Revised: September 18, 2025

Stealthwatch Security Analytics Service on Cisco Catalyst Center User Guide, Release 3.1.3

Stealthwatch Security Analytics Service on Catalyst Center

Stealthwatch Security Analytics service on Catalyst Center

The Stealthwatch Security Analytics service on Catalyst Center works with Cisco Stealthwatch to provide real-time monitoring of all network traffic.

Note

Cisco Stealthwatch is also known as Cisco Secure Network Analytics.

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 Catalyst Center automates the provisioning of network elements (using best practices). This automation allows network elements to send data to Cisco Stealthwatch. As a result, you gain more visibility and improve your malware detection capabilities.

With Stealthwatch Security Analytics, you can

- assess network readiness for deployment
- enable Stealthwatch Security Analytics
- monitor the deployment status, and
- monitor up to 1,000 devices per site.

Stealthwatch Security Analytics supported versions

This table lists the minimum software version and required licenses for Stealthwatch Security Analytics.

Product family	Minimum version	Product components required	License and capacity required
Stealthwatch Enterprise	7.0	• Stealthwatch Management Console • Flow Collector	See *Stealthwatch Management Console VE and Flow Collector VE Installation and Configuration Guide*.

Stealthwatch Security Analytics supported devices

Supported devices for enabling Encrypted Traffic Analytics

Use this table to identify supported devices and check minimum versions and license requirements for enabling Encrypted Traffic Analytics.

Note

Some devices support both Encrypted Traffic Analytics and Flexible NetFlow. For these devices, you can disable Encrypted Traffic Analytics using the **ETA Telemetry** toggle button. When you disable Encrypted Traffic Analytics, only Flexible NetFlow is enabled.

Product family	Minimum version	License required
Cisco Catalyst 9300 Series Switches	Cisco IOS XE Release 16.9.1	DNA Advantage
Cisco Catalyst 9400 Series Switches	Cisco IOS XE Release 16.9.1	DNA Advantage
Cisco 4000 Series Integrated Services Routers	Cisco IOS XE Release 16.6.4	Your device requires one of these licenses: • DNA Advantage • SEC/K9
Cisco 1000 Series Aggregation Services Routers	Cisco IOS XE Release 16.6.4	Your device requires one of these licenses: • DNA Advantage • SEC/K9

Supported devices for enabling Flexible NetFlow

This 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 Series Switches	Cisco IOS XE Release 16.9.1	DNA Advantage
Cisco Catalyst 3850 Series Switches	Cisco IOS XE Release 16.9.1	DNA Advantage
Cisco Catalyst 3650 Series Switches	Cisco IOS XE Release 16.9.1	DNA Advantage

Set Up Stealthwatch Security Analytics

Install Stealthwatch Security Analytics

Step 1 From the main menu, choose **System** > **Software Management**.

Step 2 In the **Available Applications for the release** area, check the check box next to **Stealthwatch Security Analytics**.

Step 3 Click **Install**.

After the installation is complete, click **View Installed Applications** to ensure that the Stealthwatch Security Analytics service is listed.

Access control for Stealthwatch Security Analytics

Access control for Stealthwatch Security Analytics on Catalyst Center can be managed using these configurations:

Configuration	Description
Role	Defines the available permissions for users to access the Catalyst Center features. You can create a custom role and select the required permission for **Stealthwatch**. When you select a permission for **Stealthwatch**, Catalyst Center automatically assigns the necessary permissions for its dependent capabilities, including network design, network management, network provision, and system. You can modify these permissions, if needed.
Access group	Restricts access for a role to a specific scope based on the site hierarchy. For a custom role, when you set the **Stealthwatch** permission to **Read** or **Write**, choose the **Global** scope for the corresponding access group.
Users	Defines the username, password, and related information. Limits the access to features based on the access group.

To create roles, access groups, and users, see "Manage Users" in the *Cisco Catalyst Center Administrator Guide*.

Permission requirement for Stealthwatch Security Analytics

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

Access	Description	Permission
Security > **Stealthwatch**	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic.	Write
Network Design > **Profiles and Settings**	Manage sitewide network settings such as AAA, NTP, and DHCP. Manage telemetry and profiles.	Write
Network Management > **Hierarchy**	Create a network hierarchy of areas, buildings, and floors based on geographic location. This role also includes CMX server settings.	Read
Network Management > **Inventory**	Add, update, or delete devices on your network. Manage device attributes; view and manage network topology and configurations.	Read
Network Provision > **Device Provision**	Provision devices with site-specific settings and policies that are configured for the network.	Write
System > **System Administration**	Manage core system administrative capabilities, including HA, Disaster Recovery, and Backup and Restore.	Read
System > **System Settings**	Manage core system connectivity settings. This role includes Integrity Verification, Integration Settings, Debugging Logs, Telemetry Collection, System EULA, IPAM, Data Platform, Cisco Credentials, Smart account, Smart Licensing, SSM Connection Mode, and Device EULA.	Read

Register Stealthwatch

Step 1 From the main menu, 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.

