Managing Cisco Catalyst SD-WAN Firewall Capabilities with Security Cloud Control

First Published: 2025-04-19

Last Modified: 2025-08-19

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

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

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 1

Overview of Security Cloud Control

An Introduction to Security Cloud Control

Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation.

Security Cloud Control helps you optimize your security policies by identifying inconsistencies with them and by giving you tools to fix them. Security Cloud Control gives you ways to share objects and policies, as well as make configuration templates, to promote policy consistency across devices.

Because Security Cloud Control coexists with local device managers such as the Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by Security Cloud Control and by other managers, and then reconcile the differences between managers.

Security Cloud Control has an intuitive user interface that allows you to 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 also provides a guided "Day 0" experience helping you quickly onboard threat defense devices to your on-premises or cloud-delivered Firewall Management Center. It also presents you with other key features you may benefit from and helps you enable and configure them.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively "Cisco") are committed to protecting your privacy and providing you with a positive experience on our websites and while using our products and services ("Solutions"). Please read Cisco Online Privacy Statement carefully to get a clear understanding of how we collect, use, share, and protect your personal information.

Security Cloud Control Licenses

Security Cloud Control requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control 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 gives you a Security Cloud Control organization, and for every device you choose to manage using Security Cloud Control, you need separate device licenses.

To onboard and manage devices from Security Cloud Control, you need to 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 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 for three years, if you purchase a three-year software subscription to the Cisco Firepower 1010 device.

Note Catalyst SD-WAN doesn't require an additional license. Customers using DNA or WAN Essentials license will be able to integrate with Security Cloud Control.

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

Note You can integrate with Security Cloud Control leveraging your existing DNA Essentials/Advantage licensing. This will also extend to WAN Essentials/Advantage, and no other license is required. For logging into Security Analytics and Logging, you should be on the DNA Advantage (or WAN Advantage) license as well as purchase a separate Security Analytics and Logging license

Note You cannot manage Security Cloud Control licensing through the Cisco smart licensing portal.

Software Subscription Support

The Security Cloud Control 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 the software support is selected by default, you can also leverage the Security Cloud Control solution support based on your requirement.

Security Cloud Control Platform Maintenance Schedule

Security Cloud Control 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 this maintenance period, you can still access your organization and if you have a cloud-delivered Firewall Management Center or Multicloud Defense Controller, you can access those portals as well. Additionally, the devices that you have onboarded to Security Cloud Control continue to enforce their security policies.

Note

- We advise against using Security Cloud Control to deploy configuration changes on the devices it manages during maintenance periods.
- If there is any issue that stops Security Cloud Control from communicating, we address that failure on all affected tenants as quickly as possible, even if it is outside the maintenance window.

CHAPTER 2

Sign in to Security Cloud Control

Get Started With Security Cloud Control

The **Get started with Security Cloud Control** is an intuitive interface that guides you through sequential tasks for efficiently setting up and configuring your firewalls.

Sign in to Security Cloud Control and in the top menu, click (🚀).

- The **Manage firewalls** page provides links to:
  - Onboard and manage Catalyst SD-WAN.
  - Subscribe to receive notifications for troubleshooting common issues.

Sign in to Security Cloud Control

To sign in to Security Cloud Control, you need a Cisco Security Cloud Sign On account. If you don’t have an account, you can create one using Creating a Security Cloud Sign On Account and configure multifactor authentication with either Duo MFA or Google Authenticator.

If you have only one organization associated with your account, it is always the default account when you log in. If you have multiple organizations that are associated with your account, the one that you used last is selected after you sign in.

- Open Security Cloud Control at https://security.cisco.com/.
- Sign in with your Security Cloud Sign On credentials and MFA options that you established when creating your account.

The Security Cloud Control Dashboard

The Security Cloud Control dashboard is your central hub for monitoring and managing organization-level details across various categories. Upon logging in, you can access a customizable dashboard that offers critical insights and actions to optimize security and operational efficiency.

Customize Your Dashboard

Make your dashboard fit your specific needs by customizing the visible widgets.

1. On the **Home** page, click **Customize**.
2. Select or deselect the widgets you want to view on the dashboard.
3. You can drag and drop the widgets to arrange them as you prefer.

- **Top Intrusion and Malware Events**: Helps you monitor and respond to top intrusion and malware events. The widget displays Intrusion Events and Malware Events and allows you to filter data for the last 90, 60, and 30 days. You can filter between Allowed (default) and Blocked events.

Note Catalyst SD-WAN Manager will show the data for the last 30 days only on cross launch.

Announcements

Click the **Announcements** icon to view the most recent Security Cloud Control features and updates. Links to related documentation are provided if you need more information on any of the items listed.

CHAPTER 3

Overview of Catalyst SD-WAN Devices

An Introduction to Catalyst SD-WAN Devices

Catalyst SD-WAN devices are advanced networking solutions designed to provide secure, high-performance connectivity. These devices integrate SD-WAN capabilities with robust security features, enabling organizations to connect users to applications seamlessly across multicloud environments, branch offices, and data centers.

Supported Operations on Catalyst SD-WAN Devices

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.

  See About Security Devices Page.
- View the configuration file of the onboarded devices.
- Cross-launch policy groups on the Catalyst SD-WAN platform.

Note A given Security Cloud Control organization can be onboarded to only one Catalyst SD-WAN Manager.

View Configuration of Catalyst SD-WAN Devices

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

Procedure

Step 1 In the left pane, choose **Manage** > **Security Devices**.

Step 2 Click the **WAN Branch Edge** tab.

Step 3 Select a device and click **Configuration**.

Step 4 To export the list of devices as a CSV file, click the ⬇ icon.

Cross-Launch Policy Groups on Catalyst SD-WAN

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

Procedure

Step 1 In the left pane, click **Manage** > **Security Devices**.

Step 2 Click the **WAN Branch Edge** tab.

Step 3 Select a device and click **Policy Groups**.

CHAPTER 4

Integrate Catalyst SD-WAN Manager with Security Cloud Control

Overview of Catalyst SD-WAN integration with Security Cloud Control

Cisco's SD-WAN solutions, including the Catalyst and Secure Router series, are designed to seamlessly integrate with Cisco's security portfolio, offering comprehensive control and management over network security features.

