Security Cloud Control Integration

Table 1: Feature History

Feature	Release Information	Description
Security Cloud Control Integration with Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Security Cloud Control 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's integration with Cisco SD-WAN Manager provides centralized management for Cisco Catalyst SD-WAN Branch WAN environments. The integration allows you to do the following: • Efficiently manage security policies and objects, configure and edit them, and push changes using the Security Cloud Control dashboard. • Effective monitoring and detection of security threats. from a centralized Security Cloud Control dashboard. • Analyze security threats from logs and events in Security Cloud Control dashboard using data sent from Security Analytics and Logging.

Security Cloud Control Integration

A Security Cloud Control is a unified security management platform that

- integrates with Cisco SD-WAN Manager to enable centralized security policy management and configuration,
- allows configuration of objects and policies in the Cisco SD-WAN Manager from SCC's Micro frontend (MFE) user interface,
- provides a unified interface for configuration and monitoring of security policy,
- configures, monitors, and troubleshoots security policies for the Secure Router or Catalyst Next-Generation Firewall (NGFW), and
- provides centralized orchestration, security discovery, policy creation, log and analytics viewing, and security policy implementation across multiple Cisco solutions.

Integration of Security Cloud Control with Cisco SD-WAN Manager helps Network Operations (NetOps) and Security Operations (SecOps) team optimize their day-to-day operations. NetOps teams can use Cisco SD-WAN Manager to handle networking events, configurations, and workflows, while Security Cloud Control serves as a dedicated tool for configuring and managing security functions.

For more information about Security Cloud Control, see Overview of Security Cloud Control

Key aspects of Security Cloud Control integration

Security Cloud Control integration includes:

- Configuring security objects and policies from Security Cloud Control and pushing them to Secure Router devices through Cisco SD-WAN Manager,
- Automatically synchronizing Next-Generation Firewall (NGFW) policies with Security Cloud Control to Cisco SD-WAN Manager,

Note The security policies in NGFW are managed by the Cisco SD-WAN Manager, providing advanced security features like intrusion prevention, malware protection, and URL filtering. You can create the following objects and policies in Security Cloud Control after a successful integration.

- Objects: Application List, Data Prefix, FQDN, Geolocation, Identity, Port, Protocol, Security Group Tag, Signature, URL Allow, URL Block, and Zone.
- Policies: Advanced Inspection Profile, Advanced Malware Protection, Intrusion Prevention, TLS/SSL Decryption, TLS/SSL Profile, and URL Filtering.

- Synchronizing existing Cisco Catalyst objects and profiles in Cisco SD-WAN Manager with Security Cloud Control,
- Synchronizing device inventory in Cisco SD-WAN Manager with the SCC Tenant periodically,
- Creating and editing new Next-generation firewall (NGFW) policies within Security Cloud Control, and
- Visualizing logs and events through Security Cloud Control. It requires the following:
  - Security Analytics and Logging license.
  - Analytics is enabled under cloud services admin settings.

  Cisco SD-WAN Analytics provides analytics data to Security Services Exchange (SSX). SSX normalizes logs and events after receiving them from Cisco SD-WAN Manager and stores it in Cisco Security Analytics and Logging for visualization through Security Cloud Control.
- Automatic role assignment for Security Cloud Control users in Cisco SD-WAN Manager. For more information, see User roles in Security Cloud Control and Cisco Catalyst SD-WAN Manager, on page 8

Integration Scenarios

The integration of Cisco SD-WAN Manager with Security Cloud Control enables seamless policy management for both new and existing SecOps users. This integration supports two types of deployment scenarios:

- New Users: Cisco SD-WAN Manager has no pre-existing policy objects, policies, or security configurations.
- Existing Users: Cisco SD-WAN Manager has pre-existing policy objects, policies, and security configurations.

The integration process involves syncing and reconciling policies between Cisco SD-WAN Manager and Security Cloud Control that may already be deployed in the devices.

Prerequisites for Security Cloud Control Integration

For seamless integration of Cisco SD-WAN Manager with Security Cloud Control, you must ensure the following:

with

- Cisco SD-WAN Manager version is 20.18 or later.
- Cloud services is enabled in Cisco SD-WAN Manager.
- The organization to be onboarded in Security Cloud Control is accessible through the Smart Account and Virtual Account.

