

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.

- Overview of Cloud-Delivered Firewall Management Center, on page 1
- Navigate to the Cloud-Delivered Firewall Management Center in your Security Cloud Control Tenant, on page 3
- Determine the Cloud-Delivered Firewall Management Center Version in Security Cloud Control Firewall Management, on page 3
- Enable Cloud-Delivered Firewall Management Center , on page 4
- Hardware and Software Support, on page 5
- Security Cloud Control Firewall Management platform maintenance schedule, on page 5
- Licensing, on page 6
- Integrate an On-Premises Firewall Management Center with Cisco Security Cloud, on page 6
- Security Cloud Control Firewall Management Integrations Page , on page 9

Overview of Cloud-Delivered Firewall Management Center

Cloud-Delivered Firewall Management Center is a software-as-a-service product that

- manages Secure Firewall Threat Defense devices through Security Cloud Control Firewall Management
- provides many of the same functions as an On-Premises Firewall Management Center, and
- has the same appearance and behavior as an On-Premises Firewall Management Center and uses the same FMC API.

Migration and onboarding details

A migration wizard is available to help you migrate Threat Defense devices from an On-Premises Firewall Management Center to Cloud-Delivered Firewall Management Center.

Devices must run one of these Threat Defense software releases before you migrate them:

- Minimum On-Premises Firewall Management Center: 7.2
- Minimum Threat Defense: 7.2.x (not supported for Version 7.1)

Threat Defense 7.1 releases are not supported for migration.

You onboard Threat Defense devices in Security Cloud Control Firewall Management by using familiar methods, such as entering the serial number or using a CLI command that includes a registration key.

After onboarding:

- The device appears in both Security Cloud Control Firewall Management and Cloud-Delivered Firewall Management Center.
- You configure the device in Cloud-Delivered Firewall Management Center.
- In Security Cloud Control Firewall Management, you can review device information such as version, configuration status, connectivity, health status, and node status.
- When you click the health status in Security Cloud Control Firewall Management, the platform opens the device health monitoring page in the Cloud-Delivered Firewall Management Center user interface.

Because it is a SaaS product, the Security Cloud Control Firewall Management operations team deploys and maintains the Cloud-Delivered Firewall Management Center software. As new features are introduced, the operations team updates the Cloud-Delivered Firewall Management Center in your Security Cloud Control Firewall Management organization.

Availability and security analytics

Security Cloud Control Firewall Management supports high availability for the Threat Defense devices that it manages through the data interface. This feature is supported for devices that run software version 7.2 or later.

You can analyze security events from onboarded threat defense devices by using either Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises):

- Security Analytics and Logging (SaaS) stores events in the cloud, and you view those events in Security Cloud Control Firewall Management.
- Security Analytics and Logging (On-Premises) stores events on an on-premises Secure Network Analytics appliance, and analysis occurs in the On-Premises Firewall Management Center.

In both cases, you can still send logs directly from firewalls to a log collector of your choice.

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.

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

This task enables you to access the Cloud-Delivered Firewall Management Center from your Security Cloud Control tenant to perform firewall management actions.

The Cloud-Delivered Firewall Management Center is accessible through the Services page in your Security Cloud Control tenant, where you can access management functions, settings, and other actions.

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 Firewall Management 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.

You have successfully navigated to the Cloud-Delivered Firewall Management Center and can now access management functions, settings, and perform firewall management actions.

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

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 Firewall Management.

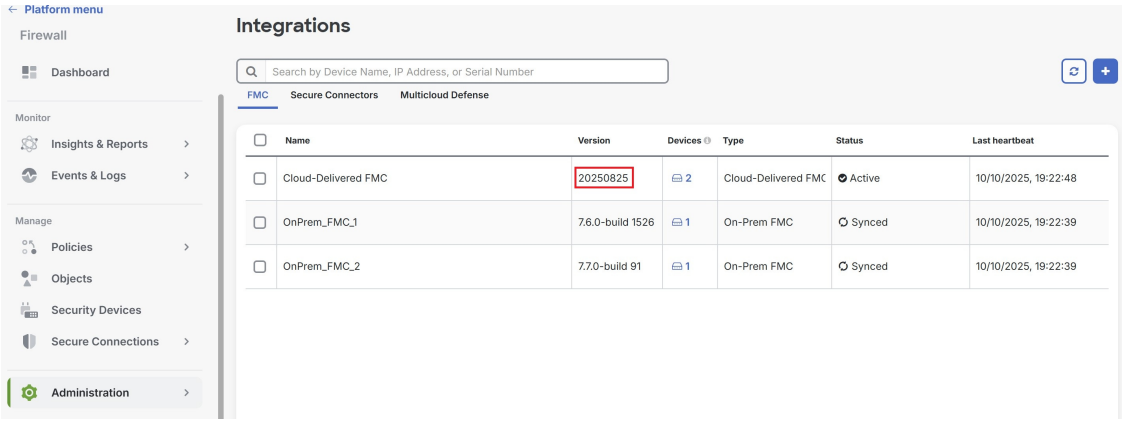
Before you begin

Enable Enable Cloud-Delivered Firewall Management Center in your organzation.