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

Security Cloud Control provides:

- **Security Discovery**: Identifies existing security configurations and policies through the onboarded Catalyst SD-WAN Manager.
- **Policy Creation**: Enables the creation of new security objects and policies using its platform.

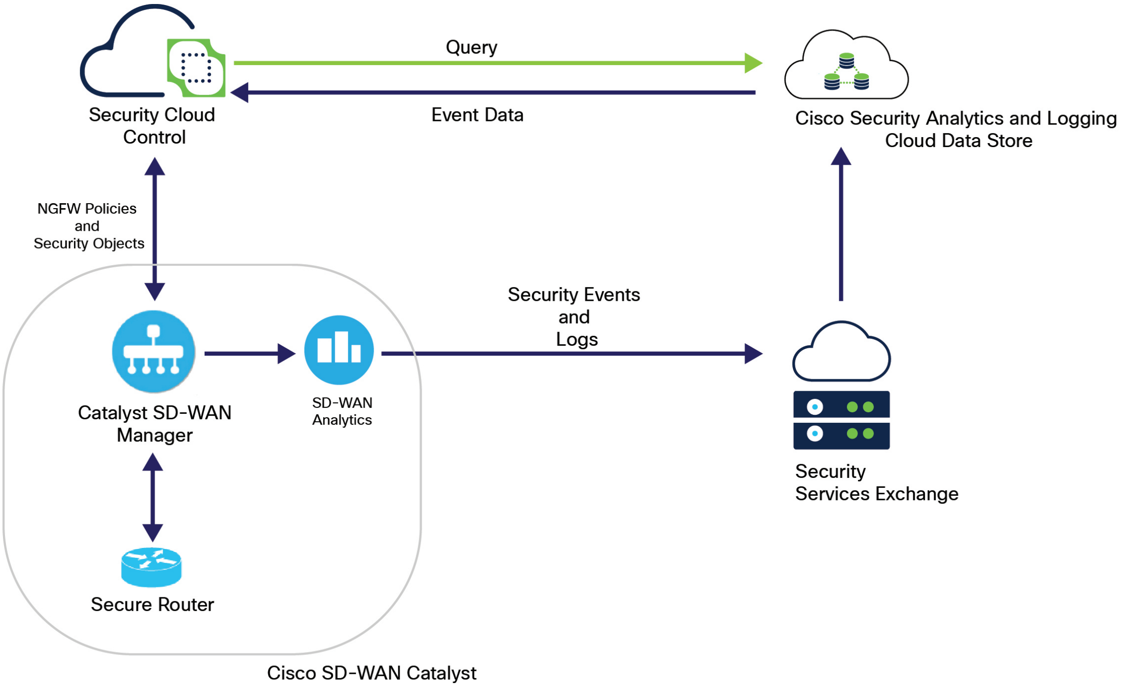
- **Cohesive Strategy**: Supports a cohesive strategy for implementing security objects, policies, and profiles across multiple Cisco solutions.
- **Log and Analytics Viewing**: Offers capabilities for viewing logs and analytics data.
- **View intrusion and malware events**: Displays intrusion and malware events detected within the network from Secure Router.

System Topology Diagram

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

The following topology diagram illustrates the integration of Catalyst SD-WAN with Security Cloud Control and other cloud services. It 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 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:

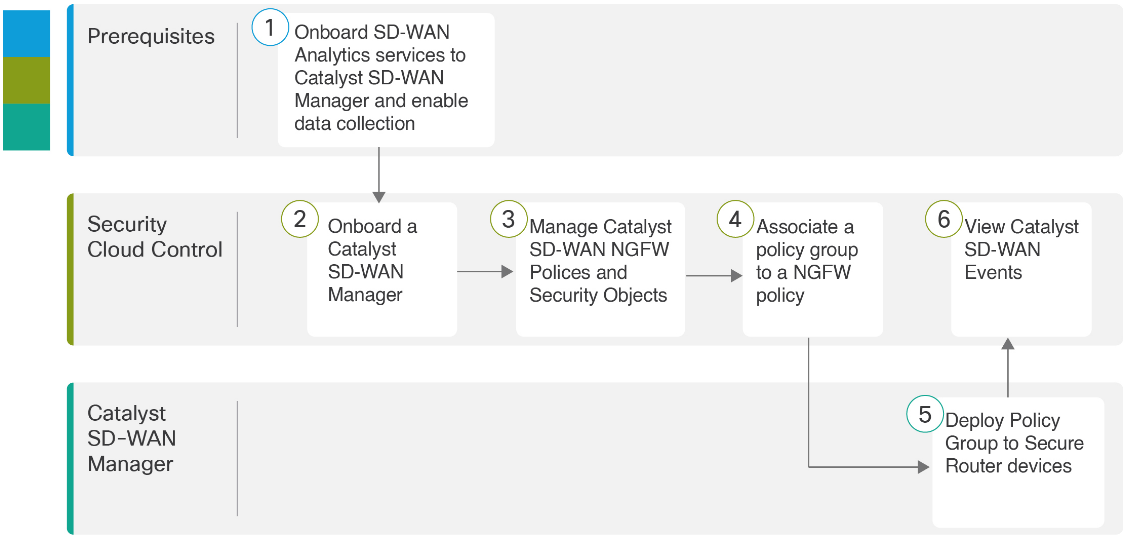
  - **Catalyst SD-WAN Manager:** Manages the SD-WAN fabric and shows NGFW policies and security objects on the Security Cloud Control when onboarded to it. The Catalyst SD-WAN Manager sends the event data received from the Secure Router to **SD-WAN Analytics**.
  - **SD-WAN Analytics**: Provides analytics 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 the **Security Services Exchange**, which obtains the analytics data from the 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

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


Prerequisites
1
Onboard SD-WAN Analytics services to Catalyst SD-WAN Manager and enable data collection
Security Cloud Control
2
Onboard a Catalyst SD-WAN Manager
3
Manage Catalyst SD-WAN NGFW Polices and Security Objects
4
Associate a policy group to a NGFW policy
6
View Catalyst SD-WAN Events
Catalyst SD-WAN Manager
5
Deploy Policy Group to Secure Router devices

Step	Application	Description
1	Prerequisites	Onboard the SD-WAN Analytics services to the Catalyst SD-WAN Manager and enable data collection. For more information, see Onboard Cisco SD-WAN analytics.

