VNICs allowed for a VM. The number of VNICs can from range 8–32 and by default, the value is 8.
Management VNIC ID	Mandatory	The management VNIC ID corresponding to the management interface. The valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	The number of VNICs.
High Availability VNIC ID	Mandatory	The VNIC IDs where high availability is enabled. The valid range is from 0–maximum number of VNICs. It shouldn't conflict with management VNIC Id. By default, the value is 1.
Number of High Availability VNICs ID	Mandatory	The maximum number of VNIC IDs where high availability is enabled. The valid range is 0–(maximum number of VNICs-number of management VNICs-2) and by default, the value is 1.

Step 11 To add day-0 configuration drive options, expand **Day 0 Configuration Drive options** and enter the following information.

Table 48: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	The volume label of the Day-0 configuration drive. The options are: V1 or V2. By default, the option is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.

Field	Mandatory or Optional	Description
Init Drive	Optional	The Day-0 configuration file as a disk when mounted. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. The supported values for a bus are: virtio, scsi, and ide. By default, it's ide.

The Software Repository table displays the customized VNF image, and image is available for choosing when creating a custom service chain.

View VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**.

Step 3 To filter the search results, use the filter option in the search bar.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. Software images can be stored either in the repository on the Cisco SD-WAN Manager server or in a repository in a remote location.

The **Version Type Name** column provides the type of firewall.

The **Available Files** column lists the names of the VNF image files.

The **Update On** column displays when the software image was added to the repository.

Step 4 For the desired VNF image, click **...** and choose **Show Info**.

Delete a Software Image from the Repository

To delete a software image from the Cisco SD-WAN Manager software repository:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 For the desired software image, click **...** and choose **Delete**.

If a software image is being downloaded to a router, you cannot delete the image until the download process completes.

Delete VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**. The images in the repository are displayed in a table.

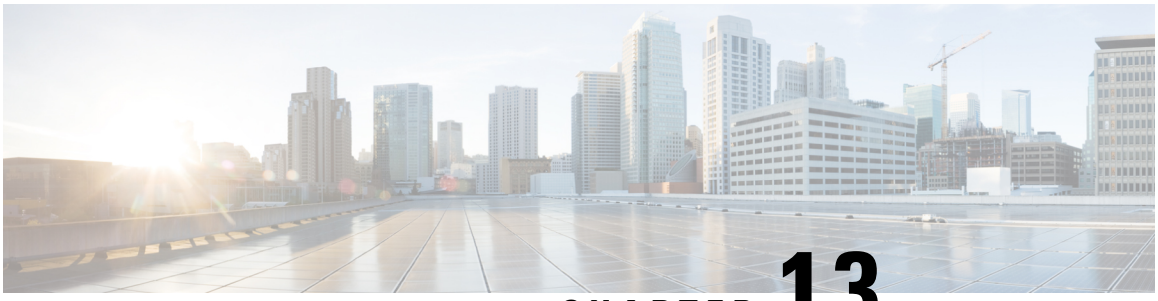
Step 3 For the desired image, click **...** and choose **Delete**.



Note If you're downloading a VNF image to a device, you can’t delete the VNF image until the download process completes.



Note If the VNF image is referenced by a service chain, it can’t be deleted.



CHAPTER 13

Software Upgrade Workflow

Table 49: Feature History

Feature Name	Release Information	Description
Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 Cisco SD-WAN Release 20.8.1	This feature introduces a guided workflow through which you can upgrade the software image on your Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices and monitor the status of the software upgrade. With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step.
Schedule the Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	This feature introduces an option to schedule software upgrades for edge devices using Cisco SD-WAN Manager.
Software Upgrade Workflow Support for Additional Platforms	Cisco vManage Release 20.9.1	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
Software Upgrade Scheduling Support for Additional Platforms	Cisco vManage Release 20.10.1	Added support for software upgrade scheduling for Cisco Catalyst Cellular Gateways.

Feature Name	Release Information	Description
Device Software Upgrade Workflow Enhancements	Cisco Catalyst SD-WAN Manager Release 20.18.1	The new workflow for device software upgrade includes the following key enhancemnets: • Uploading software image from local drive. • Filtering devices for software upgrade using device tags and network hierarchy. • Scheduling a software upgrade based on a device's local time zone.

- Information About Software Upgrade Workflow, on page 246
- Information About Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later , on page 247
- Supported Devices for the Software Upgrade Workflow, on page 247
- Prerequisites for Using the Software Upgrade Workflow, on page 248
- Restrictions for software upgrade, on page 248
- Access the Software Upgrade Workflow, on page 249
- Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 and Later , on page 250
- Schedule Software Upgrade Workflow, on page 251
- Schedule a Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later, on page 252
- Cancel the Scheduled Software Upgrade Workflow, on page 252
- Delete a Downloaded Software Image, on page 252

Information About Software Upgrade Workflow

Using this workflow, you can download and upgrade software images on the various supported Cisco devices with an option to schedule the upgrade process at your convenience. The workflow also shows the status of the software upgrade. This workflow provides you with two options to perform the software upgrade and they are: **Download and Upgrade** and **Download Only**.

Benefits of Software Upgrade Workflow

- The software upgrade workflow helps you prevent various device software upgrade failures by displaying device upgrade status. For example, if the upgrade process fails at any particular stage, the workflow flags it as **failed**.
- With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step. You can schedule the workflow at your convenience as well.

Information About Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later

From Cisco Catalyst SD-WAN Manager Release 20.18.1, the Software Upgrade Workflow is renamed to Device Software Upgrade Workflow. The new workflow is easy to manage and reduces the chances of upgrade failure.

This workflow includes the following enhancement in device software upgrade:

- Uploading software image from your local drive.
- Adding the platform details for each software image. It ensures you do not upload an incompatible software image for upgrade.

Note Starting Cisco Catalyst SD-WAN Manager Release 20.18.1, you cannot choose different software images for each device platform class. You can only choose one software image version that is compatible with all device platforms.

- Filtering devices for software upgrade using network hierarchies, device tags and software version.
- Scheduling the software upgrade in the device's local time zone.
- Additional preupgrade and postupgrade checks to reduce the chances of upgrade failures.

Supported Devices for the Software Upgrade Workflow

Devices	Minimum Supported Releases	Comments
Cisco IOS XE Catalyst SD-WAN devices	Cisco SD-WAN Manager: Cisco vManage Release 20.8.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Scheduled software upgrade supported from: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
Cisco vEdge devices	Cisco SD-WAN Manager: Cisco vManage Release 20.8.1 Devices: Cisco SD-WAN Release 20.8.1	Scheduled Software Upgrade feature supported from: Cisco SD-WAN Release 20.9.1
Cisco Catalyst 8200 uCPE Series Edge Platforms	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	None

Devices	Minimum Supported Releases	Comments
Cisco 5400 Series Enterprise Network Compute System (ENCS)	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	None
Cisco Catalyst Cellular Gateways	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS CG Release 17.9.1	Scheduled software upgrade supported from: Cisco vManage Release 20.10.1 and Cisco IOS CG Release 17.9.1

Prerequisites for Using the Software Upgrade Workflow

- Ensure that the Cisco devices are running the required software versions for using the software upgrade workflow feature. For the respective device requirements, see Supported Devices for the Software Upgrade Workflow, on page 247.
- From Cisco Catalyst SD-WAN Control Components Release 20.18.1, if you want to filter devices for software upgrade using tags, ensure that you have already assigned tags to the devices. For more information about device tagging, see Device Tagging.
- You cannot use a software image from a remote repository directly in the workflow. Navigate to **Maintenance** > **Software Repository** and edit the software image to add the version and platform information.

Restrictions for software upgrade

TLOC extension configuration

If a device

- is using Cisco IOS XE Catalyst SD-WAN Release 17.9.x or earlier, and
- the device has a tunnel interface configuration includes a TLOC extension,

then you cannot upgrade to one of these:

- 17.12.1 through 17.12.4
- 17.15.1 through 17.15.2

Attempting such an upgrade causes the device to crash and enter a rollback state.

If you have a TLOC extension configured and need to perform such an upgrade, remove the TLOC extension configuration from the tunnel interface configuration before upgrading.

This issue was fixed and does not apply for upgrades to one of these releases:

- 17.12.5 and later releases of 17.12.x

- 17.15.3 and later releases of 17.15.x
- 17.18.1a and later

Access the Software Upgrade Workflow

Before You Begin

To check if there is an in-progress software upgrade workflow:

From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

Access the Software Upgrade Workflow

1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.



Note In the Cisco vManage Release 20.8.1, the **Workflow Library** is titled **Launch Workflows**.

2. Start a new software upgrade workflow: **Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. Follow the on-screen instructions to start a new software upgrade workflow.



Note Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.



Note In a multi-node cluster setup, if the control connection switches to a different node during a device upgrade from Cisco SD-WAN Manager, the upgrade may be impacted due to NetConf session timeout. The device then establishes control connection to a different node. You need to re-trigger the upgrade activity.

Verify the Status of the Software Upgrade Workflow

To check the software upgrade workflow status:

1. From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the + icon to view the details of a task.

Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 and Later

Before you begin

To filter devices for upgrade using tags, ensure the devices that you want to choose have tags. For more information, see Prerequisites for Using the Software Upgrade Workflow.

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Device Software Upgrade**.

Step 3 Choose the devices using the network hierarchy panel.

Alternatively, use the filters **Search**, **Device tags**, and **Software version** options or a combination of these filters to search and choose devices.

Note
In the workflow, you can choose a specific software image version from a dropdown to upgrade devices. Before choosing the software image version, you must select the devices for upgrade. Software image versions only show up in the dropdown if all choosen devices in the workflow have the necessary images available in a local or remote repository. If the supported software image version is not available in the repository for one or more devices, then you cannot choose that software image version from the dropdown.

Note
In the upgrade workflow, do not choose different types of devices together. Specifically, avoid the combination of the following devices: Cisco IOS XE Catalyst SD-WAN devices together, Cisco Enterprise NFVIS (Cisco Enterprise Network Function Virtualization Infrastructure Software) devices, or Cisco Catalyst Cellular Gateway devices.

Step 4 Choose one for the following upgrade type:

a. **Upgrade**: To install and activate the software image.

b. **Patch**: To apply patch fixes on the existing software.

Step 5 Choose one of the following options to add a software image:

- **+ Add New Image** to upload an image from local drive.
- **+ Add New Remote Server** to add a remote server for upgrade and then add a software image.

Note
Software images created before upgrading the Cisco SD-WAN Manager to version Cisco Catalyst SD-WAN Manager Release 20.18.1 lack platform family and version details. To use these images after the upgrade, edit them in **Maintenance** > **Software Repository** and add the required platform family and version information.

Step 6 Follow the on-screen instructions to complete the software upgrade workflow.

Note
Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Note
For an error during device software upgrade, see Error message during software upgrade or setting default software version.

What to do next

To view the list of successful upgrades on the devices. Click the **Task log** in the task bar.

Schedule Software Upgrade Workflow

Introduced in Cisco vManage Release 20.9.1, the scheduler in the software upgrade workflow enables you to schedule workflows at your convenience and avoid any downtime due to the software upgrade process. A scheduler enables you to schedule the upgrade workflow either **Now** or **Later**. If you choose to schedule an upgrade for a later time, you can enter the **Start Date**, **Start time**, and **Select Timezone**.

Schedule Software Upgrade Workflow

Use the following steps to schedule a software upgrade workflow:

1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**

   OR

   Starting from Cisco vManage Release 20.9.1, click **Workflows** > **Popular Workflows** > **Software Upgrade.**.
2. Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.
3. In the **Scheduler** section, choose **Later**.

Note Use the **Now** option to perform the software upgrade for the selected devices immediately.

4. Choose the **Start Date**, **Start Time**, and **Select Timezone**.

Note Start date and time should always be greater than the Cisco SD-WAN Manager server date and time.

5. Click **Next**.

6. The software upgrade workflow is scheduled.

Schedule a Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later

Before you begin

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Device Software Upgrade**.

Step 3 After choosing the devices, in the **Action** section, choose **Download and Upgrade** to schedule upgrade.

Step 4 In the **Scheduler** section, choose **Later**.

Note
Choose the **Now** option to upgrade device software immediately after completing the workflow.

Step 5 Add a **Task Name** and choose the **Start Date**, **Start Time**, and **Select Timezone**.
Alternately, choose **Site Time** to perform the software upgrade in the device's local time zone.

Step 6 Follow the on-screen instructions to complete the workflow.

What to do next

To view the list of sucessful upgrades on the devices. click on the **Task log** in the task bar.

Cancel the Scheduled Software Upgrade Workflow

To cancel a scheduled software upgrade workflow,

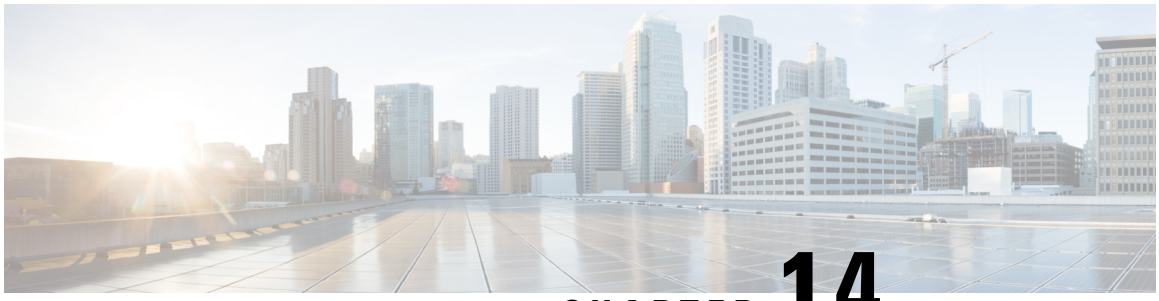
1. From the Cisco SD-WAN Manager menu, click **Maintenance** > **Software Upgrade**.
2. Choose the device that is scheduled for a software upgrade from the list of devices.
3. Click **Cancel Software Upgrade**.

Delete a Downloaded Software Image

To delete downloaded software images from WAN edge devices:

1. From the Cisco Catalyst SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**.

3. Click **Delete Downloaded Images**
4. In the **Delete Downloaded Images** pop-up window, choose the image or images to delete.
5. Click **Delete**.



CHAPTER 14

Software Maintenance Upgrade

- Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices, on page 255
- Information About Software Maintenance Upgrade, on page 255
- Supported Devices for Software Maintenance Upgrade, on page 257
- Manage Software Maintenance Upgrade Images, on page 257
- Install and Activate an SMU Image Using the CLI, on page 259
- Deactivate and Remove an SMU Image Using the CLI, on page 262

Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices

Table 50: Feature History

Feature Name	Release Information	Description
Support for Software Maintenance Upgrade Package	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables support for a Software Maintenance Upgrade (SMU) package that can be installed on Cisco IOS XE Catalyst SD-WAN devices. The SMU package provides a patch fix or a security resolution to a released Cisco IOS XE image. Developers can build this package that provides a fix for a reported issue without waiting for the fix to become available in the next release.
SMU Support for Cisco ISR1100 and ISR1100X Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Added support for Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers.

Information About Software Maintenance Upgrade

A software maintenance upgrade (SMU) is a point fix for a critical bug in released software that attempts to minimize disruption to the router, if possible. An SMU is not designed to replace a maintenance release.

Cisco provides SMU fixes as package files, a file for each release and each component of Cisco Catalyst SD-WAN. The package contains metadata that describes the content of the package and the fix for a reported issue.

SMU Image Files

Each SMU image filename in the software repository includes a base image version and the defect ID related to the fix. In the image name:

- *base_image_version* is the Cisco IOS XE image version.
- *defect_id* is the identifier of the defect for which the SMU package has the fix.

SMU Types

An SMU type describes the effect of an installed SMU package on a Cisco IOS XE Catalyst SD-WAN device. The following are the SMU package types:

- Hot SMU (non-reload): Enables an SMU package to take effect after an SMU image activation without rebooting (reloading) the Cisco IOS XE Catalyst SD-WAN device.
- Cold SMU (reload): Enables an SMU package to take effect after rebooting (reloading) the Cisco IOS XE Catalyst SD-WAN device.

Benefits of Software Maintenance Upgrades

- Allow you to address a network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE Catalyst SD-WAN device internally validates the SMU image compatibility and does not allow you to install non-compatible SMU packages.
- Allow you to install or activate only one SMU package on devices at a time to simplify the initial implementation process.
- Allow you to install an SMU package on multiple Cisco IOS XE Catalyst SD-WAN devices at the same time when installing using Cisco SD-WAN Manager. To install an SMU package on multiple devices using the CLI, ensure that you repeat the install process on multiple devices.

Supported Devices for Software Maintenance Upgrade

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.9.5a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.9.x Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and later	• Cisco ISR 1000 Series Integrated Services Routers • Cisco IR1101 Integrated Services Router Rugged • Cisco ISR 4000 series Integrated Services Routers • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Series Edge Platforms • Cisco Catalyst 8000v Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	• Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200L Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers

Manage Software Maintenance Upgrade Images

Use Cisco SD-WAN Manager to add, upgrade and activate, or deactivate and remove an SMU image.

Note When you activate or deactivate an SMU image, the device may reboot, depending on the SMU image. A non-reload SMU type does not trigger a device reboot; a reload SMU type triggers a device reboot.

Add, View, and Activate an SMU Image

1. Add an SMU image using the Cisco SD-WAN Manager software repository.

   See the Cisco SD-WAN Manager Add Software Images to Repository procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

2. View SMU images using the Cisco SD-WAN Manager software repository.

   See theCisco SD-WAN Manager View Software Images procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*. Note the following points when viewing SMU images:

- The **Available SMU Versions** column displays the number of SMU images available for the current base image version (Cisco IOS XE image version).
- View the defects that are associated with an SMU image by clicking a desired entry in the **Available SMU Versions** column. In the **Available SMU Versions** dialog box, you can view the defect ID, the corresponding SMU version, and the SMU types, such as non-reload or reload.
- In the **Available SMU Versions** dialog box, delete an SMU version by clicking the delete icon next to an SMU version.

3. Upgrade an SMU image using the Cisco SD-WAN Manager software upgrade window.

   See the Cisco SD-WAN Manager Upgrade the Software Image on a Device procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*. Note the following points about the SMU image that you choose to upgrade:

   - In the devices table, the **Available SMUs** column displays the number of SMU images that are available for the current base image version.
   - View a list of all available SMU versions and the upgrade images for a device by clicking a desired entry under the **Available SMUs** column. In the **Available SMUs** dialog box, you can view the SMU versions, SMU types, and the state of an SMU version.

     The SMU version is in the format *base_image_version.cdet_id*.
   - In the **Upgrade** dialog box, optionally check **Activate and Reboot** to activate an SMU image and perform a reboot of the Cisco IOS XE Catalyst SD-WAN device automatically.

     After you check the **Activate and Reboot** check box, Cisco SD-WAN Manager installs and activates the SMU image on a device and triggers a reload based on the SMU type. For more Information about activating a software image, see the Cisco SD-WAN Manager Activate a Software Image procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

   After a successful upgrade of an SMU image, the Cisco IOS XE Catalyst SD-WAN device sends a corresponding success message.

Deactivate or Remove an SMU Image

Deactivate an SMU image and remove the image from a device using the Delete a Software Image procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Onboarding ISR1100 to Cisco SD-WAN Manager

1. Do not enable the Cisco IOS XE Catalyst SD-WAN device interface on the ISR1100 device.
2. Add the serial.viptela file to Cisco SD-WAN Manager to add the device.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Migrate Device** to migrate from viptela operating system to Cisco IOS XE operating system.
4. Enable the Cisco IOS XE Catalyst SD-WAN device interface to bring up the control connections.
5. Verify the device sync up in Cisco SD-WAN Manager.

Install and Activate an SMU Image Using the CLI

Device reboot:

When you activate an SMU image, the device may reboot, depending on the SMU image. A non-reload SMU type does not trigger a device reboot; a reload SMU type triggers a device reboot.

Before you begin

- Download an SMU image from Cisco:

  Download an SMU image for your release from the Cisco site, https://software.cisco.com.

- Upload an SMU image:

  Upload an SMU image to make it available for installation.

  - Upload an SMU image by adding the image to the device software repository using Cisco SD-WAN Manager. For more information about adding, viewing, and activate an SMU image, see Manage Software Maintenance Upgrade Images, on page 257.
  - Upload an SMU image by copying the image to the bootflash of your device using the CLI.

Procedure

Step 1 Use the **copy** command to upload the SMU image from the file server to the bootflash of the device.

Step 2 If not already configured, configure the time limit for confirming that an SMU image activation is successful.

The range is 1 to 60 minutes. We recommend a time limit of at least 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

Step 3 Install an SMU image from the bootflash of your device and perform a compatibility check for the device and SMU package version.

```
Device# request platform software sdwan smu install file-path
```

Step 4 Use the **show install summary** command to confirm that the SMU image is installed.

If the **request platform software sdwan smu install** command was successful, the IMG row of the command output shows the build number. Make note of the version number. Use this as the build number in a subsequent step.

```
Device# show install summary
```

Step 5 Use the **show install package** command with **| include Defect ID** to display the defect ID of the issue addressed by the SMU image.

```
show install package bootflash:filename | include Defect ID
```

The command output shows the defect ID.

Step 6 Activate the SMU image on a Cisco IOS XE Catalyst SD-WAN device. For the build number, use the five-part build number displayed in a previous step. For the SMU defect ID, use the defect ID displayed in a previous step.

```
Device# request platform software sdwan smu activate build-number.smu-defect-id
```

Step 7 Confirm the upgrade of the SMU image within the configured confirmation time limit.

```
Device# request platform software sdwan smu upgrade-confirm
```

Note
If you don't issue this command on the device within the time limit that is specified in the **upgrade-confirm** *minutes* command, the device automatically reverts to the state that it was in before the SMU image activation.

Step 8 Use the **show install summary** command to confirm that the image is activated. For the IMG and SMU rows, the St column shows the letter C to indicate that the image is activated and committed.

Example

The following commands configure an upgrade confirmation time limit of 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm 15
```

The following commands install and activate an SMU image, and confirm that the image is successfully activated.

```
Device# request platform software sdwan smu install
bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin
install_add: START Thu May 30 09:22:47 UTC 2024
install_add: Adding IMG
 [1]  R0 Downloading (null)
 [1]  R0 Downloading (null)
--- Starting initial file syncing ---
Copying bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin
from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
Checking status of SMU_ADD on [R0]
SMU_ADD: Passed on [R0]
Finished SMU Add operation

SUCCESS: install_add
/bootflash/isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin Thu May
30 09:23:08 UTC 2024


Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.03.0.3740
SMU   I   bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin
```

```
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------


Device# show install package
bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin | include
 Defect ID
include Defect ID: CSCwj48209


Device# request platform software sdwan smu activate 17.12.03.0.3740.CSCwj48209
install_activate: START Thu May 30 09:23:40 UTC 2024
install_activate: Activating SMU
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
 [1] SMU_ACTIVATE package(s) on  R0
 [1] Finished SMU_ACTIVATE on  R0
Checking status of SMU_ACTIVATE on [R0]
SMU_ACTIVATE: Passed on [R0]
Finished SMU Activate operation

SUCCESS: install_activate Thu May 30 09:24:20 UTC 2024


Device# request platform software sdwan smu upgrade-confirm
install_commit: START Thu May 30 09:24:33 UTC 2024
--- Starting Commit ---
Performing Commit on all members
 [1] SMU_COMMIT packages(s) on  R0
 [1] Finished SMU_COMMIT packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Thu May 30 09:24:51 UTC 2024


Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.03.0.3740
SMU   C   bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

What to do next

If the SMU image is compatible with the Cisco IOS XE software image on the device, the upgrade task is successful and the SMU image is installed and activated on the device. If the upgrade task is not successful, the device automatically reverts to the state that it was in before the SMU image activation.

Deactivate and Remove an SMU Image Using the CLI

- Device reboot:

  When you deactivate an SMU image, the device may reboot, depending on the SMU image. A non-reload SMU type does not trigger a device reboot; a reload SMU type triggers a device reboot.

- Failed deactivation:

  If the SMU image deactivation on a device fails, the device automatically reverts to the state that it was in before the image deactivation.

Before you begin

Deactivate an image before removing:

Ensure that you deactivate the SMU image before you remove it.

Procedure

Step 1 If not already configured, configure the time limit for confirming that a SMU image deactivation is successful.

The range is 1 to 60 minutes. We recommend a time limit of at least 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

Step 2 Deactivate an SMU image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan smu deactivate build-number.smu-defect-id
```

Step 3 Verify that the SMU image is deactivated. In the SMU line of the command output, in the St column, the letter D indicates deactivated.

```
Device# show install summary
```

Step 4 Complete the SMU image deactivation.

```
Device# request platform software sdwan smu upgrade-confirm
```

If you do not issue this command on the device within the time limit specified in the **upgrade-confirm** *minutes* command, the image deactivation fails and the device automatically reverts to the state that it was in before the SMU image deactivation.

Step 5 Verify that the SMU image is inactive. In the SMU line of the command output, in the St column, the letter I indicates inactive.

```
Device# show install summary
```

Step 6 Get the version number of the image.

a) Use the **show install package** command to display the version number.

```
show install package bootflash:filename | include Version
```

b) The Version line of the output shows several numbers separated by periods. Copy the first five numbers of the version.

For example, if the output shows 17.12.03.0.27.1717035922..Dublin, copy 17.12.03.0.27. Use this as the build number in a subsequent step.

Step 7 Use the **show install package** command with **| include Defect ID** to display the defect ID of the issue addressed by the SMU image.

```
show install package bootflash:filename | include Defect ID
```

The command output shows the defect ID.

Step 8 Remove the SMU image from the device.

```
Device# request platform software sdwan smu remove build-number.smu-defect-id
```

Step 9 Verify that the SMU image has been removed. If successful, the command output does not have an SMU line for the removed SMU image.

```
Device# show install summary
```

Example

The following commands configure an upgrade confirmation time limit of 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm 15
```

The following commands inactivate and uninstall an SMU image, and confirm that the image is removed.

```
Device# request platform software sdwan smu deactivate 17.12.03.0.3740.CSCwj48209
install_deactivate: START Thu May 30 09:25:28 UTC 2024
install_deactivate: Deactivating
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation

SUCCESS: install_deactivate Thu May 30 09:26:08 UTC 2024


Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.03.0.3740
SMU   D   bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 00:29:52
--------------------------------------------------------------------------------
```

```
Device# request platform software sdwan smu upgrade-confirm
install_commit: START Thu May 30 09:26:21 UTC 2024
--- Starting Commit ---
Performing Commit on all members
 [1] SMU_COMMIT packages(s) on  R0
 [1] Finished SMU_COMMIT packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Thu May 30 09:26:38 UTC 2024


Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.03.0.3740
SMU   I    bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------

Device# show install package
bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin | include
 Version
Version: 17.12.03.0.27.1717035922..Dublin


Device# show install package
bootflash:isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin | include
 Defect ID
include Defect ID: CSCwj48209

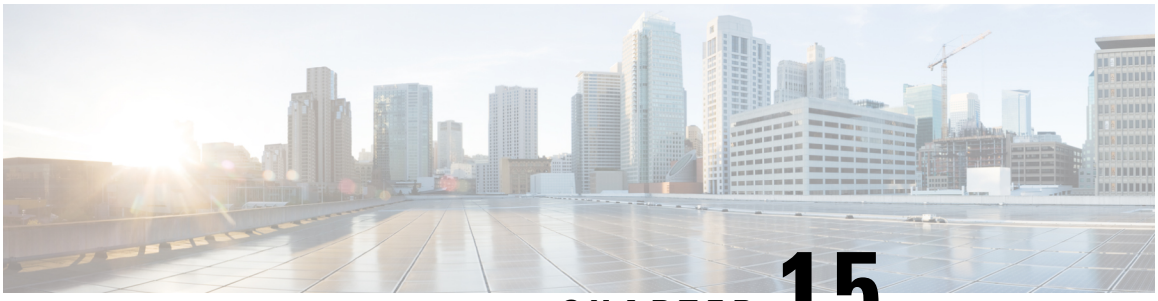

Device# request platform software sdwan smu remove 17.12.03.0.27.CSCwj48209
install_remove: START Thu May 30 09:27:39 UTC 2024
install_remove: Removing SMU
Preparing packages list to remove ...
 prepare_rm_pkg_list
/bootflash/isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin

The following files will be deleted:
   [R0]: /bootflash/isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin
Deleting file
/bootflash/isr1100be-universalk9.2024-05-29_19.25_smudev.0.CSCwj48209.SSA.smu.bin ... done.
SUCCESS: Files deleted.
SUCCESS: install_remove Thu May 30 09:27:47 UTC 2024


Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.03.0.3740

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

