Stealthwatch Security Analytics Service on Cisco DNA Center

First Published: 2019-04-24

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: www.cisco.com go trademarks. 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)

© 2018–2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **About Stealthwatch Security Analytics Service on Cisco DNA Center** 1

About Stealthwatch Security Analytics Service on Cisco DNA Center 1

Stealthwatch Supported Versions 1

Stealthwatch Security Analytics Supported Devices 2

CHAPTER 2 **Set Up Stealthwatch Security Analytics** 5

Install Stealthwatch Security Analytics 5

Register Stealthwatch 5

Stealthwatch Security Analytics Readiness Checks 6

Enable Stealthwatch Security Analytics 7

View Not Ready Devices 8

CHAPTER 3 **Manage Stealthwatch Security Analytics** 9

Review Status of Sites and Fabrics 9

View Scheduled Tasks 9

Disable Stealthwatch Security Analytics 10

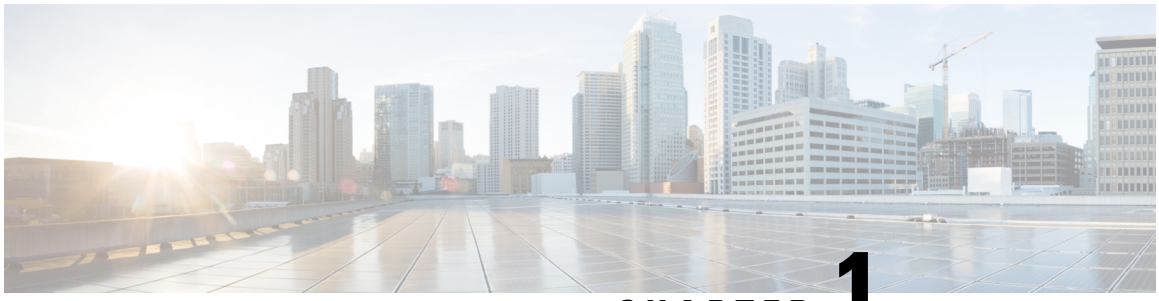
CHAPTER 4 **Troubleshoot Stealthwatch Security Analytics** 11

View Audit Logs 11

Troubleshoot Using Task Manager 12

Troubleshoot on Supported Devices 12

Device is not listed 12



CHAPTER 1

About 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 1
- 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 Network as a Sensor with Encrypted Traffic Analytics, you can enhance the protection of your network against encrypted threats without decrypting the traffic. You can also use the Stealthwatch Security Analytics service to enable Network as a Sensor on devices that do not support Encrypted Traffic Analytics.

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

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	6.10.2	• Stealthwatch Management Console • Flow Collector	See *Stealthwatch Management Console VE and Connector Flow VE Installation and Configuration Guide*.

Stealthwatch Security Analytics Supported Devices

Supported Devices for Enabling Network as a Sensor with Encrypted Traffic Analytics

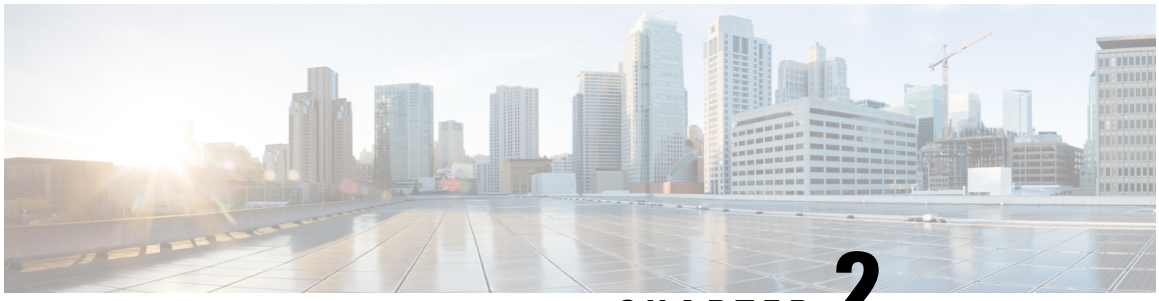
The following table lists the supported devices, minimum version, and license and platform requirements for enabling Network as a Sensor with Encrypted Traffic Analytics.

Product Family	Minimum Version	License Required	Platforms
Catalyst 9300	IOS-XE 16.6.4	DNA Advantage	• C9324 • C9348
Catalyst 9400	IOS-XE 16.6.4	DNA Advantage	• C9404 • C9407 • C9410
ISR 4k	IOS-XE 16.6.4	Either of the following: • DNA Advantage • SEC/K9	• 4221 • 4321 • 4331 • 4351 • 4431 • 4451
ASR 1k	IOS-XE 16.6.4	Either of the following: • DNA Advantage • SEC/K9	• 1001-X • 1001-HX • 1002-X • 1002-HX

Supported Devices for Enabling Network as a Sensor

The following table lists the supported devices and the minimum version and license requirements for enabling Network as a Sensor.