Step	Application	Description
2	Security Cloud Control	Onboard a Catalyst SD-WAN Manager that also imports 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 NGFW policies. For more information, see Manage security objects and profiles and Manage NGFW policies.
4	Security Cloud Control	Associate a group policy to a Catalyst SD-WAN NGFW policy. For more information, see Associate a group policy.
5	Catalyst SD-WAN Manager	Deploy 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

Here are the 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: From 20.18 version of Catalyst SD-WAN Manager, devices supported by the last two versions are compatible; for example, for Catalyst SD-WAN Manager 20.18, there is backward compatibility with the devices of the last two versions, that is, 20.15 and 20.12 devices. Contact Cisco TAC to check and drop any non-compatible indexes. For more information, see Cisco SD-WAN Control Components Compatibility Matrix.

Onboard a Catalyst SD-WAN Manager to Security Cloud Control Firewall Management

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

Note Once Catalyst SD-WAN Manager is onboarded to Security Cloud Control, security operations (management of policies, objects, and profiles) can be carried out only from Security Cloud Control.

Version Control feature is not supported in Security Cloud Control.

Before you begin

- You have Smart Account Administrator or Virtual Account Administrator privileges on a virtual account that is 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 should know the **Organization Name** of your Catalyst SD-WAN Manager, as it will be required during the onboarding process.

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

     The **Organization Name** field provides the information. It is a unique identifier used to establish secure control connections within the SD-WAN environment.

- Ensure easy onboarding is successful with **Service Access Authorization** enabled.

  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 the Catalyst SD-WAN Manager, regardless of their **Device Status**, will be onboarded to Security Cloud Control Firewall Management.

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

Procedure

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

Step 2 Click the + icon at the top-right corner of the **Catalyst SD-WAN** tab.

Step 3 Click the **Catalyst SD-WAN Manager** tile.

Alternatively, you can use the **Get started with Security Cloud Control** interface to onboard Cisco 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.

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

The organizations displayed in the list are based on the region where the Security Cloud Control is deployed.

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

Labels are applied to the device after it is onboarded to Security Cloud Control. Labels allow you to group devices and filter them in the **Security Devices** page.

Step 6 Click **Close** after verifying the details of the Cisco Catalyst SD-WAN Manager you are onboarding.

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

After a successful onboarding, the following information is displayed in the Security Cloud Control:

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

What to do next

In the **Management** pane on the right, click **Devices** to see the onboarded Secure Router devices.

Remove Catalyst SD-WAN Manager from Security Cloud Control Firewall Management

Removing the Catalyst SD-WAN Manager will also automatically remove the associated devices, policies, and objects from the Security Cloud Control Firewall Management.

Note When you deboard Catalyst SD-WAN Manager from Security Cloud Control, all the policies and objects you create through Security Cloud Control are deleted from it, but remain in Catalyst SD-WAN Manager. You can now modify security objects and policies from the Catalyst SD-WAN Manager.

Procedure

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

Step 2 Select the manager that you want to delete, and then click **Remove SD-WAN Devices**.

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

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

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 RBAC (Role-Based Access Control) models across these platforms are aligned to ensure consistent and seamless user actions.

A user with elevated permissions in Security Cloud Control 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 without appropriate permissions in Catalyst SD-WAN Manager will result in errors. For example: a user assigned the 'Super Admin' role in Security Cloud Control will be unable to save NGFW security policies changes to Catalyst SD-WAN Manager if they are assigned the 'Operator' role in the latter.

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

Table 1:

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

Security Cloud Control Role Name	Catalyst SD-WAN Manager Role Name	Allowed Actions
Edit Only	security_operations	- Not allowed to onboard or deboard Catalyst SD-WAN Manager - Unrestricted access to all functions in Security Cloud Control - Allocated SecOps user role in Catalyst SD-WAN Manager

How Security Cloud Control Firewall Management Manages Catalyst SD-WAN NGFW Capabilities

When the Catalyst SD-WAN Manager is integrated with Security Cloud Control Firewall Management, the existing NGFW policies, security objects, and security profiles from the Catalyst SD-WAN Manager are automatically imported into the Security Cloud Control. Users can modify these NGFW parameters or create new ones directly from Security Cloud Control. All the changes made in Security Cloud Control are synchronized and saved within the Catalyst SD-WAN Manager.

After the Catalyst SD-WAN Manager is onboarded to Security Cloud Control, the management of policies, objects, and profile can no longer be performed through the Catalyst SD-WAN Manager. Instead, these management tasks must be carried out exclusively from Security Cloud Control.

A "*Managed by Security Cloud Control (SCC)*" banner will be displayed on the Catalyst SD-WAN Manager that is onboarded to Security Cloud Control, indicating the integration. This message can be viewed in the Catalyst SD-WAN Manager by navigating to the relevant configuration sections:

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

Restrictions for Security Cloud Control and Catalyst SD-WAN Manager Integration

- **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, objects, and profiles**

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

- **Customized IPS profiles not supported**

  Security profiles do not support IPS policies (Signature set objects) that are editable or customized.

- **Live logs unavailable with SAL**

Live logs cannot be viewed on Security Cloud Control using Cisco Security Analytics and Logging. You can only view historical events.

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

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

- **On-Prem multitenant Catalyst SD-WAN Manager not supported**

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

- **Dark mode not supported**

  It is recommended not to enable dark mode in Security Cloud Control when Catalyst SD-WAN Manager is integrated.

Note Changes can be made to the NGFW policies, objects, and profiles from the Catalyst SD-WAN Manager after it has been deboarded from Security Cloud Control.

Security Cloud Control allows you to perform the following operations:

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

Policy deployment to Secure Router devices

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

View Intrusion Events

The Intrusion Prevention System (IPS) detects and blocks network intrusions and malicious activities based on Cisco Talos threat intelligence.

The **Top Intrusion & Malware Events** dashlet on the Security Cloud Control 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

Step 1 In the Security Cloud Control platform menu, click **Dashboard**.

Step 2 Navigate to the **Top Intrusion & Malware Events** dashlet.

Step 3 Click **SDWAN** under **Data Sources**.

Step 4 Click the **Intrusion Events** tab.