```
Auto abort timer: inactive
------------------------------------------------------------------------------
```



CHAPTER 15

Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Table 51: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Control Components Upgrade Workflow	Cisco Catalyst SD-WAN Control Components Release 20.18.1	With the guided workflow you can upgrade the software image of all the Cisco SD-WAN Control Components. It also allows you to apply patch release upgrades to Cisco SD-WAN Control Components, for bug fixes and minor improvements. From Cisco Catalyst SD-WAN Control Components Release 20.18.1, you can schedule full OS and patch upgrades for Cisco SD-WAN control plane components (SD-WAN Manager, SD-WAN Validator, SD-WAN Controller) for a specific future date and time.

- Information About Cisco Catalyst SD-WAN Control Components Upgrade Workflow, on page 268
- Benefits of Using Cisco Catalyst SD-WAN Control Components Upgrade Workflow, on page 268
- Prerequisite for Cisco Catalyst SD-WAN Control Components Upgrade Workflow, on page 269
- Restrictions for Cisco Catalyst SD-WAN Control Components Upgrade Workflow, on page 269
- Upgrade Cisco Catalyst SD-WAN Control Components Using a Workflow, on page 269
- Scheduling Cisco Catalyst SD-WAN Control Components Upgrade Using Workflow, on page 270
- Reschedule a Cisco Catalyst SD-WAN Control Components Upgrade, on page 271
- Cancel a Scheduled Cisco Catalyst SD-WAN Control Components Upgrade, on page 271

Information About Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

A Cisco SD-WAN Control Components upgrade workflow is a process that:

- integrates the software image upgrade of the Cisco SD-WAN Control Components—Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator, and
- reduces the complexity of upgrading each Cisco SD-WAN Control Component separately.

The workflow upgrades the Cisco SD-WAN Control Components in the following sequence:

1. Cisco SD-WAN Manager
2. Cisco SD-WAN Validator
3. Cisco SD-WAN Controller

In the workflow, you can download software images from the Cisco Software Download repository and upload software images from a local drive.

During the upgrade process, you can monitor the progress for each control component separately.

Information About Patch Release Upgrade For Control Components

A patch release upgrade is a targeted update that addresses specific bugs and introduces minor improvements to the software. It is designed to complement the existing software.

You can apply a patch release upgrade only to its compatible software release version. For example, if your software version is 20.18.1, you can apply patches designed only for 20.18.1. A patch release image is named as a 6-tuple, with the last digit indicating the patch number (e.g., 20.18.1.0.0.1). It is applied on a compatible base 5-tuple release version (e.g., 20.18.1.0.0)

Benefits of Using Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

- Streamlined upgrade process: All Cisco SD-WAN Control Components are upgraded in the correct sequence, reducing the risk of errors.
- Progress monitoring: With better visibility into the progress of each control component's upgrade, you can track and manage the upgrade process more efficiently.
- Pre-check and post-check tasks: The workflow includes a list of validation tasks that run before and after the upgrade. This flexibility ensures that the upgrade completes successfully.
- Flexibility in software image selection: You can either use the recommended image versions or choose a compatible custom image. For software compatibility information, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources

- Operational efficiency: Implementing patch release upgrades simplifies the process of fixing minor issues, thereby minimizing operational overhead in addressing minor problems.

Prerequisite for Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

You must ensure that the Cisco SD-WAN Control Components are running on the compatible software versions before using the Control Components Upgrade workflow.

Restrictions for Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

- You cannot select or deselect specific Cisco SD-WAN Control Components for upgrade.
- The workflow does not support older versions of Cisco SD-WAN Control Components.

Restrictions for Patch Release Upgrade

You cannot uninstall a patch release upgrade, after you apply it to the Cisco SD-WAN Control Components. We recommend taking a VM snapshot before upgrading.

Upgrade Cisco Catalyst SD-WAN Control Components Using a Workflow

Before you begin

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

If you are planning to upload software images from your local drive, ensure all the appropriate software image files for Cisco SD-WAN Control Components are available for upload. To ensure that the current device versions support the new software image verision, see Cisco SD-WAN Compatibility Matrix

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

a) Start a **Control Components Upgrade** workflow.

Step 2 Choose the type of upgrade:

- Upgrade: To install and activate all Cisco SD-WAN Control Components.

  .
- Patch: To install and activate patch image to Cisco SD-WAN Control Components.

Step 3 Select Image Version.

- **Recommended Image** shows an image that is recommended based on compatibility, if logged into cisco.com.
- **Custom** allows you to select from a dropdown of images that include images already uploaded in the Software Repository. Or, if you are logged into cisco.com you can select images from software.cisco.com that aren't necessarily the recommend version, but are options to upgrade to.
- **+ Add New Image** allows you to select an image from software.cisco.com (either from the Recommended Image option or from the Custom dropdown). The image automatically downloads from CCO.

Step 4 Follow the on-screen instructions to continue with the Cisco SD-WAN Control Components upgrade.

Note

- Click **Exit** to exit from an in-progress upgrade workflow. You can resume the in-progress workflow at your convenience.
- You cannot cancel the Cisco SD-WAN Control Components upgrade process after initializing it.

Note

Click **View upgrade status** to monitor the progress of software upgrade for each control component during the upgrade process.

Alternatively, you can navigate to **Maintenance** > **Software Upgrade** > **Control Components** and click **View upgrade status** to monitor the progress of software upgrade.

What to do next

Verify the success or failure of the Cisco SD-WAN Control Components upgrade or patch upgrade by reviewing the task logs. For more information about viewing task logs, see View Log of Software Upgrade Activities.

Scheduling Cisco Catalyst SD-WAN Control Components Upgrade Using Workflow

Use the following steps to schedule a Cisco SD-WAN Control Components upgrade workflow.

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

Step 3 In the **Scheduler** section, select **Later**.

Note
Use the **Now** option to perform the software upgrade for the selected devices immediately.

Step 4 Select the **Start Date**, **Start Time**, and **Select Timezone**.

Step 5 Click **Next**.

Note
If an upgrade fails, Cisco SD-WAN Manager initates a rollback.

Reschedule a Cisco Catalyst SD-WAN Control Components Upgrade

Use the following steps to reschedule a previously scheduled Cisco SD-WAN Control Components upgrade workflow that has not started yet.

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Step 2 Go to your scheduled software upgrade workflow: **Workflow Library** > **Software Upgrade**.

Step 3 Click on the **Control Components** tab and click **Reschedule upgrade**.

Step 4 Select the **Start Date**, **Start Time**, and **Select Timezone**.

Cancel a Scheduled Cisco Catalyst SD-WAN Control Components Upgrade

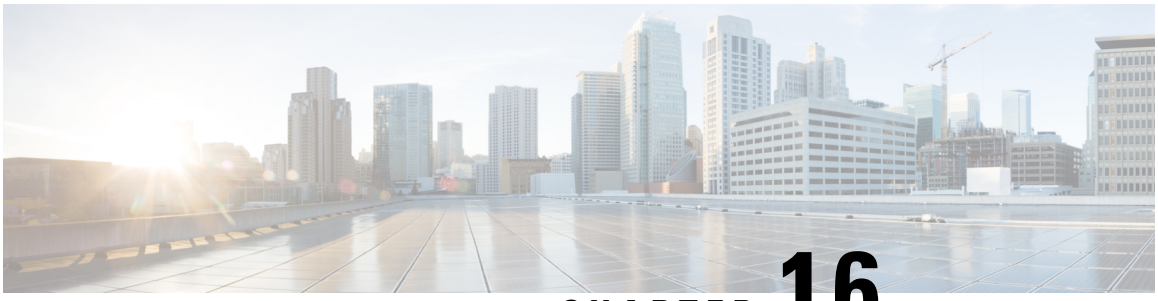
Use the following steps to cancel a scheduled Cisco Catalyst SD-WAN Control Components upgrade that has not started yet:

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Maintenance** > **Software Upgrade**.

Step 2 Choose the device that is scheduled for a software upgrade from the list of devices.

Step 3 Click **Cancel Software Upgrade**.



CHAPTER 16

Configuration Consistency across Cisco Catalyst SD-WAN Controllers

Table 52: Feature History

Feature Name	Release Information	Description
Configuration Consistency across Cisco SD-WAN Controllers	Cisco Catalyst SD-WAN Control Components Release 20.18.1	This process ensures consistency in configuration across all Cisco SD-WAN Controllers using a multi-stage approach. The multi-stage approach includes the following stages: • Validation: Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to validate the configuration. • Application: Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to validate and apply the configuration. • Rollback (Optional): Cisco SD-WAN Manager reverts changes if any issues arise during the application stage. This process prevents issues arising from Cisco SD-WAN Controllers operating on different configurations.

- Information about Configuration Consistency across Cisco Catalyst SD-WAN Controllers, on page 274
- Supported Devices for Configuration Consistency across Cisco Catalyst SD-WAN Controllers, on page 275
- Restrictions for Configuration Consistency across Cisco Catalyst SD-WAN Controllers, on page 275

• Scenarios for Offline Cisco Catalyst SD-WAN Controllers, on page 276
• Verify Consistent Configuration across Cisco Catalyst SD-WAN Controllers, on page 278

Information about Configuration Consistency across Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

Configuration consistency across Cisco SD-WAN Controllers is a process that:

- ensures configuration consistency across all Cisco SD-WAN Controllers in the cluster for single tenants,
- ensures configuration consistency only for Cisco SD-WAN Controllers that are part of the tenant,
- employs a multi-stage approach to implement configuration changes,
- uses an error-handling mechanism to rollback changes when failures occur, and
- prevents issues arising due to Cisco SD-WAN Controllers operating on different configurations.

This process applies to Cisco SD-WAN Controllers in both single tenant and multitenant deployments.

Multi-stage Approach for Configuration Consistency across Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

The multi-stage approach is a two-stage process for validating and applying configuration changes across Cisco SD-WAN Controllers using Cisco SD-WAN Manager. This approach ensures uniformity in configuration across Cisco SD-WAN Controllers in a network.

The multi-stage approach includes the following stages:

1. Stage 1: Validate Configuration

   During this stage, Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to perform various validation checks on the configuration.

   - Resource validation
   - Syntax validation
   - Semantic validation

2. Stage 2: Apply Configuration

   Upon successful completion of Stage 1, Cisco SD-WAN Manager instructs all Cisco SD-WAN Controllers to apply the configuration. The Cisco SD-WAN Controllers perform another resource validation check before committing the configuration.

3. Stage 3: Rollback Configuration

   This is an optional stage. Cisco SD-WAN Manager initiates this stage only when Stage 2 fails. This stage involves rollback of configuration changes on all Cisco SD-WAN Controllers if one or more controllers are unable to accept or apply the configuration. Cisco SD-WAN Manager rolls back the configuration

changes on all devices on which it is deployed successfully. Rollback prevents partial implementation of configurations and ensures uniformity in configuration across Cisco SD-WAN Controllers in a network.

Interim Acknowledgements(ACKs) and Handling Timeouts

During Stage 1 and Stage 2 in the multi-stage approach, Cisco SD-WAN Manager sends requests to validate and apply configuration changes to Cisco SD-WAN Controllers. To keep the communication open and active with Cisco SD-WAN Manager, Cisco SD-WAN Controllers send periodic interim ACKs back to the Cisco SD-WAN Manager. This communication serves two primary purposes:

- Status display: It allows the Cisco SD-WAN Manager to display the ongoing status of validation and application of configuration through task logs.
- Task or activity timer management: It helps in adjusting the task or activity timer for an operation and prevents Cisco SD-WAN Manager from timeout.

Rolling Timeouts

Rolling timeout is an important mechanism in the multi-stage approach. It is a dynamic timeout mechanism where the timeout period is continuously reset based on successful communication between Cisco SD-WAN Controller and Cisco SD-WAN Manager. The rolling timeout period of 25 minutes starts after Cisco SD-WAN Manager receives the last successful interim ACK from any Cisco SD-WAN Controller. If a timeout occurs, Cisco SD-WAN Manager terminates applying configuration changes to all the Cisco SD-WAN Controllers in the network. When applying configuration changes fails, Cisco SD-WAN Manager initiates a rollback. This mechanism ensures that there is no inconsistency in the configuration across Cisco SD-WAN Controllers.

Supported Devices for Configuration Consistency across Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

All the devices operating in Cisco SD-WAN Controller version 20.17.1 and Cisco Catalyst SD-WAN Manager Release 20.18.1 support the process.

Restrictions for Configuration Consistency across Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

These are the restrictions for maintaining configuration consistency across Cisco SD-WAN Controllers:

- Cisco Catalyst SD-WAN Manager Release 20.18.1 supports the multi-stage approach for maintaining configuration consistency only for Cisco SD-WAN Controller version 20.18.1 and later. Cisco Catalyst SD-WAN Manager Release 20.18.1 does not support the multi-stage approach for Cisco SD-WAN Controller 20.16.1 and below. For Cisco SD-WAN Controller versions prior to 20.16.1, Cisco SD-WAN Manager implements configuration changes through the older one-step configuration deployment method.

- The Cisco SD-WAN Controllers older than version 20.18.1 do not support the multi-stage approach. During the validation before configuration deployment, if Cisco SD-WAN Manager detects older version alongside Cisco SD-WAN Controllers with version 20.18.1 and later, it stops the configuration deployment.
- Although the process is designed to maintain configuration consistency across Cisco SD-WAN Controllers, this process may occasionally be unsuccessful. If Cisco SD-WAN Manager fails to apply configuration changes and configuration rollback does not restore consistency, you may have to manually fix the validation issues.

Scenarios for Offline Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

In a successful configuration deployment scenario, the Cisco SD-WAN Manager validates and applies the configuration changes across all Cisco SD-WAN Controllers without encountering any validation issues. If one or more Cisco SD-WAN Controllers are offline during validation checks, Cisco SD-WAN Manager displays warning message when you try to apply the configuration changes. In such scenarios, Cisco SD-WAN Manager schedules the multi-stage approach for configuration deployment to a time when the Cisco SD-WAN Controller or Cisco SD-WAN Controllers are back online.



Note To avoid any validation errors, ensure that Cisco SD-WAN Controllers are online before implementing the configuration changes.

Offline Cisco SD-WAN Controllers During Validation

The following table lists the scenarios where a Cisco SD-WAN Controller or multiple Cisco SD-WAN Controllers connected to other Cisco SD-WAN Control Components are offline during the validation stage before applying configuration changes.

Table 53: Scenarios for Offline Cisco SD-WAN Controller During Validation

Connected to Cisco SD-WAN Manager	Connected to Cisco SD-WAN Validator	Connected to Peer Cisco SD-WAN Controller	Result
Yes	Yes There is no validation check as there is a connection between Cisco SD-WAN Controller and Cisco SD-WAN Manager.	Yes There is no validation check as there is a connection between Cisco SD-WAN Controller and Cisco SD-WAN Manager.	Cisco SD-WAN Manager allow configuration changes.

Connected to Cisco SD-WAN Manager	Connected to Cisco SD-WAN Validator	Connected to Peer Cisco SD-WAN Controller	Result
No	Yes	Yes There is no validation check as there is a connection between Cisco SD-WAN Controller and Cisco SD-WAN Validator.	Cisco SD-WAN Manager does not allow configuration changes.
No	No	Yes	Cisco SD-WAN Manager does not allow configuration changes.
No	No	No	For a single tenant or a multitenant provider, Cisco SD-WAN Manager allows configuration changes. You can proceed with configuration deployment. For more information, see the section following this table. We recommend not to proceed with offline Cisco SD-WAN Controllers.
			For multitenant provider, Cisco SD-WAN Manager does not allow configuration changes unless the offline Cisco SD-WAN Controller is in valid mode.

For the last scenario in the preceding table, where an offline Cisco SD-WAN Controller is not connected to other Cisco SD-WAN Control Components, you can continue with configuration changes. If you agree to proceed with configuration deployment, and the offline Cisco SD-WAN Controller is in valid mode, then the offline Cisco SD-WAN Controller moves to configuration initialization mode (config-init mode). In this mode, the Cisco SD-WAN Controller is not active in the network.

Cisco SD-WAN Manager schedules the configuration deployment for the offline Cisco SD-WAN Controllers to a time when these Cisco SD-WAN Controllers are back online.

When the Cisco SD-WAN Controller is back online, it receives the configuration successfully, Cisco SD-WAN Manager changes the mode to valid mode.

Note We recommend not to use config-init mode unless it is absolutely necessary. The Cisco SD-WAN Controllers in config-init mode in the network do not participate in the route distribution, which affects network functionality. Instead of using config-init mode when Cisco SD-WAN Controllers are offline, try to bring the Cisco SD-WAN Controller back online.

Rolling Timeout for Offline Cisco SD-WAN Controllers

If one or more Cisco SD-WAN Controllers are offline during the validation or application stage, a rolling timeout occurs 25 minutes after the last successful interim ACK from any of these Cisco SD-WAN Controllers.

Warning Messages for Offline Cisco SD-WAN Controllers

When deploying a configuration on Cisco SD-WAN Controllers, Cisco SD-WAN Manager displays a warning message during validation if it detects one or more offline Cisco SD-WAN Controllers. This message includes details of the validation issues. It appears during the validation stage in the following procedures:

- When activating centralized policy. For more information about the procedure, see Activate a Centralized Policy.
- When deploying a topology group to the Cisco SD-WAN Control Components. For more information about the procedure, see Activate the Topology.
- After pushing the configuration to the devices. For more information about the procedure, see Attach a Device Template to Devices.
- When saving an application-aware policy in the Cisco SD-WAN Controllers. For more information about the procedure, see Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Verify Consistent Configuration across Cisco Catalyst SD-WAN Controllers

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

Use the following commands to verify the configuration consistency across Cisco Catalyst SD-WAN Controller.

The following is a sample output from the command **show config-pull transactions detail** using the detail keyword:

```
Device# show config-pull transactions detail
config-pull transactions 1
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497
 tenant     default
 start-time 2025-01-26T03:49:15
 activity 2025-01-26T03:49:20.124
  type    validate-in-progress
  message "Time elapsed: 5 secs"
 activity 2025-01-26T03:49:24.302
  type    validate-in-progress
  message "Time elapsed: 9 secs"
```

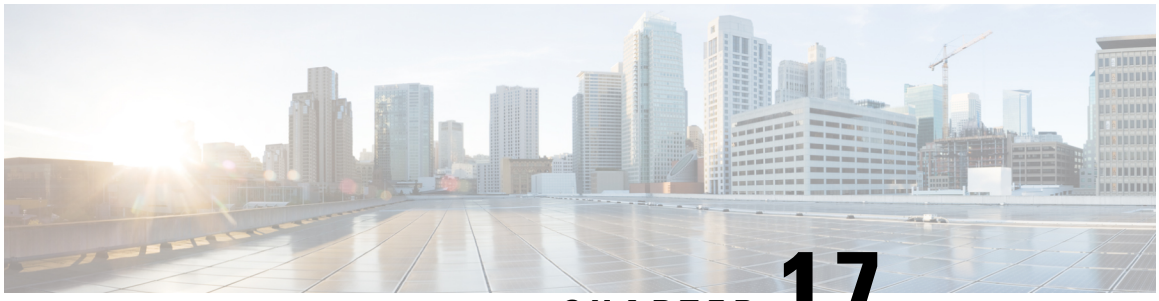
```
 activity 2025-01-26T03:49:32.461
  type    validate-in-progress
  message "Time elapsed: 17 secs"
 activity 2025-01-26T03:49:36.626
  type    validate-success
  message "Config validation success"
 activity 2025-01-26T03:49:41.752
  type    apply-in-progress
  message "Time elapsed: 4 secs"
 activity 2025-01-26T03:49:45.917
  type    apply-in-progress
  message "Time elapsed: 8 secs"
 activity 2025-01-26T03:49:54.094
  type    apply-in-progress
  message "Time elapsed: 17 secs"
 activity 2025-01-26T03:50:10.332
  type    apply-in-progress
  message "Time elapsed: 33 secs"
 activity 2025-01-26T03:50:18.521
  type    apply-success
  message "OMP readiness check progress 100%"
```

In this example, you can view the transaction details for a **config-pull** transaction. It provides information on each transaction, intermittent state status, and so on.

The following is a sample output from the **show config-pull history** command using the detail keyword:

```
Device# show config-pull history detail
config-pull history 1
 start-time 2025-01-26T03:49:15
 tenant     default
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497
 stage      validate
 duration   21
 result     success
config-pull history 2
 start-time 2025-01-26T03:49:37
 tenant     default
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497
 stage      apply
 duration   41
 result     success
```

In this example, you can view the history of validation and application of a configuration on a Cisco SD-WAN Controller.



CHAPTER 17

Export and Import Cisco SD-WAN Manager Configurations

Table 54: Feature History

Feature Name	Release Information	Description
Export and Import Cisco SD-WAN Manager Configurations	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	Export and import configuration groups, policy groups, and topologies from Cisco SD-WAN Manager as a .tar.gz file.

- Information About Exporting and Importing Cisco SD-WAN Manager Configurations, on page 281
- Prerequisites for Exporting and Importing Cisco SD-WAN Manager Configurations, on page 282
- Restrictions for Exporting and Importing Cisco SD-WAN Manager Configurations, on page 282
- Use Cases for Exporting and Importing Cisco SD-WAN Manager Configurations, on page 282
- Export Cisco SD-WAN Manager Configurations, on page 282
- Import Cisco SD-WAN Manager Configurations, on page 283

Information About Exporting and Importing Cisco SD-WAN Manager Configurations

Cisco SD-WAN Manager can export configuration files containing configuration group, policy group, or topology information. The file format is .tar.gz. You can import a configuration file to a Cisco SD-WAN Manager instance to load these configurations.

Benefits of Exporting and Importing Cisco SD-WAN Manager Configurations

- Share configuration across a network.
- Achieve consistency in configuring Cisco SD-WAN edge devices across different Cisco SD-WAN fabrics.

Prerequisites for Exporting and Importing Cisco SD-WAN Manager Configurations

Familiarity with Configuration Groups and Policy Groups in Cisco SD-WAN Manager.

Restrictions for Exporting and Importing Cisco SD-WAN Manager Configurations

- When a configuration file import encounters a name clash with existing config groups, policy groups, or topology in the Cisco SD-WAN Manager, it triggers an error on the task-list page, aborts the import, and the reason for the error is displayed. Edit the conflicting entities in the existing config groups, policy groups, or topology to rename.

  You can also create a copy using the Cisco SD-WAN Manager before attempting to reimport.

- When importing a configuration file into a Cisco SD-WAN Manager with existing feature profiles that have matching names, the Cisco SD-WAN Manager automatically omits the conflicting profiles from the import and retains the pre-existing configurations, ensuring no overwriting occurs.

Use Cases for Exporting and Importing Cisco SD-WAN Manager Configurations

- When you expand your network to include new branch offices or remote sites, export a working configuration from an existing Cisco SD-WAN Manager and import it into another Cisco SD-WAN Manager.
- Export a working configuration from a Cisco SD-WAN Manager and import the configuration to another Cisco SD-WAN Manager for quicker deployments.
- In a multitenant environment, the tenants receive the exported configurations from the provider and can import them into their respective environments. The tenants can rapidly apply standardized configurations provided by the provider, ensuring consistency across their network devices and services. This facilitates a uniform network management approach and aids in maintaining alignment with predefined policies and security protocols. For more information, see Overview of Cisco SD-WAN Multitenancy.

Export Cisco SD-WAN Manager Configurations

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** or **Configuration** > **Policy Groups** or **Configuration** > **Topology**.
2. Click **Export**.
3. Depending on your choice in step 1, perform one of the following:

In the **Configuration Group** tab, choose the configuration groups to export.

or

In the **Policy Group** tab, choose the policy groups that you'd like to export.

or

In the **Topology** tab, choose the topologies that you'd like to export.



Note You can select multiple configuration groups, policy groups, and topologies from each of the tabs. For example, you can choose two configuration groups from the **Configuration Group** tab, navigate to the **Policy Group** tab and choose two policy groups. You can export the configurations together as a single configuration.

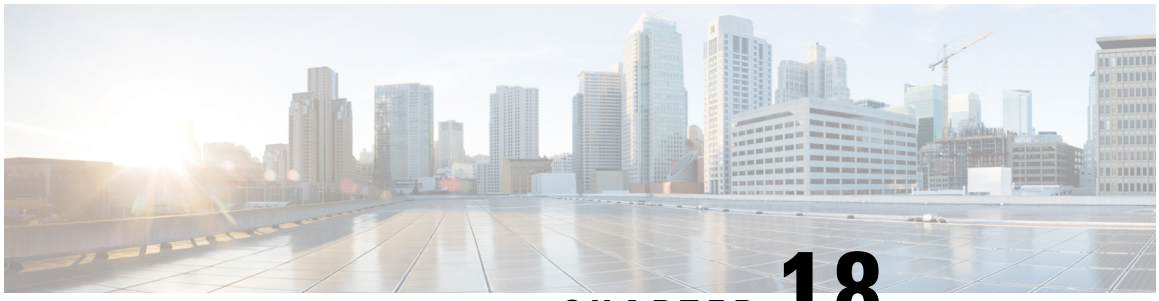
4. Click **Export**.

   The configurations are downloaded to your local storage as a .tar.gz file.

Import Cisco SD-WAN Manager Configurations

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** or **Configuration** > **Policy Groups** or **Configuration** > **Topology**.
2. Click **Import**.
3. Navigate to the file location of the .tar.gz file to import and click **Import**.

   Cisco SD-WAN Manager imports the file and loads the configuration.



CHAPTER 18

Cellular Modem Firmware Upgrade

- Cellular Modem Firmware Upgrade, on page 285
- Information About Cellular Modem Firmware Upgrade, on page 286
- Supported Platforms for Cellular Modem Firmware Upgrade, on page 288
- Supported Platforms for Wi-Fi module firmware upgrade, on page 288
- Prerequisites for Cellular Modem Firmware Upgrade, on page 288
- Prerequisites for Wi-Fi module firmware upgrades, on page 289
- Restrictions for Cellular Modem Firmware Upgrade, on page 289
- Order of firmware upgrade, on page 289
- Upgrade the Cellular Modem Firmware of a Device, on page 290
- View the Status of a Cellular Modem Firmware Upgrade, on page 291
- Configure a Remote File Server for Firmware Upgrade Images, on page 292
- Firmware upgrade for P-LTE-450 MHz modules, on page 292
- Firmware upgrade for Wi-Fi modules, on page 293
- Upgrading module firmware using Cisco SD-WAN Manager, on page 293
- Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules, on page 294

Cellular Modem Firmware Upgrade

Table 55: Feature History

Feature Name	Release Information	Feature Description
Cellular Modem Firmware Upgrade	Cisco IOS CG Release 17.12.1 Cisco Catalyst SD-WAN Control Components Release 20.12.1	Cisco SD-WAN Manager supports upgrading the cellular modem firmware of the following devices running Cisco IOS CG software: • Cisco Catalyst Wireless Gateways (CG113-4GW6) • Cisco Catalyst Cellular Gateways (CG522-E, CG418-E)

Feature Name	Release Information	Feature Description
Cellular Modem Firmware Upgrade for Cisco IOS XE Platforms	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	Extended support to the following platforms, when equipped with a cellular modem: • Cisco ISR1100 and ISR1100X Series Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms
P-LTE-450 MHz Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports upgrading the P-LTE-450 MHz module firmware on the following platforms: • Cisco IR1101 platform • Cisco IR1800 Series platforms See the Firmware upgrade for P-LTE-450 MHz modules section.
Wi-Fi Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports upgrading the Wi-Fi module firmware on Cisco IR1800 platforms.

Information About Cellular Modem Firmware Upgrade

Using Cisco SD-WAN Manager, you can upgrade the cellular modem firmware of devices that include a cellular modem.

Notification of Available Firmware Upgrades

On the Cisco Software Download site, you can log in with your user account and set notifications to inform you of when a firmware upgrade is available for your devices.

Upgrade Process

After you download firmware upgrade files from the Cisco Software Download site, the overall process is as follows:

- Save the downloaded firmware upgrade files to a file server accessible by the devices in the network. For details, see **Before You Begin** in Upgrade the Cellular Modem Firmware of a Device, on page 290.

- Using the workflow described in Upgrade the Cellular Modem Firmware of a Device, on page 290, select the devices for which to upgrade the modem firmware using the downloaded files. In that workflow, you indicate the location of the file server and directory. If a firmware update file is available for a selected device, Cisco SD-WAN Manager automatically determines the correct file to use and upgrades the modem firmware on the device.

The workflow enables you to schedule the firmware upgrade for a specific time, such as to align with a maintenance window.

Example Illustrating Cellular Modem Firmware Upgrade

The following example scenario illustrates how the firmware upgrade affects only the active firmware on the device.

1. You begin with the following firmware versions on a cellular-enabled device:

```
Router#show cellular 0/2/0 firmware
 Idx Carrier              FwVersion        PriVersion   Status
 1   DOCOMO               02.24.05.06      001.007_000  Inactive
 2   GENERIC              02.24.05.06      002.026_000  Active
 3   KDDI                 02.24.05.06      001.005_000  Inactive

Firmware Activation mode  =  AUTO
```

   The command output indicates, for example, that the GENERIC firmware type has firmware version 02.24.05.06, and that the GENERIC firmware type is the active one.

2. You learn that there are two firmware upgrades available:
   - For GENERIC, you can download 02.24.05.07.
   - For DOCOMO, you can download 02.24.05.07.
3. You download both of the files and put them on the file server.
4. You run the firmware upgrade workflow, described in Upgrade the Cellular Modem Firmware of a Device, on page 290.
   - The device finds the GENERIC 02.24.05.07 firmware upgrade file and uses it to upgrade the GENERIC firmware type, which is the active firmware type.
   - The device does not upgrade the DOCOMO firmware type, even though there is a firmware upgrade file that could accomplish that. This is because DOCOMO is not an active firmware type on the device.
5. After the upgrade, check the firmware versions and note that the firmware upgrade occurred only for the GENERIC firmware type, which is the active one.

