CHAPTER 17

Configuring Endpoint Profiling Policies

This chapter describes the profiler 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 profiler service in detail.

Note For information about configuring endpoints and endpoint identity groups, see Chapter 4, "Managing Identities and Admin Access."

Profiler Service in Cisco ISE

Cisco ISE profiler 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, in order 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 information on the profiler service in detail, see the "Understanding the Profiler Service" section on page 17-2.

The Profiler in Cisco ISE

The 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 the attributes and their attribute values that are collected from the endpoints to the analyzer.

  The probe manager within the sensor provides support to the profiler service, initializing and controlling various probes that run on the sensor. The probe manager allows you to configure probes to start and stop collecting the attributes and their values from the 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 to the endpoint identity groups and stores endpoints with the matched profiles in the database.
- An analyzer evaluates endpoints using the configured policies and the identity groups to match the attributes and their attribute values collected, which classifies endpoints to the specified group and stores endpoints with the matched profile in the Cisco ISE database.

Understanding the Profiler Service

The profiler service collects attributes of endpoints from the network devices and the network, classifies endpoints in 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. You must allow new attribute entries to the profiler dictionaries for profiling endpoints. All the attributes that are handled by the profiler 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 attach a varying set of attributes to endpoints based on their 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 information on endpoint profiling on Cisco ISE, see the "Endpoint Profiling" section on page 17-3.

For information on licenses that you need to install for the profiler service, see the "Licenses for the Profiler Service" section on page 17-3.

For information on how to deploy the profiler service, see the "Deploying the Profiler Service" section on page 17-4.

For information on Profiled Endpoints dashlet, see the "Profiled Endpoints Dashlet" section on page 17-6.

For information on endpoint profiling reports, see the "Viewing Profiler Reports" section on page 17-7.

Endpoint Profiling

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

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:

- Facilitating 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
- Identifying, locating, and determining the capabilities of all of the attached network endpoints regardless of endpoint types
- Protecting against inadvertently by denying access to some endpoints

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

In order 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 three endpoint identity groups: Blacklist, Profiled, and Unknown.

An endpoint profiling policy contains 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 policy.

A condition is a check that maps a specific value to an attribute at first 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. The certainty metric for each condition contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty metric for all the valid conditions 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.

An exception action is a configurable action, which you can define in an endpoint profiling policy that is triggered when the exception conditions associated to the endpoint profile match.

Licenses for the Profiler Service

Prerequisites:

Before you begin, you should have an understanding on how licenses restrict the usage of Cisco ISE profiler service with both the base and advanced license packages.

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 1.0*.

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

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 viewing on the Endpoint Identity Groups page. For more details, see Endpoints, page 4-14, and Endpoint Identity Groups, page 4-62 sections in Chapter 4, "Managing Identities and Admin Access."

To enable the profiler 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, Posture, Guest, Client Provisioning, and profiler services, depending on your configuration on the nodes.

Deploying the Profiler 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 profiler service either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). Depending on the type of your deployment and the license you have installed, the profiler 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.

The ISE distributed deployment includes support for the following:

- The Deployment Nodes page supports the infrastructure for the distributed nodes in the distributed deployment.
- A node specific configuration of probes—The Probe Config page allows you to configure the probe per node.
- Global Implementation of the profiler Change of Authorization (CoA).
- Configuration to allow syslogs to be sent to the appropriate profiler node.

Configuring the Profiler 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 profiler service for your Cisco ISE deployment.

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

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

The Deployment menu window appears on the left pane of the user interface. You can use the Table view button or the List view button to display the nodes in your Cisco ISE deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the right pane of the user interface.

Note To view the nodes in your deployment in a tree, click the **List** view button. An arrow appears in front of the Deployment menu. Click the arrow in front of the Deployment menu to view the nodes that are registered in your deployment in a tree view. The List view displays all the nodes in the Deployment menu window in a tree.

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

To deploy the profiler service, complete the following steps:

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

The Deployment menu window appears. You can use the Table view or the List view button to display the nodes in your deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the Deployment Nodes page of the user interface. 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 that are registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, apart from 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 on the node.

Step 5 Click the **Edit** button.

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. 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 on the node.

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

If you have the Policy Service check box unchecked, both the session services and the profiler 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 profiler service, check the **Enable Profiling Services** check box. To stop the Profiler service, uncheck the **Enable Profiling Services** check box.