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.

The Cloud-Delivered Firewall Management Center version information is now visible in the Version column under the FMC tab.

Enable Cloud-Delivered Firewall Management Center

Enable Cloud-Delivered Firewall Management Center to manage your Secure Firewall Threat Defense devices through Security Cloud Control.

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

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

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**.

What to do next:

a. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager.

b. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

After the provisioning is complete, the status changes to **Active** and you receive readiness notifications. You can then proceed to register with the Smart Software Manager and onboard your devices.

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



Note

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

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 an On-Premises Firewall Management Center with Cisco Security Cloud

This integration enables your management center to be registered to the Cisco cloud tenancy and provides centralized management capabilities for your firewall devices.

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

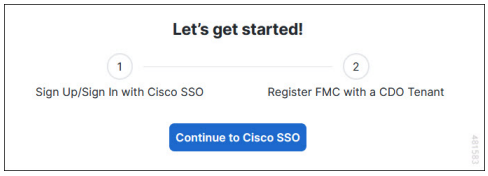
Step 1 Based on your On-Premises Firewall Management Center version, do:

- 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**.
- For On-Premises Firewall Management Center version 10.0 or later, click **Security Cloud Control**.

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.

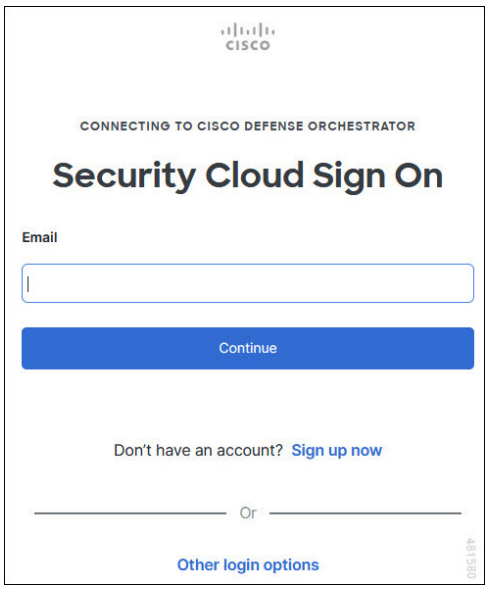
Step 2 Click **Continue to Cisco SSO**.

Figure 1: Cisco security cloud welcome page



Step 3 Log in to your Security Cloud Control account.

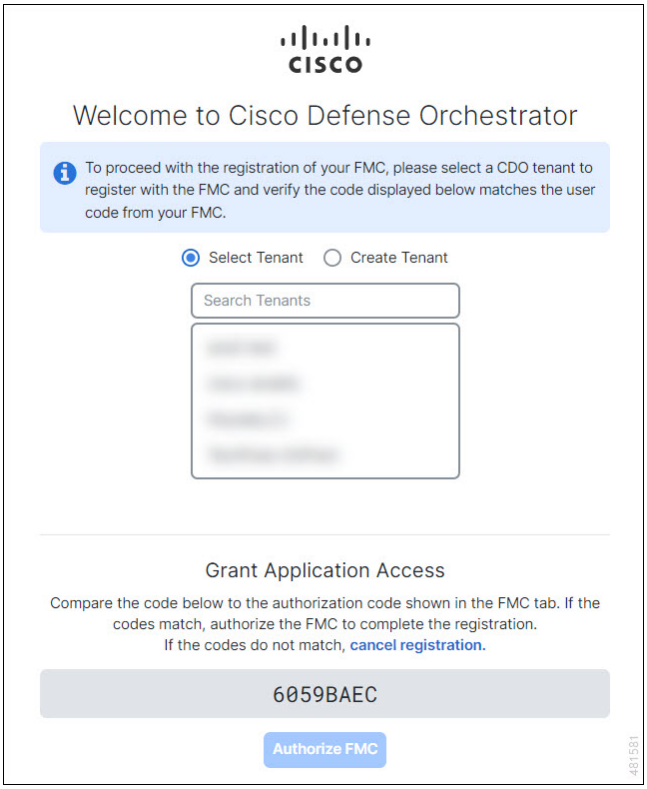
Figure 2: Cisco security cloud sign on



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.

Step 4 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.

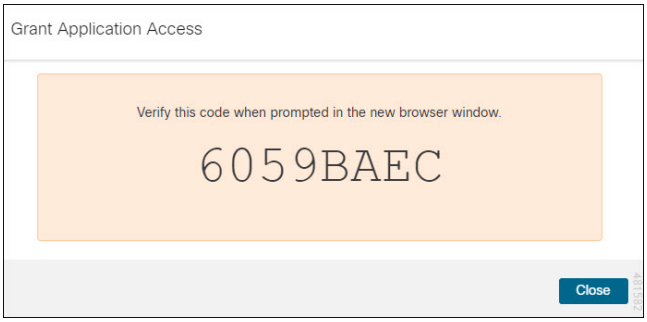
Figure 3: Choose the Security Cloud Control Tenant



If you do not 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 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 6 Click **Authorize FMC**.

