aWIPS Profiles

About aWIPS Profiles

aWIPS profile configuration allows you to select the required signatures, configure the threshold values used in the detection of aWIPS denial of service (DoS) attacks, and enable forensic capture at the signature level. Threshold configuration helps to adjust the number of alarms that are generated for a specific duration for each aWIPS signature.

aWIPS profile configuration support is available for the following devices with software version 17.4 and later:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Catalyst 9800-CL Cloud Wireless Controller
- Cisco Embedded Wireless Controller on Catalyst Access Points
- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Note For SD-Access use cases only, you must enable the wireless module on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500 Series Switches for aWIPS profiles to work.

Prerequisites for aWIPS Profile

- Verify the network connectivity between the Cisco Wireless Controller and Catalyst Center.
- Make sure that the network device is reachable from Catalyst Center and has downloaded the aWIPS profile configuration from Catalyst Center.
- For forensic capture to take place make sure that there is network connectivity between APs and Catalyst Center.
- For forensic capture to take place make sure that the Google Protocol RPC (gRPC) tunnel interface has been established between APs and Catalyst Center. Use the **show ap icap connection** command to make sure that the status is READY.
- For forensic capture to take place the required ports must be opened between Catalyst Center and network device links.
- For forensic capture to take place there should be no time lag between Catalyst Center and access points.
- If you have upgraded Catalyst Center from a release earlier than Release 2.2.1, you must disable and enable **aWIPS** from the **Rogue and aWIPS** dashboard to subscribe to an additional subscription. For more information, see Monitor the Rogue Management and aWIPS Dashboard.

Note For a new installation of Catalyst Center, you do not have to disable and enable **aWIPS** from the **Rogue and aWIPS** dashboard to subscribe an additional subscription.

Create an aWIPS Profile Configuration Workflow

This section provides information about how to create an aWIPS profile.

Step 1 From the top-left corner, click the menu icon and choose **Workflows** > **Create an aWIPS Profile**.

Alternatively, you can create an aWIPS profile by choosing **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** > **Add Profile**.

The **Create an aWIPS Profile** window is displayed.

Step 2 Click **Let's Do it**.

The **aWIPS Profile Creation** window is displayed.

Step 3 In the **Profile Name** field, enter a name for the aWIPS profile.

Step 4 The **Signatures** table lists the following aWIPS profile parameters:

- **Signature**: Shows the standard aWIPS signatures that detect the various DoS attacks.
- **Default Threshold**: Shows the predefined threshold value for the respective aWIPS signature.
- **Configure Threshold**: Shows the manually configured threshold value for the respective aWIPS signature.

- **Time Interval (In Seconds)**: Shows the time interval of packets.
- **Forensic Capture**: Captures the aWIPS DoS attack packets in real time for the given signature.

Step 5 In the **Signature** column, check the check box next to the aWIPS signature that you want to select or deselect for an aWIPS profile.

Note If an aWIPS signature is not selected for an aWIPS profile, Catalyst Center does not detect the DoS attack for that particular aWIPS signature.

Step 6 In the **Configure Threshold** column, for the chosen aWIPS signature, enter the threshold value within the specified range that is displayed on top of the respective **Configure Threshold** field.

For some signatures, the configuration threshold is not applicable. The threshold configuration value for those signatures is displayed as **NA** on top of the respective **Configure Threshold** field.

Note The **Configure Threshold** value cannot contain alphanumeric characters.

Step 7 In the **Forensic Capture** column, click the toggle button to enable or disable the forensic capture for a particular aWIPS signature.

Note
- Catalyst Center does not allow you to edit the **Default Threshold** value and the **Time Interval (In Seconds)** value for the aWIPS profile.
- If you enable forensic capture for an aWIPS signature, Catalyst Center allows you to download packets from the **Threat 360** window.
- If you disable forensic capture for an aWIPS signature, Catalyst Center does not capture the aWIPS DoS attack for the given signature.
- Enabling **Forensic Capture** for RTS Flood and CTS Flood signatures might impact the performance of Catalyst Center.

Step 8 (Optional) Click **Reset to Default** to get the default aWIPS profile configuration.

Note Default aWIPS profile is configured for high security environment and not suitable for general purpose deployment. Configure aWIPS profile based on your requirement.

Step 9 Click **Next**.

Note In the **Configure Threshold** column, for the chosen aWIPS signature, if you enter a threshold value that is out of the specified range, an error message is displayed on top of the **Create an aWIPS Profile** window, asking you to enter a value within the specified range.

Step 10 In the **Profile Summary** window, the **Profile Summary** table displays the summary of the profile that was configured in the **aWIPS Profile Creation** window.

