



Stealthwatch Security Analytics Service on Cisco DNA Center User Guide, Release 2.2.1

First Published: 2021-02-08

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Stealthwatch Security Analytics Service on Cisco DNA Center	1
	About Stealthwatch Security Analytics Service on Cisco DNA Center	1
	Stealthwatch Supported Versions	2
	Stealthwatch Security Analytics Supported Devices	2

CHAPTER 2	Set Up Stealthwatch Security Analytics	5
	Install Stealthwatch Security Analytics	5
	Register Stealthwatch	5
	Set Up User Datagram Protocol Director	6
	Enable Stealthwatch Security Analytics	7
	Stealthwatch Security Analytics Prechecks	8
	View Not Ready Devices	9

CHAPTER 3	Manage Stealthwatch Security Analytics	11
	Review Status of Sites and Fabrics	11
	View Scheduled Tasks	11
	Update Stealthwatch Security Analytics	12
	Disable Stealthwatch Security Analytics	13

CHAPTER 4	Troubleshoot Stealthwatch Security Analytics	15
	View Audit Logs	15
	Troubleshoot Using Task Manager	16
	Troubleshoot on Supported Devices	16
	Device Is Not Listed	16



CHAPTER 1

Stealthwatch Security Analytics Service on Cisco DNA Center

- [About Stealthwatch Security Analytics Service on Cisco DNA Center, on page 1](#)
- [Stealthwatch Supported Versions, on page 2](#)
- [Stealthwatch Security Analytics Supported Devices, on page 2](#)

About Stealthwatch Security Analytics Service on Cisco DNA Center

The Stealthwatch Security Analytics service on Cisco DNA Center, in conjunction with Cisco Stealthwatch, provides real-time monitoring of all network traffic. When you use the Stealthwatch Security Analytics service to enable Encrypted Traffic Analytics, you can enhance the protection of your network against encrypted threats without decrypting the traffic.

The Stealthwatch Security Analytics service on Cisco DNA Center automates the provisioning of network elements (based on best practices) so that they send data to Cisco Stealthwatch, enabling you to gain additional visibility, and improving your malware detection capabilities.

With Stealthwatch Security Analytics, you can:

- Assess what parts of the network are ready for deployment
- Enable Stealthwatch Security Analytics
- Monitor the status of deployment



Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Stealthwatch Supported Versions

The following table lists the minimum software version and the required licenses for Stealthwatch.

Product Family	Minimum Version	Product Components Required	License/Capacity Required
Stealthwatch Enterprise	7.0	<ul style="list-style-type: none"> Stealthwatch Management Console Flow Collector 	See the <i>Stealthwatch Management Console VE and Connector Flow VE Installation and Configuration Guide</i> .

Stealthwatch Security Analytics Supported Devices

Supported Devices for Enabling Encrypted Traffic Analytics

The following table lists the supported devices, minimum version, and license and platform requirements for enabling Encrypted Traffic Analytics.

Product Family	Minimum Version	License Required	Platforms
Cisco Catalyst 9300	Cisco IOS-XE 16.9.1	Cisco DNA Advantage	<ul style="list-style-type: none"> C9324 C9348
Cisco Catalyst 9400	Cisco IOS-XE 16.9.1	Cisco DNA Advantage	<ul style="list-style-type: none"> C9404 C9407 C9410
Cisco ISR 4000	Cisco IOS-XE 16.6.4	Either of the following: <ul style="list-style-type: none"> Cisco DNA Advantage SEC/K9 	<ul style="list-style-type: none"> 4221 4321 4331 4351 4431 4451
Cisco ASR 1000	Cisco IOS-XE 16.6.4	Either of the following: <ul style="list-style-type: none"> Cisco DNA Advantage SEC/K9 	<ul style="list-style-type: none"> 1001-X 1001-HX 1002-X 1002-HX

Supported Devices for Enabling Flexible NetFlow

The following table lists the supported devices and the minimum version and license requirements for enabling Flexible NetFlow.

