Connect the Appliance to Cisco Defense Orchestrator

This chapter contains the following sections:

Overview of Cisco Defense Orchestrator Integration

The Cisco Defense Orchestrator is a cloud-based platform that helps network operations staff establish and maintain an end-to-end security posture by managing security policies across Cisco security devices. You can connect your appliances with Cisco Defense Orchestrator and analyze security policy configuration of your appliances to identify and resolve policy inconsistencies, model policy changes to validate their impact, and orchestrate policy changes to achieve consistency and maintain clarity in security posture.

How to Configure and Use Features in Cisco Defense Orchestrator Mode

Use of the features included in the Cisco Defense Orchestrator subset is the same as in standard mode, except as noted. See Configuration Changes and Constraints in Cisco Defense Orchestrator Mode, on page 2 for additional information.

This chapter links to locations within this documentation that provide information about some of the major features of the Web Security Appliance that are common to both standard mode and Cisco Defense Orchestrator mode.

This chapter also includes information about configuring Cisco Defense Orchestrator that is not applicable in standard mode.

This document does not include information about Cisco Defense Orchestrator. Cisco Defense Orchestrator documentation is available from https://docs.defenseorchestrator.com.

Deployment in Cisco Defense Orchestrator Mode

Depending on your requirements, you can use one of the following methods to configure your appliance in Cisco Defense Orchestrator mode:

- **Using System Setup Wizard**. Use this option when you have a new appliance. Choose the Cisco Defense Orchestrator mode of operation while running the System Setup Wizard. For instructions, see Configuring Your Appliance in Cisco Defense Orchestrator Mode Using System Setup Wizard, on page 3.
- **Using the Cisco Defense Orchestrator Settings page in the web interface**. Use this option if you have an existing device in the standard mode and have existing policies. You will be able to manage these policies using the Cisco Defense Orchestrator. For instructions, see Configuring Your Standard Mode Appliance in Cisco Defense Orchestrator Mode Using the Web Interface, on page 5.

Configuration Changes and Constraints in Cisco Defense Orchestrator Mode

This section specifies the configuration changes that will occur in your Web Security Appliance after on-boarding it to the Cisco Defense Orchestrator. It also specifies configurable options and constraints.

Note There are no limitations in the web interface other than what is specified below. Authentication is not supported from the Cisco Defense Orchestrator.

Constraints in the Web Security Appliance after on-boarding:

In the appliance, you will not be able to configure the features that are administered through the Cisco Defense Orchestrator. Configurations for these features are migrated to the Cisco Defense Orchestrator when the appliance is on-boarded. All other configuration settings in the appliance are set to default settings.

Barring features administered through the Cisco Defense Orchestrator, all other features will be available in your appliance.

After on-boarding, Access Policies are controlled through Cisco Defense Orchestrator. Exceptions are specified below. You can configure the following Access Policies features only in the Web Security Appliance:

- Access Policies- Policy Definitions
  - Protocols and User Agents
  - Anti-Malware and Reputation
- Custom URL Categories (External Live Feed Category)

You can configure the following features only in the Cisco Defense Orchestrator:

- Custom URL Categories (Local Custom Category)
- URL Filtering, Applications, and Objects (except size and custom MIME type)

- Global and non global access policies
- Access Policies support:
  - Adding multiple access policies is supported.
  - Adding, reordering, deleting access policies is supported.
  - URL filtering (Predefined URL Category Filtering), applications, and objects (object types), with the following limitations:
    - Bandwidth limits for applications and application-types is not supported.
    - For archived objects, inspect is not supported.
    - Advanced membership definitions for access policies and identities are not supported.
    - Range Request Forwarding is not supported.
    - Time and volume quota management is not supported.
    - Safe Search, Referred Exceptions, Site Content Rating are not supported for URLs

If reporting through Cisco Defense Orchestrator is enabled:

- Summarized reports in the Cisco Defense Orchestrator will be available.
- Reporting will also be available in the Web Security Appliance.
- Reporting will not be available in the Security Management Appliance.