Step 5 Select **Blocked** from the dropdown on the right of the dashlet; by default, **Allowed** is selected.

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

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

Step 7 Navigate to the **Intrusion Prevention** dashlet to view the event.

View Malware Events

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 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

Step 1 In the Security Cloud Control platform menu, click **Dashboard**.

Step 2 Navigate to the **Top Intrusion & Malware Events** dashlet.

Step 3 Click **SDWAN** under **Data Sources**.

Step 4 Click the **Malware Events** tab.

Step 5 Select **Blocked** from the dropdown on the right of the dashlet; by default, **Allowed** is selected.

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

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

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

Additional Resources

- 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

CHAPTER 5

Manage Catalyst SD-WAN Security Objects and Security Profiles

An Introduction to Catalyst SD-WAN Security Objects and Security Profiles

Security objects and security profiles in Catalyst SD-WAN Manager are the foundational building blocks for defining and enforcing security NGFW policies. They ensure that your network is protected from threats while maintaining seamless connectivity and application performance.

Create new Catalyst SD-WAN Security Objects and Security Profiles

This section provides the steps to create new Catalyst SD-WAN objects and profiles using Security Cloud Control Firewall Management.

Procedure

Step 1 In the left pane, click **Manage** > **Objects**.

Step 2 Click the **WAN Branch Edge** tab.

Step 3 Click the **Create Object** (+) icon.

Step 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

Step 5 Click **Save**.

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

SDWAN Application List

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

Table 2: Application

Field	Description
Object Name	Name of the application list.
Application List	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," and so on.

Field	Description
Application Family	The **Application Family** groups applications based on their functional category, for example, "Web," "Instant Messaging," "Network Services," and so on.

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

SDWAN Data Prefixes

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

Table 3: SDWAN Data Prefixes

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

SDWAN FQDN

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

Table 4: Application

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

SDWAN Geolocation

Allows you to configure firewall rules based on geographical locations rather than IP addresses.

Table 5: Geolocation

Field	Description
Object Name	Name of the geolocation object.
Geolocation	Select one or more geo locations from the drop-down list. For example, Africa, Antartic, Asia, Europe, and so on.

SDWAN Identity

Table 6: SDWAN Identity

Field	Description
Object Name	Name of the application list.
Users	The source of **Users** and **User Groups** is ISE AD, which is configured in Catalyst SD-WAN Manager.
User Groups	

SDWAN Port Object

A configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

Table 7: Port Object

Field	Description
Object	Name of the port object.
Port	The port values separated by comma. The range is 0 to 65530.

SDWAN Protocol Object

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.

Table 8: Protocol Object

Field	Description
Object Name	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, and so on.

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

SDWAN Security Group Tag

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 SGT as matching criteria.

You cannot create or edit an SGT in Security Cloud Control. All SGTs must be created in ISE.

Table 9: Security Group Tag

Field	Description
Object Name	Name of the security group tag.
Security Group Tags	Select the security group tag.

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

SDWAN Signatures

The signature set blocks vulnerability with a Common Vulnerability Scoring System (CVSS) score that is greater than or equal to 9. It also blocks Common Vulnerabilities and Exposures (CVEs) published in the last two years and that have the rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

Table 10: Application

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

SDWAN URL Allow List

The URL allow list object is used to define URLs that should be explicitly permitted through the SD-WAN's URL Filtering feature.

Here are some important points to note about these lists:

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

Table 11: URL Allow List

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

SDWAN URL Block List

The URL block list object is used to define URLs that should be denied through the SD-WAN's URL Filtering feature.

Table 12: URL Block List

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

SDWAN Zone

Zones are 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	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. The options are: • 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.

SDWAN Advanced Inspection Profile Policy

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.

Table 14: Advanced Inspection Profile Policy

Field	Description
Object Name	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.
TLS Action	Choose the TLS action. The options are: • Decrypt • Pass Through • Do not Decrypt

SDWAN Advanced Malware Protection Policy

Note that for some advanced configurations, a Threat Grid Server configuration is required in Catalyst SD-WAN.

Table 15: Advanced Malware Protection Policy

Field	Description
Object Name	Name of the advanced malware protection policy name.
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 that you want to be analyzed.

SDWAN Intrusion Prevention Policy

A security feature designed to detect and block known network attacks by leveraging predefined rules and signature.

Table 16: Intrusion Prevention Policy

Field	Description
Object Name	Name of the intrusion prevention policy.
Signature Set	Choose a signature set that defines the rules for evaluating traffic from the **Signature Set** drop-down list.
Inspection Mode	Choose 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.

SDWAN TLS/SSL Decryption Policy

The **TLS/SSL Decryption** object refers to a feature or configuration that enables administrators to inspect and manage encrypted traffic passing through the network.

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

Table 17: TLS/SSL Decryption Policy

Field	Description
Object Name	Name of the policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	
Expired Certificate	Defines what the policy should do if the server certificate has expired. The options are: • Drop: Drop traffic • Decrypt: Decrypt traffic

Field	Description
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: • 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. The options are **Enabled** or **Disabled**.
Unknown Revocation Status	Defines what the policy does, 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. • Decrypt: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • Drop: Drop the unsupported cipher suites. • Decrypt: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are close and open.
Certificate Bundle	Check the **Use default CA certificate bundle** checkbox to use the default CA.
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: TLS 1.0, TLS 1.1, TLS 1.2
Proxy Certificate Attributes	
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: 1024 bit RSA, 2048 bit RSA, 4096 bit RSA
EC Key Type	Defines the key type. The options are: P256, P384, P521
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

SDWAN TLS/SSL Profile 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, you need to 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 Policy

Field	Description
Object Name	Name of the TLS/SSL profile.
Categories to assign action	Set the categories between the 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.

SDWAN URL Filtering Policy

A security feature that allows administrators to control access to websites based on categories, reputation, and custom lists.

Table 19: URL Filtering Policy

Field	Description
Object Name	Name of the URL filtering policy.
Web Category	Choose the web category. The options are 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.
Allow URL List	Select an allow URL list.
Block URL List	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

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

Procedure

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

Step 2 In the left pane, click **Manage > Objects**.

Step 3 Click the **WAN Branch Edge** tab.

Step 4 Check the security object or profile you want to modify. You can use the filter to search an object.

Step 5 In the **Actions** pane on the right, click **Edit**.

