Custom Classification of Rogue APs

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 a bulk, and process bulk allowed list of selected Access Point 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 this workflow:

- Rogue on Wire
- Honeypot
- Interferer
- Neighbor

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

- 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 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 In the Cisco DNA Center GUI, 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 screen 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, you can search for the MAC addresses that were already added in the previous workflow.

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

Step 4 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.

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

Step 5 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 6 Click **Next**.

Step 7 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 8 Click **Continue to allowed list**, and in the warning pop-up window, click **Yes**.

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

Step 9 Click the **Go to Rogue and aWIPS Home Page** link.

The **Rogue and aWIPS** dashboard appears.

In the **Threat** table, Cisco DNA Center now categorizes the specified rogue AP MAC addresses as **Allowed List** under the **Type** column.

Step 10 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 11 Click the **Action** drop-down list and choose **Add to Allowed list**.

To remove the rogue AP MAC address from the allowed list individually, in 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

Create a Custom Rogue Rule

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Create a Rogue Rule**.

Step 2 In the **Create a Rogue Rule** screen, 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 those rogue rule names that were deleted before.

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

Step 5 Click **Next**.

Step 6 In the **Create Rogue Rule** screen, choose the threat level and add conditions for your rule.

Step 7 Select one of the **Threat Level** radio buttons to add a threat level to the rule. The available threat levels are: **High**, **Potential**, or **Informational**.

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

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

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

Step 10 Click **Next**.

Step 11 To assign this rule to an existing rule profile, click **Yes** in the **Do you want to assign this rule to a rule profile?** screen.

Creating only rogue rules will not work as an entity. Rogue rules should always 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. You cannot assign more than five rules to a rule profile.

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

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

Note Once 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** page.

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 To create another rogue rule, click the **Create Another Rogue Rule** button and follow Step 3 through Step 13 in this procedure.

Step 16 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 navigating to this path: In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rules**.

Edit a Rogue Rule

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** tab.

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

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

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

Delete a Rogue Rule

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** tab.

By default, the **Rogue Rules** tab is opened.

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

Note If the rogue rule which you are deleting is the only rule available in a rule profile, then the rule profile is also deleted.

Step 3 Click **Delete** in the confirmation dialog box that appears.

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

About Rogue Rule Profile

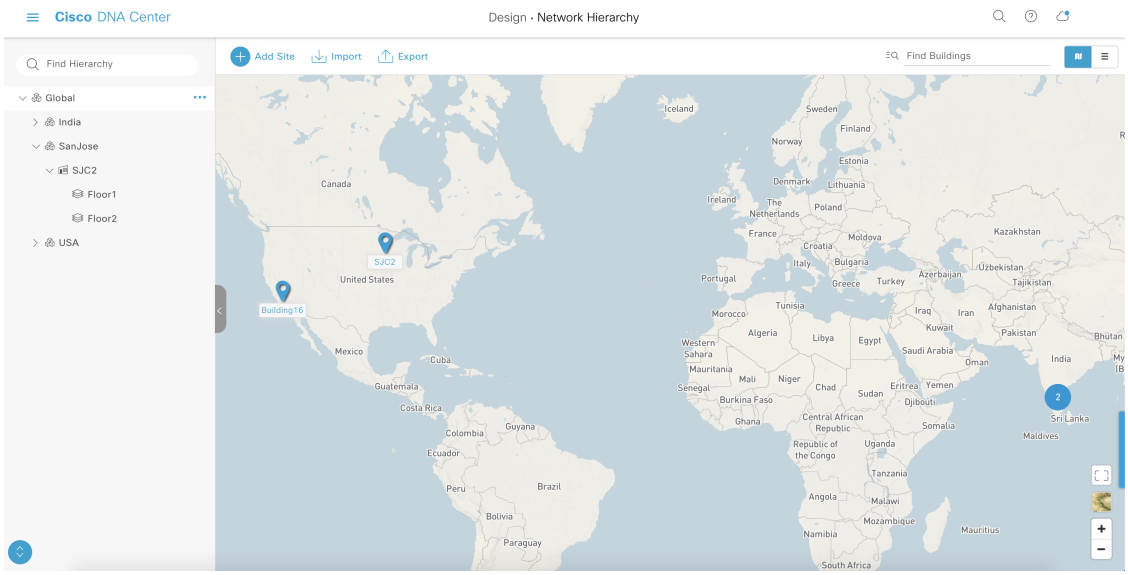
You can create a rogue rule with specific conditions and then associate it to a rule profile. You can prioritize rogue rules after associating them to a rogue rule profile.

