CHAPTER 18

Configuring Endpoint Profiling Policies

This chapter describes the profiling service in the Cisco Identity Services Engine (Cisco ISE) appliance, which allows you to efficiently manage an enterprise network of varying scale and complexity.

This chapter guides you through the features of the Cisco ISE profiling service in detail.

Profiling Service in Cisco ISE

The Cisco ISE profiling service provides a unique functionality in discovering, locating, and determining the capabilities of all the attached endpoints on your network (known as identities in Cisco ISE), regardless of their device types, to ensure and maintain appropriate access to your enterprise network. It primarily collects an attribute or a set of attributes of all the endpoints on your network and classifies them according to their profiles.

For details on the profiling service, see the "Understanding the Profiling Service" section on page 18-2.

The Profiler in Cisco ISE

The Cisco ISE profiler is comprised of the following components:

- The sensor contains a number of probes. The probes capture network packets by querying network access devices and forward attributes and attribute values that are collected from endpoints to the analyzer.

  The probe manager within the sensor provides support to the profiling service, initializing and controlling various probes that run on the sensor. The probe manager allows you to configure probes to start and stop collecting attributes and their values from endpoints. An event manager within the sensor allows communication of the events between the probes in the probe manager.

  A forwarder stores endpoints into the Cisco ISE database along with their attributes data, and then notifies the analyzer of new endpoints detected on your network. The analyzer classifies endpoints into endpoint identity groups and stores endpoints with the matched profiles in the Cisco ISE database.

- An analyzer evaluates endpoints, by using configured policies and identity groups to match attributes and their attribute values that are collected, which classifies endpoints into the specified group and stores endpoints with the matched profile in the Cisco ISE database.

Understanding the Profiling Service

The profiling service collects attributes of endpoints from the network devices and the network, classifies endpoints into a specific group according to their profiles, and stores endpoints with their matched profiles in the Cisco ISE database. You can use a list of possible attributes that includes any or all of the attributes defined in the system dictionaries. You can leverage the existing dictionaries as well as define an ad-hoc dictionary for any attribute during run-time. All the attributes that are handled by the profiling service need to be defined in the profiler dictionaries.

An endpoint is a network-capable device that connects to your enterprise network. The MAC address is always the unique representation of an endpoint, but you can also identify an endpoint with a varying set of attributes and the values associated to them, called an attribute-value pair. You can collect a varying set of attributes for endpoints based on the endpoint capability, the capability and configuration of the Network Access Devices (NADs), and the methods (probes) that you use to collect these attributes.

You can associate each endpoint on your network to an existing endpoint identity group in the system, or to a new group that you can create and associate to the parent group. By grouping endpoints, and applying endpoint profiling policies to the group, you can determine the mapping of endpoints to the endpoint profiles by checking the corresponding endpoint profiling policies.

For details on endpoint profiling on Cisco ISE, see "Endpoint Profiling" section on page 18-3.

For details on licenses that you need to install for the profiling service, see "Licenses for the Profiling Service" section on page 18-4.

For details on how to deploy the profiling service, see "Deploying the Profiling Service" section on page 18-4.

For details on Profiled Endpoints dashlet, see "Profiled Endpoints Dashlet" section on page 18-7.

For details on endpoint profiling reports, see the "Viewing Profiler Reports" section on page 18-8.

Endpoint Profiling

Endpoint profiling in Cisco ISE identifies each endpoint on your network, and groups those endpoints according to their profiles.

The Cisco ISE profiler provides you with an efficient and effective means of addressing the challenge in the deployment and management of the following next-generation security mechanisms:

- Facilitates an efficient and effective deployment and ongoing management of authentication by using IEEE standard 802.1X port-based authentication access control, MAC Authentication Bypass (MAB) authentication, and Network Admission Control (NAC) for any enterprise network of varying scale and complexity.
- Identifies, locates, and determines the capabilities of all of the attached network endpoints regardless of endpoint types.
- Protects against inadvertently denying access to some endpoints.

The profiler provides a contextual inventory of all the endpoints that are using your network resources to identify what is connected to your network, and where it exists on your network. The profiler allows both static and dynamic endpoint profiling, where dynamic endpoint profiling allows you to discover endpoints on your Cisco ISE enabled network, and notify attribute changes resulting from the network to your Cisco ISE deployment.

To effectively profile endpoints on your network, you require a thorough understanding of the types of endpoints (devices) that are connecting to your network, their location, and their abilities relative to the state of the port on which they currently reside. You can define endpoint profiling policies in Cisco ISE, which allow you to group endpoints according to their profiles. Cisco ISE deployment creates the following four endpoint identity groups by default: Registered Devices, Blacklist, Profiled, and Unknown. In addition, the system creates two more identity groups: the Cisco-IP-Phone group and the Workstation group, which are both children of the Profiled group.

An endpoint profiling policy can contain a single condition, or a set of conditions (compound condition) that are logically combined using an AND or OR operator, against which you check and categorize endpoints. All the conditions can either be used with an AND operator or an OR operator together for a given rule in a policy. However, the rules in a given policy are evaluated separately, and only by using an OR operator.

A condition is used to check the collected endpoint attribute value against the value specified in the condition for an endpoint. If you map more than one attribute, you can logically group the conditions, which helps you to classify and categorize endpoints on your network. You can check endpoints against one or more such conditions with a corresponding certainty metric (an integer value that you define) associated with it in a rule. The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty metric for all the valid rules are added together to form the matching certainty. The certainty metric measures how each condition contributes which improves the overall classification of endpoints on your network. Each policy has a minimum certainty metric (an integer value) associated to it.

An exception action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the exception conditions that are associated with the action are met.

An endpoint scan action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the conditions that are associated with the network scan action are met.

Licenses for the Profiling Service

Prerequisites:

To enable the profiling service in Cisco ISE, you must install an advanced license package on top of the base license. You can utilize all of the session services, including the Network Access, Guest, Posture, Client Provisioning, Profiling Service, and Security Group Access (SGA) depending on your configuration.

Cisco ISE allows you to configure the profiling service to run on multiple nodes that assume the Policy Service persona in a distributed Cisco ISE deployment. You can also configure the profiling service on a single node in a standalone Cisco ISE deployment.

Note To promote device status replication and network profiling efficiency among Policy Service ISE nodes, Cisco recommends installing multiple Policy Service ISE nodes within local area network segments tangent to the Administrative ISE node, and avoid relying on wide-area network connections between Policy Service ISE nodes as much as possible.

With a Base license installed, you cannot profile endpoints on your network. You can only manage endpoints including import and the static assignment of endpoints by using the Endpoints page, and view endpoints in the Endpoint Identity Groups page. For more details, see the Endpoints, page 4-15, and Endpoint Identity Groups, page 4-71 sections in Chapter 4, “Managing Identities and Admin Access.”

Cisco ISE consumes Advanced licenses when endpoints are matched to an authorization policy. For more information, see “Excluding Static Endpoints in Advanced Licenses” section on page 18-78.

For more information on Cisco ISE license packages, refer to the Performing Post Installation Tasks chapter in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

Deploying the Profiling Service

Prerequisites:

Before you begin, you should have an understanding of the centralized configuration and management of Cisco ISE nodes in the distributed deployment.

For information on Cisco ISE distributed deployment, Chapter 9, “Setting Up Cisco ISE in a Distributed Environment”

You can deploy the Cisco ISE profiling service either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). Depending on your deployment type and the license you have installed, the profiling service of Cisco ISE can run on a single node or on multiple nodes. You need to install either the base license to take advantage of the basic services or the advanced license to take advantage of all the services of Cisco ISE.

Cisco ISE distributed deployment includes support for the following:

- The Deployment Nodes page supports the infrastructure for distributed nodes in the distributed deployment.
- A node specific configuration of probes—The Profiling Configuration page allows you to configure the probe per node from the Administration ISE node.

- Global Implementation of the profiler Change of Authorization (CoA).
- Configuration to allow syslogs to be sent to the appropriate profiler node.

Configuring the Profiling Service in Cisco ISE

From the Administration menu, you can choose Deployment to manage the Cisco ISE deployment on a single node or multiple nodes. You can use the Deployment Nodes page to configure the profiling service for your Cisco ISE deployment.

To manage the Cisco ISE deployment, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

The Deployment navigation pane appears. Use the format selector icons to view the nodes in rows or in a tabbed display.

Step 2 Click the row view icon.

Step 3 Click the quick picker (right arrow) to view the nodes that are registered in your deployment.

The row view displays all the nodes that are registered in a row format in the Deployment Nodes page.

Note To view the nodes in your deployment in a tree, click the tabbed view icon. An arrow appears in front of Deployment in the Deployment navigation pane. Click the arrow in front of the Deployment navigation pane to view the nodes that are registered in your deployment in a tabbed view.

From the Deployment Nodes page, you can configure the profiling service on any Cisco ISE node that assumes the Policy Service persona in a distributed deployment.

To deploy the profiling service, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

The Deployment navigation menu appears. Use the Table view or the List view to display the nodes in your deployment.

Step 2 Click the Table view.

Step 3 Click the quick picker (right arrow) to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format in the Deployment Nodes page. The Deployment Nodes page displays the nodes that you have registered along with their names, personas, roles, and the replication status for the secondary nodes in your deployment.

Step 4 Choose a Cisco ISE node from the Deployment Nodes page.

Note If you have more than one node registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, along with the primary node. You have the option to configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas), or an Inline Posture node. If you have the Policy Service persona enabled, but the Enable Profiling Services check box unchecked, Cisco ISE does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab that prevents you from configuring the probes in the node.

Step 5 Click **Edit**.

The Edit Node page appears. This page contains the General Settings tab to configure the deployment and the Profiling Configuration tab to configure the probes on each node. The Profiling Configuration tab will not be made available on the secondary Administration ISE node.

Note If you have the Policy Service persona disabled, or if enabled but the Enable Profiling Services option is not selected, then the Cisco ISE administrator user interface does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any Cisco ISE node, Cisco ISE displays only the General Settings tab. It does not display the Profiling Configuration tab that prevents you from configuring the probes in the node.

Step 6 On the General Settings tab, check the **Policy Service** check box, if it is not already active.

If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 7 For the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services, check the **Enable Session Services** check box, if it is not already active. To stop the session services, uncheck the **Enable Session Services** check box.

Step 8 For the Policy Service persona to run the profiling service, check the **Enable Profiling Services** check box. To stop the profiling service, uncheck the **Enable Profiling Services** check box.

Note The profiling service only runs on Cisco ISE nodes that assume the Policy Service persona and does not run on Cisco ISE nodes that assume the Administration and Monitoring personas in a distributed deployment.

Step 9 Click **Save** to save the node configuration.

Next Steps:

See the "Configuring the Probes" section on page 18-13 for more information on how to configure the profiler probes after installing the Cisco ISE application for your network.

Profiled Endpoints Dashlet

The Profiled Endpoints dashlet summarizes the number of dynamically profiled endpoints for the last 24-hour period, as well as 60 minutes from the current system time. It refreshes data every minute and displays it in the dashlet. You can invoke the Endpoint Profiler Summary report from the tool tips that are displayed in the 24-hour and 60-minutes sparklines for a specific period. The stack bars display endpoint distribution details by Place in Network (PIN), matching endpoint profiles, and identity groups.

The Profiled Endpoints dashlet does not reflect endpoints for the following type of endpoints:

- Endpoints that are classified as Unknown
- Endpoints that are statically assigned to endpoint profiles. (Static assignment can be done from the Endpoints list page by editing endpoints and setting the Static Assignment flag to true.)
- Endpoints that are imported with specified profiles.

For endpoints imported from a .csv file, the Profiled Endpoints dashlet will reflect endpoints for which an endpoint profile is not specified.

The dashlet provides profiler distribution details for the last 24-hour period, as well as 60-minutes from the current system time.

Table 18-1 describes the Profiled Endpoints dashlet details in Cisco ISE.

Table 18-1 Profiled Endpoints Dashlet

Name	Description
Unique	A summary of unique endpoints profiled in Cisco ISE for the last 24-hour from the current system time.
PIN (Place in Network)	The location of all the profiled endpoints with subnet mask information.
Profile	The endpoint profiling policies that are used to profile endpoints.
Identity Group	
Endpoint Identity Group	Displays endpoint identity groups of endpoints that they belong, which do not fall under 802.1X authentication. In addition, it also displays endpoint identity groups of endpoints and user identity groups of users for 802.1X authentication.
User Identity Group	Displays the user identity groups of users when endpoints are 802.1X authenticated.

Viewing Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to efficiently manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to view more details. For large reports, you can also schedule reports and download them in various formats.

For more information on how to generate reports and work with the interactive viewer, see Chapter 25, "Reporting."

For more information on endpoint profiling reports, see "Standard Reports" section on page 18-8.

Standard Reports

For your convenience, the standard reports present a common set of predefined report definitions. You can click the Report Name link to run the report for today. You can query the output by using various system predefined parameters. You can enter specific values for these parameters.

You can use the Run button to run the report for a specific period, as well as use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. The Add to Favorite button allows you to add reports that you use frequently to the Operations > Reports > Favorites location. The Reset Reports button allows you to reset your reports in this catalog to factory defaults.

You can run the reports on endpoint profiling from the following location:

Operations > Reports > Catalog > Endpoint.

The following are the standard reports for endpoint profiling:

- Endpoint_MAC_Authentication_Summary—A report that lets you view the RADIUS authentication summary information for a particular MAC/MAB along with a graphical representation for a selected time period.

- Endpoint_Profiler_Summary—A report that lets you view the profiler summary information for a particular MAC address for a selected time period.
- Endpoint_Time_To_Profile—A report that lets you view the time to profile information for a particular MAC address for a selected time period.
- Top_N_Authentications_By_Endpoint_Calling_Station_ID—A report that lets you view the top N passed/failed/total authentications count for RADIUS protocol with respect to an endpoint calling station ID for a selected time period.
- Top_N_Authentications_By_Machine—A report that lets you view the top N passed/failed/total authentications count for RADIUS protocol with respect to machine information for a selected time period.

In addition, you can view a fewer accounting records for intervals of less than an hour with an enhanced option for profiling endpoints that uses an embedded IOS sensor.

For more information, see RADIUS Accounting Reports, page 18-78.

Change of Authorization

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) for endpoints that are already authenticated to enter your network. The global configuration of CoA in Cisco ISE enables the profiling service with more control over endpoints.

You can use the global configuration option to disable CoA by using the default No CoA option or enable CoA by using port bounce and reauthentication options. If you have configured Port Bounce CoA in Cisco ISE, the profiling service may still result in issuing other CoAs as described in the CoA Exemptions section. For information on CoA exemptions, see the "CoA Exemptions" section on page 18-10.

You can primarily make use of the RADIUS probe or the Monitoring persona REST API to address the authentication of endpoints. For performance reasons, you can enable the RADIUS probe, which allows faster performance. If you have enabled CoA, then we recommend you to enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application. The profiling service can then issue an appropriate CoA for endpoints by using the RADIUS attributes that are collected. If you have disabled the RADIUS probe in the Cisco ISE application, then you can also rely on the Monitoring persona REST API to issue CoAs. This allows the profiling service to support a wider range of endpoints without requiring the support of the RADIUS probe.

Note Since both primary and secondary Monitoring nodes have identical session directory information, Cisco ISE arbitrarily designates one of those nodes as the default destination for REST queries.

No CoA

You can use this default option to disable the global configuration of CoA.

Port Bounce

You can use this option only if there is only one session on a switch port. If the port exists with multiple sessions, then the CoA option that is used is the Reauth option.

Reauth

You can use this option to enforce reauthentication of an already authenticated endpoint when profiled.

If you have multiple active sessions on a single port, the profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option. This function potentially avoids disconnecting other sessions as might occur with the Port Bounce option.

The profiling service initiates the CoA in the following cases:

- An exception action is configured
- An endpoint is profiled for the first time
- Endpoint deleted
- An endpoint identity group has changed

An Exception Action is Configured

The profiling service issues a CoA for an endpoint, if you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint so that the profiling service moves the endpoint to the corresponding static profile by issuing a CoA.

For more information on exception action, see the "Profiling Exception Actions" section on page 18-60.

An Endpoint is Profiled for the First Time

The profiling service issues a CoA for an endpoint that is not statically assigned and profiled for the first time, for example, the profile changes from an unknown to a known profile.

An Endpoint is Deleted

The profiling service issues a CoA when an endpoint is deleted from the Endpoints page and the endpoint is most likely disconnected or removed from the network.

An Endpoint Identity Group has changed

The profiling service issues a CoA when an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

- The endpoint identity group changes for endpoints when they are dynamically profiled
- The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint

The profiling service does not issue a CoA when there is a change in an endpoint identity group and the static assignment is already true.

For more information on CoA exemptions, see the "CoA Exemptions" section on page 18-10.

For more information on CoA configuration details, see Table 18-2.

CoA Exemptions

The implementation of CoA in Cisco ISE is described in "Change of Authorization" section on page 18-9.

This section describes a few environments in Cisco ISE where the profiler does not issue a CoA even though it matches as described in the Change of Authorization section.

An Endpoint Disconnected from the Network

The profiling service does not issue a CoA when a disconnected endpoint from your network is discovered.

Authenticated Wired EAP-Capable Endpoint

The profiling service does not issue a CoA when an authenticated wired EAP-capable endpoint is discovered.

Multiple Active Sessions per Port

The profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option when you have multiple active sessions on a single port. This function potentially avoids disconnecting other sessions as might occur with the Port Bounce option.

Packet-of-Disconnect CoA (Terminate Session) when a Wireless Endpoint is Detected

If an endpoint is discovered as wireless by using the Wireless - 802.11 or Wireless - Other values according to the NAS-Port-Type attribute (the values for RADIUS Attribute 61) of that endpoint, then a Packet-of-Disconnect CoA (Terminate-Session) is issued instead of the Port Bounce CoA. The benefit of this change is to match the Wireless LAN Controller (WLC) CoA.

Note Here, the No CoA and Reauth CoA configurations are not affected and it applies the same for wired and wireless endpoints. Refer to Table 18-2.

Table 18-2 summarizes CoA for different environments for each CoA configuration in Cisco ISE.

Table 18-2 Change of Authorization for Each CoA Configuration

Scenarios	CoA Configuration - No CoA	CoA Configuration - Port Bounce	CoA Configuration - Reauth	Additional information
Global CoA configuration in Cisco ISE (typical)	No CoA	Port Bounce	Reauthentication	
An endpoint is disconnected on your network	No CoA	No CoA	No CoA	It is determined by RADIUS attribute Acct -Status -Type value Stop.
An authenticated wired EAP-capable endpoint	No CoA	No CoA	No CoA	If authentication fails, then it is the same as the typical configuration.
Wired with Multiple Active Sessions on the same switch port	No CoA	Reauthentication	Reauthentication	It avoids disconnecting other sessions.

Table 18-2 Change of Authorization for Each CoA Configuration (continued)

Scenarios	CoA Configuration - No CoA	CoA Configuration - Port Bounce	CoA Configuration - Reauth	Additional information
Wireless endpoint	No CoA	Terminate Session (PoD)	Reauthentication	Support to WLC.
Incomplete CoA data	No CoA	No CoA	No CoA	Due to missing RADIUS attributes.

An Endpoint Created through Guest Device Registration flow

The profiling service does not issue a CoA when endpoints are created through device registration for the guests eventhough CoA is enabled globally in Cisco ISE in order not to break the device registration flow. In particular, the PortBounce CoA global configuration breaks the flow of the connecting endpoint.

CoA Global Configuration

You can use the Settings menu window to configure the CoA globally on your Cisco ISE distributed deployment.

