



## Monitor the Rogue and aWIPS Dashboard

---

- [Access the Rogue Management and aWIPS Application, on page 1](#)
- [Monitor the Rogue Management and aWIPS Dashboard, on page 1](#)
- [Monitor Network Rogue Threats, on page 5](#)
- [Obtain Rogue AP and Rogue Client Details from Threat 360° View, on page 9](#)
- [Download aWIPS Profile Forensic Capture from Threat 360° View, on page 12](#)

## Access the Rogue Management and aWIPS Application

---

**Step 1** To access the Rogue Management and aWIPS application, log in to Cisco DNA Center.

**Step 2** From the top-left corner, click the menu icon and choose **Assurance > Rogue and aWIPS**.

The **Rogue and aWIPS** dashboard is displayed.

**Note** Before using the Cisco DNA Assurance application, you must configure it. For more information, see [Basic Setup Workflow](#).

## Monitor the Rogue Management and aWIPS Dashboard

---

Use the **Rogue and aWIPS** dashboard to get a detailed threat analysis and a global view of all the rogue APs and aWIPS signatures detected in the network. The Rogue and aWIPS dashboard also provides insight into the highest-priority threats so that you can quickly identify them. The Rogue Management application uses streaming telemetry to retrieve data on rogue APs.

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

The **Rogue and aWIPS** window is displayed. By default, Cisco DNA Center displays the **Overview** dashboard.

**Note** If a Cisco AireOS Controller does not meet the minimum software version required, a notification is displayed at the top of the dashboard. Click **Go To Devices** in the notification to upgrade to the supported version.

**Step 2** In the **Site** menu, click **Global**.

The **Site Selector** slide-in pane is displayed.

a) Enter a site name in the **Search Hierarchy** search bar or expand **Global** to choose a site.

- Note**
- If a site has more than 254 subsites, that site is disabled by default.
  - Site hierarchies that do not have floors are not listed in the site selector slide-in pane.

**Step 3** From the **Actions** drop-down list, choose **Rogue > Enable** to enable rogue subscription on the Cisco Wireless Controller and the Cisco Catalyst 9800 Series Wireless Controller.

**Step 4** Click **Yes** in the **Warning** dialog box that is displayed.

**Step 5** In the **Rogue and aWIPS Subscription** slide-in pane, do the following:

**Note** The **Configuration Preview** tab appears only when the **Configuration Preview** is enabled. For information on how to enable configuration preview or ITSM approval, see the "Enable Visibility and Control of Configurations" topic in the *Cisco DNA Center Administrator Guide*.

- a) Choose whether to enable rogue subscription **Now** or **Later**, and then click **Apply**.
- b) To preview the CLI configuration, click the **Generate Configuration Preview** radio button.
- c) In the **Task Name** field, enter a task name of your choice and click **Apply**.
- d) View the CLI or NETCONF configuration details and click **Deploy** or **Submit for Approval**.

**Note** **Submit for Approval** is displayed if **ITSM Approval** is enabled.

- e) Click the **Now** radio button, and click **Apply**.
- f) To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- g) In the confirmation window, click **Yes**.

**Step 6** Choose **Rogue > Disable** to disable the rogue actions temporarily.

**Step 7** Click **Yes** in the **Warning** dialog box that is displayed.

After the rogue management functionality is disabled, data from the wireless controller will not be pushed to Cisco DNA Center until the rogue management functionality is enabled.

**Step 8** In the **Rogue and aWIPS Subscription** slide-in pane, do the following:

- a) Choose whether to disable rogue subscription **Now** or **Later**, and then click **Apply**.
- b) To preview the CLI configuration, click the **Generate Configuration Preview** radio button.
- c) In the **Task Name** field, enter a task name of your choice and click **Apply**.
- d) View the CLI or NETCONF configuration details and click **Deploy** or **Submit for Approval**.

**Note** **Submit for Approval** is displayed in case of **ITSM Approval** is enabled.

- e) Click the **Now** radio button, and click **Apply**.
- f) To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- g) In the confirmation window, click **Yes**.

