Cisco AI Endpoint Analytics

Introduction to Cisco AI Endpoint Analytics

Visibility is the first step towards securing an endpoint. Cisco AI Endpoint Analytics is an endpoint visibility solution that helps you identify and profile endpoints and Internet of Things (IoT) devices. The Cisco AI Endpoint Analytics engine enables you to assign labels to endpoints, using the telemetry information received from the network from various sources.

You can assign profile labels to endpoints based on factors like the endpoint type, hardware model, manufacturer, operating system type, and so on. This is called multifactor classification.

Cisco AI Endpoint Analytics helps you gather endpoint telemetry from different sources. The primary source is the Network-Based Application Recognition (NBAR) mechanism. The NBAR mechanism is embedded in Cisco Catalyst 9000 Series switches (access devices) and performs deep packet inspection (DPI).

You can gather endpoint context information from various sources such as Cisco ISE, self-registration portals, and configuration management database (CMDB) software such as ServiceNow.

You can aggregate varied endpoint information and use the data to profile endpoints in Cisco AI Endpoint Analytics. After endpoints are profiled, AI and machine learning algorithms can also be used to reduce the number of unknown endpoints by intuitively leveraging different methods.

Key Features of Cisco AI Endpoint Analytics

- **Cisco AI Endpoint Analytics dashboard**

The Cisco AI Endpoint Analytics dashboard gives you a comprehensive view of the endpoints that are connected to your network. You can view the number of known, unknown, profiled, and unprofiled endpoints. You can also view intelligent profiling suggestions that are provided to enhance endpoint profiling and management.

- **Reduce net unknowns with machine learning capabilities**

  Cisco AI Endpoint Analytics provides profiling suggestions based on learnings from endpoint groupings. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.

- **Manage endpoints with system and custom profiling rules**

  Use Cisco-provided system rules and custom rules of your design to reliably profile and manage the endpoints connected to your network.

- **Registration of endpoints through Cisco AI Endpoint Analytics**

  You can onboard and profile endpoints using Cisco AI Endpoint Analytics. The endpoint attribute data that is collected through this registration process is used to profile the endpoints.

- **Registration of endpoints using external sources**

  You can connect some external sources of endpoint data, such as Configuration Management Databases (CMDB), to Cisco AI Endpoint Analytics. This allows you to easily register, manage, and profile endpoints in your network.

Set Up Cisco AI Endpoint Analytics in Cisco DNA Center

Set Up Cisco AI Endpoint Analytics

Software Updates

Download and install the following software packages:
- Cisco AI Endpoint Analytics
- AI Network Analytics (Optional)
- Application Visibility Service

Join and Configure Data Sources

Join and configure the following data sources:
- Cisco Identity Services Engine
- Cisco Catalyst 9000 Series Access Devices for wired endpoints visibility
- (Optional) Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) for wired and wireless endpoints visibility, and for third-party network devices visibility
- (Optional) Cisco Catalyst 9800 Series Wireless Controllers for wireless endpoints visibility
- (Optional) CMDB

Install Software Updates

Install software updates in Cisco DNA Center to use Cisco AI Endpoint Analytics, as described in the following procedure.

Step 1   Log in to Cisco DNA Center.

Step 2   In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Software Updates**.

Step 3   In the **Updates** tab displayed, check if **Cisco AI Endpoint Analytics**, **AI Network Analytics**, and **Application Visibility Service** are listed in the **Application Updates** section. If any of these application updates are visible, click the **Install All** button.

- Install the **Cisco AI Endpoint Analytics** update to access the endpoint profiling solution in your Cisco DNA Center.

- Install the **AI Network Analytics** update to use machine learning and AI capabilities to receive intelligent profiling suggestions.

- Install the **Application Visibility Service** update to use NBAR and Controller-Based Application Recognition (CBAR) techniques to inform endpoint profiling.

Step 4   If any of these updates are not listed in the **Updates** tab, click **Installed Apps** tab to check if the updates are already installed and are available for use. The **Installed Apps** tab also confirms if the software installation has been successful.

Connect and Enable Data Sources

Note   The data sources that Cisco AI Endpoint Analytics uses may already be connected to your Cisco DNA Center. If the data sources are connected, see the following instructions to ensure that the data sources are available for use by Cisco AI Endpoint Analytics.

You must add Cisco ISE or Catalyst 9000 Series access devices to Cisco DNA Center for Cisco AI Endpoint Analytics to provide results.

1. **Connect Cisco ISE to Cisco DNA Center.**

   See the "Integrate Cisco ISE with Cisco DNA Center" section in "Complete First-Time Setup" in the *Cisco DNA Center Appliance Installation Guide*.

   The following Cisco ISE releases support Cisco AI Endpoint Analytics:

   - 2.4 Patch 11 and later

   - 2.6 Patch 5 and later

   - 2.7 Patch 1 and later

   - 3.0

   In your Cisco ISE administration portal:

   a.   Choose **Work Centers** > **Profiler** > **Settings**.

b. Check the **Enable Probe Data Publisher** check box.

After Cisco ISE authenticates endpoints through 802.1X or MAB authentication methods, the endpoint attributes collected are made available to Cisco AI Endpoint Analytics. The information is communicated through the probe data publisher.

2. **Connect Cisco 9000 Series access devices to Cisco DNA Center for wired endpoints visibility.**

See "Discover Your Network" in the *Cisco DNA Center User Guide*.

To enable Cisco AI Endpoint Analytics, upgrade your Cisco 9000 Series access devices to Cisco IOS-XE Release 17.3.1 or later.

To enable CBAR for the required access devices, click the **Menu** icon (≡) in Cisco DNA Center:

a. Choose **Provision** > **Services** > **All Services** > **Application Visibility**.

b. Select the Cisco Catalyst 9000 access device that you need data from. Check the check box next to the device name in the **Site Devices** section.

c. Click **Enable CBAR**.

3. **(Optional) Connect Cisco Catalyst 9800 Series Wireless Controllers to Cisco DNA Center for wireless endpoints visibility.**

The following Cisco Catalyst 9800 Series Wireless Controller models are supported by Cisco AI Endpoint Analytics, in nonfabric mode:

- 9800-CL

- 9800-40

- 9800-80

- 9800-L

To configure and provision a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, see Cisco Catalyst 9800 Series Wireless Controller Overview.