To configure CoA, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 In the Settings navigation pane, choose **Profiling**.

Step 3 Configure the CoA.

The profiling configuration for CoA has the following options:

- No CoA (default)
- Port Bounce
- Reauth

Step 4 Click **Save**.

Configuring the Probes

Prerequisite:

Before you begin, you should have a basic understanding of the Cisco ISE distributed deployment. Review the following:

Deploying the Profiling Service to understand how the profiling service is enabled in the Cisco ISE distributed deployment.

A probe is a method used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the database. The Profiling Configuration tab in the Edit Node page contains the configuration options that allow you to enable or disable the probes on each node, where a node specific configuration of probes can be done on your Cisco ISE appliances.

For more information on filtering endpoints attributes, see the Filtering Endpoint Attributes, page 18-14.

You can reach the Deployment menu from the Administration menu. The Deployment menu window displays the registered nodes in your deployment. You can use the Table view or the List view to display the nodes in your deployment. You can also select a node from the Deployment menu window.

To configure a probe on a node, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 In the Deployment Nodes page, click the node.

The Deployment Nodes page displays the nodes that you have registered with their names, personas, roles, and the replication status in your deployment.

Note If you have a single node registered, only the node that you have registered appears in the Deployment Nodes page. You need to enable the Administration, Policy Service, and Monitoring personas on it. If you have more than one node registered, all the nodes that you have registered appear in the Deployment Nodes page. You have the option to configure each node as an ISE node (Administration, Policy Service, and Monitoring personas) or an Inline Posture node. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab, which prevents you from configuring the probes in the node.

Step 3 From the Deployment Nodes page, choose **Edit**.

The Edit Node page appears. This page contains the General Settings tab for configuring Cisco ISE deployment and the Profiling Configuration tab for configuring probes on each node.

Note If you have the Policy Service persona enabled, but the **Enable Profiling Services** check box is unchecked, Cisco ISE does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab that allows you to configure the probe in the node.

Step 4 Click the **Profiling Configuration** tab.

The Probe Configuration page displays all the probes that Cisco ISE supports and their configuration options in a single page.

Step 5 Configure the values in the Edit Node page for each probe.

The procedures for configuring each probe on a node in the profiling service includes the following tasks:

- Configuring the NetFlow Probe
- Configuring the DHCP Probe
- Configuring the DHCP SPAN Probe
- Configuring the HTTP Probe
- Configuring the RADIUS Probe
- Configuring the Network Scan (NMAP) Probe
- Configuring the DNS Probe
- Simple Network Management Protocol
  - Configuring the SNMP Query Probe
  - Configuring the SNMP Trap Probe

Step 6 Click **Save** to save the probe configuration.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Filtering Endpoint Attributes

Cisco ISE, when enabled with multiple probes per node, experiences a considerable performance degradation due to numerous attributes per endpoint that are collected and stored in the administration node database. Some of the attributes that are collected are temporal in nature as well as not required for endpoint profiling. The huge collection of attributes per probe for each endpoint that cannot be used for endpoint profiling results in Cisco ISE administration node database persistence and performance degradation.

To address performance degradation of Cisco ISE, filters for RADIUS, DHCP (both DHCP Helper and DHCP SPAN), HTTP, and SNMP probes have been implemented in the profiler probes, except for the NetFlow probe. Each probe filter contains the list of attributes that are temporal and irrelevant for endpoint profiling and removes those attributes from the attributes collected by the probes.

The forwarder component of the profiler invokes the filter event to remove attributes that are specified in each of the filter. They remove attributes from the collection before merging them with existing attributes and their values in the endpoint cache. In addition to removing attributes from the attributes that are collected from all the probes, the profiler dictionaries also have been updated with a list of attributes that are required for endpoint profiling.

A DHCP filter for both the DHCP Helper and DHCP SPAN contains all the attributes that are not necessary and they are removed after parsing DHCP packets. The attributes after filtering are merged with existing attributes in the endpoint cache for an endpoint.

An HTTP filter is used for filtering attributes from HTTP packets, where there is no significant change in the set of attributes after filtering.

A RADIUS filter is used once the syslog parsing is complete and endpoint attributes are merged into the endpoint cache for profiling.

A SNMP filter removes all the attributes that are not relevant after the SNMP Query probe collects a large number of attributes.

The Cisco ISE Bootstrap log contains messages that deal with the creation of dictionaries as well as filtering of attributes from the dictionaries. You can also log a debug message when endpoints go through the filtering phase to indicate that filtering has occurred.

Global Setting for Endpoint Attribute Filter

Cisco ISE writes endpoints attributes data that are received from the secondary ISE nodes to the primary Administration ISE node, and stores endpoint data in the Administration ISE node primary database. Cisco ISE assumes a synchronous and guaranteed messaging to all the secondary ISE nodes during replication, which means that for every message sent from the primary Administration ISE node requires an acknowledgement from the secondary ISE nodes before sending the next message.

When the endpoint attributes collection rate is very high from the network, the number of events sent to the primary ISE node for endpoint activities is also very high, and so the replication events are also high. In a high latency deployment, or if a primary ISE node slows down for various reasons, replication messages might pile-up in the primary ISE node, which might cause an out of memory error in the primary ISE node and the node might crash.

You can do the following to reduce the replication events:

- Buffering—You can buffer endpoint attributes data in the Policy Service nodes for a minute that delays writing endpoint data to the Administration ISE node by one minute, which reduces the number of persistence events and replication events. The Administration ISE node may not have the most recent endpoint attributes collected for a minute.
- Whitelisting—You can reduce the number of endpoint attributes collected that do not change frequently at the collection point. By reducing the set of endpoint attributes to collect, you can reduce the number of persistence events and replication events.

Whitelisting

A whitelist is a set of attributes collected that are used in custom endpoint profiling policies for profiling endpoints, and that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function in Cisco ISE as expected.

Any attribute that is not present in the whitelist is dropped immediately at the time of collection, and the attribute cannot participate in profiling endpoints. When combined with the buffering, the number of persistence events can be reduced.

You must ensure that the whitelist contains a set of attributes determined from the following two sources:

- A set of attributes that are used in the default profiles so that you can match endpoints to the profiles.
- A set of attributes that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function as expected.

Limitations of Whitelisting

You have the following limitations when you are using whitelisting:

- Any new attribute other than that are specified in the whitelist will not be collected and persisted in the primary database. Any custom profile will not work as expected that uses new attributes, which are not specified in the whitelist.

- Dynamic whitelisting—You can extend the whitelist to other attributes that you find it useful, which supports the customization of endpoint policies by allowing the whitelist to be modified dynamically through the endpoint profile changes. If you determine dynamic endpoint attribute collection, then you might experience the replication issues again as before.
- Active whitelisting—You must ensure an updated list of endpoint attributes and their appropriate values depending on your requirement.

The following table lists the default Whitelist endpoint attributes:

AcsSessionID	AuthState	Calling-Station-ID
Certificate Expiration Date	Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description	DestinationIPAddress
Device Identifier	Device Name	DeviceRegistrationStatus
EapAuthentication	EapTunnel	EndPointPolicy
EndPointPolicyID	EndPointProfilerServer	EndPointSource
FQDN	FirstCollection	Framed-IP-Address
IdentityGroup	IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT	LastNmapScanTime
MACAddress	MatchedPolicy	MatchedPolicyID
MessageCode	NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type	NmapScanCount
NmapSubnetScanID	OS Version	OUI
PolicyVersion	PortalUser	PostureApplicable
Product	RegistrationTimeStamp	Service-Type
StaticAssignment	StaticGroupAssignment	TimeToProfile
Total Certainty Factor	User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId	cdpCachePlatform
cdpCacheVersion	ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name	hrDeviceDescr
ifIndex	ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription	operating-system
sysDescr	-	-

Configuring Endpoint Attribute Filter

You can globally configure endpoint attribute filtering in Cisco ISE.

Step 1 Choose **Administration > System > Settings**.

Step 2 In the Settings navigation pane, choose **Profiling**.

Step 3 Check the EndPoint Attribute Filter check box to enabled endpoint attribute filtering.

Step 4 Click **Save**.

Configuring the NetFlow Probe

Table 18-3 describes the fields that allow you to configure the NetFlow probe in the Edit Nodes page.

Table 18-3 NetFlow Configuration

Field	Description
The Enable check box	To enable the NetFlow probe on a node, check the **Enable** check box. To disable the NetFlow probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the NetFlow probe.

Cisco ISE profiler implements Cisco IOS NetFlow Version 9, and supports earlier versions that are beginning with Version 5. The MAC address is not a part of IP flows in earlier versions of NetFlow. This requires you to profile endpoints with their IP addresses by correlating the attributes information collected from the network access devices in the endpoints cache.

Cisco IOS NetFlow Version 9 is a proprietary Cisco product that allows you to access to IP flows on your network and export IP flows from the NetFlow-enabled network access devices. The Cisco IOS software allows NetFlow to export IP flows by using the UDP, a non congestion-aware protocol.

The basic output of NetFlow is a flow record and the most recent evolution of the flow record format is NetFlow Version 9. The distinguishing feature of NetFlow Version 9 is that the flow record format is based on a template. The template describes the flow record format, and the attributes of the fields (such as type and length) within the flow record. The template provides flexibility, and it is extensible to the flow record format, a format that allows future enhancements to the NetFlow services without requiring concurrent changes to the basic output. It provides the versatility needed to support new fields, and also record types. The templates cannot be stored in network access devices, and are refreshed every time from IP flows.

You can collect NetFlow Version 9 attributes from the NetFlow-enabled network access devices to create an endpoint, or update an existing endpoint in the Cisco ISE database. You can configure NetFlow Version 9 to attach the source and destination MAC addresses of endpoints and update them. You can also create a dictionary of NetFlow attributes to support NetFlow-based profiling.

If you have Cisco IOS NetFlow Version 9, the values of the ICMP_TYPE field are based on the PROTOCOL field in the NetFlow attributes collected by the NetFlow probe.

- If the value of the PROTOCOL field in the NetFlow attributes that are collected by the NetFlow probe is 6 (TCP) or 17 (UDP), then the value of the ICMP_TYPE field will always be equal to the value of the L4_DST_PORT field.
- If the value of the PROTOCOL field in the NetFlow attributes that are collected by the NetFlow probe is 1 (ICMP), then the value of the ICMP_TYPE field will be a combination of ICMP Type and ICMP code.

For more detailed information, see Table 6, NetFlow Version 9 Field Type Definitions of The NetFlow Version 9 Flow Record Format in the following link:

http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html

The following are the known attributes that are collected by the NetFlow probe:

IN_BYTES	IN_PKTS	FLOWS
PROTOCOL	SRC_TOS	TCP_FLAGS
L4_SRC_PORT	IPV4_SRC_ADDR	SRC_MASK
L4_DST_PORT	IPV4_DST_ADDR	DST_MASK
IPV4_NEXT_HOP	LAST_SWITCHED	FIRST_SWITCHED
OUT_BYTES	OUT_PKTS	IPV6_SRC_ADDR
IPV6_DST_ADDR	IPV6_SRC_MASK	IPV6_DST_MASK
IPV6_FLOW_LABEL	ICMP_TYPE	DST_TOS
IN_SRC_MAC	OUT_DST_MAC	SRC_VLAN
DST_VLAN	IP_PROTOCOL_VERSION	DIRECTION

Cisco IOS NetFlow Version 5

Cisco IOS NetFlow Version 5 packets do not contain MAC addresses of endpoints. The attributes that are collected from NetFlow Version 5 cannot be directly added to the Cisco ISE database. You can discover endpoints by using their IP addresses, and append the NetFlow Version 5 attributes to endpoints. However, these endpoints must have been previously discovered with the RADIUS or SNMP probe. It can be done by combining IP addresses of the network access devices, and IP addresses obtained from the NetFlow Version 5 attributes.

For more detailed information on the NetFlow Version 5 Record Format, see the following link:

http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html#wp1030618

To support the Cisco ISE profiling service, Cisco recommends using the latest version of NetFlow (Version 9), which has additional functionality needed to operate the profiler. If you use NetFlow Version 5 in your network, then you can use Version 5 only on the primary NAD at the access layer, as it will not work anywhere else.

The following are the known attributes that are collected by the NetFlow Version 5:

srcaddr	dstaddr	nexthop
input	output	first
last	srcport	dstport
tcp_flags	prot	flow_sequence
sys_uptime	—	—

Configuring the DHCP Probe

Table 18-4 describes the fields that allow you to configure the DHCP probe in the Edit Nodes page.

Table 18-4 DHCP Configuration

Field	Description
The Enable check box	To enable the DHCP probe on a node, check the **Enable** check box. To disable the DHCP probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the DHCP probe.

Dynamic Host Configuration Protocol (DHCP) is an auto configuration protocol, which is used on IP networks for allocating IP addresses dynamically, or statically. It provides reliability in several ways such as periodic renewal, rebinding, and failover in client-server communications. There are two versions of DHCP, one for IPv4, and one for IPv6. While both the versions bear the same name DHCP, and perform much the same purpose, the details of the DHCP protocol for IPv4 and IPv6 are sufficiently different that they can be considered as separate protocols.

A DHCP server manages a pool of IP addresses and information about client configuration parameters. In addition to allocating IP addresses, DHCP also provides other configuration information such as the subnet mask, default gateway, domain name, and name servers to DHCP clients on an IP network. DHCP clients that do not use DHCP for IP address configuration may still use it to obtain other configuration parameters.

DHCP uses the same UDP ports as defined for the BOOTP protocol by Internet Assigned Numbers Authority (IANA). DHCP messages are sent to the DHCP server UDP port 67 from a client to a server, and from a server to a client are sent to the DHCP client UDP port 68. As DHCP communications are connectionless, DHCP clients and servers on the same subnet communicate by using UDP broadcasts. If they are on different subnets, then the clients send DHCP discovery, and request messages by using UDP broadcasts, but receive DHCP lease offer, and acknowledgement messages by unicast.

A DHCP server processes the following incoming DHCP messages from a DHCP client based on the current state of the binding for that client: DHCPDISCOVER, DHCPREQUEST, and also such as DHCPDECLINE, DHCPRELEASE, and DHCPINFORM. A DHCP server responds to the client with the following DHCP messages: DHCPOFFER, DHCPACK, and also such as DHCPNAK.

DHCPDISCOVER—A message that a DHCP client broadcasts to locate available DHCP servers

DHCPOFFER—A message that a DHCP server sends to DHCP clients in response to discovery messages with an offer for client configuration parameters

DHCPREQUEST—A message that a DHCP client sends to DHCP servers either requesting the offered parameters from one server, and implicitly declining offers from all others, or confirming correctness of previously allocated address after a system reboot, or extending the lease on a particular network address.

DHCPACK—A message that a DHCP server sends to DHCP clients with configuration parameters, including committed network addresses.

The DHCP probe in your Cisco ISE deployment, when enabled, allows the Cisco ISE profiling service to re-profile endpoints based only on new requests of INIT-REBOOT, and SELECTING message types. Though other DHCP message types are processed such as RENEWING, and REBINDING, they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

DHCPREQUEST Generated During INIT-REBOOT State:

If the DHCP client checks to verify a previously allocated and cached configuration, then the client must not fill in the Server identifier (server-ip) option, but fill in the Requested IP address (requested-ip) option with its notion of the previously assigned IP address, and fill in the 'ciaddr' (client's network address) field with zero in its DHCPREQUEST message. The DHCP server sends a DHCPNAK message to the client, if the requested IP address is incorrect, or the client is located in the wrong network.

DHCPREQUEST Generated During SELECTING State:

The DHCP client inserts the IP address of the selected DHCP server in the Server identifier option, fill in the Requested IP address (requested-ip) option with the 'yiaddr' field value from the chosen DHCPOFFER by the client, and fill in the 'ciaddr' field with zero in its DHCPREQUEST message.

Table 18-5 describes the different states of DHCP client messages. For more information on DHCP, refer to www.faqs.org/rafts/rfc2131.html.

Table 18-5 DHCP Client Messages from Different States

	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

DHCP IP Helper

DHCP clients send out discovery messages (broadcast) to locate a DHCP server on a network, and in the process, these messages are relayed to the remote DHCP servers as unicast. When DHCP clients and servers are not located in the same subnet, you can configure the network access devices on your network by using the "ip helper-address x.x.x.x" command along with the IP addresses of DHCP servers. This helps the Cisco ISE profiler to receive DHCP packets from one or more interfaces, and parse them to capture endpoint attributes, which can be used for profiling.

For example,

```
Router(config-if)#ip helper-address x.x.x.x
```

You can create a profiling condition of DHCP type, where you can use the dhcp-requested-address attribute for profiling an endpoint. For a fully qualified domain name (FQDN) lookup, the Domain System Name (DNS) probe extracts the source IP address from the dhcp-requested-address attribute, which is collected by the DHCP

Wireless LAN Controller Configuration

Cisco recommends that you configure WLCs in DHCP bridging mode, where you can forward all the DHCP packets from the wireless clients to Cisco ISE. You must also ensure that the DHCP IP helper command points to the Cisco ISE Policy Service node.

You must uncheck the Enable DHCP Proxy check box in the WLCs by using the WLC web interface: **Controller > Advanced > DHCP Master Controller Mode > DHCP Parameters > Enable DHCP proxy**.

Configuring the DHCP SPAN Probe

Table 18-6 describes the fields that allow you to configure the DHCP SPAN probe in the Edit Nodes page.

Table 18-6 DHCP SPAN Configuration

Field	Description
The Enable check box	To enable the DHCP SPAN probe on a node, check the **Enable** check box. To disable the DHCP SPAN probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Description	The description of the DHCP SPAN probe.

DHCP Switched Port Analyzer (SPAN) probe, when initialized on a Cisco ISE node, listens to network traffic, which are coming from network access devices on a specific interface. You need to configure network access devices to forward DHCP SPAN packets to the Cisco ISE profiler from the DHCP servers. The profiler receives these DHCP SPAN packets and parses them to capture the attributes of an endpoint, which can be used for profiling endpoints.

You can create a profiling condition of DHCP type, where you can use the dhcp-requested-address attribute for profiling an endpoint. For a FQDN lookup, the Domain System Name (DNS) probe extracts the source IP address from the dhcp-requested-address attribute, which is collected by the DHCP SPAN probe.

Configuring the HTTP Probe

Table 18-7 describes the fields that allow you to configure the HTTP probe in the Edit Nodes page.

Table 18-7 HTTP Configuration

Field	Description
The Enable check box	To enable the HTTP probe on a node, check the **Enable** check box. To disable the HTTP probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose an interface.
Description	The description of the HTTP probe.

Hypertext Transfer Protocol (HTTP) is an application layer protocol, which is designed within the framework of the Internet Protocol Suite. It is a generic, stateless, protocol which can be used in distributed object management systems beyond its use for hypertext. It functions as a request-response protocol, which is widely used for communications within distributed client-server architectures. A web browser is a client application (often referred as user agent), which implements HTTP originating an HTTP request message. When the web browser operates, it typically identifies itself, its application type, operating system, software vendor, and software revision by submitting a characteristic identification string to its operating peer. In HTTP, this is transmitted in an HTTP request-header field User-Agent.

The User-Agent is an attribute, which can be used to create a profiling condition of IP type, and check the web browser information. The profiler captures the web browser information from the User-Agent attribute, as well as other HTTP attributes from the request messages, and add them to the list of endpoint attributes. Cisco ISE provides many default profiles, which are built into the system to identify endpoints based on the User-Agent attribute.