Note The profiler 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 17-11 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 profiled endpoints dynamically for the last 24 hours period, as well as 60 minutes from the current system time. It refreshes data every minute and displays it on the dashlet. You can invoke the Endpoint Profiler Summary report from the tool tips that are displayed on the 24 hour and 60 minutes spark lines for a specific period. The stack bars display endpoints distribution details by Place in Network (PIN), matching endpoint profiles, and identity groups.

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

Table 17-1 describes the details, which are shown in the Profiled Endpoints dashlet on Cisco ISE.

Table 17-1 Profiled Endpoints Dashlet

Name	Description
Unique	A summary of unique endpoints profiled in Cisco ISE for the last 24 hours 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 in profiling endpoints.
Identity Group	
Endpoint Identity Group	Displays the 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 look into more details. You can also schedule reports (specially for large reports) and download it in various formats.

For more information on how to generate reports and work with the interactive viewer, see Chapter 23, "Reporting."

For more information on endpoint profiling reports, see "Standard Reports" section on page 17-7.

Standard Reports

For your convenience, the standard reports present a common set of predefined report definitions. You can click on the Report Name link to run the report for today. You can query the output by using various parameters, which are predefined in the system. 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 your reports that you use frequently to the Monitor > 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:

Monitor > Reports > Catalog > Endpoint.

The following are the standard reports for endpoint profiling:

- Endpoint MAC Authentication Summary—a report to 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 to view the profiler summary information for a particular MAC for a selected time period
- Top N Authentications By Endpoint Calling Station ID—a report to 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 Endpoint MAC Address—a report to view the top N passed/failed/total authentications count for RADIUS protocol with respect to MAC/MAB address for a selected time period
- Top N Authentications By Machine—a report to view the top N passed/failed/total authentications count for RADIUS protocol with respect to machine information for a selected time period

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 profiler 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 profiler 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 17-9.

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 Cisco recommends you to enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application. The profiler 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 profiler service to support a wider range of endpoints without requiring the support of the RADIUS probe.

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 profiler 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 profiler service implements the CoA in the following cases:

- Static assignment of an endpoint
- An exception action is configured
- An endpoint is profiled for the first time
- Endpoint deleted

Static Assignment of an Endpoint

The profiler service issues a CoA, if you have an existing endpoint successfully authenticated already on your network that is now statically assigned to a different profile or a different endpoint identity group and the endpoint profiling policy has changed.

An Exception Action is Configured

The profiler service issues a CoA for an endpoint, if you have an exception condition and an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint so that the profiler 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 17-42.

An Endpoint is Profiled for the First Time

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

An Endpoint is Deleted

The profiler 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.

For more information on CoA exemptions, see the "CoA Exemptions" section on page 17-9.

For more information on CoA configuration details, see Table 17-2.

CoA Exemptions

The implementation of CoA in Cisco ISE is described in the Change of Authorization section. For information on CoA, see the "Change of Authorization" section on page 17-7.

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

Authenticated Wired EAP-Capable Endpoint

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

Multiple Active Sessions per Port

The profiler 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 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 the Table 17-2.

Table 17-2 summarizes CoA for different environments for each CoA configuration in Cisco ISE.

Table 17-2 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.
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.

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**.

The Settings menu window appears. RSA Prompts

Step 2 From the Settings menu window, 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 Profiler Service to understand how the profiler 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 from 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 17-12.

You can reach the Deployment menu from the Administration mega menu. The Deployment menu window displays the registered nodes in your deployment. You can use the Table view or the List view button 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 From the Deployment menu window, choose 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, 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 on 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 the probe 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 on the node.

Step 4 Choose 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 profiler 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 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-17

Filtering Endpoint Attributes

Cisco ISE, when enabled with multiple probes per node, experiences a considerable performance degrading due to numerous attributes per endpoint 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 of the endpoint, which cannot be used for endpoint profiling, result in Cisco ISE administration node database persistence and performance degrading.

To address performance degrading of Cisco ISE, filters for RADIUS, DHCP for both the 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 unnecessary 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 the 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 in the endpoint cache for profiling.

A SNMP filter removes all the attributes that are irrelevant after the SNMP Query probe collects a large number of attributes.

The Cisco ISE Bootstrap log contains messages that deals 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.