4. **(Optional) Connect Cisco DNA Traffic Telemetry Appliances to Cisco DNA Center for wired and wireless endpoints visibility, and for third-party network device visibility.**

Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) generate telemetry from mirrored network traffic for endpoint analytics. This appliance enables Network-Based Application Recognition (NBAR)-based protocol inspection and endpoint attribute extraction.

To receive endpoint attributes collected through the telemetry appliance in Cisco AI Endpoint Analytics, you must integrate Cisco ISE with Cisco DNA Center.

See Cisco DNA Traffic Telemetry Appliances for information on installing the appliances, connectivity configurations, and managing the appliances in Cisco DNA Center.

Enable CBAR on Switched Port Analyzer (SPAN)-receiving ports of access switches connected to Cisco DNA Traffic Telemetry Appliances with the following command:

```
ip nbar protocol-discovery
```

Not all endpoints that are connected to the telemetry appliances are visible in Cisco AI Endpoint Analytics. Only endpoints that are also connected to Network Access Devices (NADs) which are managed in Cisco DNA Assurance, are visible in Cisco AI Endpoint Analytics.

5. **(Optional) Enable ServiceNow in Cisco DNA Center.**

   After connecting ServiceNow to Cisco DNA Center, click the **Menu** icon (☰) in Cisco DNA Center and choose **Platform** > **Manage** > **Bundles**.

   If the **Status** of the bundle **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is **New**, click **Enable** for the bundle.

6. **(Optional) Enable AI Endpoint Analytics in Cisco DNA Center.**

   To receive suggestions about AI-based endpoint groupings, automated custom profiling rules, and endpoint labels, you must enable **Cisco AI Analytics**.

   You must install the software AI Network Analytics to receive these AI-based suggestions.

   a. From the main menu of Cisco DNA Center, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**.

   b. Click the **AI Endpoint Analytics** toggle button to set it to green.

Endpoint Telemetry Sources

Cisco AI Endpoint Analytics receives telemetry data in the following ways.

- **Deep Packet Inspection**

  Deep packet inspection is an advanced method of packet analysis that is carried out by Cisco Catalyst 9000 Series access devices. These access devices run NBAR, which inspects application traffic and performs protocol analysis to discover, identify, and profile endpoints with high fidelity.

  Deep packet inspection profiling is based on various attributes that are collected from endpoint traffic to the network. These attributes are collected across multiple protocols, from packet header layers 4 to 7.

- **Configuration Management Database Connection**

  Cisco AI Endpoint Analytics receives endpoint data from your Configuration Management Database Connection (CMDB) for greater accuracy in endpoint profiling. The connection with ServiceNow enables you to receive information from the CMDB to Cisco AI Endpoint Analytics.

- **Machine Learning Capabilities**

  Data collected for profiling is anonymized and sent to a Cisco cloud location that serves as a device data lake. Here, machine learning algorithms analyze the data available to create profiling rules that you can evaluate and apply, as needed. Smart profiling rules are suggested through Cisco AI Endpoint Analytics to help make endpoint profiling and management simpler and more efficient for you. Existing rules too are evaluated and improvement suggestions provided based on this continuous learning.

Cisco AI Endpoint Analytics Overview Window

Choose **Policy** > **AI Endpoint Analytics** from the Cisco DNA Center main menu.

The **Overview** window displays the following dashlets:

- **Total Endpoints**

This dashlet displays the total number of endpoints in your network in two groups, **Fully Profiled** and **Missing Profiles**. Cisco AI Endpoint Analytics profiles endpoints on the basis of four factors, Endpoint Type, OS Type, Hardware Model, and Hardware Manufacturer. If one or more of these factors are missing for an endpoint, it is profiled in the **Missing Profiles** group.

- **AI Proposals**

Cisco AI Endpoint Analytics uses smart grouping algorithms to group unknown endpoints in your network that have similar profiling data. If you have enabled AI Endpoint Analytics, you will receive the following types of rule proposals. These rule proposals are based on learnings from endpoint clusters:

  - New rules for profiling endpoints that may be similar.

  - Modification proposals for previously accepted rules.

  - Review of profiling rules that are no longer needed.

For more details, see .

- **Endpoints Missing Profile Label**

This dashlet displays the number of endpoints in your network with missing profiles, categorized by profile label type. There is some overlap in these displays. For example, if an endpoint does not have information for both OS Type and Hardware Model, the endpoint will be included in the count of both labels.

To check the endpoints with a specific missing profile label, click the label in this dashlet. The **Endpoint Inventory** window displays a list of endpoints. This list is filtered to display the endpoints for which the selected profile label is unknown.

Endpoint Inventory

The endpoints that are connected to Cisco AI Endpoint Analytics through the data sources, in the **Endpoint Inventory** window. The window displays a table with the connected endpoints and their profiling information.

The window displays profiling information such as **Endpoint Type**, **OS Type**, **Location**, **LLDP System Description**, and so on.

To select the profiling information you want to view for the endpoints, click the vertical ellipsis icon at the top-right corner of the table. Choose one of the following sets of profiling information and click **Apply**:

- **All**: All the profiling information that are available is displayed. You cannot edit this set.

- **General**: This is a selection of profiling information that gives you a generic view of the endpoints. This is the set of columns displayed by default. You cannot edit this set.

- **Detailed**: This is a selection of profiling information that provides a deeper view of the endpoints. You cannot edit this set.

- **Custom**: This is the only set that you can edit. Check or uncheck the profiling information you want to view in the **Endpoint Inventory** window.

You can easily filter a set of endpoints based on your requirement. You can register endpoints, and edit, delete, and profile registered endpoints. To see the complete profiling details of an endpoint, click the **MAC Address** of the endpoint. The dialog box displayed contains user details, endpoint details, and attribute details of the

endpoint. In the **Endpoint Details** section, the following new fields are displayed in Cisco DNA Center Release 2.2.2 with the details received from Cisco ISE:

- **Authentication Status**: This field displays **Started** when an endpoint is authenticated through Cisco ISE, and **Disconnected** when it is not.

- **Authorization Profile**: The authorization policies configured for an endpoint in Cisco ISE are displayed here.

- **Scalable Group Tag**: The Scalable Group Tags configured for an endpoint in Cisco ISE are displayed here.

For information on these attributes, see the Cisco ISE Administrator Guide for the Cisco ISE release that you use.

You can select single or multiple endpoints by checking the check box adjacent to the MAC addresses to filter or perform the corresponding action.

