Cisco Security Cloud Control: Catalyst SD-WAN Integration Guide

Cisco Security Cloud Control
Updated NaN,

© 2025-2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

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)

Topics included

1 Security Cloud Control Firewall Management.....5
Overview of Security Cloud Control Firewall Management.....6
Security Cloud Control Firewall Management licenses.....6
Security Cloud Control Firewall Management Platform Maintenance Schedule.....7

2 Integrate Catalyst SD-WAN Manager with Security Cloud Control.....9
Overview of Catalyst SD-WAN integration with Security Cloud Control Firewall Management.....10
System topology diagram 10
End-to-end workflow to manage Catalyst SD-WAN Manager using Security Cloud Control.....12
Minimum software requirements.....13
Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager.....13
Onboard Catalyst SD-WAN Manager to Security Cloud Control.....14
Deboard Catalyst SD-WAN Manager from Security Cloud Control.....16
How Security Cloud Control Firewall Management manages Catalyst SD-WAN NGFW capabilities.....17
View intrusion events.....19
View malware events.....20
Additional resources.....20

3 Manage Catalyst SD-WAN Devices.....21
Overview of Catalyst SD-WAN devices.....22
Supported operations on Catalyst SD-WAN devices.....22
View configuration of Catalyst SD-WAN devices.....22
Cross-launch policy groups from Security Cloud Control Firewall Management.....23

4 Manage Catalyst SD-WAN Security Objects and Security Profiles.....25
Overview of Catalyst SD-WAN security objects and security profiles.....26
Create new Catalyst SD-WAN security objects and security profiles.....26
Application List.....27
Data Prefix.....28
FQDN.....28
Geolocation.....28
Identity.....28
Port.....29
Protocol.....29
Security Group Tag.....29
IPS Signature.....30
Allow URL.....30

Block URL....31
Zone....31
Advanced Inspection Profile....31
Advanced Malware Protection....32
Intrusion Prevention....33
TLS/SSL Decryption....33
TLS/SSL Profile....35
URL Filtering....35
Modify Catalyst SD-WAN security objects and security profiles....36
Delete Catalyst SD-WAN security objects....37
Filter Catalyst SD-WAN security objects....38

5 Manage Catalyst SD-WAN Security Policies....41
An introduction to Catalyst SD-WAN NGFW security policies....42
Manage existing Catalyst SD-WAN NGFW security policies....42
Create Catalyst SD-WAN security policies....42
Associate a policy group to Catalyst SD-WAN NGFW policy....47
Deploy policy group from Catalyst SD-WAN Manager....48

6 Cisco Security Analytics and Logging....49
About Security Analytics and Logging (SaaS) in Security Cloud Control....50
Event types in Security Cloud Control....50
Deprovisioning Cisco Security Analytics and Logging (SaaS)....50
Security Analytics and Logging licenses....51
Subscribing to a Security Analytics and Logging license....52
View Security Analytics and Logging license information....54
View Security Analytics and Logging Storage usage and event ingest rate....54
Monitor Security Analytics and Logging service availability....56
Extend event storage duration and increase event storage capacity....57
View Security Analytics and Logging alerts....57
Frequently asked questions about Security Analytics and Logging license....58
Security Analytics and Logging for Catalyst SD-WAN....59
How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management....59
Requirements and guidelines for SD-WAN integration....61
View Catalyst SD-WAN events in Security Cloud Control Firewall Management....61

1 Security Cloud Control Firewall Management

Topics:

- Overview of Security Cloud Control Firewall Management
- Security Cloud Control Firewall Management licenses
- Security Cloud Control Firewall Management Platform Maintenance Schedule

This document guides users through setting up and managing firewalls, customizing dashboards for monitoring security events, and staying informed about new features and updates within Security Cloud Control.

Overview of Security Cloud Control Firewall Management

An overview of Security Cloud Control Firewall Management for managing firewall devices, policies, objects, and configuration consistency.

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator or CDO) is a cloud-based security policy manager that helps simplify and unify security policies across your Cisco firewalls and other devices such as Cisco IOS and SSH. The firewalls and devices can be managed from **Firewall**, which is listed under **Products** in the Security Cloud Control dashboard.

Security Cloud Control Firewall Management helps you optimize your security policies by identifying inconsistencies within them and by providing with the tools to fix them. It provides you with ways to share objects and policies, as well as create configuration templates, to promote policy consistency across devices.

Because Security Cloud Control Firewall Management coexists with Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by ASDM and reconciles the differences.

You can manage a wide range of devices in one place. Advanced users will also find their traditional CLI interface with some new enhancements to make management even more efficient for them.

Security Cloud Control Firewall Management also provides a guided "Day 0" experience, helping you to quickly onboard Threat Defense devices to your on-premises or Cloud-Delivered Firewall Management Center. It also presents you with other key features that you may benefit from and helps you enable and configure them.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the Cisco Online Privacy Statement carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Security Cloud Control Firewall Management licenses

Security Cloud Control Firewall Management requires a base subscription and device licenses to manage firewalls and supported devices. Choose term-based plans to match your deployment needs, access software updates, and receive Cisco TAC support. Catalyst SD-WAN doesn't require an additional license; customers using Cisco Digital Network Architecture (DNA) or WAN Essentials license can integrate with Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control Firewall Management base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription provides you with a Security Cloud Control Firewall Management organization. For every device you choose to manage using Security Cloud Control Firewall Management, you need separate device licenses.

To onboard and manage devices from Security Cloud Control Firewall Management, you must purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base**: Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control Firewall Management organization and onboard adequately licensed devices.
- **Device License**: Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control Firewall Management for three years if you purchase a three-year software subscription for the Cisco Firepower 1010 device.

When managing your firewalls with Security Cloud Control Firewall Management, you can combine Security Analytics and Logging with your Security Cloud Control Firewall Management subscription, or you can obtain Security Analytics and Logging entitlement as a separate subscription. For more information about Security Analytics and Logging subscriptions, see Security Analytics and Logging licenses on page 51.

Important

You do not require two separate device licenses to manage a high-availability device pair in Security Cloud Control Firewall Management. If you have a high-availability pair, purchasing one device license is sufficient because Security Cloud Control Firewall Management considers the pair of high-availability devices as one single device.

Note

- Catalyst SD-WAN does not require an additional license for integration with Security Cloud Control Firewall Management. Customers with Cisco Digital Network Architecture (DNA) or WAN Essentials licenses can use these existing licenses for integration without needing any other license.
- Customers with Cisco Digital Network Architecture (DNA) Essentials or Advantage, as well as WAN Essentials or Advantage licenses, can use these existing licenses for integration without needing any other license. However, to access Security Analytics and Logging, a DNA Advantage (or WAN Advantage) license is required along with a separate Security Analytics and Logging license.

Note

You cannot manage Security Cloud Control Firewall Management licensing through the Cisco Smart Licensing portal.

Software Subscription Support

The Security Cloud Control Firewall Management base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC) at no extra cost. While software support is selected by default, you can also leverage Security Cloud Control Firewall Management solution support based on your requirement.

Security Cloud Control Firewall Management Platform Maintenance Schedule

Security Cloud Control Firewall Management receives weekly platform updates every Thursday from 09:00 to 12:00 UTC, delivering new features and quality improvements. Access remains available during maintenance, but avoid deploying configuration changes to ensure uninterrupted policy enforcement and stable device management.

Security Cloud Control Firewall Management updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

Day of the week	Time of day (24-hour time, UTC)
Thursday	09:00 UTC - 12:00 UTC

During the Security Cloud Control Firewall Management upgrade period, you can still access your organization and the Cloud-Delivered Firewall Management Center. Additionally, the devices that you have onboarded to Security Cloud Control Firewall Management continue to enforce their security policies.

Note

- During the maintenance period of the Security Cloud Control Firewall Management, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control Firewall Management from communicating, Cisco addresses that issue in all the affected tenants as quickly as possible, even if it is outside the maintenance window.

2 Integrate Catalyst SD-WAN Manager with Security Cloud Control

Topics:

- Overview of Catalyst SD-WAN integration with Security Cloud Control Firewall Management
- System topology diagram
- End-to-end workflow to manage Catalyst SD-WAN Manager using Security Cloud Control
- Minimum software requirements
- Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager
- Onboard Catalyst SD-WAN Manager to Security Cloud Control
- Deboard Catalyst SD-WAN Manager from Security Cloud Control
- How Security Cloud Control Firewall Management manages Catalyst SD-WAN NGFW capabilities
- View intrusion events
- View malware events
- Additional resources

This chapter explains the integration of Catalyst SD-WAN Manager with Security Cloud Control.

Overview of Catalyst SD-WAN integration with Security Cloud Control Firewall Management

The integration of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager enables efficient configuration, monitoring, and enforcement of security policies, advanced threat detection, log analysis, and AI-driven troubleshooting.

You can use Cisco SD-WAN solutions, including the Catalyst and Secure Router series, with Cisco security portfolio to control and manage network security features.

The integration of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager provides centralized management for Cisco Catalyst SD-WAN and Branch WAN environments. This enables organizations to configure, monitor, and enforce security policies across their networks. It also facilitates advanced troubleshooting, rule optimization, and change management on Catalyst SD-WAN Manager.

Benefits

This integration allows you to:

- Efficiently manage security policies and objects, configure and edit them, and push changes using the Security Cloud Control Firewall Management dashboard.
- Effective monitoring and detection of security threats from a centralized Security Cloud Control Firewall Management dashboard.
- Analyze security threats from logs and events in the Security Cloud Control Firewall Management dashboard with data sent from Security Analytics and Logging.

Security Cloud Control Firewall Management provides these capabilities:

- Identifies existing security configurations and policies through the onboarded Catalyst SD-WAN Manager.
- Enables the creation of new security objects and policies using its platform.
- Supports a cohesive strategy for implementing security objects, policies, and profiles across multiple Cisco solutions.
- Offers capabilities for viewing logs and analytics data.
- Displays intrusion and malware events detected within the network from Secure Router.

System topology diagram

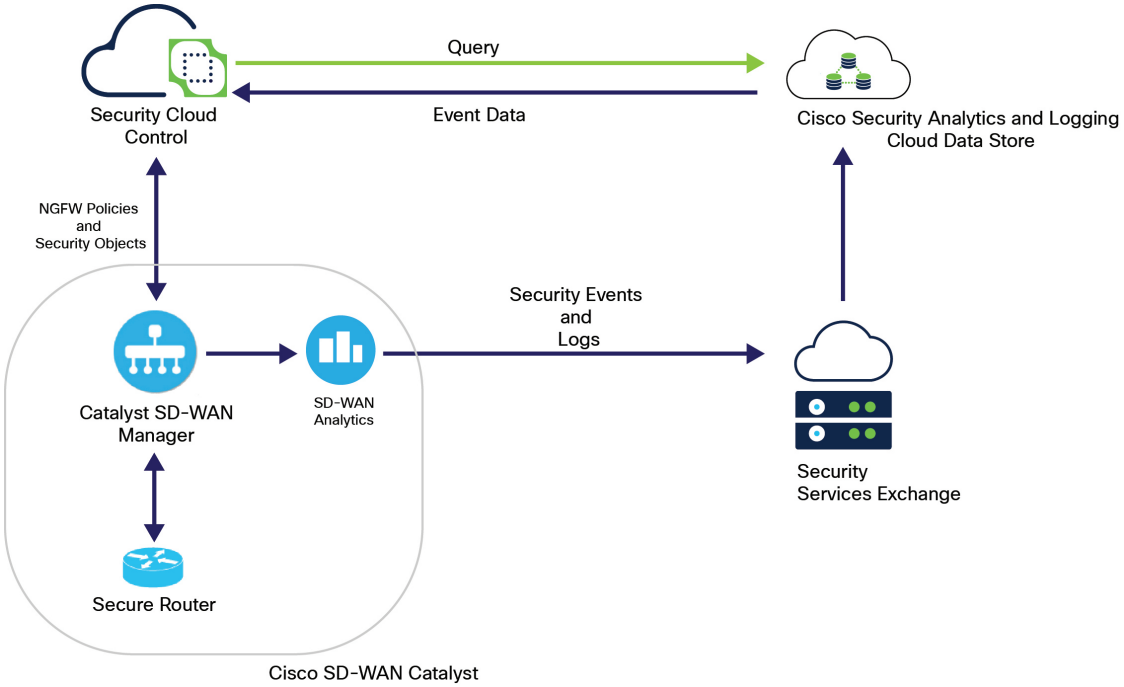
Topology diagram illustrates the integration of Catalyst SD-WAN with Security Cloud Control Firewall Management and other cloud services. It shows the flow of information and interactions between various components.

The primary use case for managing the Next-Generation Firewall (NGFW) capabilities of Catalyst SD-WAN through Security Cloud Control Firewall Management is to streamline and centralize security management across Cisco's security products.

The topology diagram illustrates the integration of Catalyst SD-WAN with Security Cloud Control Firewall Management and other cloud services. The diagram shows the flow of information and interactions between various components.

Note

The Cisco Catalyst 8000 and Secure 8000 devices are collectively referred to as the 'Secure Router' hereafter.



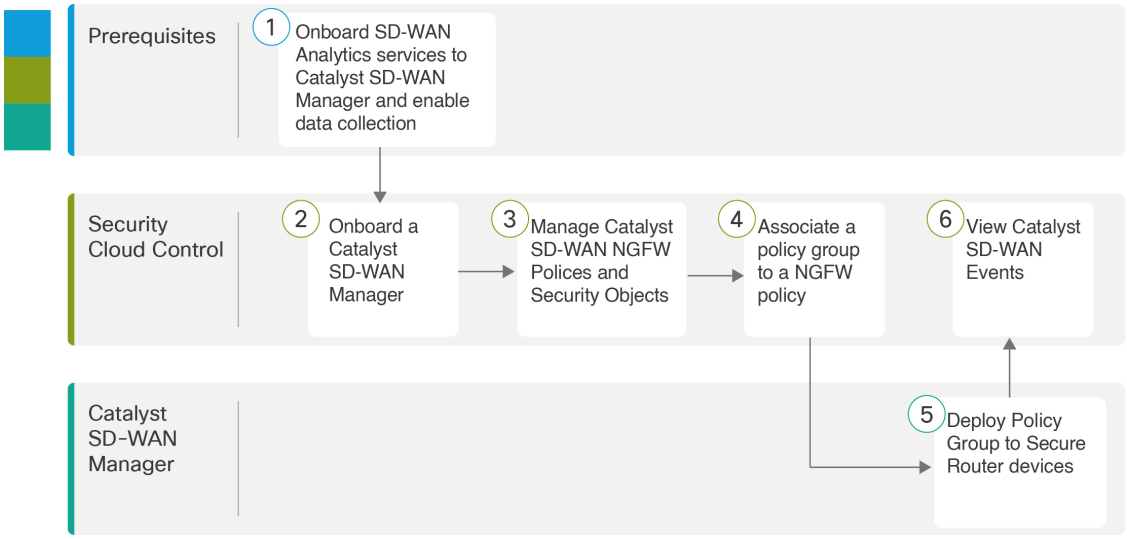
- **Security Cloud Control**: A central point for security policy enforcement and event correlation. It reads Next-Generation Firewall (NGFW) policies and security objects from the onboarded Catalyst SD-WAN Manager and allows customers to modify these NGFW configurations. It also sends queries to Cisco Security Analytics and Logging cloud data store for events.
- **Cisco Catalyst SD-WAN** consists of:
  - **Catalyst SD-WAN Manager:** Manages the SD-WAN fabric and displays NGFW policies and security objects in Security Cloud Control when onboarded to it. Catalyst SD-WAN Manager sends the event data received from Secure Router to **SD-WAN Analytics**.
  - **SD-WAN Analytics**: Provides analytics data to the Security Services Exchange.
  - **Secure Router:** The SD-WAN edge device.
- **Cisco Security Analytics and Logging Cloud Data Store**: A cloud-based repository for security analytics and logging data. It receives security events and logs from **Security Services Exchange**, which obtains the analytics data from SD-WAN Analytics engine.
- **Security Services Exchange**: A cloud-based platform designed to facilitate the integration, communication, and management of various Cisco security services. It sends security events and logs received from the SD-WAN environment and forwards them to the Cisco Security Analytics and Logging Cloud data store.