Configuring the NetFlow Probe

Table 17-3 describes the fields that allow you to configure the NetFlow probe on the Edit Nodes page.

To enable the NetFlow probe, configure the following fields:

Table 17-3 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, as well as supports earlier versions that are beginning with version 5. The MAC address is not a part of IP flows in earlier versions of NetFlow, which 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, but 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 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	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
SRC_MAC	DST_MAC	SRC_VLAN
DST_VLAN	IP_PROTOCOL_VERSION	DIRECTION

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, but these endpoints must be discovered before 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:

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

Configuring the DHCP Probe

Table 17-4 describes the fields that allow you to configure the DHCP probe on the Edit Nodes page.

To enable the DHCP probe, configure the following fields:

Table 17-4 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 profiler 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 on 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 17-5 describes the different states of DHCP client messages. For more information on DHCP, refer to www.faqs.org/rafts/rfc2131.html.

Table 17-5 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 on the same subnet, you can configure the network access devices on your network by using the "IP helper-address" 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 profiler 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 Service Name (DNS) probe extracts the source IP address from the dhcp-requested-address attribute, which is collected by the DHCP

Configuring the DHCP SPAN Probe

Table 17-6 describes the fields that allow you to configure the DHCP SPAN probe on the Edit Nodes page.

To enable the DHCP SPAN probe, configure the following fields:

Table 17-6 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 profiler condition of DHCP type, where you can use the dhcp-requested-address attribute for profiling an endpoint. For a FQDN lookup, the Domain Service 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 17-7 describes the fields that allow you to configure the HTTP probe on the Edit Nodes page.

To enable the HTTP probe, configure the following fields:

Table 17-7 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 profiler 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 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 iPods, iPads and iPhones, 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 iPods, iPads and iPhones. Now, the Cisco ISE server listens to communication from the web browsers on both the port 80, as well as port 8080.

You can create a profiler condition of IP type, where you can use the IP attribute to capture the source IP address of the web browser. For a FQDN lookup, the Domain Service 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.

In order 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 17-8 describes the fields that allow you to configure the RADIUS probe on the Edit Nodes page.

To enable the RADIUS probe, configure the following fields:

Table 17-8 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 user name 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 can be used 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 profiler condition of RADIUS type, where you can use the Framed-IP-Address attribute for profiling an endpoint. For a FDDN look up, the Domain Service 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	Framed-IP-Address	Acct-Session-Time
NAS-IP-Address	Calling-Station-Id	Acct-Terminate-Cause
NAS-Port	Acct-Session-Id	

Configuring the DNS Probe

Table 17-9 describes the fields that allow you to configure the DNS probe on the Edit Nodes page.

To enable the DNS probe, configure the following fields:

Table 17-9 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 1.0.*

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 17-10 describes the fields that allow you to configure the SNMP Query probe on the Edit Nodes page.

To enable the SNMP Query probe, configure the following fields:

Table 17-10 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**.**

Table 17-10 SNMP Query Configuration

Field	Description
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 17-24.

Note When you configure SNMP settings on the network devices, you need to ensure in addition that Cisco Device Protocol (CDP) is enabled 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.

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.

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

In addition to configuring SNMP Query probe, you must also configure other SNMP settings in the following location:

Administration > Network Resources > Network Devices.

Configuring the SNMP Trap Probe

Table 17-11 describes the fields that allow you to configure the SNMP Trap probe in the Edit Nodes page.

To enable the SNMP TRAP probe, configure the following fields:

Table 17-11 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.

Table 17-11 SNMP Trap Configuration

Field	Description
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.

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. In order to make this feature to be 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 Enable **Link Trap Query**.

Step 10 Enable **MAC Trap Query**.

Step 11 Click **Summit**.

To configure the SNMP Trap, complete the following steps:

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

Step 2 Enable **Link Trap Query**.

Step 3 Enable **Mac Trap Query**.

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 systems, 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).

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 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—It is 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 simple (single) condition, or a set of conditions that are logically combined (a compound condition) against which you can categorize, and group endpoints in Cisco ISE. Cisco ISE always considers a chosen policy for an endpoint rather than an evaluated policy, which is the matched policy when the profiler conditions that are defined in the profiling policy are met for profiling the endpoint in the system.