Product Family	Minimum Version	License Required
Cisco Catalyst 9200	Cisco IOS-XE 16.9.1	Cisco DNA Advantage
Cisco Catalyst 3850	Cisco IOS-XE 16.9.1	Cisco DNA Advantage
Cisco Catalyst 3650	Cisco IOS-XE 16.9.1	Cisco DNA Advantage



CHAPTER 2

Set Up Stealthwatch Security Analytics

- [Install Stealthwatch Security Analytics, on page 5](#)
- [Register Stealthwatch, on page 5](#)
- [Set Up User Datagram Protocol Director, on page 6](#)
- [Enable Stealthwatch Security Analytics, on page 7](#)
- [Stealthwatch Security Analytics Prechecks, on page 8](#)
- [View Not Ready Devices, on page 9](#)

Install Stealthwatch Security Analytics

Step 1 From the Cisco DNA Center home page, navigate to **System > Software Updates**.

Step 2 Ensure that **Updates** is selected in the left pane.

Step 3 Click **Install** next to **Stealthwatch Security Analytics**.

After the installation is complete, the Stealthwatch Security Analytics service shows up under the **Installed Applications** page.

Register Stealthwatch

Step 1 From the Cisco DNA Center home page, navigate to **System > Settings** from the menu.

Step 2 In the left pane, enter **Stealthwatch** in the **Search Settings** bar.

Step 3 Click **Stealthwatch** in the left pane.

Step 4 Enter the IP address of the Stealthwatch Management Console or the fully qualified domain name (FQDN).

Step 5 Enter the username and password for the user account that you'd like to use to access the Stealthwatch Management Console.

The following are the minimum privileges required for the Stealthwatch user account:

- Data Role: Read only
- Function Roles: Configuration Manager and Network Engineer

Note You can create a custom user role in Cisco DNA Center to enable another user to provision Stealthwatch Security Analytics on devices. For more information about how to create a custom user role, see the *Cisco DNA Center User Guide*.

The following table lists the minimum permissions required for a user to provision Stealthwatch Security Analytics on a device.

Access	Description	Permission
Network Design > Advanced Network Settings	Advanced network settings for AAA, PKI certificates and Stealthwatch	Write
Network Design > Network Settings	Common site-wide network settings such as AAA, NTP, DNS servers, and IP pools. Need Write permissions on Network Profiles to create Wireless Profile.	Write
Network Provision > Provision	Provision devices with the site settings and policies that are configured for the network.	Write
Network Services > Stealthwatch	Configure devices with the site settings and policies that are configured for the network.	Read
System > Basic	Access to individual user settings. All users are granted this access.	Write

Step 6 Click **Save**.

After Stealthwatch has successfully been registered, the status displays as **Active | Registered and Running** just above the **IP Address** field.

Set Up User Datagram Protocol Director

The User Datagram Protocol (UDP) Director receives and replicates NetFlow and other traffic to multiple destinations.

Before you begin

You should already have installed and configured UDP Director in the Stealthwatch Management Console. For more information, see the *UDP Director Virtual Edition Installation and Configuration Guide (for Stealthwatch System v6.9.0)*.

Step 1 From the Cisco DNA Center home page, navigate to **Design > Network Settings**.

Step 2 (Optional) Use the left pane to drill down to the site for which you want to configure the Stealthwatch Flow Destination.

- Step 3** Click **Add Servers** in the top-right portion of the GUI.
- Step 4** From the **Add Servers** pop-up, check the **Stealthwatch Flow Destination** check box and click **OK**.
After you click **OK**, you might need to scroll down to find the **Stealthwatch Flow Destination** configuration section.
- Step 5** To add a flow destination configured in the Stealthwatch, click the corresponding radio button. Alternatively, you can add a destination that isn't managed by the Stealthwatch Management Console by clicking the corresponding radio button.
- Step 6** If you've chosen to select a flow destination configured in Stealthwatch, select the desired flow destination. If you see the error **No Stealthwatch flow destination server configured**, see [Register Stealthwatch, on page 5](#).
If you've chosen to add an external flow destination, specify the IP address and port of the desired flow destination.
- Step 7** Click **Save**.
-