Step 11 Click **Next**.

Step 12 In the **Profile Creation Done** window, click **Assign Profile to Device(s)** to assign this aWIPS profile to a device.

The **Assign aWIPS Profile** window appears.

You can also assign an aWIPS profile to a device in the **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** window by checking the check box next to the aWIPS profile name and choosing **More Actions** > **Assign**.

Note You cannot assign more than one aWIPS profile to a device at a time.

Step 13 In the **Assigned WLCs** column, click the number link to view the number of wireless controllers assigned to an aWIPS profile.

The **Profile Assigned to WLC** window shows the following attributes of the network device:

- **Device Name**: Shows the name of the network device.
- **IP Address**: Shows the IP address of the network device.
- **Profile Config URL Push Status**: Shows the status of the profile configuration URL push to the network device. The possible values are **Success**, **Failure**, and **In Progress**.

  If the status is **Failure**, hover your cursor over the **i** icon next to **Failure** to see the reason for failure.
- **Profile Config Download Status (On Device)**: Shows the profile configuration download status on the device. The possible values are **Success**, **Failure**, and **In Progress**.

  If the status is **Failure**, hover your cursor over the **i** icon next to **Failure** to see the reason for failure.

  Note
  - If the aWIPS subscription is disabled on Catalyst Center, an error message appear top of the **aWIPS Profile** dashboard. You must have an aWIPS subscription to see the value of **Profile Config Download Status (On Device)**. To subscribe the aWIPS data collection, enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS Dashboard.
  - HTTP protocol reachability must be possible between the device and Catalyst Center for the device to download the profile configuration from the profile configuration URL.
- **Forensic capture config Status**: Shows the forensic capture configuration status on the **default-ap-profile** AP Join Profile on the device. The possible values are **Success**, **Failure**, and **In Progress**.

  If the status is **Failure**, hover your cursor over the **i** icon next to a **Failure** to see the reason for failure.
- **Forensic Capture**: Shows whether the forensic capture is enabled or disabled on the **default-ap-join** AP Join Profile on the device. Forensic capture on custom AP join profile is not supported.

  Hover your cursor over the **i** icon next to the corresponding Forensic capture. A tooltip stating **Shows the current Forensic Capture status on default-ap-profile AP Join Profile on the device** appears.

  Note In the **Profile Assigned to WLC** window, you cannot enable or disable **Forensic Capture**.
- **Assigned On**: Shows the date and time the aWIPS profile is assigned to the wireless controller.

Step 14 Click **Next**.

The **Profile Creation Done** window appears.

View an aWIPS Profile

From the top-left corner, click the menu icon and choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile**.

The **aWIPS Profile(s)** dashboard appears.

Note When you navigate to the **aWIPS Profile** tab for the first time, a message appears on top of the **aWIPS Profile** dashboard, asking you to subscribe to the upgraded subscription even if **aWIPS** is enabled in Catalyst Center. To subscribe to the upgraded subscription, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS Dashboard.

The aWIPS Profile dashboard displays the following information:

- **Profile Name**: Shows the list of aWIPS profiles names.
- **Assigned WLCs**: Shows the number of assigned wireless controllers to an aWIPS profile.
- **Last Changed**: Shows the last created or updated date and time of an aWIPS profile.

Assign an aWIPS Profile to the Network Device

Before you begin

If you upgrade Catalyst Center from a release earlier than Release 2.2.2.0, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe to the additional subscription. See Monitor the Rogue Management and aWIPS Dashboard.

Note For a new installation of Catalyst Center, you do not have to disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe to the additional subscription.

Step 1 From the top-left corner, click the menu icon and choose **Workflows** > **Assign an aWIPS Profile**.

The **Assign an aWIPS Profile** window appears.

To skip this window in the future, check the **Don't show this to me again** check box.

Step 2 Click **Let's Do it**.

The **Assign aWIPS Profile** window appears.

Step 3 From the **Profile Name** drop-down list, choose the aWIPS profile name that you want to assign to a device.

Step 4 In the left pane, you can either search for a site by entering its name in the **Find Hierarchy** field, or expand **Global** to choose a site.

You can also search for a network device by entering its name in the **Search Table** field.

The **Network Devices** table shows the **Device Name**, **IP Address**, **Software Version**, **Reachability**, and **Forensic Capture** of the device and lists the network devices in the following sections:

- **Reachable & Supported**: Shows the list of reachable and supported network devices with software version 17.4, and reachability status with a green check mark.
- **Not Reachable/Not Supported**: Shows the list of unreachable or unsupported network devices with software version 17.4. You cannot assign an aWIPS profile to unreachable or unsupported network devices.

