Configure Cloud-Delivered Firewall Management Center-Managed Secure Firewall Threat Defense

This chapter provides information on how to manage the Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense onboarded to Security Cloud Control.

Introduction to Cloud-Delivered Firewall Management Center

The Cloud-Delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices and is delivered via Security Cloud Control. The Cloud-Delivered Firewall Management Center offers many of the same functions as an On-Premises Firewall Management Center.

The Cloud-Delivered Firewall Management Center has the same appearance and behavior as an On-Premises Firewall Management Center and uses the same FMC API.

As a SaaS product, the Security Cloud Control operations team is responsible for deploying and maintaining Cloud-Delivered Firewall Management Center software. As new features are introduced, the Security Cloud Control operations team updates your Security Cloud Control tenant's Cloud-Delivered Firewall Management Center for you.

A migration wizard is available to help you migrate your Secure Firewall Threat Defense devices from your On-Premises Firewall Management Center to the Cloud-Delivered Firewall Management Center. The devices must have Threat Defense software Version 7.0.3 or a later 7.0.x release, or Version 7.2 or later installed to be migrated. Threat Defense 7.1 releases are not supported.

Onboarding Secure Firewall Threat Defense devices is carried out in Security Cloud Control using familiar processes such as onboarding a device with its serial number or using a CLI command that includes a registration key. Once the device is onboarded, it is visible both in Security Cloud Control and in the Cloud-Delivered Firewall Management Center, however, you configure the device in the Cloud-Delivered Firewall Management Center. In Security Cloud Control, you can view device-specific information such as version, configuration status, connectivity, health status, and node status. When you click on the health status from Security Cloud Control, you are taken to the respective device's health monitoring page in the Cloud-Delivered Firewall Management Center user interface.

Security Cloud Control provides high availability support for the threat defense devices that it manages through the data interface. This feature is supported for devices running software version 7.2 or later.

You can analyze security events generated by your onboarded threat defense devices using Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises). The SaaS version stores events in the cloud and you view the events in Security Cloud Control. The on-premises version stores events in an on-premises Secure Network Analytics appliance and analysis is done in the On-Premises Firewall Management Center. In both cases, just as with an On-Premises Firewall Management Center today, you can still send logs to a log collector of your choice directly from the sensors.

Licenses

The license for Cloud-Delivered Firewall Management Center is a per-device-managed license and there is no license required for the Cloud-Delivered Firewall Management Center itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the Secure Firewall Threat Defense For more information, see Cloud-Delivered Firewall Management Center license.

The **Unified Events** feature in Cloud-Delivered Firewall Management Center uses Cisco Security Analytics and Logging (SaaS) as its event data source. You must have a valid Cisco Security Analytics and Logging (SaaS) subscription plan to view firewall events on the **Unified Events** page. When you enable Cloud-Delivered Firewall Management Center, a 90-day trial subscription for Security Analytics and Logging (SaaS) is automatically issued.

Existing customers can continue to use Security Cloud Control for managing other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use Security Cloud Control to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with Security Cloud Control as well.

To learn how to have a Cloud-Delivered Firewall Management Center provisioned on your tenant, see Enable Cloud-delivered Firewall Management Center on Your Security Cloud Control Tenant.

Navigate to the Cloud-Delivered Firewall Management Center in your Security Cloud Control Tenant

Procedure

Step 1 In the left pane, click **Administration** > **Integrations** > **Firewall Management Center** to view the **Services** page.

The **Services** page displays the information about the Cloud-Delivered Firewall Management Center provisioned for the Security Cloud Control tenant.

Step 2 Choose **Cloud-Delivered FMC** and click the links in the **Actions**, **Management**, or **Settings** pane to navigate to Cloud-Delivered Firewall Management Center to perform various actions. See Security Cloud Control Integrations Page, on page 9.

Once in the Cloud-Delivered Firewall Management Center, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and further action you can take.