Enable Stealthwatch Security Analytics

- Step 1** From the Cisco DNA Center home page, navigate to **Provision > Stealthwatch Security Analytics** from the menu.
- Step 2** In the left pane, use the drop-down list to select **All Sites** or **All Fabrics**, depending on whether you want to enable Stealthwatch Security Analytics for sites or for fabrics. By default, **All Sites** is selected.
- Step 3** In the left pane, drill down to the site or fabric for which you want to enable Stealthwatch Security Analytics. Alternatively, you can search for the site or fabric using the search bar.
- Step 4** Select the site or fabric for which you want to enable Stealthwatch Security Analytics by clicking the site card. If required, you can navigate the site and fabric hierarchy down to a specific floor.
The site card displays the number of devices that are enabled, ready, and not ready.
Note At least one device must be ready for you to enable Stealthwatch Security Analytics.
- Step 5** Review the prechecks and click **Get Started**.
- Step 6** Review the flow destination set up for the selected site or fabric. If you want to change the flow destination, click **Change Settings**. Set a new flow destination and restart the workflow.
If you see the error **Select a flow destination for the site to proceed**, click **Update Settings** to set a flow destination. Restart the workflow.
- Step 7** Click **Next**.
- Step 8** Ensure that the **Ready** tab is selected in the device table.
- Step 9** Review the list of devices that will be enabled.
From here, use the toggle switch to exclude all or specific devices from being enabled.
- Step 10** Select the corresponding radio button to deploy the application immediately (**Now**), or at a later time (**Later**).
Note For deployments scheduled for a later time, you can edit the scheduled time from the Notifications list in the upper-right corner of the screen, by clicking **Edit**.
A series of prechecks will be run close to the time of the deployment, including a precheck on the CPU of the device at that time. Any prechecks that fail will be listed in the task manager.

Step 11 Click **Enable**.

Step 12 To view the deployment status, click **View Deployment Status**. Alternatively, navigate to **Activity > Scheduled Tasks** from the Cisco DNA Center main menu to view the deployment status.

After your task is complete, the status of the deployment changes from **In Progress** to **Success**. To ensure that you're viewing the updated status, click the **Refresh** button in the upper-right corner of the Notifications list.

Note Prior to the provisioning action, whether it is run immediately or at a later time, an additional set of prechecks is run. The task will fail if:

- The device's CPU exceeds 70% at that point in time.
- NBAR is enabled on the access switches
- There are no Stealthwatch Security Analytics applicable interfaces on the switch.
- There is no route information for routers.

Stealthwatch Security Analytics Prechecks

The Stealthwatch Security Analytics service conducts an automatic precheck of the devices in your sites and fabrics to ensure they meet the criteria for deployment.

The following checks are conducted:

- **Required Software:** The software running on your devices must meet the minimum requirements.
- **Required Device Role:** The device role must support the deployment of the service. If you're using ASR and ISR series routers, then ensure that their **Device Role** is set to Border Router. If you're using 9300 and 9400 series switches, then ensure that their **Device Role** is set to Access.
- **Required Hardware:** The device hardware must support the deployment of the service.
- **Required Licenses:** The active license on the devices in your site must meet the minimum requirements.
- **No Conflicts with Other Services:** There should be no compatibility issues with other services. This check will fail if:
 - The device is managed by vManage.
 - NBAR is enabled on the device.



Note NBAR conflict is applicable to devices for Enable Flexible NetFlow as well as Catalyst 9300 and Catalyst 9400 switches running versions prior to 17.3.1.

- One or more interfaces on this device already have existing netflow monitors enabled.

The total number of devices that meet all of these criteria are considered to be **Ready**.



Note See [Stealthwatch Security Analytics Supported Devices, on page 2](#) for hardware, software, and license requirements.

View Not Ready Devices

Devices that have failed one or more of the software, compatibility, and license checks are considered to be not ready for the enablement of Stealthwatch Security Analytics. To view the list of devices that are **Not Ready**, complete the following steps:

-
- Step 1** From the Cisco DNA Center main menu, navigate to **Provision > Stealthwatch Security Analytics**.
 - Step 2** In the left pane, drill down to the site or fabric for which you want to view the devices that are not ready for Stealthwatch Security Analytics enablement. Alternatively, you can search for the site or fabric using the search bar.
 - Step 3** Select the site or fabric for which you want to view the not ready devices by clicking the appropriate site card.
 - Step 4** Click **Get Started**.
 - Step 5** Click **Next**.
 - Step 6** In the device table, click **Not Ready**.