```
Router#show cellular 0/2/0 firmware
 Idx Carrier              FwVersion        PriVersion   Status
 1   DOCOMO               02.24.05.06      001.007_000  Inactive
 2   GENERIC              02.24.05.07      002.026_000  Active
 3   KDDI                 02.24.05.06      001.005_000  Inactive

Firmware Activation mode  =  AUTO
```

Benefits of Cellular Modem Firmware Upgrade

Cisco SD-WAN Manager provides an easy-to-use workflow for upgrading modem firmware on one or more devices, making it unnecessary to execute modem firmware upgrade using CLI commands on each device individually.

Supported Platforms for Cellular Modem Firmware Upgrade

- From Cisco Catalyst SD-WAN Control Components Release 20.12.1:
  - Cisco Catalyst Wireless Gateways (CG113-4GW6)
  - Cisco Catalyst Cellular Gateways (CG522-E, CG418-E)
- From Cisco Catalyst SD-WAN Control Components Release 20.14.1:
  - Cisco ISR1100 and ISR1100X Series Platforms
  - Cisco Catalyst 8200 Series Edge Platforms
  - Cisco Catalyst 8300 Series Edge Platforms
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, for P-LTE-450 modules:
  - Cisco IR1101 Platform
  - Cisco IR1800 Series Platforms

Supported Platforms for Wi-Fi module firmware upgrade

Wi-Fi module firmware upgrade

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the Cisco IR1800 series supports Wi-Fi module firmware upgrade using Cisco SD-WAN Manager.

Prerequisites for Cellular Modem Firmware Upgrade

File Server Accessibility

Ensure that the file server storing the firmware upgrade files is accessible by the devices in the network.

Firmware Download

Download the required firmware updates from Cisco.com, for the cellular-modem-equipped devices you wish to upgrade.

Prerequisites for Wi-Fi module firmware upgrades

Minimum Firmware Version – Wi-Fi Module

The Wi-Fi module must be running a firmware version 17.17.1 or higher. If the module's firmware version is earlier than 17.17.1, you cannot upgrade to 17.18.x or later using Cisco SD-WAN Manager.

To verify the current firmware version of a Wi-Fi module, use the `show wireless-bridge status` CLI command.

Restrictions for Cellular Modem Firmware Upgrade

- After downloading a firmware upgrade file from Cisco.com, do not change the filename. A device uses the filename to determine which firmware upgrade files are relevant to it.
- Cisco SD-WAN Manager only supports upgrading the currently active firmware type. For example a device may have five different firmware types, such as generic and firmware for four specific carriers. Only one firmware type can be active at a given time and Cisco SD-WAN Manager upgrades only the the active one.
- Firmware downgrade is not supported by Cisco SD-WAN Manager.
- The P-LTE-450 firmware upgrade will not start if the device is turned off or unreachable.

Order of firmware upgrade

Upgrade Sequence

The firmware upgrade process follows a specific order of precedence based on the firmware files present on the remote server. Modules are upgraded in this order:

- Wi-Fi Module
- P-LTE-450 module
- LTE module

To ensure the correct module is upgraded, save only the relevant firmware files on the remote server.

For example, if you want to upgrade the firmware for LTE modules, make sure that no Wi-Fi firmware files are stored on the server. If firmware files for other modules, such as Wi-Fi or P-LTE-450 module are present, those modules will be upgraded first, following the precedence order, even if you do not intend to upgrade them.

Note For WI-FI modules, the upgrade process works only when the device is in Workgroup Bridge (WGB) mode.

If the Wi-Fi module is turned off or unreachable, Wi-Fi module firmware upgrade will be skipped and cellular modem firmware upgrade will continue.

Upgrade the Cellular Modem Firmware of a Device

Before You Begin

- See the prerequisites and restrictions sections of this documentation.
- Download firmware upgrade files from the Cisco Software Download site.
- Save the downloaded firmware upgrade files to a file server accessible by devices in the network. The file types of the downloaded files may differ, according to the different modem hardware used in your Cisco products. Example file types include .bin, .cwe, .nvu, and .spk.

  You can download firmware upgrade files for different types of cellular-enabled devices and in most cases, save them to the same directory on the file server. If the firmware upgrade for your device requires two files for two upgrade steps (a modem firmware upgrade file, and a separate OEM PRI file) save the two files to separate directories.

Upgrade the Cellular Modem Firmware of a Device

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Firmware Upgrade**.
2. In the workflow, follow the prompts to select the devices to upgrade, the server, and the firmware image path.

   When configuring a server for storing firmware upgrade images, enter the following fields:

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID, Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

Note For information about configuring a remote server for storing device software upgrade images, see Register Remote Server in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

If a relevant firmware upgrade file exists at the image path location, the device uses the file for the upgrade. If more than one relevant firmware upgrade file is available, the device uses the latest version. If no relevant file exists at the image path location, the **Summary** page of the workflow indicates that no file is available, and no firmware upgrade occurs.

Cisco SD-WAN Manager upgrades only the currently active firmware type.

Note The workflow prompts you to configure a remote server. Alternatively, you can configure a file server as described in Configure a Remote File Server for Firmware Upgrade Images, on page 292.

3. Optionally, schedule the upgrade for a specific time, for example to coincide with a maintenance window.

Note To cancel a scheduled upgrade before it occurs, do the following:

   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

   b. Click **Firmware**.

   c. Click **Cancel Firmware Upgrade** to cancel a scheduled upgrade.

4. On the **Summary** page, review the details and click **Next** to begin the upgrade task.

   The upgrade takes several minutes.

5. (Optional) Click **Check my upgrade task** to show the status of the upgrade or upgrades for each device.

View the Status of a Cellular Modem Firmware Upgrade

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **Firmware**.

   The table shows devices in the process of firmware upgrade or awaiting a scheduled upgrade. See the **CurrentVersion** column to view the firmware version of a device.
3. (Optional) Click **Cancel Firmware Upgrade** to cancel a scheduled upgrade.

Configure a Remote File Server for Firmware Upgrade Images

Before You Begin

This procedure addresses configuring a remote server for firmware upgrade images, for the firmware upgrade use case. For information about configuring a remote server for storing device software upgrade images, see Register Remote Server in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Configure a Remote File Server for Firmware Upgrade Images

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** and click **Remote Server**.
2. Click **Add Remote Server** and enter the following fields:

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID, Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files, or enter **/** by itself, which enables you to specify the path while executing the Firmware Upgrade workflow.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

3. Click **Add**.

Firmware upgrade for P-LTE-450 MHz modules

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can upgrade the firmware for P-LTE-450 MHz modules on Cisco IOS XE Catalyst SD-WAN devices from the Cisco SD-WAN Manager.

A P-LTE-450 module firmware upgrade is a process that:

- provides you a simplified workflow in Cisco SD-WAN Manager for upgrade,
- enables you to upgrade multiple devices at the same time, and
- allows you to track upgrade status and schedule tasks from a central interface.

Firmware upgrade for Wi-Fi modules

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can upgrade the Wi-Fi modules (PID is WP-WIFI6) on Cisco IOS XE Catalyst SD-WAN devices directly from the Cisco SD-WAN Manager.

A Wi-Fi module firmware upgrade is a process that:

- provides you a simplified workflow in Cisco SD-WAN Manager for upgrade,
- enables you to upgrade multiple devices at the same time, and
- allows you to track upgrade status and schedule tasks from a central interface.

Upgrading module firmware using Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the following module firmware upgrades are supported:

- P-LTE-450 MHz module
- Wi-Fi module

Summary

The module firmware upgrade process involves a sequence of actions between the SD-WAN Manager, remote server, and devices. Cisco SD-WAN Manager sends the necessary instructions to each device, which then performs pre-checks, downloads, validates, and installs the firmware. Throughout the process, Cisco SD-WAN Manager provides real-time status updates, allowing you to monitor and confirm the completion of the upgrade across all selected devices.

Workflow

These are the stages of upgrading firmware for P-LTE-450 MHz and Wi-Fi modules:

1. Identify device or module: Identify the device or module that requires a firmware upgrade. Cisco SD-WAN Manager displays the list of devices that are eligible for firmware upgrade. Each of these devices have either a Wi-Fi module, P-LTE-450 MHz module, or a cellular modem or a combination of these.

   Before you proceed with upgrading the firmware for the module, make a note of which devices to upgrade. This is an important step because firmware upgrade is done in a specific order. For more information, see Order of firmware upgrade, on page 289.

2. Download firmware files: Download the firmware files for the Wi-Fi module from Cisco Software Central. All the firmware files are hosted on Cisco Software Central. After identifying the device to be upgraded, search and download the specific firmware software.

   Download the firmware files for the P-LTE-450 MHz module from the Intelliport product website. For any assistance, contact the Intelliport representatives. You can download the Pluggable Interface Module (PIM) firmware or modem firmware or both.

Save the downloaded firmware upgrade files to a file server accessible by devices in the network.

3. Configure a remote server to host the firmware image:

   The P-LTE-450 PIM has an integrated modem, which is a core component for establishing and managing the connection to the LTE 450 MHz mobile networks. The firmware upgrade of P-LTE-450 module includes upgrading the PIM firmware and the modem firmware.

   There are two phases in the P-LTE-450 firmware upgrade process, each using a separate firmware file. The sequence of upgrade is as follows:

   a. Modem firmware is upgraded first

   b. PIM firmware is upgraded next

   You can also upgrade the modem firmware and PIM firmware seperately. If the firmware upgrade fails either for PIM or modem, an error message with error details appears on Cisco SD-WAN Manager.

   To configure remote file server for firmware upgrade, see Configure a Remote File Server for Firmware Upgrade Images, on page 292.

4. Understand the order of upgrading firmware:The firmware upgrade process follows a specific order of precedence based on the firmware files present on the remote server. For more information, see Order of firmware upgrade, on page 289

   .

5. Start or Schedule the firmware upgrade: Use the firmware upgrade workflow in Cisco SD-WAN Manager. You can start the upgrade right away or schedule it for a specific time, for example to coincide with a maintenance window. For more information, see Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules, on page 294.

6. Processing upgrade: Cisco SD-WAN Manager sends an upgrade request, including server details and the firmware path, to each device for the modules requiring an upgrade. Each device verifies the files, then downloads and installs the firmware either at the scheduled time or immediately.

7. Track progress: Use Cisco SD-WAN Manager to monitor the status of your firmware upgrades.

8. Upgrade execution: After verification, the P-LTE-450 MHz or the Wi-Fi module firmware is upgraded.

9. Verify the firmware upgrade: After the upgrade, verify that the devices have successfully updated to the new firmware version. For more information, see View the Status of a Cellular Modem Firmware Upgrade, on page 291.

Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

This section provides the steps to upgrade the firmware on your Cisco IOS XE Catalyst SD-WAN device.

Before you begin

- See the prerequisite and restrictions sections.
- See the Supported Platforms for Cellular Modem Firmware Upgrade, on page 288 section.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Firmware Upgrade**.

Step 2 In the workflow, follow the prompts to choose the devices to upgrade. Proceed with one of the methods in the following table based on your scenario.

If..	Then..
If you have configured the remote server for storing firmware image files.	Follow the prompts to choose the server, and the firmware image path.
If you want to configure a remote server in the firmware upgrade workflow.	After choosing the device or devices to upgrade, configure a remote file server for the firmware upgrade images. To configure a remote file server, click the **Select remote server** dropdown, then click **Create New**, and enter the following fields in the **Add Remote Server**. See the following table "Add Remote Server" to enter the fields.
If you want to configure a remote server from **Maintenance** > **Software Repository**.	Configure a file server as described in Configure a Remote File Server for Firmware Upgrade Images, on page 292.

Table 56: Add Remote Server

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol. **Note** For P-LTE-450 MHz and Wi-Fi modules, choose only SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID and Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

The following table describes different scenarios when one, multiple, or no relevant firmware upgrade files are found at the specified location.

Table 57: Image Path Location

If..	Then..
If a relevant firmware upgrade file exists at the image path location.	The device uses the file for the upgrade.
If more than one relevant firmware upgrade file is available.	The device uses the latest version.
If no relevant file exists at the image path location.	The device checks the availability of files on the specified remote server. The firmware upgrade fails if no valid files are found on the remote server. This status is indicated in the **Summary** page of the workflow.

Cisco SD-WAN Manager upgrades only the currently active firmware type.

Step 3 If you have not configured a remote server, you can configure it after selecting a device. To configure a remote file server for firmware upgrade images, click the **Select remote server** dropdown, then click **Create New**, and enter the required fields.

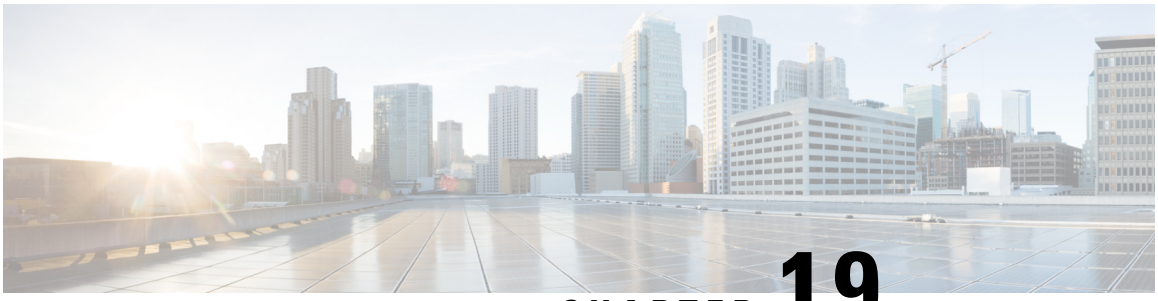
Step 4 Optionally, schedule the upgrade for a specific time, for example to coincide with a maintenance window.

Step 5 On the **Summary** page, review the details and click **Next** to begin the upgrade task.

Step 6 (Optional) Click **Check my upgrade task** to see the status of the upgrade or upgrades for each device.

What to do next

View status of the firmware upgrade, View the Status of a Cellular Modem Firmware Upgrade



CHAPTER 19

Protocol Pack Management and Compliance

- Protocol Pack Management and Compliance, on page 297
- Information About Protocol Pack Management and Compliance, on page 298
- Upgrading when a device becomes compatible, on page 299
- Restrictions for Protocol Pack Management and Compliance, on page 299
- Upload a Protocol Pack to Cisco SD-WAN Manager, on page 300
- Upgrade a device Protocol Pack, on page 301
- Check Protocol Pack Compliance, on page 301
- View Protocol Pack Status, on page 302
- Delete Protocol Packs, on page 303

Protocol Pack Management and Compliance

Table 58: Feature History

Feature Name	Release Information	Feature Description
Protocol Pack Management and Compliance	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	Cisco SD-WAN Manager management of Protocol Packs includes functions such as the following: • Upgrading Protocol Pack releases on routers in the network. • Flagging the status of routers using an older Protocol Pack release than the current reference release.

Feature Name	Release Information	Feature Description
Pending requests for upgrading a device Protocol Pack	Cisco Catalyst SD-WAN Control Components Release 20.18.1	If you attempt to execute a Protocol Pack upgrade for a set of devices, it is possible that one or more of the devices are using a software version that does not support the Protocol Pack. In this case, the upgrade does not proceed for those devices. You can choose an option for Cisco SD-WAN Manager to keep the pending request to upgrade the device's Protocol Pack, to execute later. SD-WAN Manager checks the device when it receives a software upgrade, and if the new software version supports the Protocol Pack, SD-WAN Manager completes the upgrade.
Delete Protocol Packs	Cisco Catalyst SD-WAN Control Components Release 20.18.1	You can delete a Protocol Pack loaded into Cisco SD-WAN Manager. This is useful for removing Protocol Packs that are no longer in use in your network.

Information About Protocol Pack Management and Compliance

Cisco SD-WAN Manager includes a pre-installed Protocol Pack, which is a standard set of protocols for classifying network traffic according to the application producing the traffic. The protocols, also called applications, can be used for application-aware policy, security policy, and QoS policy, to match traffic based on the application producing the traffic. And they are used for tracking which applications are producing traffic within the network—called application visibility.

Protocol Pack Releases

Periodic Protocol Pack releases include updates to the application set, such as the following:

- Expanding individual applications to a set of related applications to enable more granular classification of traffic

  For example, a Protocol Pack release may enable classifying the traffic produced by a multimedia application, and a subsequent release could distinguish with better granularity between the audio traffic and the video traffic that the multimedia application produces.

- New applications
- Renamed applications

Upgrading the Protocol Pack Installed on Devices

Devices running a long-lived Cisco IOS XE release support upgrading from the Protocol Pack built into the release to a later Protocol Pack release. This is supported from Cisco Catalyst SD-WAN Manager Release 20.15.1.

Uses for the Reference Protocol Pack Release

You can upload new Protocol Pack releases into Cisco SD-WAN Manager when they become available. For the procedure, see Upload a Protocol Pack to Cisco SD-WAN Manager, on page 300. The latest release uploaded into Cisco SD-WAN Manager has a specific role. It functions as the reference Protocol Pack release. Cisco SD-WAN Manager displays the current reference release on the **Configuration** > **Application Catalog** > **Application Source Settings** page, in the **Version** field.

Cisco SD-WAN Manager uses the reference Protocol Pack release for the following functions:

- Checking whether each router in the network is using the latest Protocol Pack available through Cisco SD-WAN Manager. If a router is using an earlier Protocol Pack, the table on the **Configuration** > **Application Catalog** > **Application Source Settings** page shows the status in the **Compatibility Status** column.
- Checking whether policies that match traffic by application use applications that have been changed in a more recent Protocol Pack release. For information about policy compliance, see Protocol Pack Management and Compliance, on page 297.

Upgrading when a device becomes compatible

If you attempt to execute a Protocol Pack upgrade for a set of devices, it is possible that one or more of the devices are using a Cisco IOS XE software version that does not support the new Protocol Pack. In this case, the upgrade does not proceed for those devices.

You can choose an option for SD-WAN Manager to save the upgrade request. SD-WAN Manager then checks the device when it receives a software upgrade, and if the new software version supports the Protocol Pack, SD-WAN Manager completes the upgrade.

Dropping the request

In unusual cases, SD-WAN Manager may drop the request to upgrade a device's Protocol Pack. This occurs when the next software upgrade on the device also does not support the Protocol Pack that you tried to push to the device.

Here's a scenario that demonstrates this:

1. You try to push a Protocol Pack x to a device using a software version that does not support the Protocol Pack x.

   Result: SD-WAN Manager does not push the Protocol Pack. It saves the request and checks back later to determine when the device will be able to support Protocol Pack x.

2. You upgrade the device's software to another version that still does not support Protocol Pack x.

   Result: In this case, SD-WAN Manager still cannot push the Protocol Pack to the device, and it drops the pending request.

Restrictions for Protocol Pack Management and Compliance

- Minimum Cisco SD-WAN Manager release for upgrading Protocol Packs: Cisco Catalyst SD-WAN Manager Release 20.15.1

- We recommend upgrading the reference Protocol Pack on Cisco SD-WAN Manager to the latest version before upgrading the Protocol Pack on any devices in the network to that version.
- We recommend using Cisco SD-WAN Manager to upgrade the Protocol Pack release on devices in the network, and not to do this individually on devices by CLI.

Upload a Protocol Pack to Cisco SD-WAN Manager

Before You Begin

For information about Protocol Pack releases, see the Cisco Protocol Pack documentation. A list of Protocol Packs appears on the NBAR2 Protocol Pack Library page.

Uploading a Protocol Pack that is a later release than previously uploaded Protocol Packs has two effects:

- As with any upload, the Protocol Pack is available for upgrading compatible devices in the network.
- If the uploaded Protocol Pack is a later release than previously uploaded Protocol Packs, it becomes the new reference release for Cisco SD-WAN Manager.

  Cisco SD-WAN Manager shows the current reference release on the **Configuration** > **Application Catalog** > **Application Source Settings** page, in the **Version** field.

  Cisco SD-WAN Manager uses the reference release as the basis for determining application compliance, policy compliance, and device Protocol Pack version compliance. For more information about compliance, see Protocol Pack Management and Compliance, on page 297.

Upload a Protocol Pack to Cisco SD-WAN Manager

1. Download a Protocol Pack from the Cisco Software Download site.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
3. Locate the **SD-WAN Manager Protocol Pack** section of the page.
4. Click **Upload SDWAN Manager Protocol Packs** to save the Protocol Pack to Cisco SD-WAN Manager.

   The uploaded Protocol Pack is available to upgrade any compatible devices in the network.

   As noted in **Before You Begin**, if the uploaded Protocol Pack is a later release than previously uploaded Protocol Packs then it becomes the new reference release. A pop-up window shows whether changing the reference Protocol Pack release would affect policy or device compliance.

   If any protocols in the Protocol Pack introduce name conflicts with existing custom applications, the upload does not proceed. See Information About Application Compliance in the *Policy Groups Configuration Guide*.
5. Click **Update** or **Ignore and Proceed** to complete the upload.



Note If you do not want to complete the upload, such as if you do not want to change the reference Protocol Pack release, click **Cancel Update**.

Upgrade a device Protocol Pack

Before You Begin

Install and enable Cisco SD-AVC on Cisco SD-WAN Manager before you upgrade device Protocol Packs. Cisco SD-AVC is required to use the Upgrade Device Protocol Pack feature. For more information, see Enabling SD-AVC on Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Use these steps to upgrade a device Protocol Pack.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.
3. Select one or more devices in the table by checking the check boxes for the devices.
4. Click **Upgrade Device Protocol Pack**.
5. In the pop-up window, choose a Protocol Pack release to install. Optionally, choose a scheduled upgrade.

Note If you schedule an upgrade for a later time, you cannot perform additional upgrades until that upgrade is complete. Only one upgrade task can be active at a given time. In a multitenant scenario, it is one upgrade task per tenant.

6. In case one or more selected devices have a software version that does not support the Protocol Pack, you can optionally select to upgrade the Protocol Pack later. Choose the Auto upgrade when device is compatible.

   SD-WAN Manager saves the request to upgrade the Protocol Pack on those devices. SD-WAN Manager monitors the devices when they receive a software upgrade, and if the new software version supports the Protocol Pack, SD-WAN Manager completes the intended upgrade, installing the Protocol Pack.

Cisco SD-WAN Manager upgrades the Protocol Pack on the device if the device software version allows the upgrade. See the Protocol Pack documentation for information about compatible Cisco IOS XE software versions.

Check Protocol Pack Compliance

Before You Begin

When you upload a new Protocol Pack, Cisco SD-WAN Manager automatically checks whether each device in the network is using the latest available Protocol Pack—called compliance. In addition, it checks policy and device Protocol Pack compliance at regular intervals. For more information about compliance, see Protocol Pack Management and Compliance, on page 297.

You can trigger the compliance check manually using this procedure. This may be helpful, for example, to check compliance after upgrading the Protocol Pack on one or more devices.

Check Protocol Pack Compliance

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.
3. Click **Sync Compliance**.

View Protocol Pack Status

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.

   At the top of the section, the **Version** field shows the latest Protocol Pack release uploaded to Cisco SD-WAN Manager.

   The table shows each router, the loaded Protocol Pack release, and related information, as described here:

Field	Description
Hostname	Device hostname.
Site ID	Device site ID.
Device Model	Device model name.
Software Version	Software release operating on the device.
Protocol Pack Version	Protocol Pack release loaded on the device.
Reachability	Reachability of the device by Cisco SD-WAN Manager.
Compatibility Status	• Green: The Protocol Pack loaded on the device matches the Protocol Pack loaded in Cisco SD-WAN Manager. • Red: The Protocol Pack loaded on the device does not match the Protocol Pack loaded in Cisco SD-WAN Manager.

Field	Description
Upgrade Status	Indicates whether a Protocol Pack upgrade has been performed on the device, and the status of the update: • **No job history**: No attempt to upgrade the Protocol Pack. • **In-progress**: Cisco SD-WAN Manager is currently upgrading the Protocol Pack on a device. • **Success**: Cisco SD-WAN Manager has upgraded the Protocol Pack. • **Skipped**: Cisco SD-WAN Manager did not find a compatible Protocol Pack. • **Failure**: Cisco SD-WAN Manager has tried unsuccessfully to upgrade a Protocol Pack. • **Scheduled**: Cisco SD-WAN Manager is scheduled to upgrade the Protocol Pack. • **Canceled**: Cisco SD-WAN Manager has canceled a scheduled upgrade.

Delete Protocol Packs

Procedure

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

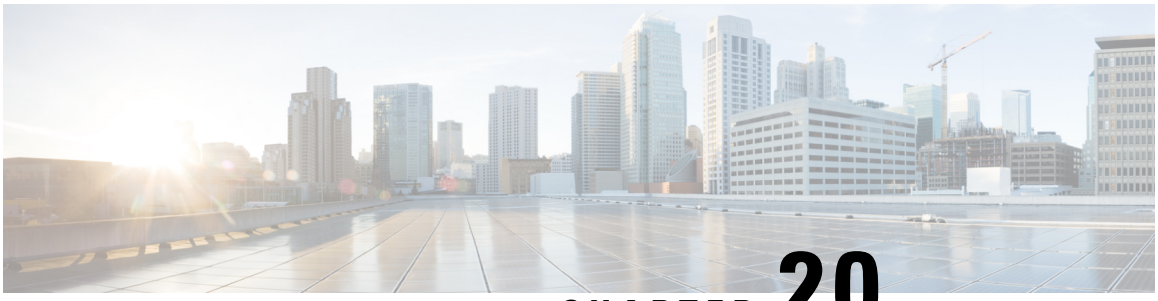
Step 2 Open **Application Source Settings**.

Step 3 Click **Delete Protocol Pack**.

SD-WAN Manager shows a list of the loaded Protocol Packs. The list provides an option to delete Protocol Packs that are not in use in the network, and that don't meet other conditions that require them to remain available. The conditions include, but are not limited to:

- Protocol Packs that are currently deployed or scheduled for deployment
- The Protocol Pack that SD-WAN Manager is using as its reference Protocol Pack

Step 4 From the list of loaded Protocol Packs, delete any desired Protocol Pack that has the delete option available.



CHAPTER 20

Remote Server Support for ZTP Software Upgrade

Table 59: Feature History

Feature Name	Release Information	Description
Remote Server Support for ZTP Software Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	This features introduces remote server support for upgrading the software of Cisco IOS XE Catalyst SD-WAN devices at scale using Zero Touch Provisioning (ZTP). Upload the software upgrade images to Cisco SD-WAN Manager using a preferred remote server and then upgrade the respective devices.

- Information About Remote Server Support for ZTP Upgrade, on page 305
- Benefits of Remote Server Support for ZTP Upgrade, on page 306
- Supported Devices for Remote Server Support for ZTP Upgrade, on page 307
- Prerequisites for Remote Server Support for ZTP Upgrade, on page 307
- Restrictions for Remote Server Support for ZTP Upgrade, on page 307
- Enable Enforce Software Version (ZTP), on page 308
- Upload Device List, on page 308
- Use Cisco Catalyst SD-WAN Manager to Configure and Upgrade a Device, on page 309
- Monitor the ZTP Software Install, on page 310

Information About Remote Server Support for ZTP Upgrade

You can onboard and upgrade numerous Cisco IOS XE Catalyst SD-WAN devices together, using the software images hosted on a remote server. The physical WAN edge onboard and upgrade options include the following:

- Manual
- Bootstrap
- Automated deployment

In Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and earlier, the software upgrade images are hosted only on Cisco SD-WAN Manager. During the software upgrade process, the devices fetch the upgrade information from Cisco SD-WAN Manager to upgrade the devices with the latest software.

From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, remote server support for ZTP upgrades enables you to upgrade Cisco IOS XE Catalyst SD-WAN devices using the software images stored in a remote server. The remote server support for ZTP upgrade feature enables you to register a remote server with Cisco SD-WAN Manager and add locations of the software images that are present in the remote server to theCisco SD-WAN Manager software repository. When you upgrade a device, the device downloads the new software image from the remote server, without overwhelming the Cisco SD-WAN Manager server.

When using the Cisco Catalyst SD-WAN hosted service, it is possible to enforce a version of the Cisco SD-WAN software to run on a router as it joins the fabric for the first time. When you enable ZTP, you can see the platform version and status details of the devices running on a router. For example, ISR1101 Disabled, C8000AES Disabled, ISR4400 Disabled, C8000AEP Disabled, ASR1001-X Disabled and so on.

Benefits of Remote Server Support for ZTP Upgrade

- Enables you to upgrade Cisco IOS XE Catalyst SD-WAN devices using software images stored on a remote server, thus removing the dependency on the Cisco SD-WAN Manager software repository.
- Many software upgrade image file formats are supported.
- Cisco SD-WAN Manager provides the devices that are being upgraded with the information they require to download the necessary software images from the servers hosting the images. The devices retrieve the images directly from the servers. This minimizes performance demands on Cisco SD-WAN Manager, as compared to storing images in the Cisco SD-WAN Manager software repository.

Supported Devices for Remote Server Support for ZTP Upgrade

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	• ASR 1000 • ISR 1000 • ISR 4000 series router models (with exception of ISR1100-4G/6G) • IR 1001 • IR 8340 • IR 8100 • Ciso 8000 series router models • Cisco Catalyst Wireless Gateway CG113 Series • ASR 1001-X • Cisco 1100 • Ciso ESR6300

Prerequisites for Remote Server Support for ZTP Upgrade

- Ensure that a remote server is registered to the Cisco SD-WAN Manager Software Repository. For more information see, the section Register Remote Server.
- Ensure that you add a new software image using the **Remote Server (preferred)** option. For more information see, the section Add Software Images to the Repository.

Note Ensure that the **Image Filename** matches the **Image Filename** in the **Remote Server Name** field.

- Make sure the device can reach the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers.
- To be upgraded, a device must be in the **Valid** or the **Staging Certificate** state.

Restrictions for Remote Server Support for ZTP Upgrade

- You cannot upgrade Cisco SD-WAN Manager along with devices that are present in a group upgrade operation. You must upgrade and reboot the only the Cisco SD-WAN Manager server.

- The ZTP upgrade flow doesn't restart automatically when the devices are interrupted by an unforeseen manual device reload or a power failure.
- The **Enforce Software Version (ZTP)** option is available only for Cisco IOS XE Catalyst SD-WAN devices.
- We recommend that you perform all software upgrades from Cisco SD-WAN Manager rather than from the CLI.
- Remote server support for ZTP upgrades is available only through VPN-0.

Note For software compatibility information, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Enable Enforce Software Version (ZTP)

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Enforce Software Version (ZTP)**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Enable the software version for the corresponding device.
4. In the **Image Location** window, click the **Remote Server** radio button.
5. From the **Remote Server Name** drop-down list, choose a remote server.
6. From the **Image Filename** drop-down list, choose an image.
7. Click **Save**.

Upload Device List

You can upload a list of devices that you want to upgrade, to Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Upload WAN Edge List**.
3. Upload the .CSV file that you have created from the Sample CSV.
4. Check the **Validate the uploaded vEdge List and send to controllers** checkbox.
5. Click **Upload**.

Note You can upload device lists to Cisco SD-WAN Manager using your Cisco Smart Account as well. For more information about enabling PnP Connect Sync see, Enable PnP Connect Sync.

Use Cisco Catalyst SD-WAN Manager to Configure and Upgrade a Device

Devices in the overlay network that are managed by Cisco SD-WAN Manager must be configured using Cisco SD-WAN Manager in order to be upgraded.

Use the following steps to configure and upgrade a device, using Cisco SD-WAN Manager:

1. Create feature templates:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and choose **Add Templates**.
2. Create device templates.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose **Create Templates**.
3. Attach device templates to individual devices.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose a template.
   c. Click **…**, and choose **Attach Devices**.
   d. You can see the added device in the list of **Available Devices** list. Send the particular device to the **Selected Devices** window using the **Right arrow** button.
   e. Click **Attach**.
4. In the **Device Template** window, click **...** to update the device template by entering the following parameters:

Field	Description
Status	Displays the current status of the device template.
Chassis Number	Displays the chassis number of the device.
System IP	Displays the system IP address, if applicable.
Host Name	Displays the host name, if applicable.
DNS Address (vpn_dns_primary)	Enter the DNS address.
Host Name	Enter the host name.
System IP	Enter the system IP address.
Site ID	Enter the site ID.

5. Click **Update**. and then click **Next**.

6. After the device template is added, select the device template and click **Configure Devices**.
7. The **Config Preview** is displayed.
8. Click **Configure Devices**.
9. You are routed to the **Task List** window, where you can see the status of the configuration.
10. The configuration is attached to the device once the device is online.
11. Cisco SD-WAN Manager creates a task for this software upgrade through the ZTP server, and you can monitor the status of the upgrade using the **Task List** window.

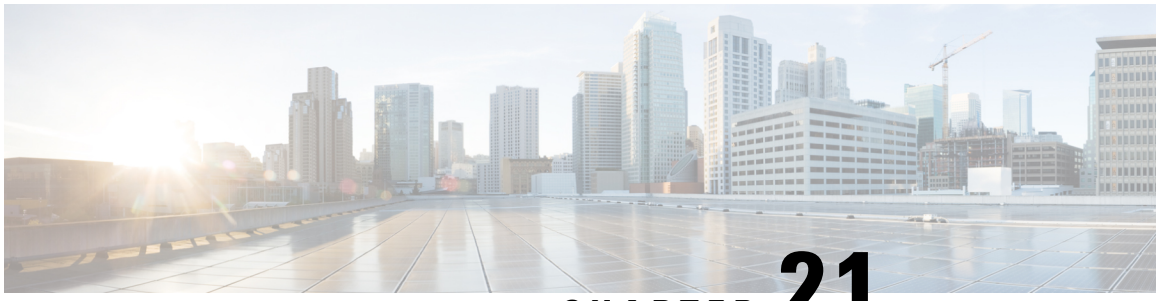
Monitor the ZTP Software Install

In Cisco SD-WAN Manager, click the task list icon at the top-right corner of the window.

The task list shows open software installation tasks, if any, and indicates the status of these tasks.



Note Cisco SD-WAN Manager pushes the device template to a device only after the software upgrade process is complete. You can monitor the status of the software upgrade using the **Tasks** window.



CHAPTER 21

Connectivity Fault Management

- Information About Connectivity Fault Management, on page 311
- Introduction to Ethernet CFM, on page 311
- Restrictions for Configuring Ethernet CFM, on page 311
- How CFM Works in Cisco Catalyst SD-WAN, on page 312
- Configure Ethernet CFM using Cisco SD-WAN Manager CLI Template, on page 313

Information About Connectivity Fault Management

Table 60: Feature History

Feature Name	Release Information	Description
Ethernet Connectivity Fault Management Support on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	The Ethernet Connectivity Fault Management functionality helps to monitor the Carrier Ethernet Network links.

Introduction to Ethernet CFM

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance ethernet layer operation, administration, and management (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large ethernet metropolitan-area networks (MANs) and wide-area-networks (WANs). Service provider networks are large and complex and have a wide user base. OAM protocols help in isolating failures and responding to them in a timely manner.

Restrictions for Configuring Ethernet CFM

- You can configure CFM only through CLI on Cisco SD-WAN Manager. Therefore, you can access the CFM execution for link fault detection, verification and isolation in the SSH terminal of your device.
- UP MEPs and maintenance intermediate points (MIPs) are not supported.

- CFM trouble-shooting functionality such as, layer 2 traceroute and ping by CFM is not supported on Cisco SD-WAN Manager. This functionality can be executed only on the device.

How CFM Works in Cisco Catalyst SD-WAN

In a network where the provider edge routers and customer premise equipment (CPE) are connected through carrier ethernet network, it is necessary to monitor the links for any breakage. With the support for CFM on carrier ethernet networks, CFM messages are exchanged between provider edges and CPEs, and the CFM protocol ensures the provider edge is aware of any link failures in the network.

CFM in Cisco Catalyst SD-WAN is supported on these interface types:

- VDSL interfaces
- SHDSL interfaces
- GigabitEthernet interfaces

The following components support the functioning of CFM on Cisco Catalyst SD-WAN.

Down Maintenance End Points

A maintenance domain is a management space for managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to the domain and at its boundary. A maintenance association identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a maintenance association.

A maintenance end point (MEP) is a demarcation point on an interface that participates in CFM within a maintenance domain. MEPs drop all lower-level frames and forward all higher-level frames. MEPs are defined per maintenance domain (level) and service (S-VLAN or ethernet virtual circuit (EVC)). They are at the edge of a domain and define the boundary and confine CFM messages within that boundary. MEPs can proactively transmit CFM continuity check messages (CCMs) and at the request of an administrator, transmit traceroute, and loopback messages.

A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. For CFM frames coming from the relay side, the down MEP drops all lower-level frames and those that are at its level. For CFM frames coming from the wire side, the down MEP processes all frames at its level and drops lower-level frames, except for traffic going to the other lower level down MEP. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or through the wire.

In order to deploy down MEP per subinterface, you must first create a EVC+VLAN maintenance association, configure the VLAN id under the subinterface, and then configure down MEP under the parent interface of that subinterface.

Ethernet CFM and Ethernet OAM Interaction

Ethernet Virtual Circuit

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by an edge device either to find an alternative path into the service

provider network or in some cases, to fall back to a backup path over Ethernet or over another alternative service such as asynchronous transfer mode (ATM).

OAM Manager

OAM manager is an infrastructure element that streamlines interaction between OAM protocols. The OAM manager requires two interworking OAM protocols, in this case, Ethernet CFM and Ethernet OAM. Interaction is unidirectional from the OAM manager to the CFM protocol and the only information exchanged is the user network interface (UNI) port status. Additional port status values available are:

- REMOTE_EE—Remote excessive errors
- LOCAL_EE—Local excessive errors
- TEST—Either remote or local loopback

After CFM receives the port status, it communicates that status across the CFM domain.

SNMP Traps

MEPs generate two types of Simple Network Management Protocol (SNMP) traps: continuity check (CC) traps and cross-check traps.

Continuity check traps:

- MEP up: Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down: Sent when a timeout or last gasp event occurs.
- Cross-connect: Sent when a service ID does not match the VLAN.
- Loop: Sent when a MEP receives its own continuity check messages (CCM).
- Configuration error: Sent when a MEP receives a continuity check with an overlapping MPID.

Cross check traps:

- Service up: Sent when all expected remote MEPs are up in time.
- MEP missing: Sent when an expected MEP is down.
- Unknown MEP: Sent when a CCM is received from an unexpected MEP.

Configure Ethernet CFM using Cisco SD-WAN Manager CLI Template

The following commands are used to configure Ethernet CFM.

1. To enable CFM IEEE version of CFM:

   Device(config)# **ethernet cfm ieee**

2. To enable CFM processing globally on the device:

Device(config)# **ethernet cfm global**

3. To enable caching of CFM data learned through traceroute messages:

   Device(config)# **ethernet cfm traceroute cache**

4. To enable ethernet CFM syslog messages:

   Device(config)# **ethernet cfm logging**

5. To enable SNMP trap generation for ethernet CFM continuity check events:

   Device(config)# **snmp-server enable traps ethernet cfm cc**

6. To enable SNMP trap generation for ethernet CFM continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs:

   csnmp-server enable traps ethernet cfm crosscheck

7. To define an EVC and enter EVC configuration mode:

   Device(config)# **ethernet evc *evc-id***

8. To define a CFM maintenance domain at a particular maintenance level and enter ethernet CFM configuration mode:

   Device(config)# **ethernet cfm domain *domain-name* level *level-id***

9. To include the sender ID TLVs and the attributes containing type, length, and values for neighbor devices:

   Device(config)# **sender-id chassis**

10. To configure a maintenance association within a maintenance domain and enter ethernet CFM service configuration mode:

    Device(config-ecfm)# **service *short-ma-name* evc *evc-name* vlan *vlanid* direction down**

11. To configure offload sampling:

    Device(config)# **offload sampling *sample***

12. To enable the transmission of CCMs:

    Device(config-ecfm-srv)# **continuity-check**

13. To configure the time period between CCMs transmission (the default interval is 10 seconds):

    Device(config-ecfm-srv)# **continuity-check [interval *cc-interval*]**

14. To configure the MEP domain and ID on the interface:

    Device(config)# **interface *interface-name***

    Device(config-if)# **cfm mep domain *domain-name* mpid *id* service *service-name***

For a detailed explanation on the purpose of each command, see Configuring Ethernet CFM.

Example Configurations

The following configuration example shows you how to configure CFM per subinterface for EVC+VLAN maintenance association:

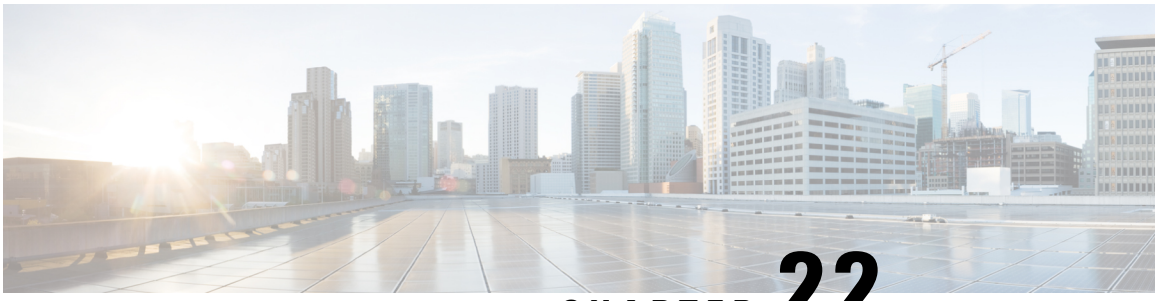
```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet evc USER-SERVICE
 !
 ethernet cfm domain USER level 7
  service USER-SERVICE evc USER-SERVICE vlan 112 direction down
   continuity-check
   continuity-check interval 10s
   continuity-check loss-threshold 3
 !
 ethernet cfm logging
 !
 interface GigabitEthernet0/0/1
  no ip address
  speed 100
  no negotiation auto
  ethernet cfm mep domain USER mpid 1562 service USER-SERVICE
   cos 2
 !
 interface GigabitEthernet0/0/1.112
  description NAME 2286884663
   encapsulation dot1Q 112
   ip address 192.0.2.1 255.255.255.0
```

The following configuration example shows you how to configure CFM per physical interface for port maintenance association:

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet cfm traceroute cache
 ethernet cfm domain USER level 1
  sender-id chassis
  service USER-SERVICE port
   continuity-check
   continuity-check interval 1m
   sender-id chassis
 !
 ethernet cfm logging
 !
 interface Ethernet0/1/0
  no ip address
  load-interval 30
  speed [10/100/1000]
  duplex [half/full]
  ethernet oam mode passive
  ethernet oam remote-loopback supported
  ethernet oam
  ethernet cfm mep domain USER mpid 101 service USER-SERVICE
   alarm notification all
 !
 interface Ethernet0/1/0.101
  encapsulation dot1Q 101
  pppoe enable group global
  pppoe-client dial-pool-number 1
  no cdp enable
  ethernet loopback permit external
```