HTTP SPAN Probe

An HTTP session is a sequence of network request-response transactions. The web browser initiates an HTTP request message, which establishes a Transmission Control Protocol (TCP) connection to a particular port on the web server (typically port 80). A web server listening on that port waits for the HTTP request message from the web browsers. The HTTP probe in your Cisco ISE deployment, when enabled with the SPAN probe, allows the profiler to capture HTTP packets from the specified interfaces. You can use the SPAN capability on port 80, where the Cisco ISE server listens to communication from the web browsers.

HTTP Switched Port Analyzer (SPAN) collects HTTP attributes of an HTTP request-header message along with the IP addresses in the IP header (L3 header), which can be associated to an endpoint based on the MAC address of an endpoint in the L2 header. This information is useful for identifying different mobile and portable IP enabled devices such as Apple devices, as well as computers with different operating systems. Identifying different mobile and portable IP enabled devices is now made more reliable by having the Cisco ISE server redirect capture during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute, as well as other HTTP attributes, from the request messages and then identify devices such as Apple devices. The Cisco ISE server listens to communication from the web browsers on both port 80, as well as port 8080.

You can create a profiling condition of IP type, where you can use the IP attribute to capture the source IP address of the web browser. For an FQDN lookup, the Domain System Name (DNS) probe extracts the source IP address from the IP attribute, which is collected by the HTTP SPAN probe.

Cisco ISE Profiler Does Not Collect HTTP Traffic When the Profiler Is Running On VMware

If you deploy Cisco ISE on an ESX server (VMware), the Cisco ISE profiler collects the DHCP traffic but does not collect the HTTP traffic due to configuration issues on the vSphere client.

To collect HTTP traffic on a VMware setup, you have to configure the security settings by changing the Promiscuous Mode to Accept from Reject (by default) of the virtual switch that you create for the Cisco ISE profiler. When the SPAN probe for DHCP and HTTP are enabled, Cisco ISE profiler collects both the DHCP and HTTP traffic.

Configuring the RADIUS Probe

Table 18-8 describes the fields that allow you to configure the RADIUS probe in the Edit Nodes page.

Table 18-8 RADIUS Configuration

Field	Description
The Enable check box	To enable the RADIUS probe on a node, check the **Enable** check box. To disable the RADIUS probe on a node, uncheck the **Enable** check box.
Description	The description of the RADIUS probe.

RADIUS is an application layer protocol, which is used in client-server communication. It provides centralized Authentication, Authorization and Accounting (AAA) management for authentication and authorization of users, or devices before granting them access to network services, and also accounting for usage of network services. It supports a variety of methods for user authentication by using a username and password. RADIUS is an extensible protocol, where all the client-server transactions comprise of variable length attribute-value pairs (AVPs), and also new attribute-value pairs can be added without disturbing existing implementations of the protocol. The attribute-value pairs carry data in both the RADIUS request and response messages for authentication, authorization, and accounting transactions.

A Network Access Server (NAS) functions as a client of RADIUS, which provides user credentials to a RADIUS server. The RADIUS server returns configuration information necessary for NAS to deliver requested services to the user. Cisco ISE can function as a RADIUS server, as well as a RADIUS proxy client to other RADIUS servers. When it acts as a proxy client, it uses external RADIUS servers to process RADIUS requests and response messages. You can configure Cisco ISE for authentication with RADIUS, where you can define a shared secret that you can use in client-server transactions. For more information on Cisco ISE network device configuration, see Chapter 6, "Managing Network Devices."

With the RADIUS request and response messages received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints.

You can create a profiling condition of RADIUS type, where you can use the Framed-IP-Address attribute for profiling an endpoint. For an FQDN lookup, the Domain System Name (DNS) probe extracts the source IP address from the Framed-IP-Address attribute, which is collected by the RADIUS probe.

For a list of attributes and RADIUS RFCs, refer to http://en.wikipedia.org/wiki/RADIUS.

The following are the known attributes that are collected by the RADIUS probe:

User-Name	NAS-IP-Address	NAS-Port	Framed-IP-Address
Calling-Station-Id	Acct-Session-Id	Acct-Session-Time	Acct-Terminate-Cause

Configuring the Network Scan (NMAP) Probe

Table 18-9 describes the fields that allow you to configure the Network Scan (NMAP) probe in the Edit Nodes page.

To enable the Network Scan probe, configure the following fields:

Table 18-9 Network Scan Configuration

Field	Description
The Enable check box	To enable the Network Scan probe in the Policy Service ISE node, check the **Enable** check box. To disable the Network Scan probe in the Policy Service ISE node, uncheck the **Enable** check box.
Description	The description of the Network Scan probe.

Table 18-9 Network Scan Configuration

Field	Description
Manual Scan Subnet	Enter a valid subnet format to initiate a subnet scan manually. If you enter an invalid subnet format like 10.0.10.10 in the Manual Scan Subnet field, Cisco ISE displays the following error message: "Invalid Subnet: 10.0.10.10. Enter a valid subnet format, such as: 10.0.10.10/24 and 10.0.10.10/32." It is active and available for you to enter the subnet only when you enable the Network Scan probe in the Edit Nodes page to run the manual scan.
Run Scan	Click the **Run Scan** button to start a manual subnet scan. It is only active before you initiate to run the subnet scan manually.
Cancel Scan	Click the **Cancel Scan** button to stop a manual subnet scan. It is only active while the manual subnet scan is running.
Click to see latest scan results link	Click the **Click to see latest scan results** link, which redirects you to Administration > Identities > Identities. Choose **Latest Network Scan Results.** to view the most recently detected endpoints.

When you initiate a subnet scan, the NMAP probe scans the specified subnet and detect endpoints and their operating systems when SNMP ports (UDP 161 and 162) are open in the endpoint.

The following NMAP command scans a subnet:

nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>

Table 18-10 NMAP Commands for a Subnet Scan

-O	Enables OS detection
-sU	UDP scan
-p <port ranges>	Scans only specified ports. For example, U:161, 162
oN	Normal output
oX	XML output

A Network Scan

A network scan is a very specific way to scan a subnet on your network, by using the Network Scan probe to run from the Policy Service ISE nodes. The network scan allows you to detect endpoints on a specified subnet, their operating systems, and SNMP ports (UDP 161 and 162) in any distributed deployment.

Cisco ISE displays a message that running a network scan on a specified subnet is a lengthy procedure, as it depends on the size and density of the subnet. Also scanning a subnet is highly resource intensive. You can also cancel a subnet scan at any time while the subnet scan is in progress. The number of active scans is always restricted to one scan, and so you can scan only a single subnet at a time.

Each subnet scan has a unique numeric ID that is used to update an endpoint source information with that scan ID. Upon detection, the endpoint source information can also be updated to indicate that it is discovered by the Network Scan probe.

The network scan is augmented with an SNMP Query whenever the scan discovers that UDP port 161 is open on an endpoint. This SNMP Query can result in more attributes being collected for greater classification accuracy. The SNMP Query uses the default community string settings (public), which allows you to collect additional attributes such as the system description, and others.

Depending on the location of the subnet that you are scanning, the Network Scan may or may not return the MAC addresses of endpoints. The Network Scan may not be able to resolve MAC addresses for those endpoints, as an ARP resolution is entirely dependent on the network topology and the subnet being scanned which is away from the Policy Services ISE node. Having implemented an IP-MAC binding, Cisco ISE must be able to resolve their MAC addresses for those endpoints from the IP addresses received. If they are not resolved to MAC addresses, then there is no way to map those IP addresses to actual endpoints, and they are dropped.

The NMAP manual subnet scan requires the MAC address of an endpoint in order to add the endpoint to the database, as the MAC address is the unique identifier for all the endpoints.

The following limitations do not apply to dynamic endpoints that join the Cisco ISE network, as they are authenticated, and assigned to an IP address dynamically, and those endpoints are detected by the profiling service through the RADIUS and DHCP probes.

Cisco ISE enables you to detect devices, by using the NMAP manual subnet scan. The manual subnet is useful to detect devices that are constantly connected to the ISE network with a static IP address assigned to them, such as printers, and therefore those devices cannot be discovered by other probes.

Scanned devices are added to the endpoints list, only if the IP address to the MAC address binding exists. During the manual subnet scan, the NMAP probe detects whether the SNMP port 161 is open on the device. If the port is open, an SNMP Query is triggered with a default community string (public). If the device supports SNMP and the default community string is set to public, you can obtain the MAC address of the device from the MIB value “ifPhysAddress”.

When scanning a subnet that is not adjacent to the Policy Service node, but contains devices in the subnet that do not support SNMP, then you have to define the NAD that resides in the subnet in the Cisco ISE administrator user interface. You must also enable the SNMP probe in the Policy Service node in order to retrieve the ARP table from the NAD that provides the IP address to MAC address binding for those endpoints that are scanned in the subnet.

If there is a L2 adjacency to the Policy Service node that performs the manual subnet scan, the NMAP scan can detect the MAC address, and add the endpoints to Cisco ISE.

For an iDevice, and other devices that do not support SNMP, the MAC address can be discovered by the ARP table, which can be queried from the network access device (NAD) by an SNMP Query probe. iDevices can also be profiled using DHCP.

Latest Network Scan Results

The most recent network scan results are stored in **Administration > Identities > Identities (menu window) > Latest Network Scan Results**.

For more information on the latest network scan results, see the section on Latest Network Scan Results, page 4-27.

For more information on the manual network scan, see Chapter 18, “Configuring the Network Scan (NMAP) Probe.”

Configuring the DNS Probe

Table 18-11 describes the fields that allow you to configure the DNS probe in the Edit Nodes page.

Table 18-11 DNS Configuration

Field	Description
The Enable check box	To enable the DNS probe on a node, check the **Enable** check box. To disable the DNS probe on a node, uncheck the **Enable** check box.
Timeout	Enter the timeout in seconds.
Description	The description of the DNS probe.

Note For the DNS probe to work on a particular ISE node in a distributed deployment, you must enable any one of the following probes: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For a DNS lookup, one of the probes mentioned above must be started along with the DNS probe.

When you deploy Cisco ISE in a standalone, or in a distributed environment for the first time, you are prompted to run the setup utility to configure the Cisco ISE appliance. Here, you will configure the Domain Name System (DNS) domain and the primary nameserver (primary DNS server), where you can configure one primary nameserver, and one or more nameservers during setup. You can also change, or add DNS nameservers later after deploying Cisco ISE using the CLI commands.

For more information on the CLI commands, refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x.*

The DNS probe in your Cisco ISE deployment, when enabled, allows the profiler to lookup an endpoint, and get the fully qualified domain name (FQDN) of that endpoint. A DNS lookup tries to determine the endpoint fully qualified domain name. Upon an endpoint detection on your Cisco ISE enabled network, a list of endpoint attributes is collected from the NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP probes. For a DNS lookup, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP.

The following list shows the specific endpoint attribute, and the probe that collects the attribute:

- The dhcp-requested-address attribute—an attribute collected by the DHCP, and DHCP SPAN probes
- The SourceIP attribute—an attribute collected by the HTTP probe
- The Framed-IP-Address attribute—an attribute collected by the RADIUS probe
- The cdpCacheAddress attribute—an attribute collected by the SNMP probe

This allows the DNS probe in the profiler to do a reverse DNS lookup (FQDN lookup) against specified name servers that you define in your Cisco ISE deployment. A new attribute is added to the attribute list for an endpoint, which can be used for an endpoint profiling policy evaluation. The FQDN is the new attribute, which exists in the system IP dictionary. You can create an endpoint profiling condition to validate the FQDN attribute, and its value for profiling.

Inline Posture Deployment in Bridged Mode and DNS Probe

For more information on Inline Posture deployment, see Chapter 10, “Setting Up Inline Posture.”

For DNS probe to work with Inline Posture deployment in the Bridged mode, you must ensure that you configure the callStationIdType information sent in RADIUS messages for the Wireless LAN Controllers (WLC). The WLCs need to be configured to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages. Once configured in the WLCs,

this configuration uses the selected calling station ID for communications with RADIUS servers and other applications. It results in endpoints authentication, and then the DNS probe to do a reverse DNS lookup (FQDN lookup) against the specified name servers, and update the FQDN of endpoints.

Wireless LAN Controller GUI Configuration

You can use the WLC web interface to configure the Call Station ID Type information. You can go to the Security tab of the WLC web interface, and choose RADIUS > Authentication from AAA. Here, you can configure the System MAC Address from the drop-down list to the Call Station ID Type on the RADIUS Authentication Servers page. The MAC Delimiter field is set to Colon by default.

For more information on various WLC GUI configuration, refer to the Using the GUI to Configure RADIUS section (Chapter 6, "Configuring Security Solutions") in the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*.

Wireless LAN Controller CLI Configuration

You can use the config radius callStationIdType command with the macAddr option in the command-line interface (CLI) for the Wireless LAN Controllers.

For more information on WLC CLI configuration, refer to the config radius callStationIdType command (Chapter 2, "CLI Commands") in the *Cisco Wireless LAN Controller Command Reference, Release 7.0.*

For example, you can go to the configuration mode for the WLCs, and enter the following command:

config radius callStationIdType {ipAddr | macAddr | ap-macAddr-only | ap-macAddr-ssid}

Syntax Description

config	Configure parameters.
radius callStationIdType	Configure callStationIdType information.
{ipAddr | macAddr | ap-macAddr-only | ap-macaddr-ssid}	• Enter ipAddr to configure Call Station ID type to IP address (only layer 3) • Enter macAddr to configure Call Station ID type to the system's MAC address (layers 2 and 3) • Enter ap-macAddr-only to configure Call Station ID type to use the access point's MAC address (layers 2 and 3) • Enter as-macAddr-ssid to config Call Station ID type to use the access point's MAC address with SSID

Command Modes

Configuration.

Usage Guidelines

The Framed-IP-Address attribute in RADIUS messages does not contain the Call Station ID type in the MAC address format. Therefore, RADIUS messages cannot be associated with the MAC address of endpoints, and the DNS probe is unable to perform the reverse DNS lookup. In order to profile endpoints, you must enable the RADIUS, and DNS probes in Cisco ISE, and then configure the WLCs to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages.

Examples `config radius callStationIdType macAddr`

Configuring the SNMP Query Probe

Table 18-12 describes the fields that allow you to configure the SNMP Query probe in the Edit Nodes page.

Table 18-12 SNMP Query Configuration

Field	Description
The Enable check box	To enable the SNMP Query probe on a node, check the **Enable** check box. To disable the SNMP Query probe on a node, uncheck the **Enable** check box.
Retries	Enter the number of retry attempts allowed**.**
Timeout	Enter the timeout in seconds.
EventTimeout	Enter the SNMP event timeout in seconds.
Description	The description of the SNMP Query probe.

For more information on SNMP, see the "Simple Network Management Protocol" section on page 18-32.

From the Network Devices list page, you can configure new network devices where SNMP settings can also be configured. The polling interval that you specify here query network access devices at regular intervals. In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in the following location:

Administration > Network Resources > Network Devices.

You can turn on and turn off SNMP querying for specific NADs based on the following configurations:

- SNMP Query on Link up and New MAC notification turned on or turned off
- CDP SNMP Query on Link up and New MAC notification turned on or turned off
- SNMP Query timer for once an hour for each switch by default

Note When you configure SNMP settings on the network devices, you must ensure that the Cisco Device Protocol (CDP) is enabled (by default) on all the ports of the network devices. If you disable CDP on any of the ports on the network devices, then you may not be able to profile properly as you will miss the CDP information of all the connected endpoints. You must also ensure that the Link Layer Discovery Protocol (LLDP) is running on all the ports of the network devices.

CDP Attributes Collection

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network.

You must enable CDP globally by using the **cdp run** command on a network device, and enable CDP by using the **cdp enable** command on any interface of the network access device. To disable CDP on the network device and on the interface, use the **no** keyword at the beginning of the command.

LLDP Attributes Collection

IEEE 802.1AB Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol that runs over Layer 2 (the data link layer), which allows two systems running different network layer protocols to learn about each other. LLDP is used for network devices to advertise information about themselves to other devices on the network. A switch that supports the IEEE 802.1AB LLDP provides support to devices that are not cisco devices, and it allows for inter operability between other devices.

The Cisco ISE profiler has enhanced data collection capabilities, because it uses an SNMP Query to collect LLDP attributes. You can also collect LLDP attributes from an IOS sensor, which is embedded in the network device by using the RADIUS probe.

You must enable LLDP globally to allow a device to send LLDP packets, by using the **lldp run** command on a network device, but no changes are required at the interface level. You can also configure any interface to send and receive LLDP packets, by using the **lldp transmit** and **lldp receive** commands. To disable LLDP on the network device and on the interface, use the **no** keyword at the beginning of the command.

To change the default LLDP settings, use the LLDP global configuration and LLDP interface configuration commands on the network access devices.

Table 18-13 shows the default LLDP configuration.

Table 18-13 Default LLDP Configuration

Feature	Feature
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Enabled to send and receive all TLVs.
LLDP interface state	Enabled
LLDP receive	Enabled
LLDP transmit	Enabled
LLDP med-tlv-select	Enabled to send all LLDP-MED TLVs

The **Attribute List** of an endpoint displays a single character value for lldpCacheCapabilities and lldpCapabilitiesMapSupported attributes. The values are the Capability Codes that are displayed for the network access device that runs cdp and lldp.

Example1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

Example2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

Example 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
```

```
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

LLDP-MIB (v1)

For more information, see LLDP-MIB (v1). LLDP-MIB (v1) is MIB that was recently added to the existing list of supported MIBs for an SNMP Query.

The local attributes are collected once during an SNMP Query as a result of polling LLDP capable local network devices. The remote attributes are tabular, and they correspond to each LLDP capable remote device that is attached to the local network device. These attributes are collected during an SNMP Query as a result of polling the MIB, as well as when a notification is received through traps or a RADIUS Accounting Start message (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value “start”).

The Cisco ISE profiler reads all the remote attributes of LLDP capable network devices and associates them to the local attributes by using MIB data when creating endpoints.

For example, Cisco ISE creates an endpoint when it reads the lldpRemSysName (a remote attribute) of an endpoint and associates it to lldpLocSysName (a local attribute) that represents its own system name attribute.

The following are the local attributes that are collected from the lldpLocalSystemData group:

lldpLocalSystemData group(1.0.8802.1.1.2.1.3)—refers to iso(1). std(0). iso8802(8802). ieee802dot1(1). ieee802dot1mibs(1). lldpMIB(2). lldpObjects(1). lldpLocalSystemData(3)

lldpLocSysCapSupported	1.0.8802.1.1.2.1.3.5.0
lldpLocSysCapEnabled	1.0.8802.1.1.2.1.3.6.0

The following are the remote attributes that are collected from the lldpRemoteSystemsData group that refers to the attributes of LLDP capable remote network devices:

lldpRemoteSystemsData group(1.0.8802.1.1.2.1.4)—refers to iso(1). std(0). iso8802(8802). ieee802dot1(1). ieee802dot1mibs(1). lldpMIB(2). lldpObjects(1). lldpRemoteSystemsData(4)

lldpRemPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpRemPortDesc	1.0.8802.1.1.2.1.4.1.1.8
lldpRemSysName	1.0.8802.1.1.2.1.4.1.1.9
lldpRemSysDesc	1.0.8802.1.1.2.1.4.1.1.10
lldpRemSysCapSupported	1.0.8802.1.1.2.1.4.1.1.11
ldpRemSysCapEnabled	1.0.8802.1.1.2.1.4.1.1.12

Configuring the SNMP Trap Probe

Table 18-14 describes the fields that allow you to configure the SNMP Trap probe in the Edit Nodes page.