To export a list of endpoints and their details from this window, click **Export**. If you apply any filters in the **Endpoint Inventory** window, only the filtered endpoints will be processed for export. To export the details of all the endpoints, ensure that no filters are applied when you click **Export.**

When you click **Export**, a new tab opens with the **Reports** window. The **Generated Reports** window contains a list of exports initiated, with the latest export request at the top of the list. A report generated from the Endpoint Inventory window contains **AI Endpoint Analytics** in its **Template Category** column. Report generation takes a few minutes. When a report is ready for download, the value in the **Last Run** column changes from **Not Initiated** to a timestamp with a download icon next to it. The timestamp refers to the time at which the export list was generated. Click the download icon to download a CSV file of the list of endpoints to your system.

You can also export Cisco AI Endpoint Analytics data from the **Reports** window, through the following steps:

> **Note** You must run your first export of AI Endpoint Analytics data for endpoints from the **Endpoint Inventory** window. Then you can generate AI Endpoint Analytics reports directly from the **Reports** window.

1. Choose **Reports** from the main menu.

2. Click **Report Templates**, and choose **AI Endpoint Analytics** from the menu.

3. Click **Let's Do It** in the **Generate a New Report** dialog box.

4. In the **Select Report Template** window, the template **Endpoint Profiling** is applied by default. Click **Next**.

5. In the **Setup Report Scope** window, enter a value in the **Report Name** field. Define the filters that you want to apply to the list of endpoints to be exported from the **Endpoint Inventory** window. To export the details of all endpoints, do not choose any values in the **Scope** area. Click **Next**.

6. In the **Select File Type** window, the **Client Details** area allows you to review the chosen parameters. Edit the information to be exported by checking or unchecking the check boxes next to the relevant fields. Click **Next**.

7. In the **Schedule Report** window, click the radio button for **Run Now**, **Run Later (One-Time**, or **Run Recurring**. The **Run Later (One-Time** and **Run Recurring** options display scheduling fields to define the time of export. Click **Next**.

8. In the **Delivery and Notification** window, do not check the **Email Report** check box. Click **Next**.

9. In the **Summary** window, review all the configurations chosen in this workflow. To edit any configurations click the corresponding **Edit** option. Click **Next**.

10. The final window of the workflow informs you that your report is being generated. Click the **View Reports** link in this window for a list of generated reports. It takes a few minutes for the report to be generated and displayed in this window.

Filter Endpoints

Using the filter option, you can view and action upon a set of endpoints. These endpoints can you be filtered based their profiling data, primary profiling labels, known profiles, and health status.

In order to filter the endpoints, follow the below steps:

1. In the **Endpoint Inventory** window, click **Filter**.

2. Choose a value from each of the following drop-down list:

   • **Mac Address**

   • **Endpoint Type**

   • **Hardware Model**

   • **Hardware Manufacturer**

   • **OS Type**

   • **Registration status**

3. Click **Apply**.

You can also filter the profiled endpoints displayed by the four primary profiling labels. Click one or more of the labels in the **View Known Profiles** section.

The health status of endpoints is updated every five minutes.

Attribute Glossary

Attribute glossary is a list of all the profiling attributes available from Cisco ISE probe data.

In order to view all the profiling attributes, follow these steps:

1. In the **Endpoint Inventory** window, click the MAC address of an endpoint.

2. In the new area that is displayed on the right side, click **View Attribute Glossary**.

The **Attribute Glossary** window displays the following information for each attribute:

   • **Key profiling attributes**

   • **Description**

   • **Associated Profile Labels**

- **Source**

- **Dictionary**

- **Discovery Method**

The glossary gives you a detailed view of all the profiling attributes. If a profiling attribute is frequently used to create a profile label, the label is listed in the **Associated Profile Labels** column.

You can also view the attribute glossary in the **Choose Attribute Condition** window while creating a logical condition for the rules. For more information, see Create a Custom Rule.

Register Endpoints

You can onboard and profile new endpoints by registering them in Cisco AI Endpoint Analytics. The profiling information of an endpoint is the source of truth for classification. You can also update new profile information for a registered endpoint using the **Register Endpoint** option.

Step 1 Choose **Actions** > **Register Endpoints**.

Step 2 Choose whether you want to register a single endpoint or multiple endpoints, by clicking the **Single** or **Bulk** radio button.

Option	Steps
Single	Enter the **MAC Address**, **Endpoint Type**, **Hardware Model** and **Hardware Manufacturer** for the endpoint.
Bulk	a. Download a .csv template by clicking the **Download .csv Template** option. b. In the downloaded .csv file, enter the following details for each endpoint you must register: MAC address, endpoint type, hardware model, and hardware manufacturer. Save this file. c. Upload the .csv file using the **Choose a File** option. You can register a maximum of 500 endpoints at a time using the **Bulk** option.

Step 3 Click **Next**.

Step 4 Review the endpoint details in the **Review Endpoint** window. You can also edit the endpoint details, if changes are required.

Note While registering an existing endpoint, the profile label changes of the endpoint are reflected in purple color and can be edited.

Step 5 Click **Next** to continue with the registration process.

Step 6 Click **Register**.

Edit Registered Endpoints

You can update the profiling information of registered endpoints from the **Endpoint Inventory** window.

Step 1 Check the check box adjacent to the MAC address of the endpoint that you want to edit.

Step 2 Click **Actions**.

Step 3 Click **Edit Endpoint**.

Step 4 Enter the **Endpoint Type**, **Hardware Model**, and **Hardware Manufacturer** details.

Step 5 Click **Save**.

Delete Registered Endpoints

If there are registered endpoints that are no a longer part of your network, you can delete them from Cisco AI Endpoint Analytics.

Step 1 Check the check box adjacent to the MAC address of the endpoints that you want to delete.

Step 2 Click **Actions**.

Step 3 Click **Delete Endpoint**.

The following message is displayed:

```
Do you really want to delete the selected endpoint(s)?
```

Step 4 Click **Yes** to permanently delete the endpoint from Cisco AI Endpoint Analytics.

Trust Scores for Endpoint Spoofing Detection

Cisco AI Endpoint Analytics analyzes NetFlow telemetry data, and network probe data from Cisco ISE and SD-AVC devices, to detect spoofed endpoints.