End-to-end workflow to manage Catalyst SD-WAN Manager using Security Cloud Control

This concept explains the high-level end-to-end workflow for managing the firewall capabilities of Catalyst SD-WAN Manager using Security Cloud Control.

The integration of Catalyst SD-WAN Manager with Security Cloud Control Firewall Management enables you to manage Next-Generation Firewall (NGFW) capabilities through Security Cloud Control platform.

This flowchart illustrates the high-level workflow for managing the firewall capabilities of Catalyst SD-WAN Manager using Security Cloud Control.



Step	Application	Description
1	Prerequisites	Onboard your SD-WAN Analytics services to Catalyst SD-WAN Manager and enable data collection. For more information, see Onboard Cisco SD-WAN analytics.
2	Security Cloud Control	Onboard your Catalyst SD-WAN Manager. The onboarding process also imports your associated Secure Router routers. For more information, see Integrate Catalyst SD-WAN Manager with Security Cloud Control on page 9.
3	Security Cloud Control	Create, modify, or delete Catalyst SD-WAN security objects, security profiles, and Next-Generation Firewall (NGFW) policies. For more information, see Manage objects and profiles and Manage NGFW policies.
4	Security Cloud Control	Associate a policy group to your Catalyst SD-WAN NGFW policy. For more information, see Associate a group policy.
5	Catalyst SD-WAN Manager	Deploy the policy group to Secure Router routers. For more information, see Policy groups configuration.
6	Security Cloud Control	View the security events received from Catalyst SD-WAN with Security Analytics and Logging for monitoring and threat detection. For more information, see Security Analytics and Logging (Saas) for Catalyst SD-WAN Devices.

Minimum software requirements

This concept explains that Catalyst SD-WAN integration with Security Cloud Control Firewall Management requires Catalyst SD-WAN Manager version 20.18 or later. Secure router compatibility follows Catalyst SD-WAN Manager backward support for the previous two device releases (for example, 20.15 and 20.12 with 20.18).

Minimum software requirements for Catalyst SD-WAN integration with Security Cloud Control Firewall Management:

- Catalyst SD-WAN Manager supported versions: 20.18 or later
- Secure Router supported versions: Devices supported by the last two versions of Catalyst SD-WAN Manager are compatible from version 20.18 onward. For example, if you use Catalyst SD-WAN Manager version 20.18, devices from versions 20.15 and 20.12 are compatible.

  Contact Cisco TAC to check which indexes are not compatible, and remove any incompatible indexes. For more information, see Cisco SD-WAN Control Components Compatibility Matrix.

Network Requirements

If a firewall protects your network, add *.sdwan.cisco.com to the allowed list for inbound port 443 traffic to Catalyst SD Manager. This configuration allows the Cisco API Gateway to communicate with your environment.

Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager

This concept explains that user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management operate independently, with each role defined by its specific responsibilities. However, the Role-Based Access Control (RBAC) models for both platforms are aligned to provide consistency and seamless user actions.

User roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management operate independently, with each role defined by its specific responsibilities. However, the Role-Based Access Control (RBAC) models across these platforms are aligned to ensure consistent and seamless user actions.

A user with elevated permissions in Security Cloud Control Firewall Management may still encounter restrictions if their role in Catalyst SD-WAN Manager has lower permissions, and vice versa.

Attempting to save changes in Security Cloud Control Firewall Management without appropriate permissions in Catalyst SD-WAN Manager results in an error. For example, users assigned the 'Super Admin' role in Security Cloud Control Firewall Management cannot save NGFW security policies changes to Catalyst SD-WAN Manager if they have the 'Operator' role in that platform.

This table outlines the access permissions for various combinations of user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management.

Table 1: RBAC mapping of user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management

Security Cloud Control Firewall Management Role Name	Catalyst SD-WAN Manager Role Name	Allowed Actions
Read Only	Operator	Allowed read-only access in Security Cloud Control Firewall Management Allowed read-only access in Catalyst SD-WAN Manager
VPN Sessions Manager	Operator	Allowed read-only access in Catalyst SD-WAN Manager

Security Cloud Control Firewall Management Role Name	Catalyst SD-WAN Manager Role Name	Allowed Actions
Administrator	security_operations	Allowed to create/edit security policies in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager
Super Administrator	security_operations	Unrestricted access to all functions in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager
Deploy Only	Operator	Not allowed to create/edit security policies in Security Cloud Control Firewall Management Allowed read-only access in Catalyst SD-WAN Manager
Edit Only	security_operations	Not allowed to onboard or deboard Catalyst SD-WAN Manager Unrestricted access to all functions in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager

Onboard Catalyst SD-WAN Manager to Security Cloud Control

Learn how to onboard Catalyst SD-WAN Manager to Security Cloud Control, verify Smart or Virtual Account admin privileges, note the SD-WAN Organization Name, and enable Cloud Services, Analytics, and Service Access Authorization.

Use this procedure to onboard Catalyst SD-WAN Manager to Security Cloud Control platform.

Note

After you onboard Catalyst SD-WAN Manager to Security Cloud Control, security operations (management of policies, objects, and profiles) can be carried out only from Security Cloud Control.

The version control feature is not supported in Security Cloud Control.

Before you begin

Note

Use a publicly resolvable URL or public IP address to access Cisco Catalyst SD-WAN Manager. The Cisco API Gateway must be able to reach the address from the Cisco cloud environment. Internal-only URLs and private IP addresses prevent the API Gateway from connecting and cause onboarding and other cloud services to fail.

- You must have Smart Account Administrator or Virtual Account Administrator privileges on a virtual account linked to a controller profile containing the information of the organization you want to onboard.

  For more information about Smart Account and Virtual Account, see Access the Cisco Catalyst SD-WAN Portal.

- You must have the **Organization Name** of your Catalyst SD-WAN Manager because it will be required during onboarding.

  1. Log in to your Catalyst SD-WAN Manager.
  2. Choose **Administration > Settings > System > Organization Name**.

     The **Organization Name** field contains a unique identifier that establishes secure control connections within the SD-WAN environment.

- Enable **Service Access Authorization** to ensure the onboarding process completes successfully.

  1. Log in to your Catalyst SD-WAN Manager.
  2. Choose **Administration > Settings > Cloud Services**.
  3. Enable **Cloud Services**, **Analytics**, and **Service Access Authorization**.

Note

All Secure Router devices managed by Catalyst SD-WAN Manager are onboarded to Security Cloud Control regardless of their **Device Status**.

- You must have either an Admin or Super Admin role on Security Cloud Control.

Procedure

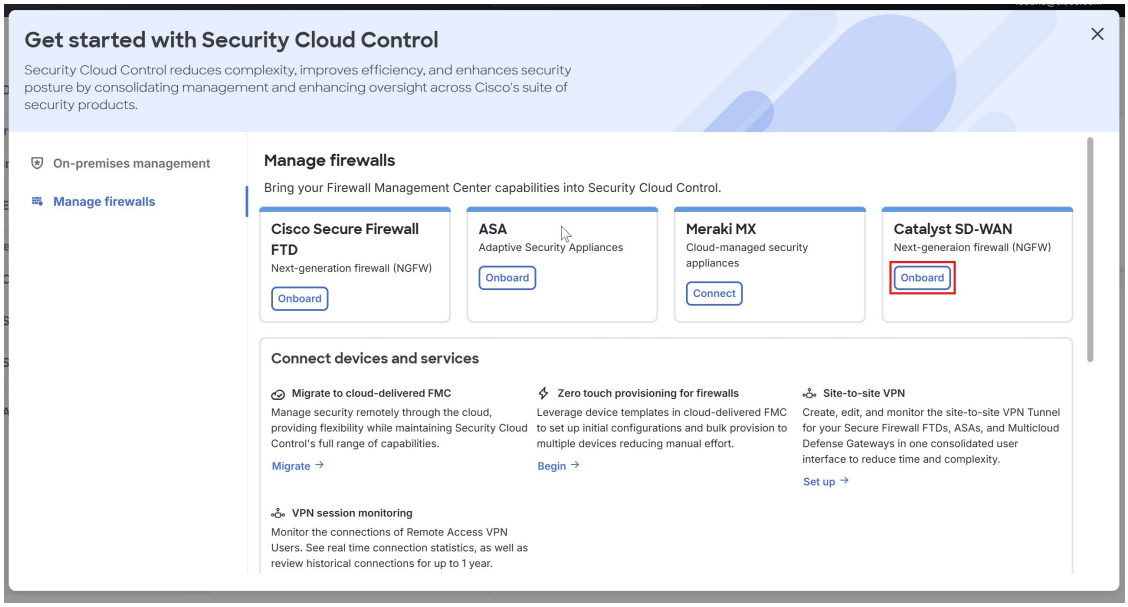
1. In the left pane, choose **Administration** > **Integrations** > **Catalyst SD-WAN**.

2. Click the + icon at the top-right corner of the **Catalyst SD-WAN** tab.
3. Alternatively, you can use the **Get started with Security Cloud Control** interface to onboard Catalyst SD-WAN Manager.

   a. In the top menu, click .

   b. Click the **Manage firewalls** tab.

   c. Click **Onboard** on the **Catalyst SD-WAN** tile.



4. From the **Select Organization** drop-down list, choose an organization.

   The list of organizations displayed in the drop-down depends on the region where Security Cloud Control is deployed.

5. In the **Create label** field, enter the desired label and click **Connect**.

   After you onboard the device to Security Cloud Control, the system applies labels. You can use these labels to group devices and filter them on the **Security Devices** page.

6. Verify the details on the Catalyst SD-WAN Manager you are onboarding, and then click **Close**.

   In the **Services** page, the **Catalyst SD-WAN** displays the onboarded manager.

After a successful onboarding, these details are displayed in Security Cloud Control:

- All security objects, security profiles, and NGFW policies. The system displays these imported policies in **Policies > WAN Branch Edge**.
- Secure Router devices and their running configuration.

What to do next: In the **Management** pane, click **Devices** to see the onboarded Secure Router devices.

Deboard Catalyst SD-WAN Manager from Security Cloud Control

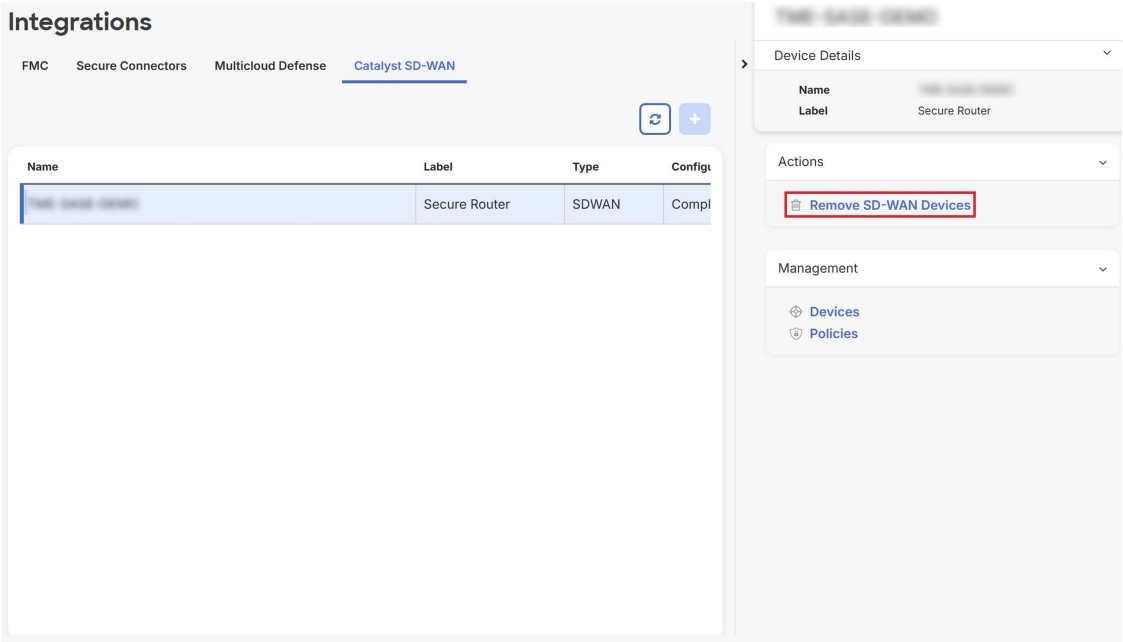
Learn how deboarding Catalyst SD-WAN Manager from Security Cloud Control automatically removes associated devices, NGFW policies, and security objects from Security Cloud Control.

Deboarding Catalyst SD-WAN Manager from Security Cloud Control automatically removes its associated devices, policies, and objects from Security Cloud Control.

> **Note**
>
> When you deboard Catalyst SD-WAN Manager from Security Cloud Control, all the policies and objects created through Security Cloud Control are deleted from Security Cloud Control but remain in Catalyst SD-WAN Manager. You can then edit security objects and policies from Catalyst SD-WAN Manager.

Procedure

1. Choose **Administration** > **Integrations** > **Catalyst SD-WAN**.
2. Select the manager that you want to delete and click **Remove SD-WAN Devices**.



3. Click **OK** to confirm the action.

How Security Cloud Control Firewall Management manages Catalyst SD-WAN NGFW capabilities

Security Cloud Control Firewall Management lets you create, modify, and delete Next-Generation Firewall (NGFW) policies, security objects, and profiles, with global search and policy group association for Catalyst SD-WAN NGFW policies. Changes are automatically saved to Catalyst SD-WAN Manager, but must be manually deployed to Secure Router devices via Catalyst SD-WAN Manager. Direct device deployment from Security Cloud Control Firewall Management is not supported.