Modify the configurations you want.

Step 6 Click **Save** to confirm.

Delete Catalyst SD-WAN Security Objects

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

- If the security object was synchronized with Catalyst SD-WAN Manager, its deletion will be reflected across both Security Cloud Control Firewall Management and Catalyst SD-WAN Manager to maintain consistency.
- Any security policies or configurations referencing 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 audit purposes, ensuring traceability of changes. To view the logs:
  - In the Security Cloud Control application, choose **Monitor** > **Events & Logs** > **Logs** > **Change Log**.
  - In the Catalyst SD-WAN Manager application, choose **Monitor > Logs > Audit Logs**.

Before you begin

Make sure the Catalyst SD-WAN security objects you intend to delete are not being used or referenced in other objects, policies, or configurations.

Procedure

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

Step 2 In the left pane, click **Manage > Objects**.

Step 3 Click the **WAN Branch Edge** tab.

Step 4 Check one or multiple security objects you want to delete.

Step 5 In the **Actions** pane on the right, click **Remove**.

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

Filter Catalyst SD-WAN Security Objects

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. Streamlining the management processes helps maintain optimal system performance.

Two filtering parameters used are **Object Type** and **Profile Type**.

1. In the left pane, choose **Manage > Objects**.
2. Click the **WAN Branch Edge** tab.
3. Click the filter (▼) icon and select for objects based on the object type or profile type.

You can use filters to search for the desired objects and further refine the results by typing the object name, IP address, or port number to narrow down the search within the results.

CHAPTER 6

Manage Catalyst SD-WAN Security Policies

An Introduction to Catalyst SD-WAN NGFW Security Policies

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 provides a comprehensive framework for both implementing and managing NGFW security policies.

Manage Existing Catalyst SD-WAN NGFW Security Policies

Note that you cannot delete an NGFW policy from Security Cloud Control Firewall Management that is already associated with a policy group in Catalyst SD-WAN.

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 Navigate to the policy and click the ellipsis (…) under the **Action** column.

Step 3 Click **View**, **Edit**, **Delete**, or **Copy**.

Create Catalyst SD-WAN Security Policies

Before you begin

Ensure that these devices are deployed and managed using a configurations group. For more information about creating configuration groups, see Configuration Groups and Feature Profiles.

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 On the **Catalyst SD-WAN NGFW Policies** page, click **Add NGFW Policy**.

This launches the Create NGFW policy workflow.

Step 3 On the **Security Policy Name** tab, enter **Policy Name** and **Description**, and under **Device Solution**, select the **sdwan** radio button and click **Next**.

Step 4 On the **Select the optional Configuration Group to associate with the security policy** page, choose the configuration group to associate with the NGFW policy and click **Next**.

Step 5 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.
Source Zone	Choose the zone that is the source of the data packets. The options are: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted To create a new Source Zone, click **+ Create New**. Enter the **Name** and select the **VPN**. Note that multiple VPNs can be selected within a Source Zone.

Field	Description
Destination Zone	Select the zone/s to which data traffic is sent. The options are: • 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**. Note that multiple VPNs can be selected within a Source Zone.

Step 6 Click **Additional Settings** to configure additional settings for a security policy. Refer to the steps used in the procedure, Configure NGFW Additional Settings. Click **Save**.

Step 7 Click on the ellipsis (...) at the top left corner of the existing sub-policy to **Edit**, **Delete**, or **Copy** it.

Step 8 To add a 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.

Field	Description
Match	Choose the desired match conditions from the **Add Conditions** drop-down list. The options are: • Source • Geo Location • IPv4 Prefix • Port • Destination • FQDN • Geo Location • IPv4 Prefix • Port • Protocol • Applications When ISE is enabled, then SGT option is available in the **Source** and **Destination**. Identity User or User group is only supported for **Source**.
Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action.

Step 9 To modify an existing rule, click the pencil icon to **Edit**, **Disable**, **Delete**, **Clone rule**, **Add rule on top**, or **Add rule below**.

Associate a Policy Group to Catalyst SD-WAN NGFW Policy

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 Navigate to the policy you want to associate with a policy group. Click the ellipsis (…) under the **Action** column and click **Associate Policy Group**.

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

Deploy Policy Group from Catalyst SD-WAN Manager

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

NGFW policy modifications, including security objects and profiles, from Security Cloud Control Firewall Management, must be deployed to Secure Router devices using the Catalyst SD-WAN Manager.

You can access the workflow by choosing **Workflows** > **Deploy Policy Group** menu in Catalyst SD-WAN Manager. The **Deploy Policy Group** 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.

CHAPTER 7

Monitor and Report Change Logs, Workflows, and Jobs

Security Cloud Control effectively monitors configuration change logs, bulk device operations, and the process that runs when communicating with devices. This helps you understand how your network's existing policies influence its security posture.

Manage Change Logs in Security Cloud Control

A Change Log captures the configuration changes made in Security Cloud Control, providing a single view that includes changes in all the supported devices and services. These are some of the features of the change log:

- Provides a side-by-side comparison of changes made to device configuration.
- Provides labels for all change log entries.
- Records onboarding and removal of devices.
- Detects policy change conflicts occurring outside Security Cloud Control.
- Provides answers about who, what, and when during an incident investigation or troubleshooting.
- Enables downloading of the complete change log, or only a portion of it, as a CSV file.

Note Changes made in Cloud-Delivered Firewall Management Center are not reflected in the change log.

Manage Change Log Capacity

Security Cloud Control retains the change log information for one year and deletes data older than a year.

There is a difference between the change log information stored in Security Cloud Control's database and what you see in an exported change log. See Export the Change Log, on page 43 for more information.

Change Log Entries

A change log entry reflects the changes to a single device configuration, an action performed on a device, or the change made to a device outside Security Cloud Control:

- For change log entries that contain configuration changes, you can view details about the change by clicking anywhere in the corresponding row.
- For out-of-band changes made outside Security Cloud Control and are detected as conflicts, the **System User** is reported as the **Last User**.
- Security Cloud Control closes a change log entry after a device's configuration on Security Cloud Control is synced with the configuration on the device, or when a device is removed from Security Cloud Control. Configurations are considered to be in sync after they read the configuration from the device to Security Cloud Control or after deploying the configuration from Security Cloud Control to the device.
- Security Cloud Control creates a new change log entry immediately after completing an existing entry, irrespective of whether the change was a success or failure. Additional configuration changes are added to the new change log entry that opens.
- Events are displayed for read, deploy, and delete actions for a device. These actions close a device's change log.
- A change log is closed after Security Cloud Control is in sync with the configuration on the device (either by reading or deploying), or when Security Cloud Control no longer manages the device.
- If a change is made to the device outside of Security Cloud Control, a *Conflict detected* entry is included in the change log.

