# Troubleshoot Cisco Catalyst SD-WAN Security

**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.



# 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 are the support articles associated with this technology:

| Document | Description |
|---|---|
| Install UTD Security Virtual Image on cEdge Routers | This document describes how to install Unified Threat Defense (UTD) Security Virtual Image to enable security features on Cisco IOS XE Catalyst SD-WAN Devices. |
| Configure Cisco Catalyst SD-WAN Zone-Based Firewall (ZBFW) and Route Leaking | This document describes how to configure, verify and troubleshoot Zone-Based Firewall (ZBFW) with Route-Leaking between Virtual Private Networks (VPN). |
| Configure Integration with Cisco Umbrella and Troubleshooting Common Problems | This document describes Cisco SD-WAN Manager/Cisco IOS® -XE SDWAN software part of the integration with the Cisco Umbrella DNS security solution. |
| Configure Cisco Catalyst SD-WAN Advanced Malware Protection (AMP) Integration and Troubleshoot | This document describes how to configure and troubleshoot the Cisco Catalyst SD-WAN Advanced Malware Protection (AMP) integration on a cEdge device with Cisco IOS® XE, as an integral part of the Cisco Catalyst SD-WAN edge security solution that aims visibility and protection for users at a branch from Malware. |
| Troubleshoot Datapath Handling by UTD and URL-Filtering | This document describes how to troubleshoot Unified Threat Defense (UTD) also known as Snort and Uniform Resource Locator (URL) Filtering on IOS® XE WAN Edges routers. |
| Collect an Admin-Tech in Cisco Catalyst SD-WAN Environment and Upload to TAC Case | This document describes how to initiate an `admin-tech` in a Cisco Catalyst SD-WAN environment. |
| Troubleshoot Cisco IOS XE Catalyst SD-WAN Router IPsec Anti-Replay Failures | This document describes the IPsec Anti-Replay behavior in SD-WAN IPsec for Cisco IOS XE SD-WAN routers and how to troubleshoot Anti-Replay issues. |
| Install and Uninstall UTD Engine in Cisco Catalyst SD-WAN with CLI | This document describes the procedure to install and uninstall Unified Threat Defense (UTD) via CLI in Cisco Catalyst SD-WAN routers. |
| SD-WAN Manager: How to Check and Verify Single Sign On | This document describes the basics in order to enable Single Sign On (SSO) on Cisco SD-WAN Manager and how to check/verify on Cisco SD-WAN Manager, when this feature is enabled |
| Configure OKTA Single Sign-On (SSO) on Cisco Catalyst SD-WAN | This document describes how to integrate OKTA Single Sign-On (SSO) on Cisco Catalyst SD-WAN. |
| Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios | This document describes how to configure Cisco Umbrella Secure Internet Gateway (SIG) tunnels with IPsec in both Active/Active and Active/Standby |
| Configure and Verify SD-WAN IPsec SIG Tunnel with Zscaler | This document describes the configuration steps and verification of SD-WAN IPsec SIG tunnels with Zscaler. |

| Document | Description |
|---|---|
| Understand SD-WAN and Traditional Tunnels SPI Recover Differences | This document describes how to recover SD-WAN and Third Party Tunnels from %RECVD_PKT_INV_SPI error. |
| Collect SAML-Trace and HAR File | This document describes how to initiate an **SAML-Trace** and **HAR File** in a Cisco Catalyst SD-WAN environment. |
| Configure Service Side IPSec Tunnel with a C8000V on Cisco Catalyst SD-WAN | This document describes how to configure an IPSec tunnel between a SD-WAN Cisco Edge Router and a VPN Endpoint with service VRF. |

# 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.