When Catalyst SD-WAN Manager is integrated with Security Cloud Control Firewall Management, the existing Next-Generation Firewall (NGFW) policies, security objects, and security profiles from Catalyst SD-WAN Manager are automatically imported into Security Cloud Control Firewall Management. You can modify these NGFW parameters or

create new ones in Security Cloud Control Firewall Management. Any changes you make in Security Cloud Control Firewall Management are synchronized and saved in Catalyst SD-WAN Manager.

After Catalyst SD-WAN Manager is onboarded to Security Cloud Control Firewall Management, you can no longer manage policies, objects, or profiles through Catalyst SD-WAN Manager. You must manage them exclusively from Security Cloud Control Firewall Management.

A "*Managed by Security Cloud Control (SCC)*" banner is displayed on Catalyst SD-WAN Manager that is onboarded to Security Cloud Control Firewall Management, indicating the integration. You can view this message in Catalyst SD-WAN Manager by navigating to the relevant configuration sections.

- For Security Objects and Profiles: Choose **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.
- For NGFW Policies: Choose **Configuration** > **Policy Groups** > **NGFW**

Restrictions for Catalyst SD-WAN Manager integration with Security Cloud Control Firewall Management:

- Cloud connectivity is essential

  Catalyst SD-WAN Manager can be deployed either on-premises or hosted in the Cisco cloud. To function properly, it must have cloud connectivity. If Catalyst SD-WAN Manager is placed behind a NAT device, it is supported but with restrictions. Specifically, only port 443 (HTTPS) needs to be open to enable cloud connectivity.

- Deboard Catalyst SD-WAN Manager to edit NGFW policies, security objects, and security profiles

  To make changes in NGFW policies, security objects, and security profiles from Catalyst SD-WAN Manager, you have to deboard it from Security Cloud Control Firewall Management.

- Customized IPS profiles not supported

  You cannot edit or customize IPS policies (Signature set objects) within security profiles.

- Live logs unavailable with Cisco Security Analytics and Logging (SAL)

  Live logs cannot be viewed on Security Cloud Control Firewall Management using SAL. You can only view historical events.

- Modify user role privileges for Security Cloud Control Firewall Management users with caution

  Exercise caution when changing user role privileges on Catalyst SD-WAN Manager for users who are part of Security Cloud Control Firewall Management. Modifying privileges for Security Cloud Control Firewall Management-associated users can result in configuration failures.

- On-premises multitenant Catalyst SD-WAN Manager not supported

  On-premises multitenant deployments of Catalyst SD-WAN Manager are not supported in Security Cloud Control Firewall Management for version 20.18.1. In this release, only single-tenant Catalyst SD-WAN Manager deployments are compatible with Security Cloud Control Firewall Management.

- Dark mode not supported

  Keep dark mode disabled in Security Cloud Control Firewall Management when Catalyst SD-WAN Manager is integrated.

> **Note**
>
> Changes to NGFW policies, objects, and profiles can only be made in Catalyst SD-WAN Manager after it has been deboarded from Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management allows you to perform these operations:

- Create, modify, or delete NGFW policies, security objects, and security profiles.
- Search for security objects across devices using global search functionality.
- Associate a policy group with a Catalyst SD-WAN NGFW policy.

Policy deployment to Secure Router devices

Changes that are made to NGFW policies, security objects, and security profiles in Security Cloud Control Firewall Management are automatically saved to Catalyst SD-WAN Manager. However, the updated configuration must be manually deployed to Secure Router devices using Catalyst SD-WAN Manager. These changes cannot be pushed directly to devices from Security Cloud Control Firewall Management.

View intrusion events

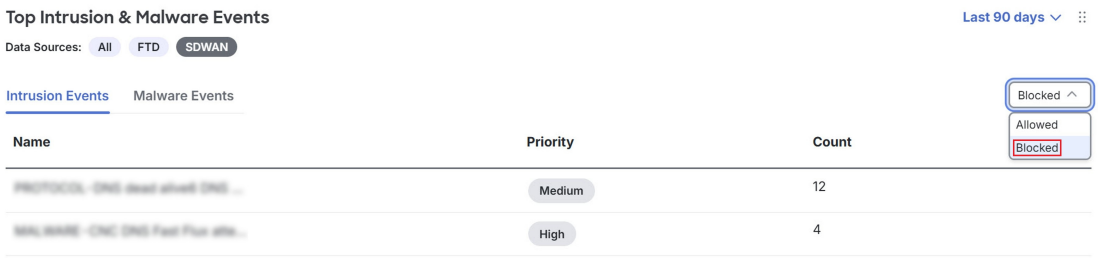
Intrusion Prevention System (IPS) dashlet highlights blocked and allowed network attacks using Cisco Talos threat intelligence. This dashboard view maps to Catalyst SD-WAN Manager Security Monitor IPS/AMP dashlets.

The Intrusion Prevention System (IPS) helps you detect and block network intrusions and malicious activities based on Cisco Talos threat intelligence.

The **Top Intrusion & Malware Events** dashlet in the Security Cloud Control Firewall Management dashboard is mapped to **Intrusion Prevention** and **Advanced Malware Protection** dashlets in the **Monitor** page of Catalyst SD-WAN Manager on the **Security** tab.

Procedure

1. Click **Dashboard**.
2. Navigate to the **Top Intrusion & Malware Events** dashlet.
3. Click **SDWAN** under **Data Sources**.
4. Click the **Intrusion Events** tab.
5. Select **Blocked** in the drop-down near the dashlet.
   By default, **Allowed** is selected.



6. Click the event you want to view in Catalyst SD-WAN Manager.
   A cross-launch window of the Catalyst SD-WAN Manager **Monitor** page appears.
7. Navigate to the **Intrusion Prevention** dashlet to view the event.

View malware events

View the Advanced Malware Protection (AMP) events dashlet, which shows malicious, unknown, and clean file counts over time. This dashboard view maps to Catalyst SD-WAN Manager Security Monitor IPS/AMP dashlets.

The Advanced Malware Protection (AMP) events dashlet displays the counts of malicious, unknown, and clean files identified by AMP over a selected period. AMP blocks malware based on file reputation and uploads unknown files to Cisco AMP Threat Grid for further analysis.

The **Top Intrusion & Malware Events** dashlet on the Security Cloud Control Firewall Management dashboard is mapped to the **Intrusion Prevention** and **Advanced Malware Protection** dashlets on the **Monitor** page of Catalyst SD-WAN Manager on the **Security** tab.

Procedure

1. Click **Dashboard**.
2. Navigate to the **Top Intrusion & Malware Events** dashlet.
3. Click **SDWAN** under **Data Sources**.
4. Click the **Malware Events** tab.
5. Select **Blocked** in the drop-down near the dashlet. By default, **Allowed** is selected.



6. Click the event you want to view in Catalyst SD-WAN Manager.

   A cross-launch window of the Catalyst SD-WAN Manager **Monitor** page appears.

7. Navigate to the **Advanced Malware Protection** dashlet to view the event.

Additional resources

This concept provides the additional resources such as Catalyst SD-WAN configuration guide and policy groups configuration guide.

- Cisco Catalyst SD-WAN Security Configuration Guide
- Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN
- Security Cloud Control Integration with Cisco Catalyst SD-WAN Manager

3 Manage Catalyst SD-WAN Devices

Topics:

- Overview of Catalyst SD-WAN devices
- Supported operations on Catalyst SD-WAN devices
- View configuration of Catalyst SD-WAN devices
- Cross-launch policy groups from Security Cloud Control Firewall Management

Security Cloud Control lets you view the device configuration of your onboarded devices on the Security Devices page and cross-launch to the Policy Groups page in Catalyst SD-WAN Manager.

Overview of Catalyst SD-WAN devices

Learn how to manage Catalyst SD-WAN devices in Security Cloud Control Firewall Management, including viewing onboarded devices and templates, reviewing device configurations, launching policy groups, and removing devices.

Catalyst SD-WAN devices are advanced networking solutions designed to provide secure, high-performance connectivity. These devices integrate SD-WAN capabilities and robust security features, enabling organizations to connect users to applications seamlessly across multicloud environments, branch offices, and data centers. Security Cloud Control Firewall Management provides centralized visibility and security policy management for Catalyst SD-WAN devices.

Supported operations on Catalyst SD-WAN devices

Learn how to manage Catalyst SD-WAN devices in Security Cloud Control Firewall Management, including viewing onboarded devices and templates, reviewing device configurations, launching policy groups, and removing devices.

Catalyst SD-WAN devices are the onboarded WAN Branch Edge or Secure Router devices that can be managed through Security Cloud Control Firewall Management after the related Catalyst SD-WAN Manager is onboarded. Security Cloud Control Firewall Management provides the ability to view, manage, and remove your onboarded devices on the **Security Devices** page. From the **Security Devices** page, you can:

- View onboarded devices and templates in separate tabs.

  For more information, see About Security Devices Page.
- View the configuration file of the onboarded devices.
- Launch policy groups on the Catalyst SD-WAN platform.

> **Note**
>
> You can onboard only one Security Cloud Control Firewall Management organization to a single Catalyst SD-WAN Manager.

View configuration of Catalyst SD-WAN devices

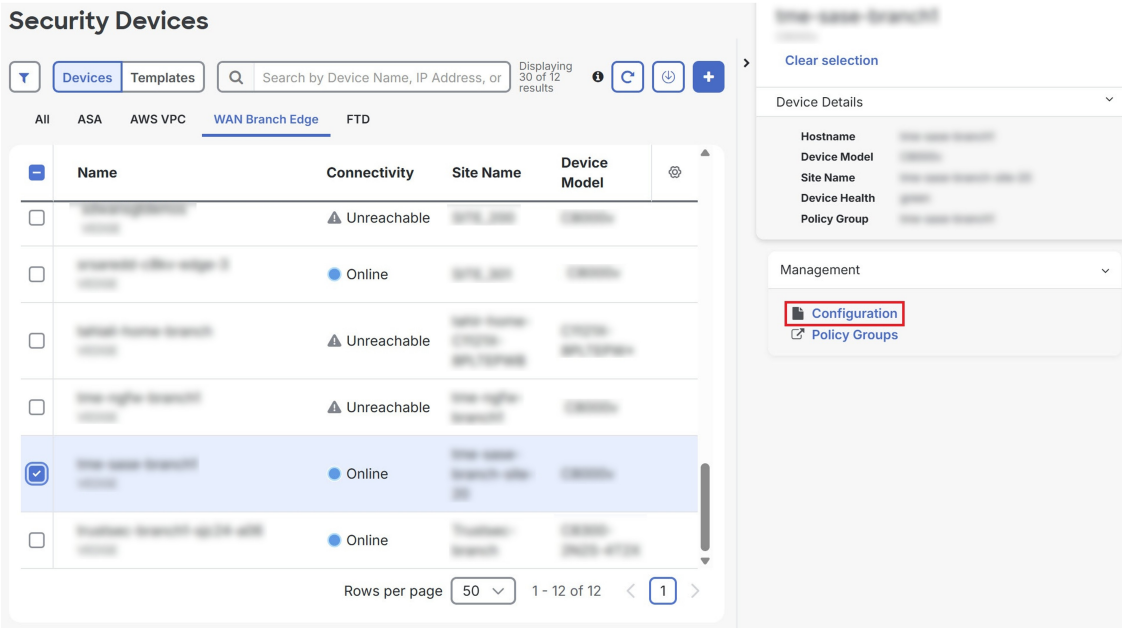
Learn how to manage Catalyst SD-WAN devices in Security Cloud Control Firewall Management, including viewing onboarded devices and templates, reviewing device configurations, launching policy groups, and removing devices.

Security Cloud Control Firewall Management provides the ability to view the device configuration of your onboarded devices on the **Security Devices** page.

-

Procedure

1. Choose **Manage** > **Security Devices**.
2. Click the **WAN Branch Edge** tab.
3. Select a device and click **Configuration** under **Management**.



4. To export the list of devices as a CSV file, click the export icon ( ).

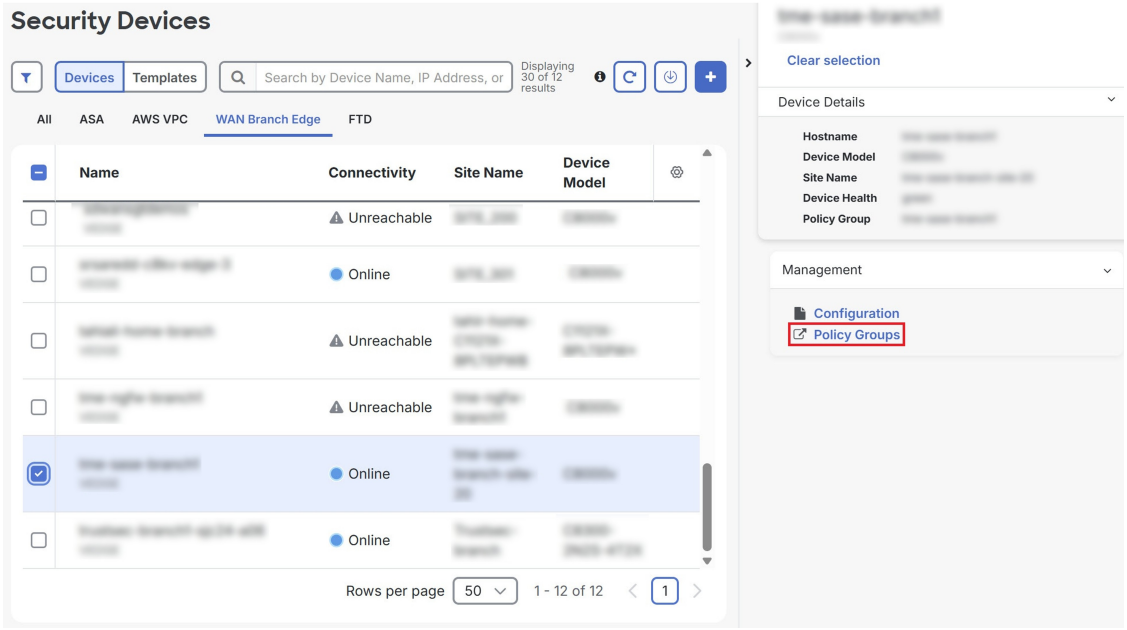
Cross-launch policy groups from Security Cloud Control Firewall Management

Learn how to manage Catalyst SD-WAN devices in Security Cloud Control Firewall Management, including viewing onboarded devices and templates, reviewing device configurations, launching policy groups, and removing devices.

Security Cloud Control Firewall Management lets you cross-launch to the **Policy Groups** page in Catalyst SD-WAN Manager for the onboarded Catalyst SD-WAN Manager.