Configuring Your Appliance in Cisco Defense Orchestrator Mode Using System Setup Wizard

You can configure your new appliance in Cisco Defense Orchestrator mode while installing it, using the System Setup Wizard.

Before you begin

See Configuration Changes and Constraints in Cisco Defense Orchestrator Mode, on page 2 to know more about the configuration changes that will occur in your Web Security Appliance after on-boarding it to the Cisco Defense Orchestrator.

Step 1 Open a browser and enter the IP address of the Web Security appliance. Use the default IP address when you run the System Setup Wizard for the first time:

`https://192.168.42.42:8443`

-or-

`http://192.168.42.42:8080`

Where `192.168.42.42` is the default IP address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for HTTPS.

Otherwise, if the appliance is currently configured, use the IP address of the M1 port.

Step 2 When the appliance login screen appears, enter the username and passphrase to access the appliance. By default, the appliance ships with the following username and passphrase:

- Username: `admin`
- Passphrase: `ironport`

Step 3 Select **System Administration > System Setup Wizard**.

Step 4 Accept the terms of the license agreement.

Step 5 Click **Begin Setup**.

Step 6 Select **Cisco Defense Orchestrator** for the appliance mode.

Step 7 Configure all settings using the reference tables provided in the following sections as required. See System Setup Wizard Reference Information, page 2-11.

Step 8 Review and install:

a) Review the installation.
b) Click **Previous** to go back and make changes.
c) Click **Install This Configuration** to continue with the information you provided.

Depending on the IP address, hostname, or DNS settings you configured during setup, you may lose connection to the appliance at this stage. If a "page not found" error is displayed in your browser, change the URL to reflect any new address settings and reload the page. Enter your credentials if prompted.

Step 9 Click **Cisco Defense Orchestrator Portal**. The portal opens in a new window or tab, according to your browser settings.

Step 10 On the Cisco Defense Orchestrator portal, perform the following steps:

a) Log in to the Cisco Defense Orchestrator portal.
b) On-board the Web Security Appliance in the portal.
c) Copy the registration token (key).

Step 11 Complete the Cisco Defense Orchestrator registration on your Web Security Appliance. Perform the following steps:

a) Select **Network** > **Cisco Defense Orchestrator**.
b) Enter the registration token (key) and click **Register**.
c) A success message displays after successful registration.

Note After you perform this step, any Content Security Management Appliance used for policy enforcement will be unable to effect policy changes in the Cisco Web Security Appliance.

What to do next

- (Optional) Configure your appliance to send reports to Cisco Defense Orchestrator. See How to Enable Cisco Defense Orchestrator Reporting, on page 7.
- Configure access policies in Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/.

Related Topics

Troubleshooting Cisco Defense Orchestrator Mode Issues, on page 7

Configuring Your Standard Mode Appliance in Cisco Defense Orchestrator Mode Using the Web Interface

Use this procedure if you have existing policies on your appliance and you want to manage these policies using Cisco Defense Orchestrator.

Before you begin

See Configuration Changes and Constraints in Cisco Defense Orchestrator Mode, on page 2 to know more about the configuration changes that will occur in your Web Security Appliance after on-boarding it to the Cisco Defense Orchestrator.

Step 1 Select **Network > Cisco Defense Orchestrator**.

Step 2 Under Cisco Defense Orchestrator Settings, click **Edit Settings**.

Step 3 Select **Enable** and click **Submit**.

Step 4 Commit your changes.

Note After you perform this step, any Content Security Management Appliance used for policy enforcement will be unable to effect policy changes in the Cisco Web Security Appliance.

Step 5 Click **Cisco Defense Orchestrator Portal**. The portal opens in a new window or tab, according to your browser settings.