The list of devices that are not ready for Stealthwatch Security Analytics enablement is displayed, along with the status of each check for each device.
 - Step 7** Hover your cursor over the red icon to view more information about any failed checks.
-



CHAPTER 3

Manage Stealthwatch Security Analytics

- [Review Status of Sites and Fabrics, on page 11](#)
- [View Scheduled Tasks, on page 11](#)
- [Update Stealthwatch Security Analytics, on page 12](#)
- [Disable Stealthwatch Security Analytics, on page 13](#)

Review Status of Sites and Fabrics

With Stealthwatch Security Analytics, you can view the status of the devices for each site or fabric.

-
- Step 1** From the Cisco DNA Center main menu, navigate to **Provision > Stealthwatch Security Analytics**.
- Step 2** In the left pane, drill down to the site or fabric for which you want to view the status.
- The card for the site or fabric indicates whether it is Deployed (full green circle) or Ready to deploy (open green circle).
- Step 3** To view device specific status, click a site or fabric card to view the devices that are **Ready**, **Not Ready**, or **Enabled**, and then click the corresponding tab.
- The following are the different statuses for the devices in a particular site or fabric:
- **Enabled Devices:** These devices have Stealthwatch Security Analytics enabled.
 - **Not ready Devices:** These devices have failed either one or more of the prechecks. The green check marks indicate the prechecks that the device has passed, while the red icons indicate the precheck that the device has failed. Hover over the red icon to view more information about the failed checks. See [Stealthwatch Security Analytics Prechecks, on page 8](#).
 - **Ready Devices:** These devices pass all the prechecks, and can be enabled for Stealthwatch Security Analytics. See [Enable Stealthwatch Security Analytics, on page 7](#).
-

View Scheduled Tasks

-
- Step 1** From the Cisco DNA Center main menu, navigate to **Activity > Scheduled Tasks**.

A list of completed and scheduled tasks is displayed.

Step 2 Use the **FILTERS** drop-down list to view only Stealthwatch Security Analytics tasks.

From here, you can view the list of scheduled and completed tasks. Click a task to view further information about it or to reschedule the task.

Update Stealthwatch Security Analytics

With Stealthwatch Security Analytics, you can update the configurations on devices that have previously been enabled, as changes to the network can occur over time.

Step 1 From the Cisco DNA Center main menu, navigate to **Provision > Stealthwatch Security Analytics**.

Step 2 In the left pane, drill down to the site or fabric for which you want to disable Stealthwatch Security Analytics. Alternatively, you can search for the site or fabric using the search bar.

Step 3 Select the site or fabric for which you want to disable Stealthwatch Security Analytics by clicking the site card.

The site card displays the number of devices that are **Enabled**, **Ready**, and **Not Ready**.

Note At least one device must be enabled for you to update Stealthwatch Security Analytics.

Step 4 Click **Get Started**.

Step 5 Review the flow destination set up for the selected site or fabric. If you want to change the flow destination, click **Change Settings**. Set a new flow destination and restart the workflow.

If you see the error **Select a flow destination for the site to proceed**, click **Update Settings** to set a flow destination. Restart the workflow.

Step 6 Click **Next** to continue.

Step 7 Ensure that the **Enabled** tab is selected in the device table.

Step 8 Select the **Update** radio button.

Note Updating devices will configure only what needs to be updated on the relevant network devices. For example, if 10 access interfaces had previously been enabled and there is one interface that is now relevant, updating the device will only push a configuration change to the one new interface.

Updating the device includes the following:

- A new line card is added
- Changes are made to interfaces that have Access Points plugged in
- Changes are made to VLANs

Step 9 Select the corresponding radio button to update Stealthwatch Security Analytics immediately (**Now**), or at a later time (**Later**).

Note If you have chosen to update Stealthwatch Security Analytics at a later time, then you can edit the scheduled time from **Activity > Scheduled Tasks** in the main menu.

Step 10 Click **Apply**.

Step 11 You can view the status of your deployment from **Activity > Scheduled Tasks** in the main menu.

After your task is complete, the status of the deployment changes from **In Progress** to **Success**.

Note To ensure that you're viewing the updated status, click the **Refresh** button in the top-right corner of the Notifications list.

