Set Up Stealthwatch Security Analytics

Install Stealthwatch Security Analytics

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Updates**.

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

Step 3 Next to **Stealthwatch Security Analytics**, click **Install**.

After the installation is complete, the Stealthwatch Security Analytics service is displayed under the **Installed Applications** window.

Register Stealthwatch

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings**.

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

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.

Note After adding a new user to the Stealthwatch Management Console, make sure that the user logs in to the Stealthwatch Management Console at least once before integrating it with Cisco Stealthwatch. Upon first login, the user is prompted to set a new password and activate the API access.

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 *Cisco DNA Center Administrator 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. Write permissions are required on Network Profiles to create a 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 is registered successfully, the status is displayed as **Active | Registered and Running** just above the **IP Address** field.

Set Up the User Datagram Protocol Director

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

Before you begin

Install and configure UDP Director in the Stealthwatch Management Console. For more information, see *UDP Director Virtual Edition Installation and Configuration Guide (for Stealthwatch System v6.9.0)*.

Step 1 From the top-left corner, click the menu icon and choose **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 Scroll down and expand the **Stealthwatch Flow Destination** area.

Step 4 To add a flow destination configured in 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 5 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 1.

If you've chosen to add an external flow destination, specify the IP address and port of the desired flow destination.

Step 6 Click **Save**.

Enable Stealthwatch Security Analytics

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Stealthwatch Security Analytics**.

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 Use the toggle switch in the **ETA Telemetry** column to enable or disable the collection of Encrypted Traffic Analytics telemetry data. By default, this option is enabled for devices that are Encrypted Traffic Analytics capable. For a list of devices that are compatible with Encrypted Traffic Analytics, see Enable Stealthwatch Security Analytics, on page 3.

Step 11 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 12 Click **Enable**.

Step 13 To view the deployment status, click **View Deployment Status**. Alternatively, from the Cisco DNA Center main menu, choose **Activity** > **Tasks** 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 fails 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, ensure that their **Device Role** is set to Border Router. If you're using 9300 and 9400 series switches, 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 fails if:
    - The device is managed by vManage.
    - NBAR is enabled on the device.

Note An NBAR conflict applies to devices for Enable Flexible NetFlow as well as Catalyst 9300 and Catalyst 9400 switches running versions earlier than 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 Prechecks, on page 4 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 top-left corner, click the menu icon and choose **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 use the search bar to search for the site or fabric.

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.

Enable Flexible NetFlow Export to the Stealthwatch Cloud

You can configure Stealthwatch Security Analytics to enable Flexible NetFlow export to the Stealthwatch cloud.

The Stealthwatch cloud supports Cisco Catalyst 9200 and 9300 devices that are running Cisco IOS XE Release 17.3.1 and later.

Before you begin

- Make sure that you have the Cisco DNA Advantage software license.
- Confirm that the Stealthwatch Security Analytics user role has Configuration Manager and Network Engineer permissions.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature, and add them to sites.

Step 1 In the Stealthwatch cloud portal, choose **Settings** > **Sensors** > **Service key**.

Step 2 In the Service key field, copy the service key and save it for later use.

The Stealthwatch cloud can send Flexible NetFlow data to the following regions:

- US
- EU
- APJC

The service key varies by region. Depending on your sites, you can have up to three different service keys.

Step 3 Configure the Stealthwatch flow destination to the Stealthwatch cloud.

a) From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Network**.
b) Use the left pane to drill down to the site for which you want to configure the Stealthwatch Flow Destination.
c) Scroll down and expand the **Stealthwatch Flow Destination** area.
d) Click the **Stealthwatch Cloud** radio button.
e) In the **Service Key** field, paste the service key that you copied earlier.
f) Click **Save**.

Step 4 Choose **Provision** > **Services** > **Stealthwatch Security Analytics**.

Step 5 In the left pane, drill down to the desired site.

Step 6 Click the site card and then click **Get Started**.

Step 7 Confirm that the flow destination is set to **Stealthwatch Cloud**, then click **Next**.

Step 8 In the **Ready** tab, choose the devices to deploy for the Stealthwatch cloud, then click **Enable**.

Step 9 To monitor the status of the deployment, click **View Deployment Status**.

Step 10 Click **Close**.

Step 11 The **Enabled** tab shows the new devices with an SWC Status of Enabled. Select the corresponding radio button to apply the updates immediately (**Now**), or at a later time (**Later**). Click **Apply**.

Step 12 Return to the Stealthwatch cloud portal and choose **Settings** > **Sensors**. Look for the new sensor (the sensor name is the device hostname). The sensor turns green when data starts uploading to the Stealthwatch cloud portal. The sensor turns red when data is not sent.
In the Stealthwatch cloud portal, when the sensors turn green, traffic details are visible in the dashboard.