**Step 9** Choose **Rogue > Status** to view the rogue configuration job status.

**Step 10** Filter the rogue subscription status by **All**, **Failure**, **Success**, or **In Progress** by clicking the respective tabs.

The **Operation** column shows **Enable** if the rogue-detection operation is enabled successfully on the wireless controller.

The **Status** column shows **Success** if the subscription configuration changes are successfully pushed to the wireless controller.

**Step 11** Choose **aWIPS > Enable** to enable aWIPS data collection on Cisco DNA Center.

**Step 12** Click **Yes** in the **Warning** dialog box that is displayed.

**Step 13** In the **Rogue and aWIPS Subscription** slide-in pane, do the following:

**Note** The **Configuration Preview** tab appears only when the **Configuration Preview** is enabled. For information on how to enable configuration preview or ITSM approval, see the "Enable Visibility and Control of Configurations" topic in the *Cisco DNA Center Administrator Guide*.

- a) Choose whether to enable aWIPS subscription **Now** or **Later**, and then click **Apply**.
- b) To preview the CLI configuration, click the **Generate Configuration Preview** radio button.
- c) In the **Task Name** field, enter a task name of your choice and click **Apply**.
- d) View the CLI or NETCONF configuration details and click **Deploy** or **Submit for Approval**.

**Note** **Submit for Approval** is displayed if **ITSM Approval** is enabled.

- e) Click the **Now** radio button, and click **Apply**.
- f) To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- g) In the confirmation window, click **Yes**.

**Step 14** Choose **aWIPS > Disable** to disable the aWIPS actions temporarily.

Click **Yes** in the **Warning** dialog box that is displayed.

**Step 15** In the **Rogue and aWIPS Subscription** slide-in pane, do the following:

- a) Choose whether to disable aWIPS subscription **Now** or **Later**, and then click **Apply**.
- b) To preview the CLI configuration, click the **Generate Configuration Preview** radio button.
- c) In the **Task Name** field, enter a task name of your choice and click **Apply**.
- d) View the CLI or NETCONF configuration details and click **Deploy** or **Submit for Approval**.

**Note** **Submit for Approval** is displayed if **ITSM Approval** is enabled.

- e) Click the **Now** radio button, and click **Apply**.
- f) To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- g) In the confirmation window, click **Yes**.

**Step 16** Choose **aWIPS > Status** to view the aWIPS subscription status.

**Step 17** Filter the aWIPS subscription status by **All**, **Failure**, **Success**, or **In Progress** by clicking the respective tabs.

The **Operation** column shows **Enable** if the aWIPS subscription operation is enabled successfully on the wireless controller.

The **Status** column shows **Success** if the subscription configuration changes are successfully pushed to the wireless controller.

**Step 18** Use the **Threats** dashlets to display following information:

- **TOTAL ROGUE THREATS**: Displays the total number of rogue threats.

- **TOTAL AWIPS THREATS:** Displays the total number of aWIPS threats.
- **TOTAL UNIQUE ROGUE CLIENTS:** Displays the total number of unique rogue clients.
- **ROGUES CONTAINED:** Displays the total number of rogues contained.

The **Active High Threats** and **High Threats Over Time** graphs below the timeline slider display the threat details accordingly.

**Step 19** The **Active High Threats**, **Top Locations Affected**, and **High Threats Over Time** graphs display information about rogue APs detected in the last three hours by default. The graph information is based on the time interval that you choose from the **Hours** drop-down list.

- The options are **Last 3 hours**, **Last 24 hours**, and **Last 7 days**.

**Note** Choose **Custom** to select a specific time range.



**Step 20** Use the **High Threats Summary** dashlet to display the following information:

| High Threats Summary Dashlet  |   |
|-------------------------------|---|
| Item                          | Description   |
| <b>Active High Threats</b>    | Displays information about active threat levels in the form of a donut graph. You can filter the active high threats by <b>Top 10</b> or <b>All</b> threat types.<br><br>Click each colored slice of the donut graph to view detailed information about the threats. Hover your cursor over the graph to see the number of active high threats.<br><br>Click <b>All</b> to display the threat types and counts in a table format. |
| <b>Top Locations Affected</b> | Displays the top five locations affected per selected site for high threats.  |