Step 7 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.

The On-Premises Firewall Management Center is now integrated with Cisco Security Cloud and registered to your selected tenant for centralized management capabilities.

Security Cloud Control Firewall Management Integrations Page

The **Integrations** page provides a comprehensive view of your managed infrastructure within Security Cloud Control Firewall Management:

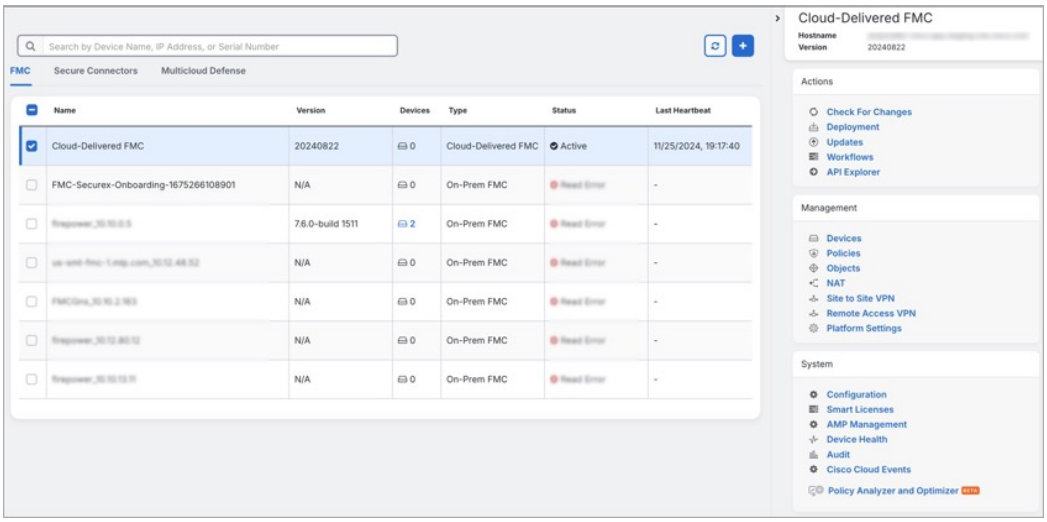
- **FMC** tab:
  - View the Cloud-Delivered Firewall Management Center that is linked to the Security Cloud Control Firewall Management account. Refer to Request a Cloud-delivered Firewall Management Center for your Security Cloud Control tenant .
  - View which On-Premises Firewall Management Centers are onboarded to Security Cloud Control Firewall Management. Devices managed by these On-Premises Firewall Management Centers appear in **Security Devices**. Refer to Managing On-Prem Firewall Management Center with Security Cloud Control.
  - Lists the **Secure Device Connector** and **Secure Event Connector** available under the **Secure Connectors**. Refer to Secure Device Connector and Secure Event Connectors.

Security Cloud Control. page. The **Integrations** page also lists tab.

Click the **FMC** tab, then click **Onboard FMC** ( ) icon to onboard an On-Premises Firewall Management Center. In the right pane, perform device actions as needed. Refer to Onboard an On-Prem Firewall Management Center.

View device information, including version, device count, device type, and synchronization status. Click the managed devices icon to go to the **Security Devices** page. Devices managed by the selected On-Premises Firewall Management Center are filtered and displayed. On the **Integrations** page, select multiple On-Premises Firewall Management Center to perform actions on several management centers at once. Deselect the Cloud-Delivered Firewall Management Center before selecting other On-Premises Firewall Management Center. 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 this information:

- If you do not have a Cloud-Delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. Refer to 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 time shows when the Cloud-Delivered Firewall Management Center's status and device count last 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 is 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. Refer to Deploy Configuration Changes.
- **Workflows**: Takes you to the **Workflows** page to monitor every process that Security Cloud Control runs when communicating with devices. Refer to Workflows page.
- **API Explorer**: Takes you to the page that lists the Cloud-Delivered Firewall Management Center REST APIs. Refer to 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, refer to 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. Refer to 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. Refer to Manage Access Control Policies.
- **Objects**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to manage reusable objects. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to System Configuration .
- **Smart Licenses**: Takes you to the smart licenses page on the Cloud-Delivered Firewall Management Center portal to assign licenses to devices. Refer to Assign Licenses to Devices.
- **AMP Management**: Takes you to the AMP management page on the Cloud-Delivered Firewall Management Center portal that supplies data the system uses to detect and block malware on your network. Refer to Cloud Connections for Malware Protection.
- **Device Health**: Takes you to the health monitoring page on the Cloud-Delivered Firewall Management Center portal, which tracks various health indicators to ensure the hardware and software in the system are working correctly. Refer to 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). Refer to Send Events to SAL (SaaS).

After you open the Cloud-Delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** for more information.

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 on the Security Cloud Control page and enter your search terms in the search field.

  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 If you switch to a new Security Cloud Control tenant, the Cloud-Delivered Firewall Management Center portal open in another tab logs out automatically.