Procedure

1. Choose **Manage** > **Security Devices**.
2. Click the **WAN Branch Edge** tab.
3. Select a device and click **Policy Groups** under **Management**.


Security Devices
Devices
Templates
Search by Device Name, IP Address, or
Displaying 30 of 12 results
All
ASA
AWS VPC
WAN Branch Edge
FTD
Name
Connectivity
Site Name
Device Model
Unreachable
Online
Unreachable
Unreachable
Online
Online
Rows per page
50
1 - 12 of 12
1
Clear selection
Device Details
Hostname
Device Model
Site Name
Device Health
Policy Group
Management
Configuration
Policy Groups

4 Manage Catalyst SD-WAN Security Objects and Security Profiles

Topics:

- Overview of Catalyst SD-WAN security objects and security profiles
- Create new Catalyst SD-WAN security objects and security profiles
- Modify Catalyst SD-WAN security objects and security profiles
- Delete Catalyst SD-WAN security objects
- Filter Catalyst SD-WAN security objects

This document guides users through creating, modifying, deleting, and managing Catalyst SD-WAN security objects and profiles, enabling precise enforcement of network security policies and streamlined control of application, traffic, and access settings within the SD-WAN environment.

Overview of Catalyst SD-WAN security objects and security profiles

Security objects and security profiles in Catalyst SD-WAN Manager are essential for creating and enforcing next-generation firewall (NGFW) security policies. They safeguard networks from cyber threats while ensuring seamless connectivity and optimized application performance, making them vital for robust network security management and effective NGFW policy implementation.

Catalyst SD-WAN security objects and security profiles are essential for creating and enforcing next-generation firewall (NGFW) security policies and safeguard networks from cyber threats, ensure seamless connectivity, and optimize application performance. They are reusable policy components that Security Cloud Control Firewall Management imports, manages, and synchronizes for Catalyst SD-WAN security policy control. They are vital for robust network security management and effective NGFW policy implementation.

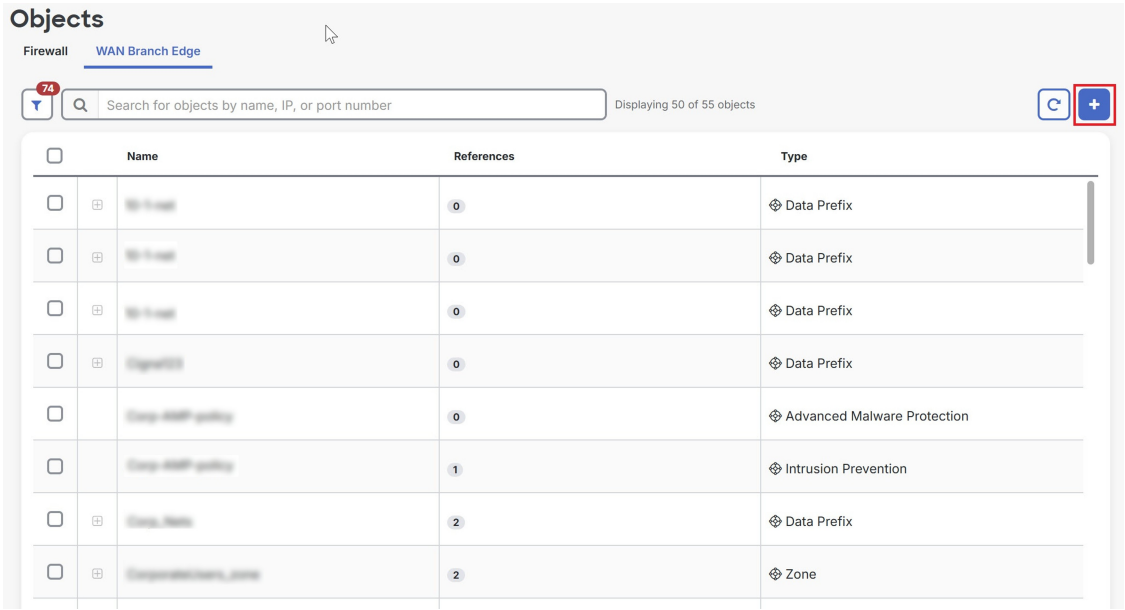
Create new Catalyst SD-WAN security objects and security profiles

Create new Catalyst SD-WAN security objects and security profiles using Security Cloud Control Firewall Management.

Use Security Cloud Control Firewall Management to create new Catalyst SD-WAN security objects and security profiles.

Procedure

1. Choose **Objects**.
2. Click the **WAN Branch Edge** tab.
3. Click the **Create Object** (+) icon.



4. Click the object or profile you want to create:

   Objects:

   - Application List
   - Data Prefix
   - FQDN

- Geolocation
- Identity
- Port
- Protocol
- Security Group Tag
- Signature
- URL Allow
- URL Block
- Zone

Profiles:

- Advanced Inspection Profile
- Advanced Malware Protection
- Intrusion Prevention
- TLS/SSL Decryption
- TLS/SSL Profile
- URL Filtering

5. Click **Save**.

The objects are created in Security Cloud Control Firewall Management. To see the logs in Catalyst SD-WAN Manager, navigate to **Monitor** > **Logs** > **Audit Logs**.

Application List

The application list object groups applications into a list for use in NGFW policies.

The **Application List** object groups applications into a list for use in NGFW policies.

Table 2: Application List

Field	Description
Object Name	The name of the application list.
Application or Application Family	The **Application** is a collection of specific applications grouped together for policy configuration. It allows administrators to define and manage traffic rules for multiple applications as a single entity. For example, "Webex," "Microsoft Teams," "Zoom." The **Application Family** groups applications based on their functional category. For example, "Web," "Instant Messaging," "Network Services."

The **Selected items** field displays the items that have been chosen.

Data Prefix

The data prefix objects are specific IP address ranges or prefixes that are used to define and manage traffic routing policies within the SD-WAN fabric.

The **Data Prefix** objects are specific IP address ranges or prefixes that are used to define and manage traffic routing policies within the SD-WAN fabric.

Table 3: Data Prefix

Field	Description
Object Name	The name of the data prefix object.
Data Prefix	The data prefix value.

FQDN

The Fully Qualified Domain Name (FQDN) object is used to match standalone servers in data centers or private clouds. When matching public URLs, the recommended match action is drop.

The Fully Qualified Domain Name (FQDN) object is used to match standalone servers in data centers or private clouds. When matching public URLs, the recommended match action is **drop**. If you use **inspect** for public URLs, you must define all the related sub URLs and redirect URLs.

Table 4: FQDN

Field	Description
Object Name	The name of the FQDN object.
FQDN	The URL names separated by commas. For example, cisco.com.

Geolocation

The geolocation object allows you to configure firewall rules based on geographical locations rather than IP addresses.

The **Geolocation** object allows you to configure firewall rules based on geographical locations rather than IP addresses.

Table 5: Geolocation

Field	Description
Object Name	The name of the geolocation object.
Geolocation	Select one or more geolocations from the drop-down list. For example, Africa, Antarctica, Asia, or Europe.

Identity

The identity object is a security object used to represent user identities and user groups within the SD-WAN fabric. This identity information is integrated into the SD-WAN fabric to enable identity-based firewall policies and micro-segmentation.

The **Identity** object is a security object used to represent user identities and user groups within the SD-WAN fabric. This identity information is integrated into the SD-WAN fabric to enable identity-based firewall policies and micro-segmentation.

Table 6: Identity

Field	Description
Object Name	The name of the identity object.
Users **User Groups**	The source of **Users** and **User Groups** is Cisco Identity Services Engine (ISE) Active Directory (AD), which is configured in Catalyst SD-WAN Manager.

Port

The port object is a configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

The **Port** object is a configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

Table 7: Port

Field	Description
Object Name	The name of the port object.
Port	The port values separated by commas. The range is 0 to 65535.

Protocol

Within security policies, protocols can be selected from a predefined list (for example, TCP, UDP, ICMP) to define specific rules for traffic management and security enforcement.

Within security policies, **Protocol** objects can be selected from a predefined list (for example, TCP, UDP, ICMP) to define specific rules for traffic management and security enforcement.

Table 8: Protocol

Field	Description
Object Name	The name of the protocol object.
Protocol	Select one or more protocol names from the drop-down list. For example, SNMP, TCP, UDP, ICMP, Echo, Telnet.

The **Selected items** field displays the items that have been chosen.

Security Group Tag

Use Cisco Identity Services Engine (ISE) to define and use security group tag (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria.

If you use Cisco Identity Services Engine (ISE) to define and use security group tag (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGTs as matching criteria.

SGTs cannot be created or edited in Security Cloud Control Firewall Management. You must create all SGTs in ISE.

Table 9: Security Group Tag

Field	Description
Object Name	The name of the security group tag.
Security Group Tags	Choose the security group tags by checking the appropriate checkboxes.

The **Selected items** field displays the items that have been chosen.

IPS Signature

The IPS signature object in Catalyst SD-WAN Manager refers to a set of rules used by the Intrusion Prevention System (IPS) to detect and prevent network attacks.

The **IPS Signature** object refers to a set of rules used by the Intrusion Prevention System (IPS) to detect and prevent network attacks. It blocks vulnerabilities that have a Common Vulnerability Scoring System (CVSS) score of 9 or higher. It also blocks Common Vulnerabilities and Exposures (CVEs) published within the last two years if they belong to the rule categories of Malware CNC, Exploit Kits, SQL Injection, or blocked list.

Table 10: IPS Signature

Field	Description
Object Name	The name of the object.
IPS Signature	The IPS signatures in the format `Generator ID:Signature ID`, separated by commas. For example, `1234:5678`. Range is 0 to `4294967295`.

Allow URL

The allow URL object in Catalyst SD-WAN Manager is used to define URLs that should be explicitly permitted through SD-WAN URL filtering feature.

The **Allow URL** object is used to define URLs that should be explicitly permitted through SD-WAN URL filtering feature.

Some important points to note about these lists are:

- URLs that are allowed are not subjected to any category-based filtering.
- If the same item is configured under both the allowed and blocked lists, the traffic is allowed.
- If the traffic does not match either the allowed or blocked lists, it is subjected to category-based and reputation-based filtering.

Table 11: Allow URL

Field	Description
Object Name	The name of the allow URL object.
Allow URL	The URLs to allow.

Block URL

The block URL object in Catalyst SD-WAN Manager is used to define URLs that should be denied through SD-WAN URL filtering feature.

The **Block URL** object is used to define URLs that should be denied through SD-WAN URL filtering feature.

Table 12: Block URL

Field	Description
Object Name	The name of the block URL object.
Block URL	The URLs to block.

Zone

The zone object in Catalyst SD-WAN Manager is used to define security boundaries for traffic control.

The **Zone** object is used to define security boundaries for traffic control. Zones can be configured based on **VPNs** or **Interfaces**:

- Zones can be created for specific VPNs, such as the Payment Processing Network, Corporate Users, or Local Internet for Guests. These zones allow you to apply security policies to traffic within or between VPNs.
- Interfaces can also be assigned to zones. For example, Ethernet, GigabitEthernet, or other interface types can be grouped into zones. This allows for granular control of traffic between interfaces.

Table 13: Zone

Field	Description
Object Name	The name of the zone.
VPN	Choose to configure zones with zone type as **VPN**. Add the VPNs to the zones from the drop-down list. Available options include: - Payment Processing Network - Corporate Users - Local Internet for Guests - Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface**. Add the interfaces to the zones from the **Add Interface** drop-down list.

The **Selected items** field displays the items that have been chosen.

Advanced Inspection Profile

Apply a global Advanced Inspection Profile (AIP) at the device level. This ensures that all traffic matching the device's predefined rules is thoroughly inspected using the advanced inspection profile.

Apply a global **Advanced Inspection Profile** (AIP) at the device level. This ensures that all traffic matching the device's predefined rules is thoroughly inspected using the AIP.

Table 14: Advanced Inspection Profile

Field	Description
Object Name	The name of the advanced inspection profile.
Intrusion Prevention	Choose an intrusion prevention option from the drop-down list.
URL Filtering	Choose a URL filter from the drop-down list.
Advanced Malware Protection	Choose an advanced malware protection option.
TLS Action	Choose the TLS action. Available options include: - Decrypt - Pass Through - Do not Decrypt

Advanced Malware Protection

The advanced malware protection policy is a security policy specifically designed to integrate advanced malware protection capabilities into the unified security policy framework.

The **Advanced Malware Protection** (AMP) policy is a security policy specifically designed to integrate advanced malware protection capabilities into the unified security policy framework.

> **Note**
>
> For some advanced configurations, a Threat Grid Server configuration is required in Catalyst SD-WAN.

Table 15: Advanced Malware Protection

Field	Description
Object Name	The name of the advanced malware protection policy.
AMP Cloud Region	**AMT Cloud Region** refers to the **Analytics, Management, and Telemetry (AMT) Cloud Region** associated with the Cisco SD-WAN cloud architecture.
Alert Log Level	All syslog messages are associated with priority levels that indicate the severity of syslog messages to save.
File Analysis	Enables file analysis on the uploaded files.
TG Cloud Region	Choose a region. This refers to the geographical region where the Threat Grid (TG) cloud services are hosted.
File Types	Choose the file types to be analyzed.

Intrusion Prevention

The intrusion prevention policy profile is a security feature designed to detect and block known network attacks by leveraging predefined rules and signatures.

The **Intrusion Prevention** policy profile is a security feature designed to detect and block known network attacks by leveraging predefined rules and signature.

Table 16: Intrusion Prevention

Field	Description
Object Name	The name of the intrusion prevention policy.
Signature Set	Choose a signature set that defines rules for evaluating traffic from the **Signature Set** drop-down list.
Inspection Mode	Select the inspection mode.
Custom Signature Set:	Select one or more web categories from the drop-down list. Custom signature must be enabled from Catalyst SD-WAN Manager under **Administration** > **Settings** > **External Services** > **UTD Snort Subscribe Signature** > .
Signature Allow List	Select a signature allow list.
Alerts Log Level	Choose the alert log level. This refers to the severity levels of logs generated by the system, which can be configured to control the granularity of information logged.

TLS/SSL Decryption

The TLS/SSL decryption profile in Catalyst SD-WAN Manager refers to a feature or configuration that enables administrators to inspect and manage encrypted traffic passing through the network.

The **TLS/SSL Decryption** profile allows administrators to inspect and manage encrypted traffic within the network.

> **Note**
>
> Before creating a **TLS/SSL Decryption** profile in Security Cloud Control Firewall Management, you must configure certificate authority (CA) from Catalyst SD-WAN Manager under **Configuration** > **Certificates** > **Certificate Authority**.