When a rogue rule profile is assigned to a site, the rogues which are being reported from that site will be verified against the rules which are defined in the rule profile.

You can assign only one rogue rule profile to a site.

Because of the site inheritance, all 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 below image, Floor1 and Floor2 will inherit the rogue rule profile which is mapped at the SanJose level.

A rogue rule profile mapped to a floor gets precedence over a rogue rule inherited from a parent site. For example as shown in the below image, if the Rogue Rule Profile A is directly mapped to Floor1, then the Rogue Rule Profile A takes precedence over the Rule Profile B which is assigned to the parent site which is SJC2.



Create a Rogue Rule Profile

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Create a Rogue Rule Profile**.

Step 2 In the **Create Rogue Rule Profile** screen, click **Get Started**.

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

Step 4 Click **Next**.

Step 5 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 6 In the **Sort rules in order of priority** screen, drag and drop a rule into the desired priority with the highest priority on top to reorder rules based on your priority.

Step 7 Click **Next** to associate a rogue rule profile to a desired location.

Step 8 Check the check box next to the site to associate this rule profile, and click **Next**.

Rule profile 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 a same site, then the vendor rule takes precedence.

Step 9 Review the rogue rule profile configuration in the **Summary** screen.

Step 10 In the **Summary** screen, click the **Back** button to make any changes to the values entered in the previous screens.

Step 11 Click **Create Rule Profile**.

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

Step 12 To view all rogues and profiles, click the **View all Rogue Rules and Profiles** button.

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

You can also view the created rule profiles by navigating to this path: In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rule Profiles**.

Edit a Rogue Rule Profile

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** tab.

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 that appears, make the necessary changes and click **Save**.

Edited rule profiles will not modify any previously classified data. It is applied only on the new data which is processed after changes are made.

Delete a Rogue Rule Profile

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** tab.

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 Click **Delete** in the confirmation dialog box that appears.

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 upto five vendors to the allowed list.

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

Create a List of Allowed Vendors

Use this procedure to 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 In the Cisco DNA Center GUI, 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 choose **Assurance** > **Rogue and aWIPS** > **Allowed List** tab.

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

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

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

Step 3 Select a threat level to apply when the Vendor name with threat matches with the Vendor rule name from the **Threat Level** radio button.

The available threat levels are: **Potential** or **Informational**.

Step 4 From the **Selection Criteria** drop-down list, choose a selection criteria for the vendor name. The available selection criterias are: **Exactly Matches** or **Contains**.

Step 5 In the **Vendor Name** field, enter the vendor name.

The Vendor Name match is case-sensitive.

Step 6 Click to add more vendor to the allowed.

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

Step 7 In the **Site Selection** screen, check the check box next to the site where you want to apply your allowed vendor list.

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

Step 8 Click **Next**.

Step 9 In the **Summary** page, you can view details about the allowed vendor and site selection details.

Step 10 Click **Done**.

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

Step 11 To create another allowed vendor list, click the **Create New Allowed Vendor List**button and follow Step 3 through Step 8 in this procedure.

Step 12 To view the created vendor list, click **View all allowed Lists**.

View Vendor Rule List Information

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.**Allowed List** tab.

Step 2 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

This procedure shows how to edit a vendor list.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.**Allowed List** tab.

Step 2 In the **Allowed Vendor List** table, click the Vendor Name that you want to edit.

Step 3 In the **Edit Allowed Vendor List** window that appears which allows you to edit the following parameters:

- Threat Level
- Match Criteria
- Vendor Name
- Associated Sites

Step 4 After making the necessary changes, click **Save**.

Delete a Vendor Rule

This procedure shows how to delete a vendor.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.**Allowed List** tab.

Step 2 In the **Allowed Vendor List** table, check the check box of the **Vendor Name** which you want to delete, and click **Delete**.

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

Step 3 Click **Delete**.

A message saying `Selected Allowed vendor(s) deleted successfully` is displayed.