Each endpoint type has a behavior model that is developed using machine learning algorithms. If an endpoint's behavior is unexpected of its endpoint type profile, the endpoint is assigned a Trust Score and listed as a spoofed endpoint.

The applications and server ports that are used by an endpoint are analyzed in this spoofing detection process. For example, if an endpoint profiled as a printer uses a video calling application, it is identified as a spoofed endpoint and assigned a Trust Score.

The trust scores assigned range from 1 through 10, and are categorized as follows:

Trust Score Category	Range	Probability of Spoofing
Low	1–3	High
Medium	4–6	Moderate
High	7–10	Low

You can then apply Adaptive Network Control (ANC) policies from Cisco ISE to enforce appropriate remediation actions on the endpoints. See section "Adaptive Network Control" in Chapter "Cisco ISE Admin Guide: Maintain and Monitor" of the *Cisco ISE Administrator Guide*.

The ANC policies are defined in Cisco ISE and allow you to apply remediation actions on chosen endpoints. You can apply ANC policies to quarantine, shut down, or port bounce an endpoint, or force endpoint reauthentication. When you apply an ANC policy to an endpoint with an undesirable Trust Score in Cisco AI Endpoint Analytics, a Change of Authorization (CoA) is sent to the endpoint from Cisco ISE.

An endpoint is identified by its MAC address. Cisco ISE sends the CoA to the endpoints that hold an active session for the identified MAC address at the time of the ANC application. Any endpoint with the same MAC address that does not have an active session in Cisco ISE at the time will match the ANC policy when a new session starts or when it must reauthenticate at the end of the configured reauthentication timer.

To verify which endpoint is being acted upon by the ANC policy, log in to your Cisco ISE administration portal. From the main menu, choose **Operations** > **RADIUS** > **Live Sessions**. Enter the MAC address of the spoofed endpoint in the **Endpoint ID** column, to filter the endpoints that share the same MAC address and currently have live sessions in Cisco ISE. These are the endpoints that will be affected by the ANC policy.

To view a historic log of the RADIUS sessions in Cisco ISE, from the main menu, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **RADIUS Authentications**.

To view or modify ANC policy application on endpoints in Cisco ISE, from the main menu, choose **Context Visibility** > **Endpoints**. Check the check box next to the MAC address of an endpoint and click the options displayed at the top of the list, as required.

Prerequisites

Prerequisites for receiving Trust Scores for spoofed endpoints:

- Cisco DNA Center is upgraded to Release 2.2.2 or later.

- Cisco ISE is connected to your on-premise Cisco DNA Center.

- Network access devices are managed by both Cisco DNA Assurance and Cisco ISE.

Note   The endpoint spoofing detection feature supports a maximum of 500 network access devices with NetFlow export flows, as Cisco DNA Assurance supports only 500 NetFlow exporters.

- Endpoints connected to network access devices are authenticated through Cisco ISE.

- **AI Spoofing Detection** must be enabled.
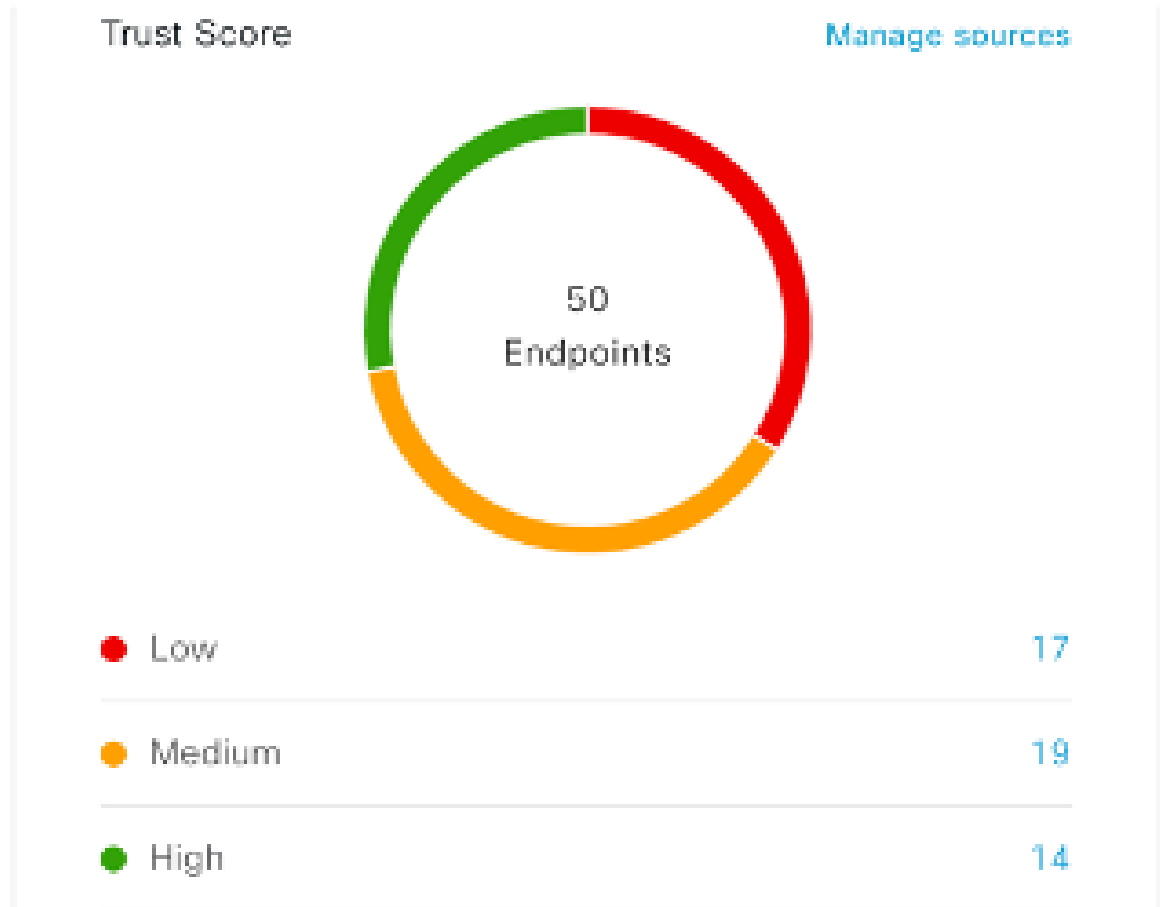
AI Spoofing Detection Capability

The **Cisco AI Analytics** software update for Cisco DNA Center Release 2.2.2 includes the capability **AI Spoofing Detection**. This capability is enabled by default.