Step 6 On the Cisco Defense Orchestrator portal, perform the following steps:

a) Log in to the Cisco Defense Orchestrator portal.
b) On-board the Web Security Appliance in the portal.
c) Copy the registration token (key).

Step 7 Complete the Cisco Defense Orchestrator registration on your Web Security Appliance. Perform the following steps:

a) Select **Network** > **Cisco Defense Orchestrator**.
b) Enter the registration token (key) and click **Register**.
c) A success message displays after successful registration.

What to do next

- (Optional) Configure your appliance to send reports to Cisco Defense Orchestrator. See How to Enable Cisco Defense Orchestrator Reporting, on page 7.
- Analyze your appliance's access policies on Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/.

Related Topics

Troubleshooting Cisco Defense Orchestrator Mode Issues, on page 7

Disabling Cisco Defense Orchestrator

Before you begin

After disabling Cisco Defense Orchestrator, if you need to enable it, you will have to regenerate the registration token (key) from the Cisco Defense Orchestrator portal, and on-board the appliance again. See Enabling Cisco Defense Orchestrator, on page 6.

Step 1 Select **Network > Cisco Defense Orchestrator**.

Step 2 Click **Edit Settings**.

Step 3 Uncheck **Enable**.

Step 4 Submit and commit the change.

Enabling Cisco Defense Orchestrator

Before you begin

Ensure you have connectivity to the Cisco Defense Orchestrator portal.

Step 1 Select **Network > Cisco Defense Orchestrator**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable**.

Step 4 Submit and commit the change.

Step 5 Click **Cisco Defense Orchestrator Portal**. The portal opens in a new window or tab, according to your browser settings.

Step 6 On the Cisco Defense Orchestrator portal, perform the following steps:

a) Log in to the Cisco Defense Orchestrator portal.
b) On-board the Web Security Appliance in the portal.
c) Copy the registration token (key).

Step 7 Complete the Cisco Defense Orchestrator registration on your Web Security Appliance. Perform the following steps:

a) Navigate to the **Cisco Defense Orchestrator Registration** section.
b) Enter the registration token (key) and click **Register**.
c) A success message displays after successful registration.

Note After you perform this step, any Content Security Management Appliance used for policy enforcement will be unable to effect policy changes in the Cisco Web Security Appliance.

Cisco Defense Orchestrator Reporting

After deploying your appliance in Cisco Defense Orchestrator mode, you can configure your appliance to send reports to Cisco Defense Orchestrator.

To enable Cisco Defense Orchestrator reporting, see How to Enable Cisco Defense Orchestrator Reporting, on page 7. You will not be able to view and manage your report data on Security Management Appliance also.

How to Enable Cisco Defense Orchestrator Reporting

Before you begin

Deploy your appliance in Cisco Defense Orchestrator mode. For instructions, see Deployment in Cisco Defense Orchestrator Mode, on page 2.

Step 1 Select **Security Services** > **Reporting** and click **Edit Settings**.

Step 2 Select **Local Reporting**.

Step 3 Select **Cisco Defense Orchestrator Reporting**.

Step 4 Submit and commit your changes.

Note Once you enable Cisco Defense Orchestrator reporting, centralized reporting using Security Management appliance will no longer work. However, you can continue to use Advanced Web Security Reporting application for centralized reporting.

What to do next

View your appliance's summary reports on Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/.

Troubleshooting Cisco Defense Orchestrator Mode Issues

Unable to Register Cisco Defense Orchestrator

After enabling Cisco Defense Orchestrator mode on your appliance, if you are unable to register Cisco Defense Orchestrator, do the following:

Step 1 Make sure that the registration key obtained from the Cisco Defense Orchestrator portal is correct.

Step 2 Make sure that the registration key obtained from the Cisco Defense Orchestrator portal is valid.

If the registration key has expired, generate a new registration key on Cisco Defense Orchestrator. For more information, see https://docs.defenseorchestrator.com.