Custom Classification of Rogue Access Points

About Allowed List Workflow

The Cisco DNA Center Rogue Management and aWIPS workflow allows you to review and mark the MAC address of rogue access points, that you want to move to the allowed list in bulk, and process bulk allowed list of selected AP MAC addresses.

Rogue Management and aWIPS workflow supports APs that are associated with Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

You can move the following rogue AP types to the allowed list using Set Up the Allowed List Workflow, on page 2:

- Rogue on Wire

- Honeypot

- Interferer

- Neighbor

You cannot move the following rogue AP types to the allowed list using :

- Beacon Wrong Channel
- Beacon DS Attack
- AP Impersonation
- Friendly

Set Up the Allowed List Workflow

This procedure shows how to move rogue AP MAC addresses to the allowed list in bulk. These addresses are the ones that you do not want to report as high threat in Cisco DNA Center.

Before you begin

To perform the following task, you must have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Set up Rogue Management and aWIPS**.

The **Set up Rogue Management and aWIPS** window appears.

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

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

The **Bulk upload allowed access points** window appears.

Step 3 In the **Search** field, search for the MAC addresses that were already added in the .

Step 4 Click **Export** to export the allowed list.

Step 5 You can download the sample CSV template file and manually add the MAC address, operation, and category to create the bulk allowed list template. Click the **Download the sample CSV template from here** link.

Hover your cursor over the notification symbol to view the format of allowed MAC addresses, operations, and categories.

Step 6 You can either drag and drop the CSV file into the boxed area or click **Choose a file** and browse to the CSV file on your system. The maximum size of the CSV file is 1.2 MB.

Note Cisco DNA Center performs a validation check. An error message appears if the uploaded CSV file does not meet the following requirements:

- The MAC address is not a valid rogue point MAC address.
- All the rogue access point MAC addresses exist in the system already, or no rogue access point MAC addresses are eligible for the delete operation.
- A green check mark indicates that the uploaded CSV file content is valid.

Step 7 Click **Next**.

Step 8   In the **Summary** window, the **Uploaded bulk allowed list MAC addresses** table displays the list of allowed MAC addresses in bulk, and the respective operation and action.

- **All**: Shows the list of all the MAC addresses in bulk, and their respective operation and action.

- **Create**: Shows the list of created MAC addresses in bulk, and their respective operation and action.

- **Delete**: Shows the list of deleted MAC addresses in bulk, and their respective operation and action.

- **No Action**: Shows the list of MAC addresses that are already deleted, and their respective operation and action.

Step 9   Click **Continue to allowed list**, and in the dialog box that is displayed, click **Yes**.

The **Done! Allowed List Updated** window appears.

Step 10   Click **Go to Rogue and aWIPS Home Page**.

The **Rogue and aWIPS** dashboard appears.

Click the **Threats** tab, that displays **Threat** table, Cisco DNA Center now categorizes the specified rogue AP MAC addresses as **Allowed List** under the **Type** column.

Step 11   To add or delete a rogue AP MAC address individually, click the rogue MAC address listed under the **Threat MAC address** column.

The **Threat 360** window appears.

Step 12   From the **Action** drop-down list and choose **Add to Allowed list**.

To remove a rogue AP MAC address from the allowed list individually, from the **Action** drop-down list, choose **Remove from Allowed list**.

About Custom Rogue Rule Creation

Rogue rules are an easy way to segregate and manage rogues with different risk profiles. Rogue rules are easy to configure and they are applied in order of priority. They reduce false positives, noise for sites with interferers, number of alerts, and provide the ability to adjust organizational risk profiles on global and site basis.

You can move the following rogue AP types to the custom classification type:

- Interferer

- Neighbor

Edit a Rogue Rule

Step 1   Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS** > **Rules**.

Step 2   In the **Rogue Rules** table, click the rule name that you want to edit.

Step 3   On the **Edit Rogue Rule** window, make any necessary changes.

Note The previous classification, based on old rules, is not modified even if the rule conditions are modified. The change affects only the new data classification.

Step 4 (Optional) Check the **Enable Auto-Containment** check box to autocontain the rogue rule.

Note
- Cisco Catalyst 9800 Series Wireless Controllers has a limit of only 625 Rogue Containment Configurations at a time. Once the limit is reached, containment won't work for any new rogue on those devices.
- You can only autocontain **Honeypot** and the custom rule with the **High** level threat.

Step 5 Click **Save**.

Verify whether the rogue containment is enabled or not in the **Auto-Containment** column.