Table 18-14 SNMP Trap Configuration

Field	Description
The Enable check box	To enable the SNMP Trap probe on a node, check the **Enable** check box. To disable the SNMP Trap probe on a node, uncheck the **Enable** check box.
Link Trap Query check box	To receive and interpret the linkup and linkdown notifications received through the SNMP Trap, check the **Link Trap Query** check box.
MAC Trap Query check box	To receive and interpret MAC notifications received through the SNMP Trap, check the **MAC Trap Query** check box.
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the SNMP Trap probe.

The SNMP Trap receives information from the specific NADs that support MAC notification, linkup, linkdown, and informs. For SNMP Trap to be fully functional, you must enable SNMP Query also. The SNMP Trap probe receives information from the specific NADs when ports come up or go down and endpoints disconnect or connect to your network. The information received is not sufficient to create endpoints in Cisco ISE.

Note Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

For more information on supported MIBs in Cisco ISE, refer to the SNMP OID Mapping, page 18-33.

For SNMP Trap probe has to be fully functional and create endpoints in Cisco ISE, the SNMP Query must also be enabled so that the SNMP Query probe triggers a poll event on the particular port of the NAD when a trap is received. To make this feature to be fully functional you should configure the NAD and SNMP Trap.

For more information on configuring network devices, see Chapter 6, “Managing Network Devices.”

To configure the NAD, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the name of the network device.

Step 4 Enter the description of the network device.

Step 5 Check the **SNMP Settings** check box.

Step 6 Choose the SNMP version (mandatory field) from the drop-down list.

You can choose SNMP Version 1, 2c, or 3.

Step 7 Configure other mandatory SNMP settings as required depending on the SNMP version you choose.

Step 8 From the **Polling interval** field (mandatory field), enter the SNMP polling interval in seconds.

Step 9 Check the Link Trap Query check box.

Step 10 Check the MAC Trap Query check box.

Step 11 Click **Summit**.

To configure the SNMP Trap, complete the following steps:

Step 1 Choose **Administration > System > Deployment > Deployment Nodes > Edit Node > Profiling Configuration**.

Step 2 Check the Link Trap Query check box.

Step 3 Check the MAC Trap Query check box.

Step 4 Choose the Interface from the drop-down list.

For example, GigabitEthernet 0.

Step 5 Enter the Port number.

For example, 162.

Step 6 Enter the description of the SNMP Trap.

For example, SNMP TRAP.

Step 7 Click **Save**.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. It is used mostly in network-management systems (NMS) to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed devices, which describe the system configuration. These variables can be queried, and at sometimes can also be set by the managing applications. SNMP permits active network management tasks such as modifying, and applying new configurations through remote modification of these variables. These variables, which are accessible via SNMP are all organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable) are described by Management Information Bases (MIBs). A MIB is a virtual database and the database is hierarchical (tree-structured). The entries are addressed through object identifiers (OID). An object identifier (or object ID or OID) uniquely identifies a managed object in the MIB hierarchy. The managed object (sometimes called a MIB object, or an object, or a MIB) is one of any number of the special characteristics of the managed device. Managed objects are made up of one or more object instances (identified by their OIDs), which are essentially variables.

For more information, refer to RFC 1155, “Structure and Identification of Management Information for TCP/IP based internets”, and its two companions, RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, “A Simple Network Management Protocol.”

For a network-management system to understand a trap sent to it by an agent, the management system must know what the object identifier (OID) defines. It must have the MIB for that trap loaded. This provides the correct OID information so that the network-management system can understand the traps sent to it.

1.3.6.1.2.1 is the base OID for MIB-2 defined SNMP variables, and 1.3.6.1.4.1 is the base OID for IANA-registered Private Enterprises, and IEEE8021-PAE-MIB: RFC IEEE 802.1X for managing IEEE 802.1X.

For more information on supported MIBs in Cisco ISE, refer to the SNMP OID Mapping, page 18-33.

An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs using SNMP. Sometimes called network elements, these managed devices can include, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information, and translates this information into a form compatible with SNMP.

An NMS executes applications, which monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network-management. One or more NMSs must exist on any managed network.

SNMP OID Mapping

#IF-MIB
1.3.6.1.2.1.2.2.1.1=ifIndex
1.3.6.1.2.1.2.2.1.2=ifDescr
1.3.6.1.2.1.2.2.1.3=ifType
1.3.6.1.2.1.2.2.1.5=ifSpeed
1.3.6.1.2.1.2.2.1.6=ifPhysAddress
1.3.6.1.2.1.2.2.1.7=ifAdminStatus
1.3.6.1.2.1.2.2.1.8=ifOperStatus

#SNMPv2-MIB
1.3.6.1.2.1.1=system
1.3.6.1.2.1.1.1.0=sysDescr
1.3.6.1.2.1.1.2.0=sysObjectID
1.3.6.1.2.1.1.3.0=sysUpTime
1.3.6.1.2.1.1.4.0=sysContact
1.3.6.1.2.1.1.5.0=sysName
1.3.6.1.2.1.1.6.0=sysLocation
1.3.6.1.2.1.1.7.0=sysServices
1.3.6.1.2.1.1.8.0=sysORLastChange
1.3.6.1.2.1.1.9.0=sysORTable

#IP-MIB
1.3.6.1.2.1.4.20.1.2=ipAdEntIfIndex
1.3.6.1.2.1.4.20.1.3=ipAdEntNetMask
1.3.6.1.2.1.4.22.1.2=ipNetToMediaPhysAddress

#CISCO-CDP-MIB
1.3.6.1.4.1.9.9.23.1.2.1.1=cdpCacheEntry
1.3.6.1.4.1.9.9.23.1.2.1.1.1=cdpCacheIfIndex
1.3.6.1.4.1.9.9.23.1.2.1.1.2=cdpCacheDeviceIndex
1.3.6.1.4.1.9.9.23.1.2.1.1.3=cdpCacheAddressType
1.3.6.1.4.1.9.9.23.1.2.1.1.4=cdpCacheAddress
1.3.6.1.4.1.9.9.23.1.2.1.1.5=cdpCacheVersion
1.3.6.1.4.1.9.9.23.1.2.1.1.6=cdpCacheDeviceId
1.3.6.1.4.1.9.9.23.1.2.1.1.7=cdpCacheDevicePort
1.3.6.1.4.1.9.9.23.1.2.1.1.8=cdpCachePlatform
1.3.6.1.4.1.9.9.23.1.2.1.1.9=cdpCacheCapabilities
1.3.6.1.4.1.9.9.23.1.2.1.1.10=cdpCacheVTPMgmtDomain
1.3.6.1.4.1.9.9.23.1.2.1.1.11=cdpCacheNativeVLAN
1.3.6.1.4.1.9.9.23.1.2.1.1.12=cdpCacheDuplex
1.3.6.1.4.1.9.9.23.1.2.1.1.13=cdpCacheApplianceID
1.3.6.1.4.1.9.9.23.1.2.1.1.14=cdpCacheVlanID
1.3.6.1.4.1.9.9.23.1.2.1.1.15=cdpCachePowerConsumption
1.3.6.1.4.1.9.9.23.1.2.1.1.16=cdpCacheMTU
1.3.6.1.4.1.9.9.23.1.2.1.1.17=cdpCacheSysName
1.3.6.1.4.1.9.9.23.1.2.1.1.18=cdpCacheSysObjectID
1.3.6.1.4.1.9.9.23.1.2.1.1.19=cdpCachePrimaryMgmtAddrType
1.3.6.1.4.1.9.9.23.1.2.1.1.20=cdpCachePrimaryMgmtAddr
1.3.6.1.4.1.9.9.23.1.2.1.1.21=cdpCacheSecondaryMgmtAddrType
1.3.6.1.4.1.9.9.23.1.2.1.1.22=cdpCacheSecondaryMgmtAddr
1.3.6.1.4.1.9.9.23.1.2.1.1.23=cdpCachePhysLocation
1.3.6.1.4.1.9.9.23.1.2.1.1.24=cdpCacheLastChange

# CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.3.1.1.18.1=vtpVlanIfIndex
1.3.6.1.4.1.9.9.46.1.3.1.1.4.1=vtpVlanName
1.3.6.1.4.1.9.9.46.1.3.1.1.2.1=vtpVlanState

# CISCO-STACK-MIB
1.3.6.1.4.1.9.5.1.4.1.1.11=portIfIndex
1.3.6.1.4.1.9.5.1.9.3.1.3.1=vlanPortVlan

# BRIDGE-MIB
1.3.6.1.2.1.17.4.3.1.2=dot1dTpFdbPort
1.3.6.1.2.1.17.1.4.1.2=dot1dBasePortIfIndex

# OLD-CISCO-INTERFACE-MIB
1.3.6.1.4.1.9.2.2.1.1.20=locIfReason

# CISCO-LWAPP-AP-MIB
1.3.6.1.4.1.9.9.513.1.1.1=cLApEntry
1.3.6.1.4.1.9.9.513.1.1.1.1.1=cLApSysMacAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.2=cLApIfMacAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.3=cLApMaxNumberOfDot11Slots
1.3.6.1.4.1.9.9.513.1.1.1.1.4=cLApEntPhysicalIndex
1.3.6.1.4.1.9.9.513.1.1.1.1.5=cLApName
1.3.6.1.4.1.9.9.513.1.1.1.1.6=cLApUpTime
1.3.6.1.4.1.9.9.513.1.1.1.1.7=cLLwappUpTime
1.3.6.1.4.1.9.9.513.1.1.1.1.8=cLLwappJoinTakenTime
1.3.6.1.4.1.9.9.513.1.1.1.1.9=cLApMaxNumberOfEthernetSlots
1.3.6.1.4.1.9.9.513.1.1.1.1.10=cLApPrimaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.11=cLApPrimaryControllerAddress

1.3.6.1.4.1.9.9.513.1.1.1.1.12=cLApSecondaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.13=cLApSecondaryControllerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.14=cLApTertiaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.15=cLApTertiaryControllerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.16=cLApLastRebootReason
1.3.6.1.4.1.9.9.513.1.1.1.1.17=cLApEncryptionEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.18=cLApFailoverPriority
1.3.6.1.4.1.9.9.513.1.1.1.1.19=cLApPowerStatus
1.3.6.1.4.1.9.9.513.1.1.1.1.20=cLApTelnetEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.21=cLApSshEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.22=cLApPreStdStateEnabled
1.3.6.1.4.1.9.9.513.1.1.1.1.23=cLApPwrInjectorStateEnabled
1.3.6.1.4.1.9.9.513.1.1.1.1.24=cLApPwrInjectorSelection
1.3.6.1.4.1.9.9.513.1.1.1.1.25=cLApPwrInjectorSwMacAddr
1.3.6.1.4.1.9.9.513.1.1.1.1.26=cLApWipsEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.27=cLApMonitorModeOptimization
1.3.6.1.4.1.9.9.513.1.1.1.1.28=cLApDomainName
1.3.6.1.4.1.9.9.513.1.1.1.1.29=cLApNameServerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.30=cLApNameServerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.31=cLApAMSDUEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.32=cLApEncryptionSupported
1.3.6.1.4.1.9.9.513.1.1.1.1.33=cLApRogueDetectionEnabled

# CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1=cldcClientEntry
1.3.6.1.4.1.9.9.599.1.3.1.1.1=cldcClientMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.2=cldcClientStatus
1.3.6.1.4.1.9.9.599.1.3.1.1.3=cldcClientWlanProfileName
1.3.6.1.4.1.9.9.599.1.3.1.1.4=cldcClientWgbStatus
1.3.6.1.4.1.9.9.599.1.3.1.1.5=cldcClientWgbMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.6=cldcClientProtocol
1.3.6.1.4.1.9.9.599.1.3.1.1.7=cldcAssociationMode
1.3.6.1.4.1.9.9.599.1.3.1.1.8=cldcApMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.9=cldcIfType
1.3.6.1.4.1.9.9.599.1.3.1.1.10=cldcClientIPAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.11=cldcClientNacState
1.3.6.1.4.1.9.9.599.1.3.1.1.12=cldcClientQuarantineVLAN
1.3.6.1.4.1.9.9.599.1.3.1.1.13=cldcClientAccessVLAN
1.3.6.1.4.1.9.9.599.1.3.1.1.14=cldcClientLoginTime
1.3.6.1.4.1.9.9.599.1.3.1.1.15=cldcClientUpTime
1.3.6.1.4.1.9.9.599.1.3.1.1.16=cldcClientPowerSaveMode
1.3.6.1.4.1.9.9.599.1.3.1.1.17=cldcClientCurrentTxRateSet
1.3.6.1.4.1.9.9.599.1.3.1.1.18=cldcClientDataRateSet

# CISCO-AUTH-FRAMEWORK-MIB
1.3.6.1.4.1.9.9.656.1.2.1.1=cafPortConfigEntry
1.3.6.1.4.1.9.9.656.1.4.1.1.2=cafSessionClientMacAddress
1.3.6.1.4.1.9.9.656.1.4.1.1.5=cafSessionStatus
1.3.6.1.4.1.9.9.656.1.4.1.1.6=cafSessionDomain
1.3.6.1.4.1.9.9.656.1.4.1.1.10=cafSessionAuthUserName
1.3.6.1.4.1.9.9.656.1.4.1.1.12=cafSessionAuthorizedBy
1.3.6.1.4.1.9.9.656.1.4.1.1.14=cafSessionAuthVlan

```
# EEE8021-PAE-MIB: RFC IEEE 802.1X
1.0.8802.1.1.1.1.2.1.1.5=dot1xAuthAuthControlledPortStatus
1.0.8802.1.1.1.1.2.1.1.6=dot1xAuthAuthControlledPortControl
1.0.8802.1.1.1.1.2.4.1.9=dot1xAuthSessionUserName
```

SNMP Version 1 PDUs

SNMP Version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used network-management protocol in the internet community.

SNMPv1 specifies the following five core protocol data units (PDUs):

- GetRequest—A manager-to-agent request, which is used to retrieve the value of a variable, or list of variables. A Response with current values for the variables is returned.
- SetRequest—A manager-to-agent request, which is used to change the value of a variable, or list of variables. A Response with (current) new values for the variables is returned.
- GetNextRequest—A manager-to-agent request, which is used to discover available variables and their values. A Response with variable binding for the next variable in the MIB is returned. The entire MIB of an agent can be walked by iterative application of GetNextRequest starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.
- Response—It returns variable bindings, and acknowledgement from the agent to the manager for GetRequest, SetRequest, GetNextRequest, GetBulkRequest and InformRequest. Although it is used as a response to both GetRequest and SetRequest PDUs, this PDU is also called as GetResponse in SNMPv1.
- Trap—An asynchronous notification, which is sent from the agent to the manager. The format of the trap message is changed in SNMPv2, and this PDU is renamed as SNMPv2-Trap.

SNMP Version 2c PDUs

SNMP Version 2 (SNMPv2) is an evolution of the initial version SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduces GetBulkRequest, an alternative to iterative GetNextRequests of SNMP v1 for retrieving large amounts of management data in a single request. The Community-Based Simple Network Management Protocol Version 2 (SNMP v2c) comprises of SNMP v2, which uses the simple community-based security scheme of SNMPv1.

Two other PDUs, GetBulkRequest and InformRequest are added in SNMPv2, and are carried over to SNMPv3.

- GetBulkRequest—It is introduced in SNMPv2. This is an optimized version of GetNextRequest, which is a manager-to-agent request for multiple iterations of GetNextRequest. It returns a Response with multiple variable bindings walked from the variable binding, or bindings in the request.
- InformRequest—It is introduced in SNMPv2. This is an acknowledged asynchronous notification from a manager-to-manager request. This PDU uses the same format as the SNMPv2 version of Trap (SNMPv2-Trap). The manager-to-manager notifications are already possible in SNMPv1 (using a Trap), but as SNMP protocol commonly runs over UDP where delivery is not assured, and dropped packets are not reported, and so the delivery of a Trap is not guaranteed. InformRequest fixes this by sending back an acknowledgement on receipt and the receiver replies with a Response parroting all information in the InformRequest.

SNMP Version 3

Although SNMPv3 makes no changes to the protocol, SNMPv3 primarily has added security, and remote configuration enhancements to SNMP.

SNMPv3 provides the following important security features:

- Confidentiality—Encryption of packets to prevent snooping by an unauthorized source
- Integrity—Message integrity to ensure that a packet has not been tampered within transit including an optional packet replay protection mechanism
- Authentication—verifies that the message is from a valid source

Endpoint Profiling Policies

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. Cisco ISE creates three identity groups by default, and two other identity groups that are specific to Cisco IP phones and workstations in the system. It also allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. Profiling policies are hierarchical, and they are applied at the endpoint identify groups level. By grouping endpoints to endpoint identity groups, and applying profiling policies to identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

An endpoint profiling policy contains a single condition, or a combination of multiple single conditions that are logically combined against which you can categorize and group endpoints. Cisco ISE always considers a chosen policy for an endpoint rather than an evaluated policy, which is the matched policy when the profiling conditions that are defined in the profiling policy are met for profiling the endpoint in the system.

If the rules of an endpoint profiling policy match, then the profiling policy and the matched policy is the same for that endpoint, which is dynamically discovered on your network. The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty factor for all the valid rules are added together and must exceed the minimum certainty factor that is defined in an endpoint profiling policy. Here, the status of static assignment for that endpoint is set to false in the system. But, this can be set to true after it is statically reassigned to an existing profiling policy in the system by using the static assignment feature during an endpoint editing.

Each rule in an endpoint profiling policy has a certainty metric (an integer value) associated to it. The certainty metric is a measure that is added for all the valid rules in an endpoint profiling policy. A rule can also have either an exception action or a network scan action associated to it and the exception action or the network scan action is used to trigger the configurable action while evaluating the profiling policies with respect to the overall classification of endpoints.

Create a Matching Identity Group

This option allows you to create a matching identity group for endpoints and it will be the child of the Profiled identity group when an endpoint profile matches an existing profile.

Use Hierarchy

This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent endpoint identity group. Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.

Policy Enabled

This option allows you to associate a matching profiling policy, when you profile an endpoint.

Minimum Certainty Factor

Each policy has a minimum certainty metric (an integer value), which is associated to it.

Exception Action

This option allows to trigger an exception action (a single configurable action) that is associated to the endpoint profiling policy, when an endpoint profiling policy matches, and at least one of the exception rules matches.

Network Scan (NMAP) Action

This option allows you to trigger a network scan action (a single configurable action) that is associated to the endpoint profiling policy, when an endpoint profiling policy matches, and at least one of the network scan action rules matches.

To trigger a network scan action that you define in the rule, you must ensure that the Network Scan (NMAP) probe is enabled in the **Administration > System > Deployment > Edit Node > Profiling Configuration**.

Parent Policy

This option allows you to choose an endpoint profiling policy from which you can inherit conditions to its child.

Prerequisite:

Before you begin to configure endpoint profiling policies in Cisco ISE, you should have a basic understanding of the endpoint profiling policies. Review the following:

- Endpoint Profiling Hierarchy, page 18-38
- Unknown Profile, page 18-39
- Profiling Statically Added Endpoint, page 18-39
- Profiling a Static IP Device, page 18-39

Endpoint Profiling Hierarchy

The endpoint profiling policy is hierarchical, where you can inherit rules (one or more conditions) from a parent profiling policy to its child. You can create a generic policy for a device and inherit conditions into its child profiling policies. If an endpoint has to be classified, then the endpoint profile has to first match the parent, and its descendant (child) policies.