Determine Cloud-Delivered Firewall Management Center Version in Security Cloud Control

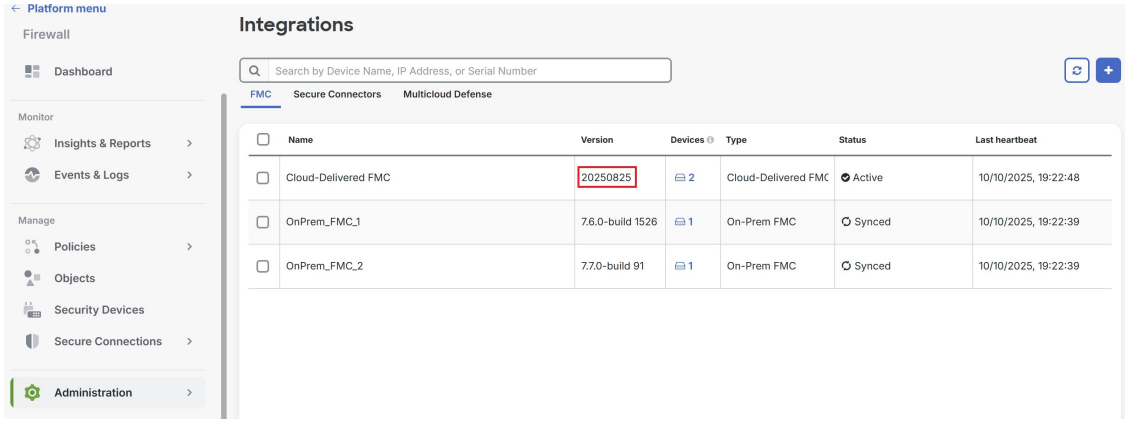
Information about the Cloud-Delivered Firewall Management Center version is required primarily for migration planning, feature support verification, troubleshooting, licensing, and operational management.

Use this procedure to determine the current version of your Cloud-Delivered Firewall Management Center in Security Cloud Control.

Procedure

Step 1 In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**.

Step 2 Under the **FMC** tab, the version is displayed under the **Version** column.



For more information about Cloud-Delivered Firewall Management Center versions, see Release Notes for Cloud-Delivered Firewall Management Center.

Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant

If you want to manage your Secure Firewall Threat Defense devices, you can enable the Cloud-Delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

Step 1 From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

Step 2 Security Cloud Control starts provisioning a Cloud-Delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-Delivered Firewall Management Center is Ready** notification on the Security Cloud Control notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

Note
After you receive the **Cloud-Delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

You can then onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

Hardware and Software Support

Cloud-Delivered Firewall Management Center supports these Secure Firewall Threat Defense software versions when they are installed on any supported hardware or virtual device:

- Verion 7.0.3 or later 7.0.x versions.
- Version 7.2 and later versions.

Note Software Version 7.1 is _not_ supported.

See Firepower Threat Defense Support Specifics for more information.

Security Cloud Control Firewall Management Platform Maintenance Schedule

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

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

During 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 Firewall Management continue to enforce their security policies.

Note

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

Licensing

The **Unified Events** page uses the Cisco Security Analytics and Logging data store as its event data source. You must have a valid Cisco Security Analytics and Logging subscription plan to view firewall events on the **Unified Events** page.

Integrate On-Premises Firewall Management Center With Cisco Security Cloud

This procedure describes how to integrate the On-Premises Firewall Management Center with Cisco Security Cloud. By enabling Cisco Security Cloud integration, your management center gets registered to the Cisco cloud tenancy.

Before you begin

When onboarding an on-premises Firewall Management Center:

- If you already have a Security Cloud Control tenant, you will be prompted to confirm whether you want to attach the on-premises Firewall Management Center to that existing tenant.

- If you do not have a tenant or account, the on-premises Firewall Management Center integration wizard will automatically create a new tenant for you during the registration task the onboarding process. This tenant is a free tier provided exclusively for on-premises Firewall Management Center AI Assist enablement. Allow the wizard to manage tenant creation so that you do not receive a trial tenant that would later require conversion. The wizard manages this process to provide a seamless experience.
- If you intend to use the Cloud-Delivered Firewall Management Center or manage firewalls using the Security Cloud Control, you must purchase a base license and device entitlements. For detailed licensing information and product options, refer to the Security Cloud Control Licensing Overview.

Procedure

Step 1 In your on-premises Firewall Management Center, do the following:

- For on-premises Firewall Management Center version between 7.2 and 7.4.x, go to **Integration** > **SecureX**.
- For on-premises Firewall Management Center version 7.6 or later, go to **Integration** > **Cisco Security Cloud**.

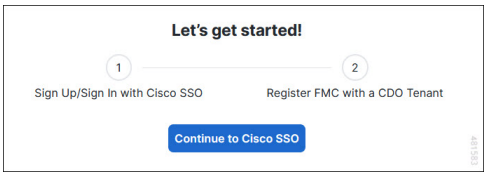
Step 2 Based on your on-premises Firewall Management Center version, do the following:

- For on-premises Firewall Management Center version between 7.2 and 7.4.x, click **Enable Secure X**.
- For on-premises Firewall Management Center version 7.6 or later, click **Cisco Security Cloud**.