Delete a Rogue Rule

Step 1 Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS** > **Rules**.

Step 2 In the **Rogue Rules** table, click the **Rule Name** that you want to delete and click **Delete**.

Note If you delete the only rogue rule in a rule profile, the rule profile is also deleted.

Step 3 In the confirmation dialog box, click **Delete**.

Note **Honeypot** is a predefined rule; you cannot delete it.

Step 4 (Optional) To view the deleted rules, click the **Inactive** tab in the **Rogue Rules** table.

Create a Custom Rogue Rule

You can create a rule with specific conditions and then associate the rule to a rule profile.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Create a Rogue Rule**.

Step 2 In the **Create a Rogue Rule** window, click **Get Started**.

Step 3 In the **Rule Name** field, enter a unique name for the rule.

While creating new rogue rules, you cannot enter the rogue rule names that were deleted earlier.

Step 4 In the **Description** field, enter a description for the rule.

Step 5 Click **Next**.

Step 6 In the **Create Rogue Rule** window, choose one of the following threat level options: **High**, **Potential**, and **Informational**.

Step 7 (Optional) Check the **Enable Auto-Containment** check box to autocontain the rogue rule.

Note	• Cisco Catalyst 9800 Series Wireless Controllers has a limit of only 625 Rogue Containment Configurations at a time. Once the limit is reached, containment won't work for any new rogue on those devices.
	• Autocontainment is only applicable to rogue rules classified with the **High** threat level. By default, **Enable Auto-containment** is disabled for the **Potential** and **Informational** threat levels.

Step 8 From the **Match** drop-down list, choose either **All** to match all the conditions or **Any** to match your choice of conditions.

Step 9 From the **Add Condition** drop-down list, choose the rule conditions.

You can add multiple conditions to a rule. The available rule conditions are: **SSID**, **RSSI**, **Encryption Condition**, and **Minimum Rogue Client Count**.

Step 10 Click **Next**.

Step 11 (Optional) To assign this rule to an existing rule profile, click **Yes** in the **Do you want to assign this rule to a rule profile?** dialog box.

Creating only rogue rules will not work as an entity. Rogue rules must be assigned to a rule profile.

Step 12 In the **Available rule profiles** table, check the check box next to the profile name, and click **Next**.

You can select one or more rule profiles.

Note	You cannot assign more than five rules to a rule profile.

Step 13 In the confirmation dialog box, click **Proceed**.

The new rule is set to the lowest priority. You can edit the rule profile to change the priority.

Note	After the rogue rule is created, you cannot use the same rogue rule name to create another rogue rule.

Step 14 Review the rogue rule configuration in the **Summary** window.

Note	Previous classification based on old rules is not modified even if the new rule conditions match. The change affects only the new data classification.

Step 15 (Optional) To create another rogue rule, click the **Create Another Rogue Rule** button and repeat Step 3 through Step 13 in this procedure.

Step 16 (Optional) To view the created rogue rules, click the **View all Rogue Rules and Profiles** button.

The **Rogue Rules** tab lists all the rogue rules created.

You can also view the created rogue rules by clicking the menu icon (≡) and choosing **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rules**.

About Rogue Rule Profile

You can create a rogue rule with specific conditions and then associate it to a rule profile. You can prioritize rogue rules after associating them to a rogue rule profile.

When a rogue rule profile is assigned to a site, the rogues reporting from the site are verified against the rules in the rule profile.

Note that you can assign only one rogue rule profile to a site.

Because of site inheritance, all the floors under a particular site inherit the rogue rule profile that is mapped at the area, site, or building level. For example, as shown in the following figure, **Floor1** and **Floor2** will inherit the rogue rule profile that is mapped at the **SanJose** level.

A rogue rule profile mapped to a floor has precedence over a rogue rule inherited from a parent site. For example, as shown in the following figure, Rogue Rule Profile A is directly mapped to **Floor1**, Rogue Rule Profile A takes precedence over Rule Profile B that is assigned to the parent site, **SJC2.**