Disable Stealthwatch Security Analytics

Step 1 From the Cisco DNA Center main menu, navigate to **Provision > Stealthwatch Security Analytics**.

Step 2 In the left pane, drill down to the site or fabric for which you want to disable Stealthwatch Security Analytics. Alternatively, you can search for the site or fabric using the search bar.

Step 3 Select the site or fabric for which you want to disable Stealthwatch Security Analytics by clicking the site card.

The site card displays the number of devices that are **Enabled**, **Ready**, and **Not Ready**.

Note At least one device must be enabled for you to disable Stealthwatch Security Analytics.

Step 4 Review the prechecks and click **Get Started**.

Step 5 Review the flow destination set up for the selected site or fabric. If you want to change the flow destination, click **Change Settings**. Set a new flow destination and restart the workflow.

If you see the error **Select a flow destination for the site to proceed**, click **Update Settings** to set a flow destination. Restart the workflow.


Step 6 Click **Next**.

Step 7 Ensure that the **Enabled** tab is selected in the device table.

Step 8 Use the toggle switch to exclude all or specific devices.

Step 9 Click the **Disable** radio button.

Step 10 Select the corresponding radio button to disable Stealthwatch Security Analytics immediately (**Now**), or at a later time (**Later**).

Note If you have chosen to disable Stealthwatch Security Analytics at a later time, then you can edit the scheduled time from the Notifications list () in the upper-right corner of the screen by clicking **Edit**.

Step 11 Click **Apply**.

Step 12 You can view the status of your deployment from the **Scheduled Tasks** tab under the Notifications list.

After your task is complete, the status of the deployment changes from **In Progress** to **Success**.

Note To ensure that you're viewing the updated status, click the **Refresh** button in the top-right corner of the Notifications list.



CHAPTER 4

Troubleshoot Stealthwatch Security Analytics

The Stealthwatch Security Analytics service displays error messages within the GUI to ensure that your usage of the application is as problem-free as possible. Apart from the error messages, you can use the information in this chapter to troubleshoot any issues you might be facing.

- [View Audit Logs](#) , on page 15
- [Troubleshoot Using Task Manager](#), on page 16
- [Troubleshoot on Supported Devices](#), on page 16

View Audit Logs

Audit logs capture information about the various applications running on Cisco DNA Center.

Step 1 From the Cisco DNA Center main menu, navigate to **Activity > Audit Logs**.

The **Audit Logs** window appears, where you can view logs about what has happened across the system.

The following information is displayed for each audit log:

- **Description:** Audit log description
- **Site:** Name of the site for the specific audit log
- **Device:** Devices for the audit log
- **Requestor:** User requesting the action that is being logged
- **Source:** Source of an audit log
- **Created On:** Date on which the audit log was created

Step 2 Expand the arrows corresponding to view an audit log to view the corresponding child audit logs.

Note An audit log captures data about a task performed by Cisco DNA Center. Child audit logs are subtasks to a task performed by Cisco DNA Center.

Step 3 Filter the audit logs by clicking the **Filter** icon, entering a specific parameter, and then clicking **Apply**.

You can filter audit logs by using the following parameters:

- **Description**

- **Site**
- **Device**
- **Requestor**
- **Source**
- **Start Date**
- **End Date**

Step 4 (Optional) Click the dual arrow icon in the upper-right corner of the application screen to refresh the data displayed in the window.

Step 5 (Optional) Click **Log Id** to view the ID of the log and to copy the log ID to your clipboard.

Troubleshoot Using Task Manager

Step 1 From the Cisco DNA Center main menu, navigate to **Activity > Scheduled Tasks**.

Step 2 Identify the **Failed** task in the list, and click to view more details.

Note A single task may include multiple devices. The overall status of a task will show as **Failed** if even one device fails, although the other devices included in the task succeed.

Troubleshoot on Supported Devices

Following are some common troubleshooting issues experienced on supported devices.

Device Is Not Listed

If Cisco DNA Center does not list a device to enable or disable Stealthwatch Security Analytics, ensure that:

- If you are using ASR and ISR Series Routers, the **Device Role** is set to Border Router.
- If you are using 9300 and 9400 Series Switches, the **Device Role** is set to Access.
- If your device is not part of the fabric, the **Device Role** is set to Distribution.