  For more information about Smart Account and Virtual Account, see Access the Cisco Catalyst SD-WAN Portal
- Use Configuration group for policy configuration.
- Register Security Cloud Control to Cisco SD-WAN Manager in offline mode. Cisco Catalyst SD-WAN Self-Service Portal (SSP) assigns a (client ID, and client secret) for Security Cloud Control. The portal URL is https://ssp.sdwan.cisco.com/The client ID and client secret is delivered by SSP to Security Cloud Control.
- The tenant ID and tenant name must be generated. Your SSP account must have the same Security Cloud Control tenant and Cisco Catalyst SD-WAN tenant.

Note The tenant name is not the organization name. You may need to provide the tenant name and organization name when you contact Cisco Technical Assistance Center (TAC).

- The Security Cloud Control tenant must have 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. For more information, see Security Analytics and Logging license and Data Storage Plans.
- Onboard the Cisco SD-WAN Analytics services to the Cisco SD-WAN Manager and enable data collection. For more information, see Cisco Security Analytics and Logging.
- For viewing logs and events in Security Cloud Control, you must ensure the following:
  - A valid Security Analytics and Logging license.
  - Enable Security Unified Logging
- For Cisco SD-WAN Manager with on-premises deployment, ensure that inbound access on port 443 is allowed to your on-premises overlay network.

Restrictions for Security Cloud Control Integration

Cloud connectivity is essential

Cisco SD-WAN Manager can be deployed either on-premises or hosted in the Cisco cloud. To function properly, it must have cloud connectivity. If Cisco 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 Cisco SD-WAN Manager to edit NGFW policies, objects, and profiles

To make changes in the NGFW policies, objects, and profiles from the Cisco 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 (SAL). You can only view historical events.

Modify user role privileges for SCC Users with caution

Exercise caution when changing user role privileges on Cisco 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 SD-WAN Manager not supported

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

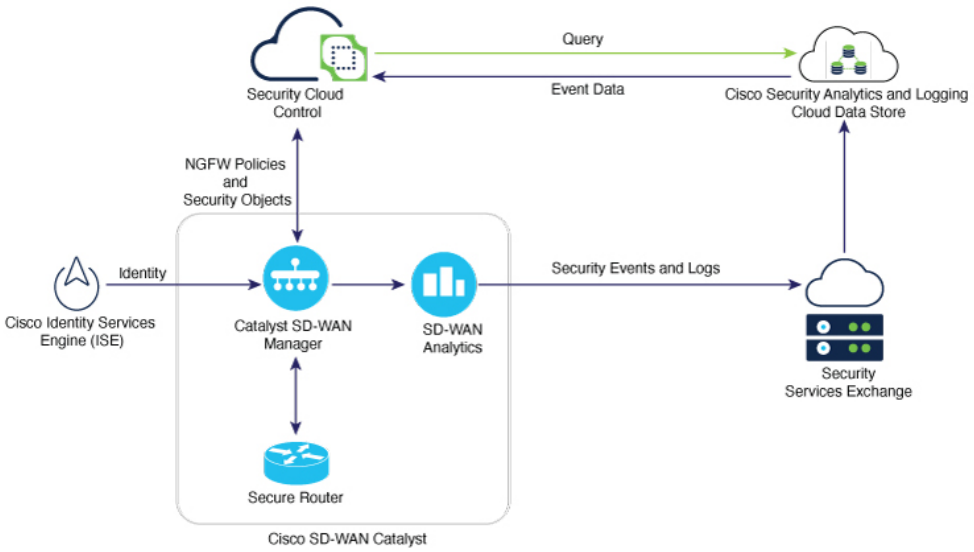
Dark mode not supported

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

Integrating Security Cloud Control with Cisco Catalyst SD-WAN Manager and other components

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

Figure 1: Topology Diagram



The integration of Security Cloud Control with Cisco Catalyst SD-WAN involves onboarding, managing, and deploying security policies to secure router devices. The key components involved in the process are:

- Security Cloud Control: A central point for security policy enforcement and event correlation. It receives identity information from ISE, reads NGFW policies and security objects from the onboarded Cisco SD-WAN Manager and empowers 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 that comprises of :
  - Catalyst SD-WAN Manager: Onboards and manages Catalyst SD-WAN devices. It also manages the NGFW policies and security objects that are onboarded to Security Cloud Control. Cisco SD-WAN Manager sends the event data received from the Secure Router to Cisco SD-WAN Analytics.
  - Cisco SD-WAN Analytics: Onboards analytics services to Cisco SD-WAN Manager and enables data collection. It provides the analytics data to SSX.
  - Secure Router: These are Cisco IOS XE Catalyst SD-WAN devices, which are also called edge devices.
- Cisco Identity Services Engine (ISE): Provides identity information to the Security Cloud Control.
- 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 SSX, which obtains the analytics data from the Cisco SD-WAN Analytics engine.
- Security Services Exchange (SSX): A component of Cisco Security Analytics and Logging that normalizes events and logs received from Cisco SD-WAN Manager. It converts event data from PSV to JSON format, and sends it to Cisco Security Analytics and Logging for storage and visualization by Secure Cloud Control. It is a component of SAL that is specifically involved in Cisco Security Analytics and Logging-based logging.