These minimum privileges are 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 Catalyst Center to enable another user to provision Stealthwatch Security Analytics on devices. For more information, see Access control for Stealthwatch Security Analytics, on page 2.

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 UDP Director

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

You must install and configure 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 main menu, choose **Design** > **Network Settings**.

Step 2 (Optional) From the left hierarchy tree, select the site for which you want to configure the Stealthwatch Flow Destination.

Step 3 In the **Servers** tab, expand the **Stealthwatch Flow Destination** area.

Step 4 Select one of these options to add a flow destination:

If you selected...	Then...
Select from flow destinations configured in the Stealthwatch	from the **Select flow destination** drop-down list, select a flow destination. If you see the error **No Stealthwatch flow destination server configured**, see Register Stealthwatch, on page 4.
Add an external flow destination server	enter the IP address and port of the flow destination in the corresponding fields.

Step 5 Click **Save**.

Enable Stealthwatch Security Analytics

Step 1 From the main menu, choose **Provision** > **Stealthwatch Security**.

Step 2 In the left pane, use the drop-down list to choose the desired option.

If you want to enable Stealthwatch Security Analytics for...	Then select...
sites	**All Sites**
fabrics	**All Fabrics**

By default, **All Sites** is selected.

Step 3 From the left hierarchy tree, select the site or fabric for which you want to enable Stealthwatch Security Analytics.

You can also search for the site or fabric using the search bar.

Step 4 Click the site card to select the site or fabric on which you want to enable Stealthwatch Security Analytics.

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 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...	Then...
want to change the flow destination	**a.** Click **Change Settings**. **b.** Set a new flow destination and restart the workflow.
see the **Select a flow destination for the site to proceed** error	**a.** Click **Update Settings**. **b.** Set a flow destination and 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 on which Stealthwatch Security Analytics will be enabled.

If you want to exclude enabling Stealthwatch Security Analytics on...	Then...
all devices	click the **Exclude all devices** toggle button.
specific devices	under the **Exclude Device** column, click the corresponding toggle button.

Step 10 Use the toggle button 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 5.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 8.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 9.

Step 12 On the **Tasks** window, monitor the task deployment.

Note

Before 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 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, or
- 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 that they meet the criteria for deployment.

The service conducts these checks:

- **Required Software**: Your device software must meet the minimum requirements.
- **Required Device Role**: The device role must support the deployment of the service.
  - For Cisco ASR and ISR Series Routers, set the **Device Role** to Border Router.
  - For Cisco Catalyst 9300 or 9400 Series Switches, set the **Device Role** to Access.
- **Required Hardware**: Your 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 existing configurations**: Ensure that there are no compatibility issues with other services.

  This check fails if
  - the device is managed by vManage,
  - NBAR is enabled on the device, or
  - one or more interfaces on this device already have existing NetFlow monitors enabled.

Note

An NBAR conflict applies to devices for Enable Flexible NetFlow, and Cisco Catalyst 9300 and Cisco Catalyst 9400 switches running versions earlier than Cisco IOS XE Release 17.3.1.

Devices that meet all these criteria display **Ready** as their status.

Note

For information about requirements (hardware, software, and license), see Stealthwatch Security Analytics supported devices, on page 1.

View Not Ready devices

Devices that fail software, compatibility, or license checks are labeled **Not Ready**. Complete this procedure to view devices that are not ready for Stealthwatch Security Analytics enablement.

Step 1 From the main menu, choose **Provision** > **Stealthwatch Security**.

Step 2 From the left hierarchy tree, select the site or fabric for which you want to view the devices that are not ready.

You can also use the search bar to search for a site or fabric.

Step 3 Click the site card for the site or fabric where you want to view the devices that are not ready.

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 appears, along with the status of the checks for each device.

Step 7 Hover your cursor over the red icon to view more information for a failed check.

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.

- Make sure that you have the DNA Advantage software license.
- Confirm that the Stealthwatch Security Analytics user role has Configuration Manager and Network Engineer permissions.
- Use the Discovery feature to add devices to your inventory and assign them to sites if you do not already have devices in your inventory.

Step 1 In the Stealthwatch Cloud portal, complete these steps:

a) Choose **Settings** > **Sensors** > **Service key**.

b) In the **Service key** field, copy the service key and save it for later use.