For example, if an endpoint has to be classified as a Cisco-IP-Phone 7960, then the endpoint profile for this endpoint has to first match the parent Cisco-Device policy, its child Cisco-IP-Phone policy, and then it matches the Cisco-IP-Phone 7960 profiling policy for better classification.

Unknown Profile

An unknown profile is the default system profile that is assigned to an endpoint, where an attribute or a set of attributes collected for that endpoint do not match with existing profiles in Cisco ISE. When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to the unknown profile. If there is no matching endpoint profiling policy for a statically added endpoint, then you can assign the unknown profile to an endpoint, and change it later.

Profiling Statically Added Endpoint

If you have an endpoint added statically to your network, the statically added endpoint is not profiled by the profiling service in Cisco ISE. For the statically added endpoint to be profiled, the profiling service computes a profile for the endpoint by adding a new MATCHEDPROFILE attribute to the endpoint. The computed profile is the actual profile of an endpoint when dynamically assigned. This allows you to find the mismatches between in profiling the statically added endpoint by using the computed profile with an endpoint profile for that endpoint when it is dynamically assigned.

The endpoint profiling policy is never changed for the statically added endpoint. For the endpoint that is statically assigned, the profiling service computes the MATCHEDPROFILE. For all the endpoints that are dynamically assigned, the MATCHEDPROFILEs are identical to the endpoint profiles.

Profiling a Static IP Device

If you have an endpoint with a statically assigned IP address, you can create a profile for such static IP devices. If you have the RADIUS probe or SNMP Query and SNMP Trap probes enabled, then you can profile the endpoint.

Related Topics:

Configuring DACLs, page 17-35 section in Chapter 17, “Managing Authorization Policies and Profiles.”

Filtering, Creating, Editing, Duplicating, Importing, and Exporting Endpoint Profiling Policies

This section describes the basic operations that allow you to manage endpoint profiling policies from the Endpoint Policies page.

The Endpoint Policies page allows you to manage endpoint profiling policies, and provides an option to filter profiling policies by their names and description. This page displays a list of predefined policies (default profiles) for Apple devices, notebooks, workstations, printers, access points, smart phones, and gaming consoles.

The procedures for managing endpoint profiling policies includes the following tasks:

- Filtering Endpoint Policies, page 18-40
- Creating an Endpoint Profiling Policy, page 18-42
- Editing an Endpoint Profiling Policy, page 18-52
- Deleting an Endpoint Profiling Policy, page 18-52
- Duplicating an Endpoint Profiling Policy, page 18-53
- Exporting Endpoint Profiling Policies, page 18-54
- Importing Endpoint Profiling Policies, page 18-54

Filtering Endpoint Policies

You can use the Show drop-down list, or click the filter icon to both invoke a quick filter and close it in the Endpoint Policies page. A quick filter is a simple filter that you can use to filter endpoint profiling policies in the Endpoint Policies page. The quick filter filters profiling policies based on field descriptions, such as the endpoint policy name and description in the Endpoint Policies page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, in the Endpoint Policies page. The advanced filter filters profiling policies based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Endpoint Policies page. Once you have created and saved a preset filter, you can choose a preset filter from the list. You can also edit preset filters and remove them from the preset filters list.

To filter endpoint profiling policies, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears, which lists all the predefined profiling policies.

Step 2 In the Endpoint Policies page, click the Show drop-down list to choose the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-15.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 18-40 and the To filter by using the Advanced Filter option, complete the following steps:, page 18-41.

Note To return to the profiling policies list, choose **All** from the Show drop-down list to display all the profiling policies without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling policies based on each field description in the Endpoint Policies page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Endpoint Policies page. If you clear the field, it displays the list of all the profiling policies in the Endpoint policies page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Endpoints Policies page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling policies by using variables that are more complex. It contains one or more filters that filter profiling policies based on the values that match the field descriptions. A filter on a single row filters profiling policies based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter profiling policies by using any one or all of the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or click **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 18-15 describes the fields that allow you to filter the endpoint profiling policies in the Endpoint Policies page.

Table 18-15 Filtering Endpoint Profiling Policies

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Endpoint Policy Name	This field enables you to filter endpoint profiling policies by the name of the endpoint profiling policy.
	Policy Enabled	This field enables you to filter endpoint profiling policies by their association to a matching profiling policy.
	Description	This field enables you to filter endpoint profiling policies by the description of the endpoint profiling policy.

Table 18-15 Filtering Endpoint Profiling Policies (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Endpoint Policy Name • Policy Enabled • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter endpoint profiling policies.
	Value	From the Value field, choose the value for the field description that you selected against, which the endpoint profiling policies are filtered.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Creating an Endpoint Profiling Policy

The Endpoint Policies page allows you to add a new endpoint profiling policy to the existing default profiles. The default profiles are predefined in Cisco ISE, and installed when deployed. As endpoint profiling policies are hierarchical, you can find that the Endpoint Policies page displays the list of generic (parent) policies for some devices such as Apple, Cisco, Aruba, Avaya and HP, and their child policies to which their parent polices are associated on this page. Other policies for all Android and BlackBerry smart phones are also available on this page, which include a set of devices.

Caution When you choose to create an endpoint profiling policy in the Endpoint Policies page, do not use the Stop button on your web browsers. This action stops the loading of the New profiler Policy page in Cisco ISE. Cisco ISE also loads other list pages when you access them, as well as the menus within the list pages. But it prevents you from performing operations on all the menus within the list pages except the Filter menus. You will need to log out of Cisco ISE, and then log in again to perform operations on all the menus within the list pages.

To create a profiling policy in the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears.

Step 2 From the Endpoint Policies page, choose **Create**.

Modify the values in the New Profiler Policy page, as shown in Table 18-16.

Step 3 Click **Submit**.

The profiling policy that you create appears in the Endpoint Policies page.

Step 4 Click the **Profiler Policy List** link from the New Profiler Policy page to return to the Endpoint Policies page.

Table 18-16 describes the fields in the Endpoint Policies page that allow you to create an endpoint profiling policy.

Table 18-16 Creating an Endpoint Profiling Policy

Field Name	Description
Name	In the Name field, enter the name of the endpoint profiling policy that you want to create.
Description	In the Description field, enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	To associate a matching profiling policy, check the **Policy Enabled** check box.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy.
Exception Action	To associate an exception action with the profiling policy, click the drop-down arrow to view exception actions that you have already defined. Choose an exception action.
Network Scan (NMAP) Action	To associate a network scan action with the profiling policy, click the drop-down arrow to view the network scan actions that you have already defined. Choose a network scan action.
Create matching identity group	When checked, this option creates a matching identity group as a child of the Profiled identity group when endpoint profiles match an existing profile. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile. To create a matching identity group, check the **Create matching identity group** check box.
Use Hierarchy	When checked, this option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under Profiled endpoint identity groups. If endpoints match the Cisco-IP-Phone profile, then they are grouped under Cisco-IP-Phone, and those match the Workstation profile are grouped under Workstation endpoint identity groups. The Cisco-IP-Phone and Workstation are associated to the Profiled endpoint identity group in the system. To assign endpoints to the matching parent endpoint identity group, check the **Use Hierarchy** check box.

Table 18-16 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Parent Policy	From the Parent Policy field, click the drop-down arrow to view parent policies that exist on the system. Choose a parent policy that you want to associate with the new profiling policy.
Rules	To define the rule, choose one or more profiling conditions from the library, and associate an integer value for the certainty factor for each condition, or associate an action either an exception action or a network scan action for that condition for the overall classification of an endpoint.
If Condition	Choose one or more conditions from the Conditions field. Here, you can save all the conditions that you create to the library by using the Save Icon button. **Note** If you select more than one condition to define an endpoint profiling policy, the conditions are logically combined by using an AND operator by default.
Conditions	Choose the **Select Existing Condition from Library** option or **Create New Condition** option.
Select Existing Condition from Library	You can define an expression by selecting predefined conditions from the policy elements library. Click Action Icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete Here, you can use the AND or OR operator. You can add ad-hoc attribute/value pairs to your expression in the subsequent steps. Click Action Icon to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete

Table 18-16 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Create New Condition (Advance Option)	You can define an expression by selecting attributes from various system or user-defined dictionaries. Click Action Icon to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete Here, you can use the AND or OR operator. You can add pre-defined conditions from the policy elements library in the subsequent steps. Click Action Icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete
Then	Click the drop-down arrow to view, and choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases • Take Exception Action • Take Network Scan Action
Value	If you select the Certainty Factor Increases option, then enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification.
Action Icon	Click the Action Icon to do the following: • Insert new rule above • Insert new rule below • Delete

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

A Quick Reference to Creating a New Endpoint Profiling Policy in Cisco ISE

Cisco ISE provides you with a set of predefined default profiling policies for some endpoints, like workstations, notebooks, IP phones, smart phones, gaming consoles, printers, and fax machines.

Before you create a new endpoint profiling policy for an endpoint in the New Profiler Policy page, it is recommended that you review the following topics:

- Configuring the Probes, page 18-13—This section describes various attribute collection methods that are used in Cisco ISE.
- Endpoint Profiling Policies, page 18-37—This section describes endpoint profiling policies in detail and the fields that are used to configure an endpoint profiling policy.
- Endpoint Profiling, page 18-55—This section describes how to configure conditions (a check) that are necessary to create a rule. A rule contains one or more conditions that are associated with it, and an endpoint profiling policy contains one or more rules.
- Profiling Exception Actions, page 18-60—This section describes a single configurable action that is associated to an endpoint profiling policy.
- Profiling Network Scan Actions, page 18-65—This section describes a single configurable action that is associated to an endpoint profiling policy.
- Endpoints, page 4-15—This section describes on how endpoints are managed statically and dynamically in Cisco ISE.
- Endpoint Identity Groups, page 4-71—This describes on how to manage endpoints in Cisco ISE.

This section guides you on how to create a new endpoint profiling policy for an endpoint in the New Profiler Policy page.

Table 18-16 on page 18-43 describes the fields that you use to create a new endpoint profiling policy.

Cisco ISE provides you with options that allow you to make use of predefined policies, and their hierarchical construction by using the Policy Enabled, Use hierarchy, and Parent Policy options in the New Profiler Policy page. You can also categorize endpoints to a matching endpoint identity group when identified.

Cisco ISE recommends that you create a generic policy (a parent) for a set of endpoints from which its children can inherit the rules and conditions. An endpoint must match a child policy as well as its parent policy in the hierarchy when you are profiling an endpoint. For example, Apple-Device is a generic endpoint profiling policy for all Apple devices. and other policies for Apple devices are children of Apple-Device. You can also create a unique endpoint profiling policy for an endpoint. For example, SonyPS3 is an endpoint profiling policy for a Sony game console.

You must first identify the distinguishing characteristics of the newly identified endpoints in order to profile them appropriately in Cisco ISE. An unknown profile is a default system profile that is assigned to an endpoint, where an attribute or a set of attributes that are collected for that endpoint do not match with existing profiles in Cisco ISE. When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to an unknown profile. If there is no matching endpoint profiling policy for a statically added endpoint, then you can assign the unknown profile to an endpoint, and change it later.

To create an endpoint profiling policy in the New Profiler Policy page, complete the following steps:

Step 1 Go to **Policy > Profiling > Profiling Policies**.

Step 2 From the Endpoint Policies page, choose **Create**.

This section describes how to create an endpoint profile for devices.

Perform the following actions:

- Enter a policy name. You must create a generic (parent) policy for a set of devices, and then create children for the other devices that belong to this group.

  For example, use Apple as the prefix in the policy name for all the policies that you create for Apple devices. Create Apple-Device, a parent endpoint profiling policy for all Apple devices and then create policies for each Apple device, as its children.

- Enter a description for the endpoint profiling policy.

  For example, enter the description as “Generic policy for all Apple devices” for Apple-Device, and “Policy for all Apple MacBooks” for Apple notebooks.

- Check the **Policy Enabled** option.

  For example, Cisco ISE uses all policy enabled endpoint profiling policies and their children to match discovered endpoints.

- Enter a value for **Minimum Certainty Factor**. The certainty values for all the valid conditions are added together to form the matching certainty. It must exceed the minimum certainty factor as defined in the policy, for the policy to be considered as a match.

- Choose an **Exception Action**. The default value is NONE. For more information, see Profiling Exception Actions, page 18-60.

- Choose a **Network Scan (NMAP) Action**. The default value is NONE. For more information, see Profiling Network Scan Actions, page 18-65.

- Choose either to **Create Matching Identity Group** to assign profiled endpoints to an endpoint identity group or choose **Use Hierarchy**.

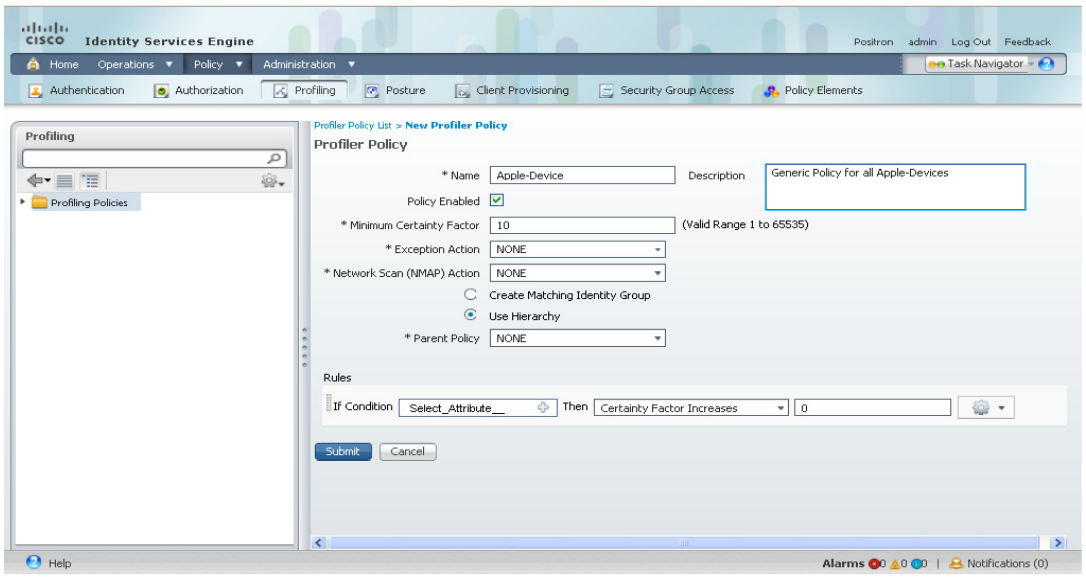
- Choose a **Parent Policy**. It is NONE when you create any parent policy. You can choose a parent endpoint profiling policy from the drop-down list for other policies.

  For example, Apple-Device is the parent policy for all other child policies of Apple devices.

- Define one or more rules for each policy. A rule comprises of one or more conditions that are logically combined using an AND or OR operator. Each rule can be associated with a certainty value, an exception action, or a network scan action. Cisco ISE adds certainty values for all the valid conditions to form the matching certainty from one or more rules, or it initiates an associated exception action or a network scan action when profiling an endpoint.

  When you create a new rule for an endpoint profiling policy, you can choose the existing conditions by using Select Existing Condition from Library. See Figure 18-1.

Figure 18-1 Creating a New Endpoint Profiling Policy



Cisco ISE provides you with a set of predefined checks that you can find in the **Administration > Policy Elements > Conditions > Profiling > Conditions** list page.

To create one or more rules for an endpoint profiling policy, perform the following actions:

- Choose the **Conditions** field. Click the plus [+] sign to expand the Conditions anchored overlay. To close the anchored overlay, click the minus [-] sign.
- Choose **Select Existing Condition from Library**.
- Choose the **Condition Name** field. From the Conditions Name field, click the **Select Condition Quick Picker** (down-arrow) icon. The Dictionaries widget appears, which contains all the checks that you have created and saved in the Administration > Policy Elements > Conditions > Profiling > Conditions list page.
- Choose **Apple-MacBookRuleCheck1**.
- Choose the **AND** or **OR** logical operator.
- Choose **Add Condition from Library** to add another existing condition from the policy elements library. Here, you can also create a new condition and save it to the policy elements library. Choose a new attribute from the list of profiler dictionaries, such as CDP, DHCP, IP, LLDP, MAC, NETFLOW, NMAP, and SNMP and enter a value for that new attribute. When it is saved to the policy elements library, you can use it from the library.
- Choose **Apple-MacBookRuleCheck2**.

  For example, the Apple-MacBook uses a single rule that contains Apple-MacBookRuleCheck1 and Apple-MacBookRuleCheck2 conditions in the rule with an associated certainty value. Both these checks use an IP User-Agent attribute having Mackintosh and Mac OS as values.

  See Figure 18-2 and Figure 18-3.

Figure 18-2 Creating A New Rule from Exiting Conditions -Step 1

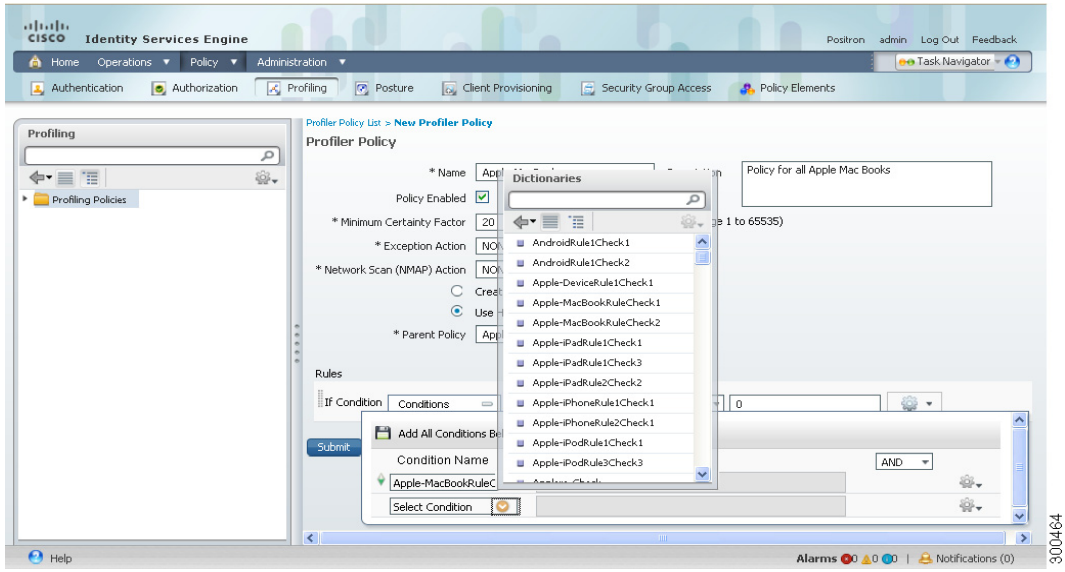
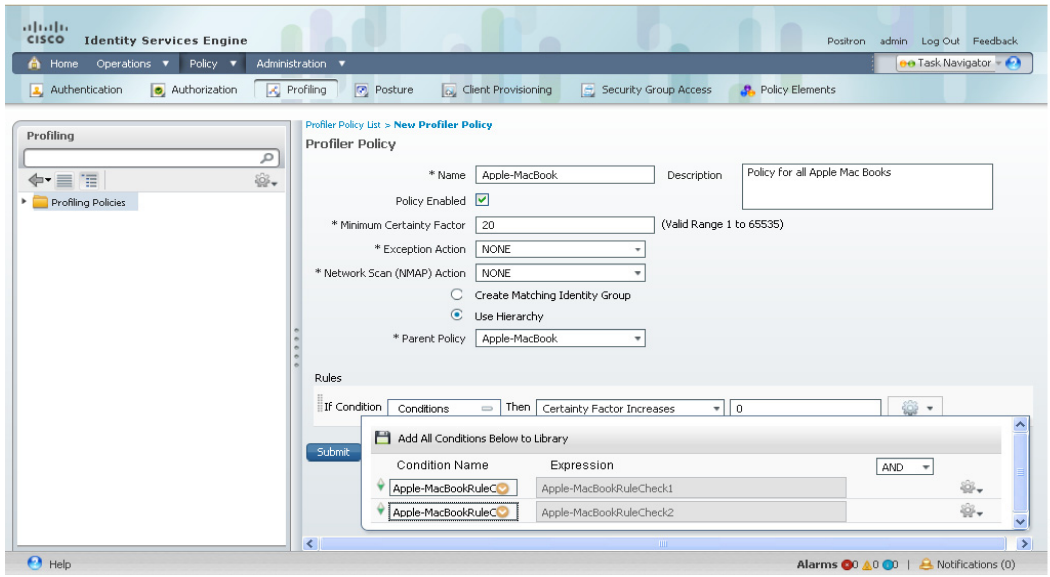


Figure 18-3 Creating A Rule with Existing Conditions-Step2



When you create a new rule for an endpoint profiling policy, you can choose an attribute from the available system dictionaries and associate a value to the attribute by using **Create New Condition (Advance Option)**.