You can use this configuration in the CLI template on Cisco SD-WAN Manager as well as the CLI Add-On template.

For information on CLI Add-On Templates on Cisco SD-WAN Manager, see Create a CLI Add-On Feature Template



CHAPTER 22

Troubleshooting

Table 61: Feature History

Feature Name	Release Information	Description
Improved Access to Troubleshooting Tools in Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	The troubleshooting tools are now easily accessible from the various monitoring pages of Cisco SD-WAN Manager, such as **Site Topology**, **Devices**, **Tunnels**, and **Applications**, thereby providing you with context-based troubleshooting guidance. Earlier, the troubleshooting tools were accessible only from the device dashboard.
Connect to and troubleshoot Cisco Catalyst SD-WAN solution using Cisco RADKit	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Use tools and Python modules from Cisco Remote Automation Development Kit (RADKit) to securely connect to remote terminals, WebUIs, or desktops. Using RADKit, a TAC engineer can request the required information during the troubleshooting process, from the various devices and services, in a secure and controlled way.
Cisco RADKit in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	The Cisco Remote Automation Development Kit (RADKit), a tool for remote automation and troubleshooting, is integrated directly into Cisco SD-WAN Manager. This integration provides the capability to enable or disable the RADKit service using the API in Cisco SD-WAN Manager.

- Troubleshoot Common Cellular Interface Issues, on page 318
- Troubleshoot WiFi Connections, on page 321
- Troubleshoot a Device, on page 325
- BFD Tunnel Troubleshooting, on page 332
- On-Demand Troubleshooting, on page 334
- Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit, on page 339

Troubleshoot Common Cellular Interface Issues

Resolve Problems with Cellular Interfaces

This topic describes the most common issues and error messages that occur with cellular connections from the router to the cellular network, and the steps to resolve them.

Insufficient Radio Signal Strength

Problem Statement

The cellular module in the router cannot detect a radio signal from the service provider network.

Identify the Problem

- The signal strength displayed in the Cisco SD-WAN Manager Cellular Status screen or with the **show cellular status** CLI command, or in the Cellular Radio screen or with the **show cellular radio** command is no signal, poor, or good. It should be excellent. The following table lists the ranges of signal strengths:

Table 62:

Signal	Excellent	Good	Fair	Poor
Received signal strength indicator (RSSI)	>= -65 dBm	-65 to -75 dBm	-75 to -85 dBm	<= -85 dBm
Reference signal receive power (RSRP)	>= -80 dBm	–80 to -90 dBm	–90 to -100 dBm	<= -100 dBm
Reference signal receive quality (RSRQ)	>= -10 dBm	-10 to -15 dB	-15 to -20 dB	< –20 dB
Signal-to-noise ratio (SNR)	>= 20 dB	13 to 20 dB	0 to 13 dB	<= 0 dB

Note All parameters must be considered together and not in isolation. For example, a strong RSSI does not mean signal quality is good if RSRP is bad.

- The wireless LED on the router is lit (solid or blinking) and is red, orange or yellow, or it is blinking green. It should be solid green.

Resolve the Problem

1. Examine the router to verify that both basic antennas are correctly installed.
2. Contact the service provider to verify that the location has coverage.
3. Move the router to a new location within the building.
4. Procure an additional external cabled antenna and connect it to the router.

Modem Status Remains in Low-Power Mode

Problem Statement

End users cannot connect to the cellular network, and the modem status remains in low-power mode.

Identify the Problem

- End users cannot connect to the cellular network.
- The error message "Missing or unknown APN" is generated.
- The signal strength is less than excellent.

Resolve the Problem

1. Verify that there is sufficient radio signal strength. If there is not, follow the instructions in the Insufficient Radio Signal Strength section.
2. Verify that the cellular0 interface is operational. When the cellular interface is shut down, the modem status is set to Low Power mode. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   Then click **Real Time**, and from the **Device Options** drop-down list, choose **Interface Detail**.

   To do this from the CLI, use the **show interface** command. Check that the Admin Status and Oper Status values are both Up.
3. Verify that the modem temperature is not above or below the threshold temperatures. To view the modem temperature, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select the router.

   Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Modem**.

   From the CLI, use the **show cellular modem** command.
4. Check that the access point name (APN) in the profile for the cellular0 interface matches the name expected by your service provider. Some service provides required that you configure the APN, and they include configuration instructions in the SIM card package.
   a. To check which APN name is configured, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select the router.

      Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

      Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Profiles**.

      From the CLI, use the ; **show cellular profiles** command. The APN column shows the name of the APN. Each profile specifies an access point name (APN), which is used by the service provider to determine the correct IP address and connect to the correct secure gateway. For some profiles, you must configure the APN.

   b. If the APN is not the one required by the service provider, configure the correct APN. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** and use the **Cellular Profile** feature template.

To configure this from the CLI, use the **cellular cellular0 profile apn** command.

5. If none of the previous steps works, reset the cellular interface.

Error Messages

The following table list the most common error messages that are displayed regarding cellular interfaces:

Table 63:

Error Message	Problem Statement	How Do I Fix the Problem
Authentication failed	End user authentication failed, because the service provider cannot authenticate either the user's SIM card or the Cisco vEdge device SIM card.	Contact the cellular service provider.
Illegal ME	The service provider denied access to an end user, because the end user is blocked from the network.	Contact the cellular service provider.
Illegal MS	The service provider denied access to an end user, because the end user failed the authentication check.	Contact the cellular service provider.
Insufficient resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
IPV4 data call throttled	The SIM card being used in the Cisco vEdge device requires that you configure static APN.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Missing or unknown APN	End users cannot connect to the cellular network, either because an APN is required and is not included in the cellular profile or because the APN could not be resolved by the service provider.	See the profile's APN, as described in Modem Status Remains in Low-Power Mode , above.
MS has no subscription for this service	The service provided denied access to an end user, because the end user has no subscription.	Contact the cellular service provider.
Network failure	The service provider network is experiencing difficulties.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.

Error Message	Problem Statement	How Do I Fix the Problem
Network is temporarily out of resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
Operator has barred the UE	The service provided denied access to an end user, because the operator has barred the end user.	Contact the cellular service provider.
Requested service option not subscribed	The SIM card being used in the Cisco vEdge device requires that you configure a static APN entry.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Service not supported by the PLMN	The Public Land Mobile Network (PLMN) does not support data service.	Contact the cellular service provider.

Troubleshoot WiFi Connections

This topic describes how to check and resolve connection problems between a WiFi client and a WiFi network that is provided by a WiFi router. The procedures described here are applicable to devices that support WiFi only.

Check for WiFi Connection Problems

If a WiFi client is unable to connect to a WiFi network when a router is providing the WiFi network, follow these steps to determine the source of the problem. To perform each step, use a method appropriate for the WiFi client.

1. Verify that the WiFi client can locate the service identifier (SSID) advertised by the router. If the client cannot find the SSID, see the section, SSID Not Located.
2. Verify that the WiFi client can connect to the SSID advertised by the router. If the client cannot connect to the SSID, see the section, SSID Connection Fails.
3. Verify that the WiFi client has been assigned an IP address. If the client cannot obtain an IP address, see the section, Missing IP Address.
4. Verify that the WiFi client can access the Internet. If the client cannot connect to the Internet, see section, Internet Connection Failure.
5. If the WiFi client connection is slow or if you notice frequent disconnects, see section, WiFi Speed Is Slow.

Resolve Problems with WiFi Connections

This section describes the most common issues that occur with WiFi connections between a WiFi client and a router, and it describes steps to resolve the issues.

SSID Not Located

Problem Statement

The WiFi client cannot locate the SSID advertised by the router.

Resolve the Problem

1. Ensure that the basic service set identifier (BSSID) address for the SSID is valid:
   a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   b. Choose a device from the device list that appears.

   c. From the left pane, choose WiFi. The right pane displays information about WiFi configuration on the router.

   d. In the right pane, locate the SSID. Check that the BSSID for this SSID does not have a value of 00:00:00:00:00:00.

   e. If the BSSID is 00:00:00:00:00:00, the WLAN (VAP) interface for this SSID may be misconfigured. Ensure that the WLAN interface has been added to a bridge during the configuration process. To view the running configuration of the device, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. For the desired device, click **...**and choose **Running Configuration**.

      To view the running configuration of the device from the CLI, run the **show running-config** command. To add the WLAN interface to a bridge — from the Cisco SD-WAN Manager, choose **Configuration** > **Templates**.

      Click **Feature Templates**, and choose the **Bridge** feature template.



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

2. Eliminate static channels. A static channel is one where you explicitly configure the radio channel rather than allowing the router to automatically select the best radio channel. A slow static channel may appear to be an unreachable SSID.
   a. View the current SSID channel setting for the router. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the list of devices that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose WLAN Clients or WLAN Radios.

      From the CLI, run the **show wlan clients** or **show wlan radios** command.

   b. If the channel is set to a specific number, change the value to "auto". To do this, use the WiFi Radio feature template in Cisco SD-WAN Manager.

      From the CLI, run the **wlan channel auto** command.

3. Ensure that the WiFi client is using the same radio band as the router, either 2.4 GHz (for IEEE 802.11b/g/n) or 5 GHz (for IEEE802.11a/n/ac):
   a. Check which radio band the WiFi client supports.
   b. Check the router's Select Radio setting. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Radios**.

      From the CLI, run the **show wlan radios** command.
   c. If the router and WiFi client radio band settings do not match, either change the WiFi client's radio band or change the settings on the router so that they match. To do this, use the Wifi Radio feature template.

      From the CLI, run the **wlan** command.

SSID Connection Fails

Problem Statement

The WiFi client can locate the SSID advertised by the router but cannot connect to it.

Resolve the Problem

1. If you configure passwords locally on the router, ensure that the WiFi client's password matches the SSID's password.
2. If you are using a RADIUS server, ensure that the RADIUS server is reachable and that the WiFi client's username and password match the RADIUS configuration:
   a. To verify that the RADIUS server is reachable from the router, ping the server. To do this in Cisco SD-WAN Manager, ping a device. From the CLI, run the **ping** command.
   b. Check for matching passwords on the RADIUS server and WiFi client.
3. Ensure that you do not exceed the maximum number of clients for this SSID:
   a. Verify the number of used clients and the maximum number of clients:
      - From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. From the left pane, select WiFi. In the right pane, locate the SSID. Check the No. of Clients field. If the used/maximum values are equal, no more clients can connect to this SSID.
      - From the CLI, run the **show wlan interfaces detail** command.
   b. If needed, increase the maximum clients setting for your SSID. To do this use the WiFi SSID feature template in Cisco SD-WAN Manager.

      From the CLI, run the **max-clients** command.
4. Ensure that the WiFi client supports WPA2 management security:
   a. Check your Management Security setting. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Interfaces**.

From the CLI, run the **show wlan interfaces** command. If the management security value is set to "required," the WiFi client must support WPA2 security.

b. If necessary, change the Management Security setting for your SSID to "optional" or "none." To do this in Cisco SD-WAN Manager, use the WiFi SSID feature template.

From the CLI, run the **mgmt-security** command.

Missing IP Address

Problem Statement

The WiFi client can connect to the SSID, but cannot obtain an IP address.

Resolve the Problem

Ensure that a DHCP server is reachable and has an available IP address in its address pool:

1. If the router is acting as a DHCP helper (DHCP relay agent), ping the DHCP server to ensure that it is reachable from the router.. From the CLI, run the **ping** command.
2. If you are using a remote DHCP server, check that the remote DHCP server has an available IP address in its address pool.
3. If the router is acting as the local DHCP server:
   a. View the number of addresses being used. From the Cisco SD-WAN Manager menu, **Monitor** > **Devices** and choose a device from the device list that appears. Next, click **Real Time**, and from the **Device Options** drop-down list, choose **DHCP Servers**.

   From the CLI, run the **show dhcp server** command.

   b. Compute the number of IP addresses in the pool based on the configured DHCP address pool size and the number of addresses excluded from the DHCP address pool. To view these values in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. For the desired router, click **...** and choose **Running Configuration**.

   To view them from the CLI, run the **show running-config** command.

   c. If necessary, increase the range of addresses in the router's DHCP address pool using the DHCP-Server feature template in Cisco SD-WAN Manager.

Internet Connection Failure

Problem Statement

The WiFi client is connected to the SSID and has an IP address, but it cannot connect to the Internet.

Resolve the Problem

Ensure that the WiFi client has received the correct default gateway and DNS settings from the DHCP server:

1. If the DHCP server is remote, check the settings on the server.
2. If the router is the DHCP server, ensure that the default gateway and DNS server settings are the same as those on the WiFi client. To view the settings in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device from the device list that is displayed. Click **Real Time,** and in the **Device Options** drop-down list, choose **DHCP Interfaces**.

From the CLI, run the **show dhcp interface** command.

WiFi Speed Is Slow

Problem Statement

The WiFi client can connect to the Internet, but the connection speed is slow.

Resolve the Problem

Allow the router to choose the best WiFi channel:

1. View the current SSID channel setting for the router. To do this in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device from the device list that is displayed. Click **Real Time,** and in the **Device Options** drop-down list, choose **WLAN Clients**.

   From the CLI, run the **show wlan clients** or **show wlan radios** command.

2. If the channel is set to a specific number, change the value to "auto". To do this in Cisco SD-WAN Manager, use the WiFi Radio feature template.

   From the CLI, run the **wlan channel auto** command.

Troubleshoot a Device

You can troubleshoot the connectivity or traffic health for all the devices in an overlay network.

Check Device Bringup

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Device Bringup**.

The **Device Bringup** window opens.

Ping a Device

Table 64: Feature History

Feature Name	Release Information	Description
IPv6 Support in Cisco SD-WAN Manager UI Troubleshooting	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Added support for using an IPv6 address when pinging a device. Also added support for using an IPv6 address when running a traceroute, configuring packet capture, and simulating flows.

Before You Begin

Ensure that **Device Monitoring** and **Events** features have read and write permissions and **Tools** has read permission. For more information on different permission settings, see Manage Users.

With the set permissions to the usergroup, ensure that you are able to access the required features.

To verify that a device is reachable on the network, ping the device to send ICMP ECHO_REQUEST packets to it:

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Ping**.
5. In the **Destination IP** field, enter the IP address of the device to ping.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
6. In the **VPN** field, choose the VPN to use to reach the device.
7. In the **Source/Interface** field, choose the interface to use to send the ping packets.
8. In the **Probes** field, choose the protocol type to use to send the ping packets.
9. In the **Source Port** field, enter the number of the source port.
10. In the **Destination Port** field, enter the number of the destination port.
11. Click **Advanced Options** to specify additional parameters:
    a. In the **Count** field, enter the number of ping requests to send. The range is 1 to 30. The default is 5.
    b. In the **Payload Size** field, enter the size of the packet to send. The default is 64 bytes, which comprises 56 bytes of data and 8 bytes of ICMP header. The range for data is 56 to 65507 bytes.
    c. Enter the **MTU**.

Note The **MTU** option does not apply beginning with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

d. Click the **Rapid** slider to send five ping requests in rapid succession and to display statistics only for the packets transmitted and received, and the percentage of packets lost.

e. In the **Type of Service** field, enter the value to be included in the ping packets.

f. In the **Time to Live** field, enter the round-trip time, in milliseconds, for sending this ping packet and receiving a response.

g. Click the **Don't Fragment** option to set the **Don't Fragment** bit in the ping packets.

12. Click **Ping**.

From Cisco vManage Release 20.10.1, the **Ping** option can be accessed using one of these methods:

- Choose **Monitor** > **Devices**, click **…** adjacent to the device name, and choose **Ping**.
- In the **Site Topology** page, click a device name or tunnel name, and then click **Ping** in the right navigation pane.

Speed Test

Table 65: Feature History

Feature Name	Release Information	Description
Speed Test	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This feature enables you to carry out speed testing between two edge devices or between a local edge device to a remote iperf3 server.
Speed Test Enhancement	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature allows you to specify your own or preferred iperf3 server for Internet speed test.

Information About Speed Test

Iperf3 is a network bandwidth test tool used for detecting bandwidth-related network problems.

There are two types of speed test:

- Site-to-site speed test: Cisco SD-WAN Manager tests the network speed and available bandwidth between two devices. Cisco SD-WAN Manager designates one device as the source and the other as the destination.
- Internet speed test: Cisco SD-WAN Manager tests the network speed and available bandwidth between a device and an iperf3 server reachable by the network. Starting from Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, users can specify the IP address (or domain

name) and port of an iperf3 server to perform Internet speed tests. Cisco SD-WAN Manager designates the device as the client and the iperf3 server as the server.

The speed tests measure upload speed from the source device to the destination device, and measure download speed from the destination device to the source device.

The speed test traffic between edges ignore per-tunnel QoS on hub side and causes impact on the spoke side when WAN interface is congested.

Restrictions for speed test

Unbound loopback interfaces are not supported for speed test.

The speed test sends and receives traffic through the control plane, so the test result depends on the router's punt/inject (control plane to data plane communication) efficiency and control plane CPU usage.

Prerequisites for Speed Test

Speed testing requires the system ID and the device host name of the destination device.

Run Speed Test

Perform the following steps to run a speed test.

Run Site-to-Site Speed Test

Before You Begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.
   - **Destination Device**: From the drop-down list, choose the remote device by its device name and system IP address.
   - **Destination Circuit**: From the drop-down list, choose the color of the tunnel interface on the remote device.
6. Click **Start Test**.

The right pane shows the results of the speed test, the download, and upload speed between the source and destination. The download speed shows the speed from the destination to the source, and the upload speed shows the speed from the source to the destination in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table in the lower part of the right pane.

From Cisco vManage Release 20.10.1, the **Speed Test** option is also accessible as follows:

- On the **Monitor** > **Devices** page, click **…** adjacent to the device name and choose **Speed Test**.
- On the **Monitor** > **Applications** page, click **…** adjacent to the application name and choose **Speed Test**.
- On the **Site Topology** page, click a device name, and then click **Speed Test** in the right navigation pane.

Run Internet Speed Test

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.
   - **Destination Device**: From the drop-down list, choose **Internet**.
   - Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a
     - **iPerf3 Server**: (Optional) Enter the hostname or iPer3 server's IP address in IPv4 format.
     - **Server Port Range**: (Optional) Enter the server port or a port range. For example, 5201, 5210, or 5201-5205.
     - Built-in public iperf3 servers list and their port ranges:
       - ping.online.net (5203-5208)
       - iperf.par2.as49434.net (9231-9236)
       - paris.testdebit.info (9201-9240)
       - speedtest.serverius.net(5002)
       - speedtest.uztelecom.uz (5205-5209)
       - iperf.biznetnetworks.com (5201-5203)



Note If you do no provide an iPerf3 server then the built-in iPerf3 servers will be automatically used. The Server Port Range option is only applicable when a user-specified iPerf3 server is entered. If no port range is provided, the system defaults to port 5201. When using the built-in servers, the speed test selects the server with the shortest ICMP ping RTT (Round-Trip Time).

6. Click **Start Test**.

   The speed test begins to measure the download and upload speeds between the two endpoints.

Troubleshooting Speed Test Issues

The speed test uses iperf3 with the TCP protocol. The speed test result depends on the latency and packet loss between the client and server.

The built-in speed test servers are not based on geographic proximity, so end users are highly recommended to input and use an iPerf3 server located near them.

The following table provides troubleshooting information for speed testing:

Table 66: Troubleshooting Scenarios

Error Information	Possible Root Cause
Failed to resolve iperf server address	DNS server is not configured at edge device or is unable to resolve the iperf server from the configured DNS server at edge device.
Speed test servers not reachable	The speed test server ping failed. The edge device cannot reach the server IP.
iPerf client: unable to connect stream: Resource temporarily unavailable	Unable to connect to the speed test server. Access may be blocked by access-control list (ACL) permissions.
iPerf client: unable to connect to server	The iPerf3 server is not providing the test service at the user-specified port or default port 5201.
Device Error: Speed test in progress	The selected source or destination device is performing a speed test and cannot start a new one.
Device error: Failed to read server configuration	The data stream configuration is missing. Workaround: Running a CLI command at the edge device and clearing the Cisco Catalyst SD-WAN control connections can fix the issue.
Speed test session has timed out	The speed test has not successfully completed in 180 seconds. This might be because the edge device has lost the control connection to Cisco SD-WAN Manager during the speed testing.

Run a Traceroute

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Trace Route**.

5. In the **Destination IP** field, enter the IP address of the corresponding device in the network.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

6. From the **VPN** drop-down list, choose a VPN to use to reach the device.
7. From the **Source/Interface for VPN** drop-down list, choose the interface to use to send the traceroute probe packets.
8. Click **Advanced Options**.
9. In the **Size** field, enter the size of the traceroute probe packets, in bytes.
10. Click **Start** to trigger a traceroute to the requested destination.

The lower part of the right pane displays the following information:

- Raw output of the path the traceroute probe packets take to reach the destination.
- Graphical depiction of the path the traceroute probe packets take to reach the destination.

If the traceroute is for the service-side traffic, a Cisco vEdge device generates traceroute responses from any of the interfaces on the service VPN.

From Cisco vManage Release 20.10.1, the **Trace Route** option can be accessed using one of these methods:

- Choose **Monitor** > **Devices**, click **…** adjacent to the device name, and choose **Trace Route**.
- In the **Site Topology** page, click a device or tunnel name, and then click **Trace Route** in the right navigation pane.

Discover Underlay Paths

Minimum release: Cisco vManage Release 20.10.1

Diagnostic Monitoring Log Capture

Table 67: Feature History

Feature Name	Release Information	Description
Diagnostic Monitoring Log Capture	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature enables you to collect and record diagnostic data, such as logs and traces, to help diagnose and troubleshoot issues in Cisco SD-WAN Manager, Cellular Gateways and Cisco IOS XE Catalyst SD-WAN devices.

Configure Diagnostic Monitoring Log Capture

Before you begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

Procedure

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

Step 2 To choose a device, click the device name in the **Hostname** column.

Step 3 Click **Troubleshooting** in the left pane.

Step 4 In the **Logs** area, click **Diagnostic Monitoring Log Capture**.

The **Diagnostic Monitoring Log Capture** page opens.

Step 5 From the **Interface for VPN** drop-down list, choose a cellular interface.

Step 6 Expand the **Advance Settings** drop-down list.

Step 7 In the **Modem radio reset**, turn modem radio off and back on for log collection and check the **Enable rotation** field to enable continuous log collection.

Logs consist of multiple files. By default, when file size limit is reached for any given file, log collection continue into the next file until log size limit is reached. If rotation is enabled, log collection continues after log size limit is reached by overwriting the oldest file. Log collection stops when you stop the log collection or when the auto stop timer is reached.

Step 8 In the **Timer**, enable **auto stop timer** to automatically stop log collection after specified time is reached or optionally you can set a **Stop time**.

The range for stop time is 1 to120 minutes.

Step 9 In the **Filter upload**, upload the filter file.

The supported filter file formats are `.sqf`, `.cfg`, and `.bin`.