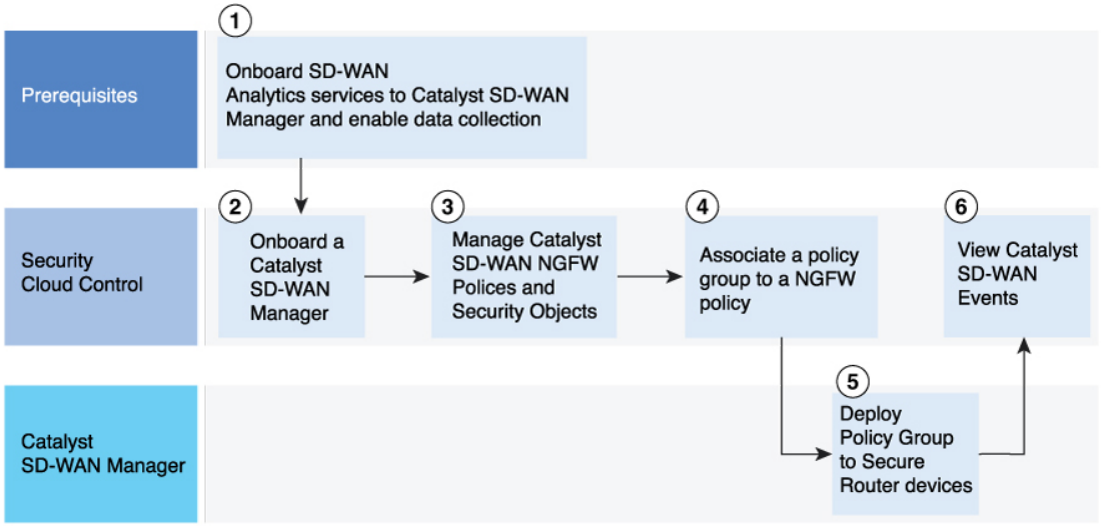
Summary

The following section describes the stages of Security Cloud Control integration with Cisco SD-WAN Manager and other components.

Workflow

Figure 2: Integration Process

These are the stages of Security Cloud Control integration:



1. To begin with, onboard the SD-WAN Analytics services to the Cisco SD-WAN Manager and enable data collection. For more information, see Onboard Cisco SD-WAN Analytics.
2. In Security Cloud Control, onboard Cisco SD-WAN Manager that also imports associated Secure Router devices.

Note Before onboarding Cisco SD-WAN Manager, add tags to devices. You can use the tags for grouping, describing, finding, or managing devices. You can also add devices to configuration groups based on tagging.

For more information, see Device Tagging.

3. In Security Cloud Control, create, modify, or delete Catalyst SD-WAN NGFW policies, security objects, and security profiles
4. In Security Cloud Control, associate a group policy to a Catalyst SD-WAN NGFW policy.

   (Optional) In Security Cloud Control, Security Cloud Control, delete Branch WAN edge devices.
5. In Cisco SD-WAN Manager, deploy Policy Group to Secure Routers or Cisco IOS XE Catalyst SD-WAN devices. For more information, see Policy Group.
6. In Security Cloud Control, view the security events received from Cisco Catalyst SD-WAN with Security Analytics and Logging for monitoring and threat detection.

Note Extending log retention is based on your existing Security Cloud Control device license subscription.

Result

After Cisco SD-WAN Manager is onboarded to Security Cloud Control, the management of policies, objects, and profile can no longer be performed through the Cisco SD-WAN Manager. Instead, these management tasks must be carried out exclusively from Security Cloud Control. For more information on creating objects and policies in Security Cloud Control, see Manage Catalyst SD-WAN Security Objects and Security Profiles.

Note Policies are created using Security Cloud Control but stored only in Cisco SD-WAN Manager.