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



CHAPTER 2

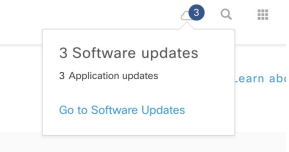
Set Up Stealthwatch Security Analytics

- Install Stealthwatch Security Analytics, on page 5
- Register Stealthwatch, on page 5
- Stealthwatch Security Analytics Readiness Checks, on page 6
- Enable Stealthwatch Security Analytics, on page 7
- View Not Ready Devices, on page 8

Install Stealthwatch Security Analytics

Step 1 On the Cisco DNA Center home page, click the **Software Updates** icon.

Step 2 Click **Go to Software Updates**.



Step 3 Ensure that the **Updates** is selected in the tab on the left.

Step 4 Under **Automation**, click **Install** next to **Stealthwatch Security Analytics**.

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

Register Stealthwatch

Step 1 From the Cisco DNA Center home page, click the gear icon (⚙) and select **System Settings**.

Step 2 Click **Settings** from the bar at the top.

Step 3 From the left navigation pane, select **Stealthwatch**.

Step 4 In the **IP Address** field, enter the IP address of your Stealthwatch Management Console.

If the IP address to which you are attempting to connect does not have a certificate signed by an official Certificate Authority, an alert appears.

Note By default, Stealthwatch Management Console ships with a self-signed certificate, which is not trusted.

If the alert appears because your Stealthwatch Management Console certificate is not trusted, then complete the following steps:

a) Click the red alert icon.
b) Select the check box to allow Cisco DNA Center to access the specified IP address and add the untrusted certificate to the Cisco DNA Center trust pool.
c) Review the certificate details.
d) Click **Allow**.

The red alert icon changes to a green check mark.

Step 5 Enter the **Username** and **Password** for the Stealthwatch User that you would like to use.

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

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

Step 6 Click **Apply**.

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

Stealthwatch Security Analytics Readiness Checks

The Stealthwatch Security Analytics service conducts an automatic readiness check 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.

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.

Enable Stealthwatch Security Analytics

Step 1 From the Cisco DNA Center home, navigate to the **Provision** page.

Step 2 Select the **Services** tab.

Step 3 Click **Stealthwatch Security Analytics**.

Step 4 In the left pane, select **All Sites** or **All Fabrics**, depending on whether you want to enable Stealthwatch Security Analytics for a site or fabric. By default, **All Sites** is selected.

Step 5 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 6 Select the site or fabric for which you want to enable Stealthwatch Security Analytics by clicking the site card. If you choose, you can navigate the site and fabric heirarchy 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 7 Review the readiness check and click **Get Started**.

Step 8 From the drop-down list, select the IP address of the Stealthwatch Flow Collector that you wish to use for this site or fabric.

If you do not see the desired Stealthwatch Flow Collector in the drop-down list, it probably has not been defined in the Stealthwatch Management Console. For more information, see the *Stealthwatch Management Console VE and Flow Collector VE Installation and Configuration Guide*.

Step 9 Click **Next**.

Step 10 Ensure that the **Ready** tab is selected in the device table.

Step 11 Review the list of devices that will be enabled.

Step 12 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 readiness checks will be run close to the time of the deployment, including a readiness check on the CPU of the device at that time. Any readiness checks that fail will be listed in the task manager.

Step 13 Click **Enable**.

Step 14 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**. To ensure that you're viewing the updated status click the **Refresh** button in the upper-right corner of the Notifications list.

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 home, navigate to the **Provision** page.

Step 2 Select the **Services** tab.

Step 3 Click **Stealthwatch Security Analytics**.

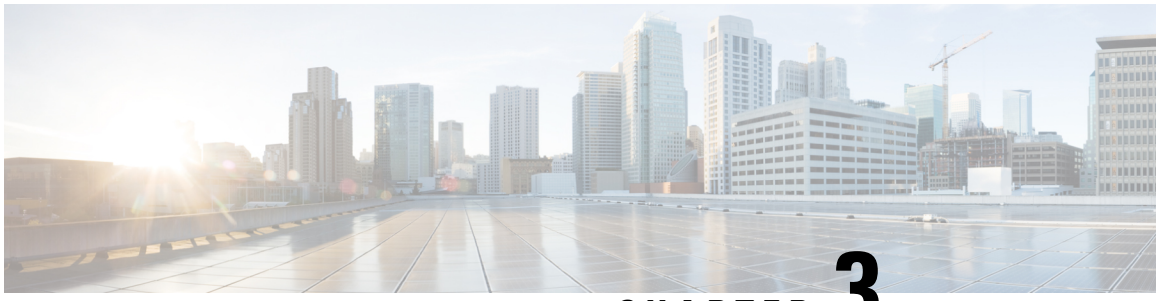
Step 4 In the left pane, drill down to the site or fabric for which you want to view the devices that are not ready for Stealthwatch Security Analytics enablement. Alternatively, you can search for the site or fabric using the search bar.