To create a new condition in a rule, perform the following tasks:

- Choose the **Conditions** field. Click the plus [+] sign to expand the Conditions anchored overlay. To close the anchored overlay, click the minus [-] sign.
- Choose **Create New Condition (Advance Option)**.
- Choose the **Expression** field. From the Expression field, click the **Select Attribute Quick Picker** icon. The Dictionaries widget appears, which displays Profiler CDP, DHCP, IP, LLDP, MAC, NETFLOW, NMAP, and SNMP dictionaries. For more information, you can find system dictionaries in **Policy > Policy Elements > Dictionaries**.

For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.

For example, create an expression such as MAC:OUI CONTAINS Apple, which is a new condition, and save it as Apple-DeviceRule1Check1 in the rule. This rule contains Apple-DeviceRule1Check1, a single condition in the Apple-Device policy to check for Apple devices. If an endpoint is an Apple device, Apple-Device is a matching policy, which is a generic (parent) to all the Apple devices. Other Apple devices use the IP User-Agent and DHCP host name in the conditions for further refinement.

Xerox-Device is the parent policy for all Xerox Corporation devices. It uses MAC:OUI CONTAINS XEROX CORPORATION first in Xerox-DeviceRule1Check1in a single rule. You can refine endpoint profiling with the dhcp-class-identifier next in other conditions in its children for profiling other Xerox devices. It provides you device-specific information, such as device manufacturer, type of device, and model number. Xerox-Printer-Phaser3250 is a child of Xerox-Device. You must enable DHCP/DHCP SPAN probes. For example, you can create two expressions for a Xerox-Printer-Phaser3250 in the New Profiler Policy page.

Create an expression such as DHCP:dhcp-class-identifier CONTAINS Xerox and save it as Xerox-Printer-Phaser3250Rule1Check1. Create an expression such as DHCP:dhcp-class-identifier CONTAINS Phaser 3250 and save it as Xerox-Printer-Phaser3250Rule1Check2. See Figure 18-4 and Figure 18-5 that shows how to create new conditions from the New Profiler Policy page.

Figure 18-4 Creating a New Condition-Step1

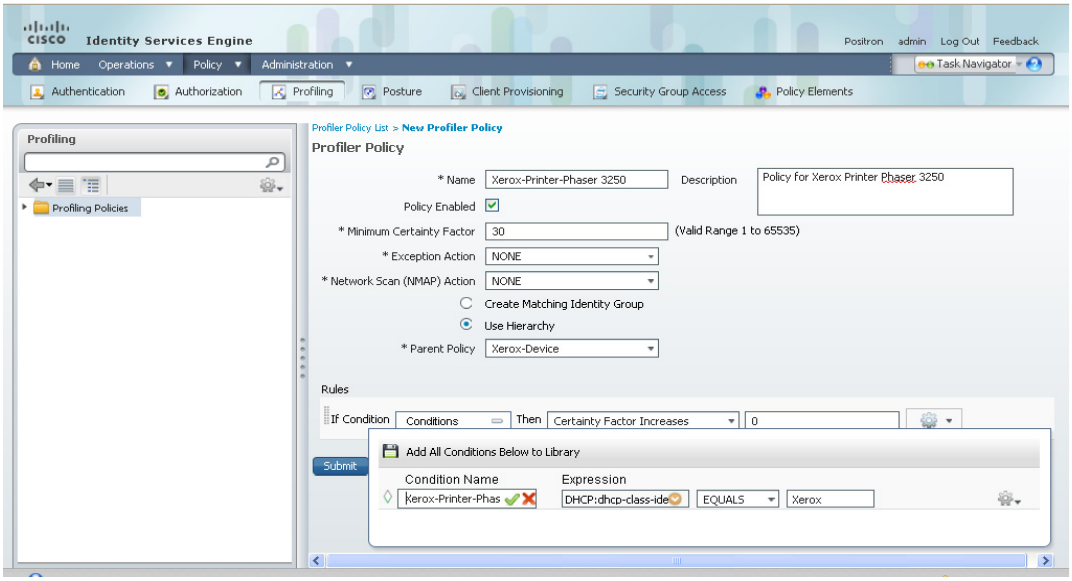
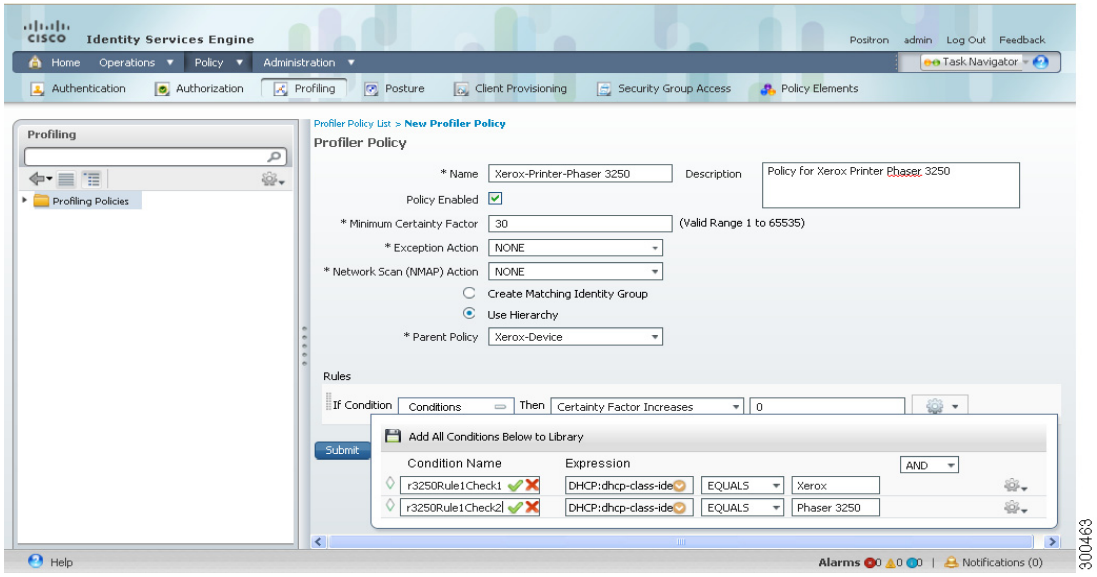


Figure 18-5 Creating a New Condition-Step2



  - For some products, you can also obtain MIB information through SNMP as a result of a Network (NMAP) Scan. If SNMP is enabled on the device, then you can use hrDeviceDescr, hrDeviceStatus, sysContact, sysDescr, sysLocation, sysName, sysObjectID, and sysUpTime attributes in new conditions. You must enable the SNMP Query probe and run the Network (NMAP) Scan.

- Choose from the following:
  - Certainty Factor Increases
  - Take Exception Action
  - Take Network Scan Action
- Click **Submit** to create a new endpoint profile.

Draeger Medical Devices

Cisco ISE contains default endpoint profiling policies for Draeger medical devices that include a generic policy for Draeger medical devices, a policy for Draeger-Delta medical device, and a policy for Draeger-M300 medical device. Both the medical devices share ports 2050 and 2150 in common, and therefore you cannot classify the Draeger-Delta and Draeger-M300 medical devices appropriately, when using the default Draeger endpoint profiling policies.

Cisco ISE includes the following profiling conditions that are used in the endpoint profiling policies for the Draeger medical devices:

- Draeger-Delta-PortCheck1 that contains port 2000
- Draeger-Delta-PortCheck2 that contains port 2050
- Draeger-Delta-PortCheck3 that contains port 2100
- Draeger-Delta-PortCheck4 that contains port 2150
- Draeger-M300PortCheck1 that contains port 1950
- Draeger-M300PortCheck2 that contains port 2050

- Draeger-M300PortCheck3 that contains port 2150

If these Draeger devices share ports 2050 and 2150 in common in your environment, you must add a rule in addition to check for the device destination IP address in the default Draeger-Delta and Draeger-M300 endpoint profiling policies, which allows you to distinquish these medical devices.

Editing an Endpoint Profiling Policy

You can choose an endpoint profiling policy in the Endpoint Policies page in order to edit it.

Note During an upgrade, Cisco ISE overwrites any configuration that you have saved it in the predefined endpoint profiles. You must save all your configurations on a copy of the predefined endpoint profiles only.

To edit a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears.

Step 2 In the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Edit**.

Step 4 Modify the values of the fields in the edit page, as shown in Table 18-16 on page 18-43.

During an edit, you can click the **Reset** button without saving the current input data in the edit page. Here, you can retain the configuration without saving the current input data in the edit page. Click the **Profiler Policy List** link from the edit page to return to the Endpoint Policies page.

Step 5 Click **Save** to save the current input data in the edit page.

Step 6 Click the **Profiler Policy List** link from the edit page to return to the Endpoint Policies page after editing an endpoint profiling policy.

Deleting an Endpoint Profiling Policy

The Endpoint Policies page lists all the canned profiles that are already created in Cisco ISE for your deployment. You can choose an endpoint profiling policy to delete that you create in the Endpoint Policies page.

You can also select all the endpoint policies from the Endpoint Policies page to delete from your Cisco ISE deployment. To delete all the endpoint policies, you need to check the check box that appears in front of the Endpoint Policy Name title in the Endpoint Policies page.

When you select all the endpoint policies and try to delete them in the Endpoint Policies page, some of them may not be deleted. The endpoint policy may be a parent to other endpoint policies or mapped to an authorization policy and a parent to other endpoint policies.

Note You cannot delete a parent profile in the Endpoint Policies page when an endpoint profile is defined as a parent to other endpoint profiles. For example, Cisco-Device is a parent to other endpoint policies for Cisco devices. You cannot delete an endpoint profile when it is mapped to an authorization policy. For example, Cisco-IP-Phone is mapped to the Profiled Cisco IP Phones authorization policy and it is a parent to other endpoint policies for Cisco IP Phones.

To delete a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears.

Step 2 In the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Delete**.

If you choose to delete an endpoint profile from the Endpoint Policies page, Cisco ISE displays a confirmation dialog. Clicking **OK** in the dialog deletes the policy in the Endpoint Policies page. Clicking **Cancel** in the dialog returns to the Endpoint Policies page without deleting the policy.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Duplicating an Endpoint Profiling Policy

Duplicating an endpoint profiling policy allows you to quickly create a similar characteristic profiling policy that you can modify instead of creating a new profiling policy by redefining all conditions.

To duplicate a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies.**

The Endpoint Policies page appears.

Step 2 In the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Duplicate**.

A copy of the profiling policy appears in the Endpoint Policies page.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Exporting Endpoint Profiling Policies

You can choose endpoint profiling policies in the Endpoint policies page to export them to other Cisco ISE deployments. Or, you can use it as a template for creating your own policies to import.

To export a profiling policy from the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears.

Step 2 Choose one or more profiling policies that you want to export.

Step 3 Choose **Export**.

A dialog appears that prompts you to open the profiler_policies.xml with an appropriate application or save it. This is a file in XML format that you can open in a web browser, or in other appropriate applications. You can also download the file to your system in the default location, which can be used for importing later.

Step 4 Click **OK**.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Importing Endpoint Profiling Policies

You can import endpoint profiling polices from a file in XML by using the same format that you have previously created in the export function. If you import newly created profiling policies that has parent policies associated, then you must define parent policies before you define child policies. The imported file shows the hierarchy of endpoint profiling policies that contains the parent policy first, the profile that you imported next along with the rules and checks that are defined in the policy.

To import a profiling policy from the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling Policies**.

The Endpoint Policies page appears.

Step 2 Choose **Import**.

Step 3 Browse to locate the file that you previously exported and want to import.

Note Please note that the file should be in XML format as previously created in the export function.

Step 4 Click **Submit**.

Profiling policies, which are imported appear in the Endpoint Policies page.

Step 5 Click the **Profiler Policy List** link from the Import Profiler Policies page to return to the Endpoint Policies page.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Endpoint Profiling

A profiling condition is a check that allows you to provision specific values that can be associated to a set of attributes of an endpoint. You can logically group one or more of these conditions into a rule that allows you to validate and classify endpoints to a category. You can create a condition that allows you to provision specific values to one or more attributes of the endpoint, which helps you to validate and classify endpoints in a category.

This section describes the basic operations that allow you to provision a specific value to an attribute of an endpoint. You can use the Conditions page to display and manage Cisco ISE profiling conditions.

The procedures for managing profiling conditions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiling Condition

Related Topics:

- Endpoint Profiling Policies, page 18-37
- Profiling Exception Actions, page 18-60
- Profiling Network Scan Actions, page 18-65

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Filtering, Creating, Editing, and Deleting a Profiling Condition

The Conditions page allows you to manage profiling conditions, which provides an option to filter profiling conditions. This page lists profiling conditions along with their names, description and the expression that you have defined in these conditions in the Conditions page.

The procedures for managing profiling conditions include the following tasks:

- Filtering Conditions, page 18-55
- Creating a Profiling Condition, page 18-57
- Editing a Profiling Condition, page 18-59
- Deleting a Profiling Condition, page 18-59

Filtering Conditions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it in the Conditions page. A quick filter is a simple filter that you can use to filter profiling conditions in the Conditions page. The quick filter filters conditions based on field descriptions, such as the name of the profiling check, the description, and the expression that is used in the condition in the Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, in the Conditions page. The advanced filter filters conditions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Conditions page. Once you have created and saved a preset filter, you can choose a preset filter from the list. You can also edit preset filters and remove them from the preset filters list.

To filter conditions from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, choose **Profiling**.

The Conditions page appears, which lists all the predefined conditions.

Step 3 In the Conditions page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter**,** an Advanced Filter for filtering or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-17.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 18-56 and the To filter by using the Advanced Filter option, complete the following steps:, page 18-56.

Note To return to the conditions list, choose **All** from the Show drop-down list to display all the conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling conditions based on each field description in the Conditions page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Conditions page. If you clear the field, it displays the list of all the conditions in the Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling conditions by using variables that are more complex. It contains one or more filters that filter conditions based on the values that match the field descriptions. A filter on a single row filters conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter conditions by using any one or all of the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or click **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 18-17 describes the fields in the Conditions page that allow you to filter the profiling conditions.

Table 18-17 Filtering Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Check Name	This field enables you to filter conditions by the name of the profiling check (condition).
	Expression	This field enables you to filter conditions by an attribute and its attribute value within the profiling check.
	Description	This field enables you to filter conditions by the description of the profiling check.
Advanced Filter	Choose the field description from the following: • Profiler Check Name • Expression • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter profiling conditions.
	Value	From the Value field, choose the value for the field description that you selected against, which the profiling conditions are filtered.

Creating a Profiling Condition

To create a profiling condition in the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling**.

The Conditions page appears.

Step 2 From the Conditions page, choose **Create**.

You can create a condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP and NMAP type.

Step 3 Modify the values in the New Profiler Condition page, as shown in Table 18-18.

Step 4 Click **Submit**.

The profiling condition that you create appears in the Conditions page.

Step 5 Click the **Profile Condition List** link in the New Profiler Condition page to return to the Conditions page.

Table 18-18 describes the fields in the Conditions page that allow you to create a profiling condition:

Table 18-18 Creating a Profiling Condition

Field Name	Description
Name	In the Name field, enter the name of the profiling condition that you want to create.
Description	In the Description field, enter the description of the profiling condition that you want to create.
Type	From the Type field, click the drop-down arrow to view the following predefined profiling conditions types: • DHCP • MAC • SNMP • IP • RADIUS • Netflow • CDP • LLDP • NMAP Choose a type.
Attribute Name	From the Attribute Name field, click the drop-down arrow to view the predefined attributes for the type you have selected in the Type field.
Operator	Click the drop-down arrow to view the following predefined operators: • EQUALS • NOTEQUALS • GREATERTHAN • LESSTHAN • CONTAINS Choose an operator.
Attribute Value	Enter the value for the attribute name that you selected in the Attribute Name.

Editing a Profiling Condition

You can edit a profiling condition from the Conditions page.

To edit a condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling**.

The Conditions page appears.

Step 2 From the Conditions page, choose a profiling condition.

Step 3 Choose **Edit**.

Step 4 Modify the values of the fields in the edit page, as shown in Table 18-18 on page 18-58.

During an edit, you can click **Reset** without saving the current input data in the edit page. Here, you can retain the configuration without saving the current input data in the edit page. Click the **Profiler Condition List** link from the edit page to return to the Conditions page without saving the current input data.

Step 5 Click **Save** to save the current input data in the edit page.

Step 6 Click the **Profiler Condition List** link from the edit page to return to the Conditions page after editing a profiling condition.

Deleting a Profiling Condition

You can delete a profiling condition from the Conditions page.

To delete a condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling**.

The Conditions page appears.

Step 2 From the Conditions page, choose a profiling condition.

Step 3 Choose **Delete**.

If you choose to delete a profiling condition from the Conditions page, Cisco ISE displays a confirmation dialog. Clicking **OK** in the dialog deletes the condition in the Conditions page. Clicking **Cancel** in the dialog returns to the Conditions page without deleting the profiling condition.

Profiling Results

Cisco ISE provides configurable network access to identities.

Cisco ISE policy model comprises of policy based services for authentication and authorization, profiling, posture, client provisioning, and Cisco security group access for identities in Cisco ISE.

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the arrow next to Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Choose **Exception Actions**. See Profiling Exception Actions, page 18-60.

Here, you can create editable exception actions that you can use for profiling endpoints on a Cisco ISE network. Cisco ISE includes three noneditable exception actions, such as an EndpointDelete, FirstTimeProfile, and StaticAssignment.

Or

Step 5 Choose **Network Scan (NMAP) Actions**. See Profiling Network Scan Actions, page 18-65.

Here, you can create editable network scan actions that you can use for profiling endpoints on a Cisco ISE network. Cisco ISE includes three predefined network scan actions such as an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan

Profiling Exception Actions

An exception action is a single configurable action that is associated to an endpoint profiling policy. You can define, and associate one or more exception rules to a single profiling policy. This association triggers an exception action, when the profiling policy matches, and at least one of the exception rules matches in profiling endpoints in Cisco ISE.

Cisco ISE triggers the following non-editable profiling exception actions from the system when profiling endpoints on a Cisco ISE network:

Endpoint Delete

An exception action is triggered in Cisco ISE, and a CoA is issued when an endpoint is deleted from the system in the Endpoints page, or reassigned to the unknown profile from the edit page on a Cisco ISE network.