Step 10 Click **Start** to start the log capture.

You can check the log capture status and download the file after the file is ready.

BFD Tunnel Troubleshooting

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the **Tunnel Troubleshooting** pane is available on the **Monitor** > **Devices** > **Tunnel** page in Cisco SD-WAN Manager:

You can initiate BFD troubleshooting through the Cisco SD-WAN Manager. It provides a user-friendly workflow for identifying and resolving issues. The integration of detailed forensic data and automated debugging steps helps streamline the troubleshooting process, making it more accessible and efficient for

network administrators. A functioning BFD session involves various elements like, TLOC, BFD-session, SDWAN-session, IPsec-session, and NAT under the hood functioning and programmed correctly across the layers. When you enable BFD logging for all the existing BFD sessions, the relevant logs for a BFD helps in troubleshooting.

Cisco SD-WAN Manager provides a method to logically group the BFD down sessions so that you can make logical analysis and launch BFD troubleshoot.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that is displayed.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Tunnel Troubleshooting**. The **Tunnel Troubleshooting** window opens.
5. Choose the device from the **Select Device** drop-down box. Or you can search for a device from the **Search** field.
6. Choose the local circuit from the **Select local circuit** drop-down box.
7. Choose the remote device from the **Select remote device** drop-down box
8. Choose the remote circuit from the **Select remote circuit** drop-down box.
9. Choose the encapsulation details from the **Encapsulation** drop-down box.
10. Click **Go**

    You can check the **Progress** and **Conclusions** pane for details on BFD sessions.

Progress Examples

- Collecting troubleshoot data from a local device.
- Checking BFD session, Tunnel, SDWAN session, resource allocation and anomalies from device.
- Collecting troubleshoot data from a remote device.
- Processing troubleshoot data collected from local and remote device.
- Verifying BFD session setup, state machine, echo packets, tunnel setup, sdwan session setup, underlay setup, symnat for BFD session

Conclusion Examples

- Machine reasoning has completed
- Local Device : Local TLOC is created
- Local Device : Remote TLOC is created
- Local Device : IPSec session is created
- Local Device : BFD session is created
- Local Device : SDWAN session is created
- Local Device : BFD discriminator is allocated

- Local Device : IPSec flow ID is allocated
- Local Device : Adjacency is resolved
- Local Device : BFD state is Up
- Remote Device : Local TLOC is created
- Collecting troubleshoot data from a local device.

On-Demand Troubleshooting

Table 68: Feature History

Feature Name	Release Information	Description
On-Demand Troubleshooting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature lets you view detailed information about the flow of traffic from a device. You can use this information to assist with troubleshooting.
Enhancement to On-Demand Troubleshooting	Cisco vManage Release 20.11.1	You can view the detailed troubleshooting progress of the flow of traffic from a device.

Information About On-Demand Troubleshooting

On-demand troubleshooting lets you view detailed information about the flow of traffic from a device.

By default, Cisco SD-WAN Manager captures aggregated information about flows. You can obtain detailed information for specific devices and for specific historical time periods by adding an on-demand troubleshooting entry. When you add an entry, Cisco SD-WAN Manager compiles detailed information according to parameters that you configure.

To conserve system resources, Cisco SD-WAN Manager compiles detailed information only when you request it by adding an entry. In addition, Cisco SD-WAN Manager stores the information for a limited time (3 hours by default), then removes it. You can request the same information again, if needed.



Note On a Cisco SD-WAN Manager cluster setup, only a connected node can remove an on-demand troubleshooting task or mark it as complete.

Restrictions for On-Demand Troubleshooting

Ensure that no Cisco or third-party APIs that instruct on-demand troubleshooting to stop are called when you are using on-demand troubleshooting. These APIs prevent on-demand troubleshooting from compiling information.

Page Elements

The **On Demand Troubleshooting** window provides options for configuring and adding an on-demand troubleshooting entry. The **On Demand Troubleshooting** window displays information about existing on-demand troubleshooting entries and provides the following information and options.

Item (Field)	Description
ID	System-assigned identifier of the entry.
Device ID	System IP of the device to which the entry applies.
Data Type	Type of data for which the entry provides detailed information.
Creation Time	Date and time that you added the entry.
Expiration Time	Date and time that the entry expires. At this expiration time, the entry is removed from the table automatically, and the corresponding detailed information is no longer available. By default, an entry is removed 3 hours after its creation time.
Data Backfill Start Time	Start date and time of the data backfill period.
Data Backfill End Time	End date and time of the data backfill period.
Status	Status of the entry: • **IN_PROGRESS**: Detailed troubleshooting information is in the process of being compiled. • **QUEUED**: Detailed troubleshooting information is queued for compilation. • **COMPLETED**: Detailed troubleshooting information has been compiled.

Configure On-Demand Troubleshooting

You can configure on-demand troubleshooting for a device from the **Tools** > **On Demand Troubleshooting** window in Cisco SD-WAN Manager. This window provides options for adding an on-demand troubleshooting entry, and for managing existing entries.

Cisco vManage Release 20.6.1 and earlier: You can configure on-demand troubleshooting for a device from the **Monitor** > **On Demand Troubleshooting** window in Cisco SD-WAN Manager.

You can also start on-demand troubleshooting from various locations in the **Monitor** > **Devices** window for a device. See View On-Demand Troubleshooting Information for a Device, on page 337.

Cisco vManage Release 20.6.1 and earlier: You can start on-demand troubleshooting from various locations in the **Monitor** > **Network** window for a device.

On-demand troubleshooting is qualified for troubleshooting entries for up to 10 devices concurrently.

Add an On-Demand Troubleshooting Entry

Adding an entry in the **On Demand Troubleshooting** window instructs Cisco SD-WAN Manager to compile detailed troubleshooting information for the device that you specify, using the parameters that you configure.

To add an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. From the **Select Device** drop-down list, choose the Cisco IOS XE Catalyst SD-WAN device or the Cisco vEdge device for which you want to enable on-demand troubleshooting.

3. From the **Select Data Type** drop-down list, choose **SAIE** or **ConnectionEvents**.

4. Choose an option for the data backfill period:

   - **Last 1 hour**: Provides detailed stream information for the period beginning 1 hour before you add the troubleshooting entry and ending at the time that you add the entry.
   - **Last 3 hours**: Provides detailed stream information for the period beginning 3 hours before you add the troubleshooting entry and ending at the time that you add the entry.
   - **Custom Date and Time Range**: Use the **Start date and time** and the **End date and time** fields to designate the backfill period that you want. Note that the **End date and time** value cannot be later than the current date and time.

5. Click **Add**.

   The troubleshooting entry appears in the table of entries. When the value in the **Status** field for the entry shows the value **Completed**, you can view the troubleshooting information from the **Monitor** > **Devices** window, as described in View On-Demand Troubleshooting Information for a Device, on page 337.

Update an On-Demand Troubleshooting Entry

Update an on-demand troubleshooting entry to make changes to its configuration settings. For example, update an entry to adjust its backfill period.

Only entries that are in the QUEUED state can be updated.

To update an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. In the table of entries, click **…** adjacent to the entry that you want to update and choose **Update**.

3. In the **Update Troubleshoot Status** dialog box that is displayed, configure the settings as needed, and click **Add**.

Delete an On-Demand Troubleshooting Entry

Deleting an on-demand troubleshooting entry removes the entry from Cisco SD-WAN Manager. After you delete an entry, you can no longer view its detailed information.

Deleting an entry can help free resources in Cisco SD-WAN Manager.

To delete an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. In the table of entries, click **…** adjacent to the entry that you want to delete and choose **Delete on demand queue**.

3. In the **Delete On Demand Status** window that is displayed, click **OK**.

View On-Demand Troubleshooting Information for a Device

You can view on-demand troubleshooting information for a device from the **Network** window for that device.

Before you can view this information, at least one on-demand troubleshooting entry must exist for the device. Add an entry from the **On Demand Troubleshooting** window as described in Add an On Demand Troubleshooting Entry, or add an entry from the **Network** window as described in the following procedure.

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

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. In the **Hostname** column, click the device for which you want to view the information.

3. Perform either of these actions:

   - To view the troubleshooting information for an SAIE application:

     a. Click **SAIE Applications**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Applications** is called **DPI Applications**.

     b. In the **Applications Family** table, click an application family.

     c. In the **Applications** table, click an application.

   - To view troubleshooting information for a specific metric, in the left pane, under **ON-DEMAND TROUBLESHOOTING** click an option. Not all options apply to all device types.

     - **FEC Recovery Rate**
     - **SSL Proxy**
     - **AppQoe TCP Optimization**
     - **AppQoE DRE Optimization**
     - **Connection Events**

       From Cisco Catalyst SD-WAN Manager Release 20.16.1, if you enable unified logging for your device, you can view the firewall security connection events for inspect, pass, and drop actions. The connection event information also includes the reason for traffic drop by the firewall policy.

- **WAN Throughput**
- **Flows**
- **Top Talkers**

The **Flows** and **Top Talkers** metrics are only for TCP Optimized flows.

If on-demand troubleshooting is configured for the device, detailed troubleshooting information appears. This information includes traffic statistics and metrics such as source IP address, destination IP address, number of packets, number of bytes, and more. Use the options that are available and hover your cursor over elements on the graphs to view the information that you need.



Note Starting from Cisco IOS XE Release 17.9.1a, use the **policy ip visibility features enable** command to manually enable or disable the feature fields in Flexible Netflow (FNF). Use the **show sdwan policy cflowd-upgrade-status** command to check which features were enabled before the version upgrade. You have to manually control the features after a version upgrade using the disable or enable commands.

For more information, see policy ip visibility command page.

If on-demand troubleshooting information is not configured, the **Enable On Demand Troubleshooting** option is displayed. Continue to Step 4.

4. If the **Enable On Demand Troubleshooting** option is displayed, perform these actions to start this feature for the selected device:
   a. Click **Enable On Demand Troubleshooting**.
   b. Choose one of the following options:
      - **Quick Enable**: Starts an on-demand troubleshooting entry with a backfill period of 3 hours. With this option, detailed stream information for the past 3 hours becomes available.

        After you choose this option, click **Refresh** to view the detailed troubleshooting information. It can take a few minutes for this information to become available. Alternatively, click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window that includes the entry that you just added.
      - **Go to On Demand Troubleshooting**: Displays the **On Demand Troubleshooting** window. Add an entry in this window as described in Add an On Demand Troubleshooting Entry. Repeat Steps 1 to Step 3 in this procedure to view the detailed information.

View Progress of On-Demand Troubleshooting

Minimum supported release: Cisco vManage Release 20.11.1

After you enable on-demand troubleshooting, the **On-demand Troubleshooting in Progress** message appears on the **Monitor** > **Devices** page. The message remains until the troubleshooting is complete.

Click a chart option to view the troubleshooting progress in a graphical format. Select a time period to display data or click **Custom** to display a selection of a custom time period.

You can use the **request nms olap-db** command to start, stop, or restart the Cisco SD-WAN Manager online analytical processing (OLAP) database or view the status of the database.

For more information about this command, see request nms olap-db.

View Detailed Top Source Data

After on-demand troubleshooting is configured, you can view detailed information about top application usage for a device. To do so, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** > **Top Applications**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** > **Top Applications**.

2. In the **SAIE Application** tab, click an application usage bar in the chart.

Note In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Application** is called **DPI Application**.

3. In the chart for the application that you selected, click the device usage bar.

   If on-demand troubleshooting is configured for the device, detailed top source data appears.

   If on-demand troubleshooting information is not configured, the **Go to On Demand Troubleshooting** option appears. Continue to Step 4.

4. If the **Go to On Demand Troubleshooting** option appears, perform these actions:

   a. Click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window.

   b. In the **On Demand Troubleshooting** window, add an entry, as described in Add an On Demand Troubleshooting Entry.

   c. Repeat Step 1 to Step 3 in this procedure to view the detailed information.

Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1

Use Cisco RADKit to troubleshoot devices in Cisco Catalyst SD-WAN. RADKit, a Software Development Kit (SDK), is a set of ready-to-use tools and Python modules, which helps you

- securely connect to remote terminals, WebUI's or desktops,
- leverage APIs for remote or local automations, and
- share support data privately with Cisco Services without any impact on data privacy.

Before You Begin

- Ensure that you have an internet connection and have configured DNS in the transport VPN (VPN0).

- Ensure that you are running compatible operating systems. For information about supported operating systems, see Compatibility.

Installation

The RADKit installation includes a client and a service that connects to the Cisco RADKit cloud to interactively connect you to remote terminals, WebUIs, or desktops.

To install the RADKit service, go to Cisco's Support Services Technical Assistance Center (TAC) and open a support case. After you have installed the RADKit service, you can enroll to the RADKit client. For more information, see Initial Client Setup.

For more information and downloads, see RADKit.

Cisco RADKit in Cisco SD-WAN Manager

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco RADKit, version 1.8.6rc1, is directly installed in Cisco SD-WAN Manager which provides the environment and resources for RADKit to operate, including the file system, shell access, and network connectivity.

Cisco RADKit is a tool used for remote automation and troubleshooting. With it now directly installed in Cisco SD-WAN Manager, it helps you to

- eliminate the need for a separate virtual machine, simplifying deployment, and saving resources
- ensure the service remains active and functions correctly even during Cisco SD-WAN Manager reboots or upgrades, and
- quicken operations with direct access to devices , improving performance by eliminating the need for an intermediate jumphost.

Enablement and disablement of Cisco RADKit Service using API

You can enable or disable the Cisco RADKit service in Cisco SD-WAN Manager using the Cisco SD-WAN Manager API. When enabled, the service initializes, performing its setup and startup process. During enablement, the service automatically registers itself with the Cisco Catalyst SD-WAN Portal for the Cisco RADKit service to function correctly.

Cisco RADKit Restrictions

Cisco RADKit and Cisco SD-WAN Manager cluster deployment

Cisco RADKit does not support clustering. However, it can operate where Cisco SD-WAN Manager is deployed as a cluster.

Enable Cisco RADKit service in Cisco SD-WAN Manager

Enabling Cisco RADKit service in Cisco SD-WAN Manager allows you to activate its capabilities for remote automation, operation, and troubleshooting of network equipment directly from Cisco SD-WAN Manager.

This section provides the steps to enable Cisco RADKit service in Cisco SD-WAN Manager.

Before you begin

- To make API requests that modify system settings, such as enabling or disabling the RADKit service, you must have administrative privileges to access Cisco SD-WAN Manager API interface (https://<sd-wan-manager-ip>/apidocs).
- Ensure proper internet and DNS connectivity for the Cisco RADKit service to function correctly.

Procedure

Step 1 Open your web browser and navigate to the Cisco SD-WAN Manager API documentation by entering the URL: `https://<sd-wan-manager-ip>/apidocs` (replace <**`sd-wan-manager-ip`**> with the actual IP address of your Cisco SD-WAN Manager instance).

Step 2 Within the API documentation, look for the API endpoint related to container services or specifically for RADKit, for example, `/dataservice/settings/configuration/<type>` where type is radkit .

Step 3 Make a POST request to this endpoint.

You will find an option to make a `POST` request to this endpoint.

Step 4 In the request body, provide the following JSON payload:

```
{"mode": "enabled"}
```

Step 5 Click **Execute**.

Once the API call is successfully executed, the RADKit service is enabled, and it will begin its initialization and setup process.

What to do next

Confirm that the RADKit container is running and healthy. You can do this by using the CLI command `request nms container-manager diagnostics`.

To disable the service, post an API request to the RADKit service endpoint in Cisco SD-WAN Manager with a JSON payload of `{"mode": "disabled"}`.

Use the Cisco RADKit Service APIs

This task explains how to correctly format URLs for making API calls to the Cisco RADKit service. To successfully access RADKit functionalities, you must include `/radkit` as a mandatory prefix before the specific API endpoint in your URL. This ensures your request is properly routed within the Cisco SD-WAN Manager environment.

To access RADKit Service API endpoints, follow these steps:

Before you begin

Ensure you have access to your Cisco SD-WAN Manager instance's IP address and port.

Procedure

Construct the API URL by including the /radkit prefix before the actual endpoint.

Example:

To access the login API, the format for the URL is:

```
https://<sd-wan-manager-ip>:<port>/radkit/your/api/endpoint
```

Example:

```
https://10.240.185.84:8443/radkit/api/v1/auth/login
```

You have successfully constructed the correct URL format for accessing a Cisco RADKit Service API endpoint.

What to do next

Proceed to make your API calls to the Cisco RADKit Service using the constructed URL.

Verify Cisco RADKit service in Cisco SD-WAN Manager

By verifiying Cisco RADKit service in Cisco SD-WAN Manager, you can confirm the Cisco RADKit Service's operational status (enabled or disabled).

This section provides the steps to verify whether the Cisco RADKit service in Cisco SD-WAN Manager is enabled or disabled.

Before you begin

- Ensure you have CLI access to Cisco SD-WAN Manager.

Procedure

From the CLI interface of Cisco SD-WAN Manager, execute the following command:

request nms container-manager diagnostics

```
NMS container manager
Checking container-manager status

Listing all images
-----------------------
REPOSITORY                  TAG          IMAGE ID       CREATED        SIZE
sdwan/reporting             latest       10d3363a0c7c   15 hours ago   941MB
sdwan/messaging-server      0.20.0       30547ceba4b9   15 hours ago   150MB
sdwan/radkit                1.8.6rc1     5ebe514b17d4   15 hours ago   782MB
sdwan/cluster-orchestrator  1.0.1        5aa1fd0e8e18   15 hours ago   669MB
sdwan/configuration-db      4.4.38       d6b9eb6fd60e   15 hours ago   548MB
sdwan/olap-db               24.3.6.48    219369311a35   15 hours ago   409MB
sdwan/cloudagent-v2         1.0.0        a56c3552ab49   15 hours ago   703MB
sdwan/upgrade-coordinator   2.0.0        d95f20da260b   15 hours ago   141MB
sdwan/application-server    24.0.1       7d505d68bf3f   15 hours ago   1.15GB
```

```
sdwan/coordination-server    3.8.4       91b45542b9e2   15 hours ago   346MB
sdwan/vault                  1.0.1       b2323a89ada8   2 weeks ago    511MB
sdavc                        4.7.0       d1512d663ac7   7 weeks ago    749MB
sdavc-gw                     4.7.0       4ed15cea64ee   7 weeks ago    463MB

Listing all containers
-----------------------
CONTAINER ID   IMAGE                                COMMAND                  CREATED         STATUS
                     PORTS

                                                       NAMES
ed8024e0dbb5   sdwan/messaging-server:0.20.0        "/bin/bash /entrypoi…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:4222->4222/tcp, 127.0.0.1:6222->6222/tcp, 127.0.0.1:8222->8222/tcp

                                                         messaging-server
9013b37451d9   sdwan/olap-db:24.3.6.48              "/usr/bin/tini -- /e…"   6 minutes ago   Up 6
minutes (healthy)        127.0.0.1:8123->8123/tcp, 127.0.0.1:9363->9363/tcp

                                                             olap-db
95fea11679e7   sdwan/cloudagent-v2:1.0.0            "./entrypoint.sh"        6 minutes ago   Up 6
minutes (healthy)        127.0.0.1:9051-9052->9051-9052/tcp

                                                             cloudagent-v2
2e534bbea1af   sdwan/reporting:latest               "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes                  80/tcp, 127.0.0.1:9080->9080/tcp

                                                             reporting
b25381e8e543   sdwan/coordination-server:3.8.4      "/docker-entrypoint.…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:2181->2181/tcp, 127.0.0.1:2888->2888/tcp, 127.0.0.1:3888->3888/tcp,
 127.0.0.1:4888->4888/tcp
                                                        coordination-server
0b696e5f38d5   sdwan/vault:1.0.1                    "docker-entrypoint.s…"   6 minutes ago   Up 6
minutes (healthy)        8200/tcp, 127.0.0.1:8201-8202->8201-8202/tcp

                                                             vault
3c7254a24f5a   sdavc:4.7.0                          "/usr/local/bin/sdav…"   6 minutes ago   Up About
 a minute (healthy)   127.0.0.1:10503->8080/tcp, 127.0.0.1:10504->8443/tcp

                                                        sdavc
944e74177a8f   sdavc-gw:4.7.0                       "/bin/bash -c 'exec …"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:8444->8444/tcp, 127.0.0.1:10501->8080/tcp, 127.0.0.1:10502->8443/tcp,
 127.0.0.1:10000->50000/udp
                                                      sdavc-gw
0c9c29dbf0a8   sdwan/configuration-db:4.4.38        "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:2004->2004/tcp, 127.0.0.1:5000->5000/tcp, 127.0.0.1:6000->6000/tcp,
 127.0.0.1:6362->6362/tcp, 127.0.0.1:6372->6372/tcp, 127.0.0.1:7000->7000/tcp,
127.0.0.1:7473-7474->7473-7474/tcp, 127.0.0.1:7687-7688->7687-7688/tcp   configuration-db
c7fe7153a21a   sdwan/application-server:24.0.1      "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes (healthy)

                                                             base-application-server
6c8f3ec5103f   sdwan/cluster-orchestrator:1.0.1     "/entrypoint.sh"         7 minutes ago   Up 7
minutes (healthy)        127.0.0.1:9090->9090/tcp, 127.0.0.1:9099->9099/tcp

                                                             cluster-orchestrator

Docker info
-----------------------
Client:
 Context:    default
 Debug Mode: false

Server:
 Containers: 11
```

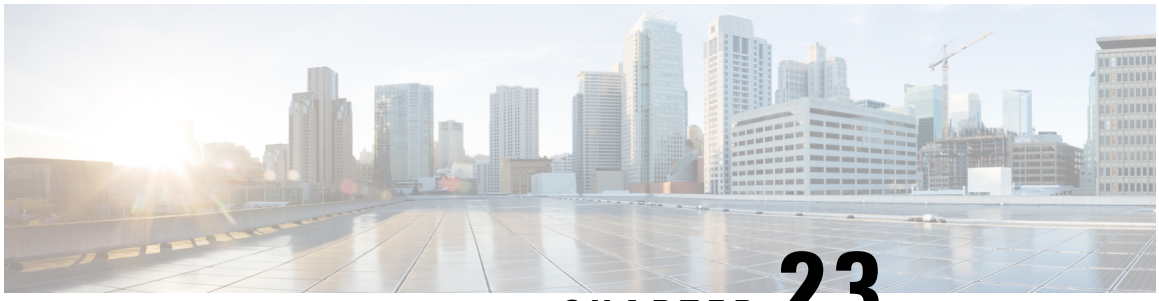
```
 Running: 11
 Paused: 0
 Stopped: 0
Images: 13
Server Version: 23.0.6
Storage Driver: overlay2
 Backing Filesystem: extfs
 Supports d_type: true
 Using metacopy: false
 Native Overlay Diff: true
 userxattr: false
Logging Driver: local
Cgroup Driver: cgroupfs
Cgroup Version: 1
Plugins:
 Volume: local
 Network: bridge host ipvlan macvlan null overlay
 Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
Swarm: inactive
Runtimes: io.containerd.runc.v2 runc
Default Runtime: runc
Init Binary: docker-init
containerd version: b1624c3628954e769dd50783b63823040b2db38c.m
runc version: v1.1.14-0-g2c9f5602-dirty
init version: b9f42a0-dirty
Security Options:
 seccomp
  Profile: builtin
Kernel Version: 6.6.21-yocto-standard
Operating System: viptela 20.18.1 (scarthgap)
OSType: linux
Architecture: x86_64
CPUs: 8
Total Memory: 23.48GiB
Name: vm
ID: 7f6e3203-ad3a-40af-aacd-21e43cbe1c9c
Docker Root Dir: /var/lib/nms/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false

WARNING: No cpu cfs quota support
WARNING: No cpu cfs period support
WARNING: No blkio throttle.read_bps_device support
WARNING: No blkio throttle.write_bps_device support
WARNING: No blkio throttle.read_iops_device support
WARNING: No blkio throttle.write_iops_device support
```

What to do next

Analyse the output within the **Listing all containers** section; the `radkit` container will be listed there Cisco RADKit service if is enabled.

For detailed information on Cisco RADKit user operations, see the documentation: https://radkit.cisco.com/docs/control_api/control_api.html#user-operations.



CHAPTER 23

Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS

Table 69: Feature History

Feature Name	Release Information	Description
Unified Debug Condition To Match IPv4 and IPv6 Over MPLS	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature introduces a debug condition to identify and resolve issues related to matching IPv4 and IPv6 traffic over an MPLS network.

- Information About the Unified Debug Condition, on page 345
- Restrictions of the Unified Debug Condition, on page 346
- Use Cases for the Unified Debug Condition, on page 346
- Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI, on page 346
- Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS, on page 348

Information About the Unified Debug Condition

The Cisco IOS XE Catalyst SD-WAN devices support the ability to add a debug condition for IPv4 and IPv6 traffic over MPLS packets. You can specify a filter condition to select the overlay IP address and optionally, the underlay MPLS label with a stack depth. Use the unified debug condition to troubleshoot MPLS networks by identifying specific packets that match certain filtering criteria and troubleshoot any issues related to the MPLS traffic to ensure that your network runs smoothly. The matching of IPv4 and IPv6 over MPLS is a three step process:

1. Debugging
2. Specifying the filtering conditions
3. Applying the filer conditions to the devices

In Cisco IOS XE Catalyst SD-WAN devices, the MPLS label is used to represent an IP VRF and is distributed by OMP protocol.

Restrictions of the Unified Debug Condition

- The debug condition for IPv4 and IPv6 over an MPLS network is supported only using the device CLI.
- Cisco SD-WAN Manager doesn't display the filtered debugging results as part of the packet trace debugging output. For more information see, Packet Trace.
- You can't enable the debug condition to match IPv4 traffic over MPLS and IPv6 traffic over MPLS at the same time.
- You can match only one MPLS label with either IPv4 or IPv6 traffic.
- The number of configurable Feature Invocation Array (FIA) entries per array is 31.

Use Cases for the Unified Debug Condition

The following are the use cases for matching IPv4 and IPv6 traffic over an MPLS network using a debug condition:

- Debugging conditions can help troubleshoot connectivity or performance issues in the network. By matching specific IPv4 and IPv6 traffic over the MPLS network, administrators can isolate the traffic that is causing the issue and analyze the behavior in more detail.
- Debugging conditions can also be useful for implementing QoS policies on the network. By matching specific IPv4 and IPv6 traffic over the MPLS network, administrators can apply different QoS policies to different types of traffic based on their characteristics, such as bandwidth requirements, latency sensitivity, or priority. For more information see, Cisco SD-WAN Forwarding and QoS Configuration Guide.

Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI

Use the **debug platform condition mpls match-inner** command to match IPv4 and IPv6 traffic over MPLS using various filtering conditions such as *match-inner ipv4*, *match-inner ipv6*, and *allow-no-label*. Specify the MPLS label information, inner IPv4 and IPv6 address based on the debugging requirement.

1. Debug the MPLS network.

   ```
   debug platform condition mpls
   ```

2. Specify the debugging conditions as per your requirement.
   - Use the following condition to debug IPv4 traffic over an MPLS network without specifying the MPLS label:

     ```
     match-inner ipv4
     ```

   - Use the following condition to debug IPv6 traffic over an MPLS network without specifying the MPLS label:

     ```
     match-inner ipv6
     ```

- Use **allow-no-label** condition to match IPv4 or IPv6 packets irrespective of the MPLS labels being encapsulated or not. Use the allow-no-label condition when you want the decapsulated router traffic from the MPLS network to be transmitted as IPv4 or IPv6 packets:

  match-inner ipv4 *{ipv4-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

  or

  match-inner ipv6 *{ipv6-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

- Specify the MPLS label and depth to filter IPv4 packets flowing through a particular MPLS interface:

  [interface *interface-name interface-number*] **mpls** *depth-of-mpls-label* **match-inner ipv4** *{ipv4-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

- Specify the MPLS label and depth to filter IPv6 packets flowing through a particular MPLS interface:

  [interface *interface-name interface-number*] **mpls** *depth-of-mpls-label* **match-inner ipv6** *{ipv6-source-prefix | any | host | payload-offset | protocol}{ipv6-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

3. Exit the privileged EXEC mode:

   exit

Examples

The following example shows how to use the debug condition **debug platform condition mpls** command to enable matching of IPv4 or IPv6 traffic over MPLS networks :

```
Device# debug platform condition mpls match-inner ipv4
Device# debug platform condition mpls match-inner ipv4 any any
Device# debug platform condition mpls match-inner ipv4 any any both
Device# debug platform condition mpls match-inner ipv4 any any both allow-no-label
```

For more information see, debug platform condition mpls command page.

The following example shows how to use the debug condition **debug platform condition interface mpls** command to enable matching of IPv4 or IPv4 traffic over MPLS networks for a specific interface:

```
Device# debug platform condition interface
Device# debug platform condition interface Loopback 3 mpls
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888 any both
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888 any both allow-no-label
```

Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS

Verify the Debug State

The following is a sample output from the **show platform conditions** command:

```
Device# show platform conditions

Conditional Debug Global State: Start

Conditions
     Direction
------------------------------------------------------------------------------------------|---------
All Interfaces                           & MPLS [ALL LABEL] & IPV4 Filter [ALL PROTO] [host
 10.20.24.17] [host 10.20.25.16] both bi



Feature Condition       Type                     Value
----------------------|----------------------|-----------------------------------------------------



Feature      Type           Submode
                                Level
————————|————————|————————————————————————————————————————————————————|————————
```

In this output, **Conditional Debug Global State: Start** indicates that the debugging is enabled. You can verify the debug filter configuration as well.

Packet Trace Statistics

The following is a sample output from the **show platform packet-trace statistics** command:

```
Device# show platform packet-trace statistics
Packets Summary
  Matched  2
  Traced   2
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     0
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA              0              0              0
TCP                0              0              0
UDP                0              0              0
IP                 0              0              0
IPV6               0              0              0
ARP                0              0              0
```

```
          PKT_DIR_OUT
              Dropped       Consumed       Forwarded
INFRA               0              0               0
TCP                 0              0               0
UDP                 0              0               0
IP                  0              0               0
IPV6                0              0               0
ARP                 0              0               0
```

In this output, **Matched** and **Traced** indicates the number of matched and traced packets.