From the main menu of Cisco DNA Center, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. The **AI Spoofing Detection** section contains the **Enable AI Spoofing Detection** toggle button. This section also includes the **Send data to help Cisco improve the model** toggle button, also enabled by default.

You can disable either component by clicking the relevant toggle buttons in this window.

View and Manage Spoofed Endpoints

Figure 1: Trust Score dashlet in Cisco AI Endpoint Analytics Overview tab

After Cisco DNA Center is upgraded to Release 2.2.2 and AI Spoofing Detection is enabled, the Cisco AI Endpoint Analytics **Overview** tab (**Main Menu > Policy > AI Endpoint Analytics**) displays the **Trust Scores** dashlet. This dashlet contains the following:

- The total number of spoofed endpoints identified.

- A donut chart and a list of the number of endpoints with low, medium, and high trust scores.

To view the details of endpoints in a trust score category, click its endpoint count in the **Trust Scores** dashlet. The **Endpoint Inventory** tab is displayed with the appropriate filters applied.

In the **Endpoint Inventory** tab, you can view endpoints with Trust Scores in two ways:

- Click the **Focus:** drop-down list and choose **Trust Score** to see all the endpoints with Trust Scores assigned.
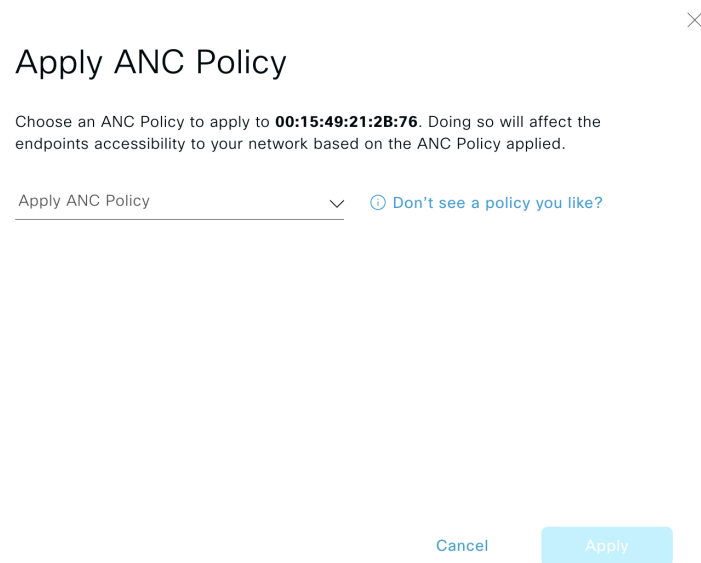
• Click **View endpoints in Trust Score View** from the caution message that is displayed, to see endpoints with Low and Medium scores.

The Trust Score views contain the following important columns, among others. You can also sort the data displayed according to these values:

• **Date Trust Score Reported**: The date and time when the endpoint's Trust Score was first reported.

• **Date ANC Policy Applied**: The date and time when the ANC Policy in use was applied to the endpoint.

• **Current ANC Policy**: The name of the ANC Policy in use.

You can perform the following actions on endpoints with Trust Scores:

• **Apply an ANC Policy**

×

Apply ANC Policy

Choose an ANC Policy to apply to **00:15:49:21:2B:76**. Doing so will affect the endpoints accessibility to your network based on the ANC Policy applied.

| Apply ANC Policy ⌄ | ⓘ Don't see a policy you like? |

Cancel   Apply

Click the **Apply ANC Policy** button to choose an ANC policy to be applied to an endpoint. The endpoint's access to the network is modified accordingly. ANC policies are imported from Cisco ISE and displayed in the drop-down list in the pop-up window displayed.

• **Replace an ANC Policy**

Change ANC Policy

Choose an ANC Policy to apply to **6** endpoints. Doing so will affect the endpoints accessibility to your network based on the ANC Policy applied.

Change ANC Policy ⌃ ⓘ Don't see a policy you like?

🔍 Search

No results found

Cancel Change

Click **Change ANC Policy** button to replace an existing ANC policy of an endpoint with another ANC policy. From the pop-up window displayed, choose the new policy to be applied from the **Change ANC Policy** drop-down list.

• **Remove an ANC Policy**

Click the **Remove ANC Policy** button to remove an applied ANC policy from an endpoint. In the pop-up window displayed, click **Remove**. This removes the remediation policy that was applied to the endpoint, and allows the endpoint to connect to the network normally.

• **Reset Trust Score**

Figure 2: Reset Trust Score for an Endpoint Without an ANC Policy

Figure 3: Reset Trust Score for an Endpoint with an ANC Policy

Click **Reset Trust Score** button to remove an endpoint from the Trust Score inventory. In the pop-up window displayed, click **Reset**.

If you choose this option for an endpoint after applying an ANC policy, you will not see this endpoint in the Trust Score inventory again. In this case, to modify the ANC policy for such an endpoint, you must remove the policy from Cisco ISE instead.

If you reset the score for an endpoint without applying an ANC policy, you may see the endpoint in the Trust Score inventory again with the next automatic refresh of Trust Score data.

The buttons for each of the actions are displayed in two locations in the **Endpoint Inventory** tab. The actions can be performed a single endpoint, or on multiple endpoints.

- **Manage Trust Score for Single Endpoint**

Figure 4: Trust Score Options for an Endpoint Without an ANC Policy

Figure 5: Trust Score Options for an Endpoint with an ANC Policy

From the list of endpoints with a Trust Score, click the MAC Address of the endpoint you want to manage. In the endpoints details pane that is displayed, click the **Trust Score** tab.

Here, **Expected Endpoint Type** and **Likely Endpoint Type** values are displayed. The **Applications Used** field lists the applications that are used by the endpoint, that are unusual for the expected endpoint type.

This pane includes buttons to start the workflows of accepting and removing ANC policies, and to reset the Trust Score. Click the button for the intended task.

Alternatively, you can check the check box for an individual endpoint on the **Endpoint Inventory** window, click **Actions**, and choose the required option from the drop-down list.

