Rogue Management and aWIPS Workflow

About aWIPS Profiles

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

The 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 You must enable wireless module on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500 Series Switches for aWIPS profiles to work (It is only applicable for SD-Access use cases).

Prerequisites

- Verify the network connectivity between the Cisco Wireless Controller and Cisco DNA Center.
- Make sure that the network device is reachable from Cisco DNA Center and has downloaded the aWIPS profile configuration from Cisco DNA Center.
- For forensic capture, make sure that there is network connectivity between APs and Cisco DNA Center.
- For forensic capture, make sure that the Google Protocol RPC (gRPC) tunnel interface has been established between APs and Cisco DNA Center. Use the **show ap icap connection** command to make sure that the status is READY.
- For forensic capture, the required ports must be opened between Cisco DNA Center and network device links.
- For forensic capture, there should not be a time lag between Cisco DNA Center and access points.
- If you have upgraded Cisco DNA Center from an earlier release, you must disable and enable **aWIPS** from the **Rogue and aWIPS** dashboard to subscribe an additional subscription. For more information, see Monitor the Rogue Management and aWIPS Dashboard.

Note For a new installation of Cisco DNA 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 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Create an aWIPS Profile**.

You can also create an aWIPS profile by navigating to this path: In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** > **Add Profile**.

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

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

The **aWIPS Profile Creation** window appears.

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 which detect the various denial of service (DoS) attacks. To know more about aWIPS signatures, see About Adaptive Wireless Intrusion Prevention System.
- **Default Threshold**: Shows the predefined threshold value for the respective aWIPS signature
- **Configure Threshold**: Shows 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.

If an aWIPS signature is not selected for an aWIPS profile, then the Cisco DNA 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 respective **Configure Threshold** field.

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

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
- Cisco DNA Center does not allow you to edit the **Default Threshold** value and **Time Interval (In Seconds)** value for aWIPS profile.
- If you enable forensic capture for an aWIPS signature, Cisco DNA Center allows you to download packets from the **Threat 360** window.
- If you disable forensic capture for an aWIPS signature, then Cisco DNA 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 Cisco DNA Center.

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

Step 9 Click **Next**.

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

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

Step 11 Click **Next** in the **Profile Summary** window.

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

The **Assign aWIPS Profile** window appears.

You can also assign aWIPS profile to a device on the **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** page 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 the 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 profile configuration URL push to the network device. The possible values of push status are **Success**, **Failure**, and **In Progress**.

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

  In case of **Failure** status, hover your mouse over the **i** icon next to the **Failure** to see the failure reason.

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

  In case of **Failure** status, hover your mouse over the **i** icon next to the **Failure** to see the failure reason.
- **Forensic Capture**: Shows whether the forensic capture is enabled/disabled on **default-ap-join** AP Join Profile on the device. Forensic capture on custom AP join profile is not yet supported.

  Hover your mouse over the i icon next to the Forensic capture, a tooltip saying **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 the **Forensic Capture**.
- **Assigned On**: Shows the date and time of aWIPS profile assigned to wireless controller.

Step 14 Click **Next**.

The **Profile Creation Done** window appears.

View aWIPS Profiles

In the Cisco DNA Center GUI, 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, an error message appears on top of the **aWIPS Profile** dashboard to subscribe the upgraded subscription even if **aWIPS** is enabled in Cisco DNA Center. To subscribe 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 Cisco DNA Center from an earlier release, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe the additional subscription. See Monitor the Rogue Management and aWIPS Dashboard.

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Assign an aWIPS Profile**.

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

To skip this screen 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 the sites.

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 devices or an individual device.

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

Step 6 In the **Forensic Capture** column, click the toggle button to enable or disable the forensic capture for the chosen network device at the device level.

This configures forensic capture at the **default-ap-profile** AP join profile. Forensic capture configuration at the custom AP join profile is not supported.

Step 7 Click **Next**.

Step 8 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 9 Click **Next**.

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

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

Step 10 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 aWIPS Profiles.

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 In the Cisco DNA Center GUI, 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**.

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 Cisco DNA 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 In the Cisco DNA Center GUI, 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 the network device. Instead, 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 warning window, click **Delete**.