Table 17: TLS/SSL Decryption

Field	Description
Object Name	The name of the TLS/SSL decryption policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	

Field	Description
Expired Certificate	Defines what the policy should do if the server certificate has expired. Available options include: • Drop: Drop traffic • Decrypt: Decrypt traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. Available options include: • Drop: Drop traffic • Decrypt: Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. Available options include: **Enabled** or **Disabled**.
Unknown Revocation Status	Defines the policy action if the OCSP revocation status is **unknown**. • Drop: Drop traffic • Decrypt: Decrypt traffic
Unsupported Mode Checks	
Unsupported Protocol Versions	Defines the unsupported protocol versions. • Drop: Drop the unsupported protocol versions. • No Decrypt: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • Drop: Drop the unsupported cipher suites. • No Decrypt: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are **Close** and **Open**.
Certificate Bundle	Select the **Use Default CA Certificate** checkbox to use the default CA.
Minimal TLS Version	Sets the minimum version of TLS that the proxy should support. Available options include: TLS 1.0, TLS 1.1, or TLS 1.2
Proxy Certificate Attributes	
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. Available options include: 1024-bit RSA, 2048-bit RSA, or 4096-bit RSA
EC Key Type	Defines the key type. Available options include: P256, P384, or P521
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate (in days).

TLS/SSL Profile

The TLS/SSL profile policy in Catalyst SD-WAN Manager is used to manage encrypted traffic within a unified security policy.

The **TLS/SSL Profile** policy is used to manage encrypted traffic within a unified security policy. To create a TLS/SSL profile policy in Security Cloud Control Firewall Management, you must first configure the certificate authority (CA) certificate in Catalyst SD-WAN. This is a prerequisite for enabling the TLS proxy functionality.

Table 18: TLS/SSL Profile

Field	Description
Object Name	The name of the TLS/SSL profile.
Categories to assign action	Set the categories and assign actions: Decrypt, No Decrypt, and Pass Through URL Categories. Alternatively, choose multiple categories and set the action.
Reputation	Enable reputation to choose the **Decrypt Threshold**. Supports actions based on URL reputation levels.
Decrypt Domain List	Choose the decrypt domain list.
No Decrypt Domain List	Choose the no decrypt domain list.
Fail Decrypt	Enable the fail decrypt option if decryption fails.

URL Filtering

The URL filtering profile policy in Catalyst SD-WAN Manager is a security feature that allows administrators to control access to websites based on categories, reputation, and custom lists.

The **URL Filtering** profile policy is a security feature that allows administrators to control access to websites based on categories, reputation, and custom lists.

Table 19: URL Filtering

Field	Description
Object Name	The name of the URL filtering policy.
Web Category	Choose the web category. Available options include: Block and Allow. The websites are classified into categories.
Web Reputation	Choose the web reputation from the drop-down list. The URLs are assigned a reputation score based on their risk level.
Allowlist	Select an allow URL list.
Blocklist	Select a block URL list.

Field	Description
Block Page Server	Choose one of the options: • Block Page Content: Enter the default content header and content body. • Redirect URL: Enter the redirect URL. The blocked users can be redirected to a custom page or shown a message.
Alerts and Logs	Choose the alert and log type: • Blocklist • Allowlist • Reputation/Category

Modify Catalyst SD-WAN security objects and security profiles

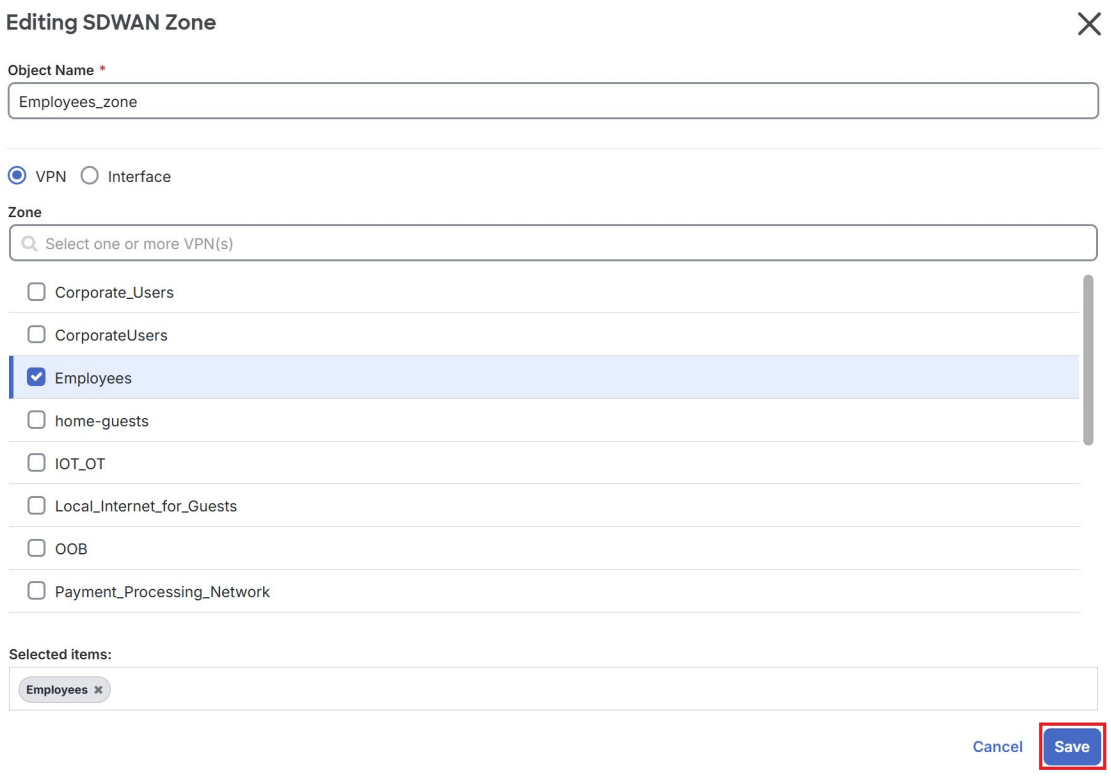
Edit the values associated with the Catalyst SD-WAN security objects and security profiles from Security Cloud Control Firewall Management.

Use this procedure to modify the values associated with Catalyst SD-WAN security objects and security profiles from Security Cloud Control Firewall Management.

Procedure

1. Choose **Administration** > **Integrations** > **Catalyst SD-WAN**.
2. Choose **Objects**.
3. Click the **WAN Branch Edge** tab.
4. Select the security object or profile to modify. To find an object, use the filter.
5. In the **Actions** pane, click **Edit**.

   Modify the configurations you want to change.
6. Click **Save** to confirm.



Delete Catalyst SD-WAN security objects

You can delete Catalyst SD-WAN security objects in Security Cloud Control Firewall Management if they are not referenced by any policies, objects, or configurations. Before deleting an object, you must manually remove all references to it in security policies. The system logs deleted objects for traceability and compliance.

You can delete one or multiple Catalyst SD-WAN security objects.

- If the security object was synchronized with Catalyst SD-WAN Manager, deleting it updates both Security Cloud Control Firewall Management and Catalyst SD-WAN Manager for consistency.
- Security policies or configurations that reference the deleted object do not get deleted automatically. You must remove the references manually from the security policies before deleting the object.
- Delete actions are logged for auditing and traceability.

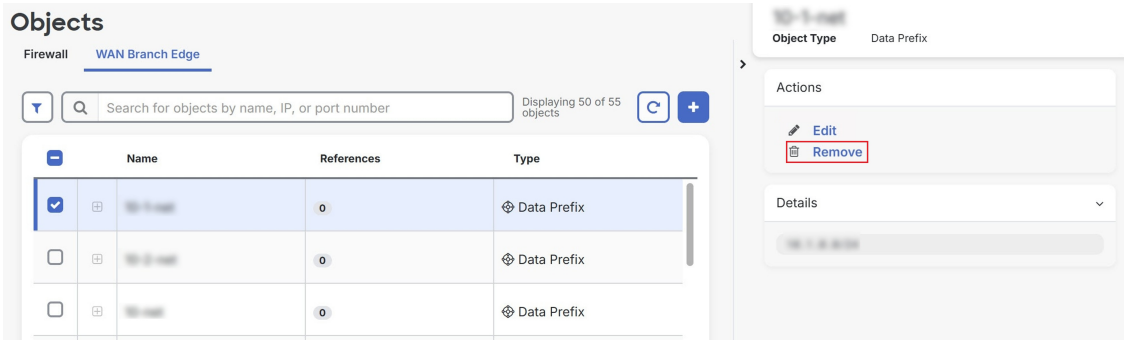
Before you begin

Verify that the Catalyst SD-WAN security objects you want to delete are not used or referenced in other objects, policies, or configurations.

Procedure

1. Choose **Administration** > **Integrations** > **Catalyst SD-WAN**.
2. Choose **Objects**.
3. Click the **WAN Branch Edge** tab.
4. Check one or multiple security objects you want to delete.

5. In the **Actions** pane, click **Remove**.



6. Click **OK** to confirm.

Selected Catalyst SD-WAN security objects are deleted. Delete actions are logged for audit purposes, ensuring traceability of changes.

To view the logs:

- In the Security Cloud Control application, choose **Events & Logs** > **Logs** > **Change Log**.
- In the Catalyst SD-WAN Manager application, choose **Monitor** > **Logs** > **Audit Logs**.

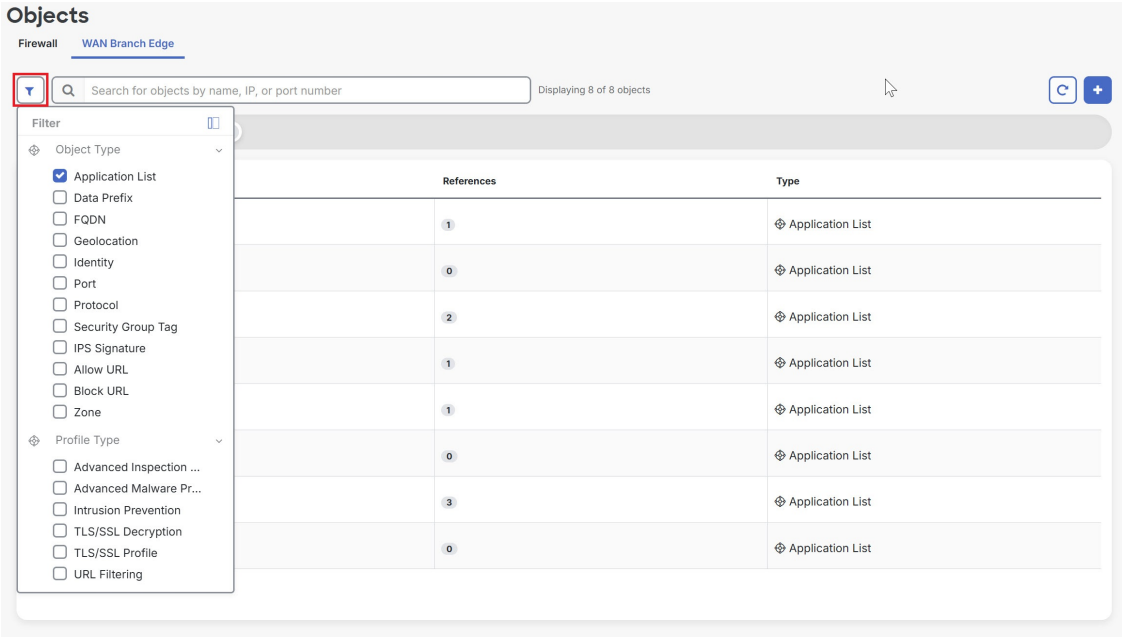
Filter Catalyst SD-WAN security objects

Catalyst SD-WAN Manager enables users to efficiently filter and search security objects by Object Type and Profile Type, streamlining network security management. This feature enhances the ability to locate, review, modify, or delete security objects, optimizing system performance and ensuring effective SD-WAN security object administration for WAN Branch Edge environments.

The ability to filter and search for Catalyst SD-WAN security objects by **Object Type** and **Profile Type** allows users to efficiently locate, review, modify, and, when needed, delete these objects. This approach helps maintain optimal system performance.

You can filter objects using two parameters: **Object Type** and **Profile Type**.

1.
2. Choose **Administration** > **Integrations** > **Catalyst SD-WAN**.
3. Choose **Objects**.
4. Click the **WAN Branch Edge** tab.
5. Click the filter icon ( ) and select objects by **Object Type** or **Profile Type**.



You can use filters to search for objects. Refine the results by typing the object name, IP address, or port number to narrow the search.

5 Manage Catalyst SD-WAN Security Policies

Topics:

- An introduction to Catalyst SD-WAN NGFW security policies
- Manage existing Catalyst SD-WAN NGFW security policies
- Create Catalyst SD-WAN security policies
- Associate a policy group to Catalyst SD-WAN NGFW policy
- Deploy policy group from Catalyst SD-WAN Manager

This document explains how the integration of Security Cloud Control and Catalyst SD-WAN Manager allows you to manage (create, view, edit, and deploy) Catalyst SD-WAN NGFW security policies, including configuring sub-policies, source/destination zones, and policy groups, and deploying policy groups to Secure Router devices.

An introduction to Catalyst SD-WAN NGFW security policies

Catalyst SD-WAN Manager NGFW security policies offer robust protection for networks, systems, and data against unauthorized access and threats. With a comprehensive management framework, users can efficiently implement and manage Next-Generation Firewall (NGFW) security policies, ensuring advanced cybersecurity, streamlined policy control, and enhanced threat prevention for enterprise environments.

The NGFW security policies in Catalyst SD-WAN Manager are a set of rules and configurations designed to protect systems, networks, and data from unauthorized access, misuse, or threats. Catalyst SD-WAN Manager offers a comprehensive framework for implementing and managing NGFW security policies.

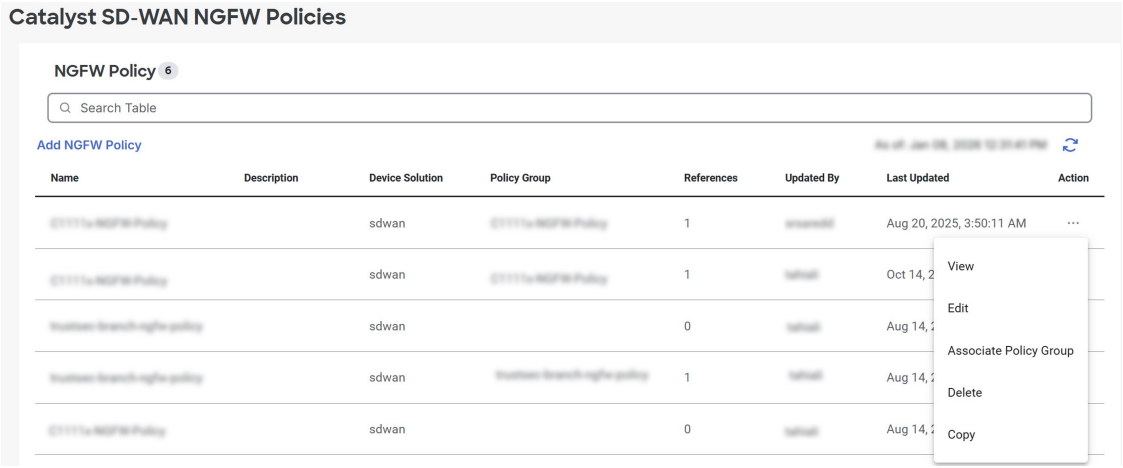
Manage existing Catalyst SD-WAN NGFW security policies

View, edit, associate policy group, delete, or copy Catalyst SD-WAN NGFW security policies from Security Cloud Control Firewall Management.