Pending and Completed Change Log Entries

Change logs have a status of either Pending or Completed. As you make changes to a device's configuration using Security Cloud Control, these changes are recorded in a Pending change log entry. The following activities complete a Pending change log, and after this a new change log is created for recording future changes.

- Reading a configuration from a device to Security Cloud Control
- Deploying changes from Security Cloud Control to a device
- Deleting a device from Security Cloud Control
- Running a CLI command that updates the running configuration file

Search and Filter Change Log Entries

You can search and filter change log entries. Use the search field to find events. Use the filter (▼) to find the entries that meet the criteria you specify. You can also combine the two tasks by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

Change Request Management

Change Request Management enables the linking of a **Change Request** and its business justification to a **Change Log** event. The **Change Request** is opened in a third-party ticketing system.

Use **Change Request Management** to create a **Change Request** in Security Cloud Control and associate it with change log events. You can search for this change request by **Name** within the change log.

Note In Security Cloud Control, **Change Request Tracking** and **Change Request Management** refer to the same functionality.

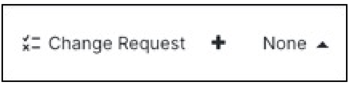
Enable Change Request Management

Enabling change request tracking affects all users of your organization.

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Enable the **Change Request Tracking** toggle button.



When enabled, the **Change Request** menu appears at the bottom-left corner and the **Change Request** drop-down list is available in the **Change Log** page.

Create a Change Request

Procedure

Step 1 In Security Cloud Control, click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Enter a **Name** and **Description**.

Ensure that the **Name** corresponds to a **Change Request** name that your organization intends to use, and that the **Description** describes the purpose of the change.

Note
You cannot modify the name of a **Change Request** after you create it.

Step 3 Click **Save**.

Note

When a **Change Request** is saved, Security Cloud Control associates all the new changes with the corresponding **Change Request** name. This association continues until you either disable change requests or clear the change request details from the menu.

Associate a Change Request with a Change Log Event

Procedure

Step 1 In the left pane, click **Monitor** > **Events & Logs** > **Logs** > **Change Log**.

Step 2 Expand the change log to view the events you want to associate with a **Change Request**.

Step 3 Click the drop-down list adjacent to the corresponding change log entry.

Note
The latest change requests are displayed at the top of the change request list.

Step 4 Select a change request and click **Select**.

Search for Change Log Events with Change Requests

Procedure

Step 1 In the left pane, click **Monitor** > **Events & Logs** > **Logs** > **Change Log**.

Step 2 In the change log search field, enter the name of a change request to find the associated change log events.

Security Cloud Control highlights the change log events that are exact matches.

Search for a Change Request

Procedure

Step 1 In Security Cloud Control, click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Enter the name of the **Change Request** or a relevant keyword in the search field. As you enter a value, the results that partially match your input, appear in both the **Name** and **Description** fields.

Filter Change Requests

Procedure

Step 1 In the left pane, click **Monitor** > **Events & Logs** > **Logs** > **Change Log**.

Step 2 Click the filter icon to view all the options.

Step 3 In the search field, enter the name of a **Change Request**.

As you enter a value, the results that partially match your entry appear.

Step 4 Select a change request by checking the corresponding check box.

The matches appear in the **Change Log** table. Security Cloud Control highlights the change log events that are exact matches.

Clear the Change Request Toolbar

To avoid automatic association of change log events with an existing change request, clear the information in the change request toolbar.

Procedure

Step 1 Click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Click **Clear**.

The **Change Request** menu now displays **None**.

Clear a Change Request Associated with a Change Log Event

Procedure

Step 1 In the left pane, click **Monitor** > **Events & Logs** > **Logs** > **Change Log**.

Step 2 Expand the **Change Log** to view the events that you want to disassociate from **Change Requests**.

Step 3 Click the drop-down list adjacent to the corresponding change log entry.

Step 4 Click **Clear**.

Delete a Change Request

Deleting a **Change Request** removes it from the change request list, but not from the **Change Log**.

Procedure

Step 1 Click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Select the change request and click the bin icon to delete it.

Step 3 Click the check mark to confirm.

Disable Change Request Management

Disabling **Change Request Management** or **Change Request Tracking** affects all users of your account.

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Disable the **Change Request Tracking** toggle button.

Change Request Management Use Cases

These use cases assume that you have enabled Change Request Management.

Track Changes Made to the Firewall Device to Resolve a Ticket Maintained in an External System

This use case describes a scenario where you want to make changes to a firewall device to resolve a ticket maintained in an external system and want to associate the change log events resulting from these firewall changes to a change request. Follow this procedure to create a change request and associate change log events to it:

1. Create a Change Request, on page 39.
2. Use the ticket name or number from the external system as the name of the change request and add the justification for the change and other relevant information in the **Description** field.
3. Ensure that the new change request is visible in the change request toolbar.
4. Make the changes to the firewall device.
5. In the navigation pane, click **Change Log** and find the change log events that are associated with your new change request.
6. Clear the Change Request Toolbar, on page 41 to avoid automatic association of change log events with an existing change request.

Manually Update Individual Change Log Events After Changes are Made to the Firewall Device

This use case describes a scenario where you have made changes to a firewall device to resolve a ticket that is maintained in an external system, but forgot to use the Change Request Management feature to associate change requests with the change log events. You want to update the change log events with the ticket number. Follow this procedure to associate change requests with change log events:

1. Create a Change Request, on page 39. Use the ticket name or number from the external system as the name of the change request. Use the **Description** field to add the justification for the change and other relevant information.

2. In the navigation pane, click **Change Log** and search for the change log events that are associated with the changes.

3. Associate a Change Request with a Change Log Event, on page 40.

4. Clear the Change Request Toolbar, on page 41 to avoid automatic association of change log events with an existing change request.