• **Manage Trust Score for Multiple Endpoints**
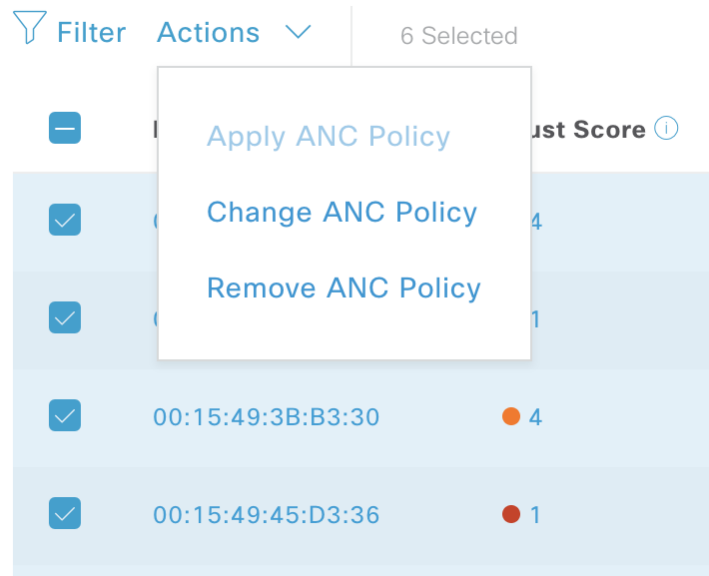
In the **Endpoint Inventory** tab, check the check boxes for all the endpoints you must perform a specific action on. Click **Actions** and choose the required action from the drop-down list.

Profiling Rules

Profiling rules in Cisco AI Endpoint Analytics enable you to group endpoints with a combination of common attributes. These attributes allow endpoint identification by Endpoint Type, OS Type, Hardware model, and Hardware Manufacturer. The profiling rules help you administer and manage many endpoints with ease.

Cisco AI Endpoints Analytics receives profiling data from network devices through DPI, media protocols, medical industry protocols, and more. Profiling data from Cisco ISE is communicated through pxGrid. These profiling attributes are then available in the device dictionary for authoring profile rules.

You can view the profiling rules in the **Profiling Rules** tab of Cisco AI Endpoints Analytics. In the table that is displayed under this tab, click a **Rule Name** entry to view the assigned profiles and attributes used.

The profiling rules that are used to profile the endpoints in Cisco AI Endpoint Analytics are:

• System Rules

• Custom Rules

• Cisco AI Rules

Rule Prioritization

The profiling rules in Cisco AI Endpoint Analytics have an order of priority. Profiling rule execution follows this rule priority to profile endpoints with high fidelity.

As user inputs are primary in Cisco AI Endpoint Analytics, the priority of the profiling rules is as follows:

- Administrator-created static profiles, for example, profiles added using the **Register Endpoints** option.

- Administrator-created custom rules.

- Cisco-provided system rules that are available by default.

- Auto-generated rules through the machine learning-enabled Smart Grouping workflow.

To view the set rule priority, click **Rule Prioritization** in the **Profiling Rules** window.

A registered endpoint can be profiled by multiple Cisco AI Endpoint Analytics rules for different profiling labels. The following table shows the design of profiling rules for two endpoints.

Endpoint 1	Endpoint 2
Hardware Model profiled by System Rule	Hardware Model profiled by System Rule
OS Type profiled by Cisco AI Rule	Hardware Model profiled by Custom Rule
Hardware Manufacturer profiled by Custom Rule	Hardware Model profiled by Cisco AI Rule

For Endpoint 2, rule priority results in the precedence of the custom rule over the others. The Hardware Model label for Endpoint 2 is profiled by the custom rule.

For Endpoint 1, different rules define different profile labels, and each label is profiled accordingly.

Filter Profiling Rules

Step 1   In the **Profiling Rules** window, click **Filter**.

Step 2   Enter a name in the **Rule Name** field.

Step 3   Select values for endpoint attributes from the corresponding drop-down lists, to filter for a set of endpoints.

Step 4   Click **Apply**.

View Updated Profiling Rules

Step 1   Go to the **Endpoint Inventory** window.

Step 2   Click the check box adjacent to the MAC Address of the endpoint to view the profiling details of the endpoint.

Step 3   Click the information icon next to profile labels, and click the rule name to view the assigned profile and attributes details.

System Rules

Cisco AI Endpoint Analytics provides predefined rules called System rules for profiling endpoints. When Cisco AI Endpoint Analytics is deployed, it provides day zero visibility into endpoints without any need to configure specific rules.

Newly onboarded endpoints are profiled using system rules by default.

Network devices are managed in Cisco DNA Center in the **Provision** > **Network Devices** > **Inventory** window.

These network devices are profiled by the system rules and are not visible in the Cisco AI Endpoint Analytics **Endpoint Inventory** window. However, you can view the endpoints profiled by custom rules because the custom rules are created with network device as **Device Type**.

Automatic System Rule Updates for Endpoint Profiling

The system rules that are used for endpoint profiling in Cisco AI Endpoint Analytics are regularly updated to enhance profiling accuracy. Schedule automatic updates to receive updates in endpoint profiling system rules from Cisco. Your Cisco DNA Center receives updates at the configured time, and the changes are applied in Cisco AI Endpoint Analytics. In the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**), review the details of the changes in endpoint profiles, and accept or decline the system rule update.

If an endpoint's hardware model value changes due to an accepted system rule update, when you view the endpoint's details in the **Endpoint Inventory** tab, the **Hardware Model** field contains the name of the system rule update.

Before you begin

Configure and enable NBAR Cloud. See Configure the NBAR Cloud Connector.

To check the status of NBAR Cloud, choose **Policy** > **AI Endpoint Analytics** > **Overview**, and click **Configuration**.

Step 1   From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Profile Rule Settings**.

The **Enabled** toggle button in the **Schedule Automatic Updates** area is set to active by default.

Step 2   Click the buttons for the days of the week on which you want to schedule updates. You can choose multiple days. Then, use the **Time Slot** text fields to select the time for the update. It takes 30 minutes for the updates to be received by Cisco DNA Center. The second time slot area is not editable and displays the time when the scheduled update is expected to complete.

Step 3   When your Cisco DNA Center receives a system rule update, a notification is displayed in the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**). The following notification is displayed when you click **Expand** in the dialog box:

You are updated to the latest version *Name of Latest Version* and a recent Cisco profiling rule has changed the profiles of some endpoints. Review Update.

