



Integrate Catalyst SD-WAN Manager with Security Cloud Control

- [Overview of Catalyst SD-WAN integration with Security Cloud Control, on page 1](#)
- [System Topology Diagram , on page 2](#)
- [End-to-End Workflow to Manage Catalyst SD-WAN Manager using Security Cloud Control, on page 3](#)
- [Minimum Software Requirements, on page 4](#)
- [Onboard a Catalyst SD-WAN Manager to Security Cloud Control Firewall Management, on page 4](#)
- [Remove Catalyst SD-WAN Manager from Security Cloud Control Firewall Management, on page 6](#)
- [Alignment of RBAC Models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager, on page 7](#)
- [How Security Cloud Control Firewall Management Manages Catalyst SD-WAN NGFW Capabilities, on page 8](#)
- [View Intrusion Events, on page 9](#)
- [View Malware Events, on page 10](#)
- [Additional Resources, on page 10](#)

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.

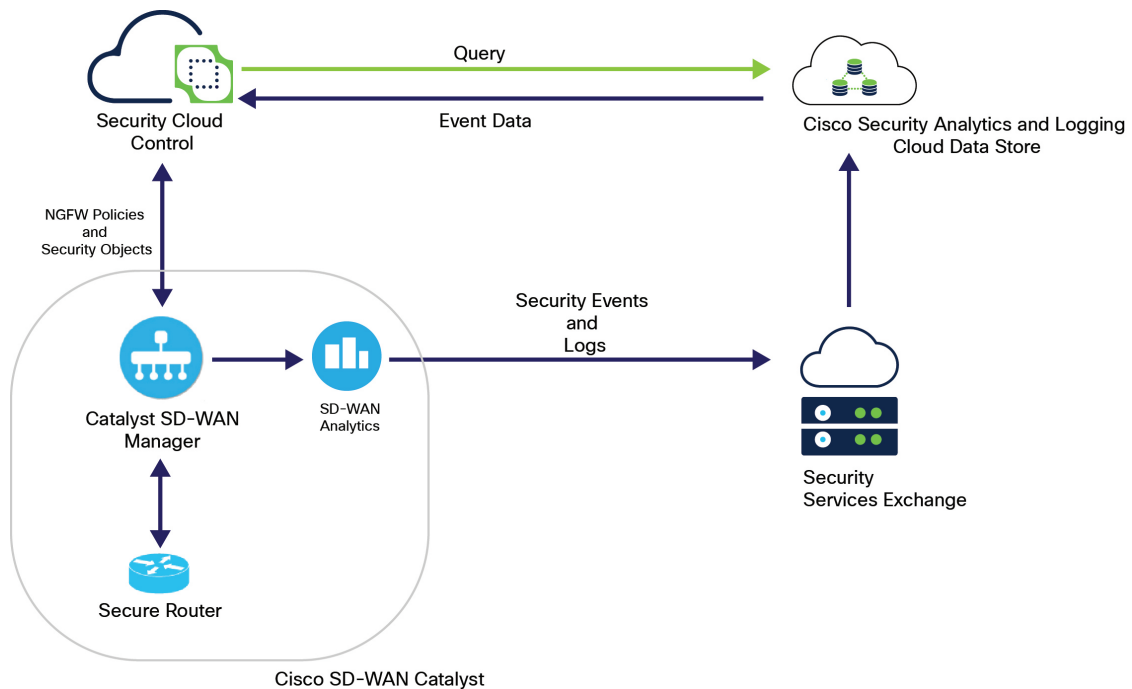
System Topology Diagram

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.

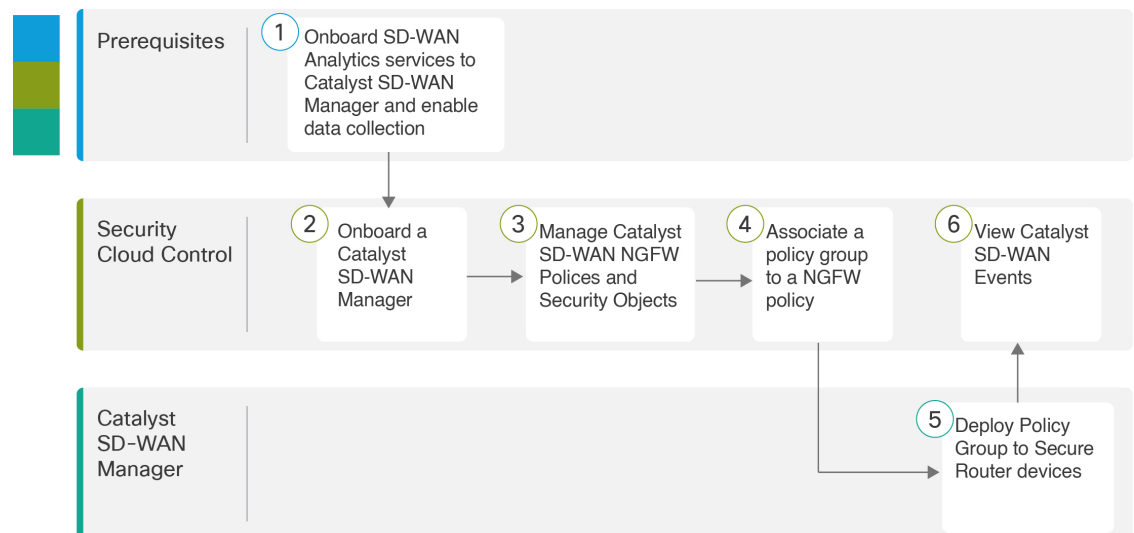


- **Security Cloud Control:** A central point for security policy enforcement and event correlation. It reads NGFW policies and security objects from the onboarded Catalyst SD-WAN Manager and allows customers to modify these NGFW configurations. It also sends queries to Cisco Security Analytics and Logging 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.



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 1 .
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	<ul style="list-style-type: none"> - Allowed read-only access in Security Cloud Control - Allowed read-only access in Catalyst SD-WAN Manager
VPN Sessions Manager	Operator	<ul style="list-style-type: none"> - Allowed read-only access in Catalyst SD-WAN Manager
Administrator	security_operations	<ul style="list-style-type: none"> - Allowed to create/edit security policies in Security Cloud Control - Allocated SecOps user role in Catalyst SD-WAN Manager
Super Administrator	security_operations	<ul style="list-style-type: none"> - Unrestricted access to all functions in Security Cloud Control - Allocated SecOps user role in Catalyst SD-WAN Manager
Deploy Only	Operator	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 NGFW 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](#)