A separate browser tab opens to log you in to your Security Cloud Control account. Make sure this page is not blocked by a pop-up blocker.

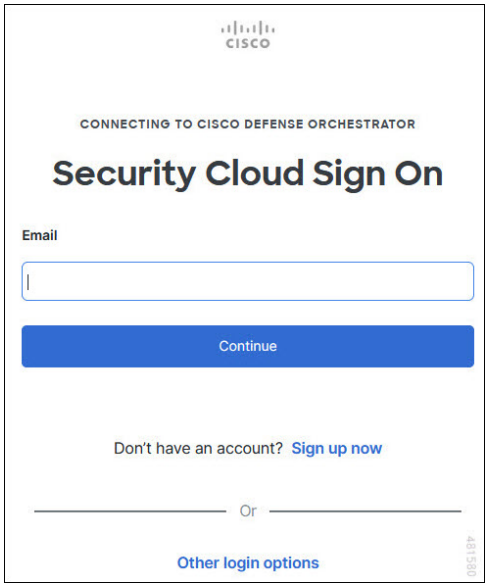
Step 3 Click **Continue to Cisco SSO**.

Figure 1: Cisco Security Cloud Welcome Page



Step 4 Log in to your Security Cloud Control account.

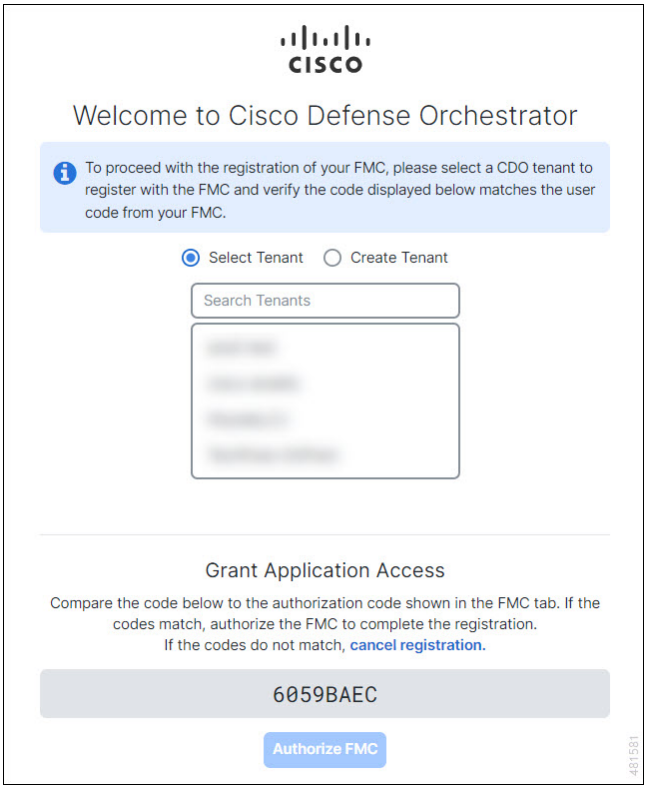
Figure 2: Cisco Security Cloud Sign On



If you do not have a security cloud sign on account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. See Create a New Cisco Security Cloud Sign On Account.

Step 5 Choose a Security Cloud Control tenant that you want to use for this integration. The on-premises Firewall Management Center and the managed devices get onboarded to the Security Cloud Control tenant that you choose here.

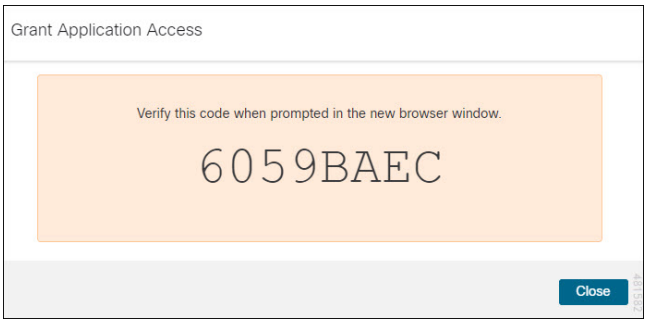
Figure 3: Choose the Security Cloud Control Tenant



If you do not already have a Security Cloud Control tenant or if you want to use a new tenant for this integration, create a new tenant.

Step 6 Verify that the code displayed in the Security Cloud Control login page matches the code provided by the on-premises Firewall Management Center.

Figure 4: Verification Code in the on-premises Firewall Management Center



Step 7 Click **Authorize FMC**.