Static Assignment

An exception action is triggered in Cisco ISE, and a CoA is issued upon when an endpoint has connected to your Cisco ISE network, but you statically assign an endpoint profile for that endpoint.

FirstTimeProfiled

An exception action is triggered in Cisco ISE, and a CoA is issued, when an endpoint is profiled in Cisco ISE for the first time, where the profile of that endpoint changes from an unknown profile to an existing profile, but that endpoint is not successfully authenticated on a Cisco ISE network.

The procedures for managing exception actions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiling Exception Action, page 18-61

Related Topics:

Endpoint Profiling Policies, page 18-37

Filtering, Creating, Editing, and Deleting a Profiling Exception Action

The Exception Actions page allows you to manage exception actions, and provides an option to filter them, which lists all the exception actions along with their names and descriptions.

The procedures for managing exception actions include the following tasks:

- Filtering Exception Actions, page 18-61
- Creating an Exception Action, page 18-63
- Editing an Exception Action, page 18-64
- Deleting an Exception Action, page 18-65

Filtering Exception Actions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it in the Exception Actions page. A quick filter is a simple filter that you can use to filter profiling exception actions in the Exception Actions page. The quick filter filters exception actions based on field descriptions, such as the name of the profiling exception action and the description in the Exception Actions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, in the Exception Actions page. The advanced filter filters exception actions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime which displays the filtered results in the Exception Actions page. Once created and saved a preset filter, you can choose a preset filter of filtered results in the Exception Actions page. You can also edit preset filters and remove them from the preset filters list.

To filter exception actions from the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Exceptions Actions**.

The Exception Actions page appears.

Step 5 In the Exception Actions page, click the Show drop-down list to choose the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-19.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 18-62 and the To filter by using the Advanced Filter option, complete the following steps:, page 18-62.

Note To return to the exception actions list, choose **All** from the Show drop-down list to display all the exception actions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling exception actions based on each field description in the Exception Actions page. When you click inside any field, and as you enter the search criteria in the field, the quick filter refreshes the page with the results in the Exception Actions page. If you clear the field, it displays the list of all the exception actions in the Exception Actions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Exceptions Actions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling exception actions by using variables that are more complex. It contains one or more filters that filter exception actions based on the values that match the field descriptions. A filter on a single row filters exception actions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter exception actions by using any one or all of the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 18-19 describes the fields in the Exception Actions page that allow you to filter exception actions.

Table 18-19 Filtering Exception Actions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Exception Action Name	This field enables you to filter exception actions by the name of the profiling exception action.
	Description	This field enables you to filter exception actions by the description of the profiling exception action.
Advanced Filter	Choose the field description from the following: • Profiler Exception Action Name • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter exception actions.
	Value	From the Value field, choose the value for the field description that you selected against, which the exception actions are filtered.

Creating an Exception Action

To create an exception action in the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Exception Actions**.

The Exception Actions page appears.

Step 5 In the Exception Actions page, click **Create**.

Step 6 Modify the values in the New Profiler Exception Action page, as shown in Table 18-20.

Step 7 Click **Submit**.

The exception action that you created appears in the Exception Actions page.

Table 18-20 describes the fields in the New Profiler Exception Actions page that allow you to create an exception action:

Table 18-20 Creating an Exception Action

Field Name	Field Description
Name	In the Name field, enter the name of the exception action that you want to create.

Table 18-20 Creating an Exception Action (continued)

Field Name	Field Description
Description	In the Description field, enter the description of the exception action that you want to create.
CoA Action check box to enforce CoA	To enforce CoA, check the **CoA Action** check box. When you associate an exception action in the endpoint profiling policy and enforce a CoA, you must configure CoA globally in Cisco ISE that can be done in the following location: Administration > System > Settings > Profiling. For information, see the Change of Authorization, page 18-9.
Policy Assignment	Click the drop-down arrow to view the endpoint profiles that are configured and choose the profile against which the endpoint will be profiled when the exception action is triggered, regardless of its matched value.

Editing an Exception Action

You can edit an exception action from the Exception Actions page.

To edit an exception action in the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Exception Actions**.

The Exception Actions page appears.

Step 5 In the Exception Actions page, choose an exception action.

Step 6 Click **Edit**.

Step 7 Modify the field values in the edit page, as shown in Table 18-20 on page 18-63.

During an edit, click **Reset** without saving the current input data in the edit page. Here, you can retain the configuration without saving the current input data. Click the **Profiler Exception Action List** link in the edit page to return to the Exception Actions page without saving the current input data.

Step 8 Click **Save** to save the current input data in the edit page.

Step 9 Click the **Profiler Exception Action List** link in the edit page to return to the Exception Actions page after editing an exception action.

Deleting an Exception Action

You can delete an exception action from the Exception Actions page.

To delete an exception action in the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Exception Actions**.

The Exception Actions page appears.

Step 5 In the Exception Actions page, choose an exception action.

Step 6 Choose **Delete**.

If you choose to delete a profiling exception action from the Exception Actions page, Cisco ISE displays a confirmation dialog. Clicking **OK** in the dialog deletes the exception action in the Exception Actions page. Clicking **Cancel** in the dialog returns you to the Exception Actions page without deleting the exception action.

Profiling Network Scan Actions

A network scan action is a single configurable action that is associated to an endpoint profiling policy. You can define, and associate one or more network scan rules in a single endpoint profiling policy. You can also define the type of scanning in each network scan actions. This association triggers a network scan action, when the profiling policy matches, and at least one of the network scan rules matches in profiling endpoints in Cisco ISE.

Note When scanning an operating system for endpoints, the NMAP OS-scan results may be unreliable. This is due to the limitations of the NMAP tool that you use for an OS-scan. For example, when scanning an operating system of network devices such as switches and routers, the NMAP OS-scan may provide an incorrect operating-system attribute for those devices. For these devices, you can configure endpoint policies that use the NMAP operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values).

The procedures for managing network scan actions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiling Network Scan Action, page 18-66.

Related Topics:

Endpoint Profiling Policies, page 18-37.

Filtering, Creating, Editing, and Deleting a Profiling Network Scan Action

The Network Scan Actions page allows you to manage network scan actions, and provides with an option to filter them that lists all the network scan actions, along with their names and descriptions.

The procedures for managing network scan actions include the following tasks:

- Filtering Network Scan Actions, page 18-66
- Creating a Network Scan Action, page 18-68
- Editing a Network Scan Action, page 18-70
- Deleting a Network Scan Action, page 18-71

Filtering Network Scan Actions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it in the Network Scan Actions page. A quick filter is a simple filter that you can use to filter profiling network scan actions in the Network Scan Actions page. The quick filter filters network scan actions based on field descriptions, such as the name of the profiling network scan action and the description in the Network Scan Actions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, in the Network Scan Actions page. The advanced filter filters network scan actions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter from the list has a session lifetime, which displays the filtered results in the Network Scan Actions page. Once created and saved a preset filter, you can choose a preset filter of filtered results in the Network Scan Actions page. You can also edit preset filters and remove them from the preset filters list.

To filter network scan actions from the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 5 In the Network Scan Actions page, click the Show drop-down list to choose the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-19.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-67 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-67.

Note To return to the network scan actions list, choose **All** from the Show drop-down list to display all the network scan actions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling network scan actions based on each field description in the Network Scan Actions page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Network Scan Actions page. If you clear the field, it displays the list of all the network scan actions in the Network Scan Actions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Network Scan Actions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling network scan actions by using variables that are more complex. It contains one or more filters that filter network scan actions based on the values that match the field descriptions. A filter on a single row filters network scan actions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter network scan actions by using any one or all of the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**. Click **Cancel** to clear the filter without saving the filter.

Step 8 Click **Clear Filter** after filtering.

Table 18-21 describes the fields on the Network Scan Actions page that allow you to filter exception actions.

Table 18-21 Filtering Network Scan Actions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Network Scan Action Name	This field enables you to filter network scan actions by the name of the profiling network scan action.
	Description	This field enables you to filter network scan actions by the description of the profiling network scan action.
Advanced Filter	Choose the field description from the following: • Profiler Network Scan Action Name • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter network scan actions.
	Value	From the Value field, choose the value for the field description that you selected against, which the network scan actions are filtered.

Creating a Network Scan Action

To add a network scan action in the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 5 In the Network Scan Actions page, click **Add**.

Step 6 Modify the values in the New Network Scan Action page, as shown in Table 18-22.

Step 7 Click **Submit**.

The network scan action that you created appears in the Network Scan Actions page.

Table 18-22 describes the fields on the Network Scan Actions page that allow you to add an exception action.

Table 18-22 Creating a Network Scan Action

Field Name	Field Description
Name	In the Name field, enter the name of the network scan action that you want to create.
Description	In the Description field, enter the description of the network scan action that you want to create.
Scan	Choose options to scan from the following: • Scan OS—Scans an operating system. • Scan SNMP Port—Scans SNMP ports (161, 162). • Scan Common Port—Scans common ports. See Table 18-26.

A network scan action that is associated with an endpoint profiling policy scans an endpoint for an operating system, SNMP ports and common ports.

The following NMAP command scans the operating system when you associate Scan OS with an endpoint profiling policy:

nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP address>

Table 18-23 NMAP Commands for an Endpoint OS Scan

-sS	TCP SYN scan. SYN scan is the default
-O	Enables OS detection
-F	(Fast (limited port) scan). Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.
oN	Normal output
oX	XML output
IP address	IP address of an endpoint that is scanned

The following NMAP command scans SNMP ports (UDP 161 and 162) when you associate Scan SNMP Port with an endpoint profiling policy:

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

Table 18-24 NMAP Commands for an Endpoint SNMP Port Scan

-sU	UDP scan
-p <port ranges>	Scans only specified ports. For example, scans UDP ports 161 and 162
oN	Normal output
oX	XML output
IP address	IP address of an endpoint that is scanned

The following NMAP command scans common ports when you associate Scan Common Port with an endpoint profiling policy:

nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

Table 18-25 NMAP Commands for an Endpoint Common Ports Scan

-sTU	Both TCP connect scan and UDP scan
-p <port ranges>	Scans specified ports for TCP and UDP For example, scans TCP ports: 21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080 and UDP ports: 53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900
oN	Normal output
oX	XML output
IP address	IP address of an endpoint that is scanned.

Editing a Network Scan Action

You can edit a network scan action from the Network Scan Actions page.

To edit a network scan action in the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

Step 4 Click **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 5 In the Network Scan Actions page, choose a network scan action.

Step 6 Choose **Edit**.

Step 7 Modify the values of the fields in the edit page, as shown in Table 18-22 on page 18-69.

During an edit, click **Reset** without saving the current input data in the edit page. Here, you can retain the configuration without saving the current input data. Click the **Network Scan Action List** link in the edit page to return to the Network Scan Actions page without saving the current input data.

Step 8 Click **Save** to save the current input data in the edit page.

Step 9 Click the **Network Scan Action List** link from the edit page to return to the Network Scan Actions page after editing a network scan action.

Deleting a Network Scan Action

You can delete a network scan action from the Network Scan Actions page.

To delete a network scan action in the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane, choose **Profiling**.

Step 3 Click the right navigation arrow to expand Profiling to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Click **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 5 In the Network Scan Actions page, choose a network scan action.

Step 6 Choose **Delete**.

If you choose to delete a profiling network scan action from the Network Scan Actions page, Cisco ISE displays a confirmation dialog. Clicking **OK** in the dialog deletes the network scan action in the Network Scan Actions page. Clicking **Cancel** in the dialog returns you to the Network Scan Actions page without deleting the network scan action.

Endpoint Profiling by Integrating Network Mapper in Cisco ISE

Network Mapper (NMAP) is a free, open source utility that can be used to explore networks and perform other network related tasks. It is designed to rapidly scan large networks, and works on a single host. NMAP uses raw IP packets for many network-related tasks, such as identifying endpoints (hosts that are available), the operating systems (and OS versions) they run, and the services (application name and version) they offer.

NMAP is a powerful tool that you can use to scan huge networks of y hundreds of thousands of machines. NAMP is portable and supports many operating systems. In addition to its command-line executable, the NMAP suite includes an advanced graphical user interface, a results viewer, a flexible data transfer redirection, and debugging tool, a utility for comparing scan results, and a packet generation and response analysis tool. It is highly flexible that supports advanced techniques for mapping out networks where devices such as IP filters, firewalls, routers are present, including port scanning mechanisms (both TCP and UDP), operating system detection, version detection, ping sweeps, and more.

For more information on NMAP, see Network Mapper (NMAP) and the NMAP documentation that is available at http://nmap.org/docs.html.

NMAP is integrated with the Cisco ISE profiler to augment its profiling capability for better endpoint classification, particularly iDevices and other mobile devices. You can either perform a manual subnet scan on a specific subnet by using the Network Scan probe, or you can associate a network scan action to an endpoint profile (a specific profile) to perform a scan on an endpoint.

For more information on the network scanning, see the "A Network Scan" section on page 18-24.

For more information on the endpoint scanning, see the "Endpoint Scan" section on page 18-72.

Endpoint Scan

An endpoint scan is used to scan endpoints in order to limit resources usage in the Cisco ISE system. A network scan action scans a single endpoint as compared to resource intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. Endpoint scans can be processed only one at a time.

You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefines three scanning types for a network scan action, which can include one, or all three scanning types, for instance, an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan. You can also create a new network scan action of your own. Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint.

For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is no longer matched to an Apple-Device profile, but it is matched to an appropriate profile for an Apple device.

The following are the scanning types that are predefined in any network scan action for an endpoint scan.

OS-scan

This type scans an operating system (and OS version) that an endpoint is running. It is a resource intensive scan.

SNMPPortsAndOS-scan

This type scans an operating system (and OS version) that an endpoint is running, as well as triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.

CommonPortsAndOS-scan

This type scans an operating system (and OS version) that an endpoint is running, as well as common ports (TCP and UDP), but not SNMP ports.

Table 18-26 lists the total of 30 common ports (15 TCP and 15 UDP ports) that NMAP uses for scanning.

Table 18-26 Common Ports

TCP Ports		UDP Ports	
Ports	**Service**	**Ports**	**Service**
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds

Table 18-26 Common Ports (continued)

TCP Ports		UDP Ports	
Ports	**Service**	**Ports**	**Service**
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

Endpoint Profiling by Using an IOS Sensor on a Network Access Device

Cisco ISE enforces certain configurations on the DHCP probe. For example, you can collect DHCP packets from one or more interfaces only when you configure the DHCP IP helper by using the ip helper - address command on the network devices, or on a specific interface, by using DHCP SPAN. The Cisco ISE profiler receives these DHCP packets and parses them to capture other attributes of endpoints, along with DHCP attributes. Similarly, you can collect the CDP/LLDP attributes of all the connected endpoints only when the SNMP Query probe is enabled. You must ensure that CDP and LLDP are enabled on all the ports of the network devices.

Cisco ISE addresses these configuration restrictions by implementing a functionality to work with an IOS based sensor that is embedded in the switch. The IOS sensor integration resolves any topology restriction on your deployment that you might have experienced in previous releases, due to the nature of event collection of endpoint attributes from various probes. IOS sensor integration allows Cisco ISE runtime and the Cisco ISE profiler to collect any or all of the attributes that are sent from the switch. You can collect DHCP, CDP, and LLDP attributes directly from the switch by using an already existing RADIUS protocol. The attributes that are collected for DHCP, CDP, and LLDP are then parsed and mapped to attributes in the Cisco ISE dictionaries.

For more information on Cisco ISE system dictionaries and the attributes that are defined in the dictionaries, you can navigate to **Policy > Policy Elements > Dictionaries** from the administration user interface.

Cisco ISE contains the list of default profiles that are updated for LLDP, as well as new profiles. For more information on the list of default profiles in Cisco ISE, navigate to **Policy > Profiling > Endpoint Profiling**.

For more information on IOS sensor supported network access devices, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x*.

Integrating an IOS Sensor with Cisco ISE

Integrating an IOS sensor enabled switch with Cisco ISE involves an IOS sensor, the data collector that is embedded in the network device (switch) for gathering DHCP, CDP, and LLDP data, and analyzers for processing the data and determining the device-type of endpoints. The distinct advantage of embedding a sensor in the switch is that the sensor is the closest point present to the source of the data.

There are two ways of deploying an analyzer, but they are not expected to be used in conjunction with each other:

- An analyzer can be deployed in Cisco ISE

- Analyzers can be embedded in the switch as the sensor

The choice of deploying an analyzer in either way depends on your implementation. Both deployments use the same classification rule-set, but the analyzer deployed in Cisco ISE provides a functional superset of the embedded capabilities of the analyzers deployed in the switches. Both analyzers are the clients of the IOS sensor component-set and require the same information from the sensor. With the embedded analyzers in the switch, this deployment can be used where Cisco ISE is not available either for a visibility-only deployment or in conjunction with an OEM AAA server.

An IOS Sensor and Analyzers

A network access device (switch) has an IOS sensor embedded, and the sensor has both internal clients (analyzers) and one external client (Cisco ISE analyzer).

The IOS sensor lets you to specify attribute filters using the CLI to define the target data-set. The attribute filters must be applied as close to the source of the attributes as possible to minimize redundant memory usage and processing across the system.

The filter commands must include the following capabilities:

- An all option per protocol (default)
- A none option per protocol
- An include list per protocol
- An exclude list per protocol

The internal clients, including the Device Classifier (local analyzer), use the session API as exposed by the session management (identity) infrastructure. Apart from the Device Classifier (DC), ASP, MSI-Proxy, and EnergyWise components are the other illustrated internal clients that are primarily interested in the device-type of the connected endpoints. Once the device-type is determined, it can be returned back to the session management infrastructure by using the same session API and stored against the appropriate session, and in the form of a RADIUS CoA in the future. It is also available to any client of the Session API (through notification and/or in response to a direct query). The same session management infrastructure can accommodate both the cases where endpoint profiling can be configured in conjunction with access-control for a typical identity deployment, or for a visibility-only deployment.

The external client, the Cisco ISE analyzer, initially uses the RADIUS accounting messages to receive the additional endpoint data. The existing RADIUS Accounting message types (start and interim) are augmented with the profiling data. Additional accounting messages can be generated if the profiling data changes in the middle of the session.

When appropriately configured, a switch with the sensor capability captures endpoint information from CDP, LLDP, DHCP, and MAC OUI, and (subject to statically configured filters that can be dynamically configured in future phases of implementation) makes this information available to its registered clients in the context of an access session (which represents an endpoint's connection to the network device). Notifications can only be generated if a change is detected in the information provided by an endpoint (subject to statically configured filters).

Endpoint Profiling in Cisco ISE with an IOS Sensor Enabled on NADs

You can create endpoints and classify them according to the endpoint profiling policies that are currently available by default in Cisco ISE with DHCP, CDP, and LLDP attributes, by using IOS sensor enabled switches. This allows you to overcome the earlier configuration restrictions on DHCP and SNMP Query probes, by using the existing RADIUS probe alone.

You must configure network access devices that allow the IOS sensor to collect DHCP, CDP, and LLDP information from the endpoints that connect to your network and to send them through the RADIUS accounting messages to Cisco ISE. Cisco ISE receives these RADIUS accounting messages from the switches, and the runtime protocol parses and forwards these messages as syslogs to the RADIUS probe of the profiler. The RADIUS probe populates DHCP, CDP, and LLDP attributes for the endpoints from the syslogs and contributes to the classification of endpoints. The result of this classification can also be returned in the form of the RADIUS CoA, with attributes in future releases.