User roles in Security Cloud Control and Cisco Catalyst SD-WAN Manager

An alignment of user roles between SD-WAN Manager and Security Cloud Control is a role-based access control (RBAC) practice that:

- coordinates user permissions across both platforms,
- maintains independent role definitions for each system, and
- ensures user actions are consistent and limited by the lowest assigned permission.

Alignment of user roles in Security Cloud Control and Cisco SD-WAN Manager

User roles in Cisco Security Cloud Control and Catalyst SD-WAN Manager operate independently but are aligned to ensure seamless and consistent user actions. If you have elevated permissions in Security Cloud Control but lower permissions in SD-WAN Manager, your effective access is limited to the lower of the two roles. For example, being a Super Admin in Security Cloud Control but only an Operator in Catalyst SD-WAN Manager restricts your ability to save certain configuration changes.

If a user exists in Security Cloud Control but not in SD-WAN Manager, SCC sends the user's role to the API Gateway. The API Gateway maps the Security Cloud Control role to a SD-WAN Manager role. The API Gateway then asks SD-WAN Manager to create the user and assign a user group based on the Security Cloud Control role. If no user group is specified, the default group assigned is BASIC.

When onboarding, if a user already exists in Cisco SD-WAN Manager, their role remains unchanged, regardless of their role in Security Cloud Control. If a user is new, their SD-WAN Manager role is assigned based on their role in Security Cloud Control. This alignment enables strong security by ensuring users cannot bypass restrictions through role discrepancies between the two systems.

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

Table 2: Access permissions for user roles

Allowed Action	Security Cloud Control Role	Catalyst SD-WAN Manager Role
Read-only access in Security Cloud Control Read-only access in Catalyst SD-WAN Manager	Read Only	Operator
Read-only access in Catalyst SD-WAN Manager	VPN Sessions Manager	Operator
Create or edit security policies in Security Cloud Control SecOps user role in Catalyst SD-WAN Manager	Administrator	security_operations (global resource group)
Unrestricted access to all functions in Security Cloud Control SecOps user role in Catalyst SD-WAN Manager	Super Administrator	security_operations (global resource group)
Not allowed to create or edit security policies in Security Cloud Control Read-only access in Catalyst SD-WAN Manager	Deploy Only	Operator
Unrestricted access to all functions in Security Cloud Control Allocated SecOps user role in	Edit Only	security_operations (global resource group)

Onboard a Cisco Catalyst SD-WAN Manager on Security Cloud Control

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

Before you begin

- Minimum requirements:
  - Supported Cisco IOS XE version: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a.
  - Secure Router: version 20.12 or later
- You must know the registered organization name associated with your Cisco SD-WAN Manager.
- Log in to Cisco SD-WAN Manager. Choose **Administration** > **Settings** > **Organization Name**.

The **Organization Name** field is a unique identifier used to establish Secure Control Connections within the Cisco Catalyst SD-WAN environment.

- Ensure easy onboarding is successful with service access authorization enabled.

Note Cisco SD-WAN Manager manages all Secure Router devices, regardless of their **Device Status**.

Procedure

Step 1 Log in to the Security Cloud Control tenant with your SSP account credentials.

Step 2 In the left pane of Security Cloud Control, choose **Administration** > **Integrations**.

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

Step 4 Click the plus icon on top right corner.

Step 5 In the **Select an integration** page, choose **Catalyst SD-WAN Manager**.

Step 6 From the **Select Organization** dropdown, choose an organization.

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

Step 7 In the **Create label** field, enter your desired label and click **Connect**.

Note
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 8 Click **Close** after verifying the details of the Cisco SD-WAN Manager you are onboarding.

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

After a successful onboarding, you can see the following in the Security Cloud Control screen:

- All security objects, security profiles, and NGFW policies. These imported policies are available in **Manage** > **Policies** > **Catalyst SD-WAN**.
- Secure Router devices and their running configuration.
- A "Managed by Security Cloud Control (SCC)" banner on the Cisco SD-WAN Manager that is onboarded to Security Cloud Control.

What to do next

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

You can create new Catalyst SD-WAN security objects and security profiles from Security Cloud Control. For more information, see Manage Catalyst SD-WAN Security Objects and Security Profiles.

Remove a Cisco Catalyst SD-WAN Manager from Security Cloud Control

Use this procedure to deboard the Cisco SD-WAN Manager to the Security Cloud Control platform.

Procedure

Step 1 In the left pane of Security Cloud Control, choose **Administration** > **Integrations**.