Step 8 In the on-premises Firewall Management Center UI, click **Save** to save the configuration.

You can view the task progress under **Notifications** > **Tasks**.

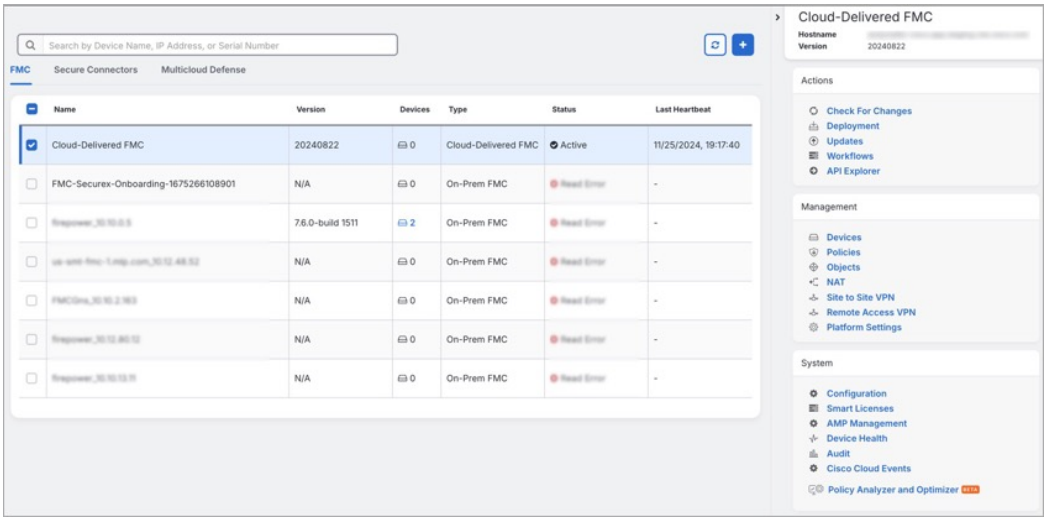
The registration task can take up to 90 seconds to complete. If you must use on-premises Firewall Management Center while the registration task is in progress, open the on-premises Firewall Management Center in a new window.

Security Cloud Control Integrations Page

The **Integrations** page displays a list of Firewall Management Centers that Security Cloud Control manages. Selecting the **FMC** tab lists the Cloud-Delivered Firewall Management Center that is linked to the Security Cloud Control account and all the on-premises Firewall Management Centers onboarded to Security Cloud Control. The devices that are managed by these on-prem management centers are listed in the **Security Devices** page. The **Integrations** page also lists the secure connectors under the **Secure Connectors** tab.

You can click the **FMC** tab and onboard an on-premises Firewall Management Center by clicking the blue plus icon (+), and perform device actions using the options in the right pane. You can also see device information such as version, number of devices being managed by the management center, device type, and the synchronization status of the device. Clicking on the managed devices icon takes you to the **Security Devices** page, where devices managed by the selected on-premises Firewall Management Center are filtered automatically and displayed. The **Integrations** page also allows you to select more than one on-premises Firewall Management Center at a time for you to perform actions on a group of management centers all at once. You cannot select any on-premises Firewall Management Center while the Cloud-Delivered Firewall Management Center is selected. To add a new secure connector or perform actions on existing secure connectors, choose the **Secure Connectors** tab and click +.

In the left pane, click **Administration** > **Firewall Management Center**.



For your Cloud-Delivered Firewall Management Center, the Integrations page displays the following information:

- If you do not have a Cloud-Delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. See Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant for more information.

- The number of Secure Firewall Threat Defense devices deployed on the Cloud-Delivered Firewall Management Center.
- Status of the connection between Security Cloud Control and the Cloud-Delivered Firewall Management Center page.
- The last heartbeat of the Cloud-Delivered Firewall Management Center. This represents the last time the status of the Cloud-Delivered Firewall Management Center itself and the number of devices that it manages were synchronized with the table on this page.
- The hostname of the selected Cloud-Delivered Firewall Management Center.

Choose **Cloud-Delivered FMC** and using the links in the **Actions**, **Management**, or **Settings** pane, you open the Cloud-Delivered Firewall Management Center user interface to perform the configuration tasks that are associated with the link you clicked.

