



## Overview of Security Cloud Control

- [An Introduction to Security Cloud Control](#), on page 1
- [Security Cloud Control Licenses](#), on page 1
- [Security Cloud Control Platform Maintenance Schedule](#), on page 3

## An Introduction to Security Cloud Control

Security Cloud Control (formerly Cisco Defense Orchestrator) 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 helps you optimize your security policies by identifying inconsistencies with them and by giving you tools to fix them. Security Cloud Control gives you ways to share objects and policies, as well as make configuration templates, to promote policy consistency across devices.

Because Security Cloud Control coexists with local device managers such as the Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by Security Cloud Control and by other managers, and then reconcile the differences between managers.

Security Cloud Control has an intuitive user interface that allows you to 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 also provides a guided "Day 0" experience helping you quickly onboard threat defense devices to your on-premises or cloud-delivered Firewall Management Center. It also presents you with other key features you may benefit from and helps you enable and configure them.

### Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively "Cisco") are committed to protecting your privacy and providing you with a positive experience on our websites and while using our products and services ("Solutions"). Please read [Cisco Online Privacy Statement](#) carefully to get a clear understanding of how we collect, use, share, and protect your personal information.

## Security Cloud Control Licenses

Security Cloud Control requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control base subscriptions based on the number

of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription gives you a Security Cloud Control organization, and for every device you choose to manage using Security Cloud Control, you need separate device licenses.

To onboard and manage devices from Security Cloud Control, you need to purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

### Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base** - Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control organization and onboard adequately licensed devices.
- **Device License** - Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control for three years, if you purchase a three-year software subscription to the Cisco Firepower 1010 device.



#### Note

Catalyst SD-WAN doesn't require an additional license. Customers using DNA or WAN Essentials license will be able to integrate with Security Cloud Control.



#### Important

You do not require two separate device licenses to manage a high availability device pair in Security Cloud Control. If you have a high availability pair, purchasing one device license is sufficient, as Security Cloud Control considers the pair of high availability devices as one single device.



#### Note

You can integrate with Security Cloud Control leveraging your existing DNA Essentials/Advantage licensing. This will also extend to WAN Essentials/Advantage, and no other license is required. For logging into Security Analytics and Logging, you should be on the DNA Advantage (or WAN Advantage) license as well as purchase a separate Security Analytics and Logging license



#### Note

You cannot manage Security Cloud Control licensing through the Cisco smart licensing portal.

### Software Subscription Support

The Security Cloud Control base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC), at no extra cost. While the software support is selected by default, you can also leverage the Security Cloud Control solution support based on your requirement.

# Security Cloud Control Platform Maintenance Schedule

Security Cloud Control 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 continue to enforce their security policies.

**Note**

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