You cannot delete a Next-Generation Firewall (NGFW) policy from Security Cloud Control Firewall Management if it is already associated with a policy group in Catalyst SD-WAN.

Procedure

1. Choose **Policies** > **WAN Branch Edge**.
2. Navigate to the policy and click the ellipsis (...) under the **Action** column.
3. Click **View**, **Edit**, **Associate Policy Group**, **Delete**, or **Copy**.



Create Catalyst SD-WAN security policies

Create Catalyst SD-WAN NGFW security policies in Security Cloud Control Firewall Management using the Create NGFW policy workflow.

Before you begin

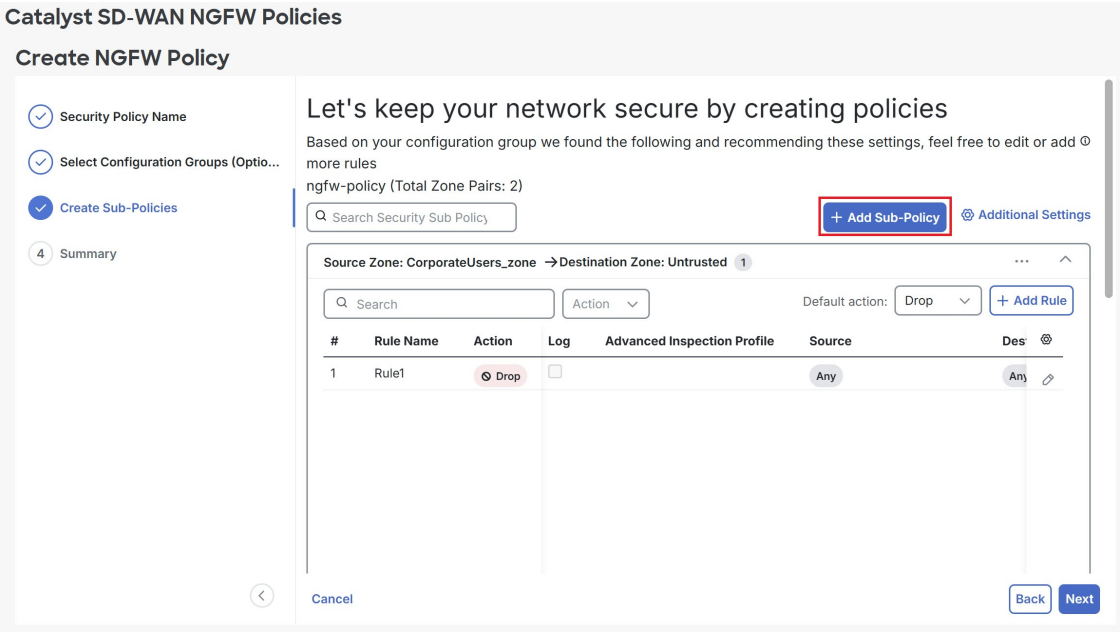
Make sure you have deployed and managed these devices using a configuration group. For more information about creating configuration groups, see Configuration Groups and Feature Profiles.

Follow these steps to create Catalyst SD-WAN NGFW security policies in Security Cloud Control Firewall Management using the Create NGFW policy workflow.

Procedure

1. Choose **Policies** > **WAN Branch Edge**.
2. Click **Add NGFW Policy** on the **Catalyst SD-WAN NGFW Policies** page.

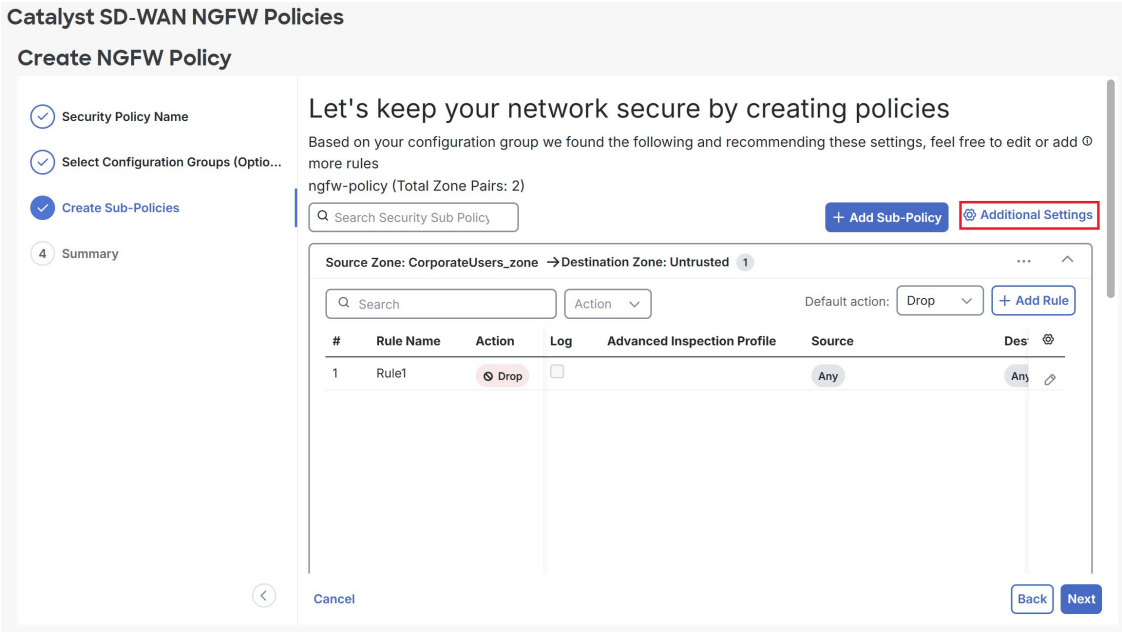
   This launches the **Create NGFW policy** workflow.
3. On the **Security Policy Name** tab, enter **Policy Name** and **Description**, and under **Device Solution**, click the **SDWAN** radio button.
4. Click **Next**.
5. On the **Select the optional Configuration Group to associate with the NGFW policy** page, choose the configuration group to associate with the NGFW policy and click **Next**.
6. On the **Create Sub-Policies** tab, click **+Add Sub-Policy** to add sub-policies for a security policy.



Field	Description
VPN / Interface	Specify the VPN or the interface.

Field	Description
Source Zone	Choose the zone that is the source of the data packets. You can choose from these options: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted Click **+ Create New** to create a new Source Zone. Enter the **Name** and select the **VPN** from the drop-down. **Note** You can select multiple VPNs within a Source Zone.
Destination Zone	Select the zones to which data traffic is sent. You can choose from these options: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted To create a new Destination Zone, click **+ Create New**. Enter the **Name** and select the **VPN** from the drop-down. **Note** You can select multiple VPNs within a Destination Zone.

7. Click **Additional Settings** to configure additional settings for a security policy. For more information about the steps used in the procedure, Configure NGFW Additional Settings.
8. Click **Save**.



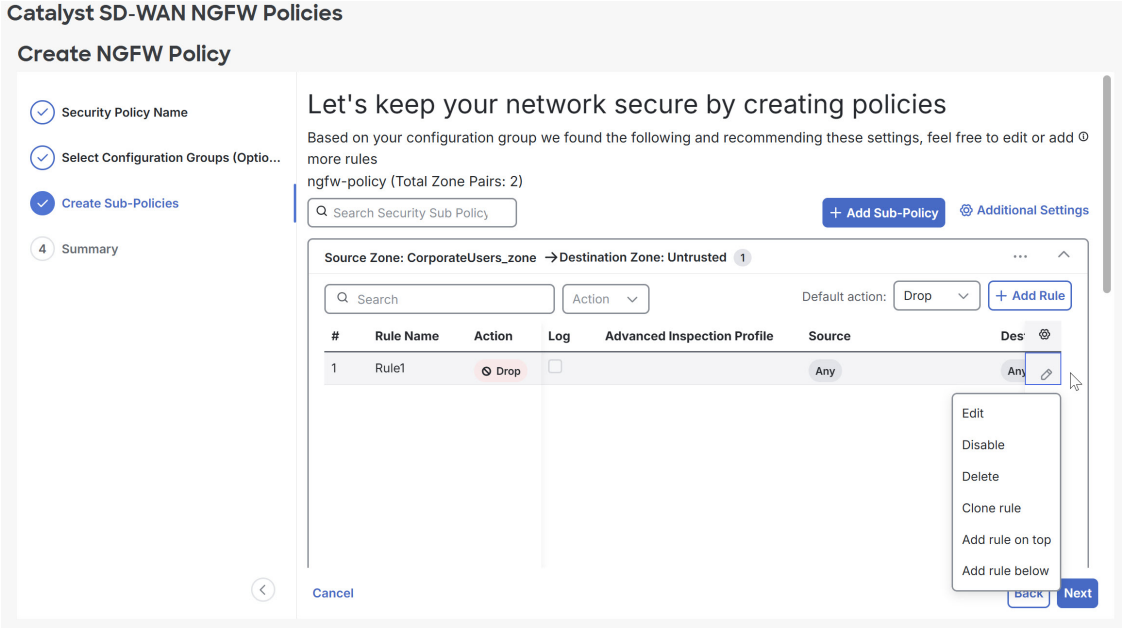
9. Click the ellipsis (...) at the top-left corner of the existing sub-policy to **Edit**, **Delete**, or **Copy** it.
10. To add an NGFW policy rule to a sub-policy, navigate to the sub-policy and click **+ Add Rule**.

Field	Description
Rule Name	The name of the rule.
Sequence	Specify the sequence.

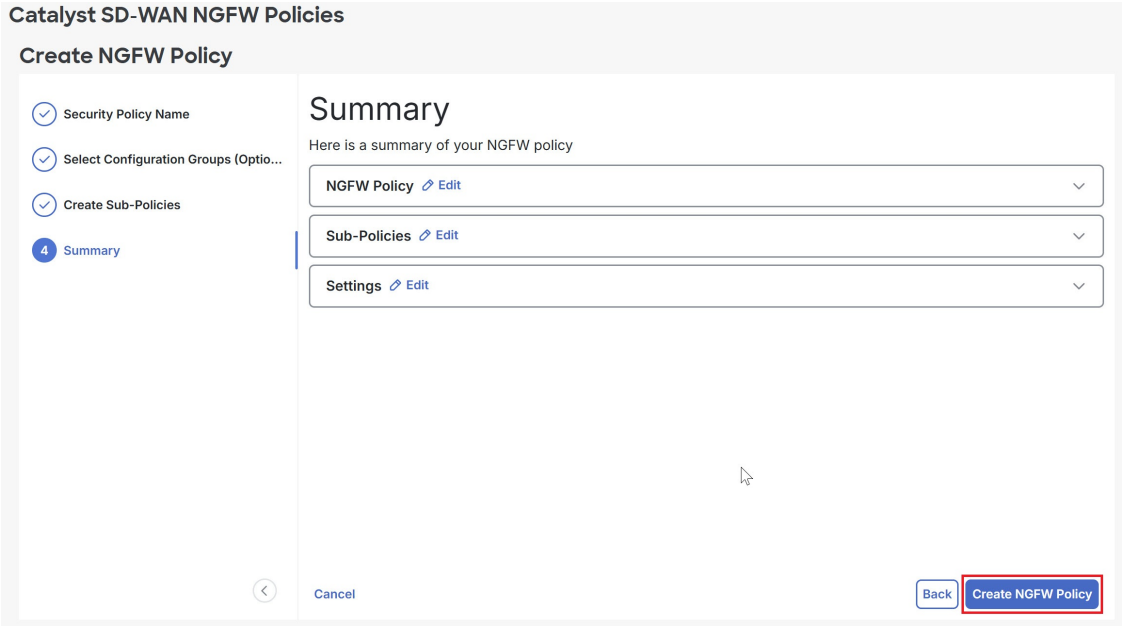
Match	Choose the desired match conditions from the **Add Conditions** drop-down list. You can choose from these options:
	• Source
	  ◦ Geo Location
	  ◦ IPv4 Prefix
	  ◦ Port
	• Destination
	  ◦ FQDN
	  ◦ Geo Location
	  ◦ IPv4 Prefix
	  ◦ Port
	• Protocol
	• Applications
	When Identity Services Engine (ISE) is enabled, the SGT option is available in the **Source** and **Destination** fields. Identity User or User group is only supported for **Source**.

Field	Description
Action	Choose the desired action conditions. You can choose from these options: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action.

11. To modify an existing rule, click the pencil icon to **Edit**, **Disable**, **Delete**, **Clone rule**, **Add rule on top**, or **Add rule below**.



12. Click **Next**.
13. Review the **NGFW Policy**, **Sub-Policies**, and **Settings** on the **Summary** page, and click **Create NGFW Policy**.



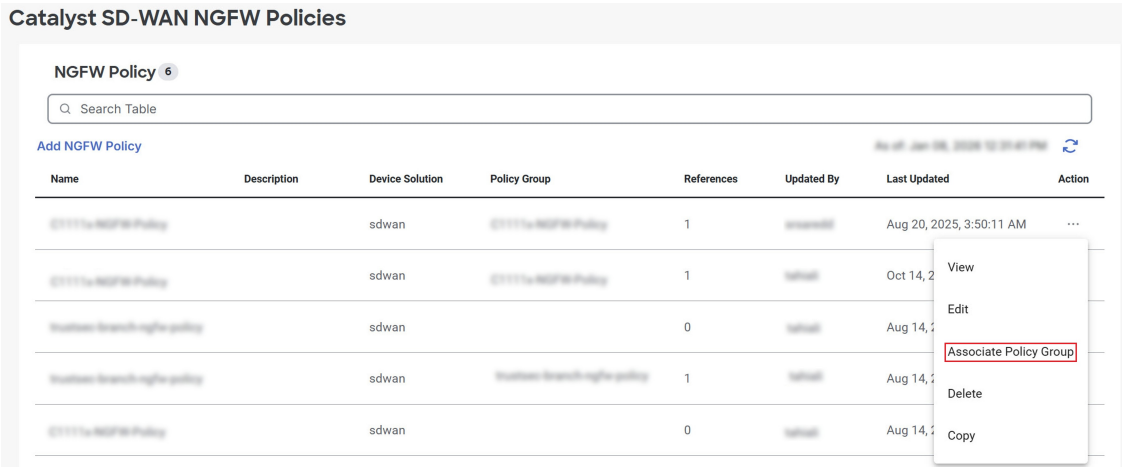
Associate a policy group to Catalyst SD-WAN NGFW policy

Associate a policy group with a Catalyst SD-WAN NGFW policy to ensure consistent security enforcement across managed devices. Using Security Cloud Control Firewall Management, administrators can easily link policy groups to NGFW policies and deploy them, streamlining network security management and enhancing centralized policy deployment for WAN Branch Edge environments.