The Stealthwatch Cloud can send Flexible NetFlow data to these regions:

- United States (US)
- European Union (EU)
- Asia Pacific, Japan, and China (APJC)

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

Step 2 In Catalyst Center, configure the Stealthwatch flow destination to the Stealthwatch Cloud.

a) From the main menu, choose **Design** > **Network Settings** > **Network**.
b) From the left hierarchy tree, select the site for which you want to configure the Stealthwatch flow destination.
c) Scroll to the **Stealthwatch Flow Destination** area and expand it.
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 3 Enable Stealthwatch Security Analytics, then confirm that the flow destination is set to **Stealthwatch Cloud**.

See Enable Stealthwatch Security Analytics, on page 5 for more information.

Step 4 The **Enabled** tab shows the new devices with an SWC Status of Enabled.

Step 5 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 8.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 9.

Step 6 On the **Tasks** window, monitor the task deployment.

Step 7 Return to the Stealthwatch Cloud portal and choose **Settings** > **Sensors**.

Look for the new sensor.

Tip

The sensor name is the device hostname.

When data is uploaded to the Stealthwatch Cloud portal, the sensor status indicator is green. If data is not sent, the sensor status indicator is red.

In the Stealthwatch Cloud portal, when the sensors turn green, traffic details are visible in the dashboard.

Deploy your device configurations now or later

At the scheduling step of a workflow that supports Visibility and Control of Configurations, complete this procedure to deploy your device configurations immediately or at a later time.

Ensure that you have disabled Visibility and Control of Configurations in the settings.

Step 1 Click **Now** or **Later**. Update the task name if needed.

Note If only visibility is enabled, or if both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected by default. The options **Now** and **Later** are dimmed.

Step 2 On the **Performing Initial Checks** window, prepare and submit the task for deployment.

a) Address all the issues to deploy the device configurations.

Ensure all validations are successful by clicking **Recheck**.

b) Click **Submit**.

The device configurations deploy at the scheduled time. View the task in the **Tasks** window.

Preview and deploy your device configurations

When you reach the scheduling step in a workflow that supports Visibility and Control of Configurations, complete this procedure to preview and deploy your device configurations.

Ensure that Visibility and Control of Configurations is enabled in the settings.

Step 1 Click **Preview and Deploy (Recommended)** and, if necessary, update the task name.

Note By default, if only visibility is enabled or both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected. The **Now** and **Later** options are dimmed.

Step 2 On the **Performing Initial Checks** window, address all the issues to continue with your current deployment.

Ensure all validations are successful by clicking **Recheck** in the lower right corner of the window.

Step 3 On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations.

Tip This preparation can take some time. You can click **Exit and Preview Later** and view the work item in the **Tasks** window.

Step 4 In the **Preview Configuration** window, review the device configurations. The window displays a deployment option.

Click...	**To...**
Deploy or **Submit for Approval**	deploy the device configurations.
Exit and Preview Later	review and deploy the device configurations later. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

Step 5 Schedule the deployment.

a) Indicate when and, if applicable, where you want to deploy the configuration.

If you are submitting the configurations for review, add notes for the IT administrator.

b) Click **Submit**.

You can check the work item approval status or the task deployment status on the **Tasks** window. If it is not approved, resubmit the work item for ITSM approval. When it is approved, the item is deployed at the scheduled time.

Note After submitting the task, view the progress of the provisioning task with the **Task Progress** bar in the **Activities** > **Tasks** window by clicking the task name.

Manage Stealthwatch Security Analytics

Review the 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 main menu, choose **Provision** > **Stealthwatch Security**.

Step 2 In the left pane, select a site or fabric to view its status.

Each site or fabric card displays these colors:

- Blue: For devices on which Stealthwatch Security Analytics is enabled.
- Green: For devices that have passed the prechecks and on which Stealthwatch Security Analytics can be enabled.
- Red: For devices that have failed the prechecks and on which Stealthwatch Security Analytics cannot be enabled.
- Purple: For devices on which ETA telemetry is enabled.

Step 3 To view device status, click a site or fabric card.

View the devices that are **Ready**, **Not Ready**, or **Enabled**, and then click the corresponding tab.

Devices in a site or fabric have these statuses:

- **Enabled Devices**: These devices have Stealthwatch Security Analytics enabled.
- **Not ready Devices**: These devices have failed one or more prechecks.

  Green check marks indicate the prechecks the device passed. Red icons indicate the prechecks the device failed. Hover your cursor over the red icon to view details about failed checks.
- **Ready Devices**: These devices have passed all prechecks and can be enabled for Stealthwatch Security Analytics.

View scheduled tasks

Step 1 From the main menu, choose **Activities** > **Tasks**.

By default, the **Tasks** window displays

- all upcoming, in-progress, failed, and successful tasks, and
- existing, pending-review, and failed work items.