Search for Change Log Events Associated with a Change Request

This use case describes a scenario where, you want to find out what change log events were recorded in the change log because of the work done to resolve a ticket maintained in an external system. Follow this procedure to search for change log events that are associated with a change request:

1. In the navigation pane, click **Change Log.**

2. Search for change log events that are associated with change requests using one of the following methods below:

    - In the **Change Log** search field, enter the exact name of the change request to find change log events associated with that change request. Security Cloud Control highlights change log events that are exact matches.

    - Filter Change Requests, on page 41 to find the change log events.

3. View each change log to find the highlighted change log events showing the associated change request.

Export the Change Log

You can export all or a subset of the Security Cloud Control change log to a comma-separated value (.csv) file so that you can filter and sort the information, as required.

To export the change log to a .csv file, follow this procedure:

Procedure

Step 1 In the left pane, click **Monitor** > **Events & Logs** > **Logs** > **Change Log**.

Step 2 Find the changes you want to export by doing one of the following tasks:

- Use the filter ( ) and the search field to find what you want to export. For example, filter by device to see only the changes for your selected device or devices.
- Clear all the filters and search criteria in the change log. This allows you to export the entire change log.

Note
Security Cloud Control retains 1 year of change log data. It is recommended to filter the change log contents and download the results to a .csv file rather than downloading the entire change log history for a year.

Step 3 Click the export icon at the top right corner of the page.

Step 4 Save the .csv file to your local file system, with a descriptive name.

Differences Between Change Log Capacity in Security Cloud Control and Size of an Exported Change Log

The information that you export from Security Cloud Control's Change Log page is different from the change log information that Security Cloud Control stores in its database.

For every change log, Security Cloud Control stores two copies of the device's configuration–the *starting* configuration and either the *ending* configuration in the case of a closed change log or the *current* configuration in the case of an open change log. This allows Security Cloud Control to display configuration differences side by side. In addition, Security Cloud Control tracks and stores every step (*change event*) with the username that made the change, the time the change was made, and other details.

However, when you export the change log, the export does not include the two complete copies of the configuration. It only includes the *change events*, which makes the export file much smaller than the change log that Security Cloud Control stores.

Security Cloud Control stores change log information for a year. This includes two copies of the configuration.

CHAPTER 8

Cisco Security Analytics and Logging

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

Terminology Note: In this documentation, when Cisco Security Analytics and Logging is used with the Secure Cloud Analytics portal (a software as a service product) 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 connection events from all of your Catalyst SD-WAN devices and view them in one place in Security Cloud Control. The events are stored in the Cisco cloud and viewable from the **Event Logging** page in Security Cloud Control, where you can filter and review them to gain a clear understanding of what security rules are triggering in your network.

With additional licensing, after you capture these events, you can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you. Secure Cloud Analytics is a software as a service (SaaS) solution that tracks the state of your network by performing a behavioral analysis on events and network flow data. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Event Types in Security Cloud Control

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.

Note that the Catalyst SD-WAN device currently logs only connection events under SD-WAN event types. SD-WAN Catalyst device do not support sending syslog events to Security Cloud Control. To learn more about syslog ID 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, but in general 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 discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on.
- Metadata about why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on.

Security Analytics and Logging license and Data Storage Plans

To obtain Security Analytics and Logging entitlement, you can purchase one of the following licenses:

- **Security Cloud Control Device License Subscription with Unlimited Logging**: This license combines Cisco Defense Orchestrator management license for managing Cisco firewalls device with unlimited volume of event logging. By default, 90 days of storage retention is available with this license. You have the option to extend log retention period to 1, 2, or 3 years by purchasing additional data retention extension licenses.
- **Cisco Logging and Troubleshooting License Subscription**: This license supports logging 1 GB volume per day with 90 days of storage retention. You can extend log retention to 1, 2, or 3 years by purchasing additional data retention extension licenses.

For more information, see About Security Cloud Control Licenses.

You need to purchase a data storage plan that corresponds to the volume of events the Cisco cloud receives from your onboarded security devices on a daily basis. This volume is referred to as your daily ingest rate. Data plans are available in whole number amounts of GB/day and in 1-, 3-, or 5-year terms. The most effective method to determine your ingest rate is to participate in a free trial of Secure Logging Analytics (SaaS) before making a purchase. This trial will provide an accurate estimate of your event volume.

With Security Cloud Control device license subscription, you receive 90 days of rolling data storage. This policy ensures that the most recent 90 days of events are stored in the Cisco cloud, and data older than 90 days is deleted.

You have the option to upgrade to additional event retention beyond the default 90 days or to increase daily volume (GB/day) through a change order to an existing subscription. Billing for these upgrades will be prorated for the remainder of the subscription term.

See the Subscriptions section of *Guidelines for Quoting Secruity Cloud Control Products* for more information about the storage and subscription plans.

Note If you have a Security Analytics and Logging license and data plan, then obtain a different Security Analytics and Logging license, you are not required change your data plan. Similarly, if your network traffic throughput changes and you obtain a different data plan, this change alone does not require you to obtain a different Security Analytics and Logging license.

What data gets counted against my allotment?

All events sent to the Secure Event Connector accumulate in the Secure Logging Analytics (SaaS) cloud and count against your data allotment.

Filtering what you see in the events viewer does not decrease the number of events stored in the Secure Logging Analytics (SaaS) cloud, it reduces the number of events you can see in the events viewer.

We're using up our storage allotment quickly, what can we 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 what you are currently logging to determine if it is necessary to log events from as many rules and policies.

View Security Analytics and Logging License Information

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, the 90-day rolling data storage details appear in the licensing information.

Procedure

Step 1 From the left navigation bar, click **Administration** > **Logging Settings**.

Step 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 the **Storage Utilization** button to view the Security Analytics and Logging license information.

Extend Event Storage Duration and Increase Event Storage Capacity

To extend your rolling event storage or increase the amount of event cloud storage, do the following steps:

Procedure

Step 1 Log in to your account on Cisco Commerce.

Step 2 Select your Security Cloud Control PID.

Step 3 Follow the prompts to upgrade the length or capacity of your storage capacity.

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

View Security Analytics and Logging Alerts

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

Procedure

Step 1 From the left navigation bar, click **Administration** > **Logging Settings**.