This section outlines the steps to associate a policy group with a Catalyst SD-WAN NGFW policy, enabling the policy to be deployed to devices managed by that group. This ensures consistent security enforcement across those devices. Once associated, you can deploy the policy group to activate the policy on the devices.

Procedure

1. Choose **Policies** > **WAN Branch Edge**.
2. Navigate to the policy you want to associate with a policy group. Click the ellipsis (...) under the **Action** column, then select **Associate Policy Group**.



3. Select the policy and click **Save**.

Deploy policy group from Catalyst SD-WAN Manager

A policy group in Catalyst SD-WAN is a logical grouping for NGFW security policies, streamlining deployment across multiple devices or sites. Using Catalyst SD-WAN Manager, administrators can deploy policy group updates, including security objects and profiles, to Secure Router devices, optimizing network security management and simplifying SD-WAN policy enforcement.

A policy group in Catalyst SD-WAN is a logical grouping of related items or configurations used in Next-Generation Firewall (NGFW) security policies. These groups simplify the process of applying policies across multiple devices or sites.

You can deploy NGFW policy modifications, including security objects and security profiles, from Security Cloud Control Firewall Management to Secure Router devices using Catalyst SD-WAN Manager.

You can access the workflow from the **Workflows** > **Deploy Policy Group** menu in Catalyst SD-WAN Manager. This workflow enables you to associate Secure Router devices and deploy the policy group to the selected devices.

For more information, refer to the *Deploy Policy Group Workflow* section in the Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN.

6 Cisco Security Analytics and Logging

Topics:

- About Security Analytics and Logging (SaaS) in Security Cloud Control
- Event types in Security Cloud Control
- Deprovisioning Cisco Security Analytics and Logging (SaaS)
- Security Analytics and Logging licenses
- Security Analytics and Logging for Catalyst SD-WAN
- How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management
- Requirements and guidelines for SD-WAN integration
- View Catalyst SD-WAN events in Security Cloud Control Firewall Management

About Security Analytics and Logging (SaaS) in Security Cloud Control

Learn how Cisco Security Analytics and Logging (SAL) collects and centralizes firewall security events in the cloud, enabling unified visibility and filtering through Security Cloud Control.

Terminology Note: In this documentation, when Cisco Security Analytics and Logging (a software as a service product) is used with Security Cloud Control for security event monitoring and analysis, you will see this integration referred to as Cisco Security Analytics and Logging (SaaS) or SAL (SaaS).

Cisco Security Analytics and Logging (SAL) allows you to capture supported types of security events from all of your firewall devices and view them in one place in Security Cloud Control. The events are stored in the Security Analytics and Logging cloud and viewable from the **Event Logging** page. The **Event Logging** page allows you to search, filter and analyze the security event data to understand which security rules are being triggered in your network.

Event types in Security Cloud Control

Secure Logging Analytics (SaaS) enables you to filter and analyze security events from ASA, FTD, and , Catalyst SD-WAN, devices by event types such as AAA, BotNet, Firewall Traffic, Intrusion, and AI Defense. These filters help monitor network activity, detect threats, and enforce security policies for comprehensive security visibility.

When filtering the security events logged in Secure Logging Analytics (SaaS), you can choose from a list of Catalyst SD-WAN event types that Security Cloud Control supports. From the Security Cloud Control menu, navigate **Analytics** > **Event Logging** and click the filter icon to choose events.

Catalyst SD-WAN devices currently log only connection events under SD-WAN event types. SD-WAN Catalyst devices do not support sending syslog events to Security Cloud Control. To learn more about syslog IDs for Catalyst SD-WAN events, see Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.

You can generate events for connections as users generate traffic that passes through the system. Enable connection logging on access rules to generate these events. You can also enable logging on Security Intelligence policies and SSL decryption rules to generate connection events.

Connection events contain data about the detected sessions. The information available for any individual connection event depends on several factors. In general, this information includes:

- Basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on.
- Additional connection properties the system discovers or infers: applications, requested URLs, users associated with the connection, and so on.
- Metadata explaining why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, and details about encrypted and decrypted connections.

Deprovisioning Cisco Security Analytics and Logging (SaaS)

Cisco Security Analytics and Logging (SaaS) subscription management ensures ongoing access to security event data and analytics. Maintaining an active subscription prevents data loss and preserves your ability to monitor, analyze, and respond to security threats using stored firewall events and behavioral analytics.

If you allow your Cisco Security Analytics and Logging (SaaS) paid subscription to lapse, collection of new events stops immediately. After 90 days from expiry, you will no longer be able to view or query your existing event data. You have 180 days to renew your subscription.

If you allow the 180-day grace period to lapse, the system purges all of your event data. You can no longer view security events on the **Event Logging** page, nor have dynamic entity modeling (DEM) behavioral analytics applied to your security events and network flow data.

Security Analytics and Logging licenses

Lists Security Analytics and Logging subscription options for managing firewall logs in Security Cloud Control, including per-device licenses and customizable log storage and retention.

Security Analytics and Logging subscriptions offer flexible options for managing firewall logs in Security Cloud Control, including per-device licenses and customizable log storage and retention. Choose between Essentials, Advantage, and Premier tiers to meet operational and compliance requirements, with retention periods up to five years and storage capacities up to 10 TB.

Security Analytics and Logging subscription overview

You can combine SAL with your Security Cloud Control subscription. When managing your firewalls with Security Cloud Control, you can obtain Security Analytics and Logging entitlement in these ways:

- Device management with unlimited logging: This option provides a per-device license. It includes device management capabilities for your firewall device and unlimited log storage for a rolling period of 90 days.
- Device management only with optional cloud logging: This option involves purchasing a per-device license for management only. You can then add Security Analytics and Logging as a separate cloud logging subscription. This allows you to customize logging data storage and log retention based on your specific operational and compliance needs.

90-day free trial

To accurately estimate your daily ingest rate, log in to Security Cloud Control and navigate to the **Events & Logs** > **Events** > **Event Logging** tab to request a 90-day trial. You can purchase the desired subscription plan to continue the service by reviewing the instructions in the Security Cloud Control Firewall Management Ordering Guide.

Security Analytics and Logging paid subscription tiers

If you choose not to use device management with unlimited logging option, you can purchase logging capacity separately. This standalone Security Analytics and Logging subscription provides greater flexibility, longer default retention, and increased storage entitlements. The default minimum retention period for these subscription tiers is 1 year.

Select these flexible Security Analytics and Logging subscription tiers if:

- You have already purchased your firewall devices as part of a different order.
- You have specific logging estimates and want to buy a tier based on a fixed amount of ingest, storage, and logging retention.
- You want a log retention period that is more than 90 days.

Security Analytics and Logging subscription is categorized into three tiers—Essentials, Advantage, and Premier. This table lists the storage capacities and log retention periods for each tier.

Description	Retention Period	Storage Limit	Subscription Term
Cisco SAL Essentials Subscriptions	1, 2, or 3 years	2 TB	0 to 5 years
Cisco SAL Advantage Subscriptions	1, 2, or 3 years	4 TB	0 to 5 years

Description	Retention Period	Storage Limit	Subscription Term
Cisco SAL Premier Subscriptions	1, 2, or 3 years	10 TB	0 to 5 years

For more information about the subscription plans, refer to the Security Cloud Control Firewall Management Ordering Guide.

Note

For paid subscriptions, Security Analytics and Logging automatically manages your event data to ensure that it aligns with your licensed retention period. Security Analytics and Logging removes event data that is older than your specified retention period on a daily basis, and ensures that you always retain access to all event data within your full retention period.

Estimate your daily ingest rate

Purchase a subscription plan that matches the number of events the Cisco cloud receives from your onboarded firewall devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your subscription plan.

Subscribing to a Security Analytics and Logging license

Describes the process for subscribing to a Security Analytics and Logging license, including starting a trial, purchasing a subscription, claiming licenses, and maintaining renewal.

Security Analytics and Logging trial provides full feature access for 90 days, allowing you to evaluate event logging performance, estimate daily ingest rates, and determine storage requirements. Gain valuable insights to select the optimal subscription and ensure continuous access to your firewall security data in the Cisco cloud.

Purchase a data storage plan that matches the daily event volume your onboarded security devices send to Cisco cloud. This volume is referred to as your daily ingest rate. Before making a purchase, participate in a free trial of Security Analytics and Logging to accurately estimate your daily ingest rate.

Summary

The key components involved in the Security Analytics and Logging subscription process are:

- Customer: Starts trial, evaluates performance, and determines subscription requirements
- Cisco representative or authorized partner: Facilitates subscription purchase
- Security Cloud Control administrator: Claims and activates subscription
- Trial period: 90 days with full feature access for evaluation
- Grace periods: 90 days for trial data retention, 180 days for paid subscription data retention

Workflow

These are the stages of subscribing to a Security Analytics and Logging license:

1. The customer starts a Security Analytics and Logging trial subscription to evaluate requirements and performance.
   - With this trial plan, you gain access to all Security Analytics and Logging features for 90 days.

- During the 90-day trial period, your onboarded firewalls send events to Security Analytics and Logging. Monitor your event ingestion rates, understand your storage requirements, and evaluate performance. This data helps you to plan and select the most appropriate paid subscription.
- If you activate a paid Security Analytics and Logging subscription while a trial is active, Security Cloud Control replaces the trial license for the product instance with the paid license and ends the trial.
- If you choose not to apply the paid subscription to the trial, event ingestion automatically stops after 90 days. After this, you cannot access Security Analytics and Logging features. However, your existing log data remains in the Security Analytics and Logging cloud for an additional 90 days from the trial expiry date.

> **Note**
>
> If you do not subscribe to a paid Security Analytics and Logging license within this 90-day grace period, all your trial data is permanently deleted.

This stage enables the customer to gain hands-on experience with Security Analytics and Logging capabilities and accurately determine their subscription requirements.

2. The customer orders a paid Security Analytics and Logging subscription based on trial insights.
   - Use the insights that you gained from your trial (daily ingest rate, required retention, storage volume) to determine the most suitable Security Analytics and Logging subscription plan.
   - Work with your Cisco representative or authorized partner to purchase the appropriate Security Analytics and Logging subscription.

   This stage ensures the customer selects a subscription plan that matches their actual usage requirements and establishes the commercial relationship.
3. The Security Cloud Control administrator claims the Security Analytics and Logging subscription to activate it.

   After you purchase a new Security Analytics and Logging subscription, you receive a claim code to activate it within Security Cloud Control. A welcome email containing your subscription claim code is automatically sent to the Provisioning Contact you specified during the purchasing process. If you included an End Customer contact, they also receive a copy. You will receive this email on the requested start date of your subscription.

   A Security Cloud Control administrator uses the claim code to activate the subscription for their organization. For detailed instructions on claiming and activating subscriptions, refer to Claim a Subscription.

   This stage completes the activation process and makes the paid subscription services available to the organization.
4. The customer maintains their Security Analytics and Logging subscription through timely renewal.

   Maintaining an active Security Analytics and Logging subscription ensures continuous logging and access to your historical data.
   - If your Security Analytics and Logging subscription expires without renewal, event ingestion from your firewalls stops immediately.
   - You can continue to view and search existing event data for 90 days after the subscription expires. After 90 days, event data is no longer accessible.
   - Your existing data remains in the Security Analytics and Logging cloud for a 180-day grace period from the subscription expiry date.
   - If the Security Analytics and Logging subscription is not renewed within this 180-day grace period, all your event data is permanently deleted from the Security Analytics and Logging cloud.

This stage ensures continuous service availability and prevents data loss through proactive subscription management.

Result

The subscription process results in continuous access to Security Analytics and Logging logging services, properly sized to match actual usage requirements, with established renewal processes to prevent service interruption and data loss.

View Security Analytics and Logging license information

Configure monitoring of your Security Analytics and Logging license to track storage limits and retention periods. The dashboard helps you optimize event data management, prevent overages, and maintain compliance within your Security Cloud Control subscription.

Monitor your Security Analytics and Logging license to track storage limits and retention periods to optimize event data management and prevent overages.

View your Security Analytics and Logging license information such as the entitled monthly storage limit and the event storage retention period. If you do not have a separate Security Analytics and Logging license and data plan, you see the 90-day rolling data storage details in the licensing information.

Procedure

1. Choose **Administration** > **Logging Settings**.
2. Click **View Logging Storage Usage**.

> **Tip**
>
> Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** and then click the **View Dashboard** button to view the Security Analytics and Logging license information.
>
> The **Event Logging Overview** dashboard provides a comprehensive overview of your Security Analytics and Logging license subscription:
>
> - **Retention policy**: Displays the event log retention period according to your subscription. Event data that is older than your retention period is removed daily, and you always retain access to all event data within your full retention period.
> - **Storage capacity**: Displays the total entitled data under your Security Analytics and Logging license, the amount of storage currently used, and the remaining available storage.

The Security Analytics and Logging license information is displayed, showing your entitled monthly storage limit, event storage retention period, and current usage details.

View Security Analytics and Logging Storage usage and event ingest rate

Configure insights into storage usage and event trends in Security Cloud Control with interactive dashboards.

Gain insights into storage usage and event trends in Security Cloud Control with interactive dashboards. Regular analysis helps you optimize event logging, adjust storage settings, prevent overages, and maintain efficient compliance and performance across your security environment.

View the current Security Analytics and Logging storage utilization and analyze event logging trends. You can analyze the storage utilization trends by event type, device type, and individual devices to gain deeper insights into storage utilization

patterns. Use the data visualizations for quick and easy analysis. This helps you assess the current storage capacity and take measures to reduce the logging rate if the storage utilization approaches the limits that are specified in your Security Analytics and Logging license.

Procedure

1. Choose **Administration** > **Logging Settings**.
2. Click **View Logging Storage Usage**.

   Tip

   Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click the **View Dashboard** button to view the Security Analytics and Logging storage usage and event ingestion trends.

3. Use these dashboards to customize and analyze storage utilization and gain insights into event logging trends in your firewall deployment:
   - **Usage Trends**: Displays the event logging storage usage for the last 12 months. Hover over a bar to see the data usage for the corresponding month.
   - **Events per second (EPS) trends**: Displays the event ingest rate for the onboarded devices. Customize your events per second trends view for a specific time period or device to get more granular data. You can filter the data for the past 1 week, 2 weeks, 3 weeks, or 1 month.