**Step 21** Use the **High Threats Over Time** dashlet to display the following information:

| High Threats Over Time Dashlet |   |
|--------------------------------|---|
| Item                           | Description   |
| <b>Threats Over Time</b>       | Displays detailed information about high threats over time, based on the selected time period.<br><br>Click each threat type below <b>Total Active High Threat</b> . Threat information is displayed in a graph view.<br><br>High threat deviation is measured on a color value scale: <ul style="list-style-type: none"> <li>• Green color indicates threat deviation that is less than 0.</li> <li>• Orange color indicates threat deviation from 0 to 9.</li> <li>• Red color indicates threat deviation that is more than or equal to 10.</li> </ul><br>Hover your cursor over the graph to view the number of high threats that occurred at a particular time. |
| <b>View Threats</b>            | Click <b>View Threats</b> to view the threats table. A list of high threats is displayed.   |

**Step 22** Use the **Threats By Location** dashlet to view information about threats in the map view:

| Location Option   |   |
|---|---|
| Item  | Description   |
| <br><b>Map View</b>  | <p>Click this toggle button to display a map view of the locations affected by threats.</p> <p>Hover your cursor over the corresponding location in the map to view all the threat levels and counts.</p> |
| <br><b>List View</b> | <p>Click this toggle button to display a list view of the locations affected by threats.</p>  |

**Step 23** Use the **Threat Setting Summary** dashlet to view following information:

| Threat Setting Summary Dashlet |  |
|--------------------------------|--|
| Item                           | Description  |
| <b>Allowed AP List</b>         | <p>Displays information about the allowed AP count and configured threat level.</p> <p>Click <b>View Details</b> to display the <b>Allowed List</b> window to view detailed information on the <b>Allowed Access Point List</b>.</p> |
| <b>Allowed Vendor List</b>     | <p>Displays information about the allowed vendors count and configured threat level.</p> <p>Click <b>View Details</b> to display the <b>Allowed List</b> window to view information on the <b>Allowed Vendor List</b>.</p>           |
| <b>Rogue Rule</b>              | <p>Displays information about a rule, its conditions type, rule profiles associated to it, and threat level.</p> <p>Click <b>View Details</b> to display the <b>Rules</b> window to view detailed information on rogue rules.</p>    |

**Step 24** (Optional) Use the **Tips** dashlet for a direct link to workflows such as Create Allowed AP List, Create Allowed Vendor List, Create Rogue Rule, and so on.

**Step 25** (Optional) Click **View All** to view all the available workflows.


## Monitor Network Rogue Threats

**Step 1** In the **Site** menu, click **Global**.

The **Site Selector** slide-in pane is displayed.


a) Enter a site name in the **Search Hierarchy** search bar or expand **Global** to choose a site.

- Note**
- If a site has more than 254 subsites, that site is disabled by default.
  - Site hierarchies that do not have floors are not listed in the **Site Selector** slide-in pane.

**Step 2** Click the time range setting (  ) at the top-right corner to specify the time range of the data that you want displayed in the **Threats** table:

- From the drop-down menu, choose a time range: **3 hours**, **24 hours**, **7 days**, or **Custom**.  
If you choose the **Custom** time range, specify the **Start Date** and time and the **End Date** and time.
- Click **Apply**.


**Step 3** Use the **Threats** table to view detailed information about the threats in your network:

| Threats Table  |  |
|--|--|
| Item   | Description  |
| <br><b>Filter</b> | Click this icon at the top-right corner of the table to filter the data to be displayed in the table based on the following criteria: <b>ID, Threat Level, Threat MAC Address, Type, State, Connection, Detecting AP, Detecting AP Site, RSSI (dBm), SSID, Clients, Containment Status, Last Reported, and Vendor</b> .<br><br><b>RSSI, SSID, and Clients</b> are not displayed for aWIPS. |

| Threats Table |             |
|---------------|-------------|
| Item          | Description |
| Threat Table  |             |