Step 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 the **Storage Utilization** button to view the Security Analytics and Logging license information.

The **Alerts and Notifications** section displays alerts about the settings that impact event logging, enabling 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.

View Security Analytics and Logging Storage Usage and Event Ingest Rate

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, enabling you to 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

Step 1 From the left navigation bar, click **Administration** > **Logging Settings**.

Step 2 Click **View Logging Storage Usage**.

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

Step 3 Use the following dashboards to customize and analyze the storage utilization and gain more insights into the 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 for a specific device to get more granular data. You can filter the data for the last 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.

Deprovisioning Cisco Security Analytics and Logging (SaaS)

If you allow your Cisco Security Analytics and Logging (SaaS) paid license to lapse, you have a grace period of 90 days. If you renew your paid license during this grace period, there is no interruption in your service.

Otherwise, if you allow the 90-day grace period to elapse, the system purges all of your customer data. You can no longer view Catalyst SD-WAN events from the **Event Logging** page, nor have dynamic entity modeling behavioral analytics applied to your Catalyst SD-WAN events and network flow data.

About Security Analytics and Logging for Catalyst SD-WAN

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

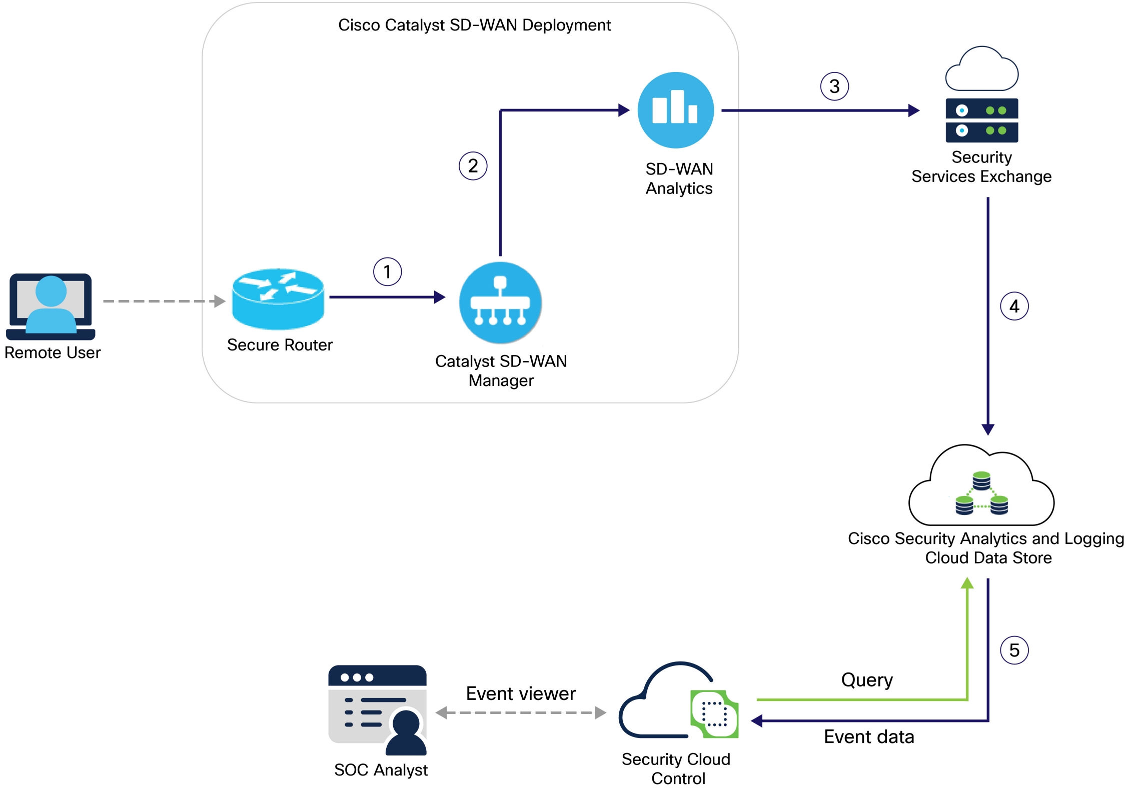
- Catalyst SD-WAN integrates security features directly into the SD-WAN fabric, enabling secure Direct Internet Access (DIA) and Direct Cloud Access (DCA).
- It includes next-generation firewall, integrated intrusion prevention capabilities, and URL filtering.
- The Catalyst SD-WAN platform enables you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

Onboard the Catalyst SD-WAN Manager to Security Cloud Control Firewall Management for managing the security capabilities of the managed devices. You can view the security events from Catalyst SD-WAN with Security Analytics and Logging for monitoring and threat detection. The events get stored in the Security Analytics and Logging cloud data store, and you can view them in the **Event Logging** page in Security Cloud Control, where you can filter and analyze them to identify security rules getting triggered in your network.

How Catalyst SD-WAN Router Share Events with Security Cloud Control Firewall Management

The following diagram describes how Catalyst SD-WAN shares security events with Security Cloud Control Firewall Management.

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



Step	Description
1	A remote user accesses the network and the Catalyst SD-WAN device generates event log for the corresponding traffic. The device then exports the event data to a PSV file and sends it to the 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) process the event data using various services to classify and enrich it for use by the Security Cloud Control. It stores the event data in the cloud data store, which is queried by the event viewer to provide SOC analysts with the relevant event data.

Prerequisites

- A Security Cloud Control Firewall Management organization with a valid Security Analytics and Logging subscription plan. For more information about the subscription plans, see Security Analytics and Logging license and Data Storage Plans, on page 46.
- Onboard the Catalyst SD-WAN Manager to the Security Cloud Control organization where you want to view the security events. For more information, see Onboard a Catalyst SD-WAN Manager to Security Cloud Control Firewall Management, on page 12.
- Onboard the SD-WAN Analytics services to your Catalyst SD-WAN Manager and enable data collection. For more information, see Onboard Cisco SD-WAN Analytics.

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

Before you begin

Ensure that you have met all the requirements described in Prerequisites, on page 52.

Procedure

Step 1 In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.

Step 2 Click the filter (▼) icon.

Step 3 Scroll to the **Catalyst SD-WAN Events** section and check the **Connection** check box.