     Note

     The device drop-down list displays the managed firewall devices that are sending events to the Cisco Security Cloud.

   - **Utilization by event type trends**: Displays event data storage used, in bytes per day, for different event types. Use this widget to monitor storage use by event types and identify surges, if any, or unusual changes in storage use for specific event types. This insight enables you to adjust logging settings for a specific event type and manage storage use.
   - **Utilization by device type trends**: Displays event data storage used, in bytes per day, for each managed device type. Use this widget to monitor storage use by the device type and identify surges, if any, or unusual changes in storage use for a specific type of device.
   - **Utilization by device trends**: Displays event data storage used, in bytes per day, for each security device that sends events to Security Cloud Control. This widget focuses on devices with storage use exceeding the average bytes per second value, showing only the top five devices to improve usability. Use this widget to monitor storage use for each device and identify surges or unusual changes. This insight allows you to adjust logging settings for specific devices and manage storage use effectively.

You can view storage utilization and event logging trends across multiple dashboards, allowing you to monitor usage patterns and make informed decisions about storage settings and event logging configurations.

Monitor Security Analytics and Logging service availability

Verify Security Analytics and Logging service availability, review FTD device event logging status, and check when Security Analytics and Logging last received events from managed Firewall Threat Defense devices.

Monitor the availability and health of Security Analytics and Logging(SaaS) service, review Firewall Threat Defense device event logging status, and determine when Security Analytics and Logging last received events from managed devices.

> **Note**
>
> The **Service Status** tab currently supports Firewall Threat Defense devices.

Before you begin

Enable the managed Firewall Threat Defense devices to send events to the Security Analytics and Logging cloud so you can view meaningful device logging status and last-event details.

Procedure

1. Choose **Administration** > **Logging Settings**.
2. Click **View Logging Storage Usage**.

   > **Tip**
   >
   > Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** and then click the **View Dashboard** button to view the Security Analytics and Logging service status.

3. Click the **Service Status** tab.
4. Review the **SAL Service Availability** widget to check the current Security Analytics and Logging service status.

   If the Security Analytics and Logging service status displays **Degraded**, your Security Analytics and Logging service is affected and event ingestion might be delayed or disrupted.

5. Check the **Last Event Received** widget to determine when Security Analytics and Logging last received an event from a device.
6. Review the **Firewall Logging Status** widget to check Firewall Threat Defense device event logging status.
   - **Connected**: Indicates the number of Firewall Threat Defense devices that are enabled to send events to the Security Analytics and Logging.
   - **Disabled**: Indicates the number of Firewall Threat Defense devices that are disabled from sending events to the Security Analytics and Logging.
7. In the **Firewall Details** list, check when each Firewall Threat Defense device last sent an event to Security Analytics and Logging.

   Use this information along with **SAL Service Availability** and **Last Event Received** widgets to identify whether events might be delayed or not ingested.

You have reviewed the Security Analytics and Logging service status, device logging configuration, and last event timestamps to ensure proper event ingestion and identify any potential issues with the service or device connectivity.

Extend event storage duration and increase event storage capacity

Configure your Security Analytics and Logging license to extend event storage from the default 90 days to up to three years and increase storage capacity for long-term data retention and compliance.

Upgrade your Security Analytics and Logging license to extend event storage from the default 90 days to up to three years. Enhancing storage capacity ensures long-term data retention, compliance, and improved security visibility for network monitoring.

Perform this task when your organization needs increased event storage or retention.

Procedure

1. Log in to your account on Cisco Commerce.
2. Select your Security Cloud Control PID.
3. Follow the prompts to upgrade the duration or capacity of your storage.

   The increased cost will be prorated based on the term remaining on your existing license. See the Guidelines for Quoting Cisco Defense Orchestrator Products for detailed instructions.

Your Security Analytics and Logging license is upgraded with extended event storage duration and increased storage capacity based on your selected options.

View Security Analytics and Logging alerts

Configure real-time alerts for Security Analytics and Logging configuration and event issues on firewall devices. Addressing notifications promptly helps prevent data loss, maintain compliance, and ensure reliable security monitoring for your network.

Monitor and address Security Analytics and Logging configuration and event issues to maintain security compliance and prevent data loss.

View alerts and notifications for the Security Analytics and Logging configurations and event settings for the managed firewall devices.

Procedure

1. Choose **Administration** > **Logging Settings**.
2. Click the **View Logging Storage Usage** button.

   Tip

   Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click **View Dashboard** to view the Security Analytics and Logging license information.

   The **Alerts and Notifications** section displays alerts about the settings that impact event logging. These alerts enable you to take action to resolve any issues. Some of these settings include:

   - Sending events to cloud setting is disabled.

- Sending events to the cloud setting is disabled at device level.
- Secure Event Connector becomes unavailable.
- Increase in events ingestion rate.
- Security Analytics and Logging license is expired or the allotted data storage is exceeded.

The **Alerts and Notifications** section displays current alerts for Security Analytics and Logging configurations and event settings, enabling you to identify and resolve issues that may impact event logging.

Frequently asked questions about Security Analytics and Logging license

Lists common questions about Security Analytics and Logging data allotment, storage management, license expiration, and retention periods.

Learn which events count toward your Security Analytics and Logging data allotment, how to manage storage limits, what happens if your license expires, and how retention periods affect long-term data storage. Gain practical tips to optimize storage and maintain continuous access to your security event data.

Which data gets counted against my Security Analytics and Logging allotment?

All events sent to the Cisco cloud directly or to the Secure Event Connector accumulate in Security Analytics and Logging and count against your data allotment.

Filtering the events viewer does not decrease the number of stored events in Security Analytics and Logging. It only reduces the number of events you see in the events viewer.

We're using up our storage allotment quickly. what should i do?

Here are two approaches to address that problem:

- Request more storage.
- Consider reducing the number of rules that log events. You can log events from SSL policy rules, security intelligence rules, access control rules, intrusion policies, and file and malware policies. Review your current logging settings to determine if you need to log events from all the rules and policies that you have configured.

What happens to my data if my Security Analytics and Logging license expires?

If your paid Security Analytics and Logging license expires, event ingestion from your firewalls stops immediately. However, your existing data remains accessible in the Security Analytics and Logging cloud for a 180-day grace period. If you renew your paid license during this grace period, your service continues without interruption. If you do not renew within these 180 days, all your data is permanently deleted.

If I purchase a Security Analytics and Logging subscription with a 1-year retention period and a 5-year term, will my data be stored for all 5 years?

The retention period defines how long each log is stored. With a 1-year retention period, only the most recent 1-year log data is available at any given time. Log data older than 1 year is overwritten or deleted when new data is collected. A 5-year term means that data for that duration will continue to be ingested, but the retention limit is applicable to the log data itself.

Security Analytics and Logging for Catalyst SD-WAN

Describes how Catalyst SD-WAN integrates advanced firewall and security features for centralized policy enforcement and secure cloud access. Explains how onboarding devices to Security Cloud Control enables centralized monitoring and analysis of connection events.

Security Analytics and Logging for Catalyst SD-WAN is a security management solution that

- integrates advanced firewall and security features directly into the SD-WAN fabric
- enables centralized policy enforcement and secure cloud access through Direct Internet Access (DIA) and Direct Cloud Access (DCA)
- provides centralized monitoring and analysis of connection events when devices are onboarded to Security Cloud Control, and
- supports threat hunting and comprehensive security management across distributed networks.

Security capabilities

The Secure Router integrates firewall capabilities into its architecture, ensuring robust security across distributed networks.

- Catalyst SD-WAN integrates security features directly into the SD-WAN fabric, enabling secure Direct Internet Access (DIA) and Direct Cloud Access (DCA).
- It includes next-generation firewall, integrated intrusion prevention capabilities, and URL filtering.
- The Catalyst SD-WAN platform enables you to enforce centralized policies for all users, extending enterprise VPN architectures into your private cloud.

Onboard Catalyst SD-WAN Manager to Security Cloud Control to manage the security capabilities of managed devices.

- Onboarded Catalyst SD-WAN devices send connection events to Security Analytics and Logging for storage in the cloud data store.
- Security Analytics and Logging enables you to view connection events from all Catalyst SD-WAN devices in one centralized location–the **Event Logging** page in Security Cloud Control.
- On the **Event Logging** page, you can view, filter, and search for events to perform threat hunting and analyze security rules triggered in your network.

How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management

Describes how Catalyst SD-WAN event flow enables automated sharing of security events with Security Cloud Control, allowing seamless data export, cloud storage, and enrichment for enhanced threat detection.

This process describes how Catalyst SD-WAN shares security events with Security Cloud Control Firewall Management in Security Cloud Control. This integration streamlines event visibility and analysis, empowering SOC analysts to monitor network activity and enhance threat detection using Catalyst SD-WAN security data in real time.

Summary

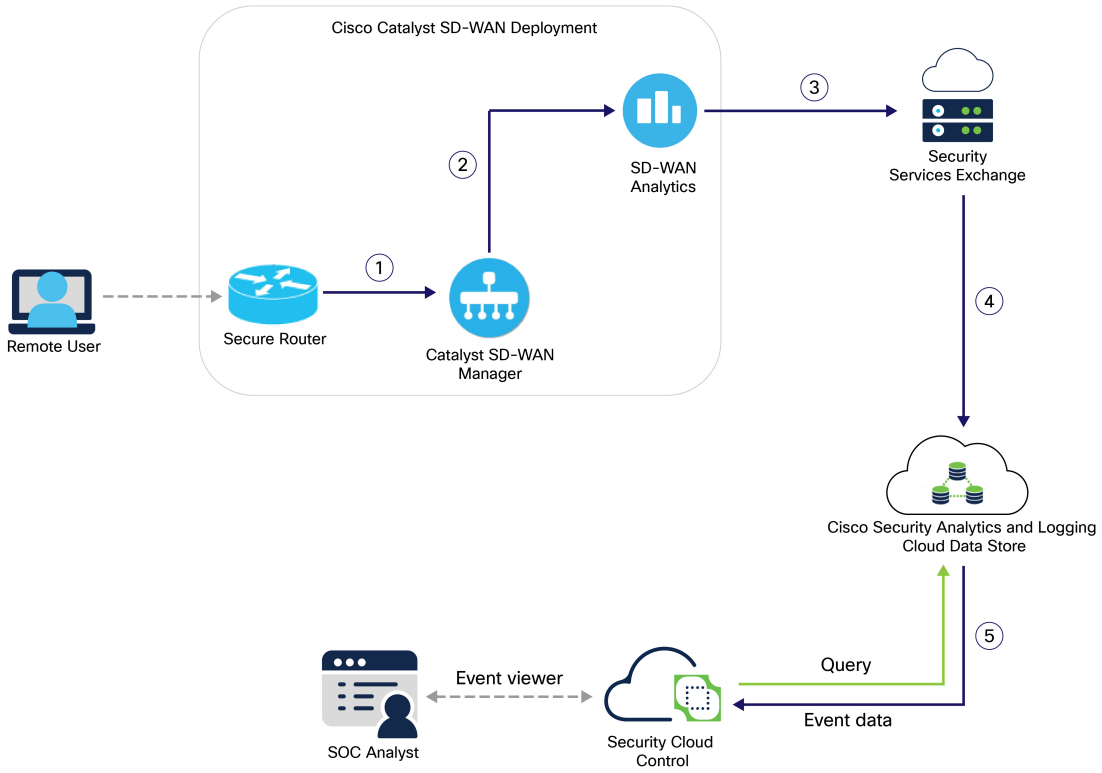
The key components involved in the event sharing process are:

- Catalyst SD-WAN device: Generates event logs for network traffic and exports data to PSV files
- Catalyst SD-WAN Manager: Receives event data from SD-WAN devices and forwards to analytics cloud

- SD-WAN Analytics cloud: Stores event data and notifies Security Services Exchange
- Security Services Exchange: Downloads event data and converts from PSV to JSON format
- Security Analytics and Logging (SaaS): Processes, classifies, and enriches event data for SOC analysts

Workflow

Figure 1: Event flow from Catalyst SD-WAN to Security Cloud Control



These stages describe how security events flow from Catalyst SD-WAN to Security Cloud Control:

1. A remote user accesses the network, and the Catalyst SD-WAN device generates an event log for the corresponding traffic. The device then exports the event data to a PSV file and sends it to Catalyst SD-WAN Manager.
2. Catalyst SD-WAN Manager sends the event data to the SD-WAN Analytics cloud.
3. SD-WAN Analytics stores the event data in cloud to make it accessible for Security Services Exchange and notifies Security Services Exchange.

   After receiving the notification from SD-WAN Analytics cloud, Security Services Exchange downloads the event data from SD-WAN AWS cloud.
4. Security Services Exchange converts the event data from PSV to JSON format and sends it to Cisco Security Analytics and Logging (SaaS).
5. Security Analytics and Logging (SaaS) processes the event data using various services to classify and enrich it for use by Security Cloud Control.

   Security Analytics and Logging (SaaS) stores the event data in the cloud data store. The event viewer queries this data store to provide security operations center (SOC) analysts with relevant event data.

Requirements and guidelines for SD-WAN integration

Outlines the requirements and guidelines for onboarding Catalyst SD-WAN Manager to Security Cloud Control for centralized visibility of connection events.

Onboard the Catalyst SD-WAN Manager to the Security Cloud Control organization where you want to view the security events.

Onboard the SD-WAN Analytics services to your Catalyst SD-WAN Manager and enable data collection.

Ensure you have a Security Cloud Control Firewall Management organization with a valid Security Analytics and Logging subscription plan.

Note that this integration supports only viewing the connection events from your Catalyst SD-WAN devices in Security Cloud Control.

Ensure that you have a Security Analytics and Logging subscription plan that reflects the number of events the Cisco cloud receives from your on-boarded Catalyst SD-WAN devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your data plan.

If you do not have a Security Analytics and Logging plan subscribed, you can request a 90-day trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events** > **Event Logging** tab. You can accurately estimate your daily ingest rate and purchase the desired subscription plan by following the instructions in the Security Cloud Control Firewall Management Ordering Guide.

View Catalyst SD-WAN events in Security Cloud Control Firewall Management

Configure filtering for Catalyst SD-WAN connection events in the event logging page to quickly identify network activity and security events.

This task enables you to streamline event analysis, enhance threat detection, and maintain compliance by filtering specific network events.

Network administrators should perform this task regularly for effective security monitoring. Use this feature to focus on relevant connection events and improve your network security posture.

Before you begin

Ensure that you have met all the requirements described in Requirements and guidelines for SD-WAN integration on page 61.

Follow these steps to view Catalyst SD-WAN events in Security Cloud Control Firewall Management:

Procedure

1. In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.
2. Click the filter (▼) icon.
3. Scroll to the **Catalyst SD-WAN Events** section and check the **Connection** check box.

The event logging page displays filtered Catalyst SD-WAN connection events, allowing you to focus on relevant network activity and security events for analysis.