| Threats Table |  |
|---------------|--|
| Item          | Description  |
|               | <p>Displays the following information about threats in a table format:</p> <ul style="list-style-type: none"> <li>• <b>Threat Level:</b> Displays color-coded classified threat levels. Cisco DNA Center classifies threats into these categories: <ul style="list-style-type: none"> <li>• <b>High Threat</b></li> <li>• <b>Potential Threat</b></li> <li>• <b>Informational</b></li> </ul> </li> <li>• <b>Mac Address:</b> Displays the MAC address of a rogue AP.</li> <li>• <b>Type:</b> Displays threat types.</li> <li>• <b>State:</b> Displays the state of a rogue AP or aWIPS attacks.</li> <li>• <b>Source/Target:</b> Shows whether the displayed MAC address is the source of an aWIPS attack or the target of an aWIPS attack. This column is not applicable for rogue data.</li> <li>• <b>Connection:</b> Displays whether the rogue AP is located on the wired network or wireless network. This column shows the aWIPS attacks on the wireless network.</li> <li>• <b>Detecting AP:</b> Displays the name of the AP that is currently detecting a rogue AP. If multiple APs detect a rogue, the detecting AP with the highest signal strength is displayed. This column is applicable for both rogue AP and aWIPS attacks.</li> <li>• <b>Detecting AP Site:</b> Displays the site location of the detecting AP. This column is applicable for both rogue AP and aWIPS attacks.</li> <li>• <b>RSSI (dBm):</b> Displays the RSSI value reported by the detecting AP. RSSI (dBm) is only applicable for rogue APs.</li> <li>• <b>SSID:</b> Displays the service set identifier that a rogue AP is broadcasting. SSID is only applicable for rogue APs.</li> <li>• <b>Clients:</b> Displays the number of rogue clients associated with an AP. This column is only applicable for rogue APs.</li> </ul> <p><b>Note</b>      The client count that is displayed in the <b>Threats</b> table differs from the client count displayed in the <b>Threats 360 degrees</b> window. This happens if the data that is processed in a Cisco DNA Center release earlier than 2.3.2 is migrated to Cisco DNA Center 2.3.2 or later. Cisco DNA Center 2.3.2 or later displays the correct client count for the newly processed data if the time range that is selected has the new data.</p> <ul style="list-style-type: none"> <li>• <b>Containment Status:</b> Displays the possible values (<b>Contained</b>, <b>Pending</b>, <b>Open</b>, and <b>Partial</b>) of a rogue AP. For autocontained rogue APs, the status is displayed as <b>Contained (Auto)</b>, <b>Pending (Auto)</b>, <b>Open (Auto)</b> and <b>Partial (Auto)</b>. Wireless containment status is only applicable for rogue APs.</li> <li>• <b>Last Reported:</b> Displays the date, month, year, and time at which a rogue AP or aWIPS attack was last reported.</li> </ul> |



| Threats Table   |   |
|---|---|
| Item  | Description   |
|   | <ul style="list-style-type: none"> <li>• <b>Vendor:</b> Displays the rogue AP vendor information. This column is not applicable for aWIPS attacks.</li> </ul>   |
|  | <p>Customize the data that you want displayed in the table:</p> <ol style="list-style-type: none"> <li>In the <b>Table Appearance</b> tab, set the table density and striping.</li> <li>In the <b>Edit Table Columns</b> tab, check the check boxes for the data that you want displayed.</li> <li>Click <b>Apply</b>.</li> </ol> |

## Obtain Rogue AP and Rogue Client Details from Threat 360° View

You can quickly view the precise location details of a specific rogue AP or rogue client on a floor map, in the **Threat 360°** view.

Getting these details, however, depend on the detecting AP's strongest signal strength. With the Cisco Connected Mobile Experiences (CMX) or Cisco Spaces integration, you can get the exact location of your rogue AP or rogue client.

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

**Step 2** To launch the **Threat 360°** view for a particular rogue AP or aWIPS threat, click the corresponding row in the **Threats** table.

The **Threat 360°** pane is displayed.

The upper part of the pane displays the following information:





- **MAC address of the rogue AP**
- **Threat level**
- **Threat type**
- **Status**
- **Vendor**
- **Containment**
- **Count**
- **Last reported**

The middle part of the pane shows the estimated location of a rogue AP or a threat on the floor map:

- Site details and floor number.
- Floor map shows the names of the managed APs.