Actions:

- **Check For Changes**: The Device Count and Status information in the table will be updated with the information available the last time this page and the Cloud-Delivered Firewall Management Center were synchronized. Synchronization happens every 10 minutes.
- **Deployment**: Takes you to the device configuration deployment page on Cloud-Delivered Firewall Management Center. See Deploy Configuration Changes.
- **Workflows**: Takes you to the **Workflows** page to monitor every process that Security Cloud Control runs when communicating with devices. See Workflows page.
- **API Explorer**: Takes you to the page that lists the Cloud-Delivered Firewall Management Center REST APIs. See Secure Firewall Management Center REST API Guide.
- **Unified Events**: Takes you to the **Unified Events** page on the Cloud-delivered Firewall Management Center portal, which provides a single-screen view of various firewall events, including connection, intrusion, file, malware, and security-related connection events. For more information, see Unified Events.

Note The Unified Events feature requires activation. If you have not yet activated this feature, contact your Cisco sales representative to enable it.

Management:

- **Devices**: Takes you to the Firewall Threat Defense device listing page on the Cloud-Delivered Firewall Management Center portal. See Configure Devices.
- **Policies**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to edit system-provided access control policies and create custom access control policies. See Manage Access Control Policies.
- **Objects**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to manage reusable objects. See Object Management.
- **NAT**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to configure Network Address Translation policies on the Firewall Threat Defense devices. See Manage NAT policies.

- **Site to Site VPN**: Takes you to the site-to-site VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure site-to-site VPN policy between two sites. See Site-to-Site VPNs.
- **Remote Access VPN**: Takes you to the remote access VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure a remote access VPN configuration. See Remote Access VPN.
- **Platform Settings**: Takes you to the platform settings page on the Cloud-Delivered Firewall Management Center portal to configure a range of unrelated features whose values you might want to share among several devices. See Platform Settings.

System:

- **Configuration**: Takes you to the system configuration settings page on the Cloud-Delivered Firewall Management Center portal to configure system configuration settings. See System Configuration.
- **Smart Licenses**: Takes you to the smart licenses page on the Cloud-Delivered Firewall Management Center portal to assign licenses to devices. See Assign Licenses to Devices.
- **AMP Management**: Takes you to the AMP management page on the Cloud-Delivered Firewall Management Center portal that provides intelligence that the system uses to detect and block malware on your network. See Cloud Connections for Malware Protection.
- **Device Health**: Takes you to the health monitoring page on the Cloud-Delivered Firewall Management Center portal that tracks various health indicators to ensure that the hardware and software in the system are working correctly. See About Health Monitoring.
- **Audit**: Takes you to the audit log page on the Cloud-Delivered Firewall Management Center portal to show the generated audit record for each user interaction with the web interface.
- **Cisco Cloud Events**: Takes you to the configure Cisco Cloud events page on the Security Cloud Control portal to configure Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS). See Send Events to SAL (SaaS).

After opening the Cloud-Delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and what further action you can take.

Support to Open Security Cloud Control and Cloud-Delivered Firewall Management Center Applications in Separate Tabs

As you configure Firewall Threat Defense devices or objects in Cloud-Delivered Firewall Management Center, you can open the appropriate configuration pages in additional browser tabs to work simultaneously in the Security Cloud Control and the Cloud-Delivered Firewall Management Center portals without logging off.

For example, you can create an object on Cloud-Delivered Firewall Management Center and simultaneously monitor event logs on Security Cloud Control that are generated from the security policies.

This feature is available for all Security Cloud Control links that navigate to the Cloud-Delivered Firewall Management Center portal. To open the Cloud-Delivered Firewall Management Center portal in a new tab:

On the Security Cloud Control portal, press and hold the Ctrl (Windows) or Command (Mac) button, then click the corresponding link.

Note A single click opens the Cloud-Delivered Firewall Management Center page in the same tab.

Here are some examples of opening the Cloud-Delivered Firewall Management Center portal page in a new tab:

- Choose **Administration** > **Firewall Management Center** and select **Cloud-Delivered FMC**. In the right pane, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the page that you want to access.
- Choose **Objects** > **Other FTD Objects**.
- Click the search icon in the top-right corner of the Security Cloud Control page and enter the search strings in the search field that appears.

  From the search result, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the arrow icon.
- Choose **Dashboard** > **Quick Actions**. Press and hold the Ctrl (Windows) or Command (Mac) button, and then click **Manage FTD Policies** or **Manage FTD Objects**.

Note When you switch to a new Security Cloud Control tenant, the corresponding Cloud-Delivered Firewall Management Center portal already opened in a new tab logs out.

Related Topics

- Managing On-Prem Firewall Management Center with Security Cloud Control
- Onboard an On-Prem Firewall Management Center
- Request a cloud-delivered Firewall Management Center for your Security Cloud Control tenant
- Secure Device Connector
- Secure Event Connectors