Step 5 Select the site or fabric for which you want to view the not ready devices, by clicking the appropriate site card.

Step 6 At the device table, click **Not Ready**.

The list of devices that are not ready for Stealthwatch Security Analytics enablement are displayed, along with the status of each check for each of the devices.

Step 7 Hover your cursor over the red icon to view more information about failed checks.



CHAPTER 3

Manage Stealthwatch Security Analytics

- Review Status of Sites and Fabrics, on page 9
- View Scheduled Tasks, on page 9
- Disable Stealthwatch Security Analytics, on page 10

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 home page, navigate to the **Provision** page.

Step 2 Select the **Services** tab.

Step 3 Click **Stealthwatch Security Analytics**.

Step 4 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 5 To view device specific status, click a site or fabric card to view the devices that are **Ready**, **Not Ready**, or **Enabled**, 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 readiness checks. The green check marks indicate the readiness checks that the device has passed, while the red icons indicate the readiness check that the device has failed. Hover over the red icon to view more information about the failed checks. See Stealthwatch Security Analytics Readiness Checks, on page 6.
- **Ready Devices** - These devices pass all the readiness checks, and can be enabled for Stealthwatch Security Analytics. See Enable Stealthwatch Security Analytics, on page 7.

View Scheduled Tasks

To view scheduled tasks, complete the following steps:

Step 1 From Cisco DNA Center, click the Notifications icon in the upper-right corner of the application window. By default, the **Scheduled Tasks** tab is selected.

A list of completed and scheduled tasks is displayed.

Step 2 Filter the list of tasks to view only Stealthwatch Seecurity Analytics tasks.

a) Click **Filter**.
b) From the **Type** drop-down list, select **SSA**.
c) Click **Apply**.

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.

Disable Stealthwatch Security Analytics

Step 1 From the Cisco DNA Center home, navigate to the **Provision** page.

Step 2 Select the **Services** tab.

Step 3 Click **Stealthwatch Security Analytics**.

Step 4 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 5 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 6 Ensure that the **Enabled** tab is selected in the device table.

Step 7 Select the corresponding radio button to disable Stealthwatch Security Analytics immediately (**Now**), or at a later time (**Later**).

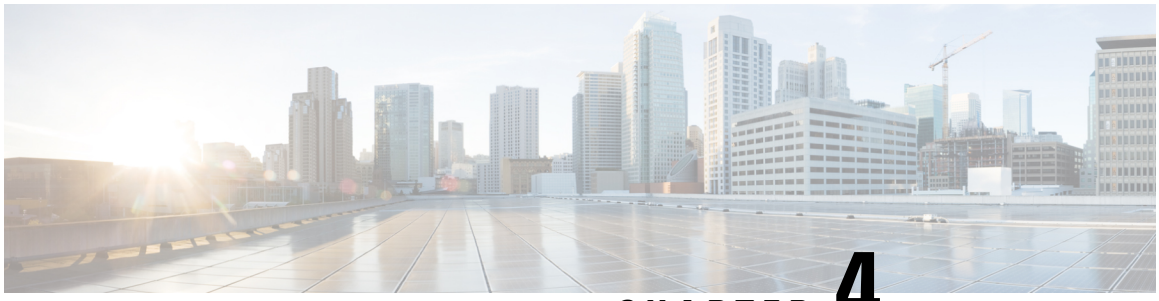
Note If you have chosen to disable Stealthwatch Security Analytics at a later time, then you can edit the scheduled time from the Notifications list ( ) in the upper-right corner of the screen, by clicking **Edit**.

Step 8 Click **Disable**.

Step 9 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 upper-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 11
- Troubleshoot Using Task Manager, on page 12
- Troubleshoot on Supported Devices, on page 12

View Audit Logs

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

Step 1 From the Cisco DNA Center home page, click the gear icon (⚙) and choose **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 Click the plus icon (+) next to an audit log to view the corresponding child audit logs.

Each audit log can be a parent to several child audit logs. By clicking this plus icon, you can view a series of additional 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 the following parameters:

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

Step 4 (Optional) Click the dual arrow icon to refresh the data displayed in the window.

Step 5 (Optional) Click the download icon to download a local copy of the audit log in .csv file format.

A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on Cisco DNA Center.

Troubleshoot Using Task Manager

Step 1 On the Cisco DNA Center home page, click the Notifications icon ( ) in the upper-right portion of the application screen.

Step 2 Ensure that the **Scheduled Tasks** tab is selected.

Step 3 Identify the **Failed** task in the list, and click the corresponding arrow.

The entry expands to show you the details of the task.

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

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, then 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`.

Device is not listed