If the profiler conditions 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. 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 condition in an endpoint profiling policy has a certainty metric (an integer value), or an exception action (a single configurable action) associated to it. The certainty metric is a measure that is added for all the valid policies, and the exception action is used to trigger the configurable action while evaluating 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 as a 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.

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 17-27
- Unknown Profile, page 17-27

- Profiling Statically Added Endpoint, page 17-27
- Profiling a Static IP Device, page 17-27

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 profiler service in Cisco ISE. For the statically added endpoint to be profiled, the profiler 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 profiler 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.

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

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

Related Topics

Configuring DACLs, page 16-32 section in Chapter 16, “Managing Authorization Policies and Profiles.”

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

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 endpoints like notebooks, workstations, printers, access points, IP phones, smart phones, iPods, iPads, and gaming consoles from Apple, Cisco, Avaya, Blackberry, HP, and Sony devices.

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

- Filtering Endpoint Policies, page 17-28
- Creating an Endpoint Profiling Policy, page 17-30
- Editing an Endpoint Profiling Policy, page 17-34
- Deleting an Endpoint Profiling Policy, page 17-34
- Duplicating an Endpoint Profiling Policy, page 17-35
- Exporting Endpoint Profiling Policies, page 17-36
- Importing Endpoint Profiling Policies, page 17-36

Filtering Endpoint Policies

A quick filter is a simple and quick filter that can be used to filter endpoint profiling policies on the Endpoint Policies page. It filters profiling policies based on the field descriptions, such as the endpoint policy name and description on the Endpoint Policies page.

An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results, on the Endpoint Policies page. It 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. Once created and saved, the Show drop-down lists all the preset filters. You can choose a preset filter and view the results on the Endpoint Policies page.

To filter the endpoint profiling policies, complete the following steps:

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

The Profiling menu appears.

Step 2 From the Profiling menu window, choose **Profiling Policies**.

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

Step 3 From the Endpoint Policies page, click the **>>** icon.

The Filter menu appears.

Step 4 Choose **Filter**.

The Quick Filter and Advanced Filter options appear. See Table 17-12.

Step 5 From the Filter menu, choose the filter option.

For more information, see the “To filter using the Quick Filter option, complete the following steps:” section on page 17-29 and “To filter using the Advanced Filter option, complete the following steps:” section on page 17-29.

Step 6 From the Show drop-down, choose a preset filter.

The preset filter displays the filtered results on the Endpoint Policies page.

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

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

A quick filter filters profiling policies based on each field description on 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 on the Endpoint Policies page. If you clear the field, it displays the list of all the profiling policies on the Endpoint policies page.

Step 1 To filter, click the **Go** button in each field.

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

To filter 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 view and choose the field description, click the drop-down arrow.

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

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

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button 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 Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 17-12 describes the fields that allow you to filter the endpoint profiling policies on the Endpoint Policies page.

Table 17-12 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.
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 can be used 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-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.

Warning **When you choose to create an endpoint profiling policy on 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**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears.

Step 3 From the Endpoint Policies page, choose **Create**.

Modify the values on the New Profiler Policy page, as shown in Table 17-13.

Step 4 Click **Submit.**

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

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

Table 17-13 describes the fields on the Endpoint Policies page that allow you to create an endpoint profiling policy.

Table 17-13 Creating an Endpoint Profiling Policy

Field Name	Description
Name	From the Name field, enter the name of the endpoint profiling policy that you want to create.
Description	From 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.
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 on 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.

Table 17-13 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
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.
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 profiler conditions from the library, and associate an integer value for the certainty factor for each condition, or associate an exception action for a 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.

Table 17-13 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Select Existing Condition from Library	If you choose, then you can define an expression by selecting pre-defined conditions from the policy elements library. Click the **Action Icon** button 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 the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete
Create New Condition (Advance Option)	If you choose, then you can define an expression by selecting attributes from various system or user-defined dictionaries. Click the **Action Icon** button 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 the **Action Icon** button 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 profiler condition: • Certainty Factor Increases • Take Exception Action

Table 17-13 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Value	If you select the Certainty Factor Increases option, then enter the certainty value for each condition, which can be added for all the valid policies with respect to the overall classification.
Action Icon	Click the **Action Icon** button 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-17

Editing an Endpoint Profiling Policy

You can choose an endpoint profiling policy on the Endpoint policies page to edit it from the Endpoint Policies page.