Prerequisites:

You must ensure that the network access devices (switches) and Cisco ISE are properly configured.

This section summarizes a list of tasks that you must perform on the switches and Cisco ISE.

Review the following:

- Ensure that the RADIUS probe is enabled in Cisco ISE.
- Ensure that network access devices support an IOS sensor for collecting DHCP, CDP, and LLDP information.
- Ensure that network access devices run the following CDP and LLDP commands to capture CDP and LLDP information from endpoints:

  ```
  cdp enable
  lldp run
  ```
- Ensure that session accounting is enabled separately, by using the standard AAA and RADIUS commands.

  For example, use the following commands:

  ```
  aaa new-model
  aaa accounting dot1x default start-stop group radius

  radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
  radius-server vsa send accounting
  ```
- Ensure that you run IOS sensor-specific commands.

  Enabling Accounting Augmentation

  You must enable network access devices to add IOS sensor protocol data to the RADIUS accounting messages, as well as to generate additional accounting events when it detects new sensor protocol data. This means that any RADIUS Accounting message should include all CDP, LLDP, and DHCP attributes.

  Enter the following (new) global command:

  ```
  device-sensor accounting
  ```

  Disabling Accounting Augmentation

  To disable (accounting) network access devices and add IOS sensor protocol data to the RADIUS accounting messages for sessions that are hosted on a given port (if the accounting feature is globally enabled), enter the following command at the appropriate port:

  ```
  no device-sensor accounting
  ```

  TLV Change Tracking

By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a TLV (type, length, and value) that has not been received previously in the context of a given session.

You must enable client notifications and accounting events for all TLV changes where there are either new TLVs, or where previously received TLVs have different values. Enter the following command:

```
device-sensor notify all-changes
```

- Be sure that you disable the IOS Device Classifier (local analyzer) in the network access devices.

  Enter the following command:

  ```
  no macro auto monitor
  ```

Note This command prevents network access devices from sending two identical RADIUS accounting messages per change.

Auto Smartports Configuration in Cisco ISE

You can configure Auto Smartports in an authorization profile in Cisco ISE, with an event trigger that enables the VSA cisco-av-pair with the value, “auto-smart-port=event trigger”. The event trigger is used to map the Auto Smartports macro to the source port of the event.

For example, when you connect a Cisco IP phone to a port, Auto Smartports automatically applies the Cisco IP phone macro. The Cisco IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

The macros that are embedded in the switch software are groups of command-line interface (CLI) commands.

Auto Smartports Macros

Auto Smartports macros dynamically configure ports based on the device type that is detected on the port. When the switch detects a new device on a port, it applies the appropriate macro on that port. When there is a link-down event on the port, the switch removes the macro. Auto Smartports uses event triggers to map devices to port macros.

Static Smartports Macros

Static Smartports macros provide port configurations that you manually apply based on the device connected to the port. When you apply a static macro, the macro CLI commands are added to the existing port configuration. When there is a link-down event on the port, the switch does not remove the static macro configuration.

Event Triggers

Auto Smartports uses event triggers to map macros to the source port of the event. The most common triggers are based on Cisco Discovery Protocol (CDP) messages that are received from a connected device.

A CDP event trigger occurs when these devices are detected:

- Cisco switch
- Cisco router
- Cisco IP Phone

- Cisco Wireless Access Point, including autonomous and lightweight access points
- Cisco IP video surveillance camera

Additional event triggers for Cisco and third-party devices are user-defined MAC address groups, MAC authentication bypass (MAB) messages, IEEE 802.1x authentication messages, and Link Layer Discovery Protocol (LLDP) messages.

LLDP supports a set of attributes that are used to discover neighbor devices. These type, length, and value attributes and descriptions are referred to as TLVs. LLDP-supported devices use TLVs to receive and send information. This protocol advertises details such as device configuration information, capabilities, and identity. Auto Smartports uses the LLDP system capabilities TLV as the event trigger. You can use the event trigger control feature whether specify if the switch applies a macro based on the detection method, device type, or configured trigger.

For devices that do not support CDP, MAB, or 802.1x authentication, such as network printers, LLDP, or legacy Cisco Digital Media Players, you can configure a MAC address group with a MAC operationally unique identifier (OUI)-based trigger. You map the MAC address to a built-in or user-defined macro that has the desired configuration.

macro auto execute

To replace built-in macro default values and to configure mapping from an event trigger to a built-in or user-defined macro, use the **macro auto execute** command in global configuration mode.

macro auto execute *event trigger* {[***builtin*** *built-in macro name*]} [*parameter=value*]

Syntax Description

macro auto execute	Configures mapping from an event trigger to a built-in macro.
event trigger	Specifies the event trigger that is used for mapping an Auto Smartports macro to the source port of the event.
builtin	Defines mapping from an event trigger to a built-in macro.
built-in macro name	Specifies a built-in macro name.
parameter=value	Replaces default values for parameter values shown for the builtin-macro name. Enter new values in the form of a name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...].

Defaults

.This command has no default setting.

Command Modes

Global configuration

Usage Guidelines

Use the **macro auto execute** global configuration command to replace the built-in macro default values with values that are specific to your switch.

The switch automatically maps from event triggers to built-in macros. The built-in macros are system-defined macros in the software image. You can also create user-defined macros by using the Cisco IOS shell scripting capability.

Examples

This example shows how to use two built-in macros for connecting Cisco switches and Cisco IP phones to the switch.

Example 1

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#!!! the next command modifies the access and voice vlans
Switch(config)#!!! for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
```

Example 2

```
Switch(config)#
Switch(config)#!!! the next command maps the switch event to the built in Cisco switch
Switch(config)#!!! auto smartport macro
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
Switch(config)#
```

RADIUS Accounting Reports

The RADIUS_Accounting report has enhanced options to run the report for intervals of less than an hour. The Run button provides a list of short intervals starting with a minimum of a minute. This allows you to view accounting records at short intervals that are less than an hour so that you can view a fewer number of records depending on the interval.

You can choose the Query and Run option to run the RADIUS_Accounting report for every minute past and thereafter at other intervals including the past 5 minutes, 15 minutes, 30 minutes, one hour and so on. When you choose to run the report by using the Query and Run option from the Run button, you can view the **RADIUS_Accounting > Query and Run** page. This page displays the Time Range field, where you can choose intervals in minutes for time ranges that are less than an hour.

Excluding Static Endpoints in Advanced Licenses

In Cisco ISE, licensing enables you to provide coverage for increasing numbers of endpoints and to offer more complex policy services, depending on the capabilities of the license or licenses that you choose to apply. Cisco ISE licenses are available in Base, Advanced, and Wireless packages. Each package includes a number of SKUs that is equal to the number of licenses that are included in the package. To use Cisco ISE, you must have a valid Base, Base and Advanced, or Wireless license package

Cisco ISE licensing is based on the number (a count value) of concurrent endpoints across the entire deployment for both the Base, Advanced and Wireless licenses. This defines how Cisco ISE determines the number of endpoints that utilize the licenses against the number of endpoints that are defined in the current licensing scheme that you are using.

Cisco ISE implements a change where Cisco ISE cannot consume Advanced licenses when endpoints are statically assigned to a profile. The number of endpoints that are dynamically profiled, and the profile of those endpoints is used in an authorization policy can be compared only with the limit of the Advanced licenses.

The endpoints that are statically assigned to a profile are now excluded from utilizing licenses that are included in the Advanced license package, but they are still compared against the limit of Base licenses. Earlier, it compares the total number of concurrent endpoints across the entire deployment against the limit of the Advanced licenses.

For more information on how licenses are used in the Cisco ISE profiling service, see Licenses for the Profiling Service, page 18-4.

For more information on managing licenses in Cisco ISE, see Chapter 12, "Managing Licenses."

For more information on the license types that are available in the Cisco ISE licensing scheme, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.*

IP Address and MAC Address Binding in Cisco ISE

You can only create or update endpoints by using their MAC addresses in an enterprise network. If you do not find an entry in the ARP cache, then you can create or update endpoints by using the L2 MAC address of an HTTP packet and IN_SRC_MAC of a NetFlow packet in the Cisco ISE.

Earlier, the profiling service is dependent on L2 adjacency when endpoints are only a hop away. When endpoints are L2 adjacent, the IP addresses and MAC addresses of endpoints are already mapped, and there is no need for IP-MAC cache mapping. If endpoints are not L2 adjacent and are multiple hops away, there may not be a reliable mapping.

Some of the known attributes of NetFlow packets that you collect are PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC and OUT_SRC_MAC. When endpoints are not L2 adjacent and are multiple L3 hops away, the IN_SRC_MAC attributes carry only the MAC addresses of L3 network devices.

When the HTTP probe is enabled in Cisco ISE, you can only create endpoints by using the MAC addresses of HTTP packets, as the HTTP request messages do not carry IP addresses and MAC addresses of endpoints in the payload data.

The Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map IP addresses and MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry IP addresses and MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.

A network scan may or may not return the MAC addresses of endpoints. It uses an IP-MAC address binding for those endpoints from the IP addresses received.

Integrating Cisco ISE with Cisco Network Admission Control Appliance

Cisco ISE support integration with the Cisco Network Admission Control (NAC) Appliance Release 4.9. The integration support is compatible only with the Cisco NAC Appliance, Release 4.9 and available when you have installed an Advanced or Wireless license in Cisco ISE.

Integrating Cisco ISE with Cisco NAC Appliance, Release 4.9 allows you to utilize the Cisco ISE profiling service in a Cisco NAC deployment. The Cisco ISE profiler is similar to the Cisco Network Admission Control (NAC) Profiler in a Cisco NAC deployment, which manages endpoints in an enterprise network. This integration allows you to replace the existing Cisco NAC Profiler that is installed in a Cisco NAC deployment. It allows you to synchronize profile names from the Cisco ISE profiler, as well as the result of endpoint classification, into the Cisco Clean Access Manager (CAM).

Prerequisites:

You must have installed the Cisco NAC Appliance and performed initial configuration to introduce the Clean Access Manager (CAM) and Clean Access Server (CAS) into the network.

Note You must export the contents of X509 Certificate from the Clean Access Manager in Administration > Clean Access Manager > SSL, and import the same into the primary Administration ISE node in the Cisco ISE under Administration > System > Certificates > Certificate Trust Store for a proper secure communication between Cisco ISE and CAM.

For more information on installing Cisco NAC Appliance hardware, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9*. You must also use the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9* to install, configure and administer the Cisco NAC Appliance, Release 4.9.

Refer to the compatible set of documents for Cisco NAC Appliance, Release 4.9 in the following locations:

- http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html
- http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html
- http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html

For more information on configuring CAMs in Cisco ISE, see the Configuring Cisco Clean Access Managers in Cisco ISE, page 18-80.

Configuring Cisco Clean Access Managers in Cisco ISE

The primary Administration ISE node is responsible for all the communication between Cisco ISE and the Cisco NAC Appliance. You can have only one primary Administration ISE node in a distributed deployment, and it must assume the Administration persona. You can also have a maximum of two Administration ISE nodes that assume the Administration persona, one being the primary node and the other being the secondary node for high availability. This allows a failover support in a high-availability configuration of a Cisco ISE distributed deployment. There is no automatic failover for the Administration ISE nodes.

In a high-availability configuration, the primary Administration ISE node is in the active state, to which all configuration changes are made. The secondary Administration ISE node is in the standby state, to which all configuration changes are updated from the primary Administration ISE node. When the primary Administration ISE node goes down, you must log into the user interface of the secondary Administration ISE node and make it the primary node. Therefore, you always have a complete copy of the configuration from the primary Administration ISE node.

For more information, see Chapter 9, “Setting Up Cisco ISE in a Distributed Environment.”

You can configure CAMs only in the primary Administration ISE node in Cisco ISE. The credentials that are used at the time of registering one or more CAMs in the primary Administration ISE node are used to authenticate connectivity with CAMs.

The communication between Cisco ISE and the Cisco NAC Appliance is secure over Secure Sockets Layer (SSL). It is also bidirectional in nature, as Cisco ISE pushes the profiler configuration changes to CAMs, and CAMs periodically pull the list of MAC addresses of endpoints and their corresponding profiles, as well as the list of all the profile names, from Cisco ISE.

The Cisco ISE profiler notifies the profiler configuration changes to all the registered CAMs from the primary Administration ISE node. It avoids duplicating notification in a Cisco ISE distributed deployment. It uses the REST APIs to notify the profiler configuration changes when there are endpoints added or removed, and endpoint policies changed, in the Cisco ISE database. During an import of endpoints, the Cisco ISE profiler notifies CAMs only after the import is complete.

The following REST API flows are implemented to push the profiler configuration changes to CAMs:

- Cisco ISE profiler endpoint change push—When endpoints are profiled and there are changes in the profiles of endpoints in Cisco ISE, then the Cisco ISE profiler notifies all the registered CAMs about the changes in the endpoint profiles.

You can also configure Cisco ISE in CAMs, which allow you to synchronize CAMs with Cisco ISE, depending on your Sync Settings in CAMs. You must create rules, where you can select one or more matching profiles from the list of Cisco ISE profiles and map endpoints to any one of the Access Types in CAMs. CAMs periodically retrieve endpoints and their corresponding profiles, as well as the list of all the profile names, from the Cisco ISE profiler.

The following REST API flows are implemented to pull the profiler configuration changes from the Cisco ISE profiler:

- NAC Manager endpoint pull—Pulls the list of MAC addresses of endpoints and their corresponding profiles of known endpoints.
- NAC Manager profile pull—Pulls the profile names from the Cisco ISE profiler.

The Cisco ISE profiler notifies the Cisco ISE Monitoring persona of all the events that can be used to monitor and troubleshoot Cisco ISE and Cisco NAC Appliance Release 4.9 integration.

The Cisco ISE profiler log captures the following events for monitoring and troubleshooting integration:

- Configuration changes for NAC Settings (Information)
- NAC notification event failure (Error)

Filtering, Adding, Editing, and Deleting Clean Access Managers in Cisco ISE

Cisco ISE allows you to register multiple CAMs on a primary Administration ISE node in a distributed deployment for REST APIs communication settings. The list of CAMs that is registered in Cisco ISE is the list to which all the profiler configuration changes are notified. When registering CAMs in Cisco ISE, you must provide the IP addresses of CAMs, usernames, and passwords that allow you to log into the CAMs.

Note You can use the virtual service IP address that a pair of CAMs share in a high-availability configuration. This allows a failover support of CAMs in a high-availability configuration. For more information on how to set up a pair of CAMs for high availability, see the compatible link for Cisco NAC Appliance, Release 4.9.
http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/49/hi_ha.html#wp1084663.

The NAC Managers page allows you to configure multiple CAMs, which provides an option to filter the CAMs that you have registered. This page lists the CAMs along with their names, descriptions, IP addresses, and the status that displays whether endpoint notification is enabled or not for those CAMs.

The procedure for managing Cisco CAMs includes the following tasks:

- Filtering Cisco Clean Access Managers in Cisco ISE, page 18-82

- Adding Cisco Clean Access Managers to Cisco ISE, page 18-84
- Editing Cisco Clean Access Managers in Cisco ISE, page 18-84
- Deleting Cisco Clean Access Managers in Cisco ISE, page 18-85

Filtering Cisco Clean Access Managers in Cisco ISE

You can use the Show drop-down list, or click the filter icon both to invoke a quick filter and close it in the NAC Managers page. A quick filter is a simple filter that you can use to filter CAMs in the NAC Managers page. The quick filter filters CAMs based on field descriptions, such as the names, the descriptions, and IP addresses in the NAC Managers page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, in the NAC Managers page. The advanced filter filters CAMs based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter from the list has a session lifetime, which displays the results in the NAC Managers page. Once created and saved a preset filter, you can choose a preset filter of filtered results in the NAC Managers page. You can also edit preset filters and remove them from the preset filters list.

To filter CAMs in the NAC Managers page, complete the following steps:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears, which lists all the CAMs that are registered in Cisco ISE.

Step 2 In the NAC Managers page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-27.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 18-82 and the To filter by using the Advanced Filter option, complete the following steps:, page 18-83.

Note To return to the list of CAMs, choose **All** from the Show drop-down list to display all the CAMs without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters CAMs based on each field description in the NAC Managers page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results in the NAC Managers page. If you clear the field, it displays the list of all the CAMs in the NAC Managers page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the NAC Managers page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter CAMs by using variables that are more complex. It contains one or more filters, which filter CAMs based on the values that match the field descriptions. A filter on a single row filters CAMs based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter the CAMs by using any one or all of the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filter.

Step 5 Choose **All** to match the value in each filter, or choose **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or click **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 18-27 describes the fields that allow you to filter CAMs in the NAC Managers page.

Table 18-27 Filtering Clean Access Managers

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter CAMs by using the name of the CAM.
	IP Address	This field enables you to filter CAMs by using the IP address that is registered with Cisco ISE.
	Description	This field enables you to filter CAMs by using the description of the CAM.
Advanced Filter	Choose the field description from the following: • Name • IP Address • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter CAMs.
	Value	From the Value field, choose the value for the field description that you selected against, which the CAMs are filtered.

Adding Cisco Clean Access Managers to Cisco ISE

To add CAMs in the NAC Managers page, complete the following steps:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears.

Step 2 From the NAC Managers page, click **Add**.

Caution Once created and saved, the IP Address of the CAM is not editable.

The New NAC Manager page appears.

Step 3 Modify the values in the New NAC Manager page, as shown in Table 18-28.

Step 4 Click **Save**.

The Cisco Clean Access Manager that you configured appears in the NAC Managers page.

Step 5 Click the **NAC Manager List** link in the New NAC Manager page to return to the NAC Managers page.

Table 18-28 describes the fields in the New NAC Manager page that allow you to create a CAM.

Table 18-28 Adding NAC Managers

Field Name	Description
Name	In the Name, enter the name of the Cisco Access Manager (CAM).
Status	In the Status check box, click the check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	In the Description, enter the description of the CAM.
IP Address	In the IP Address, enter the IP address of the CAM. Once you have created and saved a CAM on Cisco ISE, the IP address of the CAM cannot be edited. You cannot use 0.0.0.0 and 255.255.255.255, as they are excluded when validating the IP addresses of the CAMs in Cisco ISE, and so, they are not valid IP addresses that you can use in the IP Address field for the CAM.
Username	In the Username, enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.
Password	In the Password, enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.

Editing Cisco Clean Access Managers in Cisco ISE

You can edit the details of CAMs from the NAC Managers page, except for the IP address of the CAM.

To edit a CAM in the NAC Managers page, complete the following:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears.

Step 2 From the NAC Managers page, choose a CAM.

Step 3 Click **Edit**.

Step 4 Modify the field values in the edit page, as shown in Table 18-28 on page 18-84.

Click the **NAC Manager List** link in the edit page to return to the NAC Managers page without saving the current input data. During an edit, you can also click the **Reset** without saving the current input data in the edit page. Here, you can retain the configuration without saving the current input data in the edit page.

Step 5 Click **Save** to save the current input data in the edit page.

Step 6 Click the **NAC Manager List** link from the edit page to return to the NAC Managers page after editing a CAM.

Deleting Cisco Clean Access Managers in Cisco ISE

You can delete a CAM from the NAC Managers page.

To delete a CAM in the NAC Managers page, complete the following:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears. From the NAC Managers page, choose a CAM.

Step 2 Choose **Delete**.

If you choose to delete a CAM from the NAC Managers page, Cisco ISE displays a confirmation dialog. Clicking **Delete** in the dialog deletes the CAM from the NAC Managers page. Clicking **Cancel** in the dialog returns to the NAC Managers page without deleting the CAM.