

Welcome to Cisco Security Cloud Control Firewall Management for Government

- Overview of Security Cloud Control Firewall Management, on page 1
- Create a Security Cloud Control Tenant, on page 2
- Security Cloud Control Firewall Management dashboard, on page 4

Overview of Security Cloud Control Firewall Management

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator or CDO) is a cloud-based security policy manager that helps simplify and unify security policies across your Cisco firewalls and other devices such as Cisco IOS and SSH. The firewalls and devices can be managed from **Firewall**, which is listed under **Products** in the Security Cloud Control dashboard.

Security Cloud Control Firewall Management helps you optimize your security policies by identifying inconsistencies within them and by providing with the tools to fix them. It provides you with ways to share objects and policies, as well as create configuration templates, to promote policy consistency across devices.

Because Security Cloud Control Firewall Management coexists with Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by ASDM and reconciles the differences.

You can manage a wide range of devices in one place. Advanced users will also find their traditional CLI interface with some new enhancements to make management even more efficient for them.

Security Cloud Control Firewall Management also provides a guided "Day 0" experience, helping you to quickly onboard Threat Defense devices to your on-premises or Cloud-Delivered Firewall Management Center. It also presents you with other key features that you may benefit from and helps you enable and configure them.

Supported Features for Security Cloud Control Management: Firewall for Government

Cisco Security Cloud Control Management: Firewall for Government provides you with the following security functions:

- Management of Secure Firewall ASA and Secure Firewall Threat Defense devices, supporting both physical and virtual form factors.
- Security Analytics & Logging (SAL) Integration: Integration with the Security Cloud Control dashboard for enhanced event viewing and security analytics.

- Lightweight Security Package (Snort 3) updates for advanced intrusion detection.
- Automatic updates for Vulnerability Database (Vdb) and Geolocation Database (Geo db).

Device onboarding requirements

Before you onboard a device, complete these prerequisites:

- Complete the installation wizard.
- License the device.

After you complete those prerequisites, use the Security Cloud Control Firewall Management onboarding wizard to onboard the device.

Keep these restrictions in mind:

- After you onboard devices to a Security Cloud Control Firewall Management associated with an organization, you cannot migrate those devices to another organization.
- To move devices to a new organization, you must re-onboard them to the new organization.

Cisco Online Privacy Statement

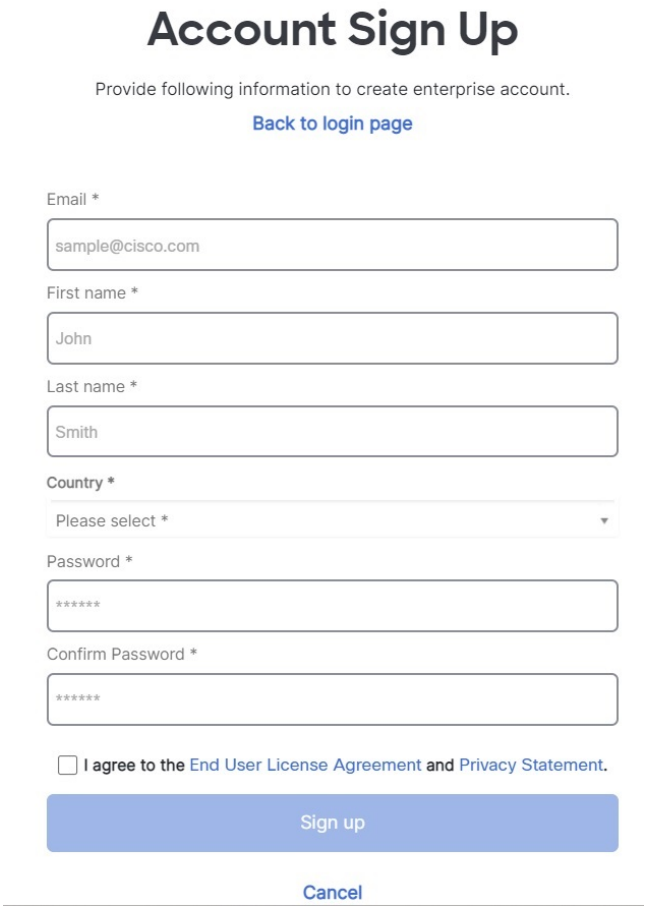
Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the Cisco Online Privacy Statement carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Create a Security Cloud Control Tenant

You can provision a new Security Cloud Control tenant to onboard and manage your devices. If you use an On-Premises Firewall Management Center Version 7.2 and later, and want to integrate it with the Cisco Security Cloud, you can also create a Security Cloud Control tenant as part of the integration workflow.