To edit a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Edit**.

Step 4 Modify the values of the fields on the edit page, as shown in Table 17-13 on page 17-31.

During an edit, you can click the **Reset** button without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data on 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 on 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 on 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 on the Endpoint Policies page.

When you select all the endpoint policies and try to delete them on 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 on 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**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From 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** from the dialog deletes the policy from the Endpoint Policies page. Clicking **Cancel** from 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-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**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Duplicate**.

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

Troubleshooting Topics

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

Exporting Endpoint Profiling Policies

You can choose endpoint profiling policies on 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** (menu window).

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. Choose the profiling policy that you want to export.

Step 3 Choose **Export**.

The Opening profiler_policies.xml dialog appears. This is a file in XML format that you can open in a web browser, or in other appropriate applications. You can 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-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** (menu window).

Step 2 From the Profiling Policies menu window, choose **Profiling Policies.**

The Endpoint Policies page appears.

Step 3 Choose **Import**.

Step 4 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 5 Click **Submit**.

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

Step 6 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 C-5
- Cannot Authenticate on Profiled Endpoint, page C-17

Endpoint Profiling

A profiler 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 window from the Profiling menu to display and manage Cisco ISE profiler conditions.

The procedures for managing profiling conditions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiler Condition

Related Topics

- Profiling Exception Actions, page 17-42
- Endpoint Profiling Policies, page 17-25

Troubleshooting Topics

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

Filtering, Creating, Editing, and Deleting a Profiler Condition

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

The procedures for managing profiling conditions include the following tasks:

- Filtering Conditions, page 17-38
- Creating a Profiler Condition, page 17-40
- Editing a Profiler Condition, page 17-41
- Deleting a Profiler condition, page 17-42

Filtering Conditions

A quick filter is a simple and quick filter that can be used to filter profiler conditions on the Conditions page. It filters conditions based on the field descriptions, such as the name of the profiler check, description, and the expression that is used in the condition on the Conditions page.

An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results, on the Conditions page. It filters conditions 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. Once created and saved, the Show drop-down lists all the preset filters. You can choose a preset filter and view the results on the Conditions page.

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

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 Choose **Profiling**.

The Conditions page appears.

Step 3 From the Conditions page, choose **Filter**.

Step 4 Click the drop-down arrow to list the filter options.

The Quick Filter and Advanced Filter options appear. See Table 17-14.

Step 5 From the Filter menu, choose the filter option.

For more information, see the "To filter using the Quick Filter option, complete the following steps:" section on page 17-38 and "To filter using the Advanced Filter option, complete the following steps:" section on page 17-39.

Step 6 From the Show drop-down, choose a preset filter.

The preset filter displays the filtered results on the Conditions page.

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

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

A quick filter filters profiler conditions based on each field description on 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 on the Conditions page. If you clear the field, it displays the list of all the conditions on the Conditions page.

Step 1 To filter, click the **Go** button in each field.

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

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

An advanced filter enables you to filter profiler 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 view and choose the field description, click the drop-down arrow.

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

Step 3 Enter the value for the field description selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button 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 Preset Filter dialog appears. Enter a file name to save the filter and click **Save**. or **Cancel** to clear the filter.

Table 17-14 describes the fields on the Conditions page that allow you to filter the profiler conditions.

Table 17-14 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 profiler check (condition).
	Expression	This field enables you to filter conditions by an attribute and its attribute value within the profiler check.
	Description	This field enables you to filter conditions by the description of the profiler 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 can be used to filter profiler conditions.
	Value	From the Value field, choose the value for the field description that you selected against which the profiler conditions are filtered.

Creating a Profiler Condition

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

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling** (menu window).

The Conditions page appears.

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

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

Step 3 Modify the values on the New Profiler Condition page, as shown in Table 17-15.

Step 4 Click **Submit**.

The profiler condition that you create appears on the Conditions page.

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

Table 17-15 describes the fields on the Conditions page that allow you to create a profiler condition:

Table 17-15 Creating a Profiler Condition

Field Name	Description
Name	From the Name field, enter the name of the profiler condition that you want to create.
Description	From the Description field, enter the description of the profiler condition that you want to create.
Type	From the Type field, click the drop-down arrow to view the following predefined profiler conditions types: • DHCP • MAC • SNMP • IP • RADIUS • Netflow 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.