Figure 1: Network Hierarchy
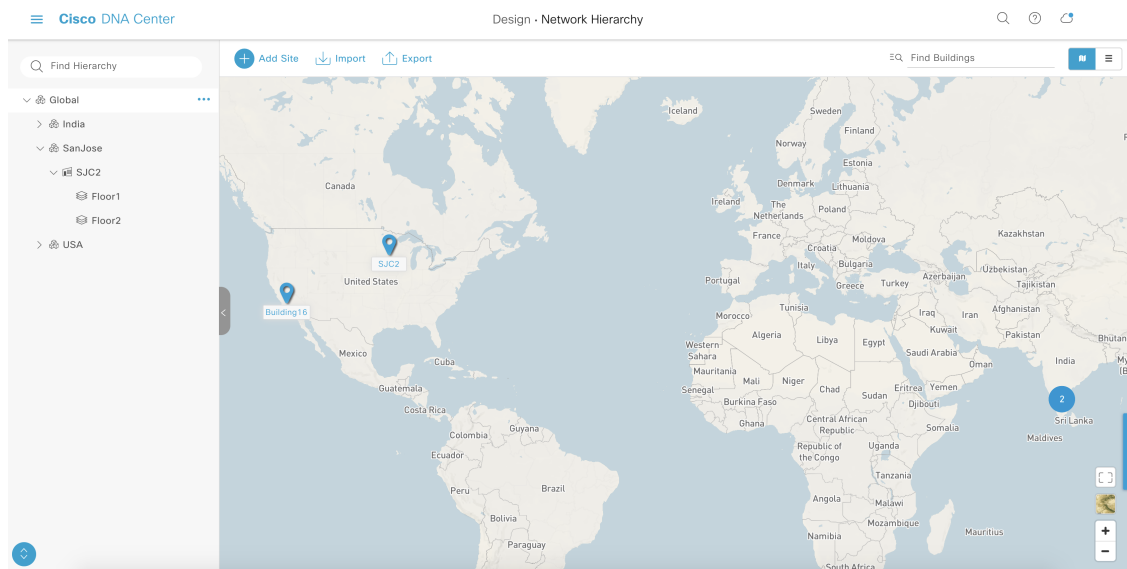
Edit a Rogue Rule Profile

Step 1 Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS** > **Rules**.

Step 2 Click the **Rogue Rule Profiles** tab.

Step 3 In the **Rogue Rule Profiles** table, click the profile name that you want to edit.

Step 4 In the **Edit Rule Profile** window, make the necessary changes.

Note Edited rule profiles do not modify any previously classified data. The edits only apply to new modified data that is processed after changes are made.

Step 5 (Optional) Check the **Enable Auto-Containment** check box to autocontain the rogue rule.

Note
- Cisco Catalyst 9800 Series Wireless Controllers has a limit of only 625 Rogue Containment Configurations at a time. Once the limit is reached, containment won't work for any new rogue on those devices.

- **Honeypot** is a predefined rule, that is added to all newly created rogue rule profiles by default.

Step 6	In the confirmation window click **Yes**.
Step 7	(Optional) You can toggle between **User Defined** and **Predefined** to view the corresponding rules.
Step 8	Verify whether the rogue containment is enabled or not in the **Auto-containment** column.
Step 9	Click **Save**.

Delete a Rogue Rule Profile

Step 1	Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS** > **Rules**.
Step 2	Click the **Rogue Rule Profiles** tab.
Step 3	In the **Rogue Rules** table, click the profile name that you want to delete and click **Delete**.
Step 4	In the confirmation dialog box, click **Delete**.

Create a Rogue Rule Profile

> You can create a rule with specific conditions and then associate it to a rogue rule profile.

Step 1	Click the menu icon (≡) and choose **Workflows** > **Create a Rogue Rule Profile**.
Step 2	In the **Create Rogue Rule Profile** window, click **Get Started**.
Step 3	In the **Profile Name** field, enter a unique name for the rule profile.
Step 4	(Optional) Check the **Enable Auto-Containment** check box to autocontain the rogue rule.

| **Note** | • **Cisco Catalyst 9800 Series Wireless Controllers has a limit of only 625 Rogue Containment Configurations at a time. Once the limit is reached, containment won't work for any new rogue on those devices.** |
| | • You can only autocontain **Honeypot** and the custom rules classified with the **High** threat level. |

Step 5	In the confirmation window, click **Yes**.
Step 6	Click **Next**.
Step 7	In the **Rule List** table, check the check box next to the rule name, and click **Next**.
	You can add up to five rogue rules in a profile.
Step 8	In the **Sort rules in order of priority** window, drag and drop a rule into the desired priority with the highest priority on top to reorder rules based on your priority.
Step 9	Click **Next** to associate a rogue rule profile to a location.
Step 10	Check the check box next to a site to associate this rule profile to that site, and click **Next**.
	Rule profiles can exist without being assigned to any site. Rules are not checked unless the rule profile is assigned to a site.