Click **Review Update**

Step 4   The **Endpoint Profile Update Review** dialog box is displayed. The dialog box contains information on the current stable update applied, the latest update received, and more. It also contains the following sections that you can click to view the related endpoint profile updates:

a. **Major Updates**: Lists the endpoints whose profiles have had major changes, such as a Windows endpoint that is now recorded as a Linux endpoint.

b. **Minor Updates**: Lists the endpoints whose profiles have had minor changes, such as an updated version of Windows OS.

c. **Newly Profiled**: Lists the endpoints that were unprofiled previously and have now been assigned profile information.

Step 5 After you review the endpoint profile changes, to accept the profile update, click **Mark As Approved Version** in the **Endpoint Profile Update Review** dialog box. If you do not agree with the endpoint profile changes, click **Rollback**.

When you choose rollback, you must choose if you want to roll back to the last running version, or the last approved version, by clicking the corresponding option.

You can also perform the accept and rollback actions from the **AI Endpoint Analytics** > **Overview** > **Configuration** window.

Step 6 Click **X** to close the dialog box.

Custom Rules

In addition to the system rules, you can also create custom rules for profiling endpoints using a combination of endpoint attributes. Custom rules precede all the other endpoint profiling rules in Cisco AI Endpoint Analytics.

Logic and Conditions for Profiling Rules

You can create custom profiling rules in the **Endpoint Inventory** window. To create a custom profiling rule, you must create a logical condition based on endpoint attributes and values. These attributes are collected from network probe data and are different from the classification attributes available in the **Attribute Glossary** window.

A value is a user input that uniquely identifies the group of endpoints. The attributes and values create a regular expression with the help of the following operators.

Operators	Description
Contains	Attribute has the selected value.
Equals	Attribute is strictly mapped to the selected value.
Matches	Attribute should match the regular expression pattern of the selected value.
Starts With	Attribute should start with the selected value.

Note Contains, Equals, and Starts With are case-sensitive operators. For case-insensitive values, use the Matches operator.

These conditions can be further combined with the help of logic (**AND** and **OR**) to create a nested rule.

Create and Edit a Logical Condition

Follow the below instruction to create a logical condition.

Step 1   In the **Choose Attribute Conditions** window, check the check box adjacent to the **Attribute** that you want to update.

Step 2   Choose a option from the **Operator** drop-down lists.

Step 3   Enter the value in the **Value** field.

Step 4   Click **Next**.

Step 5   In the **Add Logic to Conditions** window that is displayed, drag and drop the **AND** logic or the **OR** logic between the conditions in order to create a logical sequence of conditions for a custom rule.

> **Note**   You can also add or edit an attribute condition in the **Add Logical Conditions** window using the vertical ellipsis next to a condition.

Step 6   Click **Next**.

Create a Custom Rule

Step 1   In the **Endpoint Inventory** window, check the check box adjacent to the MAC address of the endpoints that you want to profile.

Step 2   Click **Actions** and select **Profile with Custom Rules**.

Step 3   In the **Name Rule and Type** window that is displayed, in the **Rule Name** field, enter a name for the rule, and from the **Profile Label** drop-down list, choose a label.

Depending on what you choose from the **Profile Label** drop-down list, a corresponding field, whose name is dynamically updated, is displayed. For example, if you choose **Endpoint Type**, the **Endpoint Type** field appears.

Step 4   Enter a value in the new field that is displayed. As you start entering information, matching options are displayed. If an option matches your requirements, select the same. Otherwise, enter the complete type name.

Step 5   Click **Next**.

Step 6   In the **Choose Attribute Conditions** window that is displayed, create a logical condition.

For more information, see Logic and Conditions for Profiling Rules

Step 7   In the **Review Rule** window, review the list of endpoints that are going to be profiled with this custom rule.

Step 8   Click **Next**.

Step 9   Click **Profile**.

Edit a Custom Rule

Step 1   In the **Profiling Rules** window, check the check box adjacent to the admin rule you want to edit.

Step 2   Click **Actions** and select **Edit**.

Step 3   In the **Edit** window that is displayed, in the **Rule Name** field, enter a name for the rule, and select or enter the profile details based on the **Profile Label** selected during the rule creation.

Step 4   In the **Logic and Conditions** section, click on the vertical ellipsis and select **Edit** to update the logic and conditions for profiling rules. For more information, see Logic and Conditions for Profiling Rules.

Step 5   Click **Next**.

Step 6   Click **Apply**.

After the existing rule is updated with new profiling details, the endpoints profiled with this rule are updated with new profiling details.

Delete a Custom Rule

Step 1   In the **Profiling Rules** window, check the check box next to the rule that you want to delete.

Step 2   Click **Actions** and choose **Delete**.

The following message is displayed:

```
Do you really want to delete the selected Rule(s)?
```

Step 3   Click **Yes** to permanently delete the rule from Cisco AI Endpoint Analytics.

After the custom rule is deleted, the endpoints profiled with this rule are updated with system rules.

Cisco AI Rules or Smart Grouping

Cisco AI Endpoint Analytics uses ML cloud to group unknown endpoints on your network dynamically. It also allows you to assign custom labels to groups of unknown endpoints. You can review the clusters and accept or reject the profiling suggestions provided.

When you accept the profiling suggestions, a profiling rule is automatically created to profile the selected endpoints, and to profile similar endpoints that join your network in the future.