Decode the IPv4 and IPv6 Matching over MPLS

The following is a sample output from the **show platform packet-trace** *packet 0* **decode** command:

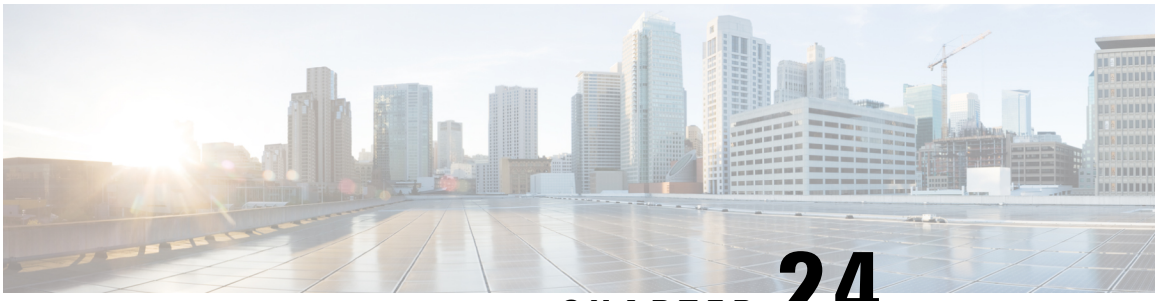
```
Device# show platform packet-trace packet 0 decode
Packet: 0 CBUG ID: 39872
Summary
Input : GigabitEthernet5
Output : GigabitEthernet1
State : FWD
Timestamp
Start : 10090556741529 ns (12/02/2022 05:54:03.730220 UTC)
Stop : 10090556747391 ns (12/02/2022 05:54:03.730226 UTC)
Path Trace
Feature: MPLS(Output)
Input : GigabitEthernet5
Output : Tunnel1
Label Stack Entry[1]: 0x003eb17f
StackEnd:YES, TTL:127, EXP:0, Label:1003, is SDWAN:YES
SDWAN Proto: IPV4, SDWAN dst_vpn: 1
Feature: MPLS_OUTPUT_L2_REWRITE
Entry : Output - 0x81323e6c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 239 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x81499d88
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 33 ns
Feature: MPLS_OUTPUT_FRAG
Entry : Output - 0x814cdb3c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 152 ns
Feature: SDWAN_LOSS_PROTECT_TX
Entry : Output - 0x814d962c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 15 ns
Feature: MPLS_SDWAN_TUNNEL_OUTPUT_FINAL
Entry : Output - 0x814d60cc
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 157 ns
Feature: SDWAN_TUNNEL_PRE_CHK_LKUP
Entry : Output - 0x814d911c
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 19 ns
Feature: SDWAN_TUNNEL_PRE_QOS_OUTPUT
Entry : Output - 0x814d956c
Input : GigabitEthernet1
```

```
Output : Tunnel1
Lapsed time : 70 ns
Feature: SDWAN_TUNNEL_OUTPUT_UNIFY_FNF_FINAL
Entry : Output - 0x814aaa68
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 95 ns
Feature: IPV4_OUTPUT_IPSEC_SDWAN_FEATURE
Entry : Output - 0x814c7480
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 101 ns
Feature: IPV4_OUTPUT_IPSEC_CLASSIFY
Entry : Output - 0x814c7438
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 151 ns
Feature: IPV4_IPSEC_FEATURE_RETURN
Entry : Output - 0x814c7478
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 35 ns
Feature: IPV4_TUNNEL_PRE_GOTO_OUTPUT
Entry : Output - 0x814d60c4
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 461 ns
Feature: CBUG_OUTPUT_FIA
Entry : Output - 0x81499d68
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 35 ns
Feature: IPV4_VFR_REFRAG
Entry : Output - 0x814c894c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 33 ns
Feature: DEBUG_COND_APPLICATION_OUT_CLR_TXT
Entry : Output - 0x81499d74
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 11 ns
Feature: IPV4_OUTPUT_L2_REWRITE
Entry : Output - 0x81323e50
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 53 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x81499d88
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 34 ns
Feature: DEBUG_COND_APPLICATION_OUT
Entry : Output - 0x81499d78
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 11 ns
Feature: IPV4_OUTPUT_FRAG
Entry : Output - 0x814c78e8
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 44 ns
Feature: IPV4_OUTPUT_DROP_POLICY
Entry : Output - 0x814d16b8
```

```
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 247 ns
Feature: IPV4_OUTPUT_SDWAN_FNF_FINAL
Entry : Output - 0x814aaa4c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 74 ns
Feature: DEBUG_COND_OUTPUT_PKT
Entry : Output - 0x81499d8c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 24 ns
Feature: MARMOT_SPA_D_TRANSMIT_PKT
Entry : Output - 0x814df374
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 780 ns
Packet Copy In
003eb17f 4500002a 0eb70000 7f11ed0a 10000001 30000001 a2c42710 00160000
801296c3 9baf96f9 9b56c437 0aca
Unable to decode layer 2 trying to skip to layer 3
MPLS
Label Stack Entry[1]
TTL : 127
Label : 1003
EXP : 0
StackEnd : YES
SDWAN : YES
SDWAN Label : 1003
SDWAN Proto : IPV4
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 42
Identifier : 0x0eb7
IP Flags : 0x0
Frag Offset : 0
TTL : 127
Protocol : 17 (UDP)
Header Checksum : 0xed0a
Source Address : 10.0.0.1
Destination Address : 10.0.0.1
UDP
Source Port : 41668
Destination Port : 10000
Length : 22
Checksum : 0x0000
Decode halted - unsupported udp port number
Packet Copy Out
52540095 dbed5254 007ffb83 08004500 0046ab1a 4000ff2f 9d4d0a01 0f0f0a01
10100000 8847003e b17f4500 002a0eb7 00007f11 ed0a1000 00013000 0001a2c4
27100016 00008012 96c39baf 96f99b56 c4370aca
ARPA
Destination MAC : 5254.0095.dbed
Source MAC : 5254.007f.fb83
Type : 0x0800 (IPV4)
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 70
Identifier : 0xab1a
```

```
IP Flags : 0x2 (Don't fragment)
Frag Offset : 0
TTL : 255
Protocol : 47 (GRE)
Header Checksum : 0x9d4d
Source Address : 10.0.0.1
Destination Address : 10.0.0.1
GRE ver 0
Optional Fields : None
Strict Source Route : NO
Recursion Control : 0
Flags : 0x00
Protocol : 0x8847 (MPLS)
MPLS
Label Stack Entry[1]
TTL : 127
Label : 1003
EXP : 0
StackEnd : YES
SDWAN : YES
SDWAN Label : 1003
SDWAN Proto : IPV4
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 42
Identifier : 0x0eb7
IP Flags : 0x0
Frag Offset : 0
TTL : 127
Protocol : 17 (UDP)
Header Checksum : 0xed0a
Source Address : 10.255.255.255
Destination Address : 10.255.255.254
UDP
Source Port : 41668
Destination Port : 10000
Length : 22
Checksum : 0x0000
Decode halted - unsupported udp port number
```

In this example, **Source Address** and **Destination Address** indicate that the debugging condition is successful. The **MPLS** section displays the SD-WAN labels specified.



CHAPTER 24

Packet Trace

Table 70: Feature History

Feature Name	Release Information	Description
Bidirectional Support for Packet Tracing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	This feature provides a detailed understanding of how data packets are processed by the edge devices in both the directions. Bidirectional debugging can help you to diagnose issues and troubleshoot them more efficiently.
Packet Trace Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature offers the following enhancements to packet trace: • A new command **show platform packet-trace fia-statistics**, available on Cisco IOS XE Catalyst SD-WAN devices, displays Feature Invocation Array (FIA) statistics in a packet trace. In FIA statistics, you can find data about a packet trace's feature count, the average processing time, the minimum processing time, and the maximum processing time. • View label information for the Multiprotocol Label Switching (MPLS) feature in a packet trace.

- Information About Packet Trace, on page 354
- Configure Packet Trace, on page 355
- Monitor Packet Trace, on page 356
- Configuration Examples for Packet Trace, on page 361

Information About Packet Trace

The Packet Trace feature enables you to debug packet loss on edge devices and to inspect any forwarding behavior of traffic flows on the devices in the network. You can configure packet tracer with various conditions based on which the flow of the packets is segregated and is captured for tracing. This helps you to diagnose issues and troubleshoot them more efficiently.

Packet tracer includes 2048 bytes of internal memory that is used to copy path data. This memory is overwritten during circular mode of tracing.

The Packet Trace feature provides three levels of inspection for packets—accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet-processing capability. However, packet trace limits the inspection of packets that match the **debug platform condition** statements, and is a viable option even under heavy-traffic situations in customer environments.

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, bidirectional support is added on the edge devices for a conditional debugging match filter. Conditional debugging allows you to filter out some of the debugging information on the edge device. You can check the debugging information that matches a certain interface, MAC address, or username.

Table 71: Packet Trace Levels

Packet Trace Level	Description
Accounting	Packet trace accounting provides a count of packets that enter and leave the network processor. Packet trace accounting is a lightweight performance activity, and runs continuously until it is disabled.
Summary	At the summary level of packet trace, data is collected for a finite number of packets. Packet trace summary tracks the input and output interfaces, the final packet state, the consumed packet state and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface.
Path data	Packet trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data. Path data also has two optional capabilities—packet copy and Feature Invocation Array (FIA) trace. The packet copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3, or layer 4). The FIA trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing. **Note** Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. We recommend that you use path-data level in a limited way or in situations where packet performance change is acceptable.

Usage Guidelines for Configuring Packet Trace

Consider the following best practices while configuring the Packet Trace:

- Use of ingress conditions when using the packet trace is recommended for a more comprehensive view of packets.
- Packet trace configuration requires data plane memory. On systems where data plane memory is constrained, carefully consider how you will select the packet trace values. A close approximation of the amount of memory consumed by packet trace is provided by the following equation:

  memory required = (statistics overhead) + (number of packets) * (summary size + data size + packet copy size).

When the Packet Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

Note The amount of memory consumed by the packet trace feature is affected by the packet trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting other router services.

Limitations

- Only IP packets are supported. L2 (ARP) packets, bridge packets, fragmented packets, and multicast packets are not supported.
- IPv6 is not supported.
- Packet duplication is not supported.
- Any packet that goes through resubmission (for example, IPsec or GRE encrypted packets) and matches the configured filters in both the inner packet (decrypted packet) as well as the outer packet (encrypted packet) will have individual trace entries. To use the packet tracer more efficiently, you should configure as many filters as possible with the available information to debug the issue.

Configure Packet Trace

Use the **debug platform packet-trace** command to configure a packet tracer on edge devices with various conditions such as bidirectional, VPN, circular, destination IP, source IP, interface, start, stop, logging, and clear.

Configure Packet Trace on Cisco IOS XE Catalyst SD-WAN devices

1. Enable packet trace for the traffic and specify the maximum number of packets:

   ```
   Device# debug platform packet-trace packet [number of traced packets]
   ```

2. Specify the matching criteria for tracing packets. Matching criteria provides the ability to filter by protocol, IP address and subnet mask, interface, and direction:

```
Device# debug platform condition [interface interface name] {match ipv4|ipv6|mac src
dst}  {both|ingress|egress} [bidirectional]
```

3. Enable MPLS output label trace. A MPLS output label trace is included in debug path to reduce the impact on performance.

```
Device# debug platform hardware qfp active feature cef-mpls datapath mpls all
```

4. Enable the specified matching criteria and start packet tracing:

```
Device# debug platform condition start
```

5. Deactivate the condition and stop packet tracing:

```
Device# debug platform condition stop
```

6. Exit the privileged EXEC mode:

```
exit
```

Configure Packet Trace on Cisco vEdge devices

The following example shows how to configure conditions for packet tracing:

```
Device# debug packet-trace condition source-ip 10.1.1.1
Device# debug packet-trace condition vpn-id 0
Device# debug packet-trace condition interface ge0/1
Device# debug packet-trace condition stop
```

For more information, see debug packet-trace condition command page.

Monitor Packet Trace

Packet trace configuration is based on the AND operation of the specified conditions, with the packets matching all the configured conditions being traced.

Monitor Packet Trace on Cisco vEdge devices

Use the **show packet-trace statistics** command on Cisco vEdge devices to view the summary of all the packets matching the specified condition.

The following example displays all the conditions that are configured for packet tracing:

```
Device# show debugs
debugs packet-trace condition source-ip 10.1.1.1
debugs packet-trace condition vpn-id 0
debugs packet-trace condition interface ge0/1
debugs packet-trace condition state Stopped
```

Use the **show packet-trace statistics** command on Cisco vEdge devices to view the summary of all the packets matching the specified condition.

The following example displays a packet trace statistics for the specified interface, in this case, ge 0:

```
Device# show packet-trace statistics source-interface ge0_0
packet-trace statistics 0
source-ip 10.1.15.13
source-port 0
destination-ip 10.4.0.5
destination-port 0
```

```
source-interface ge0_0
destination-interface loop0.0
decision PUNT
duration 40
```

For more information, see show packet-tracer command page.

Detailed Packet View

The following is a sample output of the **show packet-trace details** command, which is displayed for the specified trace ID 10:

```
Device# show packet-trace details 10
```

```
Pkt-id     src_ip(ingress_if)     dest_ip(egress_if)     Duration     Decision
==========================================================================================
10         10.1.15.15:0 (ge0_0)   12.168.255.5:0 (ge0_0)     15 us          PUNT
INGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f 0f
e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00
00 00 00 00 00
EGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f 0f
e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00
00 00 00 00 00
Feature Data
-------------------------------------
TOUCH : fp_proc_packet
-------------------------------------
TOUCH : fp_proc_packet2
-------------------------------------
TOUCH : fp_send_to_host
-------------------------------------
FP_TRACE_FEAT_PUNT_INFO:
icmp_type : 0
icmp_code : 0
qos : 7
-------------------------------------
TOUCH : fp_hw_x86_pkt_free
```

Use the **show packet-trace details** command to view detailed information for the specified trace ID. The detailed packet view output displays three sections - summary data section, packet dump section, and featured data section.

Monitor Packet Trace on Cisco IOS XE Catalyst SD-WAN Devices

Summary View

Use the **show platform packet-trace summary** command on Cisco IOS XE Catalyst SD-WAN devices to view the summary of all the packets matching the specified condition.

The following example displays a packet trace summary on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace summary
```

```
Pkt    Input                    Output                   State  Reason
0      INJ.12                   Gi2                      FWD
```

```
1     Gi2                       internal0/0/rp:0          PUNT   5
2     INJ.1                     Gi2                       FWD
3     INJ.1                     Gi2                       FWD
4     Gi2                       internal0/0/rp:0          PUNT   5
5     Gi2                       internal0/0/rp:0          PUNT   5
6     INJ.1                     Gi2                       FWD
7     INJ.1                     Gi2                       FWD
8     Gi2                       internal0/0/rp:0          PUNT   5
9     Gi2                       internal0/0/rp:0          PUNT   5
10    Gi2                       internal0/0/rp:0          PUNT   5
11    INJ.1                     Gi2                       FWD
12    Gi2                       internal0/0/rp:0          PUNT   5
13    INJ.1                     Gi2                       FWD
14    INJ.1                     Gi2                       FWD
```

Detailed Packet View

The following is a sample output of the **show platform packet-trace packet 0** command on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace packet 0

Packet: 0           CBUG ID: 4321
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 1124044721695603 ns (09/20/2022 01:47:28.531049 UTC)
    Stop    : 1124044722142898 ns (09/20/2022 01:47:28.531497 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.10.10.10
    Destination : 20.20.20.20
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x814670b0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 600 ns
  Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
    Entry       : Input - 0x81494d2c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1709 ns
  Feature: IPV4_INPUT_ARL_SANITY
    Entry       : Input - 0x814690e0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1274 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x81494d28
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 269 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x81494d34
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 384 ns
  Feature: DEBUG_COND_APPLICATION_IN
```

```
  Entry       : Input - 0x814670a0
  Input       : GigabitEthernet2
  Output      : <unknown>
  Lapsed time : 107 ns
Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
  Entry       : Input - 0x8146709c
  Input       : GigabitEthernet2
  Output      : <unknown>
  Lapsed time : 36 ns
Feature: IPV4_INPUT_LOOKUP_PROCESS
  Entry       : Input - 0x81494d40
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 38331 ns
Feature: IPV4_INPUT_IPOPTIONS_PROCESS
  Entry       : Input - 0x81495258
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 259 ns
Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
  Entry       : Input - 0x8146ab58
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 9485 ns
Feature: IPV4_VFR_REFRAG
  Entry       : Output - 0x81495c6c
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 520 ns
Feature: IPV6_VFR_REFRAG
  Entry       : Output - 0x81496600
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 296 ns
Feature: MPLS(Output)
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Label Stack Entry[1]: 0x03e850fe
    StackEnd:NO, TTL:254, EXP:0, Label:16005, is SDWAN:NO
  Label Stack Entry[2]: 0x000121fe
    StackEnd:YES, TTL:254, EXP:0, Label:18, is SDWAN:NO
Feature: MPLS_OUTPUT_ADD_LABEL
  Entry       : Output - 0x8145e130
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 29790 ns
Feature: MPLS_OUTPUT_L2_REWRITE
  Entry       : Output - 0x812f4724
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 23041 ns
Feature: MPLS_OUTPUT_FRAG
  Entry       : Output - 0x8149ae5c
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 785 ns
Feature: MPLS_OUTPUT_DROP_POLICY
  Entry       : Output - 0x8149ebdc
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 14697 ns
Feature: MARMOT_SPA_D_TRANSMIT_PKT
  Entry       : Output - 0x814ac56c
  Input       : GigabitEthernet2
```

```
    Output      : GigabitEthernet3
    Lapsed time : 45662 ns
Packet Copy In
  00505683 d54f0050 56830863 08004500 00641018 0000ff01 6f450a0a 0a0a1414
  14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd abcdabcd abcdabcd
Packet Copy Out
  00505683 d4900050 5683429a 884703e8 50fe0001 21fe4500 00641018 0000fe01
  70450a0a 0a0a1414 14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd
```

Use the **show platform packet-trace summary** command to view detailed information for the specified trace ID. The detailed packet view output displays three sections—summary data section, packet dump section, and featured data section.

- Summary data section: Displays packet trace ID, ingress interface, egress interface, and the forward decision taken for the packet to traverse across the device information for the specified trace ID.
- Packet dump section: Displays ingress and egress packet information. Only the first 96 bytes of packet header details are displayed.

Note The complete packet dump is not displayed because of tracer-memory limitations.

- Feature data section: Displays forwarding plane features that generate feature-specific tracing data and provides feature data decodes. These features provide debugging information to packet tracer, such as forward result, drop reason, and other behavior.

View FIA Statistics

Minimum supported releases: Cisco vManage Release 20.11.1 and Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Use the **show platform packet-trace fia-statistics** command on Cisco IOS XE Catalyst SD-WAN devices to view to FIA statistics. FIA statistics provides details about the number of features, and the time details–minimum time, maximum time, and average time about a feature.

The following example displays FIA statistics on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace fia-statistics

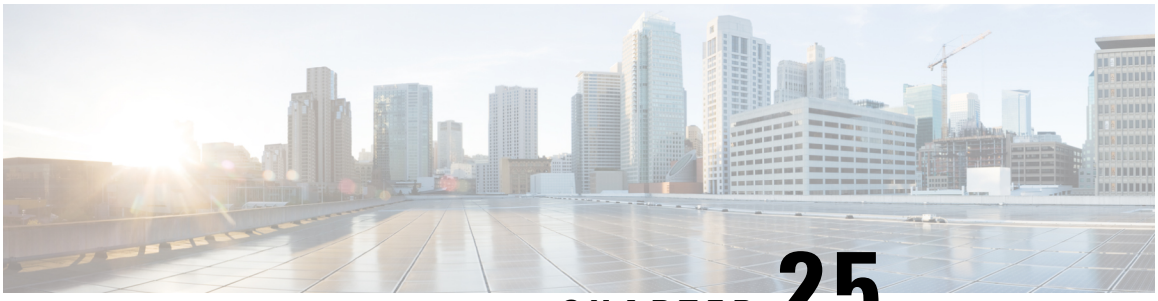
Feature                                        Count  Min(ns)   Max(ns)   Avg(ns)
-------------------------------------------------------------------------------
INTERNAL_TRANSMIT_PKT_EXT                         66     4720     28400     13333
MARMOT_SPA_D_TRANSMIT_PKT_EXT                     16     4560     16920     11955
L2_SVI_OUTPUT_BRIDGE_EXT                           1     3640      3640      3640
INTERNAL_INPUT_GOTO_OUTPUT_FEATURE_EXT            16     1680      3880      2755
IPV4_INPUT_LOOKUP_PROCESS_EXT                      1     2720      2720      2720
IPV4_OUTPUT_L2_REWRITE_EXT                         1     2240      2240      2240
IPV4_OUTPUT_DROP_POLICY_EXT                        4     1040      2880      2050
IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT               1     1960      1960      1960
SSLVPN_INJECT_TX_MSG_EXT                          15      600      2440      1746
IPV4_INTERNAL_FOR_US_EXT                           1     1560      1560      1560
LAYER2_OUTPUT_QOS_EXT                             63      280      2480      1537
LAYER2_OUTPUT_DROP_POLICY_EXT                     78      120      3120      1525
LAYER2_INPUT_LOOKUP_PROCESS_EXT                   15      280      2240      1312
UPDATE_ICMP_PKT_EXT                                1     1280      1280      1280
DEBUG_COND_MAC_EGRESS_EXT                          3      840      1160       973
IPV4_INTERNAL_INPUT_SRC_LOOKUP_CONSUME_EXT         1      960       960       960
IPV4_PREF_TX_IF_SELECT_EXT                         1      800       800       800
```

```
DEBUG_COND_OUTPUT_PKT_EXT                      66       80       1640       707
IPV4_INTERNAL_ARL_SANITY_EXT                    3      240        960       666
IPV4_INTERNAL_INPUT_SRC_LOOKUP_ISSUE_EXT        1      640        640       640
IPV4_VFR_REFRAG_EXT                             5      320        920       640
EVC_EFP_VLAN_TAG_ATTACH_EXT                    15       80       1040       629
L2_SVI_OUTPUT_GOTO_OUTPUT_FEATURE_EXT           1      520        520       520
LAYER2_VLAN_INJECT_EXT                         15      120        760       504
L2_ES_OUTPUT_PRE_TX_EXT                        16        0       1000       502
DEBUG_COND_APPLICATION_IN_EXT                   1      480        480       480
DEBUG_COND_APPLICATION_OUT_CLR_TXT_EXT          3       80        720       426
DEBUG_COND_INPUT_PKT_EXT                       16       80        880       417
IPV4_OUTPUT_FRAG_EXT                            1      360        360       360
DEBUG_COND_APPLICATION_IN_CLR_TXT_EXT           1      320        320       320
DEBUG_COND_APPLICATION_OUT_EXT                  3      240        280       266
LFTS_INJECT_PKT_EXT                            16       40        480       250
LAYER2_BRIDGE_INJECT_EXT                       15       40        560       234
```

Configuration Examples for Packet Trace

The following example shows how to configure and monitor the conditions for packet tracing:

```
Device# debug platform packet-trace packet 2048
Device# debug platform condition ingress
Device# debug platform condition start
Device# debug platform condition stop
Device# show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/2.3060 Gi0/0/2.3060 DROP 402
1 internal0/0/rp:0 internal0/0/rp:0 PUNT 21 2 internal0/0/recycle:0 Gi0/0/2.3060 FWD
```



CHAPTER 25

Underlay Measurement and Tracing Services

Table 72: Feature History

Feature Name	Release Information	Description
Underlay Measurement and Tracing Services	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	The underlay measurement and tracing services (UMTS) feature provides visibility into the exact paths that tunnels take between local and remote Cisco IOS XE Catalyst SD-WAN devices, through the underlay network (the physical devices that comprise the network). For a specific tunnel, the path includes all the nodes between the two devices. You can enable UMTS using Cisco SD-WAN Manager. You can view the resulting path information in Cisco SD-WAN Manager and in Cisco SD-WAN Analytics.
On-demand Underlay Measurement and Tracing Services	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	UMTS can now be used to discover the underlay path even when the BFD session (tunnel) is **down**.

- Information About Underlay Measurement and Tracing Services, on page 364
- Prerequisites for Underlay Measurement and Tracing Services, on page 365
- Restrictions for Underlay Measurement and Tracing Services, on page 365
- Configure Underlay Measurement and Tracing Services, on page 366
- Configure Underlay Measurement and Tracing Services Using a CLI Template, on page 367
- Trace and View Tunnel Paths On Demand, on page 368
- Troubleshooting Underlay Measurement and Tracing Services, on page 369
- Configuration Example for Underlay Measurement and Tracing Services, on page 369

Information About Underlay Measurement and Tracing Services

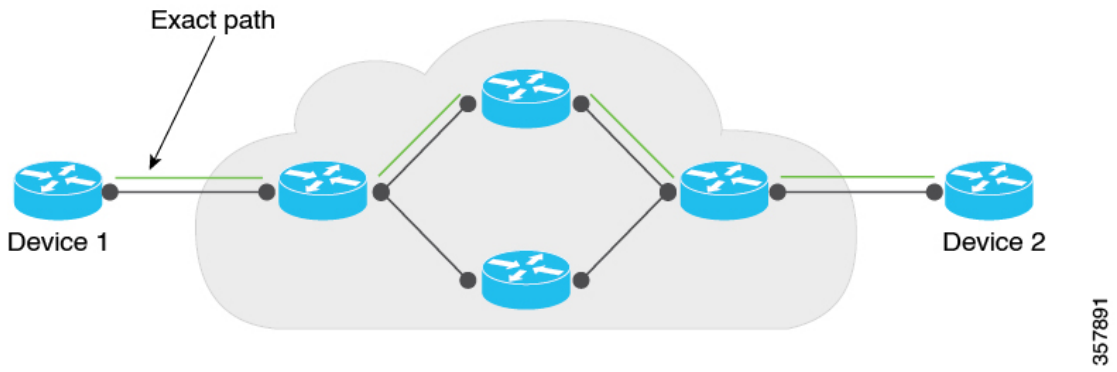
UMTS provides visibility into the exact path that a tunnel takes between local and remote Cisco IOS XE Catalyst SD-WAN devices, through the underlay network (the physical devices that comprise the network). For a specific tunnel, the path includes all the nodes between the two devices.

When a device creates an IPsec or GRE tunnel to a remote device, connecting through devices in the underlay network, more than one path may be possible from the local device to the remote device. The number of paths and the hops in the paths depend on the variability of the underlay network. The path that a tunnel takes through the underlay network can change over time. For example, if a tunnel uses a path that includes router A, and if router A becomes unavailable later, the tunnel will require a different path.

Each possible path through the underlay network is called a candidate path. The actual path that the tunnel is using at the moment is called the exact path. UMTS traces only the exact path. It does not discover or trace candidate paths.

The following illustration shows an underlay network that provides multiple paths for a tunnel between Device 1 and Device 2, and shows the exact path used by the tunnel.

Figure 13: Exact Path



You can trace the path of the tunnels in a network using one of these options:

- Monitoring: Trace tunnel paths regularly according to a configured time interval.
- Event-Driven: Trace tunnel paths when triggered by one of the following events:
  - A change in the service-level agreement (SLA) for the tunnel.
  - A change in the path maximum transmission unit for the tunnel.
- On demand: Trace the path of tunnels on demand, and display the results in Cisco SD-WAN Manager. For information, see View Exact Paths On Demand.

Mechanism for Underlay Measurement and Tracing Services

For UMTS interval-based monitoring and event-driven monitoring, Cisco SD-WAN Manager provides monitoring configuration (interval, event types) as part of the overall device configuration. In accordance with the configuration, Cisco IOS XE Catalyst SD-WAN devices use an UMTS probe packet mechanism to

trace the exact paths of tunnels across all hops, and collect network metrics such as delay and loss. Latency is only supported hop by hop.

The devices send the resulting information to Cisco SD-WAN Manager, which in turn, sends it to Cisco SD-WAN Analytics. Cisco SD-WAN Analytics uses the information to graphically display the exact path of the tunnels in the network.

For the on-demand option, Cisco SD-WAN Manager sends a request to the Cisco IOS XE Catalyst SD-WAN devices in the network to probe the network and trace the exact paths of tunnels. This request is in the form of a NETCONF action, and not a device configuration. The devices use the UMTS probe packet mechanism to trace the exact paths of the tunnels across all the hops, and to collect network metrics such as delay and loss. The devices send the resulting information to Cisco SD-WAN Manager, and Cisco SD-WAN Manager graphically displays the exact path of the tunnels in the network.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the UMTS probe works irrespective of BFD state.

Benefits of Underlay Measurement and Tracing Services

UMTS provides details of the exact path of each Cisco Catalyst SD-WAN tunnel, which can be useful in identifying problems with the tunnels.

Prerequisites for Underlay Measurement and Tracing Services

- To view the exact path graphs in Cisco SD-WAN Analytics, you must enable application visibility and flow visibility.

Note This prerequisite does not apply to on-demand viewing of graphs in Cisco SD-WAN Manager.

For more information about configuring application visibility and flow visibility, see Configure Global Application Visibility, Configure Global Flow Visibility.

- **Data Stream** must be enabled in Cisco SD-WAN Manager (from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**) to trace the path of tunnels on demand and display the results in Cisco SD-WAN Manager.
- Cisco SD-WAN Manager and Cisco SD-WAN Analytics must be integrated to view visualizations in Cisco SD-WAN Analytics. For more information about integrating Cisco SD-WAN Analytics with Cisco SD-WAN Manager, see Onboard Cisco SD-WAN Analytics.

Restrictions for Underlay Measurement and Tracing Services

- UMTS is supported only on Cisco Catalyst SD-WAN tunnels using IPv4 addresses.

- For the interval- and event-driven options, you can view the graphical representation of the exact paths only in Cisco SD-WAN Analytics. For the on-demand option, you can view the exact paths in Cisco SD-WAN Manager.
- Cisco SD-WAN Analytics UMTS graphs cannot distinguish between monitoring records and SLA and path maximum transmission unit events.
- Jitter and loss measurements are not supported.

Configure Underlay Measurement and Tracing Services

Configure UMTS Using Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **System Profile**.
4. Click **Add Feature**.
5. From the **Type** drop-down list, choose **Performance Monitoring**.
6. In the **Feature Name** field, enter a name for the feature.
7. In the **Description** field, enter a description for the feature.
8. Click **Underlay Measurement Track Service**.
9. To trace the tunnel paths regularly, based on a time interval, do the following:
   a. From the **Monitoring** drop-down list, choose **Global**.
   b. Click the toggle button to enable the continuous monitoring option in UMTS.
   c. In the **Monitoring Interval (Minutes)** drop-down list, choose a time.

      This option enables you to monitor the exact path during a specific time period.
10. To trace tunnel paths when triggered by an event, do the following:
    a. Click the **Event Driven** drop-down list, and choose **Global**.
    b. Click the **Event Type** drop-down list, and choose one or more event types.
    c. Click **Save**.
11. Click the **Associated Devices** tab.
12. From the list of Cisco IOS XE Catalyst SD-WAN devices, choose one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Deploy**.
13. In the **Process Overview** window, click **Next**.

    The **Selected Devices to Deploy** window displays the Cisco IOS XE Catalyst SD-WAN devices selected previously.

14. Check or uncheck the check boxes adjacent to the Cisco IOS XE Catalyst SD-WAN devices and then click **Next**.
15. In the **Summary** window, click **Deploy** to deploy the configurations in the Cisco IOS XE Catalyst SD-WAN devices.



Note With the **Monitor** option enabled in Cisco SD-WAN Manager, time-series data for the exact path can be generated and displayed in Cisco SD-WAN Analytics.

For more information on using configuration groups, see Configuration Groups and Feature Profiles.

Configure Underlay Measurement and Tracing Services Using a CLI Template

Use the CLI templates to configure continuous monitoring and event types for exact paths. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.



Note By default, CLI templates execute commands in global config mode.

This procedure configures interval-based monitoring and event-driven UMTS monitoring of tunnel paths.

1. Monitor the exact paths of tunnels continually, with a specific time interval:

```
sdwan
umts
 monitor
 periodicity seconds
 local-color-all
 remote-color-all
 remote-system-ip-all
```

Tunnel periodicity range is from 10 to 4294967295 seconds.

2. Monitor the exact paths of tunnels when triggered by a change in a tunnel's service-level agreement (SLA) or path maximum transmission unit:

```
sdwan
event
 event-type event-type
 local-color-all
 remote-color-all
 remote-system-ip-all
```

The following is a complete configuration example:

```
sdwan
umts
 monitor
```

```
 periodicity 1800
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event
 event-type tunnel-sla-change
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event-type tunnel-pmtu-change
 local-color-all
 remote-color-all
 remote-system-ip-all
!
```

Trace and View Tunnel Paths On Demand

Before You Begin

You can configure UMTS to trace exact paths at intervals or when triggered by an event. See Configure Underlay Measurement and Tracing Services, on page 366.

Alternatively, you can trace tunnel paths on demand, and view the paths using this procedure.

Trace and View Tunnel Paths On Demand

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click **…** adjacent to the corresponding device name and click **Underlay Discovery**.
3. Enter the parameters required to retrieve the exact path details.
4. Click **Start**.

   A graph with details about the exact path a network traffic taking is displayed.

Alternatively, you can trace and view the exact paths on demand using any of the following navigation paths in Cisco SD-WAN Manager.

- From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**, click **…** adjacent to the corresponding tunnel name, and choose **Underlay Discovery**.
- From the Cisco SD-WAN Manager menu, choose **Monitor** > **Applications** page, click **…** adjacent to the corresponding application name, and choose **Underlay Discovery**.
- In the **Site Topology** window, click a device or tunnel name, and then click **Underlay Discovery** in the right pane.

Troubleshooting Underlay Measurement and Tracing Services

Zero IP Address

Problem

Cisco SD-WAN Manager displays hops with a zero IP address (0.0.0.0) in the exact path.

Possible Causes

- The intermediate hops in the public internet may not respond because Internet Control Message Protocol (ICMP) time exceeded messages are disabled or blocked by a firewall. In such cases, hops are shown with a zero IP address.
- The destination edge device could be a Cisco vEdge device, which does not support UMTS.

Solution

Zero IP addresses in the exact path does not imply any functional problems with the tunnel. Verify that the zero IP address is because of one of the reasons described in Possible Causes section.

Timeout Error

Problem

A timeout error is displayed after starting an UMTS session, on demand, in Cisco SD-WAN Manager.

Possible Causes

- You are not using the minimum required releases--Cisco IOS XE Catalyst SD-WAN Release 17.10.1a or later for Cisco IOS XE Catalyst SD-WAN devices, and Cisco Catalyst SD-WAN Control Components Release 20.10.1 or later.
- There are network connectivity issues.

Solution

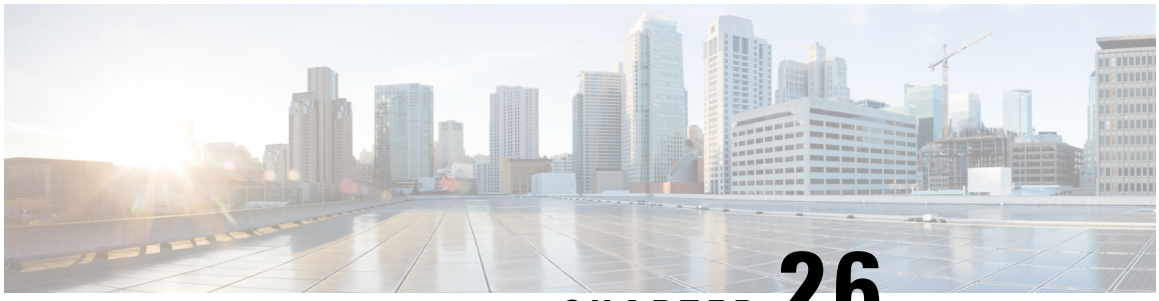
Check for the causes listed in Possible Causes section, and try the trace again.

Configuration Example for Underlay Measurement and Tracing Services

This example displays the configuration for the **Monitoring** and **Event-Driven** options configured in a Cisco IOS XE Catalyst SD-WAN device:

```
sdwan
umts
```

```
 monitor
 periodicity 1800
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event
 event-type tunnel-sla-change
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event-type tunnel-pmtu-change
 local-color-all
 remote-color-all
 remote-system-ip-all
!
```



CHAPTER 26

Analytics

- Internet Outages, on page 371
- View Internet Outages, on page 371

Internet Outages

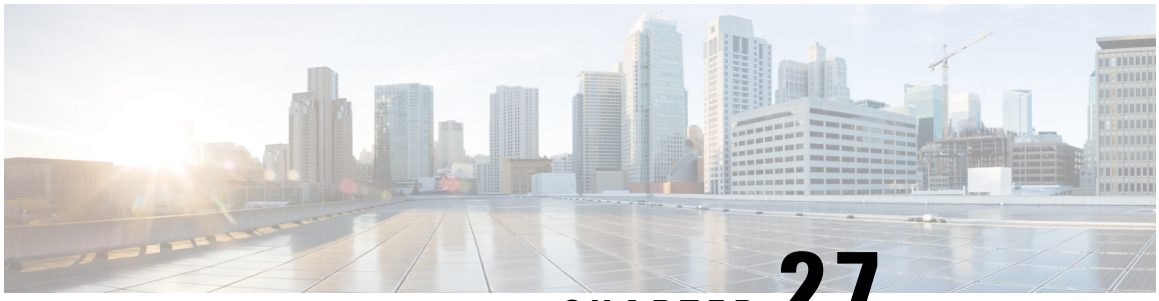
Table 73: Feature History

Feature Name	Release Information	Description
Internet Outages	Cisco IOS XE Catalyst SD-WAN Release 17.9.2a Cisco Catalyst SD-WAN Control Components Release 20.9.2	The Internet Outages feature powered by Cisco ThousandEyes WAN Insights displays the internet outages on a map at the affected locations and end points.

View Internet Outages

From the Cisco SD-WAN Manager menu, choose **Analytics** > **Internet Outages**.

The Internet outages map displays details about global Internet health over the last 24 hours, including number of outages, affected locations, and affected end points.



CHAPTER 27

Troubleshoot Cisco Catalyst SD-WAN Solution

- Overview, on page 373
- Support Articles, on page 373
- Feedback Request, on page 374
- Disclaimer and Caution, on page 374

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
Perform a Packet Capture on SD-WAN vManage	This document describes how to do a Packet Capture on Cisco SD-WAN Manager.
Quick Start Guide - Data Collection for Various SD-WAN Issues	This document describes several Cisco Catalyst SD-WAN issues along with relevant data that must be collected in advance before you open a TAC case to improve the speed of troubleshooting and/or problem resolution.

Document	Description
Troubleshoot IOS XE SD-WAN Upgrade Failure: Insufficient Space	This Cisco TAC-authored document describes the process to diagnose and resolve the issue when an upgrade fails due to insufficient storage capacity.
Error message during software upgrade or setting default software version	This troubleshooting document describes scenarios in which error messages can occur during device software upgrade or when setting the default software version.

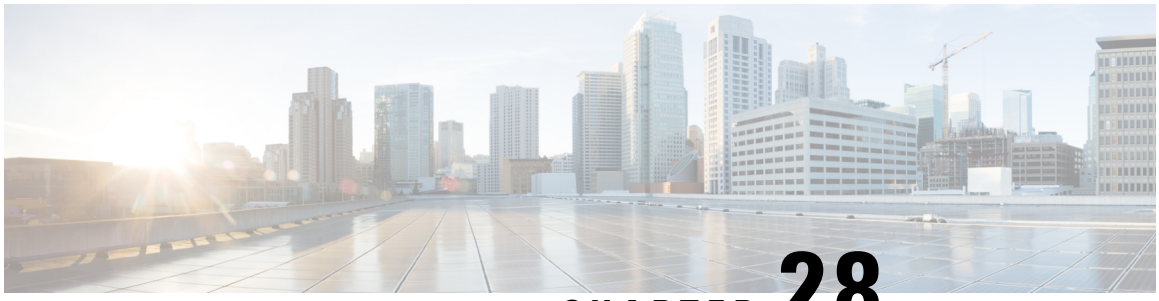
Feedback Request

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.



CHAPTER 28

Appendix

- Syslog Messages, on page 375
- Permanent Alarms and Alarm Fields, on page 416

Syslog Messages

The tables below list the syslog messages generated by Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices. The messages are grouped based on the software module that generates them. The software modules are typically processes (daemons) that run on the device.

All syslog messages are generated on all the devices unless otherwise indicated.

Each syslog message has a corresponding number. The tables list all syslog messages and their number even if the messages are defined in the header files but are not currently used in the operating software. For these messages, the Message Format, Description, and Action fields are empty.

In these tables, the Action field indicates the recommended action you should take in response to the syslog message:

- A—Automatically open a ticket in your organization's support team.
- AE—Automatically open a support ticket and escalate the ticket
- E—Send email to the appropriate team within your organization.

If you see a syslog message that is not listed in one of the tables below, please send the message, along with the device and software version, to Cisco support.

Note For information about Cisco SD-WAN Manager syslog message format, syslog message levels, and system log files, see Syslog Messages.

CFGMGR: Configuration Manager Process

Priority: Informational

Message	Number	Message Format	Description	Action
CFGMGR_SYSLOG_END	399999	Terminating cfgmgr	Configuration manager is stopping	E
CFGMGR_SYSLOG_SPEED_DUPLEX_NOT_SUPPORTED	300003	—	Interface does not support duplex mode	E
CFGMGR_SYSLOG_SPURIOUS_TIMER	300002	—	Internal error	A
CFGMGR_SYSLOG_IF_STATE	300004	—	Interface state reported by configuration manager	E
CFGMGR_SYSLOG_START	300001	Starting cfgmgr	Configuration manager is starting	E

CFLOWD: Cflowd Traffic Flow Monitoring Process

Priority: Informational

Message	Number	Message Format	Description	Action
CFLOWD_SYSLOG_MSG	2200002	Received information about vpn_id %ld, vpn_id	Cflowd detected a VPN change	E

Priority: Notice

Message	Number	Message Format	Description	Action
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd because sysmgr terminated	Cflowd module going down at request of sysmgr	E
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd with error code %d	Cflowd initialization failed and cflowd is about to go down, or cflowd module is going down	A
CFLOWD_SYSLOG_START	2200001	Starting module cflowd	Cflowd module is starting	E

CHMGR: Chassis Manager

The chassis manager process runs only on physical routers.

Priority: Informational

Message	Number	Message Format	Description	Action
CHMGR_CHASSIS_INFO	100009	Chassis-Type %s max-modules %d	Informational message indicating chassis type and maximum number of modules (PIMs + fixed) supported by chassis	E
CHMGR_FAN_SPEED_HIGH	100003	—	Fan speed is high	E
CHMGR_FAN_SPEED_NORMAL	100004	—	Fan speed is normal	E
CHMGR_FANTRAY_INSERTED	100052	Fantray %d inserted	Fan tray inserted (on vEdge 2000 only)	E
CHMGR_FANTRAY_REMOVED	100053	Fantray %d removed	Fan tray removed (on vEdge 2000 only)	E
CHMGR_MODULE_INSERTED	100007	Module %d inserted - port type: %s, num_ports: %s	PIM module inserted	E
CHMGR_MODULE_REMOVED	100008	Module %d removed	PIM module removed	E
CHMGR_PIM_OK	100057	—	PIM module status is normal	E
CHMGR_PORT_INSERTED	100005	Port %s inserted in module %d	SFP inserted	E
CHMGR_PORT_REMOVED	100006	Port %s removed from module %d	SFP removed	E
CHMGR_SIGTERM	100024	Received sigterm, exiting gracefully	Debug-level message indicating that chassis manager is going down	E
CHMGR_SYSLOG_START	100001	Starting chassis manager	Chassis manager process is starting	E
CHMGR_USB_INSERTED	100058	USB media inserted in slot %d	USB media inserted	E
CHMGR_USB_REMOVED	100059	USB media removed from slot %d	USB media removed	E

Priority: Notice

Message	Number	Message Format	Description	Action
CHMGR_EMMC_OK	100039	eMMC read successful	EMMC read was successful	E
CHMGR_FAN_OK	100041	Fan Tray %d Fan %d fault cleared, ftrayid, id	Fan fault cleared	E

Message	Number	Message Format	Description	Action
CHMGR_FANTRAY_OPER	100055	Fan tray '%d' up, ftrayid	Fan tray detected	A
CHMGR_FLASH_OK	100037	Flash memory status read successful	Flash read successful	E
CHMGR_PEM_OK	100043	Power supply '%d' fault cleared	Power supply fault cleared	E
CHMGR_PEM_OPER	100045	Power supply '%d' up	Power supply inserted or detected	E
CHMGR_SDCARD_OK	100047	SD card read successful	SD card read successful	E
CHMGR_SFP_UNSUPPORTED	10060	SFP %s is not supported	SFP is not supported	E
CHMGR_SHORT_RESET_REQUEST	100018	—	Chassis manager received a request to reboot the router	E
CHMGR_TEMP_GREEN	100030	%s temperature (%d degrees C) is below yellow threshold (%d degrees C)	Temperature sensor reading below yellow threshold	E
CHMGR_TEMP_OK	100027	%s temperature sensor fault cleared	Temperature sensor read successful after a previous failed attempt	E

Priority: Warning

Message	Number	Message Format	Description	Action
CHMGR_HOTSWAP_DIFF_MOD	100051	Hot-Insertion of a module of different type requires reboot. Module %d will remain down,	PIM module of a different type was inserted in the slot; it was detected, but will remain down until the next reboot	E

Priority: Error

Message	Number	Message Format	Description	Action
CHMGR_CONFD_DATACB_REGISTER_FAILED	100023	Failed to register data cb	Internal error registering a data callback function with confd	AE

Message	Number	Message Format	Description	Action
CHMGR_CONFD_REPLY_FAILED	100022	Failed to send oper data reply - %s (%d)	Internal error occurred when processing chassis manager–related configuration of **show** command	A
CHMGR_EEPROM_READ_FAILED	100011	Failed to read module %d eeprom on chassis %s, module, chassis-name	Failed to read details of inserted PIM	AE
CHMGR_EEPROM_VERSION_ERROR	100012	Unsupported eeprom format version for module %d	EEPROM version of PIM module is supported; module will not be recognized	AE
CHMGR_EMMC_FAULT	100038	eMMC fault detected	Error occurred reading EMMC information	A
CHMGR_FAN_FAULT	100040	Fan Tray %d Fan %d fault detected, ftrayid, id	Fan fault detected	A
CHMGR_FANTRAY_DOWN	100054	Fan tray '%d' not present, ftrayid id	Fan tray not detected	A
CHMGR_FLASH_FAULT	100036	Flash memory status fault	Internal error reading flash	AE
CHMGR_GET_HWADDR_FAILED	100010	Failed to get macaddr for %s, p_ifname	Internal error resulting from failure to obtain an interface's MAC address	A
CHMGR_GET_IFFLAG_FAILED	100016	Failed to get ifflags for %s err %d, p_port->kernel_name, errno	Interface initialization failure; interface may remain down, or device may reboot	A

Message	Number	Message Format	Description	Action
CHMGR_IFFLAGS_SET_FAIL	100050	—	Setting an interface flag failed	E
CHMGR_IF_GSO_OFF_FAILED	100025	—	Setting interface options failed	E
CHMGR_PEM_DOWN	100044	Power supply '%d' down or not present	Power supply removed or not detected	A
CHMGR_PEM_FAULT	100042	Power supply '%d' fault detected	Power supply fault detected	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault	PIM power fault detected	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault cleared	PIM power fault cleared	A
CHMGR_SDCARD_FAULT	100046	SD card fault detected (no present or unreadable)	SD card fault detected	A
CHMGR_SET_IFFLAG_FAILED	100017	Failed to set ifflags to %x for %s err %d	Interface initialization failure; interface may remain down, or device may reboot	A
CHMGR_SHORT_RESET_CLEAR_FAILED	100019	—	Clearing a reboot request failed.	A
CHMGR_SHORT_RESET_FAILED	100020	—	Request to reset the router by rebooting failed	A
CHMGR_SPURIOUS_TIMER	100035	Spurious timer ignored what = %#x arg = %p	Internal error	A
CHMGR_SYSOUT_OF_RESOURCES	100049	Timer add failed. Out of resources	Interal error; if fatal, device may reboot to recover	A

Message	Number	Message Format	Description	Action
CHMGR_UNKNOWN_MODULE_TYPE	100013	Invalid module-type %x in module-slot %d on chassis %s,	Unrecognized PIM module type in slot	AE
CHMGR_UNSUPPORTED_MODULE_TYPE	100014	Module-Type %s not supported in slot %d on chassis %s	PIM module is not supported in slot in which it is inserted	A

Priority: Critical

Message	Number	Message Format	Description	Action
CHMGR_IF_RENAME_FAILED	100015	Unable to rename %s to %s	Interface initialization failed; interface may remain down or the device may reboot	A
CHMGR_TEMP_FAULT	100026	%s temperature sensor fault detected. Unable to read temperature	Failed to read from a temperature sensor; possible temperature sensor failure	A
CHMGR_TEMP_RED	100028	%s temperature (%d degrees C) is above red threshold (%d degrees C).	Temperature sensor reading above red threshold	AE
CHMGR_TEMP_YELLOW	100029	%s temperature (%d degrees C) is above yellow threshold (%d degrees C),	Temperature sensor reading above yellow threshold	A

Priority: Alert

Message	Number	Message Format	Description	Action
CHMGR_CONFD_INIT_FAILED	100021	Initialization failed. vconfd_module_init returned %d	Chassis manager failed to initialize and start	AE

CVMX: Internal Cavium Driver Process

Priority: Informational

Message	Number	Message Format	Description	Action
CVMX_SYSLOG_END	999999	Terminating Cavium drivers	Internal Cavium drivers ending	E
CVMX_SYSLOG_START	900001	Starting Cavium drivers	Internal Cavium drivers starting	E

CXP: Cloud onRamp for SaaS Process

Priority: Informational

Message	Number	Message Format	Description	Action
CXP_SYSLOG_END	2799999	Terminating Cloud onRamp process	Cloud onRamp for SaaS ending	E
CXP_SYSLOG_START	2700001	Starting Cloud onRamp process	Cloud onRamp for SaaS starting	E

CONTAINER: Containers

Priority: Informational

Message	Number	Message Format	Description	Action
CONTAINER_SYSLOG_END	2699999	Terminating container process	Container process ending	E
CONTAINER_SYSLOG_START	2600001	Starting container process	Container process starting	E

DBGD: Debug Process

Priority: Informational

Message	Number	Message Format	Description	Action
DBGD_SYSLOG_END	2900001	Terminating debug process	Debug process ending	E
DBGD_SYSLOG_START	2999999	Starting debug process	Debug process starting	E

DHCPC: DHCP Client

The DHCP client process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_CLEAR_INTERFACE	1300006	Clearing dhcp state for interface %s,	DHCP client cleared DHCP state for interface	E
DHCP_SYSLOG_DISCOVER_TIMEOUT	1300005	No response for dhcp discover packets for interface %s,	DHCP discovery failure	E
DHCP_SYSLOG_END	1300001	Terminating syslog process	Syslog process ending	E

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_IP_ADDR_ASSIGNED	1300002	Assigned address %s to interface %s	DHCP client assigned address to interface	E
DHCP_SYSLOG_IP_ADDR_RELEASED	1300003	Released address for interface %s	DHCP client released address	E
DHCP_SYSLOG_IP_ADDR_RENEWED	1300010	Renewed address %s for interface %s	DHCP client address renewed	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [50%%] for interface %s address %s/%d	DHCP client renewal request at 50% of lease expiration time	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [85%%] for interface %s address %s/%d	DHCP client renewal request at 85% of lease expiration time	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [100%%] for interface %s address %s/%d	DHCP client renewal request at 100% of lease expiration time	E
DHCP_SYSLOG_START	1399999	Starting syslog process	Syslog paroces starting	E

Priority: Critical

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_IP_ADDR_CONFLICT	1300007	Interface %s IP Address %s conflict with interface %s,	DHCP client detected IP address conflict with another interface	E

DHCP: DHCP Server

The DHCP server process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server bindings for interface %s, vpn %ld,	DHCP server cleared bindings for interface	E
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server binding for interface %s, vpn %ld, mac addr %x:%x:%x:%x:%x:%x,	DHCP server cleared bindings for interface	E

FPMD: Forwarding Policy Manager Process

Priority: Informational

Message	Number	Message Format	Description	Action
FPMD_SYSLOG_ACL_PROGRAM_SUCCESS	1100005	Successfully reprogrammed access list - %s	Access list successfully created	E
FPMD_SYSLOG_END	1199999	Terminating fpmd	Forwarding policy manager process is ending	E
FPMD_SYSLOG_POLICY_PROGRAM_SUCCESS	1100004	Successfully reprogrammed policy %s - %s	Policy created successfully	E
FPMD_SYSLOG_START	1100001	Starting fpmd	Forwarding policy manager process is starting	E

Priority: Alert

Message	Number	Message Format	Description	Action
FPMD_SYSLOG_ACL_PROGRAM_FAILED	1100003	Failed to allocate memory for access list %s. Continuing without the access	Access list could not be created	A
FPMD_SYSLOG_POLICY_PROGRAM_FAILED	1100002	Failed to allocate memory for policy %s - %s. Continuing without the policy	Policy could not be created	A

FTMD: Forwarding Table Management Process

The forwarding table management process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
FTMD_SLA_CLASS_ADD	1000020	SLA Class %s added at index %d: loss = %d%%, latency = %d ms	SLA class added	E
FTMD_SYSLOG_BFD_STATE	1000009	record with discriminator %u invalid	BFD state is invalid	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_BFD_STATE	1000009	BFD Session %s.%u->%s.%u %s:%u->%s:%u %s %s %s %d	BFD state changed	E
FTMD_SYSLOG_DBGD_STATE	1000036	Connection to DBGD came up Connection to DBGD went down DBGD FTM: Initialized message queue DBGD FTM oper %d vpn %u sip %s:%u dip %s %u DBGD FTM: oper %d vpn %lu localc %d remote %d remoteip %s	Messages related to the FTM debugging process	E
FTMD_SYSLOG_DPI_FLOW_OOM	1000024	Out-of-memory status for DPI flows: %s	Memory status for SAIE flows **Note** In Cisco vManage Release 20.7.1 and earlier releases, the Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.	E
FTMD_SYSLOG_DPI_WRITE_OFF	1000032	Turning off writing DPI records to disk	SAIE records are no longer being written to disk **Note** In Cisco vManage Release 20.7.1 and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_END	1999999	Terminating FTM process	Forwarding table management process ending	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB6 memory to accommodate larger tables):	IPv6 forwarding table size is being increased	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB memory to accommodate larger tables):	IPv4 forwarding table size is being increased	E
FTMD_SYSLOG_IF_STATE	1000001	VPN %lu Interface %s %s,	FTM detected interface state change	E
FTMD_SYSLOG_LR_ADD	1000027	LR: Adding Iface %s as LR	Last-resort interface is being added	E
FTMD_SYSLOG_LR_ADD	1000027	LR: Iface %s has become an LR	Interface has become a last-resort interface	E
FTMD_SYSLOG_LR_DEL	1000028	LR: Found iface %s while looking for iface %s	Last-resort interface found while looking for another interface	E
FTMD_SYSLOG_LR_DEL	1000028	LR: iface %s has become non-LR. Hence set OPER UP on that interface	Last-resort interface has become an active interface	E
FTMD_SYSLOG_LR_DEL	1000028	LR: Iface %s has become a non-LR LR: Removing Iface %s as LR	Messages related to an interface that is no longer a last-resort interface	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_LR_DOWN	1000030	LR: At least one bfd session of non-LR is active LR: At least one non-LR's bfd session in Up LF bfd session = SIP: %s DIP:%s SPORT:%u DPORT:%u PROTO:%u is Up for at least &u interval msecs LR: Bringing LR's wan if Down in %u msecs LR: Bringing LR's wan if Down right away LR: Cleared LR down_in-progress	Messages related to shutting down an interface of last resort	E
FTMD_SYSLOG_LR_UP	1000029	LR: All bfd sessions gone down. Setting LR %s's OPER state to UP	Last-resort interface's status set to Up because no other circuits on the router are active	E
FTMD_SYSLOG_LR_UP	1000029	LR: Bring LR's wan if up immediately as no other circuit's bfd sessions are up	Last-resort interface activated because no other circuits on the router are active	E
FTMD_SYSLOG_LR_UP	1000029	LR: Starting hold up timer immediately !!	Hold timer for last-resort interface activated because no other circuits on the router are active	E
FTMD_SYSLOG_NAT_FLOW_ADD	1000039	NAT flow add: Private %s, Public %s	FTM detected the addition of a NAT flow with the specified private and public IP addresses	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_NAT_FLOW_DELETE	1000040	NAT flow delete: Private %s, Public %s	FTM detected the deletion of a NAT flow with the specified private and public IP addresses	E
FTMD_SYSLOG_PIM_DOWN	1000017	—	FTM detected that PIM ended	E
FTMD_SYSLOG_PIM_UP	1000018	—	FTM detected that PIM started	E
FTMD_SYSLOG_ROUTE_ADD_FAIL	1000004	Route Add for prefix %s Failed. Reason %s	FTM failed to add a route received from the RTM	E
FTMD_SYSLOG_ROUTE_VERIFY	1000033	Successfully verified RIB and FIB routes on the Cisco vEdge device	FTM verified the routes in the router's RIB and FIB	E
FTMD_SYSLOG_ROUTE_VERIFY_FAIL	1000034	—	RIB and FIB router verification failed	E
FTMD_SYSLOG_SIGTERM	1000005	Received Cleanup signal. Exiting gracefully	FTM received termination signal from sysmgr and is about to go down	E
FTMD_SYSLOG_START	1000001	Starting FTM process	Forwarding table management process starting	E
FTMD_SYSLOG_TCPD_STATE	1000035	Sent tcp_opt_disable successfully for vpn %ld	Disabling of TCP options was successful on the interface	E
FTMD_SYSLOG_TUNNEL_ADD_FAIL	1000015	Tunnel Add to TLOC %s.%s Failed. Reason %s	Failed to add new TLOC; reported by TTM	E
FTMD_SYSLOG_WWAN_STATE	1000025	Bring %s last resort circuit	Up or down status of circuit of last resort	E
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN came up	Circuit of last resort came up	E
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN went down	Circuit of last resort went down	E

Priority: Notice

Message	Number	Message Format	Description	Action
FTMD_SLA_CLASS_DEL	1000022	Sla class %s at index %d removed: loss = %d%%, latency = %d ms, jitter = %d ms	SLA class deleted	A
FTMD_SLA_CLASS_MOD	1000021	Sla class %s at index %d modified: loss = %d%%, latency = %d ms, jitter = %d ms	SLA class changed	A
FTMD_SLA_CLASS_VIOLATION	1000023	[%lu] SLA class violation application %s %2:%u._%s:&u protocol: %d dscp: %d %s, status - %s	SLA class violation for application in specified VPN, with specified source address and port, destination address and port, protocol, DSCP, and reason	A
FTMD_SYSLOG_DOT1X_HOST	1000031	Host %s denied access on interface %s in single host mode	An 802.1X interface in single-host mode is denying access, because it has already granted access to a client	E
FTMD_SYSLOG_FLOW_LOG	1000026	%s	FTM detected a new flow	E
FTMD_SYSLOG_FP_CORE_FAIL	1000013	FP core watchdog expired (rc = %d). %s, rc, action_str	FTM detected that FP may not be functioning; device will reboot soon	A
FTMD_SYSLOG_PMTU_LOWERED	1000016	Tunnel %s/%d -> %s/%d MTU Changed to %u due to Path-MTU Discovery,	MTU size on a tunnel changed due to path MTU discovery	E
FTMD_SYSLOG_ZBFW_FLOW_ADD	1000037	ZBF flow created zone-air %s key %s src_vpn %d dst_vpn %d expiry secs %d state %s	FTM detected the creation of a zone pair	E
FTMD_SYSLOG_ZBFW_FLOW_DEL	1000038	ZBF flow deleted zone-air %s key %s src_vpn %d dst_vpn %d state %s	FTM detected the deletion of a zone pair	E

Priority: Critical

Message	Number	Message Format	Description	Action

FTMD_SYSLOG_BUFFER_POOL_LOW **Note** This error message is available from Cisco SD-WAN Release 20.7.1.	1000041	Critical Alert: Buffer Pool <num>: available buffers are x% of total buffers	FTM detected that the specified buffer pool has gone below 20% of its capacity	E

Priority: Warning

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_BUFFER_POOL_LOW **Note** This error message is available from Cisco SD-WAN Release 20.7.1.	1000041	Warning Alert: Buffer Pool <num>: available buffers are x% of total buffers	FTM detected that the specified buffer pool has gone below 50% of its capacity	E
FTMD_SYSLOG_TTM_DOWN	1000008	Connection to TTM went down. p_msgq %p p_ftm %p,	FTM connection with TTM went down; BFD sessions will be cleared	E
FTMD_SYSLOG_TTM_UP	1000007	Connection to TTM came up. p_msgq %p p_ftm %p,	FTM connected with TTM	E
FTMD_TUNNEL_SLA_CHANGED	1000019	SLA changed for session: %s.%u->%s:%u->%s:%u. New loss = %d%%, latency = %d ms, jitter = %d ms, SLA Classes: %s (ox%x) %s%s	FTM detected SLA changes on a tunnel	E

Priority: Error

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register bfd show data cb	FTM failed to register data callback wtih confd; device may reboot	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register policer show data cb	FTM failed to register data callback with confd; device may reboot	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to register data cb, __FUNCTION__	FTM failed to register data callback with confd; device may reboot	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to send oper data reply - %s (%d) : %s,	FTM failed to respond correctly to confd; some **show** commands may not work	A

FTMD_SYSLOG_FP_COREDUMP	1000011	FP Core %d Died. Core file recorded at %s,	FTM detected an FP crash; device will reboot soon	AE
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of forwarding interface records	Interface not added because of insufficient forwarding interface database records	A
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of snmp interface indices	Interface not added because of insufficient SNMP interface indices	A
FTMD_SYSLOG_INIT_FAIL	1000002	vconf_module_init returned %d	FTM failed to start with confd	A
FTMD_SYSLOG_LR_DEL	1000028	LR: LR is not enabled...while we are trying to remove iface %s as last resort	Interface being removed is not configured as a last-resort interface	A
FTMD_SYSLOG_LR_DEL	1000028	LR: Unable to remove iface %s as LR	Interface is no longer a last-resort interface so it cannot be deleted	A
FTMD_SYSLOG_RTM_DECODE_FAIL	1000006	Bad RTM Msg: Msg-Type %u Msg-Len %u len: %u decoded-len %u,	Could not process route or interface change message from RTM	A
FTMP_SYSLOG_SPURIOUS_TIMER	1000010	Spurious timer ignored what = %#x arg = %p,	Internal error	A

GPS: Global Positioning System

Priority: Informational

Message	Number	Message Format	Description	Action
GPS_SYSLOG_END	2599999	Terminating GPS	GPS process is ending	E
GPS_SYSLOG_GGA_FIX	2500002	GGA %d:%d:%d lat=%f lon=%f alt=%f sat=%d hdop %f fix%d	GPS fix information	E
GPS_SYSLOG_GSA_FIX	2500004	GSA %s pdop=%.2f hdop=%.2f vdop=%.2f	GPS satellite and dilution of precision (DOP) information	E
GPS_SYSLOG_PSTOP	2500005	Polling disabled Stopping polling timers	Messages related to polling for GPS information	E
GPS_SYSLOG_RMC_FIX	2500003	RMC %s %d %d lat=%f lon=%f speed %f course=%s status valid	Essential minimum GPS information	E

Message	Number	Message Format	Description	Action
GPS_SYSLOG_START	2500001	Starting GPS	GPS process is starting	E

IGMP: Internet Group Management Protocol

Priority: Informational

Message	Number	Message Format	Description	Action
IGMP_SYSLOG_END	1800001	Terminating IGMP	IGMP process is ending	E
IGMP_SYSLOG_START	1899999	Starting IGMP	IGMP process is starting	E

LIBBSS: UNIX BSS Library

Unused Messages

Message	Number	Message Format	Description	Action
LIBBSS_SYSLOG_END	1699999	Terminating libbss	UNIX BSS library process is ending	E
LIBBSS_SYSLOG_START	1600001	Starting libbss	UNIX BSS library process is starting	E

LIBCHMGR: Chassis Manager Library Process

Unused Messages

Message	Number	Message Format	Description	Action
LIBCHMGR_SYSLOG_END	1599999	Terminating libchmrg	Chassis manager library process is ending	E
LIBCHMGR_SYSLOG_START	1500001	Starting libchmgr	Chassis manager libryary process is starting	E

MSGQ: Message Queue Process

Ununsed Messages

Message	Number	Message Format	Description	Action
MSGQ_SYSLOG_END	899999	Terminating msgq	Message queue process is ending	E
MSGQ_SYSLOG_START	800001	Starting msgq	Message queue process is starting	E

OMP: Overlay Management Protocol

Priority: Informational or Other

Message	Number	Message Format	Description	Action
OMP_NUMBER_OF_CISCO_VSMARTS	400005	Number of Cisco vSmarts connected: %u	Number of Cisco Catalyst SD-WAN Controllers to which device is connected (on Cisco vEdge devices only)	E
OMP_PEER_STATE_CHANGE	400002	%s peer %s state changed to %s,	OMP peer stated changed to up or down	E
OMP_POLICY_CHANGE	400007	Using policy from peer %s,	Forwarding policy received from Cisco Catalyst SD-WAN Controller (on Cisco vEdge devices only)	E
OMP_STATE_CHANGE	400003	Operational state changed to %s,	OMP internal operational state changed	E
OMP_TLOC_STATE_CHANGE	400004	TLOC %s state changed to %s for address-family: %s,	TLOC state changed	E

Priority: Notice

Message	Number	Message Format	Description	Action
OMP_SYSLOG_END	400006	Terminating	OMP process is stopping	E
OMP_SYSLOG_START	400001	Starting	OMP process is starting	E

PIM: Protocol-Independent Multicast Process

Priority: Informational

Message	Number	Message Format	Description	Action
IGMP_SYSLOG_END	1900001	Terminating	PIM process is ending	E
IGMP_SYSLOG_START	1999999	Starting	PIM process is starting	E

Priority: Notice

Message	Number	Message Format	Description	Action
PIM_SYSLOG_IF_STATE_CHANGE	1900003	VPN %lu Interface %s %s	In specified VPN, interface state changed to up or down	E
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s state changed to up	PIM neighbor came up	E
PIM_SYSLOG_TUNNEL_STATE_CHANGE	1900004	Tunnel %s state changed to %s	Tunnel used for PIM when down or came up	E

Priority: Error

Message	Number	Message Format	Description	Action
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s stated changed to down	PIM neighbor went down	E

POLICY: Policy Process

Unused Messages

Message	Number	Message Format	Description	Action
POLICY_SYSLOG_END	799999	Terminating policy	Policy process is ending	E
POLICY_SYSLOG_START	700001	Starting policy	Policy process is starting	E

RESOLV: Resolver Process

Unused Messages

Message	Number	Message Format	Description	Action
RESOLV_SYSLOG_END	2000001	Terminating resolver	Resolver process is ending	E
RESOLV_SYSLOG_START	2099999	Starting resolver	Resolver process is starting	E

SNMP Listener Process

Unused Messages

Message	Number	Message Format	Description	Action
SNMP_SYSLOG_END	2100001	Terminating SNMP listener	SNMP listener process is ending	E
SNMP_SYSLOG_START	2199999	Starting SNMP listener	SNMP listener process is starting	E

SYSMGR: System Manager Process

The system manager process (daemon) spawns, monitors, and terminates all the processes in the system, and it collects and logs vital system information, such as memory and CPU status.

Priority: Informational

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE1_INFO	200041	Generated authorized keys on %s, p_sysmgr->cfg.my_personality	Generated authorized keys for SSH-based login between the Cisco SD-WAN Manager server and the Cisco SD-WAN device	E
SYSMGR_CONFD_PHASE2_SUCCESS	200007	Confd Phase2 Up	Successful device bringup	E
SYSMGR_DAEMON_START	200017	Started daemon %s @ pid %d in vpn %lu,	System manager started process in VPN	E
SYSMGR_DAEMON_UP	200011	Daemon %s @ pid %d came up in vpn %lu (%d %d)	Daemon started by system manager came up as expected	E
SYSMGR_SIGTERM	200001	Received sigterm, stopping all daemons except confd	System manager received termination signal and will initiate termination of all processes	E
SYSMGR_VPN_DESTROY	200022	vpn %lu destroy. lookup returned %p	Stopping all processes in VPN	E

Priority: Notice

Message	Number	Message Format	Description	Action
SYSMGR_CLOCK_SET	200025	System clock set to %s	System clock set by user	E
SYSMGR_CONFD_CDB_NOT_INITED	200031	Confd db initialization not complete. Deleting cdb and starting afresh.	First-time initialization of configuration database	E

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE1_INFO	200041	Install successfully completed from %s to %s	Failed to read installation ID; will fall back to default	E
SYSMGR_CORE_FILE_COMPRESSED	200045	—	Core file was compressed	E
SYSMGR_DAEMON_EXIT_NORMAL	200021	—	A process terminated normally	E
SYSMGR_DAEMON_RESTARTED	200043	—	A process restarted	E
SYSMGR_DISK_ALERT_OFF	200036	Disk usage is below 60%%.	Disk usage is below threshold	E
SYSMGR_MEMORY_ALERT_OFF	200058	System memory usage is below 50%	System memory usage is below 50%	E
SYSMGR_MISC	200065	—	Miscellaneous message	E
SYSMGR_REBOOT	200038	System going down for a reboot.. (%s), reason	System manager initiating a device reboot, possibly because of a process failure	E
SYSMGR_SHM_FAIL	200042	Created shared memory %s	Successfully initialized shared memory for communication with other processes	E
SYSMGR_SHUTDOWN	200040	System shutting down.. (%s), reason	System manager is powering down the device; device will not come back up unless it is physically power-cycled	A
SYSMGR_SYSTEM_GREEN	200050	System up with software version %s	System status is green, indicating that all processes came up as expected	E

Message	Number	Message Format	Description	Action
SYSMGR_SYSTEM_RED	200051	System status red (software version '%s')	System status is red, possibly because of a process failure	A
SYSMGR_SYSTEM_START	200002	Starting system with Cisco SD-WAN software version %s	System has stated; usually one of the first messages during device bringup	E
SYSMGR_TIMEZONE_SET	200028	System timezone changed from %s to %s	System timezone changed as result of configuration change	E
SYSMGR_UPGRADE_AUTO_CONFIRMED	200063	—	A software upgrade was automatically confirmed	E
SYSMGR_UPGRADE_NOT_CONFIRMED	200049	—	A software upgrade was as not confirmed	E
SYSMGR_UPGRADE_PENDING_CONFIRMATION	200059	—	A software upgrade is pending confirmation	E
SYSMGR_VDEBUG_LOG_CLEANUP_NEEDED	200066	Debug logs exceed expected storage quota. Performing age-based cleanup to restore debug logging operations.	Debug logs were deleted to create space	A
SYSMGR_DAEMON_TERMINATED	200020	—	A process terminated	E
SYSMGR_WATCHDOG_EXPIRED	200062	—	The watchdog process expired	A

Priority: Warning

Message	Number	Message Format	Description	Action
SYSMGR_CORE_FILE_DELETED	200044	—	Core file was deleted	A
SYSMGR_DAEMON_RESTART_ABORTED	200060	—	The restarting of a process was terminated.	A
SYSMGR_DAEMON_STOP	200018	Stopping daemon %s @ pid %d. Sending signal %d	System manager stopped a daemon	E
SYSMGR_DISK_ALERT_ORANGE	200054	Disk usage is above 75%%. Please clean up unnecessary files.	Disk usage is above 75%	E
SYSMGR_DISK_ALERT_YELLOW	200035	Disk usage is above 60%%. Please clean up unnecessary files.	Disk usage is above 60%	E
SYSMGR_FILE_DELETED	200064	Deleted file %s (size %lu MB) to recover disk space	File deleted to free up disk space	A
SYSMGR_MEMORY_ALERT_ORANGE	200056	System memory usage is above 75%%	System memory usage is above 75%	E
SYSMGR_MEMORY_ALERT_YELLOW	200057	System memory usage is above 60%%	System memory usage is above 60%	E

Priority: Error

Message	Number	Message Format	Description	Action
SYSMGR_BAUD_RATE_SET	200046	Console baud rate changed to '%d', baud_rate	Console baud rate changed	E
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in OS to '%d'	Failed to set user-specified console baud rate in Linus	A
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in U-boot to '%d'	Failed to set user-specified console baud rate in Uboot	A
SYSMGR_CLOCK_SET_FAIL	200026	Cannot set system clock to %s	Failed to set system clock to time specified by user	A

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_CDB_INIT_OPEN_FAIL	200030	Failed to open cdb init file (%s)	Failed to open the configuration database	A
SYSMGR_DAEMON_EXIT_FAIL	200023	—	A process could not terminate	A
SYSMGR_CONFD_DATACB_REGISTER_FAIL	200010	Failed to register data cb	Failed to register data callback function with confd; device may reboot	A
SYSMGR_CONFD_CDB_DEL_FAIL	200032	Failed to remove cbd directory '%s'	Failed to reinitialize configuration database to recover from failure	AE
SYSMGR_CONFD_FORK_FAILURE	200003	Cannot move confd to phase2 (err %s)	Failed to move confd to Phase 2; device will reboot soon	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate archive keys	Failed to generate keys required for archiving configuration	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate authorized keys on %s, p_sysmgr->cfg.my_personality	Failed to generate keys required for SSH-based login between the Cisco SD-WAN Manager server and the Cisco SD-WAN device	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate SSH keys for archive	Failed to generate SSH keys	E

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get install id from file, using 00_00	Failed to read previous system version	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get previous version, using 0.0	Failed to read system version	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to transition confd to phase1. Re-initializing CDB..	Confd module failed to move to Phase 1, indicating a possible configuration database failure; device will reboot soon	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Verified that archive keys exist	Verified that configuration archive keys exist	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to get current version, using 0.0	Failed to read system version file	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to open %s, version_file	Failed to open system version file	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to read %s, version_file	Failed to read system version file	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to transition confd to phase2	Confd module failed to move to Phase 2, indicating a possible configuration database failure; device will reboot soon	A

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_REPLY_FAIL	200009	Failed to send oper data reply - %s (%d)	Failed to reply to confd; some **show** commands may not work	A
SYSMGR_CONFD_SETPGID_FAILURE	200004	setpgid(0,0) failed: %d	Process group failed to start	A
SYSMGR_DAEMON_DOWN	200012	Daemon %s [%u] went down in vpn %lu,	Process started by system manager went down	A
SYSMGR_DAEMON_EXECV_FAILURE	200016	execv %s failed	Internal failure occurred while starting a process	A
SYSMGR_DAEMON_FORK_FAILURE	200014	Cannot start daemon %s: %s	Internal failure occurred while starting a process	A
SYSMGR_DAEMON_INACTIVE	200033	Daemon %s[%lu] @ pid %d died. Rebooting device..	System manager detected a process failure and is about to reboot the device	A
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to daemon %s. err %d	Failed to establish message queue with process; device may reboot soon	A
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to quagga daemon %s. err %d	Failed to establish message queue with routing process; device may reboot soon	A

Message	Number	Message Format	Description	Action
SYSMGR_DAEMON_SETAFFINITY_FAILURE	200061	—	The scheduling of a process failed	E
SYSMGR_DAEMON_SETPGID_FAILURE	200015	setpgid(0,0) failed	Internal failure setting process group of a process	A
SYSMGR_DAEMON_STOPPED	200019	Daemon %s @ pid %u terminated - %s	Daemon started by system manager terminated; device may reboot soon (except for the Cisco Catalyst SD-WAN Validator)	A
SYSMGR_RTC_CLOCK_SET_FAIL	200027	Cannot set hardware clock to %s - %s (errno	Failed to update hardware clock to system time specified by user	A
SYSMGR_SHM_FAIL	200042	Failed to close shared memory %s with an error %d	Failed to completely and properly close the shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to map shared memory %s	Failed to initialize shared memory for communication with other processes	E

Message	Number	Message Format	Description	Action
SYSMGR_SHM_FAIL	200042	Failed to open shared memory %s with an error %d	Failed to open shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to truncate shared memory %s with an error %d	Failed to initialize shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to unmap shared memory %s	Failed to completely and properly close shared memory for communication with other processes	E
SYSMGR_SWITCHBACK_FAILED	200053	Software upgrade to version %s failed because of %s	Software upgrade failed	A
SYSMGR_TIMEZONE_SET_FAIL	200029	Failed to set system timezone to %s (rc = %d)	Failed to set system timezone to timezone specified by user	A
SYSMGR_TRACE_ERROR	200024	—	A trace error occurred	A

Priority: Critical

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_INIT_FAIL	200008	Sysmgr child in charge of migrating confd/ncs to phase2 exited with error code %d	System manager detected a confd process failure; device may reboot	AE
SYSMGR_DISK_ALERT_RED	200034	Disk usage is above 90%% (critically high). Please clean up unnecessary files.	Disk usage is above 90%	AE

Message	Number	Message Format	Description	Action
SYSMGR_MEMORY_ALERT_RED	200055	System memory usage is above 90%% (critically high)	System memory usage is above 90%	AE
SYSMGR_REBOOT_HALTED	200039	Reboot (reason: %s) terminated...too many reboots	System manager stopped short of rebooting the device because it detected too many reboots in a short period of time	AE
SYSMGR_UPGRADE_FAILED	200052	Software upgrade to version %s failed because of reason	Software upgrade failed	AE

TCPD: TCP Options Process

Priority: Informational

Message	Number	Message Format	Description	Action
TCPD_MSGQ_SERVER	2800002	Server Exception: %s	Proxy server did not accept connection	E
TCPD_PROXY	2800004	Enabled TCP_OPT for vpn %lu: %s:%u %s Starting sysmgr_app object tcpd<->ftmd channel established tcpd<->ftmd = Will try connecting	Messages related to starting a proxy	E
TCPD_PROXY	2800004	tcpd error counters -%s	Count of TCP option errors	E
TCPD_SYSLOG_END	2800001	Terminating TCP options	TCP options process ending	E
TCPD_SYSLOG_START	2899999	Starting TCP options	TCP options process starting	E
TCPD_SYSMGR_APP	2800003	%s Exception: %s %s - Sysmgr app::connect -Exception - %s	Messages related to the connection between the system manager and the TCP proxy process	E

Priority: Debug

Message	Number	Message Format	Description	Action
TCPD_SYSMGR_APP	2800003	%s - Registering for send_hello-msg %s: Sending following register msg Sending msg of length %u %s - Sysmgr app::connect %s - Write %u bytes %s - Wrote register msg %u	Messages related to the connection between the system manager and the TCP proxy process	E

TRACKER: Interface Tracker Process

Priority: Informational

Message	Number	Message Format	Description	Action
TRACKER_SYSLOG_CONN_DOWN	1700003	Connection to %s %s Down	Connection to interface is down	E
TRACKER_SYSLOG_CONN_UP	1700002	Connection to %s %s Up	Connection to interface is up	E
TRACKER_SYSLOG_END	1700001	Terminating	Interface tracker process is ending	E
TRACKER_SYSLOG_START	1799999	Starting	Interface tracker process is starting	E

VCONFD: Cisco Catalyst SD-WAN Configuration Process

Priority: Informational

Message	Number	Message Format	Description	Action
VCONFD_SYSLOG_END	1400001	Terminating	Configuration process is ending	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s process name: %s process id: %s reason: %s	Configuration at specified date and time for a process, with reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s status: %s install id: %s message %s	Configuration at specified date and time, with specified status (minor, major)	E

Message	Number	Message Format	Description	Action
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reason: %s	Configuration at specified date and time, with reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reboot reason: %s	Configuration at specified date and time, with reboot reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s username: %s remote host: %s	Configuration at specified date and time, for username and remote host	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s vpn id: %s if name: %s mac addr: %s ip-addr:%s	Configuration at specified date and time, for VPN, interface, MAC address, and IP address	E
VCONFD_SYSLOG_START	1499999	Starting	Configuration process is starting	E

VDAEMON: Cisco Catalyst SD-WAN Software Process

Priority: Informational

Message	Number	Message Format	Description	Action
VDAEMON_SYSLOG_DOMAIN_ID_CHANGE	500006	System Domain-ID changed from '%d' to '%d',	System domain ID changed	E
VDAEMON_SYSLOG_END	599999	—	Process ending	E
VDAEMON_SYSLOG_ORG_NAME_CHANGE	500008	System Organization-Name changed from '%s' to '%s'	System organization name changed	E
VDAEMON_SYSLOG_PEER_STATE	500003	Peer %s Public-TLOC %s Color %u %s,	Peer state changed to up or down	E
VDAEMON_SYSLOG_SITE_ID_CHANGE	500005	System Site-ID changed from '%d' to '%d'	System site ID changed	E

Message	Number	Message Format	Description	Action
VDAEMON_SYSLOG_START	500001	—	Process starting	E
VDAEMON_SYSLOG_SYSTEM_IP_CHANGE	500007	System-IP changed from '%s' to '%s'	System IP address changed	E

Priority: Error

Message	Number	Message Format	Description	Action
VDAEMON_BOARD_ID_CHALLENGE_FAILED	500002	—	Board ID could not be verified	E
VDAEMON_BOARD_ID_INIT_FAILED	500001	—	Board initialization failed because board ID could not be verified	E
VDAEMON_SYSLOG_CERT_STORE_FAIL	500009	Certificate store init failed	Certificate not stored	AE
VDAEMON_SYSLOG_PEER_AUTH_FAIL	500004	Peer %s Public-TLOC %s Color %u %s	Authentication with a vdaemon peer failed	E
VDAEMON_SYSLOG_PEER_STATE	500003	Failed to read system host name	Internal error reading system hostname; device will not register with the Cisco SD-WAN Manager server or ZTP will fail	A

VRRP: Virtual Router Redundancy Protocol

The VRRP process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
VRRPD_STATE_CHANGE	600002	Group %d, interface %s, vpn %lu state changed to %s	VRRP interface state change	E
VRRPD_SYSLOG_END	699999	Terminating VRRPD	VRRP process is ending	E
VRRPD_SYSLOG_START	600001	Starting VRRPD	VRRP process is starting	E

WLAN: Wireless LAN Process

The wireless LAN process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
WLAN_SYSLOG_END	2300001	Terminating wlan	WLAN process is ending	E
WLAN_SYSLOG_START	2399999	Starting wlan	WLAN process is starting	E

WWAND: Cellular Process

The wireless WAN process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_ADMIN_DWL	2400010	Cellular%d interface is set for deletion	Cellular interface is about to be deleted	E
WWAN_SYSLOG_ADMIN_DOWN	2400009	Cellular%d interface is set to admin down	Cellular interface is administratively Down	E
WWAN_SYSLOG_ADMIN_UP	2400008	Cellular%d interface is set to admin up	Cellular interface is administratively Up	E
WWAN_SYSLOG_CONNECT	2400002	Connected to Cellular%d modem	Connection to cellular modem established	E
WWAN_SYSLOG_CONNECT_DATA	2400006	—	—	E
WWAN_SYSLOG_DATA_MONITOR	2400032	Info: %lld bytes left Info: exceeded by %lld bytes	Information about amount of data remaining in billing cycle	E
WWAN_SYSLOG_DATA_SESSION	2400019	Data session started successfully	Data session on cellular interface started successfully	E
WWAN_SYSLOG_DATA_SESSION_BEARER	2400028	Data bearer changed to %s (%lx)	Data carrier changed	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_DATA_SESSION_DISCONNECT	2400023	Data session disconnect: restarting session	Data session was disconnected and is restarting	E
WWAN_SYSLOG_DATA_SESSION_DISC_REASON	2400024	Data session disconnect reason: %s	Reason data session was disconnected	E
WWAN_SYSLOG_DATA_SESSION_DISC_VERB	2400025	Data session disconnect reason verbose: %s	More information about why data session disconnected	E
WWAN_SYSLOG_DATA_SESSION_DOMAIN	2400026	Packet-switched domain state change to %s: registration: %s ran: %s if: %s	Packet-switched domain changed	E
WWAN_SYSLOG_DATA_SESSION_DORMANCY	2400029	Dormancy state changed to %s	Session dormancy state changed	E
WWAN_SYSLOG_DATA_SESSION_NETWORK	2400027	Network registration changed to %s: domain: %s ran: %s if: %s	Network registration changed	E
WWAN_SYSLOG_DATA_SESSION_START	2400018	Starting data session on Cellular%e	Data session on cellular interface is starting	E
WWAN_SYSLOG_DATA_SESSION_STATE	2400020	Data session state changed to %s	Data session status	E
WWAN_SYSLOG_DATA_SESSION_STOP	2400022	Data session stopped successfully	Data session stopped	E
WWAN_SYSLOG_DISCONNECT	2400003	Disconnected LTE modem %d	Disconnection from LTE modem	E
WWAN_SYSLOG_END	2400001	Terminating WWAND	Ending WWAN process	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_FIRMWARE	2400007	Failed to get firmware details after upgrade on modem %d Firmware upgrade failed on modem %d Firmware upgrade successful on modem %d Upgrading firmware configuration on modem %d Upgrading firmware image on modem %d	Messages related to firmware upgrade on the cellular modem	E
WWAN_SYSLOG_LR_DOWN	2400012	%s%d: bringing down	Last-resort interface is shutting down	E
WWAN_SYSLOG_LR_UP	2400011	%s%d: bringing up	Last-resort interface is starting	E
WWAN_SYSLOG_MODEM_ACTIVATION	2400039	Modem activation status: %s (%lu)	Modem actual state and status	E
WWAN_SYSLOG_MODEM_PMODE	2400017	Modem is not in online mode Modem is not in online mode (tmp: %s degrees C) Modem power state is: %s (prev: %s) Modem set to %s (prev: %s) Powered off the modem %d	Messages related to modem power mode status	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_MODEM_STATE	2400034	Modem device state changed to %s	Modem state changed	E
WWAN_SYSLOG_MODEM_TEMP	2400037	Modem temperature %d degree C: %s	Modem temperature and state	E
WWAN_SYSLOG_MODEM_UP	2400035	WWAN cellular%d modem is back up	Modem reconnected	E
WWAN_SYSLOG_OMA_DM_DONE	2400041	Modem OMA DM configuration completed	Modem OMA-DM configuration finished	E
WWAN_SYSLOG_OPER_DOWN	2400014	Cellular%d set if down	Cellular interface is operationally Down	E
WWAN_SYSLOG_OPER_UP	2400013	Cellular%d set if up	Cellular interface is operationally Up	E
WWAN_SYSLOG_PROFILE_CHECK	2400030	Profile %lu with PDP: %s APN: %s Auth: %s User: %s	Cellular profile information	E
WWAN_SYSLOG_REBOOT	2400040	Cellular%d modem mode updated: rebooting; %s reason	Reason why celluar modem rebooted	E
WWAN_SYSLOG_SDK_DOWN	2400005	SDK got terminated: %s	Connection to software development kit terminated	E
WWAN_SYSLOG_SDK_UP	2400004	Connected to Cellular%d sdk process	Connection to cellular software development kit established	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_SIM_STATUS	2400033	SIM status changed to: %s	SIM status changed	E
WWAN_SYSLOG_START	2499999	Starting WWAND	Starting WWAN process	E
WWAN_SYSLOG_TRACK_GW_UP	2400015	Cellular%d gateway %s is reachable	Cellular gateway is reachable	E

Priority: Error

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_AUTO_PROFILE_MISS	2400031	Manually configure APN profile for the data connection	Data session could not start because required APN could not be located	E
WWAN_SYSLOG_MODEM_DOWN	2400036	WWAN cellular%d modem went down	Modem is disconnected	E
WWAN_SYSLOG_MODEM_RESET	2400038	Failed to recover Cellular %d modem	Connection to modem could not be reestablished	E
WWAN_SYSLOG_TRACK_GW_DOWN	2400016	Cellular%d gateway %s is not reachable	Cellular gateway is not reachable	E

UTD Syslogs

The tables below list the syslog messages generated by the following United Threat Defense (UTD) features:

Intrusion Prevention System/Intrusion Detection System

Message	Message Format	Description	Action
IPS Activity	<DATE-TIMESTAMP> [**] [Hostname: <SYSTEM_HOSTNAME>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] <ACTION> [**] [1:21475:4] <DESCRIPTION> [**] [Classification: <CLASSIFICATION_TYPE>] [Priority: <PRIORITY_VALUE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>:<SOURCE_PORT_NUM> -> <DESTINATION_IP_ADDR>:<DEST_PORT_NUM>	Based on classification the IPS alert or drop action is done which is indicated in the log message.	Alert / Drop

URL Filtering

Message	Message Format	Action
UTD WebFilter Whitelist	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Pass [**] UTD WebFilter Whitelist [**] [URL: <URL>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Pass
UTD WebFilter Blacklist	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Drop [**] UTD WebFilter Blacklist [**] [URL: <URL>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Drop
UTD WebFilter Category/Reputation	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: <URL>] ** [Category: <CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Drop

TLS Decryption

Message	Message Format	Action
UTD TLS Decryption Whitelist	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Never-Decrypt [**] UTD TLS Decryption Whitelist [**] [URL: <URL>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Never-Decrypt
UTD TLS Decryption Graylist	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Skip-Decrypt [**] UTD TLS Decryption Graylist [**] [URL: <URL>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Skip-Decrypt
UTD TLS Decryption Blacklist	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Decrypt [**] UTD TLS Decryption Blacklist [**] [URL: <URL>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Decrypt

Message	Message Format	Action
UTD TLS Decryption Category Never-Decrypt	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Never-Decrypt [**] UTD TLS Decryption Category Never-Decrypt [**] [URL: <URL>] ** [Category: <SSL_CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Never-Decrypt
UTD TLS Decryption Reputation Decrypt	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Decrypt [**] UTD TLS Decryption Reputation Decrypt [**] [URL: <URL>] ** [Category: <SSL_CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Decrypt
UTD TLS Decryption Reputation Skip-Decrypt	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Skip-Decrypt [**] UTD TLS Decryption Reputation Skip-Decrypt [**] [URL: <URL>] ** [Category: <SSL_CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Skip-Decrypt
UTD TLS Decryption Category Decrypt	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Decrypt [**] UTD TLS Decryption Category Decrypt [**] [URL: <URL>] ** [Category: <SSL_CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Decrypt
UTD TLS Decryption Category Skip-Decrypt	<DATE-TIMESTAMP> [**] [Hostname: <HOSTNAME_VALUE>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <ID_NUM>] [**] Skip-Decrypt [**] UTD TLS Decryption Category Skip-Decrypt [**] [URL: <URL>] ** [Category: <SSL_CATEGORY_NAME>] ** [Reputation: <REP_SCORE>] [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR> -> <DESTINATION_IP_ADDR>:<PORT_NUM>	Skip-Decrypt

AMP File Inspection

Message	Message Format	Action
Clean File Signature	<DATE-TIMESTAMP> [**] [Hostname: <SYSTEM_HOSTNAME>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <instance_id>] [**] Allow [**] UTD AMP DISPOSITION CLEAN [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE> [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>:<PORT_NUM> -> <DESTINATION_IP_ADDR>: <PORT_NUM>	Allow

Message	Message Format	Action
Unknown File Signature	<DATE-TIMESTAMP> [**] [Hostname: <SYSTEM_HOSTNAME>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <instance_id>] [**] Allow [**] UTD AMP DISPOSITION UNKNOWN [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE> [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>:<PORT_NUM> -> <DESTINATION_IP_ADDR>: <PORT_NUM>	Allow
Malicious File Signature	<DATE-TIMESTAMP> [**] [Hostname: <SYSTEM_HOSTNAME>] [**] [System_IP: <SYSTEM_IP_ADDR>] [**] [Instance_ID: <instance_id>] [**] Allow [**] UTD AMP DISPOSITION MALICIOUS [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE> [VRF: <VRF_ID>] {<PROTOCOL>} <SOURCE_IP_ADDR>:<PORT_NUM> -> <DESTINATION_IP_ADDR>: <PORT_NUM>	Drop

Threatgrid

Message	Message Format	Action
Retro Clean	<DATE-TIMESTAMP> [**] Allow [**] UTD AMP RETRO CLEAN [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Allow
Retro Unknown	<DATE-TIMESTAMP> [**] Allow [**] UTD AMP RETRO UNKNOWN [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Allow
Retro Malicious	<DATE-TIMESTAMP> [**] Drop [**] UTD AMP RETRO MALICIOUS [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Drop
Retro Error	<DATE-TIMESTAMP> [**] Error [**] UTD AMP RETRO ERROR [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Error
File Upload Fail	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD FAILED [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Success	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD SUCCESS [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Not interesting	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD NOT INTERESTING [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Limit Reached	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD LIMIT REACHED [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown

Message	Message Format	Action
File Upload API Key Invalid	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD APIKEY INVALID [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Internal Error	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD INT ERROR [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload System Error	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD SYS ERROR [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Not Supported	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD NOT SUPPORTED [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown
File Upload Whitelisted	<DATE-TIMESTAMP> [**] Unknown [**] TG FILE UPLOAD WHITELISTED [**] SHA: <SHA_VALUE> Malware: None Filename: <FILENAME> Filetype: <FILETYPE>	Unknown

Permanent Alarms and Alarm Fields

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

Use the Alarms screen to display detailed information about alarms generated by control components and routers in the overlay network.

For more details, see Alarms section.