Step 2 Choose the Cisco SD-WAN Manager instance you want to delete, and then click **Remove SD-WAN Devices**.

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

Removing the Cisco SD-WAN Manager automatically removes the associated devices from the Security Cloud Control.

Verifying Security Cloud Control Integration

A "Managed by Security Cloud Control (SCC)" banner displays on the Cisco SD-WAN Manager that is onboarded to Security Cloud Control, indicating a successful integration. This message can be viewed in the Cisco SD-WAN Manager by navigating to the relevant sections:

- For **Security Objects and Profiles** page, navigate to **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.
- For NGFW policies, navigate to **Configuration** > **Policy Groups** > **NGFW** > **NGFW Policy**.

After onboarding a Cisco SD-WAN Manager to Security Cloud Control, you can only view the NGFW policies in that Cisco SD-WAN Manager.

Monitor Event Logs with Cisco Security Analytics and Logging

A Cisco IOS XE Catalyst SD-WAN device is a Cisco Catalyst SD-WAN fabric features:

- advanced firewall capabilities in its architecture, ensuring robust security across distributed networks.
- is secured with next-generation firewall (NGFW), integrated with intrusion prevention capabilities, and URL filtering,
- enables secure Direct Internet Access (DIA) and Direct Cloud Access (DCA) through embedded security features, and
- enforces centralized policies to extend enterprise VPN architectures into private cloud environments.

Note Security Unified Logging must be enabled to view logs from Cisco SD-WAN Manager in Security Cloud Control for the data sent from Cisco Security Analytics and Logging.

After onboarding the Cisco SD-WAN Manager to Security Cloud Control, it manages the security features of the Cisco IOS XE Catalyst SD-WAN devices. This integration allows you to monitor security events from Catalyst SD-WAN using Cisco Security Analytics and Logging.

Security Analytics and Logging allows you to capture connection, intrusion, file, malware, security intelligence, syslog, and Netflow Secure Event Logging (NSEL) events from all of your ASA and Secure Firewall Threat Defense devices and view them in one place in Security Cloud Control. The security events are stored in the Security Analytics and Logging Cloud Data Store and viewable from the **Event Logging** page in Security Cloud Control. Use the filtering and analysis tools on this page to identify which security rules are triggered in your network.

For more information about the process on how Cisco IOS XE Catalyst SD-WAN devices shares events with Security Analytics and Logging and Security Cloud Control, see the following:

- Cisco Security Analytics and Logging
- How Catalyst SD-WAN Router Share Events with Security Cloud Control Firewall Management

View the Cisco Catalyst SD-WAN Manager Events in Security Cloud Control

Cisco SD-WAN Manager shares data about security events and logs with SSX which then shares the data with SAL. Security Cloud Control sends queries to Cisco Security Analytics and Logging (SAL) for event data. Data about connection events are stored in SAL. It sends the events data to Security Cloud Control.

Use this procedure to view event logs in the Security Cloud Control platform.

Before you begin

- A Security Cloud Control tenant with a valid Security Analytics and Logging subscription plan.
- Onboard the Catalyst SD-WAN Manager to the Security Cloud Control tenant where you want to view the security events.
- Onboard the Cisco SD-WAN Analytics services to your Cisco SD-WAN Manager and enable data collection. For more information, see Cisco Security Analytics and Loggin.

  For more information about the prerequisites, see How Catalyst SD-WAN Router Share Events with Security Cloud Control..

Procedure

Step 1 In the navigation pane of Security Cloud Control, 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** checkbox.

What to do next

You can review and analyze connection events and take appropriate actions, such as for events with inspect action.

View Audit Logs in Cisco Catalyst SD-WAN Manager

Security Cloud Control records user-related and system-level actions related to objects and policies in **Audit Logs**. The same changes are captured in the **Audit Logs** of Cisco SD-WAN Manager.

Using audit logs, you can monitor unauthorized activities such as multiple failed login attempts and excessive logins. You can also configure notifications for unauthorized activity.

In Security Cloud Control, you can monitor change logs, workflows, and jobs. For more information, see Monitor and Report Change Logs, Workflows, and Jobs.

Use this procedure to view audit logs in Cisco SD-WAN Manager.

Procedure

Step 1 To view the logs in Cisco SD-WAN Manager, navigate to **Monitor** > **Logs** > **Audit logs**.

Step 2 Review the following columns:

- **Action**
- **Details**
- **Date/Time**
- **User**

.