Step 2 In the left pane, under **Type**, click **Task** to view only tasks.

Step 3 In the left pane, under **Status**, check the **Upcoming** check box to view only scheduled tasks.

Step 4 In the left pane, complete these steps to view only the scheduled Stealthwatch Security Analytics tasks:

a. Expand **Categories**.

b. Click **Show all**.

c. In the **Search** field, enter **SSA**.

d. Check the **SSA** check box.

Step 5 To view more information about a task, click it.

For more information about managing your task, see "View, Edit, and Delete Tasks" in the *Cisco Catalyst Center Administrator Guide*.

Update Stealthwatch Security Analytics

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

Step 1 From the main menu, choose **Provision** > **Stealthwatch Security**.

Step 2 In the left pane, use the drop-down list to select the required option.

If you want to enable Stealthwatch Security Analytics for...	Then select...
sites	**All Sites**
fabrics	**All Fabrics**

By default, **All Sites** is selected.

Step 3 From the left hierarchy tree, select the site or fabric for which you want to update Stealthwatch Security Analytics.

Alternatively, you can use the search bar to search for the site or fabric.

Step 4 Click the site card to select the site or fabric for which you want to update Stealthwatch Security Analytics.

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

Note You must enable at least one device to update Stealthwatch Security Analytics.

Step 5 Click **Get Started**.

Step 6 Review the flow destination setup for the selected site or fabric.

If you want to exclude updating Stealthwatch Security Analytics on...	Then...
all devices	click the **Exclude all devices** toggle button.

If you want to exclude updating Stealthwatch Security Analytics on...	Then...
specific devices	under the **Exclude Device** column, click the corresponding toggle button.

Step 7 Click **Next**.

Step 8 Ensure that the **Enabled** tab is selected in the device table.

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

Note Updating devices configures only the necessary changes on relevant network devices. For example, if 10 access interfaces had previously been enabled and now only one interface is relevant, updating the device pushes a configuration change only to the new interface.

Updating the device includes these updates:

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

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 8.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 9.

Step 11 On the **Tasks** window, monitor the task deployment.

Disable Stealthwatch Security Analytics

Step 1 From the main menu, choose **Provision** > **Stealthwatch Security**.

Step 2 In the left pane, select the option you need from the drop-down list.

If you want to disable Stealthwatch Security Analytics for...	Then select...
sites	**All Sites**
fabrics	**All Fabrics**

By default, **All Sites** is selected.

Step 3 From the left hierarchy tree, select the site or fabric for which you want to enable Stealthwatch Security Analytics.

You can also search for the site or fabric using the search bar.

Step 4 To disable Stealthwatch Security Analytics for a site or fabric, click the site card..

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

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

Step 5 Review the prechecks. Click **Get Started**.

Step 6 Review the flow destination setup for the selected site or fabric.

If you...	Then...
want to change the flow destination	**a.** Click **Change Settings**. **b.** Set a new flow destination and restart the workflow.
see the **Select a flow destination for the site to proceed** error	**a.** Click **Update Settings**. **b.** Set a flow destination and restart the workflow.

Step 7 Click **Next**.

Step 8 Verify that the **Enabled** tab is selected in the device table.

Step 9 Review the list of devices on which Stealthwatch Security Analytics will be disabled.

If you want to exclude enabling Stealthwatch Security Analytics on...	Then...
all devices	click the **Exclude all devices** toggle button.
specific devices	under the **Exclude Device** column, click the corresponding toggle button.

Step 10 Click the **Disable** radio button.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 8.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 9.

Step 12 On the **Tasks** window, monitor the task deployment.

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

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

Step 1 From the main menu, choose **Activities** > **Audit Logs**.

After the **Audit Logs** window opens, you can view logs of system activity.

This information is provided 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 who requested 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 drop-down for an audit log to view its child audit logs.

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

Step 3 Filter the audit logs

a) Click the **Filter** icon.
b) Enter a specific parameter for filtering the audit logs.
c) Click **Apply**.

Step 4 (Optional) Click the dual arrow icon located at the upper right of the window to refresh the data.

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

Troubleshoot using task manager

Step 1 From the main menu, choose **Activities** > **Tasks**.

Step 2 Identify the problematic task in the list. Click **Failed** to view more details.

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

Troubleshoot on supported devices

These issues are some common issues that you can troubleshoot on supported devices.

Device is not listed

If Catalyst Center doesn't list a device to enable or disable Stealthwatch Security Analytics, verify the device role.

If you're using...	Ensure that the device role is set to...
Cisco ASR and ISR Series Routers	Border Router
Cisco Catalyst 9300 and 9400 Series Switches	Access
a device that isn’t a part of the fabric	Distribution