Step 5 In the **Reachable & Supported** tab, check the check box next to the device that you want to assign to the selected aWIPS profile. You can either select all the devices or an individual device.

Note You can assign an aWIPS profile to a maximum of 100 devices at a time.

Step 6 Click **Next**.

Step 7 In the **Profile and devices Mapped Summary** window, expand **aWIPS Profile Details** to view the configuration summary of the selected aWIPS profile, and **Device Map** to view the configuration summary of assigned devices.

Step 8 Click **Next**.

The **Profile Assignment to Devices initiated successfully** window appears.

Note Profile assignment to the devices takes some time to complete. You must wait before retrying the assignment process.

Step 9 To view the status of the assigned aWIPS profile to the device, click the **Go to Rogue and aWIPS Home Page** link. For more information, see View an aWIPS Profile, on page 4.

Edit an aWIPS Profile

This procedure describes how to edit an aWIPS profile.

Before you begin

To subscribe the additional subscription, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS Dashboard.

Step 1 From the top-left corner, click the menu icon and choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile**.

Step 2 In the **aWIPS Profile(s)** table, click the profile name that you want to edit.

Step 3 In the **Edit aWIPS Profile** window that appears, make the necessary changes and click **Save**.

Note You cannot edit the default aWIPS profile.

The profile is saved and pushed to all the devices that are assigned to the given aWIPS profile.

Note In the **Configure Threshold** column, for the chosen aWIPS signature, if you enter a threshold value that is out of the specified range, an error message appears on the top of the **Edit aWIPs Profile** window to enter the correct value within the specified range.

Delete an aWIPS Profile

This procedure describes how to delete an aWIPS profile from Catalyst Center.

Before you begin

To subscribe the additional subscription, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS Dashboard.

Step 1 From the top-left corner, click the menu icon and choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile**.

The **aWIPS Profile** dashboard appears.

Step 2 In the **aWIPS Profile(s)** table, check the check box next to the aWIPS profile name that you want to delete.

Note
- You cannot delete a default aWIPS profile.
- You cannot delete an aWIPS profile that is assigned to a network device. In such a scenario, you must reassign the device to the default aWIPS profile and then delete it.

Step 3 From the **More Actions** drop-down list, choose **Delete**.

Step 4 In the confirmation window, click **Delete**.

Enable or Disable aWIPS or aWIPS Forensic Capture

Catalyst Center allows you to enable or disable aWIPS or aWIPS forensic capture at the site level. You can enable or disable aWIPS for all the Cisco Catalyst 9800 Wireless Controllers in a network.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Note The sites, buildings, and floors inherit the settings from the global level. The settings saved at the site, building, or floor level override the global network settings.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, hover your cursor over **Add**, and choose **AP Profile for IOS-XE**.

Step 6 Click the **Security** tab.

Step 7 To enable aWIPS, click the **aWIPS** toggle button.

By default, **aWIPS** is enabled at the global level.

Step 8 (Optional) To disable aWIPS, click the **aWIPS** toggle button.

Step 9 To enable forensic capture, click the **Forensic Capture** toggle button.

Note To enable forensic capture, aWIPS must be enabled. If you disable aWIPS when forensic capture is enabled, forensic capture will also be disabled.

Step 10 Click **Save**.

Note After you configure **aWIPS** or aWIPS Forensic Capture settings, provision or reprovision a device to push the changes to the device.

Step 11 (Optional) To reset the **aWIPS and Forensic Capture Enablement** settings, click **Reset**.

Note If you are migrating from a Catalyst Center release earlier than Release 2.3.2.0, configure the network settings with **aWIPS** or **aWIPS Forensic Capture** settings so that the configurations are updated in wireless controllers.

The **aWIPS** or **aWIPS Forensic Capture** settings belong to the AP join profiles on the devices. When a Cisco Catalyst 9800 Series Wireless Controller device is provisioned, all the AP join profiles associated with the device are fetched, and the following actions take place:

- The default AP join profile inherit the **aWIPS** or **aWIPS Forensic Capture** settings from the site to which the device is assigned.
- The custom profiles which are created using Catalyst Center as part of row AP provisioning, inherit the **aWIPS** or **aWIPS Forensic** settings from the **Country** site level for which the corresponding row AP profile is created.
- The custom profiles created using Catalyst Center as part of mesh AP provisioning, inherit the settings from the floor site level for which the corresponding Mesh AP profile is created.
- The custom AP join profiles created outside Catalyst Center do not inherit the settings.