Procedure

1. Go to https://us.manage.security.cisco.com/provision.
2. Select the region where you want to provision your Security Cloud Control tenant and click **Sign Up**.
3. On the **Security Cloud Sign On** page, provide your credentials.
4. If you do not have a Security Cloud Sign On account and want to create one, click **Sign up now**.
   a. Provide the information to create an account.



Here are some tips:

- **Email**: Enter the email address that you will eventually use to log in to Security Cloud Control.
- **Password**: Enter a strong password.

b. Click **Sign up**. Cisco sends you a verification email to the address you registered with.

c. Open the email and click **Activate account** both on the mail and the **Security Cloud Sign On** page.

d. Configure multifactor authentication using Duo on a device of your choice and click **Log in with Duo** and **Finish**.

Note We recommend installing the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

5. Provide a name for your tenant and click **Create new account**.
6. A new Security Cloud Control tenant is created in the region that you have chosen; you will also receive an email about your Security Cloud Control tenant being created, with the details. If you are associated with multiple Security Cloud Control tenants already, on the **Choose a tenant** page, select the tenant you

just created to log in to it. If you have created a new Security Cloud Control tenant for the first time, you get logged into your tenant directly.

For information about managing a Security Cloud Control tenant and various tenant settings, see Tenant Management.

Upgrade your Security Cloud Control tenant to full version

If you are using a free trial version of Security Cloud Control, you will keep seeing the **You are in a free trial of** Security Cloud Control banner, with the number of days left in the trial period. You can choose to upgrade your Security Cloud Control tenant to the full version anytime during the trial period. Contact your Cisco sales representative or contact Cisco Sales, and they can place an order on your behalf and get you the sales order number.

Once you obtain the sales order number, click **Upgrade to full version** on the banner and enter the order number to begin using the full version of Security Cloud Control.

Request Security Cloud Control trial period extension

If you want to continue using the trial version for 30 days, click **Request for an extension**.

Security Cloud Control Firewall Management dashboard

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

Customize your dashboard

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

1. On the **Home** page, click **Customize**.
2. Select or deselect dashboard widgets and drag and drop them to arrange in your preferred order.

Top Information

This section provides detailed insights into various tenant-level metrics. If enabled, you can view the following widgets:

- **Configuration States**: Indicates the discrepancies between the configurations on your devices and those maintained by Security Cloud Control. This comparison helps identify any inconsistencies or conflicts that may exist.

  For more information, see Device Management.

- **Change Log Management**: Helps you manage the change logs for precise operational control. The widget displays **Completed** and **Pending** change logs.

  For more information, see Change Logs.

- **RA VPN Sessions**: Helps you monitor your Remote Access VPN sessions.

  For more information, see RA VPN Sessions.

- **Overall Inventory**: Helps you monitor the health and status of all devices. The widget displays the total number of devices, categorized into **Issues**, **Pending Actions**, **Other**, **Online** and devices that are nearing or have already reached their last day of hardware support.

  For more information, see All Devices.

- **Site-to-Site VPN**: Helps you manage and assess your site-to-site VPN connections. The widget displays the total number of VPN tunnels and the percentage that are **Active** and **Idle**.

  For more information, see Site-to-site VPN.

- **Accounts and Assets**:

  - Helps you track and manage your multicloud accounts and resources effectively. You can launch the Multicloud Defense Controller from here.
  - Click **+Add Account** to add a new account.

  For more information, see Multicloud Defense Controller.

- **Top Risky Destinations**: Helps you identify and monitor the top risky destinations that are granted access. The widget lists Applications and URL Categories and allows you to filter data for the last 90, 60, or 30 days. You can filter between **Allowed** (default) and **Blocked** traffic.

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

Announcements

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