**Note** Floor Map section is not displayed for global location.










**Step 3** Perform the following tasks, as required:

- Click the  icon at the right-hand corner of the floor map to see the IP address of the wireless controller that manages the APs, along with the reachability status.
- Click the  icon at the right-hand corner of the floor map to zoom in on a location. The zoom levels depend on the resolution of an image. A high-resolution image provides more zoom levels. Each zoom level comprises a different style map that is shown at different scales, with the corresponding details. Some maps are of the same style, but on a smaller or larger scale.
- Click the  icon to see a map with fewer details.
- Click the  icon to view the details of the map icons.


The following table provides descriptions of the floor map icons.

**Table 1: Map Icons and Descriptions**

| Floor Map Icon  | Description  |
|---|--------------|
| <b>Devices</b>  |              |
|  | Access Point |
|  | Sensor       |
|  | Rogue AP     |
|  | Marker       |
|  | Planned AP   |
|  | Switch       |
|  | Interferer   |
|  | Client       |


| Floor Map Icon  | Description           |
|---|-----------------------|
|    | Rogue Client          |
|    | Reporting AP          |
|    | Detecting AP          |
| <b>Average Health Score</b>   |                       |
|    | Health score: 8-10    |
|    | Health score: 4-7     |
|    | Health score: 1-3     |
|    | Health score: Unknown |
| <b>AP Status</b>  |                       |
|  | Covered by sensor     |
|  | Not covered by sensor |

**Step 4** The bottom area of the **Threat 360°** pane enables you to perform these tasks:

- Click the **Switch Port Detail** tab to get rogue-on-wire details, including **Host Mac**, **Device Name**, **Device IP**, **Interface Name**, **Last Updated**, **Port Mode**, and **Admin Status**.
  - Note**
    - The **Admin Status** column shows the interface status as either **UP** or **DOWN**.
    - The **Port Mode** column shows the interface mode as either **ACCESS** or **TRUNK**.
  - Note** Cisco switches are required for rogue-on-wire detections.
- Click the **Detections** tab to view information such as **Detecting AP**, **Detecting AP Site**, **Adhoc**, **Rogue SSID**, **RSSI (dBm)**, **Channels**, **Radio Type**, **SNR**, **State**, and **Last Updated**.
- Click the **Filter** (  ) icon at the left end of the table to narrow down the search results based on **Rogue SSID**, **RSSI**, **Radio Type**, **Security**, and **SNR**.
- Click the **Export** icon and save it to your system.
- Click the **Clients** tab to view details such as **MAC Address**, **Gateway Mac**, **Rogue AP Mac**, **IP Address**, and **Last Heard** about the clients that are associated with the rogue AP.

- Click the **Forensic Captures** tab to view details such as **Detecting AP**, **Detecting AP Site** and **Last Updated**.

**Note** The **Forensic Captures** tab is shown only for aWIPS threats.

- Click the **Filter** (  ) icon at the left end of the table to narrow down the results based on your search criteria.

---

## Download aWIPS Profile Forensic Capture from Threat 360° View

This procedure describes how to download the forensic capture of various DoS attacks from the Threat 360° view.




---

**Note** Cisco DNA Center enables or disables forensic capture only on the default AP profile. You must enable or disable forensic capture in existing deployments where you have created custom AP join profiles.

---

### Before you begin

You must verify the network connectivity between the APs and Cisco DNA Center.

- 
- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Rogue and aWIPS > Threats**.
- Step 2** In the **Threat MAC address** column, click the aWIPS attack link.  
The **Threat 360** window is displayed.
- Step 3** Click the **Forensic Capture** tab to view information such as **Detecting AP**, **Alarm ID**, **CaptureFilename**, and **Last Updated**.
- Step 4** In the **Capture Filename** column, click the **pcap** file to download the aWIPS profile forensic capture.
- Step 5** Click **Download All** to download all the **pcap** files.
- Step 6** Click the **Filter** icon to narrow down the search results based on **Detecting AP**.
- Step 7** Click the **Export** icon to save the **CSV** file to your workspace.

**Note** Cisco DNA Center shows a maximum of 50 forensic captures at a time.

---