Table 17-15 Creating a Profiler Condition

Field Name	Description
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 Profiler Condition

You can edit a profiler 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** (menu window).

The Conditions page appears. From the Conditions page, choose a profiler condition.

Step 2 Choose **Edit**.

Step 3 Modify the values of the fields on the edit page, as shown in Table 17-15 on page 17-40.

During an edit, you can click **Reset** button without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data on 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 4 Click **Save** to save the current input data on the edit page.

Step 5 Click the **Profiler Condition List** link from the edit page to return to the Conditions page after editing a profiler condition.

Deleting a Profiler condition

You can delete a profiler 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** (menu window).

The Conditions page appears. From the Conditions page, choose a profiler condition.

Step 2 Choose **Delete**.

If you choose to delete a profiler condition from the Conditions page, Cisco ISE displays a confirmation dialog. Clicking **OK** from the dialog deletes the condition from the Conditions page. Clicking **Cancel** from the dialog returns to the Conditions page without deleting the profiler 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 > Results** (menu window).

Step 2 Choose **Profiling**.

Step 3 Click the right navigation arrow to go to the profiling menu window.

Step 4 From the Profiling menu, choose **Exceptions Actions**.

Here, you can create editable exception actions as well as non-editable exception actions, which can be used for profiling endpoints on a Cisco ISE network.

Profiling Exception Actions

An exception action is a single configurable action, which 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 profiler 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 on 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 Profiler Exception Action, page 17-43

Related Topics

Endpoint Profiling Policies, page 17-25

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

The 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 description.

The procedures for managing exception actions include the following tasks:

- Filtering Exception Actions, page 17-43
- Creating an Exception Action, page 17-45
- Editing an Exception Action, page 17-46
- Deleting an Exception Action, page 17-46

Filtering Exception Actions

A quick filter is a simple and quick filter that can be used to filter profiler exception actions on the Actions page. It filters exception actions based on the field descriptions, such as the name of the profiler exception action and description on the Actions page.

An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results, on the Actions page. It filters exception actions 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. Once created and saved, the Show drop-down lists all the preset filters. You can choose a preset filter and view the results on the Actions page.

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

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Results** (menu window).

Step 2 Choose **Profiling**.

Step 3 Click the right navigation arrow to go to the profiling menu window.

Step 4 From the Profiling menu, choose **Exceptions Actions**.

The Actions page appears.

Step 5 From the Actions page, choose **Filter**.

Step 6 Click the drop-down arrow to list the filter options.

The Quick Filter and Advanced Filter options appear. See Table 17-16.

Step 7 From the Filter menu, choose the filter option.

For more information, see the "To filter using the Quick Filter option, complete the following steps:" section on page 17-44 and "To filter using the Advanced Filter option, complete the following steps:" section on page 17-44.

Step 8 From the Show drop-down, choose a preset filter.

The preset filter displays the filtered results on the Actions page.

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

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

A quick filter filters profiler exception actions based on each field description on the 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 on the Actions page. If you clear the field, it displays the list of all the exception actions on the Actions page.

Step 1 To filter, click the **Go** button in each field.

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

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

An advanced filter enables you to filter profiler 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 view and choose the field description, click the drop-down arrow.

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

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

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button 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 Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 17-16 describes the fields on the Actions page that allow you to filter exception actions.

Table 17-16 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 profiler exception action.
	Description	This field enables you to filter exception actions by the description of the profiler 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 can be used 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 on the Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Actions page appears.

Step 4 From the Actions page, click **Create**.

Step 5 Modify the values on the New Profiler Exception Action page, as shown in Table 17-17

Step 6 Click **Submit**.

The exception action that you create appears on the Actions page.

Table 17-17 describes the fields on the Actions page that allow you to create an exception action:

Table 17-17 Creating an Exception Action

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

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

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Actions page appears. From the Actions page, choose an exception action.

Step 4 Choose **Edit**.

Step 5 Modify the values of the fields on the edit page, as shown in Table 17-17 on page 17-46.

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

Step 6 Click **Save** to save the current input data on the edit page.

Step 7 Click the **Profiler Exception Action List** link from the edit page to return to the Actions page after editing an exception action.

Deleting an Exception Action

You can delete an exception action from the Actions page.

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

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Actions page appears. From the Actions page, choose an exception action.

Step 4 Choose **Delete**.

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