Modify Profiling Rule Suggestions

The **AI Proposal** dashlet on the **Endpoint Analytics** home page displays rule suggestions based on the endpoint clusters generated by Smart Grouping. To view an AI proposal, click **Review** adjacent to the corresponding proposal type and proceed according to the following decision chart.
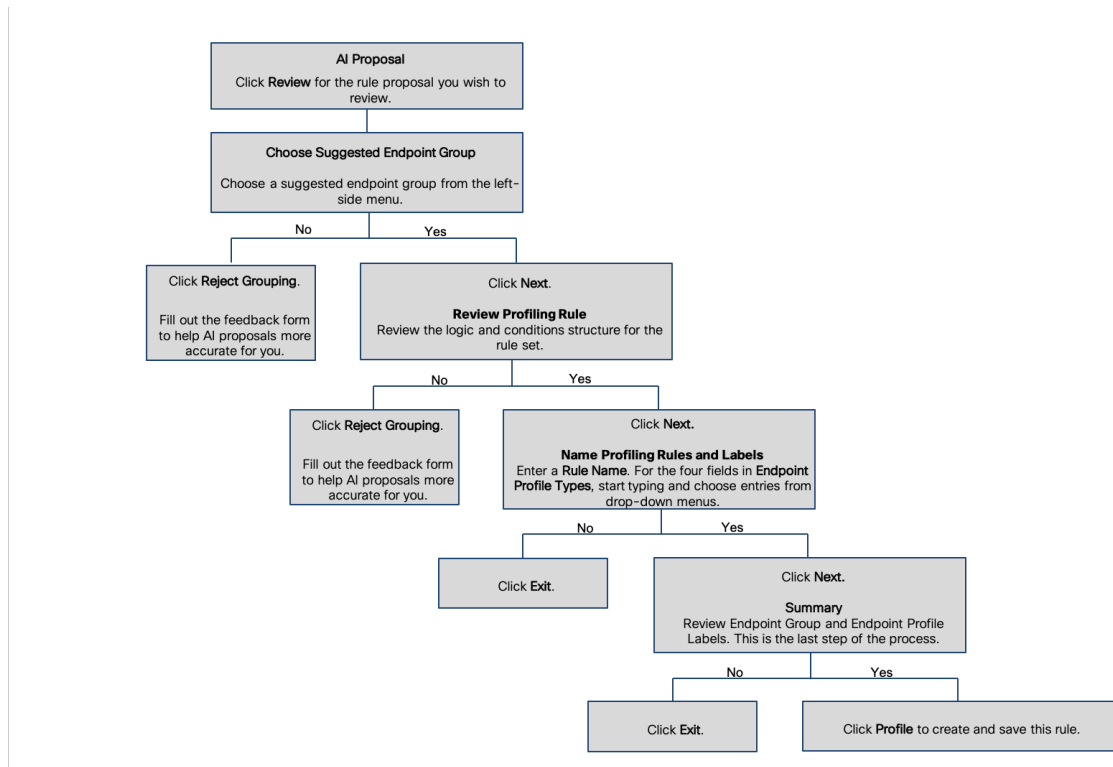
Import Profiling Rules

You can migrate your custom profiling rules and Cisco AI rules by importing the .json files.

Step 1   In the **Profiling Rule** window, click **Actions**

Step 2   Choose **Import Profiling Rules**.

Step 3   Click **Choose a file** and browse to the .json file in your system.

Step 4   Click **Ok**.

Export Profiling Rules

You can export and back up custom rules and Cisco AI profiling rules from Cisco AI Endpoint Analytics. The **Export Profiling Rules** option exports all the available custom rules and Cisco AI profiling rules. You cannot selectively export rules.

Step 1   In the **Profiling Rules** window, click **Actions**.

Step 2   Choose **Export Profiling Rules**.

Step 3   Click **Yes** to export all the custom and ML profiling rules. Click **No** to exit.

Note	You can import the same file again into Cisco AI Endpoint Analytics.

Hierarchy

Cisco AI Endpoint Analytics hierarchy helps you create logical groupings of endpoints, based on the endpoint types. Creating categories and subcategories for the endpoints focuses on endpoint visibility and simplifies the authorization process.

You can create categories from the **All Endpoints** default parent category. The category details such as total number of endpoints, endpoint types, and subcategories are listed within individual boxes in the **Hierarchy** window.

You can create, edit, and delete the categories to reorder the hierarchy.

Create Category and Subcategory

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the parent category.

Step 2 Click **Create Category**.

Step 3 Enter a category name.

Step 4 Click **Enter**.

What to do next

After you create a category, you can drag and drop endpoint types from the **Endpoint Type** window, or edit the category to add endpoints to it.

Edit a Category or Subcategory

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.

Step 2 Click **Edit**.

Step 3 In the **Edit** window that is displayed, enter the **Category Name**.

Step 4 Enter the **Parent Category** from the drop-down menu, if you want to reassign the category.

Step 5 Click the **Endpoint Type** tab.

Step 6 Click **Actions** and select **Add Endpoint Type**.

Step 7 Choose the endpoint type from the **Search Dropdown** list.

Step 8 Click **Save**.

What to do next

In the Endpoint Type window, you can filter the endpoint types as **All**, **Available**, and **Assigned**.

Delete Endpoint Types from Category

Step 1   In the **Hierarchy** window, click the horizontal ellipsis of the category that you want to delete.

Step 2   Click **Edit**.

Step 3   In the **Edit** window, click the **Endpoint Type** tab.

Step 4   Check the check box adjacent to the endpoint type that you want to delete.

Step 5   Click **Actions** and choose **Remove From Category**.

The following message displays:

```
Are you sure you want to delete this category?
```

Step 6   Click **Yes** to delete the endpoint from the category. Click **No** to exit.

Reassign Endpoint Types from Category

Step 1   In the **Hierarchy** window, click the horizontal ellipsis of the category.

Step 2   Click **Edit**.

Step 3   In the **Edit** window, click the **Endpoint Type** tab.

Step 4   Check the check box adjacent to the endpoint type that you want to reassign.

Step 5   Click **Actions** and choose **Re-assign to existing category** or **Re-assign to a new category**.

Option	Steps
Re-assign to existing category	a. In the **Reassign** window, choose an existing category from the **Category** drop down list. b. Click **Save**.
Re-assign to a new category	a. In the **Reassign** window, choose **New Category** from the **Category** drop down list. b. Choose a parent category from the **Parent Category** drop down list. c. Enter the category name in the **New Category** field. d. Click **Save**

Delete a Category

Before you begin

Before you delete a parent category, check its subcategories. You can reassign the subcategories to another existing category or to a new category. Otherwise, all the subcategories will get deleted along with the parent category. You can also reassign the subcategories while you are deleting a category.

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.

Step 2 Click **Delete**.

If you are deleting a category that has subcategories assigned to it, the **Reassign Relationships** dialog box is displayed. Select the one of the following options:

Option	Condition	Steps
Reassign to an existing category	Reassign the subcategories to an existing category.	a. Select a category from the **Category** drop-down list. b. Click **Reassign**. The parent category is deleted and its subcategories will be reassigned to the selected category.
Reassign to a new category	Reassign the subcategories to an existing category.	a. Select a category from the **Parent Category** drop-down list. b. Enter the category name in the **New Category** field. c. Click **Reassign**. The parent category is deleted and its subcategories are reassigned to the new category.
Remove from category	Delete the subcategories along with the parent category.	Click **Reassign**. The parent category and its subcategories are deleted.