Note	If a vendor rule and rule profile are mapped to the same site, the vendor rule takes precedence.

Step 11 In the **Summary** window, review the rogue rule profile configuration.

Step 12 Click the **Back** button to make any changes to the values entered in the previous windows.

Step 13 Click **Create Rule Profile**.

A message is displayed, stating that the rule profile is created successfully.

Step 14 (Optional) To view all the rogue rules and profiles, click **View all Rogue Rules and Profiles**.

The **Rogue Rule Profiles** tab lists all the created rogue rules and rule profiles.

You can also view the created rule profiles by clicking the menu icon (≡) and choosing **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rule Profiles**.

View the Allowed Access Points List

Step 1 Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS**.

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

Step 2 In the **Allowed List** tab, click the **Allowed Access Points List**.

The **Allowed Access Points List** table shows the **MAC Address** and **Last Changed** details of all the allowed access points.

Step 3 Click the search or filter icon to find a particular access point in allowed list.

Step 4 Click **Add Access Point List** to add a rogue AP MAC address to the allowed list. For more information, see Set Up the Allowed List Workflow, on page 2.

Step 5 Click **Export** to export the allowed access points list to a CSV file.

Step 6 Select an access point and click **Delete** to remove the access point from the allowed list.

About Allowed Vendor List

With the allowed vendor list feature, you can define whether APs from specific vendors will trigger a specific threat level. You can create a list of allowed vendors, so that threats from these vendors are not marked as High threats. You can decide whether they need to be marked as Potential or Informational threats. In a given workflow, you can add up to five vendors to the allowed list.

An allowed vendor rule that is mapped at any level takes precedence over the inherited rule. For example, if allowed vendor rule A is mapped to a floor level, vendor rule A takes precedence over allowed vendor rule B that is present at the site, area, or building level.

View Vendor Rule List Information

Step 1   Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS**.

Step 2   Click the **Allowed List** tab.
The **Allowed Vendor List** table shows the list of allowed vendors with the following details. Each vendor rule is displayed as an entity:

- **Vendor Name**

- **Match Criteria**

- **Threat Level**

- **Associated Site(s)**

- **Last Changed**

Edit a Vendor Rule

Step 1   Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS**.

Step 2   Click the **Allowed List** tab.

Step 3   In the **Allowed Vendor List** table, click the vendor name that you want to edit.

Step 4   In the **Edit Allowed Vendor List** window, edit the following parameters, as necessary:

- **Threat Level**

- **Match Criteria**

- **Vendor Name**

- **Associated Sites**

Step 5   Click **Save**.

Delete a Vendor Rule

Step 1   Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS**.

Step 2   Click the **Allowed List** tab.

Step 3   In the **Allowed Vendor List** table, check the check box of the vendor name that you want to delete, and click **Delete**.

The following message `Deleting the selected allowed vendor(s) will impact all sites associated with it. There is 1 site associated with this allowed vendor(s).`

Step 4 Click **Delete**.

Create a List of Allowed Vendors

You can create a list of vendors to be on the allowed list, so that threats from these vendors are not marked as High threats.

You can add five vendors in a single workflow for a set of sites.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Create Allowed Vendor List**.

You can also create a list of allowed vendors by clicking the menu icon and choosing **Assurance** > **Rogue and aWIPS** > **Allowed List**.

Step 2 In the **Create Allowed Vendor List** window, click **Let's Do it**.

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

The **Create Allowed Vendor List** window appears.

Step 3 From the **Selection Criteria** drop-down list, choose a selection criteria (**Exactly Matches** or **Contains**) for the vendor name.

Step 4 In the **Vendor Name** field, enter the vendor name.

The vendor name match is case-sensitive.

Step 5 Click ⊕ to add another vendor to the allowed list.

In a given workflow, you can add a maximum of five vendors to the allowed list.

Step 6 In the **Site Selection** window, check the check box next to the site to which you want to apply your allowed vendor list.

Because of site inheritance, all the floors under a particular site inherit the vendor rule that is mapped to the area, site, or building level.

Step 7 Click **Next**.

Step 8 In the **Summary** window, view the details about the allowed vendor and site selection.

Step 9 Click **Done**.

The **Allowed Vendor List Created** window appears.

Step 10 To create another allowed vendor list, click **Create New Allowed Vendor List** and repeat Step 3 to Step 8.

Step 11 To view the created vendor lists, click **View all allowed Lists**.